

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

**Μεταπτυχιακό Πρόγραμμα Σπουδών
Πληροφοριακά και Επικοινωνιακά Συστήματα**

Μεταπτυχιακή Διατριβή



**Εισαγωγή Κινητικότητας στο Πρότυπο WirelessHART
Introduction of Mobility in the WirelessHART Standard**

Νικόλαος Παναγιωτόπουλος

**Επιβλέπων Καθηγητής
Βάσος Βασιλείου**

Σεπτέμβριος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών.

Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

**Εισαγωγή Κινητικότητας στο Πρότυπο WirelessHART
Introduction of Mobility in the WirelessHART Standard**

Νικόλαος Παναγιωτόπουλος

**Επιβλέπων Καθηγητής
Βάσος Βασιλείου**

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Σεπτέμβριος 2015

Η σελίδα αυτή είναι σκόπιμα λευκή

Περίληψη

Τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται σε βιομηχανικές εφαρμογές, για παρακολούθηση και έλεγχο στις βιομηχανίες διεργασιών, όπως είναι εργοστάσια, διυλιστήρια, πλατφόρμες εξόρυξης πετρελαίου, χημικές βιομηχανίες, βιομηχανικές αποθήκες, πετροχημικά. Το πρότυπο WirelessHART, επιτρέπει την ενδο-βιομηχανική επικοινωνία και αποτελεί εξέλιξη του παλαιότερου ενσύρματου προτύπου HART (Highway Addressable Remote Transducer Protocol). Το WirelessHART, παρέχει τη δυνατότητα ασύρματης τεχνολογίας, η οποία είναι πιο ευέλικτη, με χαμηλό κόστος, χωρίς να έχει τους περιορισμούς των καλωδίων.

Ένα ασύρματο δίκτυο αισθητήρων (WSN Wireless Sensor Network), γενικά, αποτελείται από ένα πλήθος ασύρματων συσκευών αισθητήρων, χαμηλού κόστους, διασκορπισμένων σε μια περιοχή, που ονομάζεται «πεδίο». Στις βιομηχανικές εγκαταστάσεις, οι αισθητήρες συνήθως είναι ενσωματωμένοι σε έξυπνα όργανα μέτρησης που χρησιμοποιούνται για παρακολούθηση φυσικών μεγεθών, όπως είναι η θερμοκρασία, η πίεση, η σύνθεση αερίων, η ροή ρευστών, το ιξώδες ή άλλες μεταβλητές περιβάλλοντος, ενώ οι τιμές των μετρήσεων, αποθηκεύονται τοπικά στη μνήμη των έξυπνων οργάνων. Τα όργανα αυτά, λέγονται «συσκευές πεδίου» και σχηματίζουν ένα ασύρματο δίκτυο αισθητήρων σε τοπολογία πλέγματος (mesh). Τα δεδομένα μετρήσεων, συγκεντρώνονται από τους αισθητήρες και προωθούνται, μέσω του ασύρματου δικτύου WirelessHART, σε μία κεντρική συσκευή ελέγχου, που ονομάζεται Πύλη (gateway) και έχει το ρόλο της κύριας συσκευής (master), ενώ οι συσκευές πεδίου είναι οι εξαρτώμενες συσκευές (slaves). Μέσω της Πύλης, τα δεδομένα μπορούν να αποσταλούν και σε άλλα δίκτυα της βιομηχανικής εγκατάστασης, για περισσότερη επεξεργασία και αξιοποίηση τους.

Σε αυτή την εργασία, παρουσιάζεται μία γενική θεώρηση των τεχνολογιών HART και WirelessHART, καθώς επίσης παρουσιάζονται και άλλα θέματα, σχετικά με τα ασύρματα δίκτυα αισθητήρων. Επειδή στο πρότυπο WirelessHART οι κόμβοι είναι στατικοί, εξετάζεται η πιθανότητα ενσωμάτωσης κινητών κόμβων. Η εισαγωγή κινητικότητας παρουσιάζει προκλήσεις, όπως είναι η εξάντληση της ενέργειας των κόμβων και η καθυστέρηση μετάδοσης δεδομένων από τους κόμβους αισθητήρες στην Πύλη. Θεωρήσαμε ένα πιθανό σενάριο εφαρμογής δύο δικτύων WirelessHART σε ένα διυλιστήριο, για να εξεταστεί η δυνατότητα να ενσωματωθούν οι κινητοί κόμβοι αισθητήρες στους εργάτες που κινούνται στο χώρο 2 δεξαμενών του διυλιστηρίου, όπου υπάρχουν επικίνδυνα αέρια και τοξικές ουσίες, ώστε αν κινδυνέψει ένας εργάτης, να ενεργοποιηθούν κατάλληλοι συναγερμοί ασφαλείας.

Τα αποτελέσματα δείχνουν ότι υπάρχουν ακόμη περιθώρια βελτιώσεων, μέχρι να φτάσουμε στον τελικό στόχο.

Summary

Wireless Sensor Networks (WSN) are deployed in industrial applications, for monitoring and control in Process Industries, such as factories, refineries, oil drilling platforms, chemical plants, industrial warehouses, petrochemicals. WirelessHART standard, allows intra-industrial communications, and is an evolution of the older wired HART (Highway Addressable Remote Transducer Protocol). WirelessHART is enabling wireless technology, which is more flexible, low cost, without constraints of cables.

A Wireless Sensor Network (WSN), in general, consists of a number of low cost wireless sensor devices, dispersed in an area, which is called “field”. In industrial plants, sensors are usually embedded in the smart instruments, deployed for monitoring physical quantities, such as temperature, pressure, gas composition, fluids’ flow, viscosity or other environmental variables, and the measurement values are stored locally, in the memory of the smart instruments. These smart instruments are called “field devices”, and form a wireless sensor network, in mesh topology. Measurement data, are collected from sensors, and forwarded via the WirelessHART network, to a central controller device, called a “Gateway”, which is the master device, while field devices are the slave devices. Through the Gateway, data can be sent to other industrial plant networks, for further processing and recovery.

In this thesis, an overview of HART and WirelessHART standards is presented, as well as other issues related to wireless sensor networks.

Since nodes are static in WirelessHART standard, we consider the possibility of incorporating mobile nodes. Introduction of mobility has challenges, such as depletion of nodal energy, and data transmission delay while sending sensor data to the Gateway.

We considered a possible application scenario, of deploying two WirelessHART networks into a refinery, to examine the possibility to integrate mobile sensor nodes to workers who move between 2 tanks in a tank area of a refinery, where hazardous gases and toxic substances exist, so, if a worker is in danger, the proper security alarms should be activated.

The results show that there is still room for improvement, until we reach the ultimate goal.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα της Μεταπτυχιακής Διατριβής, κ. Βάσο Βασιλείου για την συνεχή καθοδήγηση του, καθώς και για την στήριξη του σε όλη την διάρκεια αυτής της προσπάθειας, αλλά και για την πολύπλευρη ενημέρωση που προσέφερε σε κρίσιμα θέματα, απαραίτητα για να ολοκληρωθεί η παρούσα Μεταπτυχιακή Διατριβή. Οι πολύτιμες συμβουλές του και οι υποδείξεις του, μαζί με την ευρεία γνώση και πείρα που είχε αποκομίσει, από μελέτες και εγκαταστάσεις διάφορων συστημάτων, αποτέλεσαν πολύ σημαντικές πηγές έμπνευσης που διαφώτισαν τον τρόπο σκέψης μου και συνέβαλλαν ουσιαστικά στην διεκπεραίωση της παρούσης Μεταπτυχιακής Διατριβής.

Θερμές ευχαριστίες θα ήθελα να εκφράσω και προς όλους τους Καθηγητές του Ανοικτού Πανεπιστημίου Κύπρου, για την ποιοτική και οργανωμένη εκπαίδευση που μας προσέφεραν, σε όλα τα προηγούμενα έτη σπουδών, με βάση τις επιστημονικές τους γνώσεις και την εξειδικευμένη εμπειρία τους, ώστε μας οδήγησαν σε μία εποικοδομητική πορεία απόκτησης πολύτιμων γνώσεων που απαιτούνται για την επαγγελματική μας ανάπτυξη.

Απεριόριστη ευγνωμοσύνη θέλω να εκφράσω και προς τους γονείς μου, οι οποίοι με στήριξαν και συμπαράστηκαν στην εκπαίδευσή μου, ενισχύοντας διαρκώς την προσπάθειά μου να ολοκληρώσω τις σπουδές μου στο Ανοικτό Πανεπιστήμιο Κύπρου.

στην Μητέρα του Θεού, Παναγία,

που γιορτάζει στις 15 Αυγούστου.

N. Π.

Περιεχόμενα

Ανοικτό Πανεπιστήμιο Κύπρου	i
Περίληψη	iv
Περιεχόμενα.....	vii
Ευρετήριο Εικόνων	xii
Εισαγωγή	1
1.1 Γενικά.....	2
1.1.1 Βελτιώσεις στην Κεντρική Διαχείριση.....	3
1.1.2 Περιορισμοί στην Ενέργεια των Συσκευών.....	4
1.1.3 Ασύρματα Δίκτυα Αισθητήρων σε Βιομηχανικό περιβάλλον	6
1.2 Πρόβλημα	8
1.2.1 Η Δική μας Πρόταση.....	9
1.3 Μεθοδολογία.....	11
1.4 Δομή Διατριβής	13
1.4.1 Η Δομή του κεφαλαίου: Ασύρματα Δίκτυα Αισθητήρων.....	13
1.4.2 Η Δομή του Κεφαλαίου: Δίκτυα για Βιομηχανικές Εφαρμογές.....	13
1.4.3 Η Δομή του Κεφαλαίου: Κινητικότητα στα Ασύρματα Δίκτυα Αισθητήρων	14
1.4.4 Η Δομή του Κεφαλαίου: η Δική μας Πρόταση	14
1.4.5 Η Δομή του Κεφαλαίου: Συμπεράσματα και Μελλοντική Εργασία.....	15
1.4.6 Η Δομή για το Παράρτημα Α.....	15
Ασύρματα Δίκτυα Αισθητήρων.....	16
2.1 Γενικά για τα ασύρματα δίκτυα αισθητήρων (WSN)	16
2.1.1 Χαρακτηριστικά των ασύρματων δικτύων αισθητήρων	18
2.1.2 Πλεονεκτήματα και μειονεκτήματα των ασύρματων δικτύων αισθητήρων.....	34
2.1.3 Επιπλέον ζητήματα των ασύρματων δικτύων αισθητήρων	35
2.1.4 Εφαρμογές	37
2.2 Στρώματα.....	44
2.2.1 Τα επίπεδα του μοντέλου OSI-7	44
2.2.2 Στρώματα του ασύρματου δικτύου αισθητήρων WSN.....	46
2.2.3 Τα Ασύρματα Δίκτυα Αισθητήρων διαφέρουν από τα ασύρματα δίκτυα υπολογιστών Ad Hoc	52
2.3 Το πρότυπο IEEE 802.15.4.....	56
2.3.1 Τύποι συσκευών στο πρότυπο IEEE 802.15.4	56

2.3.2 Τοπολογία	59
2.3.3 Διευθύνσεις.....	63
2.3.4 Συχνότητες λειτουργίας	64
2.3.5 Το φυσικό επίπεδο (PHY Layer) για το IEEE 802.15.4.....	67
2.3.5.1 Η δομή του πακέτου δεδομένων (packet structure) φυσικού στρώματος	71
2.3.6 Το στρώμα MAC (υποεπίπεδο πρόσβασης μέσου) στο IEEE 802.15.4.....	71
2.3.6.1 Γενική δομή πλαισίων δεδομένων (frame structure) στρώματος MAC.....	74
2.3.6.2 Data frame (Πλαίσιο δεδομένων)	76
2.3.6.3 Beacon frame (Πλαίσιο σήματος Beacon)	77
2.3.6.4 Acknowledgement frame (πλαίσιο αναγνώρισης ή πλαίσιο επιβεβαίωσης λήψης πακέτου).....	79
2.3.6.5 MAC command frame (πλαίσιο εντολών MAC).....	79
2.3.7 Γενικές λειτουργίες (General Functions).....	82
2.3.8 Χαρακτηριστικά ασφάλειας του IEEE 802.15.4.....	87
2.4 TDMA	89
2.4.1 Χαρακτηριστικά του TDMA	89
2.4.2 Το TDMA στο δίκτυο WirelessHART.....	94
2.4.3 Ο Συγχρονισμός σε διαφορετικά συστήματα από το WirelessHART	96
2.4.4. Ο συγχρονισμός στο δίκτυο WirelessHart.....	97
Δίκτυα για.....	104
3.1 Το πρωτόκολλο HART	105
3.1.1 HART γενικά στοιχεία	106
3.1.2 Τα επίπεδα του μοντέλου OSI και η σύγκριση τους με το HART.....	108
3.1.3 Χαρακτηριστικά του δικτύου HART.....	116
3.1.4 Πακέτο δεδομένων του HART.....	127
3.2 WirelessHART	132
3.2.1 Σύντομη περιγραφή χαρακτηριστικών δικτύου WirelessHART	133
3.2.2 Αναλυτική περιγραφή για τις δικτυακές συσκευές (Network Devices).....	148
3.2.3 Τα αρχεία EDD files σε γλώσσα EDDL	167
3.2.4 Η συσκευή δρομολογητής (Router Device).....	171
3.2.5 Αναλυτική περιγραφή του Adaptor ή Adapter: Προσαρμογέας WirelessHART	171
3.2.6 Αναλυτική περιγραφή των Συσκευών χειρός (Handheld Communicators)	177
3.2.7 Αναλυτική περιγραφή για την Πύλη (Gateway)(GW) και το σημείο πρόσβασης (Access Point) (AP).....	179
3.2.8 Αναλυτική περιγραφή για τον Φιλοξενητή (Host).....	189

3.2.9 Αναλυτική περιγραφή του Διαχειριστή δικτύου (Network Manager) (NM) και του διαχειριστή ασφάλειας (Security Manager) (SM).....	192
3.2.10 Συγχρονισμός Επικοινωνίας με βάση τις σχισμές χρόνου (time slots)	197
3.2.11 Τα στρώματα του πρωτοκόλλου WirelessHART	211
3.2.12 Το MAC υπό-επίπεδο ελέγχου πρόσβασης μέσου (Media Access Control)	238
3.2.13 Πίνακες επικοινωνίας (Communication Tables) και ενδιάμεσες μνήμες απομόνωσης (Buffers)	240
3.2.14 Επίπεδο Δικτύου (Network Layer) και Επίπεδο Μεταφοράς (Transport Layer)	241
3.2.15 Το πακέτο δεδομένων TPDU στο επίπεδο μεταφοράς (Transport Layer)	262
3.2.16 Το επίπεδο εφαρμογών (Application Layer).....	265
3.2.17 Δυναμικές μεταβλητές (Dynamic Variables) και μεταβλητές συσκευών (Device Variables).	277
3.3 Το πρωτόκολλο GinMAC.....	279
3.3.1 Βασικά χαρακτηριστικά του GinMAC.....	280
3.3.2 Αποκλειστικό TDMA (Exclusive TDMA)	282
3.3.3 Δομή δέντρου.....	284
3.3.4 Προσαρμογή της καθυστέρησης (delay conform) για έλεγχο της αξιοπιστίας.....	285
3.3.5 Ρυθμός λήψης πακέτων Packet Reception Rate (PRR)	285
3.3.6 Σφάλματα καταιγισμού (burst errors)	286
3.4 ISA 100.11a Γενικά	288
3.4.1 Περιγραφή του ISA 100.11a	289
3.4.2 Στρώματα (layers) στο δίκτυο ISA100.11a.....	296
3.4.3 Σύγκριση των πρωτοκόλλων επικοινωνίας.....	301
Κινητικότητα στα	319
4.1 Γενικά.....	319
4.2 Είδη Κινητικότητας.....	321
4.2.1 Επίπεδα αρχιτεκτονικής	324
4.2.2 Βασικά προβλήματα	327
4.2.3. Μοντέλα κινητικότητας.....	331
4.3 Κινητικότητα στο Επίπεδο DLL (Στρώμα MAC)	359
4.3.1 Διάφορα είδη πρωτοκόλλων MAC	360
4.3.2 Η Επέκταση στο S-MAC για Εισαγωγή Κινητικότητας.....	393
Η Δική μας Πρόταση	399
5.1 Η δική μας πρόταση.....	400

5.1.1 Αρχικές θεωρητικές εκτιμήσεις και ερωτήματα	402
5.1.2 Σενάριο κινητικότητας στο χώρο δεξαμενών διυλιστηρίου, για καθαρισμό, στο οποίο βασίστηκε η δική μας λύση	412
Συμπεράσματα και Μελλοντική	426
6.1 Συμπεράσματα.....	426
6.1.1 Το WirelessHART είναι πλήρως συμβατό με το παλαιότερο πρότυπο HART.	426
6.1.2 Το WirelessHART είναι απλή και ανθεκτική τεχνολογία για δίκτυα πλέγματος (mesh).....	428
6.1.3 Το WirelessHART έχει σχεδιαστεί με στόχο την διαλειτουργικότητα.....	428
6.1.4 Οι συσκευές WirelessHART υποστηρίζουν τη γλώσσα DDL.....	428
6.1.5 Η επικοινωνία στο δίκτυο WirelessHART βασίζεται στο TDMA με superframes	429
6.1.6 Το WirelessHART δημιουργεί δύο διαφορετικούς τύπους ζεύξεων	429
6.1.7. Δεδομένα κυκλικά και Δεδομένα ακυκλικά.....	430
6.1.8 Το WirelessHART υποστηρίζει πολλαπλές λειτουργίες μηνυμάτων.....	431
6.1.9 Τα στρώματα στο WirelessHART δημιουργήθηκαν ως μία επέκταση των στρωμάτων του HART	433
6.1.10 Το WirelessHART είναι κατάλληλο εφαρμογές και σε μεγάλες βιομηχανικές εγκαταστάσεις και σε μικρότερες εγκαταστάσεις	433
6.1.11 Το WirelessHART υποστηρίζει τη συνύπαρξη με άλλα ασύρματα δίκτυα	434
6.2 Μελλοντική Εργασία	437
6.2.1. Επιτήρηση κατά μήκος ενός αγωγού Διυλιστηρίου πετρελαίου.....	437
6.2.2. Αποθήκη.....	439
6.2.3 Εργοστάσιο παραγωγής αυτοκινήτων	440
6.2.4 Βιομηχανία χαρτοποιίας	440
6.2.5 Βιομηχανία με αγωγούς μεταφοράς πετρελαίου	441
6.2.6 Βιομηχανία με Πετροχημικά.....	442
6.2.7 Βιομηχανία Κατασκευής Υαλικών και πιάτων.....	443
6.2.8 Βιομηχανία δημιουργίας αντισεισμικών υλικών και πρόσθετων υλικών που χρησιμοποιούνται στην παραγωγή πλαστικών	443
6.2.9 Βιομηχανία επεξεργασίας και μεταφοράς με αγωγούς νερού και λυμάτων	444
6.2.10 Βιομηχανία επεξεργασίας ξυλείας, αγωγός που μεταφέρει πριονίδι.....	445
Βιβλιογραφία	447
Παράρτημα Α.....	1
A.1 Τοπολογία Αστέρα.....	1
A.2 Τοπολογία peer to peer	1

A.3	Τοπολογία Δικτύου Πλέγματος (Mesh)	2
A.4	Τοπολογία Δέντρου Συστοιχιών	2
A.5	Τοπολογία συστοιχιών με μορφή αστέρα	3
A.6	Τοπολογία υβριδική αστέρα πλέγματος.....	4
A.7	Μορφές Δρομολόγησης	5
A.8	Διαμορφώσεις σήματος σε ασύρματες επικοινωνίες.....	6
A.8.1	TDMA	6
A.8.2	CDMA	6
A.8.4	CSMA	8
A.8.5	Διαμοιρασμός ενός καναλιού σε πολλούς κόμβους	13

Ευρετήριο Εικόνων

Εικόνα 1 Τοπολογίες δικτύων που αποτελούνται από κόμβους αισθητήρες (sensor nodes).....	18
Εικόνα 2. Ένα σχεδιάγραμμα για το υλικό (hardware) ενός κόμβου αισθητήρα. Διακρίνονται τέσσερα υποσυστήματα: α) αισθητήρων, β) επεξεργαστή, γ) επικοινωνίας, δ) τροφοδοσίας ενέργειας. Πηγή: [5]....	20
Εικόνα 3. Ο κόμβος αισθητήρας AquisGrain, Πάνω: η μία όψη, κάτω η άλλη όψη. Πηγή: [6]	22
Εικόνα 4 . Ο κόμβος αισθητήρας WiSense. Αριστερά : η μία όψη, δεξιά η άλλη όψη. Πηγή: Wisense (https://wisense.wordpress.com/).....	22
Εικόνα 5. Ένα άλλο σχεδιάγραμμα για το υλικό (hardware) ενός κόμβου αισθητήρα. Πηγή [5].....	26
Εικόνα 6 Διαφορετικά είδη κόμβων αισθητήρων (moten) από διαφορετικούς κατασκευαστές, που έχουν χρησιμοποιηθεί σε προηγούμενα έτη, στα ασύρματα δίκτυα αισθητήρων.....	29
Εικόνα 7 Το στρώμα Data Link Layer αποτελείται από τα υποπεπίεδα LLC και MAC. Πηγή: [1].....	45
Εικόνα 8 Στοιβά στρωμάτων για τα ασύρματα δίκτυα αισθητήρων (WSN) και διαφορά από το μοντέλο OSI 7	47
Εικόνα 9 Σύγκριση του μοντέλου Στρωμάτων OSI 7 και του μοντέλου στρωμάτων για το WirelessHART. Πηγή: [7, p. 31].....	54
Εικόνα 10 Τοπολογία Αστέρα.....	60
Εικόνα 11 Τοπολογία peer to peer.	61
Εικόνα 12 Τοπολογία Δικτύου Πλέγματος.....	62
Εικόνα 13. Τοπολογία δέντρου συστοιχιών (cluster tree)	63
Εικόνα 14 Το στρώμα MAC και το φυσικό στρώμα PHY στο πρότυπο IEEE 802.15.4. Το Φυσικό επίπεδο χωρίζεται σε 2 τμήματα.....	64
Εικόνα 15. Τα κανάλια από 0 ως 10 στις συχνότητες του IEEE 802.15.4.....	65
Εικόνα 16. Τα κανάλια από 11 ως 26 στις συχνότητες του IEEE 802.15.4.....	65
Εικόνα 17. Η δομή του πακέτου δεδομένων IEEE 802.15.4 για το φυσικό στρώμα.....	71
Εικόνα 18. Η γενική δομή του πλαισίου δεδομένων IEEE 802.15.4 για το στρώμα MAC.	74
Εικόνα 19. Ένα παράδειγμα της δομής του υπερπλαισίου (Superframe Structure).....	83
Εικόνα 20 Το υπερπλαίσιο με τις περιόδους CAP και CFP Πηγή: [10].....	85
Εικόνα 21 Η χρονική περίοδος χωρίς συγκρούσεις CFP μπορεί να στεγάσει (accommodate) μέχρι 7 εγγυημένες σχισμές χρόνου GTSS.....	86
Εικόνα 22 Οι σχισμές χρόνου (slots) σε ένα πλαίσιο (frame)TDMA. [16]	93

Εικόνα 23 Πάνω: Σχισμή χρόνου (time slot) σε μεγέθυνση. Κάτω: υπερπλαίσιο (superframe) TDMA στο δίκτυο WirelessHART που περιλαμβάνει πολλές διαδοχικές σχισμές χρόνου (time slots). Πηγή: [18].....	95
Εικόνα 24 Οι σχισμές χρόνου (time slots) στο WirelessHART. [8]	98
Εικόνα 25. Ενεργός συγχρονισμός.....	101
Εικόνα 26. Παθητικός συγχρονισμός	102
Εικόνα 27. Η εξέλιξη από το πρωτόκολλο HART στο πρωτόκολλο WirelessHART	106
Εικόνα 28 Το FieldComm group έχει ως στόχο την ενοποίηση διαφορετικών τεχνολογιών έξυπνων συσκευών στους βιομηχανικούς αυτοματισμούς.....	107
Εικόνα 29 HART. Το ψηφιακό σήμα με διαμόρφωση FSK.....	114
Εικόνα 30 Η μέση τιμή του ημιτονοειδούς σήματος είναι 0 για την κάθε συχνότητα και έτσι δεν επηρεάζεται το αναλογικό σήμα	115
Εικόνα 31. HART. Στο αναλογικό σήμα 4-20 mA γίνεται υπέρθεση ενός ψηφιακού σήματος με διαμόρφωση FSK	115
Εικόνα 32. HART. Στο αναλογικό σήμα 4-20 mA γίνεται υπέρθεση ενός ψηφιακού σήματος με διαμόρφωση FSK. Πηγή: PEPPERL+FUCHS	116
Εικόνα 33. Στη συνδεσμολογία σημείο προς σημείο μόνο μία συσκευή συνδέεται με δύο καλώδια, στην πηγή τροφοδοσίας ή/και σε σύστημα εισόδων/εξόδων.....	118
Εικόνα 34. Το HART μεταφέρει ταυτόχρονα ένα αναλογικό σήμα και ένα ψηφιακό σήμα. Πηγή: [19].....	119
Εικόνα 35 Συσκευή πεδίου HART.....	120
Εικόνα 36. Πρωτεύων κύριος σταθμός (primary master) και δευτερεύων κύριος σταθμός (secondary master) σε σύνδεση πολλαπλών σημείων (multidrop). Η ενέργεια στις συσκευές πεδίου παρέχεται από μία εξωτερική πηγή τροφοδοσίας που δεν εικονίζεται στο σχήμα. Πηγή: [19].....	122
Εικόνα 37 Πρωτεύων κύριος σταθμός (primary master) και δευτερεύων κύριος σταθμός (secondary master) σε σύνδεση σημείο προς σημείο point-to-point. πηγή [19].....	122
Εικόνα 38. Short frame address (1byte).....	129
Εικόνα 39 Long frame address (5 bytes).....	130
Εικόνα 40. πειραματική διάταξη συσκευών WirelessHART.	133
Εικόνα 41. Συσκευές πεδίου (field devices). Είναι αισθητήρες που συνδέονται στα έξυπνα όργανα μέτρησης και τοποθετούνται σε φυσικές θέσεις μέσα σε μία βιομηχανική εγκατάσταση.....	135
Εικόνα 42 Συσκευές πεδίου (field devices) που τοποθετήθηκαν σε σωλήνες που μεταφέρουν νερό για να εκτελέσουν διάφορες μετρήσεις.....	135

Εικόνα 43. Ο πομπός (transmitter) μιας συσκευής πεδίου wirelessHART μπορεί να συνδεθεί σε διαφορετικά όργανα μέτρησης και να ρυθμιστεί για να δείχνει κατάλληλες ενδείξεις και να στέλνει δεδομένα μέσω ασύρματου δικτύου.....	136
Εικόνα 44. Προσαρμογείς (adaptors) WirelessHART από διαφορετικούς κατασκευαστές.....	137
Εικόνα 45 Προσαρμογείς (adaptors) WirelessHART με μορφή κυλίνδρου διαφορετικών κατασκευαστών (bullet της MACTek, THUM της emerson, SITRANS της Siemens).	137
Εικόνα 46. Ο προσαρμογέας (adaptor) συνδέεται σε μία παλαιότερη συσκευή πεδίου HART και την μετατρέπει σε συσκευή WirelessHART.	137
Εικόνα 47. Σχεδιάγραμμα σύνδεσης του προσαρμογέα (adaptor) σε μία συσκευή πεδίου HART	138
Εικόνα 48. Ο προσαρμογέας (adaptor) τύπου bullet συνδέεται σε μία παλαιότερη συσκευή πεδίου HART και την μετατρέπει σε συσκευή WirelessHART.	138
Εικόνα 49 Συσκευές χειρός (Handhelds) από διαφορετικούς κατασκευαστές, που χρησιμοποιούνται στο δίκτυο WirelessHART και στο HART.....	139
Εικόνα 50. Πύλες (Gateways) του WirelessHART διάφορων κατασκευαστών.	140
Εικόνα 51. Δίκτυο πλέγματος (Mesh network) WirelessHART. Οι συσκευές πεδίου FD (Field Devices) τοποθετούνται σε διάφορα σημεία της εγκατάστασης και η πύλη GW (Gateway) επικοινωνεί ασύρματα με όλες τις συσκευές. Πηγή: Pepperl+Fuchs.....	141
Εικόνα 52. Μία συσκευή Διαχειριστής Δικτύου (Network Manager) (NM) του WirelessHART. Κατασκευαστής: dust. Πηγή: http://www.digikey.com/	142
Εικόνα 53. Τα σημεία πρόσβασης Access Points (AP) συνδέουν τις συσκευές πεδίου με μία πύλη (Gateway).	145
Εικόνα 54. Δίκτυο πλέγματος (Mesh network) WirelessHART. Συνδέεται μέσω της πύλης (Gateway) στο δίκτυο αυτοματισμού της εγκατάστασης που μπορεί να είναι ένα δίκτυο κορμού της εγκατάστασης. Η πύλη, ο διαχειριστής δικτύου και ο διαχειριστής ασφαλείας μπορεί να βρίσκονται στο ίδιο κουτί	146
Εικόνα 55. Δίκτυο πλέγματος (Mesh network) WirelessHART. Οι εφαρμογές φιλοξενητή (host applications) συνδέονται μέσω της πύλης (gateway) στο δίκτυο WirelessHART. Πηγή: Smar (www.smar.com).	147
Εικόνα 56. Συσκευές Πεδίου (Field Devices) (FD) του δικτύου WirelessHART από διάφορους κατασκευαστές, ...	149
Εικόνα 57 Οι συσκευές πεδίου χρησιμοποιούνται για έλεγχο στάθμης υγρών σε δεξαμενές.....	150
Εικόνα 58 Σχεδιάγραμμα (exploded diagram) που δείχνει μερικά κομμάτια από τα οποία αποτελείται μια συσκευή πεδίου WirelessHART. πηγή:smar (www.smar.com).	150
Εικόνα 59 Αντίστοιχη εικόνα (exploded view) όπου φαίνονται κομμάτια από τα οποία αποτελείται μια συσκευή πεδίου HART. πηγή:Honeywell.....	150

Εικόνα 60 Οι συσκευές πεδίου WirelessHART μετρούν διάφορα φυσικά μεγέθη, όπως είναι ροή, θερμοκρασία, πίεση, στάθμη, κραδασμούς.....	151
Εικόνα 61. μετρητές διαφορικής πίεσης.....	153
Εικόνα 62. Ροόμετρο Coriolis για μέτρηση ροής αερίου. Κατασκευαστής: Emerson.....	155
Εικόνα 63 Ροόμετρο Coriolis. Παρατηρούμε επιπλέον, ότι ο πομπός είναι συσκευή HART και έχει συνδεθεί με έναν προσαρμογέα (adapter) για μετατρέπει σε συσκευή WirelessHART.....	156
Εικόνα 64. Μετρητής στάθμης υγρών για ανοικτές δεξαμενές, ή για κλειστές δεξαμενές χωρίς πίεση ή για κανάλια, πηγάδια κλπ.....	158
Εικόνα 65. Διάφοροι αισθητήρες που μετρούν το pH υγρών.....	160
Εικόνα 66. πομπός HART που συνδέεται στον αισθητήρα μέτρησης pH υγρών.	160
Εικόνα 67. Μετρητής πυκνότητας υγρού και μετρητής πυκνότητας αερίου.....	161
Εικόνα 68. Η θύρα συντήρησης (maintenance port). Στους ακροδέκτες CN1,CN2 γίνεται σύνδεση με μία ενσύρματη συσκευή χειρός (Handheld Communicator), για να γίνουν διάφορες ρυθμίσεις στην συσκευή πεδίου field device. Πηγή: SMAR (www.smar.com).....	164
Εικόνα 69 Τα εργαλεία λογισμικού λαμβάνουν πληροφορίες για τις συσκευές πεδίου σε γλώσσα EDDL και τις εμφανίζουν σε οθόνη σε ένα γραφικό περιβάλλον υπολογιστή.....	169
Εικόνα 70. Σύνδεση σημείο προς σημείο. Όργανο HART 4-20 mA που ο adaptor έχει τροφοδοσία από βρόχο ή από μπαταρία και συνδέεται πάνω στο όργανο HART σε μία ελεύθερη θύρα σύνδεσης.....	174
Εικόνα 71. Σύνδεση σημείο προς σημείο. Όργανο HART 4-20 mA που ο adaptor έχει τροφοδοσία από βρόχο ή από μπαταρία και έχει εγκατασταθεί στην ίδια γραμμή πάνω στο βρόχο που συνδέεται το όργανο.....	174
Εικόνα 72. Σύνδεση σημείο προς σημείο. Ο adaptor με τροφοδοσία από το όργανο πεδίου (field) ή από την ίδια μπαταρία που δίνει τροφοδοσία και στο όργανο HART χωρίς να χρειάζεται το όργανο HART να έχει τροφοδοσία από βρόχο 4-20mA.	175
Εικόνα 73. Σύνδεση πολλαπλών σημείων (multidrop). Ο προσαρμογέας adaptor συνδέεται με το ένα από τα όργανα πεδίου (field instruments) και τα υπόλοιπα όργανα συνδέονται μεταξύ τους με ενσύρματο δίκτυο HART.	175
Εικόνα 74 Σύγκριση του μοντέλου Στρωμάτων OSI και του μοντέλου στρωμάτων για το WirelessHART. Πηγή: [7, p. 31].....	212
Εικόνα 75. Αλληλεπιδράσεις μεταξύ των στρωμάτων N και N-1, σε ένα διάγραμμα ακολουθίας.....	214
Εικόνα 76. Πακέτο Δεδομένων Data Link Protocol Data Unit (DLPDU). Πηγή: [26].....	229
Εικόνα 77 Δομή των πακέτων δεδομένων DLPDU. Και σύγκριση με τη δομή πακέτων δεδομένων PhPDU του Φυσικού επιπέδου. Πηγή: [8].....	230

Εικόνα 78. ο προσδιοριστής DLPDU Specifier μέσα στο πακέτο DLPDU βρίσκεται στη θέση 7 και αποτελείται από 1 byte δηλαδή 8 bits.....	231
Εικόνα 79 ο προσδιοριστής DLPDU Specifier.Πηγή: [7, p. 43].....	231
Εικόνα 80. ο προσδιοριστής DLPDU Specifier και οι τιμές που παίρνουν τα bits σε διάφορες περιπτώσεις. Πηγή: [8]	232
Εικόνα 81. ο προσδιοριστής DLPDU Specifier και οι τιμές που παίρνουν τα bits σε διάφορες περιπτώσεις. Πηγή: [8]	235
Εικόνα 82. Στο πακέτο δεδομένων DLPDU ο κώδικας MIC είναι το πεδίο που βρίσκεται στην ουρά (footer) στη θέση 9, αμέσως μετά τα δεδομένα payload.	236
Εικόνα 83. Χρονισμός σχισμών (Slot Timing). Πηγή [8].....	238
Εικόνα 84 Η εμβέλεια του επιπέδου δικτύου (network layer).Πηγή: [8]	243
Εικόνα 85 Το πακέτο δεδομένων NPDU Network Layer Protocol Data Unit. Πηγή [7, p. 47].....	251
Εικόνα 86. Η δομή του πακέτου δεδομένων NPDU στο WirelessHART.Πηγή [8].....	252
Εικόνα 87. Το πακέτο δεδομένων NPDU Network Layer Protocol Data Unit. Πηγή: [7, p. 47]	252
Εικόνα 88. Το byte Ελέγχου (Control Byte) είναι ένα πεδίο που βρίσκεται στη θέση 1, στο πακέτο δεδομένων NPDU του επιπέδου δικτύου (Network Layer).....	253
Εικόνα 89. Το byte Ελέγχου (Control Byte). Πηγή: [7]	254
Εικόνα 90. Το byte Ελέγχου (Control Byte) Πηγή [8]	254
Εικόνα 91 Το προαιρετικό πεδίο Proxy Route στο πακέτο δεδομένων NPDU.....	255
Εικόνα 92. Το προαιρετικό πεδίο Source Route στο πακέτο δεδομένων NPDU.....	256
Εικόνα 93. Το πεδίο TTL στο πακέτο δεδομένων NPDU	256
Εικόνα 94. Το πεδίο ASN στο πακέτο δεδομένων NPDU	257
Εικόνα 95. Το πεδίο Graph ID στο πακέτο δεδομένων NPDU	258
Εικόνα 96. Τα πεδία διευθύνσεων πηγής και προορισμού στο πακέτο δεδομένων NPDU.	258
Εικόνα 97: Το υπο-επιπεδο ασφαλείας (Security Sublayer) περιέχεται μέσα στο πακέτο δεδομένων NPDU ως μία επικεφαλίδα με 3 πεδία. Πηγή: [26]	259
Εικόνα 98: Η επικεφαλίδα του υπο-επιπέδου ασφαλείας (Security Sublayer) στο πακέτο δεδομένων NPDU. Πηγή: [7]	259
Εικόνα 99 Το 1ο byte είναι το πεδίο ελέγχου ασφαλείας (Security Control).....	260
Εικόνα 100 Το byte ελέγχου ασφαλείας (security control byte)	260
Εικόνα 101. Το πεδίο του μετρητή nonce counter στο πακέτο δεδομένων του υπο-επιπέδου ασφαλείας.	261

Εικόνα 102. Το πεδίο MIC στο πακέτο δεδομένων του υπο-επιπέδου ασφαλείας.....	261
Εικόνα 103. Το πακέτο δεδομένων TPDU στο Επίπεδο μεταφοράς (Transport Layer) περιέχεται μέσα στο πεδίο Payload του πακέτου NPDU. Πηγή: [26].....	263
Εικόνα 104 Το πακέτο δεδομένων TPDU. Πηγή: [8].....	263
Εικόνα 105. το πεδίο byte μεταφοράς (transport byte)μέσα στο πακέτο TPDU.....	264
Εικόνα 106. το byte μεταφοράς (transport byte)	264
Εικόνα 107. το πεδίο Device Status /Extended Status μέσα στο πακέτο TPDU	265
Εικόνα 108 Οι συγκεντρωμένες εντολές μέσα στο πακέτο TPDU	265
Εικόνα 109. Η μορφή εντολών (command format) του WirelessHART.	265
Εικόνα 110 Αρχιτεκτονική του ISA100.11a. Πηγή: [32]	290
Εικόνα 111 Δρομολόγηση (routing) σε δίκτυο ISA100.11a Πηγή: [30]	295
Εικόνα 112. Αρχιτεκτονική ενός επιπέδου ή επίπεδη (Planar architecture). Πηγή [39].	325
Εικόνα 113. Αρχιτεκτονική δύο επιπέδων (2 layer architecture). Πηγή [39]	326
Εικόνα 114. Αρχιτεκτονική τριών επιπέδων (3 layer architecture).Πηγή [39].	327
Εικόνα 115. Μοντέλα κινητικότητας.	334
Εικόνα 116 Οι χρονικές περίοδοι λειτουργίας listen και sleep του πρωτοκόλλου S-MAC . Πηγή [1].....	363
Εικόνα 117. Οι χρονικές περίοδοι του πρωτοκόλλου S-MAC όταν οι κόμβοι είναι συγχρονισμένοι. Πηγή [42].	363
Εικόνα 118. Ο κύκλος συγχρονισμού στο S-MAC, φαίνονται οι περίοδοι Listen, Sleep, Sync. Πηγή: [43] ...	368
Εικόνα 119. Κλιμακωτή ενεργοποίηση κόμβων στο D-MAC. Πηγή [2].....	381
Εικόνα 120. Μόλις ανιχνευθεί κινητικότητα, το MS-MAC μπαίνει σε περίοδο συγχρονισμού. Πηγή: [43].	395
Εικόνα 121. Γύρω από τον κινητό κόμβο καθορίζεται η ενεργή ζώνη που είναι οι κόμβοι σε απόσταση R hops από τον κινητό κόμβο και R hops από τους συνοριακούς κόμβους Πηγή: [43].....	397
Εικόνα 122. Διάγραμμα ακολουθίας για τη σύνδεση του νέου κόμβου στο δίκτυο WirelessHART. Πηγή [44]	421
Εικόνα 123. Υπερπλαίσιο διαχείρισης (management superframe) στο WirelessHART. Πηγή [44]	423

Κεφάλαιο 1

Εισαγωγή

Η τεχνολογία ασύρματων δικτύων αισθητήρων (WSN) διαρκώς αναπτύσσεται και εξελίσσεται, ώστε πολλά προβλήματα του παρελθόντος έχουν επιλυθεί. Τα βιομηχανικά περιβάλλοντα, έχουν μεγάλες απαιτήσεις σε αξιοπιστία και αυξημένη ποιότητα υπηρεσιών (Quality of Service), QoS. Η ποιότητα υπηρεσιών QoS, για διάφορα δίκτυα, σημαίνει ότι οι ρυθμοί μετάδοσης δεδομένων, οι ρυθμοί σφαλμάτων και άλλες παράμετροι, μπορούν να μετρηθούν, να βελτιωθούν και καθορίζει ότι οι τιμές των παραμέτρων θα είναι εγγυημένες εκ των προτέρων και θα βρίσκονται εντός συγκεκριμένων ορίων, χωρίς να επηρεάζονται από τις ενέργειες των τελικών χρηστών.

Υπάρχουν διάφορες κατηγορίες ασύρματων δικτύων αισθητήρων και πάρα πολλές εφαρμογές για διαφορετικούς σκοπούς. Τα ασύρματα δίκτυα αισθητήρων, μπορούν να βρουν εφαρμογή στη βιομηχανία με το πρότυπο WirelessHART, όπως και με τη χρήση άλλων προτύπων. Σε αυτή την Μεταπτυχιακή Διατριβή γίνεται κυρίως η αναφορά στα χαρακτηριστικά του προτύπου WirelessHART. Όμως, επιπλέον, παρουσιάζονται και μερικά χαρακτηριστικά άλλων προτύπων που έχουν ίδιους στόχους με το WirelessHART και έχουν χρησιμοποιηθεί στη βιομηχανία. Επιπλέον αναφέρονται και διάφορα άλλα θέματα που αφορούν γενικότερα τα ασύρματα δίκτυα αισθητήρων.

Στις βιομηχανίες, τα τελευταία χρόνια έγιναν σημαντικές βελτιώσεις στα όργανα μέτρησης και στα τελικά στοιχεία ελέγχου. Στα όργανα αυτά, ενσωματώθηκαν αισθητήρες και μικροεπεξεργαστές. Αρχικά απέκτησαν δυνατότητα ενσύρματης μετάδοσης πληροφοριών και τελικά προστέθηκαν τεχνολογίες ασύρματης μετάδοσης δεδομένων. Δημιουργήθηκαν τα έξυπνα όργανα ή έξυπνες συσκευές, που μπορούν να συγκεντρώνουν περισσότερες πληροφορίες και γνώσεις για τις βιομηχανικές διεργασίες και έτσι μειώνεται το κόστος παραγωγής, και βελτιώνεται συνολικά όλη η λειτουργία μίας βιομηχανικής εγκατάστασης.

Τα όργανα αυτά, περιλαμβάνουν διάφορες λειτουργίες και χρήσιμα χαρακτηριστικά, όπως είναι η διάγνωση υγείας των συσκευών και ο έλεγχος των βιομηχανικών διεργασιών στις οποίες συνδέονται. Επιπλέον, οι έξυπνες συσκευές, εκτελούν διαγνωστικούς ελέγχους και έχουν ικανότητα ανίχνευσης σφαλμάτων στην εγκατάσταση, επειδή από τα δεδομένα μετρήσεων που

συγκεντρώνονται εντοπίζονται διάφορα προβλήματα, όπως είναι φραγμένες σωληνώσεις, φθορές στα έδρανα κινητήρων, αστάθεια στη φλόγα του καυστήρα, απώλεια αναδευτήρα, διαρροές αερίων, φθορές σε μηχανικά μέρη, π.χ. σπηλαιώσεις και άλλα. Επειδή οι έξυπνες συσκευές στέλνουν ειδοποιήσεις όταν οι ίδιες αντιμετωπίζουν προβλήματα στη λειτουργία τους και ενημερώνουν ότι χρειάζονται συντήρηση, μπορεί άμεσα το προσωπικό της βιομηχανικής εγκατάστασης να τις επισκευάζει και αυτό είναι σημαντικό πλεονέκτημα, διότι δεν χάνεται πολύς χρόνος στον εντοπισμό σφαλμάτων. Με αυτό τον τρόπο, μειώνεται το κόστος που θα προέκυπτε από διακοπή ή καθυστέρηση της παραγωγής, που θα συνέβαινε, αν αργούσαν τα προβλήματα να εντοπιστούν.

Διάφορες δυσκολίες παρουσίασε αρχικά η υιοθέτηση αυτών των τεχνολογιών, στα πεδία των βιομηχανικών εγκαταστάσεων. Μία δυσκολία ήταν το αυξημένο αρχικό κόστος τους και άλλη δυσκολία ότι έπρεπε να γίνουν σημαντικές αλλαγές σε καλωδιώσεις για τα όργανα μετρήσεων που ήδη υπήρχαν, αλλά και για τους πίνακες. Τη λύση στο πρόβλημα των καλωδιώσεων έδωσαν οι νεότερες συσκευές που δημιουργήθηκαν, οι οποίες χρησιμοποιούν την ασύρματη τεχνολογία. Η τεχνολογία WirelessHART είναι συμβατή προς τα πίσω και είναι ίδια με την προηγούμενη, αλλά οι νεότερες συσκευές διαθέτουν βελτιωμένους επεξεργαστές και βελτωμένους αισθητήρες που έχουν χαμηλότερη κατανάλωση ενέργειας σε σύγκριση με τις παλιότερες συσκευές.

Σε αυτή τη Μεταπτυχιακή διατριβή, περιγράφονται ορισμένα πρωτόκολλα που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων. Για κάθε πρωτόκολλο, παρουσιάζονται διάφορα χαρακτηριστικά και παράμετροι που θεωρήθηκαν ότι είναι χρήσιμο να αναφερθούν, ενώ ιδιαίτερα γίνεται εστίαση στο πρωτόκολλο WirelessHART που αποτελεί το κυρίως θέμα της Μεταπτυχιακής Διατριβής. Στην Μεταπτυχιακή διατριβή επανααναλύονται πληροφορίες και δεδομένα από άλλες πηγές, υπό νέο θεωρητικό πρίσμα.

1.1 Γενικά

Στις βιομηχανίες ελέγχου διεργασιών, για πολλά χρόνια, καθιερώθηκαν οι ενσύρματες τεχνολογίες δικτύων, όπως οι Foundation Fieldbus, Profibus, και HART. Αυτές οι ενσύρματες τεχνολογίες, έχουν το πλεονέκτημα, ότι χρησιμοποιούνται επί μία μεγάλη σειρά ετών και συνεπώς, αποκτήθηκε πολύ μεγάλη εμπειρία στη χρήση τους, που οδήγησε σε πολλές καθιερωμένες πρακτικές. Έτσι, επικράτησαν οι τεχνολογίες αυτές και έγιναν πολύ χρήσιμες για τις βιομηχανικές εγκαταστάσεις. Όμως, το μειονέκτημά τους είναι πως απαιτούνται να γίνονται ρυθμίσεις περίπλοκων καλωδιώσεων και μπορεί να είναι σημαντικό το κόστος της εγκατάστασης και της

συντήρησής τους. Επιπλέον, δεν ήταν εύκολες οι αλλαγές θέσης των ενσύρματων συσκευών και έπρεπε να τοποθετούνται μόνιμα σε κάποιες σταθερές θέσεις μέσα στην βιομηχανική εγκατάσταση.

Επειδή οι ενσύρματες τεχνολογίες ήταν καλά εδραιωμένες, υπήρξε μία σχετική απροθυμία από τους τεχνικούς να αντικαταστήσουν αυτά τα ενσύρματα δίκτυα, που ήταν καλά γνωστά, για να εισάγουν νέα είδη δικτύων. Οι τρεις βασικοί στόχοι των βιομηχανιών ήταν α) η βελτίωση της παραγωγικότητας, β) η βελτίωση της ασφάλειας και γ) η μείωση του κόστους. Για να επιτευχθούν αυτοί οι τρεις στόχοι, κρίθηκε ότι θα ήταν αποτελεσματική λύση να χρησιμοποιηθούν τα ασύρματα όργανα μετρήσεων του WirelessHART που χρησιμοποιούν την ίδια γλώσσα με τα παλαιότερα ενσύρματα όργανα μετρήσεων και ελέγχου του ενσύρματου προτύπου HART. Ένας από τους λόγους που προτιμήθηκε το WirelessHART, για χρήση σε πολλές βιομηχανίες, ήταν ότι οι βιομηχανίες αυτές είχαν ήδη εγκατεστημένα όργανα HART που μπορούσαν να λειτουργήσουν και στο νεότερο σύστημα WirelessHART. Άλλες βιομηχανίες επέλεξαν να υιοθετήσουν διαφορετικές τεχνολογίες ασύρματων δικτύων που κρίθηκαν ότι είναι πιο ευέλικτες από τις ενσύρματες. Όμως, οι διαφορετικές ασύρματες τεχνολογίες συχνά δεν ήταν συμβατές με το ενσύρματο πρότυπο HART ώστε έπρεπε να αλλαχθούν και τα όργανα HART και τα συστήματα καλωδιώσεων, που υπήρχαν ήδη εγκατεστημένα. Αυτό δεν θεωρήθηκε συμφέρον από οικονομική άποψη. Το WirelessHART, παρείχε δυνατότητα να γίνουν αρχικά μικρές αλλαγές, χαμηλού κόστους, με χρήση των παλαιότερων οργάνων, ενώ σταδιακά μπορούσαν να γίνουν επεκτάσεις με νεότερες συσκευές WirelessHART, οι οποίες θα έπρεπε να προστεθούν αργότερα στα υπάρχοντα δίκτυα.

Καθώς εξελίχθηκαν τα ασύρματα δίκτυα αισθητήρων και αυξήθηκε η χρήση τους, βελτιώθηκε και η εμπιστοσύνη στην τεχνολογία αυτή. Η τεχνολογία των ασύρματων δικτύων αισθητήρων έφερε βελτιώσεις στις συσκευές στην ασφάλεια, στην τεχνολογία του δικτύου και στη διαχείριση του δικτύου.

1.1.1 Βελτιώσεις στην Κεντρική Διαχείριση

Η κεντρική διαχείριση δικτύου, που παρέχεται στα ασύρματα δίκτυα αισθητήρων, παρέχει βελτιωμένες δυνατότητες. Η κεντρική διαχείριση, είναι σημαντική για τη λειτουργία του δικτύου. Ο διαχειριστής δικτύου είναι μία κεντρική μονάδα υλικού ή/και λογισμικού που μεταξύ άλλων έχει τα παρακάτω καθήκοντα:

α) Διαχειρίζεται αποτελεσματικά τους πόρους του δικτύου.

β) Καθορίζει τον χρονοπρογραμματισμό των επικοινωνιών, ανάλογα με τις απαιτήσεις των εφαρμογών.

γ) Καθορίζει την δρομολόγηση στο δίκτυο, ώστε να καλύψει τους στόχους για αξιοπιστία και καλή απόδοση του δικτύου.

Άλλη δυνατότητα του ασύρματου δικτύου αισθητήρων είναι οι διαγνωστικοί έλεγχοι και οι αναφορές για την υγεία του δικτύου. Αυτές οι πληροφορίες χρησιμοποιούνται από το διαχειριστή δικτύου, για αυτόματη προσαρμογή του δικτύου στις μεταβαλλόμενες συνθήκες. Οι πόροι του δικτύου ανακατανέμονται κατ' απαίτηση για να καλύψουν τις αλλαγές στην απόδοση. Άλλες βασικές απαιτήσεις που πρέπει να καλύψει ο διαχειριστής δικτύου είναι η ασφάλεια, η αξιοπιστία, η ευκολία στη χρήση, η εξοικονόμηση διάρκειας ζωής της μπαταρίας των συσκευών. Η ευελιξία στην υλοποίηση επικοινωνιών επιτρέπει σε κατασκευαστές να κάνουν διαφορετικές υλοποιήσεις στο σύστημα επικοινωνιών. Αυτό συνήθως, οδηγεί σε ζητήματα διαλειτουργικότητας που σημαίνει ότι αν τοποθετηθούν σε ένα δίκτυο συσκευές που δεν έχουν το ίδιο σύστημα επικοινωνιών, ενδέχεται να υπάρξει ασυμβατότητα μεταξύ τους και να μην μπορούν να συνεργάζονται.

1.1.2 Περιορισμοί στην Ενέργεια των Συσκευών

Οι ασύρματες συσκευές τροφοδοτούνται είτε από γραμμή (line-powered) είτε από μπαταρίες είτε από συλλέκτες ενέργειας (energy harvesters).

Οι ασύρματες συσκευές που δεν τροφοδοτούνται από γραμμή, έχουν μεγαλύτερη ευελιξία στη χρήση τους επειδή μπορούν να αλλάξουν θέση, αν χρειαστεί, αλλά απαιτείται χαμηλή κατανάλωση ενέργειας, διότι αλλιώς δεν είναι πρακτικές και εξαντλείται γρήγορα η ενέργεια τους. Αν και αυτές οι συσκευές μπορούν να μεταδώσουν μηνύματα σε χρονικό διάστημα ενός δευτερολέπτου, είναι πιο συνηθισμένος ένας μέσος όρος, κάθε 15 δευτερόλεπτα ή περισσότερο. Η πιο κοινή εφαρμογή για αυτές τις συσκευές είναι να υποστηρίζουν περιοδικές επικοινωνίες. Οι συσκευές μπορούν να υποστηρίζουν αναφορές κατ' εξαίρεση και έχουν μία δυνατότητα με προχωρημένες τεχνικές να παράγουν προαιρετικά αυξημένους ρυθμούς αναφορών όταν βρίσκονται υπό κάποιες ειδικές συνθήκες. Ως επί το πλείστον, τα μηνύματα που στέλνονται από τις συσκευές και κυκλοφορούν μέσα στο δίκτυο, περιέχουν τα δεδομένα ενημερωμένων τιμών από τις μετρήσεις των συσκευών πεδίου. Το κάθε μήνυμα περιέχει μερικές δεκάδες bytes

δεδομένων. Επιπρόσθετα με τις τρέχουσες τιμές μετρήσεων, μερικές συσκευές μεταδίδουν αποθηκευμένα αρχεία μετρήσεων, ή μεταδίδουν ακολουθίες δεδομένων για χρονικά διαστήματα, που λαμβάνονται σε καθημερινή βάση ή κατ' απαίτηση και μπορεί να είναι δεκάδες kbytes δεδομένων.

Σε όλες αυτές τις περιπτώσεις, μία συσκευή που δεν τροφοδοτείται από γραμμή, επηρεάζεται από βασικούς παράγοντες στη λειτουργία της, που μειώνουν την ενέργεια της.

α) Ένας παράγοντας είναι ο λόγος ανοίγματος/κλεισίματος (on/off ratio) δηλαδή το πόσο συχνά γίνεται η μετάβαση κατάστασης από ανοικτή σε κλειστή. Όσο πιο συχνά συμβαίνει αυτό, τόσο περισσότερο αυξάνεται η ισχύς που καταναλώνει η συσκευή. Το υποσύστημα ασύρματων επικοινωνιών των συσκευών είναι αυτό που καταναλώνει τη μεγαλύτερη ενέργεια.

β) Οι συγκρούσεις, δηλαδή όταν δύο ή περισσότερες συσκευές επιχειρούν να μεταδώσουν ταυτόχρονα δεδομένα, είναι άλλος παράγοντας που μειώνει την ενέργεια των κόμβων, διότι τότε κάποια πακέτα δεδομένων χάνονται. Κατά τις συγκρούσεις, τα πακέτα που λαμβάνονται, αν έχουν σφάλματα απορρίπτονται. Μετά πρέπει να μεταδοθούν εκ νέου. Έτσι αυξάνεται η κατανάλωση ενέργειας από τις πολλές μεταδόσεις [1]. Επιπλέον, αυξάνεται και η καθυστέρηση στην παράδοση των πακέτων.

γ) Όταν οι συσκευές παραμένουν ενεργές και ακούν στο δίκτυο για πακέτα αλλά το κανάλι είναι άδειο (idle listening). [1] [2]. Η κατάσταση Idle listening συμβαίνει όταν ο κόμβος αισθητήρας βρίσκεται σε κατάσταση «ακοής» και περιμένει ενεργοποιημένος στο ασύρματο κανάλι για να λάβει πιθανά πακέτα δεδομένων που ενδεχομένως κυκλοφορούν μέσα στο δίκτυο, όμως το κανάλι είναι άδειο στην πραγματικότητα και δεν στέλνεται κανένα πακέτο δεδομένων στο δίκτυο. Σε αυτή την περίπτωση, ο κόμβος μένει για αρκετό χρόνο ενεργοποιημένος σε κατάσταση αδράνειας (idle state) και η ενέργεια που δαπανά άσκοπα, είναι αρκετά μεγάλη και ενδέχεται να είναι περίπου η μισή ή μέχρι και ίση με αυτή που δαπανάται όταν μεταδίδει πακέτα δεδομένων.

δ) Όταν οι συσκευές λαμβάνουν πολλά πακέτα που προορίζονται για άλλους κόμβους (overhearing). Οι κόμβοι αισθητήρες που λαμβάνουν πολλά πακέτα που δεν προορίζονται για αυτούς, έχουν άσκοπη σπατάλη ενέργειας που αυξάνεται σημαντικά, όταν το φορτίο κυκλοφορίας στο δίκτυο είναι αυξημένο καθώς και όταν υπάρχει μεγάλη πυκνότητα κόμβων στο δίκτυο.

ε) Όταν οι κόμβοι αισθητήρες λαμβάνουν πολλά πακέτα ελέγχου από το διαχειριστή δικτύου με αυξημένο overhead (control overhead). Συνήθως ένα πρωτόκολλο MAC απαιτεί να αποστέλλονται και να λαμβάνονται αρκετά πακέτα ελέγχου (control packets) στο δίκτυο, τα οποία χρειάζονται για την ορθή λειτουργία του δικτύου. Όμως αυτά τα πακέτα είναι ένα

πρόσθετο φορτίο για το δίκτυο και γίνονται αιτία καταναλώνεται ενέργεια από τους κόμβους του δικτύου, ενώ οι πληροφορίες που περιέχουν δεν είναι δεδομένα επικοινωνίας προς μετάδοση, που πρόκειται να ανταλλάξουν οι κόμβοι μεταξύ τους σε μία ζεύξη. Επίσης όταν οι συσκευές ακούν στο δίκτυο για αυτά τα πακέτα ελέγχου, δαπανάται και πάλι ενέργεια.

Χρησιμοποιούνται τεχνικές που περιορίζουν την κατανάλωση ενέργειας στα ασύρματα δίκτυα αισθητήρων από τα πρωτόκολλα που προσπαθούν να ελέγξουν την χρήση του ασύρματου συστήματος επικοινωνιών, ή και άλλους παράγοντες που προκαλούν αυξημένη κατανάλωση ενέργειας.

1.1.3 Ασύρματα Δίκτυα Αισθητήρων σε Βιομηχανικό περιβάλλον

Δεν υπάρχουν περιορισμοί στο μέγεθος των βιομηχανικών εγκαταστάσεων που μπορούν να χρησιμοποιήσουν τα ασύρματα δίκτυα αισθητήρων. Αν οι βιομηχανίες είναι μικρές μπορούν να εγκατασταθούν μικρά δίκτυα ενώ αν είναι μεγάλες, εγκαθίστανται περισσότερες ασύρματες συσκευές για να δημιουργήσουν μεγαλύτερα δίκτυα. Ένα πρόβλημα, είναι το περίπλοκο περιβάλλον ραδιοκυμάτων RF που υπάρχει στους βιομηχανικούς χώρους, διότι συχνά προκαλεί πολλές παρεμβολές και εμπόδια στην ασύρματη σύνδεση των συσκευών. Η δημιουργία και διατήρηση ασύρματων δικτύων είναι δύσκολη σε μία βιομηχανική εγκατάσταση. Συνήθως όμως ο διαχειριστής δικτύου είναι αρκετά περίπλοκος, ώστε να κρύβει αυτή την πολυπλοκότητα από τον τελικό χρήστη.

Στην περίπτωση ενός μεγάλου δικτύου, μπορούν να χρησιμοποιηθούν πολλαπλά ασύρματα δίκτυα μέσα στην ίδια περιοχή με επικαλυπτόμενες ασύρματες επικοινωνίες που θα είναι ξεχωριστά δίκτυα μεταξύ τους χωρίς να υπάρχει επικοινωνία ανάμεσα στα διαφορετικά δίκτυα (internetwork communication). Επειδή το προσωπικό των εγκαταστάσεων πρέπει να προσαρμόζεται γρήγορα από την αλλαγή ενός παλαιότερου ενσύρματου συστήματος, θα πρέπει να είναι εύκολη η εγκατάσταση και συντήρηση των δικτύων. Αυτό σημαίνει ότι το ασύρματο δίκτυο αισθητήρων μπορεί να λειτουργεί και αυτόματα να προσαρμόζεται όταν υπάρχουν παρεμβολές από άλλα δίκτυα, ή εσωτερικές παρεμβολές, ή σκιάσεις στην μετάδοση.

Πρέπει να θεωρείται πάντοτε ότι το ασύρματο περιβάλλον διαρκώς μεταβάλλεται. Συχνά οι έρευνες πεδίου που γίνονται αρχικά για τη χρήση ασύρματων δικτύων, μετά από κάποιο διάστημα γίνονται ξεπερασμένες, διότι έχουν γίνει αλλαγές στο περιβάλλον και τότε έχουν

περιορισμένη χρησιμότητα και δεν μπορεί κανείς να βασιστεί σε αυτές για μακροχρόνια λειτουργία ενός δικτύου.

1.2 Πρόβλημα

Στα ασύρματα δίκτυα αισθητήρων WirelessHART, σε μια βιομηχανική εγκατάσταση, όπως εξηγείται στα επόμενα κεφάλαια αυτής της Διατριβής, οι κόμβοι τοποθετούνται σε σταθερές θέσεις και σχηματίζουν μία τοπολογία πλέγματος (mesh topology) όπου τα μηνύματα μεταφέρονται μέσω του δικτύου, ακολουθώντας διαδρομές πολλαπλών αλμάτων (multihop routes) και συγκεντρώνονται σε μία κεντρική συσκευή που ονομάζεται Πύλη.

Αυτό έχει ως αποτέλεσμα, να δημιουργούνται διάφορα στατικά δίκτυα κόμβων αισθητήρων στο χώρο της βιομηχανικής εγκατάστασης. Η έρευνα αυτή είναι σημαντική διότι συγκεντρώνει διάφορες πληροφορίες σχετικά με το πρότυπο WirelessHART, αλλά και από διαφορετικά πρότυπα και αυτές οι πληροφορίες μπορούν να οδηγήσουν σε νέες εφαρμογές του προτύπου WirelessHART.

Είναι επιθυμητό, να ενσωματωθούν στα δίκτυα WirelessHART και επιπλέον κινητοί κόμβοι αισθητήρες για να βελτιωθούν οι λειτουργίες των δικτύων αυτών. Οι κινητοί κόμβοι αισθητήρες αναφέρεται ενδεικτικά ότι μπορούν να τοποθετηθούν σε μικρά οχήματα, ή σε αυτόνομα οχήματα (UAV) ή ακόμη και σε καροτσάκια που κινούνται στο χώρο βιομηχανικής εγκατάστασης, σε άτομα που μετακινούνται σε χώρους, σε συσκευές φορητές που κρατάει ο εργάτης, σε ένα ρομπότ που κινείται μέσα στους διαδρόμους ή σε κινητά μέρη συσκευών όπως σε μηχανικό βραχίονα συναρμολόγησης προϊόντων. Επιπλέον, πρόσφατα, έχουν σχεδιαστεί μικρές βάσεις με ρόδες, πάνω στις οποίες μπορεί να στέκεται ένας άνθρωπος και να μετακινείται στους διαδρόμους αντί να περπατάει. Θα μπορούσαν σε αυτές τις βάσεις να τοποθετηθούν κινητοί κόμβοι αισθητήρες. Με αυτό τον τρόπο, μπορούν να σχεδιαστούν διάφορες εφαρμογές, όπου οι κινητοί κόμβοι αναρτώνται και τοποθετούνται ή ενσωματώνονται σε διάφορα κινούμενα αντικείμενα. Οι δυνατότητες τοποθέτησης κινητών κόμβων αισθητήρων είναι απεριόριστες και μπορούν να επινοηθούν διάφορες χρήσεις των κινητών κόμβων για διαφορετικούς σκοπούς.

Το πρόβλημα που παρατηρήθηκε ήταν ότι τα περισσότερα δίκτυα WirelessHART, όταν σχεδιάστηκαν αρχικά, δεν έλαβαν υπόψη τους την εισαγωγή κινητών κόμβων και έτσι έλειπαν κάποιες προτάσεις που ενσωματώνουν τους κινητούς κόμβους στο δίκτυο WirelessHART. Στην Μεταπτυχιακή Διατριβή, επιχειρήθηκε αρχικά να εντοπιστεί μία πρόταση λύσης κινητικότητας που μπορεί χρησιμοποιηθεί στα ασύρματα δίκτυα αισθητήρων γενικότερα, και έπειτα να προσαρμοστεί με κατάλληλες μετατροπές ώστε μπορέσει να γίνει η χρήση της στο WirelessHART. Όμως, στην τρέχουσα βιβλιογραφία που αναζητήθηκε, αν και συμπεριλαμβανόταν πολλές και λεπτομερείς πληροφορίες για το WirelessHART και για τα ασύρματα δίκτυα αισθητήρων γενικότερα, παρόλα αυτά, δεν βρέθηκαν όσες πληροφορίες αναζητήθηκαν για την εισαγωγή

κινητών κόμβων συγκεκριμένα στο δίκτυο WirelessHART, και για αυτό το λόγο, δεν ήταν εφικτό να επιλεγεί μία πρόταση λύσης από τις πηγές που αναζητήθηκαν.

1.2.1 Η Δική μας Πρόταση

Στο τέλος της Διπλωματικής Διατριβής, επιχειρήθηκε να παρουσιαστεί μία δική μας πρόταση, για τοποθέτηση των κινητών κόμβων σε εργάτες που μετακινούνται σε χώρους δεξαμενών ενός διυλιστηρίου πετρελαίου. Οι κινητοί κόμβοι αισθητήρες μπορούν να τοποθετηθούν στις κινητές συσκευές που χρησιμοποιούν οι εργάτες, ή να προσαρτηθούν στις στολές των εργατών, είτε να χρησιμοποιηθεί μια κατάλληλη συσκευή με μορφή βραχιολιού που να έχει ενσωματωμένους αισθητήρες και να τη φορά ο εργάτης όπως φοριέται ένα ρολόι χειρός. Αυτή η πρόταση, βασίστηκε σε άλλα συστήματα που είχαν εφαρμοστεί σε διυλιστήρια πετρελαίου για την παρακολούθηση υγείας και ασφάλειας των εργατών. Επειδή το περιβάλλον του διυλιστηρίου πετρελαίου είναι εξαιρετικά τοξικό, με πολλές επικίνδυνες ουσίες που μπορούν να προκαλέσουν λιποθυμίες στους εργάτες, στην πρότασή μας θεωρήθηκε ότι μπορούν να τοποθετηθούν κάποιοι αισθητήρες στους εργάτες, ώστε τα δεδομένα τους να συγκεντρώνονται και να μεταφέρονται μέσω δικτύων WirelessHART στο κέντρο ελέγχου που βρίσκεται σε μία άλλη περιοχή. Το κέντρο ελέγχου θα ενημερώνεται για δεδομένα που αφορούν την πίεση στο αίμα του εργάτη, την στάση σώματος του, δηλαδή αν βρίσκεται σε θέση οριζόντια ή κάθετη και άλλα στοιχεία, ώστε όταν ο εργάτης λιποθυμήσει ή αν η πίεση του αίματός του δώσει ανησυχητικές ενδείξεις, να ενεργοποιηθούν κατάλληλοι συναγερμοί που ειδοποιούν το προσωπικό υγείας για να επέμβει και να μεταβεί στη θέση που βρίσκεται ο εργάτης και να τον απομακρύνει από τον επικίνδυνο χώρο.

Αυτή η πρόταση μας παρουσιάζεται στο τέλος της Μεταπτυχιακής Διατριβής, αλλά αναλύεται μόνο ως πιθανό σενάριο κινητικότητας, που μπορεί να εφαρμοστεί στο δίκτυο WirelessHART και γίνεται αρχική ανάλυση και περιγραφή ενός υποθετικού συστήματος, ως προς το πλήθος των κόμβων αισθητήρων και την τοπολογία του, καθώς επίσης γίνονται και διάφορες περιγραφές για τις πιθανές λειτουργίες ενός τέτοιου υποθετικού συστήματος. Πρέπει να τονισθεί ότι γίνονται γενικά σχόλια, χωρίς όμως η πρότασή μας αυτή να έχει δοκιμαστεί σε ένα πραγματικό περιβάλλον διυλιστηρίου, που σημαίνει ότι δεν είναι εφικτό να εγγυηθούμε την ορθή λειτουργία ενός τέτοιου συστήματος υπό πραγματικές συνθήκες, διότι υπάρχουν πολλοί παράγοντες που μπορούν να προκαλέσουν εμπόδια. Επειδή κατά το σχεδιασμό συχνά γίνονται εξιδανικεύσεις και απλοποιήσεις, ενώ δεν λαμβάνονται υπόψη διάφορες παράμετροι που εμφανίζονται στην πραγματικότητα, δεν μπορούμε να θεωρήσουμε ότι η αρχική πρότασή μας δεν παρουσιάζει

σφάλματα ως προς τη σύλληψη της ιδέας. Για αυτό παραμένουμε στα πλαίσια του σχεδιασμού και δεν επεκτεινόμαστε περισσότερο. Επιπλέον παρουσιάζουμε ενδεικτικά ένα σύνολο βιομηχανιών που θα μπορούσαν να χρησιμοποιήσουν το WirelessHART για άλλες βιομηχανικές διεργασίες. Μία περισσότερο εκτενής ανάλυση και μια μελλοντική υλοποίηση ενός τέτοιου συστήματος για τον έλεγχο της υγείας των εργατών, καθώς και για χρήσεις του δικτύου WirelessHART για διαφορετικές βιομηχανικές διεργασίες, θα μπορούσαν να αποτελέσουν προτάσεις για μελλοντικές εργασίες.

1.3 Μεθοδολογία

Σε αυτή τη Μεταπτυχιακή Διατριβή, ακολουθείται η μέθοδος της διαδοχικής παρουσίασης διαφορετικών συστημάτων και τεχνολογιών των ασύρματων δικτύων αισθητήρων, ενώ στο τέλος παρουσιάζονται οι γενικές μέθοδοι κινητικότητας. Δηλαδή υπό ένα νέο θεωρητικό πρίσμα, επανααναλύονται πληροφορίες που ήδη υπάρχουν με στόχο να εξεταστούν νέες εφαρμογές στο πρότυπο WirelessHART.

Ο βασικός σκοπός για τον οποίο αναφέρονται, στα διαφορετικά συστήματα, οι τεχνολογίες και στρατηγικές για τη μεταφορά δεδομένων μεταξύ των κόμβων, είναι να υπάρξει μία κατανόηση της λειτουργίας των συστημάτων και των δυνατοτήτων τους, καθώς και να φανούν ορισμένα πλεονεκτήματα και μειονεκτήματα που υπάρχουν στη χρήση διαφορετικών συστημάτων. Επιπλέον, ένας λόγος που παρουσιάζονται τα διαφορετικά συστήματα, είναι πως όταν καθιερώνεται μία βέλτιστη πρακτική που εφαρμόζεται επιτυχώς σε ένα σύστημα, με θετικά αποτελέσματα, ενδεχομένως να μπορεί να υιοθετηθεί και από άλλα συστήματα, αφού πρώτα προσαρμοστεί βέβαια, στις ιδιαίτερες απαιτήσεις τους. Το μεγαλύτερο μέρος της Μεταπτυχιακής Διατριβής είναι αφιερωμένο στα ασύρματα δίκτυα αισθητήρων και συγκεκριμένα στο πρότυπο WirelessHART, που χρησιμοποιείται στις βιομηχανίες διεργασιών. Η Μεταπτυχιακή Διατριβή, δεν περιορίζεται μόνο στην περιγραφή του WirelessHART, αλλά περιγράφει βασικά στοιχεία και από άλλα πρότυπα και πρωτόκολλα που έχουν σχεδιαστεί για τα ασύρματα δίκτυα αισθητήρων σε βιομηχανικές εγκαταστάσεις. Βέβαια, δεν ήταν δυνατόν να αναλυθούν στην Μεταπτυχιακή Διατριβή όλα τα γνωστά πρωτόκολλα ασύρματων δικτύων αισθητήρων, ή ενσύρματων δικτύων, που υπάρχουν στη βιομηχανία και για αυτό έχει γίνει μία επιλογή από αντιπροσωπευτικά πρωτόκολλα, χωρίς αυτό να σημαίνει ότι άλλα πρωτόκολλα που δεν αναφέρονται εδώ, είναι λιγότερο σημαντικά, ή ότι έχουν περισσότερα μειονεκτήματα. Από τα ενσύρματα βιομηχανικά πρωτόκολλα, περιγράφεται το πρωτόκολλο HART, πάνω στο οποίο βασίστηκε η εξέλιξη του WirelessHART.

Στη συνέχεια, παρουσιάζονται γνωστές μέθοδοι για την κινητικότητα των κόμβων στα ασύρματα δίκτυα αισθητήρων. Όπως αναλύεται στη Διατριβή, η κινητικότητα περιγράφεται με τα μοντέλα κινητικότητας και αναφέρονται μερικά γνωστά μοντέλα που μπορούν να εφαρμοστούν ή έχουν εφαρμοστεί σε διαφορετικές περιπτώσεις. Τα μοντέλα κινητικότητας διακρίνονται σε κατηγορίες με βάση διάφορα κριτήρια, όπως είναι, μεταξύ άλλων, ανάλογα με το αν κινείται ή όχι ο κεντρικός κόμβος, αν κινούνται μερικοί κόμβοι αισθητήρες, αν κινούνται όλοι οι κόμβοι, αν υπάρχουν προκαθορισμένες θέσεις που πρέπει να παραμένουν οι κινητοί κόμβοι για

ένα διάστημα, ή αν οι κινήσεις είναι τυχαίες, ή αν ακολουθείται συγκεκριμένη τροχιά αν υπάρχουν ομάδες κόμβων που κινούνται μαζί, και άλλα.

Τέλος, στο δίκτυο WirelessHART αναφέρονται κάποια υποθετικά σενάρια χρήσης, και γίνονται κάποιες προτάσεις σεναρίων για εισαγωγή και εφαρμογή στο δίκτυο WirelessHART αυτών των μοντέλων κινητικότητας που αναλύθηκαν στις προηγούμενες ενότητες. Το σενάριο στο οποίο βασίζεται η δική μας πρόταση, με τους εργάτες που κινούνται στις δεξαμενές ενός διυλιστηρίου παρουσιάζεται στο τέλος της εργασίας και επιχειρούνται να περιγραφούν βασικές περιπτώσεις χρήσης αυτού του υποθετικού συστήματος.

1.4 Δομή Διατριβής

Η δομή της Μεταπτυχιακής Διατριβής, για τα κεφάλαια που ακολουθούν, περιλαμβάνει την γενική περιγραφή των Ασύρματων δικτύων αισθητήρων, στο κεφάλαιο 2, μετά γίνεται μία εστίαση του ενδιαφέροντος στα Δίκτυα αισθητήρων για Βιομηχανικές Εφαρμογές, στο κεφάλαιο 3 και στη συνέχεια, γίνεται μία ανάλυση και περιγραφή για τα μοντέλα κινητικότητας που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων στο κεφάλαιο 4. Στο κεφάλαιο 5 παρουσιάζεται η δική μας πρόταση με τη μορφή ενός υποθετικού σεναρίου χρήσης και επιπλέον συμπεριλαμβάνεται μία σχετική συζήτηση για τη σύλληψη και το σχεδιασμό υποθετικών σεναρίων, καθώς και για διάφορα ζητήματα σχεδιασμού που προκύπτουν. Τέλος, στο κεφάλαιο 6 παρουσιάζονται τα συμπεράσματα και μερικές προτάσεις για μελλοντικές εργασίες, με τη μορφή σεναρίων, που θα μπορούσαν να υλοποιηθούν σε διάφορες βιομηχανίες.

Επιπλέον, στο Παράρτημα Α παρουσιάζονται πολύ συνοπτικά γενικές τοπολογίες δικτύων, και κάποιες περιγραφές διαμορφώσεων ασύρματης μετάδοσης δεδομένων.

Η δομή της Μεταπτυχιακής Διατριβής παρουσιάζεται εν συντομία, στις ακόλουθες παραγράφους 1.4.1 ως 1.4.5.

1.4.1 Η Δομή του κεφαλαίου: Ασύρματα Δίκτυα Αισθητήρων

Το κεφάλαιο 2 αφορά συνολικά τα ασύρματα δίκτυα αισθητήρων και περιγράφει γενικά θέματα. Στην παράγραφο 2.1 παρουσιάζονται γενικές πληροφορίες, για τα υποσυστήματα που αποτελούν έναν κόμβο αισθητήρα, τα είδη των αισθητήρων, τα πλεονεκτήματα και τα μειονεκτήματα. Επίσης παρουσιάζονται διαφορετικές εφαρμογές των δικτύων αισθητήρων σε διάφορους τομείς.

Στην παράγραφο 2.2 αναφέρονται τα Στρώματα ενός δικτύου αισθητήρων σε σύγκριση με τα στρώματα του μοντέλου OSI. Στην παράγραφο 2.3 γίνεται μία περιγραφή για το πρότυπο IEEE 802.15.4, ενώ στην παράγραφο 2.4 παρουσιάζεται το TDMA.

1.4.2 Η Δομή του Κεφαλαίου: Δίκτυα για Βιομηχανικές Εφαρμογές

Το κεφάλαιο 3 παρουσιάζει τα Δίκτυα για Βιομηχανικές Εφαρμογές και περιγράφει, στην παράγραφο 3.1, το πρότυπο HART και αναφέρει τα στρώματα του μοντέλου OSI και σύγκριση με το HART, επιπλέον παρουσιάζει τα χαρακτηριστικά του δικτύου και τα πακέτα δεδομένων του HART. Στην παράγραφο 3.2 αναλύεται το πρωτόκολλο WirelessHART, παρουσιάζονται οι συσκευές WirelessHART, αρχικά σε σύντομη περιγραφή και στη συνέχεια σε πιο αναλυτική περιγραφή. Παρουσιάζονται επίσης άλλα χαρακτηριστικά και τα διάφορα στρώματα του πρωτοκόλλου. Στην παράγραφο 3.3 παρουσιάζεται το GinMAC που είναι ένα πρωτόκολλο με διαφορετικά χαρακτηριστικά και αναφέρονται διάφορα βασικά στοιχεία που αφορούν το GinMAC.

Στην παράγραφο 3.4, περιγράφεται το πρωτόκολλο ISA100.11a, που είναι και αυτό ένα διαφορετικό πρωτόκολλο για ασύρματα δίκτυα αισθητήρων. Παρουσιάζεται μία σύγκριση του ISA100.11a και του WirelessHART και σε μορφή περιγραφής και σε μορφή συγκριτικών πινάκων.

1.4.3 Η Δομή του Κεφαλαίου: Κινητικότητα στα Ασύρματα Δίκτυα Αισθητήρων

Το κεφάλαιο 4 αφορά την κινητικότητα στα Ασύρματα δίκτυα αισθητήρων. Στην παράγραφο 4.1 γίνεται μια γενική περιγραφή, στην παράγραφο 4.2 παρουσιάζονται τα είδη κινητικότητας, τα επίπεδα αρχιτεκτονικής κινητικότητας και κάποια βασικά μοντέλα κινητικότητας. Στην παράγραφο 4.3 αναφέρονται διαφορετικά είδη πρωτοκόλλων του στρώματος MAC (Media Access Control).

1.4.4 Η Δομή του Κεφαλαίου: η Δική μας Πρόταση

Το κεφάλαιο 5 αναφέρεται στη δική μας πρόταση για την κινητικότητα, η οποία έχει μορφή ενός υποθετικού σεναρίου. Στην παράγραφο 5.1 αναφέρεται μία συζήτηση για γενικές θεωρητικές εκτιμήσεις που έγιναν αρχικά πριν να καταλήξουμε στην σύλληψη του σεναρίου, ενώ στην παράγραφο 5.1.2 αναφερόμαστε στη δική μας λύση όπου δίνουμε μία περιγραφή του σεναρίου μας και αναφερόμαστε σε μία συνολική επισκόπηση. Επίσης παρουσιάζονται υποθέσεις για περιπτώσεις του σεναρίου και κάποιοι δείκτες μέτρησης.

1.4.5 Η Δομή του Κεφαλαίου: Συμπεράσματα και Μελλοντική Εργασία

Το κεφάλαιο 6 είναι το τελικό κεφάλαιο της Μεταπτυχιακής Διατριβής και παρουσιάζει κάποια συμπεράσματα για το WirelessHART και τα χαρακτηριστικά του.

Στην παράγραφο 6.1 παρουσιάζονται συμπεράσματα που αφορούν τις δυνατότητες του WirelessHART και τους τύπους επικοινωνίας που υποστηρίζει. Αυτή η ενότητα λειτουργεί και ως ανακεφαλαίωση που τονίζει μερικά σημαντικά στοιχεία του WirelessHART, τα οποία αναφέρονται στις προηγούμενες ενότητες.

Στην παράγραφο 6.2, γίνεται μία γενική συζήτηση για διάφορες βιομηχανίες που θα μπορούσαν να χρησιμοποιήσουν το πρωτόκολλο WirelessHART σε σενάρια χρήσης, χωρίς όμως να αναφέρονται αναλυτικές λεπτομέρειες για όλες τις περιπτώσεις. Αυτές οι προτάσεις θα μπορούσαν να μελετηθούν και να αναλυθούν σε μελλοντικές εργασίες.

1.4.6 Η Δομή για το Παράρτημα Α

Το παράρτημα Α αναφέρεται σε βασικές τοπολογίες ασύρματων δικτύων αισθητήρων, όπως είναι η τοπολογία Αστέρα, η τοπολογία Πλέγματος και η τοπολογία Δέντρου Συστοιχιών, μεταξύ άλλων. Επίσης παρουσιάζονται με εικόνες οι μορφές αποστολής δεδομένων από έναν κόμβο σε άλλους κόμβους. Τέλος, γίνεται μία περίληπτική εξήγηση επιλεκτικά για κάποιες διαμορφώσεις σήματος που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων για τη μετάδοση δεδομένων.

Θεωρώ, ότι η αυτή η Μεταπτυχιακή Διατριβή παρουσιάζει συγκεντρωτικά διάφορα στοιχεία που αφορούν το WirelessHART, καθώς και άλλα πρότυπα που έχουν τους ίδιους σκοπούς, ώστε να αποτελέσουν μία πηγή πληροφοριών για τους ερευνητές που επιθυμούν να βρουν νέες εφαρμογές και νέους τρόπους χρήσης του προτύπου WirelessHART στις βιομηχανικές εγκαταστάσεις.

Κεφάλαιο 2

Ασύρματα Δίκτυα Αισθητήρων Wireless Sensor Networks (WSN)

Σε αυτό το κεφάλαιο, παρουσιάζονται γενικές πληροφορίες για τα ασύρματα δίκτυα αισθητήρων και αναφέρονται τα βασικά τους χαρακτηριστικά, περιγράφεται η δομή τους, καθώς και τα πλεονεκτήματα και τα μειονεκτήματά τους. Στη συνέχεια, αναφέρονται ορισμένα επιπλέον ζητήματα και παρουσιάζονται συνοπτικά οι εφαρμογές των ασύρματων δικτύων αισθητήρων σε διάφορους τομείς, όπως είναι η χρήση τους σε εργοστάσια για παρακολούθηση της παραγωγής, η παρακολούθηση αγροτικών εκτάσεων, οι στρατιωτικές εφαρμογές, οι εφαρμογές για το περιβάλλον, η επιτήρηση δασών, η παρακολούθηση ζώων. Άλλες εφαρμογές είναι η διαχείριση καταστροφών, οι εφαρμογές υγείας, τα έξυπνα κτήρια, ο έλεγχος κυκλοφορίας των δρόμων. Επίσης μπορούν να χρησιμοποιηθούν και σε επιστημονικές εφαρμογές, όπως η ιατρική, η επιτήρηση των ωκεανών, η παρακολούθηση οικοσυστημάτων και πολλές άλλες εφαρμογές αναμένονται να υλοποιηθούν μελλοντικά. Στο υπόλοιπο μέρος του κεφαλαίου, γίνεται μία περιγραφή για τα στρώματα των ασύρματων δικτύων αισθητήρων και μετά παρουσιάζονται δύο σημαντικά πρωτόκολλα που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων, που είναι το πρότυπο IEEE 801.15.4 και το TDMA και εξηγούνται ορισμένα στοιχεία σχετικά με την λειτουργία τους.

2.1 Γενικά για τα ασύρματα δίκτυα αισθητήρων (WSN)

Τα ασύρματα δίκτυα αισθητήρων είναι τομέας με πολλαπλές εφαρμογές που προσελκύει το ενδιαφέρον πολλών κλάδων έρευνας, όπως η μικροηλεκτρονική, η πληροφορική και η ρομποτική.

Ένα ασύρματο δίκτυο αισθητήρων Wireless Sensor Network (WSN) είναι ένα σύνολο από μικρές αυτόνομες ηλεκτρονικές συσκευές, που περιλαμβάνουν ενσωματωμένους αισθητήρες (sensors) και μικροεπεξεργαστές. Οι συσκευές αυτές ονομάζονται ασύρματοι κόμβοι αισθητήρες (wireless sensor nodes) και συνδυάζουν υποσυστήματα με δυνατότητες για ανίχνευση/μέτρηση ιδιοτήτων φυσικών μεγεθών (sensing), υπολογιστικές δυνατότητες και δυνατότητες ασύρματης επικοινωνίας. Οι συσκευές αυτές μερικές φορές ονομάζονται motes, κυρίως στην Αμερική.

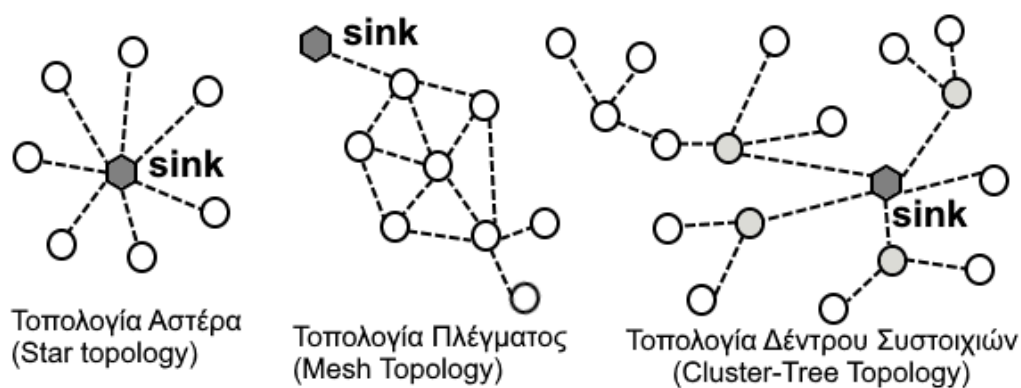
Τα τελευταία χρόνια, η πρόοδος που παρατηρήθηκε στα μικρομηχανικά συστήματα (micro-mechanical systems) (MEMs), τα οποία αποτελούν επέκταση του κλάδου της μικροηλεκτρονικής, έδωσε την δυνατότητα να κατασκευαστούν αισθητήρες με μικρό μέγεθος που έχουν πολλές λειτουργίες με χαμηλή κατανάλωση ενέργειας και χαμηλό κόστος. Παράλληλα, αναπτύσσεται με γρήγορους ρυθμούς η τεχνολογία των μικροεπεξεργαστών και έτσι το μέγεθος των συσκευών αυτών έγινε πολύ μικρό και το κόστος μειώθηκε σημαντικά. Δημιουργήθηκαν μπαταρίες τροφοδοσίας μεγάλης χρονικής διάρκειας που επιτρέπουν στις συσκευές να λειτουργήσουν ακόμη και για χρόνια χωρίς επέμβαση από άνθρωπο. Σε ένα δίκτυο μπορούν να κατανέμονται από εκατοντάδες μέχρι χιλιάδες αισθητήρες για να καλύψουν μία μεγάλη γεωγραφική περιοχή που ονομάζεται πεδίο (field). Οι αισθητήρες που τοποθετούνται στην περιοχή αυτή ονομάζονται συσκευές πεδίου (field devices).

Το χαμηλό κόστος επιτρέπει επίσης την προσωρινή λειτουργία ενός δικτύου αισθητήρων που μπορούν να τοποθετηθούν σε μία περιοχή με ρίψη από αεροσκάφος ή με άλλο τρόπο, για να ληφθούν τοπικά μετρήσεις για περιορισμένη χρονική περίοδο.

Οι συσκευές αυτές, κατανέμονται στο χώρο μίας περιοχής, που πρέπει να παρατηρηθεί και δημιουργούν ένα ασύρματο δίκτυο, το οποίο είναι αυτό-οργανωμένο, έχει πυκνή ανάπτυξη, έλλειψη ελέγχου από άνθρωπο και συνεργασία μεταξύ των κόμβων. Μέσω του δικτύου, οι συσκευές έχουν δυνατότητα να συνεργάζονται μεταξύ τους και να παρακολουθούν τιμές φυσικών μεγεθών ή μεταβλητές του περιβάλλοντος (environmental variables) τις οποίες μπορούν να καταγράφουν στη μνήμη τους. Μία κεντρική συσκευή του δικτύου η οποία λέγεται sink, συλλέγει τις πληροφορίες που μεταδίδουν όλοι οι κόμβοι, μέσω του ασύρματου δικτύου. Από τον sink, έπειτα, οι πληροφορίες μπορούν να μεταφερθούν σε μία κεντρική περιοχή ελέγχου ώστε εκεί να δεχθούν επεξεργασία από άλλα συστήματα ή να συνδεθούν με άλλα δίκτυα.

Στο ασύρματο δίκτυο αισθητήρων οι πληροφορίες ακολουθούν μία διαδρομή δρομολόγησης πολλαπλών αλμάτων (multi-hop) ανάμεσα στους κόμβους του δικτύου. Οι αισθητήρες μπορούν να μετρήσουν πίεση, ροή, θερμοκρασία, ακτινοβολία, φως, υγρασία, ήχους, κραδασμούς, κίνηση,

επιτάχυνση, ύπαρξη αερίων, χημικών ουσιών κλπ. Τα μεγέθη που παρατηρούν οι αισθητήρες τα καταγράφουν και στη συνέχεια τα μεταδίδουν προς τον κεντρικό κόμβο sink σε περιοδικά χρονικά διαστήματα, που μερικές φορές ονομάζονται «εποχές» (epochs) ή πλαίσια (frames). Συχνά οι κόμβοι χωρίζονται σε ομάδες. Όταν οι κόμβοι του δικτύου είναι πυκνοί και τοποθετούνται σε στατικές θέσεις, μπορεί να είναι τοποθετημένοι σε τοπολογία πλέγματος (mesh), ή σε τοπολογία δένδρου (tree). Υπάρχει και η τοπολογία αστέρα (star) που είναι τοπολογία ενός άλματος (single hop) αλλά δεν μπορεί να περιλαμβάνει πολλούς κόμβους. Επιπλέον επιτρέπεται να υπάρχει κινητικότητα στο δίκτυο, αλλά τότε κινητοί είναι ορισμένοι μόνο κόμβοι, ενώ όλοι οι υπόλοιποι κόμβοι είναι στατικοί.



Εικόνα 1 Τοπολογίες δικτύων που αποτελούνται από κόμβους αισθητήρες (sensor nodes).

Όλες οι μετρήσεις μπορούν να χρησιμοποιούνται με πολλούς και διαφορετικούς τρόπους και να σχεδιάζονται διάφορες εφαρμογές. Μπορούν να επινοηθούν διάφοροι τρόποι χρήσης των ασύρματων δικτύων αισθητήρων.

Υπάρχουν περιοχές που απαιτείται η παρακολούθησή τους και σε αυτές μπορούν να τοποθετηθούν ασύρματα δίκτυα αισθητήρων. Τέτοιες περιοχές ενδεικτικά είναι: οι δασικές εκτάσεις, ο βυθός των ωκεανών, τα ηφαίστεια, οι βιομηχανικές εγκαταστάσεις, τα αεροδρόμια, οι πλατφόρμες γεωτρήσεων πετρελαίου, κ.α. Επιπλέον, υπάρχουν και στρατιωτικές εφαρμογές όπου οι αισθητήρες τοποθετούνται σε πεδία των μαχών, για κατασκοπεία του εχθρού, ή για εντοπισμό της παρουσίας χημικών ουσιών, έλεγχο στόχων, κλπ.

2.1.1 Χαρακτηριστικά των ασύρματων δικτύων αισθητήρων

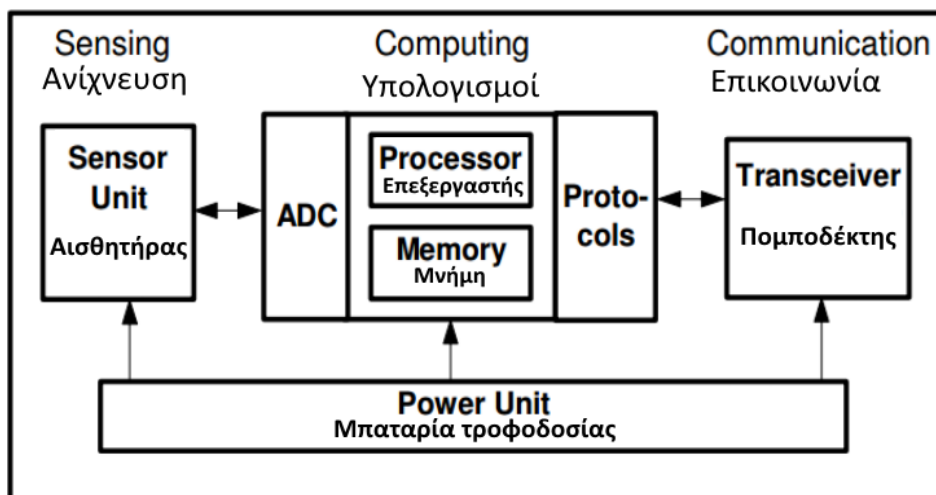
Γενικά χαρακτηριστικά που περιγράφουν τις συσκευές κόμβων αισθητήρων (sensor nodes) που συνδέονται σε ασύρματο δίκτυο, είναι τα παρακάτω [3]:

- α) Υπάρχει ενσωματωμένος μικροεπεξεργαστής και μνήμη.
- β) Υπάρχουν αισθητήρες που μετρούν τιμές φυσικών μεγεθών ή μεταβλητές του περιβάλλοντος και παρέχεται πρόσβαση στις τιμές που μετρούνται.
- γ) Υπάρχει η ασύρματη επικοινωνία, με κατάλληλο σύστημα που αποτελείται από ασύρματη κεραία και πρωτόκολλο ασύρματου δικτύου για επικοινωνία μεταξύ των κόμβων του δικτύου.
- δ) Κάθε συσκευή μπορεί να προγραμματίζεται και να ρυθμίζεται μέσω δικτύου ή με κάποιες εξωτερικές συσκευές που συνδέονται στον κόμβο.
- ε) Η μπαταρία κάθε συσκευής έχει μεγάλη αυτονομία και επιτρέπει τη λειτουργία της συσκευής για αρκετά χρόνια.
- στ) Κάθε συσκευή έχει χαμηλό κόστος και το μέγεθος της είναι πολύ μικρό και καθώς εξελίσσεται η τεχνολογία, οι νεότερες συσκευές έχουν συνεχώς μικρότερο μέγεθος, χωρίς να στερούνται δυνατότητες λειτουργιών.
- ζ) Κύκλος λειτουργίας (Duty Cycle). Ορίζεται ως το κλάσμα χρόνου που ο κόμβος είναι ενεργός προς το συνολικό χρόνο ζωής του.

Κάθε κόμβος αισθητήρας (sensor node) περιλαμβάνει τα εξής 4 βασικά υποσυστήματα [4]:

- α) υποσύστημα αισθητήρων (sensing subsystem),
- β) υποσύστημα επεξεργαστή (processor)
- γ) υποσύστημα επικοινωνίας.
- δ) υποσύστημα ενέργειας τροφοδοσίας

Τα υποσυστήματα φαίνονται στις παρακάτω εικόνες 2 και 3. Υπάρχουν πολλές διαφορετικές επιλογές για το πώς θα ενοποιηθούν τα υποσυστήματα αυτά σε μία ενιαία συσκευή και από τους διαφορετικούς κατασκευαστές κυκλοφορούν πολλές διαφορετικές συσκευές στο εμπόριο που εκτελούν τις ίδιες βασικές λειτουργίες.



Εικόνα 2. Ένα σχεδιάγραμμα για το υλικό (hardware) ενός κόμβου αισθητήρα. Διακρίνονται τέσσερα υποσυστήματα: α) αισθητήρων, β) επεξεργαστή, γ) επικοινωνίας, δ) τροφοδοσίας ενέργειας. Πηγή: [5]

Μπορεί να γίνει επίσης μία κατηγοριοποίηση σε χαρακτηριστικά του υλικού (hardware) και σε χαρακτηριστικά του λογισμικού (software). Μία τέτοια περιγραφή παρουσιάζεται παρακάτω.

Το υλικό (hardware) αποτελείται από τα παρακάτω υποσυστήματα:

Μικροεπεξεργαστής CPU (Central Processing Unit)(κεντρική μονάδα επεξεργασίας ΚΜΕ)

Ο μικροεπεξεργαστής είναι συνήθως ένας μικροελεγκτής γενικού σκοπού που παρέχει υπολογιστικές δυνατότητες στη συσκευή και επιτρέπει να εκτελούνται πολύπλοκες λειτουργίες. Οι δυνατότητες του όμως είναι περιορισμένες και έχει μικρή πολυπλοκότητα σε σύγκριση με έναν επεξεργαστή CPU που χρησιμοποιείται σε υπολογιστές, για αυτό έχει πολύ χαμηλό κόστος. Ο μικροεπεξεργαστής, στους αισθητήρες, είναι σχεδιασμένος έτσι ώστε να έχει μικρή κατανάλωση ενέργειας, χαμηλή τάση λειτουργίας ώστε να μην εξαντλείται γρήγορα η μπαταρία τροφοδοσίας της συσκευής. Η επιλογή ενός επεξεργαστή (processor) καθορίζει σε τι βαθμό θα υπάρχει μία ανταλλαγή (tradeoff) ανάμεσα στην ευελιξία (flexibility) και την αποτελεσματικότητα (efficiency) – όσον αφορά την κατανάλωση ενέργειας και την απόδοση (performance) [4].

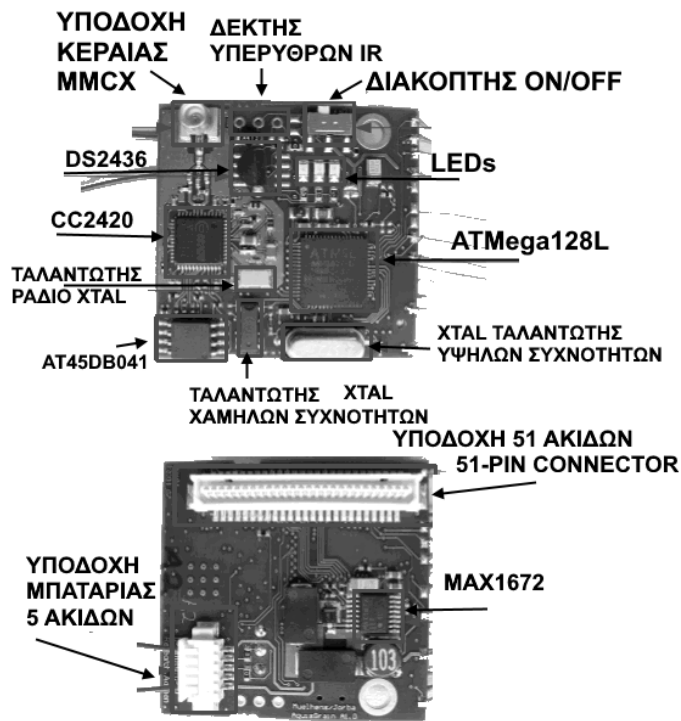
Παραδείγματα από μικροεπεξεργαστές που χρησιμοποιήθηκαν σε πειραματικές διατάξεις [3] ήταν επεξεργαστές 16 bit από διάφορους κατασκευαστές. Οι μικροελεγκτές (microcontrollers) είναι επεξεργαστές γενικού σκοπού. Υπάρχουν περιπτώσεις, που μία συσκευή αισθητήρα χρειάζεται να εκτελεί πολύ απλές λειτουργίες ανίχνευσης (sensing) που είναι πάντοτε ίδιες και

επαναλαμβάνονται για μία εφαρμογή. Τότε χρησιμοποιούνται άλλες κατηγορίες επεξεργαστών, ειδικού σκοπού, κατώτεροι σε υπολογιστικές δυνατότητες, όπως είναι τα ολοκληρωμένα κυκλώματα DSP (Digital signal processors) για επεξεργασία ψηφιακών σημάτων, ή τα προγραμματιζόμενα επί τόπου ολοκληρωμένα κυκλώματα FPGA (field programmable gate arrays-πίνακες προγραμματιζόμενων πυλών) ή άλλα εξειδικευμένα ολοκληρωμένα κυκλώματα με βάση την εφαρμογή.

Τα ολοκληρωμένα κυκλώματα αυτά, έχουν πολύ χαμηλή κατανάλωση ενέργειας και επαρκούν για απλές λειτουργίες των αισθητήρων. Όμως επειδή εξαρτώνται από την εφαρμογή, η διαδικασία σχεδιασμού και υλοποίησης είναι πιο περίπλοκη και έχει μεγαλύτερο κόστος. Οι μικροελεγκτές είναι προτιμότεροι και χρησιμοποιούνται στους περισσότερους κόμβους αισθητήρες (sensor nodes) διότι υπάρχουν πολλές σύνθετες διεργασίες (tasks) οι οποίες κατά τη διάρκεια εκτέλεσης (runtime) των προγραμμάτων του επεξεργαστή απαιτούν περισσότερες υπολογιστικές δυνατότητες και περισσότερο χώρο επεξεργασίας. Αυτές τις δυνατότητες μπορεί να τις παρέχει ένας μικροελεγκτής αλλά δεν μπορεί να τις παρέχει ένας άλλος κατώτερος επεξεργαστής ειδικού σκοπού. Τέτοιες διεργασίες ενδέχεται να είναι: α) η αλλαγή του στόχου των αισθητήρων, β) η αλλαγή/ενημέρωση του λογισμικού (software) που εκτελείται στον κόμβο αισθητήρα, γ) η αποσφαλμάτωση από απόσταση.

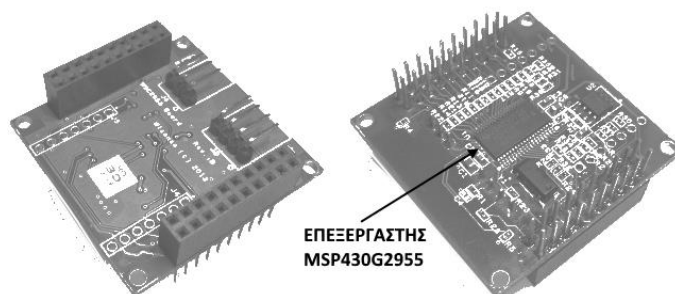
Και στο πεδίο της έρευνας χρησιμοποιείται ο μικροελεγκτής γενικού σκοπού, ώστε να μπορούν να σχεδιάζονται νέα πρωτόκολλα επικοινωνίας και αλγόριθμοι και να επιτρέπεται να γίνει δυναμική εγκατάσταση του κώδικα. Επιπλέον υπάρχουν και τα ολοκληρωμένα κυκλώματα ειδικού σκοπού που λέγονται ASICs (Application-Specific Integrated Circuits) που τοποθετούνται σε κάποια υποσυστήματα. Ένα ASIC λειτουργεί για το υποσύστημα, ως βοηθητικός ενσωματωμένος επεξεργαστής που χρησιμοποιείται μαζί με τον κύριο μικροελεγκτή ώστε να αναλαμβάνει τις απλές διεργασίες ειδικού σκοπού για το υποσύστημα που επαναλαμβάνονται. Έτσι απαλλάσσεται ο μικροελεγκτής από αυτές τις διεργασίες. Τέτοιες διεργασίες για το υποσύστημα επικοινωνιών είναι ο κυκλικός έλεγχος πλεονασμού CRC (cyclic redundancy check), η ακύρωση του θορύβου, η βελτίωση ποιότητας του σήματος.

Ενδεικτικά αναφέρουμε κόμβους αισθητήρες του εμπορίου, και τον τύπο μικροελεγκτή που διαθέτουν. Γνωστός ασύρματος κόμβος αισθητήρα, είναι ο AquisGrain της PFL Connectivity GROUP, ο οποίος υπάρχει στο εμπόριο από το 2004 και διαθέτει το μικροελεγκτή ATmega128 της Atmel που είναι μικροελεγκτής 8bit βασισμένος στην αρχιτεκτονική AVR, 8bit Advanced RISC (που διαθέτει πάνω στο chip μικροελεγκτή ενσωματωμένη μνήμη flash για αποθήκευση του προγράμματος).



Εικόνα 3. Ο κόμβος αισθητήρας AquisGrain, Πάνω: η μία όψη, κάτω η άλλη όψη. Πηγή: [6]

Άλλος, νεότερος, ασύρματος κόμβος αισθητήρας, που υπάρχει στο εμπόριο από το 2014, είναι ο αισθητήρας WiSense, της WiSense Technologies, που βασίζεται στον μικροελεγκτή 16 bit MSP430G2955 Mixed Signal Microcontroller της TEXAS INSTRUMENTS. Μερικά χαρακτηριστικά του μικροελεγκτή αυτού, είναι η χαμηλή τάση τροφοδοσίας 1.8 V ως 3.6 V και η αρχιτεκτονική 16-Bit RISC (Reduced Instruction Set Computer) που είναι βελτιστοποιημένη ως προς το σύνολο εντολών του επεξεργαστή. Ο επεξεργαστής αυτός διαθέτει έναν ψηφιακά ελεγχόμενο ταλαντωτή (digitally controlled oscillator) (DCO) που επιτρέπει στον επεξεργαστή να ξυπνάει (wake-up) από τις λειτουργίες χαμηλής κατανάλωσης ενέργειας, σε λειτουργία ενεργοποίησης (active mode) σε χρόνο λιγότερο από 6μs. Διαθέτει μνήμη 4 KB RAM και 56 KB flash.



Εικόνα 4 . Ο κόμβος αισθητήρας WiSense. Αριστερά : η μία όψη, δεξιά η άλλη όψη. Πηγή: Wisense (<https://wisense.wordpress.com/>).

Άλλοι γνωστοί κόμβοι αισθητήρες στο εμπόριο, είναι οι Wasmote, που υποστηρίζουν πάνω από 100 διαφορετικά είδη αισθητήρων και 15 διαφορετικά είδη διαμόρφωσης ραδιοσημάτων επικοινωνίας μακρινής εμβέλειας (3G / GPRS / LoRa / 868 / 900MHz), μεσαίας εμβέλειας (ZigBee / 802.15.4 / WiFi) και κοντινής εμβέλειας (RFID / NFC / Bluetooth 4.0) και πολλά βιομηχανικά πρωτόκολλα (RS-232, RS-485, Modbus, CAN Bus, 4-20mA). Πληροφορίες για τους αισθητήρες Wasmote υπάρχουν στη διεύθυνση <http://www.libelium.com/products/wasmote/overview/>

Οι κόμβοι αισθητήρες Wasmote διαθέτουν μικροεπεξεργαστή ATmega1281 ο οποίος είναι 8 bit αρχιτεκτονικής AVR. Παρόμοιοι επεξεργαστές υπάρχουν και σε άλλους αισθητήρες του εμπορίου.

Μνήμη

Υπάρχουν μνήμες RAM και flash. Στους επεξεργαστές αρχιτεκτονικής AVR υπάρχει ενσωματωμένη μνήμη Flash και μικρή μνήμη RAM καθώς και μνήμη EEPROM εσωτερικά στο chip του επεξεργαστή. Σε πειραματική διάταξη [3] η μνήμη που χρησιμοποιήθηκε ήταν 10 kb RAM και 48 kb Flash, ενώ σε άλλες περιπτώσεις έχουν χρησιμοποιηθεί μνήμες 4kB RAM και 128 kb Flash. Ενδεικτικά αναφέρουμε μνήμες που χρησιμοποιούνται σε γνωστούς αισθητήρες του εμπορίου.

Ο κόμβος αισθητήρας AquisGrain χρησιμοποιεί τον μικροελεγκτή ATmega128 της Atmel. Αυτός ο μικροελεγκτής 8 bit, αρχιτεκτονικής AVR, εσωτερικά στο chip διαθέτει 128 Kbytes μνήμη Flash για αποθήκευση του προγράμματος, που είναι αυτοπρογραμματιζόμενη, διαθέτει 4Kbytes μνήμη EEPROM και 4Kbytes μνήμη εσωτερική SRAM (στατική RAM που διατηρεί δεδομένα της όσο υπάρχει τροφοδοσία). Οι κόμβοι αισθητήρες Wasmote χρησιμοποιούν επεξεργαστή ATmega1281 της Atmel ο οποίος είναι 8 bit αρχιτεκτονικής AVR και διαθέτει πάνω στο chip του επεξεργαστή μνήμες 64K/128K/256KBytes Flash, 4Kbytes EEPROM και 8Kbytes Internal SRAM. Επίσης διαθέτουν κάρτα μνήμης SD card.

Παρόμοιες μνήμες υπάρχουν και σε άλλους κόμβους αισθητήρες του εμπορίου.

Αισθητήρας (sensor transducer)

Ο αισθητήρας λέγεται και sensor transducer (μετατροπέας μορφής). Ο transducer είναι συσκευή που μετατρέπει μία μορφή ενέργειας σε άλλη μορφή ενέργειας. Με την πρόοδο των

μικρομηχανικών συστημάτων (MEMS) δημιουργήθηκαν πολλά είδη αισθητήρων που μετρούν και ποσοτικοποιούν διάφορες φυσικές ιδιότητες και τις μετατρέπουν σε ηλεκτρικά σήματα που συνήθως είναι σήματα τάσης (voltage) [4]. Οι αισθητήρες αυτοί έχουν μικρό κόστος αγοράς και μπορούν να τοποθετούνται σε πολλά σημεία μέσα στο χώρο. Το σήμα εξόδου ενός transducer συνήθως είναι ένα συνεχές αναλογικό σήμα που το πλάτος του μεταβάλλεται στη διάρκεια του χρόνου. Το υποσύστημα αισθητήρων (sensing subsystem) μπορεί να περιλαμβάνει έναν ή περισσότερους αισθητήρες και έναν ή περισσότερους μετατροπείς αναλογικού σε ψηφιακό σήμα (AD Converters) που με έναν μηχανισμό πολύπλεξης λαμβάνουν τα αναλογικά σήματα των αισθητήρων και τα μετατρέπουν σε ψηφιακά για να τα στείλουν στον επεξεργαστή.

Η μπαταρία τροφοδοσίας που παρέχει ενέργεια στη συσκευή

Οι μπαταρίες είναι αρκετά εξελιγμένες και εξασφαλίζουν μεγάλη αυτονομία στον κόμβο αισθητήρα ώστε να μπορεί να λειτουργεί για αρκετό καιρό χωρίς να χρειάζεται αντικατάσταση.

Σύστημα ασύρματης επικοινωνίας

Στέλνει και λαμβάνει σήματα μέσω του ασύρματου δικτύου. Σε πειραματικές διατάξεις έχει χρησιμοποιηθεί ως ασύρματο δίκτυο και το δίκτυο τεχνολογίας Bluetooth όπου ο ρυθμός μετάδοσης ήταν 250 kbps. [3].

Μετατροπέας από αναλογικό σε ψηφιακό σήμα (A/D converter)

Μετατρέπει τα σήματα που μετράει ο αισθητήρας από αναλογικά σε ψηφιακά ώστε να τα στείλει στον μικροεπεξεργαστή. Μπορούν να συνδεθούν δύο ή περισσότεροι αισθητήρες (sensors) με ένα σύστημα μετατροπής σήματος από αναλογικό σε ψηφιακό με πολλαπλά κανάλια που είναι μία ενοποίηση σε ένα μόνο γραμμικό ολοκληρωμένο κύκλωμα (chip) για πολλούς μετατροπείς αναλογικού σε ψηφιακό σήμα. Όμως αυτοί οι τύποι των μετατροπέων από αναλογικό σε ψηφιακό σήμα (ADCs) είναι κατάλληλοι μόνο για σήματα με χαμηλές συχνότητες διότι μόνο τότε δεν παρουσιάζουν θόρυβο και παραμορφώσεις. Σε σήματα με υψηλές συχνότητες παρουσιάζεται το πρόβλημα της συνακρόασης (crosstalk). Έτσι μπορεί σε μερικά κανάλια να αυξάνεται ο ασυσχέτιστος θόρυβος (uncorrelated noise) και να μειώνεται έτσι ο λόγος σήματος προς θόρυβο signal-to-noise ratio (SNR). Επιπλέον στις υψηλότερες συχνότητες όταν δύο σήματα βρεθούν στο ίδιο κανάλι, δημιουργούνται παραμορφώσεις σήματος spurs που είναι όμοιες με τους αρμονικούς όρους (harmonic terms), που μειώνουν το spurious free dynamic range (SFDR) και την ολική αρμονική παραμόρφωση total harmonic distortion (THD). [4]

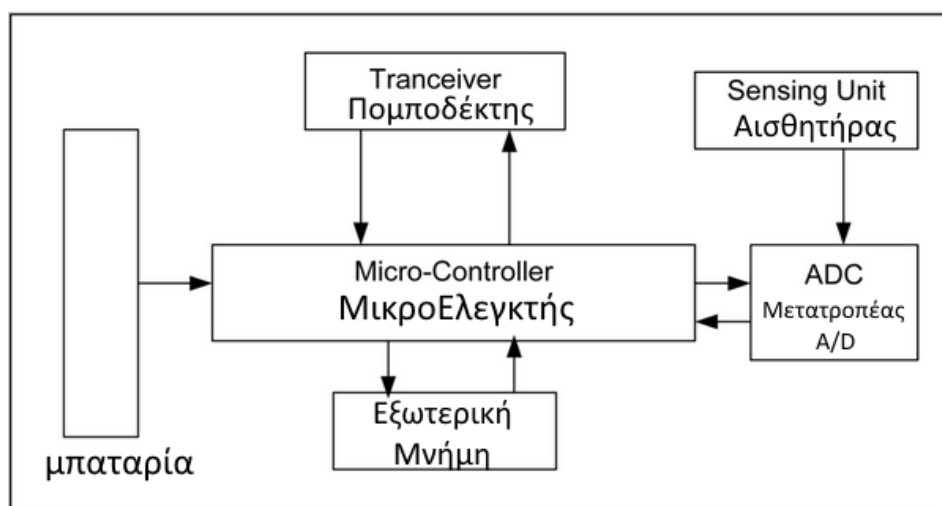
Μερικοί αισθητήρες έχουν δικό τους ενσωματωμένο μετατροπέα από αναλογικό σε ψηφιακό σήμα (ADC) που μπορεί να συνδεθεί άμεσα με τον επεξεργαστή με ένα πρωτόκολλο chip-to-chip protocol. Οι περισσότεροι μικροελεγκτές (microcontrollers) διαθέτουν έναν ή περισσότερους εσωτερικούς μετατροπείς από αναλογικό σε ψηφιακό σήμα (ADCs) για σύνδεση με τις αναλογικές συσκευές (analog devices). [4]

Η μετατροπή από αναλογικό σε ψηφιακό σήμα, περιλαμβάνει δύο βήματα.

α) Το αναλογικό σήμα κβαντίζεται και από συνεχές αναλογικό σήμα μετατρέπεται σε διακριτό σήμα ως προς το χρόνο και ως προς το πλάτος.

Σε αυτό το βήμα καθορίζεται το πλήθος επιτρεπόμενων διακριτών τιμών. Το πλήθος των τιμών αυτών εξαρτάται από τη συχνότητα και το πλάτος του σήματος καθώς και από τους διαθέσιμους πόρους της συσκευής για επεξεργασία δεδομένων και αποθήκευση. Ένα πρόβλημα που προκύπτει στο σήμα μετά από αυτό το βήμα είναι το σφάλμα κβαντισμού.

β) Εφαρμόζεται δειγματοληψία στο σήμα με μία συχνότητα δειγματοληψίας. Για ένα σήμα με περιορισμένο εύρος ζώνης (band-limited signal), ο ρυθμός δειγματοληψίας του Nyquist θέτει ως κατώτατο όριο μία ελάχιστη τιμή στη συχνότητα δειγματοληψίας (sampling frequency). Ο ελάχιστος ρυθμός δειγματοληψίας πρέπει να είναι 2 φορές το εύρος ζώνης (bandwidth) του σήματος. Αν και στην ψηφιακή επεξεργασία σημάτων εφαρμόζεται ο ρυθμός δειγματοληψίας του Nyquist, αντίθετα, στο ασύρματο δίκτυο αισθητήρων υπάρχει μεγάλος θόρυβος και έτσι δεν αρκεί ο ρυθμός δειγματοληψίας του Nyquist. Πρέπει να γίνει μία υπερδειγματοληψία (Oversampling). Ένα πρόβλημα που προκύπτει στο σήμα μετά από αυτό το βήμα είναι η μη εξομάλυνση του σήματος (aliasing).



Εικόνα 5. Ένα άλλο σχεδιάγραμμα για το υλικό (hardware) ενός κόμβου αισθητήρα. Πηγή [5].

Ζητήματα που χρειάζονται να δοθεί έμφαση.

Μεγιστοποίηση της διάρκειας ζωής

Το μεγαλύτερο μέρος της ενέργειας μπαταρίας ενός κόμβου αισθητήρα, δαπανάται από το υπο-σύστημα ασύρματης επικοινωνίας, ενώ το υπο-σύστημα του μικροελεγκτή συνήθως δεν καταναλώνει μεγάλη ενέργεια τροφοδοσίας, διότι έχει βελτιστοποιηθεί για χαμηλή κατανάλωση ενέργειας. Όταν οι κόμβοι αισθητήρες μεταδίδουν πολλά δεδομένα σε άλλους κόμβους, μέσω του ασύρματου δικτύου, εξαντλούν πιο γρήγορα την ενέργεια τους. Για αυτό σχεδιάζονται τεχνικές ώστε να μην καταναλώνεται ενέργεια από ορισμένους μόνο κόμβους και λιγότερη από άλλους, αλλά να είναι συνολικά ομοιόμορφη η κατανάλωση της ενέργειας στο δίκτυο, μέσω δρομολόγησης πολλαπλών αλμάτων (multi-hop) με στόχο να υπάρχει μεγαλύτερη διάρκεια ζωής του δικτύου. Χρησιμοποιούνται τεχνικές βελτίωσης που διαφέρουν αρκετά μεταξύ τους. Μία τεχνική είναι ο επεξεργαστής να συμπίεζει σε μεγάλο βαθμό τις πληροφορίες που πρόκειται να μεταδοθούν ώστε να μειώνονται συνολικά οι επικοινωνίες δεδομένων. Η πιο συνηθισμένη τεχνική είναι να μεταβαίνουν περιοδικά οι κόμβοι σε κατάσταση ύπνου και να ξυπνούν μόνο όταν πρόκειται να μεταδώσουν ή να λάβουν δεδομένα, με βάση έναν χρονικό προγραμματισμό, ώστε να μην καταναλώνουν διαρκώς ενέργεια μένοντας αδρανείς. Υπάρχουν διάφορες καταστάσεις ύπνου όπως Sleep, Deep Sleep, Hibernate. Λιγότερη ενέργεια καταναλώνεται στην κατάσταση Hibernate.

Επίσης, η διάταξη των κόμβων σε ένα δίκτυο πλέγματος, επιτρέπει εκπομπή σημάτων σε μικρή εμβέλεια μετάδοσης από κάθε κόμβο προς τους γειτονικούς του κόμβους ενώ αποφεύγεται μια μεγάλη εμβέλεια μετάδοσης σημάτων προς απομακρυσμένους κόμβους. Αυτό θα δαπανούσε μεγάλο μέρος της ενέργειας τροφοδοσίας του κόμβου αισθητήρα. Παρόλες τις προσπάθειες που γίνονται για μεγαλύτερη αυτονομία σε ενέργεια, χρειάζονται να βρεθούν νέοι τρόποι και να γίνουν περισσότερες βελτιώσεις ώστε να μειωθεί η άσκοπη δαπάνη ενέργειας από τους κόμβους, είτε να βρεθούν νέοι τρόποι τροφοδοσίας, ώστε οι κόμβοι να μπορούν να επαναφορτίζουν πιο γρήγορα τις μπαταρίες τους για να μεγιστοποιήσουν τη διάρκεια λειτουργίας τους. Μεγάλες περίοδοι αυτόνομης λειτουργίας μπορούν να καλυφθούν και με ανανεώσιμες πηγές ενέργειας.

Ανθεκτικότητα στα σφάλματα

Η ανθεκτικότητα σε σφάλματα μπορεί να βελτιωθεί αν χρησιμοποιηθούν πολλοί κόμβοι αισθητήρες σε ένα πυκνό δίκτυο. Τότε οποιαδήποτε βλάβη σε ένα μικρό ποσοστό αισθητήρων δεν

θα επηρεάζει τους υπόλοιπους κόμβους και έτσι το δίκτυο θα συνεχίζει τη λειτουργία του σε αποδεκτά επίπεδα.

Ακρίβεια μετρήσεων.

Η ακρίβεια των μετρήσεων βελτιώνεται όταν οι μετρήσεις λαμβάνονται από μία ομάδα γειτονικών κόμβων σε μία περιοχή που δίνουν πληροφορίες μετρήσεων από πολλά γειτονικά σημεία. Αυτή η μέτρηση δίνει μεγαλύτερη ακρίβεια από ότι αν υπήρχε μόνο ένας κόμβος σε ένα σημείο και κατέγραφε μετρήσεις μόνο από ένα σημείο στην περιοχή.

Το λογισμικό (software) αποτελείται από:

α) Λειτουργικό σύστημα Microcode

Τα λειτουργικά συστήματα δεν είναι πολύπλοκα όπως αυτά που χρησιμοποιούνται στους υπολογιστές, διότι οι υπολογιστικές δυνατότητες που έχουν οι συσκευές κόμβοι αισθητήρες (sensor nodes) είναι περιορισμένες. Μερικά γνωστά λειτουργικά συστήματα που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων είναι τα MANTIS, TinyOS, LiteOS, Contiki, Btnut, nanoRK και άλλα.

Από αυτά, ξεχωρίζουμε το TinyOS, που είναι λειτουργικό σύστημα ειδικά σχεδιασμένο για ασύρματα δίκτυα αισθητήρων. Τα προγράμματα του TinyOS χρησιμοποιούν χειριστές συμβάντων (event handlers). Εξωτερικά συμβάντα είναι π.χ. μια ανάγνωση τιμής από τον αισθητήρα ή ένα πακέτο δεδομένων που εισέρχεται. Το TinyOS δίνει σήμα στον κατάλληλο χειριστή συμβάντων (event handler) να χειριστεί το συμβάν και αυτός εκκινεί μία διεργασία (task) που εκτελείται για να εξυπηρετηθεί το συμβάν. Οι χειριστές συμβάντων (event handlers) μπορούν να αναβάλλουν κάποια συμβάντα να εξυπηρετηθούν σε μεταγενέστερο χρόνο. Οι εργασίες (tasks) που εξυπηρετούν τα συμβάντα, εκτελούνται με το μοντέλο (run-to-completion, RTC) δηλαδή, κάθε εργασία εκτελείται μέχρι να ολοκληρωθεί, ενώ τα συμβάντα που πρόκειται να εξυπηρετηθούν, μπαίνουν σε μία ουρά (event queue). Η ουρά συμβάντων συνήθως εξυπηρετείται με τη σειρά. Μπορεί να παρακάμπτεται σε ειδικές περιπτώσεις και τα συμβάντα να εξυπηρετούνται με βάση τη λήξη προθεσμίας του καθενός. Άλλες φορές, μπορεί να ορίζονται προτεραιότητες και να επιλέγονται τα συμβάντα βάσει προτεραιότητας.

Άλλο λειτουργικό σύστημα για ασύρματα δίκτυα αισθητήρων είναι το LiteOS το οποίο υποστηρίζει δυνατότητα χρήσης της γλώσσας προγραμματισμού C.

Το λειτουργικό σύστημα Contiki χρησιμοποιεί και αυτό πιο απλή μορφή προγραμματισμού σε γλώσσα C και παρέχει εξελιγμένα χαρακτηριστικά όπως είναι το 6LoWPAN και τα Protothreads.

β) Sensor Drivers. Είναι τα προγράμματα οδήγησης του υποσυστήματος αισθητήρων. Επειδή κάθε κόμβος αισθητήρας μπορεί να χρησιμοποιείται σε διαφορετικές εφαρμογές, υποστηρίζει διαφορετικά είδη αισθητήρων, ανάλογα με την εφαρμογή. Κάθε διαφορετικός τύπος αισθητήρα απαιτεί ένα συνοδευτικό πρόγραμμα οδήγησης του, ώστε να μπορεί ο επεξεργαστής να επικοινωνήσει με τον αισθητήρα και να επεξεργαστεί τα δεδομένα που ανιχνεύει ο αισθητήρας.

γ) Communication Processors. Είναι προγράμματα επεξεργασίας των επικοινωνιών. Το υποσύστημα επικοινωνιών του κόμβου αισθητήρα διαχειρίζεται διάφορα είδη ασύρματων σημάτων. Για να μπορεί να διαχειριστεί ο επεξεργαστής τα σήματα αυτά, πρέπει να υπάρχει ένα λογισμικό επεξεργασίας των σημάτων.

δ) Communication Drivers. Είναι πρόγραμμα οδήγησης για το υποσύστημα επικοινωνιών. Επειδή υπάρχουν διαφορετικά υποσυστήματα επικοινωνιών που υποστηρίζουν διαμόρφωση και αποδιαμόρφωση διαφορετικών σημάτων, πρέπει να υπάρχει κατάλληλο λογισμικό που θα διαχειρίζεται αυτές τις μεταδόσεις και λήψεις. Επίσης απαιτείται το πρόγραμμα οδήγησης διότι πρέπει ο επεξεργαστής να συνεργάζεται με το υποσύστημα επικοινωνιών.

ε) Data Processing Mini-apps. Είναι μικροεφαρμογές για επεξεργασία δεδομένων

Ζητήματα που χρειάζονται να δοθεί έμφαση.

Λειτουργικό σύστημα,

Middleware

Κινητικότητα.

Τα τρία παραπάνω θέματα αποτελούν ένα αντικείμενο έρευνας στα ασύρματα δίκτυα αισθητήρων και διαρκώς επινοούνται νέες μέθοδοι και νέα λογισμικά και πρωτόκολλα για να βελτιώσουν τα προβλήματα που παρατηρούνται στα συστήματα που υπάρχουν σήμερα.

2.1.1.1 Είδη αισθητήρων



Εικόνα 6 Διαφορετικά είδη κόμβων αισθητήρων (motes) από διαφορετικούς κατασκευαστές, που έχουν χρησιμοποιηθεί σε προηγούμενα έτη, στα ασύρματα δίκτυα αισθητήρων.

Στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται διάφορα είδη αισθητήρων, που μπορούν να ανιχνεύσουν φυσικά μεγέθη και τις ιδιότητες τους. Υπάρχει μεγάλο πλήθος διαφορετικών τύπων αισθητήρων, και ορισμένοι κόμβοι αισθητήρες, όπως ο Wasp mote, μπορούν να υποστηρίξουν πάνω από 100 διαφορετικά είδη αισθητήρων. Παρακάτω αναφέρονται ενδεικτικά μερικοί τύποι αισθητήρων.

1. Αισθητήρας Υγρασίας. Μετράει τη σχετική και την απόλυτη υγρασία του χώρου. Μπορεί να χρησιμοποιηθεί σε εφαρμογές γεωργίας για να μετρήσει την υγρασία του εδάφους, σε ιατρικές εφαρμογές για να μετρήσει υγρασία στο σώμα κ.α. Η μέτρηση σχετικής υγρασίας του αέρα, μετράται με τη μορφή ενός ποσοστού που αντιστοιχεί στο ποσοστό νερού που απορροφάται από τον αέρα. Όταν ο αέρας δεν έχει καθόλου υγρασία τότε το ποσοστό υγρασίας είναι 0 (σημείο ξηρότητας). Όταν ο αέρας φτάσει στο σημείο εκκίνησης υγραποίησης το ποσοστό υγρασίας είναι 100. Όμως αυτές οι τιμές είναι σχετικές και ισχύουν μόνο για συγκεκριμένες τιμές πίεσης και θερμοκρασίας, (όπως π.χ. για ατμοσφαιρικές συνθήκες και για συγκεκριμένη θερμοκρασία) και δεν ισχύουν για άλλες τιμές. Η απόλυτη υγρασία του χώρου, είναι μία άλλη τιμή που δεν επηρεάζεται από αλλαγές στην πίεση και τη θερμοκρασία.
2. Αισθητήρας υγρασίας του εδάφους. Μετράει την υγρασία του εδάφους. Χρησιμοποιείται σε εφαρμογές γεωργίας, για διαχείριση λιπασμάτων και νερού.
3. Αισθητήρας Υποήχων. Μετράει τα ακουστικά κύματα διάσεισης που μπορούν να προκληθούν από σεισμούς ή εκρήξεις ηφαιστείων.

4. Αισθητήρας Σεισμικός. Μετράει τα πρωτεύοντα και τα δευτερεύοντα σεισμικά κύματα (δονήσεις του περιβάλλοντος, κύμα σώματος). Χρησιμοποιείται για ανίχνευση των σεισμών.
5. Αισθητήρας Υπερήχων για μέτρηση Ροής Αίματος. Μετράει τη μετατόπιση Doppler από την ανάκλαση ενός κύματος υπερήχων στο αίμα. Το φαινόμενο Doppler είναι η αλλαγή στην παρατηρούμενη συχνότητα ενός κύματος λόγω κίνησης πηγής ή του στόχου. Χρησιμοποιείται σε εφαρμογές ιατρικής.

Επίσης ο αισθητήρας υπερήχων μπορεί να εντοπίζει παρουσία αντικειμένων που βρίσκονται σε εγγύτητα. Μπορεί να χρησιμοποιηθεί σε οχήματα. Υπάρχουν δύο είδη Αισθητήρων Υπερήχων, ο ηλεκτροστατικός και ο πιεζοηλεκτρικός.
6. Αισθητήρας Μαγνητικός. Μετράει την αλλαγή του μαγνητικού πεδίου στο χώρο. Επίσης με κατάλληλους υπολογισμούς, μπορεί κατ' επέκταση να εντοπίσει την παρουσία αντικειμένου στο χώρο, την κατεύθυνση κίνησης και την περιστροφή αντικειμένου. Επειδή τα οχήματα περιέχουν σίδηρο, το μαγνητικό πεδίο τα εντοπίζει. Εκτός από την παρουσία οχημάτων στο χώρο, μπορεί να ανιχνεύει και την πυκνότητα ενός οχήματος και τη συμφόρηση στους δρόμους. Μπορεί να χρησιμοποιηθεί σε εφαρμογές ελέγχου κυκλοφορίας ή εφαρμογές μεταφοράς προϊόντων με φορτηγά. Χρησιμοποιείται ακόμη σε εφαρμογές πλοήγησης και στον εντοπισμό αυτοκινήτων που κινούνται με μεγάλες ταχύτητες.
7. Αισθητήρας Οξύμετρο. Μετράει την οξυγόνωση του αίματος στην αιμοσφαιρίνη. Επίσης μπορεί να μετρήσει καρδιαγγειακή κόπωση και την κόπωση που έχει σχέση με την σωματική άσκηση. Μπορεί να χρησιμοποιηθεί σε ιατρικές εφαρμογές.
8. Αισθητήρας οξυγόνου. Μετράει την ποσότητα και την αναλογία του οξυγόνου στο αίμα. Χρησιμοποιείται σε εφαρμογές ιατρικής.

9. Αισθητήρας PH sensor. Μετράει συγκέντρωση ιόντων υδρογόνου. Δείχνει το όξινο ή αλκαλικό περιεχόμενο του νερού. Μπορεί να χρησιμοποιηθεί για έλεγχο καθαρότητας του νερού, έλεγχο διαβρωτικών ουσιών και άλλες χρήσεις. Μπορεί να τοποθετηθεί για παράδειγμα σε σωλήνες που μεταφέρουν νερό ή άλλα υγρά.
10. Αισθητήρας Φωτοακουστικός Φασματοσκοπίας. Μετράει την παρουσία αερίου. Μπορεί να χρησιμοποιηθεί σε αγωγούς αερίου για να ανιχνεύει διαρροές αερίων στον αγωγό.
11. Αισθητήρας Πιεζοηλεκτρικός κύλινδρος. Μετράει την ταχύτητα του αερίου. Μία διαρροή αερίου μπορεί να προκαλέσει έναν θόρυβο υψηλής συχνότητας που παράγει μία δόνηση η οποία ανιχνεύεται από τον πιεζοηλεκτρικό αισθητήρα.
12. Αισθητήρας Θερμοκρασίας. Μετράει τη θερμοκρασία του εδάφους ή γενικά του περιβάλλοντος και μπορεί να χρησιμοποιηθεί σε εφαρμογές γεωργίας ή σε εφαρμογές υγείας. Ένας συνήθης αισθητήρας θερμοκρασίας είναι το θερμοζεύγος (thermocouple) που βασίζεται στο θερμοηλεκτρικό φαινόμενο. Αποτελείται από δύο ανόμοια καλώδια από διαφορετικό κράμα μετάλλων, τα οποία ενώνονται τουλάχιστον στο ένα άκρο τους που είναι η επαφή μέτρησης, ενώ μπορεί να είναι ασύνδετα ή όχι στο άλλο άκρο τους που είναι η επαφή αναφοράς. Ανάλογα με τη διαφορά θερμοκρασίας μεταξύ των 2 άκρων τους, δημιουργείται μία θερμοηλεκτρική τάση.
- Άλλα θερμόμετρα είναι τα θερμόμετρα αντίστασης, στα οποία αλλάζει η τιμή της αντίστασής τους αναλόγως με τις αλλαγές στην τιμή της θερμοκρασίας και αυτά αντέχουν σε υψηλές θερμοκρασίες.
- Υπάρχουν και θερμόμετρα που βασίζονται στην ανίχνευση της ακτινοβολίας που προκαλείται από τη θερμότητα του αντικειμένου που μετράται, όπως είναι η θερμική ακτινοβολία, ή οι υπέρυθρες ακτινοβολίες. Τα πυρόμετρα ανιχνεύουν την θερμική ακτινοβολία που εκπέμπει ένα αντικείμενο, ενώ τα οπτικά πυρόμετρα αντιλαμβάνονται μία λάμψη στην επιφάνεια του αντικειμένου λόγω ακτινοβολίας θερμότητας. Τα υπέρυθρα θερμόμετρα ανιχνεύουν την υπέρυθρη ακτινοβολία που προκαλείται λόγω θερμοκρασίας. Μία άλλη κατηγορία εξελιγμένων θερμομέτρων, είναι τα θερμόμετρα με

οπτικές ίνες που μπορούν να μετρήσουν τη θερμοκρασία από απόσταση και στηρίζονται στις αρχές της Φυσικής που αφορούν την ακτινοβολία μέλανος σώματος .

13. Αισθητήρας Βαρομετρικός ή πίεσης. Μετράει την πίεση που ασκείται σε ένα υγρό. Μπορεί να χρησιμοποιηθεί σε εφαρμογές υγείας ή σε εφαρμογές γεωργίας, ή σε δεξαμενές και σε άλλες περιπτώσεις. Μπορεί να μετρήσει το ύψος στήλης υγρού, το υψόμετρο, την πτώση πίεσης και τη ροή ενός υγρού, το βάρος και το βάθος για ένα αντικείμενο που έχει βυθιστεί καθώς και το ογκομετρικό εκτόπισμα.

14. Αισθητήρας Υπέρυθρων Παθητικός. Μετράει την ακτινοβολία υπέρυθρων που εκπέμπεται από διάφορα αντικείμενα στον χώρο. Μπορεί κατ' επέκταση να ανιχνεύσει την κίνηση αντικειμένων.

15. Αισθητήρας Επιταχυνσιόμετρο. Μετράει την επιτάχυνση των κινήσεων αντικειμένων ή ανθρώπων, σε επίπεδο 2D και 3D. Έχει πάρα πολλές χρήσεις. Μπορεί να συλλάβει τα σεισμικά κύματα, για αυτό μπορεί να χρησιμοποιηθεί σε εφαρμογές μέτρησης ηφαιστειακών δραστηριοτήτων. Μπορεί να μετρήσει την σκληρότητα της δομής αντικειμένων και να ελέγξει αλλαγές στη δομή τους. Έχει και εφαρμογές στην ιατρική διότι μπορεί να ελέγξει τη σκληρότητα των οστών. Μια άλλη χρήση στην ιατρική είναι να ελέγξει τη διακύμανση κινήσεων ατόμων με Parkinson (βραδυκινησία ή υπερκινησία).

Στα μέσα μεταφοράς μπορεί να χρησιμοποιηθεί για παράδειγμα στο σιδηρόδρομο ώστε να ελέγξει την δομή των τροχών, των αξόνων και των γραμμών.

Άλλη εφαρμογή είναι να χρησιμοποιηθεί σε φόρτωση/εκφόρτωση κιβωτίων εύθραυστων υλικών και να ανιχνεύσει αν τα υλικά μέσα στο κιβώτιο έχουν σπάσει.

16. Αισθητήρας μέτρησης ταχύτητας. Υπάρχουν αισθητήρες που μετρούν την ταχύτητα σωμάτων που κινούνται γραμμικά, χρησιμοποιώντας την μαγνητική επαγωγή. Ένας μαγνήτης προσαρτάται πάνω σε ένα κινούμενο σώμα, που η κίνηση του είναι γραμμική, και μετά το σώμα διέρχεται μέσα από σπείρες ενός πηνίου. Τότε μία τάση από επαγωγή, ανάλογη με την ένταση του πεδίου και την ταχύτητα του μαγνήτη προκαλείται στους

ακροδέκτες του πηνίου. Αυτή η τάση χρησιμοποιείται για τον υπολογισμό ταχύτητας του αντικειμένου.

17. Αισθητήρας Εκπομπής ακουστικών σημάτων. Μπορεί να ανιχνεύσει ελαστικά κύματα που παράγονται και διαδίδονται όταν υπάρχει μία ρωγμή σε ένα υλικό. Μπορεί να μετρήσει μικρές αλλαγές στη δομή αντικειμένων, ή μετατοπίσεις.
18. Αισθητήρας Ακουστικών σημάτων. Μπορεί να ανιχνεύσει τη δόνηση από ακουστική πίεση δηλαδή την μεταβολή στην ατμοσφαιρική πίεση που προκαλείται από ένα ακουστικό κύμα. Στον αέρα η ακουστική πίεση μπορεί να μετρηθεί με μικρόφωνο ενώ μέσα στο νερό με υδρόφωνο. Σε εφαρμογές κυκλοφορίας, μπορεί να ανιχνεύσει την παρουσία οχημάτων. Μπορεί να μετρήσει αστοχίες και ασυνέχειες στη δομή υλικών. Χρησιμοποιείται και σε εφαρμογές αγωγών μεταφοράς αερίου διότι μπορεί να μετρήσει τη ρύπανση από επικίνδυνα αέρια.
19. Αισθητήρας Χωρητικός. Μετράει συγκέντρωση μίας διαλυμένης ουσίας σε διάλυμα. Μπορεί να χρησιμοποιηθεί στη γεωργία, για να μετρήσει το περιεχόμενο νερού στο έδαφος.
20. Αισθητήρας ηλεκτροκαρδιογραφήματος ECG. Μετράει τους καρδιακούς ρυθμούς.
21. Αισθητήρας ηλεκτροεγκεφαλογραφήματος EEG. Μετράει την ηλεκτρική δραστηριότητα του εγκεφάλου
22. Αισθητήρας ηλεκτρομυογραφήματος EMG. Μετράει τη δραστηριότητα των μυών.
23. Αισθητήρας Ηλεκτρικός/Ηλεκτρομαγνητικός. Μετράει ηλεκτρική αντίσταση, αγωγιμότητα, χωρητικότητα ή επαγωγή. Μπορεί να χρησιμοποιηθεί σε εφαρμογές γεωργίας για να ελέγξει μεταβολές επαγωγής ή χωρητικότητας που προκαλούνται
24. Αισθητήρας Γυροσκόπιο. Μετράει τη γωνιακή ταχύτητα.

Οι αισθητήρες που αναφέρθηκαν παραπάνω είναι μόνο ένα μικρό μέρος από το σύνολο αισθητήρων που υπάρχουν και χρησιμοποιούνται σε διάφορες εφαρμογές.

2.1.2 Πλεονεκτήματα και μειονεκτήματα των ασύρματων δικτύων αισθητήρων

Ένα ασύρματο δίκτυο αισθητήρων παρουσιάζει τα παρακάτω πλεονεκτήματα:

- Μικρό μέγεθος
- Χαμηλό κόστος
- Χαμηλή κατανάλωση ενέργειας
- Εύκολη υλοποίηση του δικτύου
- Αυτό-οργάνωση του δικτύου
- Αποδέχεται εισαγωγή νέων συσκευών οποιαδήποτε στιγμή
- Παράλληλη επεξεργασία πληροφοριών
- Μη ελεγχόμενο από ανθρώπους.
- Δέχεται πρόσβαση από ένα κεντρικό κόμβο που συγκεντρώνει τα δεδομένα των αισθητήρων.
- Αποφυγή καλωδίων
- Υποδομή που υποστηρίζει διαφορετικές τοπολογίες.
- Πολλαπλά και διασταυρωμένα δεδομένα.

Όμως στα ασύρματα δίκτυα αισθητήρων υπάρχουν και τα παρακάτω μειονεκτήματα:

- Περιορισμός στην ενέργεια τροφοδοσίας όταν υπάρχει αύξηση της κυκλοφορίας δεδομένων.
- Χαμηλοί ρυθμοί μετάδοσης δεδομένων, καθυστέρηση.
- Περιορισμένη μνήμη
- Υπερχείλιση ενδιάμεσης μνήμης.
- Περιορισμένες υπολογιστικές δυνατότητες.
- Περιορισμός στην εμβέλεια μετάδοσης ασύρματου σήματος, π.χ. εμβέλεια μέχρι 80 m.

- Περιορισμός μετάδοσης από εμπόδια ή παρεμβολές.
- Τα δίκτυα είναι ευαίσθητα σε κακόβουλες εισβολές και ο υπολογιστής ενός hacker μπορεί να λειτουργήσει ως Access Point του δικτύου.

2.1.3 Επιπλέον ζητήματα των ασύρματων δικτύων αισθητήρων

Θέματα Ασφάλειας

διαχείριση κλειδιών, πιστοποίηση, ανίχνευση κακόβουλης εισβολής, προστασία ιδιωτικών πληροφοριών.

προστασία από διακοπή των επικοινωνιών.

Επιθέσεις

Sybil attack,

Μια επίθεση που επινοήθηκε το 2002 από τον «Brain Zill» και εισάγει ξένες ταυτότητες σε ένα δίκτυο ισότιμων κόμβων (peer to peer)

traffic analysis attack.

υποκλέπτει και εξετάζει τα μηνύματα (messages). Προσπαθεί να συμπεράνει πληροφορίες για την επικοινωνία από δεδομένα που έρχονται με συγκεκριμένη σειρά (patterns). Μπορεί να ανιχνεύσει τα κρυπτογραφημένα μηνύματα, αλλά δεν μπορεί να τα αποκρυπτογραφήσει.

Δύο κατηγορίες δικτύων

Τα ασύρματα δίκτυα αισθητήρων (WSN) διακρίνονται σε δύο κατηγορίες ανάλογα με το πλήθος κόμβων και τον τρόπο που εγκαθίστανται:

α) Τα μη δομημένα ασύρματα δίκτυα αισθητήρων (WSN)

Αυτά τα δίκτυα έχουν ένα μεγάλο πλήθος κόμβων και οι κόμβοι αισθητήρες τοποθετούνται με μεγάλη πυκνότητα στις περιοχές κάλυψης.

Τα δίκτυα αυτά έχουν συμπεριφορά δικτύου πλέγματος μεταξύ ισότιμων κόμβων. Η συντήρηση του δικτύου είναι δύσκολη διότι υπάρχουν πολλοί αισθητήρες και δεν είναι εύκολο να εντοπισθούν και να αντικατασταθούν αυτοί που παρουσιάζουν αστοχίες. Συνήθως αν κάποιος

αισθητήρες παρουσιάσουν πρόβλημα, δεν αντικαθίστανται και το δίκτυο βασίζεται στους υπόλοιπους αισθητήρες οι οποίοι επαρκούν για την κάλυψη της περιοχής.

β) Τα δομημένα ασύρματα δίκτυα αισθητήρων (WSN)

Τα δίκτυα αυτά έχουν σχετικά μικρό πλήθος κόμβων οι οποίοι είναι κατανεμημένοι σε συγκεκριμένα σημεία. Η εγκατάστασή τους γίνεται με προσχεδιασμένο τρόπο και έχει αποφασιστεί από πριν σε ποιες θέσεις θα τοποθετηθούν οι αισθητήρες για να ελέγξουν συγκεκριμένα μεγέθη.

Η συντήρηση του δικτύου γίνεται εστιασμένα στα καθορισμένα σημεία θέσεων των αισθητήρων και είναι πιο εύκολη διότι εντοπίζονται γρήγορα οι αισθητήρες που παρουσιάζουν βλάβη και αντικαθίστανται.

Η κατανάλωση ενέργειας.

Οι κόμβοι του δικτύου καταναλώνουν ενέργεια στις παρακάτω περιπτώσεις:

α) Ενεργοποίηση ασύρματου δικτύου.

Ανάλογα με την τεχνολογία ασύρματου δικτύου που χρησιμοποιείται καταναλώνεται αντίστοιχα μία ενέργεια τροφοδοσίας

β) Μετάδοση δεδομένων.

Ανάλογα με την ισχύ μετάδοσης του σήματος και το πλήθος bit που μεταδίδονται καταναλώνεται μια αντίστοιχη ενέργεια τροφοδοσίας.

γ) Λήψη δεδομένων.

Ο κόμβος καταναλώνει ενέργεια όσο είναι ενεργός και λαμβάνει δεδομένα

δ) Αναμονή για δεδομένα

Ο κόμβος βρίσκεται σε κατάσταση αναμονής και περιμένει να έρθουν δεδομένα αλλά δεν λαμβάνει δεδομένα εκείνη τη στιγμή.

ε) Συχνή εναλλαγή μεταξύ λειτουργίας εκπομπής και λειτουργίας λήψης. Ο κόμβος αισθητήρας απαιτείται σε κάποιες στιγμές να μεταβεί από λειτουργία εκπομπής σε λειτουργία λήψης. Αυτές οι εναλλαγές απαιτούν κατανάλωση ενέργειας και πρέπει να μην γίνονται υπερβολικά συχνά διότι εξαντλούν τη μπαταρία της συσκευής.

2.1.4 Εφαρμογές

Οι εφαρμογές των ασύρματων δικτύων αισθητήρων (WSN) είναι πάρα πολλές και μπορούν να χρησιμοποιηθούν σε όλους τους τομείς της τεχνολογίας. Διάφορα σενάρια είτε ήδη έχουν υλοποιηθεί είτε μελετώνται για μελλοντική υλοποίηση.

Μερικές χρήσεις είναι οι παρακάτω:

Παρακολούθηση αντικειμένων και κατασκευών.

Τα ασύρματα δίκτυα αισθητήρων (WSN) μπορούν να χρησιμοποιηθούν σε εργοστάσια για παρακολούθηση κατασκευών ή για σχεδιασμό συντηρήσεων μηχανικών μερών με βάση τις συνθήκες που επικρατούν στο περιβάλλον. Οι αισθητήρες μπορούν να συλλέγουν δεδομένα για τους κραδασμούς (vibration), για τις ρωγμές σε μηχανικά μέρη και να αναφέρουν τα δεδομένα σε πραγματικό χρόνο.

Αυτό έχει το πλεονέκτημα ότι αυτοματοποιούνται οι διαδικασίες και το κόστος είναι χαμηλότερο για αρκετές τάξεις μεγέθους.

Παρακολούθηση αγροτικών εκτάσεων .

Η παρακολούθηση με ακρίβεια των αγροτικών εκτάσεων (Precision Agriculture)(PA) έχει στόχο να κάνει πιο αποτελεσματικές τις αγροτικές εργασίες και παράλληλα να μειώσει τις αρνητικές επιπτώσεις για το περιβάλλον. Οι αισθητήρες συλλέγουν πληροφορίες για τις συνθήκες του εδάφους, πχ. υγρασίας, θερμοκρασίας, συστατικών εδάφους, επίπεδα του pH, σύσταση ατμόσφαιρας, χρώμα φύλλων και διάμετρο στελέχους των φυτών, που βοηθούν να γίνουν εκτιμήσεις για τη βέλτιστη πυκνότητα με την οποία πρέπει να τοποθετηθούν οι σπόροι ή να φυτεύονται τα φυτά, να υπολογιστεί η ποσότητα λιπασμάτων που απαιτούνται στο έδαφος, να βρεθούν άλλες απαιτήσεις για τις καλλιέργειες και να γίνει μία πρόβλεψη με σχετική ακρίβεια της πιθανής ποσότητας συγκομιδής.

Εναλλακτικά συστήματα για παρακολούθηση των αγροτικών εκτάσεων είναι οι αεροφωτογραφίες, η χαρτογράφηση και οι εικόνες από δορυφόρο. Όμως τα ασύρματα δίκτυα αισθητήρων είναι ένας πιο εύκολος και πιο οικονομικός τρόπος για να γίνεται η παρακολούθηση των αγροτικών περιοχών.

Συνθήκες Αγροτικών καλλιεργειών.

Πλεονέκτημα των ασύρματων δικτύων αισθητήρων, είναι ότι μπορούν να λαμβάνουν σε πραγματικό χρόνο, τιμές από μεταβλητές, για τις συνθήκες που επικρατούν στις καλλιέργειες και σε όλη την αγροτική περιοχή ή/και μεμονωμένα σε ξεχωριστά φυτά. Όμως, συνήθως η αποστολή των δεδομένων από τους κόμβους αισθητήρες προς τον κεντρικό κόμβο sink, δεν γίνεται συνεχώς, αλλά κάθε μία ώρα. Αυτό συμβαίνει για να μην υπερφορτώνεται το λογισμικό με πολλά δεδομένα τα οποία δεν προλαβαίνει να τα διαχειριστεί και επίσης να μην εξαντλείται γρήγορα η ενέργεια των αισθητήρων καθώς στέλνουν τα δεδομένα. Το περιβάλλον κάθε περιοχής, μπορεί να απαιτεί εξειδικευμένο λογισμικό ανάλογα με τον τύπο του εδάφους και τα συγκεκριμένα φυτά που καλλιεργούνται, ώστε να υπολογίζει τις ακριβείς ποσότητες νερού, λιπασμάτων και εντομοκτόνων που χρειάζονται.

Επειδή οι αισθητήρες βρίσκονται σε αγροτική περιοχή, η τροφοδοσία των αισθητήρων είναι εφικτό να γίνεται και με ηλιακή ενέργεια ή με αιολική ενέργεια.

Όταν η ηλιακή ενέργεια συνδυάζεται με μπαταρίες υψηλής απόδοσης τότε οι αισθητήρες λειτουργούν χωρίς άλλη εξωτερική πηγή ενέργειας. Η χρήση της ηλιακής ενέργειας δίνει μεγαλύτερη διάρκεια ζωής στο δίκτυο (life cycle) και δίνει δυνατότητα να χρησιμοποιούνται μικρότερες μπαταρίες στις συσκευές και έτσι να μειωθεί το μέγεθος των συσκευών συνολικά.

Επιτήρηση στρατιωτικών περιοχών.

Υπάρχουν πολλές εφαρμογές για στρατιωτικούς σκοπούς. Ασύρματα δίκτυα αισθητήρων μπορούν να χρησιμοποιούνται για επίβλεψη περιοχών, αναγνώριση εχθρικού εδάφους, στόχευση, συστήματα πληροφοριών, συναγερμών κλπ.

Για παράδειγμα, υπάρχουν στόχοι στα πεδία μαχών, που μπορεί να μην αναγνωρίζονται εύκολα, διότι είναι μικροί σε μέγεθος και κινούνται με μεγάλες ταχύτητες. Ο εντοπισμός τέτοιων στόχων επιτυγχάνεται τοποθετώντας πυκνά ασύρματα δίκτυα αισθητήρων στο εχθρικό έδαφος ώστε να επιτρέπεται η παρακολούθηση του χώρου. Τα οπλικά συστήματα μπορεί να εστιάζουν στο στόχο λαμβάνοντας δεδομένα από το ασύρματο δίκτυο αισθητήρων.

Πριν από την προώθηση στρατιωτικών μονάδων σε μία άγνωστη περιοχή, μπορεί να προηγηθεί μία ρίψη αισθητήρων από αεροπλάνα και να γίνει η διασπορά τους στο χώρο. Έτσι σχηματίζεται ένα πυκνό ασύρματο δίκτυο αισθητήρων. Στη συνέχεια εισβάλλουν οι στρατιώτες και καθώς κινούνται μέσα στον εχθρικό χώρο λαμβάνουν πληροφορίες από τους αισθητήρες για διάφορα

στοιχεία της περιοχής και αποκτούν γνώση για την ακριβή θέση που βρίσκονται εμπόδια, οπλισμός, και τι αντικείμενα υπάρχουν κοντά σε αυτούς.

Επίσης με τους αισθητήρες, μπορεί να γίνει ένας έλεγχος των στρατιωτικών χώρων για να διαπιστωθεί αν έχουν εισβάλλει εχθροί, ή να ελεγχθεί αν υπάρχουν στο έδαφος και στην ατμόσφαιρα επικίνδυνες ουσίες, αέρια, ή χημικά όπλα και εκρηκτικά, να γίνει αναγνώριση μολυσμένων περιοχών και να ενεργοποιούνται συναγερμοί όταν ανιχνευθεί κάποιος κίνδυνος. Άλλες πιθανές στρατιωτικές εφαρμογές είναι: Επιτήρηση των χώρων εξοπλισμού, των καυσίμων και των πυρομαχικών, αναγνώριση του εχθρικού οπλισμού, εκτίμηση των καταστροφών.

Εφαρμογές στο περιβάλλον.

Οι μεταβλητές περιβάλλοντος που παρατηρούνται, όπως π.χ. η θερμοκρασία, υγρασία είναι κατανοημένες σε μία μεγάλη περιοχή. Η χρήση ασύρματου δικτύου επιτρέπει να λαμβάνονται μετρήσεις χωρίς να δημιουργούνται μεγάλες επεμβάσεις στο περιβάλλον.

Μερικές εφαρμογές για το περιβάλλον είναι η παρακολούθηση άγριων ζώων στη φύση, η επιτήρηση των δασών, παρακολούθηση πυρκαγιών σε δάση, η ανίχνευση πλημμυρών, η παρατήρηση του καιρού, η παρακολούθηση μόλυνσης του περιβάλλοντος, παρακολούθηση ποιότητας νερού, παρακολούθηση παγετώνων,

εξερεύνηση για παρουσία ορυκτών και μεταλλευμάτων σε ορισμένες περιοχές.

Διαχείριση καταστροφών

Τα ασύρματα δίκτυα αισθητήρων μπορούν να αξιοποιηθούν σε μεγάλες καταστροφές και σε επιχειρήσεις αναζήτησης και διάσωσης ανθρώπων που βρίσκονται σε κίνδυνο. Ο εντοπισμός παγιδευμένων ατόμων μέσα σε συντρίμια, μπορεί να βοηθηθεί ανιχνεύοντας διάφορα στοιχεία που δηλώνουν την παρουσία ατόμων. Για παράδειγμα από την αναπνοή τους μπορούν να εντοπιστούν άτομα που είναι παγιδευμένα σε έναν χώρο. Στην περιοχή καταστροφής μπορεί να γίνει ρίψη αισθητήρων για να εντοπιστούν θύματα.

Όταν κατασκευάζονται τα κτήρια μπορούν να τοποθετούνται ασύρματα δίκτυα αισθητήρων σε αυτά, για να παρακολουθούν τη σεισμική δραστηριότητα στις πόλεις. Στην περίπτωση που υπάρχουν ενδείξεις ότι πλησιάζει σεισμός, θα μπορούσαν να ειδοποιούνται οι ένοικοι των κτηρίων για να απομακρύνονται από τα κτήρια μέχρι να περάσει ο σεισμός.

Οι ορειβάτες που κινδυνεύουν συχνά, μπορούν να διαθέτουν αισθητήρες στον φορητό εξοπλισμό τους, ώστε αν συμβούν κατολισθήσεις και καταπλακωθούν από βράχους ή από χιονοστιβάδες, να εντοπίζονται πιο γρήγορα από τις ομάδες διάσωσης.

Αντίδραση σε επείγουσες καταστάσεις

Σε χώρους που μπορούν να πιάσουν εύκολα φωτιά, όπως εργοστάσια, δασικές εκτάσεις ή αποθήκες εύφλεκτων υλικών μπορεί να υπάρχει μία συνεχής επιτήρηση με ασύρματα δίκτυα αισθητήρων. Με αυτό τον τρόπο γίνεται ένας έλεγχος για την πρόληψη ατυχημάτων. Διάφοροι ανιχνευτές καπνού που τοποθετούνται σε σημεία υψηλού κινδύνου εμφάνισης πυρκαγιάς, όπως δάση, κτήρια, εργοστάσια, σπίτια μπορούν να συμβάλλουν στην ανίχνευση εξάπλωσης της πυρκαγιάς.

Για παράδειγμα αν σε ένα δάσος ανάψει μία φωτιά τοπικά μπορεί να εντοπίζεται από τους αισθητήρες η ακριβής θέση της φωτιάς και να ενεργοποιείται ένας συναγερμός άμεσα στους πυροσβέστες ώστε να την σβήνουν γρήγορα πριν εξαπλωθεί σε μεγαλύτερη έκταση.

Εφαρμογές υγείας στην Ιατρική και στη Βίο-Ιατρική

Παρακολούθηση υγείας, μετρήσεις των επιπέδων ουσιών στο αίμα, ρυθμός της καρδιάς είναι κάποια στοιχεία που ανιχνεύονται. Αισθητήρες μπορούν να τοποθετηθούν σε νοσοκομεία, για να παρακολουθούν σημαντικές παραμέτρους και να αναφέρουν τις αποκλίσεις από τις φυσιολογικές τιμές. Μπορούν να ελέγχουν τις ανάγκες των ασθενών. Ειδικοί αισθητήρες που ελέγχουν την πίεση του αίματος, τη θερμοκρασία σώματος, και το ηλεκτροκαρδιογράφημα ECG μπορούν ακόμα και να ράβονται πάνω στην ύφανση των ρούχων ή των σκεπασμάτων του ασθενούς. Για ηλικιωμένα άτομα μπορεί να γίνεται μία επιτήρηση από απόσταση ώστε να καταγράφονται πληροφορίες που αφορούν την κατάσταση τους και να ειδοποιείται με κάποιο συναγερμό ο νοσηλευτής αν υπάρχει πρόβλημα στον ασθενή.

Στο κτήριο του νοσοκομείου οι αισθητήρες μπορούν να ελέγχουν τον φωτισμό και τη θερμοκρασία. Στον ασθενή μπορούν να ελέγχουν την παρουσία οξυγόνου, την παρουσία ορού και άλλα στοιχεία.

Ένα ειδικό είδος δικτύου αισθητήρων σώματος (body sensor network) (BSN) έχει αναπτυχθεί για αισθητήρες που φοριούνται ή εμφυτεύονται για να στέλνουν συνεχείς πληροφορίες σε πραγματικό χρόνο και να γίνονται καταγραφές για την κατάσταση του ασθενή μέσω δικτύου.

Σε περιοχές όπου υπάρχουν επικίνδυνες μολυσματικές ασθένειες μπορούν να τοποθετηθούν ασύρματα δίκτυα αισθητήρων και να συλλέξουν πληροφορίες για την εξάπλωση των ιών. Επιπλέον, η μέτρηση μεγεθών από το περιβάλλον όπως η υγρασία, οι βροχοπτώσεις, μπορούν οδηγήσουν σε εκτιμήσεις ότι το περιβάλλον είναι επικίνδυνο για να αναπτυχθούν και να εξαπλωθούν επικίνδυνοι ιοί που προκαλούν ασθένειες και να προβλεφθεί ο κίνδυνος ξεσπάσματος επιδημιών λαμβάνοντας κατάλληλα μέτρα προστασίας.

Έξυπνο Σπίτι, έξυπνα κτήρια, έξυπνα γραφεία.

Οι αισθητήρες ελέγχουν οικιακές συσκευές μέσα στο σπίτι.

Ο φωτισμός και η θέρμανση στα κτήρια μπορεί να ελέγχεται με ασύρματα δίκτυα αισθητήρων.

Μια μελλοντική εφαρμογή για τα έξυπνα κτήρια είναι η δημιουργία του έξυπνου χώρου. Σε ένα σπίτι ενσωματώνονται αισθητήρες σε οικιακές συσκευές και σε έπιπλα και έτσι δημιουργούν ένα ασύρματο δίκτυο αισθητήρων.

Ένα σενάριο χρήσης είναι το παρακάτω: Ελέγχονται συνεχώς τα τρόφιμα που βρίσκονται μέσα σε ένα ψυγείο. Αν αφαιρεθεί π.χ. ένα κοτόπουλο από το ψυγείο για να μαγειρευτεί, τότε ένας έξυπνος φούρνος μπορεί να λάβει από το ψυγείο μία ειδοποίηση και ο φούρνος να ρυθμιστεί αυτόματα σε ένα έτοιμο πρόγραμμα με κατάλληλη θερμοκρασία για το ψήσιμο.

Αν υπάρξει μόλυνση σε ένα τρόφιμο που βρίσκεται στο ψυγείο αρκετό καιρό, τότε μπορεί να χτυπήσει κάποιος συναγερμός.

Στις μεγαλουπόλεις κατασκευάζονται μεγάλα συγκροτήματα κτηρίων όπως είναι οι ουρανοξύστες, τα γραφεία εταιριών, τα εμπορικά κέντρα. Εκεί, υπάρχουν απαιτήσεις να ελέγχεται ο κλιματισμός των κτηρίων. Οι συνθήκες σε ένα μεγάλο κτήριο δεν είναι πάντα ιδανικές, ούτε είναι ίδιες σε όλους τους χώρους του. Με τη χρήση ασύρματων δικτύων αισθητήρων μπορεί να ελέγχεται η υγρασία, η θερμοκρασία, η ποιότητα της ατμόσφαιρας σε διάφορους χώρους του κτηρίου και με βάση αυτές τις πληροφορίες να ρυθμίζεται αυτόματα ο κλιματισμός για κάθε χώρο. Επίσης ο φωτισμός μπορεί να ρυθμίζεται αυτόματα, ανάλογα με την παρουσία προσωπικού ή όχι στο χώρο.

Κυκλοφορία δρόμων, κίνηση οχημάτων.

Η παρακολούθηση κυκλοφορίας των οχημάτων γίνεται συνήθως με κάμερες που τοποθετούνται σε διάφορα κεντρικά σημεία των οδών που έχουν μεγάλη κυκλοφορία. Επειδή όμως οι κάμερες αυτές έχουν ακριβό κόστος, το πλήθος τους δεν επαρκεί για να καλύψουν όλους τους δρόμους που

χρειάζονται παρακολούθηση και έτσι τοποθετούνται μόνο σε περιορισμένα τμήματα των δρόμων.

Χρησιμοποιώντας επιπλέον τα ασύρματα δίκτυα αισθητήρων η ροή οδικής κυκλοφορίας μπορεί να παρακολουθείται σε περισσότερα και μεγαλύτερα τμήματα των δρόμων και να επιτρέπεται ακόμη και ο έλεγχος κυκλοφορίας μέχρι ένα βαθμό. Η τοποθέτηση των αισθητήρων μπορεί να γίνεται και στα αυτοκίνητα και σε σημεία του δρόμου για παρακολούθηση της κυκλοφορίας. Επειδή το κόστος των αισθητήρων είναι χαμηλό, μπορούν να τοποθετηθούν σε χώρους πάρκινγκ, στις πλευρές του δρόμου κατά μήκος μεγάλων δρόμων, ή στη διαχωριστική γραμμή του δρόμου ή σε άλλα σημεία. Μια εφαρμογή των αισθητήρων είναι η εύρεση του πλησιέστερου χώρου στάθμευσης για τα οχήματα, καθοδηγώντας τα σε ένα πάρκινγκ όπου υπάρχουν πολλά οχήματα. Ρυθμίσεις οδικής κυκλοφορίας σε πραγματικό χρόνο.

Στις διασταυρώσεις οδικών δικτύων, οι αισθητήρες μπορεί να είναι τοποθετημένοι στα φώτα του δρόμου ή στα φανάρια, ή να είναι θαμμένοι κάτω από το οδόστρωμα. Οι αισθητήρες αυτοί μπορούν να ανιχνεύουν τα διερχόμενα οχήματα και να ρυθμίζουν τα φανάρια ανάλογα με την κίνηση που ανιχνεύεται σε πραγματικό χρόνο. Με χρήση των αισθητήρων μπορεί να βελτιωθεί η κίνηση των οχημάτων προς τον προορισμό και να αποφεύγονται περιττές κινήσεις που θα οδηγήσουν τα οχήματα σε περιοχές με μποτιλιάρισμα.

Βιομηχανία και Εμπόριο

Πολλές εφαρμογές μπορούν να σχεδιαστούν για βιομηχανίες, εργοστάσια και βιομηχανικές αποθήκες, όπως είναι:

Έλεγχος προϊόντων αποθηκών, εξοπλισμός βιομηχανικών εγκαταστάσεων, συντηρήσεων, βιομηχανικός έλεγχος, έλεγχος ροής διεργασιών.

Στην παρούσα εργασία γίνεται εστίαση σε δίκτυα που χρησιμοποιούνται σε βιομηχανικές εφαρμογές.

Επιστημονικές εφαρμογές

Παρακολούθηση ωκεανών

Τα υποβρύχια δίκτυα αισθητήρων περιλαμβάνουν οχήματα και ρομπότ εξοπλισμένα με αισθητήρες που εκτελούν αποστολές σε διάφορες περιοχές του βυθού. Ένα κέντρο ελέγχου

συγκεντρώνει όλα τα δεδομένα. Ένας κινητός κόμβος, που μπορεί να είναι ένα ρομπότ, ή ένα υποβρύχιο όχημα έχει το ρόλο του κεντρικού κόμβου. Μέσα στον ωκεανό είναι τοποθετημένοι αισθητήρες. Ο κινητός κόμβος συλλέγει όλα τα δεδομένα από τους αισθητήρες και τα μεταφέρει στο κέντρο ελέγχου. Μερικές ενδείξεις που μετρούν οι αισθητήρες σε περιβάλλοντα ωκεανών είναι: περιεκτικότητα σε αλάτι, επίπεδα βακτηρίων, επίπεδα μόλυνσης, ωκεανογραφικά δεδομένα, ναυάγια, αρχαιολογικά ευρήματα, υπόγεια κοιτάσματα.

Μία άλλη χρήση των αισθητήρων σε ωκεανούς είναι η παρακολούθηση σεισμικής δραστηριότητας και η πληροφόρηση για κίνδυνο εμφάνισης επικίνδυνων κυμάτων.

Τα υποβρύχια δίκτυα λειτουργούν κυρίως με ήχους και όχι με ραδιοκύματα διότι ο ήχος διαδίδεται καλύτερα μέσα στο νερό. Για το σκοπό αυτό χρησιμοποιούνται μόντεμ με συχνότητες ήχου για τους αισθητήρες, όμως αυτό παρουσιάζει μειονεκτήματα διότι υπάρχει μικρή ταχύτητα μετάδοσης των ηχητικών σημάτων, υπάρχει μεγάλη καθυστέρηση και υπάρχει μεγάλος θόρυβος.

Παρακολούθηση οικοσυστημάτων

Σε περιβάλλοντα από διάφορα οικοσυστήματα μπορούν να τοποθετούνται ασύρματα δίκτυα αισθητήρων για πολλά χρόνια, και να αντικαθίστανται μετά την πάροδο ορισμένων ετών, ώστε να υπάρχει μία συνεχής και μακροχρόνια παρακολούθηση του οικοσυστήματος. Με αυτό τον τρόπο καταγράφονται μακροχρόνια διάφορα φαινόμενα με συνεχή ροή πληροφοριών που αφορούν τα οικοσυστήματα.

2.2 Στρώματα

Σε αυτή την ενότητα, αρχικά παρουσιάζεται το γενικό μοντέλο OSI-7 που αποτελείται από επτά στρώματα (layers). [7], [8].

Μετά παρουσιάζεται η στοίβα αρχιτεκτονικής στρωμάτων για τα ασύρματα δίκτυα αισθητήρων WSN.

Στην συνέχεια, γίνεται μία περιγραφή τις διαφορές που υπάρχουν στα ασύρματα δίκτυα αισθητήρων WSN σε σύγκριση με τα ασύρματα δίκτυα υπολογιστών. Αυτές οι διαφορές είναι ο λόγος για τον οποίο στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται διαφορετικά πρωτόκολλα, λιγότερο περίπλοκα, που μπορεί να έχουν λιγότερα επίπεδα από τα 7 στρώματα του μοντέλου OSI-7.

Επιπλέον υπάρχουν και άλλα πρωτόκολλα που χρησιμοποιούν τη μη-διαστρωματωμένη αρχιτεκτονική (cross-layered) δηλαδή τα δεδομένα που βρίσκονται σε ένα στρώμα αλληλοεπιδρούν συγχρόνως και με άλλα στρώματα.

2.2.1 Τα επίπεδα του μοντέλου OSI-7

Η αρχιτεκτονική των ασύρματων δικτύων στηρίζεται σε ένα σύνολο από στρώματα (ή επίπεδα). Τα στρώματα θεωρούνται ότι βρίσκονται το ένα πάνω από το άλλο ώστε να σχηματίζουν μία στοίβα (stack) που ονομάζεται layer stack (ή protocol stack). Σε κάθε στρώμα εκτελούνται συγκεκριμένες λειτουργίες στα δεδομένα.

Το μοντέλο OSI-7 είναι μοντέλο καταρράκτη. Αυτό σημαίνει ότι τα δεδομένα που βρίσκονται σε ένα στρώμα, πρώτα δέχονται επεξεργασία από εκείνο το στρώμα και στη συνέχεια πηγαίνουν στο επόμενο στρώμα και στο τέλος έχουν περάσει διαδοχικά από όλα τα στρώματα.

Για διαφορετικά πρότυπα υπάρχουν διαφορές στο σύνολο στρωμάτων δικτύου που χρησιμοποιούνται.

Γενικό μοντέλο που περιγράφει όλα τα στρώματα είναι το μοντέλο OSI-7.

Η περιγραφή των στρωμάτων ξεκινά από το χαμηλότερο επίπεδο και καταλήγει στο υψηλότερο επίπεδο.

Τα στρώματα σύμφωνα με το μοντέλο OSI-7, σε μορφή πίνακα συνοψίζονται στον πίνακα 2.1:

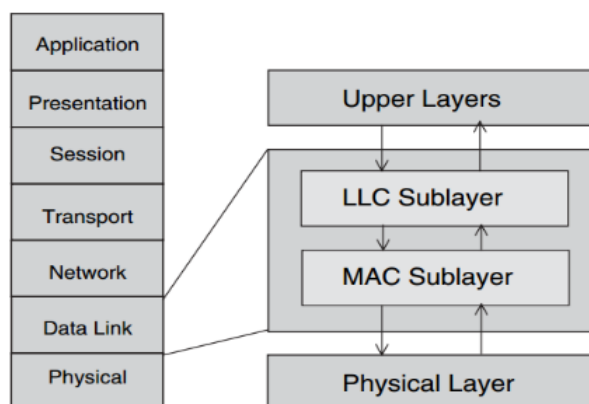
7ο Στρώμα	Επίπεδο Εφαρμογών (Application Layer)
6ο Στρώμα	Επίπεδο Παρουσίασης (Presentation Layer)
5ο Στρώμα	Επίπεδο Συνόδου (Session Layer)
4ο Στρώμα	Επίπεδο Μεταφοράς (Transport Layer)
3ο Στρώμα	Επίπεδο Δικτύου (Network Layer)
2ο Στρώμα	Επίπεδο Ζεύξης δεδομένων (Data Link Layer, DLL)
1ο Στρώμα	Φυσικό Επίπεδο (Physical Layer ή PHY Layer)

Πίνακας 2.1: Στοιβά στρωμάτων για το OSI-7. Το χαμηλότερο επίπεδο είναι το φυσικό επίπεδο (PHY layer) ενώ το υψηλότερο επίπεδο είναι το επίπεδο εφαρμογής (Application Layer).

Το Επίπεδο ζεύξης δεδομένων (Data Link Layer) αποτελείται από δύο υπό-επίπεδα (sublayers):

Επίπεδο λογικού ελέγχου ζεύξης Logical Link Control (LLC) layer

και επίπεδο πρόσβασης μέσου Medium Access Control (MAC) layer.



Εικόνα 7 Το στρώμα Data Link Layer αποτελείται από τα υποεπίπεδα LLC και MAC. Πηγή: [1]

2.2.2 Στρώματα του ασύρματου δικτύου αισθητήρων WSN

Σε ένα ασύρματο δίκτυο αισθητήρων WSN τα πρωτόκολλα έχουν λιγότερη πολυπλοκότητα και μερικά στρώματα διαφέρουν από αυτά που έχει το γενικό πρωτόκολλο OSI-7. Οι λόγοι που υπάρχουν διαφορές εξηγούνται παρακάτω στην παράγραφο 2.3.

Σε μία αρχιτεκτονική στοίβας στρωμάτων για ένα ασύρματο δίκτυο αισθητήρων, συνήθως δεν περιέχονται όλα τα στρώματα του μοντέλου OSI-7 αλλά μόνο ορισμένα. [7]

Ένα πρωτόκολλο για ασύρματα δίκτυα αισθητήρων απαιτείται να έχει τουλάχιστον τα παρακάτω τέσσερα στρώματα:

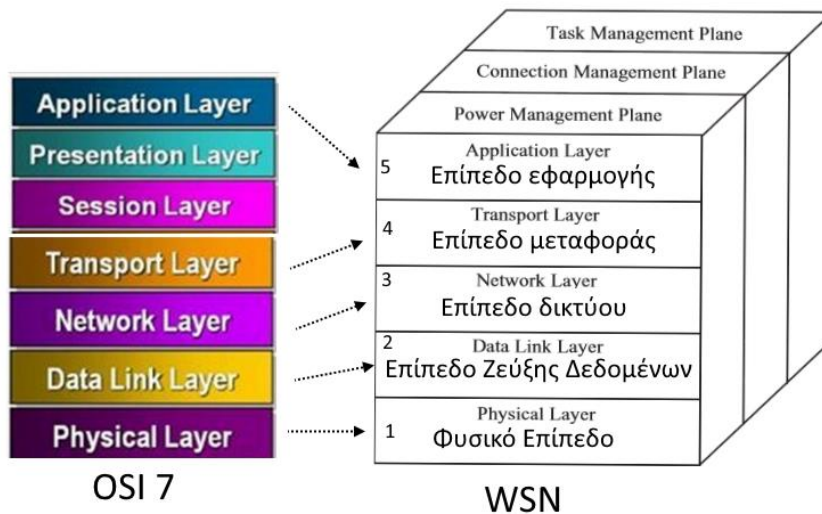
α) το στρώμα φυσικού επιπέδου (PHY Layer)

β) το στρώμα medium access control (MAC) layer που είναι το στρώμα πρόσβασης μέσου, και είναι υπό-στρώμα (sublayer) του επιπέδου ζεύξης δεδομένων (Data Link Layer). Το στρώμα MAC βρίσκεται ακριβώς πάνω από το φυσικό στρώμα.

γ) το στρώμα δικτύου (Network layer)

δ) το στρώμα εφαρμογής (Application layer).

Στην παρακάτω εικόνα φαίνεται μία γενική μορφή αρχιτεκτονικής πέντε στρωμάτων που χρησιμοποιείται στα ασύρματα δίκτυα αισθητήρων και γίνεται μία σύγκριση με τα επτά στρώματα του μοντέλου OSI-7. Συνήθως στο ασύρματο δίκτυο αισθητήρων υπάρχουν τουλάχιστον τα τέσσερα στρώματα αλλά κάποιες φορές υπάρχουν τα πέντε που φαίνονται στην εικόνα.



Εικόνα 8 Στοίβα στρωμάτων για τα ασύρματα δίκτυα αισθητήρων (WSN) και διαφορά από το μοντέλο OSI 7

Στις επόμενες παραγράφους γίνεται μία σύντομη παρουσίαση για τα 5 στρώματα της στοίβας που υπάρχουν στην αρχιτεκτονική των ασύρματων δικτύων αισθητήρων, ξεκινώντας από το χαμηλότερο επίπεδο.

2.2.2.1 Φυσικό επίπεδο (PHY Layer)

Το 1ο στρώμα είναι το φυσικό επίπεδο (physical layer) που είναι το χαμηλότερο. Στο φυσικό επίπεδο διαμορφώνεται το σήμα που θα μεταδοθεί στο κανάλι, που είναι το φυσικό μέσο επικοινωνίας. Απαιτείται να υπάρχει μία απλή διαμόρφωση του σήματος αλλά να είναι ανθεκτική σε παρεμβολές. Επιπλέον στο φυσικό επίπεδο, γίνεται επιλογή συχνότητας και παράγεται η συχνότητα του σήματος που θα μεταδοθεί. Τα δεδομένα πρώτα κρυπτογραφούνται, και στη συνέχεια, γίνεται η μετάδοση (transmission) και η λήψη (receiving) των δεδομένων, μέσα από το κανάλι επικοινωνίας.

Η διαμόρφωση και η από-διαμόρφωση του σήματος εκτελούνται από τον ασύρματο πομποδέκτη. Η τεχνική διαμόρφωσης πρέπει να μην έχει αρκετά μεγάλη πολυπλοκότητα, ώστε να μην είναι αυξημένο το κόστος του αισθητήρα. Το υλικό (hardware) του αισθητήρα πρέπει να είναι σχετικά απλό, χαμηλού κόστους, αλλά η αξιοπιστία στις μετρήσεις χρειάζεται να είναι όσο το δυνατόν μεγαλύτερη.

Για τη μετάδοση των σημάτων, χρησιμοποιούνται οι τεχνικές του εξαπλωμένου φάσματος (spread spectrum). Στις τεχνικές εξαπλωμένου φάσματος, οι κυματομορφές που εκπέμπονται, έχουν ένα εύρος ζώνης (bandwidth) που είναι αρκετά μεγαλύτερο από το ελάχιστο εύρος ζώνης που απαιτείται για να μεταδοθούν τα δεδομένα. Αυτές οι τεχνικές μετάδοσης χρησιμοποιούνται επειδή έχουν κάποια πλεονεκτήματα. Ένα θετικό αποτέλεσμα που έχουν οι τεχνικές εξαπλωμένου φάσματος είναι ότι το σήμα μεταδίδεται σε μεγάλο εύρος συχνοτήτων. Έτσι αν σε κάποιες συχνότητες παρουσιαστούν παρεμβολές από άλλα σήματα, τότε θα επηρεαστεί μόνο ένα μέρος του σήματος, που εκπέμπεται σε εκείνες τις συχνότητες, ενώ το μεγαλύτερο μέρος του σήματος θα μεταδοθεί κανονικά επειδή είναι πιθανό ότι στις υπόλοιπες συχνότητες που δεν θα υπάρχουν παρεμβολές. Επιπλέον, το μεταδιδόμενο σήμα, θα έχει μεγαλύτερη αντίσταση στην εξασθένιση, διότι η εξασθένιση θα παρουσιαστεί μόνο σε μερικές συχνότητες ενώ σε άλλες όχι.

Μια άλλη απαίτηση είναι η ασφάλεια από υποκλοπές του σήματος. Αν το σήμα εκπέμπεται με τεχνικές εξαπλωμένου φάσματος και κάποιος επιχειρήσει να υποκλέψει μία συχνότητα, θα λάβει τα δεδομένα μόνο από ένα μικρό μέρος του σήματος και δεν θα είναι εύκολο να αποκρυπτογραφήσει ολόκληρο το σήμα.

Άλλο πλεονέκτημα είναι ότι στο ίδιο κανάλι μπορούν να εκπέμπουν διαφορετικές συσκευές χωρίς να προκαλούν πολλές παρεμβολές η μία στην άλλη.

2.2.2.2 Επίπεδο Ζεύξης Δεδομένων (Data Link Layer)

Το επίπεδο ζεύξης δεδομένων (data link layer) είναι το 2ο στρώμα και εκτελεί πολυπλεξία σε ροές δεδομένων (data streams), ανίχνευση πλαισίων δεδομένων (frame detection). Έχει το υποεπίπεδο ελέγχου πρόσβασης μέσου Media Access Control (MAC) και εκτελεί έλεγχο σφαλμάτων (error control). Συχνά το περιβάλλον έχει πολλές παρεμβολές και μπορεί να υπάρχουν κινητοί κόμβοι, για αυτό, το υποεπίπεδο MAC πρέπει να έχει επίγνωση της κατανάλωσης ενέργειας και να μπορεί να ελαχιστοποιεί τις συγκρούσεις με εκπομπές δεδομένων από τους γειτονικούς κόμβους.

Το πρωτόκολλο του επιπέδου ζεύξης χρησιμοποιείται προκειμένου να μεταφέρει ένα δεδομένογραμμα (datagram) ή πακέτο επάνω σε μία ζεύξη. Ορίζει τη μορφή των πακέτων που ανταλλάσσονται ανάμεσα στους κόμβους, στα άκρα της ζεύξης, καθώς και τις ενέργειες που γίνονται από αυτούς τους κόμβους όταν στέλνουν και λαμβάνουν αυτά τα πακέτα. Οι μονάδες δεδομένων που ανταλλάσσονται από ένα πρωτόκολλο επιπέδου ζεύξης ονομάζονται πλαίσια

(frames) και συνεπώς οι ενέργειες που γίνονται από αυτά τα πρωτόκολλα κατά την αποστολή και λήψη τους είναι η ανίχνευση σφάλματος, η αναμετάδοση, ο έλεγχος ροής και η τυχαία πρόσβαση. Το πρωτόκολλο αυτό σε ένα ασύρματο multi-hop και αυτο-οργανούμενο δίκτυο αισθητήρων, έχει ως στόχους τη δημιουργία της υποδομής του δικτύου και το δίκαιο και αποδοτικό διαχωρισμό των πόρων επικοινωνίας μεταξύ των κόμβων του δικτύου.

Για τον έλεγχο σφαλμάτων (error control) υπάρχουν δύο μέθοδοι:

α) Έλεγχος σφαλμάτων με αυτόματη αίτηση επανάληψης (Automatic Repeat Request-ARQ).

Η μέθοδος ARQ στα ασύρματα δίκτυα αισθητήρων πολλαπλών αλμάτων (multi-hop) έχει δύο περιορισμούς. Υπάρχει επιπλέον κόστος ενέργειας για την αναμετάδοση αιτήσεων και υπάρχει το overhead.

β) Διόρθωση σφάλματος χωρίς επαλήθευση (Forward Error Correction-FEC)

Η μέθοδος FEC έχει μια μεγάλη πολυπλοκότητα αποκωδικοποίησης, διότι ενσωματώνει κώδικες ελέγχου σφαλμάτων (error control).

Για αυτό προτιμούνται οι απλοί κώδικες ελέγχου σφαλμάτων (error control) ώστε η κωδικοποίηση και αποκωδικοποίηση να έχουν μικρότερη πολυπλοκότητα και να χρησιμοποιηθούν στα ασύρματα δίκτυα αισθητήρων.

2.2.2.3 Επίπεδο Δικτύου (Network Layer)

Το επίπεδο δικτύου (network layer) είναι το 3ο στρώμα. Το επίπεδο δικτύου αναλαμβάνει τη δρομολόγηση (routing) των δεδομένων, τα οποία έρχονται από το επίπεδο μεταφοράς (transport layer). Η δρομολόγηση γίνεται με συγκεκριμένα πρωτόκολλα ασύρματης επικοινωνίας πολλαπλών αλμάτων (multi-hop) και τα δεδομένα μεταφέρονται από τους κόμβους αισθητήρες (sensor nodes) στον κεντρικό κόμβο sink.

Στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται τεχνικές δρομολόγησης διαφορετικές από αυτές που χρησιμοποιούνται στα ασύρματα δίκτυα υπολογιστών, που λέγονται ad-hoc.

Μια από τις αρμοδιότητες του network layer είναι να παρέχει διασύνδεση με εξωτερικά δίκτυα (πχ. άλλα δίκτυα αισθητήρων ή το διαδίκτυο).

Βασικές αρχές για το επίπεδο δικτύου είναι οι παρακάτω:

α) Πρέπει να έχει αποτελεσματική διαχείριση της ενέργειας τροφοδοσίας.

β) Απαιτείται να είναι εστιασμένο στα δεδομένα δηλαδή να είναι data-centric.

γ) Πρέπει να επιτρέπει συγκέντρωση των δεδομένων (data aggregation). Αλλά αυτή η συγκέντρωση θα πρέπει να συντελείται χωρίς να παρεμποδίζει τη συνεργασία ανάμεσα στους κόμβους αισθητήρες.

δ) Για να θεωρηθεί ένα ασύρματο δίκτυο αισθητήρων ότι είναι ιδανικό, θα πρέπει να δίνονται διευθύνσεις στους κόμβους που να βασίζονται σε ιδιότητες (attribute-based) και να υπάρχει επίγνωση της τοποθεσίας.

Διαδρομές δρομολόγησης που είναι αποτελεσματικές ως προς τη διαχείριση ενέργειας (energy-efficient) αναζητούνται είτε με βάση τη διαθέσιμη εναπομένουσα ενέργεια σε κάθε κόμβο (available power - PA) είτε με βάση την ενέργεια που απαιτείται για τη μετάδοση δεδομένων μέσω των διαδρομών δρομολόγησης. Γνωστοί αλγόριθμοι για επιλογή της βέλτιστης διαδρομής δρομολόγησης ως προς την εξοικονόμηση ενέργειας είναι:

Maximum PA route, επιλέγεται η διαδρομή δρομολόγησης που έχει τη μεγαλύτερη συνολική εναπομένουσα ενέργεια για τους κόμβους, η οποία υπολογίζεται αθροίζοντας μαζί όλες τις εναπομένουσες ενέργειες των κόμβων που ανήκουν στην συγκεκριμένη διαδρομή δρομολόγησης.

Minimum energy (ME) route, επιλέγεται το δρομολόγιο το οποίο απαιτεί την ελάχιστη ενέργεια για τη μεταφορά των πακέτων μεταξύ των κόμβων.

Minimum hop route (MH), επιλέγεται το δρομολόγιο το οποίο θα έχει τον ελάχιστο αριθμό αλμάτων (hops) μέχρι το κόμβο που θα λάβει τα δεδομένα.

Maximum minimum PA note route, επιλέγεται το δρομολόγιο του οποίου η ελάχιστη εναπομένουσα ενέργεια θα είναι μεγαλύτερη από την ελάχιστη εναπομένουσα ενέργεια των υπολοίπων δρομολογίων.

2.2.2.4 Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς (transport layer) είναι το 4ο στρώμα. Έχει ως ρόλο του να διατηρεί την ροή δεδομένων όταν απαιτηθεί από κάποια εφαρμογή του δικτύου αισθητήρων. Η χρησιμότητα

του επιπέδου μεταφοράς είναι κυρίως ότι επιτρέπει σε ένα ασύρματο δίκτυο αισθητήρων, να δέχεται πρόσβαση από το διαδίκτυο, αν το σύστημα είναι σχεδιασμένο έτσι ώστε να διαθέτει αυτή τη δυνατότητα. Επίσης επιτρέπει στο σύστημα να συνδεθεί σε άλλα εξωτερικά δίκτυα.

Τα πρωτόκολλα για το επίπεδο μεταφοράς που χρησιμοποιούνται στα ασύρματα δίκτυα αισθητήρων δεν είναι ίδια με το TCP που χρησιμοποιείται στο διαδίκτυο. Επειδή οι κόμβοι του ασύρματου δικτύου αισθητήρων έχουν μικρή μνήμη, δεν μπορούν να υποστηρίξουν πρωτόκολλα που μοιάζουν στη δομή τους με το πρωτόκολλο TCP για αυτό χρειάζονται ένα άλλο πρωτόκολλο που να είναι λιγότερο πολύπλοκο. Έχουν γίνει συνολικά περιορισμένες προσπάθειες για να σχεδιαστεί το επίπεδο μεταφοράς και γενικά δεν έχουν προταθεί αρκετές προσεγγίσεις.

2.2.2.5 Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής (application layer) είναι το 5ο και υψηλότερο στρώμα. Διάφορες εφαρμογές λογισμικού χρησιμοποιούν το επίπεδο εφαρμογής (application layer) ανάλογα με τις διεργασίες που πρέπει να εκτελεστούν από τη συσκευή. Το στρώμα εφαρμογής έχει το ρόλο να καθιστά τα χαμηλότερα στρώματα διαφανή για τον τελικό χρήστη, δηλαδή να αποκρύπτει από τον τελικό χρήστη τις λειτουργίες που εκτελούν τα χαμηλότερα στρώματα που αφορούν το υλικό (hardware) και το λογισμικό (software).

Στα ασύρματα δίκτυα αισθητήρων, έχουν σχεδιαστεί πρωτόκολλα, για το επίπεδο εφαρμογής και υπάρχουν πάρα πολλά, κυρίως πρωτόκολλα διαχείρισης δεδομένων.

Μεταξύ άλλων, υπάρχουν και τα παρακάτω πρωτόκολλα για το στρώμα εφαρμογής:

- α) Sensor Management Protocol (SMP) (Πρωτόκολλο διαχείρισης αισθητήρων).
- β) Task Assignment and Data advertisement Protocol (TADAP) (Πρωτόκολλο ανάθεσης των διεργασιών και «διαφήμισης» των δεδομένων).
- γ) Sensor Query and Data Dissemination Protocol (SQDDP) (Πρωτόκολλο ερώτησης αισθητήρων και διάδοσης δεδομένων).

2.2.2.6 Τα 3 επίπεδα Planes

Επιπλέον υπάρχουν τα 3 επίπεδα που ονομάζονται Planes. Αυτά είναι:

α) Power Plane

Παρακολουθεί την κατανομή ενέργειας ανάμεσα στους κόμβους αισθητήρες

β) Mobility Plane

Παρακολουθεί την κινητικότητα των κόμβων αισθητήρων

γ) Task Management Plane

Παρακολουθεί την κατανομή των διεργασιών που υπάρχει ανάμεσα στους κόμβους αισθητήρες.

Αυτά τα επίπεδα planes βοηθούν τους κόμβους αισθητήρες (sensor nodes) να συνεργάζονται και συντονίζουν τις διεργασίες τους ώστε να μειώνεται η κατανάλωση ενέργειας τροφοδοσίας συνολικά στο δίκτυο.

2.2.3 Τα Ασύρματα Δίκτυα Αισθητήρων διαφέρουν από τα ασύρματα δίκτυα υπολογιστών Ad Hoc

Τα ασύρματα δίκτυα αισθητήρων WSNs είναι δίκτυα κόμβων όπου για να μεταφερθούν οι πληροφορίες γίνονται πολλαπλά άλματα ανάμεσα σε κόμβους (multihop networks).

Υπάρχουν πολλά διαφορετικά πρωτόκολλα επικοινωνιών και τα πρωτόκολλα για ασύρματα δίκτυα υπολογιστών Wi-Fi διαφέρουν από τα πρωτόκολλα για ασύρματα δίκτυα αισθητήρων WSN. Αυτό συμβαίνει διότι οι αισθητήρες δεν είναι υπολογιστές, αλλά είναι συσκευές που διαθέτουν περιορισμένη υπολογιστική ισχύ, μνήμη και περιορισμένη διάρκεια ζωής μπαταρίας.

Τα δίκτυα υπολογιστών μεταξύ ισότιμων κόμβων λέγονται δίκτυα ad-hoc και έχουν αρκετές διαφορές από τα ασύρματα δίκτυα αισθητήρων WSN.

Μία βασική διαφορά είναι το πρωτόκολλο που χρησιμοποιείται.

Για τα ασύρματα δίκτυα υπολογιστών WiFi χρησιμοποιείται η οικογένεια προτύπων IEEE 802.11 b/g/n, ενώ για τα ασύρματα δίκτυα αισθητήρων χρησιμοποιείται το πρότυπο IEEE 802.15.4.

Οι ασύρματοι αισθητήρες είναι συσκευές χαμηλού κόστους.

Για αυτό δεν εκτελούν τόσο περίπλοκες λειτουργίες όπως οι υπολογιστές. Επειδή οι μπαταρίες στους αισθητήρες έχουν περιορισμένη διάρκεια, οι αισθητήρες συχνά μπαίνουν σε κατάσταση ύπνου sleep mode για εξοικονόμηση ενέργειας μπαταρίας. Σε μερικές περιπτώσεις χρησιμοποιείται ηλιακή ενέργεια για επαναφόρτιση των μπαταριών.

Επιπλέον, όταν υπάρχει μία μεγάλη πυκνότητα κόμβων στο δίκτυο αισθητήρων, ή υπάρχει ένα περιβάλλον δύσκολο στην πρόσβαση, δεν μπορεί να γίνεται σε τακτική βάση η αλλαγή μπαταριών στις συσκευές του δικτύου αισθητήρων. Συχνά όταν ένας κόμβος αισθητήρας πάθει βλάβη δεν αντικαθίσταται αμέσως και μπορεί να αντικατασταθεί αργότερα σε μία προγραμματισμένη συντήρηση, ή και καθόλου. Το δίκτυο όμως συνεχίζει να λειτουργεί κανονικά παρά την αστοχία ορισμένων κόμβων αισθητήρων.

Τα πρωτόκολλα σχεδιάζονται με στόχο να διαχειριστούν την ενέργεια με αποτελεσματικό τρόπο ώστε να υπάρχει ελάχιστη κατανάλωση και έτσι να μεγιστοποιηθεί η διάρκεια ζωής του δικτύου.

Οι κόμβοι σε ένα ασύρματο δίκτυο αισθητήρων στέλνουν τα δεδομένα τους με χαμηλό ρυθμό και συχνά χρησιμοποιούν τον πλεονασμό δηλαδή επαναμεταδόσεις των ίδιων πακέτων δεδομένων για να εξασφαλιστεί ότι έφτασαν στον προορισμό τους.

Μερικές διαφορές των ασύρματων δικτύων υπολογιστών σε σύγκριση με τα ασύρματα δίκτυα αισθητήρων αναφέρονται [9] παρακάτω:

α) Διαφορές ως προς την κινητικότητα (mobility). Στα ασύρματα δίκτυα υπολογιστών (ad hoc) η κινητικότητα (mobility) υπάρχει σε όλους τους φορητούς υπολογιστές και τις συσκευές τάμπλετ. Αντίθετα η κινητικότητα στα WSNs δεν υπάρχει σε όλους τους κόμβους αλλά αφορά ένα υποσύνολο των κόμβων. Οι περισσότεροι κόμβοι είναι στατικοί και μερικοί κόμβοι είναι κινητοί. Επίσης η κινητικότητα σε ένα ασύρματο δίκτυο αισθητήρων σχεδιάζεται ειδικά με βάση τις συγκεκριμένες εφαρμογές για τις οποίες χρησιμοποιείται. Ανάλογα με την εφαρμογή καθορίζεται ποιοι κόμβοι θα είναι κινητοί και ποιοι θα είναι σταθεροί.

β) Πλήθος των κόμβων του δικτύου. Σε ένα ασύρματο δίκτυο υπολογιστών οι κόμβοι είναι πολύ λιγότεροι από ότι σε ένα ασύρματο δίκτυο αισθητήρων. Σε μεγάλο δίκτυο υπολογιστών μπορεί να υπάρχουν μερικές εκατοντάδες κόμβοι. Σε μεγάλα ασύρματα δίκτυα αισθητήρων WSNs μπορεί να υπάρχουν χιλιάδες κόμβοι. Αυτό ισχύει διότι οι κόμβοι αισθητήρες έχουν χαμηλή υπολογιστική ικανότητα και περιορισμένες δυνατότητες αποθήκευσης δεδομένων και έτσι το κόστος τους είναι σχετικά χαμηλό.

γ) Ενέργεια τροφοδοσίας και διαθεσιμότητα υπολογιστικών πόρων. Σε ένα δίκτυο υπολογιστών (ad hoc) ο φορητός υπολογιστής Laptop ή μία συσκευή tablet είναι κινητοί κόμβοι (portable). Σε αυτούς τους κόμβους η ενέργεια και οι υπολογιστικοί πόροι δεν είναι περιορισμένοι, διότι οι μπαταρίες που διαθέτουν είναι επαναφορτιζόμενες, οι υπολογιστές έχουν μεγάλη διαθέσιμη μνήμη, και ο επεξεργαστής τους εκτελεί ίδιο λογισμικό με αυτό που εκτελούν οι μεγάλοι στατικοί υπολογιστές. Αντίθετα, οι κόμβοι του ασύρματου δικτύου αισθητήρων WSN είναι περιορισμένοι

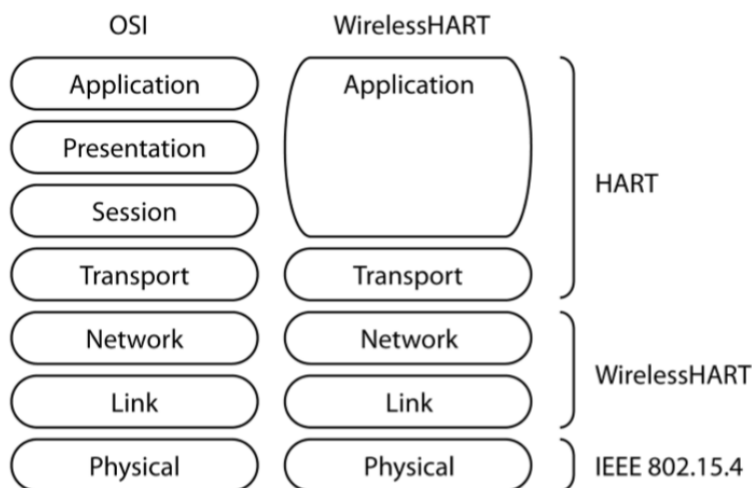
και ως προς την ενέργεια τροφοδοσίας και ως προς τους υπολογιστικούς πόρους. Οι κόμβοι αισθητήρες συνήθως δεν αντικαθίστανται στις θέσεις που βρίσκονται και γίνονται άχρηστοι αν χαλάσουν ή αν τελειώσει η ενέργεια τους. Η διαθέσιμη μνήμη ενός κόμβου αισθητήρα είναι πολύ μικρή δηλαδή είναι της τάξης των KBs, και οι υπολογιστικές δυνατότητες του είναι περιορισμένες. Για αυτό τον λόγο χρησιμοποιούνται προσαρμοσμένα λειτουργικά συστήματα, και πρωτόκολλα με μειωμένη πολυπλοκότητα. Επίσης χρησιμοποιείται εξειδικευμένο λογισμικό.

δ) Επικοινωνίες δεδομένων. Στα δίκτυα υπολογιστών (Ad hoc) οι επικοινωνίες δεδομένων γίνονται μεταξύ ισότιμων κόμβων (peer-to-peer) και υπάρχουν πολλά διαθέσιμα πρωτόκολλα. Ένας κόμβος υπολογιστής που επιθυμεί να επικοινωνήσει με έναν ή περισσότερους άλλους κόμβους υπολογιστές θα επιλέξει ένα διαθέσιμο πρωτόκολλο. Όμως οι υπολογιστές δεν θέτουν ως προτεραιότητα την διατήρηση της μπαταρίας, αλλά θέτουν ως προτεραιότητα την καλή ποιότητα υπηρεσιών QoS και το αποτελεσματικό εύρος ζώνης.

Στα ασύρματα δίκτυα αισθητήρων WSNs οι κόμβοι δεν είναι όλοι ισότιμοι αλλά υπάρχουν οι κόμβοι αισθητήρες (sensor nodes) και οι κεντρικοί κόμβοι συλλογής δεδομένων που ονομάζονται sinks. Από τους αισθητήρες μεταφέρονται τα δεδομένα στους κεντρικούς κόμβους sinks. Μόλις ο κόμβος αισθητήρας ανιχνεύσει ένα συμβάν (event) δημιουργεί ένα αντίστοιχο πακέτο δεδομένων (data packet) και το στέλνει στους κόμβους sinks συνήθως μέσω μίας διαδρομής δρομολόγησης πολλαπλών αλμάτων (multihop route).

Σύγκριση στρωμάτων του OSI7 με το μοντέλο στρωμάτων του WirelessHART

Το πρότυπο WirelessHART σε σύγκριση με το μοντέλο OSI έχει τα παρακάτω στρώματα:



Εικόνα 9 Σύγκριση του μοντέλου Στρωμάτων OSI 7 και του μοντέλου στρωμάτων για το WirelessHART.
Πηγή: [7, p. 31]

Περισσότερες λεπτομέρειες για τα στρώματα στο WirelessHART θα αναφέρουμε στο κεφάλαιο 3.

2.3 Το πρότυπο IEEE 802.15.4

Σε αυτή την ενότητα, παρουσιάζεται το πρότυπο IEEE 802.15.4, που αφορά τα ασύρματα δίκτυα αισθητήρων. Μία έκδοση του προτύπου, δημιουργήθηκε το 2006, από το IEEE (Institute of Electrical and Electronics Engineers). Το πρότυπο IEEE 802.15.4 συνδυάζει την επικοινωνία με χρονοπρογραμματισμό (schedule-based) και την επικοινωνία με συγκρούσεις (contention-based).

Αρχικά παρουσιάζονται κάποια χαρακτηριστικά του προτύπου, δηλαδή οι συσκευές, η τοπολογία, οι διευθύνσεις και οι συχνότητες λειτουργίας. Στις παραγράφους που ακολουθούν παρουσιάζεται το Φυσικό επίπεδο (PHY Layer) [10] και το επίπεδο MAC. [10] [11]

Το πρότυπο IEEE, 802.15.4, ορίζει το φυσικό στρώμα physical layer (PHY) και το υπό-επίπεδο MAC medium access control sublayer για ασύρματη σύνδεση χαμηλού ρυθμού δεδομένων (low data rate), ανάμεσα σε κόμβους αισθητήρες δηλαδή συσκευές που είναι σχετικά απλές και καταναλώνουν ελάχιστη ενέργεια και συνήθως η απόσταση μεταξύ δύο συσκευών είναι 10 m ή μικρότερη. Αυτή η απόσταση ονομάζεται Personal Operating Space (POS).

Επίσης το IEEE, 802.15.4, αφορά τα ασύρματα δίκτυα προσωπικής περιοχής (wireless personal area network) χαμηλού ρυθμού δεδομένων (low rate) LR-WPAN. Ο κύκλος λειτουργίας (duty cycle) των δικτύων αυτών, περιλαμβάνει ένα ενεργό μέρος και ένα ανενεργό μέρος, τα οποία μπορούν να αυξομειώνονται, κατά τη διάρκεια της δημιουργίας και διαμόρφωσης ενός δικτύου προσωπικής περιοχής PAN.

Επιπλέον, υπάρχουν και άλλες εκδόσεις ή παραλλαγές αυτού του προτύπου, η IEEE 802.15.4a και η IEEE 802.15.4b που έγιναν για βελτιώσεις και διορθώσεις στο αρχικό πρότυπο.

Η έκδοση IEEE 802.15.4a ορίζει ένα εναλλακτικό φυσικό στρώμα, έχει μεγαλύτερη εμβέλεια και βελτιωμένη ανθεκτικότητα στις ασύρματες επικοινωνίες και υποστηρίζει την κινητικότητα.

Η έκδοση IEEE 802.15.4.b υποστηρίζει νέες κατανομές συχνοτήτων για την Ευρώπη την Κίνα και την Ιαπωνία, έχει μία επέκταση που επιτρέπει υψηλότερους ρυθμούς δεδομένων για τις χαμηλότερες ζώνες συχνοτήτων. Παρακάτω δίνεται η περιγραφή για τα χαρακτηριστικά που αφορούν το γενικό πρότυπο IEEE 802.15.4 αλλά δεν περιγράφονται τα χαρακτηριστικά διάφορων παραλλαγών του προτύπου.

2.3.1 Τύποι συσκευών στο πρότυπο IEEE 802.15.4

Στο πρότυπο IEEE 802.15.4 καθορίζονται τρεις τύποι συσκευών. Αυτοί, περιγράφονται στη συνέχεια.

2.3.1.1 Συντονιστής Δικτύου Προσωπικής Περιοχής PAN (PAN coordinator)

Το πρότυπο 802.15.4 στα δίκτυα αισθητήρων χρησιμοποιεί έναν κεντρικό κόμβο ελεγκτή (central controller) που ονομάζεται PAN coordinator. Αυτός, δημιουργεί ένα δίκτυο στην εμβέλεια δικτύου προσωπικής περιοχής PAN (Personal Area Network). [12]

Πρέπει να υπάρχει μόνο ένας PAN coordinator. Τα καθήκοντα του είναι:

- α) Αναθέτει στο δίκτυο ένα αναγνωριστικό PAN
- β) Βρίσκει ένα κατάλληλο κανάλι ραδιοσυχνότητας για τη λειτουργία του δικτύου
- γ) Αναθέτει στον εαυτό του μία διεύθυνση short address
- δ) Χειρίζεται αιτήσεις (requests) από άλλες συσκευές (devices) που θέλουν να συνδεθούν (join) στο δίκτυο.
- ε) Αναμεταδίδει (relays) μηνύματα (messages) από έναν κόμβο σε άλλο, κυρίως στην τοπολογία αστέρα ή δέντρου, αλλά όχι σε όλα τα είδη τοπολογιών.

2.3.1.2 Τοπικός Συντονιστής

Ο τοπικός συντονιστής λέγεται local coordinator

Στις τοπολογίες δέντρου, υπάρχουν ένας ή περισσότεροι τοπικοί συντονιστές (local coordinator). Κάθε τοπικός συντονιστής λειτουργεί ως κεντρικός κόμβος τοπικά και παρέχει υπηρεσίες στους κόμβους-παιδιά του.

Οι εργασίες που κάνει τοπικός συντονιστής είναι:

- α) Χειρίζεται αιτήσεις (requests) από κόμβους που θέλουν να συνδεθούν (join) στο δίκτυο.
- β) Αναμεταδίδει (relays) μηνύματα από έναν κόμβο σε άλλο.

2.3.1.3 Τελική Συσκευή

Η τελική συσκευή λέγεται end-device.

Είναι ένας κόμβος (node) αισθητήρας που λέγεται και τελικός κόμβος. Μπορεί να έχει λειτουργίες εισόδου/εξόδου (input/output) δεδομένων αλλά δεν έχει λειτουργίες συντονιστή. Στο IEEE 802.15.4 δεν λέγεται "End Device" αλλά συσκευή. Οι συσκευές στο δίκτυο χωρίζονται σε 2 κατηγορίες

α) FFD Συσκευή πλήρων λειτουργιών (full function device). Είναι μία συσκευή που εκτελεί όλες τις υπηρεσίες (services) του στρώματος MAC του IEEE 802.15.4 και έτσι αν χρειαστεί μπορεί να γίνει και συντονιστής (coordinator). Η συσκευή FFD μπορεί να λειτουργεί σε 3 διαφορετικές λειτουργίες (modes) που είναι είτε ο συντονιστής του δικτύου προσωπικής περιοχής (PAN coordinator), είτε ο συντονιστής (coordinator) είτε μια τελική συσκευή device.

β) RFD Συσκευή μειωμένων λειτουργιών (reduced function device). Είναι μία συσκευή που παρέχει μειωμένο σύνολο υπηρεσιών του στρώματος MAC του IEEE 802.15.4 και δεν μπορεί να λειτουργήσει ως συντονιστής διότι οι πόροι σε μνήμη και σε υπολογιστική ισχύ είναι περιορισμένοι στις συσκευές RFD. Επομένως, οι συντονιστές είναι μόνο συσκευές FFD, ενώ οι απλοί κόμβοι μπορούν να είναι είτε FFD είτε RFD.

Μία συσκευή FFD μπορεί να μιλήσει και σε συσκευές RFDs και σε άλλες FFDs.

Μία συσκευή RFD μπορεί να μιλήσει μόνο σε συσκευή FFD και προορίζεται για πολύ απλές εφαρμογές. Η RFD μπορεί να λειτουργήσει μόνο ως τελική συσκευή (device).

Όλες οι τελικές συσκευές (devices) πρέπει πάντα να σχετίζονται με έναν συντονιστή (coordinator) σε όλες τις συνθήκες του δικτύου. Αν υπάρχουν πολλαπλοί συντονιστές (coordinators) μπορούν να λειτουργήσουν όλοι μαζί σε μία τοπολογία δικτύου και ένας από αυτούς γίνεται ο συντονιστής PAN (PAN coordinator).

2.3.1.4 Οι Τρεις Κατηγορίες Λογικών Συσκευών σε δίκτυο PAN

Ένα δίκτυο προσωπικής περιοχής (Personal Area Network) (PAN) μπορεί να βασίζεται στο πρωτόκολλο Zigbee που έχει το ίδιο υποεπίπεδο MAC με το IEEE 802.15.4. Σε δίκτυα PAN καθορίζονται οι τρεις κατηγορίες λογικών συσκευών [1] που είναι όμοιες με αυτές που αναφέρθηκαν:

α) Συντονιστής δικτύου (Network coordinator): μία συσκευή FFD που είναι υπεύθυνη για τη λειτουργία και για τον έλεγχο του δικτύου. Επιλέγει βασικές παραμέτρους για τη ρύθμιση και για την εκκίνηση λειτουργίας του δικτύου. Επιπλέον αποθηκεύει πληροφορίες για το δίκτυο και δρα ως αποθετήριο (repository) για κλειδιά ασφαλείας.

β) Δρομολογητής (Router): Μία συσκευή FFD που υποστηρίζει τη λειτουργία δρομολόγησης δεδομένων (data routing). Μπορεί να λειτουργεί ως ενδιάμεση συσκευή για να συνδέει διαφορετικά συστατικά στοιχεία του δικτύου (components) και για να προωθεί τα μηνύματα από τις απομακρυσμένες συσκευές σε διάφορες διαδρομές πολλαπλών αλμάτων (multihop paths). Ένας δρομολογητής (router) μπορεί να επικοινωνεί με άλλους δρομολογητές και άλλες τελικές συσκευές.

γ) Τελικές συσκευές (end devices). Είναι συσκευές RFD που περιέχουν μόνο τις απαραίτητες λειτουργίες για να επικοινωνούν με τον κόμβο γονέα τους. Ο κόμβος γονέας μπορεί να είναι ο συντονιστής δικτύου (network coordinator) ή ένας δρομολογητής (router). Μία τελική συσκευή δεν μπορεί να αναμεταδίδει μηνύματα δεδομένων σε άλλες τελικές συσκευές.

Ουσιαστικά, οι τύποι συσκευών στο πρωτόκολλο Zigbee είναι οι ίδιοι που αναφέρθηκαν για το IEEE 802.15.4.

2.3.2 Τοπολογία

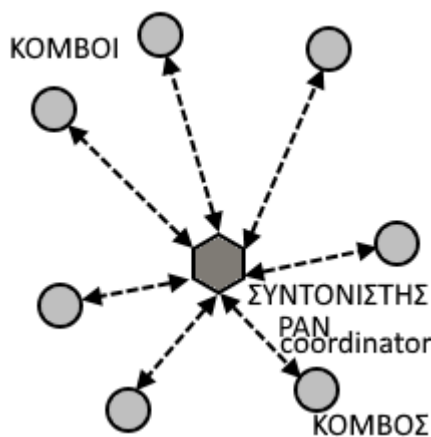
Η σύνδεση μεταξύ δύο συσκευών ονομάζεται άλμα (hop), ενώ αν στο δίκτυο συνδέονται περισσότερες από δύο συσκευές τότε έχουμε περισσότερα άλματα μεταξύ των συσκευών. Η τοπολογία σε ένα δίκτυο IEEE 802.15.4 μπορεί να είναι τοπολογία αστέρα ενός άλματος (one-hop star), ή αν η απόσταση επικοινωνιών ξεπεράσει τα 10 μέτρα μπορεί το δίκτυο να είναι αυτορρυθμιζόμενο δίκτυο πολλαπλών αλμάτων (multi-hop network).

Το πρότυπο IEEE 802.15.4 χρησιμοποιεί 3 τοπολογίες [12] για τα δίκτυα αισθητήρων, αυτές περιγράφονται παρακάτω:

2.3.2.1 Ο αστέρας (Star)

Ο κεντρικός κόμβος βρίσκεται σε ένα κεντρικό σημείο και οι υπόλοιποι κόμβοι έχουν απόσταση 1 hop από τον κεντρικό κόμβο.

Ο κεντρικός κόμβος είναι ο συντονιστής που λέγεται PAN Co-ordinator για το δίκτυο προσωπικής περιοχής PAN. Οι υπόλοιποι κόμβοι που περιβάλλουν τον συντονιστή λέγονται τελικές συσκευές (End Devices). Κάθε τελικός κόμβος (node) επικοινωνεί μόνο με τον κεντρικό κόμβο PAN Co-ordinator. Για αυτό για να στείλει μήνυμα ο τελικός κόμβος σε άλλο τελικό κόμβο, θα πρέπει πρώτα το μήνυμα να φτάσει στον κεντρικό κόμβο Co-ordinator, και αυτός να αναμεταδώσει το μήνυμα στον κόμβο προορισμού. Το πρόγραμμα εφαρμογών που υπάρχει στον κόμβο Co-ordinator έχει την εργασία να αναμεταδίδει τα μηνύματα (relaying messages). Όταν ένας τελικός κόμβος χάσει τη σύνδεση του με τον κεντρικό κόμβο, τότε δεν υπάρχει εναλλακτική διαδρομή. Αυτό είναι το βασικό μειονέκτημα της τοπολογίας αστέρα και ένα ακόμη μειονέκτημα είναι στον κεντρικό κόμβο PAN Coordinator συγκεντρώνονται όλα τα σήματα και πρέπει να διαχειρίζεται τις συμφορήσεις του δικτύου. Στην παρακάτω εικόνα φαίνεται η τοπολογία αστέρα (star)

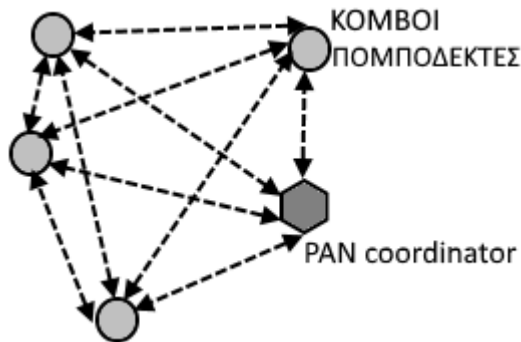


Εικόνα 10 Τοπολογία Αστέρα.

Η τοπολογία αστέρα (star) είναι κατάλληλη περισσότερο για τις εφαρμογές που είναι κρίσιμες ως προς την καθυστέρηση (delay). Επίσης είναι κατάλληλη όταν η περιοχή δικτύου κάλυψης είναι σχετικά μικρή.

2.3.2.2 Ομότιμοι Κόμβοι (peer-to-peer)

Ο κεντρικός κόμβος βρίσκεται σε ένα σημείο και συνδέεται με όλους τους κόμβους με ένα άλμα (hop), όπως ο αστέρας, αλλά υπάρχουν επιπλέον εναλλακτικές διαδρομές πολλαπλών αλμάτων (multi-hop), που συνδέουν τους κόμβους μεταξύ τους.

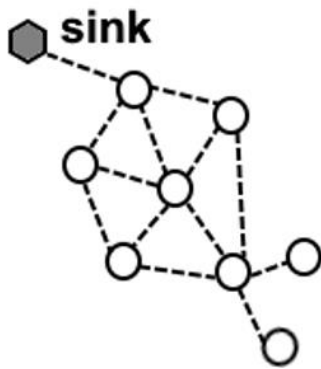


Εικόνα 11 Τοπολογία peer to peer.

Η τοπολογία peer-to-peer μπορεί να εφαρμοστεί σε δίκτυα που καλύπτουν σχετικά μεγάλες περιοχές, με διαδρομές πολλαπλών αλμάτων (multi-hop). Όμως, παρουσιάζει μεγαλύτερη καθυστέρηση δικτύου (network latency).

2.3.2.3 Τοπολογία δικτύου πλέγματος (mesh)

Η τοπολογία δικτύου πλέγματος (Mesh network) είναι το ίδιο με την τοπολογία peer-to-peer. Οι συσκευές είναι όλες ισότιμες και υπάρχει μόνο ένας κεντρικός κόμβος, ο PAN Co-ordinator και τοποθετούνται όλες σε μία μορφή δικτύου ad hoc δηλαδή χωρίς να υπάρχει δομή συγκεκριμένη στο δίκτυο. Ορισμένοι κόμβοι επικοινωνούν άμεσα μεταξύ τους ενώ άλλοι όχι. Υπάρχουν κόμβοι που δεν βρίσκονται στην εμβέλεια κάποιων άλλων κόμβων. Τα μηνύματα όμως μπορούν να περνούν από τον έναν κόμβο στον άλλο και με πολλαπλά άλματα να φτάνουν στον τελικό προορισμό τους. Για κάποιους προορισμούς υπάρχουν πολλαπλές εναλλακτικές διαδρομές και έτσι τα μηνύματα μπορούν να φτάσουν στον προορισμό αν γίνει αποσύνδεση κάποιου κόμβου και διακοπεί μία διαδρομή.

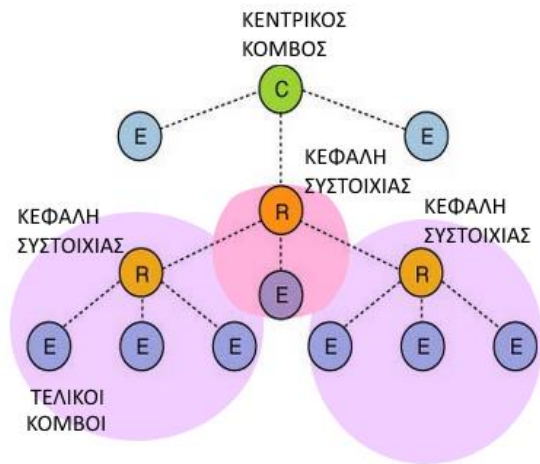


Εικόνα 12 Τοπολογία Δικτύου Πλέγματος.

2.3.2.4 Cluster Tree (Δέντρο Συστοιχιών)

Είναι μία τοπολογία δέντρου (Tree network topology), που έχει μία δομή βασισμένη στις σχέσεις κόμβων γονέα-παιδιού (parent-child relationships). Ο κεντρικός κόμβος PAN Co-ordinator είναι η αρχή του δέντρου. Κάθε άλλος κόμβος έχει έναν κόμβο γονέα. Ο κάθε κόμβος μπορεί επίσης να έχει ένα ή περισσότερα παιδιά αλλά μπορεί και κανένα παιδί. Κάθε κόμβος μπορεί να επικοινωνήσει μόνο με τον γονέα του ή το παιδί, του αν έχει. Κάθε κόμβος γονέας, αν έχει παιδιά, δρα ως τοπικός συντονιστής (local Co-ordinator) για τα παιδιά του. Τότε η μορφή του δικτύου είναι ένα δέντρο όπου ο συντονιστής PAN Co-ordinator είναι στην ρίζα (root) δηλαδή στην κορυφή. Μπορεί να θεωρηθεί και ως μία τοπολογία αστέρα με πολλούς κλάδους. Οι κλάδοι μπορούν να ομαδοποιηθούν σε συστοιχίες που περιέχουν ομάδες γονέων-παιδιών. Κάθε συστοιχία έχει έναν τοπικό κεντρικό κόμβο συστοιχίας που είναι η κεφαλή συστοιχίας. Για αυτό λέγεται δέντρο συστοιχιών (cluster tree). Σε κάθε συστοιχία δίνεται ένα μοναδικό αναγνωριστικό Cluster ID ώστε να ξεχωρίζει από τις άλλες συστοιχίες. Το δέντρο συστοιχιών είναι ειδική περίπτωση της τοπολογίας δέντρου.

Σε άλλα πρότυπα ασύρματων δικτύων αισθητήρων, όπως είναι το Zigbee ή το JenNet, τα οποία για μεταφορά δεδομένων χρησιμοποιούν το 802.15.4, οι τοπικοί συντονιστές (local Coordinators) ή κεφαλές συστοιχίας λέγονται δρομολογητές (routers) [13].



Εικόνα 13. Τοπολογία δέντρου συστοιχιών (cluster tree)

2.3.3 Διευθύνσεις

Μια συσκευή σε ένα δίκτυο IEEE 802.15.4 μπορεί να χρησιμοποιήσει μία διεύθυνση από τους δύο παρακάτω 2 τύπους διευθύνσεων.

2.3.3.1 Διεύθυνση IEEE (MAC)

Η διεύθυνση τύπου IEEE(MAC) λέγεται και Extended address (Εκτεταμένη διεύθυνση). Είναι μία διεύθυνση 64-bit IEEE address (8 byte). Αυτός ο τύπος διεύθυνσης προσδιορίζει τη συσκευή με μοναδικό τρόπο ώστε δεν μπορεί κάποια άλλη συσκευή να πάρει την ίδια διεύθυνση σε κανένα διαφορετικό δίκτυο.

2.3.3.2 Σύντομη διεύθυνση (Short address)

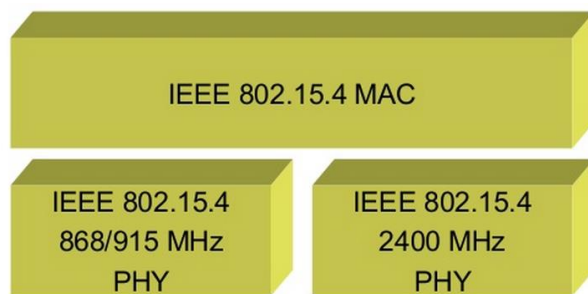
Η διεύθυνση τύπου Short address είναι μία διεύθυνση 16-bit (2 byte) που προσδιορίζει τον κόμβο σε ένα τοπικό δίκτυο και ανατίθεται στον κόμβο με τη διαδικασία συσχέτισης (association procedure). Η διεύθυνση ανατίθεται στον κόμβο από τον συντονιστή (coordinator), όταν ο νέος

κόμβος εισέρχεται στο δίκτυο. Όμως σε διαφορετικά τοπικά δίκτυα δύο κόμβοι μπορούν να έχουν την ίδια διεύθυνση τύπου Short.

Το πλεονέκτημα των διευθύνσεων short είναι ότι έχουν πιο μικρό μέγεθος πακέτου από τις διευθύνσεις extended. Το μικρό μέγεθος πακέτου βελτιστοποιεί τη χρήση του εύρους ζώνης (bandwidth) του δικτύου.

Ένα δίκτυο IEEE 802.15.4 network μπορεί να στεγάσει μέχρι 64k (2^{16}) συσκευές (devices).

2.3.4 Συχνότητες λειτουργίας



Εικόνα 14 Το στρώμα MAC και το φυσικό στρώμα PHY στο πρότυπο IEEE 802.15.4. Το Φυσικό επίπεδο χωρίζεται σε 2 τμήματα.

Οι ασύρματες ζεύξεις στο IEEE 802.15.4 μπορούν να λειτουργούν σε 3 συχνότητες της ζώνης συχνοτήτων ISM industrial scientific medical, που η χρήση της είναι δωρεάν, χωρίς να απαιτείται ειδική άδεια.

Αυτές οι 3 συχνότητες είναι: 2.4 GHz, 915 MHz, 868 MHz. Συμβολίζονται και ως εξής: 868/915/2450 MHz ISM bands.

Χρησιμοποιείται περισσότερο η ζώνη συχνοτήτων 2.4 GHz που εκτείνεται από 2.4 ως 2.483 GHz. και ονομάζεται high-band.

Οι συχνότητες 868/915 MHz ονομάζονται low-band.

Κάθε συχνότητα στεγάζει σε ασύρματες συνδέσεις διαφορετικούς ρυθμούς δεδομένων (data rates).

α) Στη συχνότητα 2.4 GHz ο ρυθμός δεδομένων είναι 250 kb/sec (αν εκφραστεί σε ρυθμό συμβόλων symbols, 62.5 ksym/sec)

β) Στη συχνότητα 915 MHz, ο ρυθμός δεδομένων είναι 40 kb/sec (40 ksym/sec)

γ) Στη συχνότητα 868 MHz ο ρυθμός δεδομένων είναι 20 kb/sec (20 ksym/sec)

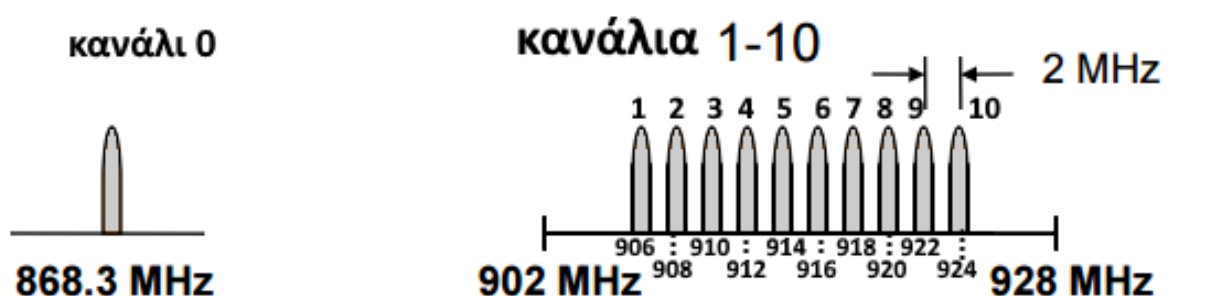
Υπάρχουν 27 κανάλια συνολικά που κατανέμονται στο πρότυπο IEEE 802.15.4. στις 3 ζώνες συχνοτήτων:

α) Το 1 κανάλι στη ζώνη 868 MHz band (Κανάλι 0)

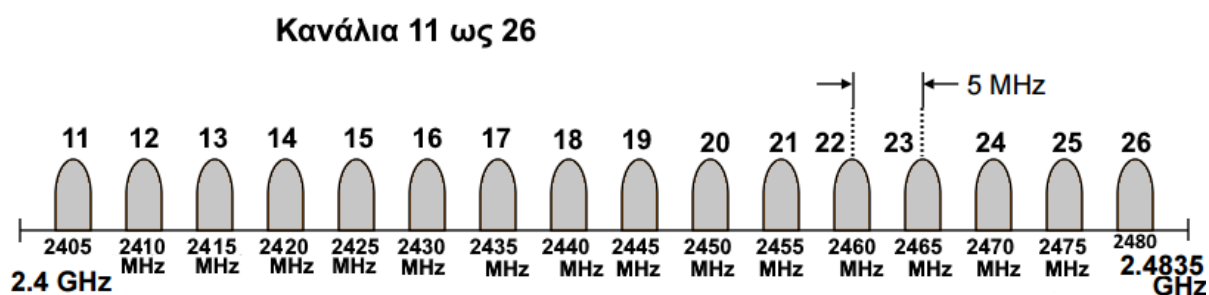
β) Τα 10 κανάλια στη ζώνη συχνοτήτων 915 MHz band (Κανάλια 1 ως 10),

γ) Τα 16 κανάλια στη ζώνη συχνοτήτων 2.4 GHz band (Κανάλια 11 ως 26),

Αυτές οι συχνότητες λειτουργίας φαίνονται στις παρακάτω εικόνες:



Εικόνα 15. Τα κανάλια από 0 ως 10 στις συχνότητες του IEEE 802.15.4



Εικόνα 16. Τα κανάλια από 11 ως 26 στις συχνότητες του IEEE 802.15.4

Η αρίθμηση των καναλιών φαίνεται στον παρακάτω πίνακα.

Ζώνη Συχνοτήτων	Αριθμός Καναλιού	Κεντρική συχνότητα MHz	Γεωγραφική περιοχή
868 MHz	0	868.3	Ευρώπη

915 MHz	1	906	Αμερική, Αυστραλία
-	2	908	-
-	3	910	-
-	4	912	-
-	5	914	-
-	6	916	-
-	7	918	-
-	8	920	-
-	9	922	-
-	10	924	-
2400 MHz	11	2405	Παγκοσμίως
-	12	2410	-
-	13	2415	-
-	14	2420	-
-	15	2425	-
-	16	2430	-
-	17	2435	-
-	18	2440	-
-	19	2445	-
-	20	2450	-
-	21	2455	-
-	22	2460	-
-	23	2465	-
-	24	2470	-
-	25	2475	-
	26	2480	

Πίνακας 2.3 Αρίθμηση των καναλιών στις συχνότητες του IEEE 802.15.4

2.3.5 Το φυσικό επίπεδο (PHY Layer) για το IEEE 802.15.4

Το φυσικό επίπεδο (PHY layer).

Το φυσικό επίπεδο (PHY layer) παρέχει μία διεπαφή (interface) ανάμεσα στο υπό-επίπεδο MAC και το φυσικό κανάλι ασύρματης επικοινωνίας (physical radio channel). Παρέχει δύο υπηρεσίες, οι οποίες είναι προσβάσιμες από δύο σημεία πρόσβασης υπηρεσιών (service access points) (SAPs). Αυτές είναι:

- α) η υπηρεσία δεδομένων (PHY data service)
- β) η υπηρεσία διαχείρισης (PHY management service).

Το φυσικό επίπεδο (PHY layer) είναι υπεύθυνο για τις παρακάτω διεργασίες (tasks):

- 1) Ενεργοποίηση / Απενεργοποίηση του ασύρματου πομποδέκτη
- 2) ED Ανίχνευση ενέργειας (Energy detection) μέσα στο τρέχον κανάλι
- 3) LQI Ένδειξη ποιότητας ζεύξης (Link Quality indication) για λαμβανόμενα πακέτα
- 3) CCA έλεγχος καθαρού καναλιού για CSMA-CA
- 4) Επιλογή συχνότητας καναλιού (Channel frequency selection)
- 5) Μετάδοση δεδομένων (Data transmission) και λήψη (reception).

Παρακάτω αναλύονται αυτές οι εργασίες:

- Ενεργοποίηση (activation) και απενεργοποίηση (deactivation) του ασύρματου πομποδέκτη (radio transceiver): Θέτει τον ράδιο πομποδέκτη (radio transceiver) σε μία από τις 3 καταστάσεις λειτουργίας του, δηλαδή:

- α) εκπομπή,
- β) λήψη,
- γ) κατάσταση «ύπνου» (sleeping),

σύμφωνα με την ανάλογη αίτηση (request) που δέχεται από το υπό-επίπεδο MAC sublayer.

Ο χρόνος αλλαγής (turnaround time) από την εκπομπή (transmitting) στη λήψη (receiving), ή το αντίστροφο, δεν θα πρέπει να είναι περισσότερος από 12 symbol periods.

- Ανίχνευση ενέργειας (Energy detection) (ED) μέσα στο τρέχον κανάλι:

Είναι μία εκτίμηση της λαμβανόμενης ισχύος σήματος (signal power) μέσα στο εύρος ζώνης (bandwidth) ενός καναλιού IEEE 802.15.4. Δεν γίνεται καμία προσπάθεια να προσδιοριστούν (identify) ή να αποκωδικοποιηθούν (decode) τα σήματα στο κανάλι σε αυτή τη διαδικασία. Ο χρόνος για την ανίχνευση ενέργειας (energy detection time) θα ισούται με 8 symbol periods. Το αποτέλεσμα από την ανίχνευση ενέργειας (energy detection) μπορεί να χρησιμοποιηθεί από το επίπεδο δικτύου (network layer) ως μέρος του αλγορίθμου επιλογής καναλιών ή για το σκοπό του ελέγχου καναλιών (έλεγχος καθαρού καναλιού) (CCA) (μόνο του ή συνδυασμένο με ανίχνευση φέροντος carrier sense).

- Η ένδειξη ποιότητας ζεύξης Link quality indication (LQI) για τα ληφθέντα πακέτα: Η μέτρηση για την ένδειξη ποιότητας ζεύξης (Link quality indication) εκτελείται για κάθε πακέτο που λαμβάνεται. Το φυσικό επίπεδο (PHY layer) χρησιμοποιεί την ανίχνευση ενέργειας του δέκτη (energy detection) (ED), ένα λόγο σήματος προς θόρυβο (signal-to-noise ratio), ή ένα συνδυασμό αυτών των δύο, για να μετρήσει την ισχύ και/ή την ποιότητα της ζεύξης (link) από την οποία έχει ληφθεί ένα πακέτο. Όμως η χρήση του αποτελέσματος LQI από το επίπεδο δικτύου (network layer) ή από το επίπεδο εφαρμογών (application layer) δεν καθορίζεται στο πρότυπο.

- Έλεγχος καθαρού καναλιού (Clear channel assessment) (CCA) για (CSMA-CA), πολλαπλή πρόσβαση με ανίχνευση φέροντος (carrier sense multiple access) με αποφυγή συγκρούσεων (collision avoidance) :

Τον έλεγχο του καθαρού καναλιού CCA τον ζητά με αίτηση (request) το στρώμα MAC και υλοποιείται από το φυσικό στρώμα (PHY layer).

Το φυσικό επίπεδο (PHY layer) απαιτείται να εκτελέσει έλεγχο καθαρού καναλιού CCA χρησιμοποιώντας την ανίχνευση ενέργειας (energy detection), την ανίχνευση φέροντος (carrier sense), ή ένα συνδυασμό αυτών των δύο.

Όταν ένας κόμβος εκπέμπει δεδομένα στο κανάλι πρέπει να μην γίνει σύγκρουση με δεδομένα που εκπέμπει ένας άλλος κόμβος την ίδια χρονική στιγμή, για αυτό ο κόμβος πριν εκπέμψει ελέγχει αν είναι άδειο (Clear) ή απασχολημένο (busy) το κανάλι. Υπάρχουν 3 λειτουργίες:

α) Στην λειτουργία ανίχνευσης ενέργειας (energy detection mode), το μέσο (δηλ. το ασύρματο κανάλι) θεωρείται απασχολημένο (busy) αν ανιχνευθεί μια οποιαδήποτε τιμή ενέργειας που είναι μεγαλύτερη από μια προκαθορισμένη τιμή ενέργειας κατώτατου ορίου (energy threshold).

β) Στην λειτουργία ανίχνευσης φέροντος (carrier sense mode), το μέσο θεωρείται απασχολημένο (busy) αν ανιχνευθεί ένα σήμα με τη διαμόρφωση και τα χαρακτηριστικά του IEEE 802.15.4.

γ) Στη συνδυασμένη λειτουργία (combined mode), και οι δύο συνθήκες που αναφέρονται παραπάνω πρέπει να ισχύουν ώστε να βγει το συμπέρασμα ότι το μέσο είναι απασχολημένο (busy).

Αν το κανάλι είναι απασχολημένο (busy), τότε ο κόμβος δεν εκπέμπει το πακέτο, αλλά περιμένει για μία τυχαία χρονική περίοδο που ονομάζεται back-off period. Μετά προσπαθεί ξανά να μεταδώσει το πακέτο.

- Επιλογή συχνότητας καναλιού: Οι ασύρματες ζεύξεις στο 802.15.4 μπορούν να λειτουργήσουν σε 27 διαφορετικά κανάλια, αλλά κάθε ένα συγκεκριμένο δίκτυο επιλέγει να υποστηρίξει μόνο ορισμένα από αυτά τα κανάλια. Έτσι το φυσικό επίπεδο (PHY layer) πρέπει να είναι ικανό να συντονίζει τον πομποδέκτη του (transceiver) σε ένα συγκεκριμένο κανάλι κατά τη λήψη μιας αίτησης (request) από το υπό-επίπεδο MAC sublayer.

- Μετάδοση δεδομένων (Data transmission) και λήψη: Αυτό είναι μία σημαντική εργασία (task) για το φυσικό επίπεδο (PHY layer). Σε αυτό το κομμάτι χρησιμοποιούνται τεχνικές διαμόρφωσης και εξάπλωσης (Modulation and spreading).

Στων παρακάτω πίνακα παρουσιάζονται κάποια χαρακτηριστικά για τις 3 ζώνες συχνοτήτων του IEEE 802.15.4.

Ζώνη συχνοτήτων	Δύο	Low-Band	868 MHz	1 κανάλι	20 kb/s
Frequency	PHYs	BPSK	915 MHz	10 κανάλια	40 kb/s
Band		High-Band	2.4 GHz	16 κανάλια	250 kb/s
		O-QPSK			
Πρόσβαση στο κανάλι (Channel Access)	CSMA-CA και slotted CSMA-CA				
Εμβέλεια	10 ως 20 m				

(Range)	
Διευθύνσεις Addressing	διευθύνσεις IEEE είτε short (δηλ. μεγέθους 8 bit), είτε μεγέθους 64 bit

Πίνακας 2.4 οι 3 ζώνες συχνοτήτων του IEEE 802.15.4 και διάφορα χαρακτηριστικά τους. Πηγή: [10]

Ζώνη Συχνοτήτων 2.4 GHz

Όπως φαίνεται και από τον παραπάνω πίνακα, Η ζώνη συχνοτήτων 2.4 GHz λέγεται High-Band. [12]. Στα 2.4 GHz, το φυσικό επίπεδο PHY, χρησιμοποιεί μια τεχνική διαμόρφωσης 16-ary quasi-orthogonal, στην οποία κάθε 4 bits πληροφορίας, αντιστοιχίζονται (mapped) σε μία ακολουθία ψευδό-τυχαίου θορύβου 32-chip pseudo-random noise (PN) sequence. Μετά, οι ακολουθίες ψευδό-τυχαίου θορύβου (PN sequences) για διαδοχικά σύμβολα δεδομένων (data symbols) συνενώνονται (concatenated) και διαμορφώνονται (modulated) πάνω στο φέρον (carrier) με χρήση offset quadrature phase shift keying (O-QPSK).

Ο Ρυθμός συμβόλων (Symbol rate) είναι 250 kb/s (4 bits/symbol, 62.5 kBaud).

Διαμόρφωση δεδομένων: 16-ary quasi orthogonal modulation.

16 σύμβολα ρυθμίζονται ορθογωνικά με 32-chip κώδικες ψευδοτυχαίου θορύβου PN codes.

Διαμόρφωση Chip : MSK στα 2.0 Mchips/s

Ζώνες Συχνοτήτων 869/915 MHz

Όπως φαίνεται και στον παραπάνω πίνακα, οι ζώνες συχνοτήτων 868/915 MHz λέγονται low-band. Στα 868/915 MHz το φυσικό επίπεδο PHY χρησιμοποιεί ευθείας ακολουθίας εξάπλωση φάσματος direct sequence spread spectrum (DSSS) με binary phase shift keying (BPSK) που χρησιμοποιείται για τη διαμόρφωση chip modulation και διαφορική κωδικοποίηση (differential encoding) που χρησιμοποιείται για την κωδικοποίηση συμβόλων (data symbol encoding). Κάθε σύμβολο (data symbol) αντιστοιχίζεται (mapped) σε μία ακολουθία ψευδό-τυχαίου θορύβου (PN sequence) 15-chip και μετά οι συνενωμένες (concatenated) ακολουθίες ψευδό-θορύβου (PN sequences) διαμορφώνονται (modulated) πάνω στο φέρον (carrier) με χρήση BPSK με raised cosine pulse shaping.

Ρυθμός συμβόλων (Symbol rate):

20 kb/s (1 bit/symbol, 20 kBaud) στη ζώνη συχνοτήτων 868 MHz.

40 kb/s (1 bit/symbol, 40 kBaud) στη ζώνη συχνοτήτων 915 MHz.

Διαμόρφωση δεδομένων: BPSK με διαφορική κωδικοποίηση (differential encoding)

Κώδικας εξάπλωσης (spreading code) : ακολουθία 15 chip m-sequence.

Διαμόρφωση του chip: BPSK

300 kchips/s στη ζώνη συχνοτήτων 868 MHz

600 kchips/s στη ζώνη συχνοτήτων 915 MHz.

Κοινές παράμετροι

Μερικές κοινές παράμετροι είναι: Η Ισχύς μετάδοσης (transmit power) του πομπού είναι τουλάχιστον 1mW. Η ανοχή (tolerance) στην κεντρική συχνότητα μετάδοσης (transmit center frequency) είναι ± 40 ppm. Η ευαισθησία του δέκτη είναι -85dBm στη ζώνη συχνοτήτων 2.4 GHz, ενώ είναι -92 dBm στις ζώνες συχνοτήτων 868/915 MHz.

2.3.5.1 Η δομή του πακέτου δεδομένων (packet structure) φυσικού στρώματος

Η δομή του πακέτου δεδομένων για το φυσικό στρώμα, φαίνεται στην παρακάτω εικόνα

Preamble	Start of Packet delimiter	PHY Header	PHY Service Data Unit (PSDU)

Εικόνα 17. Η δομή του πακέτου δεδομένων IEEE 802.15.4 για το φυσικό στρώμα.

Preamble. Αυτό το πεδίο αποτελείται από 4 bytes = 32 bit και περιλαμβάνει δεδομένα συγχρονισμού και χρησιμοποιείται για συγχρονισμό συμβόλων.

Start of Packet Delimiter. Οριοθέτης της αρχής του πακέτου. Αποτελείται από 1 byte = 8 bit και χρησιμοποιείται για το συγχρονισμό πλαισίων (frames).

PHY header. Είναι η επικεφαλίδα του φυσικού επιπέδου. Αποτελείται από 1 byte και προσδιορίζει το μέγεθος (length) του πεδίου δεδομένων PSDU.

PHY Service Data Unit (PSDU) είναι το πεδίο δεδομένων προς μετάδοση που είναι το πακέτο υπηρεσιών του φυσικού στρώματος. Αποτελείται από 0 ως 127 bytes

2.3.6 Το στρώμα MAC (υποεπίπεδο πρόσβασης μέσου) στο IEEE 802.15.4

Το υποεπίπεδο MAC sublayer παρέχει μια διεπαφή (interface) ανάμεσα στο υποεπίπεδο σύγκλισης με συγκεκριμένες υπηρεσίες service specific convergence sublayer (SSCS) και το φυσικό επίπεδο (PHY layer).

Όπως το φυσικό επίπεδο PHY layer, έτσι και το υποεπίπεδο MAC sublayer παρέχει δύο υπηρεσίες:

- α) υπηρεσία δεδομένων MAC data service
- β) υπηρεσία διαχείρισης MAC management service.

Το υποεπίπεδο MAC sublayer έχει τις παρακάτω εργασίες (tasks):

- 1) Δημιουργία των beacons του δικτύου αν η συσκευή είναι συντονιστής (coordinator)
- 2) Συγχρονισμός των beacons
- 3) Υποστηρίζει την συσχέτιση (association) και την από-συσχέτιση (disassociation) στο δίκτυο προσωπικής περιοχής PAN
- 4) Υποστηρίζει την ασφάλεια συσκευών (device security)
- 5) Χρησιμοποιεί το μηχανισμό CSMA-CA για πρόσβαση στο κανάλι
- 6) Χειρίζεται και διατηρεί το μηχανισμό GTS (εγγυημένες χρονικές σχισμές)
- 7) Παρέχει αξιόπιστη ζεύξη ανάμεσα σε δύο ισότιμες (peer) οντότητες MAC από διαφορετικούς κόμβους.

Αναλυτικότερα, οι εργασίες αυτές παρουσιάζονται παρακάτω.

- Δημιουργία ειδοποιήσεων beacons δικτύου (network beacons) αν η συσκευή (device) είναι ένας συντονιστής (coordinator): Ένας συντονιστής (coordinator) μπορεί να καθορίζει αν πρέπει να μπει σε λειτουργία που επιτρέπει σήματα beacons (beacon enabled mode), στην οποία χρησιμοποιείται μία δομή υπερπλαίσιου (superframe structure). Το υπερπλαίσιο (superframe) περιβάλλεται από network beacons και διαιρείται σε aNumSuperframeSlots (προκαθορισμένη τιμή 16) ίσες χρονικές σχισμές (equally sized slots). Ένας συντονιστής (coordinator) στέλνει προς τα έξω ειδοποιήσεις beacons περιοδικά για να συγχρονίσει τις συνδεδεμένες συσκευές (attached devices) και για άλλους σκοπούς.
- Συγχρονισμός στα σήματα beacons: Μια συσκευή (device) συνδεδεμένη σε συντονιστή (coordinator) που λειτουργεί σε λειτουργία που επιτρέπει τα σήματα beacons (beacon enabled mode) μπορεί να ανιχνεύσει τα σήματα beacons για να συγχρονιστεί με το συντονιστή

(coordinator). Αυτός ο συγχρονισμός είναι σημαντικός για data polling, εξοικονόμηση ενέργειας, και ανίχνευση (detection) ορφάνιας (orphanings).

- Υποστήριξη στο δίκτυο προσωπικής περιοχής (personal area network) (PAN) για λειτουργίες της συσχέτισης (association) και της αποσυσχέτισης (disassociation): Για να υποστηρίξει την αυτορρύθμιση (selfconfiguration), το 802.15.4 ενσωματώνει τις λειτουργίες συσχέτισης (association) και αποσυσχέτισης (disassociation) στο δικό του υπό-επίπεδο MAC sublayer.

Με βάση αυτές τις λειτουργίες, αν ένα δίκτυο είναι τοπολογίας αστέρα (star) μπορεί να ρυθμίζεται αυτόματα, ενώ μπορεί να δημιουργηθεί και ένα δίκτυο αυτορρυθμιζόμενο (self-configuring), με τοπολογία ισότιμων κόμβων (peer-to-peer network).

- Η χρήση του μηχανισμού ανίχνευσης φέροντος με πολλαπλή πρόσβαση (carrier sense multiple access) με αποφυγή συγκρούσεων (collision avoidance) (CSMA-CA) για πρόσβαση στο κανάλι:

Όπως όλα τα πρωτόκολλα που σχεδιάστηκαν για ασύρματα δίκτυα το 802.15.4 χρησιμοποιεί το μηχανισμό CSMA-CA για πρόσβαση στο κανάλι. Όμως το νέο πρότυπο δεν περιλαμβάνει το μηχανισμό request-to-send (RTS) και το μηχανισμό clear-to-send (CTS), έχοντας υπόψη του το χαμηλό ρυθμό δεδομένων (low data rate) που χρησιμοποιείται στα LR-WPANs.

- Χειρισμός (Handling) και διατήρηση του μηχανισμού εγγυημένης χρονικής σχισμής (guaranteed time slot) (GTS): Όταν λειτουργεί στη λειτουργία που επιτρέπει τα σήματα beacon (beacon enabled mode), ο συντονιστής (coordinator) μπορεί να ανακατανέμει τμήματα του ενεργού υπερπλασίου (active superframe) σε μία συσκευή (device). Αυτά τα τμήματα (portions) ονομάζονται GTSSs, και περιλαμβάνουν την περίοδο χωρίς συγκρούσεις (contention free period) (CFP) του superframe.

- Παρέχει μια αξιόπιστη ζεύξη (reliable link) ανάμεσα σε δύο ισότιμες (peer) οντότητες του MAC από δύο διαφορετικούς κόμβους:

Το υπό-επίπεδο MAC sublayer χρησιμοποιεί διάφορους μηχανισμούς που ενισχύουν την αξιοπιστία ζεύξης (link) ανάμεσα σε δύο ισότιμους κόμβους (peers). Τέτοιοι μηχανισμοί είναι:

α) η αναγνώριση του πλαισίου (frame acknowledgment)

β) η επαναληπτική μετάδοση (retransmission),

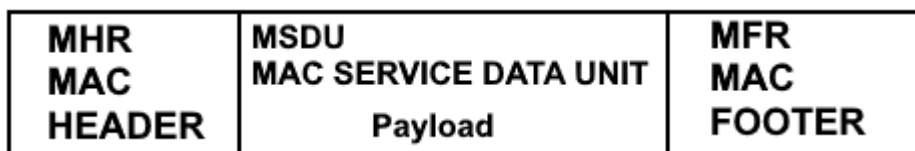
γ) η επικύρωση των δεδομένων (data verification) χρησιμοποιώντας 16-bit CRC,

δ) η τεχνική CSMA-CA.

2.3.6.1 Γενική δομή πλαισίων δεδομένων (frame structure) στρώματος MAC

Μολονότι υπάρχουν τέσσερα διαφορετικά είδη πλαισίων δεδομένων στο στρώμα MAC, που καθορίζονται στο πρότυπο IEEE 802.15.4, ισχύει ότι για όλα τα πλαίσια δεδομένων υπάρχει η ίδια γενική δομή, που αποτελείται από τρία πεδία. Στη συνέχεια, παρουσιάζεται πρώτα η γενική δομή, και ακολούθως, παρουσιάζονται τα τέσσερα διαφορετικά είδη πλαισίων MAC.

Στο παρακάτω σχήμα φαίνονται τα τρία πεδία της γενικής μορφής ενός πλαισίου MAC.



Εικόνα 18. Η γενική δομή του πλαισίου δεδομένων IEEE 802.15.4 για το στρώμα MAC.

Το κάθε ένα από αυτά τα τρία πεδία της γενικής δομής, όπως θα δούμε παρακάτω, υποδιαιρείται σε ένα ή περισσότερα πεδία δεδομένων. Όπως φαίνεται στην εικόνα, κάθε πλαίσιο MAC περιλαμβάνει:

α) την επικεφαλίδα MAC (MAC Header ή MHR)

Η επικεφαλίδα MAC (MAC header) έχει δύο πεδία:

1. Το πεδίο ελέγχου του πλαισίου (frame control field). Το πεδίο ελέγχου (frame control field) μεταφέρει πληροφορίες όπως είναι ο τύπος πλαισίου (frame type) καθώς και άλλες πληροφορίες για τον έλεγχο και τη λειτουργία του δικτύου.
2. Ένα πεδίο διευθύνσεων (addressing field). Το πεδίο διευθύνσεων καθορίζει τον προσδιοριστή PAN του κόμβου πηγής (source PAN identifier), τη διεύθυνση κόμβου πηγής (source node address), τον προσδιοριστή PAN του κόμβου προορισμού (destination PAN identifier) και τη διεύθυνση κόμβου προορισμού (destination address).

β) Τα δεδομένα προς μετάδοση (Payload) που είναι το πεδίο MSDU (MAC Service Data Unit)

Το πεδίο MSDU με τα δεδομένα προς μετάδοση (MAC payload), περιέχει το πλαίσιο με τα πραγματικά δεδομένα (data frame) που πρέπει να μεταδοθούν μεταξύ των συσκευών που επικοινωνούν.

γ) το τελευταίο πεδίο του πλαισίου (MAC footer ή MFR)

Το τελευταίο πεδίο του πλαισίου είναι το MAC footer ή MFR που περιέχει το πεδίο με την ακολουθία ελέγχου πλαισίου (frame check sequence field). Αυτό το πεδίο χρησιμοποιείται για να ανιχνεύει τα σφάλματα στο πλαίσιο.

Αυτά τα πεδία του πλαισίου MAC, φαίνονται στον παρακάτω πίνακα (με χρώμα γκρι). Στην πρώτη γραμμή του πίνακα, φαίνεται η γενική μορφή του πλαισίου με τρία πεδία δεδομένων, όπως είδαμε στην προηγούμενη εικόνα. Κάθε ένα από τα τρία αυτά πεδία υποδιαιρείται σε άλλα περισσότερα πεδία δεδομένων, τα οποία φαίνονται στη δεύτερη γραμμή του πίνακα (με χρώμα γκρι). Στην τρίτη γραμμή του πίνακα φαίνονται οι ονομασίες των πεδίων αυτών στα ελληνικά. Στην τέταρτη γραμμή του πίνακα, φαίνεται το μέγεθος του κάθε πεδίου σε Octets.

MAC header (ή MHR)						MAC Payload	MAC footer (ή MFR)
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address (Διεύθυνση Προορισμού)	Source PAN Identifier	Source Address (Διεύθυνση Πηγής)	Frame Payload	Frame Check Sequence
Έλεγχος Πλαισίου	Αριθμός ακολουθίας	Addressing Διευθυνσιοδότηση				Δεδομένα προς μετάδοση	Έλεγχος ακολουθίας πλαισίου
2 Octets	1 Octet	0 / Octets	0 ως 2 Octets	0 / Octets	0 ως 2 Octets	Μεταβλητό μέγεθος	2 Octets

Πίνακας. Αναλυτική μορφή του πλαισίου MAC.

Το πεδίο ελέγχου πλαισίου (Frame Control) έχει μέγεθος 2 Octets = 16 bits, και με τη σειρά του, υποδιαιρείται σε εννέα πεδία όπως φαίνεται στον παρακάτω πίνακα:

Frame type			Security Enabled	Frame Pending	Ack Request	Intra PAN	Reserved			Destination Addressing Mode		Reserved		Source Addressing Mode	
3 bits			1bit	1 bit	1 bit	1 bit	3 bits			bits 2		bits 2		bits 2	
b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12	b13	b14	b15

Πίνακας. Αναλυτική μορφή πεδίου Frame control (έλεγχος πλαισίου) στο πλαίσιο MAC

Το πεδίο Frame Type, αποτελείται από τρία bits , που ονομάζονται b_0 , b_1 , b_2 . Ανάλογα με τις τιμές των τριών bits στο πεδίο Frame Type, που υπάρχει στο πλαίσιο MAC, διακρίνονται τέσσερα διαφορετικά είδη πλαισίων δεδομένων MAC (MAC Frame types). Το πρότυπο IEEE 802.15.4 έχει καθορίσει τους εξής τέσσερις τύπους πλαισίων δεδομένων MAC : α) Data frame, β) Beacon frame, γ) Acknowledgement Frame, δ) MAC Command frame. Αυτοί οι τέσσερις τύποι πλαισίων θα παρουσιαστούν στη συνέχεια.

Στον παρακάτω πίνακα, φαίνονται οι τιμές των τριών bits του πεδίου Frame Type και οι αντίστοιχοι τέσσερις τύποι πλαισίων (Frame Types)

Frame Type			Περιγραφή
b_0	b_1	b_2	
0	0	0	Beacon (πλαίσιο beacon)
0	0	1	Data (πλαίσιο δεδομένων)
0	1	0	Acknowledgement (πλαίσιο αναγνώρισης)
0	1	1	MAC Command (Εντολή MAC)
Οι τιμές από 100 ως 111 είναι κρατημένες (Reserved)			

Πίνακας. πεδίο Frame Type στο πλαίσιο MAC

Παρακάτω παρουσιάζονται οι τέσσερις τύποι πλαισίων.

2.3.6.2 Data frame (Πλαίσιο δεδομένων)

Περιέχει ένα πεδίο με πραγματικά δεδομένα προς μετάδοση (payload) που έχουν μήκος μέχρι 104 octets. Κάθε πλαίσιο δεδομένων (data frame) περιέχει έναν αριθμό ακολουθίας (sequence number) ο οποίος προσδιορίζει με μοναδικό τρόπο το πλαίσιο. Ο αριθμός ακολουθίας (sequence number) εξασφαλίζει ότι όλα τα πλαίσια λαμβάνονται υπόψη στην καταμέτρηση και φτάνουν με μία προκαθορισμένη σειρά στο δέκτη. Το πεδίο FCS χρησιμοποιείται για να ανιχνεύει τα πλαίσια που έχουν σφάλματα.

Τα πεδία αυτά φαίνονται στον παρακάτω πίνακα (με χρώμα γκρι)

MAC header ή MHR			MAC Payload	MAC footer ή MFR
Frame Control	Data Sequence Number	Address Information	Data	Frame Check Sequence
2 Octets	1 Octet	4 ως 20 Octets	Μεταβλητό μέγεθος	2 Octets

Πίνακας. Η μορφή ενός πλαισίου δεδομένων (Data Frame).

2.3.6.3 Beacon frame (Πλαίσιο σήματος Beacon)

Εκπέμπεται περιοδικά από τον συντονιστή (coordinator). Το πλαίσιο beacon εξυπηρετεί πολλούς σκοπούς, όπως είναι η αναγνώριση του δικτύου και της δομής του, το «ξύπνημα» (waking up) των συσκευών από την κατάσταση ύπνου (sleep mode) και η μετάβασή τους σε κατάσταση ακοής (listening mode) και ο συγχρονισμός των λειτουργιών του δικτύου. Τα πλαίσια beacon είναι ιδιαίτερα σημαντικά σε δίκτυα με τοπολογία πλέγματος (mesh) ή σε δίκτυα με τοπολογία δέντρου συστοιχιών (cluster-tree). Διατηρούν όλους τους κόμβους του δικτύου συγχρονισμένους χωρίς να απαιτείται να παραμένουν οι κόμβοι σε κατάσταση ενεργοποίησης ή «ξύπνιοι» (awake) για μεγάλες χρονικές περιόδους και έτσι μειώνεται η κατανάλωση ενέργειας.

Τα πεδία φαίνονται στον παρακάτω πίνακα (με χρώμα γκρι)

MAC header (ή MHR)			MAC Payload				MAC footer
Frame Control	Beacon Sequence number	Source Address	Superframe Specification	GTS fields	Pending Address Fields	Beacon Payload	Frame Check Sequence
2 Octets	1 Octet	4 ως 10 Octets	2 Octets	Μεταβλητό μέγεθος	Μεταβλητό μέγεθος	Μεταβλητό μέγεθος	2 Octets

Πίνακας. Η μορφή ενός πλαισίου Beacon (Beacon Frame).

Τα πεδία του beacon frame, με τη σειρά τους, υποδιαιρούνται σε περισσότερα πεδία. Μερικά από αυτά φαίνονται αναλυτικά στους παρακάτω πίνακες:

SuperFrame Specification (Προδιαγραφή υπερπλαισίου) έχει μέγεθος 2 Octets = 16 bits

Beacon Order	SuperFrame Order	Final CAP Slot	Battery life extension	Reserved	PAN Coordinator	Association Permit
4 bits	4 bits	4 bits	1 bit	1 bit	1 bit	1 bit
0 b1 b2 b3	b4 b5 b6 b7	b8 b9 b10 b11	b12	b13	b14	b15

Πίνακας. Το πεδίο προδιαγραφή υπερπλασίου (superframe specification).

Το πεδίο Pending Address Fields

Pending Address Specification	Address List
1 Octet	Μεταβλητό μέγεθος

Πίνακας. Το πεδίο Pending Address fields.

Το πεδίο GTS Fields (Πεδία εγγυημένων σχισμών χρόνου GTS, Guarantee Time Slots) υποδιαιρείται σε τρία πεδία:

GTS Specification	GTS Directions	GTS List
1 Octet	0 ως 1 Octet	Μεταβλητό μέγεθος ως 3 Octets

Πίνακας. Το πεδίο GTS fields.

Τα τρία πεδία αυτά, φαίνονται στους παρακάτω πίνακες.

Το πεδίο GTS Specification έχει μέγεθος 1 Octet = 8 bits

GTS Descriptor Count	Reserved	GTS Permit
3 bits	4 bits	1 bit
b0 b1 b2	b3 b4 b5 b6	b7

Πίνακας Το πεδίο GTS Specification

Το πεδίο GTS Directions έχει μέγεθος μέχρι 1 Octet = 8 bits

GTS Directions Mask	Reserved
7 bits	1 bit
b0 b1 b2 b3 b4 b5 b6	b7

Πίνακας Το πεδίο GTS Directions.

Το πεδίο GTS List έχει μεταβλητό μέγεθος μέχρι 3 Octets = 24 bits

Device Short Address																GTS Starting Slot				GTS Length			
16 bis																4bits				4 bits			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Πίνακας Το πεδίο GTS List.

2.3.6.4 Acknowledgement frame (πλαίσιο αναγνώρισης ή πλαίσιο επιβεβαίωσης λήψης πακέτου)

Χρησιμοποιείται από έναν δέκτη που προηγουμένως είχε λάβει κάποιο άλλο πλαίσιο δεδομένων από τον κόμβο αποστολέα και τώρα στέλνει πίσω στον αποστολέα το πλαίσιο αναγνώρισης για να επιβεβαιώσει την επιτυχή λήψη πλαισίου δεδομένων (data frame) που είχε στείλει προηγουμένως ο αποστολέας. Όταν λάβει το πλαίσιο αναγνώρισης ο αποστολέας, αυτό συνιστά μία επιβεβαίωση ότι το αντίστοιχο πλαίσιο δεδομένων (data frame) έχει φτάσει επιτυχώς στο δέκτη, χωρίς σφάλματα και με τη σωστή σειρά. Ένα πλαίσιο δεδομένων (data frame) και το αντίστοιχο πλαίσιο αναγνώρισης (acknowledgment frame) αντιστοιχίζονται μεταξύ τους με βάση τους δικούς τους αριθμούς ακολουθίας (sequence numbers).

Τα πεδία αυτά φαίνονται στον παρακάτω πίνακα (με χρώμα γκρι) και όπως φαίνεται δεν υπάρχει πεδίο payload σε αυτό το πλαίσιο.

MAC header ή MHR		MAC Footer ή MFR
Frame Control	Data Sequence Number	Frame Check Sequence
	1 Octet	2 Octets

Πίνακας. Η μορφή ενός πλαισίου αναγνώρισης (Acknowledgement Frame)

2.3.6.5 MAC command frame (πλαίσιο εντολών MAC)

Χρησιμοποιείται από τις ενότητες MAC διαφορετικών συσκευών για διαπραγμάτευση και για επικοινωνία μεταξύ τους. Το πλαίσιο αυτό παρέχει ένα μηχανισμό για έναν κεντρικό διαχειριστή

δικτύου για να ελέγχει και να ρυθμίζει συσκευές από απόσταση, ανεξαρτήτως από το μέγεθος του και την τοπολογία του δικτύου. Συνήθεις εντολές (commands) είναι η συσχέτιση συσκευών (device association) η αποσυσχέτιση συσκευών (device dis-association) η αίτηση (request), η ειδοποίηση (notification), η αίτηση δεδομένων (data request), η ειδοποίηση διένεξης (conflict notification), με βάση το αναγνωριστικό PAN ID, η ειδοποίηση ορφάνιας (orphan notification), η αίτηση beacon request, η αίτηση GTS request, και η επανευθυγράμμιση του συντονιστή (coordinator realignment).

Τα πεδία του πλαισίου εντολών φαίνονται στον παρακάτω πίνακα (με χρώμα γκρι).

MAC header ή MHR			MAC payload		MAC footer ή MFR
Frame Control	Data Sequence	Address Information	Command Frame Identifier	Command	Frame Check Sequence
	1 Octet	4 ως ... Octets	1 Octet	Μεταβλητό μέγεθος	2 Octets

Πίνακας. Η μορφή ενός πλαισίου εντολών (Command Frame)

Κάθε πλαίσιο εντολών μπορεί να περιέχει διαφορετική εντολή. Οι εντολές που περιέχονται μέσα σε ένα πλαίσιο εντολών, καθορίζονται στο πεδίο Command Frame Identifier, που έχει μέγεθος 1 Octet και βρίσκεται στο πεδίο MAC Payload πριν από τα δεδομένα της εντολής. Τα bits του πεδίου Command Frame Identifier έχουν διαφορετικές τιμές για διαφορετικές εντολές που μεταφέρει το πλαίσιο εντολών.

Στον παρακάτω πίνακα φαίνονται διάφορες εντολές ανάλογα με τις 16-δικές τιμές που έχουν τα δεδομένα στο πεδίο Command frame Identifier.

Command Frame Identifier	Command name (Όνομα εντολής)	RFD (Κόμβος)	
		Tx (Πομπός)	Rx (Δέκτης)
0x01	Association Request (Αίτηση συσχέτισης)	X	
0x02	Association Response (Απόκριση συσχέτισης)		X
0x03	Dis-Association Notification (Ειδοποίηση Από-συσχέτισης)	X	X
0x04	Data Request (Αίτηση δεδομένων)	X	
0x05	PAN ID Conflict Notification (Ειδοποίηση διένεξης)	X	
0x06	Orphan Notification (Ειδοποίηση ορφάνιας)	X	
0x07	Beacon Request		

0x08	Coordinator realignment (Επανευθυγράμμιση συντονιστή)		X
0x09	GTS Request (Αίτηση εγγυημένων σχισμών)		
0x0a - 0	Reserved (Κρατημένες)		

Πίνακας. Οι τύποι πλαισίων εντολών (Comman Frame Types)

2.3.6.6 Οι δύο λειτουργίες

Το IEEE 802.15.4 υποστηρίζει δύο λειτουργίες:

- α) Beacon Enabled Mode, slotted CSMA/CA (λειτουργία με σήματα ειδοποίησης beacons)
- β) Non-Beacon Enabled Mode, unslotted CSMA/CA (λειτουργία χωρίς σήματα ειδοποίησης beacons)

Οι λειτουργίες αυτές εξηγούνται παρακάτω.

Beacon Enabled Mode, slotted CSMA/CA (Λειτουργία με σήματα ειδοποίησης beacons)

Η λειτουργία που επιτρέπει τα Beacon (Beacon Enabled Mode) χρησιμοποιείται για εξοικονόμηση ενέργειας. [12] Η λειτουργία beacon mode παρέχει συγχρονισμό στο δίκτυο. Χρησιμοποιεί slotted CSMA/CA (Carrier Sense Multiple Access Πολλαπλή πρόσβαση με ανίχνευση φέροντος)(Collision Avoidance αποφυγή συγκρούσεων). Οι κόμβοι δεν είναι συνεχώς ενεργοποιημένοι σε κατάσταση που ακούν το κανάλι (listening) αλλά μπορούν να μεταβαίνουν σε λειτουργία χαμηλής κατανάλωσης ενέργειας (low power) αν ξεπεραστούν κάποια όρια χρόνου που μένουν ενεργοί (wake-up). Έτσι, κάθε κόμβος παραμένει στην κατάσταση χαμηλής λειτουργίας για ένα τυχαίο χρονικό διάστημα (random delay). Μετά ό κόμβος ξυπνά ξανά (wake-up) και ακούει το κανάλι. Αυτό πρέπει να συμβεί μέσα σε 2 χρονικές σχισμές που λέγονται backoff slots. Όταν αυτοί οι κόμβοι πρόκειται να λάβουν δεδομένα, έρχεται ένα σήμα beacon που ανακοινώνει ότι υπάρχουν δεδομένα που πρέπει να ληφθούν. Τα δεδομένα περιμένουν στον κεντρικό κόμβο συντονιστή (central coordinator). Ο συντονιστής πρώτα λαμβάνει από τη συσκευή ένα μήνυμα αίτησης δεδομένων (data request message) που δηλώνει ότι η συσκευή είναι σε κατάσταση ενεργή και ακούει το δίκτυο (listening) και μετά στέλνει τα δεδομένα στην συσκευή. Στην λειτουργία που επιτρέπει beacon, υπάρχουν χρονικές περίοδοι που ανακοινώνονται από το beacon, στις οποίες ολόκληρο το δίκτυο μπορεί να τεθεί σε κατάσταση sleep για μεγαλύτερη εξοικονόμηση ενέργειας. Μαζί με το CSMA/CA, που είναι υποχρεωτική η χρήση του μπορεί να προστεθεί προαιρετικά το TDMA. Η δομή υπερπλαισίου (superframe) χρησιμοποιείται για να οργανωθεί η πρόσβαση στο

κανάλι για επικοινωνίες δεδομένων και ορίζεται στη λειτουργία beacon mode. Το υπερπλάσιο περιγράφεται παρακάτω.

Non-Beacon Enabled Mode unslotted CSMA/CA (Λειτουργία χωρίς σήματα ειδοποίησης beacons)

Το πρότυπο 802.15.4 υποστηρίζει και μια δεύτερη λειτουργία πρόσβασης μέσου (MAC) που δεν βασίζεται σε σήματα beacons και λέγεται ασύγχρονη λειτουργία. Και σε αυτόν τον μηχανισμό υπάρχει χρόνος καθυστέρησης (delay time) που ελαχιστοποιεί το χρόνο που οι κόμβοι ακούν το κανάλι. Όμως είναι πιο δύσκολο να υλοποιηθεί επειδή δεν υπάρχουν τα beacons [12]. Στη λειτουργία χωρίς beacons (non-beacon mode), στο πρότυπο IEEE 802.15.4 MAC, μόνο για τις τελικές συσκευές του δικτύου (end devices) ορίζεται ένας κύκλος ύπνου (sleep cycle) και μία περίοδος ξυπνήματος (wake-up period). Οι κεντρικοί κόμβοι συντονιστές (coordinators) είναι συνεχώς ενεργοποιημένοι και δεν μεταβαίνουν ποτέ σε κατάσταση ύπνου (sleep). Επίσης δεν υπάρχει μηχανισμός για εγγυημένες σχισμές χρόνου GTS χωρίς συγκρούσεις. Επομένως, το πρωτόκολλο IEEE 802.15.4 MAC περιλαμβάνει μόνο τη μετάδοση δεδομένων με συγκρούσεις (contention-based). Η μεταφορά δεδομένων γίνεται με έναν μηχανισμό CSMA/CA χωρίς σχισμές χρόνου (un-slotted), εκτελώντας μόνο μία φορά τον έλεγχο καθαρού καναλιού (single CCA operation). Δεν χρησιμοποιείται η μέθοδος στην οποία οι κόμβοι ακούν το δίκτυο για τα πακέτα δεδομένων που έρχονται πριν από τα κανονικά δεδομένα (preamble sampling). Μόλις τα δεδομένα ληφθούν επιτυχώς από έναν κόμβο, τότε αυτός ο κόμβος κατευθείαν στέλνει σήμα επιβεβαίωσης λήψης πακέτου ACK στον κόμβο αποστολέα. Αυτό γίνεται άμεσα για να εξασφαλιστεί ότι υπάρχει αξιοπιστία. Στη λειτουργία χωρίς beacon η εξοικονόμηση ενέργειας επιτυγχάνεται με τον κύκλο ύπνου (sleep cycle) των τελικών συσκευών, όμως η ενέργεια που εξοικονομείται είναι μικρότερη από ότι η ενέργεια που εξοικονομείται στην λειτουργία με σήματα beacon. (beacon mode).

2.3.7 Γενικές λειτουργίες (General Functions)

Το πρότυπο δίνει λεπτομερείς προδιαγραφές για τα παρακάτω στοιχεία:

- τύπος συσκευής (type of device),
- δομή του πλαισίου (frame structure),
- δομή του υπερπλαισίου (superframe structure),

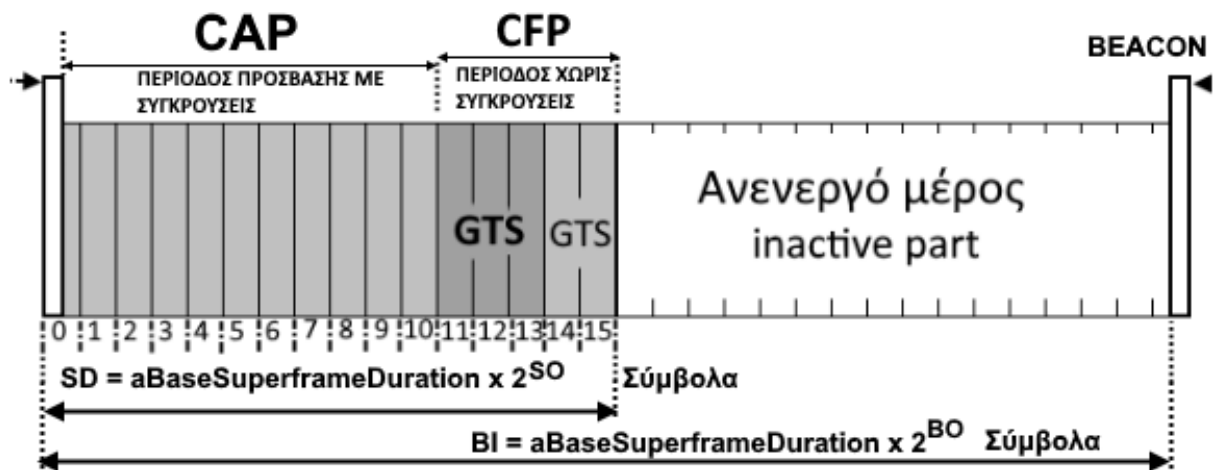
- μοντέλο μεταφοράς δεδομένων,
- ευρωστία (robustness),
- θέματα για την κατανάλωση ενέργειας,
- ασφάλεια.

Μερικά θέματα που μπορούν να παρουσιαστούν λεπτομερώς είναι ο τύπος συσκευής, η δομή υπερπλαισίου, το μοντέλο μεταφοράς δεδομένων (data transfer model), και τα θέματα κατανάλωσης ενέργειας.

2.3.7.1 Η προαιρετική χρήση της δομής υπερπλαισίου (superframe)

Το πρότυπο επιτρέπει την προαιρετική χρήση της δομής υπερπλαισίου (superframe structure), που ορίζεται στο υποεπίπεδο MAC του IEEE 802.15.4.

Η μορφή του υπερπλαισίου superframe καθορίζεται από τον συντονιστή coordinator.



Εικόνα 19. Ένα παράδειγμα της δομής του υπερπλαισίου (Superframe Structure)

Στην παραπάνω εικόνα, φαίνεται ότι το superframe περιλαμβάνει ένα ενεργό μέρος (active part) (που είναι χρωματισμένο γκρι), και ένα προαιρετικό ανενεργό μέρος (inactive part). Το superframe οριοθετείται από δύο σήματα beacons, ένα στην αρχή και ένα στο τέλος του. Το ενεργό μέρος (active part), είναι μία χρονική περίοδος που διαφείται σε 16 ίσες σχισμές χρόνου (time slots), με αρίθμηση από 0 ως 15, όπως φαίνεται στην εικόνα. Συνήθως το πλαίσιο του beacon (beacon frame) μεταδίδεται στην πρώτη χρονική σχισμή (time slot), δηλαδή στην slot 0. Το σήμα beacon

εκπέμπεται από τον συντονιστή (coordinator) και περιέχει πληροφορίες για τη μορφή του πλαισίου και ειδοποιήσεις για μηνύματα που περιμένουν στους κόμβους προς αποστολή. Όταν αυτά τα μηνύματα είναι πάρα πολλά, τότε μερικά σήματα Beacon είναι μεγαλύτερα από τα κανονικά Beacon επειδή, περιλαμβάνουν περισσότερες ειδοποιήσεις notifications. Για αυτό, η πρώτη και η δεύτερη χρονική σχισμή, δηλαδή η slot 0 και η slot 1, ονομάζονται και περίοδος επέκτασης του Beacon (Beacon extension period) BEP και δεσμεύονται για να μεταδίδονται τα μεγαλύτερα beacons. Ο βασικός σκοπός του beacon είναι να συγχρονίζει τις συσκευές, να προσδιορίζει το δίκτυο προσωπικής περιοχής PAN και να περιγράφει τη δομή του υπερπλαισίου (superframe). Το ενεργό μέρος (active part) του superframe, όπως θα αναφερθεί στη συνέχεια, διαιρείται σε δύο μέρη που είναι η περίοδος πρόσβασης με συγκρούσεις (Contention Access Period) (CAP) και η περίοδος χωρίς συγκρούσεις (Contention-Free Period) (CFP) που χρησιμοποιεί μέχρι επτά χρονικές σχισμές (time slots) και ονομάζεται αλλιώς και GTS, εγγυημένες χρονικές σχισμές (Guaranteed Time Slots).

Το μήκος του superframe (λέγεται και beacon interval, BI) και το μήκος το ενεργού μέρους του (λέγεται και διάρκεια superframe duration, SD) καθορίζονται ως εξής :

$$BI = aBaseSuperframeDuration * 2^{BO}$$

$$SD = aBaseSuperframeDuration * 2^{SO}$$

όπου,

$$aBaseSuperframeDuration = 960 \text{ symbols}$$

$$BO = \text{beacon order}$$

$$SO = \text{superframe order}$$

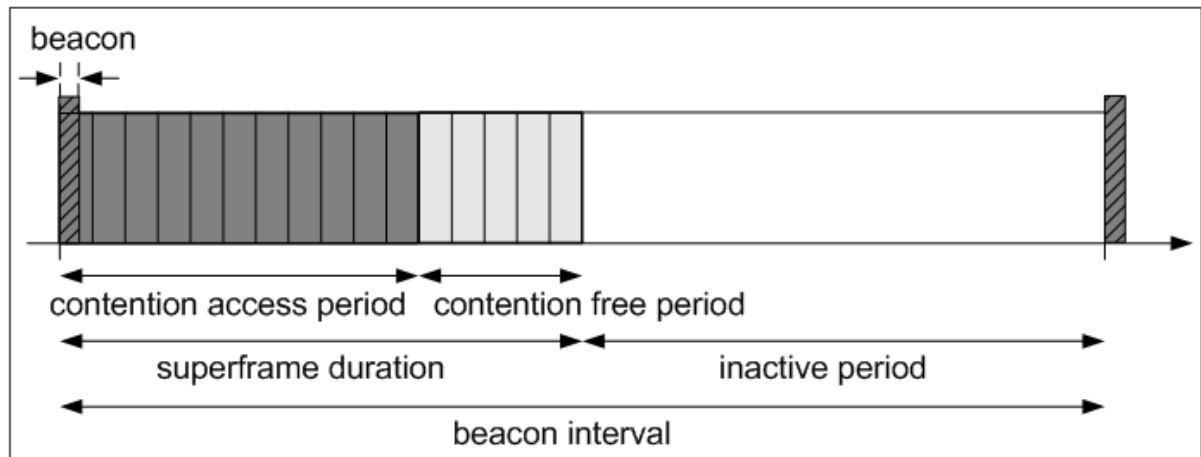
Οι τιμές BO και SO καθορίζονται από τον συντονιστή (coordinator). Το ενεργό μέρος active part του υπερπλαισίου (superframe), διαιρείται σε χρονικές σχισμές (slots) ίσου μεγέθους (equally sized) που το πλήθος τους είναι η τιμή της μεταβλητής

$$aNumSuperframeSlots \text{ (προκαθορισμένη τιμή 16).}$$

Το πλαίσιο beacon frame μεταδίδεται (transmitted) στην πρώτη χρονική σχισμή (slot) κάθε υπερπλαισίου (superframe).

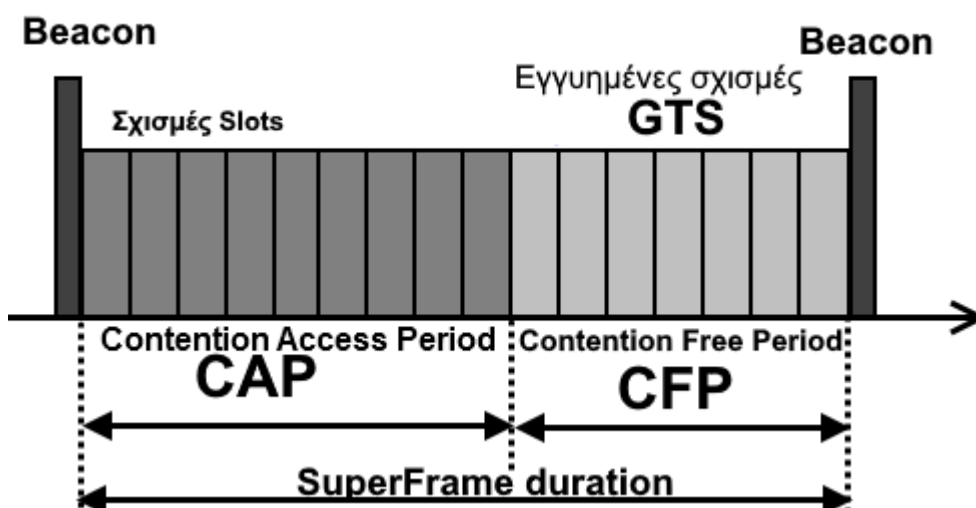
Το ενεργό μέρος (active part) του υπερπλαισίου μπορεί να διαιρεθεί επιπλέον, ακόμη περισσότερο σε 2 περιόδους, μία περίοδο χρόνου πρόσβασης με συγκρούσεις (contention access period) (CAP) και μία προαιρετική περίοδο χρόνου χωρίς συγκρούσεις (contention free period) (CFP).

Η προαιρετική χρονική περίοδος χωρίς συγκρούσεις CFP μπορεί να στεγάσει (accommodate) μέχρι 7 εγγυημένες σχισμές χρόνου (guaranteed time slots) (GTSs), και μία GTS μπορεί να καταλαμβάνει περισσότερες χρονικές περιόδους από μία χρονική σχισμή (slot). Αυτές οι περίοδοι φαίνονται στις εικόνες 14 και 15.



Εικόνα 20 Το υπερπλαίσιο με τις περιόδους CAP και CFP Πηγή: [10]

Όμως, ένα σημαντικό μέρος (portion) της χρονικής περιόδου με συγκρούσεις CAP πρέπει να παραμείνει για πρόσβαση με βάση τις συγκρούσεις (contention based access) άλλων συσκευών του δικτύου (networked devices) ή νέων συσκευών devices που θέλουν να συνδεθούν στο δίκτυο. Οι συσκευές χρησιμοποιούν slotted CSMA-CA και ανταγωνίζονται για τη χρήση των σχισμών χρόνου (slots).



Εικόνα 21 Η χρονική περίοδος χωρίς συγκρούσεις CFP μπορεί να στεγάσει (accommodate) μέχρι 7 εγγυημένες σχισμές χρόνου GTSs

Ο μηχανισμός slotted CSMA-CA χρησιμοποιείται για πρόσβαση στο κανάλι (channel access) στη διάρκεια της περιόδου πρόσβασης με συγκρούσεις CAP. Όλες οι συναλλαγές που βασίζονται σε συγκρούσεις (contention based transactions) πρέπει να ολοκληρωθούν πριν να αρχίσει η περίοδος χωρίς συγκρούσεις CFP. Επίσης όλες οι συναλλαγές GTSs πρέπει να γίνουν πριν από το χρόνο του επόμενου GTS ή στο τέλος της περιόδου χωρίς συγκρούσεις CFP.

2.3.7.2 Μεταφορά δεδομένων

Η μεταφορά δεδομένων (Data transfer) μπορεί να γίνει με 3 διαφορετικούς τρόπους:

- α) από τη συσκευή device σε έναν συντονιστή coordinator
- β) από τον συντονιστή coordinator σε μια συσκευή device
- γ) από έναν κόμβο peer σε άλλο ισότιμο κόμβο σε ένα δίκτυο peer-to-peer πολλαπλών αλμάτων (multi-hop) network.

Για τη μελέτη απόδοσης (performance study), κατηγοριοποιούμε την μεταφορά δεδομένων (data transfer) στα παρακάτω τρία είδη:

- Άμεση μετάδοση δεδομένων (Direct data transmission): Αυτό εφαρμόζεται σε όλες τις μεταφορές δεδομένων (data transfers), είτε από μία συσκευή device σε έναν συντονιστή coordinator, είτε από συντονιστή coordinator σε μία συσκευή device, ή ανάμεσα σε δύο ισότιμους κόμβους peers. Για τη μετάδοση δεδομένων χρησιμοποιείται είτε η unslotted CSMA-CA και λειτουργία χωρίς σήματα beacon) (non-beacon enabled mode), είτε χρησιμοποιείται η slotted CSMA-CA και λειτουργία με σήματα beacon (beacon enabled mode).

- Έμμεση μεταφορά δεδομένων (Indirect data transmission): Αυτό εφαρμόζεται μόνο σε μεταφορά δεδομένων (data transfer) από έναν συντονιστή coordinator στις συσκευές (devices) του. Σε αυτή τη λειτουργία (mode), ένα πλαίσιο δεδομένων (data frame) διατηρείται σε λίστα συναλλαγών (transaction list) από τον συντονιστή (coordinator), και περιμένει για εξαγωγή (extraction) από την αντίστοιχη συσκευή (device). Μία συσκευή device μπορεί να ανακαλύψει αν

υπάρχει ένα πακέτο για αυτήν που περιμένει (pending) στη λίστα συναλλαγών (transaction list) και αυτό το κάνει ελέγχοντας τα πλαίσια beacon (beacon frames) που λαμβάνει από τον συντονιστή της coordinator. Μερικές φορές, η έμμεση μετάδοση δεδομένων (indirect data transmission) μπορεί επίσης να συμβεί στη λειτουργία χωρίς σήματα beacon (non-beacon enabled mode). Για παράδειγμα, στην διαδικασία συσχέτισης (association procedure), ο συντονιστής (coordinator) διατηρεί το πλαίσιο της απόκρισης συσχετίσεων (association response frame) στη λίστα συναλλαγών του (transaction list) και η συσκευή polls και εξάγει (extracts) το πλαίσιο απόκρισης συσχέτισης (association response frame). Είτε η Unslotted CSMA-CA είτε η slotted CSMA-CA χρησιμοποιείται στη διαδικασία εξαγωγής δεδομένων (data extraction procedure).

- Η μετάδοση δεδομένων GTS data transmission: Αυτή βρίσκει εφαρμογή μόνο σε μεταφορά δεδομένων (data transfer) ανάμεσα σε μία συσκευή device και τον συντονιστή της (coordinator), είτε από τη συσκευή device προς το συντονιστή coordinator είτε από το συντονιστή coordinator προς τη συσκευή device. Δεν απαιτείται να χρησιμοποιηθεί CSMA-CA στη μετάδοση δεδομένων GTS data transmission.

Η εξοικονόμηση της ενέργειας (Power conservation) ήταν ένας στόχος της έρευνας για τα ασύρματα δίκτυα (wireless networks), διότι οι περισσότερες συσκευές σε ασύρματα δίκτυα τροφοδοτούνται από μπαταρία. Το πρότυπο που αναπτύχθηκε έλαβε υπόψη του την περιορισμένη ενέργεια τροφοδοσίας που παρέχει η μπαταρία και ο σχεδιασμός έλαβε κατάλληλα μέτρα για τις συσκευές που τροφοδοτούνται από μπαταρίες. Η δομή του υπερπλαισίου (superframe structure), η έμμεση μετάδοση δεδομένων (indirect data transmission) και η επιλογή BatteryLifeExtension είναι τέτοια παραδείγματα που σχεδιάστηκαν ειδικά για αυτές τις συσκευές. Αν η BatteryLifeExtension τεθεί στην τιμή TRUE, όλες οι συναλλαγές που βασίζονται στη διένεξη (contention based transactions) απαιτείται να ξεκινούν μέσα στην macBattLifeExtPeriods (προκαθορισμένη τιμή 6) σε περιόδους full backoff periods μετά από την χρονική περίοδο inter-frame space (IFS) period του πλαισίου beacon frame. [13]

2.3.8 Χαρακτηριστικά ασφάλειας του IEEE 802.15.4

Το πρότυπο IEEE 802.15.4 διαθέτει κάποια χαρακτηριστικά, για να αντιμετωπίζει τα διάφορα θέματα ασφάλειας που προκύπτουν. Οι ασύρματες επικοινωνίες είναι από τη φύση τους

ευαίσθητες σε παρεμβολές (interference) και σε υποκλοπές. Το πρότυπο IEEE 802.15.4 χρησιμοποιεί ένα πρωτόκολλο που βασίζεται πλήρως στην χειραψία (fully handshake) για αξιοπιστία στη μεταφορά δεδομένων (data transfer reliability) και ενσωματώνει ένα πρότυπο κρυπτογράφησης Advanced Encryption Standard (AES) για να υπάρχει ασφάλεια στη μεταφορά δεδομένων (secure data transfer). [14]. Η χειραψία (handshake) είναι μία διαδικασία πριν την έναρξη της κανονικής επικοινωνίας, όπου οι δύο σταθμοί που επικοινωνούν, ρυθμίζουν δυναμικά κάποιους κανόνες και παραμέτρους. Το πρότυπο AES είναι αλγόριθμος για μία τεχνική κρυπτογράφησης που υιοθετήθηκε στην Αμερική το 2001 από το National Institute of Standards and Technology (NIST). Ο Αλγόριθμος αυτός είναι block cipher που εκτελεί κρυπτογράφηση και αποκρυπτογράφηση των μπλοκ δεδομένων με συμμετρικά κλειδιά (symmetric key). Τα μπλοκ δεδομένων που θα κρυπτογραφηθούν είναι 128 bit και το μήκος κλειδιού επιτρέπεται να είναι ένα από τα τρία διαφορετικά μεγέθη : 128, 192 και 256 bits. Η κρυπτογράφηση αποτελείται από :

10 γύρους επεξεργασίας δεδομένων αν το μήκος κλειδιού είναι 128 bit,

12 γύρους επεξεργασίας, αν το μήκος κλειδιού είναι 192 bit και

14 γύρους επεξεργασίας, αν το μήκος κλειδιού είναι 256 bit.

Τα 128 bits του μπλοκ δεδομένων χωρίζονται σε 16 bytes και τα bytes τοποθετούνται σε έναν πίνακα 4x4 που ονομάζεται πίνακας κατάστασης (state array) του AES. Κάθε γύρος επεξεργασίας περιλαμβάνει τέσσερα βήματα αλλαγών στον πίνακα:

1. αντικατάσταση ενός μόνο byte,
2. μία μετάθεση των στοιχείων σε μία γραμμή του πίνακα,
3. μία μίξη των στοιχείων σε μία στήλη του πίνακα
4. και μία πρόσθεση του κλειδιού.

Στην αποκρυπτογράφηση τα βήματα αυτά γίνονται με διαφορετική σειρά. Η πλήρης διαδικασία κρυπτογράφησης/αποκρυπτογράφησης AES είναι αρκετά πιο πολύπλοκη και δεν περιγράφεται εδώ.

2.4 TDMA

Η πολυπλεξία με διαίρεση χρόνου TDMA (Time Division Multiplex Access) χρησιμοποιείται στα ασύρματα δίκτυα αισθητήρων. Το TDMA με διάφορες μορφές έχει χρησιμοποιηθεί στην κινητή τηλεφωνία και στις δορυφορικές επικοινωνίες.

Το πρωτόκολλο TDMA γενικά έχει στόχο να ελέγξει την πρόσβαση σε ένα κοινό κανάλι επικοινωνίας που το διαμοιράζονται πολλοί κόμβοι nodes. Αυτό το κανάλι είναι το κοινό μέσο. Για να υπάρξει πρόσβαση όλων των κόμβων στο κανάλι, πρέπει να ρυθμιστεί για όλους τους κόμβους η χρήση του καναλιού με έναν μηχανισμό που αποφεύγει τις συγκρούσεις. Η χρήση του μέσου, ρυθμίζεται από το στρώμα MAC, (Medium Access Layer) (στρώμα ελέγχου πρόσβασης μέσου) επομένως το TDMA κυρίως αφορά το στρώμα MAC. Όμως σε αυτή την παράγραφο περιγράφεται ένα γενικό μοντέλο TDMA ανεξάρτητα από οποιοδήποτε πρωτόκολλο που βασίζεται σε αυτό. Υπάρχουν διάφορα πρωτόκολλα που διαφέρουν από το γενικό μοντέλο.

Το κανάλι επικοινωνίας διαιρείται σε σχισμές χρόνου slots και κάθε σχισμή έχει σταθερό μήκος (fixed length) δηλαδή σταθερή χρονική διάρκεια. [15]

Σε αυτές τις χρονικές σχισμές slots ανατίθεται από ένα ζεύγος κόμβων (pair of nodes) που επικοινωνούν μεταξύ τους με μια ζεύξη (link). Με αυτό τον τρόπο υπάρχει ο πλήρης έλεγχος για το ποιοι κόμβοι στέλνουν δεδομένα και σε ποια χρονική στιγμή. Ο μηχανισμός πολυπλεξίας καθορίζει πότε ένας κόμβος πρέπει να μεταδώσει δεδομένα και πότε αναμένει να λάβει δεδομένα. Έτσι δεν υπάρχουν συγκρούσεις. Τέτοιες συγκρούσεις θα υπήρχαν αν περισσότεροι κόμβοι επιχειρούσαν να στείλουν δεδομένα την ίδια στιγμή στο ίδιο κανάλι επικοινωνίας.

2.4.1 Χαρακτηριστικά του TDMA

Παρακάτω περιγράφονται μερικά βασικά χαρακτηριστικά της πολυπλεξίας με διαίρεση χρόνου TDMA. Τα χαρακτηριστικά που αναφέρονται εδώ, είναι γενικά και δεν αφορούν ένα συγκεκριμένο πρότυπο. Έτσι, ενδεχομένως να υπάρχουν σημαντικές διαφορές σε άλλα πρότυπα που χρησιμοποιούν TDMA, αλλά δεν αναφέρονται εδώ, σε αυτή την εργασία.

2.4.1.1 Συγκρούσεις

Υπάρχουν δύο κατηγορίες συγκρούσεων:

α) Οι πρωτεύουσες συγκρούσεις

Συμβαίνουν όταν ένας κόμβος λαμβάνει δεδομένα και στέλνει δεδομένα στην ίδια χρονική σχισμή (time slot), ή όταν λαμβάνει δεδομένα από δύο διαφορετικούς κόμβους ταυτόχρονα στην ίδια χρονική σχισμή (time slot).

β) Οι δευτερεύουσες συγκρούσεις

Συμβαίνουν όταν ένας κόμβος προορισμού δεδομένων γίνεται δέκτης μιας μετάδοσης (transmission) που προορίζεται για αυτόν και ταυτόχρονα γίνεται δέκτης και μίας άλλης μετάδοσης που δεν προορίζεται για αυτόν.

Η μέθοδος TDMA μπορεί να οριστεί ως η διαδικασία ανάθεσης σχισμών χρόνου (time slots) στους κόμβους ώστε να αποφεύγονται οι συγκρούσεις.

2.4.1.2 Κεντρική διαχείριση από κεντρικό σταθμό βάσης

Η μέθοδος TDMA απαιτεί να υπάρχει μια κεντρική διαχείριση για την ανάθεση των χρονικών σχισμών σε κόμβους με βάση ένα χρονικό πρόγραμμα schedule.

Για αυτό, υπάρχει ένας κεντρικός κόμβος που είναι ο σταθμός βάσης (base station) και ο ρόλος του είναι να συντονίζει όλους τους κόμβους του δικτύου.

Σε κάθε κόμβο του δικτύου ανακατανέμεται ένα σύνολο σχισμών χρόνου (time slots). Σε αυτές τις σχισμές χρόνου ο κόμβος μπορεί να μεταδώσει τα δεδομένα.

Οι χρονικές σχισμές (slots) συνήθως είναι οργανωμένες σε ένα πλαίσιο (frame).

Το πλαίσιο αυτό επαναλαμβάνεται περιοδικά.

2.4.1.3 Το σήμα beacon

Στην αρχή του πλαισίου (frame) υπάρχει ένα πλαίσιο διαχείρισης (management frame) που ονομάζεται beacon και αυτό χρησιμοποιείται ώστε ο κεντρικός σταθμός βάσης να στέλνει στους κόμβους δεδομένα που είναι οι εντολές διαχείρισης και αφορούν ολόκληρο το πλαίσιο (frame). Ο κάθε κόμβος ακολουθεί τις εντολές που λαμβάνει από τον σταθμό βάσης.

2.4.1.4 Είδη χρονικών σχισμών time slots

Συχνά, οι σχισμές χρόνου (slots) που υπάρχουν σε ένα πλαίσιο (frame) χωρίζονται σε κατηγορίες ανάλογα με τη χρήση τους. Έτσι διακρίνονται σε σχισμές:

- α) downlink slots,
- β) uplink slots,
- γ) σχισμές υπηρεσιών (service slots),
- δ) σχισμές αχρησιμοποίητες (unused slots).

Αυτά τα είδη των χρονικών σχισμών (time slots) εξηγούνται στη συνέχεια:

α) Στις σχισμές downlink slots μεταδίδονται δεδομένα από τον κεντρικό σταθμό βάσης προς τους κόμβους.

β) Στις σχισμές uplink slots μεταδίδονται δεδομένα από έναν κόμβο προς τον κεντρικό σταθμό βάσης.

γ) Επιπλέον, μπορεί να υπάρχουν οι χρονικές σχισμές υπηρεσιών service slots. Μία χρονική σχισμή υπηρεσίας (service slot) χρησιμοποιείται όταν ένας κόμβος στέλνει ένα μήνυμα αίτησης για σύνδεση (connection request message). Τότε η σχισμή υπηρεσίας (service slot) επιτρέπει να κάνει ο κόμβος την αίτηση του και να γίνει κατανομή μίας σύνδεσης σε αυτόν τον κόμβο.

Σε κάποια πρότυπα δεν χρησιμοποιείται μία μόνο συχνότητα, αλλά ενδέχεται να χρησιμοποιούνται 3 διαφορετικές συχνότητες αντιστοίχως για τα 3 είδη σχισμών χρόνου που αναφέρθηκαν παραπάνω. Δηλαδή χρησιμοποιούν μία συχνότητα για πλαίσια (frames) που αποτελούνται από σχισμές χρόνου uplink slots, μια δεύτερη συχνότητα για πλαίσια που αποτελούνται από σχισμές χρόνου downlink slots και μία τρίτη συχνότητα για τις σχισμές υπηρεσιών (service slots).

δ) Επιπλέον, κάποιες χρονικές σχισμές ονομάζονται αχρησιμοποίητες (unused time slots) και υπάρχουν μόνο για να γίνεται καλύτερος συγχρονισμός των πλαισίων.

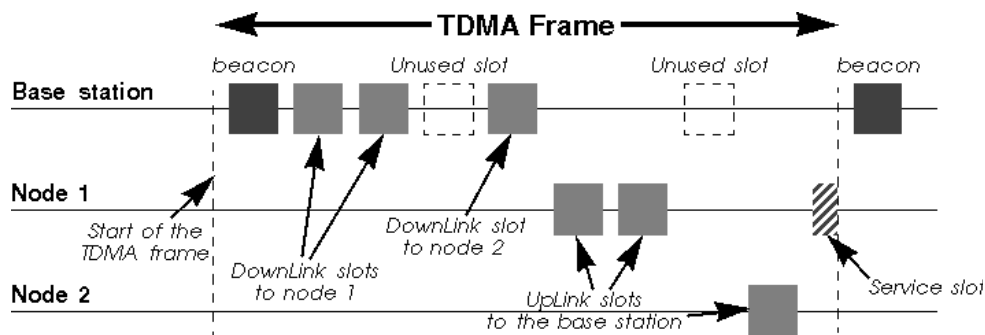
2.4.1.5 Απαιτήσεις για συγχρονισμό στο TDMA

Το TDMA μπορεί να θεωρηθεί ότι έχει ένα σταθερό σύνολο πόρων που μπορούν είτε να μειώσουν το χρόνο απόκρισης είτε να αυξήσουν το εύρος ζώνης bandwidth με βάση τη ρύθμιση των χρονικών σχισμών slots. Δηλαδή το μεγαλύτερο μέγεθος της χρονικής σχισμής slot σημαίνει ότι θα υπάρξει μεγαλύτερη καθυστέρηση latency. Υπάρχουν χρονικές σχισμές που κανένας κόμβος δεν μεταδίδει δεδομένα. Το πρωτόκολλο TDMA είναι σχεδιασμένο για κυκλοφορία δεδομένων καταιγισμού που διακόπτεται (non-continuous burst traffic) αλλά η απόδοση του δεν είναι καλή για μια κυκλοφορία που είναι συνεχής. Σε ένα σύστημα TDMA υπάρχουν απαιτήσεις αυστηρές να τηρείται ο συγχρονισμός για να μπορέσει να λειτουργήσει. Έτσι, χρειάζεται να υπάρχει υποχρεωτικά στο πακέτο δεδομένων ένα μεγάλο overhead με δεδομένα που αφορούν το συγχρονισμό. Οι κόμβοι δεν μπορούν επικοινωνήσουν με δεδομένα αν δεν έχουν συγχρονιστεί πλήρως μεταξύ τους.

2.4.1.6 Το TDMA χρησιμοποιείται στη μετάδοση δεδομένων από αισθητήρες.

Το TDMA είναι χρήσιμο για συστήματα που μετατρέπουν το αναλογικό σήμα σε ψηφιακό (A/D converters). Έτσι το TDMA είναι κατάλληλο στις περιπτώσεις όπου ένας αισθητήρας λαμβάνει αναλογικά δεδομένα μετρήσεων και τα μετατρέπει σε ψηφιακά δεδομένα για να δεχτούν επεξεργασία. Ακόμη, το TDMA είναι χρήσιμο για εξοικονόμηση της διάρκειας ζωής της μπαταρίας των συσκευών κόμβων αισθητήρων (sensor nodes), διότι αυτές οι συσκευές δεν μεταδίδουν

δεδομένα σε όλη τη χρονική περίοδο που λειτουργούν αλλά μόνο σε ορισμένες χρονικές σχισμές slots. Επομένως, μπορούν να μπαίνουν σε κατάσταση sleep κάποιες στιγμές. Επίσης, το γεγονός ότι οι πομποί εκπέμπουν δεδομένα σε διαφορετική χρονική σχισμή εξασφαλίζει ότι δεν θα εκπέμπουν ταυτόχρονα δύο πομποί και συνεπώς δεν θα προκαλέσουν παρεμβολές ο ένας στον άλλο.



Εικόνα 22 Οι σχισμές χρόνου (slots) σε ένα πλαίσιο (frame) TDMA. [16]

Στην παραπάνω εικόνα διακρίνονται τα είδη σχισμών χρόνου (slots) που αναφέρθηκαν παραπάνω: beacon, downlink slots, uplink slots, service slots, unused slots σε ένα γενικό μοντέλο TDMA.

2.4.1.7 Το TDMA χρησιμοποιήθηκε στην κινητή τηλεφωνία

Το TDMA χρησιμοποιήθηκε στα πρότυπα κινητής τηλεφωνίας όπως είναι για παράδειγμα το GSM στην Ευρώπη, το TDMA και το PCS στις ΗΠΑ, επίσης και στα πρότυπα ασύρματης τηλεφωνίας (cordless phone) όπως είναι το DECT στην Ευρώπη. Αυτό ισχύει διότι το TDMA είναι ένα πρότυπο που ταιριάζει σε εφαρμογές τηλεφωνίας επειδή έχει σταθερό ρυθμό bit (fixed bit rate). Σε κάθε μία τηλεφωνική συσκευή ανατίθεται μία σχισμή χρόνου downlink slot και μία σχισμή χρόνου uplink slot. Αυτές οι σχισμές χρόνου έχουν ένα σταθερό μέγεθος (fixed size) για το πλαίσιο που αντιστοιχεί στα δεδομένα φωνής. Το TDMA επιτυγχάνει μια χαμηλή καθυστέρηση (latency).

Το TDMA χρησιμοποιεί πακέτα σταθερού μεγέθους και συμμετρικές ζεύξεις (links). Επειδή σε εφαρμογές δικτύων υπολογιστών τα πακέτα IP μπορεί να είναι μεταβλητού μεγέθους, το TDMA δεν είναι και τόσο κατάλληλο για χρήση σε τέτοιες εφαρμογές.

Το TDMA είναι κατάλληλο για να χρησιμοποιείται σε μία αφιερωμένη ζώνη συχνοτήτων που δεν υπάρχουν πολλές παρεμβολές όπως είναι για παράδειγμα οι ζώνες συχνοτήτων της κινητής τηλεφωνίας. Σε αυτές θα λειτουργήσει σωστά και χωρίς προβλήματα.

Αν το TDMA χρησιμοποιηθεί σε ζώνες συχνοτήτων που υπάρχουν πολλές παρεμβολές και αυτό ισχύει συνήθως σε συχνότητες που δεν απαιτείται ειδική άδεια και έτσι εκπέμπουν πολλές πηγές, τότε το TDMA από μόνο του δεν μπορεί να προσαρμόζεται για να αντιμετωπίζει πολλές και τυχαίες ριπές δεδομένων καταιγισμού που έρχονται από πηγές παρεμβολών. Για αυτό χρειάζεται επιπλέον να χρησιμοποιηθεί ένας μηχανισμός που κάνει επαναλήψεις της προσπάθειας για να εκπέμπει ξανά τα σήματα σε επαναληπτικές μεταδόσεις.

2.4.2 Το TDMA στο δίκτυο WirelessHART

Τα δίκτυα WirelessHART υιοθέτησαν το TDMA [17].

Το WirelessHART διαιρεί το χρόνο σε υπερπλαίσια (superframes). Κάθε υπερπλαίσιο διαιρείται σε σχισμές χρόνου (time slots). Οι κόμβοι του δικτύου επικοινωνούν με τους άλλους κόμβους στη διάρκεια των χρονικών σχισμών. Συνεπώς υπάρχει μία ιεραρχία χρονισμού που αποτελείται από τρία επίπεδα ιεραρχικά [18].

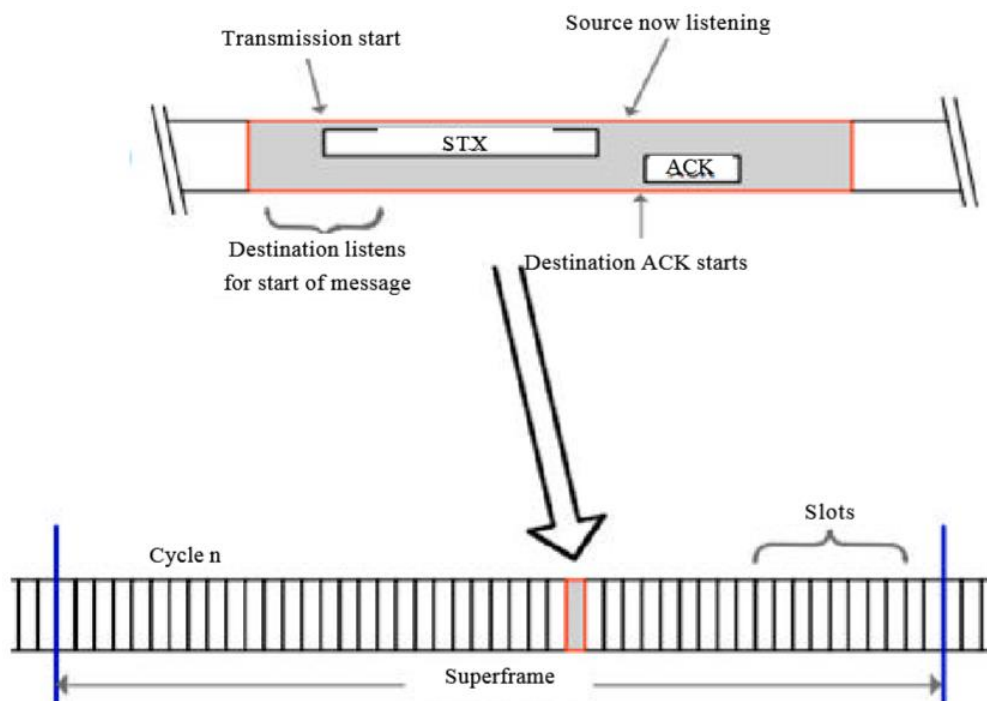
α) Το χαμηλότερο επίπεδο είναι οι μεμονωμένες σχισμές χρόνου (time slots).

β) Ένα σύνολο από συνεχόμενες σχισμές χρόνου που έχουν σταθερό μήκος, αποτελεί το υπερπλαίσιο (superframe).

γ) Ένα σύνολο από συνεχόμενα υπερπλαίσια (superframes) δημιουργεί έναν κύκλο δικτύου (network cycle).

Απαιτείται να υπάρχει συγχρονισμός στο δίκτυο ώστε η επικοινωνία να είναι ασφαλής, αξιόπιστη και χωρίς συγκρούσεις.

Στην παρακάτω εικόνα φαίνονται τα υπερπλαίσια (superframes) του μηχανισμού TDMA που χρησιμοποιείται στο WirelessHART.



Εικόνα 23 Πάνω: Σχισμή χρόνου (time slot) σε μεγέθυνση. Κάτω: υπερπλαίσιο (superframe) TDMA στο δίκτυο WirelessHART που περιλαμβάνει πολλές διαδοχικές σχισμές χρόνου (time slots). Πηγή: [18]

Στα δίκτυα WirelessHART, κάθε σχισμή χρόνου (time slot) έχει σταθερό μήκος 10 ms. Μέσα σε ένα υπερπλαίσιο (superframe), οι σχισμές χρόνου (time slots) κατανέμονται (allocated) σε κόμβους. Οι κόμβοι είτε στέλνουν προς άλλους κόμβους είτε λαμβάνουν, πακέτα δεδομένων, χρησιμοποιώντας αυτές τις σχισμές χρόνου. Μέσα σε κάθε κύκλο (cycle) ο κάθε κόμβος λαμβάνει τουλάχιστον μία σχισμή χρόνου (time slot) για τη μετάδοση δεδομένων (data transmission), αλλά μπορεί να υπάρξουν μερικοί κόμβοι που λαμβάνουν περισσότερες σχισμές χρόνου (time slots) ενώ κάποιοι άλλοι κόμβοι λαμβάνουν λιγότερες. Αυτό μπορεί να συμβεί διότι ορισμένοι κόμβοι έχουν να στείλουν περισσότερα δεδομένα ή έχουν και καθήκοντα προώθησης δεδομένων από άλλους κόμβους και για αυτό χρειάζονται περισσότερες σχισμές χρόνου. Ο διαχειριστής δικτύου (network manager) ή (NM) στέλνει ένα χρονικό πρόγραμμα (schedule) σε κάθε κόμβο και πληροφορεί τον κόμβο σε ποιες χρονικές σχισμές πρέπει ο κόμβος να εκπέμψει δεδομένα (transmits) και σε ποιες χρονικές σχισμές (slots) πρέπει να λάβει δεδομένα. Επιπλέον ο κόμβος πρέπει να διατηρεί το συγχρονισμό του με το δίκτυο ώστε να ξεχωρίζει ποια είναι τα όρια των χρονικών σχισμών και να μην υπάρχουν διενέξεις με γειτονικούς κόμβους.

2.4.2.1 Ρολόι Ακριβείας

Για να υπάρχει μία αξιοπιστία στη λειτουργία του μηχανισμού TDMA, κάθε κόμβος στο δίκτυο διαθέτει ένα ρολόι ακριβείας (precise clock) και έναν μετρητή σχισμών χρόνου (slot timer).

Στα δίκτυα WirelessHART, επιλέγονται οι κεντρικοί κόμβοι που είναι τα σημεία πρόσβασης (access points) AP ως βασικοί κόμβοι πηγής χρόνου (primary time source nodes). [18].

Οι υπόλοιποι κόμβοι συγχρονίζουν το ρολόι τους σύμφωνα με έναν κόμβο AP ή σύμφωνα με άλλους κόμβους πηγής (source nodes) που ορίζει ο διαχειριστής δικτύου (network manager). Έτσι προκύπτει ένα ομοιόμορφο ρολόι του δικτύου (uniform network clock) [18].

2.4.3 Ο Συγχρονισμός σε διαφορετικά συστήματα από το WirelessHART

Σε αυτή την παράγραφο, γίνεται μία σύντομη αναφορά μεθόδων συγχρονισμού από κάποια άλλα συστήματα που διαφέρουν από το σύστημα συγχρονισμού του δικτύου WirelessHART.

Υπάρχουν δύο παραδοσιακές μέθοδοι για συγχρονισμό που χρησιμοποιούνται ευρέως σε διαφορετικά συστήματα, αλλά τα χαρακτηριστικά τους δεν επιτρέπουν να χρησιμοποιηθούν στα ασύρματα δίκτυα αισθητήρων.

Σε κάποια συστήματα, οι μηχανισμοί για συγχρονισμό (time-sync) που έχουν διαδοθεί ευρέως και χρησιμοποιούνται, είναι το GPS (Global Positioning System) Παγκόσμιο σύστημα εντοπισμού θέσης και το πρωτόκολλο NTP (Network Time Protocol) Πρωτόκολλο χρόνου δικτύου. Η μέθοδος συγχρονισμού στο σύστημα GPS είναι πολύ ακριβής αλλά και πολύ ακριβή. Βασικό μειονέκτημα της είναι το υψηλό κόστος και η μεγάλη κατανάλωση ενέργειας. [18]

Η ακρίβεια του GPS στο συγχρονισμό, μπορεί να μειωθεί όταν το περιβάλλον είναι «δύσκολο» για τα σήματα. Η ακρίβεια της μεθόδου συγχρονισμού NTP επιτυγχάνεται επειδή εκτελούνται πάρα πολλοί υπολογισμοί και έτσι το κόστος υπολογισμών (computing cost) είναι σημαντικό. Στις εφαρμογές ασύρματων δικτύων αισθητήρων όταν γίνεται μια υλοποίηση σε μεγάλη κλίμακα, χρησιμοποιούνται αισθητήρες που έχουν μικρό μέγεθος και χαμηλό κόστος. Για αυτό η κατανάλωση ισχύος πρέπει να είναι αυστηρά περιορισμένη. Οι κόμβοι αισθητήρες τοποθετούνται σε περιβάλλον «εχθρικό» για τα σήματα. Για αυτούς τους λόγους, οι παραπάνω δύο μέθοδοι δεν

είναι κατάλληλες για ασύρματα δίκτυα αισθητήρων. Υπάρχουν και άλλες μέθοδοι συγχρονισμού που αναφέρονται στο [18]. Αυτές οι μέθοδοι βασίζονται:

- α) σε συγχρονισμό δέκτη-δέκτη,
- β) σε συγχρονισμό πομπού-δέκτη,
- γ) σε συγχρονισμό ζεύγους (pair-wise).

Στο συγχρονισμό δέκτη-δέκτη χρησιμοποιείται ο αλγόριθμος RBS (Reference Broadcast Synchronization) Συγχρονισμός με αναφορά εκπομπής.

Στο συγχρονισμό πομπού-δέκτη χρησιμοποιούνται αλγόριθμοι όπως είναι οι DMTS (Delay Measurement Time Synchronization) Συγχρονισμός με μέτρηση του χρόνου καθυστέρησης και FTSP (Flooding Time Synchronization) Συγχρονισμός με πλημμύρα χρόνου.

Στο συγχρονισμό ζεύγους χρησιμοποιούνται αλγόριθμοι όπως ο TPSN (Timing Sync Protocol for Sensor Networks) και ο συγχρονισμός LTS (Lightweight Tree-based Synchronization) Συγχρονισμός με βάση τα δέντρα ελαχίστου βάρους.

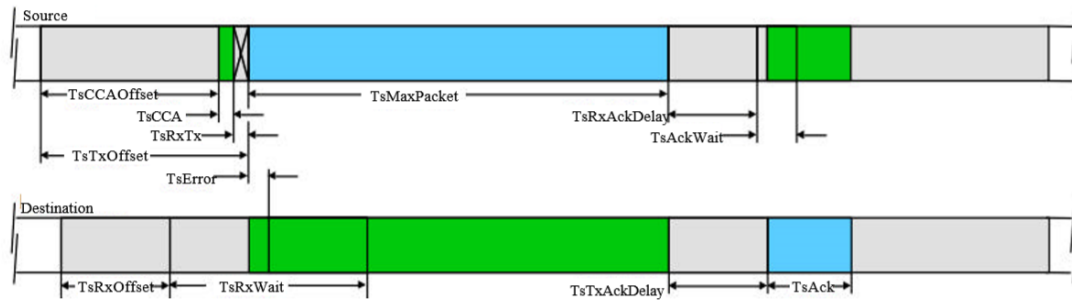
2.4.4. Ο συγχρονισμός στο δίκτυο WirelessHart

Στο WirelessHART η τεχνολογία του συγχρονισμού, αποτελεί τη βάση για τη θέση των κόμβων, το data fusion, την μέτρηση του συγχρονισμού και επίσης εγγυάται την σωστή λειτουργία και επικοινωνία του δικτύου.

Η μέθοδος συγχρονισμού του WirelessHART υιοθετεί έναν συνδυασμό της μεθόδου πομπού-δέκτη και της μεθόδου ζεύγους.

Για να ρυθμιστεί (set up) ο συγχρονισμός στο WirelessHART χρησιμοποιείται για τις σχισμές χρόνου (time slots) ένα μοντέλο ιδανικού χρόνου (ideal time) για την αποστολή δεδομένων και για τη λήψη δεδομένων. Όταν μεταφέρονται συνηθισμένα πακέτα δεδομένων στο δίκτυο, κάθε κόμβος στο δίκτυο συγχρονίζεται. Έτσι αποφεύγεται η αποστολή επιπλέον πακέτων που να είναι μόνο για συγχρονισμό και με αυτό τον τρόπο δεν αυξάνεται το φορτίο στο δίκτυο αλλά παραμένει μειωμένο. Παράλληλα, διατηρείται η ακρίβεια συγχρονισμού ανάμεσα σε διαφορετικούς κόμβους του δικτύου.

Ρύθμιση των σχισμών χρόνου (Time Slots).



Εικόνα 24 Οι σχισμές χρόνου (time slots) στο WirelessHART. [8]

Το μοντέλο των σχισμών χρόνου του WirelessHART φαίνεται στην παραπάνω εικόνα. Το μήκος κάθε χρονικής σχισμής (slot) είναι 10 ms.

2.4.4.1 Κόμβος αποστολέας.

Για την αποστολή δεδομένων, η τρέχουσα χρονική σχισμή (time slot) πρέπει να είναι σχισμή για αποστολή δεδομένων (data sending slot) από έναν κόμβο αποστολέα (sender). Αν είναι ενεργοποιημένη η λειτουργία CCA (Clear Channel Assessment) έλεγχος καθαρού καναλιού, τότε ο αποστολέας περιμένει για χρόνο $TsCCAOffset$ από την αρχή της χρονικής σχισμής (slot) και μετά εκτελεί μια ανίχνευση CCA. Αν το κανάλι είναι απασχολημένο (busy) ο αποστολέας (sender) παραιτείται από την προσπάθεια για αποστολή δεδομένων. Αν το κανάλι είναι ελεύθερο, τότε ο αποστολέας αλλάζει λειτουργία και μπαίνει στην λειτουργία αποστολής δεδομένων (data sending mode) και αυτό γίνεται για την χρονική περίοδο $TsRxTx$. Στη χρονική στιγμή $TsTxOffset$,

ο αποστολέας κόμβος (sender) στέλνει τα δεδομένα. Μόλις ολοκληρωθεί η διαδικασία αποστολής, ο αποστολέας κόμβος περιμένει για χρόνο $TsRxAckDelay$ και μετά αλλάζει τη λειτουργία του σε λειτουργία αναμονής για λήψη δεδομένων (data receiving mode) και περιμένει το σήμα επιβεβαίωσης ACK από τον δέκτη ώστε να επιβεβαιωθεί ότι έγινε η λήψη. Το σήμα ACK πρέπει να φτάσει, μέσα στο χρόνο $TsAckWait$. Αν φτάσει σωστά το σήμα ACK, τότε θεωρείται ότι όλη η επικοινωνία έγινε επιτυχώς. Αλλιώς, θεωρείται ότι υπήρξαν σφάλματα στην επικοινωνία.

2.4.4.2 Κόμβος δέκτης

Στην πλευρά του κόμβου δέκτη (receiver) η τρέχουσα σχισμή χρόνου (time slot) πρέπει να είναι σχισμή λήψης δεδομένων (data receiving slot) του κόμβου δέκτη. Από τη χρονική στιγμή του $TsRxOffset$ ο κόμβος δέκτης αλλάζει λειτουργία και μπαίνει σε λειτουργία λήψης (receiving mode). Αν δεν έρθουν καθόλου δεδομένα στη χρονική περίοδο $TsRxWait$, τότε δεν υπάρχουν δεδομένα για λήψη σε αυτή τη σχισμή χρόνου (time slot).

Αλλιώς, αν έρθουν δεδομένα και ληφθούν σωστά, μόλις τελειώσει η διαδικασία λήψης, ο κόμβος δέκτης περιμένει για χρόνο $TsTxAckDelay$ και ετοιμάζει το πακέτο δεδομένων επιβεβαίωσης ACK. Μόλις τελειώσει ο χρόνος $TsTxAckDelay$, το πακέτο δεδομένων επιβεβαίωσης ACK στέλνεται προς τον κόμβο αποστολέα (sender).

2.4.4.3 Ακολουθίες δεδομένων για σύνδεση νέου κόμβου στο δίκτυο

Το WirelessHART έχει αυστηρούς κανόνες για τις ακολουθίες δεδομένων (data sequences) που στέλνονται και λαμβάνονται.

Παράδειγμα σύνδεσης νέου κόμβου.

Έστω ότι έχουμε ένα υπαρκτό δίκτυο WirelessHART και έστω ότι ο κόμβος B είναι ένας νέος κόμβος που θέλει να συνδεθεί (join) σε αυτό το δίκτυο. Η σύνδεση θα γίνει μέσω ενός κόμβου A που είναι ήδη συνδεδεμένος στο δίκτυο.

Ο κόμβος B θα λάβει το σωστό χρόνο συγχρονισμού από τον κόμβο A που είναι συγχρονισμένος. Για να γίνει αυτή η επέκταση του δικτύου (extension), ο κόμβος A στέλνει πακέτα δεδομένων διαφήμισης (advertisement) σε περιοδικά χρονικά διαστήματα. Όταν ο κόμβος B ξεκινάει τη σύνδεση του (join), έχει ανοικτό τον δέκτη του (receiver) και ο κόμβος B βρίσκεται σε μία «ενεργή κατάσταση αναζήτησης» (active searching state) και ακούει (listen) για να ανιχνεύσει όλα τα πακέτα δεδομένων που έρχονται από το δίκτυο. Αν το πρώτο πακέτο που θα λάβει ο κόμβος B δεν είναι ένα πακέτο διαφήμισης (advertisement packet) τότε μόλις το λάβει ο κόμβος B θα καταγράψει (record) τον τοπικό χρόνο $RxLocal$ του τη στιγμή λήψης. Ο κόμβος B θα αλλάξει την κατάσταση του στην κατάσταση «το πακέτο λήφθηκε» (packet received).

Υπολογισμός σχισμών χρόνου (time slots).

Σύμφωνα με το ιδανικό μοντέλο για αποστολή και λήψη δεδομένων και με υπολογισμούς, ο κόμβος B θα αντιληφθεί ότι η αρχή της τρέχουσας χρονικής σχισμής (time slot) του δικτύου είναι $RxLocal - TsTxOffset - TsError$.

Επειδή η σχισμή χρόνου έχει διάρκεια 10ms, το τέλος της σχισμής χρόνου θα είναι

$RxLocal - TsTxOffset - TsError + 10ms$.

Όταν ο κόμβος B λάβει το πακέτο διαφήμισης (advertisement packet) αφαιρεί τον αριθμό ASN Absolute Slot Number (απόλυτο αριθμό σχισμής) του δικτύου.

Τότε ο κόμβος B αλλάζει τον τοπικό του αριθμό ASN (local ASN) και δημιουργεί (set up) τη δική του σχισμή χρόνου (time slot). Ο κόμβος B συγχρονίζεται με το δίκτυο και αλλάζει την κατάσταση του σε κατάσταση «συγχρονισμένος»

(synchronized state). Παρακάτω αναφέρονται δύο μέθοδοι συγχρονισμού, που είναι ο ενεργός συντονισμός και ο παθητικός συγχρονισμός

2.4.4.4 Ενεργός συγχρονισμός (Active time-sync)

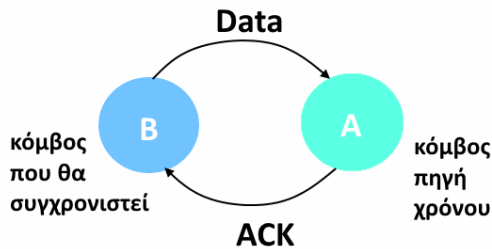
Κάθε ασύρματος κόμβος έχει ένα τοπικό ρολόι (local clock).

Χρησιμοποιούνται κρυσταλλικοί ταλαντωτές (crystal oscillators) για να οδηγούν (drive) το τοπικό ρολόι (local clock) των ασύρματων κόμβων (wireless nodes).

Υπάρχουν όμως αποκλίσεις στο χρόνο ρολογιού μεταξύ των διαφορετικών κρυσταλλικών ταλαντωτών. Αυτές οι αποκλίσεις ονομάζονται (clock drifting).

Έτσι πάντα υπάρχει ένα σφάλμα χρόνου ανάμεσα στους κόμβους το οποίο είναι επιθυμητό να διατηρείται σε χαμηλά επίπεδα. Για να παραμείνει το σφάλμα αυτό διαρκώς σε μικρό εύρος τιμών απόκλισης, είναι απαραίτητο να γίνεται ένας συγχρονισμός (time-sync). Στο δίκτυο WirelessHART ο διαχειριστής δικτύου (Network Manager) αναθέτει σε κάποιους κόμβους να είναι κόμβοι πηγής χρόνου (time source nodes). Σε άλλους κόμβους, αναθέτει να είναι συγχρονισμένοι με βάση τους κόμβους πηγής χρόνου (time source nodes).

Περιγράφεται και παραπάνω, ότι αν ένας κόμβος A είναι πηγή χρόνου (time source) για έναν άλλο κόμβο B, τότε ο κόμβος B πρέπει να συγχρονιστεί με βάση τον κόμβο A.



Εικόνα 25. Ενεργός συγχρονισμός.

Στην παραπάνω εικόνα, όταν ο κόμβος B χρησιμοποιεί την μέθοδο ενεργού συγχρονισμού (active time-sync), τότε ο κόμβος B στέλνει πακέτα δεδομένων στον κόμβο A, στην χρονική στιγμή του χρόνου μετατόπισης (Offset time) στο TxTsOffset από την αρχή της χρονικής σχισμής (time slot). Ο κόμβος A καταγράφει τον τοπικό χρόνο του (local time) RxLocal_A μόλις φτάσει το πακέτο δεδομένων από τον κόμβο B.

Τα δεδομένα payload για το σήμα ACK είναι η διαφορά χρόνου μεταξύ του κόμβου A (που είναι η πηγή χρόνου) και του κόμβου B (που συγχρονίζεται).

Αυτή η διαφορά χρόνου είναι:

$$T\_Adj = TsTxOffset + TsError - RxLocal\_A.$$

Όταν ο κόμβος B λαμβάνει το σήμα επιβεβαίωσης ACK, διαβάζει τις πληροφορίες και ρυθμίζει τον δικό του τοπικό χρόνο $T\_B = T\_B - T\_Adj$, ώστε να υλοποιηθεί ο συγχρονισμός ανάμεσα στον κόμβο B και στον κόμβο A.

2.4.4.5 Παθητικός συγχρονισμός (Passive time-sync)

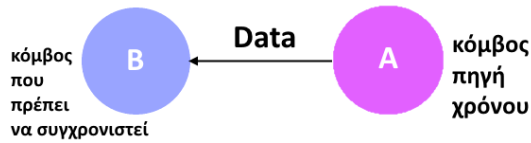
Όταν υιοθετείται η μέθοδος παθητικού συγχρονισμού, τότε ο κόμβος A που είναι η πηγή χρόνου (time source) στέλνει ένα πακέτο δεδομένων στον κόμβο B στη χρονική στιγμή TsTxOffset. Ο κόμβος B καταγράφει (records) τον τοπικό χρόνο του (local time) RxLocal_B μόλις φτάσει το πακέτο και μετά υπολογίζει το σφάλμα χρόνου (time error) ως προς την πηγή χρόνου (time source) που είναι ο κόμβος A.

$$T\_Adj = TsTxOffset + TsError - RxLocal\_B$$

Με βάση το χρόνο T_Adj, ο κόμβος B ρυθμίζει τον τοπικό χρόνο του σε

$$T\_B = T\_B + T\_Adj,$$

ώστε να γίνει συγχρονισμός του κόμβου B με τον κόμβο A.



Εικόνα 26. Παθητικός συγχρονισμός

2.4.4.6 Κύκλος Συγχρονισμού

Από το μηχανισμό συγχρονισμού που περιεγράφηκε παραπάνω, αν για μια χρονική περίοδο δεν υπάρχει καμία επικοινωνία ανάμεσα σε δύο κόμβους, τότε αυτοί δεν μπορούν να συγχρονιστούν μεταξύ τους.

Για να διατηρηθεί ο τοπικός χρόνος (local time) ώστε να είναι ο ίδιος με τον χρόνο δικτύου (network time), ένας κόμβος πρέπει να στέλνει κάποια πακέτα δεδομένων που λέγονται keep-alive (διατήρηση εν ζωή), στον κόμβο πηγής χρόνου με τον οποίο συνδέεται, αν δεν υπάρχει καμία άλλη επικοινωνία μεταξύ τους για μεγάλο χρονικό διάστημα.

Ορίζονται οι παρακάτω παράμετροι.

Έστω ότι ο κύκλος των πακέτων keep-alive είναι P.

Το ανώτερο όριο σφάλματος χρόνου ανάμεσα στους κόμβους είναι delt_T .

Το σφάλμα απόκλισης (drifting error) του κρυσταλλικού ταλαντωτή είναι delt σε ποσοστό ppm (parts per million). (π.χ. 5 ppm = $5/1000000 = 0.000005$)

Τότε προκύπτει η ανισότητα: $2 \times \text{delt} \times P \leq \text{delt\_T}$

Δηλαδή: $P \leq \text{delt\_T} / (2 \times \text{delt})$

Επιπλέον, αν υπάρχουν n άλματα hops στο δέντρο συγχρονισμού time-sync tree, ο κύκλος του πακέτου keep-alive είναι $P \leq \text{delt\_T} / ((2 \times \text{delt})(n+1))$

Από την επικοινωνία σε μία χρονική σχισμή (time slot) που αναφέρθηκε παραπάνω, αν οι κόμβοι του δικτύου στέλνουν και λαμβάνουν πακέτα δεδομένων επιτυχώς, τότε πρέπει να ικανοποιούνται οι κάτωθι ανισότητες:

$\text{delt\_T} + \text{TsRxOffset} \leq \text{TsTxOffset}$	(1)
$\text{delt\_T} + \text{TsTxOffset} + \text{TsError} \leq \text{TsTxOffset} + \text{TsRxWait}$	(2)

Στο WirelessHART ικανοποιούνται τα παρακάτω:

$2020 \mu\text{s} \leq \text{TsTxOffset} \leq 2220 \mu\text{s}$	(3)
$1020 \mu\text{s} \leq \text{TsTxOffset} \leq 1220 \mu\text{s}$	(4)
$2100 \mu\text{s} \leq \text{TsTxOffset} \leq 2300 \mu\text{s}$	(5)
$\text{TsError} = 192 \mu\text{s}$	(6)

Πίνακας 2.5 Ανισότητες που πρέπει να πληρούνται σε έναν κύκλο συγχρονισμού [8]

Κεφάλαιο 3

Δίκτυα για

Βιομηχανικές Εφαρμογές

Στο κεφάλαιο αυτό, παρουσιάζονται πρωτόκολλα δικτύων αισθητήρων που χρησιμοποιούνται σε βιομηχανικές εφαρμογές, με ιδιαίτερη εστίαση στο πρωτόκολλο WirelessHART. Στην αρχή, περιγράφεται το αρχικό ενσύρματο πρότυπο που υπήρξε πριν από το WirelessHART, δηλαδή το HART που έχει χρησιμοποιηθεί σε πολλές βιομηχανίες. Αναφέρονται γενικά στοιχεία για το HART, περιγράφεται η στοίβα στρωμάτων και τα διάφορα επίπεδα του πρωτοκόλλου. Παρουσιάζονται τα βασικά χαρακτηριστικά του HART και δίνεται περιγραφή λειτουργιών για τις συσκευές του δικτύου HART. Αναφέρονται επίσης τεχνικά στοιχεία για τα έξυπνα όργανα πεδίου HART και τα σήματα που μεταφέρονται στο δίκτυο HART, καθώς και άλλες πληροφορίες.

Στη συνέχεια, περιγράφεται λεπτομερώς το πρότυπο WirelessHART που είναι η εξέλιξη του HART. Αρχικά, γίνεται μία εστίαση στα χαρακτηριστικά του WirelessHART που ακολουθείται από μία συνοπτική περιγραφή για τα είδη συσκευών που χρησιμοποιούνται σε αυτό το πρότυπο, ώστε να υπάρξει μια γενική κατανόηση της λειτουργίας τους. Αμέσως μετά, ακολουθεί μία αναλυτική περιγραφή για όλες τις κατηγορίες συσκευών που χρησιμοποιούνται στο WirelessHART και παρουσιάζονται πιο αναλυτικά στοιχεία για αυτές. Επίσης παρουσιάζονται και εξηγούνται αναλυτικά τα πακέτα δεδομένων που αντιστοιχούν σε διαφορετικά στρώματα του πρωτοκόλλου.

Ακολούθως, παρουσιάζεται το πρότυπο GinMAC που είναι ένα άλλο πρότυπο για ασύρματα δίκτυα αισθητήρων. Περιγράφονται τα χαρακτηριστικά του, η δομή του και άλλα θέματα.

Το κεφάλαιο 3, κλείνει με παρουσίαση του προτύπου ISA 100A που είναι πρότυπο για ασύρματα δίκτυα αισθητήρων διαφορετικής τεχνολογίας από το WirelessHART, το οποίο χρησιμοποιήθηκε κυρίως στην Αμερική και υπήρξε ένας ανταγωνισμός του ISA 100A με το WirelessHART ως προς το ποιο από τα δύο πρότυπα θα έπρεπε να επικρατήσει στην αγορά. Έτσι, κάποιες βιομηχανίες

επέλεξαν το ISA 100A ενώ άλλες επέλεξαν το WirelessHART. Η εργασία αυτή δίνει έμφαση κυρίως στην περιγραφή του WirelessHART και όχι τόσο σε άλλα πρωτόκολλα.

3.1 Το πρωτόκολλο HART

Στις βιομηχανικές εφαρμογές χρησιμοποιούνται όργανα μέτρησης, αισθητήρες (sensors) και επενεργητές (actuators). Τα παλαιότερα όργανα μέτρησης (που ξεκίνησαν σε μία εποχή πριν από το 1988), ήταν τα συμβατικά αναλογικά όργανα (conventional analog instruments). Αυτά χρησιμοποιούσαν μόνο ένα συνεχές αναλογικό σήμα ρεύματος 4-20 mA για να στέλνουν την τιμή μέτρησης τους. Σε αυτά τα όργανα η διαδικασία μέτρησης (measurement process) ξεκινά με μία τεχνολογία που μετατρέπει μία φυσική ποσότητα σε ένα ηλεκτρικό σήμα 4-20 mA. Υπήρχε στο όργανο ο «συμβατικός πομπός» (conventional transmitter) που μετέδιδε το αναλογικό σήμα μέσω δύο συρμάτων. Αυτός ο πομπός δεν είχε αμφίδρομη επικοινωνία, αλλά μόνο προς μία κατεύθυνση.

Αργότερα, αναπτύχθηκαν τα «έξυπνα» ψηφιακά όργανα (smart digital instruments). Τα πρωτόκολλα έξυπνων οργάνων σχεδιάστηκαν για εφαρμογές όπου τα δεδομένα από τα όργανα μέτρησης συλλέγονται και συγκεντρώνονται με τεχνικές ψηφιακών επικοινωνιών. Τα πρότυπα αυτά συνδέουν μεταξύ τους διάφορες συσκευές αυτοματισμού που συχνά είναι από διαφορετικούς κατασκευαστές. Ο όρος smart σημαίνει ότι το όργανο διαθέτει μικροεπεξεργαστή και μπορεί να παρέχει περισσότερες λειτουργίες και δυνατότητες. Τα τμήματα αυτά συνδέονται απ' ευθείας σε PLC Προγραμματιζόμενους Λογικούς Ελεγκτές ή/και σε υπολογιστές. Επίσης οι ομάδες συσκευών χωρίζονται σε ιεραρχικά επίπεδα.

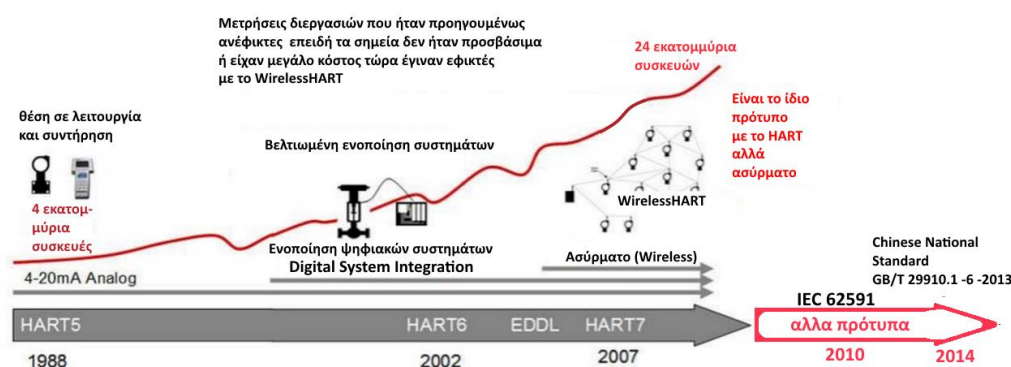
Αρχικά τα πρωτόκολλα αυτά βασίστηκαν σε συνδεσμολογία 2 καλωδίων που ονομάζεται δίαυλος (bus) για την μεταφορά δεδομένων μεταξύ των συσκευών και αργότερα προχώρησε η ασύρματη τεχνολογία στα 2.4 GHz. Τα ενσύρματα συστήματα είναι το HART και η οικογένεια προτύπων digital Fieldbuses καθώς και άλλα πρότυπα ιδιωτικά (proprietary) και εξειδικευμένα ανάλογα με την εφαρμογή. Το πρωτόκολλο HART χρησιμοποιήθηκε με επιτυχία σε πολλές εφαρμογές και σε εγκαταστάσεις που υπήρχαν εμπόδια και δύσκολα περιβάλλοντα.

Όμως τα ενσύρματα συστήματα είχαν το μειονέκτημα ότι υπήρχε αυξημένη πολυπλοκότητα, λόγω της αύξησης καλωδίων, αλλά και της δύσκολης πρόσβασης σε σημεία της εγκατάστασης που δεν μπορούσαν να τοποθετηθούν καλώδια.

3.1.1 HART γενικά στοιχεία

Σε αυτή την ενότητα αναφέρονται διάφορα στοιχεία για το πρωτόκολλο HART. Περισσότερα στοιχεία υπάρχουν στις πηγές [19], [3].

Το ενσύρματο πρωτόκολλο HART (Highway Addressable Remote Transducer) (Λεωφόρος διευθυνσιοδοτημένων απομακρυσμένων αισθητήρων) [19] δημιουργήθηκε από την Rosemount το 1986. Το HART ξεκίνησε αρχικά ως ιδιωτικό πρωτόκολλο (proprietary protocol). Σύντομα όμως η χρήση του έγινε ελεύθερη. Το 1990 δημιουργήθηκε το HART User Group και το 1993 συνεχίστηκε η εξέλιξη του HART από το ίδρυμα HART Communication Foundation (HCF). Με την έκδοση 7 το Σεπτέμβριο 2007, προστέθηκε η ασύρματη διεπαφή του HART και το ασύρματο πρότυπο ονομάστηκε WirelessHART.



Εικόνα 27. Η εξέλιξη από το πρωτόκολλο HART στο πρωτόκολλο WirelessHART

Το FieldComm Group δημιουργήθηκε στις 1 Ιανουαρίου, 2015 ως μία ενοποίηση του Fieldbus Foundation και του Hart Communication Foundation.



Εικόνα 28 Το FieldComm group έχει ως στόχο την ενοποίηση διαφορετικών τεχνολογιών έξυπνων συσκευών στους βιομηχανικούς αυτοματισμούς.

Το HART βασίστηκε στο πρότυπο Bell 202 και στη διαμόρφωση FSK (Frequency Shift Keying), στην οποία τα δυαδικά ψηφία 1 και 0 αναπαρίστανται από δύο ημιτονοειδή κύματα με διαφορετικές συχνότητες. Η διαδικασία αυτή εξηγείται πιο αναλυτικά στην επόμενη παράγραφο που αναφέρονται τα στρώματα (layers) του προτύπου HART και αφορά το φυσικό στρώμα (PHY layer).

Παρακάτω αναφέρονται μερικά πλεονεκτήματα του HART.

Το HART είναι ένα ανοικτό πρότυπο που μπορούν να το χρησιμοποιούν διαφορετικοί κατασκευαστές. Έτσι εξασφαλίζεται ότι οι πελάτες δεν εξαρτώνται από έναν μόνο προμηθευτή. Δεν είναι το μοναδικό πρότυπο που αναπτύχθηκε. Υπάρχουν παρόμοια πρωτόκολλα με το HART, όπως είναι η οικογένεια προτύπων Fieldbus. Επίσης υλοποιήθηκαν και αρκετά άλλα ανταγωνιστικά πρωτόκολλα με το HART όπως αυτά που χρησιμοποίησε η Honeywell, ή άλλες εταιρίες. Παρόλα αυτά, το HART επικράτησε στη βιομηχανία και πολλοί διαφορετικοί κατασκευαστές το υιοθέτησαν ως ένα κοινό πρότυπο για ενσύρματη σύνδεση των συσκευών. Αρκετοί λόγοι οδήγησαν στην υιοθέτηση του HART και στην προτίμηση του σε σχέση με άλλα πρότυπα. Μερικοί λόγοι από αυτούς ήταν:

- α) Επιλέχθηκε το HART διότι στο digital fieldbus δεν αναπτύχθηκε ένα μοναδικό πρότυπο, αλλά μια οικογένεια προτύπων, έτσι το HART ήταν μία κοινή λύση για διαφορετικά συστήματα.
- β) Από τη φύση του το HART είναι απλό και ισχυρό πρότυπο. [20] Η ενοποίηση των αναλογικών με τα ψηφιακά σήματα έφερε μία ευελιξία που δεν την είχαν άλλα πρωτόκολλα.
- γ) Το HART απαιτούσε λίγη εκπαίδευση για τους τεχνικούς, ενώ τα πρότυπα digital fieldbuses απαιτούσαν μεγάλη εκπαίδευση και είχαν πολυπλοκότητα.

δ) Οι digital fieldbuses κατανάλωναν περισσότερη ενέργεια. Επίσης οι fieldbuses είχαν μεγαλύτερο κόστος για εγκατάσταση και ειδικότερα το κόστος αντικατάστασης για ήδη υπαρχών εξοπλισμό ήταν πολύ ακριβό.

ε) Οι παλαιότερες συσκευές χρησιμοποιούσαν 2 καλώδια για τη σύνδεση τους με αναλογικό σήμα 4-20 mA και αργότερα τα ίδια καλώδια μπορούσαν να χρησιμοποιηθούν και στο πρωτόκολλο HART, ώστε δεν χρειαζόταν αλλαγές σε καλωδιώσεις. Αντίθετα, στο Fieldbus δεν ήταν διαθέσιμα πολλά από τα υπάρχοντα όργανα μέτρησης και χρειαζόταν αντικατάσταση.

στ) Οι εντολές του HART μπορούν να μετατραπούν σε εντολές άλλων πρωτοκόλλων με κατάλληλους μετατροπείς και να γίνει ένας συνδυασμός συσκευών με διαφορετικά πρωτόκολλα σε ένα δίκτυο.

ζ) Μια καλή λύση για το τεχνικό προσωπικό συντηρήσεων είναι οι συσκευές χειρός (handheld Communicators) που μπορούν να συνδέονται στο δίκτυο για ρυθμίσεις συσκευών, βαθμονομήσεις, θέση σε λειτουργία των συσκευών και περιοδική συντήρηση.

Επιπλέον θετικά χαρακτηριστικά του HART είναι η ακρίβεια και η σταθερότητα, η αξιοπιστία, η δυνατότητα χρήσης πολλών μεταβλητών, οι υπολογισμοί και οι διαγνώσεις, οι πολλαπλοί αισθητήρες στο δίκτυο, η ευκολία στην εγκατάσταση, η χρήση του αναγνωριστικού TagID, οι απομακρυσμένες ρυθμίσεις, οι πρόσβαση σε δεδομένα με το ιστορικό των συσκευών και άλλα.

3.1.2 Τα επίπεδα του μοντέλου OSI και η σύγκριση τους με το HART

Όπως είδαμε, το γενικό μοντέλο OSI-7 περιλαμβάνει 7 επίπεδα ή στρώματα (layers).

Στον παρακάτω πίνακα φαίνονται τα 7 επίπεδα του μοντέλου OSI και τα αντίστοιχα επίπεδα του πρωτοκόλλου HART.

Έγιναν διάφορες αναθεωρήσεις στο πρωτόκολλο HART. Η χρονική στιγμή που αναφέρεται αυτή η εργασία, είναι όταν το πρωτόκολλο βρίσκεται στην έκδοση 7.3. Ίσως υπάρξουν διαφορές σε μελλοντικές εκδόσεις.

	Στρώματα Μοντέλου OSI	Στρώματα HART
7	Στρώμα Εφαρμογών (Application Layer)	Εντολές (Commands) του HART

6	Στρώμα παρουσίασης (Presentation Layer)	
5	Στρώμα Συνόδου (Session Layer)	
4	Στρώμα Μεταφοράς (Transport Layer)	Στρώμα Μεταφοράς
3	Στρώμα Δικτύου (Network)	Στρώμα δικτύου
2	Στρώμα ζεύξης δεδομένων (Data Link Layer)(DLL)	HART protocol Message Structure (Δομή μηνυμάτων πρωτοκόλλου)
1	Φυσικό Στρώμα (PHY Layer)	Bell 202

Πίνακας 3.1. Σύγκριση των στρωμάτων του μοντέλου OSI 7 με τα στρώματα του HART

Το HART έχει 5 επίπεδα στην έκδοση 7.3. Σε παλαιότερες εκδόσεις του HART υπάρχουν διαφορές.

Το HART ακολουθεί το μοντέλο OSI αλλά έχει μόνο τα επίπεδα 1,2,3,4 και 7. Δηλαδή το φυσικό στρώμα, το στρώμα ζεύξης δεδομένων, το στρώμα δικτύου, το στρώμα μεταφοράς και το στρώμα εφαρμογών.

3.1.2.1 Στρώμα εφαρμογών (application layer)

Ορίζει τις εντολές (commands), τις αποκρίσεις (responses), τους τύπους δεδομένων (data types) και την κατάσταση (status).

Στο HART το επίπεδο εφαρμογών (application layer) αποτελείται από 3 είδη εντολών ή μηνυμάτων:

α) γενικές εντολές (universal commands) που πρέπει να εφαρμόζονται από όλες τις συσκευές πεδίου HART.

Μερικά παραδείγματα γενικών εντολών:

- Ανάγνωση (read) του κατασκευαστή της συσκευής και του τύπου συσκευής.
- Ανάγνωση (read) αναγνωριστικού συσκευής, Model ID
- Ανάγνωση (read) αναγνωριστικού συσκευής, Tag ID

- Ανάγνωση (read) της κύριας μεταβλητής (primary variable) (PV) και των μονάδων μέτρησης (units).
- Ανάγνωση (read) του ρεύματος εξόδου (current output) και του ποσοστού του εύρους τιμών (range).
- Ανάγνωση (read) ημερομηνίας (date)
- Ανάγνωση (read) προκαθορισμένων δυναμικών μεταβλητών (dynamic variables), μέχρι 4 μεταβλητές.
- Εγγραφή (write) ή ανάγνωση (read) μίας ετικέτας tag των 8 χαρακτήρων.
- Εγγραφή (write) ή ανάγνωση (read) μίας μεταβλητής descriptor των 16 χαρακτήρων.
- Εγγραφή (write) ή ανάγνωση (read) ενός μηνύματος (message) των 32 χαρακτήρων.
- Ανάγνωση (read) από τη συσκευή του εύρους τιμών της (range)
- Ανάγνωση (read) από τη συσκευή των μονάδων μέτρησης (units).
- Ανάγνωση (read) από τη συσκευή της σταθεράς χρόνου απόσβεσης (damping time). Αυτός είναι χρόνος καθυστέρησης που μεσολαβεί από την στιγμή που φτάνει ένα αρχικό σήμα εισόδου στο όργανο μέχρι να γίνουν αποσβέσεις, να σταθεροποιηθεί το σήμα και να ληφθεί μία σωστή τιμή ένδειξης για το σήμα εισόδου.
- Εγγραφή (write) ή ανάγνωση (read) του τελικού αριθμού συναρμολόγησης (final assembly number) που είναι το τελευταίο βήμα στη συναρμολόγηση.
- Εγγραφή (write) της διεύθυνσης polling address.

Οι γενικές εντολές επιτρέπουν στους κύριους σταθμούς να έχουν πρόσβαση στις παραμέτρους των συσκευών πεδίου. Στο δίκτυο HART επικοινωνούν μεταξύ τους συσκευές από διαφορετικούς κατασκευαστές.

β) Συνήθεις εντολές (common practice commands) που εφαρμόζονται στις περισσότερες συσκευές πεδίου, αλλά όχι σε όλες.

Μερικά παραδείγματα:

- Ανάγνωση (read) μέχρι 5 επιλεγμένων δυναμικών μεταβλητών (dynamic variables).

- Εγγραφή (write) της σταθεράς χρόνου απόσβεσης (damping time). Είναι σταθερός χρόνος καθυστέρησης, που μεσολαβεί από την στιγμή που φτάνει ένα αρχικό αναλογικό σήμα εισόδου στο όργανο μέχρι να γίνουν αποσβέσεις, να σταθεροποιηθεί το σήμα, να γίνει μετατροπή από αναλογικό σε ψηφιακό και να ληφθεί μία σωστή ψηφιακή τιμή ένδειξης για το σήμα εισόδου.
- Εγγραφή του εύρους τιμών της συσκευής (range values)
- Βαθμονόμηση (calibration) zero και span: Ρύθμιση του 0 (set zero) και ρύθμιση του διαστήματος βαθμονόμησης (set span).

Αυτή η εντολή πρέπει να εφαρμόζεται μόνο στα αναλογικά όργανα 4-20 mA για τα οποία αρκεί να ρυθμιστεί η τιμή του 0 (zero value) και το διάστημα βαθμονόμησης (span value) όταν η σχέση εισόδου/εξόδου είναι γραμμική, συνεπώς, γνωρίζοντας την είσοδο στο όργανο υπολογίζεται η αναμενόμενη έξοδος. Η ίδια ρύθμιση γίνεται και χειροκίνητα, πατώντας 2 αντίστοιχα κουμπιά (0 και span). Αν η σχέση εισόδου/εξόδου δεν είναι γραμμική πρέπει να είναι γνωστή η είσοδος και η συνάρτηση μεταφοράς για να υπολογιστεί η αναμενόμενη έξοδος. Γνωρίζοντας την αναμενόμενη έξοδο, μπορούν με ελέγχους να βρεθούν σφάλματα στην απόδοση του οργάνου. Η ρύθμιση αυτή πρέπει να αποφεύγεται για τις συσκευές HART που έχουν ψηφιακές τιμές διότι δεν είναι επαρκής λύση.

- Ρύθμιση (set) σταθερού ρεύματος εξόδου (output current)

Αυτή είναι μία εντολή (command) που θέτει το όργανο σε λειτουργία σταθερού ρεύματος εξόδου, που είναι μία λειτουργία ελέγχου. Αυτή η λειτουργία διαγράφει την πραγματική τιμή ρεύματος εξόδου και την αντικαθιστά με μία συγκεκριμένη σταθερή τιμή ρεύματος εξόδου, για να γίνουν διάφορα τεστ στο όργανο.

- Εκκίνηση αυτοελέγχου (self-tests).
- Ρύθμιση (trim) του 0 (zero) στην κύρια μεταβλητή PV

Αυτή η εντολή χρησιμοποιείται όταν έχει γίνει μετατόπιση της θέσης του 0 στο όργανο για να διορθώσει το σφάλμα μετατόπισης.

- Εγγραφή (write) της μονάδας unit της κύριας μεταβλητής PV.
- Ρύθμιση (trim) του 0 (zero) στο DAC και του κέρδους (gain)

Το DAC είναι σύστημα Συλλογής Δεδομένων και Ελέγχου DAC (Data Acquisition & Control) (λέγεται και SCADA Supervisory Control and Data Acquisition. Βρίσκεται μέσα σε μία εγκατάσταση).

- Εγγραφή (write) της συνάρτησης μεταφοράς (transfer function).
- Εγγραφή (write) του σειριακού αριθμού (serial number) του αισθητήρα
- Εγγραφή (write) ή ανάγνωση (read) των αναθέσεων (assignments) σε δυναμικές μεταβλητές (dynamic variables).

γ) Ειδικές εντολές (Device Specific Commands) μοναδικές σε επιμέρους συσκευές πεδίου.

Παραδείγματα εντολών:

- Εγγραφή (write) ή ανάγνωση (read) αποκοπής χαμηλής ροής (low flow cut off)
- Εκκίνηση (start) και σταμάτημα (stop) ή σβήσιμο τιμής (clear) του οργάνου totalizer.
- Εγγραφή (write) ή ανάγνωση (read) του συντελεστή βαθμονόμησης πυκνότητας (density calibration factor).
- Επιλογή της κύριας μεταβλητής (Primary Variable) PV: μάζα (mass) ροή (flow) ή πυκνότητα (density).
- Εγγραφή (write) ή ανάγνωση (read) υλικών (materials) ή πληροφοριών κατασκευής (construction information).
- Ρύθμιση (trim) της βαθμονόμησης (calibration) του αισθητήρα (sensor).
- Ενεργοποίηση (enable) του ελεγκτή PID.
- Χαρακτηρισμός της βαλβίδας (valve).
- Σημείο ρύθμισης (setpoint) της βαλβίδας (valve).
- Όρια κίνησης (travel limits).
- Μονάδες χρήστη (user units).
- Εμφάνιση πληροφοριών στην τοπική οθόνη (local display).

3.1.2.2 Στρώμα δικτύου (Network layer)

Είναι το 3ο επίπεδο στο μοντέλο OSI. Παρέχει δρομολόγηση (routing), ασφάλεια από σημείο σε σημείο, και υπηρεσίες μεταφοράς (transport services). Διαχειρίζεται τις συνόδους επικοινωνίας ("sessions") με αντίστοιχες συσκευές.

3.1.2.3 Στρώμα μεταφοράς (Transport layer)

Είναι το 2ο επίπεδο στο μοντέλο OSI.

Το επίπεδο μεταφοράς στο HART χρησιμοποιείται για να υπάρχει επιτυχής επικοινωνία από άκρο σε άκρο (end-end).

3.1.2.4 Στρώμα ζεύξης δεδομένων (data link layer)

Στο HART το στρώμα ζεύξης δεδομένων (data link layer) είναι το 2ο επίπεδο στο μοντέλο OSI. Ορίζει ένα πρωτόκολλο Κύριου / Εξαρτώμενου Σταθμού (master/slave). Αυτό το στρώμα ασχολείται με αξιόπιστη και ασύγχρονη μετάδοση των bytes (που είναι δεδομένα 8 bits). Τα δεδομένα είναι οργανωμένα σε πλαίσια και ακολουθούν τη μέθοδο κύριου-εξαρτώμενου σταθμού. Στην κανονική λειτουργία η συσκευή πεδίου στέλνει απόκριση μόνο όταν της ζητήσει ο κύριος σταθμός. Μπορεί να υπάρχουν δύο κύριοι σταθμοί. Για παράδειγμα πρωτεύων κύριος σταθμός (primary master) να είναι ένα σύστημα ελέγχου σε μία κεντρική αίθουσα ελέγχου και ένας υπολογιστής χειρός ή συσκευή χειρός στον τόπου που βρίσκεται η βιομηχανική εγκατάσταση, να είναι ο δευτερεύων κύριος σταθμός (secondary master). Μία συσκευή πεδίου μπορεί να δέχεται εντολές και από τον πρωτεύοντα και από τον δευτερεύοντα κύριο σταθμό. Η πρόσβαση στο δίκτυο ρυθμίζεται με κανόνες χρονισμού διαύλου και κανόνες διαιτησίας που ορίζουν πότε ο κάθε κύριος σταθμός μπορεί να ξεκινήσει μια συναλλαγή επικοινωνίας (communication transaction). Σε ένα ζεύγος καλωδίων σε συνδεσμολογία πολλαπλών σημείων μπορούν να συνδεθούν 15 εξαρτημένες συσκευές ή παραπάνω.

3.1.2.5 Στρώμα Φυσικό (PHY layer)

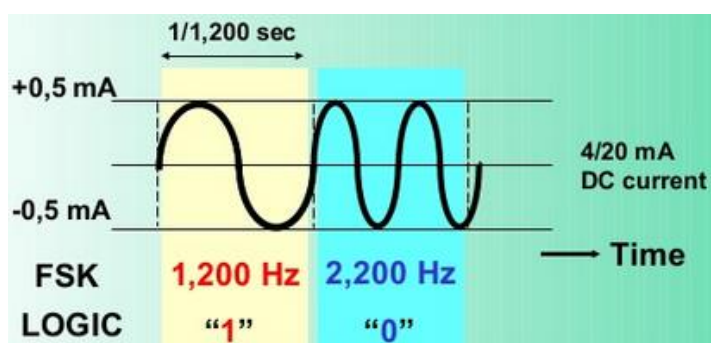
Στο HART το φυσικό στρώμα (PHY layer) είναι το επίπεδο 1 στο μοντέλο OSI.

Χρησιμοποιεί το πρότυπο Bell 202 με κωδικοποίηση FSK.

Το HART λειτουργεί με ένα συνδυασμό αναλογικής-ψηφιακής διαμόρφωσης και λέγεται υβριδικό πρότυπο, επειδή ταυτόχρονα εκπέμπει ένα σήμα σε ένα αναλογικό κανάλι και ένα σήμα σε ένα ψηφιακό κανάλι.

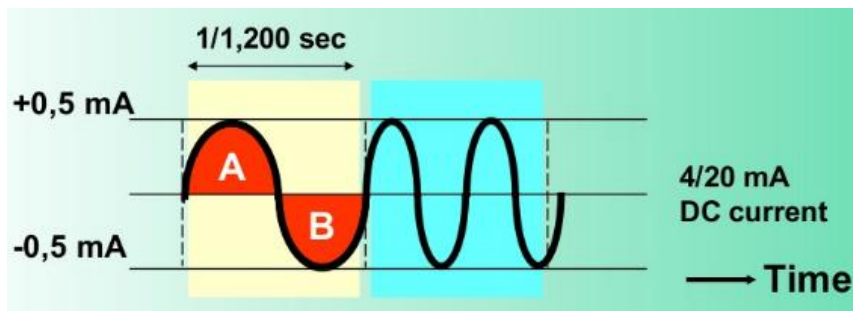
Δηλαδή σε ένα βρόχο ελέγχου 4-20mA που είναι το αναλογικό σήμα, γίνεται υπέρθεση ενός ψηφιακού σήματος FSK. [20]. Το σύστημα 4-20mA ήταν το προηγούμενο αναλογικό σύστημα που χρησιμοποιούσαν τα παλαιότερα αναλογικά όργανα [21] και το HART επιτρέπει τη χρήση των ίδιων καλωδίων αλλά με διαφορετική διαμόρφωση σήματος ώστε να μεταδίδει ταυτόχρονα αναλογικά-ψηφιακά σήματα, ώστε να υπάρχει μια υβριδική διαμόρφωση. Έτσι επιτυγχάνεται μια αμφίδρομη επικοινωνία μεταξύ των συσκευών πεδίου. Χρησιμοποιεί την τεχνική FSK Frequency Shift Keying η οποία βασίζεται στο standard Bell 202 της Bell Laboratories.

Στην διαμόρφωση FSK, Τα δυαδικά ψηφία λογικό «1» και λογικό «0» αναπαρίστανται από δύο ημιτονοειδή κύματα με συχνότητες στα 1200 Hz και 2200 Hz, αντιστοίχως, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 29 HART. Το ψηφιακό σήμα με διαμόρφωση FSK

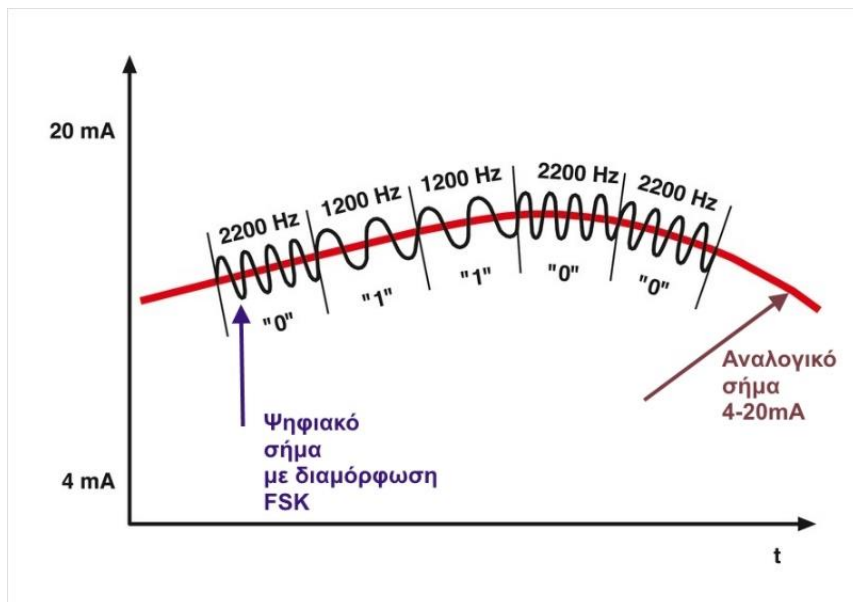
Επειδή η μέση τιμή κάθε ημιτονοειδούς κύματος είναι μηδενική (0) (στις συχνότητες 1200 και 2200Hz) που έχει τοποθετηθεί με υπέρθεση πάνω στο σήμα των 4-20mA, για αυτό το λόγο η αναλογική πληροφορία των 4-20 mA δεν αλλοιώνεται ούτε διακόπτεται, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 30 Η μέση τιμή του ημιτονοειδούς σήματος είναι 0 για την κάθε συχνότητα και έτσι δεν επηρεάζεται το αναλογικό σήμα.

Αυτή η μέθοδος παράγει ένα σήμα επικοινωνίας στο οποίο για κάθε συσκευή πεδίου, ο χρόνος απόκρισης είναι 500 ms.

Ο ρυθμός (rate) με τον οποίο μεταδίδονται τα ψηφιακά δεδομένα είναι 1200 bps. (=1kBaud). Είναι χαμηλός ρυθμός, αλλά επαρκεί για να μεταφέρονται ψηφιακά δεδομένα που απαιτούνται. Επειδή χρησιμοποιούνται δύο χαμηλές συχνότητες, ο ρυθμός αυτός μπορεί να διατηρείται, ακόμη και αν τα δύο καλώδια στα οποία μεταφέρεται το σήμα είναι κακής ποιότητας.



Εικόνα 31. HART. Στο αναλογικό σήμα 4-20 mA γίνεται υπέρθεση ενός ψηφιακού σήματος με διαμόρφωση FSK.

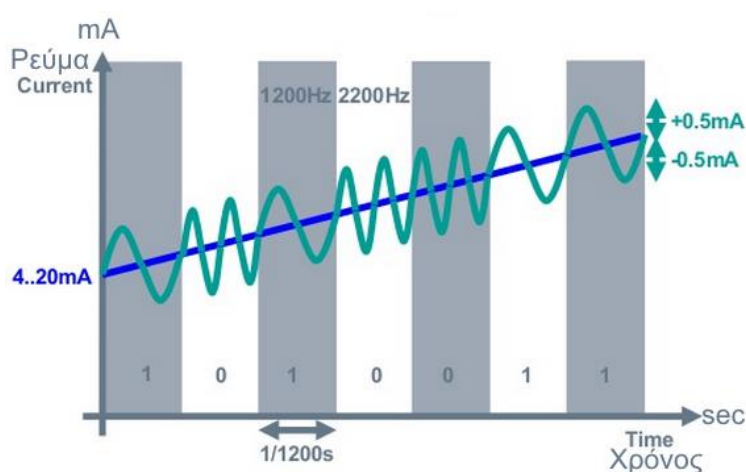
Με αυτό τον τρόπο παρέχονται ταυτόχρονα δύο κανάλια επικοινωνίας:

α) το αναλογικό σήμα ρεύματος 4-20 mA

β) το ψηφιακό σήμα FSK.

Έτσι, αν η συσκευή πεδίου είναι όργανο μέτρησης, τότε το αναλογικό σήμα χρησιμοποιείται για να μεταδώσει την τιμή της μέτρησης και το ψηφιακό σήμα χρησιμοποιείται για να μεταδώσει επιπρόσθετες πληροφορίες για τη συσκευή.

Τέτοιες πληροφορίες είναι διαγνωστικές πληροφορίες, η κατάσταση της συσκευής, υπολογισμένες τιμές. Συνήθως μία συσκευή που συνδέεται με δύο σύρματα χρησιμοποιεί ένα μικρότερης έντασης ρεύμα 3.6 mA για τη δική της τροφοδοσία και λειτουργία ενώ χρησιμοποιεί το ρεύμα 4-20 mA για να μεταδώσει την πληροφορία της μέτρησης.



Εικόνα 32. HART. Στο αναλογικό σήμα 4-20 mA γίνεται υπέρθεση ενός ψηφιακού σήματος με διαμόρφωση FSK. Πηγή: PEPPERL+FUCHS

3.1.3 Χαρακτηριστικά του δικτύου HART

Το πρωτόκολλο HART είναι της μορφής κύριος σταθμός/εξαρτώμενος σταθμός (master/slave). Ο κύριος σταθμός στέλνει μια αίτηση (request) και ο εξαρτώμενος σταθμός στέλνει απάντηση (response). Ο εξαρτώμενος σταθμός είναι η συσκευή πεδίου (field device). Η απάντηση από τον εξαρτώμενο σταθμό περιέχει ένα σήμα αναγνώρισης ACK, που δηλώνει ότι λήφθηκε η αίτηση και μπορεί να περιέχει και επιπλέον δεδομένα που ζήτησε ο κύριος σταθμός.

3.1.3.1 Οι λειτουργίες για τις συσκευές του δικτύου HART

Βασικές λειτουργίες του HART είναι:

α) Η λειτουργία σημείο προς σημείο (point-to-point) και

β) η λειτουργία πολλαπλών σημείων (multidrop)

χρησιμοποιούνται για να μεταφέρονται αμφίδρομα οι πληροφορίες ανάμεσα στις συσκευές πεδίου και στα κεντρικά συστήματα ελέγχου και παρακολούθησης.

Επιπλέον λειτουργίες ψηφιακής μετάδοσης δεδομένων (digital transmission) είναι:

γ) Η λειτουργία καταιγισμού (burst mode) που είναι προαιρετική.

Στη λειτουργία καταιγισμού η συσκευή πεδίου στέλνει συνεχώς δεδομένα στον κύριο σταθμό (Master) χωρίς να δεχθεί αίτηση (request) από αυτόν και ισχύει μόνο για τη σύνδεση σημείο προς σημείο.

δ) Η λειτουργία Poll / response mode

Στην λειτουργία Poll/response, ο κύριος σταθμός (Master) polls κάθε μία από τις συσκευές πεδίου που βρίσκονται συνδεδεμένες στο δίκτυο HART και κάνει αίτηση (request) για να του στείλουν δεδομένα. Οι συσκευές πεδίου στέλνουν απόκριση (response).

Παρακάτω γίνεται μία αναλυτική παρουσίαση των λειτουργιών.

Συσκευές πεδίου (field devices) ονομάζονται τα έξυπνα όργανα (smart instruments), διότι τοποθετούνται στο πεδίο της βιομηχανικής εγκατάστασης που ονομάζεται field.

Παρακάτω, περιγράφονται πιο αναλυτικά οι βασικές λειτουργίες των συσκευών HART:

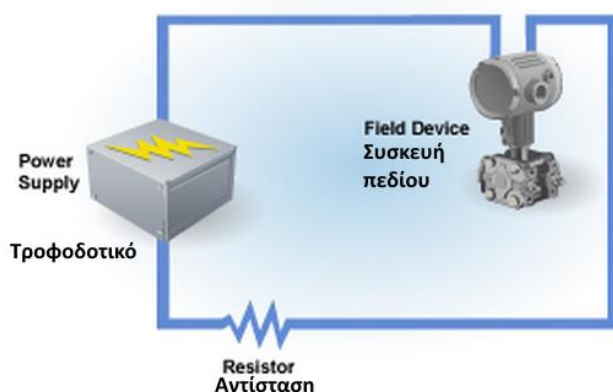
α) Η συνδεσμολογία σημείο-προς-σημείο (point-to-point).

Με τη συνδεσμολογία σημείο-προς-σημείο κάθε συσκευή πεδίου (field device) συνδέεται ξεχωριστά με δύο καλώδια στο δίκτυο.[3],[4].

Η συνδεσμολογία σημείο-προς-σημείο χρησιμοποιεί τα αναλογικά σήματα ρεύματος 4-20 mA για να μεταδώσει μόνο μία μεταβλητή από μία διεργασία (process variable). Τα αναλογικά σήματα 4-20 mA μπορούν να χρησιμοποιηθούν για έλεγχο και δεν επηρεάζονται από τα ψηφιακά σήματα HART. Αν είναι επιθυμητό να μεταδοθούν επιπλέον μεταβλητές διεργασιών (process variables), χρησιμοποιούνται τα ψηφιακά σήματα.

Σε ψηφιακή μορφή μεταδίδονται επιπρόσθετα δεδομένα των συσκευών όπως είναι μεταβλητές, δεδομένα μετρήσεων, παράμετροι διαμόρφωσης και άλλα.

Τα ψηφιακά σήματα δίνουν πρόσβαση σε δευτερεύουσες μεταβλητές και δεδομένα που χρησιμοποιούνται για γενικές λειτουργίες, εντολές συντηρήσεις και διαγνώσεις.



Εικόνα 33. Στη συνδεσμολογία σημείο προς σημείο μόνο μία συσκευή συνδέεται με δύο καλώδια, στην πηγή τροφοδοσίας ή/και σε σύστημα εισόδων/εξόδων.

Ένα έξυπνο όργανο μετρήσεων (smart instrument) είναι η συσκευή πεδίου [22, 21] (field device). Έγκυρες τιμές εξόδου (output values) από το όργανο μέτρησης είναι είτε το αναλογικό σήμα με ρεύμα 4-20 mA είτε το ψηφιακό σήμα. Η διεύθυνση polling για το όργανο μέτρησης τίθεται στο "0". Με τη συνδεσμολογία σημείο προς σημείο μόνο ένα όργανο μέτρησης μπορεί να τοποθετηθεί σε ένα ζεύγος καλωδίων. Τα δύο κανάλια επικοινωνίας, το αναλογικό και το ψηφιακό, υπάρχουν ταυτόχρονα. Για παράδειγμα, η τιμή της πίεσης (pressure) μπορεί να στέλνεται ως αναλογικό σήμα 4-20 mA, και να αναπαριστά ένα σύνολο τιμών πίεσεως, ενώ η τιμή θερμοκρασίας να στέλνεται ως ψηφιακό σήμα με τα ίδια καλώδια.



Εικόνα 34. Το HART μεταφέρει ταυτόχρονα ένα αναλογικό σήμα και ένα ψηφιακό σήμα. Πηγή: [19]

β) Η συνδεσμολογία πολλαπλών σημείων (multidrop).

Στη συνδεσμολογία πολλαπλών σημείων απαιτείται μόνο ένα ζεύγος αγωγών και αν είναι εφικτό, προστατευτικά και μία βοηθητική παροχή ισχύος. Μπορούν να συνδεθούν παράλληλα στο ίδιο ζεύγος αγωγών μέχρι 15 συσκευές πεδίου (field devices). Στην περίπτωση αυτή, όλες οι μεταβλητές της διεργασίας μεταδίδονται ψηφιακά. Όλες οι διευθύνσεις (polling addresses) των συσκευών είναι >0 και το ρεύμα σε κάθε συσκευή είναι σταθερό και παραμένει σε μια ελάχιστη τιμή, συνήθως στα 4 mA, απλώς για να διατηρούνται ενεργοποιημένες οι συσκευές και δεν μεταδίδει κανένα σήμα. Ο φιλοξενητής (host) για να ξεχωρίζει τις συσκευές πεδίου μεταξύ τους, αναθέτει σε αυτές προκαθορισμένες διευθύνσεις (preset addresses) που έχουν τιμές από 1 ως 15.

Η συνδεσμολογία πολλαπλών σημείων χρησιμοποιείται για εκτεταμένες εγκαταστάσεις που απαιτούν εποπτικό έλεγχο όπως για παράδειγμα, είναι πετρελαιοαγωγοί, σταθμοί μεταφοράς και γήπεδα δεξαμενών.

Αντίθετα όμως, οι βαλβίδες ελέγχου (control valves) δεν μπορούν να χρησιμοποιηθούν σε λειτουργία πολλαπλών σημείων (όπου χρησιμοποιούνται ψηφιακά σήματα), διότι με τα ψηφιακά σήματα το πρωτόκολλο HART καθυστερεί και δεν μπορεί να ελέγξει εγκαίρως τα προκαθορισμένα σημεία set points των βαλβίδων. Για αυτό το λόγο πάντοτε ως σήματα ελέγχου βαλβίδων χρησιμοποιούνται τα αναλογικά σήματα ρεύματος 4 ως 20 mA.



Εικόνα 35 Συσκευή πεδίου HART.

γ) Λειτουργία καταιγισμού (burst mode) ή λειτουργία εκπομπής (broadcast mode).

Οι συσκευές HART υποστηρίζουν μία προαιρετική λειτουργία επικοινωνίας που ονομάζεται «καταιγισμός» (burst), όμως αυτή η λειτουργία ισχύει μόνο στη συνδεσμολογία σημείο-προς-σημείο (point-to-point), όπου συνδέεται μόνο μία συσκευή πεδίου (field device) και μεταδίδει ψηφιακά δεδομένα.

Για να ενεργοποιηθεί η προαιρετική λειτουργία καταιγισμού (burst communication mode), η εξαρτημένη συσκευή δέχεται μία εντολή από τον κύριο σταθμό για να στέλνει αδιάκοπα δεδομένα καταιγισμού (burst data).

Με τη λειτουργία καταιγισμού επιτυγχάνονται πιο υψηλοί ρυθμοί δεδομένων ανανέωσης. Ο κύριος σταθμός παραλαμβάνει το μήνυμα πιο γρήγορα με 3-4 ενημερώσεις δεδομένων ανά sec. Για παράδειγμα, ο εξαρτημένος σταθμός μπορεί να στέλνει την τιμή μιας μεταβλητής της διεργασίας σε μήνυμα ευρείας εκπομπής ώστε ο κύριος σταθμός να έχει συνεχή ενημέρωση της τιμής και να τη χρησιμοποιήσει σε κάποια διεργασία.

Η λειτουργία καταιγισμού σταματάει όταν ο κύριος σταθμός δώσει εντολή στην εξαρτημένη συσκευή να σταματήσει.

δ) Η λειτουργία poll/response

Στη λειτουργία poll/response, ο κύριος σταθμός (master) κάνει poll σε κάθε μια συσκευή πεδίου και ζητά τις σχετικές πληροφορίες.

Συσκευές επιπέδου μηχανής

Υπάρχουν οι συσκευές του επιπέδου μηχανής που βασίζονται στην τεχνολογία HART. Οι συσκευές αυτές επιτρέπουν εύκολη και γρήγορη εγκατάσταση.

Η επικοινωνία πολλών διαφορετικών συσκευών στο πρωτόκολλο HART, μπορεί να γίνει μέσω της ίδιας δισύρματης γραμμής που είναι ένα συνεστραμμένο ζεύγος καλωδίων.

Σε αυτή τη συνδεσμολογία το πλεονέκτημα είναι ότι δεν απαιτούνται υπερβολικά πολλές καλωδιώσεις.

Δύο κύριοι σταθμοί.

Το πρωτόκολλο HART έχει δύο κύριους σταθμούς (masters). Αυτοί είναι ο πρωτεύων κύριος σταθμός (primary master) και ο δευτερεύων κύριος σταθμός (Secondary Master).

Ο πρωτεύων κύριος σταθμός είναι το σύστημα ελέγχου (control system) και ο δευτερεύων κύριος σταθμός είναι μία συσκευή χειρός (handheld).

Οι δύο κύριοι σταθμοί επικοινωνούν με τους εξαρτημένους σταθμούς. Αυτοί είναι συσκευές που ανταποκρίνονται σε εντολές των κυρίων σταθμών, δηλαδή οι συσκευές πεδίου (field devices).

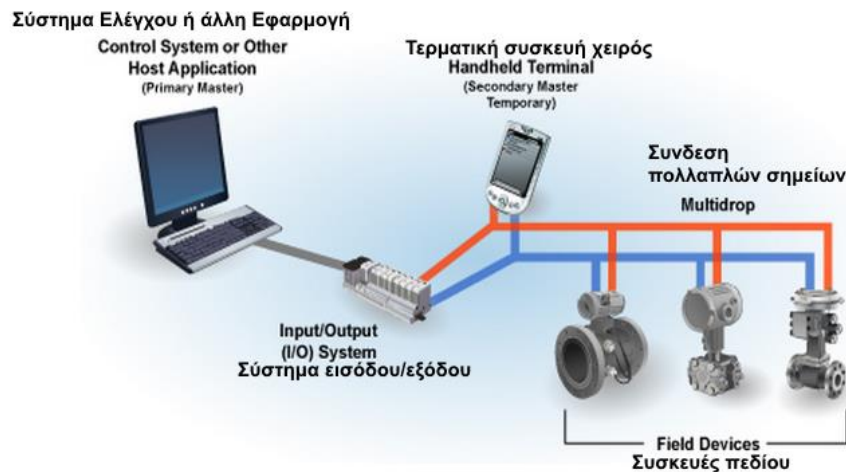
Με διάφορες τροποποιήσεις στο συνολικό πλήθος και στο είδος συσκευών που συνδέονται στο δίκτυο HART παρέχεται προσαρμοστικότητα και περισσότερες λειτουργίες.

Ο πρωτεύων κύριος σταθμός (primary master) είναι ένα κατακευματισμένο σύστημα ελέγχου (DCS, Distributed Control System), ή ένας υπολογιστής, είτε ένα PLC (προγραμματιζόμενος λογικός ελεγκτής), ή μία εφαρμογή (host application) που τρέχει σε έναν υπολογιστή.

Ο δευτερεύων κύριος σταθμός (secondary master) είναι είτε ένας υπολογιστής είτε κάποιο τερματικό χειρός (handheld terminal).

Οι εξαρτημένοι σταθμοί, μπορεί να είναι μεταδότες, επενεργητές (actuators) και ελεγκτές.

Οι δύο κύριοι σταθμοί (masters) συνδέονται παράλληλα με τις εξαρτημένες συσκευές πεδίου (field devices). Αυτό γίνεται για να μην διακόπτεται ο βρόχος ρεύματος (current loop) όταν αποσυνδέονται κάποιες συσκευές πεδίου ή όταν συνδέονται νέες συσκευές πεδίου.



Εικόνα 36. Πρωτεύων κύριος σταθμός (primary master) και δευτερεύων κύριος σταθμός (secondary master) σε σύνδεση πολλαπλών σημείων (multidrop). Η ενέργεια στις συσκευές πεδίου παρέχεται από μία εξωτερική πηγή τροφοδοσίας που δεν εικονίζεται στο σχήμα. Πηγή: [19]



Εικόνα 37 Πρωτεύων κύριος σταθμός (primary master) και δευτερεύων κύριος σταθμός (secondary master) σε σύνδεση σημείο προς σημείο point-to-point. πηγή [19].

3.1.3.2 Όργανα μετρήσεων HART (HART instruments)

Χρησιμοποιούνται στη βιομηχανία, τα έξυπνα όργανα μετρήσεων (smart instruments) που περιέχουν μικροϋπολογιστή. Τα όργανα αυτά έχουν περισσότερες δυνατότητες από τα παλαιότερα αναλογικά όργανα. Μερικά πλεονεκτήματά των έξυπνων οργάνων είναι ότι παρέχουν μεγαλύτερη ακρίβεια μέτρησης, μακροπρόθεσμα έχουν μεγάλη σταθερότητα, μπορούν να υποστηρίξουν πολλαπλούς διαφορετικούς τύπους αισθητήρων και μπορούν να μετρήσουν πολλές διαφορετικές μεταβλητές διεργασιών. Έτσι το ίδιο όργανο HART που μετράει την τιμή

μίας μεταβλητής, μπορεί σε άλλη περίπτωση να ρυθμιστεί για να μετρήσει διαφορετική κύρια μεταβλητή PV (primary variable) (μάζα, ροή ή πυκνότητα). Ένα μειονέκτημα των οργάνων αυτών είναι ότι για να επιτευχθεί ακρίβεια στη μέτρηση απαιτούνται πολλές ρυθμίσεις και τεστ στην είσοδο και στην έξοδο των οργάνων, ώστε να γίνει σωστά η βαθμονόμηση τους, ενώ αντίθετα τα αναλογικά όργανα δεν απαιτούν τόσες πολλές ρυθμίσεις [23].

Στα έξυπνα όργανα μέτρησης επιτρέπεται να χρησιμοποιούνται Αλγόριθμοι ελέγχου. Αυτοί οι αλγόριθμοι μπορούν να εκτελούνται σε συσκευές πεδίου που βρίσκονται πολύ κοντά στη διεργασία.

Επίσης με τη χρήση του HART κάποιοι μετατροπείς και επενεργητές υποστηρίζουν λειτουργίες ελέγχου σε μια συσκευή πεδίου. Μπορεί να υλοποιηθεί ένας έλεγχος με ελεγκτή PID μέσω του HART χωρίς να υπάρχει κάποιος άλλος ξεχωριστός ελεγκτής PID.

Όταν στο HART ο έλεγχος τοποθετηθεί στο επίπεδο της μηχανής, τότε έχει μεγαλύτερη λειτουργικότητα και υπάρχει μεγαλύτερη αξιοπιστία στις μετρήσεις,

διότι τα δεδομένα δεν μεταφέρονται σε απομακρυσμένους ελεγκτές και έτσι δεν υπάρχει κίνδυνος αλλοίωσης από σφάλματα που θα υπήρχαν κατά τη μεταφορά δεδομένων.

Ο αλγόριθμος ελέγχου στο HART χρησιμοποιεί το αναλογικό σήμα.

Η επικοινωνία HART επιτρέπει τις ρυθμίσεις και μετατροπές στις παραμέτρους ελέγχου. Το HART επιτρέπει την πρόσβαση σε όλα τα δεδομένα των συσκευών για να συλλεχθούν διάφορες πληροφορίες. Τα δεδομένα των μετρήσεων από τα όργανα μπορούν να συλλεχθούν και να χρησιμοποιηθούν σε υπολογισμούς. Αυτοί οι υπολογισμοί είναι χρήσιμοι σε επαληθεύσεις δεδομένων, σε συγκρίσεις μεταξύ στατιστικών στοιχείων, σε υπολογισμό του μεγέθους της εγκατάστασης, σε υπολογισμό της ενέργειας που καταναλώνει συνολικά η εγκατάσταση.

3.1.3.3 Σήματα HART

Σύμφωνα με το πρωτόκολλο HART, ο κύριος σταθμός (master device) στέλνει σήμα τάσης (voltage signal), ενώ ο εξαρτώμενος σταθμός (slave device) που είναι η συσκευή πεδίου (field device) στέλνει σήμα ρεύματος (current signal) για να μεταφέρει τα μηνύματα. Το σήμα ρεύματος μετατρέπεται σε αντίστοιχο σήμα τάσης μέσω μιας αντίστασης φορτίου που είναι 250 Ω στο

δέκτη και όλες οι συσκευές χρησιμοποιούν κυκλώματα δέκτη που είναι ευαίσθητα ως προς την τάση (voltage sensitive).

Το σήμα πρέπει να είναι ημιτονοειδές, αλλά είναι αποδεκτή και μία κυματομορφή με τραπεζοειδές σχήμα. Η τετραγωνική κυματομορφή δεν είναι αποδεκτή.

Το πρωτόκολλο HART έχει μία ελάχιστη ευαισθησία ως προς την τάση 200 mV peak-peak. Για τη διαμόρφωση ρεύματος FSK έχει ρεύμα 1mA peak-peak (+5mA ως -5mA). Το ελάχιστο φορτίο είναι 200 Ω.

Για να υπάρχει μία αξιοπιστία στη λήψη των σημάτων, το πρωτόκολλο HART καθορίζει ότι συνολικά η αντίσταση φορτίου του βρόχου ρεύματος (current loop) μαζί με την αντίσταση καλωδίων πρέπει να έχει τιμή που κυμαίνεται από την ελάχιστη τιμή των 230 Ω μέχρι τη μέγιστη τιμή των 1100 Ω. Συνήθως το ανώτερο όριο δεν ορίζεται στην προδιαγραφή αλλά προκύπτει από κάποιους υπολογισμούς που δεν αναφέρονται εδώ.

3.1.3.4 Καλώδια HART

Στο δίκτυο HART χρησιμοποιείται το συνεστραμμένο ζεύγος καλωδίων. Άλλες φορές έχει θωράκιση και άλλες φορές δεν έχει θωράκιση, ανάλογα με την απόσταση.

Όταν το καλώδιο είναι χωρίς θωράκιση, μπορεί να τοποθετηθεί σε μικρές αποστάσεις και σε σημεία όπου το περιβάλλον δεν παρουσιάζει επιδράσεις που δημιουργούν προβλήματα στην μετάδοση δεδομένων.

Για κοντινές αποστάσεις, δηλαδή μικρότερες από 1524 m, μπορεί να χρησιμοποιηθεί συνεστραμμένο ζεύγος καλωδίων χωρίς θωράκιση, όπου ο κάθε αγωγός έχει διάμετρο 0.51 mm ή διατομή 0.2 mm².

Για πιο μακρινές αποστάσεις, δηλαδή μεγαλύτερες από 1524 m, μπορεί να χρησιμοποιηθεί συνεστραμμένο ζεύγος καλωδίων με κοινή θωράκιση των δύο αγωγών, όπου ο κάθε αγωγός έχει διάμετρο 0.81 mm ή διατομή 0.5 mm².

Συνήθως για ένα δίκτυο HART η μέγιστη απόσταση είναι μέχρι 3000 m.

Για σπάνιες περιπτώσεις, που η απόσταση είναι μεγαλύτερη από 3000m θα πρέπει το συνεστραμμένο ζεύγος καλωδίων να έχει θωράκιση στον κάθε αγωγό ξεχωριστά και ο κάθε αγωγός να έχει διατομή 0.5 mm².

Όμως το μέγιστο μήκος του δικτύου εξαρτάται στην πράξη από το είδος των συσκευών που είναι συνδεδεμένες στο δίκτυο HART και από τα χαρακτηριστικά του καλωδίου όπως είναι η χωρητικότητα του (pF/m).

Τα καλώδια πρέπει να έχουν το κατάλληλο μήκος και την κατάλληλη διατομή για να μεταφέρουν σωστά τα σήματα.

Αν τα δύο καλώδια είναι πολύ λεπτά και μεγάλου μήκους, τότε αυξάνεται συνολικά η αντίσταση των καλωδίων. Αυτό έχει ως αποτέλεσμα να υπάρχει μεγαλύτερη εξασθένηση του σήματος (attenuation) και να εμφανίζονται παραμορφώσεις στο σήμα. Αυτές οι παραμορφώσεις μπορούν να συμβούν όταν μειωθεί η κρίσιμη συχνότητα (critical frequency) του πομπού (transmitter).

Τα ήδη εγκατεστημένα καλώδια που υπάρχουν στις βιομηχανικές εγκαταστάσεις, συνήθως αρκούν για να μεταδώσουν τα ψηφιακά σήματα HART διότι πληρούν τις προϋποθέσεις που αναφέρθηκαν.

Στον παρακάτω πίνακα φαίνεται ο μέγιστος επιτρεπτός αριθμός συνδεδεμένων συσκευών και το μέγιστο επιτρεπτό μήκος καλωδίου που επηρεάζεται από τη χωρητικότητα του καλωδίου.

Χωρητικότητα καλωδίου (pF/m)

Μήκος καλωδίου (m)

65 pF/m	95 pF/m	160 pF/m	225 pF/m	Πλήθος συσκευών
2769 m	2000 m	1292 m	985 m	1
2462 m	1815 m	1138 m	892 m	5
2154 m	1600 m	1015 m	769 m	10
1846 m	1415 m	892 m	708 m	15

Πίνακας 3.1. Για θωρακισμένο συνεστραμμένο ζεύγος καλωδίων με διάμετρο 1.02 mm ή διατομή 0.81 mm² τα επιτρεπτά μήκη καλωδίων και το μέγιστο πλήθος συνδεδεμένων συσκευών.

3.1.3.5 Πολυπλέκτης HART

Σύνδεση πολλαπλών σημείων (multidrop) και πολυπλέκτης (Multiplexer).

Στη διάταξη πολλαπλών σημείων (multidrop) χρησιμοποιείται ένα μοναδικό ζεύγος καλωδίων στο οποίο συνδέονται πολλαπλές συσκευές πεδίου.

Το ρεύμα τροφοδοσίας σταθεροποιείται σε μία ελάχιστη τιμή 4mA και περνάει από όλες τις συσκευές. Αυτό το ρεύμα είναι ικανό για να λειτουργήσει μία συσκευή πεδίου στο δίκτυο HART και έτσι λειτουργούν όλες οι συσκευές.

Για μία μόνο συσκευή πεδίου, ο χρόνος που απαιτείται για τον κύκλο ανάγνωσης-μετάδοσης μιας μεταβλητής είναι 500 ms.

Αν στο δίκτυο συνδεθούν 15 συσκευές τότε απαιτούνται 7500 ms = 7.5 sec

για να γίνει ανάγνωση-μετάδοση μεταβλητών από όλες τις συσκευές.

Επιπλέον σε ένα δίκτυο που έχει αυτή τη μορφή, μπορούν να συνδεθούν και ελεγκτές πεδίου HART.

Με την συνδεσμολογία πολλαπλών σημείων απαιτείται συνολικά μικρότερο μήκος καλωδίων από ότι στην συνδεσμολογία σημείο-προς-σημείο. Έτσι, η πιο οικονομική λύση από τις δύο είναι η συνδεσμολογία πολλαπλών σημείων.

Αν στο δίκτυο HART πρόκειται να συνδεθεί ένας μεγάλος αριθμός συσκευών, τότε απαιτείται να χρησιμοποιούνται πολυπλέκτες οι οποίοι είναι συμβατοί με το δίκτυο HART.

Οι συνδεσμολογίες στις οποίες μπορεί να συνδεθεί ο πολυπλέκτης είναι και η συνδεσμολογία πολλαπλών σημείων και η σημείο προς σημείο.

Επιπλέον ο πολυπλέκτης (multiplexer) έχει δυνατότητα να συμπεριφέρεται ως μία πύλη που λαμβάνει τα μηνύματα ενός δικτύου HART και τα μετατρέπει σε μηνύματα άλλων πρωτοκόλλων έτσι ώστε να επιτρέπει να διαβαστούν και από άλλα δίκτυα όπως είναι τα Modbus, PROFIBUS και Ethernet.

3.1.3.6 Εφαρμογές HART

Το πρωτόκολλο HART εφαρμόζεται σε πάρα πολλές βιομηχανίες. Ένα παράδειγμα χρήσης του είναι η παρακολούθηση δεξαμενών αποθήκευσης.

Επίσης υπάρχουν περιπτώσεις όπου το HART χρησιμοποιείται σε συνδυασμό με το PROFIBUS DP και τα δύο αυτά πρωτόκολλα συνεργάζονται μεταξύ τους.

μερικά χαρακτηριστικά του πρωτοκόλλου HART φαίνονται στον πίνακα 3.2.

Προέλευση	Από την εταιρία Rosemount το 1986 και συνεχίστηκε από το HART Communication Foundation (HCF).
Πρότυπο	Είναι σύμφωνο με το μοντέλο OSI αλλά υλοποιεί λιγότερα επίπεδα
Μέγιστο Μήκος	3000m
Ταχύτητα μετάδοσης	1200 bps, αλλά εξαρτάται από το φυσικό επίπεδο (Physical Layer) που εφαρμόζεται.
Αριθμός συσκευών	15 συσκευές σε συνδεσμολογία πολλαπλών σημείων (multidrop) ή περισσότερες με πολύπλεξη
Μέθοδος Προσπέλασης	Κύριου/ εξαρτημένου σταθμού (master/slave) όπου η εξαρτημένη συσκευή δεν αποκρίνεται αν δεν λάβει μήνυμα από την κύρια συσκευή.
Έλεγχος Λαθών	Με την μέθοδο ισοτιμίας
Τοπολογίες	Σημείο προς Σημείο (point to point), Πολλαπλών σημείων (multidrop), ασύρματο πλέγμα (Wireless mesh).

Πίνακας 3.2. Βασικά χαρακτηριστικά του HART.

3.1.4 Πακέτο δεδομένων του HART

Το πακέτο δεδομένων στο πρωτόκολλο HART φαίνεται παρακάτω. Ονομάζεται και telegram.

Preamble	SD	AD	CD	BC	Status	Data	Checksum
	Start	Address	Command	Byte Count			
	Delimiter			Number of			
	Byte			data bytes			

Πίνακας 3.3. Πακέτο δεδομένων του HART.

Μία συνοπτική περιγραφή των πεδίων φαίνεται στον παρακάτω πίνακα.

Όνομα πεδίου	Μήκος σε bytes	Σκοπός
Preamble	5-20	Συγχρονισμός και ανίχνευση φέροντος
Start byte	1	Ορίζει το πλήθος κυρίων σταθμών
Address (διεύθυνση)	1-5	Καθορίζει τον εξαρτώμενο σταθμό (slave), ορίζει τον κύριο σταθμό (master) και δείχνει τη λειτουργία καταιγισμού (burst mode)
Command (εντολή)	1	Αριθμητική τιμή για την εντολή (command) που πρέπει να εκτελεστεί.
Byte Count Number of data bytes	1	Δείχνει το μέγεθος του πεδίου δεδομένων (data field)
Status (κατάσταση)	Master (0 bytes) Slave (2 bytes)	Εκτέλεση και απόκριση για την κατάσταση της «υγείας» του συστήματος
Data (δεδομένα)	0-253	Δεδομένα που έχουν σχέση με την εντολή (command)
Checksum (parity)	1	XOR για όλα τα bytes από το Start Byte ως το Last Byte των δεδομένων.

Πίνακας 3.4: Τα πεδία στο πακέτο δεδομένων HART.

Preamble (5 ως 20 bytes), hex FF.

Κάποιες συσκευές έχουν 5 bytes στο πεδίο preamble, ενώ άλλες συσκευές έχουν 20 bytes. Οι νεότερες συσκευές συνήθως υλοποιούν τα Preamble bits με 5 bytes, διότι αν έδιναν περισσότερα bytes θα υπήρχε αυξημένο overhead και μειωμένη ταχύτητα επικοινωνίας. Οι κύριοι σταθμοί (master) πρέπει να έχουν συμβατότητα προς τα πίσω για τις εξαρτημένες συσκευές που συνδέονται σε αυτούς. Ο κύριος σταθμός (master) για να επικοινωνήσει με μία συσκευή ξεκινά με το μέγιστο μήκος του preamble length που είναι 20 bytes και αργότερα μειώνεται όταν οριστεί το μέγεθος του preamble για την συσκευή που πρόκειται να συνδεθεί.

Το preamble αποτελείται από 3 ή περισσότερους δεκαεξαδικούς χαρακτήρες FF και συγχρονίζει τα σήματα των συμμετεχόντων.

Start delimiter (οριοθέτηση αρχής) ή Start byte (1 byte).

Είναι 1 byte που περιέχει τον αριθμό των Κύριων σταθμών (master) και καθορίζει πότε αρχίζει το πακέτο με τα δεδομένα επικοινωνίας.

Καθορίζει ποια συσκευή στέλνει δεδομένα (ο κύριος σταθμός master, ένας εξαρτημένος σταθμός slave, ή ένας εξαρτημένος σταθμός slave σε λειτουργία καταιγισμού burst mode). Επιπλέον καθορίζει αν χρησιμοποιείται η μορφή πλαισίου διεύθυνσης Short Frame ή η μορφή πλαισίου διεύθυνσης Long Frame.

AD Address (διεύθυνση)

Καθορίζει τη διεύθυνση προορισμού (destination address) η οποία υλοποιείται σε μία από τις μορφές διευθυνσιοδότησης του HART.

Υπάρχουν δύο μορφές διευθύνσεων. Η μορφή πλαισίου Short frame (1byte) και η μορφή πλαισίου Long frame (5 bytes).

Short Frame (1 byte):

Είναι μία αρχική μορφή διευθυνσιοδότησης στην έκδοση 4 του HART, που χρησιμοποιούσε μόνο 4 bits για να καθορίσει τη διεύθυνση συσκευής (device address). Ένα bit χρησιμοποιείται για να διαχωρίζονται οι δύο κύριοι σταθμοί (masters). Ένα bit δείχνει την λειτουργία καταιγισμού burst mode. Η διεύθυνση των εξαρτημένων συσκευών (slaves) είναι '0'.

Αυτή η μορφή διευθύνσεων λέγεται polling.

master	burst	0	0	bit 3	bits 2, 1, 0

Εικόνα 38. Short frame address (1byte)

Αυτή η μορφή διευθύνσεων περιόριζε το πλήθος συσκευών σε 16 μαζί με τον κύριο σταθμό (Master) με διευθύνσεις 0 ως 15.

Long Frame (5 bytes):

Η δεύτερη μορφή διευθυνσιοδότησης του HART καθορίστηκε στην έκδοση 5 και χρησιμοποιεί 38 bits για να καθορίζει τη διεύθυνση της συσκευής.

Η διεύθυνση της συσκευής καθορίζεται με μοναδικό τρόπο με έναν μοναδικό προσδιοριστή (unique identifier) και δημιουργείται από τον κώδικα του κατασκευαστή ώστε καμία άλλη συσκευή να μην έχει ίδια διεύθυνση.

Περιέχει τον κώδικα συσκευής (device code) και τον αριθμό προσδιοριστή (id no).

master	burst	0	0	bit 3	bits 35,34,33, ... ,1, 0

Εικόνα 39 Long frame address (5 bytes).

Αυτή η διεύθυνση είναι μοναδική (unique).

Αυτή η διεύθυνση ζητείται (requested) από τη συσκευή χρησιμοποιώντας είτε την εντολή Command 0, είτε την εντολή Command 11.

Η μορφή πλαισίου Long frame παρέχει επιπλέον ασφάλεια διότι η συσκευή δεν μπορεί να λάβει εντολές που προορίζονται για άλλες συσκευές, όταν υπάρχουν σφάλματα παρεμβολών ή συνακρόασης.

Command (Εντολή) [1 byte]

Αυτή είναι μια αριθμητική τιμή 1 byte που αναπαριστά ποια εντολή δόθηκε από τον master και πρέπει να εκτελεστεί, από τις 3 κατηγορίες εντολών που αναφέρθηκαν στο επίπεδο εφαρμογών:

α) Γενικές εντολές (Universal commands), β) Εντολές κοινής πρακτικής (Common practice commands) γ) εντολές για συγκεκριμένες συσκευές (Device Specific commands). Η εντολή Command 0 και η εντολή Command 11 χρησιμοποιούνται για να κάνουν αίτηση (request) για τον αριθμό συσκευής.

Byte count ή Number of data bytes

Το πεδίο Byte Count αναφέρει ποιο είναι το πλήθος από data bytes επικοινωνίας που έρχονται στα 2 επόμενα πεδία που ακολουθούν. Δηλαδή τα bytes του πεδίου status (όταν αυτό υπάρχει) και τα bytes του πεδίου data. Όταν το πακέτο προέρχεται από τον master τότε δεν υπάρχει το πεδίο status. Τα bytes του πεδίου data μπορεί να είναι από 0 μέχρι 25. Το πεδίο Byte Count χρησιμοποιείται για να δείξει το μήκος του πακέτου, ώστε ο παραλήπτης του πακέτου να γνωρίζει το τελευταίο byte του πεδίου Data και ότι μετά από αυτό αρχίζει το πεδίο Checksum.

Status (Κατάσταση) (2 bytes)

Το πεδίο κατάστασης status υπάρχει μόνο στον εξαρτημένο σταθμό (slave) και είναι 2 bytes. Στον κύριο σταθμό (master) δεν υπάρχει. Αυτό το πεδίο κατάστασης status χρησιμοποιείται από τον εξαρτημένο σταθμό (slave) για να δώσει πληροφορίες στον κύριο σταθμό (master) σχετικά με το αν το μήνυμα που λήφθηκε ήταν σωστό, αν ολοκληρώθηκε η τρέχουσα διεργασία, σε ποια κατάσταση λειτουργίας βρίσκεται η εξαρτημένη συσκευή (slave), και για το ποια είναι η κατάσταση «υγείας» του συστήματος. Όταν και τα 2 status bytes είναι στο λογικό 0, τότε λειτουργεί κανονικά η εξαρτημένη συσκευή (slave).

Data

Τα δεδομένα που έχει αυτό το πεδίο εξαρτώνται από το ποια εντολή πρέπει να εκτελεστεί. Είναι από 0 μέχρι 253 bytes. Τα δεδομένα που μπορούν να μεταδοθούν ανήκουν σε διάφορους τύπους όπως: ακέραιοι χωρίς πρόσημο (unsigned integers), αριθμοί κινητής υποδιαστολής (floating point numbers), ή αλφαριθμητικά (strings) που αποτελούνται από σειρές χαρακτήρων ASCII. Η μορφή δεδομένων που χρησιμοποιείται ορίζεται στο πεδίο command που είναι ένα byte. Υπάρχουν μερικές εντολές που δεν περιέχουν δεδομένα, για αυτό το πεδίο δεδομένων δεν έχει πάντα το ίδιο πλήθος bytes.

Checksum (1 byte) (ή parity).

Αποτελείται από μία πράξη XOR για όλα τα bytes ξεκινώντας από το start byte και τελειώνοντας με το last byte του πεδίου δεδομένων.

3.2 WirelessHART

Το WirelessHART είναι ένα ανοικτό πρότυπο (open standard) για ασύρματη επικοινωνία για τον έλεγχο και την παρακολούθηση των βιομηχανικών διεργασιών. Σχεδιάστηκε ειδικά για να ικανοποιήσει τις ανάγκες της βιομηχανίας αυτοματισμού διεργασιών και βασίζεται στο ενσύρματο ανοικτό πρότυπο της βιομηχανίας HART. Το WirelessHART είναι πλήρως συμβατό με τις συσκευές, τα εργαλεία, και τις εφαρμογές του προτύπου HART.

Μερικές συντομογραφίες που χρησιμοποιούνται συνήθως για το WirelessHART είναι: WH, ή WHART, αναλόγως με τη βιβλιογραφία στην οποία περιγράφεται το πρότυπο.

Μερικά από τα καθήκοντα που υποστηρίζει, μεταξύ άλλων, είναι:

Παρακολούθηση του εξοπλισμού και των διεργασιών (processes).

Παρακολούθηση του περιβάλλοντος (Environmental monitoring), διαχείριση της ενέργειας (energy management), εκτέλεση ελέγχων συμμόρφωσης με κανονισμούς (regulatory compliance).

Διαχείριση Πόρων (Asset management), προληπτική συντήρηση (predictive maintenance), προχωρημένες διαγνώσεις (advanced diagnostics).

Έλεγχος κλειστού βρόχου (Closed-loop control) (όταν είναι κατάλληλο να υπάρχει).

Μερικά χαρακτηριστικά του WirelessHART, όπως προαναφέρθηκαν, είναι ότι στο φυσικό επίπεδο (PHY layer) χρησιμοποιεί το πρότυπο IEEE 802.15.4, εκπέμπει στα 2.4 GHz (2400 - 2483 MHz) στη ζώνη συχνοτήτων ISM με διαμόρφωση DSSS, χρησιμοποιεί 15 κανάλια, (από 11-26) για μεταπήδηση συχνότητας. Μόνο οι κόμβοι που είναι συνδεδεμένοι στο δίκτυο γνωρίζουν ποιο θα είναι το επόμενο κανάλι. Χρησιμοποιεί μαύρη λίστα καναλιών (blacklisting) ώστε να αποκλείει κανάλια που παρουσιάζουν πολλές παρεμβολές.

Χρησιμοποιεί TDMA ώστε να μην υπάρχουν συγκρούσεις, με χρονικές σχισμές (timeslots) διάρκειας 10 ms, μέγιστο ρυθμό δεδομένων (data rate) 250 kbps και έχει κεντρικό έλεγχο από το διαχειριστή δικτύου (network manager).

Η απόσταση μεταξύ των συσκευών πεδίου είναι μέχρι 250 m για επικοινωνία με οπτική επαφή (line of sight).

Για τη μετάδοση πακέτων χρησιμοποιεί μία σύγχρονη λειτουργία με αναγνώριση λήψης πακέτου ACK, αλλά για τα πακέτα που μεταδίδονται προς όλους τους κόμβους (broadcast) δεν χρησιμοποιεί αναγνώριση λήψης πακέτου ACK.

Οι τοπολογίες που χρησιμοποιούνται για το δίκτυο είναι:

α) τοπολογία πλέγματος (mesh)

β) τοπολογία αστέρα (star)

γ) συνδυασμός των δύο παραπάνω δηλ. αστέρα (star) και πλέγματος (mesh).

Η δρομολόγηση γίνεται με δύο τρόπους: δρομολόγηση γραφήματος (graph routing) και δρομολόγηση πηγής (source routing).



Εικόνα 40. πειραματική διάταξη συσκευών WirelessHART.

3.2.1 Σύντομη περιγραφή χαρακτηριστικών δικτύου WirelessHART

Η τοπολογία πλέγματος (mesh) αποτελείται από συσκευές πεδίου που τοποθετούνται στο χώρο και σχηματίζουν ένα δίκτυο πολλαπλών αλμάτων (multi-hop). Οι συσκευές πεδίου στέλνουν τα δεδομένα τους στην πύλη (gateway) η οποία είναι μία κεντρική συσκευή που περιγράφεται παρακάτω. Τα ασύρματα δίκτυα πλέγματος (mesh) του WirelessHART είναι πολύ αξιόπιστα, αυτό οργανωμένα και αυτό-θεραπευόμενα. Μπορούν να διαθέτουν πλεονάζουσες διαδρομές (redundant paths) και είναι εύκολο να εγκατασταθούν και να λειτουργήσουν χωρίς καλωδιώσεις.

Τα δίκτυα WirelessHART μπορούν να υποστηρίξουν εφαρμογές σε μεγάλες βιομηχανικές εγκαταστάσεις που εκτείνονται σε μία ευρεία γεωγραφική περιοχή όπως είναι π.χ μεγάλες

εκτάσεις με δεξαμενές, ή αγωγοί πετρελαίου, αλλά μπορούν να χρησιμοποιηθούν και σε μικρότερες μονάδες όπως είναι π.χ. οι μικρές φαρμακευτικές μονάδες που καταλαμβάνουν μικρή έκταση.

Σε ένα δίκτυο πλέγματος (mesh network) WirelessHART μπορούν να συνδεθούν αρκετά διαφορετικά είδη συσκευών (devices). Επιπλέον εκτός από τις φυσικές συσκευές, μέρη του συνολικού συστήματος είναι και συγκεκριμένες μονάδες λογισμικού (software modules). Περισσότεροι τύποι συσκευών (device types) προστίθενται σε μελλοντικές εκδόσεις του προτύπου.

Υπάρχουν συγκεκριμένοι βασικοί τύποι συσκευών και μονάδων λογισμικού που συνδέονται στο δίκτυο WirelessHART. Παρακάτω αναφέρονται οι βασικοί τύποι συσκευών συνοπτικά, ενώ σε επόμενες παραγράφους, οι ίδιες συσκευές περιγράφονται με περισσότερες λεπτομέρειες.

3.2.1.1 Συσκευές πεδίου (field devices) (FD)

Είναι οι πραγματικοί κόμβοι αισθητήρες (actual sensors) που είναι κατανεμημένοι ως κόμβοι στη βιομηχανική διεργασία (industry process), τοποθετημένοι σε διάφορα φυσικά σημεία της βιομηχανικής διεργασίας. Αποτελούνται από διάφορα υποσυστήματα, όπως είναι το υποσύστημα του οργάνου μέτρησης, το υποσύστημα του επεξεργαστή, το υποσύστημα των αισθητήρων, το υποσύστημα του πομποδέκτη ασύρματης επικοινωνίας. Συνήθως τα έξυπνα όργανα μέτρησης (Smart instruments) είναι εξοπλισμένα με τέτοιους αισθητήρες και συνδέονται στον εξοπλισμό των διεργασιών και είναι μέρος του φυσικού εξοπλισμού της βιομηχανικής εγκατάστασης. Οι αισθητήρες στα έξυπνα όργανα μέτρησης, μπορούν να συγκεντρώσουν πολλά δεδομένα μέτρησης που αφορούν μία βιομηχανική διεργασία, όπως είναι για παράδειγμα, μέτρηση πίεσης, θερμοκρασίας, ύψος στάθμης υγρού, έλεγχος σύνθεσης αερίων, παροχή υγρών, κραδασμοί, και άλλα φυσικά μεγέθη, και είναι ικανοί να δρομολογήσουν (routing) και να προωθήσουν (forwarding) πακέτα δεδομένων συνδεδεμένοι σε ένα ασύρματο δίκτυο. Οι Συσκευές πεδίου (FD) (ή αλλιώς WFD) χρησιμοποιούνται για ανίχνευση (sensing), για ενεργοποίηση των επενεργητών (actuation), και για επικοινωνία (communication) μεταξύ δικτυακών συσκευών.

Τα όργανα μέτρησης πεδίου (field instruments) έχουν ενοποιημένες δυνατότητες ασύρματης επικοινωνίας (wireless communication). Οι περισσότεροι κόμβοι σε ένα δίκτυο WirelessHART είναι συσκευές πεδίου (field devices) (FD) που είτε συλλέγουν δεδομένα διεργασιών (process

data) είτε ελέγχουν κάποια διεργασία. [8]. Όλες οι συσκευές έχουν ικανότητες δρομολόγησης (routing). Κάποιες λειτουργούν μόνο ως δρομολογητές (routers).



Εικόνα 41. Συσκευές πεδίου (field devices). Είναι αισθητήρες που συνδέονται στα έξυπνα όργανα μέτρησης και τοποθετούνται σε φυσικές θέσεις μέσα σε μία βιομηχανική εγκατάσταση.



Εικόνα 42 Συσκευές πεδίου (field devices) που τοποθετήθηκαν σε σωλήνες που μεταφέρουν νερό για να εκτελέσουν διάφορες μετρήσεις.

Πριν από το WirelessHART, τα παλαιότερα όργανα μέτρησης, συνήθως μετρούσαν μόνο ένα μέγεθος, π.χ. μόνο πίεση, ή μόνο θερμοκρασία ή μόνο ροή.

Για αυτό υπήρχε η απαίτηση να τοποθετούνται περισσότερα όργανα.



Εικόνα 43. Ο πομπός (transmitter) μιας συσκευής πεδίου wirelessHART μπορεί να συνδεθεί σε διαφορετικά όργανα μέτρησης και να ρυθμιστεί για να δείχνει κατάλληλες ενδείξεις και να στέλνει δεδομένα μέσω ασύρματου δικτύου.

Με τις νεότερες συσκευές πεδίου WirelessHART, το ίδιο όργανο μέτρησης, μπορεί να μετράει συγχρόνως περισσότερα μεγέθη. Δηλαδή να μετράει πίεση, θερμοκρασία, και ροή και να στέλνει τα δεδομένα στο ασύρματο δίκτυο WirelessHART. Έτσι χρειάζονται λιγότερα όργανα μέτρησης από ότι παλιότερα. Σε κάθε συσκευή πεδίου WirelessHART υπάρχει ένας πομπός (transmitter) που μπορεί να συνδεθεί σε διαφορετικά όργανα μέτρησης, να δείξει κατάλληλες ενδείξεις, να αποθηκεύσει και να μεταδώσει συγκεντρωτικά τιμές ενδείξεων μέσω ασύρματου δικτύου.

3.2.1.2 Προσαρμογείς (adaptors ή adapters)

Ο προσαρμογέας είναι μία συσκευή/μονάδα (module) με δυνατότητες ασύρματης επικοινωνίας που συνδέεται σε παλαιότερο εγκατεστημένο όργανο μέτρησης, που ήδη λειτουργεί με το πρωτόκολλο HART και το μετατρέπει ώστε να μπορεί να λειτουργήσει με το πρωτόκολλο WirelessHART και να συνδεθεί στο ασύρματο δίκτυο αισθητήρων.

Ο προσαρμογέας (adaptor) λειτουργεί όπως ο κύριος σταθμός (master) στο ενσύρματο δίκτυο HART (wired HART) για να παρέχει επικοινωνίες μέσω του ασύρματου δικτύου (wireless network) στις παλαιότερες συσκευές που συνδέονται με καλώδια (wired devices).

Ένας προσαρμογέας (adaptor) μπορεί να συνδεθεί είτε μόνο σε μία συσκευή HART (αν προσαρμοστεί πάνω σε αυτή ή με συνδεσμολογία σημείο προς σημείο), είτε σε περισσότερες συσκευές HART, αν χρησιμοποιήσει την συνδεσμολογία πολλαπλών σημείων (multi-drop), με καλώδια.

Η εξωτερική εμφάνιση του προσαρμογέα (adaptor).

Οι προσαρμογείς (adaptors) που κατασκευάζονται έχουν 2 μορφές:

Η μία μορφή είναι ένα κουτί με εξωτερική κεραία ασύρματου δικτύου και η άλλη μορφή είναι η μορφή ενός κυλίνδρου (π.χ. bullet της MACTek, THUM της emerson, SITRANS της Siemens).

Αυτές οι 2 μορφές φαίνονται στις παρακάτω εικόνες.



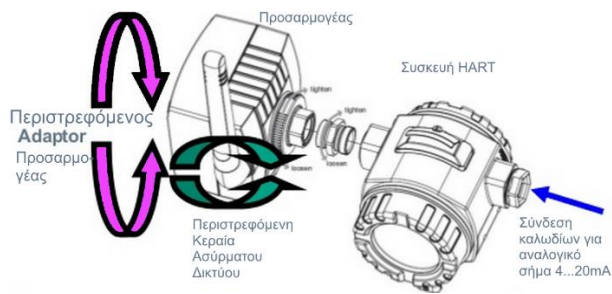
Εικόνα 44. Προσαρμογείς (adaptors) WirelessHART από διαφορετικούς κατασκευαστές



Εικόνα 45 Προσαρμογείς (adaptors) WirelessHART με μορφή κυλίνδρου διαφορετικών κατασκευαστών (bullet της MACTek, THUM της emerson, SITRANS της Siemens).



Εικόνα 46. Ο προσαρμογέας (adaptor) συνδέεται σε μία παλαιότερη συσκευή πεδίου HART και την μετατρέπει σε συσκευή WirelessHART.



Εικόνα 47. Σχεδιάγραμμα σύνδεσης του προσαρμογέα (adaptor) σε μία συσκευή πεδίου HART



Εικόνα 48. Ο προσαρμογέας (adaptor) τύπου bullet συνδέεται σε μία παλαιότερη συσκευή πεδίου HART και την μετατρέπει σε συσκευή WirelessHART.

Το πλεονέκτημα της συμβατότητας προς τα πίσω, δηλαδή η σύνδεση παλαιότερων συσκευών στο νέο δίκτυο εξοικονομεί κόστος, διότι στις αναβαθμίσεις δεν χρειάζεται να αντικατασταθούν από την αρχή όλα τα εγκατεστημένα όργανα μέτρησης.

3.2.1.3 Συσκευές χειρός (handhelds) ή Handheld Communicators (HHC)

Είναι κινητές συσκευές (mobile devices) (είτε ασύρματες είτε όχι). Μερικές είναι εξειδικευμένες όπως π.χ υπολογιστές προσαρμοσμένοι ειδικά για τη συγκεκριμένη βιομηχανική εγκατάσταση. Στο παλαιότερο ενσύρματο πρότυπο HART, υπήρχαν και οι ενσύρματες συσκευές Handheld Communicators οι οποίες μπορούν και αυτές να χρησιμοποιούνται.

Επιπλέον, ως συσκευές χειρός μπορούν να χρησιμοποιηθούν και διάφορα tablets, ή PDAs γενικής χρήσης, ακόμη και κινητά με android που διαθέτουν εγκατεστημένες κατάλληλες εφαρμογές λογισμικού και μπορούν να συνδεθούν στο ασύρματο δίκτυο WirelessHART της βιομηχανικής εγκατάστασης. Η συσκευή χειρός είναι ένα είδος υπολογιστή. Μία συσκευή χειρός (handheld)

είναι κινητός εξοπλισμός που συνήθως κρατείται από το προσωπικό που εργάζεται στο πεδίο (field personnel) και χρησιμοποιείται για διόρθωση σφαλμάτων στην εγκατάσταση (plant), για παρακολούθηση (monitoring), ρύθμιση (configuration), συντήρηση (maintenance), διαγνώσεις (diagnostics), και βαθμονόμηση (calibration) των συσκευών πεδίου (FD, field devices) στο δίκτυο WirelessHART (WH).

Αντίθετα με τους υπόλοιπους τύπους συσκευών WirelessHART, η συσκευή χειρός (handheld) είναι η μόνη κινητή (mobile) συσκευή και αναμένεται ότι θα συνδέεται με πολλαπλά δίκτυα και συσκευές WirelessHART. [8]



Εικόνα 49 Συσκευές χειρός (Handhelds) από διαφορετικούς κατασκευαστές, που χρησιμοποιούνται στο δίκτυο WirelessHART και στο HART.

Η συσκευή χειρός (handheld) μπορεί να ανιχνεύσει την ισχύ του σήματος από μία γειτονική συσκευή πεδίου, ενώ επίσης μία συσκευή πεδίου μπορεί να ανιχνεύσει την ισχύ σήματος της συσκευής χειρός (handheld). Δύο συσκευές πεδίου (field devices) δεν επικοινωνούν μεταξύ τους αλλά και οι συσκευές πεδίου (field devices) και η συσκευή χειρός στέλνουν δεδομένα περιοδικά στο διαχειριστή δικτύου (network manager) και αναφέρουν για την ισχύ του σήματος των γειτόνων τους. Έτσι ο διαχειριστής δικτύου λαμβάνει ανά ζεύγη τις τιμές για ισχύ σήματος π.χ. η συσκευή πεδίου αναφέρει ότι η συσκευή χειρός έχει ισχύ σήματος -48 dbm ενώ η συσκευή χειρός αναφέρει ότι η συσκευή πεδίου έχει ισχύ σήματος -45 dbm. Έτσι ο διαχειριστής δικτύου επιλέγει τα κατάλληλα ζεύγη κάνοντας συγκρίσεις και επιπλέον μπορεί να υπολογίσει τη θέση της συσκευής χειρός.

3.2.1.4 Πύλη (gateway) (GW)

Είναι μία κεντρική συσκευή στην οποία συνδέονται οι άλλες συσκευές για να επικοινωνήσουν μεταξύ τους. Η πύλη δημιουργεί μία κοινή σύνδεση ανάμεσα σε μία εφαρμογή φιλοξενητή (host application), στον διαχειριστή δικτύου (NM) (Network Manager), στον διαχειριστή ασφαλείας (SM)(Security Manager), και στις συσκευές πεδίου (FDs) (field devices) μέσα στο δίκτυο πλέγματος (mesh network). Η πύλη (gateway) συνδέεται στο δίκτυο WirelessHART μέσω των σημείων πρόσβασης (Access Points).



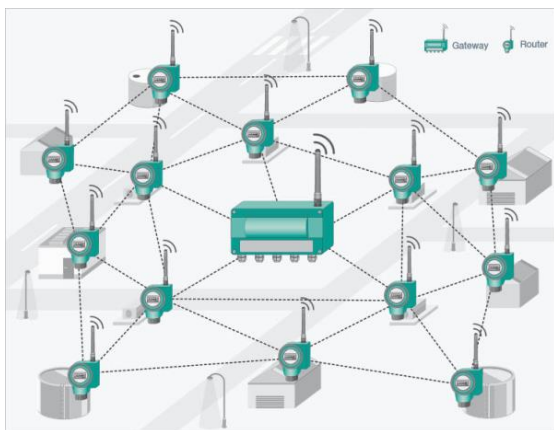
Εικόνα 50. Πύλες (Gateways) του WirelessHART διάφορων κατασκευαστών.

Επιπλέον, όταν υπάρχει ήδη ένα διαφορετικό δίκτυο αυτοματισμού σε μία βιομηχανική εγκατάσταση (plant automation network), τότε η πύλη GW, (gateway) συνδέει το δίκτυο WirelessHART με το δίκτυο αυτοματισμού της βιομηχανικής εγκατάστασης και επιτρέπει να γίνεται ανταλλαγή δεδομένων

μεταξύ των δύο δικτύων. Οι πύλες (Gateways) επιτρέπουν την ενοποίηση διαφορετικών συστημάτων και έτσι μπορούν να χρησιμοποιηθούν για τη σύνδεση ενός δικτύου WirelessHART με διαφορετικά συστήματα. Π.χ. μπορούν να συνδεθούν σε πολυπλέκτη HART (multiplexer) και σε δίκτυα διαύλου PROFINET ή PROFIBUS-DP.

Η πύλη (gateway) (GW) είναι η διεπαφή (interface) ανάμεσα στο ασύρματο δίκτυο (wireless network) και στις εφαρμογές φιλοξενητή (host applications). Η πύλη (gateway) επίσης λειτουργεί ως μία γέφυρα (bridge) ανάμεσα στο δίκτυο (network) και στο διαχειριστή δικτύου (network manager) και έτσι παρέχει πρόσβαση στο διαχειριστή δικτύου.

Ο διαχειριστής δικτύου, όπως αναφέρεται παρακάτω, είναι η κεντρική συσκευή που ελέγχει τη σύνδεση (join), τη ρύθμιση (configuration), τη συντήρηση και όλα τα καθήκοντα διαχείρισης στο δίκτυο. [8]



Εικόνα 51. Δίκτυο πλέγματος (Mesh network) WirelessHART. Οι συσκευές πεδίου FD (Field Devices) τοποθετούνται σε διάφορα σημεία της εγκατάστασης και η πύλη GW (Gateway) επικοινωνεί ασύρματα με όλες τις συσκευές. Πηγή: Pepperl+Fuchs

Η πύλη (Gateway) όπως περιεγράφηκε παραπάνω, είναι μία μεμονωμένη συσκευή. Σε πολλές περιπτώσεις, όμως, με τον όρο πύλη (Gateway) εννοείται γενικότερα ένα σύνολο συσκευών, δηλαδή ένα μεγαλύτερο κουτί μέσα στο οποίο εκτός από την μεμονωμένη συσκευή πύλη (Gateway), βρίσκονται και άλλες συσκευές μαζί, που συνεργάζονται με την πύλη και αφορούν την κεντρική διαχείριση του δικτύου. Αυτές οι συσκευές είναι οι εξής: Σημείο Πρόσβασης (Access Point), Διαχειριστής δικτύου (Network Manager), Διαχειριστής ασφαλείας (Security Manager), Ιδεατή Πύλη (Virtual Gateway) και διεπαφή φιλοξενητή (host interface). Τότε θεωρείται ότι όλες αυτές οι μονάδες είναι τα 5 στοιχεία μίας ενιαίας οντότητας που λέγεται πύλη. Αυτή είναι μία τάση ενοποίησης που συγκεντρώνει όλες τις κεντρικές συσκευές στην ίδια φυσική θέση στη βιομηχανική εγκατάσταση και ενδέχεται να υπάρχουν και ορισμένα κοινά μέρη υλικού μεταξύ τους. Σε άλλες περιπτώσεις, όμως, αυτές οι 5 μονάδες, είναι τελείως ξεχωριστές συσκευές με διαφορετικό hardware που βρίσκονται κατανομημένες σε διαφορετικές θέσεις μέσα στο δίκτυο και δεν βρίσκονται όλες μαζί μέσα στο ίδιο κουτί. Σε αυτή την εργασία, θεωρήθηκε ότι οι 5 συσκευές είναι διαφορετικές και ανεξάρτητες μεταξύ τους και για αυτό παρουσιάζονται ξεχωριστά ή κάθε μία στις παρακάτω παραγράφους.

3.2.1.5 Διαχειριστής δικτύου (network manager)(NM).

Είναι μία κεντρική εφαρμογή (application) σημαντική για όλο το δίκτυο WirelessHART και διαχειρίζεται συνολικά το δίκτυο και τις συσκευές του. Ευθύνεται για τις εξής λειτουργίες:

- α) δημιουργία και ρύθμιση του δικτύου,
- β) διαμόρφωση τοπολογίας του δικτύου,
- γ) παρακολούθηση δικτύου
- δ) την επέκταση του δικτύου,
- ε) καθορίζει την επικοινωνία με χρονοπρογραμματισμό (scheduling communication) ανάμεσα σε όλες τις συσκευές (devices), ορίζει και αναθέτει τις χρονικές σχισμές επικοινωνίας (communication slots) και τα κανάλια για όλους τους συμμετέχοντες (participants) στην επικοινωνία.
- στ) διαχειρίζεται τη δρομολόγηση (routing) στο δίκτυο χρησιμοποιώντας πίνακες δρομολόγησης (routing tables),
- ζ) την παρακολούθηση και την αναφορά της υγείας του δικτύου.



Εικόνα 52. Μία συσκευή Διαχειριστής Δικτύου (Network Manager) (NM) του WirelessHART. Κατασκευαστής: dust. Πηγή: <http://www.digikey.com/>

Άλλο καθήκον που εκτελεί ο διαχειριστής δικτύου είναι να διανέμει την ταυτότητα δικτύου (network identity) και να δημοσιοποιεί την ύπαρξή του.

Επίσης διανέμει τα κλειδιά σύνδεσης Join Key και Network Key που παραλαμβάνει από τον διαχειριστή ασφαλείας.

Ο διαχειριστής δικτύου (network manager) παρακολουθεί την τοπολογία του δικτύου και αναθέτει στα υπερπλαίσια (superframes) τις μεταδόσεις πακέτων δεδομένων από τους κόμβους. Παρέχει σε κάθε κόμβο μόνο τις πληροφορίες που χρειάζεται ο κόμβος για να μεταδώσει επιτυχώς ένα πακέτο δεδομένων. Για να επιτύχει το στόχο του ο διαχειριστής δικτύου (network manager) λαμβάνει περιοδικά ενημερώσεις (updates) από κάθε κόμβο σχετικά με τους γείτονες του, την ισχύ του σήματος (signal strength), και για δεδομένα που πρέπει να στείλει ή να λάβει ο κόμβος. Ο διαχειριστής δικτύου υπολογίζει την τοπολογία και το χρονοπρογραμματισμό υπερπλαisiών

(superframe schedule), καθορίζει ποιος κόμβος θα στείλει δεδομένα ποιος κόμβος θα ακούσει για κάθε χρονική σχισμή (time-slot). Μετά στέλνει σε κάθε συσκευή ένα μέρος του πίνακα του υπερπλαισίου (superframe table) που χρειάζεται η συσκευή.

Περισσότεροι διαχειριστές δικτύου (redundant network managers) υποστηρίζονται στα δίκτυα WirelessHART, αλλά πάντα πρέπει να υπάρχει μόνο ένας διαχειριστής δικτύου (Network Manager) που είναι ενεργός για κάθε ένα δίκτυο WirelessHART.

3.2.1.6 Διαχειριστής ασφάλειας Security Manager (SM)

Είναι μία εφαρμογή που ευθύνεται για την ασφάλεια στο δίκτυο. [24]

Ο διαχειριστής ασφαλείας Security Manager είναι υπεύθυνος για να διαχειρίζεται τις ανάγκες για κρυπτογράφηση και για πιστοποίηση των συσκευών που συνδέονται στο δίκτυο.

Διαχειρίζεται τα κλειδιά (keys) δηλαδή τους κωδικούς που χρησιμοποιούνται από τις συσκευές για να συνδεθούν στο δίκτυο. Τα κλειδιά είναι τα κλειδιά σύνδεσης (join keys), τα κλειδιά δικτύου (network keys) τα κλειδιά συνεδρίας (session keys). Ο διαχειριστής ασφαλείας είναι υπεύθυνος για να δημιουργεί, να αποθηκεύει και να διαχειρίζεται τα παραπάνω κλειδιά. Τα κλειδιά σύνδεσης (Join Keys), τα κλειδιά δικτύου (network keys) και τα κλειδιά συνεδριών (session keys) παρέχονται στον διαχειριστή δικτύου (Network Manager) NM, και τα κλειδιά σύνδεσης (join keys) παρέχονται στις δικτυακές συσκευές. Αυτά τα κλειδιά χρησιμοποιούνται για πιστοποίηση συσκευών και για κρυπτογράφηση των δεδομένων μέσα στο δίκτυο.

Ο διαχειριστής ασφαλείας (security manager) διαχειρίζεται τα κλειδιά (keys) χρησιμοποιείται και στο επίπεδο δικτύου (network layer) και στο επίπεδο σύνδεσης δεδομένων (data link layer). Ο διαχειριστής ασφαλείας μπορεί να είναι και ενσωματωμένος στη ίδια συσκευή που είναι και η πύλη (gateway) και μπορεί να εξυπηρετήσει περισσότερα δίκτυα WirelessHART. Υπάρχει μόνο ένας διαχειριστής ασφαλείας που σχετίζεται με ένα δίκτυο WirelessHART, αλλά ο διαχειριστής ασφαλείας μπορεί να είναι μία κεντρική λειτουργία σε ένα δίκτυο αυτοματισμού μίας εγκατάστασης και να υποστηρίζει περισσότερα δίκτυα WirelessHART και, σε κάποιες περιπτώσεις υποστηρίζει και άλλα δίκτυα ή εφαρμογές.

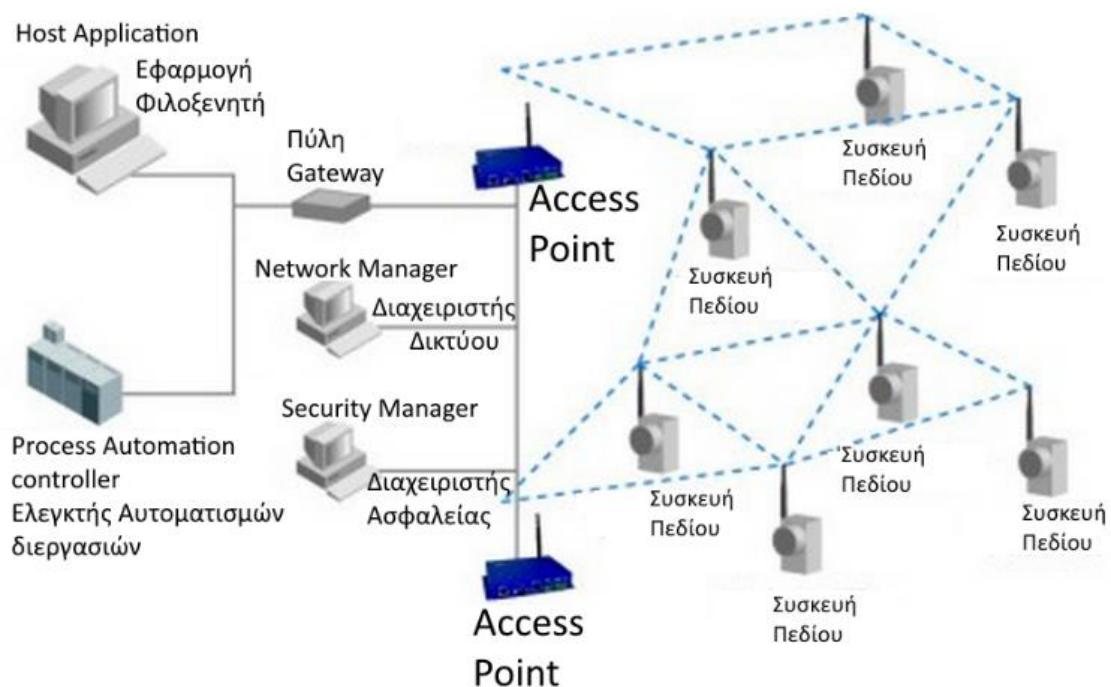
Ενοποίηση Πύλης (GW), Διαχειριστή Δικτύου (NM) και Διαχειριστή Ασφαλείας (SM) σε μία συσκευή

Σε κάποιες υλοποιήσεις του δικτύου WirelessHART, συχνά τοποθετούνται μαζί σε μία συσκευή η πύλη (gateway), ο διαχειριστής δικτύου (network manager) και ο διαχειριστής ασφαλείας (security manager), είτε ως 3 ξεχωριστές μονάδες στο ίδιο κουτί, είτε ως μία ενιαία συσκευή με ενσωματωμένες λειτουργίες αυτών των 3 μονάδων. Οι κατασκευαστές συνηθίζουν να αποκαλούν την ενιαία συσκευή είτε πύλη (gateway) είτε διαχειριστή δικτύου (network manager). Υπάρχουν και άλλες περιπτώσεις όμως, όπου απαιτείται να υπάρχει πλεονασμός και εκτεταμένη κάλυψη μιας περιοχής με συσκευές WirelessHART. Τότε το πρότυπο επιτρέπει να χρησιμοποιούνται πολλαπλές πύλες (gateways) που τις διαχειρίζεται ένας μόνο διαχειριστής δικτύου (network manager) και ένας μόνο διαχειριστής ασφαλείας (security manager).

3.2.1.7 Σημείο πρόσβασης (Access point) (AP)

Συνδέει τις συσκευές πεδίου (FDs) (Field Devices) που βρίσκονται στο δίκτυο WirelessHART (WH) με μία πύλη (gateway)(GW). Το σημείο πρόσβασης (Access Point)(AP) κάνει μόνο μία εργασία: λαμβάνει και στέλνει τα μηνύματα (messages) από το δίκτυο WirelessHART προς την πύλη (Gateway) και λαμβάνει μηνύματα από την πύλη τα οποία τα στέλνει στο δίκτυο WirelessHART.

Τα σημεία πρόσβασης συχνά χωρίζονται σε Mesh AP και σε Root AP. Τα σημεία πρόσβασης (access points) (AP) είναι οι δρομολογητές ανάμεσα στην πύλη (gateway) (GW) και όλες τις άλλες συσκευές. Η επικοινωνία ανάμεσα στο σημείο πρόσβασης (access point) (AP) και την πύλη (gateway) (GW) θεωρείται ότι είναι πολύ ισχυρή (robust) και στην ιδανική περίπτωση, θεωρείται ότι δεν καταναλώνει καθόλου εύρος ζώνης ασύρματου δικτύου (wireless bandwidth). Αυτό όμως στην πράξη εξαρτάται από τα φυσικά χαρακτηριστικά και τις προδιαγραφές αυτών των συγκεκριμένων συσκευών που είναι συνδεδεμένες στο δίκτυο και έτσι ενδέχεται στην πραγματικότητα να καταναλώνεται κάποιο εύρος ζώνης.



Εικόνα 53. Τα σημεία πρόσβασης Access Points (AP) συνδέουν τις συσκευές πεδίου με μία πύλη (Gateway).

Εκτός από τα παραπάνω 7 είδη συσκευών στο δίκτυο WirelessHART, υπάρχουν και επιπλέον μονάδες που είναι και αυτές μέρη του συστήματος. Αυτές είναι:

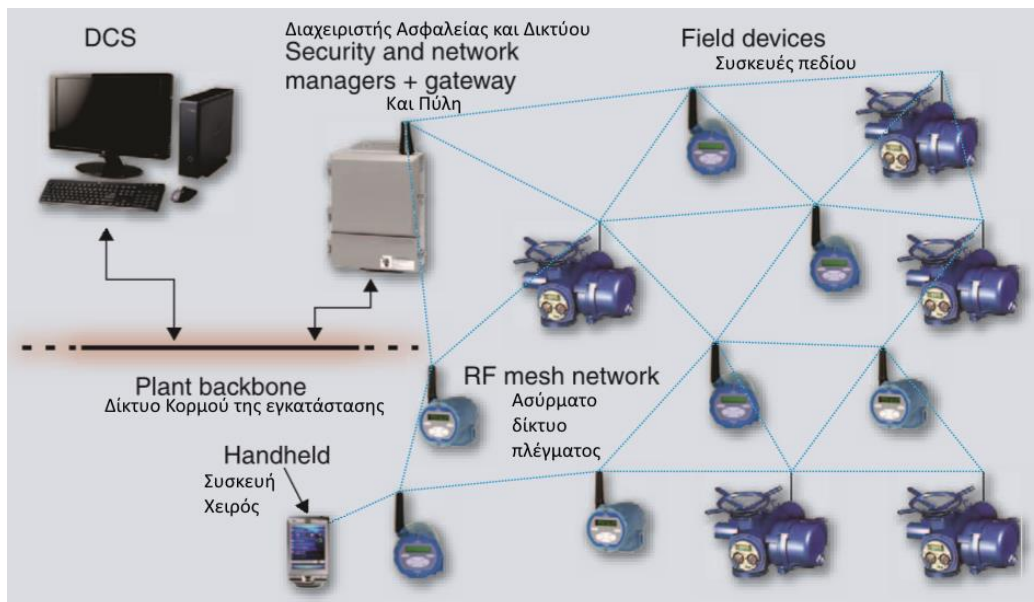
3.2.1.8 Δίκτυο Αυτοματισμού της εγκατάστασης (plant automation network)

Συχνά η βιομηχανική εγκατάσταση περιλαμβάνει ένα ξεχωριστό δίκτυο αυτοματισμού που είναι ένα φυσικό δίκτυο κορμού της εγκατάστασης (Plant backbone) και είναι διαφορετικό και ανεξάρτητο από το δίκτυο WirelessHART.

Το δίκτυο αυτοματισμού της εγκατάστασης (plant automation network) μπορεί να είναι:

- 1) ένα δίκτυο TCP-based network
- 2) ένα απομακρυσμένο σύστημα εισόδου/εξόδου (IO system)
- 3) ένας διάυλος (bus) όπως είναι το PROFIBUS DP.

Το δίκτυο αυτοματισμού της εγκατάστασης, είναι ένα εξωτερικό δίκτυο που συνδέεται με το δίκτυο WirelessHART μέσω της πύλης (Gateway).



Εικόνα 54. Δίκτυο πλέγματος (Mesh network) WirelessHART. Συνδέεται μέσω της πύλης (Gateway) στο δίκτυο αυτοματισμού της εγκατάστασης που μπορεί να είναι ένα δίκτυο κορμού της εγκατάστασης. Η πύλη, ο διαχειριστής δικτύου και ο διαχειριστής ασφαλείας μπορεί να βρίσκονται στο ίδιο κουτί.

3.2.1.9 Ο φιλοξενητής (Host)

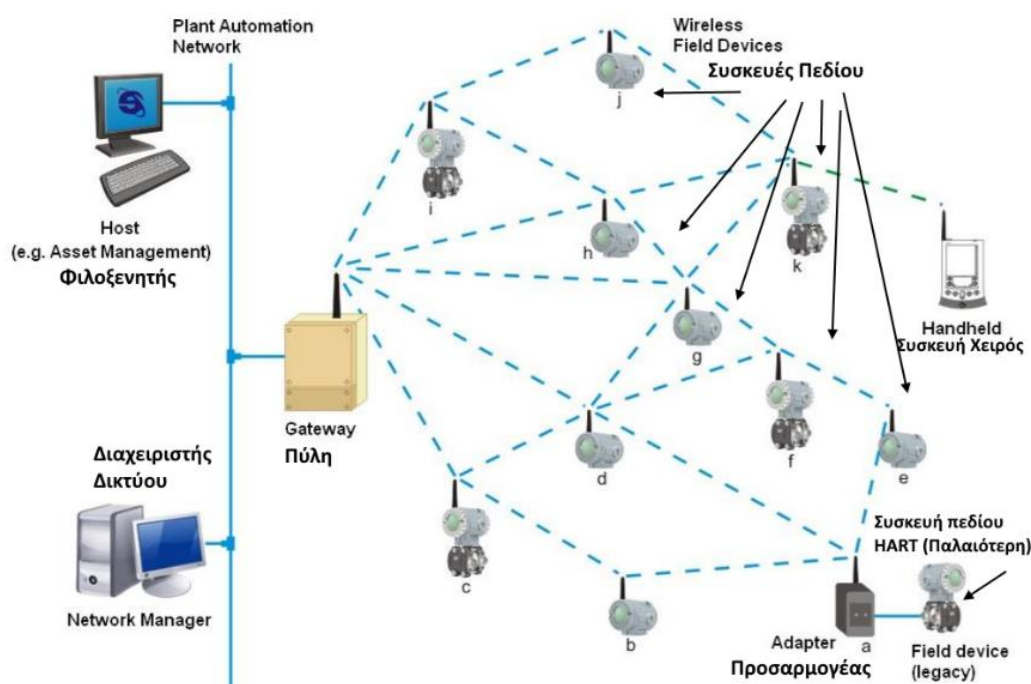
Είναι ένας υπολογιστής workstation που επιτρέπει να γίνονται αλληλεπιδράσεις με τη διεργασία (process). Στον φιλοξενητή εκτελούνται διάφορες εφαρμογές που λαμβάνουν τα δεδομένα από το WirelessHART μέσω της πύλης (Gateway). Ο φιλοξενητής μπορεί να χρησιμοποιήσει τα δεδομένα από το WirelessHART σε άλλα ενσύρματα δίκτυα. Τα δεδομένα από τα όργανα μετρήσεων που υπάρχουν στο δίκτυο WirelessHART συλλέγονται μέσω της πύλης (gateway) και μεταφέρονται από την πύλη στον φιλοξενητή.

Ο φιλοξενητής είναι υπολογιστής που χρησιμοποιεί διάφορα πρωτόκολλα για να συνδέεται στο δίκτυο της βιομηχανικής εγκατάστασης ή σε άλλα διαφορετικά φυσικά δίκτυα, όπως είναι μεταξύ άλλων τα Profibus και το Ethernet υψηλών ταχυτήτων (High Speed Ethernet)(HSE).

Η πύλη (Gateway) συνδέεται με τον φιλοξενητή, μέσω της διεπαφής φιλοξενητή (Host interface). Η διεπαφή φιλοξενητή τροφοδοτείται από τα δεδομένα που βρίσκονται αποθηκευμένα στην κρυφή μνήμη cache της πύλης. Στη συνέχεια η διεπαφή φιλοξενητή, παρέχει τα δεδομένα αυτά σε άλλα μεμονωμένα δίκτυα. Έτσι επιτυγχάνεται η σύνδεση ενός ασύρματου δικτύου WirelessHART με διαφορετικά ενσύρματα δίκτυα.

3.2.1.10 Εφαρμογές του φιλοξενητή (Host applications)

Οι εφαρμογές χρηστών (User applications) συνδέονται στο δίκτυο κορμού (backbone network) της βιομηχανίας (industry) και επικοινωνούν με τις συσκευές πεδίου (Field Devices) που είναι οι κόμβοι του δικτύου WirelessHART (WH). Οι εφαρμογές φιλοξενητή (Host applications) μπορούν να επεξεργάζονται τα δεδομένα ελέγχου (control data) και τα δεδομένα διεργασιών (process data). Η πύλη (Gateway) είναι το σημείο σύνδεσης (connection point) ανάμεσα στις εφαρμογές φιλοξενητή (host applications) και στο δίκτυο WirelessHART.



Εικόνα 55. Δίκτυο πλέγματος (Mesh network) WirelessHART. Οι εφαρμογές φιλοξενητή (host applications) συνδέονται μέσω της πύλης (gateway) στο δίκτυο WirelessHART. Πηγή: Smar (www.smar.com).

Στην επόμενη παράγραφο 3.2.2, που έχει τίτλο δικτυακές συσκευές, περιγράφονται με περισσότερες λεπτομέρειες οι ίδιες φυσικές συσκευές που αναφέρθηκαν παραπάνω. Παρουσιάζονται αναλυτικότερα τα χαρακτηριστικά τους, οι λειτουργίες τους και

διασαφηνίζονται επιπρόσθετα τεχνικά ζητήματα, που δεν ήταν δυνατόν να αναφερθούν στην συνοπτική παρουσίαση που έγινε στις προηγούμενες παραγράφους.

3.2.2 Αναλυτική περιγραφή για τις δικτυακές συσκευές (Network Devices)

Στην προηγούμενη παράγραφο 3.2.1, έγινε μία συνοπτική περιγραφή των συσκευών πεδίου (field devices). Σε αυτή την παράγραφο 3.2.2, περιγράφονται οι ίδιες συσκευές πεδίου αναλυτικότερα και παρουσιάζονται εδώ πιο πολλές πληροφορίες. Επιπλέον, στις παραγράφους που ακολουθούν, γίνεται λεπτομερής παρουσίαση για κάθε μία από τις προαναφερθείσες κατηγορίες συσκευών.

Όλες οι συσκευές που συνδέονται άμεσα στο ασύρματο δίκτυο WirelessHART ανήκουν στον τύπο των δικτυακών συσκευών (Network Device). Οι συσκευές που αναφέρθηκαν προηγουμένως ανήκουν στη γενική κατηγορία των δικτυακών συσκευών.

Οι τύποι δικτυακών συσκευών (Network Device types), όπως είδαμε, περιλαμβάνουν:

- α) συσκευές πεδίου (Field Devices)(FD),
- β) προσαρμογείς (Adaptors ή adapters),
- γ) Δρομολογητές (Routers),
- δ) σημεία πρόσβασης (Access Points) (AP)
- ε) συσκευές χειρός (Handheld Devices) ή (Handheld Communicators)(HHC)

Όλες οι δικτυακές συσκευές (Network Devices) εκπέμπουν (transmit) πακέτα δεδομένων WirelessHART , λαμβάνουν πακέτα WirelessHART και εκτελούν τις βασικές λειτουργίες που απαιτούνται για να υποστηρίξουν τη διαμόρφωση του δικτύου (network formation) και τη συντήρηση (maintenance). Όλες οι δικτυακές συσκευές (Network Devices) πρέπει να μπορούν να δημιουργούν πακέτα ως πηγές (source) και να καταστρέφουν (sink) πακέτα και να είναι ικανές να δρομολογούν πακέτα για λογαριασμό άλλων συσκευών του δικτύου (devices).

Η πηγή δηλαδή, είναι ένας κόμβος αισθητήρας (sensor node) του ασύρματου δικτύου αισθητήρων, που δημιουργεί δεδομένα τα οποία είναι τιμές μετρήσεων που λαμβάνει.

Ενώ η βύθιση (sink) (μεταφορικά) είναι ο κεντρικός κόμβος του δικτύου που συγκεντρώνει τα δεδομένα από όλους τους κόμβους του δικτύου, για να τα στείλει σε μία κεντρική περιοχή. Για αυτό, μεταφορικά, όλοι οι κόμβοι του δικτύου λέγονται «πηγές» (sources) ενώ ο κεντρικός κόμβος λέγεται «sink» (βύθιση).

Στη συνέχεια, παρουσιάζεται μία αναλυτική περιγραφή για τις συσκευές πεδίου ενώ στις επόμενες παραγράφους, που ακολουθούν, γίνεται περιγραφή για τους υπόλοιπους τύπους συσκευών.



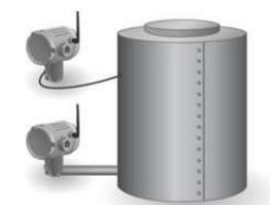
Εικόνα 56. Συσκευές Πεδίου (Field Devices) (FD) του δικτύου WirelessHART από διάφορους κατασκευαστές.

3.2.2.1 Αναλυτική περιγραφή για τις συσκευές πεδίου (Field Devices) (FD)

Συνδέονται στη διεργασία (Process) και χαρακτηρίζουν ή ελέγχουν τη διεργασία (Process). Κάθε συσκευή πεδίου είναι ένας δημιουργός (producer) των πακέτων δεδομένων WirelessHART και ένας καταναλωτής (consumer) των πακέτων δεδομένων WirelessHART. Οι συσκευές πεδίου πρέπει να είναι ικανές να δρομολογούν πακέτα για λογαριασμό άλλων δικτυακών συσκευών (Network Devices).

Οι συσκευές πεδίου (Field devices) (FD) χρησιμοποιούνται σε ένα ευρύ πεδίο εφαρμογών όπως είναι:

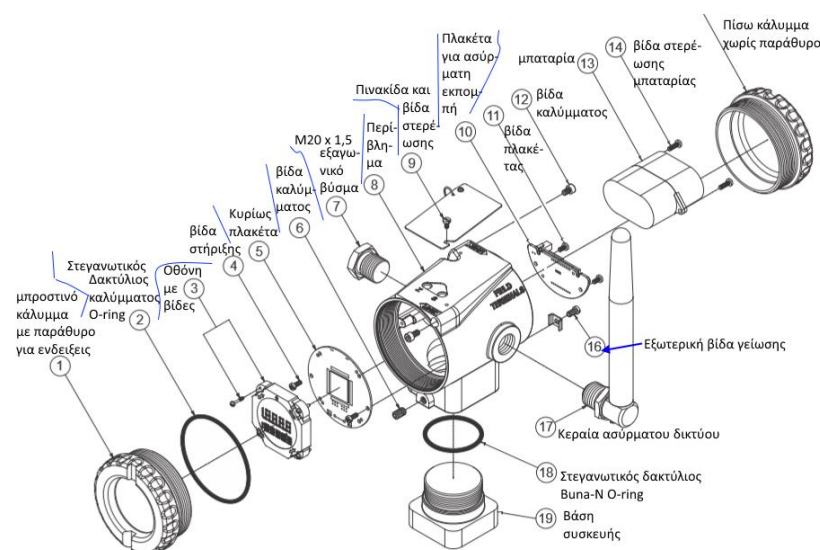
η παρακολούθηση και ο έλεγχος στάθμης υγρών που βρίσκονται σε δεξαμενές (tank levels),



Εικόνα 57 Οι συσκευές πεδίου χρησιμοποιούνται για έλεγχο στάθμης υγρών σε δεξαμενές.

η παρακολούθηση των επιπέδων εκπομπής αερίων (emission levels) και ποιότητας νερού, η παρακολούθηση της υγείας εξοπλισμού.

Οι συσκευές πεδίου (Field devices) (FD) μετρούν θερμοκρασίες (temperatures), αγωγιμότητα (conductivity), πιέσεις (pressures), ροές (flows), pH, πυκνότητα (density), σύνθεση (composition), επίπεδα εκπομπής αερίου (emission levels), κραδασμούς (vibration), βαθμό διάβρωσης κ.α.



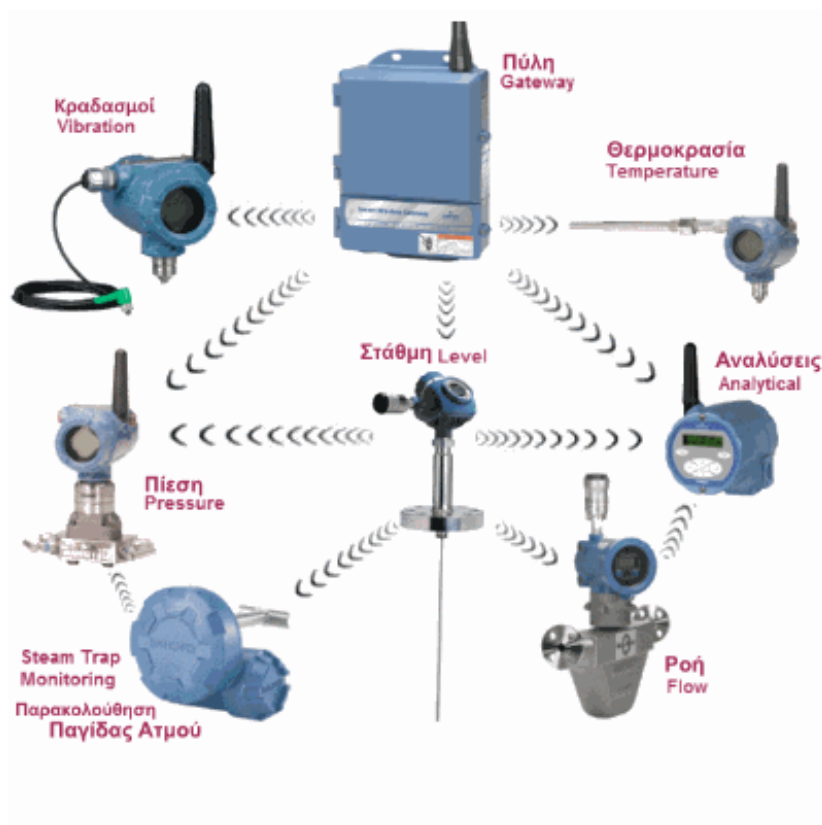
Εικόνα 58 Σχεδιάγραμμα (exploded diagram) που δείχνει μερικά κομμάτια από τα οποία αποτελείται μια συσκευή πεδίου WirelessHART. πηγή:smar (www.smar.com).



Εικόνα 59 Αντίστοιχη εικόνα (exploded view) όπου φαίνονται κομμάτια από τα οποία αποτελείται μια συσκευή πεδίου HART. πηγή:Honeywell.

3.2.2.2 Μέτρηση φυσικών μεγεθών από συσκευές πεδίου

Υπάρχουν πολλές διαφορετικές μέθοδοι μέτρησης για τις φυσικές ιδιότητες των υγρών και των αερίων που χρησιμοποιούνται σε βιομηχανικές μονάδες. Κάποιες μπορεί να είναι απλές μέθοδοι, όπως πχ. η τοποθέτηση ενός πλωτήρα (φλοτέρ) στην επιφάνεια ενός υγρού, για έλεγχο της στάθμης του υγρού, ενώ άλλες να είναι περίπλοκες μέθοδοι όπως αυτές που βασίζονται σε χρήση λέιζερ, υπερήχων, ή μαγνητικών πεδίων για τον έλεγχο της στάθμης του υγρού. Σε αυτή την εργασία δεν είναι δυνατόν να συμπεριλαμβάνονται αναλυτικά όλες οι μέθοδοι, οπότε αρκετές δεν περιγράφονται.



Εικόνα 60 Οι συσκευές πεδίου WirelessHART μετρούν διάφορα φυσικά μεγέθη, όπως είναι ροή, θερμοκρασία, πίεση, στάθμη, κραδασμούς.

Μια γενική αναφορά για συσκευές πεδίου που μετρούν ορισμένα φυσικά μεγέθη, γίνεται ενδεικτικά παρακάτω.

α) Πίεση (Pressure)

Η πίεση P είναι το αποτέλεσμα εφαρμογής μίας δύναμης F σε μία επιφάνεια με εμβαδό S .

Η πίεση P ορίζεται ως το πηλίκο της ασκούμενης δύναμης F που δρα σε μία επιφάνεια δια του εμβαδού S της επιφάνειας αυτής.

Δηλαδή $P=F/S$.

Η μέτρηση της πίεσης διακρίνεται σε 3 είδη:

1. Πραγματική ή Μανομετρική πίεση (gauge pressure)

Η πραγματική ή μανομετρική πίεση (gauge pressure) μετριέται έχοντας ως πίεση αναφοράς την ατμοσφαιρική πίεση. Για να δηλωθεί ότι η ατμοσφαιρική πίεση θεωρείται ως πίεση αναφοράς, δίπλα στις μονάδες μέτρησης μπαίνει και η λέξη Gauge ή το γράμμα “g”. Παράδειγμα: Pascals Gauge (Pa g) ή Pound per Square Inch Gauge (Psig). [25]

2. Απόλυτη πίεση (absolute pressure)

Η απόλυτη πίεση (Absolute Pressure) μετριέται έχοντας ως πίεση αναφοράς το κενό (Vacuum). Το απόλυτο κενό δεν μπορεί να υπάρξει. Επομένως το κενό δεν είναι ακριβώς κενό αλλά είναι μία πίεση πιο χαμηλή από την ατμοσφαιρική πίεση και αποκαλείται κενό. Μονάδες μέτρησης για το κενό είναι οι μονάδες Torr (Τορρικέλι) όπου $1 \text{ Torr}=133,322 \text{ Pascal}$. Επίσης το κενό μετριέται και σε μονάδες mmHg (χιλιοστά υδραργύρου).

Σε μερικές εφαρμογές, όπως για παράδειγμα σε αέρια που αλλάζει ο όγκος τους με την ατμοσφαιρική πίεση, δεν είναι επιθυμητό να υπολογιστεί η πίεση έχοντας ως αναφορά την ατμοσφαιρική πίεση.

Το κενό (vacuum) είναι η πίεση που απομένει όταν αφαιρεθεί η ατμοσφαιρική πίεση και η πραγματική (μανομετρική) πίεση. Αυτό μπορεί να γίνει με μία αντλία κενού (vacuum pump). Το ιδανικό κενό θα ήταν να μην υπήρχε καθόλου πίεση, αλλά στην πράξη πάντα παραμένει μία μικρή πίεση.

Η απόλυτη πίεση (absolute pressure) ισούται με το άθροισμα της πραγματικής πίεσης (gauge pressure) και της ατμοσφαιρικής πίεσης.

Για να μετρηθεί η απόλυτη πίεση οι αισθητήρες, οι πομποί και οι μετατροπείς (transducers) μετρούν τη διαφορά ανάμεσα στην πίεση αναφοράς που είναι το κενό (reference vacuum) και στην πίεση που μετριέται. [25]

Δεν συνηθίζεται να μετρούν ξεχωριστά την πραγματική πίεση (gauge pressure) και ξεχωριστά την ατμοσφαιρική πίεση και να τις αθροίζουν μετά.

3. Διαφορική πίεση DP (Differential Pressure)

Η διαφορική πίεση (Differential Pressure) (DP) δεν μετριέται έχοντας ως πίεση αναφοράς μία συγκεκριμένη πίεση, αλλά μετράει δύο πιέσεις P_1 , P_2 και ενδιαφέρεται για τη διαφορά μεταξύ των δύο πιέσεων. [25]

Οι πομποί διαφορικής πίεσης (Differential Pressure Transmitters) δεν έχουν την απαίτηση να υπάρχει μία σταθερή πίεση αναφοράς. Μπορεί να γίνεται αύξηση ή μείωση της διαφορικής πίεσης στη διάρκεια του χρόνου. Μια αύξηση της διαφορικής πίεσης ενδέχεται να οφείλεται στο γεγονός ότι αυξήθηκε η μία πίεση P_1 , ή μειώθηκε η άλλη πίεση P_2 .

Ομοίως, μία μείωση στη διαφορική πίεση μπορεί να συμβεί αν η P_2 αυξηθεί ή αν η P_1 μειωθεί.



Εικόνα 61. μετρητές διαφορικής πίεσης.

β) Κραδασμοί (Vibration)

Οι μετρητές των κραδασμών λέγονται vibrometres.

Η μέτρηση βασίζεται σε ένα από τα 3 μεγέθη που χαρακτηρίζουν τον κραδασμό. Αυτά είναι:

1. Η μετατόπιση.

Μία μέθοδος για να μετρηθεί η μετατόπιση είναι ο αισθητήρας δινορρευμάτων (eddy current). Ο αισθητήρας αυτός είναι ένας ηλεκτρομαγνήτης που είναι τοποθετημένος κοντά στην επιφάνεια που κινείται με κραδασμούς, αλλά δεν έρχεται ποτέ σε επαφή με την επιφάνεια. Η κίνηση της επιφάνειας γίνεται αισθητή στον ηλεκτρομαγνήτη ως αλλαγές στην αυτεπαγωγή του. Με βάση αυτές τις αλλαγές μετριέται η μετατόπιση της επιφάνειας. Όμως ο ηλεκτρομαγνήτης δεν μπορεί να μετρήσει πολύ μικρές μετατοπίσεις που συμβαίνουν σε υψηλές συχνότητες, διότι έχει μικρή δυναμική περιοχή, που είναι ο λόγος της μέγιστης τιμής προς την ελάχιστη τιμή που μπορεί να μετρηθεί.

2. Η ταχύτητα

Η ταχύτητα των κραδασμών μπορεί να μετρηθεί με αισθητήρες ταχύτητας ή με ψηφιακούς μετρητές κραδασμών (Vibrometers) που χρησιμοποιούν λέιζερ (Digital Laser Doppler Vibrometers).

Ο αισθητήρας ταχύτητας αποτελείται από έναν μαγνήτη και από ένα κινούμενο πηνίο που είναι τυλιγμένο γύρω από τον μαγνήτη, με τέτοιο τρόπο ώστε να μπορεί να μετακινείται ως προς το μαγνήτη. Ο αισθητήρας προσαρμόζεται πάνω στην επιφάνεια προς μέτρηση, η οποία κινείται από τον κραδασμό. Κατά την κίνηση της επιφάνειας, λόγω της αδράνειας το τύλιγμα θα έχει μία σχετική κίνηση ως προς το μαγνήτη. Λόγω της επαγωγής καθώς το πηνίο κινείται προς το μαγνήτη, στα άκρα του πηνίου αναπτύσσεται μία τάση που είναι ανάλογη της ταχύτητας της κίνησης. Από αυτή την τάση μετριέται η ταχύτητα.

Αυτή η μέθοδος όμως έχει μειονεκτήματα διότι οι αισθητήρες είναι ευαίσθητοι σε άλλα μαγνητικά πεδία, και έχουν πολλά κινούμενα μέρη που δέχονται καταπονήσεις και φθορές.

3. Η επιτάχυνση

Οι αισθητήρες επιτάχυνσης λέγονται επιταχυνσιόμετρα (accelerometers) και χρησιμοποιούν το πιεζοηλεκτρικό φαινόμενο. Πάνω στην επιφάνεια προς μέτρηση, που κινείται από τον κραδασμό, προσαρμόζεται μία διαφορετική μάζα που συνδέεται με έναν πιεζοηλεκτρικό κρύσταλλο. Τότε αυτή η διαφορετική μάζα, που προσαρμόστηκε, θα κινείται με την ίδια επιτάχυνση όπως και η επιφάνεια προς μέτρηση που κινείται κατά τη

διάρκεια του κραδασμού. Η μάζα τότε ασκεί μία δύναμη ανάλογη της επιτάχυνσης. Η δύναμη αυτή μεταφέρεται στον πιεζοηλεκτρικό κρύσταλλο και προκαλείται ανάπτυξη ενός ηλεκτρικού φορτίου. Αυτό το ηλεκτρικό φορτίο μετριέται με ηλεκτρονικό όργανο μέτρησης. Με βάση το ηλεκτρικό φορτίο μετριέται η επιτάχυνση.

Τα επιταχυνσιόμετρα προτιμώνται στη μέτρηση κραδασμών διότι έχουν περισσότερα πλεονεκτήματα από τις άλλες μεθόδους.

γ) Ροή (Flow)

Για τη μέτρηση ροής μάζας χρησιμοποιούνται ροόμετρα μάζας με τη μέθοδο της δύναμης Coriolis. Τα ροόμετρα αυτά λέγονται Coriolis mass flowmeters.



Εικόνα 62. Ροόμετρο Coriolis για μέτρηση ροής αερίου. Κατασκευαστής: Emerson

Η δύναμη Coriolis είναι μία αδρανειακή δύναμη που εμφανίζεται σε μία κίνηση περιστροφής. Σε μία κίνηση περιστροφής, όταν μία μάζα κινείται προς το κέντρο περιστροφής, ή απομακρύνεται από το κέντρο περιστροφής, εμφανίζεται, από επιτάχυνση, η δύναμη Coriolis.

Για παράδειγμα, έστω ένας εύκαμπτος σωλήνας, όπως το λάστιχο ποτίσματος, που είναι λυγισμένος και σχηματίζει βρόχο U και μέσα από το σωλήνα περνάει νερό. Έστω ότι κάποιος ταλαντώνει το σωλήνα με μία εξαναγκασμένη ταλάντωση που ασκείται και στα δύο άκρα του σωλήνα. Τότε, επειδή το νερό στο ένα άκρο του σωλήνα κινείται προς το κέντρο του σωλήνα, ενώ στο άλλο άκρο κινείται μακριά από το κέντρο του σωλήνα, δημιουργούνται αντίθετες δυνάμεις και προκαλούν μία συστροφή (twist) στο σωλήνα.

Στο ροόμετρο μάζας Coriolis, στο σωλήνα προκαλείται μία δόνηση για να γίνει εξαναγκασμένη ταλάντωση. Μέσα στο σωλήνα υπάρχει ροή ενός υγρού. Η ποσότητα της συστροφής του σωλήνα είναι ανάλογη με τη ροή του υγρού που διέρχεται μέσα από το σωλήνα. Χρησιμοποιούνται αισθητήρες στο ροόμετρο και ένας πομπός (transmitter) για να μετρήσουν τη συστροφή και να παράγουν ένα γραμμικό σήμα ροής.

Στα πρώτα ροόμετρα μάζας Coriolis υπήρχε μόνο ένας εύκαμπτος σωλήνας που έμοιαζε με λάστιχο ποτίσματος και είχε σχήμα U. Αυτοί παρουσίαζαν το μειονέκτημα ότι ήταν πολύ ευαίσθητοι σε εξωτερικούς κραδασμούς.

Αργότερα σχεδιάστηκαν ροόμετρα που χώριζαν τη ροή σε δύο ξεχωριστά ρεύματα (flow streams) και είχαν δύο εύκαμπτους σωλήνες. Αυτά μετρούσαν τη σχετική συστροφή (relative twist) μεταξύ των δύο σωλήνων. Τα ροόμετρα του τύπου αυτού, είχαν το πλεονέκτημα ότι δεν ήταν τόσο ευαίσθητα σε εξωτερικούς κραδασμούς. Για αυτό το λόγο εγκαταστάθηκαν σε κανονικά συστήματα σωληνώσεων, χωρίς εκτεταμένη μηχανική υποστήριξη.



Εικόνα 63 Ροόμετρο Coriolis. Παρατηρούμε επιπλέον, ότι ο πομπός είναι συσκευή HART και έχει συνδεθεί με έναν προσαρμογέα (adapter) για μετατρέπει σε συσκευή WirelessHART.

Για τα υγρά οι μονάδες μέτρησης ροής είναι lit/sec και m^3/sec . Όμως για διάφορες εφαρμογές σε βιομηχανίες άλλων χωρών, χρησιμοποιούνται και διαφορετικές μονάδες μέτρησης διεθνώς, όπως είναι: Gallons/min, bushels/min. Επιπλέον, υπάρχουν εξειδικευμένες μονάδες ροής που χρησιμοποιούνται ειδικά για μέτρηση ροής ποταμών ή για την ωκεανογραφία, όπως είναι το Sv (sverdrup) $= 10^6 * m^3/sec$, που ονομάστηκε έτσι προς τιμή του ωκεανογράφου Sverdrup.

Τα αέρια συμπιέζονται και ο όγκος τους μεταβάλλεται όταν βρίσκονται υπό πίεση, όταν θερμαίνονται, ή όταν ψύχονται, διότι ο όγκος ενός αερίου εξαρτάται από την πίεση και τη θερμοκρασία και μεταβάλλεται αν μεταβληθούν αυτές οι συνθήκες. Οι μονάδες μέτρησης ροής για τα αέρια είναι m^3/sec αλλά υπάρχουν τα πραγματικά m^3 (actual m^3 ή acm) και τα τυπικά m^3 ("standard m^3 " ή sm^3)

Για αυτό, στα αέρια χρησιμοποιούνται μονάδες όπως: sm^3/sec (τυπικά κυβικά μέτρα ανά δευτερόλεπτο), ή acm/h (πραγματικά κυβικά μέτρα ανά ώρα).

δ) Ροή διαφορικής πίεσης (Differential Pressure) (DP) Flow

Οι μετρητές διαφορικής πίεσης (Differential-pressure meters) στηρίζονται στην αρχή ότι αν περιορίσουν μερικώς τη ροή του υγρού που ρέει μέσα σε ένα σωλήνα, τότε θα δημιουργηθεί μία διαφορά στατικών πιέσεων ανάμεσα στη πλευρά ροής upstream και στην πλευρά ροής downstream της συσκευής. Μετράται αυτή η διαφορά των δύο στατικών πιέσεων (ονομάζεται και διαφορική πίεση differential pressure) και χρησιμοποιείται για να υπολογιστεί ο ρυθμός ροής. Για ένα συγκεκριμένο περιορισμό στη ροή, όσο πιο μεγάλη είναι η διαφορά πιέσεων, τόσο πιο μεγάλος θα είναι και ο ρυθμός ροής. Στη βιομηχανία χρησιμοποιούνται διάφοροι τύποι τέτοιων μετρητών για να μετρηθεί η ροή σε πολλά διαφορετικά είδη ρευστών, από αέρια, μέχρι υγρά με πολύ μεγάλο ιξώδες.

ε) Στάθμη (Level)

Η μέτρηση ύψους στάθμης του υγρού σε μία δεξαμενή, παραδοσιακά γίνεται τοποθετώντας στο τοίχωμα της δεξαμενής ένα μακρόστενο κομμάτι τοιχώματος από διαφανές υλικό (γυαλί ή πλαστικό). Αυτή η μέθοδος έχει περιορισμούς όπως ότι το διαφανές υλικό με τον καιρό διαβρώνεται και χάνει τη διαφάνεια του, ή το γυαλί θολώνει από ατμούς. Άλλος κίνδυνος είναι ότι η δεξαμενή μπορεί να βρίσκεται σε επικίνδυνο περιβάλλον με αναθυμιάσεις και χωρίς εξαερισμό ώστε κάποιος άνθρωπος δεν μπορεί να πλησιάσει για να πάρει μετρήσεις. Άλλος περιορισμός είναι ότι το τοίχωμα από διαφανές υλικό συγκολλήθηκε στο υπόλοιπο τοίχωμα της δεξαμενής και, αν η κόλληση διαβρωθεί, μπορεί να υπάρξουν διαρροές υγρών στα σημεία συγκόλλησης. Η μέτρηση στάθμης σε υγρό γίνεται και με τη χρήση ενός πλωτήρα (φλοτέρ) που έχει ειδικό βάρος το οποίο είναι ανάμεσα στο ειδικό βάρος του υγρού και στο ειδικό βάρος του ατμού του υγρού και έτσι επιπλέει συνεχώς στην επιφάνεια του υγρού και ακολουθεί την αλλαγή ύψους της

στάθμης. Αυτές οι μέθοδοι σήμερα αντικαθίστανται από πιο προηγμένες μεθόδους, όπως είναι χρήση υπερήχων, ραντάρ και λέιζερ.

Στα έξυπνα όργανα μέτρησης τα ψηφιακά σήματα κωδικοποιούνται με βάση διάφορα πρωτόκολλα όπως είναι τα RS-232, Foundation Fieldbus, Hart, Honeywell DE, Profibus. Στο WirelessHART μεταδίδονται ασύρματα σε μεγάλες αποστάσεις. Στις μεθόδους υπερήχων, ραντάρ και λέιζερ απαιτούνται να υπάρχουν και υπολογισμοί από υπολογιστή για την κωδικοποίηση των σημάτων, επομένως τα έξυπνα όργανα μπορούν να μεταφέρουν τα σήματα σε υπολογιστή για την επεξεργασία τους.



Εικόνα 64. Μετρητής στάθμης υγρών για ανοικτές δεξαμενές, ή για κλειστές δεξαμενές χωρίς πίεση ή για κανάλια, πηγάδια κλπ.

Η στάθμη (level) ενός υγρού ή ενός στερεού υλικού (π.χ σε σκόνη, ή χαλίκι κλπ.) που βρίσκεται μέσα σε μία δεξαμενή, είναι το ύψος στο οποίο το ένα υλικό σταματάει και αρχίζει το άλλο υλικό. Για αυτό η μέτρηση της στάθμης του νερού σε μία ανοικτή δεξαμενή είναι να βρεθεί η θέση που σταματά το νερό και ξεκινά ο αέρας. Αν η δεξαμενή περιέχει δύο υγρά π.χ λάδι και νερό, τότε το λάδι θα επιπλέει πάνω στο νερό. Τότε πρέπει να οριστεί που τελειώνει το ένα υγρό και αρχίζει το άλλο. Μια μέτρηση που βρίσκει που τελειώνει το νερό και αρχίζει το λάδι λέγεται μέτρηση της διεπιφάνειας (interface measurement). Όταν μετρηθεί η στάθμη του λαδιού εκεί που τελειώνει το λάδι και αρχίζει ο αέρας, τότε λέμε ότι μετريέται η στάθμη της δεξαμενής. Επίσης όταν το υγρό βράζει ή αφρίζει είναι δυσκολότερο να υπολογιστεί η στάθμη. Οι μονάδες μέτρησης της στάθμης είναι σε ποσοστά 0% και 100% τα οποία δεν αντιστοιχούν σε άδεια δεξαμενή και σε γεμάτη πλήρως δεξαμενή, αλλά σε κάποια όρια, ανώτατο και κατώτατο, που καθορίζονται ανάλογα με την εφαρμογή.

στ) Μέτρηση στάθμης (Level) με μέθοδο διαφορικής πίεσης (Differential Pressure) (DP)

Ο αισθητήρας για τη μέτρηση στάθμης (Level) με τη μέθοδο διαφορικής πίεσης differential pressure (DP), μετράει τη διαφορά της συνολικής πίεσης στον πάτο της δεξαμενής (που είναι η υδροστατική πίεση του υγρού συν την στατική πίεση μέσα στο δοχείο) μείον την στατική πίεση μέσα στο δοχείο. Η διαφορά τους είναι η υδροστατική πίεση του υγρού. Υδροστατική ονομάζεται η πίεση που ασκεί ένα ρευστό που βρίσκεται σε ισορροπία μέσα σε ένα αντικείμενο ή μέσα σε μία επιφάνεια. Η πίεση αυτή οφείλεται μόνο στο βάρος του ρευστού που βρίσκεται υπεράνω του αντικειμένου ή της επιφάνειας.

Αυτή η υδροστατική πίεση ισούται με την πυκνότητα του υγρού πολλαπλασιασμένη επί το ύψος του υγρού στο δοχείο. ο αισθητήρας μπορεί να χρησιμοποιεί ως αναφορά την ατμοσφαιρική πίεση. Τότε στην οροφή του δοχείου υπάρχει ένα άνοιγμα εξαερισμού (vent) για να διατηρείται η υδροστατική πίεση ίση με την ατμοσφαιρική πίεση. Οι αισθητήρες διαφορικής πίεσης DP μπορούν να χρησιμοποιηθούν και σε δοχεία υπό πίεση. Τότε αντί η αναφορά να είναι η ατμοσφαιρική πίεση, η θύρα αναφοράς που είναι η θύρα χαμηλής πίεσης, συνδέεται σε μία θύρα μέσα στο δοχείο που βρίσκεται πάνω από το μέγιστο επίπεδο που φτάνει το υγρό όταν γεμίζει το δοχείο.

ζ) Μανομετρική Πίεση δεξαμενής (Tank gauging)

η) pH

Οι αισθητήρες που μετρούν το pH αερίων χρησιμοποιούνται για να αφαιρέσουν το CO₂ από απαέρια (stack gases).

Για τα υγρά οι αντίστοιχοι αισθητήρες είναι εξειδικευμένοι έχουν σχεδιαστεί ανάλογα με τα χαρακτηριστικά και το είδος του υγρού που πρόκειται να μετρηθεί.

Κάποιοι αισθητήρες pH μπορούν να τοποθετηθούν μόνο σε καθαρό νερό γιατί αν υπάρχουν άλλες ουσίες μπορεί να καλύψουν τον αισθητήρα και να μειώσουν την απόδοση του.

Άλλοι αισθητήρες έχουν υψηλότερη απόδοση και τοποθετούνται σε υγρά που έχουν υψηλές πιέσεις, μπορεί να περιέχουν βακτήρια, οργανικές ουσίες, υλικά που επικαλύπτουν τον αισθητήρα και για αυτό οι αισθητήρες αυτοί χρησιμοποιούν και κάποιο ειδικό ηλεκτρολυτικό υγρό που ξαναγεμίζει.



Εικόνα 65. Διάφοροι αισθητήρες που μετρούν το pH υγρών.

Ο αισθητήρας pH συνδέεται με τον ανάλογο πομπό (transmitter) ο οποίος μεταδίδει τα σήματα σε ένα δίκτυο WirelessHART ή HART.



Εικόνα 66. πομπός HART που συνδέεται στον αισθητήρα μέτρησης pH υγρών.

θ) θερμοκρασία (temperature)

Οι αισθητήρες θερμοκρασίας συνήθως μετρούν τη θερμοκρασία αερίων, ατμόσφαιρας, υγρών και νερού. Χαρακτηρίζονται από το εύρος τιμών (range) που μπορούν να μετρήσουν δηλαδή μία ελάχιστη και μία μέγιστη τιμή θερμοκρασίας. Έχουν ανοχή της τάξης 0.1% στην ακρίβεια της μέτρησης και στέλνουν τα σήματα μετρήσεων επαναληπτικά μέσω δικτύου στην πύλη (gateway). Συνήθως χρησιμοποιούν θερμοζεύγος για τη μέτρηση θερμοκρασίας. Οι μονάδες μέτρησης θερμοκρασίας είναι συνήθως σε βαθμούς κελσίου. Όμως υπάρχουν 4 διαφορετικές κλίμακες που μπορούν να χρησιμοποιηθούν: Réaumur, Fahrenheit, Celsius, Kelvin. Μερικά είδη θερμομέτρων που υπάρχουν είναι τα θερμόμετρα αντιστάσεων (Resistance thermometers), τα Thermistors, τα θερμοζεύγη (Thermocouples) και τα θερμόμετρα συχνότητας (Frequency thermometers).

Μετατροπή μονάδων από Fahrenheit σε Celsius	Μετατροπή μονάδων από Celsius σε Fahrenheit
Celsius: $^{\circ}\text{C} = 5/9 (^{\circ}\text{F} - 32)$	Fahrenheit: $^{\circ}\text{F} = 9/5 ^{\circ}\text{C} + 32$
Μετατροπή μονάδων από Kelvin σε Celsius	Μετατροπή μονάδων από Kelvin σε Fahrenheit
$^{\circ}\text{C} = \text{K} - 273.15$	$^{\circ}\text{F} = 9/5 \text{ K} - 459.67$

Πίνακας 3.5 Μετατροπές μονάδων θερμοκρασίας.

ι) Πυκνότητα

Η πυκνότητα για διάφορα υλικά που βρίσκονται σε συγκεκριμένη φυσική κατάσταση (υγρά, στερεά ή αέρια), όπως πετρέλαιο, φυσικό αέριο, ορυκτό αλάτι, λιπαντικά λάδια, κ.α. μπορεί να μετρηθεί με όργανα μέτρησης πυκνότητας που λέγονται densitometers.

Κάποιοι παράμετροι που υπάρχουν στα περισσότερα όργανα μέτρησης, αυτού του είδους, τυπικά, είναι:

Έχουν ένα αναλογικό σήμα εξόδου 4-20 mA και ένα ψηφιακό σήμα εξόδου HART.

Τροφοδοτούνται από συνεχές ρεύμα DC από 16 ως 30 V, συνήθως 24 V.

Οι μονάδες μέτρησης των οργάνων είναι gr/cm^3 .

Η πυκνότητα ρ ορίζεται ως το πηλίκο της μάζας m του υλικού, προς τον όγκο V που καταλαμβάνει αυτή.

Δηλαδή: $\rho = m/V$

Το εύρος τιμών που μπορούν να μετρήσουν είναι είτε από 0 ως 2 gr/cm^3

είτε 0 ως 3 gr/cm^3 .

Η ακρίβεια τους είναι γύρω στα 0.001 gr/cm^3

Μπορούν να λειτουργήσουν σε υψηλές θερμοκρασίες 100°C και σε μεγάλες τιμές υγρασίας 90%.



Εικόνα 67. Μετρητής πυκνότητας υγρού και μετρητής πυκνότητας αερίου.

3.2.2.3 Τροφοδοσία Συσκευών πεδίου

Οι ασύρματες συσκευές πεδίου (Field Devices) στο WirelessHART τροφοδοτούνται από γραμμή (line), βρόχο (loop), ή μπαταρία ή με άλλο τρόπο. Μία συσκευή πεδίου (Field Device) συνδέεται στη διεργασία process ή στον εξοπλισμό της εγκατάστασης (plant). Οι συσκευές πεδίου (Field Devices) μπορεί να υποστηρίζουν ή όχι την παροχή σήματος με τον παραδοσιακό βρόχο ρεύματος. Όλες οι συσκευές πεδίου (field devices) WirelessHART πρέπει να έχουν μία θύρα συντήρησης (maintenance port) που χρησιμοποιείται για πρόβλεψη (provisioning) και τοπικές διαγνώσεις. Δεν απαιτείται για τις συσκευές WirelessHART να παρέχουν ένα σήμα αναλογικό 4-20mA.

α) γραμμή (line-powered)

β) βρόχος (loop)

γ) μπαταρία (batteries)

Οι ασύρματες συσκευές που δεν τροφοδοτούνται από γραμμή παρέχουν μεγαλύτερη ευελιξία για την υλοποίηση, αλλά απαιτείται μία χαμηλή κατανάλωση ενέργειας για να μην τελειώνει γρήγορα η μπαταρία. Η σωστή ρύθμιση της αναλογίας χρόνου που μένουν ενεργές/ανενεργές (on/off ratio) οι συσκευές είναι ένας βασικός τρόπος για να μειωθεί η κατανάλωση ενέργειας τροφοδοσίας όταν η συσκευή τροφοδοτείται από μπαταρία.

δ) ηλιακή ενέργεια

ε) συλλέκτες ενέργειας (energy harvesters).

3.2.2.4 Γενικές απαιτήσεις για τις συσκευές πεδίου

Όλες οι συσκευές πεδίου (Field Devices) (FD) πρέπει να υποστηρίζουν

α) όλες τις γενικές εντολές (Universal Commands),

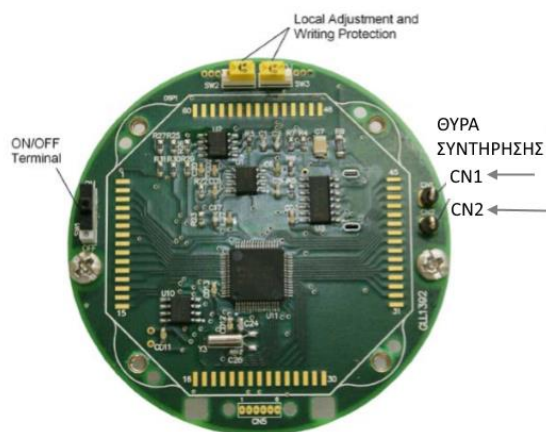
β) μερικές εντολές κοινής πρακτικής (Common Practice Commands),

γ) τις τυποποιημένες εντολές και διαδικασίες (procedures) που ορίζονται για τις συσκευές WirelessHART

Ο όρος δικτυακή συσκευή (Network Device) αναφέρεται σε οποιαδήποτε συσκευή είναι μέρος του δικτύου WirelessHART και είναι ικανή να προωθεί πακέτα δεδομένων μέσα στο δίκτυο. Η συσκευή πεδίου (Field Device) είναι η πιο κοινή δικτυακή συσκευή (Network Device). Όμως ο διαχειριστής δικτύου (Network Manager) κάποιες φορές δεν θεωρείται δικτυακή συσκευή (Network Device) διότι δεν συμμετέχει στο δίκτυο WirelessHART. Όλα τα πακέτα που έχουν ως πηγή (source) τον διαχειριστή δικτύου (Network Manager) (NM) εισάγονται μέσα στο δίκτυο WirelessHART μέσω της πύλης (Gateway) (GW).

Η θύρα συντήρησης (Maintenance Port) των συσκευών πεδίου.

Λέγεται και θύρα επικοινωνίας (Communication Port). Στη θύρα συντήρησης συνδέεται μία συσκευή χειρός (handheld communicator) για να γίνουν διάφορες ρυθμίσεις. Όλες οι συσκευές πεδίου (Field Devices) πρέπει να παρέχουν τη θύρα συντήρησης (maintenance port) που συμμορφώνεται με τις απαιτήσεις της προδιαγραφής Token-Passing Data Link Layer Specification που χρησιμοποιείται στο πρότυπο HART. Η θύρα συντήρησης (maintenance port) πρέπει επίσης να υποστηρίζει τουλάχιστον ένα από τα φυσικά επίπεδα (Physical Layers) που ορίζονται από τα πρότυπα HART standards. Αυτή η διεπαφή (interface) χρησιμοποιείται για να γίνεται πρόβλεψη και συντήρηση (π.χ., για να φορτώσει το κλειδί σύνδεσης Join Key και το αναγνωριστικό δικτύου Network ID ή για να παρακολουθεί τη διαδικασία σύνδεσης join process). Οι εφαρμογές για συσκευές χειρός (Hand held devices) και για διαχείριση πόρων (asset management) που συνδέονται στην θύρα συντήρησης (maintenance port) δεν έχουν πρόσβαση στο ασύρματο δίκτυο (wireless network).



Εικόνα 68. Η Θύρα συντήρησης (maintenance port). Στους ακροδέκτες CN1,CN2 γίνεται σύνδεση με μία ενσύρματη συσκευή χειρός (Handheld Communicator), για να γίνουν διάφορες ρυθμίσεις στην συσκευή πεδίου field device. Πηγή: SMAR (www.smar.com).

Στο WirelessHART όλες οι συσκευές πεδίου (field devices) απαιτείται να έχουν τη θύρα συντήρησης, για να μπορούν να είναι συμβατές με τις παλαιότερες συσκευές HART. Η θύρα συντήρησης επιτρέπει τη σύνδεση όλων των εργαλείων HART και την πρόσβαση σε όλες τις παραμέτρους του οργάνου.

3.2.2.5 Διεπαφή συσκευών WirelessHART (Device Interface)

Οι συσκευές πεδίου (field devices) του WirelessHART είναι πρώτα από όλα συσκευές HART και έτσι έχουν πλήρη συμβατότητα προς το παλαιότερο πρότυπο. Επομένως αυτές οι συσκευές πρέπει να ικανοποιούν όλες τις απαιτήσεις για τις συσκευές HART και επίσης να ικανοποιούν όλες τις προδιαγραφές (specifications) του WirelessHART. Ένα μέρος από τις προδιαγραφές συσκευών είναι ότι πρέπει να υποστηρίζουν όλες τις εντολές κοινής πρακτικής (Common Practice Commands). Σύμφωνα με την προδιαγραφή των συσκευών WirelessHART οι συσκευές (devices) πρέπει να υποστηρίζουν δύο ενδείξεις για την κατάσταση.

Αυτές είναι: η κατάσταση (status) και η εκτεταμένη κατάσταση (extended status).

Η κατάσταση (Status) παρέχει μία ένδειξη για την ποιότητα της μέτρησης που ονομάζεται επίπεδο καλής ποιότητας (level of goodness), για το αν η συσκευή που έκανε τη μέτρηση είναι υγιής (healthy), και για το πόσο έγκαιρη είναι η μέτρηση. Οι συσκευές

εκτελούν ελέγχους στο υλικό (hardware) και στο λογισμικό (software) που έχει σχέση με την είσοδο (input) ή την έξοδο (output) και οι συσκευές με τη σειρά τους αναφέρουν το αποτέλεσμα δίνοντας μία τιμή στη μεταβλητή status.

Υπολογίζεται η κατάσταση (status) μιας παραμέτρου εξόδου (output parameter) για να δώσει μια ρητή ένδειξη (explicit indication) για την ποιότητα της τιμής.

Υπάρχουν 4 είδη ποιότητας της τιμής:

α) καλή (good).

Μια καλή τιμή (good value) μπορεί να χρησιμοποιηθεί για έλεγχο (control).

β) χαμηλή (poor).

Μια χαμηλή τιμή (poor value) είναι ύποπτη (suspect) και μπορεί να μην αντιστοιχεί στην πραγματική τιμή μέτρησης (measurement value) ή στην υπολογισμένη τιμή (calculated value).

γ) κακή (bad).

Μία κακή τιμή (bad value) σημαίνει ότι η τιμή παραμέτρου (parameter value) δεν αντιστοιχεί στην τιμή μέτρησης (measurement value), υπολογισμένη τιμή (calculation value), η τιμή ελέγχου (control value).

δ) σταθερή (fixed).

Μία σταθερή τιμή (fixed value) σημαίνει ότι η τιμή παραμέτρου (parameter value) είναι σταθερή (constant) και δεν ενημερώνεται σε τακτά χρονικά διαστήματα.

Επίσης η κατάσταση (Status) αναφέρει επιπλέον πληροφορίες όπως είναι:

α) Αλλαγή ρύθμισης (configuration changed),

β) ψυχρή εκκίνηση (cold start),

γ) Σταθερό ρεύμα βρόχου (loop current fixed),

δ) Κορεσμός στο ρεύμα βρόχου (loop current saturated),

ε) η μη-πρωτεύουσα μεταβλητή (non-primary variable) είναι εκτός επιτρεπτών ορίων (out of limits),

στ') Η πρωτεύουσα μεταβλητή (primary variable) είναι εκτός επιτρεπτών ορίων (out of limits).

Η εκτεταμένη κατάσταση συσκευής (Extended Device Status) είναι μεταβλητή που έχει μία τιμή (value) και παρέχει τις εξής πληροφορίες ανάλογα με την ένδειξη:

α) Με την ένδειξη: Maintenance Required «απαιτείται συντήρηση», δείχνει ότι η συσκευή έχει προβληματική λειτουργία,

β) Με την ένδειξη: Device Variable Alert «Συναγερμός μίας μεταβλητής συσκευής», δείχνει ότι μια μεταβλητή της συσκευής (device variable) είναι σε κατάσταση συναγερμού (alarm) ή σε κατάσταση ανησυχίας (warning state).

γ) Με την ένδειξη Critical Power Failure «Πρόβλημα στην κρίσιμη ισχύ τροφοδοσίας» δείχνει ότι η ισχύς τροφοδοσίας (power) είναι σε πάρα πολύ χαμηλό επίπεδο (critically low).

Η Κατάσταση συσκευής (Device Status) και η εκτεταμένη κατάσταση συσκευής (Extended Device Status) είναι μεταβλητές που περιλαμβάνονται ως ένα μέρος από σύστημα επικοινωνιών βασισμένο στη λειτουργία καταιγισμού (burst mode).

Άλλο χαρακτηριστικό στοιχείο που υπάρχει στο πρότυπο WirelessHART είναι η χρονοσήμανση (timestamp) που μεταδίδεται (communicated) μαζί με όλες τις τιμές (values). Το γεγονός ότι υπάρχει η χρονοσήμανση (time stamp) στις εφαρμογές (applications) επιτρέπει να καθοριστεί πόσο έγκαιρη είναι η παράμετρος (parameter), αν υπάρχουν ή όχι παρεμβολές (jitter) που επηρεάζουν την ακρίβεια της μέτρησης (measurement), και σε μερικές περιπτώσεις, χρησιμοποιούν την τιμή του χρόνου (time value) και την τιμή της μέτρησης (measurement value) για να καθορίσουν κατάλληλες ενέργειες ελέγχου (control actions) με βάση αυτές τις παραμέτρους.

Υπάρχουν τρία άλλα βασικά χαρακτηριστικά (key features) των συσκευών πεδίου (Field Devices). Αυτά είναι:

α) Λειτουργία καταιγισμού (burst mode).

Η λειτουργία καταιγισμού (Burst mode) χρησιμοποιείται για να στείλει δεδομένα κατ' εξαίρεση (on an exception basis) με πιο γρήγορη ταχύτητα από ότι συνήθως.

β) μετάδοση μπλοκ δεδομένων (block data transfer)

Η μετάδοση μπλοκ δεδομένων (Block data transfer) χρησιμοποιείται για να μεταφέρει (transfer) δεδομένα σε ένα σύνολο μπλοκ (block of data), για παράδειγμα μια ανάλυση φάσματος (spectral analysis), από μία συσκευή (device) σε μια εφαρμογή φιλοξενητή (host application).

γ) ειδοποιήσεις συμβάντων (event notifications).

Η ειδοποίηση συμβάντων (Event Notification) δημοσιεύει τις αλλαγές που γίνονται στην κατάσταση της συσκευής (device's status), ανεξάρτητα από άλλα δεδομένα που δημοσιεύονται (data publishing) και υποστηρίζονται από άλλες εντολές (commands) που υπάρχουν στη λειτουργία καταιγισμού (Burst Mode).

Ένα βασικό χαρακτηριστικό (key feature) των συσκευών πεδίου (Field Devices) είναι ότι έχουν ικανότητα εγκατασταθούν και να χρησιμοποιηθούν σε ένα ευρύ πεδίο εφαρμογών. Όταν μία συσκευή (device) εισάγεται σε μία πραγματική διεργασία (actual process), απαιτείται να γίνουν κάποιες ρυθμίσεις στη συσκευή (device configuration). Ένα μέρος της διαδικασίας ρυθμίσεων στη συσκευή αυτή (configuration device) είναι να δίνεται μία ετικέτα (tag), κλίμακας (scaled).

Η κλίμακα σε ένα όργανο μέτρησης (instrument scaling) περιλαμβάνει τις παρακάτω τιμές:

- α) high scale value, υψηλή τιμή κλίμακας
- β) low scale value, χαμηλή τιμή κλίμακας
- γ) engineering units , μονάδες μέτρησης
- δ) decimal places, πλήθος δεκαδικών ψηφίων.

Επίσης στις ρυθμίσεις της συσκευής εφαρμόζεται μία κατάσταση σήματος (signal conditioning).

Για την περίπτωση μίας βαλβίδας, είναι σημαντικό να γνωρίζουμε προς τα ποια κατεύθυνση μετακινείται η βαλβίδα όταν αυξάνεται το εισερχόμενο σήμα στη βαλβίδα σήματος (signal valve). Οι συσκευές πεδίου (Field devices) μπορούν δέχονται ρυθμίσεις για ανάθεση λειτουργιών (commissioned) και βαθμονόμησης (calibrated). Αυτές οι ρυθμίσεις μπορούν να γίνουν:

- α) εργοστασιακά όταν κατασκευάζονται οι συσκευές.
- β) όταν οι συσκευές βρίσκονται στο χώρο καταστήματος (instrumentation shop)
- γ) όταν η συσκευή έχει εγκατασταθεί στο χώρο κανονικής λειτουργίας της.

3.2.3 Τα αρχεία EDD files σε γλώσσα EDDL

Όπως αναφέρθηκε προηγουμένως, οι έξυπνες συσκευές διαθέτουν παραμέτρους που μπορούν να ρυθμίζονται με χρήση συσκευών χειρός (Handheld Communicators). Επίσης, οι συσκευές χειρός λαμβάνουν στοιχεία διαγνώσεων (diagnostics) για αναφορά προβλημάτων τα οποία εμφανίζονται περιοδικά κατά τη λειτουργία μιας έξυπνης συσκευής και μπορεί να οφείλονται σε δυσμενείς συνθήκες που επικρατούν στο βιομηχανικό περιβάλλον, όπως για παράδειγμα, όταν διαβρωτικές ουσίες από το περιβάλλον αλλοιώσουν τη σωστή λειτουργία μιας συσκευής και χρειάζονται ρυθμίσεις διόρθωσης.

Όμως στο παρελθόν δεν ήταν εύκολο για τους τεχνικούς να διαχειριστούν ένα σύνολο από συσκευές διαφορετικών τεχνολογιών διότι κάθε κατασκευαστής καθόριζε τις δικές του διαφορετικές παραμέτρους για έξυπνες συσκευές και υπήρχαν διαφορετικές συσκευές χειρός ανάλογα με τον κάθε τύπο έξυπνης συσκευής. Για να δοθεί μια λύση σε αυτό το ζήτημα, αναπτύχθηκε σταδιακά μία κοινή γλώσσα περιγραφής (common language) που επέτρεψε να γίνει η ενοποίηση των συσκευών (device integration) και χρησιμοποιεί ένα αρχείο (file) που είναι γραμμένο σε αυτή την κοινή γλώσσα για να περιγράψει την έξυπνη συσκευή (intelligent device) με μία μορφή που γίνεται αντιληπτή από τα μηχανήματα (machine-readable format). Το σύνολο των παραμέτρων (set of parameters) που υποστηρίζει μια συσκευή και οι μέθοδοι (methods) (δηλαδή συναρτήσεις) που είναι διαθέσιμες για αυτή τη συσκευή (device), περιγράφονται σε ένα αρχείο EDD file το οποίο είναι γραμμένο σε γλώσσα EDDL (Electronic Device Description Language) (Γλώσσα περιγραφής ηλεκτρονικών συσκευών). Οι τελικοί χρήστες έχουν συνήθως έτοιμα πρότυπα (templates) που περιέχουν κάποιες τυπικές τιμές παραμέτρων (standard parameter value) για διαφορετικά είδη συσκευών. Χρησιμοποιούν αυτά τα πρότυπα (templates) για να προσαρμόζουν τις συσκευές (devices) ώστε να χρησιμοποιηθούν στις δικές τους βιομηχανικές εγκαταστάσεις (plants).

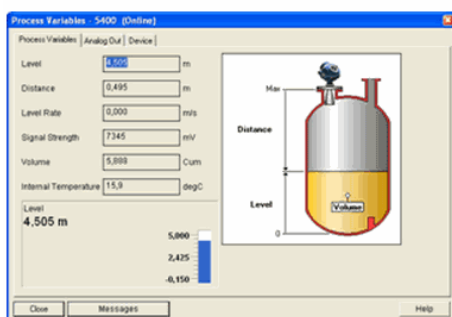
Πολλοί χρήστες έχουν στη διάθεσή τους προγραμματιστικά εργαλεία (tools) και διάφορα λογισμικά διαχείρισης των έξυπνων συσκευών, που χρησιμοποιούν τα αρχεία EDD files.

Το κάθε αρχείο EDD file έχει προσαρμοστεί ειδικά για τις απαιτήσεις ενός συγκεκριμένου μοντέλου συσκευής πεδίου. Υπάρχουν εργαλεία λογισμικού διαχείρισης που χρησιμοποιούν τη γλώσσα EDDL, τα οποία λαμβάνουν και διαχειρίζονται τις πληροφορίες που αφορούν τη συσκευή, αποκωδικοποιούν αυτές τις πληροφορίες και τις

παρουσιάζουν σε ένα γραφικό περιβάλλον υπολογιστή. Η τεχνογνωσία του κατασκευαστή για τις λειτουργίες της συσκευής περιλαμβάνεται στις μεθόδους (methods) δηλαδή στις συναρτήσεις που υπάρχουν στο script της γλώσσας EDDL. Αυτές αφορούν κυρίως τις λειτουργίες της συσκευής.

Έτσι, ο τεχνικός καθοδηγείται βήμα προς βήμα από το πρόγραμμα για να επιτελέσει περίπλοκες διαδικασίες. Τέτοιες εργασίες αφορούν συνήθως τη βαθμονόμηση έξυπνων συσκευών (calibration) καθώς και την εγκατάσταση και εκκίνηση των έξυπνων συσκευών (setup).

Τα δεδομένα που λαμβάνει το λογισμικό, τα ερμηνεύει και τα παρουσιάζει σε υπολογιστές με γραφικά περιβάλλοντα και έτσι οι χρήστες αντιλαμβάνονται καλύτερα μέσα από εικόνες, τις διάφορες πληροφορίες που παρουσιάζουν τις συνθήκες του συστήματος. Οι κατασκευαστές συσκευών μπορούν με τη γλώσσα EDDL να παρέχουν στους τεχνικούς πρόσβαση σε όλες τις λειτουργίες των συσκευών με διάφορα menu και με παραμέτρους που εμφανίζονται σε μία οθόνη όπως τα καθορίζει ο κατασκευαστής. Η γλώσσα EDDL υποστηρίζει τα γραφικά με έναν τρόπο που μοιάζει αρκετά με ιστοσελίδα σε μορφή HTML.



Εικόνα 69 Τα εργαλεία λογισμικού λαμβάνουν πληροφορίες για τις συσκευές πεδίου σε γλώσσα EDDL και τις εμφανίζουν σε οθόνη σε ένα γραφικό περιβάλλον υπολογιστή.

Τα έξυπνα όργανα HART υποστηρίζουν την γλώσσα EDDL. Το WirelessHART είναι συμβατό προς τα πίσω (backward compatible) με τη βασική τεχνολογία του πυρήνα HART. Έτσι υποστηρίζει πλήρως τη δομή εντολών του HART και τη γλώσσα περιγραφής συσκευών (Device Description Language). Όλες οι συσκευές WirelessHART (π.χ.,

διαχειριστής δικτύου network managers, πύλη gateway, συσκευές πεδίου field devices, κλπ) πρέπει να υποστηρίζουν τη γλώσσα EDDL.

Όλες οι δυνατότητες των συσκευών WirelessHART μέσω των αρχείων EDD μπορούν να είναι προσβάσιμες και να δέχονται επεξεργασία. Οι εφαρμογές που χρησιμοποιούν τα αρχεία EDD μπορούν να επικοινωνούν πλήρως με όλες τις συσκευές WirelessHART.

Με αυτό τον τρόπο, οι συσκευές (devices) μπορούν να ρυθμιστούν πλήρως όταν είναι εκτός δικτύου (off-line) και οι ρυθμίσεις να γίνουν είτε στο εργοστάσιο (factory), είτε στο κατάστημα πώλησης (shop), ή πριν από την εκκίνηση λειτουργίας τους (startup) και αυτό επιτυγχάνεται κάνοντας λήψη (downloading) στη συσκευή (device) των ρυθμίσεων εκτός δικτύου (offline configuration). Το μόνο που χρειάζεται είναι να συσχετισθεί (associate) το μοναδικό προσδιοριστικό της συσκευής (unique device identifier) στο σύστημα ρυθμίσεων (configuration system) και μετά αυτό να χρησιμοποιηθεί ως κλειδί (key) για τη συσκευή.

Πολλές φορές στη βιβλιογραφία συναντούμε και άλλους όρους για το EDDL όπως είναι οι: DD, DDL, EDD. Όλοι αυτοί οι όροι είναι πολλές διαφορετικές ονομασίες που σημαίνουν το ίδιο πράγμα. Το DD ήταν το αρχικό όνομα. Οι όροι DD και EDD αναφέρονται στο αρχείο file ενώ οι όροι DDL and EDDL αναφέρονται στη γλώσσα στην οποία γράφονται αυτά τα αρχεία. Η Enhanced EDDL αναφέρεται σε προσθήκες γραφικών που έγιναν στη γλώσσα EDDL το 2006, όπως είναι τα γραφικά κυματομορφών, οι πίνακες, οι πίνακες πλέγματος, οι εικόνες, οι δομές μενού, οι μέθοδοι και οι τρόποι αποθήκευσης δεδομένων.

Περισσότερες πληροφορίες υπάρχουν στην διαδικτυακή διεύθυνση της eddl <http://www.eddl.org/>.

Όλες οι λειτουργίες που αναφέρθηκαν νωρίτερα, δηλαδή η λειτουργία καταιγισμού (burst mode), η μεταφορά μπλοκ δεδομένων (block data transfer), η συντήρηση (maintenance), οι ρυθμίσεις (configuration), οι ειδοποιήσεις συμβάντων (event notifications) απαιτούν όλες τη χρήση πόρων του δικτύου (network resources). Το δίκτυο WirelessHART περιλαμβάνει υποστήριξη για συσκευές (devices), φιλοξενητές (hosts) και τον διαχειριστή δικτύου (network manager) για να αιτείται (request) δικτυακές υπηρεσίες (network services) και εύρος ζώνης (bandwidth) για να υποστηρίξει αυτές τις λειτουργίες (functions). Οι υπηρεσίες (Services) καθορίζονται και

περιγράφονται ως timetables (πίνακες τιμών χρόνου) στις προδιαγραφές του δικτύου WirelessHART.

3.2.4 Η συσκευή δρομολογητής (Router Device)

Μία συσκευή δρομολογητής (Router Device) είναι μία δικτυακή συσκευή (Network Device) που προωθεί (forwards) τα πακέτα δεδομένων από μία δικτυακή συσκευή (Network Device) σε μία άλλη δικτυακή συσκευή. Η δικτυακή συσκευή (Network Device) που λειτουργεί ως συσκευή δρομολογητής (Router Device) χρησιμοποιεί τα γραφήματα της (graphs) και τις συνδέσεις της (connections) για να αποφασίσει σε ποια γειτονική συσκευή (Neighbor Device) πρέπει να στείλει τα πακέτα (packets). Γενικά, δεν απαιτούνται αυτόνομοι δρομολογητές (standalone routers) διότι όλες οι δικτυακές συσκευές (Network Devices) πρέπει να υποστηρίζουν τη δρομολόγηση (routing). Όμως, σε μερικές περιπτώσεις (π.χ., όταν πρόκειται να γίνει μία επέκταση του δικτύου, ή όταν μέσα στο δίκτυο χρειάζεται να γίνει εξοικονόμηση ενέργειας τροφοδοσίας σε ορισμένες συσκευές πεδίου Field Devices) μπορεί να φανεί χρήσιμο να προστεθούν επιπλέον συσκευές για να βελτιωθεί η δρομολόγηση (routing) μέσα στο δίκτυο. Ένας δρομολογητής (router) δεν συνδέεται με τη διεργασία (process) και ούτε ενεργεί ως πύλη (gateway). Σε μερικές περιπτώσεις είναι προτιμότερο να εγκατασταθεί ένα επιπλέον σημείο πρόσβασης (Access Point) αντί να εγκατασταθεί ένας επιπλέον δρομολογητής (Router). Τα σημεία πρόσβασης (Access Points) βελτιώνουν συνολικά την απόδοση (overall throughput) και τον πλεονασμό συνδέσεων (redundancy) του δικτύου. Οι δρομολογητές (Routers) μπορούν να δρομολογούν και να προωθούν πακέτα στο δίκτυο, αλλά δεν συνδέονται με την βιομηχανική διεργασία (industrial process) δηλαδή δεν συνδέονται στους αισθητήρες (sensors) ή στους επενεργητές (actuators). Έτσι οι δρομολογητές δεν είναι γενικά απαραίτητοι και χρησιμοποιούνται μόνο όταν απαιτείται να βελτιωθεί η ασύρματη σύνδεση (wireless connectivity) του δικτύου.

3.2.5 Αναλυτική περιγραφή του Adaptor ή Adapter: Προσαρμογέας WirelessHART

Ο προσαρμογέας (adapter ή adaptor) στο WirelessHART είναι ένα εξάρτημα που συνδέεται σε μία συσκευή πεδίου (field device) συμβατή με το ενσύρματο πρότυπο HART, που ήταν ήδη συνδεδεμένη στο δίκτυο και την μετατρέπει σε μία συσκευή WirelessHART. Ή, σε άλλη περίπτωση, ο προσαρμογέας (adapter) συνδέεται σε αρκετές συσκευές πεδίου (field devices) HART που είναι σε συνδεσμολογία πολλαπλών σημείων (multi-dropped) και επιτρέπει την επικοινωνία (communication) προς όλες τις συνδεδεμένες συσκευές πεδίου (field devices) μέσω ενός δικτύου WirelessHART.

Δηλαδή οι προσαρμογείς παρέχουν μία συμβατότητα προς τα πίσω (backwards compatibility) διότι προσθέτουν δυνατότητες WirelessHART σε συσκευές HART και παρέχουν ασύρματη πρόσβαση σε μία ή περισσότερες συσκευές.

Η συσκευή HART που είναι συνδεδεμένη σε έναν προσαρμογέα (adapter) ονομάζεται sub device του προσαρμογέα, δηλαδή υπό-συσκευή.

Το πλεονέκτημα του προσαρμογέα (adaptor) είναι ότι μπορεί να αξιοποιήσει τις παλαιότερες συσκευές HART Στο δίκτυο WirelessHART.

Οι συσκευές HART παλαιότερα, συνήθως χρησιμοποιούσαν το αναλογικό σήμα 4-20mA και ήταν συνδεδεμένες σε μία αναλογική είσοδο/έξοδο (I/O) και σε ένα κατακεντρωμένο σύστημα ελέγχου (Distributed Control System) DCS. Δηλαδή, όλα τα στοιχεία ελέγχου ήταν κατακεντρωμένα σε ολόκληρη την εγκατάσταση και δεν υπήρχε κάποιος κεντρικός ελεγκτής controller να συγκεντρώνει τις αποθηκευμένες πληροφορίες από τα έξυπνα όργανα HART, διότι αυτό το σύστημα DCS δεν είχε δυνατότητες επικοινωνίας HART. Έτσι τα ψηφιακά δεδομένα που αποθηκευόταν στα έξυπνα όργανα HART, παρέμεναν «παγιδευμένα» και δεν μπορούσαν να ληφθούν για να αξιοποιηθούν σε διάφορες εφαρμογές, όπως π.χ. για παρακολούθηση, για διαγνώσεις, για συναγερμούς, για διαχείριση πόρων κλπ. Μια λύση τότε ήταν να τοποθετηθεί ένας πολυπλέκτης HART στον βρόχο ελέγχου (control loop) 4-20mA, όμως συνήθως δεν υπήρχε η προθυμία από τους τεχνικούς να κάνουν τέτοια τροποποίηση επειδή έπρεπε να γίνουν πολλές αλλαγές στην καλωδίωση που ήδη υπήρχε. Άλλη λύση ήταν η χρήση καρτών εισόδου/εξόδου (I/O) cards που έδιναν δυνατότητες HART, όμως και αυτή η μέθοδος απαιτούσε αλλαγές στις καλωδιώσεις. Επιπλέον έπρεπε να βγουν εκτός λειτουργίας οι βρόγχοι για όσο διάστημα γινόταν αλλαγές στις καλωδιώσεις και χρειαζόταν να αλλάξουν και πολλοί πίνακες rack.

Με τη χρήση του προσαρμογέα (adaptor) του WirelessHART, αυτό το πρόβλημα ξεπεράστηκε πολύ εύκολα και δόθηκε μία απλή λύση χαμηλού κόστους και χαμηλού

ρίσκου χωρίς καμία αλλαγή στις καλωδιώσεις. Έτσι υπήρχε συνεχής πρόσβαση στο δίκτυο WirelessHART και όλες οι ψηφιακές πληροφορίες που είχαν αποθηκευτεί στα έξυπνα όργανα HART έγινε εφικτό να χρησιμοποιούνται από διάφορες εφαρμογές φιλοξενητή (host applications) για διαχείριση πόρων (asset management), διαγνώσεις συναγερμούς και άλλες χρήσεις.

Η τροφοδοσία του προσαρμογέα (adaptor) σε ρεύμα μπορεί να γίνει με 3 τρόπους:

α) Τροφοδοσία του ίδιου του προσαρμογέα από μπαταρία ή ηλιακή ενέργεια.

β) Τροφοδοσία από βρόχο 4-20mA (loop powered).

γ) Τροφοδοσία από το συνδεδεμένο όργανο πεδίου (field powered), π.χ. μία συσκευή HART που έχει εξωτερική τροφοδοσία (συσκευή με 4 καλώδια), τροφοδοτεί και τον προσαρμογέα.

Σύνδεση του προσαρμογέα στο όργανο μέτρησης HART.

Η σύνδεση του προσαρμογέα (adaptor) σε μία συσκευή HART γίνεται με όμοιους τρόπους όπως μπορεί να συνδεθεί μία συσκευή χειρός (Handheld Communicator) ενσύρματη στο δίκτυο HART.

Για να συνδεθεί ο προσαρμογέας (adaptor) στα όργανα πεδίου (field instruments) που είναι συσκευές HART, χρησιμοποιείται μία από τις δύο πιθανές τοπολογίες που ισχύουν στο ενσύρματο πρωτόκολλο HART :

α) Σύνδεση του προσαρμογέα (adaptor) μόνο σε ένα όργανο HART, με την τοπολογία σημείο προς σημείο (point to point).

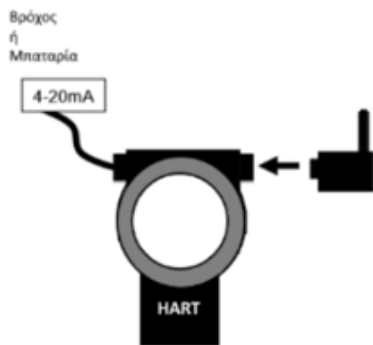
β) Σύνδεση του προσαρμογέα (adaptor) σε τοπολογία πολλαπλών σημείων (multidrop).

Πιο συνηθισμένη περίπτωση είναι ένας προσαρμογέας (adaptor) να συνδεθεί μόνο σε ένα όργανο HART με την τοπολογία σημείο προς σημείο.

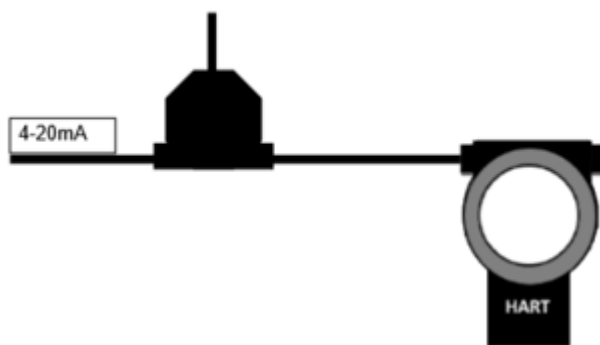
Τότε ο προσαρμογέας WirelessHART adaptor, μπορεί να βιδωθεί απευθείας πάνω στο όργανο HART και να συνδεθεί σε μία χρησιμοποιήσιμη θύρα σύνδεσης (connection port) του οργάνου.

Ένας άλλος τρόπος είναι, ο προσαρμογέας (adaptor) να συνδεθεί σε ένα κουτί επαφών (junction box) του οργάνου HART. Επίσης μπορεί ο adaptor να συνδεθεί σε μία άλλη θέση οπουδήποτε πάνω στο βρόχο (loop) και να συνδέεται στην ίδια γραμμή του βρόχου (inline) μαζί με το όργανο HART.

Διάφορες συνδεσμολογίες του adaptor με το όργανο HART φαίνονται στις παρακάτω εικόνες:



Εικόνα 70. Σύνδεση σημείο προς σημείο. Όργανο HART 4-20 mA που ο adaptor έχει τροφοδοσία από βρόχο ή από μπαταρία και συνδέεται πάνω στο όργανο HART σε μία ελεύθερη θύρα σύνδεσης.



Εικόνα 71. Σύνδεση σημείο προς σημείο. Όργανο HART 4-20 mA που ο adaptor έχει τροφοδοσία από βρόχο ή από μπαταρία και έχει εγκατασταθεί στην ίδια γραμμή πάνω στο βρόχο που συνδέεται το όργανο.

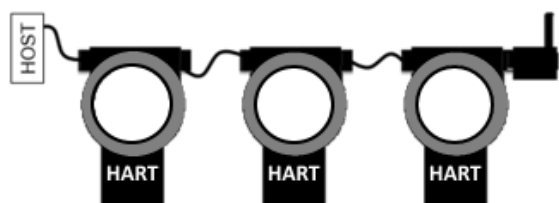


Εικόνα 72. Σύνδεση σημείο προς σημείο. Ο adaptor με τροφοδοσία από το όργανο πεδίου (field) ή από την ίδια μπαταρία που δίνει τροφοδοσία και στο όργανο HART χωρίς να χρειάζεται το όργανο HART να έχει τροφοδοσία από βρόχο 4-20mA.

Στην τοπολογία πολλαπλών σημείων (multidrop configuration) υπάρχει ένας μόνο προσαρμογέας (adaptor) για να συνδέσει συγχρόνως αρκετά όργανα πεδίου HART. Επειδή αυτή η λειτουργία όμως, χρησιμοποιείται πιο σπάνια, για αυτό δεν την υποστηρίζουν όλες οι συσκευές προσαρμογείς (adaptors) που κυκλοφορούν στο εμπόριο.

Η συνδεσμολογία πολλαπλών σημείων (multidrop) είναι αυτή που χρησιμοποιείται στο πρωτόκολλο HART. Σε αυτή την συνδεσμολογία, ο βρόχος ρεύματος (current loop) έχει μία σταθερή τιμή που διατηρείται στα 4mA.

Αυτή η συνδεσμολογία μπορεί να χρησιμοποιηθεί κυρίως σε περιπτώσεις όπου η μετρούμενη μεταβλητή διεργασίας (process variable) μεταβάλλεται σχετικά αργά. Όταν υπάρχουν τέτοιες μεταβλητές, δεν χρειάζεται να χρησιμοποιείται ένας διαφορετικός προσαρμογέας για κάθε όργανο HART, αλλά χρησιμοποιείται ένας μόνο προσαρμογέας για να συνδέσει περισσότερα όργανα. Αυτό οδηγεί και σε μία οικονομία, ως προς το συνολικό κόστος αγοράς των συσκευών.



Εικόνα 73. Σύνδεση πολλαπλών σημείων (multidrop). Ο προσαρμογέας adaptor συνδέεται με το ένα από τα όργανα πεδίου (field instruments) και τα υπόλοιπα όργανα συνδέονται μεταξύ τους με ενσύρματο δίκτυο HART.

Ο προσαρμογέας (adapter) πρέπει να περιέχει και τις δύο παρακάτω διεπαφές:

α) Μία ενσύρματη (wired) διεπαφή Token-Passing interface (με κουπόνι), που αντιστοιχεί στο πρότυπο HART.

β) Μία ασύρματη (wireless) διεπαφή TDMA interface (πολυπλεξίας με διαίρεση χρόνου), που αντιστοιχεί στο πρότυπο WirelessHART.

Με άλλα λόγια, όταν δεν γίνεται εξαίρεση ρητώς, ένας προσαρμογέας (adapter) στο WirelessHART πρέπει να πληροί όλες τις απαιτήσεις που υπάρχουν και για την ενσύρματη επικοινωνία (wired) και για την ασύρματη επικοινωνία με WirelessHART. Επιπλέον, επειδή πολλές από τις συσκευές (devices) που συνδέονται σε έναν προσαρμογέα WirelessHART Adapter, ενδεχομένως να είναι παλαιότερες και να βρίσκονται σε επίπεδο προηγούμενων εκδόσεων του προτύπου HART, για αυτό ο προσαρμογέας (Adapter) πρέπει να υποστηρίζει τις βασικές ιδιότητες του HART 7 για την συσκευή που συνδέεται (sub device). Για παράδειγμα ο προσαρμογέας (adapter) πρέπει να υποστηρίζει τουλάχιστον 5 μηνύματα σε λειτουργία καταιγισμού (burst mode messages) και δύο μηνύματα συμβάντων (event messages). Ο προσαρμογέας WirelessHART Adapter πρέπει επίσης να επιτρέπει πλήρη πρόσβαση στις ρυθμίσεις (configuration) και στην κατάσταση (status) για όλες τις συνδεδεμένες συσκευές του (sub-devices).

Ο προσαρμογέας (adapter) υποστηρίζει το πρωτόκολλο HART για επικοινωνία με τις συνδεδεμένες συσκευές πεδίου (field devices) και επιπλέον ο προσαρμογέας (adapter) δεν πρέπει να προκαλεί καθόλου αρνητικές επιδράσεις ή παρεμβολές που αλλοιώνουν το αναλογικό σήμα (analog signaling) το οποίο χρησιμοποιείται στο πρωτόκολλο HART.

Ο προσαρμογέας WirelessHART πρέπει να παρέχει υπηρεσίες δημοσίευσης δεδομένων εκ μέρους της συσκευής HART που συνδέεται, ακόμα και αν αυτή η συσκευή δεν υποστηρίζει την προαιρετική λειτουργία δεδομένων καταιγισμού (Burst Mode).

Ο προσαρμογέας (Adapter) πρέπει να υποστηρίζει:

α) τις γενικές εντολές (Universal Commands)

β) τις εντολές κοινής πρακτικής (Common Practice Commands)

γ) να δίνει μία ταυτοποίηση για τον εαυτό του στις αποκρίσεις εντολών ταυτότητας (Identity Command responses).

Επιπλέον, ο προσαρμογέας (Adapter) πρέπει να υποστηρίζει τουλάχιστον 1 σύνδεση για μεταφορά μπλοκ δεδομένων (Block Data Transfer). Ο προσαρμογέας (Adapter) έχει την ευθύνη για να γίνεται η διαπραγμάτευση (negotiating) για τη χρήση των πόρων του δικτύου (network resources) για τον εαυτό του και για τις συσκευές στις οποίες συνδέεται (sub devices).

Για παράδειγμα, σε πολλές περιπτώσεις όταν στέλνεται προς τα έξω μία εκπομπή για αναζήτηση (search broadcast), πρέπει ο προσαρμογέας (Adapter) να έχει επίσης δυνατότητα να δώσει απόκριση (responding) εκ μέρους της συσκευής που συνδέεται (sub-device).

Ο προσαρμογέας WirelessHART, μπορεί να περιλαμβάνει και τους δικούς του ξεχωριστούς αισθητήρες (sensors) ή επενεργητές (actuators) που είναι επιπρόσθετοι από αυτούς που υπάρχουν στα έξυπνα όργανα HART με τα οποία συνδέεται ο προσαρμογέας.

Πλεονεκτήματα του προσαρμογέα WirelessHART adaptor.

Ο προσαρμογέας WirelessHART adaptor όταν συνδέεται σε ένα όργανο HART τότε το όργανο HART μπορεί να συνδεθεί στο δίκτυο WirelessHART και μπορεί μέσω του δικτύου να υπάρξει πρόσβαση στις πληροφορίες του οργάνου από απόσταση (remote access).

3.2.6 Αναλυτική περιγραφή των Συσκευών χειρός (Handheld Communicators)

Οι συσκευές χειρός (Handheld Devices) ή (Handheld Communicators) (HHC), χρησιμοποιούνται για την εγκατάσταση (installation) και τη συντήρηση (maintenance) των δικτυακών συσκευών (Network Devices). Οι συσκευές χειρός (Handheld Devices) είναι φορητός εξοπλισμός (portable equipment) που τον χειρίζεται κυρίως το προσωπικό

της βιομηχανικής εγκατάστασης (plant personnel) για να ελέγξει και να ρυθμίσει τις συσκευές του δικτύου WirelessHART.

Οι συσκευές χειρός χωρίζονται σε συσκευές χειρός HART (ενσύρματες) και σε συσκευές χειρός WirelessHART (ασύρματες).

Μία εφαρμογή φιλοξενητή (Host application) μπορεί να εκτελείται σε συσκευή χειρός που είναι μία φορητή συσκευή (portable device). Οι στόχοι της συσκευής χειρός είναι ρυθμίσεις, παρακολούθηση και συντήρηση των συσκευών (devices). Μπορεί να συνδεθεί στο ασύρματο δίκτυο WirelessHART ή στο δίκτυο αυτοματισμού της εγκατάστασης (plant automation network).

Υπάρχουν 4 διαφορετικές προσεγγίσεις για να συνδεθούν στο δίκτυο οι συσκευές χειρός (Handheld Devices):

- α) Συσκευή χειρός HART συνδέεται μέσω ενός ασύρματου δικτύου WiFi,
- β) συσκευή χειρός HART συνδέεται μέσω ενός modem FSK,
- γ) συσκευή χειρός WirelessHART συνδέεται μέσω ενός δικτύου WirelessHART,
- δ) συσκευή χειρός WirelessHART συνδέεται σε μία συσκευή πεδίου (Field Device) του δικτύου WirelessHART.

Αυτοί οι 4 τρόποι σύνδεσης αναφέρονται αναλυτικότερα παρακάτω:

- α) Συσκευή χειρός HART ή συνδεδεμένη εφαρμογή (application) μέσω ενός δικτύου αυτοματισμών βιομηχανικής εγκατάστασης (Plant automation Network).

Μία συσκευή χειρός (handheld device) για να συνδεθεί στο δίκτυο αυτοματισμών βιομηχανικής εγκατάστασης (plant automation network) χρησιμοποιεί κάποια τεχνολογία ασύρματου δικτύου όπως είναι το WiFi. Αυτή η συσκευή χειρός (handheld device) επικοινωνεί με τις δικτυακές συσκευές (Network Devices) μέσω της συσκευής πύλης (gateway Device) με τον ίδιο τρόπο που επικοινωνούν και οι εξωτερικοί υπολογιστές servers της εγκατάστασης αυτοματισμών (plant automation servers). Για το δίκτυο WirelessHART αυτός ο τύπος συσκευής χειρός (handheld) είναι απλώς μία ακόμη εφαρμογή φιλοξενητή (host application).

β) Συσκευή χειρός HART (Handheld) που συνδέεται στη συσκευή (device) μέσω ενός modem FSK. Σε αυτή τη λειτουργία (mode) η συσκευή χειρός (Handheld Device) συνδέεται άμεσα στη συσκευή με ένα modem FSK. Όταν συνδεθεί σε αυτή τη λειτουργία (mode), η συσκευή χειρός (Handheld Device) δεν μπορεί να επικοινωνήσει προς τα έξω στο δίκτυο WirelessHART μέσω της συσκευής (device)

γ) Συσκευή χειρός WirelessHART (Handheld) συνδέεται σε ένα δίκτυο WirelessHART. Μια συσκευή χειρός (Handheld Device) που συνδέεται στο δίκτυο WirelessHART είναι μία ακόμη συσκευή του δικτύου WirelessHART. Σε αυτή τη λειτουργία (mode) η συσκευή χειρός WirelessHART (Handheld) έχει τους ίδιους περιορισμούς με οποιαδήποτε άλλη συσκευή (device) του ίδιου δικτύου, δηλαδή μπορεί να επικοινωνεί μόνο με την πύλη (gateway) και με τον διαχειριστή δικτύου (network manager). Αυτή η λειτουργία (mode) χρησιμοποιείται για να γράφει κλειδιά (keys) στην ασύρματη συσκευή χειρός (Wireless Handheld) και για να φαίνονται πληροφορίες για διαγνώσεις και τον έλεγχο της «υγείας» του συστήματος. Αυτή θα αναφέρεται στη συνδεδεμένη συσκευή (Connected) ως μία δικτυακή συσκευή (Network Device).

δ) Η συσκευή χειρός WirelessHART (Handheld) συνδέεται μόνο σε μία συσκευή πεδίου (Field Device) του δικτύου WirelessHART.

Μία συσκευή χειρός (Handheld Device) WirelessHART που για να συνδεθεί στο δίκτυο WirelessHART, συνδέεται σε μία συσκευή (WirelessHART Device) περιορίζεται στο να επικοινωνεί μόνο με την συσκευή WirelessHART στην οποία έχει συνδεθεί η συσκευή χειρός (handheld). Έχει γίνει μια ειδική πρόβλεψη και χρησιμοποιείται για να εξασφαλιστεί ότι η συσκευή χειρός (WirelessHART Handheld) περιορίζεται μόνο σε ένα άλμα (one hop) και να συνδέεται μία μόνο συσκευή κάθε φορά. Αυτό θα αναφέρεται στη συνδεδεμένη συσκευή (Connected) ως μία συσκευή συντήρησης (Maintenance Device). Οι συσκευές χειρός (Handheld devices) που συνδέονται με αυτόν τον τρόπο πρέπει να έχουν μία δική τους συνεδρία (session) για να χρησιμοποιείται ανάμεσα στην συσκευή χειρός (Handheld) και στη συσκευή δικτύου στην οποία συνδέεται αυτή.

3.2.7 Αναλυτική περιγραφή για την Πύλη (Gateway)(GW) και το σημείο πρόσβασης (Access Point) (AP)

Η πύλη (Gateway) και τα σημεία πρόσβασης (Access Points) συνδέουν το δίκτυο WirelessHART Network με ένα δίκτυο αυτοματισμού βιομηχανικής εγκατάστασης (plant automation network), που είναι ένα ξεχωριστό δίκτυο, διαφορετικό από το WirelessHART και είναι συνήθως ενσύρματο. Έτσι, η πύλη επιτρέπει να υπάρχει μία ροή (flow) δεδομένων ανάμεσα στα δύο διαφορετικά δίκτυα.

Σε κάποιες περιπτώσεις, όπως αναφέρθηκε, η πύλη δεν αποτελεί από μόνη της μία ξεχωριστή συσκευή αλλά βρίσκεται τοποθετημένη μαζί με άλλες συσκευές μέσα σε μία ενιαία μονάδα που συνολικά ονομάζεται «πύλη». Τότε για να ξεχωρίζει η καθαυτή συσκευή που είναι ή σκέτη πύλη, ονομάζεται Virtual Gateway. Έτσι με βάση αυτή την περιγραφή, μία πύλη μπορεί να διαιρείται σε εικονική πύλη (virtual Gateway) και στα σημεία πρόσβασης Access Points (AP) που είναι ένα ή περισσότερα. Η πύλη είναι η συσκευή που συνδέει μεταξύ τους τις εφαρμογές φιλοξενητή (host applications), το διαχειριστή δικτύου (Network manager) και το δίκτυο WirelessHART.

Η πύλη έχει την ευθύνη για αποθήκευση δεδομένων σε ενδιάμεση μνήμη απομόνωσης (buffering) και για μετατροπές πρωτοκόλλων. Επιπλέον χρησιμοποιείται ως πηγή ρολογιού για συγχρονισμό των συσκευών του δικτύου.

Η συσκευή πύλη (gateway Device) παρέχει στις εφαρμογές φιλοξενητή (host applications) την πρόσβαση (access) στις δικτυακές συσκευές (Network Devices).

Μία συσκευή πύλη (gateway Device) μπορεί να χρησιμοποιηθεί με 3 διαφορετικούς τρόπους:

- α) για να μετατρέψει δεδομένα από ένα πρωτόκολλο σε άλλο,
- β) ως ενδιάμεση συσκευή (go-between) ανάμεσα σε δύο ή περισσότερα δίκτυα που χρησιμοποιούν το ίδιο πρωτόκολλο
- γ) για να μετατρέπει τις εντολές (commands) και τα δεδομένα από μια μορφή σε άλλη μορφή (format).

Η βασική λειτουργία μιας πύλης (gateway) είναι να αποθηκεύει στην κρυφή μνήμη (cache) τα δεδομένα καταιγισμού (burst data) που αναφέρονται (reported) από

συσκευές πεδίου (field devices) του WirelessHART και μετά να επιστρέφει αυτά τα δεδομένα στις εφαρμογές φιλοξενητή (host applications).

Η αποθήκευση των δεδομένων στην κρυφή μνήμη (Caching) έχει δύο πλεονεκτήματα:

- α) βελτιώνει την άμεση απόκριση της πύλης (gateway) προς τις εφαρμογές φιλοξενητή (host applications),
- β) μειώνει σημαντικά τις επιπρόσθετες επικοινωνίες στο δίκτυο (network communications) οι οποίες προκαλούν αυξημένη κίνηση δεδομένων χωρίς να χρειάζεται.

Αν εξαιρεθούν οι επικοινωνίες που είναι ενεργοποιημένες (enabled), πολύ συχνά στο δίκτυο συνηθίζεται να μειώνονται οι επιπρόσθετες επικοινωνίες δικτύου (network communications) κατά έναν παράγοντα (factor) 10 ως 20 φορές. Σε πολλές περιπτώσεις τα δίκτυα θα έχουν περισσότερα από ένα σημείο πρόσβασης (access point). Αυτά τα πολλαπλά σημεία πρόσβασης (access points) μπορούν να χρησιμοποιηθούν για να βελτιώσουν την αποτελεσματική απόδοση (effective throughput) και την αξιοπιστία του δικτύου. Τα σημεία πρόσβασης (Access points) επικοινωνούν άμεσα με την πύλη (gateway).

Για την εγκατάσταση ενός ασύρματου δικτύου (wireless network) χρειάζονται:

- α) εγκατάσταση των ασύρματων συσκευών (wireless devices),
- β) μία πύλη (gateway) (σε μερικές περιπτώσεις μία πύλη gateway και ένα ή περισσότερα σημεία πρόσβασης access points),
- γ) μία σύνδεση (connection) σε ένα σύστημα φιλοξενίας (host) ή σε ένα σύστημα ελέγχου (control system).

Όταν η πύλη (gateway), οι συσκευές (devices), και το σύστημα ελέγχου (control system) ρυθμιστούν σωστά τότε διαμορφώνεται το δίκτυο πλέγματος (wireless mesh) και ξεκινούν οι επικοινωνίες.

Για να είναι πιο απλή η υποστήριξη για πλεονάζοντα σημεία πρόσβασης (redundant Access Points), κάθε πύλη (gateway) έχει μία σταθερή διεύθυνση που είναι καλά γνωστή (Unique ID = 0xF981000002 και Nickname = 0xF981). Υπάρχει μόνο μία πύλη (gateway) σε κάθε δίκτυο WirelessHART.

Οι πύλες (Gateways) μπορούν να είναι πλεονάζουσες (redundant), δηλαδή επιτρέπεται να υπάρχουν περισσότερες πύλες στο δίκτυο, χωρίς αυτό να είναι αναγκαίο.

3.2.7.1 Γενικές απαιτήσεις

Η πύλη (gateway) χρησιμοποιεί τις τυπικές εντολές (commands) του πρωτοκόλλου HART για να επικοινωνεί με τις δικτυακές συσκευές (network devices) και με τις εφαρμογές φιλοξενητή (host applications). Η πύλη (gateway) λειτουργεί επίσης και σαν υπολογιστής server και έχει την ευθύνη να συλλέγει (collect) και να διατηρεί (maintain) τα δεδομένα που αποθηκεύει στην κρυφή μνήμη (cached data) και τις αποκρίσεις σε εντολές (command responses) από όλες τις συσκευές μέσα στο δίκτυο. Αυτές οι αποκρίσεις που είναι αποθηκευμένες στην κρυφή μνήμη (cached responses) αντιστοιχούν σε μηνύματα καταιγισμού (burst messages), ειδοποιήσεις συμβάντων (event notifications) και αποκρίσεις (responses) για κοινές εντολές του HART. Αυτές οι αποθηκευμένες αποκρίσεις στην κρυφή μνήμη (cached responses) επιστρέφονται άμεσα σε αιτήσεις (requests) που στέλνει μία εφαρμογή φιλοξενητή (host application). Με αυτό τον τρόπο μειώνεται το φορτίο επικοινωνιών του δικτύου (network communication load), βελτιώνεται η χρήση της ενέργειας και γίνονται πιο γρήγορα οι αποκρίσεις (responses) στην εφαρμογή φιλοξενητή (host application). Η πύλη (gateway) πρέπει να υποστηρίζει εγγενώς τους προσαρμογείς (adapters) και να επιτρέπει πρόσβαση με διαφάνεια (transparent access) στις συσκευές (sub-devices) που είναι συνδεδεμένες στους προσαρμογείς (Adapters).

Οι συσκευές (devices) που συνδέονται στον προσαρμογέα (adapter) μπορούν να αναγνωρίζονται (identified) με τη διαδικασία polling του προσαρμογέα (Adapter) για τις συσκευές του (sub-devices). Η πύλη (gateway) χρησιμοποιεί την εντολή Command 74 για να καθορίσει πόσες συσκευές sub-devices μπορούν να συνδεθούν σε έναν προσαρμογέα (Adapter). Μετά η πύλη (gateway) αναφέρει την εντολή Command 75 για να διαπεράσει τους έγκυρους συνδυασμούς (legal combinations) των διευθύνσεων

polling (polling addresses), της κάρτας εισόδου/εξόδου (I/O Card), και τους προσδιοριστές καναλιού (Channel identifiers) μέχρι να προσδιοριστούν (identified) όλες οι συνδεδεμένες συσκευές sub-devices στον προσαρμογέα. Αν η πύλη (gateway) υποστηρίζει πολλαπλά σημεία πρόσβασης (Access Points), τότε ο διαχειριστής δικτύου (network manager) θα κάνει το χρονοπρογραμματισμό (schedule) για να γίνει κυκλοφορία των δεδομένων επικοινωνίας (communication traffic) μέσω όλων αυτών των σημείων πρόσβασης. Αν ένα από αυτά τα σημεία πρόσβασης (WirelessHART Access Points) παρουσιάσει σφάλμα τότε ο διαχειριστής δικτύου (network manager) θα ρυθμίσει τον χρονοπρογραμματισμό (schedule) και θα εξαπλώσει την κυκλοφορία ανάμεσα στα υπόλοιπα σημεία πρόσβασης (WirelessHART Access Points). Κάθε σημείο πρόσβασης (Access Point) έχει τη δική του φυσική διεύθυνση (physical address) και την δική του σύντομη διεύθυνση (nickname Address). Εσωτερικά στην πύλη (gateway), όλα τα σημεία πρόσβασης (Access Points) δρομολογούν την κυκλοφορία μέσω της πύλης (gateway) και την στέλνουν είτε σε μία διεπαφή φιλοξενητή (Host Interface) είτε στο διαχειριστή δικτύου (network manager). Η πύλη (gateway) του WirelessHART πρέπει να παρέχει το ρολόι δικτύου (network clock) σε άλλες δικτυακές συσκευές (Network Devices). Οι πληροφορίες ρολογιού στην ιεραρχία επιπέδων του δικτύου μεταφέρονται προς τα κάτω σαν ένα κύμα (ripples downward), ξεκινώντας από το κορυφαίο επίπεδο και φτάνοντας προς το τελευταίο επίπεδο που βρίσκεται στη βάση.

3.2.7.2 Το μοντέλο πύλης (Gateway Model)

Οι πύλες (gateways) του WirelessHART συνδέουν το δίκτυο WirelessHART, με άλλα δίκτυα όπως είναι τα δίκτυα αυτοματισμού βιομηχανικών εγκαταστάσεων (plant automation networks), που επιτρέπουν να γίνεται μία ροή από διάφορα είδη μηνυμάτων ανάμεσα στα δύο δίκτυα. Τέτοια μηνύματα είναι:

- α) εντολές/αποκρίσεις (Commands/ Responses) του HART,
- β) διοχετευμένα μηνύματα (tunneled messages),
- γ) μορφοποιημένα (formatted) μηνύματα σε XML,
- δ) διαγνώσεις (diagnostic messages)

Το δίκτυο WirelessHART Network χρησιμοποιεί μια πύλη (gateway) για να παρέχει ένα μεμονωμένο σημείο εισόδου (single entry point) στο δίκτυο WirelessHART.

Υπάρχουν δύο τύποι σημείων πρόσβασης (Access Points):

α) Τα σημεία πρόσβασης υπηρεσιών (Service Access Points) που επιτρέπουν πρόσβαση σε διεπαφές φιλοξενητών (Host interfaces).

β) Τα σημεία πρόσβασης WirelessHART (WirelessHART Access Points) που επιτρέπουν πρόσβαση στο ίδιο το δίκτυο WirelessHART.

Η πύλη (Gateway)

Η πύλη (gateway) είναι ένα μεμονωμένο σημείο εισόδου (single entry point) στο δίκτυο WirelessHART.

- Είναι μέρος του δικτύου συσκευών πεδίου WirelessHART (WirelessHART Field Device network).

1. Είναι ένας τύπος συσκευής (device type) στο δίκτυο WirelessHART.

2. Επικοινωνεί μέσω των σημείων πρόσβασης (Access Points) με οποιαδήποτε συσκευή πεδίου (Field Device) στο δίκτυο WirelessHART.

Η πύλη (gateway) πρέπει να έχει μία διαδρομή (path) προς κάθε συσκευή (device) στο δίκτυο WirelessHART.

- Μπορεί να επικοινωνεί άμεσα με τον διαχειριστή δικτύου (network manager).

- Παράγει μηνύματα για συγχρονισμό (time synchronization messages).

- Είναι τύπος συσκευής HART (HART Device Type).

1. Περιγράφεται με τη γλώσσα DDL

2. Υποστηρίζει το HART DD

- Υποστηρίζει ένα ή περισσότερα σημεία πρόσβασης υπηρεσιών (Service Access Points) για να συνδέσει το δίκτυο αυτοματισμού με το δίκτυο κορμού της βιομηχανικής

εγκατάστασης (plant backbone). Με αυτά τα σημεία πρόσβασης υπηρεσιών (Service Access Points) υποστηρίζονται τα παρακάτω:

1. Συναρτήσεις μετάφρασης (Translation functions) που ικανοποιούν τις εντολές HART (HART Commands) με τοπικά δεδομένα που είναι αποθηκευμένα στην κρυφή μνήμη (locally cached data). Η πύλη (gateway) στο WirelessHART υλοποιεί μία κρυφή μνήμη δεδομένων (data cache) για να βελτιστοποιηθεί η συνολική απόδοση του δικτύου WirelessHART και να υπάρξει βελτιωμένη απόκριση (response) στις εφαρμογές φιλοξενητή (host applications).

2. Συναρτήσεις διοχέτευσης (Tunneling functions) που μεταφέρουν τις εντολές (Commands) του HART σε αιτήσεις (requests) από το δίκτυο WirelessHART. Η πύλη (gateway) του WirelessHART μπορεί να συνδεθεί με την εφαρμογή φιλοξενητή (host application) χρησιμοποιώντας διάφορα πρωτόκολλα όπως είναι : Modbus, Profibus DP, ControlNet, HART OPC server, ιδιωτικά ή άλλα πρωτόκολλα).

Η σύνδεση αυτή βασίζεται σε διαφορετικά φυσικά επίπεδα (physical layers) όπως είναι το RS485, το Ethernet LAN, το Wi-Fi, και άλλα.

3. Προαιρετικά, υποστηρίζει μία διεπαφή (interface) σε XML

Συμβατότητα.

1. Η πύλη (gateway) του WirelessHART μπορεί να υποστηρίξει τις εντολές (commands) HART που υπάρχουν ήδη, αλλά αυτό ισχύει μόνο όταν η πύλη (gateway) είναι ρυθμισμένη για να λειτουργεί ως μεταφραστής (translator) ή ως μεσολαβητής (proxy).

Buffering

Η πύλη (gateway) επιτρέπει αποθήκευση σε ενδιάμεση μνήμη απομόνωσης (buffering) για τα παρακάτω:

1. Λειτουργία καταιγισμού (Burst Mode).

2. Ειδοποίηση συμβάντων (Event Notification).

3. Αποκρίσεις σε εντολές (command responses) που είναι αποθηκευμένες στην κρυφή μνήμη (Cached).

4. Διαγνώσεις (Diagnostics).

5. Μεταφορές μεγάλης ποσότητας δεδομένων ή αρχείων. Υπάρχουν αρκετές ειδικές περιπτώσεις χρήσης, στις οποίες μία συσκευή στέλνει πολλά δεδομένα στην πύλη (gateway). Σε άλλες περιπτώσεις και η πύλη (gateway) μπορεί να στείλει πολλά δεδομένα σε μία συσκευή. Μία περίπτωση χρήσης είναι όταν μία βαλβίδα στέλνει δεδομένα για την υπογραφή της (signature information) στην πύλη (gateway). Μια άλλη περίπτωση είναι όταν μία συσκευή στέλνει αποτελέσματα από την ανάλυση κραδασμών (vibration analysis) στην πύλη (gateway).

- Η πύλη (gateway) υποστηρίζει την δημοσίευση μεταβλητών (publishing variables) στις συσκευές (devices). Αυτές οι μεταβλητές συχνά ονομάζονται catch variables. Στην περίπτωση αυτή, η πύλη (gateway) του WirelessHART μπορεί να δημοσιεύσει (publish) δεδομένα σε λειτουργία καταιγισμού (burst mode data) τα οποία αποθηκεύονται στην κρυφή μνήμη (caching) άλλων συσκευών (devices) που βρίσκονται στο δίκτυο WirelessHART.

Το δίκτυο που χρησιμοποιείται από την πλευρά του φιλοξενητή (host) μπορεί να αποτελείται από διάφορες τεχνολογίες. Οι περισσότεροι προμηθευτές συστημάτων PLC, DCS ή SCADA χρησιμοποιούν δικά τους ιδιοταγή δίκτυα που δεν βασίζονται σε ανοικτά πρότυπα.

Οι εταιρίες διαχείρισης πόρων (Asset Management) και οι εταιρίες διαχείρισης συσκευών (Device Management) έχουν μία τάση να χρησιμοποιούν ανοικτά πρωτόκολλα (open protocols), όπως είναι το TCP/IP και κάποιο από τα διαθέσιμα τυπικά στρώματα MAC ή φυσικό στρώμα (MAC/PHY layers) όπως είναι το IEEE 802.11 και το IEEE 802.3.

3.2.7.3 Το σημείο πρόσβασης (Access Point) (AP) WirelessHART

Ένα σημείο πρόσβασης (Access Point) WirelessHART είναι μία δικτυακή συσκευή (Network Device) που συνδέει τις πύλες (gateways) μέσα στο δίκτυο WirelessHART.

Το σημείο πρόσβασης (Access Point) WirelessHART, στη μία πλευρά του έχει μία σύνδεση WirelessHART και στην άλλη πλευρά του έχει μία εξωτερική σύνδεση (external connection)

Η εξωτερική σύνδεση (external connection) θα μπορούσε να είναι μία σύνδεση Ethernet ή Wi-Fi ή μία σύνδεση με άλλο δίκτυο που χρησιμοποιεί τα δικά του ιδιοταγή πρωτόκολλα.

Η εξωτερική σύνδεση (external connection) δεν καθορίζεται από το πρότυπο WirelessHART. Το σημείο πρόσβασης (Access Point) WirelessHART δεν συνδέεται άμεσα στη διεργασία (process).

Τα σημεία πρόσβασης (Access Points) WirelessHART παρέχουν τα παρακάτω:

Είναι μέρος του δικτύου συσκευών WirelessHART

(WirelessHART Field Device network).

1. Είναι ένας τύπος συσκευής (device type) στο δίκτυο WirelessHART Network.
2. Επικοινωνούν με την πύλη (gateway) μέσω μίας αφιερωμένης ζεύξης (dedicated link) ή μιας θύρας επικοινωνίας (communication port).
3. Κάθε σημείο πρόσβασης (Access Point) WirelessHART μπορεί να υποστηρίξει την επικοινωνία με οποιαδήποτε συσκευή (device) προς την οποία υπάρχει μία διαδρομή (path) η οποία παρέχεται από τον διαχειριστή δικτύου (network manager).

3.2.7.4 Το σημείο πρόσβασης υπηρεσιών (Service Access Point: SAP)

Τα σημεία πρόσβασης υπηρεσιών (Service Access Points) παρέχουν μία σύνδεση ανάμεσα στο δίκτυο αυτοματισμού (automation network) και τον κορμό της βιομηχανικής εγκατάστασης (plant backbone).

Παρέχουν:

Μία διεπαφή (interface) προς την πύλη (gateway) για συστήματα φιλοξενητή (host systems) ή εφαρμογές (applications) που επιθυμούν να έχουν πρόσβαση σε δικτυακές συσκευές (Network Devices) οι οποίες είναι μέρος του δικτύου WirelessHART. Η διεπαφή (interface) παρέχει υποστήριξη για πρόσβαση σε όλες τις συσκευές (Devices) του ενσύρματου (wired) HART που συνδέονται στο δίκτυο μέσω των προσαρμογέων (Adapters).

Πρόσβαση σε μηνύματα αποκρίσεων (response messages) που είναι αποθηκευμένα στην κρυφή μνήμη (cached):

1. Αποκρίσεις σε λειτουργία καταιγισμού (Burst Mode Responses).
2. Αποκρίσεις σε ειδοποιήσεις συμβάντων (Event Notification Responses).
3. Αποκρίσεις σε εντολές (command responses) που είναι αποθηκευμένες στην κρυφή μνήμη (Cached).

- Πρόσβαση σε διαγνώσεις (diagnostics).
- Πρόσβαση σε δεδομένα του διαχειριστή δικτύου (network manager).
- Υποστήριξη για λειτουργία μεταφοράς μπλοκ δεδομένων (block mode data transfers). Για παράδειγμα η μεταφορά αποτελεσμάτων μιας ανάλυσης κραδασμού (vibration analysis).
- Συναρτήσεις διοχέτευσης (Tunneling functions) που μεταφέρουν εντολές (commands) του HART στο δίκτυο WirelessHART και αιτήσεις (requests) από συσκευές WirelessHART.

Μέσω αυτών των σημείων πρόσβασης υπηρεσιών SAP's η πύλη (gateway) μπορεί να συνδεθεί με την εφαρμογή φιλοξενητή (host application) με διάφορα πρωτόκολλα (όπως είναι Modbus, Profibus DP, ControlNet, HART OPC server, δίκτυα με δικά τους ιδιοταγή πρωτόκολλα, ή άλλα) που βασίζονται σε διαφορετικά φυσικά στρώματα όπως είναι RS-485, Ethernet LAN, Wi-Fi, και άλλα.

Για να υποστηριχθούν τα σημεία πρόσβασης υπηρεσιών (Service Access Points) παρέχονται δύο τύποι διεπαφών (interface).

α) Ο πρώτος τύπος διεπαφής υποστηρίζει άμεσα τις εντολές (commands) του HART. Αυτή η διεπαφή (interface) πρέπει να υποστηρίζεται από όλες τις πύλες (gateways) που υλοποιούνται από διάφορους κατασκευαστές.

β) Ο δεύτερος τύπος διεπαφής υποστηρίζει εντολές (commands) που είναι σε μορφή XML (XML-formatted commands).

Είναι προαιρετική η διεπαφή (interface) σε XML.

3.2.7.5 Πρωτόκολλα διοχέτευσης (Tunneling Protocols)

Οι πύλες (Gateways) πρέπει να μπορούν επίσης να υποστηρίξουν τα πρωτόκολλα διοχέτευσης (tunneling protocols). Τα πρωτόκολλα διοχέτευσης (Tunneling protocols) χρησιμοποιούνται για να μεταφέρουν (relay) μηνύματα (messages) ανάμεσα στο φιλοξενητή (host) που βρίσκεται έξω από το δίκτυο WirelessHART και σε μία συσκευή προορισμού (destination device) που είναι μέρος του δικτύου WirelessHART. Όλες οι πύλες (gateways) του WirelessHART πρέπει να υποστηρίζουν εντολές του HART και του WirelessHART. Συγκεκριμένα πρέπει να υποστηρίζουν τις γενικές εντολές (universal commands) και τις εντολές κοινής πρακτικής (common practice commands). Επίσης μπορεί να υποστηρίζουν και ειδικές εντολές που ισχύουν μόνο για ορισμένες συσκευές συγκεκριμένων κατασκευαστών (manufacturer specific commands).

Πολλές κατηγορίες υπάρχουν για τις πύλες που υποστηρίζουν τη διοχέτευση (Tunneling gateways). Αυτές είναι: WirelessHART, HART πάνω σε Ethernet, ανοικτό πρωτόκολλο (open protocol) όπως είναι το TCP/IP και τα ιδιοταγή πρωτόκολλα από συγκεκριμένους προμηθευτές (Vendor Specific).

3.2.8 Αναλυτική περιγραφή για τον Φιλοξενητή (Host)

Το δίκτυο WirelessHART συνδέεται και με εξωτερικά δίκτυα, όπως είναι το δίκτυο της βιομηχανικής εγκατάστασης.

Η διεπαφή (interface) του φιλοξενητή (Host) χρησιμοποιείται για να συνδέσει clients που βρίσκονται έξω από το δίκτυο WirelessHART στο δίκτυο WirelessHART και σε συσκευές (devices) που είναι μέσα στο δίκτυο WirelessHART.

Οι διεπαφές φιλοξενητή (Host interfaces) είναι διαθέσιμες με πολλές διαφορετικές μορφές. Οι πιο κοινές μορφές είναι:

- Ethernet-to-wireless Συσκευή πύλης (gateway Device)

Είναι μία συσκευή πύλης (gateway device) που περιέχει μία διαδρομή διπλής κατεύθυνσης (bidirectional path) ανάμεσα στα ενσύρματα βιομηχανικά δίκτυα Ethernet (industrial Ethernet Networks) και στο ασύρματο δίκτυο WirelessHART.

- Wi-Fi-to-wireless συσκευή πύλης (gateway device)

Είναι παραλλαγή της παραπάνω πύλης (gateway) της μορφής Ethernet-to-wireless αλλά τώρα αυτή η πύλη χρησιμοποιεί το ασύρματο δίκτυο 802.11 a/b/g radio για να συνδεθεί στο δίκτυο της βιομηχανικής εγκατάστασης (plant's network).

- Serial-to-wireless συσκευή πύλης (gateway device)

Αν στη βιομηχανική εγκατάσταση αυτοματισμού (plant automation) οι υπολογιστές servers και ο εξοπλισμός τους υποστηρίζουν σειριακές διεπαφές (serial interfaces), τότε μπορεί να χρησιμοποιηθεί η συσκευή πύλης (gateway device) serial-to-wireless για να συνδεθεί στις σειριακές διεπαφές (serial interfaces) των συσκευών.

3.2.8.1 Η λειτουργία της πύλης ως μεταφραστής (translator)

Οι πύλες (gateways) του WirelessHART πρέπει να μπορούν να αποθηκεύουν στην κρυφή μνήμη (cache) τις εντολές (commands) της λειτουργίας καταιγισμού (burst mode), αρκετές εντολές (commands) που χρησιμοποιούνται συχνά για ανάγνωση (read) και για εγγραφή (write), και διαγνώσεις (diagnostics). Για να μπορεί να εκμεταλλευτεί αυτή την αποθήκευση στην κρυφή μνήμη (caching), η πύλη (gateway) πρέπει να μπορεί επίσης να λειτουργήσει και ως μεταφραστής (translator). Ως μεταφραστής (translator), η πύλη (gateway) έχει δική της βάση δεδομένων πραγματικού χρόνου (real-time database). Η πύλη δέχεται πολλές αιτήσεις (requests) από τους φιλοξενητές (Hosts) και φτάνει σε μέγιστες τιμές (peeks) του πλήθους αιτήσεων. Αν αποθηκεύονται στην κρυφή μνήμη (cached) τα δεδομένα αποκρίσεων (response data) και είναι επίκαιρα (current), τότε η πύλη επιστρέφει αμέσως τα αποθηκευμένα στην κρυφή μνήμη (cached) μηνύματα αποκρίσεων (response messages) από τη δική της βάση δεδομένων πραγματικού χρόνου (real-time database). Έτσι δεν καθυστερούν οι φιλοξενητές (hosts) να πάρουν απόκριση.

Για παράδειγμα αν ένας client σε έναν φιλοξενητή (host) αναφέρει την εντολή HART command 0 για να κάνει μία αίτηση (request) σε μία συσκευή (device) στο δίκτυο, τότε η πύλη (gateway) θα κάνει έναν έλεγχο για να δει αν έχει αποθηκευμένη στην κρυφή μνήμη (cached) μία απόκριση (response) στην εντολή command 0. Αν η πύλη (gateway) δεν έχει αποθηκευμένη στην κρυφή μνήμη (cached) μια απόκριση (response) στην εντολή command 0, τότε η πύλη θα προωθήσει την εντολή (command) στη συσκευή (device) και θα επιστρέψει την απόκριση (response) από τη συσκευή στον client. Αν όμως

ήταν ήδη αποθηκευμένη η απόκριση στην κρυφή μνήμη, τότε θα επέστρεφε πιο γρήγορα στον client.

Οι λειτουργίες μετάφρασης (translation functions) μπορούν να συμπεριληφθούν. Οι λειτουργίες μετάφρασης αντιμετωπίζουν αλληλεπιδράσεις με το στρώμα δικτύου (network layer) καθώς και κάποιες αλληλεπιδράσεις (interactions) με το στρώμα εφαρμογών (application layer). Στο στρώμα δικτύου (network layer), υπάρχουν διαφορετικά μεγέθη στα πακέτα των αποκρίσεων (response packets) και αυτό πρέπει να αντιμετωπισθεί και επίσης γίνεται μία αντιστοίχιση (mapping) της ασφάλειας (security), της προτεραιότητας (priority), των διευθύνσεων (addresses) και άλλων ζητημάτων.

3.2.8.2 Μηνύματα αποκρίσεων αποθηκευμένα στην κρυφή μνήμη (Cached Response Messages)

Επειδή είναι επιθυμητό να υπάρχει γρήγορη απόκριση (response) της πύλης και του διαχειριστή δικτύου σε αιτήσεις (requests) που προέρχονται από τον φιλοξενητή (host), για αυτό, διάφορα μηνύματα αποκρίσεων (response messages) είναι αποθηκευμένα στην κρυφή μνήμη (cache) της πύλης ή του διαχειριστή δικτύου. Αυτά τα μηνύματα είναι:

α) Κατάσταση του δικτύου (Network Status)

Κάθε δικτυακή συσκευή (Network Device) διατηρεί διαγνώσεις (diagnostics). Οι διαγνώσεις (diagnostics) δημοσιεύονται (published) περιοδικά στο διαχειριστή δικτύου (network manager) με τη βοήθεια εντολών (commands) του HART. Ο διαχειριστής δικτύου (network manager) διατηρεί ένα πλήρες σύνολο από διαγνώσεις (diagnostics) των συσκευών και του δικτύου. Οι φιλοξενητές (Hosts) μπορούν να υποβάλλουν ερώτημα (query) στην πύλη (gateway) ή στον διαχειριστή δικτύου (network manager) για διαγνώσεις (diagnostics) συνολικά για το δίκτυο (network level).

β) Burst Mode Command Responses

Αποκρίσεις εντολών για την λειτουργία καταιγισμού.

Η βάση δεδομένων (database) αποθηκεύει στην κρυφή μνήμη (caches) όλα τα μηνύματα απόκρισης (response messages) από τη λειτουργία καταιγισμού (burst mode).

γ) Event Notification Command Responses

Αποκρίσεις εντολών για ειδοποιήσεις συμβάντων

Η βάση δεδομένων (database) αποθηκεύει στην κρυφή μνήμη (caches) όλα τα μηνύματα απόκρισης (response messages) από την ειδοποίηση συμβάντων (event notification).

δ) Cached Command Responses

Αποκρίσεις εντολών αποθηκευμένες στην κρυφή μνήμη.

Η βάση δεδομένων (database) αποθηκεύει στην κρυφή μνήμη (caches) τα τελευταία μηνύματα αποκρίσεων (response messages) για αρκετές εντολές (commands). Αυτές οι εντολές (commands) συνοψίζονται παρακάτω.

ε) Delayed Response Command Responses

Αποκρίσεις εντολών για καθυστερημένη απόκριση

Για τις εντολές (commands) του HART που έχουν τη μορφή αίτηση/απόκριση (request/response), η πύλη (gateway) διατηρεί μία πλήρη λίστα από όλες τις εντολές που εκκρεμούν (outstanding commands). Αυτές είναι εντολές που έχουν σταλθεί σε συσκευές (devices) αλλά ακόμη δεν έχει ληφθεί μία απόκριση (response) ως επιστροφή. Οι εντολές της καθυστερημένης απόκρισης (Delayed Response Commands) πρέπει να εκκαθαρίζονται αν ξεπεραστεί η προθεσμία που είναι 24 ώρες.

3.2.9 Αναλυτική περιγραφή του Διαχειριστή δικτύου (Network Manager) (NM) και του διαχειριστή ασφάλειας (Security Manager) (SM)

Ο διαχειριστής δικτύου (network manager) αντιμετωπίζεται από το δίκτυο ως τύπος δικτυακής συσκευής (Network Device). Με αυτό τον τρόπο οι συσκευές HART μπορούν να ανταλλάσσουν εντολές (Commands) του HART με τον διαχειριστή δικτύου (network manager).

3.2.9.1 Γενικά για τον διαχειριστή δικτύου (Network Manager) (NM)

Ο διαχειριστής δικτύου (network manager) έχει την ευθύνη για τη συνολική διαχείριση (management), τον χρονοπρογραμματισμό (scheduling), και τη βελτιστοποίηση (optimization) του δικτύου WirelessHART. Ένα μέρος από τα καθήκοντα του διαχειριστή δικτύου (network manager) είναι να αρχικοποιεί (initialize) και να διατηρεί (maintain) τιμές παραμέτρων που απαιτούνται για την επικοινωνία στο δίκτυο (network communication). Ο διαχειριστής δικτύου (network manager) παρέχει μηχανισμούς για συσκευές πεδίου (field devices) που συνδέονται (join) ή φεύγουν (leave) από το δίκτυο. Επίσης έχει την ευθύνη να διαχειρίζεται τους πόρους του δικτύου (network resources) οι οποίοι ενδέχεται είτε να είναι αφιερωμένοι (dedicated) σε μία μόνο συσκευή είτε να είναι διαμοιραζόμενοι (shared) για κοινή χρήση από πολλές συσκευές. Ο διαχειριστής δικτύου (network manager) επικοινωνεί με τις συσκευές (devices) στο δίκτυο WirelessHART μέσω του στρώματος δικτύου (network layer) το οποίο περιγράφεται στην προδιαγραφή του διαχειριστή δικτύου (Network Management Specification). Οι εντολές (commands) που χρησιμοποιεί ο διαχειριστής δικτύου (network manager) για έναρξη (setup), παρακολούθηση (monitor), και διαχείριση (manage) συνολικά για το δίκτυο περιγράφονται στην προδιαγραφή εντολών κοινής πρακτικής (Common Practice Command Specification) και στην προδιαγραφή εντολών ασύρματου δικτύου (Wireless Commands Specification). Ο διαχειριστής δικτύου (network manager) επίσης έχει την ευθύνη να συλλέγει (collect) και να διατηρεί (maintain) διαγνώσεις (diagnostics) σχετικά με τη συνολική «υγεία» του δικτύου. Αυτές οι διαγνώσεις (diagnostics) είναι διαθέσιμες και μπορούν να αναφέρονται (reported) στις εφαρμογές φιλοξενητή (host-based applications). Οι διαγνώσεις (diagnostics) χρησιμοποιούνται επίσης για την προσαρμογή ολόκληρου του δικτύου σε συνθήκες που μεταβάλλονται.

Για να εκτελέσει το πλήρες σύνολο των λειτουργιών του (functions) ο διαχειριστής δικτύου (network manager) χρειάζεται πληροφορίες για:

α) τις συσκευές (devices) τις ίδιες.

β) πληροφορίες σχετικά με το πώς θα χρησιμοποιηθεί το δίκτυο,

γ) απάντηση (feedback) από το δίκτυο για το πόσο καλά λειτουργεί το δίκτυο. Τις απαιτούμενες πληροφορίες για ρυθμίσεις (configuration) των συσκευών καθώς και πληροφορίες για την εγκατάσταση (setup) των συσκευών (devices) ο διαχειριστής δικτύου (network manager) μπορεί να τις διαβάσει από τις ίδιες τις συσκευές.

Οι συσκευές (devices), οι εφαρμογές (applications), και οι χρήστες (users) μπορούν να κάνουν αίτηση (request) για να χρησιμοποιήσουν τους πόρους επικοινωνιών (Communication resources) του δικτύου. Η απάντηση (Feedback) για το πόσο καλά αποδίδει το δίκτυο παρέχεται από τις ίδιες τις συσκευές (devices) μέσω των διαγνώσεων (diagnostics) και των αναφορών για την υγεία του συστήματος (health reports). Ο χρήστης διαχειριστής/συντηρητής (administrator/maintenance) αλληλοεπιδρά με την εφαρμογή του διαχειριστή δικτύου (network manager application) η οποία παράγει ένα πακέτο ελέγχου (control packet) διαχείρισης δικτύου (network management) στις δικτυακές συσκευές (Network Devices). Τα πακέτα του διαχειριστή δικτύου (Network Management packets) κινούνται μέσα στην ιεραρχία στρωμάτων, δηλαδή κινούνται μέσω του στρώματος δικτύου (Network layer), μετά μέσω του στρώματος ζεύξης δεδομένων (Data-Link layer) και του φυσικού στρώματος (Physical layer) και τέλος εκπέμπονται ασύρματα (transmitted) για να φτάσουν στη συσκευή προορισμού (destination device).

3.2.9.2 Βασικές λειτουργίες διαχειριστή δικτύου (Network Manager) (NM)

Οι βασικές λειτουργίες του διαχειριστή δικτύου είναι ένα σύνολο σημαντικών λειτουργιών που αφορούν συνολικά ολόκληρο το δίκτυο και λέγονται συναρτήσεις πυρήνα του δικτύου (Core Network Functions).

Ο διαχειριστής δικτύου (network manager) σχηματίζει το δίκτυο WirelessHART, συνδέει (joins) στο δίκτυο και ρυθμίζει (configures) νέες δικτυακές συσκευές (Network Devices) και παρακολουθεί το δίκτυο. Ο διαχειριστής δικτύου (network manager) χρησιμοποιεί πληροφορίες διαγνώσεων (diagnostic information) για να κάνει διάφορες τροποποιήσεις στην τοπολογία του δικτύου. Όλες αυτές οι μετατροπές γίνονται σε μία συνεχή βάση και

έτσι αυτή λειτουργία (operation) συνολικά αναφέρεται ως προσαρμογή (adapting) ή βελτίωση (grooming) του δικτύου.

Η αρχιτεκτονική του δικτύου WirelessHART δεν θέτει κάποιο περιορισμό ως προς τη φυσική θέση που θα πρέπει να βρίσκεται ο διαχειριστής δικτύου (network manager) μέσα στην βιομηχανική εγκατάσταση αυτοματισμού (plant automation network). Ο διαχειριστής δικτύου (network manager) μπορεί να συστεγάζεται μαζί με την πύλη (gateway) μέσα στο ίδιο κουτί (box) ή να τοποθετηθεί μόνος του σε ένα πλήρως ξεχωριστό κουτί (box) που βρίσκεται σε μία διαφορετική φυσική θέση.

Κάθε μεμονωμένο δίκτυο WirelessHART πρέπει να έχει μόνο έναν διαχειριστή δικτύου (network manager).

Ένας διαχειριστής δικτύου (network manager) όμως, μπορεί να καλύπτει πολλαπλά δίκτυα WirelessHART.

3.2.9.3 Σύνδεση μεταξύ του διαχειριστή δικτύου (Network Manager) και του διαχειριστή ασφαλείας (Security Manager)

Ο διαχειριστής ασφαλείας (Security Manager) και ο διαχειριστής δικτύου (network manager) έχουν την ευθύνη για να δημιουργήσουν και να διατηρήσουν μία σύνδεση μεταξύ τους, ώστε να μπορούν να υποστηρίζουν τις αιτήσεις (requests) για ένταξη στο δίκτυο (join) που στέλνουν συσκευές (devices) καθώς και να μπορούν να δημιουργούν συνεδρίες επικοινωνίας (sessions). Η σύνδεση ανάμεσα στο διαχειριστή δικτύου (network manager) και στο διαχειριστή ασφαλείας (Security Manager) και η μέθοδος προστασίας της δεν περιγράφονται στο πρότυπο WirelessHART. Ο διαχειριστής ασφαλείας (Security Manager) είναι πλήρως κρυμμένος ώστε δεν γνωρίζουν την ύπαρξή του οι πύλες (gateways) και δεν μπορούν να τον δουν. Αυτό ονομάζεται διαφάνεια (transparency), δηλαδή λέμε ότι ο διαχειριστής ασφαλείας είναι διαφανής για τις πύλες (gateways).

3.2.9.4 Γενικά για τον διαχειριστή ασφαλείας (Security Manager)(SM)

Ο διαχειριστής ασφαλείας (Security Manager) λειτουργεί μαζί με τον διαχειριστή δικτύου (network manager) για να προσθέσει ασφάλεια στο δίκτυο WirelessHART και να το προστατέψει από διάφορες απειλές που εμφανίζονται κατά την λειτουργία του. Ο διαχειριστής ασφαλείας (Security Manager) δημιουργεί και διαχειρίζεται κρυπτογραφήσεις που χρησιμοποιούνται από το δίκτυο. Έχει ευθύνη για τη δημιουργία (generation), αποθήκευση (storage), και διαχείριση των κλειδιών (keys). Ο διαχειριστής ασφαλείας (Security Manager) συνεργάζεται στενά μαζί με τον διαχειριστή δικτύου (network manager) σε μία αρχιτεκτονική server/client. Ο διαχειριστής ασφαλείας (Security Manager) παρουσιάζεται ξεχωριστά από τον διαχειριστή δικτύου (network manager) διότι ο διαχειριστής ασφαλείας μπορεί να είναι μία κεντρική μονάδα λειτουργιών (centralized function) σε μερικά δίκτυα αυτοματισμού βιομηχανικών εγκαταστάσεων (plant automation networks), που καλύπτει περισσότερα από ένα δίκτυα WirelessHART και σε μερικές περιπτώσεις καλύπτει και άλλα δίκτυα και εφαρμογές. Υπάρχει μόνο ένας διαχειριστής ασφαλείας (Security Manager) που αντιστοιχεί σε ένα δίκτυο WirelessHART. Απαιτείται να υπάρχει μία ασφαλής σύνδεση ανάμεσα στον διαχειριστή δικτύου (network manager) και στον διαχειριστή ασφαλείας (Security Manager). Αυτή η ασφαλής σύνδεση δεν περιγράφεται στην προδιαγραφή και έτσι μπορεί να γίνει με διαφορετικούς τρόπους.

3.2.9.5 Διαγνώσεις του δικτύου (Network Diagnostics)

Ο διαχειριστής δικτύου (network manager) εκτελεί διάφορες λειτουργίες. Μία από αυτές είναι να συλλέγει πληροφορίες για την απόδοση του δικτύου (network performance) και για διαγνώσεις (diagnostic). Σε αυτές τις πληροφορίες υπάρχει πρόσβαση κατά το χρόνο εκτέλεσης (run-time) και έτσι είναι δυνατόν ο διαχειριστής δικτύου (network manager) να δει και να αναλύσει τη συμπεριφορά ολόκληρου του δικτύου. Αν ανιχνευθούν προβλήματα, εκτελούνται εκ νέου ρυθμίσεις για το δίκτυο ενώ το δίκτυο βρίσκεται σε λειτουργία. Η πρόσβαση στις πληροφορίες διαγνώσεων (diagnostic) επιτυγχάνεται μέσω των εντολών (commands) του HART.

3.2.9.6 Βελτίωση της απόδοσης του δικτύου (Network Performance)

Το δίκτυο WirelessHART χρησιμοποιεί διάφορους μηχανισμούς ώστε να διατηρεί μία μεγάλη αξιοπιστία και να έχει μια βελτιωμένη απόδοση. Τέτοιοι μηχανισμοί είναι:

- α) Πολλαπλές εναλλακτικές διαδρομές (multiple paths) προς τις δικτυακές συσκευές (network devices),
- β) πολλαπλά ασύρματα κανάλια RF,
- γ) πολλαπλές επαναληπτικές προσπάθειες επικοινωνίας.

Όταν απαιτείται βελτίωση στην αξιοπιστία, μπορούν να προστεθούν περισσότερες διαδρομές (paths) και αυτό γίνεται αν εισαχθούν στο δίκτυο περισσότερα σημεία πρόσβασης (Access Points) του WirelessHART και περισσότερες συσκευές πεδίου (field devices). Έτσι γίνεται μία επέκταση του δικτύου πλέγματος (mesh network). Όταν προστίθενται στο δίκτυο περισσότερες συσκευές πεδίου (field devices), τότε θα υπάρχουν και περισσότερες εναλλακτικές διαδρομές πολλαπλών αλμάτων (multi-hop paths) προς τους ίδιους προορισμούς, ώστε θα υπάρχει ένα μεγάλο πλήθος διαφορετικών διαδρομών (path diversity). Συνεπώς, σε περίπτωση που θα αποκλειστεί μία διαδρομή για διάφορους λόγους, όπως είναι π.χ μία ξαφνική βλάβη σε μία συσκευή πεδίου, τότε τα δεδομένα θα μπορούν να φτάσουν στον προορισμό τους ακολουθώντας μια άλλη διαδρομή. Τα επιπρόσθετα σημεία πρόσβασης (Access Points) του WirelessHART και γενικά οι επιπρόσθετες συσκευές (devices) αυξάνουν την απόδοση (throughput), μειώνουν την καθυστέρηση (latency), και μπορούν να χρησιμοποιούνται για δρομολόγηση (route) σε εναλλακτικές διαδρομές ώστε να παρακάμπτουν πιθανά σημεία με πηγές παρεμβολών και να στέλνουν τα δεδομένα σε άλλες διαδρομές γύρω από αυτά.

3.2.10 Συγχρονισμός Επικοινωνίας με βάση τις σχισμές χρόνου (time slots)

Η επικοινωνία είναι συγχρονισμένη με βάση τις σχισμές χρόνου (Time-synchronized Communication).

Όλη η επικοινωνία στο δίκτυο WirelessHART είναι συγχρονισμένη (time-synchronized). Η βασική μονάδα μέτρησης είναι η σχισμή χρόνου (time slot) που είναι μία μονάδα χρόνου με σταθερή διάρκεια (fixed time duration) και είναι διαμοιραζόμενη μέσα στο δίκτυο από όλες τις δικτυακές συσκευές (Network Devices). Η διάρκεια (duration) μίας χρονικής σχισμής (time slot) είναι επαρκής ώστε να μπορεί να αποσταλεί ή να ληφθεί ένα πακέτο δεδομένων για κάθε ένα κανάλι και αμέσως ο προορισμός να επιστρέψει πίσω προς την πηγή ένα αντίστοιχο μήνυμα αναγνώρισης (acknowledgement) που λέγεται ACK και συνοδεύει (accompanying) συνήθως την αποστολή του πακέτου και δηλώνει ότι λήφθηκε επιτυχώς το πακέτο. Επιπλέον η επικοινωνία με σχισμές χρόνου (time slots) περιλαμβάνει και τους χρόνους φρουρούς (guard-band times) κατά τους οποίους δεν μεταδίδονται δεδομένα και χρησιμοποιούνται ώστε να υπάρχει ένας συγχρονισμός για ολόκληρο το δίκτυο (network-wide synchronization).

Η αξιολόγηση ανά κανάλι (per-channel qualification) δείχνει ότι στην ίδια χρονική σχισμή (time slot) μπορούν να συμβούν περισσότερες από μία επικοινωνίες. Ο συγχρονισμός με ακρίβεια είναι κρίσιμος για τη λειτουργία των δικτύων που βασίζονται σε TDMA (Πολυπλεξία διαίρεσης χρόνου). Επειδή όλες οι επικοινωνίες γίνονται σε σχισμές χρόνου (time slots), οι δικτυακές συσκευές (Network Devices) πρέπει να έχουν την ίδια αντίληψη του χρόνου (notion) για το πότε κάθε χρονική σχισμή (time slot) αρχίζει και πότε τελειώνει με μία ελάχιστη παραλλαγή (variation). Το πρωτόκολλο WirelessHART καθορίζει κάποιους μηχανισμούς για συγχρονισμό με βάση τις σχισμές χρόνου (time synchronization). Στο δίκτυο WirelessHART ο χρόνος διαδίδεται προς τα έξω (outward) από την πύλη (gateway) δηλαδή η πύλη παρέχει ένα ρολόι συγχρονισμού.

3.2.10.1 Οι συνεδρίες (Sessions) στο στρώμα Δικτύου (Network Layer)

Τα στρώματα του WirelessHART περιγράφονται σε επόμενη παράγραφο. Το στρώμα δικτύου (Network Layer) διαχειρίζεται τις επικοινωνίες από σημείο σε σημείο (End-to-end) χρησιμοποιώντας συνεδρίες (sessions). Κάθε συνεδρία (session) περιλαμβάνει πληροφορίες ασφάλειας για ένα ζεύγος (pair) ή μία ομάδα (group) από δικτυακές συσκευές (network devices). Όλες οι δικτυακές συσκευές (network devices) έχουν δύο συνεδρίες (sessions) με τον διαχειριστή δικτύου (network manager):

α) συνεδρία για επικοινωνία ζεύγους (pair wise communication) με βάση τον διαχειριστή δικτύου,

β) συνεδρία για επικοινωνία με εκπομπή (broadcast) από τον διαχειριστή δικτύου (network manager) προς όλους τους κόμβους του δικτύου (network broadcast communication).

Επίσης όλες οι συσκευές (devices) έχουν δύο κλειδιά (keys) που τα χρησιμοποιούν για τις συνεδρίες τους με τον διαχειριστή δικτύου. Τα κλειδιά αυτά ονομάζονται network manager session keys. Οι συνεδρίες (sessions) διακρίνονται (distinguished) μεταξύ τους, με βάση τις διευθύνσεις (addresses) των δικτυακών συσκευών (Network Device) που έχουν ανατεθεί (assigned) σε αυτές τις συνεδρίες.

Για μία συνεδρία ζεύγους (pair wise session) με τον διαχειριστή δικτύου (network manager), χρησιμοποιείται η τυπική διεύθυνση της δικτυακής συσκευής (standard Network Device address).

Για μία συνεδρία εκπομπής προς όλους τους κόμβους (broadcast session), θα χρησιμοποιηθεί μία ειδική διεύθυνση της δικτυακής συσκευής (special Network Device address) που είναι η 0xFFFF.

3.2.10.2 Σύνδεση ανάμεσα στην πύλη (Gateway) και στον διαχειριστή δικτύου (Network Manager)

Η διεπαφή (interface) ανάμεσα στην πύλη (gateway) και στο διαχειριστή δικτύου (network manager) δεν περιγράφεται από το πρωτόκολλο WirelessHART. Αυτό σημαίνει ότι μπορούν να γίνουν πολλές διαφορετικές υλοποιήσεις. Ο διαχειριστής δικτύου (network manager) και η πύλη (gateway) έχουν την ευθύνη για να δημιουργούν μία ασφαλή σύνδεση μεταξύ τους, και να διατηρούν τη σύνδεση αυτή για να εκτελούν ελέγχους (control) και για να κατευθύνουν την κυκλοφορία των δεδομένων (data traffic). Έτσι δεν είναι απαραίτητο για την πύλη (gateway) να ακολουθήσει την συνηθισμένη διαδικασία σύνδεσης (join process) όπως απαιτείται από μια δικτυακή συσκευή (network device). Όταν η πύλη (gateway) συνδεθεί στο διαχειριστή δικτύου (network manager), ο διαχειριστής δικτύου (network manager) μπορεί να ρυθμίσει την πύλη

(gateway) να ξεκινήσει να στέλνει μηνύματα διαφήμισης (advertising) προς άλλες συσκευές (devices). Μόλις καθοριστούν (establish) διαδρομές επικοινωνίας (communication paths) τότε ο διαχειριστής δικτύου (network manager) δεν συμμετέχει στις επικοινωνίες που γίνονται μεταξύ των εφαρμογών φιλοξενητή (host applications) και των δικτυακών συσκευών (network devices). Η πύλη (gateway) έχει την ευθύνη για αυτές τις επικοινωνίες.

Δηλαδή η πύλη αναλαμβάνει:

α) την αποθήκευση σε ενδιάμεση μνήμη (buffering),

β) τις επικοινωνίες μεταξύ διαφορετικών πρωτοκόλλων (protocol conversions), γ) τις προθεσμίες (timeouts),

δ) το ρολόι συγχρονισμού (time clock),

καθώς και άλλες διεργασίες που απαιτούνται για την επικοινωνία ανάμεσα στις εφαρμογές φιλοξενητή (host applications) και στις δικτυακές συσκευές (network devices).

3.2.10.3 Δημιουργία χρονοπρογραμματισμού (Scheduling) από τον Διαχειριστή Δικτύου

Οι βασικές λειτουργίες (functions) του διαχειριστή δικτύου (network manager) είναι να κάνει χρονοπρογραμματισμό (schedule), να παρακολουθεί (monitor), να διαχειρίζεται (manage), και να βελτιστοποιεί τους πόρους επικοινωνιών (communication resources) του δικτύου. Ο διαχειριστής δικτύου (network manager) για να δημιουργήσει το χρονικό πρόγραμμα (schedule) λαμβάνει υπόψη του πολλές παραμέτρους. Συνδυάζει (combines) τις πληροφορίες που έχει σχετικά με την τοπολογία του δικτύου, μαζί με διάφορες ευρετικές μεθόδους (heuristics) που σχετίζονται με τις απαιτήσεις των επικοινωνιών (communication requirements) και λαμβάνει αιτήσεις (requests) για τη χρήση πόρων επικοινωνιών (communication resources) από δικτυακές συσκευές (network devices) και εφαρμογές (applications).

Η πιο σημαντική λειτουργία του διαχειριστή δικτύου (network manager) είναι να κάνει τον χρονοπρογραμματισμό (schedule) για τους πόρους επικοινωνιών (communication

resources). Για να τα καταφέρει να τοποθετήσει μαζί αποτελεσματικά (efficient) και βελτιστοποιημένα τα διαφορετικά προγράμματα χρόνου (schedules), ο διαχειριστής δικτύου (network manager) απαιτείται να διαθέτει πληροφορίες για όλο το δίκτυο, πληροφορίες για τις απαιτήσεις των επικοινωνιών και πληροφορίες για τις δυνατότητες των ίδιων των δικτυακών συσκευών (network devices). Ο διαχειριστής δικτύου (network manager), καθώς ανακαλύπτει σταδιακά όλες αυτές τις πληροφορίες, κάνει αλλαγές στο χρονικό πρόγραμμα (schedule) μέχρι να πετύχει να καλύψει όλες τις απαιτήσεις του δικτύου. Τότε ο χρονοπρογραμματιστής (scheduler) χρησιμοποιεί την ανατροφοδότηση (feedback) από τη λειτουργία του συστήματος για να συντονίσει (tune) το χρονικό πρόγραμμα (schedule).

3.2.10.4 Απαιτήσεις για τον διαχειριστή δικτύου (Network Manager)

Ο διαχειριστής δικτύου (network manager) (NM) έχει κεντρικό ρόλο για την λειτουργία ολόκληρου του δικτύου WirelessHART. Ο διαχειριστής δικτύου (network manager) έχει ευθύνη να δημιουργεί το δίκτυο, να καθορίζει πορείες δρομολόγησης (routes), να κάνει χρονοπρογραμματισμό (scheduling) για τους πόρους επικοινωνίας (communication resources), να παρακολουθεί (monitoring) την «υγεία» του δικτύου, να κάνει προσαρμογές (adapting) και συνεχείς αλλαγές στο δίκτυο και να συνεργάζεται μαζί με τον διαχειριστή ασφαλείας (Security Manager) για την κατανομή (allocate) και διαχείριση (manage) των κλειδιών συνεδρίας (Session Keys).

Το γενικό σύνολο των απαιτήσεων παρουσιάζεται συνοπτικά στον πίνακα 3.6.

Λειτουργία δικτύου (Network Function)	Απαιτήσεις Διαχειριστή Δικτύου (Network Manager) (NM)
Διαμόρφωση δικτύου (formation) και ρυθμίσεις (Configuration)	Παρέχει τη λογική για να εκκινήσει τον εαυτό της και να ξεκινήσει την λειτουργία ενός δικτύου
-	Διαχειρίζεται την τοπολογία. Κατανοεί την τοπολογία του δικτύου. Προσαρμόζει (adapts) το δίκτυο κάνοντας αλλαγές καθώς λαμβάνει πληροφορίες διαγνώσεων από τις συσκευές.
-	Διαχειρίζεται το κλειδί δικτύου (Network Key). Το κλειδί δικτύου (Network Key) παρέχεται στον διαχειριστή

	δικτύου (Network Manager) από τον διαχειριστή ασφαλείας (Security Manager) και παρέχεται σε όλες τις δικτυακές συσκευές (Network Devices). Ο διαχειριστής δικτύου (Network Manager) κατανέμει το κλειδί δικτύου (Network Key) και το αλλάζει όταν απαιτείται από την πολιτική ασφαλείας της βιομηχανικής εγκατάστασης.
-	Ξεχωριστά κλειδιά (keys) για τον διαχειριστή δικτύου (Network Manager) και για την πύλη (Gateway) χρησιμοποιούνται για μετάδοση μόνο σε έναν κόμβο (unicast) και για μετάδοση σε όλους τους κόμβους (broadcast) δεδομένων σε κυκλοφορία (traffic) τα οποία προέρχονται από τον διαχειριστή δικτύου (Network Manager) και από την πύλη (Gateway).
-	Διαχειρίζεται την διαδικασία σύνδεσης (Join process). Ο διαχειριστής δικτύου (Network Manager) κάνει επικύρωση (validates) στις συσκευές (devices) που επιθυμούν να συνδεθούν (join) στο δίκτυο. Μετά από την πιστοποίηση μίας δικτυακής συσκευής (Network Device), ο διαχειριστής δικτύου (Network Manager) δίνει στη διαδικτυακή συσκευή Network Device, που συνδέεται (join), το κλειδί δικτύου (network key) και 4 κλειδιά συνόδων (session keys) 1 - Network Manager unicast session keys 2 - Network Manager broadcast session key 3 - Gateway unicast session key 4 - Gateway broadcast session key Οι συσκευές (Devices) πρέπει να ρυθμίζονται (configured) με το NetworkId ανεξάρτητα από το διαχειριστή δικτύου (network manager) ώστε να συνδεθούν (join) κανονικά στο δίκτυο. Το NetworkId είναι χρήσιμο για να βρουν το σωστό δίκτυο.
-	Αναθέτει (Assigns) διευθύνσεις 16-bit Nicknames. Ο διαχειριστής δικτύου (Network Manager) αναθέτει (assigns) και διαχειρίζεται διευθύνσεις του δικτύου (network addresses) που είναι μοναδικές 16-bit Nicknames σε κάθε δικτυακή συσκευή (Network Device). Ο διαχειριστής δικτύου (Network Manager) είναι υπεύθυνος για να εξασφαλίσει ότι ο πίνακας με τους γείτονες (Neighbor

	Table) που υπάρχει σε κάθε συσκευή είναι ενημερωμένος (up-to-date).
-	Δημιουργεί μία σύνδεση με την πύλη (Gateway). Κάθε φορά που η πύλη (Gateway) (μέσω των σημείων πρόσβασης Access Points της πύλης Gateway) λαμβάνει μηνύματα (messages) που προορίζονται για τον διαχειριστή δικτύου (Network Manager) η πύλη προωθεί τα μηνύματα αυτά στον διαχειριστή δικτύου (Network Manager).
-	Ρυθμίζει τουλάχιστον ένα σημείο πρόσβασης (Access Point) από αυτά που υπάρχουν στην πύλη (gateway) να παρέχει το ρολόι δικτύου (network clock)
-	Διαχειρίζεται τις ρυθμίσεις δικτύου network configuration. Διατηρεί έναν πλήρη χάρτη των ρυθμίσεων δικτύου (network configuration), που περιλαμβάνει οποιαδήποτε πληροφορία σχετικά με το δίκτυο που είναι καταναμεμένη στις δικτυακές συσκευές (network devices).
	Δίνει μία απόκριση (response) για κάθε αίτηση (request) που αναζητά πληροφορίες του δικτύου. Για παράδειγμα όταν μία εφαρμογή φιλοξενητή (host application) κάνει μία αίτηση (request) για όλες τις δικτυακές συσκευές (Network Devices) που υπάρχουν στο δίκτυο, ο διαχειριστής δικτύου (Network Manager) έχει την ευθύνη να παρέχει την απόκριση (response).
Δρομολόγηση (Routing)	Δημιουργεί και διαχειρίζεται τη διαδρομή δρομολόγησης του δικτύου (network route). Η διαδρομή δρομολόγησης του δικτύου (network route) είναι ένας πλήρης χάρτης του δικτύου.
-	Διαχειρίζεται τους πίνακες γειτόνων (Neighbor tables). Ο διαχειριστής δικτύου (Network Manager) συλλέγει στατιστικά του δικτύου (network statistics) και τις πληροφορίες του πίνακα γειτόνων (neighbor table) από κάθε συσκευή (device) μέσω των περιοδικών αναφορών «υγείας» (periodic health reports). Αυτές οι πληροφορίες χρησιμοποιούνται για να προσαρμόζεται το δίκτυο σε αλλαγές.
-	Δημιουργεί πίνακες διαδρομών δρομολόγησης (route tables) για δρομολόγηση με γραφήματα (Graph routing). Η

		δρομολόγηση με γραφήματα (Graph Routing) είναι κατάλληλη λύση για επικοινωνίες (scheduled upstream communications) και (downstream communications). Οι Upstream communications περιλαμβάνουν μετρήσεις διεργασίας (process measurements) και συναγερμούς (alarms). οι Downstream communications περιλαμβάνουν αλλαγές SP στους επενεργητές (actuators).
-		Δημιουργεί λίστες διαδρομών δρομολόγησης από την πηγή (source route lists) για δρομολόγηση ξεκινώντας από την πηγή (Source routing).
-		Ανακατανέμει (Allocates) τους πόρους επικοινωνιών (communication resources) στον εαυτό του, στις πύλες (gateways) και στις συσκευές (Devices) ώστε ο διαχειριστής δικτύου (Network Manager) να μπορεί να διαχειριστεί το δίκτυο και έτσι οι συσκευές (Devices) να μπορούν να επικοινωνήσουν μεταξύ τους.
Χρονοπρογραμματισμός δικτύου (Network Schedule)		Δημιουργεί υπερπλαίσια (Superframes). Πολλαπλά υπερπλαίσια (Superframes) θα χρησιμοποιούνται για να υποστηρίξουν τις επικοινωνίες σε συγκεκριμένους ρυθμούς ανάγνωσης (scan rates). Επιπρόσθετα υπερπλαίσια (Additional Superframes) θα ανακατανέμονται (allocated) για να υποστηρίξουν τη διαχείριση των συσκευών (device management) και τις εφαρμογές διαγνώσεων (diagnostic applications) που απαιτούν μεγάλες ποσότητες δεδομένων που έχουν κυκλοφορία (traffic) για μικρές χρονικές περιόδους.
-		Αναθέτει (Assigns) τις ζεύξεις (links) στα υπερπλαίσια (Superframes)
-		Δημιουργεί πίνακες ζεύξεων (Link tables). Κάθε ζεύξη (Link) περιλαμβάνει ακριβώς μία χρονική σχισμή (slot) που συνδέεται με ένα υπερπλαίσιο (Superframe), τον τύπο του (normal, advertising, discovery, join) τις επιλογές του (transmit, receive, shared), τις πληροφορίες για τους γείτονες (neighbor information), το channel offset, και τη συσκευή (device) που συνδέεται σε αυτή τη ζεύξη (link).

-	Ενεργοποιεί (Activates) και απενεργοποιεί (Deactivates) υπερπλαίσια (Superframes) ως απόκριση (response) σε απαιτήσεις εφαρμογών (application).
-	Διατηρεί τις συνολικές πληροφορίες διαγνώσεων (diagnostic information) για το δίκτυο WirelessHART. Για παράδειγμα όταν μία δικτυακή συσκευή (Network Device) δεν έχει λάβει ένα πακέτο από έναν από τους γείτονες της μέσα στο χρόνο KeepAliveInterval, η συσκευή (device) στέλνει μία ειδοποίηση (path-down notification) στον διαχειριστή δικτύου (Network Manager) που δείχνει ότι η διαδρομή (path) δεν είναι πλέον διαθέσιμη.
Ο χρονικός προγραμματισμός του δικτύου (Network Schedule) και η διαχείριση καναλιών (Channel Management)	Παρακολουθεί (Keeps track) τα κανάλια που είναι σε μαύρη λίστα (blacklisted channels). (Η είσοδος των καναλιών σε μαύρη λίστα blacklisting είναι μία λειτουργία που δεν γίνεται αυτόματα manual operation).
-	Παρέχει την Channel Offset. Η channel offset χρησιμοποιείται για να υπολογίσει τον αριθμό καναλιού όταν γίνεται μεταπήδηση καναλιών (channel hopping). Η channel offset λαμβάνει μία τιμή από 0 ως το πλήθος καναλιών (μείον το πλήθος των καναλιών που είναι σε μαύρη λίστα blacklisted channels).
Διαγνώσεις δικτύου (Network Diagnostics) και προσαρμογές (Adapting)	Διατηρεί καταγραφές για τις πληροφορίες «υγείας» κάθε δικτυακής συσκευής (Network Device).
-	Προσαρμόζει (Adapts) το δίκτυο σε αλλαγή περιβάλλοντος και σε απαιτήσεις των εφαρμογών (application demands). Η προσαρμογή (adaptation) περιλαμβάνει την ενημέρωση πληροφοριών (updating information) για τις διαδρομές δρομολόγησης (route) και για το χρονικό πρόγραμμα (schedule).
-	Ανακατανέμει (Allocates) τους πόρους επικοινωνιών (communication resources) όπως απαιτείται από τις δικτυακές συσκευές (Network Devices). Οι συσκευές (Devices) κάνουν αίτηση (request) για χωρητικότητα του δικτύου (network capacity) για να υποστηρίξει τη λειτουργία καταιγισμού (burst mode), την ειδοποίηση συμβάντων (event notification), και την λειτουργία κυκλοφορίας μπλοκ δεδομένων (block mode traffic). Οι πύλες (Gateways) κάνουν αίτηση σε εύρος ζώνης

	(bandwidth) για να υποστηρίξουν τις απαιτήσεις του client. Η κυκλοφορία δεδομένων στο δίκτυο (Network traffic) ωθείται να ακολουθήσει (biased) κυρίως μία συγκεκριμένη διαδρομή (path) αυξάνοντας ή μειώνοντας το πλήθος ζεύξεων (links) μέσω μίας συγκεκριμένης συσκευής (device).
-	Βελτιστοποιεί τις διαδρομές δρομολόγησης (routes) και κάνει χρονοπρογραμματισμό (schedules) με στόχο να βελτιώσει τη λειτουργία του δικτύου και παράλληλα να διατηρήσει την ενέργεια στις συσκευές (devices).
-	Δημιουργία και διαχείριση κλειδιών σύνδεσης (Join Keys).
Διαχειριστής ασφαλείας (Security Manager)	Δημιουργία και διαχείριση κλειδιών συνόδου (Session Keys).

Πίνακας 3.6. Απαιτήσεις για τον διαχειριστή δικτύου (Network manager). Πηγή: [8]

Απαιτήσεις του διαχειριστή δικτύου (NM) για το χρονοπρογραμματισμό (Schedule). Οι απαιτήσεις για να γίνει το σωστό χρονικό πρόγραμμα φαίνονται συνοπτικά στον πίνακα 3.7.

Λειτουργία	Απαιτήσεις του διαχειριστή δικτύου (NM) για Χρονοπρογραμματισμό (Schedule)
Υποθέσεις (Assumptions)	Ο διαχειριστής δικτύου (Network Manager) έχει μια λογική αναπαράσταση του γραφήματος του δικτύου (network graph).
-	Κάθε συσκευή (device) έχει ρυθμιστεί με έναν πίνακα συνδέσεων (connection table)
-	Ο διαχειριστής δικτύου (Network Manager) γνωρίζει το ρυθμό ανανέωσης (update rate) για κάθε συσκευή (device).
-	Για να υπάρχει πλεονασμός (redundancy), κάποια δεδομένα ρυθμίζονται με μία μετάδοση (transmit) και μία επαναληπτική μετάδοση (retry) σε μία διαδρομή (path) και μία άλλη επαναληπτική μετάδοση (retry) σε μία άλλη διαδρομή (path).
Περιορισμοί (Constraints)	Το μέγιστο πλήθος από ταυτόχρονα ενεργά κανάλια (concurrent active channels) καθορίζεται από τον αριθμό των ενεργοποιημένων

	καναλιών (enabled channels) και περιορίζεται από τα κανάλια που μπαίνουν σε μαύρη λίστα (black-listing).
-	Καμία συσκευή (device) δεν επιτρέπεται να προγραμματιστεί χρονικά να ακούει (listen) δύο φορές σε μία χρονική σχισμή (slot).
-	Περισσότερες από μία συσκευές μπορούν να εκπέμψουν (transmit) δεδομένα προς την ίδια συσκευή (device). Π.χ. μπορεί να συνυπάρχουν μία ζεύξη εκπομπής προς όλους τους κόμβους (broadcast link) μαζί με αφιερωμένες ζεύξεις (dedicated links) για κάθε μία από τις συσκευές που ακούν (listening devices).
-	Σε μία διαδρομή πολλαπλών αλμάτων (multi-hop path), ένα πρώτο άλμα (early hop) πρέπει να προγραμματιστεί χρονικά (scheduled) να είναι πρώτο.
-	Οι ρυθμοί ανανέωσης (update rates) που υποστηρίζονται, πρέπει να καθορίζονται ως 2n όπου το 'n' έχει θετικές ή αρνητικές ακέραιες τιμές (integer values) π.χ., e.g., επιλογές ρυθμών ανανέωσης σε $\frac{1}{4}$ 250msec, $\frac{1}{2}$ 500msec, 1 sec, 2 sec, 4 sec, 8sec, 16 sec, 32 sec, and 60 sec. (ή περισσότερο).
-	Οι επικοινωνίες βάσης του διαχειριστή δικτύου (Network Management communications) και οι επικοινωνίες σε λειτουργία καταιγισμού (Burst Mode communications) δεν πρέπει να ξεπεράσουν το 30% του διαθέσιμου εύρους ζώνης επικοινωνιών (communication bandwidth) (100 slots/sec max μέγιστη τιμή).
-	Υπηρεσίες (Services) – Ο διαχειριστής δικτύου (network manager) πρέπει να λαμβάνει υπόψη τις απαιτήσεις των υπηρεσιών (service requirements).
-	Το τελικό χρονικό πρόγραμμα (schedule) χωρίς να υπολογιστεί η προδιαγραφή της πύλης (Gateway spec) θα πρέπει να έχει ελεύθερες 50% χρονικές σχισμές (slots) δηλαδή κατανεμημένες (allocated) για επαναληπτικές προσπάθειες (retries), και για να ακούν οι κόμβοι (listens).
Υπερπλαίσιο δεδομένων (Data Superframe)	Το υπερπλαίσιο δεδομένων (data Superframe) έχει μήκος (length) που καθορίζεται από το ρυθμό ανάγνωσης δεδομένων (data scan rate).
-	Ανακατανέμονται (Allocate) οι χρονικές σχισμές (slots) ξεκινώντας από το γρηγορότερο ρυθμό ανάγνωσης (scan rate) και φτάνουν στον αργότερο ρυθμό ανάγνωσης (scan rate).

-	Από τη συσκευή που βρίσκεται στο μακρινότερο άκρο, ανακατανέμει (allocate) μία ζεύξη από κάθε δικτυακή συσκευή (Network Device) που βρίσκεται στη διαδρομή (en-route) προς την πύλη (Gateway). Ανακατανέμει (Allocate) μία δεύτερη αφιερωμένη χρονική σχισμή (slot) στην ίδια διαδρομή (path) για να χειριστεί μία επαναληπτική μετάδοση (retry). Ανακατανέμει και μία τρίτη διαμοιραζόμενη (shared) χρονική σχισμή (slot) σε μία ξεχωριστή διαδρομή (path) για να χειριστεί μία δεύτερη επαναληπτική προσπάθεια (retry).
Υπερπλαίσιο διαχείρισης (Management Superframe): Διαχείριση (Management)	Το υπερπλαίσιο διαχείρισης (Management Superframe) έχει μεγαλύτερη προτεραιότητα (priority) από τα υπερπλάσια δεδομένων (data Superframes).
-	Διαπερνά το γράφημα (graph) με αλγόριθμο breath-first search, ξεκινώντας από την πύλη (gateway), και δίνει αριθμούς στις συσκευές ως εξής: N0, N1, ... Nn.
-	Κατ' ελάχιστον, κάθε συσκευή (device) πρέπει να έχει μία χρονική σχισμή (slot) για Keep-Alives και πρέπει να υπάρχει μία αντίστοιχη διαμοιραζόμενη (shared) λήψη (receive) στην πλευρά του γονέα (parent side).
Υπερπλαίσιο διαχείρισης (Management Superframe): Διαδικασία σύνδεσης (Join Process)	Αίτηση σύνδεσης (Join-Request) – από τις συσκευές που βρίσκονται πιο μακριά (furthest devices), γίνεται μία ανακατανομή (allocate) μίας ζεύξης (link) για κάθε δικτυακή συσκευή (Network Device) που βρίσκεται στη διαδρομή (enroute) προς την πύλη (Gateway). Δεν παρέχεται πλεονασμός (redundancy).
-	Απόκριση σύνδεσης (Join Response) – Διαπέραση του γραφήματος με αλγόριθμο breath-first search, ανακατανομή (allocate) μίας ζεύξης (link) για κάθε δικτυακή συσκευή (Network Device) που βρίσκεται στη διαδρομή (en-route) από την πύλη (Gateway) προς την τελική δικτυακή συσκευή (end Network Device). Δεν παρέχεται πλεονασμός (redundancy).
-	Ανακατανομή (Allocate) των πακέτων «διαφήμισης» (advertise packets) σε κάθε συσκευή (device). Το πλήθος των πακέτων διαφήμισης (advertise packets) σχετίζεται αντιστρόφως με το πλήθος αλμάτων (hops) μακριά από την πύλη (gateway).
Υπερπλαίσιο διαχείρισης (Management Superframe):	Ανακάλυψη των γειτόνων (Neighbor discovery). ο διαχειριστής δικτύου (Network Manager) πρέπει να κάνει ανακατανομή (allocate) των συνδέσμων ανακάλυψης (discovery links) που είναι κοινοί για όλες τις δικτυακές συσκευές (Network Devices). Ο discoveryInterval

Ανακάλυψη των γειτόνων (Neighbor Discovery)	timer πρέπει να τεθεί στο να επιτρέπει (enable) την ανακάλυψη (discovery).
Υπερπλαίσιο διαχείρισης (Management Superframe): Εντολές διαχείρισης δικτύου (Network Management Commands)	Διαμοιράζεται (Share) τις ζεύξεις (links) της διαχείρισης δικτύου (Network Management) με αιτήσεις σύνδεσης (join requests) και αποκρίσεις (responses).
Κυκλοφορία δεδομένων (Traffic) από εντολές (Command) αίτησης/απόκρισης (Request/Response).	Ανακατανέμει (Allocate) τις διαμοιραζόμενες (shared) χρονικές σχισμές (slots) για να καλύψουν την κυκλοφορία δεδομένων (traffic) αίτησης (request) και απόκρισης (response) ad-hoc.
Υπερπλαίσιο πύλης (Gateway Superframe)	Το υπερπλαίσιο πύλης (Gateway Superframe) πρέπει να κατανέμεται (allocated) με μία μεγάλη τιμή ID value.
-	Το υπερπλαίσιο πύλης (Gateway Superframe) πρέπει να έχει μέγεθος 40 χρονικές σχισμές (slots). Τα σημεία πρόσβασης (Access Points) της πύλης (Gateway) πρέπει να ανακατανέμονται (allocated).
-	Ο χρονοπρογραμματισμός (Schedule) όλων των σχισμών χρόνου που δεν κατανέμονται (unallocated slots) στην πύλη (Gateway). Εναλλαγή κάθε μίας από αυτές τις χρονικές σχισμές (slots) ως XMIT, RECEIVE (οι χρονικές σχισμές receive slots πρέπει να είναι διαμοιραζόμενες shared).
Υπερπλαίσια (Superframes) Ειδικού σκοπού: Υψηλή απόδοση (Throughput)	Κατανέμονται (Allocated) από την πύλη (gateway) ή από τον client για να δώσουν λύση σε μια μεγάλη ζήτηση για αυξημένη απόδοση (high throughput demand) για να ικανοποιήσουν τη διαχείριση πόρων (asset management) και για άλλες εφαρμογές (applications). Αυτό μπορεί να κατανέμεται (allocated) ως ένας τύπος υπηρεσίας συντήρησης ("maintenance") ή μεταφοράς μπλοκ δεδομένων ("block transfer")
Υπερπλαίσια (Superframes) Ειδικού σκοπού: Υπερπλαίσιο Συντήρησης (Maintenance Superframe)	Κατανέμονται (Allocated) στις συσκευές χειρός (Handheld) και σε κάθε συσκευή πεδίου (Field Device). Αυτό το υπερπλαίσιο (Superframe) χρησιμοποιείται για να παρέχει στη συσκευή πεδίου (Field Device) και σε κάθε συσκευή χειρός (Handheld) μία σύνδεση υψηλής ταχύτητας (high-speed connection) για να μιλήσουν μεταξύ τους (talk on). Ο διαχειριστής δικτύου Network Manager θα κατανέμει 4 slots ανά second (δύο ζεύξεις links σε κάθε κατεύθυνση direction).

Πίνακας 3.7. Απαιτήσεις για τον διαχειριστή δικτύου (Network manager) για τον χρονοπρογραμματισμό.

Πηγή: [8]

3.2.10.5 Μεταβατικές καταστάσεις των συσκευών WirelessHART

Οι δικτυακές συσκευές WirelessHART μέσα στο δίκτυο WirelessHART μπορεί να βρίσκονται σε διάφορες καταστάσεις μεταβατικές. Αυτές είναι:

A) Αδρανής (idle state).

Η συσκευή βρίσκεται σε κατάσταση ηρεμίας και αδράνειας, ενώ ο ασύρματος πομποδέκτης της συσκευής δεν είναι ενεργοποιημένος. Τότε η συσκευή δεν γνωρίζει την ύπαρξη του δικτύου WirelessHART.

B) Επιχειρεί σύνδεση (joining state)

Η συσκευή ακούει το δίκτυο (listening) και περιμένει να λάβει ένα μήνυμα διαφήμισης (Advertisement message), ώστε μόλις το λάβει να κάνει μία αίτηση (request) για να συνδεθεί στο δίκτυο.

Γ) Σε καραντίνα (Quarantined state)

Η συσκευή έχει συνδεθεί στο δίκτυο WirelessHART, αλλά επικοινωνεί μόνο με τον Διαχειριστή δικτύου (Network Manager) NM και δεν μπορεί να επικοινωνήσει με την Πύλη (Gateway) ή άλλες συσκευές. Αυτό συμβαίνει διότι δεν έχει άδεια ασφαλείας (security clearance) και έτσι δεν επιτρέπεται στη συσκευή να εκτελέσει λειτουργίες ελέγχου ή λειτουργίες ανάκτησης δεδομένων από το δίκτυο.

Δ) Σε λειτουργία (Operational state)

Η συσκευή είναι συνδεδεμένη με επιτυχία στο δίκτυο και λειτουργεί πλήρως.

Συνδέεται και στον Διαχειριστή Δικτύου (Network Manager) και με την Πύλη (Gateway) ώστε μπορεί να εκτελέσει όλες τις λειτουργίες και να στείλει και να λάβει δεδομένα από το δίκτυο.

Μπορεί να δεχθεί πρόσβαση από εφαρμογές Φιλοξενητή (Host Applications) μέσω της Πύλης (Gateway).

Μετά από τη σύνδεσή της στο δίκτυο, η συσκευή ενδέχεται επιπλέον να μπει σε κατάσταση αναστολής (suspended state), ή να μπει σε κατάσταση επανασυγχρονισμού (resynching state).

3.2.11 Τα στρώματα του πρωτοκόλλου WirelessHART

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, στην παράγραφο 2.2, τα στρώματα που υπάρχουν στο πρότυπο WirelessHART, διαφοροποιούνται από το γενικό μοντέλο OSI-7, διότι το πρωτόκολλο WirelessHART αφορά ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks)(WSN) και όχι ασύρματα δίκτυα υπολογιστών.

Στη συνέχεια, αναφέρονται οι αλληλεπιδράσεις μεταξύ διαφορετικών στρωμάτων, του WirelessHART, που βασίζονται σε σύνολα εντολών. Αυτές οι εντολές λέγονται SP (service primitives), ομαδοποιούνται σε σύνολα και το κάθε ένα σύνολο εντολών συνθέτει μια διαφορετική υπηρεσία (service). Οι υπηρεσίες (services) παρέχονται από το ένα στρώμα σε ένα άλλο. Τα στρώματα χρησιμοποιούν τις υλοποιημένες υπηρεσίες χωρίς όμως να γνωρίζουν τον κώδικα υλοποίησής τους, διότι τα πρότυπα δεν περιγράφουν κάποια συγκεκριμένη υλοποίηση.

Ακολούθως, παρουσιάζονται τα στρώματα που υπάρχουν στο πρότυπο WirelessHART, που διαφοροποιούνται από το γενικό μοντέλο OSI-7.

Το WirelessHART περιλαμβάνει τα παρακάτω στρώματα:

α) Physical Layer (Φυσικό στρώμα),

που είναι το ίδιο με το φυσικό επίπεδο στο πρότυπο IEEE STD 802.15.4-2006.

β) Data Link Layer (Στρώμα ζεύξης δεδομένων)

που χρησιμοποιεί το πρότυπο TDMA

γ) Network Layer (Στρώμα δικτύου)

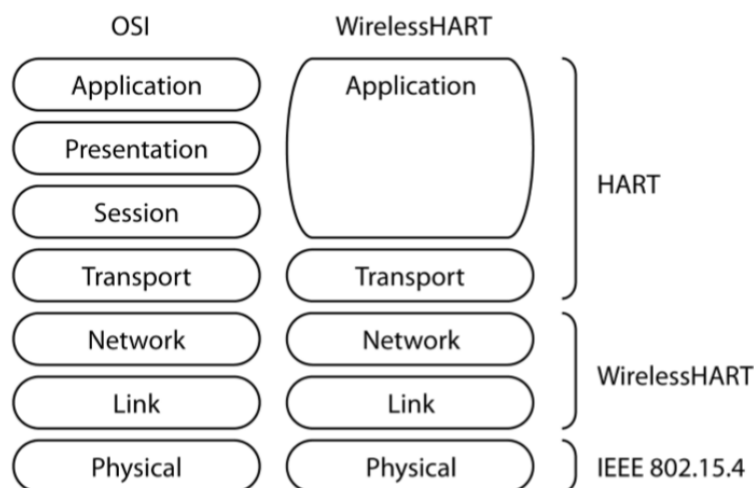
δ) Transport Layer (Στρώμα μεταφοράς)

ε) Application Layer (Στρώμα εφαρμογών)

που είναι το ίδιο με το στρώμα εφαρμογών του HART

Το πρότυπο WirelessHART συνδυάζει και στρώματα από το πρότυπο HART και στρώματα από το πρότυπο IEEE 802.15.4. Το πρότυπο HART αφορά τα ενσύρματα δίκτυα αισθητήρων, ενώ το IEEE 802.15.4 αφορά τα ασύρματα δίκτυα αισθητήρων.

Το πρότυπο WirelessHART σε σύγκριση με το μοντέλο OSI έχει τα παρακάτω στρώματα:



Εικόνα 74 Σύγκριση του μοντέλου Στρωμάτων OSI και του μοντέλου στρωμάτων για το WirelessHART.

Πηγή: [7, p. 31].

Στο WirelessHART το φυσικό επίπεδο χρησιμοποιεί το πρότυπο IEEE 802.15.4, τα επίπεδα ζεύξης και δικτύου τα ορίζει το WirelessHART, ενώ τα ανώτερα επίπεδα τα διαχειρίζεται το πρωτόκολλο HART. Για τα διάφορα στρώματα του προτύπου WirelessHART, στις παρακάτω παραγράφους, παρουσιάζονται αναλυτικά οι εντολές Service Primitives (SPs) και οι υπηρεσίες (services) που συνθέτουν οι ομάδες αυτών των εντολών SPs.

3.2.11.1 Αλληλεπιδράσεις μεταξύ των στρωμάτων

Τα στρώματα επικοινωνούν μεταξύ τους. Μηνύματα (messages) ανταλλάσσονται μεταξύ των στρωμάτων.

Κάθε αισθητήρας στο δίκτυο αισθητήρων αποτελεί έναν κόμβο (node). Οι κόμβοι (nodes) κάθε φορά που πρόκειται να στείλουν δεδομένα ο ένας στον άλλον, χρησιμοποιούν την αρχιτεκτονική στρωμάτων και ανταλλάσσουν μεταξύ τους μηνύματα (messages) ώστε υπάρχει μια ροή

μηνυμάτων (message flow) που διαπερνούν τη στοίβα στρωμάτων σε κάθε κόμβο μέχρι να φτάσουν από τον κόμβο πηγή στον κόμβο προορισμό.

Η αλληλεπίδραση ανάμεσα στα στρώματα του δικτύου. Ένα χαμηλότερο στρώμα συνήθως παρέχει ένα σύνολο από Application Program Interfaces (APIs) διεπαφές προγραμματισμού εφαρμογών στο ανώτερο στρώμα. οι APIs είναι σύνολα από εντολές. Οι εντολές αυτές επιτρέπουν να ανταλλάσσονται δεδομένα από το ένα στρώμα στο άλλο ή να εκτελούνται κάποιες υπηρεσίες μεταξύ των στρωμάτων χωρίς να ενδιαφερόμαστε για τον κώδικα που κρύβεται πίσω από τις υπηρεσίες που εκτελούνται, διότι το πρότυπο δεν καθορίζει πως θα υλοποιηθούν οι υπηρεσίες.

Ονομάζονται και Service Primitives (SPs), δηλαδή είναι σύνολα από βασικές εντολές (primitives) που το κάθε σύνολο εντολών αποτελεί μια υπηρεσία (Service). Οι SPs καθορίζονται στο πρωτόκολλο IEEE 802.15.4 το οποίο παρουσιάζεται σε επόμενη ενότητα.

Οι εντολές SPs χωρίζονται σε 2 γενικές κατηγορίες. Αυτές είναι:

α) Οι εντολές μηνύματα (Message SPs) και

β) Οι εντολές διαχείρισης (Management SPs). Οι εντολές SPs διαχείρισης χρησιμοποιούνται για να κάνουν ρυθμίσεις στο κάθε στρώμα της στοίβας.

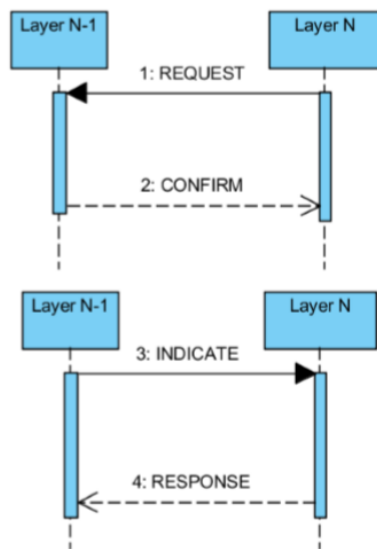
Οι εντολές SPs μηνύματα (messages) που ανταλλάσσονται διακρίνονται σε 4 είδη:

Request (αίτηση): όταν ένα ανώτερο στρώμα στέλνει αίτηση σε κατώτερο στρώμα για να του ζητήσει να παρέχει μια υπηρεσία.

Confirm (επιβεβαίωση): όταν ένα κατώτερο στρώμα απαντά σε μία αίτηση από ανώτερο στρώμα και του μεταφέρει το αποτέλεσμα της αίτησης.

Indicate (ένδειξη): όταν το κατώτερο στρώμα στέλνει μια αίτηση (request) στο ανώτερο στρώμα και συνήθως περιέχει ένα προωθημένο μήνυμα (message) προερχόμενο από έναν τρίτο κόμβο ή ένα γεγονός.

Response (απόκριση) όταν το ανώτερο επίπεδο απαντά στο μήνυμα ένδειξης (indication)



Εικόνα 75. Αλληλεπιδράσεις μεταξύ των στρωμάτων N και N-1, σε ένα διάγραμμα ακολουθίας.

Πηγή: [7, p. 26].

Επιπλέον, οι εντολές Service Primitives (SPs) χωρίζονται σε 5 ομάδες:

- α) ENABLE (ενεργοποίηση πομποδέκτη),
- β) CCA (clear channel assesment)(έλεγχος καναλιού αν είναι ελεύθερο),
- γ) DATA (δεδομένα), ERROR (σφάλμα),
- δ) LOCAL_MANAGEMENT (τοπική διαχείριση).

Παρουσιάζεται ένα παράδειγμα:

Έστω ότι υπάρχουν δύο κόμβοι αισθητήρες, ο κόμβος K και ο κόμβος Λ, και έχουν ο καθένας από N στρώματα. Ο κόμβος K στέλνει μια εντολή (command) π.χ. ENABLE στον κόμβο Λ. (η ENABLE είναι μία εντολή, που χρησιμοποιείται από το στρώμα MAC για ενεργοποίηση του Πομποδέκτη, αλλά εδώ στο παράδειγμά μας αναφερόμαστε γενικά για να παρουσιάσουμε μία οποιαδήποτε εντολή command και δεν εστιάζουμε το ενδιαφέρον μας στην συγκεκριμένη εντολή ENABLE).

Ο κόμβος Λ από την πλευρά του, στέλνει την απόκριση (command response) στην εντολή του κόμβου K.

Όλοκληρη η διαδικασία της εντολής που στέλνει ο K και της απόκρισης που στέλνει ο Λ περιγράφεται παρακάτω:

Η εντολή (command) όταν θα ξεκινήσει από τον κόμβο K αρχικά θα είναι μήνυμα αίτησης (request message) π.χ. ENABLE.request() που θα περάσει προς τα κάτω από όλα τα N στρώματα της στοίβας (stack layers) στον κόμβο K. Μετά η εντολή θα γίνει ένα μήνυμα ένδειξης (indicate message) π.χ. ENABLE.indicate() για να ειδοποιήσει ότι στέλνονται τα δεδομένα, θα φτάσει στον κόμβο Λ και θα περάσει προς τα πάνω όλα τα N στρώματα της στοίβας (stack layers) του κόμβου Λ.

Ο κόμβος Λ θα στείλει απόκριση στην εντολή (command response) που θα είναι ένα μήνυμα απόκρισης (respond message) π.χ. ENABLE.confirm() που επιβεβαιώνει την επιτυχία λήψης δεδομένων το οποίο θα περάσει προς τα κάτω όλα τα N στρώματα της στοίβας (stack layers) του κόμβου Λ.

Μετά ή ίδια εντολή θα γίνει ένα μήνυμα ένδειξης (indicate message) π.χ. ENABLE.indicate() που θα φτάσει στον κόμβο K και θα περάσει προς τα επάνω όλα τα N στρώματα της στοίβας (stack layers) του κόμβου K, για να δείξει ότι ήρθαν τα δεδομένα.

Όταν ένα μήνυμα εκπεμφθεί έξω από τον κόμβο K, τότε ένα μήνυμα επιβεβαίωσης (confirm message) π.χ. ENABLE.confirm() μπορεί να σταλεί προς τα επάνω μέσα στα N στρώματα της στοίβας του κόμβου K για να επιβεβαιώσει ότι έφυγε το μήνυμα.

Στην περίπτωσή μας, οι βασικές εντολές που συνθέτουν την υπηρεσία είναι οι Service Primitives:

ENABLE.request()

ENABLE.indicate()

ENABLE.confirm()

Στις επόμενες παραγράφους παρουσιάζονται διάφορες εντολές service primitives, SPs και υπηρεσίες.

3.2.11.2 Φυσικό επίπεδο (PHY Layer)

Το φυσικό επίπεδο (Physical Layer) καθορίζει τη σχέση ανάμεσα στους κόμβους και στο φυσικό μέσο επικοινωνίας.

Το φυσικό μέσο μεταξύ άλλων περιλαμβάνει την κεραία, το ασύρματο κανάλι, το επίπεδο ισχύος του σήματος, τις αλλαγές τιμών ηλεκτρικής τάσης, τους φυσικούς ρυθμούς δεδομένων (data rates), τις αποστάσεις εμβέλειας που απαιτείται να φτάνει η μετάδοση (transmission).

Το φυσικό επίπεδο για το WirelessHART βασίζεται πάνω στο πρότυπο IEEE 802.15.4, που είναι το πρότυπο για τα ασύρματα δίκτυα αισθητήρων, αλλά το φυσικό επίπεδο του WirelessHART είναι ένα απλοποιημένο υποσύνολο από όσα ορίζει το πρότυπο IEEE 802.15.4 και έχει μερικές τροποποιήσεις και περιορισμούς.

Στο WirelessHART το φυσικό επίπεδο (physical layer) βασίζεται στο πρότυπο IEEE 802.15.4-2006.

Χρησιμοποιεί τη συχνότητα 2.4GHz και τη διαμόρφωση DSSS (Ευθείας ακολουθίας με εξάπλωση φάσματος) για το φυσικό επίπεδο (physical layer). Το WirelessHART συμμορφώνεται πλήρως στο IEEE 802.15.4-2006.

Κάθε συσκευή (device) που χρησιμοποιεί το πρότυπο WirelessHART έχει τα παρακάτω χαρακτηριστικά:

Υπάρχουν μόνο ένα ή δύο μηνύματα (messages) IEEE 802.15.4 σε κάθε χρονική σχισμή (timeslot) που έχει διάρκεια 10 ms. Τα μηνύματα που στέλνονται από έναν κόμβο προς όλους τους κόμβους (broadcast messages) δεν δέχονται ως απάντηση ένα μήνυμα αναγνώρισης (acknowledged).

Η ελάχιστη διάρκεια χρόνου που επιτρέπεται να είναι η απόσταση ανάμεσα σε δύο μηνύματα (messages) που βρίσκονται μέσα στην ίδια χρονική σχισμή (timeslot) είναι 1 ms από το τέλος ενός μηνύματος (message) μέχρι την αρχή του μηνύματος αναγνώρισης (acknowledgement message).

Ο τύπος δεδομένων (data type) σε όλα τα μηνύματα (messages) στο WirelessHART είναι ο τύπος IEEE 802.15.4 messages.

- Μόνο η ζώνη συχνοτήτων 2.4 GHz έχει καθοριστεί για να χρησιμοποιείται από το WirelessHART.

Όπως θα δούμε στην επόμενη ενότητα, το πρότυπο IEEE 802.15.4 υποστηρίζει 27 κανάλια.

- Τα κανάλια 11-25 μπορούν να χρησιμοποιηθούν με το πρότυπο WirelessHART.

Δεν υποστηρίζεται το κανάλι 26, το οποίο δεν είναι νόμιμο σε πολλές περιοχές.

Συνοπτικά, το φυσικό στρώμα για το WirelessHART περιορίζεται στο να εκπέμπει (transmitting) και να λαμβάνει (receiving) μηνύματα δεδομένων (data messages) του τύπου IEEE 802.15.4

Ορισμένα χαρακτηριστικά στο φυσικό επίπεδο του WirelessHART είναι:

- Μεταπήδηση συχνότητας καναλιών (Channel hopping). Στο WirelessHART το ασύρματο κανάλι επικοινωνίας αλλάζει συχνότητα σε κάθε μετάδοση (transmission).
- Ισχύς του σήματος εκπομπής (Transmit power). Το πρότυπο IEEE 802.15.4 έχει καθοριστεί για δίκτυα personal area network όπου η εμβέλεια του ασύρματου σήματος φτάνει ως τα 10 m.

Ένα δίκτυο πλέγματος (mesh) με το πρότυπο WirelessHART καλύπτει μια περιοχή που είναι σχετικά μεγαλύτερη. Όλες οι συσκευές (devices) πρέπει να παρέχουν μια ισχύ εκπομπής με ονομαστική τιμή για το EIRP να είναι +10dBm (10mW) ± 3 dB.

Η ισχύς εκπομπής (transmit power) είναι προγραμματιζόμενη programmable από -10dBm μέχρι +10dBm.

Η μέγιστη απόσταση μετάδοσης σε οπτική επαφή (line of sight) φτάνει στα 100 m. Οι συσκευές που λειτουργούν με το πρότυπο WirelessHART έχουν ως ασύρματη μονάδα υλικού radio hardware, εμπορικά chips που είναι σχεδιασμένα για το πρότυπο IEEE 802.15.4

Εντολές Μηνύματα (Message SPs) για το φυσικό επίπεδο (PHY layer)

ENABLE

Enabling/Disabling the Transceiver

ενεργοποίηση/απενεργοποίηση του πομποδέκτη.

Αυτή η εντολή service primitive χρησιμοποιείται για να ενεργοποιεί και να απενεργοποιεί enable/disable κανάλια.

- ENABLE.request(state, channel)
- ENABLE.confirm(state, channel)
- ENABLE.indicate()

CCA

Clear Channel Assessment

Έλεγχος καναλιού CCA.

CCA είναι η διαδικασία να ελέγξει ότι το κανάλι δεν χρησιμοποιείται δηλαδή είναι ελεύθερο (clear) πριν από τη μετάδοση (transmission). Υπάρχουν 3 βασικοί τύποι CCA. Το WirelessHART χρησιμοποιεί CCA mode 2 που είναι CCA με ανίχνευση φέροντος (carrier sense). Ο τύπος CCA Mode 2 θα θεωρήσει ότι το μέσο είναι απασχολημένο (busy) αν ανιχνευθεί ένα άλλο σήμα IEEE 802.15.4 μετάδοσης (transmission). Αυτή η εντολή service primitive καλεί το φυσικό επίπεδο Physical Layer να εκτελέσει

- CCA.request()
- CCA.confirm(status)

DATA

Data Communication Services

Υπηρεσίες επικοινωνίας δεδομένων

Αυτές οι εντολές service primitives χρησιμοποιούνται για ανταλλαγή πακέτων δεδομένων (data packets) με το φυσικό επίπεδο (PHY layer).

- DATA.request(data)
- DATA.confirm(status, data)
- DATA.indication(rsl, data)
- ERROR.indication(status, data)

LOCAL_MANAGEMENT

Management SPs

Εντολές SPs διαχείρισης.

Αυτή ή εντολή service primitive χρησιμοποιείται για να ενεργοποιεί/ απενεργοποιεί (enable/disable) κανάλια.

- LOCAL_MANAGEMENT.request(service, [data])
- LOCAL_MANAGEMENT.confirm(service, status, [data])
- LOCAL_MANAGEMENT.request(service, status, [data])

Η πρώτη παράμετρος είναι η υπηρεσία για την οποία γίνεται η αίτηση

(requested service).

Οι υπηρεσίες (services) φαίνονται στον πίνακα 3.8:

(Service) Υπηρεσία	(Data) Δεδομένα	Περιγραφή
RESET	-	Αρχικοποιεί το φυσικό επίπεδο
READ_TX_PWR_LEVEL	Signed-8 txPwrLevel	Διαβάζει την τιμή της ισχύος εκπομπής (transmit power level) σε dBm
WRITE_TX_PWR_LEVEL	Signed-8 txPwrLevel	Γράφει την τιμή της ισχύος εκπομπής (transmit power level) σε dBm
WRITE_SLEEP_STATE	Unsigned-8 slepState	Γράφει την κατάσταση ύπνου (sleep state) για το φυσικό επίπεδο. Έχει μία από τις 2 τιμές: {sleep, awake}
WRITE_RCV_OVERFLOW_ENABLE	Boolean rcvOverflowEnable	Επιτρέπει στο δέκτη (receiver) να έχει ένδειξη για το σφάλμα υπερχείλισης (overflow error indication). Αυτή θα αναφερθεί στην κατάσταση (status) της υπηρεσίας ERROR.indication()

Πίνακας 3.8. Εντολές διαχείρισης (Management Commands) για την τοπική συσκευή (Local Device). Πηγή [8].

3.2.11.3 Επίπεδο Ζεύξης δεδομένων (Data Link Layer)

Η τεχνολογία πολυπλεξία με διαίρεση χρόνου TDMA (Time Division Multiple Access) χρησιμοποιείται στο επίπεδο ζεύξης δεδομένων (Data-Link Layer), για να εκτελεί συντονισμό επικοινωνιών και διαιτησία ανάμεσα στις δικτυακές συσκευές.

Το επίπεδο ζεύξης δεδομένων (data link layer) (DLL) υποδιαιρείται σε δύο επίπεδα:

α) το Logical Link Control (LLC) (Στρώμα Λογικού Ελέγχου Ζεύξης)

β) το Medium Access Control (MAC) (Στρώμα Ελέγχου Πρόσβασης Μέσου).

Το επίπεδο LLC layer διαχειρίζεται τις ζεύξεις (links), τις δομές δεδομένων (data structures) και τον χρονοπρογραμματισμό (scheduling).

Το επίπεδο MAC layer ελέγχει την πρόσβαση (access) στο ασύρματο κανάλι επικοινωνίας που αποτελεί το μέσο (medium).

Το στρώμα ζεύξης δεδομένων του WirelessHART είναι πλήρως συμβατό με το στρώμα MAC του προτύπου IEEE 802.15.4-2006. Το επίπεδο ζεύξης δεδομένων του WirelessHART επεκτείνει τις λειτουργίες του MAC. Χρησιμοποιεί πολυπλεξία με διαίρεση χρόνου TDMA (time division multiple access). Η χρονική σχισμή (time slot) του έχει σταθερό μήκος (fixed) με τιμή 10-ms, χρησιμοποιεί συγχρονισμένη μεταπήδηση συχνότητας (frequency hopping) και με αυτό τον τρόπο επιτυγχάνεται μια επικοινωνία χωρίς συγκρούσεις (collision-free). Για να διαχειριστεί τις χρονικές σχισμές (time slots), χρησιμοποιεί το υπερπλαίσιο (super frame) που θα το εξηγήσουμε λεπτομερώς σε επόμενη παράγραφο. Αυτό ομαδοποιεί μια σειρά (sequence) από συνεχόμενες διαδοχικές (consecutive) χρονικές σχισμές (time slots). Το υπερπλαίσιο (super frame) είναι περιοδικό, η περίοδος του είναι το σύνολο του μήκους των χρονικών σχισμών (slots) του. Όλα τα υπερπλάγια (super frames) στο δίκτυο WirelessHART, ξεκινούν με τον αριθμό ASN (absolution slot number) (απόλυτος αριθμός χρονικής σχισμής) που έχει την τιμή 0, και αυτό αντιστοιχεί στη χρονική στιγμή που δημιουργήθηκε το δίκτυο για πρώτη φορά. Κάθε υπερπλαίσιο (super frame) επαναλαμβάνει περιοδικά τον εαυτό του στη διάρκεια του χρόνου και αυτό γίνεται με βάση την περίοδο του. Στο WirelessHART, μία συναλλαγή (transaction) σε μία χρονική σχισμή (time slot) περιγράφεται από ένα διάνυσμα vector: {frame id, index, type, source address, destination address, channel offset} όπου:

frame id προσδιορίζει το συγκεκριμένο super frame.

index είναι ο δείκτης της χρονικής σχισμής (slot) στο super frame

type δείχνει τον τύπο της χρονικής σχισμής slot (transmit/receive/idle)

source address και destination address είναι οι διευθύνσεις πηγής και προορισμού αντιστοίχως.

channel offset παρέχει το λογικό κανάλι που θα χρησιμοποιηθεί στη συναλλαγή.

Για να ρυθμίζεται καλύτερα η χρήση των καναλιών, το WirelessHART χρησιμοποιεί την εισαγωγή καναλιών σε μαύρη λίστα (channel blacklisting). Τα κανάλια που είναι ευαίσθητα σε συνεχείς παρεμβολές μπορεί να τεθούν σε μαύρη λίστα. Με αυτό τον τρόπο ο διαχειριστής του δικτύου μπορεί να απενεργοποιήσει πλήρως τη χρήση αυτών των καναλιών που βρίσκονται στην μαύρη

λίστα. Κάθε συσκευή διαθέτει έναν πίνακα με ενεργά κανάλια. Επειδή πολλά κανάλια βρίσκονται σε μαύρη λίστα, ο πίνακας μπορεί να περιέχει λιγότερα από 16 κανάλια.

3.2.11.4 Τα δύο υποεπίπεδα LLC και MAC

Το επίπεδο ζεύξης δεδομένων (data link layer) παρέχει ένα αξιόπιστο μέσο για μεταφορά των δεδομένων ανάμεσα στους κόμβους του δικτύου. Η αξιοπιστία επιτυγχάνεται με ανίχνευση και πιθανή διόρθωση των σφαλμάτων που μπορεί να συμβούν στο φυσικό επίπεδο (PHY Layer). Η σημαντική εργασία (task) που επιτελεί το επίπεδο ζεύξης δεδομένων, είναι να δημιουργεί και να διαχειρίζεται τα πλαίσια των δεδομένων (data frames). Συνήθως υπάρχουν δύο υποεπίπεδα (sublayers).

Αυτά είναι:

Επίπεδο λογικού ελέγχου ζεύξης Logical Link Control (LLC) layer

και επίπεδο πρόσβασης μέσου Medium Access Control (MAC) layer.

Το στρώμα LLC layer ορίζει την υπηρεσία (service) στο επίπεδο δικτύου (network layer).

Το στρώμα MAC ορίζει με ποιο τρόπο θα έχουν πρόσβαση οι πολλαπλοί κόμβοι στο μέσο επικοινωνίας που είναι το ασύρματο κανάλι.

Το επίπεδο ζεύξης δεδομένων (data link layer) περιλαμβάνει:

- Τις υπηρεσίες (services) που παρέχει το στρώμα ζεύξης δεδομένων (Data-Link Layer) στο στρώμα δικτύου (Network Layer). Αυτές οι υπηρεσίες (services) συνθέτουν ένα μοντέλο μαύρο κουτί για τις απαιτήσεις του στρώματος ζεύξης δεδομένων (Data-Link Layer). Δηλαδή χρησιμοποιούνται οι συγκεκριμένες υπηρεσίες χωρίς να γνωρίζει το στρώμα που τις καλεί ποιος είναι ο κώδικας υλοποίησης τους.
- Τις απαιτήσεις για τον λογικό έλεγχο ζεύξης Logical Link Control (LLC). Αυτές είναι η μορφή (format) των πλαισίων HART frames, η δομή διευθύνσεων των συσκευών HART device, οι υπηρεσίες ασφαλείας (security services) που χρησιμοποιούνται για την ακεραιότητα μηνυμάτων (message integrity) και ο κώδικας ανίχνευσης σφαλμάτων που χρησιμοποιείται (error detection coding).

- Οι κανόνες για το στρώμα ελέγχου πρόσβασης μέσου Media Access Control (MAC) εξασφαλίζουν ότι οι συσκευές (devices) θα εκτελέσουν τις μεταδόσεις δεδομένων με μία καθορισμένη σειρά στο χρόνο. Δηλαδή το στρώμα MAC καθορίζει πότε θα επιτρέπεται σε μια συσκευή (device) να εκπέμψει ένα μήνυμα.
- Για τη σωστή λειτουργία του στρώματος MAC sub-layer απαιτούνται οι πραγματικές τιμές χρόνου. Αυτές οι τιμές χρόνου (timing values) έχουν άμεση αντιστοιχία με τις παραμέτρους χρόνου που αφορούν την απόδοση για το φυσικό στρώμα Physical Layer (π.χ., χρόνος για έλεγχο καναλιού αν είναι ελεύθερο Clear Channel Assessment time, χρόνος Tx/Rx για να αλλάξει η λειτουργία της συσκευής από εκπομπή σε λήψη turnaround time).

3.2.11.5 Υπηρεσίες για το επίπεδο ζεύξης δεδομένων (Data Link Layer)

Οι υπηρεσίες (services) για το επίπεδο ζεύξης δεδομένων (Data Link Layer)

διαίρούνται σε 4 κατηγορίες:

- α) transmit (μετάδοση),
- β) network events (γεγονότα στο δίκτυο),
- γ) receive (λήψη)
- δ) local management (τοπική διαχείριση).

Message SPs

Οι εντολές μηνυμάτων Message SPs συνθέτουν τις υπηρεσίες (services) που καθορίζουν τη βασική μεταφορά των δεδομένων μεταξύ των συσκευών (devices). Το επίπεδο ζεύξης δεδομένων (data link layer) επιτρέπει τα πολλαπλά μηνύματα (messages) να μπαίνουν σε μία ουρά (queue). Το πρωτόκολλο υποστηρίζει επίσης να γίνονται αυτόματα επαναληπτικές προσπάθειες (retries) ώστε να εξασφαλιστεί ότι η ανταλλαγή δεδομένων θα γίνει με ακρίβεια.

TRANSMIT

Οι εντολές μετάδοσης Transmit SPs

Είναι οι μόνες εντολές που απαιτούνται από το πρότυπο WirelessHART ενώ όλες οι υπόλοιπες εντολές είναι προαιρετικές.

- FLUSH.request (handle)

Αυτή η εντολή (service primitive) λαμβάνει ως όρισμα (argument) ένα χειριστή πακέτου (packet handle) και χρησιμοποιείται για να διαγράψει το πακέτο που αναφέρει ο χειριστής (handle).

- FLUSH.confirm (handle, localStatus)

Αυτή η εντολή (service primitive) χρησιμοποιείται ως απόκριση (response) σε μια προηγούμενη αίτηση (request).

- TRANSMIT.confirm (handle, localStatus)

Αυτή η εντολή (service primitive) είναι μια απόκριση (response) σε εντολή TRANSMIT.request() και δίνει μια ειδοποίηση (notify) στο επίπεδο δικτύου (network layer) σχετικά με το αποτέλεσμα μιας προηγούμενης αίτησης (request).

- TRANSMIT.indicate (localStatus, priority, sourceAddress, payload)

Αυτή η εντολή (service primitive) χρησιμοποιείται από το στρώμα MAC layer για να στείλει ειδοποίηση (notify) στο επίπεδο δικτύου (network layer) σχετικά με την επιτυχή λήψη ενός πακέτου που στάλθηκε σε αυτή τη συσκευή.

- TRANSMIT.request()

Αυτή η εντολή (service primitive) χρησιμοποιείται από το επίπεδο δικτύου (network layer) για να μεταδώσει (transmit) δεδομένα σε μία άλλη συσκευή (device). Όταν το επίπεδο ζεύξης δεδομένων (link layer) έχει δημιουργήσει ένα πακέτο και είναι έτοιμο να το στείλει θα καλέσει την TRANSMIT.request () που θα ζητήσει από το στρώμα MAC layer να μεταδώσει (transmit) το πακέτο.

Η ίδια εντολή μπορεί να καλείται με διαφορετικές παραμέτρους δηλαδή είναι overloaded.

- TRANSMIT.request (handle, payload, priority, timeout, graph)

- TRANSMIT.request (handle, payload, priority, timeout, sframe, bcast)
- TRANSMIT.request (handle, payload, priority, timeout, shortDestAddress)
- TRANSMIT.request (handle, payload, priority, timeout, longDestAddress)

οι παράμετροι στο overloaded TRANSMIT.request περιλαμβάνουν:

- handle – Ο χειριστής handle υποστηρίζεται για το επίπεδο client layer. Το επίπεδο ζεύξης δεδομένων (Data-Link) επιστρέφει αυτή την τιμή στην αντίστοιχη εντολή TRANSMIT.confirm()
- payload – Το σύνολο δεδομένων NPDU που πρόκειται να μεταδοθεί στη συσκευή προορισμού (destination device).
- priority – Η προτεραιότητα πακέτου (packet priority) όπως ορίζεται:

υπάρχουν 4 τύποι προτεραιότητας management, process-data, normal, alarm. Αυτοί οι τύποι εξηγούνται σε επόμενη παράγραφο.

- timeout – Χρόνος Λήξης. Ο μέγιστος χρόνος που επιτρέπεται να γίνει προσπάθεια μετάδοσης του πακέτου (packet transmission). Το επίπεδο δικτύου (Network Layer) πρέπει να ρυθμίσει αυτό το χρόνο με βάση το ASN Snippet (αυτό αναφέρεται στην προδιαγραφή διαχείρισης του δικτύου Network Management Specification).
- graph – Αυτή η παράμετρος υπάρχει μόνο αν πρέπει να χρησιμοποιηθεί δρομολόγηση με γράφημα (graph routing). Όταν εφαρμόζεται, το γράφημα δείχνει τους γειτονικούς κόμβους (neighbors) που μπορούν να χρησιμοποιηθούν ως προορισμός για το επόμενο άλμα (next hop).
- sframe – Αυτή η παράμετρος υπάρχει μόνο για μήνυμα που εκπέμπεται σε όλους τους κόμβους (broadcasting message). Το sframe δείχνει το υπερπλαίσιο (superframe) του οποίου οι ζεύξεις εκπομπής προς όλους (broadcast links) μπορούν να χρησιμοποιηθούν για να γίνει η προώθηση του πακέτου.
- bcast – Αυτή η μεταβλητή flag δείχνει το πακέτο NPDU που πρέπει να εκπεμφθεί προς όλους τους κόμβους (broadcast) στο υπερπλαίσιο (Superframe) που δείχνει.
- shortDestAddress – Αυτή η παράμετρος δείχνει ένα ψευδώνυμο (nickname) για την συσκευή προορισμού (destination device) που πρέπει να χρησιμοποιηθεί για το επόμενο άλμα (hop).
- longDestAddress – Αυτή η παράμετρος δείχνει ένα μοναδικό αναγνωριστικό Unique ID για τη συσκευή προορισμού (destination device) που πρέπει να χρησιμοποιηθεί για το επόμενο άλμα (hop).

Network Event SPs

εντολές για συμβάντα δικτύου

- DISCONNECT.indicate (localStatus, sourceAddress)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δώσει μια ειδοποίηση (notify) στο επίπεδο δικτύου (network layer) ότι μία συσκευή αποσυνδέεται από το δίκτυο, και επιτρέπει στο στρώμα MAC layer να κάνει τις απαραίτητες ρυθμίσεις.

- PATH_FAILURE.indicate (localStatus, sourceAddress)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δώσει μια ειδοποίηση (notify) στο επίπεδο δικτύου (network layer) ότι η διαδρομή (path) προς μια άλλη συσκευή δεν είναι εφικτή, δηλαδή απέτυχε (failed).

- ADVERTISE.indicate (localStatus, AdvertisePayload)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δώσει μια ειδοποίηση (notify) στο επίπεδο δικτύου (network layer) σχετικά με τη λήψη μιας «διαφήμισης» (advertisement). Το επίπεδο δικτύου (network layer) μπορεί αργότερα να χρησιμοποιήσει αυτές της πληροφορίες για να γίνει ένας συγχρονισμός με επιτυχία στο δίκτυο.

- NEIGHBOR.indicate (localStatus, sourceAddress, packetRSL)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δώσει ειδοποίηση στο επίπεδο δικτύου (network layer) σχετικά με τη λήψη ενός πακέτου από μία συσκευή που δεν υπάρχει στον πίνακα γειτονικών κόμβων (neighbor table) και έτσι επιτρέπει στο επίπεδο δικτύου να κάνει τις απαραίτητες ρυθμίσεις.

Receive SPs

εντολές για λήψη

- RECEIVE.indicate (localStatus, packetRSL, payloadDLPDU)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δείξει ότι λήφθηκε ένα πακέτο που δεν προοριζόταν για αυτή τη συσκευή (device) αλλά είχε άλλη διεύθυνση προορισμού.

Management SPs εντολές για διαχείριση

LOCAL_MANAGEMENT

Οι εντολές για διαχείριση (Management SPs) είναι ένα σύνολο εντολών που χρησιμοποιούνται για ρυθμίσεις στο στρώμα ζεύξης δεδομένων (data link layer) και επίσης για να υπάρχει πρόσβαση στα στατιστικά του στρώματος ζεύξης δεδομένων. Χρησιμοποιούνται για να γίνουν ρυθμίσεις στο στρώμα MAC layer και έχουν μια δομή όπως έχουν και οι άλλες εντολές.

- LOCAL_MANAGEMENT.request (service, [data])
- LOCAL_MANAGEMENT.confirm (service, status, [data])
- LOCAL_MANAGEMENT.indication (service, status, [data])

Η πρώτη παράμετρος είναι η υπηρεσία που ζητείται (requested service).

Οι υπηρεσίες (services) παρουσιάζονται στον παρακάτω πίνακα:

Υπηρεσία	Περιγραφή
RESET	Αρχικοποιεί το στρώμα ζεύξης δεδομένων (Data-Link Layer)
DISCONNECT	Αποσυνδέεται από το δίκτυο και σταματά την επικοινωνία.
RE_JOIN	Αποσυνδέεται από το δίκτυο, επανασυνδέεται (rejoin) στο δίκτυο, εκκαθάριση όλων (purging all) των ουρών MAC queues και σβήσιμο όλων των πινάκων MAC tables
WRITE_SUPERFRAME	Δημιουργεί έναν νέο υπερπλαίσιο (superframe)
DELETE_SUPERFRAME	Διαγράφει ένα υπάρχον υπερπλαίσιο superframe από το χρονοπρογραμματισμό (scheduling) και όλες τις ζεύξεις (links) που σχετίζονται με αυτό.
ADD_LINK	Προσθέτει έναν νέο σύνδεσμο (link) σε μια άλλη συσκευή (device) και πιθανώς να ανανεώσει τον πίνακα γειτόνων (neighbor table) και τον πίνακα συνδέσεων (connection table) σε αυτή τη διαδικασία.
DELETE_LINK	Διαγράφει έναν υπάρχον σύνδεσμο (existing link) και πιθανώς να ανανεώσει τον πίνακα γειτόνων (neighbor table) και τον πίνακα συνδέσεων (connection table) σε αυτή τη διαδικασία.

ADD_EDGE	Προσθέτει έναν νέο κόμβο γείτονα (neighbor) δηλαδή νέα ακμή στο συγκεκριμένο γράφημα
DELETE_EDGE	Διαγράφει έναν κόμβο γείτονα (neighbor) δηλαδή μία ακμή από το συγκεκριμένο γράφημα
READ_NETWORKID	Διαβάζει το αναγνωριστικό ID του δικτύου στο οποίο ανήκει η συσκευή (device)
WRITE_NETWORKID	Γράφει το αναγνωριστικό ID του δικτύου στο οποίο ανήκει η συσκευή (device)
WRITE_NETWORK_KEY	Αυτή η εντολή επιτρέπει στον διαχειριστή δικτύου (Network Manager) να γράψει το κλειδί δικτύου (network key) σε μια συσκευή δικτύου (Network Device). Τα κλειδιά (Keys) πρέπει να προστατεύονται από υποκλοπή (pilfering) (πχ, με κρυπτογράφηση).
READ_TIMEOUT_PERIODS	Διαβάζει τις τιμές χρονικής περιόδου (time period values), Διατήρηση σύνδεσης με γείτονες (Keep-Alive), Αποτυχία διαδρομής (Path-Failure), Advertise, και Discovery.
WRITE_TIMEOUT_PERIOD	Γράφει την τιμή της χρονικής περιόδου (time period) για τη χρονική περίοδο που δείχνει.
READ_CAPACITIES	Διαβάζει μέγιστες τιμές παραμέτρων maxSuperframes, maxLinks, maxNeighbors, maxPktBuffers
READ_PRIORITY_THRESHOLD	Διαβάζει τα δεδομένα DLPDU χαμηλότερης προτεραιότητας που πρέπει να τα αποδεχτεί μια άλλη συσκευή
WRITE_PRIORITY_THRESHOLD	Γράφει τα δεδομένα DLPDU χαμηλότερης προτεραιότητας που πρέπει να τα αποδεχτεί μια άλλη συσκευή
READ_JOIN_PRIORITY	Διαβάζει με ποια προτεραιότητα σύνδεσης (join priority) πρέπει η συσκευή να στείλει μήνυμα για τη διαφήμιση της (advertise).
WRITE_JOIN_PRIORITY	Γράφει με ποια προτεραιότητα σύνδεσης (join priority) πρέπει η συσκευή να στείλει μήνυμα για τη διαφήμιση της (advertise).
READ_PROMISCUOUS_MODE	Διαβάζει αν το υποεπίπεδο (sublayer) είναι σε λειτουργία «λήψη όλων» ("receive all" mode)
WRITE_PROMISCUOUS_MODE	Γράφει αν το υποεπίπεδο (sublayer) είναι σε λειτουργία «λήψη όλων» ("receive all" mode)

READ_MAX_BACK_OFF_EXPONENT	Διαβάζει τη μέγιστη τιμή που μπορεί να υποτεθεί για το backoff exponent που χρησιμοποιείται στις διαμοιραζόμενες χρονικές σχιμές (shared slots)
WRITE_MAX_BACK_OFF_EXPONENT	Γράφει τη μέγιστη τιμή που μπορεί να υποτεθεί για το backoff exponent που χρησιμοποιείται στις διαμοιραζόμενες χρονικές σχιμές (shared slots)

Πίνακας 3.9. Εντολές διαχείρισης (Management Commands.) για τις τοπικές συσκευές (Local Device).
Πηγή: [8].

3.2.11.6 Πακέτα δεδομένων PDU για τα στρώματα του WirelessHART

Για το κάθε ένα στρώμα της στοίβας στρωμάτων, υπάρχει ένα αντίστοιχο πακέτο δεδομένων PDU (Protocol Data Unit) το οποίο είναι ένα σύνολο bits. Τα bits είναι οργανωμένα σε bytes. Το σύνολο των bytes αποτελεί το συνολικό μήκος του πακέτου (packet length). Το πακέτο δεδομένων PDU περιλαμβάνει συνολικά κάποια πεδία σε bytes. Κάθε πεδίο, αποτελείται από ένα συγκεκριμένο πλήθος bytes. Το πακέτο δεδομένων PDU σε ένα στρώμα αποτελείται από 3 μέρη. Αυτά είναι:

- α) επικεφαλίδα (header), που είναι ένα σύνολο πεδίων,
- β) τα πραγματικά δεδομένα προς μετάδοση (payload),
- γ) ουρά (footer) που είναι ένα σύνολο πεδίων.

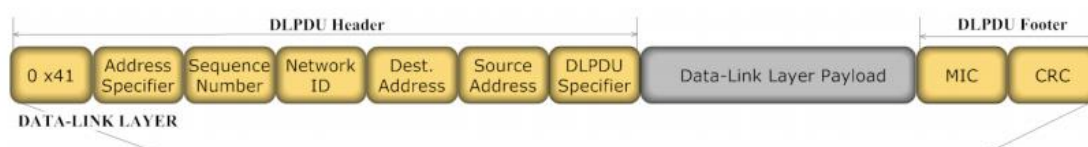
Καθώς το πακέτο ενός στρώματος μετακινείται προς τα κάτω στη στοίβα στρωμάτων, από ένα στρώμα στο επόμενο στρώμα, τότε το επόμενο στρώμα προσθέτει στο πακέτο μια νέα επικεφαλίδα (header) με επιπρόσθετα πεδία στην αρχή του, και μία νέα ουρά (footer) στο τέλος του. Τότε δημιουργείται ένα νέο πακέτο δεδομένων PDU για το νέο στρώμα, όπου το πεδίο με τα πραγματικά δεδομένα προς μετάδοση (payload) είναι τώρα ολόκληρο το πακέτο δεδομένων PDU του προηγούμενου στρώματος.

Αντίθετα, αν το πακέτο δεδομένων PDU ενός στρώματος μετακινηθεί από κάτω προς τα πάνω στη στοίβα, τότε γίνεται η αντίθετη διαδικασία και αφαιρείται η επικεφαλίδα (Header) και η ουρά (footer) και τότε απομένει το payload, το οποίο είναι το πακέτο δεδομένων PDU για το αντίστοιχο στρώμα.

Το πακέτο δεδομένων που αντιστοιχεί σε ένα στρώμα, ονομάζεται με βάση τα αρχικά του στρώματος και την κατάληξη -PDU, π.χ για το φυσικό επίπεδο, το αντίστοιχο πακέτο δεδομένων ονομάζεται PhPDU, ενώ για το στρώμα δικτύου το αντίστοιχο πακέτο δεδομένων ονομάζεται NPDU, κλπ.

3.2.11.7 Το πακέτο δεδομένων DLPDU στο υποεπίπεδο Data Link Layer

Το πακέτο δεδομένων στο Data Link Layer ονομάζεται DLPDU και είναι αυτό που φαίνεται στην



Εικόνα 76. Πακέτο Δεδομένων Data Link Protocol Data Unit (DLPDU). Πηγή: [26]

Το πακέτο δεδομένων του επιπέδου ζεύξης (Data-Link) ονομάζεται (DLPDU). Το συνολικό μήκος του πακέτου είναι 127 byte και αποτελείται από τα παρακάτω πεδία (fields):

- Ένα byte που έχει τεθεί στην διεύθυνση 0x41
- 1-byte που είναι προσδιοριστής (Specifier) διεύθυνσης (Address Specifier)
- 1-byte που είναι αριθμός ακολουθίας (Sequence Number)
- 2 byte που είναι το αναγνωριστικό δικτύου (Network ID)
- Διεύθυνση προορισμού (Destination) και διεύθυνση πηγής (Source) Addresses που κάθε μία έχει μήκος είτε 2 bytes είτε 8bytes
- 1-byte προσδιοριστής (Specifier) του πακέτου δεδομένων DLPDU
- Τα πραγματικά δεδομένα προς μετάδοση DLL payload
- 4-byte κώδικας ακεραιότητας μηνυμάτων με κλειδί keyed Message Integrity Code (MIC)
- 2-byte κυκλικός έλεγχος πλεονασμού CRC16 της ITU-T

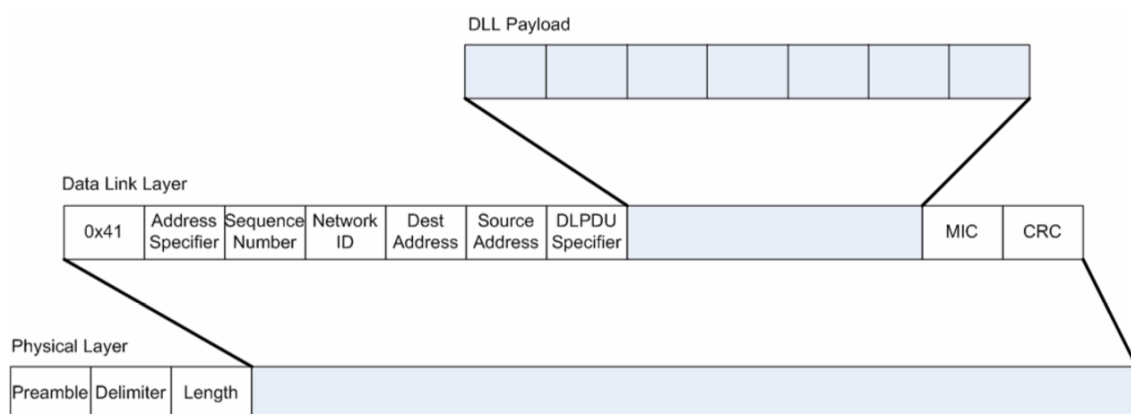
Τα παραπάνω στον πίνακα 3.10 συνοψίζονται ως εξής :

Θέση	Μήκος σε Bytes	Όνομα/ περιγραφή	Τμήμα πακέτου
1	1	0x41	Επικεφαλίδα πακέτου

2	1	Address Specifier	(header)
3	1	Sequence Number	
4	2	Network ID	
5	2 ή 8	Destination	
6	2 ή 8	Source	
7	1	DLPDU Specifier	
8	Αναλόγως με τον τύπο πακέτου	Payload	Πραγματικά δεδομένα πακέτου
9	4	Message Integrity Code (MIC)	Ουρά πακέτου (footer)
10	2	Cyclic Redundancy Check (CRC)	

Πίνακας 3.10: Πεδία του πακέτου δεδομένων DLPDU

Η παρακάτω εικόνα δείχνει ποια είναι η βασική δομή του πακέτου δεδομένων PhPDU για το φυσικό επίπεδο (PHY layer) και ποια είναι η δομή του πακέτου δεδομένων DLPDU για το επίπεδο ζεύξης δεδομένων (Data Link Layer).



Εικόνα 77 Δομή των πακέτων δεδομένων DLPDU. Και σύγκριση με τη δομή πακέτων δεδομένων PhPDU του Φυσικού επιπέδου. Πηγή: [8]

Στις παρακάτω παραγράφους παρουσιάζονται αναλυτικά μερικά πεδία από το πακέτο δεδομένων DLPDU.

3.2.11.8 Το πεδίο προσδιοριστής DLPDU Specifier

Ο προσδιοριστής DLPDU specifier είναι ένα πεδίο του πακέτου δεδομένων DLPDU και φαίνεται στην παρακάτω εικόνα. Το πεδίο αυτό έχει μήκος 1 byte και βρίσκεται μέσα στο πακέτο DLPDU στη θέση 7, πριν από τα πραγματικά δεδομένα προς μετάδοση payload.



Εικόνα 78. ο προσδιοριστής DLPDU Specifier μέσα στο πακέτο DLPDU βρίσκεται στη θέση 7 και αποτελείται από 1 byte δηλαδή 8 bits.

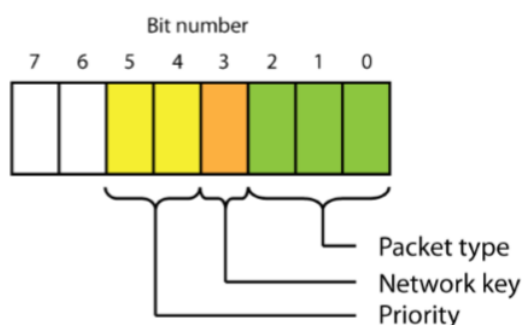
Όπως φαίνεται στην παρακάτω εικόνα, τα 8 bits του DLPDU specifier έχουν την αρίθμηση :

b7, b6, b5, b4, b3, b2, b1, b0.

Τα bits b5, b4 καθορίζουν το είδος προτεραιότητας (priority) και υπάρχουν 4 είδη προτεραιότητας, όπως θα δούμε και στη συνέχεια.

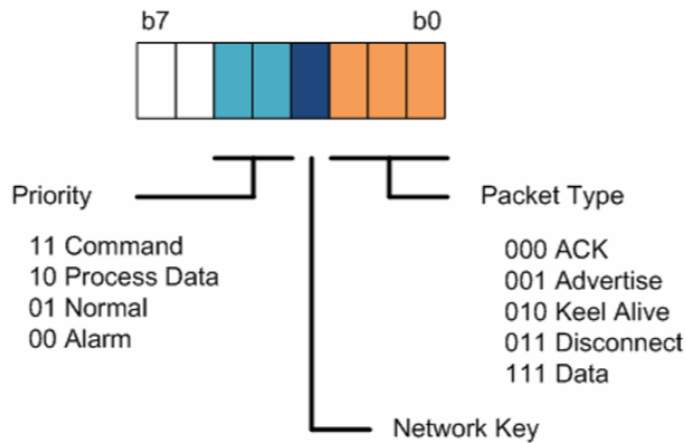
Τα bits b2,b1,b0 καθορίζουν τον τύπο του μηνύματος (message) (Packet type) δηλαδή τον τύπο του πακέτου DLPDU και υπάρχουν 5 διαφορετικοί τύποι πακέτων DLPDU.

Το bit b3 αναφέρεται στο κλειδί δικτύου. Χρησιμοποιείται για να δηλώσει αν απαιτείται το κλειδί δικτύου (network key) ή το δημόσιο κλειδί (public key) για να γίνει πιστοποίηση (authenticate) του μηνύματος (message).



Εικόνα 79 ο προσδιοριστής DLPDU Specifier. Πηγή: [7, p. 43]

Στην παρακάτω εικόνα φαίνονται διάφορες τιμές που παίρνουν τα bits για να δηλώσουν τον τύπο πακέτου (Packet type), το κλειδί δικτύου (Network Key) και την προτεραιότητα (Priority).



Εικόνα 80. ο προσδιοριστής DLPDU Specifier και οι τιμές που παίρνουν τα bits σε διάφορες περιπτώσεις.
Πηγή: [8]

3.2.11.9 Τύποι των πακέτων δεδομένων DLPDU

Υπάρχουν 5 τύποι πακέτων δεδομένων DLPDU όπως καθορίζονται από τον προσδιοριστή (specifier) των DLPDU.

b2	b1	b0	Τύποι Πακέτων
0	0	0	ACK
0	0	1	Advertise
0	1	0	Keep Alive
0	1	1	Disconnect
1	1	1	Data

Πίνακας 3.11. ο προσδιοριστής DLPDU specifier καθορίζει 5 τύπους πακέτων

Οι 5 τύποι πακέτων δηλώνονται ανάλογα με τις τιμές των bits b2,b1,b0 και είναι:

α) Data DLPDUs (111). Πακέτο μόνο με Δεδομένα. Τα πακέτα αυτά περιέχουν μόνο δεδομένα για το δίκτυο (network) και για τη συσκευή (device) για να διαμετακομιστούν (transit) στην τελική συσκευή προορισμού η οποία δηλώνεται στο πακέτο δεδομένων του στρώματος δικτύου NPDU.

β) Keep-Alive DLPDUs (010). Πακέτα ένδειξης διατήρησης σε λειτουργία. Αυτά τα πακέτα δεδομένων διευκολύνουν την διατήρηση σύνδεσης ανάμεσα σε γειτονικές συσκευές. Έχουν 3 βασικούς σκοπούς: συγχρονισμό με βάση το χρόνο (time synchronization), επιβεβαίωση συνδεσιμότητας (confirming connectivity) και ανακάλυψη γειτονικών κόμβων (neighbor discovery). Ένα πακέτο keep-alive DLPDU στέλνεται. Ο γειτονικός κόμβος στέλνει ως απάντηση ένα άλλο πακέτο αναγνώρισης ACK DLPDU και γίνεται συγχρονισμός με βάση το πεδίο ρύθμισης χρόνου (time adjustment) που υπάρχει στο πακέτο ACK DLPDU. Επίσης το πακέτο keep-alive DLPDU στέλνεται στους γειτονικούς κόμβους (neighbors) για να τους πληροφορήσει ότι ο κόμβος αποστολέας είναι ενεργός (running).

Μία συσκευή (device) ενδέχεται να δεχθεί εντολή να στείλει προς τα έξω πακέτα keep-alive DLPDUs για να γίνει γνωστή στους νέους γειτονικούς κόμβους.

γ) Advertise DLPDUs (001). Πακέτα διαφήμισης. Αυτά τα πακέτα δεδομένων παρέχουν πληροφορίες για γειτονικές συσκευές (neighboring devices) που επιθυμούν να συνδεθούν στο δίκτυο. Τα πακέτα Advertise DLPDU κάνουν μια «διαφήμιση» (advertise) του δικτύου και στέλνουν αρκετές πληροφορίες μαζί με αυτή ώστε να επιτρέψουν σε νέους κόμβους να συγχρονιστούν οι ίδιοι ώστε να μπορέσουν να ξεκινήσουν μία διαδικασία σύνδεσης (join sequence) στο δίκτυο. Το πακέτο Advertise DLPDU περιέχει βασικές πληροφορίες, όπως είναι ο τρέχων αριθμός ASN, ένας χάρτης καναλιών (channel map) με επιτρεπόμενα κανάλια, και μια λίστα από join links που μπορούν να χρησιμοποιηθούν για να ξεκινήσει μια ακολουθία σύνδεσης (join sequence).

δ) Disconnect DLPDUs (011). Πακέτα αποσύνδεσης. Αυτά τα πακέτα δεδομένων χρησιμοποιούνται για να δώσουν πληροφόρηση (advise) στις γειτονικές συσκευές (neighboring devices) ότι η συγκεκριμένη συσκευή βγαίνει από το δίκτυο. Όταν η συσκευή (field device) αποσυνδέεται από το δίκτυο στέλνει ένα πακέτο disconnect DLPDU. Η κάθε άλλη συσκευή (device) του δικτύου που λαμβάνει αυτό το πακέτο θα διαγράψει αυτόν τον κόμβο από την λίστα

με τους γειτονικούς της κόμβους (neighbors list) και πρέπει να διαγράψει όλες τις ζεύξεις (links) προς τη συσκευή που φεύγει από το δίκτυο.

ε) ACK DLPDUs (000). Πακέτα αναγνώρισης ACK. Αυτά τα πακέτα δεδομένων είναι το μήνυμα αναγνώρισης ACK. Το μήνυμα αυτό, στέλνεται στο επίπεδο ζεύξης δεδομένων DLL και το στέλνει ένας κόμβος για να δείξει ότι έλαβε ένα άλλο πακέτο. Δηλαδή αρχικά προηγείται μια λήψη άλλου πακέτου δεδομένων από έναν κόμβο πηγή (source) και μετά ο κόμβος προορισμός στέλνει ως απάντηση ένα πακέτο αναγνώρισης ACK DLPDU που αναφέρεται σε εκείνο το πακέτο. Το πακέτο ACK το στέλνει άμεσα προς τον άλλο γειτονικό κόμβο και χρησιμοποιείται ως επιβεβαίωση για να απαντήσει ότι έχει ληφθεί επιτυχώς το τελευταίο πακέτο DLPDU. Εξαιρούνται τα πακέτα που απευθύνονται σε όλους τους κόμβους (broadcast) τα οποία δεν χρειάζονται πακέτο αναγνώρισης ACK. Επίσης δεν χρειάζεται πακέτο αναγνώρισης ACK για τα ίδια τα πακέτα αναγνώρισης ACK DLPDUs, που λαμβάνονται. Το πακέτο αναγνώρισης ACK αποτελείται από έναν κώδικα απόκρισης (response code) που είναι 0 αν έχει γίνει επιτυχής μετάδοση και είναι 61, 62 ή 63 αν έχει γίνει κάποιο σφάλμα. Επιπλέον περιλαμβάνει και 2 byte που είναι για ρύθμιση χρόνου (time adjustment) σε microseconds. Ο χρόνος αυτός δείχνει αν έφτασε το πακέτο για το οποίο αναφερόταν η αναγνώριση εγκαίρως ή αν καθυστέρησε. Αν έφτασε νωρίτερα τότε ο αριθμός στα 2 byte θα είναι αρνητικός αριθμός, ενώ αν έφτασε αργότερα θα είναι θετικός αριθμός. Με αυτό τον τρόπο φαίνεται πότε έφτασε το πακέτο και αν καθυστέρησε από το χρόνο που αναμενόταν.

3.2.11.10 Προτεραιότητα (Priority) και έλεγχος ροής (Flow Control) στα πακέτα DLPDU

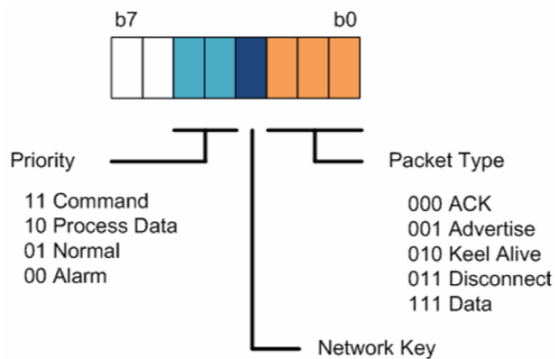
Στα πακέτα δεδομένων που κινούνται μέσα στο δίκτυο, υπάρχουν 4 επίπεδα προτεραιότητας (priority levels) τα οποία καθορίζονται στον προσδιοριστή (Specifier) των πακέτων δεδομένων DLPDU.

b5	b4	Priority levels
1	1	Management
1	0	Process Data
0	1	Normal

0	0	Alarm

Πίνακας 3.12. ο προσδιοριστής DLPDU καθορίζει 4 επίπεδα προτεραιότητας (priority levels)

Τα επίπεδα προτεραιότητας καθορίζονται από τις τιμές των bit: b5, b4. Αυτά τα 4 επίπεδα κατά σειρά προτεραιότητας είναι: Management(11), Process-data (10), Normal (01), Alarm(00).



Εικόνα 81. ο προσδιοριστής DLPDU Specifier και οι τιμές που παίρνουν τα bits σε διάφορες περιπτώσεις.
Πηγή: [8]

α) Management (11) (Πακέτα Διαχείρισης, που περιέχουν εντολές commands):

Τα πακέτα διαχειριστή δικτύου (Network management packets) έχουν πάντα υψηλότερη προτεραιότητα διότι περιέχουν εντολές που διαδίδονται στο δίκτυο έτσι ώστε ο διαχειριστής δικτύου (Network Manager) να μπορεί να διατηρεί όλες τις λειτουργίες του δικτύου να εκτελούνται χωρίς προβλήματα.

β) Alarms (00) (Συναγερμοί):

Η ροή των πακέτων συναγερμών (alarms) μέσα στο δίκτυο είναι περιορισμένη (restricted), δηλαδή έχουν πάντα τη χαμηλότερη προτεραιότητα. Αυτό γίνεται για να μην υπάρχει πλημμύρισμα δεδομένων των συναγερμών (alarm floods) μέσα στο δίκτυο, διότι θα προκαλούσαν εμπόδια που δεν θα επέτρεπαν να εκτελεστούν κάποιες λειτουργίες του δικτύου. Επειδή οι συναγερμοί (alarms) έχουν μία χρονοσήμανση (time-stamp), δεν χάνεται ποτέ καμιά πληροφορία, π.χ. αν υπάρξει αποτυχία σε ακολουθίες πακέτων δεδομένων (failure sequences).

Στην ενδιάμεση μνήμη (buffer) κάθε κόμβου μπορεί να είναι αποθηκευμένο μόνο ένα πακέτο με προτεραιότητα Alarm και όχι περισσότερα ταυτόχρονα. Καθώς γεμίζει η ενδιάμεση μνήμη, όλα τα πακέτα με χαμηλή προτεραιότητα, απορρίπτονται.

γ) Normal (01)(Κανονική):

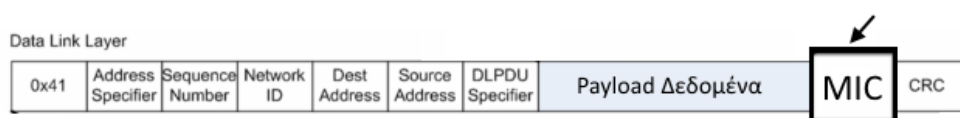
Τελικά όλη υπόλοιπη κυκλοφορία στο δίκτυο έχει μια ροή που καθορίζεται από το πόσο μεγάλος είναι ο χώρος ενδιάμεσης μνήμης απομόνωσης (buffer space) και πόσο μεγάλο είναι το εύρος ζώνης bandwidth. Αυτό είναι το κανονικό επίπεδο (normal) για τα απλά πακέτα δεδομένων που δεν ανήκουν στις άλλες κατηγορίες.

δ) Process Data (10):

Μέσα στην κυκλοφορία του δικτύου, μεγαλύτερη προτεραιότητα από το κανονικό επίπεδο (normal) έχουν τα δεδομένα διεργασιών (process data). Η λειτουργία και ο έλεγχος της διεργασίας έχουν τη δεύτερη θέση σε προτεραιότητα μόνο για να μην συμβεί καμία διακοπή στην επικοινωνία του δικτύου.

3.2.11.11 Κώδικας MIC ακεραιότητας μηνυμάτων με κλειδί (Keyed Message Integrity Code) για την ανίχνευση σφαλμάτων και για την ασφάλεια (Security)

Ο κώδικας MIC ακεραιότητας μηνυμάτων με κλειδί (keyed Message Integrity Code) χρησιμοποιείται στο στρώμα ζεύξης δεδομένων (data-link-layer), DLL, για την πιστοποίηση (authentication) του πακέτου δεδομένων DLPDU. Βρίσκεται στην ουρά (footer) του πακέτου, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 82. Στο πακέτο δεδομένων DLPDU ο κώδικας MIC είναι το πεδίο που βρίσκεται στην ουρά (footer) στη θέση 9, αμέσως μετά τα δεδομένα payload.

Οι συσκευές (Devices) θα πρέπει να απαντήσουν μόνο σε μία μετάδοση unicast, πακέτων δεδομένων DLPDUs χωρίς αναγνώριση (non-acknowledgement) τα οποία έχουν πιστοποιηθεί επιτυχώς (successfully authenticated). Αν δεν έχουν πιστοποιηθεί τα πακέτα απορρίπτονται από τη συσκευή λήψης. (Μετάδοση unicast σημαίνει ότι ο κόμβος αποστολέας, στέλνει τα πακέτα σε μία μόνο συσκευή κάθε φορά).

Ο κώδικας keyed MIC για την ακεραιότητα μηνυμάτων με χρήση κλειδιού, χρησιμοποιείται για να εξασφαλίσει ότι το πακέτο δεδομένων DLPDU προήλθε από έγκυρη συσκευή (device) η οποία είναι αποδεκτή και πιστοποιημένη (authenticated). Το πακέτο δεδομένων DLPDU δεν είναι κρυπτογραφημένο το ίδιο (enciphered) αλλά τα περιεχόμενά του είναι πιστοποιημένα (authenticated) χρησιμοποιώντας τον κώδικα MIC, ο οποίος υπολογίζεται με χρήση του αλγορίθμου CCM που περιγράφεται στο πρότυπο IEEE 802.15.4. Αυτό εξασφαλίζει ότι στην υλοποίηση με εμπορικά chips που κυκλοφορούν στην αγορά, θα αξιοποιηθεί ο επιταχυντής υλικού (hardware accelerator) που θα έχει δυνατότητα να χρησιμοποιηθεί.

Ο κώδικας ακεραιότητας μηνυμάτων MIC υπολογίζεται με βάση το κλειδί δικτύου. Αν ο δέκτης λάβει ένα πακέτο και υπολογίσει τον σωστό MIC με βάση το κλειδί δικτύου, αλλά ο MIC αυτός δεν ταιριάζει με τον MIC που υπάρχει στο πακέτο, τότε ο δέκτης θα απορρίψει το πακέτο.

Υπάρχουν δύο κλειδιά DLL keys:

Το ένα κλειδί ονομάζεται «γνωστό κλειδί» (well-known key) που χρησιμοποιείται σε μηνύματα «διαφήμισης» (advertisements) του κόμβου και όταν γίνεται σύνδεση του κόμβου στο δίκτυο.

Το δεύτερο κλειδί είναι το κλειδί του δικτύου (network key) που χρησιμοποιείται για όλες τις άλλες συναλλαγές (transactions).

Το γνωστό κλειδί (well-known key) είναι το ίδιο πάντα για όλες τις συσκευές στο πρότυπο WirelessHART και έχει τη δεκαεξαδική τιμή

7777 772E 6861 7274 636F 6D6D 2E6F 7267.

Το γνωστό κλειδί (well-known key) χρησιμοποιείται για τα μηνύματα (messages) που περνούν ανάμεσα στη συσκευή που πρόκειται να συνδεθεί στο δίκτυο και στις συσκευές που ήδη είναι συνδεδεμένες μέσα στο δίκτυο. Αυτά λέγονται μηνύματα διαφήμισης.

Το γνωστό δημόσιο κλειδί (well-known public key) είναι η τιμή ASCII των 16 χαρακτήρων που υπάρχουν στο www.hartcomm.org αν θεωρηθεί ως αλφαριθμητικό (string) και είναι η διαδικτυακή διεύθυνση web address του HART Foundation.

3.2.12 Το MAC υπό-επίπεδο ελέγχου πρόσβασης μέσου (Media Access Control)

Το πακέτο δεδομένων (PDU) του υπό-επιπέδου MAC στο WirelessHART είναι το ίδιο με το υπο-επίπεδο MAC του προτύπου IEEE 802.15.4-2006.

Οι βασικοί στόχοι του υπό-επιπέδου MAC sublayer είναι:

α) να διατηρήσει τον συγχρονισμό των χρονικών σχισμών (slot synchronization), β) να προσδιορίζει τις χρονικές σχισμές (slots) τις οποίες πρέπει να εξυπηρετήσει, γ) να ανιχνεύσει (listen) τα πακέτα που διαδίδονται από τους γειτονικούς κόμβους (neighbors)

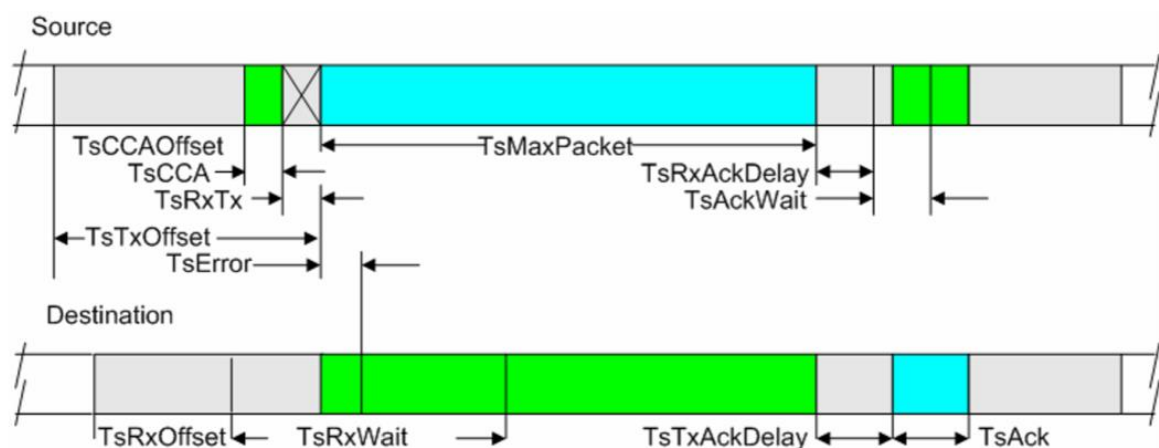
δ) να μεταδώσει τα πακέτα που λαμβάνει από το επίπεδο δικτύου (network layer)

ε) να προσδιορίσει τις συσκευές που θέλουν να έχουν πρόσβαση στο μέσο, δηλαδή στο κανάλι επικοινωνίας.

Χρονισμός των σχισμών (slot timing).

Όλες οι συναλλαγές (transactions) συμβαίνουν σε χρονικές σχισμές (slots). Αυτές πληρούν ορισμένες απαιτήσεις χρονισμού (timing requirements).

Η παρακάτω εικόνα δείχνει μια χρονική σχισμή slot και φαίνεται μια επισκόπηση για τον χρονισμό της συναλλαγής (transaction).



Εικόνα 83. Χρονισμός σχισμών (Slot Timing). Πηγή [8].

Σύμβολο	Περιγραφή
TsTxOffset	Η αρχή της χρονικής σχισμής slot μέχρι την αρχή της μετάδοσης των δεδομένων preamble
TsRxOffset	Η αρχή της χρονικής σχισμής slot μέχρι τη στιγμή που ο πομποδέκτης (transceiver) είναι στην κατάσταση που ακούει (listening)
TsRxWait	Ο ελάχιστος χρόνος αναμονής (time to wait) για την αρχή του μηνύματος (message). Αυτός σχετίζεται με το χρόνο επιτρεπτής ολίσθησης (drift) ανάμεσα στους γειτονικούς κόμβους που είναι ανεκτή (tolerated) ενώ οι επικοινωνίες διατηρούνται ακόμη.
TsError	Αυτή είναι μια διαφορά συγχρονισμού της πραγματικής αρχής του μηνύματος (message) που έρχεται, με καθυστέρηση από την ιδανική αρχή χρόνου του μηνύματος όπως την αντιλαμβάνεται η συσκευή λήψης (receiving device). Δηλαδή δείχνει κατά πόσο χρόνο η συσκευή λήψης αντιλαμβάνεται την συσκευή εκπομπής να είναι εκτός συγχρονισμού.
TsMaxPacket	Ο χρόνος που απαιτείται για να μεταδοθεί (transmit) το μέγιστο πακέτο δεδομένων ως μήνυμα (longest possible message) (Περιλαμβάνει τα δεδομένα φυσικού επιπέδου PhL preamble, delimiter, το μέγεθος length και τα δεδομένα DLPDU)
TsTxAckDelay	Το τέλος του μηνύματος ως την αρχή του μηνύματος αναγνώρισης ACK. Η συσκευή προορισμού πρέπει να επικυρώσει το STX, και να παράγει ένα ACK στη διάρκεια αυτού του χρονικού διαστήματος (interval). Προσοχή: Τα μηνύματα προς όλους τους κόμβους (Broadcast messages) δεν έχουν μήνυμα αναγνώρισης (not acknowledged).
TsRxAckDelay	Το τέλος του μηνύματος ως την στιγμή που ο πομποδέκτης (transceiver) πρέπει να ακούσει (listen) για το μήνυμα αναγνώρισης ACK.
TsAckWait	Ο ελάχιστος χρόνος αναμονής (time to wait) ως την αρχή ενός μηνύματος αναγνώρισης ACK.
TsAck	Η στιγμή για να εκπεμφθεί ένα μήνυμα αναγνώρισης ACK.
TsCCAOffset	Η αρχή της χρονικής σχισμής slot ως την αρχή του CCA έλεγχος καναλιού
TsCCA	Η στιγμή για να εκτελεστεί CCA έλεγχος καναλιού
TsRxTx	Ο μεγαλύτερος χρόνος που απαιτείται για να γίνει αλλαγή κατάστασης από εκπομπή σε λήψη ή το αντίθετο

Πίνακας 3.13. Σύμβολα που χρησιμοποιούνται για το χρονισμό σχισμών (Slot Timing Symbols).

3.2.13 Πίνακες επικοινωνίας (Communication Tables) και ενδιάμεσες μνήμες απομόνωσης (Buffers)

Όλες οι συσκευές διατηρούν ένα σύνολο από πίνακες που ελέγχουν τις επικοινωνίες που εκτελούνται από την συσκευή και συλλέγουν στατιστικά στοιχεία από αυτές τις επικοινωνίες. Επιπλέον τα πακέτα αποθηκεύονται προσωρινά σε ενδιάμεσες μνήμες (buffered) ως μηνύματα (messages) λαμβάνονται, δέχονται επεξεργασία και προωθούνται.

Οι πίνακες που ελέγχουν τις δραστηριότητες επικοινωνίας περιλαμβάνουν:

- superframe table: πίνακας των υπερπλαϊσίων. Πολλαπλά υπερπλαϊσία (superframes) μπορούν να δεχτούν ρυθμίσεις από τον διαχειριστή δικτύου network manager.
- link table. πίνακας των ζεύξεων. Πολλαπλές ζεύξεις (links) μέσα σε ένα υπερπλαϊσίο (superframe) ρυθμίζονται ώστε να καθορίσουν επικοινωνία με έναν συγκεκριμένο γειτονικό κόμβο (neighbor) ή για να εκπέμψουν ένα μήνυμα (broadcast) προς όλους τους κόμβους που ακούν τα μηνύματα αυτής της ζεύξης (link).
- neighbor table: πίνακας γειτονικών κόμβων. Ο πίνακας γειτονικών κόμβων (neighbor table) είναι μία λίστα με όλες τις γειτονικές συσκευές με τις οποίες μπορεί να επικοινωνήσει η συγκεκριμένη συσκευή.
- graph table: πίνακας γραφήματος. Τα γραφήματα (Graphs) χρησιμοποιούνται για να δρομολογηθούν τα μηνύματα (messages) από την πηγή (source) στον προορισμό τους (destination). Η συσκευή (device) δεν γνωρίζει όλη την διαδρομή δρομολόγησης αλλά το γράφημα δείχνει το επόμενο άλμα (next hop) προς τους κατάλληλους κόμβους προορισμού (destinations) οι οποίοι μετά θα προωθήσουν το πακέτο σε άλλους κόμβους για να το δρομολογήσουν προς τον προορισμό του. Επιπλέον από αυτούς τους πίνακες υπάρχει και η ουρά πακέτων (packet queue) που αποθηκεύει προσωρινά τα μηνύματα (messages) σε ενδιάμεση μνήμη (buffer).

3.2.13.1 Link Scheduling Χρονοπρογραμματισμός των Ζεύξεων

Όλες οι συσκευές πρέπει να διατηρούν ένα χρονικό πρόγραμμα ζεύξεων (link schedule) που προσδιορίζει την επόμενη χρονική σχισμή (next slot) που πρέπει να εξυπηρετηθεί. Η εξυπηρέτηση

(Servicing) μιας χρονικής σχισμής slot σημαίνει είτε ότι ο κόμβος προσπαθεί να ακούσει (listening) για να αντληφθεί τότε θα φτάσει ένα νέο πακέτο είτε ότι ο κόμβος μεταδίδει ένα πακέτο (propagating) προς άλλους κόμβους μέσα στο δίκτυο πλέγματος (mesh). Όταν μια χρονική σχισμή slot έχει 2 ζεύξεις (links) όπου ταυτόχρονα ένα πακέτο περιμένει για να μεταδοθεί (propagate) και ένα άλλο πακέτο περιμένει για να ληφθεί (receive), η προτεραιότητα δίνεται στη μετάδοση του πακέτου και έπεται η ακοή (listen) για ένα νέο πακέτο. Αν και εκ πρώτης όψης ο χρονοπρογραμματισμός ζεύξεων (scheduling) μοιάζει να είναι μία απλή και άμεση διαδικασία, στην πραγματικότητα είναι περίπλοκη διαδικασία διότι υπάρχουν προτεραιότητες στις συναλλαγές (transaction priorities), τροποποιήσεις στις ζεύξεις (links), και ενεργοποίηση (enabling) ή απενεργοποίηση (disabling) των υπερπλαisiών (superframes). Κάθε συμβάν που επηρεάζει το χρονοπρογραμματισμό ζεύξεων μπορεί να έχει ως αποτέλεσμα να γίνει μια ανακατανομή των ζεύξεων μετάδοσης (transmit links). Για παράδειγμα, αν μία συναλλαγή με υψηλή προτεραιότητα έχει αποτυχία στη μετάδοσή της τότε πρέπει να γίνει ξανά ο προγραμματισμός χρόνου (rescheduled). Συνεπώς, οι συναλλαγές με χαμηλότερη προτεραιότητα μπορεί να αναβληθούν για μια επόμενη ζεύξη και η τρέχουσα ζεύξη τους να δοθεί στην συναλλαγή υψηλής προτεραιότητας. Μπορεί αυτό να απαιτεί να γίνουν περισσότερες αλλαγές σε ευρεία έκταση, όπως για παράδειγμα να απενεργοποιηθεί ένα υπερπλαίσιο (superframe) ή να διαγραφεί πλήρως από το χρονοπρογραμματισμό.

3.2.14 Επίπεδο Δικτύου (Network Layer) και Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο δικτύου (network layer) εκτελεί τις λειτουργίες δρομολόγησης (routing) στο δίκτυο. Χειρίζεται την διευθυνσιοδότηση (addressing) και την παράδοση (delivery) των δεδομένων.

Το επίπεδο δικτύου μεταφέρει τα πακέτα από σημείο σε σημείο (end-to-end). Περιλαμβάνει και άλλα χαρακτηριστικά όπως είναι οι πίνακες δρομολόγησης (route tables), που χρησιμοποιούνται για δρομολόγηση με γραφήματα, καθώς και οι πίνακες χρόνου (time tables) που χρησιμοποιούνται για μια ανακατανομή του εύρους ζώνης σε συγκεκριμένες υπηρεσίες όπως είναι η έκδοση δεδομένων (publish data) και η μεταφορά μπλοκ δεδομένων (blocks of data). Η μεταφορά μπλοκ δεδομένων (Block transfer) υποστηρίζεται με προσωρινή κατανομή ενός μεγάλου εύρους ζώνης (high bandwidth) για τη μεταφορά δεδομένων που ονομάζεται «transport pipe» και αυτό το εύρος ζώνης ελευθερώνεται όταν ολοκληρωθεί η μεταφορά του μπλοκ

δεδομένων (block transfer). Η μεταφορά μπλόκ δεδομένων (Block transfer) είναι διαφανής στα ανώτερα στρώματα (upper layers).

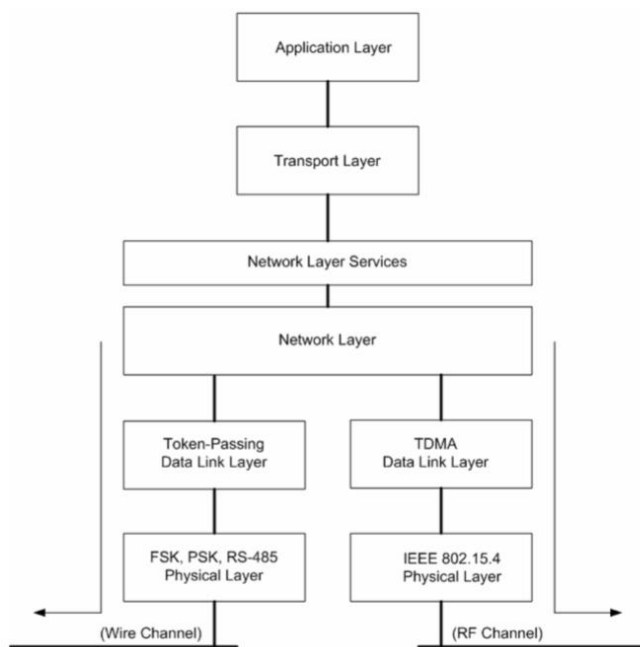
Η ασφάλεια στο επίπεδο δικτύου αποτελεί ένα υπό επίπεδο που είναι το στρώμα ασφάλειας.

Το επίπεδο μεταφοράς (transport layer)

Το επίπεδο μεταφοράς (transport layer) ελέγχει την μετάδοση των δεδομένων ώστε να γίνεται με αξιοπιστία και εγκαίρως ανάμεσα σε δύο κόμβους του δικτύου. Αυτό γίνεται με τον έλεγχο ροής, τον τεμαχισμό (segmentation) και την επανασύνθεση (desegmentation) των πακέτων δεδομένων, και με τον έλεγχο σφαλμάτων.

Τα μεγάλα σύνολα δεδομένων (Data sets) αυτόματα τεμαχίζονται (segmented) στην συσκευή πηγής (source device) και μετά συναρμολογούνται ξανά (re-assembled) στην συσκευή προορισμό (destination).

Το επίπεδο συνόδου (session layer) διαχειρίζεται το διάλογο, την σύνοδο επικοινωνίας και τις συνδέσεις μεταξύ δύο κόμβων του δικτύου. Στο πρότυπο WirelessHART το επίπεδο δικτύου (network layer) ενσωματώνει τα 3 επίπεδα του μοντέλου OSI. Είναι το σημείο που συγκλίνουν τα ενσύρματα δίκτυα του HART που είναι Token-Passing και τα ασύρματα δίκτυα του WirelessHART που βασίζονται στο TDMA. Το επίπεδο δικτύου παρέχει υπηρεσίες (services) στο ανώτερο επίπεδο που είναι το επίπεδο εφαρμογών (application link layer). Το πακέτο δεδομένων στο επίπεδο δικτύου είναι το NPDU.



Εικόνα 84 Η εμβέλεια του επιπέδου δικτύου (network layer). Πηγή: [8]

Στην παραπάνω εικόνα φαίνεται το επίπεδο μεταφοράς (transport layer) που ορίζεται ως μέρος του επιπέδου δικτύου (network layer) το οποίο διαχειρίζεται και αυτό τις συνόδους επικοινωνίας (sessions). Πάνω από το επίπεδο μεταφοράς βρίσκεται το επίπεδο εφαρμογών (application layer) του HART που ορίζει τους επιτρεπτούς τύπους δεδομένων (data types), τις διαδικασίες και τις εντολές για το HART. Κάτω από το επίπεδο δικτύου βρίσκονται τα δύο βασικά είδη δικτύων του HART: τα ενσύρματα δίκτυα TokenPassing και τα ασύρματα δίκτυα TDMA.

3.2.14.1 Δρομολόγηση (Routing)

Το επίπεδο δικτύου (network layer) για το WirelessHART υποστηρίζει δρομολόγηση με γραφήματα (Graph routing) και δρομολόγηση πηγής (Source routing)

- Δρομολόγηση με Γραφήματα (Graph routing).

Μία πορεία δρομολόγησης με γραφήματα (Graph Route) είναι ένα υποσύνολο κατευθυντικών ζεύξεων (directed links) και συσκευών (devices) που παρέχουν πλεονάζουσες (redundant) διαδρομές επικοινωνίας ανάμεσα σε έναν κόμβο πηγή (source) και σε έναν κόμβο προορισμό (destination), ώστε να υπάρχουν εναλλακτικές διαδρομές. Όταν χρησιμοποιείται η δρομολόγηση graph routing για την προώθηση ενός πακέτου NPDU, δίνεται ένα αναγνωριστικό Graph ID στο

πακέτο και απουσιάζει το προαιρετικό πεδίο source routing από το πακέτο NPDU. Μια συσκευή (device) έχει αρκετά γραφήματα και κάθε γράφημα δίνει στη συσκευή δυνατότητα να επιλέξει έναν ή περισσότερους γειτονικούς κόμβους για να προωθήσει το πακέτο σε αυτόν τον κόμβο, ώστε να φτάσει το πακέτο στον τελικό προορισμό.

Στο WirelessHART, ο διαχειριστής δικτύου (Network Manager) δημιουργεί και διατηρεί τα γραφήματα αυτά. Κάθε συσκευή πεδίου (field device) έχει τη δική της λίστα γραφημάτων (graphs) που μπορεί να τα χρησιμοποιήσει για να δρομολογήσει τα πακέτα σε οποιονδήποτε κόμβο του δικτύου. Το κάθε ένα από αυτά τα γραφήματα προσδιορίζεται από ένα αναγνωριστικό Graph ID. Το ίδιο Graph ID δίδεται σε ένα πακέτο NPDU. Το αναγνωριστικό ID δείχνει σε μια συσκευή ποιο γράφημα θα πρέπει να χρησιμοποιήσει για να δρομολογήσει το πακέτο. Στη δρομολόγηση με γραφήματα (graph routing) παρέχεται η δυνατότητα η συσκευή να επιλέξει κάθε φορά διαφορετική δρομολόγηση από διαφορετικούς γειτονικούς κόμβους, διότι συνήθως ο κάθε κόμβος έχει αρκετούς γειτονικούς κόμβους ώστε μπορεί να επιλέγει εναλλακτικές διαδρομές. Ο διαχειριστής δικτύου (Network Manager) διατηρεί τα γραφήματα (graphs) με έναν δυναμικό τρόπο. Υπάρχει αξιοπιστία ακόμα και αν κάποιο κόμβοι αποσυνδεθούν από το δίκτυο ή αν πάθουν βλάβη, διότι επιλέγεται μια εναλλακτική διαδρομή.

Το WirelessHART έχει και μία άλλη απλοποιημένη μορφή δρομολόγησης με γραφήματα (graph routing) η οποία ονομάζεται δρομολόγηση με υπερπλαίσια (superframe routing). Όταν χρησιμοποιείται αυτή, τότε το πεδίο (field) με το αναγνωριστικό γραφήματος Graph ID ρυθμίζεται ώστε να είναι ένα αναγνωριστικό superframe ID. Όταν μία συσκευή (device) προσπαθεί να ψάξει (look up) το αναγνωριστικό ID στη δική της λίστα με γραφήματα θα αποτύχει και δεν θα το βρει. Τότε θα υποθέσει ότι είναι ένα αναγνωριστικό υπερπλαισίου (superframe ID). Αν είναι έγκυρο το superframe ID τότε το επίπεδο δικτύου (Network Layer) θα ψάξει για έναν γειτονικό κόμβο (neighbor) με μία ζεύξη (link) σε αυτό το υπερπλαίσιο (superframe) και θα προωθήσει τα πακέτα σε αυτό.

- Δρομολόγηση πηγής (Source).

Μία πορεία δρομολόγησης πηγής (Source Route) είναι μία μεμονωμένη κατευθυντική διαδρομή (συσκευές και ζεύξεις) ανάμεσα σε έναν κόμβο πηγής (source) και σε έναν κόμβο προορισμού (destination) device. Η διαδρομή πηγής (source route) είναι στατική και καθορίζεται μέσα στο ίδιο το πακέτο. Το WirelessHART υποστηρίζει την δρομολόγηση πηγής. Η δρομολόγηση πηγής (Source routing) καθορίζεται από το πρότυπο WirelessHART αλλά μόνο για να χρησιμοποιείται

σε περιπτώσεις ελέγχου και αποσφαλμάτωσης των διαδρομών (paths) και όχι στην κανονική δρομολόγηση πακέτων.

Όταν είναι παρόν ένα πεδίο source routing στο πακέτο NPDU τότε αυτό φαίνεται και στο byte ελέγχου (control byte) του πακέτου, διότι το control byte έχει ένα αντίστοιχο bit σε κατάσταση set, που δηλώνει παρουσία ενός πεδίου source routing στο πακέτο. Τότε η συσκευή χρησιμοποιεί μια λίστα με διαδρομές δρομολόγησης (source route list) που βρίσκεται στο τέλος της επικεφαλίδας (header) του πακέτου NPDU. Η λίστα (source route list) ρυθμίζεται από τον διαχειριστή δικτύου (Network Manager). Κάθε φορά που ένας κόμβος (node) προωθεί ένα πακέτο, ψάχνει τη διαδρομή δρομολόγησης στη λίστα (source route list) και στέλνει το πακέτο στον επόμενο κόμβο. Αυτή η διαδικασία δρομολόγησης δεν είναι αξιόπιστη και είναι επιρρεπής σε αποτυχία των διαδρομών διότι παρέχει στατική διαδρομή χωρίς τη δυνατότητα επιλογής για διαφορετικές εναλλακτικές διαδρομές. Αυτό συμβαίνει διότι η λίστα για κάθε κόμβο επιτρέπει να προωθήσει το πακέτο σε έναν μόνο γειτονικό κόμβο. Αν κάθε κόμβος στη λίστα αποτύχει τότε δεν υπάρχει εναλλακτική διαδρομή. Το πακέτο θα απορριφθεί και δεν θα φτάσει στον προορισμό του. Έτσι η δρομολόγηση πηγής (Source routing) για το WirelessHART θεωρείται λιγότερο αξιόπιστη.

3.2.14.2 Ασφάλεια στο επίπεδο δικτύου

Το επίπεδο δικτύου για να διαχειριστεί τις επικοινωνίες από σημείο προς σημείο (end-to-end) χρησιμοποιεί συνόδους επικοινωνίας (sessions). Για να επικοινωνήσει μία συσκευή (device) με μία άλλη ίδια συσκευή (peer device) μπορεί να καθοριστούν περισσότερες από μία σύνοδοι επικοινωνίας (sessions). Μία συσκευή δικτύου πρέπει να παρακολουθεί τις πληροφορίες ασφάλειας όπως είναι κλειδιά κρυπτογράφησης και οι μετρητές nonce counters και να παρακολουθεί και τις πληροφορίες μεταφοράς όπως είναι οι αξιόπιστοι αριθμοί ακολουθίας μεταφοράς, οι μετρητές επαναληπτικών προσπαθειών για μετάδοση κ.λπ. Αυτό ισχύει για κάθε σύνοδο επικοινωνίας (session) στην οποία συμμετέχει η συσκευή. Οι σύνοδοι επικοινωνίας (Sessions) μπορούν να δημιουργηθούν ανάμεσα σε δύο οποιουσδήποτε κόμβους του δικτύου.

3.2.14.3 Υπηρεσίες για το επίπεδο δικτύου (Network Layer)

Εντολές μηνυμάτων Message SPs.

Οι εντολές μηνυμάτων Message SPs στο επίπεδο δικτύου, παρέχουν υπηρεσίες (services) που υποστηρίζουν βασικές λειτουργίες για μεταφορά δεδομένων μεταξύ των συσκευών (devices). Το επίπεδο δικτύου (network layer) υποστηρίζει επικοινωνίες για αίτηση/απόκριση (request/response) και επικοινωνίες μονής κατεύθυνσης για κυκλοφορία δεδομένων ειδοποιήσεων (notification).

TRANSMIT

- TRANSMIT.request(handle, dest, priority, timetableID, transportType, payload)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να μεταδώσει (transmit) ένα πακέτο στο επίπεδο δικτύου (Network Layer).

Οι παράμετροι που υπάρχουν στην υπηρεσία request περιλαμβάνουν:

- handle –Χειριστής. Το επίπεδο δικτύου (Network Layer) επιστρέφει την τιμή αυτή στο αντίστοιχο TRANSMIT.confirm και επιτρέπει στο επίπεδο εφαρμογών (Application Layer) να αντιστοιχίζει τις αιτήσεις (requests) με τις αποκρίσεις (responses).
- dest –δείχνει τον προορισμό του πακέτου (destination).

Ο προορισμός είναι μία από τις 3 παρακάτω περιπτώσεις :

uniqueID, nickname, broadcast, δηλαδή:

uniqueID – η μεγάλη διεύθυνση (long address) της συσκευής προορισμού (destination device)

nickname – η σύντομη διεύθυνση (short address) της συσκευής προορισμού (destination device)

broadcast – η διεύθυνση εκπομπής προς όλους τους γειτονικούς κόμβους (broadcast address) υποδεικνύεται στο πακέτο δεδομένων NPDU και το byte ελέγχου (control byte) δείχνει μια σύντομη διεύθυνση προορισμού (short destination address).

- priority - Προτεραιότητα. Η προτεραιότητα του πακέτου καθορίζεται από τα περιεχόμενα των δεδομένων payload. Κατά σειρά προτεραιότητας είναι μία από τις παρακάτω : {management, process data, normal, alarm}.
- timetableID – Αναγνωριστικό πίνακα χρόνου. Όποιος κόμβος ξεκινά την επικοινωνία έχει την ευθύνη να λάβει επαρκές εύρος ζώνης (bandwidth) από το διαχειριστή δικτύου (Network Manager) ώστε να επιτρέψει να ξεκινήσει η συναλλαγή. Το timetableID προσδιορίζει το ποσοστό

εύρους ζώνης (bandwidth quota) που πρέπει να χρησιμοποιηθεί για αυτή τη συναλλαγή (transaction).

Αν το εύρος ζώνης που απομένει δεν είναι επαρκές για το TRANSMIT.request τότε πρέπει να επιστρέψει ένα μήνυμα σφάλματος error must και τα δεδομένα payload να μη μεταδοθούν.

- transportType – Ο τύπος μεταφοράς (transport type) δείχνει ότι η λειτουργία που ζητήθηκε από το επίπεδο μεταφοράς (Transport Layer) operation requested και χρησιμοποιείται για να ρυθμίσει (set) την τιμή του Transport Byte.

- payload – Τα περιεχόμενα της παραμέτρου payload μεταδίδονται στη συσκευή προορισμού (destination device.)

Ο παρακάτω πίνακας δείχνει τους κώδικες τύπου μεταφοράς (Transport Type Codes).

Κώδικας(code)	Περιγραφή	Broadcast	ACK' ed	
0	Αίτηση μεταφοράς (Transfer Request). Αυτή χρησιμοποιείται από το μηχανισμό Block Data Transfer Mechanism από την πλευρά της κύριας συσκευής (master side)	-	-	→Req
1	Απόκριση στη μεταφορά (Transfer Response). Αυτή χρησιμοποιείται από το μηχανισμό Block Data Transfer Mechanism από την πλευρά της εξαρτώμενης συσκευής (slave side)	-	-	←Rsp
2	Αίτηση αποστολής σε έναν μόνο παραλήπτη (Request-Unicast) (TRANSMIT.request only). Αυτό χρησιμοποιείται από τις κύριες συσκευές (master side) Devices που εκτελούν συναλλαγές (transactions) αίτησης/απόκρισης (Request/Response) (π.χ, όταν ρυθμίζουν μια συσκευή)	-	X	→Req

3	Απόκριση στην αποστολή προς έναν μόνο παραλήπτη (Response-Unicast) (TRANSMIT.response only). Αυτό χρησιμοποιείται από τις εξαρτώμενες συσκευές (slave side) Devices που εκτελούν συναλλαγές αίτησης απόκρισης (Request/Response) transactions (π.χ.,όταν ρυθμίζουν μια συσκευή)	-	X	←Rsp
4	Αναζήτηση κατά την εκπομπή προς όλους (Search-Broadcast) (TRANSMIT.request only). αυτό χρησιμοποιείται όταν στέλνει ένα μήνυμα προς όλους (broadcast message) όταν προσπαθεί να προσδιορίσει μια συγκεκριμένη συσκευή (π.χ., Command 21)	X	-	→Req
5	Δημοσίευση μιας εκπομπής προς όλους (Publish-Broadcast) (TRANSMIT.response only). Αυτή είναι ανακοίνωση μίας εκπομπής προς όλους (broadcast announcement) και η ανακοίνωση αυτή στέλνεται προς όλες τις συσκευές του δικτύου (π.χ., εκπομπή τιμών χρόνου-time broadcast)	X	-	←Rsp
6	Αίτηση εκπομπής προς όλους (Request-Broadcast) (TRANSMIT.request only). (π.χ., αλλαγή του αναγνωριστικού δικτύου Network ID)	X	X	→Req
7	Απόκριση στην εκπομπή προς όλους (Response-Broadcast) (TRANSMIT.response only). Αυτό είναι απόκριση προς έναν μόνο παραλήπτη (unicast response) to στην αντίστοιχη Request-Broadcast.	X	X	←Rsp
8	Δημοσίευση/ειδοποίηση (Publish / Notify) (TRANSMIT.response only). (π.χ., process data)	-	-	←Rsp

Πίνακας 3.14. Οι κώδικες τύπου μεταφοράς (Transport type codes).Πηγή: [8]

Το επίπεδο δικτύου (Network Layer) πρέπει να έχει επαρκή ικανότητα για προσωρινή αποθήκευση σε ενδιάμεση μνήμη (buffering) που να χωράει τουλάχιστον ένα μήνυμα παραπάνω από το μήνυμα που μεταδίδεται στην τρέχουσα συναλλαγή (transaction).

- TRANSMIT.indicate (handle, srcAddr, priority, transportType, payload)

Αυτή η εντολή (service primitive) ενεργοποιείται (triggered) όταν ληφθεί ένα πακέτο στο επίπεδο δικτύου (Network Layer) και τα δεδομένα payload είναι έτοιμα για να τα διαβάσει το υψηλότερο στρώμα (higher layer).

- TRANSMIT.response (handle, payload)

Αυτή η εντολή (service primitive) χρησιμοποιείται από τη συσκευή (device) για να απαντήσει (respond) σε ένα γεγονός (event) TRANSMIT .indicate που απαιτεί μία απόκριση (response)

- TRANSMIT.confirm (handle, localStatus, [payload])

Αυτή η εντολή (service primitive) χρησιμοποιείται από το επίπεδο δικτύου (Network Layer) για να επιστρέψει την κατάσταση status μιας προηγούμενης εντολής TRANSMIT.request πίσω σε αυτόν που την κάλεσε.

- FLUSH.request (handle)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να διαγράψει ένα πακέτο με βάση τον χειριστή (handle).

- FLUSH.confirm (handle, localStatus)

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δείξει αν ένα πακέτο έχει διαγραφεί επιτυχώς ή όχι.

LOCAL_MANAGEMENT

Υπηρεσίες διαχείρισης (Management Services)

Οι εντολές διαχείρισης (Management SPs) υποστηρίζουν τη ρύθμιση του επιπέδου δικτύου (network layer) και επιπλέον υποστηρίζουν την πρόσβαση στις πληροφορίες στατιστικής που συλλέγει.

- LOCAL_MANAGEMENT.request(service, [data])

Αυτή η εντολή (service primitive) χρησιμοποιείται για να ρυθμίσει τις ιδιότητες (properties) στο επίπεδο δικτύου (Network Layer).

- LOCAL_MANAGEMENT.confirm(service, status, [data])

Αυτή η εντολή (service primitive) χρησιμοποιείται για να επιστρέψει αποτελέσματα από μία εντολή LOCAL_MANAGEMENT .confirm σε όποιον είχε εκτελέσει προηγουμένως την εντολή αίτησης (request).

- LOCAL_MANAGEMENT.indication(service, status, [data])

Αυτή η εντολή (service primitive) χρησιμοποιείται για να δώσει ειδοποίηση (notify) ότι συνέβη ένα γεγονός (event) στο επίπεδο δικτύου (Network Layer) το οποίο όμως συνέβη χωρίς να είχε γίνει προηγουμένως μια αίτηση (request) για το γεγονός αυτό.

Η πρώτη παράμετρος είναι η υπηρεσία που ζητείται (requested service).

Οι υπηρεσίες φαίνονται στον παρακάτω πίνακα.

Υπηρεσία	Περιγραφή
RESET	Επαναφορά (Reset) και αρχικοποίηση (initialize) του επιπέδου δικτύου (Network Layer). Όλοι οι πίνακες δικτύου (network tables) σβήνονται (cleared) όταν καλείται αυτή η εντολή (primitive). Αυτή η εντολή (primitive) συνήθως καλείται (invoked) όταν ενεργοποιείται μια συσκευή (device power-up) ή όταν εγκαθίσταται η συσκευή για πρώτη φορά σε ένα νέο δίκτυο.
WRITE_SESSION_KEY	Ρυθμίζει την σύνοδο επικοινωνίας (session) και το nonce.
DEL_SESSION	Διαγράφει μια σύνοδο επικοινωνίας (session)
ADD_ROUTE	Προσθέτει διαδρομή δρομολόγησης (route) προς μια συγκεκριμένη διεύθυνση προορισμού (destination address).
DEL_ROUTE	Διαγράφει τις πληροφορίες για μια διαδρομή δρομολόγησης (route).
DEFAULT_ROUTE	Θέτει μια συγκεκριμένη διαδρομή δρομολόγησης (route) ως προκαθορισμένη (default).
READ_PDU_TIMEOUT	Διαβάζει τον αριθμό χρονικών σχισμών (slots) από τη στιγμή που δημιουργείται το πακέτο μέχρι τη στιγμή που απορρίπτεται. Η συσκευή ελέγχει τον ASN Snippet σε σύγκριση με τον τρέχοντα ASN

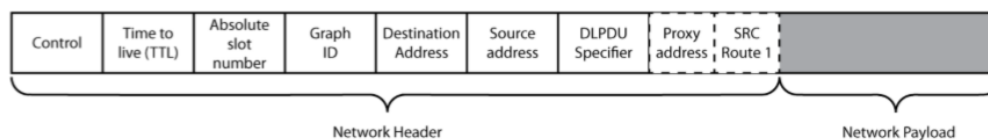
WRITE_PDU_TIMEOUT	Γράφει τον αριθμό χρονικών σχισμών slots από τη στιγμή που δημιουργείται το πακέτο μέχρι τη στιγμή που απορρίπτεται. Η συσκευή ελέγχει τον ASN Snippet σε σύγκριση με τον τρέχοντα ASN (Absolute Slot Number).
READ_TTL	Ανάγνωση της τιμής TTL (Time To Live). Η τιμή TTL αρχικοποιείται όταν δημιουργείται ένα νέο πακέτο.
WRITE_TTL	Εγγραφή της τιμής TTL

Πίνακας 3.15. Εντολές διαχείρισης (Management Commands) τοπικών συσκευών (Local Device). Πηγή: [8].

3.2.14.4 Το πακέτο δεδομένων NPDU του επιπέδου δικτύου (Network Layer)

Το επίπεδο δικτύου παρέχει δυνατότητες για δρομολόγηση (routing), ασφάλεια από σημείο σε σημείο (end-to-end) και μεταφορά (transport).

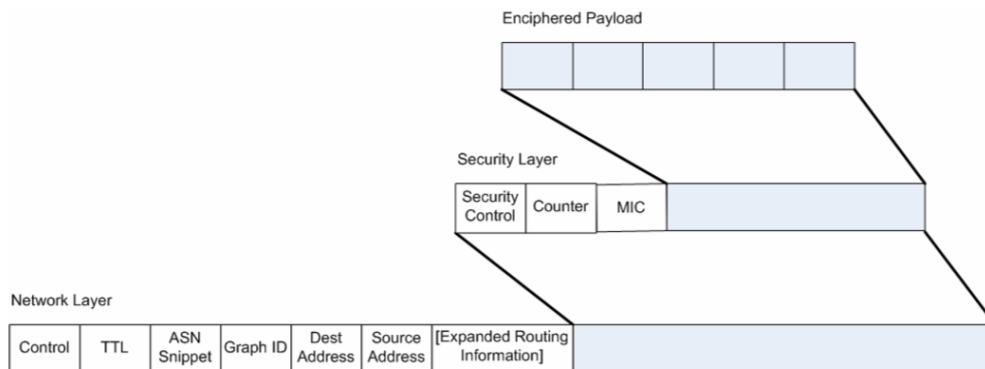
Τα πακέτα δεδομένων (PDU) του επιπέδου δικτύου (Network Layer) λέγονται NPDU.



Εικόνα 85 Το πακέτο δεδομένων NPDU Network Layer Protocol Data Unit. Πηγή [7, p. 47].

Όπως φαίνεται στην παραπάνω εικόνα, Το πακέτο δεδομένων (PDU) για το επίπεδο δικτύου (network layer), του WirelessHART αποτελείται από τρεις ξεχωριστές λειτουργίες που περιγράφονται από αντίστοιχα πεδία.

Τα 7 πεδία (fields) (από αριστερά), είναι από το επίπεδο δικτύου (network layer) και περιλαμβάνουν όλα εκείνα τα πεδία που απαιτούνται για να δρομολογηθεί (route) το πακέτο δεδομένων NPDU στον τελικό προορισμό του. Μετά από αυτά τα πεδία ακολουθούν 3 πεδία ασφάλειας (security fields) που παρεμβαίνουν στα προηγούμενα πεδία και είναι από το επίπεδο ασφάλειας (security layer). Τέλος, ακολουθούν τα πραγματικά δεδομένα προς μετάδοση NPDU payload που είναι κρυπτογραφημένα (enciphered) και περιέχουν τις πληροφορίες που ανταλλάσσονται μεταξύ των κόμβων του δικτύου.

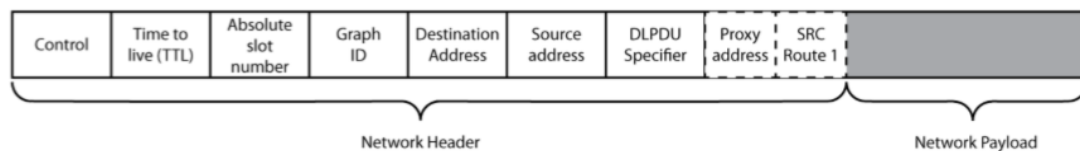


Εικόνα 86. Η δομή του πακέτου δεδομένων NPDU στο WirelessHART. Πηγή [8]

Όλα αυτά τα στοιχεία αποτελούν το πακέτο δεδομένων NPDU.

Παρακάτω εξηγούνται τα πεδία περισσότερο λεπτομερώς.

Τα πεδία από το επίπεδο δικτύου.



Εικόνα 87. Το πακέτο δεδομένων NPDU Network Layer Protocol Data Unit. Πηγή: [7, p. 47]

Τα πεδία του επιπέδου δικτύου (Network Layer) που είναι ένα τμήμα (segment) του πακέτου δεδομένων PDU είναι τα παρακάτω πεδία (fields):

- 1-byte Πεδίο ελέγχου (Control field)
- 1-byte Time To Live (TTL) μετρητής αλμάτων (hop counter)
- 2 bytes τα λιγότερο σημαντικά (least-significant) 2 bytes του Absolute Slot Number για μέτρηση της καθυστέρησης (Latency Count)
- 2-byte Graph ID αναγνωριστικό γραφήματος
- Η τελική (final) διεύθυνση προορισμού (Destination Address) και η αρχική (original) διεύθυνση πηγής (Source Address)
- Προαιρετικά (Optional) πεδία δρομολόγησης (routing fields).

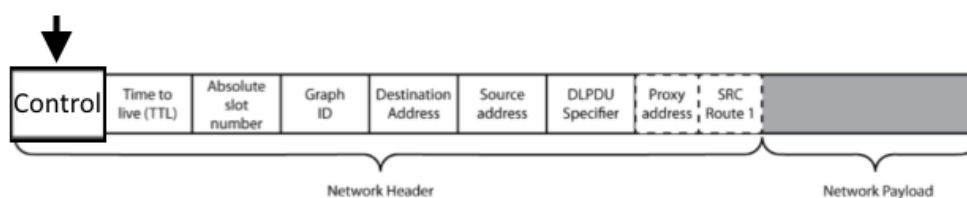
Αυτά τα πεδία συνοψίζονται στον παρακάτω πίνακα

Θέση	Μήκος σε Bytes	Όνομα / περιγραφή	Τμήμα πακέτου
1	1	Control Field	Network Header Επικεφαλίδα δικτύου
2	1	Time To Live (TTL)	
3	2	Part of the Absolute Slot Number (ASN)	
4	2	Graph ID	
5	2 ή 8	Final Destination	
6	2 ή 8	Original Source	
7-9	0-18	Optional Routing Fields	
3 Πεδία Ασφάλειας			Ασφάλεια
Πραγματικά δεδομένα Payload κρυπτογραφημένα			Payload

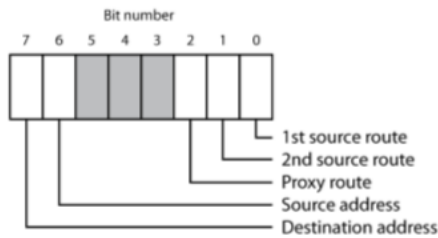
Πίνακας 3.16. Τα πεδία στο πακέτο NPDU του επιπέδου δικτύου (Network Layer).

Το συνολικό πακέτο δεδομένων NPDU για το επίπεδο δικτύου (Network Layer) αποτελείται από τα 7 πεδία της επικεφαλίδας (header), μαζί με τα 3 πεδία ασφάλειας (security fields) και αυτά ακολουθούνται από τα πραγματικά δεδομένα που πρέπει να μεταδοθούν (NPDU payload), που είναι κρυπτογραφημένα (enciphered).

Το πεδίο ελέγχου καταλαμβάνει 1 Byte (Control Byte). Είναι το πρώτο byte στο πακέτο δεδομένων Network PDU.

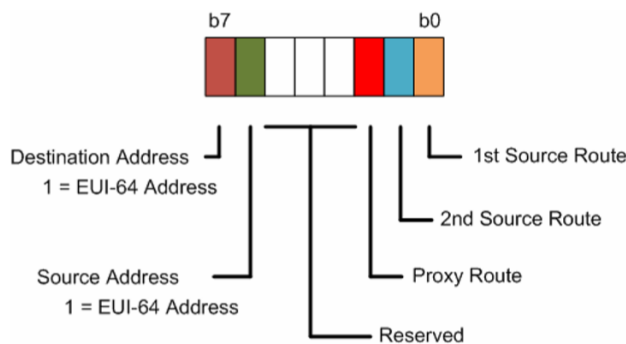


Εικόνα 88. Το byte Ελέγχου (Control Byte) είναι ένα πεδίο που βρίσκεται στη θέση 1, στο πακέτο δεδομένων NPDU του επιπέδου δικτύου (Network Layer).



Εικόνα 89. Το byte Ελέγχου (Control Byte). Πηγή: [7]

Το πρώτο byte στο πακέτο δεδομένων Network PDU είναι το πεδίο ελέγχου (Control byte) που φαίνεται στην παρακάτω εικόνα. Τα δύο πρώτα bits (bit 7 και bit 6) δείχνουν αν η διεύθυνση πηγής (source address) και η διεύθυνση προορισμού (destination address) ορίστηκαν να είναι διευθύνσεις της μορφής long (8-byte) που ονομάζεται EUI-64™ ή αν ορίστηκαν να είναι της μορφής short (2-byte) που ονομάζεται Nickname. Τα επόμενα 3 bits (bits 5-3) είναι κρατημένα (reserved) για μελλοντική χρήση και έχουν τεθεί στην τιμή 0.



Εικόνα 90. Το byte Ελέγχου (Control Byte) Πηγή [8]

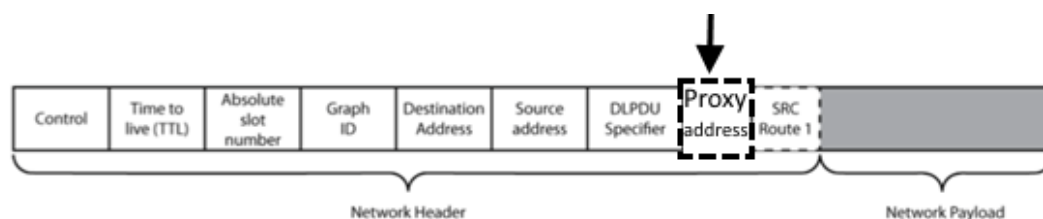
Τα bits b2, b1, b0, όταν είναι στην κατάσταση set, δείχνουν την παρουσία προαιρετικών (optional) πεδίων δρομολόγησης (routing fields) που μπορεί να περιέχονται στο πακέτο NPDU. Όταν υπάρχουν αυτά τα πεδία, τότε αν το bit 2 είναι στην κατάσταση set, χρησιμοποιείται το πεδίο Proxy route, που είναι ένα πεδίο (field) με μέγεθος 2-byte. Το κάθε ένα από τα 2 Source Routes είναι πεδίο με μέγεθος 8-bytes. Από τις τιμές των bits b1, b0 φαίνεται αν θα χρησιμοποιηθούν ή όχι η 1η Source Route και η 2η Source Route. Συνεπώς με βάση τις τιμές των bits 2-0, το μήκος (length) της επικεφαλίδας (header) ανάλογα με τις διαφορετικές περιπτώσεις μπορεί να είναι 0, 2, 10, ή 18 bytes.

Όταν το επίπεδο δικτύου (Network Layer) λάβει ένα πακέτο δεδομένων NPDU η διεύθυνση προορισμού (Destination Address) του πακέτου ελέγχεται αν είναι ίδια με τη διεύθυνση της

συσκευής (device). Αν η διεύθυνση είναι ίδια, τότε το πακέτο NPDU πιστοποιείται (authenticated) και τα δεδομένα payload αποκρυπτογραφούνται (deciphered). Όταν αυτά γίνουν με επιτυχία, τότε καλείται η εντολή (primitive) TRANSMIT.indicate για τα δεδομένα payload.

Το προαιρετικό πεδίο Proxy Route

Στο Byte Ελέγχου (Control Byte) το bit b2 δηλώνει αν θα υπάρχει το πεδίο Proxy Route. Αυτό το πεδίο (field) είναι προαιρετικό (optional) και χρησιμοποιείται όταν ο τελικός προορισμός ενός πακέτου είναι μια συσκευή η οποία δεν είναι πλήρες μέλος του δικτύου WirelessHART, είτε διότι βρίσκεται ακόμη στη διαδικασία σύνδεσης στο δίκτυο, είτε επειδή βρίσκεται σε κατάσταση καραντίνας (quarantine)



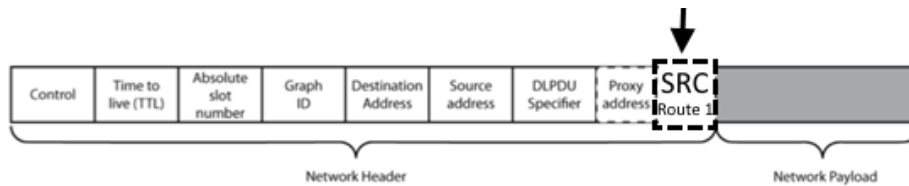
Εικόνα 91 Το προαιρετικό πεδίο Proxy Route στο πακέτο δεδομένων NPDU.

Αυτό το πεδίο Proxy Route προσδιορίζει μία διεύθυνση 2 byte του τύπου nickname η οποία δείχνει μία άλλη συσκευή που είναι ήδη πλήρες μέλος του δικτύου και επικοινωνεί με την συσκευή που δεν είναι πλήρες μέλος του δικτύου. Όταν το πακέτο φτάσει στη συσκευή που είναι πλήρες μέλος του δικτύου, τότε αυτή θα το προωθήσει προς το γειτονικό κόμβο που δεν είναι πλήρες μέλος του δικτύου και είναι ο τελικός προορισμός του πακέτου (final destination).

Το προαιρετικό πεδίο Source Route

Όπως αναφέρθηκε, στην αρχή του πακέτου NPDU, βρίσκεται το πεδίο Byte Ελέγχου (Control Byte). Στο πεδίο Control, το bit b1 και το b0, δηλώνουν την ύπαρξη ενός ή δύο προαιρετικών πεδίων Source Route.

Το πεδίο (field) Source Route πρέπει να χρησιμοποιείται μόνο σε περιπτώσεις που ελέγχονται διαδρομές (paths) μέσα στο δίκτυο και γίνεται αποσφαλμάτωση (debugging) ή έλεγχος (testing) για αυτές τις διαδρομές.



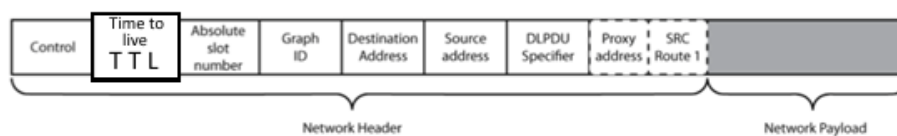
Εικόνα 92. Το προαιρετικό πεδίο Source Route στο πακέτο δεδομένων NPDU

Στο πακέτο δεδομένων NPDU μπορούν να υπάρχουν μέχρι δύο τέτοια πεδία Source Route. Αν υπάρχουν, τότε η παρουσία τους δηλώνεται από τα bit b1 και b0 που βρίσκονται στο control byte στην αρχή του πακέτου NPDU.

Το κάθε πεδίο Source Route περιέχει 4 διευθύνσεις του τύπου διεύθυνσης nickname που έχει μήκος 2 byte. Αυτές οι διευθύνσεις αντιστοιχούν σε συσκευές του δικτύου. Όταν αυτά τα πεδία (fields) Source Route είναι παρόντα, τότε το πακέτο δρομολογείται μέσω των συσκευών που αντιστοιχούν σε αυτές τις διευθύνσεις, μέχρι να φτάσει στον τελικό προορισμό του.

TTL

Το πεδίο TTL Counter (Μετρητής χρόνου ζωής πακέτου)(Time To Live) βρίσκεται στη θέση 2 και έχει μήκος 1 byte.



Εικόνα 93. Το πεδίο TTL στο πακέτο δεδομένων NPDU

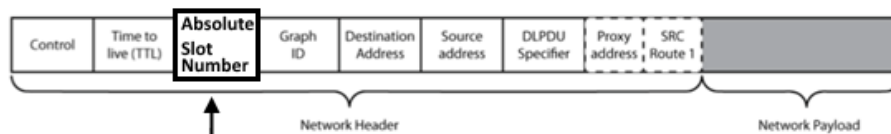
Αν μία συσκευή λάβει ένα πακέτο και η διεύθυνση προορισμού (Destination Address) του πακέτου, δεν ταυτίζεται με τη διεύθυνση της συσκευής, τότε αυτό σημαίνει ότι αυτή η συσκευή δεν ήταν τελικός προορισμός του πακέτου.

Ο μετρητής TTL Counter πρέπει να μειώσει την τιμή του κατά 1. Η τιμή που έχει ο μετρητής TTL καθορίζει αν το επίπεδο δικτύου (Network Layer) θα απορρίψει (discard) το πακέτο ή αν θα το προωθήσει (forward) μέσα στο δίκτυο. Μόλις ο μετρητής TTL φτάσει στην τιμή 0 σημαίνει ότι

έληξε ο χρόνος ζωής του πακέτου, έτσι το πακέτο απορρίπτεται και δεν προωθείται. Ο μετρητής TTL counter ελέγχει το χρόνο ζωής (Time-To-Live) του πακέτου και πρέπει να μειώνεται η τιμή του (decremented) σε κάθε άλμα (hop) που κάνει το πακέτο προς τον τελικό προορισμό του μέσα στο δίκτυο. Όταν το πακέτο ληφθεί από το επίπεδο δικτύου (Network Layer), ελέγχεται αν το TTL έχει την τιμή 0xFF. Αν έχει αυτή την τιμή το TTL, τότε δεν μειώνεται και το πακέτο προωθείται (forwarded) συνεχώς μέσα στο δίκτυο για να κινηθεί προς τον τελικό προορισμό του. Κάποια στιγμή θα φτάσει στον προορισμό του μετά από πολλά άλματα. Δηλαδή σε αυτή την περίπτωση, το TTL έχει την τιμή άπειρο (infinite).

ASN

Το πεδίο ASN Snippet έχει μήκος 2 byte.

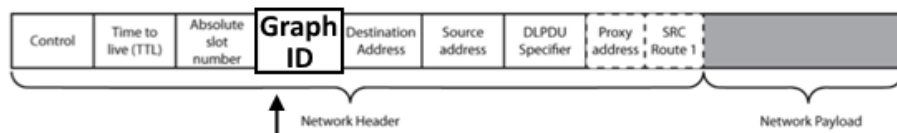


Εικόνα 94. Το πεδίο ASN στο πακέτο δεδομένων NPDU

Το πεδίο ASN Snippet field τίθεται (set) στα 16 bits που είναι τα λιγότερο σημαντικά (least significant) bits του Absolute Slot Number του δικτύου, όταν καλείται η SP εντολή TRANSMIT.request του επιπέδου δικτύου (Network Layer). Δηλαδή μια αίτηση για μετάδοση. Αυτό το πεδίο (field) παρέχει έναν δείκτη μέτρησης metric ο οποίος είναι κάπως χονδροειδής (coarse) αλλά είναι κρίσιμος για τη σωστή απόδοση σε πραγματικό χρόνο και παρέχει διαγνωστικές πληροφορίες για τη λειτουργία του δικτύου. Επίσης, όταν ο πλήρης αριθμός ASN ξαναδημιουργηθεί, παρέχει την ηλικία του πακέτου (age of the packet). Αν ο χρόνος ζωής TTL είναι έγκυρος (valid) τότε ο αριθμός ASN που αντιστοιχεί στη δημιουργία του πακέτου (packet's birthday) συγκρίνεται με τον τρέχοντα ASN για να βρεθεί η ηλικία (age) του πακέτου. Αν η ηλικία είναι μεγαλύτερη από την τιμή μέγιστης ηλικίας πακέτου maxPacketAge τότε το πακέτο απορρίπτεται (discarded). Το αποτέλεσμα αυτής της σύγκρισης πρέπει να παρέχεται ως χρόνος λήξης timeout στο επίπεδο ζεύξης δεδομένων (Data-Link).

Το πεδίο Graph ID

Το πεδίο Graph ID χρησιμοποιείται για να δρομολογηθεί (route) το πακέτο στον τελικό προορισμό του (final destination).



Εικόνα 95. Το πεδίο Graph ID στο πακέτο δεδομένων NPDU

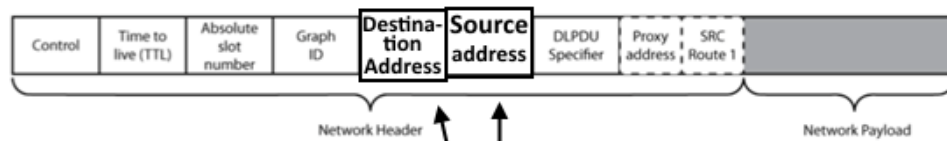
Το πεδίο Graph ID προσδιορίζει μια λίστα με κόμβους (nodes), που ο καθένας από αυτούς μπορεί να χρησιμοποιηθεί για να προωθήσει το πακέτο προς τον τελικό προορισμό.

Το πακέτο μπορεί να προωθηθεί σε οποιονδήποτε από αυτούς τους κόμβους.

Αλλιώς, αν είναι παρόντα τα προαιρετικά πεδία routing fields, τότε θα ληφθούν και αυτά υπόψη και επιπλέον το πακέτο προωθείται με βάση μία λίστα κόμβων από το Graph ID και με άλλες πληροφορίες δρομολόγησης (routing information) αν υπάρχουν. Αυτές οι πληροφορίες περιλαμβάνονται στην επικεφαλίδα (Header) του επιπέδου δικτύου (Network Layer).

Πηγή (Source) και προορισμός (Destination)

Τα πεδία διευθύνσεων Πηγής/Προορισμού (Source/Destination Addresses) υπάρχουν στα πεδία του πακέτου NPDU.



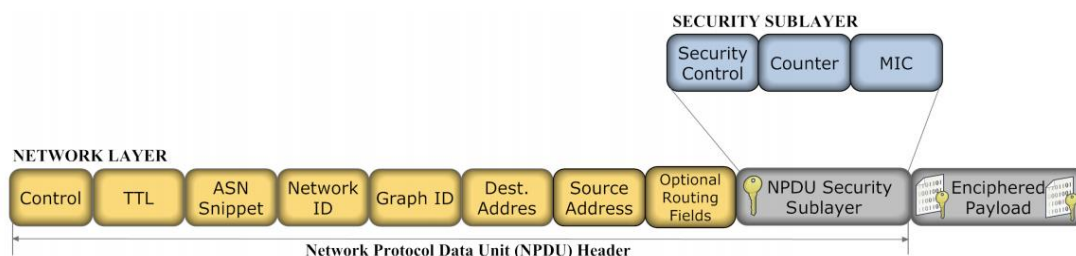
Εικόνα 96. Τα πεδία διευθύνσεων πηγής και προορισμού στο πακέτο δεδομένων NPDU.

Οι διευθύνσεις πηγής (Source Address) και προορισμού (Destination Address) έχουν η κάθε μία 2 byte αν ο τύπος της διεύθυνσης είναι nickname ή 8 byte αν ο τύπος της διεύθυνσης είναι long. Αυτές οι διευθύνσεις δεν τροποποιούνται κατά τη διάρκεια της μετάδοσης του πακέτου δεδομένων NPDU.

Η αρχική πηγή (original source) περιγράφει ποια συσκευή έστειλε αρχικά το πακέτο και ο τελικός στόχος (final destination) περιγράφει για ποια συσκευή προορίζεται.

Το υπό-επίπεδο ασφάλειας (Security Sub-Layer)

Μέσα στο επίπεδο δικτύου (network layer) υπάρχει μία επιπρόσθετη επικεφαλίδα (header) ασφαλείας που περιλαμβάνει 3 πεδία. Αυτά τα 3 πεδία βρίσκονται πριν από το πεδίο payload (που περιέχει τα πραγματικά δεδομένα που πρόκειται να μεταταδοθούν).



Εικόνα 97: Το υπο-επιπεδο ασφάλειας (Security Sublayer) περιέχεται μέσα στο πακέτο δεδομένων NPDU ως μία επικεφαλίδα με 3 πεδία. Πηγή: [26]

Αυτή η επικεφαλίδα (header) είναι ένα υπό-επίπεδο ασφαλείας (security sublayer) και χρησιμοποιείται για να περιβάλλει (encapsulate) τα δεδομένα payload τα οποία είναι κρυπτογραφημένα (enciphered).

Στην παρακάτω εικόνα φαίνεται η επικεφαλίδα (header) για το επίπεδο ασφάλειας (security layer) που υπάρχει στο πακέτο δεδομένων NPDU. Έχει σχεδιαστεί για να εξασφαλίζεται η ιδιωτικότητα στην επικοινωνία χωρίς να προκαλούνται ενοχλήσεις από ξένες ενδιάμεσες συσκευές ή από πηγές θορύβου. Επίσης επιτρέπει να γίνουν μελλοντικές βελτιώσεις στην ασφάλεια του WirelessHART.



Εικόνα 98: Η επικεφαλίδα του υπο-επιπέδου ασφάλειας (Security Sublayer) στο πακέτο δεδομένων NPDU. Πηγή: [7]

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά τα 3 πεδία του υπό-επιπέδου ασφάλειας

θέση		Μήκος σε Bytes	Όνομα/Περιγραφή

1		1	Security Control Field
2		1 ή 4	Nonce Counter
3		4	Message Integrity Code (MIC)

Πίνακας 3.17. Η επικεφαλίδα του υπό-επιπέδου ασφάλειας στο πακέτο δεδομένων NPDU.

Security Control Field

Το πρώτο πεδίο είναι 1 byte που ονομάζεται πεδίο ελέγχου ασφαλείας (Security Control Field).

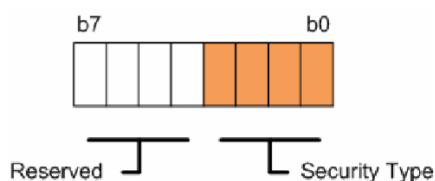


Εικόνα 99 Το 1ο byte είναι το πεδίο ελέγχου ασφαλείας (Security Control).

Όπως φαίνεται στην παρακάτω εικόνα, το byte ελέγχου ασφαλείας (security control byte) χρησιμοποιεί 4 bits (bits b3, b2, b1, b0) που σχηματίζουν μια μεταβλητή enumeration η οποία μπορεί να λαμβάνει διαφορετικές τιμές. Κάθε τιμή καθορίζει έναν τύπο ασφάλειας και δείχνει ποια στρατηγική ασφάλειας εφαρμόζεται για να κρυπτογραφηθούν (encipher) τα δεδομένα payload στο πακέτο NPDU. Επιπλέον, το byte ελέγχου ασφαλείας (security control byte) δείχνει για τον μετρητή nonce counter, αν το μέγεθος του θα είναι 1 ή 4 bytes

και εξαρτάται από το είδος κρυπτογράφησης.

Τα 4 περισσότερο σημαντικά bits (most significant bits) (bits b7, b6, b5, b4) του byte ελέγχου ασφαλείας (security control byte) είναι κρατημένα (reserved).



Εικόνα 100 Το byte ελέγχου ασφαλείας (security control byte)

Οι τύποι ασφαλείας (Security types) μπορεί να είναι:

α) session keyed, b) join keyed, c) handheld keyed.

Nonce Counter

Ο μετρητής nonce counter χρησιμοποιείται για να εκτελεστεί ο αλγόριθμος κρυπτογράφησης (encryption algorithm). Ο nonce counter ανάλογα με τον τύπο ασφαλείας που χρησιμοποιείται, μπορεί να έχει δύο μεγέθη: 1 byte όταν ο τύπος ασφαλείας είναι session keyed, ή 4 bytes αν είναι join keyed ή handheld keyed.



Εικόνα 101. Το πεδίο του μετρητή nonce counter στο πακέτο δεδομένων του υπο-επιπέδου ασφαλείας.

MIC

Το πεδίο του κώδικα MIC αναφέρθηκε προηγουμένως και για το πακέτο δεδομένων DLPDU στο στρώμα ζεύξης δεδομένων. Εδώ το πεδίο MIC αναφέρεται στο στρώμα δικτύου και στο πακέτο NPDU για το υπό-επίπεδο ασφαλείας.



Εικόνα 102. Το πεδίο MIC στο πακέτο δεδομένων του υπο-επιπέδου ασφαλείας.

Το πεδίο κώδικα ακεραιότητας μηνυμάτων MIC περιέχει μία τιμή που χρησιμοποιείται για να ελέγξει την ακεραιότητα (integrity) των δεδομένων του πλαισίου που μεταδόθηκε (transmitted frame). Αν η τιμή MIC που υπολογίζει ο δέκτης δεν ταιριάζει με την τιμή MIC που έχει τεθεί στο πακέτο τότε αυτό το πλαίσιο σημαίνει ότι έχει αλλοιωθεί, ή υπήρξε κάποιο σφάλμα στην μετάδοση. Η τιμή MIC υπολογίζεται με κάποιον αλγόριθμο που χρησιμοποιεί ένα κλειδί που γνωρίζει ο αποστολέας και ο δέκτης.

Payload

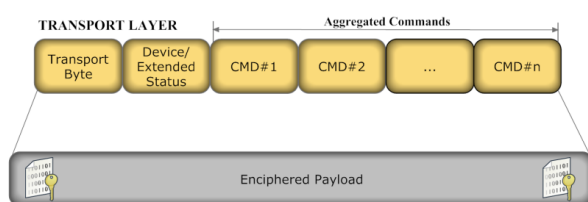
Το πεδίο με τα δεδομένα που πρέπει να μεταδοθούν είναι το Payload. Αυτά είναι κρυπτογραφημένα (enciphered) για ασφάλεια, ώστε να μην επιτρέψει σε ξένες ενδιάμεσες συσκευές (intermediate devices) την παρατήρηση των δεδομένων όταν το πακέτο δεδομένων NPDU ταξιδεύει μέσα στο δίκτυο.

Τα δεδομένα που πρόκειται να μεταδοθούν (payload) περιέχονται στο πεδίο Payload του πακέτου NPDU.

Αλλά μέσα στο ίδιο αυτό το πεδίο Payload, περιέχεται επιπλέον και ένα πακέτο TPU του στρώματος μεταφοράς (Transport Layer), που έχει μια δική του επικεφαλίδα header με επιπρόθετες πληροφορίες. Όπως θα δούμε παρακάτω, οι πληροφορίες αυτές περιλαμβάνουν κάποια πεδία όπως είναι: ένα αναγνωριστικό συναλλαγής (Transaction ID), η κατάσταση συσκευής (Device Status), η εκτενής κατάσταση συσκευής πεδίου (Extended Field Device Status), και μία ή περισσότερες εντολές (commands). αυτό το πακέτο TPU περιγράφεται παρακάτω.

3.2.15 Το πακέτο δεδομένων TPDU στο επίπεδο μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς (transport layer) έχει στόχο να εξασφαλίσει ότι τα πακέτα θα μεταδοθούν επιτυχώς στο δίκτυο με πολλαπλά άλματα (hops) για να φτάσουν στον τελικό τους προορισμό (destination). Το επίπεδο μεταφοράς (transport layer) υποστηρίζει και τις συναλλαγές με αναγνώριση (acknowledged transactions) και τις συναλλαγές χωρίς αναγνώριση (un-acknowledged transactions). Το επίπεδο μεταφοράς επίσης δείχνει την κατάσταση της συσκευής (status) και εξασφαλίζει την επιτυχή παράδοση πακέτων από άκρο σε άκρο (end-to-end)



Εικόνα 103. Το πακέτο δεδομένων TPDU στο Επίπεδο μεταφοράς (Transport Layer) περιέχεται μέσα στο πεδίο Payload του πακέτου NPDU. Πηγή: [26]

Κάθε πακέτο δεδομένων (PDU) στο επίπεδο μεταφοράς (transport layer) ονομάζεται TPDU και αποτελείται από τα παρακάτω πεδία (fields):

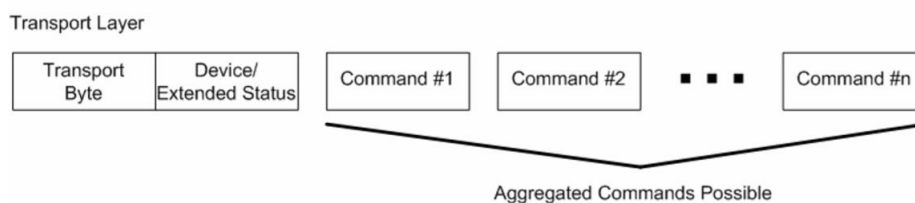
- Ένα byte μεταφοράς (transport byte) που χρησιμοποιείται για να εξασφαλίσει ότι θα γίνει η παράδοση πακέτων από σημείο σε σημείο (end-end).
- Τα bytes για την κατάσταση συσκευής (Device Status) και για την εκτενή κατάσταση συσκευής (Extended Device Status).
- Μία ή περισσότερες εντολές (commands) του πρωτοκόλλου HART.

Ο παρακάτω πίνακας δείχνει τα πεδία του πακέτου δεδομένων TPDU

Θέση	Μήκος σε Bytes	Όνομα / περιγραφή	Τμήμα πακέτου
1	1	Transport Byte	Επικεφαλίδα (header)
2	Εξαρτάται	Device/Extended Device Status	
3	Εξαρτάται	Commands	Συγκεντρωμένες εντολές

Πίνακας 3.18. Τα πεδία του πακέτου δεδομένων TPDU.

Η παρακάτω εικόνα δείχνει τη βασική δομή του πακέτου δεδομένων TPDU.



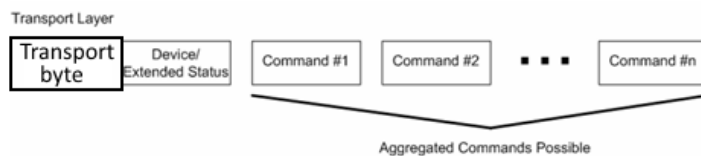
Εικόνα 104 Το πακέτο δεδομένων TPDU. Πηγή: [8].

Μία συναλλαγή (transaction) για το επίπεδο μεταφοράς (Transport Layer) μοντελοποιείται ως :

- Μία κύρια συσκευή (master) που χορηγεί ένα πακέτο μετά από αίτηση (request packet) και μία ή περισσότερες εξαρτώμενες συσκευές (slaves) που απαντούν στην κύρια συσκευή με ένα πακέτο απόκρισης (response packet) ή
- Μία εξαρτώμενη συσκευή (slave) που δημοσιεύει (publish) ένα πακέτο απόκρισης (response packet).

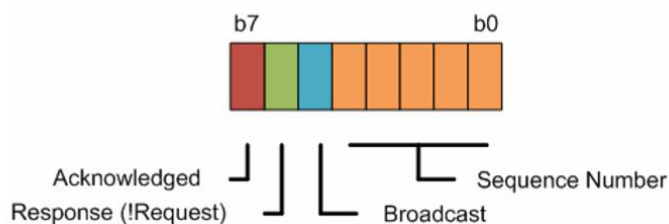
3.2.15.1 Το byte μεταφοράς (Transport Byte)

Το πρώτο byte στο πακέτο δεδομένων TPDU είναι το byte μεταφοράς (transport byte)



Εικόνα 105. το πεδίο byte μεταφοράς (transport byte) μέσα στο πακέτο TPDU

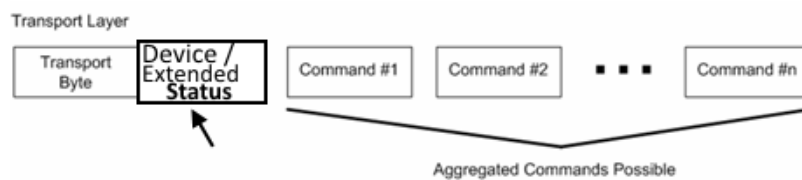
Το Transport Byte φαίνεται στην παρακάτω εικόνα.



Εικόνα 106. το byte μεταφοράς (transport byte)

3.2.15.2 Κατάσταση Συσκευής (Device Status)/Εκτενής κατάσταση (Extended Status)

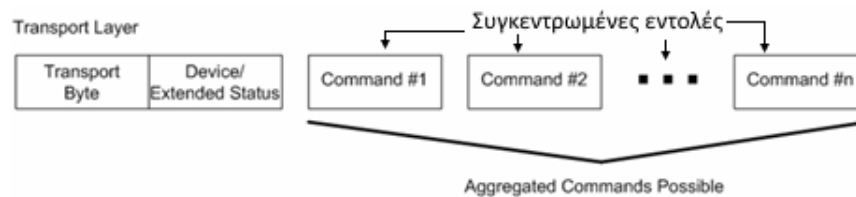
Τα bytes της κατάστασης συσκευής (Device Status) και τα bytes που έχει η εκτενής κατάσταση συσκευής (Extended Device Status) περιλαμβάνονται σε όλα τα πακέτα δεδομένων TPDU που βρίσκονται στο επίπεδο μεταφοράς.



Εικόνα 107. το πεδίο Device Status /Extended Status μέσα στο πακέτο TPDU

3.2.15.3 Συγκεντρωμένες εντολές (Aggregated Commands)

Με κάποιους περιορισμούς, το πρότυπο WirelessHART επιτρέπει σε πολλαπλές εντολές (commands) του προτύπου HART να μεταφέρονται με μία μόνο συναλλαγή (transaction).



Εικόνα 108 Οι συγκεντρωμένες εντολές μέσα στο πακέτο TPDU

Η μορφή (format) που έχουν οι εντολές (commands) που μεταφέρονται σε ένα δίκτυο WirelessHART φαίνονται στην παρακάτω εικόνα.

16-Bit Command Number	Length	Data

Εικόνα 109. Η μορφή εντολών (command format) του WirelessHART.

3.2.16 Το επίπεδο εφαρμογών (Application Layer)

Σύμφωνα με το μοντέλο OSI το επίπεδο εφαρμογών (application layer) είναι το επίπεδο (layer) που βρίσκεται πιο κοντά στον τελικό χρήστη. Παρέχει ένα μέσο για τις εφαρμογές (applications) ώστε να έχουν πρόσβαση σε πληροφορίες που υπάρχουν στο δίκτυο. Στις λειτουργίες του επιπέδου εφαρμογών περιλαμβάνονται η αναγνώριση (identify) των εταίρων που συμμετέχουν σε μία επικοινωνία, ο προσδιορισμός των διαθέσιμων πόρων στο δίκτυο και ο συγχρονισμός της επικοινωνίας. Για το δίκτυο WirelessHART, το επίπεδο εφαρμογών είναι το ίδιο με το επίπεδο

εφαρμογών του HART. Με αυτό τον τρόπο υπάρχει συμβατότητα με τις συσκευές που υποστηρίζουν το πρότυπο HART, όπως είναι υπολογιστές χειρός (handhelds), υπολογιστικά συστήματα φιλοξενίας (host systems), συστήματα διαχείρισης πόρων (asset management systems). Στο επίπεδο εφαρμογών (application layer) του WirelessHART, οι εντολές (commands) είναι τα δομικά στοιχεία (building blocks) για την επικοινωνία. Το επίπεδο εφαρμογών (application layer) του WirelessHART παρέχει υπηρεσίες στις εφαρμογές φιλοξενίας (host applications). Υπάρχουν οι δυναμικές μεταβλητές (dynamic variables) και οι μεταβλητές συσκευών (device variables), καθώς και οι 4 κλάσεις (classes) συμμόρφωσης με τη φιλοξενία (host conformance).

Το βασικό επίπεδο εφαρμογών (application layer) περιλαμβάνει:

- Τις επιτρεπτές μορφές δεδομένων (formats) που μεταδίδονται μέσω του πρωτοκόλλου.
- Κανόνες αναθεώρησης για όλες τις συσκευές πεδίου (field devices)
- Την κατανομή (allocation) των αριθμών εντολών (Commands Numbers) για να χρησιμοποιηθούν σε εντολές γενικές (Universal), κοινής πρακτικής (Common Practice), εντολές που αφορούν συγκεκριμένη συσκευή (Device-Specific), και εντολές που αφορούν οικογένεια συσκευών (Device Family).
- Τις απαιτήσεις για την κατασκευή οποιασδήποτε εντολής (command) του προτύπου HART.
- Τα bytes κατάστασης εντολών (Command Status Bytes) που απαιτούνται για να επιστραφούν μαζί με όλες τις αποκρίσεις σε εντολές (command responses).

Η κατάσταση status διακρίνεται σε τρεις τύπους που είναι η Extensive status ή standard status και η device-specific status και περιλαμβάνει την αξιολόγηση ποιότητας (quality assessment) και την κατάσταση (status) για όλες τις μεταβλητές κατάστασης (process variables).

- Τη χρήση δυναμικών μεταβλητών (Dynamic Variables) και μεταβλητών συσκευών πεδίου (Field Device Variables).
- Διαδικασίες (Procedures) που χρησιμοποιούνται από τις κύριες συσκευές (masters) για να προσδιορίζουν (identify) συσκευές πεδίου (field devices) και να διαχειρίζονται δίκτυα με το πρωτόκολλο HART.

Αυτές οι απαιτήσεις παρέχουν τη βάση για όλες τις προδιαγραφές HART στο επίπεδο εφαρμογών (application Layer).

3.2.16.1 Η διεπαφή του επιπέδου εφαρμογών (Application Layer Interface)

Το επίπεδο εφαρμογών (Application Layer) βασίζεται σε εντολές. Επομένως το σύνολο εντολών (commands) που προέρχονται είτε από τις κύριες συσκευές (master devices) είτε από τις εξαρτώμενες συσκευές (slave devices) αποτελούν τη βάση για επικοινωνία με το πρωτόκολλο HART. Κάθε εντολή έχει έναν αριθμό και ο αριθμός των εντολών (command number) που ενσωματώνονται στην επικοινωνία, καθορίζει το περιεχόμενο των μηνυμάτων (messages). Ο αριθμός των εντολών (command number) χωρίζει τα σύνολα εντολών σε διαφορετικές κατηγορίες και δείχνει μια προδιαγραφή, ώστε κάθε πακέτο δεδομένων να είναι μοναδικό χωρίς ασάφειες με σταθερό μετρητή Byte (Byte Count) και να ξεχωρίζει από τα υπόλοιπα πακέτα δεδομένων.

3.2.16.2 Οι κατηγορίες βάσει του αριθμού εντολών (Command Number Partitions)

Το σύνολο των εντολών (command set) διαιρείται στις παρακάτω κατηγορίες (classes). Κάθε αριθμός εντολής αντιστοιχεί σε μία κατηγορία.

- Γενικές εντολές (Universal Commands) – είναι ένα σύνολο εντολών (commands) που πρέπει να υποστηρίζονται από όλες τις συσκευές που χρησιμοποιούν το πρωτόκολλο HART.
- Εντολές κοινής πρακτικής (Common Practice Commands) – είναι ένα σύνολο εντολών που μπορούν να εκτελεστούν από πολλά διαφορετικά είδη συσκευών. Οι εντολές κοινής πρακτικής θα πρέπει να υποστηρίζονται από τις συσκευές όποτε αυτό είναι δυνατόν.
- Μη δημόσιες (Non-public) εντολές – είναι ένα ειδικό σύνολο εντολών (commands) που προορίζονται για να χρησιμοποιηθούν μόνο σε ρυθμίσεις εργοστασιακές (factory-only) που

εκτελούνται κατά τη διάρκεια κατασκευής των συσκευών πεδίου (field device). Αυτές οι εντολές (commands) δεν πρέπει να χρησιμοποιηθούν όταν η συσκευή λειτουργεί μέσα στο πεδίο και εξυπηρετείται από το δίκτυο.

- Ασύρματες εντολές (Wireless Commands) – είναι ένα σύνολο από εντολές (commands) που υποστηρίζουν τα προϊόντα WirelessHART. Όλα τα προϊόντα που βασίζονται στο πρότυπο WirelessHART πρέπει να έχουν υλοποιημένες τις ασύρματες εντολές (Wireless Commands).
- Εντολές για την οικογένεια συσκευών (Device Family Commands) – είναι ένα σύνολο από εντολές (commands) οι οποίες είναι κοινές για όλες τις συσκευές και επιτρέπουν να γίνεται ρύθμιση και παραμετροποίηση στις συσκευές πεδίου (field devices), δηλαδή δεν είναι οι εξειδικευμένες εντολές που προορίζονται μόνο για συγκεκριμένες συσκευές ούτε τα ειδικά προγράμματα οδήγησης (drivers) που αφορούν μόνο ορισμένες συσκευές.
- Εντολές που αφορούν μόνο συγκεκριμένες συσκευές (Device-Specific Commands) – Είναι εντολές (Commands) που καθορίζονται από τον κατασκευαστή σύμφωνα με τις απαιτήσεις για συγκεκριμένη συσκευή πεδίου (field device).

Αρ. Εντολής(Command No.)	Τύπος εντολής	Περιγραφή εντολής
0-30, 38, 48	Γενική (Universal)	Γενική εντολή. Από την προδιαγραφή γενικών εντολών.
31	Expansion Flag	Δίνει το σήμα ότι υπάρχει μια εντολή 16-bit στο πεδίο δεδομένων (data field) της εντολής. Από την προδιαγραφή διαχείρισης δικτύου.
21-121 (εκτός των 38 και 48)	Κοινής πρακτικής (Common Practice)	Εντολή κοινής πρακτικής. Από την προδιαγραφή εντολών κοινής πρακτικής

122-126	Μη δημόσιες (Non-Public)	Προορίζονται για χρήση εργοστασιακή μόνο κατά την κατασκευή της συσκευής πεδίου (field device)
127	Κρατημένη (Reserved)	-
128-253	Εντολές για συγκεκριμένες συσκευές (Device-Specific)	Εξειδικευμένες εντολές που αφορούν μόνο συγκεκριμένες συσκευές, όπως ορίζει ο κατασκευαστής τους και περιγράφονται στο εγχειρίδιο της αντίστοιχης συσκευής στην οποία αναφέρονται.
254-511	Κρατημένη (Reserved)	-
512-767	Επιπρόσθετες κοινής πρακτικής (Additional Common Practice)	Εντολές κοινής πρακτικής. Από την προδιαγραφή εντολών κοινής πρακτικής
768-1023	Εντολές WirelessHART	Εντολές από την προδιαγραφή εντολών WirelessHART
1024-33791	Εντολές για οικογένεια συσκευών (Device Family)	Εντολές από την προδιαγραφή εντολών για οικογένεια συσκευών.
33792-64511	Κρατημένες (Reserved)	-
64512-64763	Εντολές για συγκεκριμένες ασύρματες συσκευές (Wireless Device Specific)	Αυτοί οι αριθμοί εντολών είναι κρατημένοι (reserved) για να χρησιμοποιηθούν από συγκεκριμένες εντολές κατασκευαστών ασύρματων συσκευών
64766-64767	Κρατημένες (Reserved)	-
64768-65021	Επιπρόσθετες εντολές για συγκεκριμένες συσκευές (Additional Device Specific)	Αυτές οι εντολές πρέπει να χρησιμοποιούνται μόνο όταν οι αριθμοί εντολών (command numbers) που είναι εντολές 128-253 για συγκεκριμένες συσκευές έχουν καταληφθεί από συσκευή (device).

65022-65535	Κρατημένες (Reserved)	-

Πίνακας 3.19 Κατηγορίες εντολών HART με βάση τον αριθμό (HART Command Number Partitions)

Οι εντολές του WirelessHART έχουν αριθμούς εντολών 768-1023. Αυτές οι εντολές (commands) χρησιμοποιούνται για να υποστηρίξουν τη διαχείριση δικτύου (network management) και τις λειτουργίες της πύλης (gateway).

Οι εντολές του WirelessHART φαίνονται στον παρακάτω πίνακα.

Κατηγορία	Αριθμός Εντολής (Command No.)	Περιγραφή
Πρόβλεψη (Provisioning)	768	Write Join Key-Εγγραφή κλειδιού Σύνδεσης
-	769	Read Join Status-Ανάγνωση κατάστασης σύνδεσης
-	770	Request Active Advertising-Αίτηση για ενεργή διαφήμιση
-	771	Force Join Mode-Εξαναγκασμένη λειτουργία σύνδεσης
-	772	Read Join Mode Configuration-Ανάγνωση ρυθμίσεων λειτουργίας σύνδεσης
-	773	Write Network ID-Εγγραφή αναγνωριστικού δικτύου
-	774	Read Network ID-ανάγνωση αναγνωριστικού δικτύου
-	775	Write Network Tag-Εγγραφή ετικέτας δικτύου
-	776	Read Network Tag-ανάγνωση ετικέτας δικτύου
-	797	Write Radio Power Output-Εγγραφή ισχύος εξόδου του ραδιοσήματος

-	798	Read Radio Power Output-ανάγνωση ισχύος εξόδου του ραδιοσήματος
-	781	Read Device Nickname Address-Ανάγνωση της σύντομης διεύθυνσης της συσκευής
-	962	Write Device Nickname Address-Εγγραφή της σύντομης διεύθυνσης της συσκευής
Διαχείριση των υπερπλασίων (Superframes) και των ζεύξεων (Links)	783	Read Superframe List-ανάγνωση της λίστας υπερπλασίων.
-	965	Write Superframe-Εγγραφή υπερπλασίου
-	966	Delete Superframe-Διαγραφή υπερπλασίου
-	806	Read Handheld Superframe-ανάγνωση υπερπλασίου συσκευής χειρός
-	807	Request Handheld Superframe Αίτηση για υπερπλασίο συσκευής χειρός
-	784	Read Link List-Ανάγνωση λίστας ζεύξεων
-	967	Write Link-Εγγραφή ζεύξης
-	968	Delete Link-Διαγραφή ζεύξης
-	786	Read Neighbor Property Flag-Ανάγνωση σημαίας του γειτονικού κόμβου
-	971	Write Neighbor Property Flag Εγγραφή σημαίας γειτονικού κόμβου
Διαχείριση διαδρομών δρομολόγησης γραφημάτων (Graph Routes) και δρομολόγησης που ξεκινά από τον κόμβο πηγή (Source Routes)	802	Read Route List-ανάγνωση της λίστας διαδρομών
-	974	Write Route –Εγγραφή διαδρομής
-	975	Delete Route–Διαγραφή διαδρομής
-	785	Read Graph List-Ανάγνωση γραφημάτων

-	969	Write Graph Edge-Εγγραφή ακμής γραφήματος
-	970	Delete Graph Edge-Διαγραφή ακμής γραφήματος
-	803	Read Source Route-Ανάγνωση της διαδρομής που ξεκινά από τον κόμβο πηγή.
-	976	Write Source Route-Εγγραφή της διαδρομής που ξεκινά από τον κόμβο πηγή
Ασφάλεια (Security)	961	Write Network Key-Εγγραφή κλειδιού δικτύου
-	782	Read Session List-Ανάγνωση λίστας συνόδων
-	963	Write Session-Εγγραφή συνόδου
-	964	Delete Session-Διαγραφή συνόδου
-	823	Request Session-Αίτηση συνόδου
-	814	Read Device List Entries-Ανάγνωση των εγγραφών στον πίνακα συσκευών
-	815	Add Device list Table Entry-Προσθήκη εγγραφής συσκευής στον πίνακα συσκευών
-	816	Delete Device list Table Entry-Διαγραφή μιας εγγραφής συσκευής από τον πίνακα συσκευών
-	821	Write Network Access Mode-Εγγραφή της λειτουργίας προσβασιμότητας του δικτύου
-	822	Read Network Access Mode-Ανάγνωση της λειτουργίας προσβασιμότητας του δικτύου
Διαχείριση Εύρους Ζώνης (Bandwidth)	799	Request Timetable-Αίτηση του πίνακα χρόνου

-	800	Read Timetable List-Ανάγνωση της λίστας πινάκων χρόνου
-	801	Delete Timetable –διαγραφή πίνακα χρόνου
-	973	Write Timetable –Εγγραφή πίνακα χρόνου
-	812	Read Packet Receive Priority-Ανάγνωση της προτεραιότητας λήψης πακέτου
-	813	Write Packet Receive Priority-Εγγραφή της προτεραιότητας λήψης πακέτου
Διαχείριση συσκευών (Device Management)	960	Disconnect Device-αποσύνδεση συσκευής
-	972	Suspend Device(s)-Προσωρινή διακοπή συσκευής
-	777	Read Wireless Device Capabilities-Ανάγνωση Δυνατοτήτων ασύρματης συσκευής
-	778	Read Battery life-Ανάγνωση της διάρκειας ζωής μπαταρίας
-	793	Write UTC Time Mapping
-	794	Read UTC Time Mapping
Διατήρηση του δικτύου (Network Maintenance)	795	Write Time Interval-Εγγραφή σταθεράς χρόνου
-	796	Read Time Interval-Ανάγνωση σταθεράς χρόνου
-	808	Read Packet Time-To-Live-Ανάγνωση επιτρεπτού χρόνου ζωής του πακέτου
-	809	Write Packet Time-To-Live-Εγγραφή επιτρεπτού χρόνου ζωής του πακέτου
-	810	Read Join Priority-Ανάγνωση προτεραιότητας σύνδεσης
-	811	Write Join Priority-Εγγραφή προτεραιότητας σύνδεσης

-	819	Read Back-Off Exponent
-	820	Write Back-Off Exponent
Συνύπαρξη (Coexistence)	804	Read CCA Mode-Ανάγνωση λειτουργίας CCA για έλεγχο καθαρότητας καναλιού.
-	805	Write CCA Mode-Εγγραφή λειτουργίας CCA για έλεγχο καθαρότητας καναλιού.
-	817	Read Channel Blacklist-Ανάγνωση μαύρης λίστας καναλιών.
-	818	Write Channel Blacklist-Εγγραφή μαύρης λίστας καναλιών.
Αναφορές (Reporting) για την ορθή λειτουργία του δικτύου (Network Health) και για την κατάσταση του δικτύου (Status)	779	Report Device Health about the devices communication statistics-Αναφορά της κατάστασης ορθής λειτουργίας της συσκευής σύμφωνα με στατιστικά επικοινωνίας των συσκευών.
-	780	Report Neighbor Health List-Αναφορά για ορθή λειτουργία των γειτονικών κόμβων που είναι στη λίστα των γειτόνων της συσκευής.
-	787	Report Neighbor Signal Levels-Αναφορά των επιπέδων ισχύος εκπομπής που έχουν οι γειτονικοί κόμβοι
-	788	Alarm "Path Down" –Συναγερμός ότι η διαδρομή είναι εκτός λειτουργίας
-	789	Alarm "Source route Failed"-Συναγερμός αποτυχίας για διαδρομή δρομολόγησης που ξεκινάει από τον κόμβο πηγή.
-	790	Alarm "Graph route Failed"-Συναγερμός αποτυχίας για διαδρομή δρομολόγησης γραφήματος
-	791	Alarm "Transport Layer Failed"-Συναγερμός αποτυχίας για το επίπεδο μεταφοράς
Εντολές πύλης (Gateway Commands)	832	Read Network Device Identity using Unique Id –Ανάγνωση ταυτότητας της

		συσκευής δικτύου με ένα μοναδικό αναγνωριστικό
-	833	Read Network Device's Neighbor Health- Ανάγνωση της ορθής λειτουργίας της γειτονικής συσκευής
-	834	Read Network Topology Information- Ανάγνωση των πληροφοριών για την τοπολογία του δικτύου
-	835	Read Burst Message List- Ανάγνωση των μηνυμάτων με μορφή Burst
-	836	Flush Cached Responses for a Device- Διαγραφή των αποκρίσεων που παρέμειναν στην κρυφή μνήμη Cache της συσκευής
-	837	Write Update Notification Bit Mask for a Device
-	838	Read Update Notification Bit Mask for a Device
-	839	Change Notification- Ειδοποίηση Αλλαγής
	840	Read Network Device's Statistics- Ανάγνωση στατιστικών της συσκευής του δικτύου.
	841	Read Network Device Identity using Nickname -Ανάγνωση της ταυτότητας συσκευής του δικτύου με χρήση της σύντομης διεύθυνσης
	842	Write Network Device's Scheduling Flags-Εγγραφή των σημαιών χρονοπρογραμματισμού για τη συσκευή
	843	Read Network Device's Scheduling Flags- Ανάγνωση των σημαιών χρονοπρογραμματισμού για τη συσκευή
	844	Read Network Constraints-Ανάγνωση σταθερών ορίων δικτύου

	845	Write Network Constraints-Εγγραφή σταθερών ορίων δικτύου

Πίνακας 3.20. Εντολές WirelessHART με βάση τον αριθμό εντολής. Πηγή: [8].

3.2.16.3 Απαιτήσεις για τις εντολές (Commands)

- Οι εντολές (commands) στο πρωτόκολλο HART πρέπει να σχεδιάζονται έτσι ώστε να είναι αυτόνομες. Επιτρέπουν λειτουργία χωρίς κατάσταση (stateless operation) στο στρώμα εφαρμογών (application layer) της συσκευής (device).
- Μια εντολή του HART πρέπει να εκτελεί μόνο μία από τις 3 λειτουργίες Ανάγνωση (Read), Εγγραφή (Write), Εντολή (Command).
- Μια εντολή (Command) μπορεί να περιέχει δείκτες (indices) που επιτρέπουν την πρόσβαση σε πίνακες (arrays) ή πίνακες δεδομένων (tables of data) που είναι αποθηκευμένοι στην συσκευή πεδίου (field device).
- Οι εντολές (commands) που είναι για πολλαπλές συναλλαγές (Multi-transaction) πρέπει να χρησιμοποιούνται μόνο όταν μία συσκευή εξαντλήσει όλες τις εντολές από το σύνολο εντολών που είναι ειδικές για συγκεκριμένες συσκευές (device-specific commands).

3.2.16.4 Τα 2 Bytes Κατάστασης εντολών (Command Status Bytes)

Όλα τα μηνύματα (messages) που είναι αποκρίσεις των εξαρτώμενων συσκευών (slave response) πρέπει να επιστρέφουν 2 bytes κατάστασης εντολών (Command Status bytes) στα 2 πρώτα bytes του πεδίου δεδομένων (Data field). Το πρώτο byte είναι πολυπλεγμένο (multiplexed) και περιέχει είτε την κατάσταση επικοινωνίας (communication Status) είτε τον κώδικα απόκρισης (Response Code). Το δεύτερο byte περιέχει πάντα την κατάσταση της συσκευής πεδίου (Field Device Status).

3.2.17 Δυναμικές μεταβλητές (Dynamic Variables) και μεταβλητές συσκευών (Device Variables).

Το πρωτόκολλο HART σχεδιάστηκε ώστε να υποστηρίζει την τεχνολογία έξυπνων συσκευών πεδίου (smart field device) και το ρεύμα βρόχου (Loop Current) στα 4-20mA. Οι εντολές (Commands) 1 και 2 επιστρέφουν την κύρια μεταβλητή (Primary Variable) (PV), το ρεύμα βρόχου (Loop Current), και το ποσοστό Percent Range. Η εντολή (Command) 3 προσθέτει σε αυτά επιπλέον τις 3 μεταβλητές : Δευτερεύουσα μεταβλητή (Secondary Variable)(SV), Τρίτη μεταβλητή (Tertiary Variable) (TV), και Τέταρτη μεταβλητή (Quaternary Variable) (QV). Όλες οι παραπάνω μεταβλητές συλλογικά ονομάζονται δυναμικές μεταβλητές (Dynamic Variables). Η εντολή (Command) 9 επιτρέπει να επιστραφούν μέχρι 8 ψηφιακές τιμές (digital values). Η εντολή 9 επίσης περιέχει πληροφορίες για την κατάσταση (status) και μία χρονοσήμανση (timestamp) που δείχνει πότε λήφθηκαν αυτές οι μετρήσεις.

Επιπλέον το πρωτόκολλο υποστηρίζει τις μεταβλητές των συσκευών (Device Variables) που χρησιμοποιούνται στις πιο περίπλοκες συσκευές πεδίου (smart field devices) και σε συσκευές πεδίου πολλαπλών μεταβλητών (multi-variable).

Οι συσκευές πεδίου πολλαπλών μεταβλητών (multivariable) μπορούν να ρυθμίζουν ποια μεταβλητή συσκευής (Device Variable) θα συνδεθεί στο βρόχο ρεύματος (current loop).

Οι Κλάσεις συμμόρφωσης του φιλοξενητή (Host Conformance Classifications).

Κάθε κλάση συμμόρφωσης φιλοξενητή δείχνει ποιες λειτουργίες μπορεί ο φιλοξενητής (host) να παρέχει σε μία εφαρμογή. Η εφαρμογή διεκδικεί από τον φιλοξενητή ορισμένες λειτουργίες. Οι δυνατότητες που παρέχει ο φιλοξενητής σε κάθε εφαρμογή κατηγοριοποιούνται σε διαφορετικά επίπεδα. Δηλαδή κατηγοριοποιούνται σε Class 1, Class 2,... κλπ., ανάλογα με το σύνολο λειτουργιών που επιτρέπονται σε κάθε επίπεδο (level of host functionality) και τα επιτρέπει ο φιλοξενητής στις αντίστοιχες εφαρμογές. Αυτές οι λειτουργίες αφορούν το επίπεδο πρόσβασης στα δεδομένα (data access) και τον χειρισμό που παρέχει ο φιλοξενητής (host). Αυτές οι λειτουργίες περιλαμβάνουν αναφορές στις εντολές κοινής πρακτικής (Common Practice Commands) και τις εντολές οικογένειας συσκευών (Device Family Commands). Κάθε κατηγορία ή κλάση συμμόρφωσης (conformance class) περιλαμβάνει και τις λειτουργίες όλων των άλλων

κλάσεων που είναι στα χαμηλότερα επίπεδα. Η Class 1 είναι η ελάχιστη κατηγορία (minimum classification) που μπορούν να την διεκδικήσουν όλες οι εφαρμογές φιλοξενητή (host application).

Στον παρακάτω πίνακα φαίνονται όλες οι κλάσεις.

Πίνακας

Κλάσεις Συμμόρφωσης προς τον φιλοξενητή (Host Conformance Classes).

Κλάση (Class)	Περιγραφή
0	Ο φιλοξενητής (host) δεν πληροί τις ελάχιστες απαιτήσεις της κλάσης συμμόρφωσης (Conformance Class 1).
1	Ο φιλοξενητής (host) μπορεί να χρησιμοποιήσει κυκλικά δεδομένα διεργασιών (cyclical process data) από οποιαδήποτε συσκευή πεδίου (field device).
2	Ο φιλοξενητής (host) μπορεί να φέρει στο χρήστη βασικά δεδομένα ταυτοποίησης (identification) και δεδομένα ρυθμίσεων (configuration data) σχετικά με οποιαδήποτε συσκευή πεδίου (field device).
3	Ο φιλοξενητής (host) μπορεί να εκτελέσει βασικές ρυθμίσεις (configuration) για οποιαδήποτε συσκευή (device). Το ελάχιστο επίπεδο που απαιτείται για να ταξινομηθεί ως Γενικός Φιλοξενητής ("Generic Host").
4	Ο φιλοξενητής (host) παρέχει βασική υποστήριξη για ενεργοποίηση (commissioning) και βαθμονόμηση (calibration) για οποιαδήποτε συσκευή (device).
5	Ο φιλοξενητής (host) έχει ικανότητα για πρόσβαση σε όλα τα δεδομένα της συσκευής πεδίου (field device) και σε όλες τις ειδικές εντολές που αφορούν τη συσκευή (device-specific commands) για κάθε συσκευή του πεδίου (field device).

Πίνακας 3.21. Κλάσεις συμμόρφωσης φιλοξενητή. Πηγή: [8].

3.3 Το πρωτόκολλο GinMAC

Το GinMAC είναι ένα πρωτόκολλο για το επίπεδο MAC (στρώμα ελέγχου πρόσβασης μέσου, medium access control).

Το GinMAC χρησιμοποιεί πολυπλεξία με διαίρεση χρόνου Time Division Multiple Access (TDMA), βασίζεται σε δομή δέντρου (tree) και προτάθηκε για το έργο GINSENG. Το GINSENG είναι ευρωπαϊκό έργο (EU project) που είχε στόχο την σχεδίαση ενός ασύρματου δικτύου επενεργητών αισθητήρων ελεγχόμενης απόδοσης Wireless Sensor Actuator Network (WSAN). [27] Ένα ασύρματο δίκτυο επενεργητών αισθητήρων (WSAN) αποτελείται από διάφορες ετερογενείς συσκευές που είναι αισθητήρες (sensors) και επενεργητές (actuators). Είναι υπολογιστικές συσκευές χαμηλού κόστους, χαμηλής κατανάλωσης ισχύος με ασύρματη σύνδεση δεδομένων (radio modems). Συνδέονται με ασύρματες ζεύξεις δεδομένων (wireless links), αλλά συχνά και με ενσύρματες ζεύξεις. Αυτές οι συσκευές, όταν χρησιμοποιούνται για συγκεκριμένη βιομηχανική εφαρμογή, συντονίζονται μεταξύ τους ώστε να επιτύχουν διεργασίες ανίχνευσης σήματος (sensing) και διεργασίες ενεργοποίησης (actuation). Για παράδειγμα, αν ένας αισθητήρας ανιχνεύσει ότι η πίεση του υγρού σε μία δεξαμενή είναι πολύ μεγάλη, τότε στέλνει δεδομένα μέτρησης στον επενεργητή και ο επενεργητής μετακινεί το έμβολο μίας βαλβίδας, ώστε να επιτρέψει να φύγει μέρος του υγρού από τη δεξαμενή και να ελαττωθεί η πίεση του υγρού μέσα στη δεξαμενή.

Τα ασύρματα δίκτυα επενεργητών αισθητήρων WSANs είναι περίπλοκα συστήματα πραγματικού χρόνου που εκτελούν πολλαπλές λειτουργίες παράλληλα. Οι επενεργητές actuators μπορεί να έχουν πολλές πηγές εισόδου δεδομένων και να έχουν τροφοδοσία μέσω καλωδίων. Οι αισθητήρες sensors παρακολουθούν μια συγκεκριμένη περιοχή της εγκατάστασης, συλλέγουν δεδομένα και τα τροφοδοτούν στους επενεργητές (actuators) σε πραγματικό χρόνο. Τα δεδομένα μερικές φορές δεν πηγαίνουν απευθείας, από τον αισθητήρα στον επενεργητή αλλά συλλέγονται πρώτα σε μία κεντρική μονάδα που λέγεται Sink και είναι κεντρικός κόμβος του δικτύου αισθητήρων. Η κεντρική μονάδα Sink έπειτα στέλνει τα δεδομένα σε κατάλληλους επενεργητές. Ενδέχεται να γίνονται πρώτα και απαιτούμενοι υπολογισμοί.

Το πρωτόκολλο GinMAC έχει ισχυρές απαιτήσεις για αξιόπιστη και έγκαιρη παράδοση των δεδομένων. Οι εφαρμογές που υποστηρίζει το GinMAC είναι κρίσιμες ως προς το χρόνο. [28]. Οι καθυστερήσεις που επιτρέπονται είναι περιορισμένες μέσα σε αυστηρά όρια. Μία περίπτωση εφαρμογής του GinMAC υπάρχει σε διυλιστήριο πετρελαίου, που ονομάζεται GALP και βρίσκεται

στη νότια Πορτογαλία, όπου χρησιμοποιείται δίκτυο αισθητήρων και επενεργητών για την παρακολούθηση και τον έλεγχο της ροής παραγωγής.

Στο πρωτόκολλο GinMAC είναι ενσωματωμένη η λειτουργία δρομολόγησης (Routing function) με μορφή τοπολογίας δέντρου που προωθεί τα δεδομένα χωρίς διαστρωμάτωση (cross layering), [27] δηλαδή χωρίς τα στενά όρια των στρωμάτων του μοντέλου OSI των 7 στρωμάτων. Στο μοντέλο OSI, Τα 7 στρώματα διαχωρίζονται και τα δεδομένα παραμένουν αποκλειστικά μέσα στο κάθε ένα στρώμα, μετά πηγαίνουν στο επόμενο στρώμα, κ.ο.κ., μέχρι να διαπεράσουν όλη τη στοίβα στρωμάτων και έτσι δημιουργείται ένα μοντέλο καταρράκτη. Στην αρχιτεκτονική χωρίς διαστρωμάτωση (cross layering), υπάρχει μία επικοινωνία ανάμεσα στα διαφορετικά στρώματα (layers) που επιτρέπει στο ένα στρώμα να έχει πρόσβαση σε δεδομένα που ανήκουν σε άλλο στρώμα και να γίνεται μία ανταλλαγή πληροφοριών ώστε να επιτρέπεται μία αλληλεπίδραση μεταξύ των στρωμάτων.

Η τοπολογία του δικτύου βασίζεται σε δέντρο (tree). Το GinMAC επίσης δίνει μία λύση για αποτελεσματική διαχείριση της ενέργειας τροφοδοσίας (energy efficiency). Αυτό επιτυγχάνεται με τον αποτελεσματικό κύκλο λειτουργίας του (efficient duty cycling) που εισάγει αχρησιμοποίητες σχισμές (unused slots) στο πλαίσιο (frame) δεδομένων του GinMAC.

Το GinMAC θέτει αυστηρά όρια για την αξιοπιστία και για την καθυστέρηση στη μεταφορά μηνυμάτων. Επιπλέον υπάρχει και ένα πλήθος από πρόσθετες λειτουργικές μονάδες (modules) στο GINSENG οι οποίες λειτουργούν μαζί με το στρώμα MAC, στοχεύοντας σε μία ενοποίηση με το GinMAC και εγγυώνται την απόδοση του. Τέτοιες λειτουργίες είναι: ο έλεγχος τοπολογίας, η διαχείριση της ουράς και η αποσφαλμάτωση στην απόδοση.

3.3.1 Βασικά χαρακτηριστικά του GinMAC

Το πρωτόκολλο GinMAC είναι ένα πρωτόκολλο TDMA ενός μόνο καναλιού ασύρματης μετάδοσης και χρησιμοποιεί αποκλειστικές σχισμές χρόνου (slots) για μετάδοση δεδομένων. Οι γειτονικές συστοιχίες κόμβων που συνδέονται ασύρματα πρέπει να χρησιμοποιούν διαφορετικά κανάλια μετάδοσης για να υπάρχει αποφυγή των συγκρούσεων. Το πρωτόκολλο GinMAC παρέχει επιπλέον πλεονάζουσες σχισμές χρόνου (slots) για να αντισταθμίσει τις πιθανές απώλειες δεδομένων κάνοντας κάποιες επαναληπτικές μεταδώσεις. Στο GINSENG το στρώμα GinMAC

δέχεται πακέτα από τα ανώτερα στρώματα GinApp και GinSink. Τα πακέτα μπαίνουν σε μία ουρά queue και μετά εκπέμπονται από τον ασύρματο πομπό radio στην κατάλληλη χρονική στιγμή.

Το GinMAC παρέχει 4 βασικά χαρακτηριστικά με στόχο να καλύπτονται οι απαιτήσεις για αξιοπιστία. [29] Αυτά είναι:

3.3.1.1 Διαστασιολόγηση εκτός σύνδεσης (Off-line Dimensioning)

Θεωρώντας ότι είναι γνωστή και σταθερή η τοπολογία του δικτύου, στη μορφή δέντρου, γίνονται μερικοί υπολογισμοί εκ των προτέρων σχετικά με το μέγεθος του πλαισίου δεδομένων F, καθώς και για άλλες λειτουργίες.

Στην πολυπλεξία με διαίρεση χρόνου (TDMA) ο χρόνος χωρίζεται σε σχισμές χρόνου (time slots), οι σχισμές ομαδοποιούνται σε πλαίσια (frames) και γίνεται ένας χρονοπρογραμματισμός (scheduling).

Οι σχισμές χρόνου χωρίζονται σε βασικές σχισμές, επιπρόσθετες σχισμές και σε αχρησιμοποίητες σχισμές. Αυτές οι κατηγορίες παρουσιάζονται παρακάτω στην επόμενη παράγραφο για το TDMA.

Στο πρωτόκολλο GinMAC το μήκος πλαισίου (frame length) είναι σταθερό F και έχει υπολογιστεί εκ των προτέρων πριν να υλοποιηθεί το δίκτυο.

Το πρωτόκολλο επιτρέπει να υπάρχει μία επιτρεπτή καθυστέρηση (delay) σε αυστηρά περιορισμένα όρια. Αυτή η καθυστέρηση χωρίζεται σε δύο μέρη, το DS και το DA.

DS είναι η μέγιστη αποδεκτή καθυστέρηση για αποστολή δεδομένων από οποιονδήποτε αισθητήρα προς τον κεντρικό κόμβο (sink), που είναι η κεντρική μονάδα συλλογής δεδομένων.

DA είναι η μέγιστη αποδεκτή καθυστέρηση για αποστολή δεδομένων από το sink προς τους επενεργητές (actuators).

Η απαίτηση για την καθυστέρηση είναι ότι το μήκος πλαισίου F πρέπει να είναι μικρότερο από την ελάχιστη τιμή από το σύνολο τιμών DS, DA

$$F < \{DS, DA\}.$$

Όταν γίνεται διαστασιολόγηση εκτός σύνδεσης (offline dimensioning) πρέπει να ικανοποιείται αυτή η απαίτηση για την καθυστέρηση.

Το GinMAC έχει τα πλεονεκτήματα ότι μπορεί να υποστηρίξει τις επικοινωνίες πραγματικού χρόνου, να εξοικονομήσει ενέργεια για τους κόμβους, να εγγυηθεί την αξιοπιστία των επικοινωνιών σε ένα ασύρματο δίκτυο αισθητήρων. Το μειονέκτημα του είναι ότι το δίκτυο που υποστηρίζει έχει μέχρι 25 κόμβους.

3.3.2 Αποκλειστικό TDMA (Exclusive TDMA)

Αποκλειστικό, σημαίνει ότι ο κάθε κόμβος στέλνει δεδομένα πάντα στις ίδιες σχισμές χρόνου (slots) που του έχουν ανατεθεί κατά αποκλειστικότητα.

Αυτό γίνεται ώστε να μην μπορούν ταυτόχρονα να στείλουν δεδομένα δύο κόμβοι στην ίδια σχισμή χρόνου και έτσι να μην υπάρχουν συγκρούσεις.

Το GinMAC υποθέτει ότι τα δεδομένα μεταδίδονται σε ένα πλαίσιο με σχισμές χρόνου και ότι υπάρχει ένα προκαθορισμένο μέγιστο μήκος πλαισίου (maximum length) που είναι σταθερό.

Στο GinMAC καθορίζεται μια συγκεκριμένη τοπολογία (topology envelope) που έχει κάποιους περιορισμούς. Πρέπει πάντα η μέγιστη απόσταση αλμάτων (maximum hop distance) μεταξύ δύο κόμβων να είναι 3 άλματα (hops).

Ο μέγιστος αριθμός κόμβων που μπορούν να στεγαστούν σε ένα μεμονωμένο δίκτυο που το διαχειρίζεται μία κεντρική μονάδα sink πρέπει να είναι 25 κόμβοι.

Το πλαίσιο TDMA στο GinMAC περιλαμβάνει χρονικές σχισμές (time slots) που χωρίζονται σε διαφορετικές κατηγορίες. Αυτές περιγράφονται παρακάτω:

3.3.2.1 Βασικές σχισμές χρόνου (basic slots)

Οι βασικές σχισμές χρησιμοποιούνται για την κανονική μεταφορά δεδομένων (regular data transfer)

Οι βασικές σχισμές χρόνου (basic slots) είναι για την κανονική μετάδοση δεδομένων. Οι βασικές σχισμές χρησιμοποιούνται για να μεταδίδονται:

i) δεδομένα αισθητήρα (sensor data)

Τα δεδομένα αισθητήρα (sensor data) είναι δεδομένα που στέλνονται από αισθητήρες (sensors) προς την κεντρική μονάδα sink. Αυτή η ροή δεδομένων ονομάζεται ροή προς τα πάνω upstream.

ii) δεδομένα επενεργητή (actuator data),

Τα δεδομένα επενεργητή (actuator data) στέλνονται από την κεντρική μονάδα sink προς τους επενεργητές (actuators). Αυτή η ροή δεδομένων λέγεται ροή προς τα κάτω downstream.

iii) εντολές ρυθμίσεων (configuration commands)

Οι εντολές ρυθμίσεων στέλνονται σε μερικές περιπτώσεις, αν απαιτείται. Τα δεδομένα στέλνονται από το Sink προς αισθητήρες και προς επενεργητές.

3.3.2.2 Επιπρόσθετες σχισμές χρόνου (additional slots)

Οι επιπρόσθετες σχισμές (additional slots) χρησιμοποιούνται για να αυξηθεί η αξιοπιστία.

3.3.2.3 Αχρησιμοποίητες σχισμές χρόνου (unused slots)

Στο τέλος του πλαισίου υπάρχουν άλλες σχισμές (slots) που δεν είναι ούτε βασικές σχισμές (basic slots) ούτε επιπρόσθετες σχισμές (additional slots). Είναι οι αχρησιμοποίητες σχισμές (unused slots) που υπάρχουν στο πλαίσιο (frame).

Οι αχρησιμοποίητες σχισμές είναι σχισμές χρόνου που κανείς κόμβος δεν στέλνει δεδομένα. Υπάρχουν στο πλαίσιο για να επιτευχθεί ένας χαμηλός κύκλος λειτουργίας (low duty cycle) και να εξοικονομείται ενέργεια για τους κόμβους, όταν δεν χρειάζεται να στείλουν ή να λάβουν δεδομένα.

Επιπλέον, οι αχρησιμοποίητες σχισμές μπορούν να υποστηρίξουν μία δυναμική τοπολογία με περιορισμένη κινητικότητα. Πολλοί μηχανισμοί για έλεγχο της τοπολογίας έχουν προταθεί για νέους κόμβους που μπορούν να συνδεθούν στο δίκτυο υπό την προϋπόθεση ότι το πλήθος των κόμβων δεν ξεπερνά το μέγιστο αριθμό κόμβων. Το μέγιστο πλήθος κόμβων που μπορούν να συνδεθούν σε ένα sink είναι 25 κόμβοι. Αυτό είναι ένα μειονέκτημα.

3.3.2.4 Οι σχισμές χρόνου για επαναληπτικές μεταδόσεις (retransmission slots)

Στο GinMAC σε κάθε κόμβο ανατίθεται ένα σταθερό πλήθος από πλεονάζουσες διαδοχικές σχισμές χρόνου (retransmission slots), για να γίνονται επαναληπτικές μεταδόσεις δεδομένων από τον κόμβο. Αυτές επαναληπτικές μεταδόσεις (retransmissions) είναι απαραίτητο να γίνονται για να καλύπτουν τις περιπτώσεις όπου στην αρχική μετάδοση υπάρχει απώλεια δεδομένων. Το πλήθος των διαδοχικών σχισμών που ανατίθενται σε κάθε κόμβο είναι περιορισμένο διότι δεν πρέπει το συνολικό πλαίσιο να ξεπεράσει ένα μέγιστο μήκος.

Η λειτουργία αναγνώρισης (acknowledgement) ανατίθεται σε μία μεμονωμένη σχισμή χρόνου (single slot). Οι σχισμές χρόνου (slots) που χρησιμοποιούνται από έναν κόμβο για να στείλει δεδομένα είναι αποκλειστικές (exclusive) και δεν μπορούν να χρησιμοποιηθούν ξανά από άλλους κόμβους του δικτύου. Αυτό ισχύει και για τις επιπρόσθετες σχισμές (additional slots) του GinMAC.

3.3.3 Δομή δέντρου

Στο δίκτυο αισθητήρων χρησιμοποιείται η δομή δέντρου (tree). Στη ρίζα βρίσκεται ο κεντρικός κόμβος Sink. Κάποιοι κόμβοι έχουν κόμβους παιδιά και αυτοί με τη σειρά τους έχουν άλλους κόμβους παιδιά. Για κάθε έναν κόμβο γονέα (parent node) που έχει τους δικούς του κόμβους παιδιά (children), το GinMAC χρησιμοποιεί τις βασικές σχισμές (basic slots) για τον γονέα και τις επιπρόσθετες σχισμές (additional slots) για τα δικά του παιδιά (children).

Υπάρχουν και οι κόμβοι φύλλα (leaf nodes) που δεν έχουν παιδιά.

Τα δεδομένα αισθητήρων (Sensor data) από τους κόμβους φύλλα (leaf nodes) στέλνονται προς τα πάνω (upstream) προς τους κόμβους-γονείς.

Κάθε κόμβος που λαμβάνει τα δεδομένα αισθητήρων, τα στέλνει πάλι πιο πάνω, προς το δικό του κόμβο γονέα (parent node).

Αυτή η διαδικασία συνεχίζεται, μέχρι τα δεδομένα να φτάσουν στον κεντρικό κόμβο sink node.

Τα δεδομένα επενεργητή (actuator data) στέλνονται προς τα κάτω (downstream) από τον κεντρικό κόμβο sink με τελικό προορισμό τους τον κόμβο επενεργητή (actuator node). Η προώθηση δεδομένων γίνεται προς έναν από τους κόμβους παιδιά (children nodes), κάτω από τους οποίους βρίσκεται ο κόμβος επενεργητή (actuator node). Με τη σειρά του ο κάθε κόμβος παιδί προωθεί τα δεδομένα στους δικούς του κόμβους παιδιά που βρίσκονται πιο κοντά στον επενεργητή. Η διαδικασία συνεχίζεται μέχρι τα δεδομένα επενεργητή (actuator data) να φτάσουν στον κόμβο επενεργητή (actuator node)

που είναι ο τελικός προορισμός.

3.3.4 Προσαρμογή της καθυστέρησης (delay conform) για έλεγχο της αξιοπιστίας

Όπως αναφέρθηκε προηγουμένως, στο GinMAC υπάρχουν οι βασικές σχισμές χρόνου (basic slots) στις οποίες γίνεται η κανονική μετάδοση δεδομένων. Αλλά επειδή τα ασύρματα κανάλια (wireless channels) είναι ευαίσθητα σε εξωτερικές παρεμβολές, μπορεί να υπάρξουν προβλήματα στην μετάδοση αν χρησιμοποιηθούν μόνο οι βασικές σχισμές χρόνου (basic slots). Τότε μπορεί να μην υπάρχει αξιοπιστία, διότι δεν θα ικανοποιηθούν κάποιες απαιτήσεις. Για να αυξηθεί η αξιοπιστία (reliability), χρησιμοποιούνται οι επιπρόσθετες σχισμές (additional slots). Το πλήθος των πρόσθετων σχισμών που απαιτούνται για κάθε μία βασική σχισμή (basic slot) εξαρτάται από τις συνθήκες του καναλιού. Για να ελεγχθούν τα χαρακτηριστικά του καναλιού εκτελούνται κάποια πειράματα στην περιοχή εφαρμογής (deployment area) και υπολογίζεται η αξιοπιστία της ζεύξης (link reliability) για τη χειρότερη περίπτωση (worst-case).

Οι ζεύξεις (links) που έχουν επιτυχή ανταλλαγή δεδομένων σημειώνονται ως καλές ζεύξεις (good links). Τα δεδομένα στέλνονται είτε με μορφή πακέτων (packets) είτε με τη μορφή καταιγισμού (burst), δηλαδή συνεχόμενα.

Το πρωτόκολλο GinMAC χρησιμοποιεί 2 μεθόδους για να καθορίσει τις καλές ζεύξεις (good links). Αυτές είναι:

3.3.5 Ρυθμός λήψης πακέτων Packet Reception Rate (PRR)

Είναι ένας δείκτης που δείχνει την αξιοπιστία της ζεύξης για τη χειρότερη περίπτωση (worst-case link reliability).

Σε μία ζεύξη, κατά το πείραμα, ελέγχεται πόσες μεταδόσεις πακέτων είναι επιτυχείς και φτάνουν τα πακέτα κανονικά στον προορισμό τους. Τότε μετριέται ο ρυθμός λήψης πακέτων Packet Reception Rate (PRR) με μία τιμή P_{max} που δείχνει ότι σε ένα σύνολο από n μεταδόσεις (transmissions) τουλάχιστον οι P_{max} μεταδόσεις (transmissions) των πακέτων είναι επιτυχείς.

Αυτή μέθοδος καθορίζει ότι καλές ζεύξεις είναι εκείνες που έχουν καλύτερο ρυθμό PRR από ένα δεδομένο όριο ευαισθησίας (threshold).

Αυτός ο δείκτης μέτρησης (metric) έχει ένα μειονέκτημα. Αν και δείχνει πόσα πακέτα έφτασαν επιτυχώς, δεν μπορεί να δείξει τη θέση των απωλειών (losses) μέσα στην ακολουθία (sequence) των n μεταδόσεων (transmissions). [28].

Για παράδειγμα στο πείραμα που γίνεται για τον έλεγχο μίας ζεύξης, μερικές φορές η τιμή του P_{max} μπορεί να βρεθεί ότι είναι μεγάλη, αν συγκριθεί με το n . Αυτό μας δίνει την εντύπωση ότι η συγκεκριμένη ζεύξη (link) είναι καλής ποιότητας (good quality). Δεν πρέπει όμως να βασιστούμε σε αυτόν τον δείκτη P_{max} και να θεωρήσουμε ότι η ζεύξη είναι καλής ποιότητας, διότι όταν αντί για μετάδοση πακέτων γίνουν μεταδόσεις δεδομένων καταιγισμού (bursts) μπορεί να υπάρξουν απώλειες σε αυτά τα δεδομένα. Στην πράξη πάντοτε υπάρχουν απώλειες στα δεδομένα καταιγισμού που εμφανίζονται σαν συστοιχία απωλειών (losses cluster).

3.3.6 Σφάλματα καταιγισμού (burst errors)

Είναι ένας άλλος δείκτης για την αξιοπιστία ζεύξης για τη χειρότερη περίπτωση (worst-case link reliability). Θεωρείται καλύτερος δείκτης από τον PRR γιατί προσπαθεί να βρει τις απώλειες σε δεδομένα καταιγισμού (burst), κάτι που δεν μπορεί να ανιχνεύσει ο PRR.

Η μέθοδος αυτή υπολογίζει τα σφάλματα καταιγισμού δεδομένων (burst errors) που συμβαίνουν κατά το πείραμα.

Ορίζεται η αξιοπιστία της ζεύξης για τη χειρότερη περίπτωση (worst-case link reliability) χρησιμοποιώντας 2 τιμές την B_{max} και την B_{min} .

B_{max} ονομάζεται το μέγιστο πλήθος διαδοχικών σφαλμάτων ανάμεσα σε δύο σφάλματα των δεδομένων καταιγισμού (burst errors) που μεταδίδονται.

B_{min} ονομάζεται το ελάχιστο πλήθος των διαδοχικών επιτυχών μεταδόσεων, ανάμεσα σε δύο σφάλματα των δεδομένων καταιγισμού (burst errors) που μεταδίδονται.

Αυτά τα όρια B_{max} , B_{min} μπορεί να έχουν καθοριστεί από πριν, (με αρχικούς ελέγχους και δοκιμές στο κανάλι). Μία ζεύξη καλής ποιότητας (good quality) θεωρείται αυτή που βρίσκεται μέσα στα καθορισμένα όρια, δηλαδή δεν ξεπερνά τις B_{max} εσφαλμένες μεταδόσεις και έχει τουλάχιστον B_{min} επιτυχείς μεταδόσεις ανάμεσα σε δύο σφάλματα των δεδομένων καταιγισμού (burst errors).

Ένα μειονέκτημα της μεθόδου αυτής αναφέρεται στο [28]. Το σύστημα ορίζει κάποιες αρχικές τιμές για τα B_{min} και B_{max} , μετά καθορίζει ένα αρχικό χρονικό πρόγραμμα (schedule), αλλά έπειτα δεν μπορεί να αναπροσαρμόζεται κατά τις αλλαγές τιμών των B_{min} και B_{max} στη διάρκεια του χρόνου. Η αιτία που συμβαίνει αυτό είναι η εξής:

Τα όρια B_{max} , B_{min} κατά τη διάρκεια λειτουργίας του δικτύου συχνά αλλάζουν τιμές, διότι μπορεί να εμφανιστούν προσωρινές παρεμβολές στο κανάλι, ή διάφορα εμπόδια που υποβαθμίζουν την ποιότητα της ζεύξης. Έτσι, ενώ αρχικά η ποιότητα ζεύξης είχε χαρακτηριστεί ως καλή, στη διάρκεια του χρόνου μπορεί να χαρακτηριστεί ως μέτρια, ή ως κακή. Κανονικά, θα πρέπει να γίνει μία προσαρμογή και να αλλάξει το χρονικό πρόγραμμα (schedule) της μετάδοσης, ώστε να αντιμετωπίσει τις προσωρινές αλλαγές των τιμών B_{min} , B_{max} , στη διάρκεια του χρόνου, ή εναλλακτικά, θα πρέπει να εντοπιστεί η προσωρινή πηγή παρεμβολής και να αφαιρεθεί, ώστε η ποιότητα ζεύξης να γίνει καλή και το αρχικό χρονικό πρόγραμμα (schedule) να είναι έγκυρο.

Οι κόμβοι για να μπορούν έχουν μία ακριβή ανάγνωση των τιμών B_{max} και B_{min} , θα πρέπει στους κόμβους να ανατεθεί ένας επαρκής αριθμός από διαδοχικές χρονικές σχισμές μετάδοσης (transmission slots).

Όμως η εφαρμογή απαιτεί μικρό όριο χρόνου συνολικά. Αν ανατεθούν πολλές σχισμές στους κόμβους θα ξεπεραστεί το όριο χρόνου. Επομένως το πλήθος διαδοχικών σχισμών που ανατίθεται στους κόμβους δεν είναι αρκετά μεγάλο και συνεπώς δεν είναι εφικτό να ανιχνεύονται οι αλλαγές στα όρια B_{max} , B_{min} από τους κόμβους. Αυτό είναι το μειονέκτημα της μεθόδου αυτής.

3.4 ISA 100.11a Γενικά

Έχουν αναπτυχθεί διάφορα πρωτόκολλα για τα ασύρματα δίκτυα αισθητήρων.

Τα πρωτόκολλα αυτά, όπως αναφέρθηκε, αφορούν τις έξυπνες συσκευές σε μία βιομηχανική εγκατάσταση που περιλαμβάνουν προχωρημένα διαγνωστικά εργαλεία τα οποία μπορούν να διαγνώσουν την «υγεία» της συσκευής και την «υγεία» της διεργασίας με την οποία συνδέεται η συσκευή.

Επιπλέον, ένα όφελος της ασύρματης τεχνολογίας είναι η μείωση του κόστους της εγκατάστασης.

Το πρωτόκολλο WirelessHART είναι ένα διεθνές πρωτόκολλο. Στην Αμερική έχει επικρατήσει ένα άλλο αντίστοιχο πρωτόκολλο, το ISA 100.11a.

Ιδανικός στόχος για την βιομηχανία θα ήταν να σχεδιαστεί και να καθιερωθεί ένα γενικό πρότυπο (global standard) που να καλύπτει την επικοινωνία (communication) του κάθε αισθητήρα που βρίσκεται στο πεδίο, με την κεντρική αίθουσα ελέγχου (boardroom). Το πρότυπο θα πρέπει να σχεδιαστεί λαμβάνοντας υπόψη την ασφάλεια, καθώς και να καθοδηγείται από τις απαιτήσεις του τελικού χρήστη (end-user).

Αυτό το ενιαίο πρότυπο δεν είναι εύκολο να δημιουργηθεί διότι οι βιομηχανίες χωρίζονται σε δύο μεγάλες κατηγορίες που χρησιμοποιούν αντιστοίχως τα δύο διαφορετικά πρωτόκολλα: το WirelessHART και το ISA100.11a. Το WirelessHART λέγεται και IEC62591-1 και είναι ένα διεθνές πρότυπο ενώ το ISA100.11a λέγεται και ANSI/ISA100.11a-2011 και είναι αμερικάνικο πρότυπο. Τα δύο αυτά πρωτόκολλα έχουν μερικά κοινά χαρακτηριστικά, αλλά στην πραγματικότητα είναι πολύ διαφορετικά μεταξύ τους. [30].

Μερικές ομοιότητες τους είναι ότι και τα δύο πρωτόκολλα για την ασύρματη επικοινωνία χρησιμοποιούν το πρότυπο IEEE 802.15.4 με DSSS και λειτουργούν στα 2.4GHz που ανήκουν στην ασύρματη ζώνη συχνοτήτων ISM.

Και τα δύο πρότυπα παρέχουν πλήρη περιγραφή για τις ιεραρχίες στρωμάτων σε στοίβες (communication stacks) σύμφωνα με το μοντέλο OSI-7.

Παρόλο που τα δύο πρότυπα έχουν πολλές ομοιότητες, έχουν και πολλές διαφορές.

Το πεδίο ενδιαφέροντος (scope) του ISA100.11a είναι ευρύτερο από το πεδίο ενδιαφέροντος του WirelessHART. Διότι –ενώ το WirelessHART εστιάζει στην παρακολούθηση οργάνων μέτρησης πεδίου (field instruments) που έχουν δυνατότητες HART, το ISA100.11a παρέχει ένα πεδίο ενδιαφέροντος (scope) που καλύπτει από τα όργανα μέτρησης πεδίου (field instruments) μέχρι την ενοποίηση στην αίθουσα ελέγχου (control room integration). [31]

Επιπλέον το ISA100.11a είναι συμβατό με άλλα διαφορετικά πρωτόκολλα όπως είναι τα FOUNDATION Fieldbus, Profibus, Modbus καθώς και με το HART, και το ISA100.11a επιτρέπει πάνω από 1000 συσκευές (devices) να συνδεθούν στο ίδιο δίκτυο, ενώ το WirelessHART επιτρέπει μόνο γύρω σε 250 συσκευές να συνδεθούν σε ένα δίκτυο. Ένα μειονέκτημα όμως του ISA100.11a είναι ότι δεν καθορίζει πλήρως κάποιες προδιαγραφές, με αποτέλεσμα, να υπάρχουν διαφορετικές υλοποιήσεις και έτσι ορισμένες συσκευές που είναι συνδεδεμένες στο ίδιο δίκτυο ενδέχεται να μην μπορούν να επικοινωνούν μεταξύ τους.

3.4.1 Περιγραφή του ISA 100.11a

Το πρότυπο ISA100.11a λέγεται αλλιώς και ANSI/ISA100.11a. Αναπτύχθηκε από την International Society of Automation (ISA).

Η ISA είναι ένας οργανισμός για αυτοματισμούς της Αμερικής, που είναι φορέας μη κερδοσκοπικός (non-profit) και αποτελείται από 20.000 επαγγελματίες αυτοματισμών (automation professionals).

Το πρότυπο ISA100.11a σχεδιάστηκε με στόχο να ενταχθεί σε μία οικογένεια προτύπων που υποστηρίζουν ένα μεγάλο σύνολο απαιτήσεων για ασύρματες τεχνολογίες σε βιομηχανικές εγκαταστάσεις, όπως είναι η αυτοματοποίηση διεργασιών (process automation), η αυτοματοποίηση του εργοστασίου και το RFID.

Ορισμένα κριτήρια σχεδιασμού για το πρότυπο ISA100.11a μεταξύ άλλων ήταν:

1. Ευελιξία.
2. Ασφάλεια.
3. Χρήση ανοικτών προτύπων.
4. Αιτιοκρατία (determinism)(Υποστήριξη TDMA, QOS).

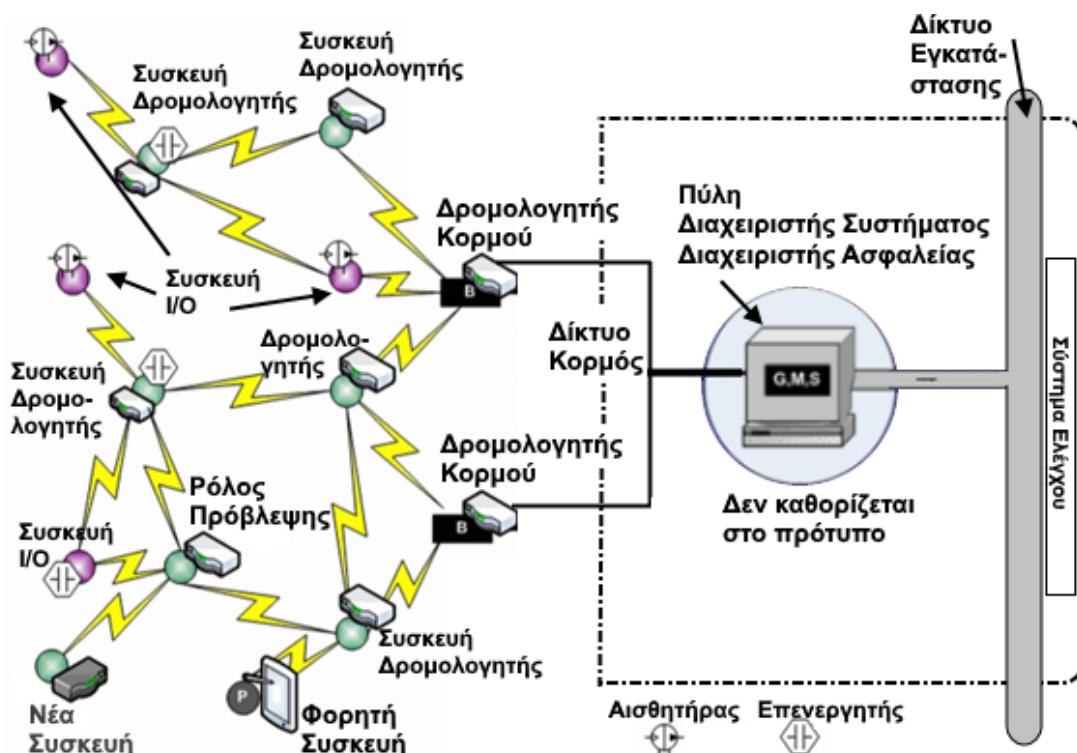
5. Υποστήριξη πολλαπλών εφαρμογών,
6. Υποστήριξη πολλαπλών πρωτοκόλλων,
7. Αξιοπιστία (ανίχνευση σφαλμάτων, μεταπήδηση συχνότητας channel-hopping)

Στο πρότυπο ISA100.11a ορίζεται η στοίβα στρωμάτων ή ιεραρχικών επιπέδων (protocol stack), οι λειτουργίες για διαχείριση συστήματος και οι λειτουργίες ασφάλειας. Προορίζεται για χρήση σε ασύρματα δίκτυα (wireless networks) που έχουν χαμηλή κατανάλωση ενέργειας (low-power), και χαμηλό ρυθμό δεδομένων (low-rate) με βάση το πρότυπο IEEE 802.15.4.

Το ISA100.11a δεν καθορίζει το στρώμα εφαρμογής (application layer) ή μία διεπαφή (interface) για σύνδεση με ένα υπάρχον πρωτόκολλο. Το μόνο που καθορίζει είναι εργαλεία (tools) για να κατασκευαστεί μία διεπαφή (interface).

3.4.1.1 Αρχιτεκτονική του ISA100.11a.

Η αρχιτεκτονική του δικτύου ISA100.11a φαίνεται στην παρακάτω εικόνα.



Εικόνα 110 Αρχιτεκτονική του ISA100.11a. Πηγή: [32]

Το δίκτυο ISA100.11a χρησιμοποιεί τους δρομολογητές κορμού (backbone routers) που είναι συσκευές που συνενώνουν ως γέφυρες (bridging) τα υποδίκτυα (subnets). Αν

χρησιμοποιηθεί ένας μόνο δρομολογητής κορμού (Backbone routers), περιορίζει την απόδοση (throughput) μέσα και έξω από ένα μεμονωμένο υποδίκτυο (single subnet) στην απόδοση (throughput) μίας μόνο ασύρματης μονάδας (one radio), αλλά οι δρομολογητές κορμού (backbone routers) μπορούν να χρησιμοποιηθούν περισσότεροι μαζί, συνδεδεμένοι σε παράλληλη σύνδεση, για να δημιουργήσουν ένα πολύ μεγάλο ασύρματο δίκτυο [33]. Επειδή οι διευθύνσεις βασίζονται στο IPv6, στην πράξη δεν υπάρχει μεγάλος περιορισμός στο πλήθος συσκευών που υποστηρίζονται σε ένα δίκτυο ISA 100.11a.

Το στρώμα δικτύου (network layer) βασίζεται στα πρότυπα 6LoWPAN και IPv6 και το στρώμα μεταφοράς (transport layer) βασίζεται στο πρότυπο UDP .

Το στρώμα ζεύξης δεδομένων (data link layer) είναι μοναδικό για το ISA100.11a και χρησιμοποιεί μία μορφή που δεν είναι συμβατή (non-compliant form) με το στρώμα ελέγχου πρόσβασης μέσου (MAC layer) του προτύπου IEEE802.15.4. Το στρώμα ζεύξης δεδομένων (data link layer) εφαρμόζει τη δρομολόγηση γραφημάτων (graph routing), τη μεταπήδηση συχνότητας (frequency-hopping) και το TDMA . Η προώθηση (forwarding) των μηνυμάτων (messages) μέσα στο ασύρματο δίκτυο (wireless network) εκτελείται στο στρώμα ζεύξης δεδομένων (data link layer) δηλαδή χρησιμοποιώντας ένα σχεδιασμό για το στρώμα ζεύξης (link-layer) που είναι mesh-under που σημαίνει ότι μπορεί να προσαρμόζει τα πακέτα που έχουν μορφή IPv6 σε μία μορφή 6LoWPAN ώστε να μπορούν να προωθούνται σε ένα δίκτυο πλέγματος. Υπάρχει μία ευελιξία στον τρόπο που καθορίζεται το επίπεδο ζεύξης δεδομένων (data link layer) στο πρότυπο ISA100.11a. Αυτή η ευελιξία προέρχεται από ένα πλήθος επιλογών όπως είναι duo-ACKs, ρυθμιζόμενο μέγεθος της χρονικής σχισμής (time slot size) και αργή μεταπήδηση συχνότητας (frequency-hopping). Επειδή δεν καθορίζονται πλήρως το μέγεθος χρονικής σχισμής (slot size) και το duo-ACKs, είναι πιθανόν να μην μπορούν να επικοινωνήσουν μεταξύ τους δύο συσκευές ISA100.11a αν έχουν διαφορετικές υλοποιήσεις.

Το ISA100.11a επιδρά στα πρωτόκολλα IPv6 και στη διευθυνσιοδότηση για δρομολόγηση (addressing for routing-over). Όλοι οι κόμβοι (nodes) που συνδέονται σε τοπολογία απλού αστέρα (star) ή σε δίκτυο πλέγματος (mesh) ονομάζονται συλλογικά «υποδίκτυο ζεύξης δεδομένων DL subnet» (data link subnet). Τα πακέτα προωθούνται

ανάμεσα σε συσκευές στο επίπεδο ζεύξης δεδομένων (data link layer) του ISA100.11a. Μέχρι ένα πακέτο να φτάσει είτε στον κόμβο προορισμού (destination node) μέσα στο DL subnet είτε στον δρομολογητή που βρίσκεται στο όριο (border router), το πακέτο δεν διερμηνεύεται (interpreted) από την προσαρμογή (adaptation) του LoWPAN και των στρωμάτων IP (IP layers). Τα μηνύματα (messages) προωθούνται μέσα στο υποδίκτυο DL subnet διαφανώς (transparently) προς τα ανώτερα στρώματα (upper layers). Αυτό έχει ως αποτέλεσμα, το επίπεδο ζεύξης δεδομένων (data link layer) του ISA100.11a να παρέχει μία αφαιρετικότητα (abstraction) ενός δικτύου τύπου broadcast (broadcast-type network) στα υψηλότερα στρώματα (higher layers). Περισσότερα για τα στρώματα του δικτύου αναφέρονται παρακάτω, στην παράγραφο 3.4.2.

3.4.1.2 Είδη Συσκευών στο πρότυπο ISA 100.11.a

Τα είδη συσκευών του ISA 100.11.a είναι τα παρακάτω [34]:

- Field device—Routing (Συσκευές πεδίου με δυνατότητα δρομολόγησης)
- Field device—Non-Routing (Συσκευές πεδίου χωρίς δυνατότητα δρομολόγησης)
- Backbone Router (Δρομολογητής κορμού)
- Gateway (Πύλη)
- System Manager (Διαχειριστής συστήματος)
- Security Manager (Διαχειριστής ασφαλείας)

Αυτές οι κατηγορίες συσκευών έχουν μία ομοιότητα με τις κατηγορίες συσκευών του WirelessHART, αλλά το ISA 100.11.a έχει πολλές διαφορές από το WirelessHART. Το σύστημα ISA100.11a βασίζεται σε μία ευέλικτη αρχιτεκτονική. Οι συσκευές λέγονται λειτουργικές μονάδες (functional entities) που περιλαμβάνουν το hardware, το software και το firmware και

συνδυάζονται μεταξύ τους για να διαμορφωθούν διάφορες τεχνολογίες δικτύου, ανάλογα με τις απαιτήσεις της κάθε εφαρμογής. Στο ISA 100.11.a καθορίζονται οι ρόλοι των συσκευών.

3.4.1.3 Δύο είδη δικτύων

Οι συσκευές πεδίου (Field Devices) δημιουργούν τα ασύρματα πακέτα wireless packets που ονομάζονται DLL subnets. [34].

Δύο είδη τοπολογιών δικτύου υποστηρίζονται στο ISA 100.11a:

α) Το δίκτυο χωρίς κεντρικό κορμό (backbone)

β) Το δίκτυο με κεντρικό κορμό (backbone).

Το δίκτυο χωρίς κεντρικό κορμό εφαρμόζεται σε εγκαταστάσεις σχετικά μικρού μεγέθους. Σε αυτό το δίκτυο, όλες οι ασύρματες συσκευές πεδίου συγκεντρώνονται μόνο σε ένα υποδίκτυο DLL subnet. Αυτό το DLL subnet επικοινωνεί απευθείας με την πύλη (Gateway) και με τον διαχειριστή δικτύου και τον διαχειριστή ασφαλείας. Τα πακέτα μεταφέρονται απευθείας και δεν παρεμβάλλεται ένα δίκτυο κορμού. Αυτή η τοπολογία έχει το πλεονέκτημα ότι ελαχιστοποιείται η καθυστέρηση (latency) στην επικοινωνία δεδομένων. Άλλο πλεονέκτημα αυτής της τοπολογίας είναι ότι επιτρέπει καλύτερη πρόβλεψη για τη συμπεριφορά του δικτύου (predictability).

Το δίκτυο με κεντρικό κορμό, αντιθέτως, εφαρμόζεται σε μεγαλύτερες εγκαταστάσεις που εκτείνονται σε μεγάλες γεωγραφικές περιοχές, όπως για παράδειγμα, όταν υπάρχουν πολλοί διασυνδεδεμένοι μεγάλοι χώροι μέσα στην εγκατάσταση. Με αυτή την τοπολογία, υπάρχουν πολλαπλά DLL subnets και όλα αυτά συνδέονται μέσω ενός δικτύου κορμού (backbone). Με αυτή την τοπολογία διευκολύνεται η επέκταση του δικτύου και σε μεγαλύτερες γεωγραφικές περιοχές και στο πλήθος των συσκευών του δικτύου.

Το κάθε ένα DLL Subnet καταλήγει στον δρομολογητή κορμού (backbone router). Ο δρομολογητής κορμού παρέχει ζεύξεις επικοινωνίας που συνδέουν τις ασύρματες συσκευές πεδίου με την υποδομή κορμού (backbone infrastructure). Έτσι τα δεδομένα για να μεταφερθούν στην πύλη (gateway) δρομολογούνται μέσω του δικτύου κορμού. Το δίκτυο του κορμού μπορεί

να είναι είτε ασύρματο είτε ενσύρματο, αλλά δεν καθορίζεται από το πρότυπο ISA 100. 11a και έτσι μπορούν να χρησιμοποιηθούν διάφορες τεχνολογίες.

3.4.1.4 Δρομολόγηση

Η δρομολόγηση (Routing) είναι συνδυασμός του mesh-under και του routing-over.

Για να αποσταλεί ένα πακέτο από μία ασύρματη συσκευή πεδίου προς την πύλη (gateway) για τη δρομολόγηση ακολουθούνται τα παρακάτω βήματα:

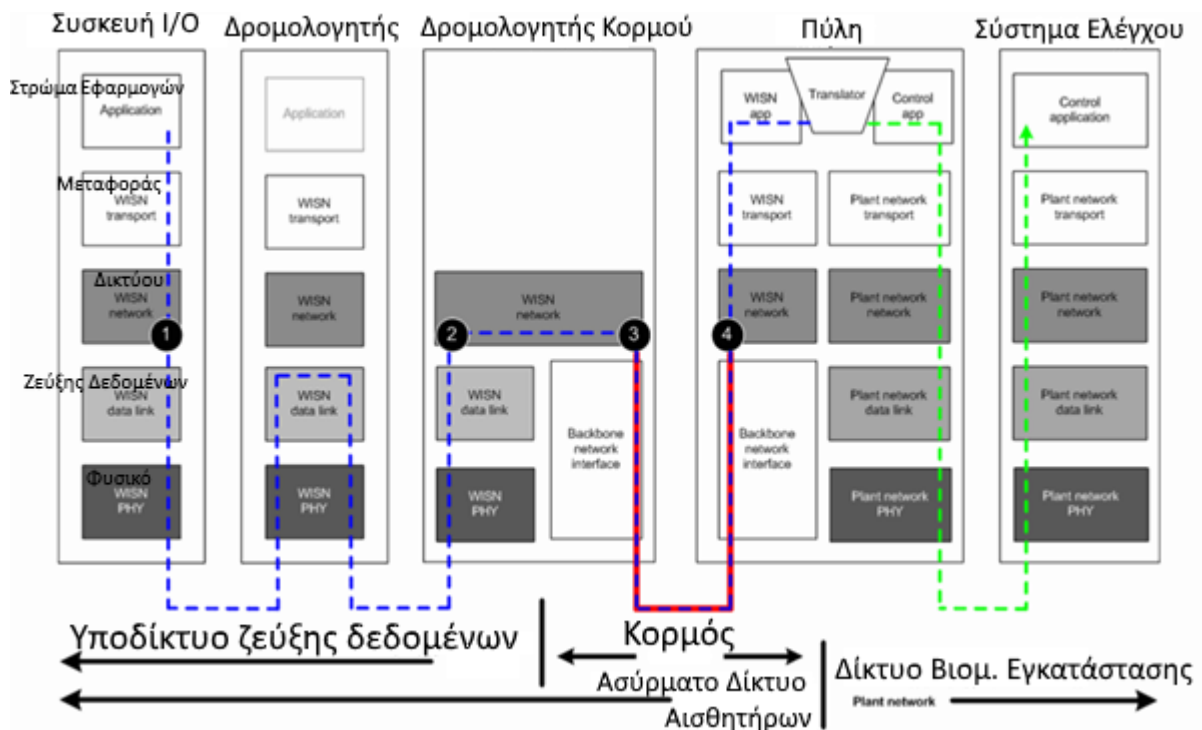
1. Το στρώμα δικτύου (network layer) της συσκευής εισόδου/εξόδου (I/O device) ως διεύθυνση πηγής (source address) δίνει τη δική της διεύθυνση 16-bit του στρώματος ζεύξης δεδομένων (data link address) και ως τελική διεύθυνση προορισμού (final destination address) δίνει την διεύθυνση 16-bit του στρώματος ζεύξης δεδομένων (data link address) της πύλης (gateway). Αν ο πίνακας συμβολαίου (contract table) δείχνει ότι το αναγνωριστικό ContractID πρέπει να περιλαμβάνεται σε ένα πακέτο, τότε χρησιμοποιείται η επικεφαλίδα contract-enabled header. Αλλιώς χρησιμοποιείται η βασική επικεφαλίδα (basic header) αν το επιτρέπει η συμπίεση (compression) που χρησιμοποιείται κατά τη μεταφορά (transport).

2. Το στρώμα ζεύξης δεδομένων (data link) στέλνει το πακέτο στο δρομολογητή κορμού (backbone router). Το στρώμα δικτύου (network layer) στο δρομολογητή κορμού (backbone router) λαμβάνει το πακέτο και αποφασίζει (determines) ότι το πακέτο δεν προορίζεται για τον δρομολογητή κορμού (backbone router), διότι η τελική διεύθυνση προορισμού (final destination address) για αυτό πακέτο είναι η διεύθυνση 16-bit του στρώματος ζεύξης (data link address) της πύλης (gateway). Ο δρομολογητής κορμού (backbone router) μεταφράζει (translates) αυτή τη διεύθυνση 16-bit του στρώματος ζεύξης (data link address) σε μία διεύθυνση 128-bit δικτύου IPv6 (IPv6 network address) που αντιστοιχεί στην πύλη (gateway) προορισμού ώστε να καθορίσει την διεύθυνση του επόμενου άλματος (next-hop address) για να φτάσει στην πύλη (gateway using) χρησιμοποιώντας έναν πίνακα δρομολόγησης (routing table) και δημιουργεί μία πλήρη επικεφαλίδα IPv6 (full IPv6 header).

3. Το πακέτο με την εκτεταμένη επικεφαλίδα δικτύου (expanded network header) παρουσιάζεται στην διεπαφή κορμού (backbone interface). Η συσκευή κορμού (backbone device) δρομολογεί (routes) το πακέτο προς τον τελικό προορισμό του (final destination). Σε αυτό το παράδειγμα, το επόμενο άλμα (next hop) είναι ο τελικός προορισμός (final destination) που είναι η πύλη (gateway).

4. Το πακέτο φτάνει στο στρώμα δικτύου IPv6 (IPv6 network layer) της πύλης (gateway) μέσω του κορμού (backbone). Το στρώμα δικτύου (network layer) στην πύλη (gateway) ορίζει ότι η διεύθυνση τελικού προορισμού (final destination address) είναι ίση με τη διεύθυνση της ίδιας της πύλης (gateway) και περνάει το πακέτο στο στρώμα μεταφοράς (transport layer).

Τότε η πύλη (gateway) ακολουθεί την διαδικασία της εφαρμογής της (its application process) και επικοινωνεί με το σύστημα ελέγχου (control system). Ανάλογα με το πρωτόκολλο που χρησιμοποιείται, αυτό το στάδιο μπορεί να περιλαμβάνει μετάφραση δεδομένων (translating data) και καταστάσεις (states).



Εικόνα 111 Δρομολόγηση (routing) σε δίκτυο ISA100.11a Πηγή: [30]

Στην παραπάνω εικόνα φαίνεται μια συσκευή εισόδου εξόδου I/O, που στέλνει δεδομένα τα οποία πρέπει να φτάσουν στο σύστημα ελέγχου. Η διαδρομή που ακολουθούν τα δεδομένα είναι η εξής: τα δεδομένα στέλνονται πρώτα σε μία συσκευή δρομολόγησης, μετά φτάνουν στο δρομολογητή κορμού, από εκεί μέσω του δικτύου κορμού (backbone) μεταφέρονται και φτάνουν στην πύλη. Από την πύλη μεταδίδονται στο κεντρικό σύστημα ελέγχου. Τα μηνύματα διαπερνούν τη στοίβα στρωμάτων κάθε συσκευής μέχρι να φτάσουν στον τελικό προορισμό. Τα είδη συσκευών αναφέρονται παραπάνω. Στην επόμενη παράγραφο ακολουθεί μία περιγραφή για τα στρώματα.

3.4.2 Στρώματα (layers) στο δίκτυο ISA100.11a

Τα στρώματα (layers) σε ένα δίκτυο ISA100.11a ακολουθούν ένα μοντέλο επικοινωνιών που βασίζεται σε μία ερμηνεία του γενικού μοντέλου OSI των 7 επιπέδων (OSI 7-layer communication model).

Η στοίβα στρωμάτων (protocol stack) του ISA100.11a περιλαμβάνει 5 επίπεδα: Φυσικό επίπεδο (physical layer)

Επίπεδο ζεύξης δεδομένων (data link layer)

Επίπεδο δικτύου (network layer)

Επίπεδο μεταφοράς (transport layer)

Επίπεδο εφαρμογής (application layer)

Επιπλέον, υπάρχει ένας κεντρικός διαχειριστής συστήματος (system manager) που είναι υπεύθυνος για τη δρομολόγηση (routing) σε όλο το δίκτυο και για το χρονοπρογραμματισμό (scheduling) της επικοινωνίας.

3.4.2.1 Φυσικό επίπεδο Physical Layer

Το φυσικό επίπεδο του ISA100.11a βασίζεται στο IEEE 802.15.4-2006 στη συχνότητα 2.4GHz και με ευθεία ακολουθία εξάπλωσης φάσματος DSSS.

3.4.2.2 Επίπεδο ζεύξης δεδομένων Data Link Layer

Το επίπεδο ζεύξης δεδομένων (data link layer) του ISA100.11a παρέχει υποστήριξη για τη δημιουργία πακέτων, τη διατήρηση των πακέτων και την προώθηση των πακέτων. Αυτές οι λειτουργίες απαιτούνται για τους ασύρματους αισθητήρες (wireless sensors). Στο μοντέλο OSI, το επίπεδο ζεύξης δεδομένων (data link layer) βρίσκεται ανάμεσα στο φυσικό επίπεδο (physical layer) και στο επίπεδο δικτύου (network layer). Δημιουργεί μία δομή πακέτων δεδομένων (data packet structure), δημιουργία πλαισίων (framing), ανίχνευση σφαλμάτων και (bus arbitration). Το επίπεδο ζεύξης δεδομένων (data link layer) περιλαμβάνει επίσης τις λειτουργίες (functions) από το επίπεδο ελέγχου πρόσβασης μέσου (medium access control) (MAC).

Στο ISA100.11a το επίπεδο ζεύξης δεδομένων (data link layer) έχει επεκταθεί ώστε να περιλαμβάνει τις παρακάτω λειτουργίες (functions):

1. Ζεύξη- τοπικές διευθύνσεις (link-local addressing)
2. Προώθηση μηνυμάτων (message forwarding)
3. Διαχείριση (management) του φυσικού επιπέδου (PHY)
4. Προσαρμοστική (adaptive) μεταπήδηση συχνότητας (channel-hopping).
5. Ελέγχους (checks) για Διευθυνσιοδότηση μηνυμάτων (message addressing), για συγχρονισμό (timing) και ελέγχους ακεραιότητας (integrity checks)
6. ανίχνευση (detection) και επανάκτηση (recovery) χαμένων μηνυμάτων (message loss)
7. Συγχρονισμό του ρολογιού (clock synchronization).

Τα μηνύματα (Messages) επικοινωνούν σε χρονικές σχισμές (time slots) Συνήθως οι συγχρονισμένες χρονικές σχισμές time-synchronized slots έχουν διάρκεια 10-millisecond, αλλά η διάρκεια τους είναι ρυθμιζόμενη. Ο συγχρονισμός (Time synchronization) παρέχει μια χρονοσήμανση με ακρίβεια (accurate time stamping), και γίνεται μία προσαρμοστική μεταπήδηση συχνότητας (adaptive channel-hopping) με αυξημένη αξιοπιστία διότι αποφεύγει τα κατειλημμένα κανάλια (occupied channels). Επιπλέον οι χρονικές σχισμές που είναι συγχρονισμένες (time synchronized slots) και η μεταπήδηση συχνότητας (channel-hopping) μειώνουν τη χρήση (utilization) για κάθε μεμονωμένο κανάλι και με αυτόν τον τρόπο βελτιώνεται για το ISA100.11a η συνύπαρξη

(coexistence) με άλλα ασύρματα δίκτυα (RF networks) που βρίσκονται στο ίδιο φάσμα (spectrum) συχνοτήτων.

Δρομολόγηση γραφημάτων

Το επίπεδο ζεύξης δεδομένων (data link layer) δημιουργεί και χρησιμοποιεί δρομολόγηση γραφημάτων (graph routing). Η δρομολόγηση γραφημάτων (Graph routing) παρέχει ένα πλήθος διαφορετικών διαδρομών δεδομένων (data paths) για διαφορετικά είδη κυκλοφορίας του δικτύου (network traffic) μέσα στο υποδίκτυο ζεύξης δεδομένων (data link subnet). Πολλαπλά γραφήματα χρησιμοποιούνται από διαφορετικές συσκευές για να μεταδώσουν (transmit) διαφορετικούς τύπους δεδομένων (types of data).

Για παράδειγμα ένας κόμβος (node) θα χρησιμοποιήσει μία διαδρομή γραφήματος (graph route) για να στέλνει περιοδικά τα δεδομένα του αισθητήρα (sensor data) στο δίκτυο της βιομηχανικής εγκατάστασης (plant network) και μία άλλη διαδρομή γραφήματος (graph route) για να στέλνει μεγάλα μπλόκ δεδομένων (large blocks of data). Ενώ όλες οι διαδρομές (routes) των γραφημάτων συνήθως συνδέονται (anchored) στο ίδιο σημείο, μέσα στο υποδίκτυο ζεύξης δεδομένων (data link subnet), η διαδρομή (path) των μηνυμάτων (messages) από οποιοδήποτε μεμονωμένο κόμβο μπορεί να διαφέρει και εξαρτάται από τον τύπο κυκλοφορίας (traffic type), το εύρος ζώνης (bandwidth) που απαιτείται και από άλλους παράγοντες. Αυτά τα διαφορετικά γραφήματα δημιουργούνται από τον διαχειριστή συστήματος (System Manager). Ο διαχειριστής συστήματος (System Manager) λαμβάνει πληροφορίες εισόδου (input) από τον σχεδιαστή (designer) του συστήματος/δικτύου (system/network) για ειδικές απαιτήσεις που υπάρχουν για το data throughput και για τις μεταδώσεις (transmissions) και λαμβάνει επίσης τις πληροφορίες που παρέχονται από τους κόμβους αισθητήρων (sensor nodes) σχετικά με το ασύρματο περιβάλλον (RF environment). Με βάση αυτές τις πληροφορίες ο διαχειριστής συστήματος (System Manager) υπολογίζει και δημιουργεί ένα σύνολο γραφημάτων και αναθέτει από ένα αναγνωριστικό contract ID σε κάθε γράφημα. Τότε οι εφαρμογές (applications) στους κόμβους αισθητήρες (sensor nodes) χρησιμοποιούν αυτά τα αναγνωριστικά contract IDs για να στείλουν ειδοποίηση στους κόμβους της διαδρομής (route) προς το δίκτυο της βιομηχανικής εγκατάστασης (plant network) για τις απαιτήσεις της μετάδοσης (transmission) και για την προώθηση (forwarding) του συγκεκριμένου μηνύματος. Τα γραφήματα υλοποιούνται (instantiated) με βάση τα συγκεκριμένα χαρακτηριστικά της κυκλοφορίας (traffic characteristics). Το ISA100.11a υποστηρίζει :

- α) Περιοδικά δεδομένα (periodic data)
- β) Δεδομένα συμβάντων (event data)
- γ) Επικοινωνίες πελάτη-διακομιστή (client-server communications)
- δ) Μεταφορές μεγάλου όγκου δεδομένων (bulk data transfers).

Ο διαχειριστής συστήματος (System Manager) χρησιμοποιεί αυτούς τους διαφορετικούς τύπους κυκλοφορίας (traffic types) μαζί με τις απαιτήσεις για την ποσότητα δεδομένων και τις απαιτήσεις για τη συχνότητα (frequency) και την καθυστέρηση (latency) για να υπολογίσει τα γραφήματα για τη συγκεκριμένη κυκλοφορία (traffic). Ο διαχειριστής συστήματος (System Manager) επίσης λαμβάνει υπόψη του την απόδοση των διάφορων καναλιών ανάμεσα σε ζεύγη κόμβων (pairs of nodes), καθώς και τους περιορισμούς στην ηλεκτρική ενέργεια τροφοδοσίας (power constraints) για κάθε κόμβο (node) από τον οποίο θα πρέπει να περάσει η κυκλοφορία (traffic). Στο τέλος των υπολογισμών τα αναγνωριστικά contract IDs ανατίθενται σε κάθε ένα από τα γραφήματα (graphs). Αυτά τα αναγνωριστικά contract IDs μεταφέρονται μέσα στην επικεφαλίδα (header) του στρώματος ζεύξης δεδομένων (data link layer) και κάθε κόμβος (node) στο γράφημα προώθησης (forwarding graph) εξετάζει το αναγνωριστικό contract ID και το αναγνωριστικό graph ID για να αποφασίσει ποιο θα είναι το επόμενο άλμα ("next hop") για το μήνυμα (message).

Με αυτό τον τρόπο, Το επίπεδο ζεύξης δεδομένων (data link layer) του ISA100.11a παρέχει μία τοπολογία δικτύου (network topology) πάνω στην οποία μπορούν να δημιουργηθούν λειτουργίες δικτύου υψηλότερων επιπέδων (higher layer network functionality). Υποστηρίζει λειτουργίες (operations) για χαμηλή κατανάλωση ενέργειας (low-power) και υψηλή διαθεσιμότητα (high-availability) ακόμα και όταν υπάρχουν τυχαίοι παρεμβολείς (non-intentional interferers) και υποστηρίζει τη μετάδοση δεδομένων (data transmission) για τους διαφορετικούς τύπους κυκλοφορίας δικτύου (network traffic) που απαιτούνται σε μία εφαρμογή (application) για έλεγχο βιομηχανικών διεργασιών ή για αυτοματισμό εργοστασίου.

3.4.2.3 Επίπεδο δικτύου (Network Layer)

Το επίπεδο δικτύου (network layer) στο πρότυπο ISA100.11a χρησιμοποιεί το 6LoWPAN. Χρησιμοποιούνται διευθύνσεις (addresses) της μορφής IPv6 για δρομολόγηση (routing) από σημείο σε σημείο (end-to-end). Σε ένα δίκτυο ISA100.11a είναι δυνατόν για τα ζευγάρια διακομιστή/πελάτη (server/client) να παράγουν πακέτα IPv6 και μετά με χρήση δρομολογητών 6LoWPAN που βρίσκονται σε άκρο (6LoWPAN edge routers) να προωθούν (forward) τα πακέτα σε συσκευές ISA100.11a που υποστηρίζουν το 6LoWPAN (6LoWPAN-enabled devices). Ο δρομολογητής που βρίσκεται σε άκρο (edge router) εκτελεί μία προσαρμογή (adaptation) από τη μορφή IPv6 σε μία μορφή 6LoWPAN που μπορεί να γίνει κατανοητή για τις συσκευές ISA100.11a devices. Το δίκτυο πλέγματος (mesh) του ISA100.11a προωθεί τα πακέτα IP στον προορισμό (destination) σύμφωνα με τις πληροφορίες δρομολόγησης (routing information) που έχουν ρυθμιστεί στην επικεφαλίδα στρώματος ζεύξης δεδομένων (DLL header). Αυτό αναφέρεται ως mesh-under. Τα πακέτα IPv6 τεμαχίζονται (fragmented) και επανασυναρμολογούνται (reassembly) στο επίπεδο προσαρμογής (adaptation layer) του 6LoWPAN. Με αυτό τον τρόπο, το ίδιο το IPv6 δεν παίζει κάποιο ρόλο στο ασύρματο δίκτυο. Είναι ενδιαφέρον το γεγονός ότι για να σταλθούν πακέτα σε ένα δίκτυο ISA100.11a απαιτείται να υπάρχει πολύ καλή γνώση των διεπαφών εφαρμογών APIs του ISA100.11a, όπως εξηγείται στο επίπεδο μεταφοράς (transport layer).

3.4.2.4 Επίπεδο μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς (transport layer) του ISA100.11a υποστηρίζει μία υπηρεσία χωρίς σύνδεση (connectionless service) που βασίζεται στο UDP και έχει ένα βελτιωμένο (enhanced) έλεγχο ακεραιότητας μηνυμάτων (message integrity check) και μία ασφάλεια από σημείο σε σημείο (end-to-end).

3.4.2.5 Επίπεδο εφαρμογών (Application Layer)

Δεν υπάρχει κάποιο στρώμα για εφαρμογές ελέγχου διεργασιών (process control application layer) που να καθορίζεται από το ISA100 για να λειτουργήσει στην στοίβα στρωμάτων (communication protocol stack). στο ISA100.11a.

Το ISA100.11a καθορίζει μόνο ένα σύνολο από υπηρεσίες για τις εφαρμογές χρήστη (user applications) και όχι μία εφαρμογή διεργασίας αυτοματισμού. Καθορίζεται μόνο η εφαρμογή διαχείρισης συστήματος (System Management application).

3.4.3 Σύγκριση των πρωτοκόλλων επικοινωνίας

Παρακάτω αναφέρονται μερικά κοινά στοιχεία και διαφορές μεταξύ των δύο προτύπων.

Στις παραγράφους που ακολουθούν, γίνεται συνοπτική περιγραφή και στους πίνακες σύγκρισεων παρουσιάζονται περισσότερα στοιχεία.

3.4.3.1 Ομοιότητες

Μερικά κοινά στοιχεία των πρωτοκόλλων είναι τα εξής:

α) Κάθε μία από τις τεχνολογίες που χρησιμοποιεί το πρότυπο IEEE 802.15.4 για ασύρματα δίκτυα προσωπικής περιοχής και χαμηλού ρυθμού (low-rate wireless personal area networks) (L-R WPAN) για να καθορίζει την ασύρματη επικοινωνία (radio). Το WirelessHART χρησιμοποιεί επίσης το IEEE802.15.4-2006 για το στρώμα MAC. Το ISA100.11a χρησιμοποιεί μία έκδοση του ίδιου MAC, που είναι τροποποιημένη και μη συμβατή (non-compliant).

β) Και τα δύο πρωτόκολλα έχουν ίδιους μηχανισμούς που διαμορφώνουν το ασύρματο δίκτυο και μεταφέρουν τα δεδομένα από και προς την πύλη (gateway).

γ) Αυτά τα δίκτυα έχουν πολύ χαμηλή κατανάλωση ηλεκτρικής ενέργειας και επιτρέπουν να χρησιμοποιούνται μπαταρίες με μεγάλη διάρκεια ζωής αντί για power taps ή ηλιακά πάνελ (solar panels) για ενέργεια τροφοδοσίας (power).

δ) Το φάσμα ζώνης συχνοτήτων που χρησιμοποιείται το κάθε ένα από τα δύο πρότυπα είναι 2.4 GHz ISM (Instrumentation, Scientific and Medical band) και δεν απαιτεί άδεια για τη χρήση του.

ε) Η ασύρματη τεχνολογία χρησιμοποιεί ένα συνδυασμό από μεταπήδηση συχνότητας (channel-hopping) και ευθεία ακολουθία εξαπλωμένου φάσματος (direct-sequence, spread spectrum) (DSSS) για να επιτευχθεί η συνύπαρξη (coexistence) με άλλους χρήστες

στο ίδιο φάσμα. Τα δίκτυα μπορεί να καταλαμβάνουν τον ίδιο φυσικό χώρο και το ίδιο φάσμα συχνοτήτων χωρίς να προκαλεί παρεμβολές το ένα δίκτυο στο άλλο.

στ) Και τα δύο πρωτόκολλα χρησιμοποιούν λειτουργίες για δρομολόγηση γραφημάτων (graph routing), δρομολόγηση πηγής (source routing), ασφάλεια και κεντρική διαχείριση του δικτύου.

Το δίκτυο ISA100.11a και το WirelessHART επιπλέον υποστηρίζουν και τα δύο:

ζ) Τοπολογίες πλέγματος (mesh), αστέρα-πλέγματος (star-mesh) και αστέρα (star). (Όμως το ISA100.11a έχει έναν περιορισμό για το πλήθος αλμάτων (hops) που μπορεί να υποστηρίξει. Απαιτούνται να υπάρχουν δρομολογητές κορμού (backbone routers)

η) Διάφορους κόμβους αισθητήρες (sensor nodes) που δεν κάνουν δρομολόγηση (non-routing). (Στο WirelessHART αυτό γίνεται με ρυθμίσεις του διαχειριστή δικτύου Network Manager)

θ) σύνδεση στο δίκτυο της βιομηχανικής εγκατάστασης (plant network) μέσω μίας πύλης (gateway).

ι) διαλειτουργικότητα (interoperability) δηλαδή ενοποιημένη συνεργασία μεταξύ συσκευών από διαφορετικούς κατασκευαστές.

ια) ενοποίηση δεδομένων (data integrity), ιδιωτικότητα (privacy), πιστοποίηση (authenticity), προστασία με επαναληπτική μετάδοση (replay protection) και προστασία από την καθυστέρηση (delay protection)

ιβ) Συνύπαρξη με άλλα ασύρματα δίκτυα.

ιγ) Ευρωστία στην παρουσία παρεμβολών (interference).

3.4.3.2 Διαφορές

Οι βασικές διαφορές του WirelessHART (IEC62591-1) από το ANSI/ISA100.11a-2011 μπορούν να φανούν άμεσα αν δούμε τη διαφορά των στόχων των δύο προτύπων. Το WirelessHART σχεδιάστηκε για να διευθετήσει τις βασικές απαιτήσεις του τελικού χρήστη (end-user) όπως είναι η αξιοπιστία, η ασφάλεια, η κατάλληλη τοποθέτηση για κάποιο σκοπό σε βιομηχανικά περιβάλλοντα, η αυστηρή διαλειτουργικότητα δηλαδή συνεργασία διαφορετικών συσκευών από άλλους κατασκευαστές, η υποστήριξη των κλάσεων εφαρμογής (Application Classes) 1 ως 5.

Το ISA100.11a σχεδιάστηκε με στόχο να παρέχει ευελιξία για τους κατασκευαστές διότι παρέχει πολλές επιλογές στην κατασκευή και επίσης πολλές επιλογές κατά τον χρόνο εκτέλεσης για να ρυθμίζεται η λειτουργία του συστήματος. Στις συσκευές ISA100.11a έχουν υλοποιηθεί επιλογές που δεν είναι συμβατές μεταξύ τους και έτσι δεν μπορούν όλες οι συσκευές να συνεργαστούν μεταξύ τους πάντα (interoperate). Αυτό μπορεί να είναι μια ευελιξία ως προς την κατασκευή αλλά ενδεχομένως να προκαλέσει σύγχυση στους τελικούς χρήστες (end users).

α) Το WirelessHART και το ISA100.11a έχουν πολλές ομοιότητες, αλλά στην αρχιτεκτονική τους διαφέρουν αρκετά. Το WirelessHART επεκτείνει το HART εισάγοντας νέους τύπους συσκευών, ενώ το ISA100.11a εισάγει την έννοια των ρόλων και επιτρέπει σε αυτούς τους ρόλους να εφαρμόζονται με διαφορετικούς συνδυασμούς [30]. Το ISA100.11a χρησιμοποιεί τους δρομολογητές κορμού (backbone routers) για να συνδέουν ως γέφυρα τα υποδίκτυα (subnets). Το WirelessHART χρησιμοποιεί τα σημεία πρόσβασης Access Points. Οι δρομολογητές κορμού (Backbone routers) περιορίζουν την απόδοση (throughput) μέσα και έξω από ένα μεμονωμένο υποδίκτυο σε μία ασύρματη μονάδα radio. Οι δρομολογητές κορμού μπορούν να χρησιμοποιηθούν παράλληλα για να δημιουργήσουν ένα πολύ μεγάλο ασύρματο δίκτυο. Οι διευθύνσεις είναι IPv6 παρέχουν πολύ μεγάλο πλήθος διευθύνσεων για τις συσκευές του δικτύου και έτσι δεν υπάρχει περιορισμός στο πλήθος των συσκευών που μπορούν να υποστηριχθούν. Το WirelessHART χρησιμοποιεί τα σημεία πρόσβασης Access Points που μπορούν να χρησιμοποιηθούν παράλληλα για να ενώσουν τα υποδίκτυα subnets σε ένα πολύ μεγάλο χώρο διευθύνσεων. Επειδή ο τύπος διεύθυνσης short address είναι ακέραιος χωρίς πρόσημο (unsigned integer), ισχύει ότι για ένα μεμονωμένο δίκτυο WirelessHART το πλήθος διευθύνσεων είναι μέχρι 30000, για αυτό υποστηρίζει μέχρι 30000 συσκευές.

Και το ISA100.11a και το WirelessHART μπορούν να συνδεθούν σε ένα καταναμημένο σύστημα ελέγχου Distributed Control System (DCS) το οποίο να συνδέεται σε πολλές πύλες Gateways.

β) Το WirelessHART χρησιμοποιεί άμεσα το πρωτόκολλο HART και απλοποιείται η υλοποίηση σημαντικά για τον τελικό χρήστη. Οι συσκευές WirelessHART ρυθμίζονται με τα διαθέσιμα εργαλεία διαχείρισης πόρων (asset management) και οι διεπαφές με τα συστήματα ελέγχου και τις εφαρμογές είναι όμοιες με το HART. Στο ISA100.11a παρέχεται ένα πλήθος επιλογών που πρέπει να καθορίζονται ή να ρυθμίζονται από τον τελικό χρήστη. Για παράδειγμα με στόχο να υπάρχει ευελιξία, το ISA100.11a δεν απαιτεί

ένα συγκεκριμένο πρωτόκολλο εφαρμογών. Αυτό όμως δημιουργεί ένα πρόβλημα στη διαλειτουργικότητα. Μέχρι να οριστεί ένα προφίλ HART για το ISA100.11a, οι χρήστες δεν μπορούν να έχουν πρόσβαση στις διαγνώσεις HART ή στις ρυθμίσεις HART και μπορούν να έχουν πρόσβαση μόνο στα δεδομένα διεργασιών με ένα μηχανισμό αντιστοίχισης (mapping) όπως είναι το Modbus που υποστηρίζεται στο PAS. Οποιοδήποτε προφίλ HART και αν σχεδιαστεί για το ISA100.11a δεν θα καταφέρει να γίνει το ίδιο αποτελεσματικό με το HART που υποστηρίζεται από το WirelessHART.

γ) Η μεταπήδηση συχνότητας στο WirelessHART που υπαγορεύεται από το πρότυπο, σχεδιάστηκε με έναν κατάλληλο τρόπο, έτσι ώστε οι συσκευές διαφορετικών κατασκευαστών να συνεργάζονται. Στο ISA100.11a έχουν καθοριστεί αρκετοί διαφορετικοί αλγόριθμοι για μεταπήδηση συχνότητας έτσι ώστε ο χρήστης να προσδιορίζει ποιος αλγόριθμος θα χρησιμοποιηθεί. Οι χρήστες που αγοράζουν μία συσκευή του ISA100.11a πρέπει μόνοι τους να ελέγξουν ότι οι μορφές μεταπήδησης συχνότητας που υποστηρίζει η συσκευή αυτή είναι συμβατές με τις μορφές μεταπήδησης συχνότητας που υποστηρίζουν άλλες συσκευές στο δίκτυο.

δ) Το WirelessHART καθορίζει ότι όλες οι συσκευές υποστηρίζουν τη δρομολόγηση, ενώ παρέχει στον τελικό χρήστη επιλογές ρυθμίσεων, ώστε αν θέλει, επιλέγει να μην χρησιμοποιηθούν οι δυνατότητες δρομολόγησης για οποιαδήποτε συγκεκριμένη συσκευή. Το ISA100.11a καθορίζει ότι η υποστήριξη δρομολόγησης από την συσκευή είναι προαιρετική και αυτό σημαίνει ότι είναι δυνατόν να δημιουργηθούν δίκτυα στα οποία οι συσκευές δεν έχουν καθόλου δυνατότητες δρομολόγησης. Αν ένα δίκτυο αποτελείται από τέτοιες συσκευές που δεν υποστηρίζουν τη δρομολόγηση τότε δεν μπορεί να προσαρμόζεται σε μεταβαλλόμενες συνθήκες και θα απαιτήσει έλεγχο της περιοχής (site surveys) για να εξασφαλιστεί ότι η τοποθέτηση της κεραίας θα είναι σωστή για ικανοποιητική ισχύ σήματος στις διαδρομές σημάτων που έχουν σχεδιαστεί. Τα δίκτυα πλέγματος (Mesh) που αποτελούνται από συσκευές που υποστηρίζουν τη δρομολόγηση, από τη φύση τους μπορούν να προσαρμόζονται σε αλλαγές και δεν απαιτούν έλεγχο της περιοχής (site surveys). Οι χρήστες του ISA100.11a πρέπει να σχεδιάσουν το δίκτυο, να επιλέξουν την τοπολογία του δικτύου, να καθορίσουν αν πρέπει να χρησιμοποιηθούν συσκευές δρομολόγησης και συσκευές που δεν υποστηρίζουν δρομολόγηση και μετά να αγοράσουν τις διάφορες συσκευές που απαιτούνται. Αυτό επίσης σημαίνει ότι για να μπορούν να γίνουν μελλοντικά επεκτάσεις και συντηρήσεις στο δίκτυο, ο τελικός χρήστης πρέπει να αγοράζει και επιπρόσθετες συσκευές, και να

αποθηκεύει διάφορα ανταλλακτικά δηλαδή συσκευές μετρήσεων που υποστηρίζουν τη δρομολόγηση ή δεν υποστηρίζουν τη δρομολόγηση, ακόμα και αν οι φυσικές μετρήσεις που λαμβάνουν είναι ίδιες. Δηλαδή, ο τελικός χρήστης θα πρέπει να αποθηκεύσει στα ανταλλακτικά, έναν πομπό για μέτρηση πίεσης, ο οποίος υποστηρίζει δρομολόγηση και να αποθηκεύσει και έναν άλλο πομπό για μέτρηση πίεσης που δεν υποστηρίζει την δρομολόγηση. Ο χρήστης πρέπει να ξέρει ποια συσκευή θα πρέπει να χρησιμοποιήσει κάθε φορά ως ανταλλακτικό. Η αγορά όμως εις διπλούν παρόμοιων συσκευών, οδηγεί και σε ένα αυξημένο κόστος για την ρύθμιση και συντήρηση του δικτύου.

ε) Το WirelessHART καθορίζει πως όλες οι επικοινωνίες πρέπει να είναι κρυπτογραφημένες. Το ISA100.11a επιτρέπει στις επικοινωνίες να μην έχουν κρυπτογράφηση. Οι χρήστες που επιθυμούν ασφάλεια πρέπει να βεβαιωθούν για τις συσκευές ISA100.11a που επιλέγουν, ότι μπορούν να υποστηρίξουν ασφαλείς επικοινωνίες και να βεβαιωθούν ότι διατηρείται η ασφάλεια.

στ) Στο WirelessHART καθορίζεται ότι οι χρονικές σχισμές slots έχουν διάρκεια 10ms. Στο ISA100.11a δεν καθορίζεται ένα σταθερό μήκος των χρονικών σχισμών slots. Οι χρήστες πρέπει να εξασφαλίσουν ότι όλες οι συσκευές ISA100.11a σε ένα συγκεκριμένο δίκτυο θα έχουν μήκος χρονικών σχισμών slots συμβατό με τις άλλες συσκευές που υπάρχουν στο ίδιο δίκτυο. Επειδή το δίκτυο ISA100.11a δεν καθορίζει παραμέτρους χρονισμού για σχισμές slots που δεν είναι 10ms, τα δίκτυα που τις χρησιμοποιούν είναι βασισμένα σε ιδιοταγή πρότυπα.

ζ) Το WirelessHART καθορίζει μόνο μία επικεφαλίδα στρώματος δικτύου (network header) χωρίς να υπάρχει διευθυνσιοδότηση IP. Το ISA100.11a καθορίζει αρκετές διαφορετικές μορφές για την επικεφαλίδα στρώματος δικτύου. Υποστηρίζει το IPv6 καθώς και αρκετές συμπιεσμένες μορφές επικεφαλίδων. Οι χρήστες πρέπει να βεβαιωθούν ότι οι συσκευές ISA100.11a σε ένα δίκτυο υποστηρίζουν συμβατές μορφές επικεφαλίδων δικτύου και είναι ρυθμισμένες κατάλληλα πριν από τη χρήση τους, ώστε να μπορούν να συνεργάζονται στο ίδιο δίκτυο. Ορισμένοι χρήστες γενικά δεν προτιμούν τις επικεφαλίδες IP headers διότι υπάρχουν ορισμένα ζητήματα ασφάλειας και κίνδυνοι για παραβίαση των διευθύνσεων IP.

η) Το WirelessHART υποστηρίζει στα μηνύματα τον κατακερματισμό και την επανασυναρμολόγηση (fragmentation/reassembly) στο στρώμα εφαρμογών (application level). Δηλαδή, μέσα σε κάθε συσκευή ή σε δρομολογητή κορμού. Οι

δρομολογητές κορμού (Backbone routers) μπορεί να συντονίζουν την επανασυναρμολόγηση των κομματιών. Αν και αυτό το χαρακτηριστικό είναι χρήσιμο, δεν έχει καθοριστεί για να υλοποιηθεί στο πρότυπο ISA100.11a. Επειδή δεν καθορίζεται πως θα επανασυναρμολογούνται τα κομμάτια (fragments) ανάμεσα στους δρομολογητές κορμού (backbone routers), το χαρακτηριστικό αυτό είναι χρήσιμο μόνο στα δίκτυα όμοιων συσκευών του ίδιου κατασκευαστή (single-sourced suppliers). Για αυτό οι χρήστες του ISA100.11a θα πρέπει να βεβαιώνονται ότι αγοράζουν συσκευές δρομολογητών κορμού (backbone router) της ίδιας μάρκας κατασκευαστή και να είναι ακριβώς του ίδιου τύπου.

θ) Το WirelessHART χρησιμοποιεί το HART στο στρώμα εφαρμογών. Το ISA100.11a δεν καθορίζει ένα στρώμα εφαρμογών ούτε καθορίζει διεπαφές για τυπικά πρωτόκολλα ελέγχου διεργασιών (process control).

ι) Το ISA100.11a ορίζει πλήρως ένα δίκτυο κορμού. Αυτό το δίκτυο κορμού (backbone) λειτουργεί καλά για μεγάλα δίκτυα. Το WirelessHART είναι συμβατό με το HART Over-IP για τη δημιουργία ενός δικτύου κορμού.

ια) Το ISA100.11a ορίζει μερικώς την μέθοδο Over the Air Provisioning (OTAP) και χρησιμοποιεί και συμμετρικά και ασύμμετρα κλειδιά. Το σύστημα OTAP λειτουργεί καλά για μεγάλα και πολύ μεγάλα δίκτυα. Το HART 7 υποστηρίζει τη λειτουργία μεταφοράς μπλοκ δεδομένων (block transfer function), αλλά δεν καθορίζει μια εφαρμογή για μεταφορά firmware μέσω ασύρματου δικτύου (over-the-air transfer firmware image application). Αυτό μένει να το υλοποιήσουν οι κατασκευαστές των συσκευών.

3.4.3.3 Συγκριτικοί πίνακες

Στον παρακάτω πίνακα φαίνεται η σύγκριση της στοίβας στρωμάτων του πρωτοκόλλου WirelessHART με τη στοίβα του πρωτοκόλλου ISA 10011a και παρουσιάζονται κάποια κοινά στοιχεία μεταξύ των δύο προτύπων.

Στρώμα	WirelessHART	ISA 100.11a
Φυσικό (PHY)	Ασύρματο, IEEE 802.15.4, 2.4 GHz, DSSS	Ασύρματο, IEEE 802.15.4, 2.4 GHz, DSSS

MAC (Medium Access Layer)	Συμβατό με το στρώμα MAC του IEEE 802.15.4-2006	Τροποποιημένο και όχι συμβατό με το στρώμα MAC του IEEE 802.15.4-2006
DLL (Data Link Layer)	Χρήση σχισμών χρόνου slots	Χρήση σχισμών χρόνου slots
	Μεταπήδηση συχνότητας καναλιών (Channel hopping)	Μεταπήδηση συχνότητας καναλιών (Channel hopping)
	Ασφαλείς Αναγνώρισεις (Secure acknowledgements)	Ασφαλείς Αναγνώρισεις (Secure acknowledgements)
	Διάδοση σήματος ρολογιού (Clock propagation)	Διάδοση σήματος ρολογιού (Clock propagation)
	Ασφάλεια: έλεγχος ακεραιότητας δεδομένων(data integrity) άλμα προς άλμα (hop-by-hop)	Ασφάλεια: έλεγχος ακεραιότητας δεδομένων(data integrity) άλμα προς άλμα (hop-by-hop) και κρυπτογράφηση.
		Δρομολόγηση γραφήματος και δρομολόγηση πηγής Σύνδεση (Joining) αργά άλματα (Slow hopping)
		Και υβριδικά αργά/γρήγορα άλματα (hybrid slow/fast hopping)
		Δύο μεγέθη σχισμών χρόνου που βασίζονται σε δύο διαφορετικές ρυθμίσεις αναγνώρισης (Acknowledgement Configuration)
		Ρητή ειδοποίηση για συκρούσεις (congestion notification)
Στρώμα Δικτύου Network Layer	Δρομολόγηση γραφήματος, δρομολόγηση πηγής. Οι διαδρομές δρομολόγησης (Graph routes) περιλαμβάνουν 1 από n σημεία πρόσβασης (Access Points) και επιτρέπονται πλεονάζουσες /πολλαπλές συνδέσεις προπρος δίκτυα κορμού (backbone networks). Και έτσι ένα μόνο δίκτυο (single network)	IETF IPv6 και 6LoWPAN κατακερματισμός (Fragmentation) και επανασυναρμολόγηση(reassembly) στο δρομολογητή κορμού (backbone router). Αν χρησιμοποιηθεί ο κατακερματισμός και η επανασυναρμολόγηση, τότε η διαδρομή γραφήματος πρέπει να τερματιστεί και να επανασυναρμολογηθούν τα μηνύματα σε έναν μόνο δρομολογητή κορμού (backbone) και έτσι να εισαχθεί μόνο ένα

		υποστηρίζει πολύ υψηλή απόδοση (throughput).	σημείο αποτυχίας (single point of failure).
		Ασφάλεια σύνδεσης: κρυπτογράφηση από σημείο σε σημείο (end-to-end encryption) και ακεραιότητα δεδομένων (data integrity)	
Στρώμα μεταφοράς Trasport Layer		Υπηρεσία Connectionless service Αξιόπιστη παράδοση με υπηρεσία αναγνώρισης (acknowledgement service)	Υπηρεσία UDP Connectionless Δηλ. κάθε πακέτο δεδομένων data unit διευθυνσιοδοτείται ατομικά και η δρομολόγηση βασίζεται σε πληροφορίες που υπάρχουν στο ίδιο το πακέτο unit, και όχι σε προκαθορισμένες πληροφορίες ενός σταθερού καναλιού δεδομένων
Στρώμα Εφαρμογών (Application Layer)	Έλεγχος διεργασιών (Process control)	HART 7	Δεν υπάρχει έλεγχος διεργασιών στο στρώμα εφαρμογών
	Διαχείριση (Management)	Διαγνώσεις Κεντρικό δίκτυο Ρύθμιση υπερπλαισίων και διαδρομών δρομολόγησης Σύνδεση στο δίκτυο	Διαγνώσεις Κεντρικό δίκτυο Ρύθμιση υπερπλαισίων και διαδρομών δρομολόγησης Σύνδεση στο δίκτυο Επιλογές για : ρύθμιση κατανεμημένου δικτύου
	Ασφάλεια	Διαχείριση Κλειδιών Keys	Διαχείριση Κλειδιών Keys
	Υποεπίπεδο στο στρώμα εφαρμογών	Δομή εντολής και απόκρισης Κωδικοποίηση δεδομένων Ασφάλεια: Κρυπτογράφηση και ακεραιότητα δεδομένων	Δομή υπηρεσιών με αντικείμενα Objects και μεθόδους methods Δομή Κωδικοποίηση δεδομένων

Πίνακας 3.22. Σύγκριση της στοίβας στρωμάτων πρωτοκόλλου WirelessHART με την στοίβα του ISA100.11a πηγή: [30]

Στον πίνακα που ακολουθεί, φαίνονται αρκετές διαφορές που υπάρχουν ανάμεσα στο πρωτόκολλο WirelessHART και στο ISA 10011a

	WirelessHART	ISA 100.11a	Σχολιασμός
Τύποι συσκευών και ρόλοι	Το WirelessHART ορίζει τύπους συσκευών	Το ISA 100.11a ορίζει ρόλους συσκευών	Στο ISA 100.11a οι συσκευές δεν υποστηρίζουν το ρόλο δρομολογητή. Έτσι στο ISA 100.11a Τα περισσότερα δίκτυα είναι σε τοπολογία αστέρα. Στο WirelessHART αντίθετα, όλες οι συσκευές πεδίου είναι και δρομολογητές και τα περισσότερα δίκτυα είναι σε τοπολογία πλέγματος (mesh).
	Συσκευή πεδίου Field device	Συσκευή Εισόδου /Εξόδου I/O	
	Σημείο πρόσβασης Access Point	Δρομολογητής router	
	Πύλη Gateway	Πρόβλεψη provisioning	
	Διαχειριστής δικτύου Network Manager	Δρομολογητής κορμού Backbone router	
	Διαχειριστής ασφάλειας Security Manager	Πύλη Gateway	
	Προσαρμογέας adapter	Διαχειριστής συστήματος System manager	
	Συσκευή χειρός Handheld	Διαχειριστής Ασφάλειας Security Manager	
		Πηγή χρόνου συστήματος System time Source	
Πρόβλεψη Provisioning	Όλες οι συσκευές πεδίου και τα σημεία πρόσβασης Access Points δέχονται αιτήματα σύνδεσης στο δίκτυο (join request) από άλλες συσκευές που θέλουν να συνδεθούν στο δίκτυο.	Το ISA100.11a καθορίζει ένα ρόλο πρόβλεψης (provisioning role) και έτσι δεν μπορούν όλες οι συσκευές πεδίου να προβλέπουν τις άλλες συσκευές που θέλουν να συνδεθούν στο δίκτυο. Μόνο όσες συσκευές έχουν ρόλο πρόβλεψης μπορούν.	Ο τρόπος που θα επιλεγθούν οι συσκευές στο ISA100.11a, θα επηρεάσει σημαντικά την τοπολογία δικτύου που θα προκύψει. Αν ο χρήστης αναγκαστεί να επιλέξει τοπολογία αστέρα, τότε θα απαιτηθεί να γίνουν site surveys δηλαδή έρευνα για ακριβή θέση, πρόσβαση και προσανατολισμό, κόμβων για να είναι σίγουρο ότι θα διαμορφωθεί το δίκτυο.
Χώρος διευθύνσεων	Στο WirelessHART περιορίζεται σε 30000 συσκευές ανά	Το ISA100.11a χρησιμοποιεί IPv6 και έχει πολύ μεγαλύτερο	Στην πράξη υπάρχει ένα όριο στο πλήθος συσκευών που

Address Space	δίκτυο WirelessHART	χώρο διευθύνσεων και αριθμό συσκευών.	υποστηρίζονται. Ανά σημείο πρόσβασης AP είναι λίγες εκατοντάδες συσκευές, ενώ ανά πύλη είναι λίγες χιλιάδες. Τα DCS μπορούν να συνδέονται σε πολλές πύλες και έτσι δεν περιορίζονται σε αριθμό συσκευών.
Επέκταση ενός μεμονωμένου δικτύου πλέγματος (mesh) με πρόσθεση σημείων choke points	Στο WirelessHART υποστηρίζονται πολλαπλά σημεία πρόσβασης AP ανά τοπικό δίκτυο. Για να αυξηθούν οι ρυθμοί δεδομένων εισόδου/εξόδου (I/O), μπορούν να προστεθούν περισσότερα access points, ενώ για μεγάλες εγκαταστάσεις μπορούν να χρησιμοποιηθούν περισσότερες πύλες	Το ISA100.11a υποστηρίζει έναν ή περισσότερους Δρομολογητές Κορμού ανά τοπικό δίκτυο. Αν σε ένα τοπικό δίκτυο ξεπεραστεί το εύρος ζώνης bandwidth μίας ασύρματης μονάδας radio, τότε προστίθενται περισσότεροι Δρομολογητές Κορμού (backbone routers).	Αυτή είναι μία σημαντική διαφορά των δύο δικτύων.
Κατακερματισμός (Fragmentation) και επανασυναρμολόγηση (Reassembly)	Το WirelessHART υποστηρίζει κατακερματισμό και επανασυναρμολόγηση στο επίπεδο εφαρμογών. Για το σκοπό αυτό, καθορίστηκε μία συγκεκριμένη λειτουργία που λέγεται μεταφορά μπλοκ δεδομένων (block data transfer)	Το ISA100.11a υποστηρίζει κατακερματισμό και επανασυναρμολόγηση στο επίπεδο δικτύου. Αυτή η ικανότητα παρέχεται από το 6LoWPAN.	Αν και το ISA100.11a υποστηρίζει κατακερματισμό και επανασυναρμολόγηση, αυτό που δεν ορίζει είναι το πώς οι πολλαπλοί δρομολογητές κορμού συντονίζουν την επανασυναρμολόγηση των πακέτων. Χωρίς αυτή τη λειτουργία ένα γράφημα πρέπει να τερματίζεται σε έναν δρομολογητή κορμού που εισάγει ένα μόνο σημείο αποτυχίας.
Πλεονασμός (Redundancy)	Το WirelessHART είναι δίκτυο πλέγματος (mesh). Όλες οι διαδρομές πρέπει να είναι πολλαπλές με βάση το σχεδιασμό του. Στο δίκτυο κορμού (backbone) μπορούν	Το ISA100.11a προαιρετικά υποστηρίζει την τοπολογία πλέγματος (mesh). Οι δρομολογητές κορμού μπορούν να σχεδιαστούν να	Η τεχνολογία DUO-CAST του ISA100.11a δεν είναι πλήρως προκαθορισμένη, αλλά έχει πολλές δυνατότητες. Υπάρχουν διάφορες υλοποιήσεις ιδιωτικές (proprietary). Και οι δύο μορφές πρέπει να λειτουργούν σωστά σε

	να χρησιμοποιούνται πολλαπλά σημεία πρόσβασης AP	υποστηρίζουν DUO-CAST.	πραγματικές εγκαταστάσεις.
Στρώμα ζεύξης δεδομένων (data link layer)	Το WirelessHART χρησιμοποιεί χρονικές σχισμές slots που διαρκούν 10 ms. Καθορίζεται ένας απλός αλγόριθμος μεταπήδησης συχνότητας. Οι κώδικες ακεραιότητας μηνυμάτων MIC είναι πάντα 4 bytes. Τα δίκτυα συντονίζονται από τον χρόνο AST, Absolute Slot Time	Το ISA100.11a υποστηρίζει ρυθμιζόμενο χρόνο σχισμών. Το 10 ms είναι ένα από τα πολλά μεγέθη σχισμών (slots) που υποστηρίζονται. Ο διαχειριστής συστήματος (System Manager) ρυθμίζει το χρόνο σχισμών, όταν μία σύσκευή συνδέεται στο δίκτυο. Ορίζονται τρεις ακολουθίες μεταπήδησης καναλιών και πέντε μορφές μεταπήδησης (hopping patterns). Οι μορφές μεταπήδησης καναλιών παρέχονται από τον διαχειριστή συστήματος όταν συνδέεται μία σύσκευή στο δίκτυο. Οι κώδικες ακεραιότητας μηνυμάτων MIC μπορεί να είναι 4 ως 16 bytes. Τα δίκτυα συντονίζονται από το χρόνο TAI time. Το ISA100.11a επίσης υποστηρίζει δρομολόγηση στο DLL.	Η δυνατότητα του ISA100.11a να υποστηρίζει ρυθμιζόμενα μεγέθη χρονικών σχισμών και μορφές μεταπήδησης συχνότητας παρέχει μεγάλη ευελιξία. Το μειονέκτημα της μορφής αργής μεταπήδησης, είναι ότι ο δέκτης πρέπει να μείνει ενεργός για πολύ μεγαλύτερες χρονικές περιόδους και έτσι καταναλώνει πολλή ενέργεια. Αντίθετα από ότι ισχύει στον ορισμό του στρώματος DLL στο OSI, η δρομολόγηση δικτύου πλέγματος (mesh networking routing) γίνεται σε επίπεδο DLL και όχι στο στρώμα δικτύου (network layer). Όλες οι διαφορετικές επιλογές του ISA100.11a, σημαίνουν ότι δεν θα μπορούν όλες οι συσκευές του ISA100.11a να συνεργαστούν μεταξύ τους.
Στρώμα δικτύου Network layer	Το WirelessHART υποστηρίζει δρομολόγηση, σύνδεση και κρυπτογράφηση/αποκρυπτογράφηση στο στρώμα δικτύου	Το ISA100.11a υποστηρίζει το IETF IPv6 και 6LoWPAN στο στρώμα δικτύου (network layer).	Τα δύο πρότυπα έχουν εντελώς διαφορετικά στρώματα δικτύου. Το WirelessHART χρησιμοποιεί το στρώμα δικτύου για να υποστηρίξει τη δρομολόγηση στο δίκτυο πλέγματος. Το ISA100.11a χρησιμοποιεί το στρώμα δικτύου για να υποστηρίξει τη δρομολόγηση στο δίκτυο κορμού (backbone), που κάνει χρήση του IPv6 και επίσης το στρώμα δικτύου υλοποιεί το

			6LoWPAN. Ως μέρος του 6LoWPAN είναι ο κατακερματισμός (fragmentation) και η επανασυναρμολόγηση (reassembly) και η συμπίεση επικεφαλίδων IPv6 headers.
Δρομολόγηση κορμού (Backbone routing)	Το WirelessHART δεν έχει μία υποχρεωτική τεχνολογία δικτύου κορμού (backbone technology). Το HART-Over-IP μπορεί να χρησιμοποιηθεί ως δίκτυο κορμού (backbone).	Το ISA100.11a χρησιμοποιεί το IPv6 για το δίκτυο κορμού (backbone) για να δρομολογήσει τα πακέτα ανάμεσα στα υποδίκτυα subnets	Η δρομολόγηση κορμού (Backbone Routing) σχεδιάστηκε για δίκτυα που επεκτείνονται. Το WirelessHART πετυχαίνει το ίδιο προσθέτοντας περισσότερα σημεία πρόσβασης και πύλες. Το ISA100.11a χρησιμοποιεί το IPv6 το οποίο μπορεί να υποστηρίζεται ή όχι από ένα δίκτυο της εγκατάστασης.
Στρώμα Μεταφοράς TL ,Transport Layer	Το WirelessHART υποστηρίζει υπηρεσίες με αναγνώριση (acknowledged services) και υπηρεσίες χωρίς αναγνώριση (unacknowledged services). Η υπηρεσία με αναγνώριση επιτρέπει στις συσκευές να στέλνουν ένα πακέτο και όταν παραδοθεί να λαμβάνουν μία επιβεβαίωση λήψης πακέτου. Οι υπηρεσίες χωρίς αναγνώριση επιτρέπουν στις συσκευές να στέλνουν πακέτα χωρίς την απαίτηση για επιβεβαίωση λήψης από άκρο σε άκρο. (end- to-end acknowledgment), και έτσι δεν εγγυώνται την	Στο ISA100.11a το στρώμα μεταφοράς TL παρέχει υπηρεσίες connectionless services μέσω του πρωτοκόλλου User Datagram Protocol (UDP) πάνω στο IPv6 με προαιρετική συμπίεση όπως καθορίζεται από την προδιαγραφή του IETF 6LoWPAN. Η επέκταση επιτρέπει καλύτερο έλεγχο για την ακεραιότητα δεδομένων (data integrity checks) από αυτόν που επιτρέπει το UDP checksum και παρέχονται επιπρόσθετοι μηχανισμοί για πιστοποίηση και κρυπτογράφηση. Το στρώμα μεταφοράς TL του ISA100.11a δεν υποστηρίζει συναλλαγές με αναγνώριση(acknowledged transactions).	Στο ISA 100.11a, το στρώμα δικτύου χρησιμοποιεί μορφές IETF IPv6 και 6LoWPAN, και το στρώμα μεταφοράς παρέχει υπηρεσία connectionless service του UDP IPv6 με συμπιεσμένες ή ασυμπίεστες τις θύρες της πηγής και του προορισμού. Τα πακέτα στο ISA 100.11a μπορούν να ταξιδέψουν στο Internet, και είναι διαφανή προς τους κομβούς δρομολογητές (routing nodes). Όμως τρία βασικά στοιχεία α) η επικεφαλίδα ασφάλειας (security header) β) τα πραγματικά δεδομένα της εφαρμογής (application payload), και γ) το πεδίο MIC σχηματίζουν το μήνυμα με τα πραγματικά δεδομένα (message payload) του UDP. Για αυτό, ο κάθε τελικός κόμβος του Internet που είτε στέλνει είτε λαμβάνει τέτοια μηνύματα, θα

	επιτυχή μετάδοση των πακέτων		πρέπει να κατανοεί αυτά τα τρία συστατικά στοιχεία. Δηλαδή πρέπει να ακολουθεί το πρωτόκολλο ασφάλειας του ISA100.11a πρέπει να ξέρει πως να στήσει την ασφάλεια του ISA100.11a με τους ομότιμους κόμβους (peer) και πώς να το χρησιμοποιήσει. Αυτό σημαίνει ότι οι εφαρμογές Internet πρέπει να σχεδιάζονται για να είναι συμβατές με το ISA100.11a. Όμως αυτό δεν είναι και τόσο ανοικτό πρότυπο όπως θα έπρεπε να ήταν. Αντίθετα το WirelessHART σχεδιάστηκε ώστε να εργάζεται με υπάρχουσες εφαρμογές HART που είχαν γίνει παλαιότερα πριν τη δημιουργία του WirelessHART.
Στρώμα εφαρμογών AL Application Layer	Το WirelessHART χρησιμοποιεί το στρώμα εφαρμογών (AL) του HART. Το στρώμα εφαρμογών AL, όπως ορίζεται και υποστηρίζεται από το HART Communication Foundation (HCF), είναι εκτεταμένο. Το AL περιλαμβάνει τις Γενικές Εντολές Universal Commands (που ορίζονται από το IEC 61158-5-20 και IEC 61158-6-20). Οι γενικές εντολές ορίζουν την ελάχιστη υλοποίηση που πρέπει να υποστηρίζεται από τη συσκευή. Επιπλέον το στρώμα εφαρμογών υποστηρίζει τις	Στο ISA100.11a το στρώμα εφαρμογών AL ορίζει αντικείμενα λογισμικού software objects για να μοντελοποιήσει τα αντικείμενα του πραγματικού κόσμου. Διαιρείται σε δύο υποεπίπεδα sublayers: το ανώτερο υποεπίπεδο upper AL (UAL) και το υποεπίπεδο εφαρμογών application sublayer (ASL). Το UAL περιέχει τις διεργασίες εφαρμογών για τη συσκευή και μπορεί να χρησιμοποιηθεί για το χειρισμό υλικού εισόδου ή/και εξόδου (input and/or output hardware), να υποστηρίζει protocol tunneling, ή να εκτελέσει μία	Αυτή είναι η πιο σημαντική διαφορά ανάμεσα στα δύο πρότυπα. Το WirelessHART υποστηρίζει πλήρως το HART. Το ISA100.11a έχει μία πιο ανοικτή προσέγγιση και επιτρέπει αλλά δεν καθορίζει πρωτόκολλα εφαρμογών (application protocols).

	εντολές κοινής πρακτικής Common Practice Commands. Αυτές οι εντολές βελτιώνουν τη συνολική λειτουργία της συσκευής. Το στρώμα εφαρμογών AL επίσης περιλαμβάνει τις εντολές οικογένειας συσκευών (device family)που επεκτείνουν περισσότερο τις λειτουργίες των συσκευών devices (π.χ. Θερμοκρασία,πίεση, ροή, κραδασμοί, διακριτές τιμές) Τέλος το επιπεδο εφαρμογών υποστηρίζει τις εντολές που είναι για συγκεκριμένες συσκευές . Αυτές οι εντολές χρησιμοποιούνται από τους κατασκευαστές για να παρέχουν λειτουργίες περισσότερες και πέρα από όσες λειτουργίες ορίζονται από τις άλλες ομάδες εντολών. Οι συσκευές WirelessHART ορίζονται με τη χρήση του EDDL και υποστηρίζεται πλήρως από τις υπάρχουσες συσκευές χειρός handhelds	λειτουργία υπολογισμού. Το ASL παρέχει τις υπηρεσίες που απαιτούνται για το UAL για να εκτελέσει τις λειτουργίες τους όπως είναι η επικοινωνία βασισμένη σε αντικείμενα (object-based communication) και δρομολόγηση σε αντικείμενα (objects) μέσα σε μία διεργασία εφαρμογής χρήστη user application process (UAP) μέσα στο δίκτυο.	
Security Ασφάλεια	Το WirelessHART υποστηρίζει κλειδιά σύνδεσης, κλειδιά δικτύου, και κλειδιά συνόδου (session keys). Τα κλειδιά	Το ISA100.11a υποστηρίζει τα κλειδιά σύνδεσης (join keys), κλειδιά δικτύου και κλειδιά συνόδου (session keys). Τα	Και το WirelessHART και το ISA100.11a ορίζουν ένα σύνολο από κλειδιά ασφαλείας που χρησιμοποιούνται για ασφάλεια των

	συνόδου (Session keys) ανακατανέμονται για επικοινωνίες από συσκευή σε συσκευή (device-to-device). Όλες οι συσκευές πρέπει να χρησιμοποιούν ένα κλειδί σύνδεσης (join key). Όλες οι επικοινωνίες πρέπει να είναι κρυπτογραφημένες με χρήση των κλειδιών συνόδου (session keys). Τα κλειδιά σύνδεσης (Join keys) προβλέπονται και όταν χρησιμοποιείται μία συσκευή χειρός. (handheld device). Τα κλειδιά που είναι συμμετρικά με κωδικοποίηση AES-128 υποστηρίζονται. Τα κλειδιά μπορούν να χρησιμοποιούνται και διαδοχικά με μία κυκλική εναλλαγή.	κλειδιά συνόδου (Session keys) ανακατανέμονται για επικοινωνίες από συσκευή σε συσκευή (device-to-device). Τα κλειδιά σύνδεσης (Join keys) είναι προαιρετικά όπως είναι και τα κλειδιά συνόδου. Τα κλειδιά σύνδεσης προβλέπονται με πρόβλεψη (over the air provisioning). Υποστηρίζονται τα κλειδιά που είναι συμμετρικά με κωδικοποίηση AES-128. Το ISA100.11a επίσης ορίζει προαιρετικά τα κλειδιά που είναι ασύμμετρα (asymmetric keys) για τη διαδικασία σύνδεσης. Τα κλειδιά μπορούν να χρησιμοποιούνται διαδοχικά με κυκλική εναλλαγή.	επικοινωνιών. Η συμμετρική κρυπτογραφία βασίζεται και στα δύο άκρα της επικοινωνίας end points που χρησιμοποιούν το ίδιο κλειδί όταν επικοινωνούν με ασφάλεια. Οι επιτιθέμενοι που δεν μοιράζονται τα κοινά κλειδιά δεν μπορούν να τροποποιήσουν τα μηνύματα χωρίς να ανιχνευθούν και δεν μπορούν να αποκρυπτογραφήσουν τα κρυπτογραφημένα δεδομένα payload. Και στα δύο πρότυπα είναι κοινό ότι μια νέα συσκευή προβλέπεται (provisioned) με ένα κλειδί σύνδεσης (join key) πριν προσπαθήσει να συνδεθεί σε ένα δίκτυο. Το κλειδί σύνδεσης (join key) χρησιμοποιείται για να πιστοποιήσει τη συσκευή για ένα συγκεκριμένο δίκτυο. Όταν η συσκευή έχει συνδεθεί επιτυχώς στο δίκτυο, ο διαχειριστής ασφαλείας θα της παρέχει τα κλειδιά για την επικοινωνία. Η χρήση του κλειδιού σύνδεσης είναι προαιρετική στο ISA100.11a. Ένα γενικό κλειδί (global key), ένα καλά γνωστό κλειδί (well-known key) χωρίς εγγυήσεις ασφαλείας, μπορεί επίσης να χρησιμοποιηθεί στην διαδικασία σύνδεσης (join process) για συσκευές που δεν υποστηρίζουν συμμετρικά κλειδιά. Το ISA100.11a επιτρέπει προαιρετικά μηνύματα κρυπτογράφησης. Στο

			ISA100.11a η μέθοδος OTAP σε συνδυασμό με τα ασύμετρα κλειδιά είναι χρήσιμη μέθοδος για να γίνεται επέκταση των δικτύων. Το WirelessHART δεν επιτρέπει στην ασφάλεια να είναι προαιρετική και αυτό εμποδίζει τους κινδύνους στο σύστημα.
Διαχειριστής Ασφαλείας Security Manager	Ο ρόλος του διαχειριστή ασφαλείας ορίζεται στο WirelessHART. Οι εντολές και η προγραμματιστική διεπαφή εφαρμογών API δεν καθορίζονται.	Το ISA100.11a παρέχει προδιαγραφές για τον διαχειριστή Ασφαλείας.	Επειδή επικρατεί μία τάση, η λειτουργία του διαχειριστή ασφαλείας να παρέχεται από κοινού με τον διαχειριστή δικτύου, στα μικρά δίκτυα και στα δίκτυα μεσαίου μεγέθους δεν υπάρχει σημαντικό όφελος αν περιγραφεί λεπτομερώς μία προδιαγραφή του διαχειριστή ασφαλείας. Στα μεγαλύτερα δίκτυα μπορεί να υπάρξει μία περίπτωση να καθοριστεί μία πιο λεπτομερής προδιαγραφή του διαχειριστή ασφαλείας.
Διαχειριστής Δικτύου/Συστήματος Network/system Manager	Το WirelessHART περιέχει μία εκτεταμένη περιγραφή και σύνολο εντολών για τον διαχειριστή δικτύου.	Το ISA100.11a περιλαμβάνει μία λεπτομερή περιγραφή και ένα σύνολο από υπηρεσίες για τον διαχειριστή συστήματος System Manager	Πολλές είναι οι διαφορές του διαχειριστή δικτύου (Network Manager) του WirelessHART από τον διαχειριστή συστήματος (System Manager) του ISA100.11a. Οι διαφορές μεταξύ άλλων, υπάρχουν στις διαγνώσεις, στη ρύθμιση και στην ενεργοποίηση των υπερπλασίων (superframes) και των ζεύξεων (links), στις διαδρομές δρομολόγησης routes, και στους πίνακες χρόνου time tables. Ο διαχειριστής συστήματος στο ISA100.11a πρέπει να παρακολουθεί τους ρόλους που υποστηρίζουν συγκεκριμένες συσκευές και πρέπει να προβλέπει σωστά και να

			διαχειρίζεται αυτές τις συσκευές. Έτσι ο διαχειριστής Συστήματος είναι πιο περίπλοκος στη χρήση του.
Διεθνές πρότυπο	Από το Μάρτιο 2010 το WirelessHART είναι πρότυπο IEC 6251-1 Μέχρι το 2007 Ήταν το πρότυπο HART-7	Το ISA100.11a είναι το πρότυπο ANSI/ISA100.11a-2011	Το WirelessHART είναι διεθνές πρότυπο από το Μάρτιο 2010, ενώ το ISA100.11a έχει μπει στη διαδικασία να γίνει το διεθνές πρότυπο IEC 62734
Διαλειτουργικότητα. Είναι η ικανότητα να συνεργάζονται πύλες από διαφορετικούς κατασκευαστές	Η διαλειτουργικότητα ανάμεσα στις συσκευές WirelessHART απαιτείται από το HCF που ορίζει το πρότυπο. Το HCF εκτελεί ελέγχους διαλειτουργικότητας με συσκευές WirelessHART διαφορετικών κατασκευαστών και για τη στοίβα στρωμάτων και για την εφαρμογή HART-7	Ο έλεγχος για συμμόρφωση με τη στοίβα (Stack conformance testing) εκτελείται από το WCI. Το ISA100.11a εστιάζει στην ευελιξία της προδιαγραφής και έτσι οδηγεί σε προαιρετικές επιλογές που μερικές δεν είναι καθορισμένες πλήρως. Οι επιλογές του ISA100.11a δεν καθορίζονται ώστε όταν υλοποιούνται, υπάρχει μία διαλειτουργικότητα με άλλες συσκευές που δεν τις χρησιμοποιούν.	Οι συσκευές ISA100.11a devices μπορούν να περάσουν τον έλεγχο WCI testing και παρόλα αυτά να μην μπορούν να συνεργαστούν μεταξύ τους. Εξαρτάται από το πώς χρησιμοποιούνται οι οι προαιρετικές επιλογές. Δεν υπάρχει έλεγχος διαλειτουργικότητας στον αυτοματισμό διεργασιών για τις συσκευές του ISA100.11a.
Συνύπαρξη	Ναι	Ναι	Τα χαρακτηριστικά του Φυσικού επιπέδου είναι η μεταπήδηση συχνότητας και το TDMA που επιτρέπουν τη συνύπαρξη.
Πλήθος κατασκευαστών που υποστηρίζουν τα προϊόντα	Οι κατασκευαστές Emerson, Siemens, ABB, Endress+Hauser, Pepperl+Fuchs, MacTech, καθώς και άλλοι κατασκευαστές (περίπου 13) υποστηρίζουν το WirelessHART, ενώ υπάρχουν πολλές άλλες εταιρίες από τις 240 που είναι μέλη της HCF που εργάζονται για να	Οι εταιρίες Honeywell και Yokogawa υποστηρίζουν το ISA100.11a	Το πλήθος προμηθευτών που υποστηρίζουν το WirelessHART είναι πολύ μεγαλύτερο από το πλήθος κατασκευαστών που υποστηρίζουν το ISA100.11a. Το WirelessHART προηγείται γιατί ξεκίνησε δύο χρόνια νωρίτερα, υποστηρίζει ένα πλήρως καθορισμένο στρώμα εφαρμογών και έχει εκτεταμένο σύνολο προμηθευτών, ενώ

	υποστηρίζουν αυτά τα προϊόντα.		χρησιμοποιήθηκε σε σημαντικό αριθμό δικτύων παγκοσμίως.
Φυσικό στρώμα και στοίβα επικοινωνιών	IEEE 802.15.4 – 2006. Η στοίβα επικοινωνιών περιλαμβάνει τις εταιρίες: Linear Technology, WiTECK, Nivis and AwiaTech	IEEE 802.15.4 – 2006. Η στοίβα επικοινωνιών περιλαμβάνει την: Nivis	
Βασικό πρωτόκολλο πακέτων δεδομένων	HART 7	ISA 100.11a	Το ISA100 πρέπει να μπορεί να στείλει δεδομένα (tunnel) σε μορφή HART7 μέσω του βασικού του πρωτοκόλλου, αλλά οι μέθοδοι που απαιτούνται για διαλειτουργικότητα δεν έχουν τυποποιηθεί προς το παρόν.
Προσαρμογείς HART για σύνδεση των συσκευών HART στο ασύρματο δίκτυο	Ναι, υποστηρίζονται από πολλούς κατασκευαστές.	Είναι εφικτό αλλά δεν υποστηρίζονται προς το παρόν.	Οι προσαρμογείς είναι βασικές συσκευές για το WirelessHART. Οι παλαιότερες συσκευές του HART 5 και 6 συνδέονται με τους προσαρμογείς στο δίκτυο WirelessHART.

Πίνακας 3.23. Διαφορές ανάμεσα στο WirelessHART και στο ISA100.11a πηγή: [30]

Κεφάλαιο 4

Κινητικότητα στα Ασύρματα Δίκτυα Αισθητήρων

Στα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks) (WSN), οι στατικοί κόμβοι αισθητήρες, τοποθετούνται σε κάποιες θέσεις και συλλέγουν δεδομένα από μία περιοχή, που τα παραδίδουν σε κεντρικούς κόμβους sinks, με διαδρομές δρομολόγησης πολλαπλών αλμάτων (multi-hop). Με τη κινητικότητα, οι κινητοί κόμβοι, κινούνται σε τροχιές, τυχαίες ή σχεδιασμένες, κοντά στους στατικούς κόμβους αισθητήρες, για να λάβουν απευθείας τα δεδομένα από αυτούς με μία μετάδοση ενός άλματος (single hop). Έχουν γίνει πολλές προτάσεις με στόχο την κινητικότητα. Σε αυτό το κεφάλαιο αρχικά γίνεται μία ανάλυση διαφορετικές κατηγορίες κινητικότητας, αναφέρονται βασικά προβλήματα και στη συνέχεια παρουσιάζονται διαφορετικά μοντέλα κινητικότητας. Το στρώμα MAC, είναι υποεπίπεδο στο επίπεδο ζεύξης δεδομένων Data (Link Layer). και ρυθμίζει την επικοινωνία δεδομένων ανάμεσα στους κόμβους, καθώς και τους τρόπους σύνδεσης και αποσύνδεσης νέων κόμβων στο δίκτυο. Έτσι το στρώμα MAC μπορεί να χρησιμοποιηθεί για να ρυθμιστεί η κινητικότητα στα ασύρματα δίκτυα αισθητήρων. Στην συνέχεια αυτού του κεφαλαίου παρουσιάζονται διάφορα πρωτόκολλα MAC.

4.1 Γενικά

Στις παραγράφους που ακολουθούν, γίνεται μία αναφορά στα είδη κινητικότητας που μπορούν να εφαρμοστούν στα ασύρματα δίκτυα αισθητήρων. Τα είδη κινητικότητας είναι πολλά και για αυτό χωρίζονται σε διαφορετικές κατηγορίες. Για την κινητικότητα πρέπει να ληφθούν υπόψη τα τέσσερα βασικά χαρακτηριστικά των ασύρματων δικτύων αισθητήρων [9] που αναφέρονται παρακάτω:

α) Κινητικότητα υποσυνόλου των κόμβων. Στα ασύρματα δίκτυα αισθητήρων, η κινητικότητα δεν αφορά όλους τους κόμβους αλλά συνήθως αφορά ένα υποσύνολο των κόμβων διότι πάντα υπάρχουν κάποιοι στατικοί κόμβοι που βρίσκονται σε σταθερά σημεία σε μία περιοχή και είναι πιο σπάνιο σε αυτά τα δίκτυα να κινούνται όλοι οι κόμβοι σε ασύρματα δίκτυα αισθητήρων που δεν χρησιμοποιούνται για στρατιωτικές εφαρμογές.

β) Μεγάλο πλήθος στατικών κόμβων. Συνήθως οι κόμβοι ενός ασύρματου δικτύου αισθητήρων είναι πάρα πολλοί και μπορεί να είναι χιλιάδες. Έτσι συχνά υπάρχουν κινητοί κόμβοι που κινούνται με τροχιές ανάμεσα σε στατικούς κόμβους, αλλά δεν μπορούν να συλλέξουν δεδομένα από τον κάθε ένα κόμβο ξεχωριστά, ούτε μπορούν να επισκεπτονται όλους τους απομακρυσμένους κόμβους έναν προς έναν. Για αυτό, όλοι οι κόμβοι ομαδοποιούνται σε συστοιχίες. Συχνά οι κινητοί κόμβοι που μετακινούνται σε μία τροχιά, επισκέπτονται μόνο έναν κεντρικό κόμβο από κάθε συστοιχία, που ονομάζεται κεφαλή συστοιχίας και συγκεντρώνει δεδομένα από όλους τους υπόλοιπους κόμβους της συστοιχίας, για να τα μεταφέρει στον κινητό κόμβο. Σε ένα δίκτυο με χιλιάδες κόμβους, αν κάποιοι κόμβοι χαλάσουν δεν αντικαθίστανται ούτε επαναφορτίζονται οι μπαταρίες τους. Έτσι, αυτοί οι κόμβοι γίνονται άχρηστοι αλλά δεν επηρεάζουν σημαντικά τη λειτουργία του υπόλοιπου δικτύου, διότι υπάρχουν πολλοί άλλοι κόμβοι στην περιοχή, ούτε επηρεάζουν το κόστος, γιατί είναι σχετικά φθηνές συσκευές και η καταστροφή τους δεν προκαλεί μεγάλη οικονομική ζημία.

γ) Μικρή διαθεσιμότητα των πόρων για τους στατικούς κόμβους. Τα ασύρματα δίκτυα αισθητήρων βασίζονται σε κόμβους που έχουν περιορισμένους πόρους. Περιορισμένοι πόροι των συσκευών είναι η μικρή αυτονομία στη μπαταρία, η υπολογιστική ισχύς και η διαθέσιμη μνήμη που είναι πολύ μικρή και για αυτό επιβάλλεται να χρησιμοποιούνται εξειδικευμένα λειτουργικά συστήματα, και εξειδικευμένο λογισμικό, ενώ δεν πρέπει να εισάγεται μεγάλη πολυπλοκότητα στο πρωτόκολλο διότι υπάρχουν περιορισμοί στις δυνατότητες του μικροελεγκτή.

δ) Μεγαλύτερη διαθεσιμότητα πόρων για τους κεντρικούς κόμβους. Στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται κάποιοι κεντρικοί κόμβοι με περισσότερους πόρους από τους υπόλοιπους κόμβους, που έχουν το ρόλο να συλλέγουν τα δεδομένα από τους στατικούς κόμβους. Σε κάποιες μορφές κινητικότητας οι κινητοί κόμβοι είναι αυτοί που διαθέτουν τους περισσότερους πόρους. Σε άλλα μοντέλα, υπάρχει ένας στατικός κεντρικός κόμβος, και οι κινητοί κόμβοι πηγαινοέρχονται ανάμεσα στους στατικούς κόμβους λαμβάνουν τα δεδομένα από αυτούς και τα μεταφέρουν στον στατικό κόμβο.

4.2 Είδη Κινητικότητας

Η κινητικότητα στα ασύρματα δίκτυα αισθητήρων μπορεί να βασιστεί σε διάφορα σενάρια και να προκύψουν πολλές διαφορετικές προσεγγίσεις.

Στα σενάρια αυτά, υπάρχει ένα σύνολο κόμβων που είναι στατικοί και ένα σύνολο κόμβων που είναι κινητοί. Οι κινητοί κόμβοι ονομάζονται mobile nodes (MN). πολλές κατηγοριοποιήσεις μπορούν να γίνουν στα διαφορετικά είδη κινητικότητας.

Μερικά σενάρια που μπορούν να αναφερθούν, μεταξύ άλλων, είναι: [35] [36] [37] [38]

1. Όλοι οι κόμβοι του δικτύου είναι στατικοί και κινείται μόνο ο κεντρικός κόμβος που είναι ο κινητός Sink, ο οποίος συλλέγει δεδομένα από όλους τους στατικούς κόμβους. Ο κινητός Sink συχνά αναφέρεται και ως Κινητός Σταθμός Βάσης (MBS Mobile Base Station)
2. Υπάρχουν πολλοί στατικοί κόμβοι του δικτύου και ένας στατικός sink, αλλά υπάρχουν και κάποιοι επιπρόσθετοι κινητοί κόμβοι που λέγονται data MULEs, που λέγονται και Κινητοί Συλλέκτες Δεδομένων (MDCs, Mobile Data Collectors) οι οποίοι κινούνται σε σταθερές τροχιές, συλλέγουν τα δεδομένα από τους στατικούς κόμβους και στη συνέχεια μεταφέρουν τα δεδομένα στον στατικό sink.
3. Υπάρχουν πολλοί στατικοί κόμβοι του δικτύου και υπάρχουν οι κινητοί κόμβοι data MULEs και ο κινητός sink που περιφέρονται ανάμεσα στους στατικούς κόμβους για να συλλέξουν τα δεδομένα από τους στατικούς κόμβους.
4. Υπάρχουν πολλαπλοί κινητοί κόμβοι sinks που κινούνται μέσα στο δίκτυο και συλλέγουν δεδομένα από τους στατικούς κόμβους.

5. Υπάρχουν κινητοί κόμβοι αισθητήρες και πλησιάζουν τους sink για να τους μεταφέρουν δεδομένα.

6. Διάφοροι συνδυασμοί των παραπάνω, όπως πολλαπλοί κινητοί κόμβοι data MULEs και πολλαπλοί κινητοί κόμβοι sinks, ή άλλοι συνδυασμοί κινητών και σταθερών κόμβων.

7. Οι κινητοί κόμβοι, μπορούν να τοποθετούνται σε οχήματα, κινούμενα μέρη μηχανών, σε ρομπότ ή σε συσκευές χειρός.

Επίσης η ταξινόμηση της κινητικότητας μπορεί να γίνει στις 2 ακόλουθες κατηγορίες:

8. Κινητικότητα κόμβου

Ο κινητός κόμβος μπορεί να μετακινείται πάντοτε σε τακτικά χρονικά διαστήματα, με την ίδια κίνηση για να επιτελέσει μία συγκεκριμένη εργασία. Δηλαδή, ο κινητός κόμβος μπορεί είναι τοποθετημένος σε ένα κινούμενο μηχανικό μέρος, όπως π.χ. σε ένα μηχανικό βραχίονα σε γραμμή παραγωγής συναρμολόγησης αντικειμένων. Ο κόμβος αισθητήρας θα κινείται πάντα με τον ίδιο τρόπο και η κίνηση του αποτελεί μέρος της εργασίας που εκτελείται. Για παράδειγμα, ο κόμβος αισθητήρας (sensor node) μπορεί να συγκεντρώνει πληροφορίες για τα αντικείμενα που συναρμολογήθηκαν ή για τα ελαττωματικά αντικείμενα που απορρίφθηκαν.

9. Κινητικότητα γεγονότος

Ο κινητός κόμβος ενεργοποιείται μόνο όταν συμβεί κάποιο γεγονός δηλαδή σε έκτακτη περίπτωση. Έτσι οι κινητοί κόμβοι δεν είναι συνεχώς παρόντες μέσα στο δίκτυο, αλλά εμφανίζονται όταν υπάρξει μία ανάγκη. Για παράδειγμα, όταν σε ένα χώρο ανιχνεύεται μία πυρκαγιά, ενεργοποιείται ένα πυροσβεστικό ρομπότ πηγαίνει να σβήσει την φωτιά, ενώ πάνω στο ρομπότ μπορεί να υπάρχει ένας κινητός κόμβος αισθητήρας που καταγράφει τη θερμοκρασία.

Συνήθως ο κεντρικός κόμβος sink έχει πιο πολλές δυνατότητες σε ενέργεια, και σε χωρητικότητα δεδομένων διότι ο ρόλος του είναι να συλλέγει δεδομένα από όλους τους κόμβους τα οποία πρέπει να αποθηκεύονται στον sink και για αυτό πρέπει ο αποθηκευτικός χώρος του να είναι πιο μεγάλος από τον αποθηκευτικό χώρο ενός απλού κόμβου. Οι υπόλοιποι κόμβοι αισθητήρες (sensor nodes) έχουν λιγότερες δυνατότητες σε ενέργεια και σε χωρητικότητα δεδομένων από ότι έχει ο sink διότι κάθε κόμβος αποθηκεύει μόνο τα δεδομένα των δικών του μετρήσεων και έτσι δεν απαιτείται μεγάλος αποθηκευτικός χώρος.

Οι κόμβοι αισθητήρες που μπορούν να συλλέξουν περισσότερα δεδομένα από πολλές πηγές, λέγονται (resource rich nodes) δηλαδή πλούσιοι σε πόρους.

Μεγάλο αποθηκευτικό χώρο θα πρέπει να έχουν και οι κόμβοι data MULEs που, όταν χρησιμοποιούνται, μεταφέρουν τα δεδομένα από τους τους στατικούς κόμβους αισθητήρες στον sink.

Οι κόμβοι αισθητήρες μπορούν να είναι πάρα πολλοί σε πλήθος επειδή το κόστος τους είναι χαμηλό. Επίσης, αν συμβεί μία αστοχία σε έναν ή περισσότερους κόμβους, συνήθως αυτό δεν αποτελεί πρόβλημα για το συνολικό δίκτυο, διότι η δρομολόγηση δεδομένων γίνεται μέσω άλλων κόμβων.

Σε ένα ασύρματο δίκτυο αισθητήρων γενικότερα, οι κόμβοι μπορεί να είναι είτε τοποθετημένοι σε συγκεκριμένες θέσεις είτε διασκορπισμένοι τυχαία σε μία περιοχή.

Σε μία βιομηχανική εγκατάσταση, κάποιοι κόμβοι δεν μπορούν να τοποθετηθούν σε τυχαία σημεία στο χώρο, διότι βρίσκονται ενσωματωμένοι στα έξυπνα όργανα μέτρησης. Τα όργανα μέτρησης είναι τοποθετημένα σε συγκεκριμένες θέσεις μέσα στην εγκατάσταση για να λαμβάνουν συγκεκριμένες μετρήσεις φυσικών μεγεθών, όπως είναι, πίεση, θερμοκρασία, ύψος στάθμης υγρών κ.α. Επομένως, η θέση των αισθητήρων δεν μπορεί να είναι τυχαία αλλά τοποθετούνται σε κατάλληλα σημεία για να γίνουν οι απαιτούμενες μετρήσεις μέσα στην βιομηχανική εγκατάσταση.

Σε ένα δίκτυο WirelessHART, ο κεντρικός κόμβος sink συνήθως είναι η πύλη (gateway) που συγκεντρώνει τα δεδομένα μετρήσεων. Έτσι η κινητικότητα σε μία βιομηχανική εγκατάσταση προϋποθέτει ότι θα υπάρχει ένα σύνολο από στατικούς κόμβους που παράγουν τα δεδομένα μετρήσεων από διάφορες περιοχές της βιομηχανικής εγκατάστασης και ένα σύνολο από κινητούς κόμβους που επισκέπτονται τους στατικούς

κόμβους και αποθηκεύουν δεδομένα από πολλούς κόμβους στη μνήμη τους για να τα μεταφέρουν σε κάποιο κεντρικό σημείο.

Αν θέλουμε να υπάρχει μία τυχαία τοποθέτηση στατικών αισθητήρων στο χώρο, αυτό θα μπορούσε να συμβεί, σε μία προσέγγιση όπου μαζί με τα έξυπνα όργανα, θα έπρεπε να τοποθετηθούν και επιπλέον αισθητήρες διασκορπισμένοι τυχαία σε ένα χώρο, οι οποίοι θα είναι ανεξάρτητοι από τα όργανα μέτρησης. Οι επιπρόσθετοι αισθητήρες θα έχουν στόχο να μετρούν συνθήκες που επικρατούν μέσα στον συνολικό χώρο, πχ, ποσοστά εύφλεκτων αερίων που υπάρχουν στην ατμόσφαιρα του χώρου, ή την παρουσία επικίνδυνων χημικών υγρών στο δάπεδο του χώρου κ.α.

Μια άλλη λύση είναι να έχουμε κάποιους αισθητήρες που μετρούν θερμοκρασία, υγρασία, ακτινοβολία, φως, ήχο, δονήσεις. Αυτοί οι αισθητήρες μπορεί να είναι τοποθετημένοι σε ρομπότ που μετακινούνται για να κάνουν διάφορες εργασίες και καθώς κινούνται σε μία τροχιά να μεταφέρουν πληροφορίες στον κεντρικό κόμβο sink, ο οποίος μπορεί να είναι στατικός και τοποθετημένος σε ένα σταθερό σημείο.

Οι κινητοί κόμβοι μπορούν να τοποθετηθούν σε οχήματα, ή σε μηχανές που φορτώνουν και εκφορτώνουν αντικείμενα, ή σε κινητά ρομπότ που περιφέρονται μέσα στην εγκατάσταση για να εκτελέσουν διάφορες διαδικασίες.

Επίσης μπορούν να τοποθετηθούν κόμβοι αισθητήρες σε συσκευές χειρός (handheld communicators) που μεταφέρουν οι εργάτες καθώς κινούνται στους χώρους της βιομηχανικής εγκατάστασης.

4.2.1 Επίπεδα αρχιτεκτονικής

Για να δημιουργηθεί ένα ασύρματο δίκτυο αισθητήρων που χρησιμοποιεί κινητούς κόμβους αισθητήρες (mobile sensor nodes) συνήθως χρησιμοποιείται μία δομή στην οποία η αρχιτεκτονική είναι βασισμένη σε ένα μέχρι τρία επίπεδα. Δηλαδή, γίνεται διαχωρισμός σε αρχιτεκτονική δικτύου ενός επιπέδου (1 layer architecture), αρχιτεκτονική δικτύου δύο επιπέδων (2 layer architecture) και αρχιτεκτονική δικτύου τριών επιπέδων (3 layer architecture). [39].

4.2.1.1 Αρχιτεκτονική ενός επιπέδου ή επίπεδη αρχιτεκτονική

Αυτή η αρχιτεκτονική ονομάζεται επίπεδη (Flat ή planar network architecture). [39]. Δηλαδή όλες οι συσκευές κινητές και στατικές σχηματίζουν ένα δίκτυο και επικοινωνούν όλες μαζί μέσα στο ίδιο δίκτυο. Το δίκτυο αυτό αποτελείται από ένα σύνολο ετερογενών συσκευών (heterogeneous devices) που επικοινωνούν μεταξύ τους με τρόπο όμοιο όπως οι ισότιμοι κόμβοι σε ένα δίκτυο ad hoc. Η επίπεδη αρχιτεκτονική χρησιμοποιείται σε συστήματα πλοήγησης.

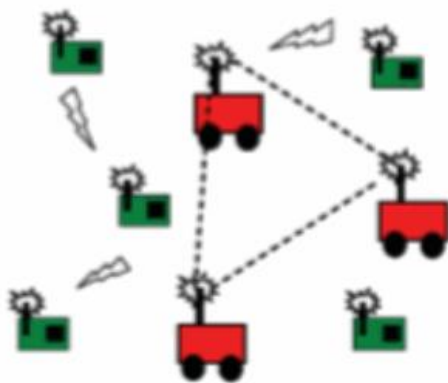


Εικόνα 112. Αρχιτεκτονική ενός επιπέδου ή επίπεδη (Planar architecture). Πηγή [39].

4.2.1.2 Αρχιτεκτονική δύο επιπέδων

Αυτή η αρχιτεκτονική αποτελείται από ένα σύνολο στατικών κόμβων (stationary nodes), που αποτελούν το 1^ο επίπεδο του δικτύου και ένα σύνολο κινητών κόμβων (mobile nodes), που είναι το 2^ο επίπεδο του δικτύου. Οι κινητοί κόμβοι δημιουργούν ένα ξεχωριστό δικό τους διαφανές δίκτυο (overlay network) που βρίσκεται μέσα στο δίκτυο των στατικών κόμβων. Οι κινητοί κόμβοι μπορεί να δρουν και ως κόμβοι που μεταφέρουν δεδομένα και τότε λέγονται data mules. Ο ρόλος των κόμβων data mules είναι να μετακινούν τα δεδομένα μέσα στο δίκτυο, για να τα μεταφέρουν από τους στατικούς κόμβους στον κεντρικό κόμβο sink. Το ξεχωριστό διαφανές δίκτυο (overlay

network) που σχηματίζουν οι κινητοί κόμβοι μπορεί να περιλαμβάνει κινητές συσκευές με μεγαλύτερες δυνατότητες επεξεργασίας δεδομένων, μεγαλύτερη εμβέλεια επικοινωνιών (range) για πιο μεγάλες αποστάσεις, και μεγαλύτερο εύρος ζώνης (bandwidth). Το ξεχωριστό διαφανές δίκτυο (overlay network) αποτελείται από ένα συγκεκριμένο πλήθος κινητών κόμβων ώστε οι κόμβοι να βρίσκονται ο ένας στην εμβέλεια του άλλου. Στόχος είναι όλοι οι κόμβοι του δικτύου αυτού να παραμένουν συνδεδεμένοι. Αν η πυκνότητα κόμβων δεν είναι κατάλληλη, τότε θα υπάρχουν αποσυνδέσεις κινητών κόμβων. Αν αποσυνδεθούν κάποιοι κινητοί κόμβοι, τότε πρέπει να μετακινηθούν σε κάποιες συγκεκριμένες θέσεις όπου που είναι γνωστό ότι υπάρχει σίγουρα το δίκτυο και θα ξαναγίνει η σύνδεσή τους, ώστε όλα τα πακέτα δεδομένων που μεταφέρουν να φτάσουν στον προορισμό τους (destination).



Εικόνα 113. Αρχιτεκτονική δύο επιπέδων (2 layer architecture). Πηγή [39]

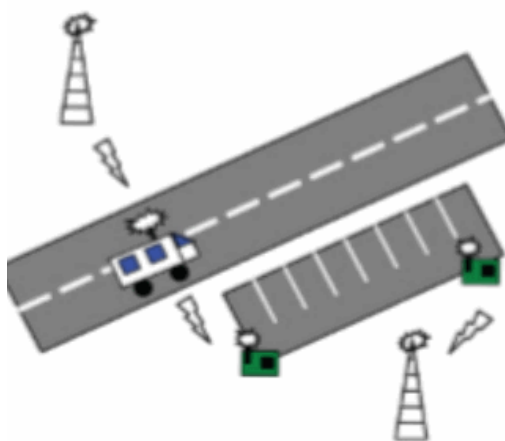
4.2.1.3 Αρχιτεκτονική τριών επιπέδων

Σε αυτή την αρχιτεκτονική, το 1^ο επίπεδο είναι ένα σύνολο από στατικούς κόμβους αισθητήρες (stationary sensor nodes). Το 2^ο επίπεδο είναι ένα σύνολο από κινητούς κόμβους (mobile nodes). Το 3^ο επίπεδο είναι ένα σύνολο από σημεία πρόσβασης (access points). Οι στατικοί κόμβοι (static nodes) στέλνουν τα δεδομένα τους στους κινητούς κόμβους, και οι κινητοί κόμβοι προωθούν τα δεδομένα στα σημεία πρόσβασης AP.

Με αυτό τον τρόπο σχηματίζεται ένα ετερογενές δίκτυο (heterogeneous network) που μπορεί να καλύψει κάποιες μεγάλες περιοχές. Αυτό το δίκτυο μπορεί να υποστηρίξει

πολλές εφαρμογές ταυτόχρονα. Ένα σενάριο χρήσης ενός τέτοιου δικτύου [39] είναι το εξής:

Υποθέτουμε ότι ένα ασύρματο δίκτυο αισθητήρων είναι τοποθετημένο σε έναν χώρο στάθμευσης οχημάτων για να ελέγχει αν υπάρχουν άδειοι χώροι στάθμευσης. Το πρώτο επίπεδο είναι ένα ασύρματο δίκτυο στατικών αισθητήρων. Αυτό το δίκτυο εκπέμπει σήματα με πληροφορίες για τις τρέχουσες διαθέσιμες θέσεις στάθμευσης. Κάθε σήμα εκπέμπεται (broadcast) προς όλους τους κινητούς κόμβους (mobile nodes) που είναι το 2^ο επίπεδο. Τέτοιοι κινητοί κόμβοι μπορεί να είναι τα smartphones ή τα PDAs των χρηστών που περνούν από εκεί κοντά. Με τη σειρά τους, οι κινητές συσκευές προωθούν αυτά τα δεδομένα για τις διαθέσιμες θέσεις στάθμευσης σε σημεία πρόσβασης (access points) που αποτελούν το τρίτο επίπεδο. Τέτοια σημεία πρόσβασης AP βρίσκονται σε πύργους κεραιών κινητής τηλεφωνίας. Έτσι τα δεδομένα μεταφέρονται σε έναν διακομιστή και αποθηκεύονται σε βάση δεδομένων. Οι χρήστες έχουν πρόσβαση στη βάση δεδομένων με μία κατάλληλη εφαρμογή που εκτελείται στο smartphone τους και συνδέεται στο διακομιστή. Έτσι οι χρήστες ενημερώνονται για τις διαθέσιμες θέσεις στάθμευσης.



Εικόνα 114. Αρχιτεκτονική τριών επιπέδων (3 layer architecture). Πηγή [39].

4.2.2 Βασικά προβλήματα

Υπάρχουν δύο βασικά προβλήματα που με τη σειρά τους οδηγούν σε αρκετά άλλα θέματα, τα οποία παρουσιάζονται στα ασύρματα δίκτυα αισθητήρων και πρέπει να επιλυθούν:

α) Η εξάντληση ενέργειας τροφοδοσίας των κόμβων, που οδηγεί στη μείωση της διάρκειας ζωής του δικτύου (network lifetime).

β) Η καθυστέρηση (latency) παράδοσης των δεδομένων από τους κόμβους αισθητήρες, στον κεντρικό κόμβο sink.

Πολλές φορές τα δύο παραπάνω ζητήματα συνδέονται με μία σχέση ανταλλαγής (tradeoff) δηλαδή αν επιτευχθεί ένα κέρδος στην εξοικονόμηση ενέργειας και αυξηθεί έτσι η διάρκεια ζωής του δικτύου, τότε παράλληλα υπάρχει ένα κόστος σε καθυστέρηση (latency).

Από την άλλη πλευρά, αν επιτευχθεί ένα κέρδος χρόνου και μικρή καθυστέρηση, τότε υπάρχει το κόστος ότι μπορεί να εξαντληθεί πιο γρήγορα η ενέργεια στους κόμβους και έτσι θα υπάρχει μικρότερη διάρκεια ζωής του δικτύου.

Ο στόχος των ερευνητών είναι να προτείνουν διάφορες λύσεις ώστε να μειωθεί η κατανάλωση ενέργειας τροφοδοσίας από τους κόμβους. Διάφορες προσεγγίσεις έχουν γίνει με στόχο την μείωση κατανάλωσης ενέργειας,

Επιπλέον, υπάρχει και ένα πλήθος από άλλα προβλήματα. Για τα δίκτυα που οι κόμβοι είναι τοποθετημένοι τυχαία, ή υπάρχουν κινητοί κόμβοι άλλα ζητήματα είναι:

γ) Ο εντοπισμός της θέσης των κόμβων.

Πρέπει να γίνεται μία διαχείριση των θέσεων (locations) που βρίσκονται οι κινητοί κόμβοι. Πολλές φορές χρειάζεται να γίνει μία επαναληπτική δρομολόγηση των πακέτων δεδομένων όταν ένας κινητός κόμβος αλλάξει τη θέση του ώστε αν χαθούν κάποια πακέτα που στάλθηκαν σε προηγούμενη θέση του κόμβου, να υπάρχει η βεβαιότητα ότι ο κόμβος θα λάβει αυτά τα πακέτα στη νέα θέση που βρίσκεται.

δ) η διαχείριση της μετάβασης (handoff) των κινητών κόμβων από ένα δίκτυο σε άλλο.

Όταν ο κινητός κόμβος κινείται από ένα δίκτυο σε άλλο, επηρεάζονται οι πληροφορίες που διατηρούνται στο δίκτυο για τις θέσεις των κόμβων, τη διαδρομή δρομολόγησης, και οι πληροφορίες της τοπολογίας του δικτύου, όπως είναι η λίστα των γειτόνων κάθε κόμβου.

Μερικά άλλα ζητήματα που προκύπτουν αναφέρονται παρακάτω.

ε) η υπερχειλίση ενδιάμεσης μνήμης (buffer overflow) λόγω της καθυστέρησης (latency).

Η μεγάλη καθυστέρηση (latency), ενός κινητού κόμβου να επισκεφθεί έναν στατικό κόμβο, οδηγεί στο πρόβλημα της υπερχειλίσης ενδιάμεσης μνήμης (buffer overflow) και στην απώλεια δεδομένων. Η αιτία που συμβαίνει αυτό, είναι η εξής: Ο κάθε στατικός κόμβος αισθητήρας συσσωρεύει τιμές μετρήσεων που λαμβάνει για διάφορα φυσικά μεγέθη, στην ενδιάμεση μνήμη του (buffer). Η ενδιάμεση μνήμη του στατικού κόμβου είναι σχετικά μικρή και μπορεί να χωρέσει ένα σύνολο δεδομένων που καταγράφονται σε μία ουρά (queue). Ένας κινητός κόμβος κινείται ανάμεσα στους στατικούς κόμβους και συλλέγει τα δεδομένα τους. Όταν φτάσει ο κινητός κόμβος στην εμβέλεια (range) ενός στατικού κόμβου, τα δεδομένα του στατικού κόμβου μεταφέρονται από την ενδιάμεση μνήμη (buffer) του μέσω ασύρματου δικτύου στη μνήμη του κινητού κόμβου, η οποία είναι μεγαλύτερη για να αποθηκεύει τα δεδομένα από πολλαπλούς κόμβους.

Αν όμως ο κινητός κόμβος καθυστερήσει να επισκεφτεί κάποιους στατικούς κόμβους, τότε η ενδιάμεση μνήμη των στατικών κόμβων (buffer) θα γεμίσει από δεδομένα μετρήσεων. Έτσι τα νέα δεδομένα μετρήσεων θα απορρίπτονται διότι δεν θα μπορούν να αποθηκευτούν στη μνήμη των στατικών κόμβων. Τότε θα υπάρχει απώλεια δεδομένων λόγω της υπερχειλίσης ενδιάμεσης μνήμης (buffer overflow). Συνεπώς, απαιτείται ένας κατάλληλος χρονοπρογραμματισμός (scheduling) ώστε να μην υπάρχει καθυστέρηση (latency) μεγαλύτερη από κάποια αποδεκτά όρια.

στ) Η εξάντληση ενέργειας από το χρόνο που παραμένουν ενεργοποιημένοι οι κόμβοι.

Ένα άλλο πρόβλημα είναι το πόση ώρα πρέπει να είναι ενεργοποιημένος ο στατικός κόμβος καθώς περιμένει να πλησιάσει σε αυτόν, ένας κινητός κόμβος για να στείλει τα δεδομένα του ο στατικός στον κινητό κόμβο. Όταν ο στατικός κόμβος είναι συνεχώς ενεργοποιημένος, τότε εξαντλείται πιο γρήγορα η ενέργεια του. Για αυτό πρέπει να προβλέπονται κάποιοι χρόνοι που ο στατικός κόμβος μεταβαίνει στην κατάσταση sleep mode και κάποιοι χρόνοι που ενεργοποιείται ώστε να στείλει δεδομένα σε έναν κινητό κόμβο. Αυτό γίνεται με μοντέλα πρόβλεψης [37] που προβλέπουν πότε περίπου πλησιάζει ο κινητός κόμβος σε κάθε στατικό κόμβο ώστε σε εκείνο το χρονικό διάστημα να ενεργοποιηθεί ο στατικός κόμβος.

ζ) Η εξάντληση ενέργειας από την μεγάλη απόσταση των κόμβων

Όπως έχουμε αναφέρει σε προηγούμενο κεφάλαιο, ο κάθε κόμβος αισθητήρας (sensor node) αποτελείται από 3 υποσυστήματα που είναι :

- i) Υποσύστημα υπολογισμών
- ii) Υποσύστημα αισθητήρα
- iii) Υποσύστημα επικοινωνιών.

Από τα 3 αυτά υποσυστήματα, μεγαλύτερη ενέργεια τροφοδοσίας καταναλώνει το υποσύστημα επικοινωνιών, διότι χρησιμοποιεί ενέργεια για να μεταδώσει τα δεδομένα σε ασύρματο δίκτυο. Αντίθετα, το υποσύστημα υπολογισμών δεν καταναλώνει πολλή ενέργεια, διότι είναι ένα ολοκληρωμένο κύκλωμα chip που έχει χαμηλή κατανάλωση ενέργειας. Για το υποσύστημα επικοινωνιών, η μεγάλη απόσταση της μετάδοσης δεδομένων από έναν στατικό κόμβο στον κεντρικό κόμβο sink, είναι αιτία μεγαλύτερης κατανάλωσης ενέργειας. Για να μειωθεί η απόσταση εκπομπής, και έτσι να καταναλωθεί λιγότερη ενέργεια, χρησιμοποιείται το στατικό δίκτυο πλέγματος και η δρομολόγηση γίνεται μέσω πολλαπλών αλμάτων (multihop routing). Με τον τρόπο αυτό, κάθε στατικός απομακρυσμένος κόμβος από τον sink μεταδίδει τα δεδομένα πρώτα στον γειτονικό του κόμβο που βρίσκεται σε κοντινή απόσταση, και μετά σταδιακά φτάνουν τα δεδομένα στον sink από τους απομακρυσμένους κόμβους με πολλαπλά άλματα. Έτσι ο κάθε απομακρυσμένος κόμβος αισθητήρας δεν ξοδεύει μεγάλη ενέργεια για να στείλει δεδομένα απευθείας στον sink αλλά ξοδεύει λιγότερη ενέργεια για να στείλει δεδομένα σε έναν γειτονικό κόμβο.

Όμως, σε ένα στατικό δίκτυο, όταν ο κόμβος αισθητήρας βρίσκεται σε απομακρυσμένη τοποθεσία τότε τα δεδομένα κινούνται μέσω πολλών κόμβων για να φτάσουν στον sink και έτσι υπάρχει μία καθυστέρηση (delay). Για να λυθεί αυτό το πρόβλημα εισάγεται η κινητικότητα των κόμβων. Ένας ή περισσότεροι κόμβοι είναι κινητοί και επισκέπτονται τους στατικούς κόμβους και τότε ο στατικός κόμβος στέλνει τα δεδομένα στον κινητό κόμβο που βρίσκεται κοντά του με ένα μόνο άλμα (one-hop). Με τον τρόπο αυτό, μειώνεται και η απόσταση στην οποία στέλνει τα δεδομένα ο στατικός κόμβος, αλλά μειώνεται και το πλήθος αλμάτων που απαιτούνται για να φτάσουν τα δεδομένα στο sink. Ανάλογα με το σενάριο κινητικότητας που χρησιμοποιείται, ο κινητός κόμβος μπορεί να είναι ο ίδιος ο sink, ή να υπάρχει ένα πλήθος κινητών κόμβων που λέγονται data MULEs οι οποίοι συλλέγουν τα δεδομένα από όλους τους κόμβους και τα μεταφέρουν στον sink.

η) Μεγάλη εξάντληση της ενέργειας των στατικών κόμβων αισθητήρων που βρίσκονται γειτονικά σε κόμβους sinks.

Το πρόβλημα αυτό λέγεται και «sink neighbours problem» [38] ή αλλιώς λέγεται «energy sink-hole problem». Παρατηρείται συνήθως σε στατικά ασύρματα δίκτυα αισθητήρων. Οι στατικοί κόμβοι αισθητήρες που βρίσκονται κοντά στους sinks, έχουν μεγαλύτερη απώλεια ενέργειας από ότι οι υπόλοιποι κόμβοι του δικτύου. Αυτό συμβαίνει διότι σε μία δρομολόγηση πολλαπλών αλμάτων, οι γειτονικοί κόμβοι του sink επιβαρύνονται περισσότερο ενεργειακά καθώς μεταδίδουν δικά τους δεδομένα στον sink, αλλά δρομολογούν και δεδομένα που προέρχονται από όλους τους άλλους κόμβους και τα μεταδίδουν στον sink. Επιπλέον, δρομολογούν και τα δεδομένα που στέλνει ο sink σε κόμβους αισθητήρες. Αντίθετα, άλλοι κόμβοι του δικτύου δεν μεταδίδουν τόσο συχνά δεδομένα και έτσι η παραμένουσα ενέργεια (node residual energy) είναι μεγαλύτερη σε αυτούς τους κόμβους. Το πρόβλημα αυτό έχει το αποτέλεσμα, να εξαντλείται η ενέργεια σε κόμβους γύρω από τον sink, και να σβήνουν πιο σύντομα. Τότε ο sink αποσυνδέεται από το υπόλοιπο δίκτυο και δεν μπορεί να λάβει άλλα δεδομένα από το δίκτυο. Αυτό το πρόβλημα δείχνει ότι δεν είναι αποτελεσματικός ο χρόνος ζωής του δικτύου, διότι όταν αποκόβεται ο sink από το δίκτυο, είναι σαν να τελειώνει η διάρκεια ζωής του δικτύου παρόλο που κάποιοι κόμβοι λειτουργούν ακόμη. Επιπλέον δείχνει ανομοιόμορφη κατανομή ενέργειας συνολικά στο δίκτυο. Ακόμα και αν ο στατικός sink βρίσκεται στην βέλτιστη θέση του που είναι το κέντρο της περιοχής του πεδίου αισθητήρων, πάλι η ενέργεια των κόμβων γύρω από τον sink εξαντλείται πιο γρήγορα.

Για να δοθεί λύση σε αυτό το πρόβλημα χρησιμοποιείται ο κινητός sink ή οι κινητοί sinks.

Όταν κινείται ο sink, οι κόμβοι αισθητήρες που βρίσκονται γύρω από τον κινητό sink δεν είναι πάντα οι ίδιοι αλλά κάθε τόσο αλλάζουν οι κόμβοι που αναμεταδίδουν δεδομένα και έτσι η ενέργεια των κόμβων εξαντλείται για όλους τους κόμβους ομοιόμορφα και διαρκεί περισσότερο.

Διάφορες λύσεις για το πρόβλημα αυτό, που χρησιμοποιούν κινητό sink ή κινητούς sinks παρουσιάζονται στην επόμενη παράγραφο που αναφέρεται σε διαφορετικά μοντέλα κινητικότητας.

4.2.3. Μοντέλα κινητικότητας

Επειδή το θέμα της κινητικότητας προκαλεί μεγάλο ενδιαφέρον στους ερευνητές, έχουν γίνει πολλές προτάσεις για μοντέλα κινητικότητας στα ασύρματα δίκτυα αισθητήρων που είναι αρκετά διαφορετικές μεταξύ τους. Στην παρούσα παράγραφο δεν μπορούμε να αναλύσουμε εκτεταμένα, όλα τα μοντέλα που υπάρχουν, αλλά παρουσιάσουμε μερικά από αυτά που θεωρούνται σημαντικά χωρίς αυτό να σημαίνει ότι αν υπάρχουν άλλα μοντέλα κινητικότητας που δεν αναφέρονται εδώ, είναι λιγότερο χρήσιμα.

Τα μοντέλα κινητικότητας (mobility models) αντιπροσωπεύουν την κίνηση των κινητών κόμβων αισθητήρων.

Τα μοντέλα κινητικότητας μπορούν να κατηγοριοποιηθούν σε : [37]

α) ομογενή μοντέλα κινητικότητας.

Τα ομογενή μοντέλα κινητικότητας έχουν ένα σύνολο από κινητούς κόμβους που χωρίζονται σε ομάδες και κάθε ομάδα ακολουθεί το ίδιο μοντέλο κινητικότητας.

Αυτά τα μοντέλα μπορούν να χρησιμοποιούνται ακόμα και αν χρειαστεί να γίνουν αλλαγές στην τοπολογία του δικτύου, διότι μπορούν να πετύχουν καλύτερη κάλυψη και συνδεσιμότητα στο περιβάλλον που τοποθετούνται.

β) ετερογενή μοντέλα κινητικότητας.

Τα ετερογενή μοντέλα κινητικότητας συνήθως έχουν μόνο έναν κινητό κόμβο, για παράδειγμα τον κινητό κόμβο sink, που κινείται σύμφωνα με ένα υιοθετημένο μοντέλο κινητικότητας μέσα στο δίκτυο και συλλέγει δεδομένα από τους στατικούς κόμβους. Αν υπάρχουν περισσότεροι κινητοί κόμβοι, τότε ο κάθε κόμβος κινείται ξεχωριστά από τους άλλους χωρίς η κίνηση του ενός κόμβου να εξαρτάται από την κίνηση του άλλου.

Έτσι τα ετερογενή μοντέλα κινητικότητας χρησιμοποιούνται είτε σε περιπτώσεις που υπάρχει ένας μόνο κινητός κόμβος sink, ή υπάρχουν περισσότεροι κινητοί sink.

Κάθε μοντέλο κινητικότητας που προτείνεται, προσπαθεί με δικό του τρόπο να δώσει λύσεις στα βασικά προβλήματα της κινητικότητας.

Ένα μοντέλο κινητικότητας εξηγεί πως αλλάζει στη διάρκεια του χρόνου η θέση (location), η κατεύθυνση (direction) η ταχύτητα (velocity) και η επιτάχυνση (acceleration) των κινητών κόμβων. Αυτοί οι παράμετροι χαρακτηρίζουν την κινητικότητα ενός κινητού κόμβου.

Σε όλα τα μοντέλα κινητικότητας υπάρχει ένα σύνολο από στατικούς κόμβους αισθητήρες (static sensor nodes) και ένα σύνολο από κινητούς κόμβους (mobile nodes) που κινούνται μέσα στο χώρο της εγκατάστασης και συλλέγουν τα δεδομένα από τους στατικούς κόμβους.

Κάποια μοντέλα κινητικότητας έχουν μόνο έναν κινητό κόμβο π.χ. μόνο τον κινητό κόμβο sink και όλοι οι άλλοι κόμβοι είναι στατικοί. Άλλα μοντέλα κινητικότητας έχουν περισσότερους κινητούς κόμβους στο δίκτυο. Τέτοια μοντέλα μπορούν να έχουν από 2 κόμβους μέχρι ένα ολόκληρο δίκτυο αισθητήρων από κινητούς κόμβους αισθητήρες που κινούνται στην περιοχή της εφαρμογής με στόχο να πετύχουν την βέλτιστη κάλυψη και την συνδεσιμότητα. [37]

Η κίνηση των κόμβων (mobile nodes) σε κάποιες περιπτώσεις μπορεί να γίνεται σε ευθείες τροχιές. Σε άλλες περιπτώσεις, η τροχιά είναι τυχαία ενώ σε άλλες περιπτώσεις η τροχιά είναι ελεγχόμενη με βάση κάποιο χάρτη ή κάποιο γράφημα.

Επιπλέον, οι κινητοί κόμβοι μπορούν να κινούνται είτε ο καθένας μεμονωμένα σε μία δική του τροχιά, είτε να χωρίζονται σε ομάδες, ώστε κάθε ομάδα κόμβων κινείται στην ίδια τροχιά.

4.2.3.1 Χρήση των μοντέλων κινητικότητας σε εξομοιώσεις (simulations)

Οι μορφές κινητικότητας που χρησιμοποιούνται έχουν επιπτώσεις στην απόδοση του πρωτοκόλλου. Τα μοντέλα κινητικότητας προσπαθούν να μιμηθούν τις μορφές κίνησης που έχουν οι κόμβοι σε πραγματικές εφαρμογές. Μέσω του κάθε μοντέλου κινητικότητας γίνεται μία εξομοίωση (simulation) που περιγράφει τη μορφή κινητικότητας που χρησιμοποιείται στο πραγματικό δίκτυο.

Υπάρχουν δύο διαφορετικές μορφές εξομοίωσης (simulation schemes) [37].

α) Η πρώτη μορφή εξομοίωσης είναι βασισμένη σε συλλογή πληροφοριών από πραγματικά δίκτυα. Συλλέγονται πληροφορίες για τις τροχιές των κόμβων σε πραγματικά δίκτυα και μετά οι πληροφορίες αυτές χρησιμοποιούνται στις εξομοιώσεις (simulations).

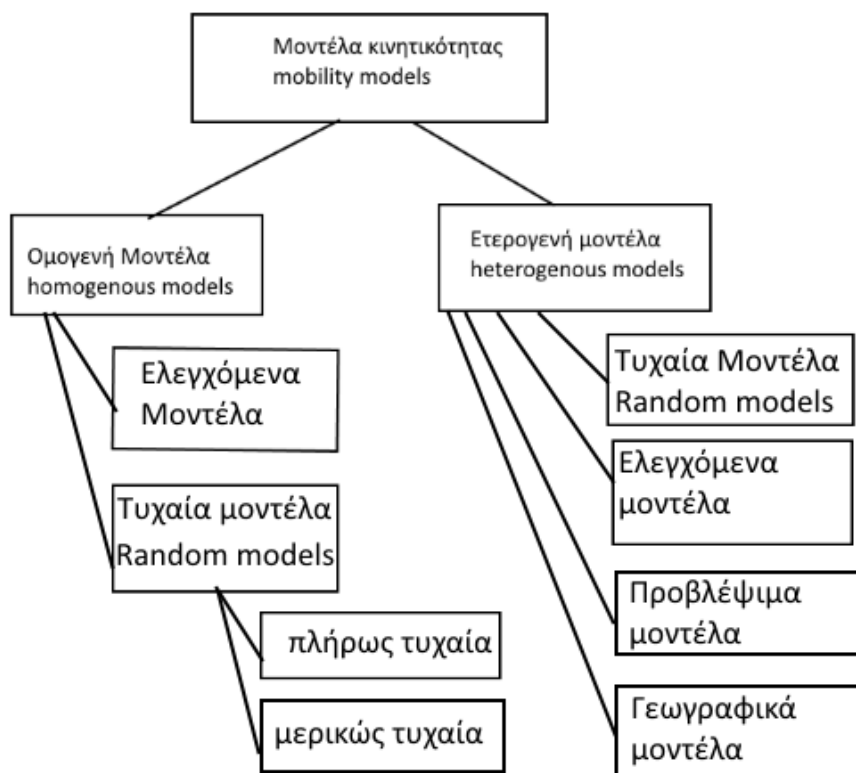
β) Η δεύτερη μορφή εξομοίωσης βασίζεται σε καθορισμένους κανόνες (rules) που διέπουν την κινητικότητα, για παράδειγμα, με ένα σύνολο από εξισώσεις υπολογίζονται οι πιθανές θέσεις που μπορούν να βρίσκονται οι κινητοί κόμβοι.

Και οι δύο αυτές μέθοδοι δεν επαρκούν πλήρως για να μοντελοποιηθούν τα πραγματικά δίκτυα και έτσι οι προσομοιώσεις που βασίζονται στα μοντέλα κινητικότητας να μην είναι έγκυρες μέχρι ένα βαθμό, αλλά δεν μπορεί να υπάρξει πλήρης ακρίβεια.

4.2.3.2 Κατηγορίες των μοντέλων κινητικότητας

Υπάρχουν δύο βασικές κατηγορίες των μοντέλων κινητικότητας που είναι τα ομογενή μοντέλα και τα ετερογενή μοντέλα και κάθε μία από αυτές χωρίζεται σε υποκατηγορίες. [37]

Οι 2 βασικές κατηγορίες και οι υποκατηγορίες φαίνονται στην παρακάτω εικόνα:



Εικόνα 115. Μοντέλα κινητικότητας.

α) Τα ομογενή μοντέλα κινητικότητας.

Έχουν ένα σύνολο κινητών κόμβων (mobile nodes) οι οποίοι συνεργάζονται μεταξύ τους και κινούνται όλοι μαζί, συχνά σε ομάδες, με το ίδιο μοντέλο κινητικότητας μέσα στην περιοχή της εγκατάστασης.

Σε τέτοια μοντέλα το πλήθος των κινητών κόμβων μπορεί να κυμαίνεται από ένα μικρό σύνολο κόμβων, μέχρι ένα ολόκληρο ασύρματο δίκτυο αισθητήρων, όπου όλοι οι κόμβοι είναι κινητοί.

Τα ομογενή μοντέλα κινητικότητας χωρίζονται σε 2 υποκατηγορίες:

1. Τα μοντέλα τυχαίας κινητικότητας που διακρίνονται σε μοντέλα με μερικώς τυχαία και πλήρως τυχαία κινητικότητα. Οι δύο αυτές κατηγορίες περιγράφονται παρακάτω:

i. Στα μοντέλα μερικώς τυχαίας κινητικότητας, όλοι οι κόμβοι εξαρτώνται ο ένας από τον άλλον για να ορίσουν την κατεύθυνση της κίνησης (direction).

Τέτοια μοντέλα είναι το μοντέλο ομάδας σημείων αναφοράς (reference point group mobility model)(RPGM)

και το μοντέλο καταδίωξης (pursue mobility model) που αναφέρονται παρακάτω.

ii. Στα μοντέλα πλήρως τυχαίας κινητικότητας, η ομάδα των κινητών κόμβων κινείται προς μία τυχαία κατεύθυνση (direction) που αλλάζει περιοδικά.

Τέτοια μοντέλα είναι το Νομαδικό μοντέλο (nomadic mobility model), το μοντέλο ιδεατής διαδρομής (virtual track-based mobility model) που παρουσιάζονται παρακάτω. Στα μοντέλα πλήρως τυχαίας κινητικότητας οι ομάδες των κινητών κόμβων στην ουσία κινούνται τυχαία μέσα στο περιβάλλον που εγκαθίστανται

Τα μοντέλα τυχαίας κινητικότητας είναι κατάλληλα για να χρησιμοποιούνται όταν δεν υπάρχει η απαίτηση να προσομοιωθεί η συμπεριφορά ανθρώπων, ζώων, ή οχημάτων που κινούνται στο χώρο. Επίσης χρησιμοποιούνται σε περιπτώσεις που δεν απαιτείται να συλλέγονται πληροφορίες για την χρονική εξάρτηση της ταχύτητας (δηλαδή τιμές ταχύτητας σε προηγούμενες χρονικές στιγμές), ούτε απαιτείται να συλλέγουν δεδομένα για τη χωρική εξάρτηση της ταχύτητας. Επίσης στα μοντέλα τυχαίας κινητικότητας δεν υπάρχουν γεωγραφικοί περιορισμοί στην κίνηση των κόμβων.

2. Τα μοντέλα ελεγχόμενης κινητικότητας.

Τα μοντέλα ελεγχόμενης κινητικότητας μπορούν να χρησιμοποιούνται σε περιπτώσεις που οι κινητοί κόμβοι απαιτείται να περιορίζονται στην περιοχή εφαρμογής του δικτύου, και η κίνηση των κόμβων έχει πολλούς περιορισμούς, που οφείλονται σε ιδιότητες του περιβάλλοντος, όπως εμπόδια, σταθερές διαδρομές μετακίνησης κλπ.

β) Τα ετερογενή μοντέλα κινητικότητας.

Στα ετερογενή μοντέλα κινητικότητας υπάρχει ένας κινητός κόμβος που κινείται ανεξάρτητα από όλους τους άλλους κινητούς κόμβους που μπορεί να υπάρχουν στο δίκτυο. Αν υπάρχουν και άλλοι κινητοί κόμβοι, τότε ο κάθε κόμβος υιοθετεί το δικό του μοντέλο κινητικότητας και δεν πηγαίνει σε άλλες θέσεις που ορίζουν τα μοντέλα κινητικότητας άλλων κόμβων.

Τα ετερογενή μοντέλα κινητικότητας χωρίζονται σε 4 υποκατηγορίες:

1. Μοντέλα τυχαίας κινητικότητας

Σε αυτά ανήκει το μοντέλο Random Way Point Mobility Model και το μοντέλο Gauss Markov που παρουσιάζονται παρακάτω.

2. Μοντέλα ελεγχόμενης κινητικότητας

Ο κινητός κόμβος κινείται με ένα προκαθορισμένο χρονικό πρόγραμμα (schedule) που δημιουργείται λαμβάνοντας υπόψη τον ρυθμό δειγματοληψίας των κόμβων αισθητήρων και τον ρυθμό συμβάντων ώστε ο κινητός κόμβος να επισκέπτεται τους κόμβους σε κατάλληλες στιγμές και να αποφεύγεται η υπερχείλιση ενδιάμεσης μνήμης (buffer overflow).

3. Μοντέλα προβλεπόμενης κινητικότητας

Σε αυτά τα μοντέλα οι στατικοί κόμβοι μπαίνουν σε κατάσταση sleep ή σε κατάσταση εξοικονόμησης ενέργειας για κάποιες χρονικές περιόδους, όταν δεν αναμένεται ο κινητός κόμβος να βρίσκεται στη περιοχή κοντά στο στατικό κόμβο. Ενώ οι στατικοί κόμβοι μεταβαίνουν σε κατάσταση ενεργοποίησης όταν αναμένεται να βρίσκεται ο κινητός κόμβος κοντά τους και ξεκινούν να στέλνουν τα δεδομένα τους. Μία μέθοδος για να επιτυγχάνεται η πρόβλεψη θέσης του κινητού κόμβου κάθε στιγμή, είναι όταν οι κόμβοι γνωρίζουν από πριν την τροχιά του κινητού κόμβου ο οποίος κινείται σε προκαθορισμένες θέσεις.

Μία άλλη μέθοδος είναι η χρήση στατιστικής που δείχνει σε ποιες θέσεις κινείται ο κόμβος συνήθως. Τα μοντέλα πρόβλεψης χρησιμοποιούνται για να γίνεται μία εξοικονόμηση στην ενέργεια που καταναλώνουν οι κινητοί κόμβοι αισθητήρες επειδή τακτικά αλλάζουν κατάσταση από ενεργοί σε αδρανείς και έτσι διατηρούν για περισσότερο χρόνο την ενέργεια τους.

4. Μοντέλα γεωγραφικής κινητικότητας.

Είναι μοντέλα ελεγχόμενης κινητικότητας όπου η κίνηση των κόμβων είναι αυστηρά περιορισμένη με βάση τη γεωγραφική μορφολογία του περιβάλλοντος.

Συνήθως σε αυτά τα μοντέλα υπάρχουν λίγοι κινητοί κόμβοι και πολλοί στατικοί,

δηλαδή υπάρχει ένας ή περισσότεροι κινητοί sinks που κινούνται σε συγκεκριμένα σημεία σε έναν χάρτη. Ο κινητός κόμβος ακολουθεί προκαθορισμένες διαδρομές με βάση ένα χάρτη ή ένα γράφημα που αντιπροσωπεύει τη γεωγραφική περιοχή. Ο κινητός κόμβος λαμβάνει υπόψη τα εμπόδια που υπάρχουν και τα σύνορα της περιοχής που καλύπτει ώστε όταν βρίσκεται στα όρια αλλάζει την κατεύθυνση του και κινείται μέσα στην περιοχή.

Μια άλλη ταξινόμηση των μοντέλων κινητικότητας σε 3 κατηγορίες, μπορεί να γίνει αν υπάρχει ο κινητός κόμβος Sink ή αν υπάρχουν οι κινητοί κόμβοι data MULEs.

Αυτά τα μοντέλα χωρίζονται σε: [35]

α) Μοντέλα κινητικότητας με κινητό σταθμό βάσης (Mobile base station, MBC).

Σε αυτές τις λύσεις κινητικότητας, υπάρχει ένας κινητός σταθμός βάσης MBC, που είναι συνήθως ο κινητός κόμβος sink ο οποίος κινείται και αλλάζει τη θέση του μέσα στην εγκατάσταση. Υπάρχουν και οι στατικοί κόμβοι αισθητήρες που τους επισκέπτεται ο κινητός sink. Οι κόμβοι αισθητήρες, διαθέτουν μία ενδιάμεση μνήμη απομόνωσης buffer και σε αυτή αποθηκεύουν σε μία ουρά τα δεδομένα τους αλλά μόνο για μικρό χρονικό διάστημα και όταν τους επισκέπτεται ο κινητός sink στέλνουν σε αυτόν τα δεδομένα τους.

β) Μοντέλα κινητικότητας με κινητό συλλέκτη δεδομένων (Mobile data collector MDC).

Στις λύσεις κινητικότητας με κινητό συλλέκτη δεδομένων MDC, ο κινητός κόμβος είναι πάλι ένας κινητός Sink που επισκέπτεται τους στατικούς αισθητήρες, αλλά τώρα οι κόμβοι αισθητήρες διατηρούν στην ενδιάμεση μνήμη αποθήκευσης buffer τους για περισσότερο χρόνο τα δεδομένα. Τότε ο κινητός sink που επισκέπτεται τους κόμβους αποθηκεύει τα δεδομένα τους με μία ασύρματη μετάδοση ενός άλματος.

γ) Μοντέλα κινητικότητας που βασίζονται σε ραντεβού.

Αυτά τα μοντέλα, είναι υβριδικά. Τότε υπάρχουν επιπλέον κάποιοι κόμβοι που λέγονται Σημεία ραντεβού (Rendezvous points). Σε κάθε ομάδα στατικών κόμβων που είναι τοποθετημένοι σε δίκτυο πλέγματος, αντιστοιχεί ένα Σημείο Ραντεβού, όπου όλοι οι στατικοί κόμβοι της ομάδας στέλνουν τα δεδομένα τους. Υπάρχουν επίσης οι κινητοί κόμβοι sinks που κινούνται σε μία συγκεκριμένη τροχιά αλλά δεν περνούν από όλους τους κόμβους. Οι κόμβοι Σημεία ραντεβού (Rendezvous points) είναι τοποθετημένοι κοντά στη διαδρομή των κινητών κόμβων sinks. Οι στατικοί κόμβοι στέλνουν τα δεδομένα τους στην ενδιάμεση μνήμη buffer των Σημείων ραντεβού οι οποίοι συγκεντρωτικά αποθηκεύουν δεδομένα από πολλούς κόμβους. Τα δεδομένα παραμένουν αποθηκευμένα στα Σημεία ραντεβού. Όταν ο κινητός κόμβος sink έρθει στην εμβέλεια ενός Σημείου ραντεβού, φορτώνει τα δεδομένα του.

Παρακάτω παρουσιάζονται μερικά γνωστά μοντέλα κινητικότητας που ανήκουν στις κατηγορίες που αναφέρθηκαν προηγουμένως.

4.2.3.3 Μοντέλο Κινητικότητας RPGM Reference Point Group Mobility Model

Το μοντέλο κινητικότητας ομάδας με σημείο αναφοράς επιδεικνύει την χωρική εξάρτηση (spatial dependency). Ανήκει στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι μερικώς τυχαία. Αυτό το μοντέλο αποτελείται από ομάδες κόμβων που συνεργάζονται. Οι κόμβοι σε αυτό το μοντέλο χωρίζονται σε δύο ομάδες. Κάθε ομάδα (group) έχει έναν κόμβο που είναι ο αρχηγός της ομάδας (group leader), ο οποίος είναι αφιερωμένος στην ομάδα και επιπλέον υπάρχει ένα ορισμένο πλήθος άλλων κινητών κόμβων που είναι τα μέλη της ομάδας (members). Σε κάθε ομάδα, ο αρχηγός (leader) κινείται σύμφωνα με το μοντέλο κινητικότητας τυχαίων σημείων διαδρομής (random way point mobility model), το οποίο παρουσιάζεται σε επόμενη παράγραφο. Σύμφωνα με αυτό το μοντέλο, ο αρχηγός (leader) επιλέγει μία κατεύθυνση (direction) τυχαία και έναν προορισμό (destination) και κινείται προς τον προορισμό με μία τυχαία ταχύτητα (velocity). Όταν φτάσει στον προορισμό του, ο αρχηγός σταματάει για ένα χρονικό διάστημα. Μετά επιλέγει έναν νέο προορισμό τυχαία, και ξεκινάει να κινείται προς τον νέο προορισμό με μία τυχαία ταχύτητα (velocity).

Η κίνηση του αρχηγού της ομάδας καθορίζει την συμπεριφορά κινητικότητας ολόκληρης της ομάδας. Οι υπόλοιποι κόμβοι της ομάδας που είναι τα μέλη, ακολουθούν την κίνηση του αρχηγού με κάποια απόκλιση.

Η κίνηση του αρχηγού της ομάδας τη χρονική στιγμή t αντιπροσωπεύεται από το διάνυσμα V_t . Κάθε μέλος σε αυτή την ομάδα αποκλίνει (deviates) σε κάποιο βαθμό από αυτό το διάνυσμα V_t . Σε κάθε κόμβο (node), η κινητικότητα (mobility) ανατίθεται με βάση ένα σημείο αναφοράς (reference point) που ακολουθεί την κίνηση της ομάδας (group movement). Η τυχαία κίνηση (random motion) είναι ανεξάρτητη όμοια κατανομημένη τυχαία διεργασία της οποίας το μήκος κατανέμεται ομοιόμορφα στο διάστημα (interval) $[0, r_{max}]$ όπου r_{max} είναι η μέγιστη επιτρεπτή απόκλιση της απόστασης (maximum allowed distance deviation) και η κατεύθυνση (direction) κατανέμεται ομοιόμορφα στο διάστημα (interval) $[0, 2\pi]$. Επειδή ο αρχηγός της ομάδας (group leader) αποφασίζει κυρίως την κινητικότητα των μελών της ομάδας (group members), η μορφή κινητικότητας της ομάδας (group mobility pattern) αναμένεται ότι θα έχει μεγάλη χωρική εξάρτηση (spatial dependence) για μικρές τιμές της ταχύτητας (speed) και για μικρή αναλογία απόκλισης γωνιών (angle deviation ratio). Ολόκληρο το

πεδίο (field) διαιρείται σε αρκετές γειτονικές περιοχές. Κάθε περιοχή (region) καταλαμβάνεται αποκλειστικά από μία μόνο ομάδα (single group). Ένα παράδειγμα είναι η επικοινωνία στο πεδίο μάχης. Διαφορετικές ομάδες με διαφορετικούς στόχους (tasks) ταξιδεύουν μέσα στο ίδιο πεδίο (field) με έναν τρόπο αλληλοκάλυψης (overlapping manner). Άλλο παράδειγμα εφαρμογής αυτού του μοντέλου είναι η επέμβαση σε καταστροφές.

4.2.3.4 Μοντέλο κινητικότητας καταδίωξης (Pursue Mobility Model)

Το μοντέλο κινητικότητας καταδίωξης (pursue mobility model) ανήκει και αυτό στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι μερικώς τυχαία.

Σε αυτό το μοντέλο κινητικότητας, υπάρχει ένας μεμονωμένος κόμβος που κινείται σύμφωνα με το μοντέλο Random Way Point Mobility Model το οποίο εξηγείται στην επόμενη παράγραφο. Ο κόμβος αυτός είναι ο κόμβος στόχος (target node). Επιπλέον υπάρχουν αρκετοί άλλοι κινητοί κόμβοι αναζητητές (seeker nodes) που προσπαθούν να ανιχνεύσουν (track) και να συλλάβουν τον συγκεκριμένο κινητό κόμβο στόχο (target node). Οι κόμβοι αναζητητές (seeker node) προσπαθούν να συναντήσουν τον κόμβο στόχο (target node) και έτσι κινούνται προς αυτόν με μία ταχύτητα ώστε να διασταυρωθεί η πορεία τους με την τροχιά του.

4.2.3.5 Νομαδικό Μοντέλο Κινητικότητας (Nomadic Mobility Model)

Αυτό το μοντέλο κινητικότητας κατατάσσεται στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι πλήρως τυχαία.

Στο νομαδικό μοντέλο, υπάρχει μία ομάδα κόμβων (group of nodes) που κινείται πλήρως τυχαία από μία κατεύθυνση σε μία άλλη. Μετά, ο κάθε κόμβος ορίζει ένα σημείο αναφοράς (reference point) του με βάση την γενική κίνηση της ομάδας κόμβων. Μέσα στην ομάδα, τοπικά, ο κάθε κόμβος κινείται κοντά στο σημείο αναφοράς του, με μία τυχαία κίνηση, που μοιάζει με την κίνηση μορίων ενός αερίου ή υγρού και ονομάζεται κίνηση “Brown” (Brownian motion). Επίσης υπάρχει ένα αντίστοιχο μαθηματικό μοντέλο που περιγράφει τέτοιες τυχαίες κινήσεις. Το όνομα της κίνησης Brown, προέκυψε από

τον βοτανολόγο Robert Brown, το 1827, που μελετούσε στο μικροσκόπιο κινήσεις σωματιδίων γύρης μέσα σε νερό.

4.2.3.6 Μοντέλο Κινητικότητας βασισμένο σε Ιδεατή διαδρομή (Virtual Track –based Mobility Model)

Το μοντέλο κινητικότητας ιδεατής διαδρομής (Virtual Track –based Mobility Model), ανήκει στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι πλήρως τυχαία.

Σε αυτό το μοντέλο, υπάρχουν κάποιοι στατικοί κεντρικοί κόμβοι που ονομάζονται σταθμοί μεταγωγής (switch stations) και επίσης υπάρχουν και κινητοί κόμβοι που περιφέρονται μέσα στο δίκτυο.

Ο κάθε κινητός κόμβος, καθορίζει όλες τις πιθανές διαδρομές (tracks) που οδηγούν τον ίδιο προς ένα σταθμό μεταγωγής (switch station). Μετά, ο κάθε κινητός κόμβος, επιλέγει τυχαία και ακολουθεί μία από αυτές τις διαδρομές (tracks) και συνεχίζει να την ακολουθεί μέχρι να φτάσει στον τελικό προορισμό του, που είναι ένας συγκεκριμένος σταθμός μεταγωγής (switch station) στον οποίο καταλήγει η διαδρομή. Η κινητικότητα μίας ομάδας κόμβων (group mobility) καθορίζεται από το ποιος είναι ο σταθμός μεταγωγής (switch station) που επιλέγουν ως προορισμό τους οι κινητοί κόμβοι. Έτσι, οι κόμβοι χωρίζονται σε ομάδες και κάθε ομάδα κατευθύνεται προς τον ίδιο σταθμό μεταγωγής (switch station). Όλοι οι σταθμοί μεταγωγής (switch stations) που υπάρχουν στο δίκτυο, συνδέονται μεταξύ τους με πολλαπλές ιδεατές διαδρομές (virtual tracks).

4.2.3.7 Μοντέλο Κινητικότητας ομάδας με ταχύτητα αναφοράς (Reference Velocity Group Mobility Model)

Το μοντέλο κινητικότητας αυτό, ανήκει στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι πλήρως τυχαία.

Σε αυτό το μοντέλο οι κινητοί κόμβοι χωρίζονται σε ομάδες.

Ο κάθε κινητός κόμβος που βρίσκεται μέσα σε μία ομάδα, κινείται με βάση ένα σύνολο από εξισώσεις. Οι εξισώσεις αυτές συνδέουν την κίνηση του κάθε κινητού κόμβου, με τις

θέσεις (positions) που βρίσκεται ένα υποσύνολο άλλων κόμβων οι οποίοι είναι μέλη της ίδιας ομάδας.

4.2.3.8 Μοντέλο Κινητικότητας δομημένης ομάδας (Structured Group Mobility Model)

Το μοντέλο κινητικότητας δομημένης ομάδας, ανήκει επίσης στην κατηγορία: ομογενή μοντέλα κινητικότητας που είναι πλήρως τυχαία.

Οι κινητοί κόμβοι βρίσκονται χωρισμένοι σε ομάδες.

Και σε αυτό το μοντέλο κινητικότητας χρησιμοποιείται ένα σύνολο εξισώσεων για να καθορίζει την κίνηση των ομάδων. Η κίνηση κάθε κόμβου καθορίζεται από τις εξισώσεις, στις οποίες λαμβάνονται υπόψη οι θέσεις των άλλων κόμβων που βρίσκονται στην ίδια ομάδα.

4.2.3.9 Μοντέλο Κινητικότητας Στήλης (Column Mobility Model)

Το μοντέλο κινητικότητας στήλης (column mobility model) ανήκει στην κατηγορία: ομογενή μοντέλα ελεγχόμενης κινητικότητας.

Σε αυτό το μοντέλο κινητικότητας υπάρχει ένα σύνολο κόμβων που κινείται προς μία ορισμένη κατεύθυνση (direction). Κάθε κινητός κόμβος έχει ένα σημείο αναφοράς (reference point). Σε κάθε χρονική σχισμή (time slot), το σημείο αναφοράς του κάθε κινητού κόμβου αλλάζει και ενημερώνεται (updated). Η αλλαγή γίνεται από τον ίδιο τον κινητό κόμβο που προσθέτει μία προκαθορισμένη μετατόπιση (predefined offset) στο δικό του σημείο αναφοράς (reference point).

Αν ένας κινητός κόμβος φτάσει στα σύνορα της περιοχής μέσα στην οποία πρέπει να κινείται, τότε αλλάζει την κατεύθυνση του (direction) κατά 180 μοίρες και κινείται προς την αντίθετη κατεύθυνση. Με αυτό τον τρόπο παραμένει συνεχώς μέσα στα όρια μίας συγκεκριμένης περιοχής. Μία εφαρμογή αυτού του μοντέλου κινητικότητας είναι η σάρωση περιοχής και αναζήτηση αντικειμένων, όπως είναι σε ένα ναρκοπέδιο, η αναζήτηση και εξουδετέρωση ναρκών.

4.2.3.10 Μοντέλο Κινητικότητας Εξαναγκασμού Ομάδας (Group Force Mobility Model)

Και το μοντέλο αυτό ανήκει στην κατηγορία: ομογενή μοντέλα ελεγχόμενης κινητικότητας.

Στο μοντέλο κινητικότητας εξαναγκασμού ομάδας, μία ομάδα κόμβων κινείται με βάση ένα κοινό χαρακτηριστικό στοιχείο στην κίνησή τους ή ένα κοινό περιορισμό, δηλαδή όλοι οι κόμβοι έχουν ένα κοινό στόχο, είτε έχουν την ίδια κατεύθυνση (direction), είτε έχουν την ίδια ταχύτητα (velocity).

Σε αυτό το μοντέλο, οι ομάδες κινητών κόμβων διακρίνονται σε δύο τύπους, που είναι οι σφικτές ομάδες (tight groups) και οι χαλαρές ομάδες (loose groups). Σε μία σφικτή ομάδα (tight group) οι κόμβοι κινούνται αλληλένδετα μεταξύ τους και η κίνησή τους είναι στενά συνδεδεμένη.

Σε μία χαλαρή ομάδα (loose group) όλοι οι κόμβοι έχουν έναν ίδιο συντελεστή όπως είναι η ίδια κατεύθυνση (direction) ή έχουν έναν περιορισμό να βρίσκονται περιοδικά ο ένας σε συγκεκριμένη απόσταση από τον άλλο (range). Σε αυτή την ομάδα όλοι οι κόμβοι κινούνται ανεξάρτητα ο ένας από τον άλλο με μία τυχαία κίνηση, αλλά έχουν έναν κοινό στόχο ή έναν κοινό περιορισμό.

4.2.3.11 Μοντέλο Κινητικότητας ομάδας αυτό-παλινδρόμησης (Auto-Regressive Group Mobility Model)

Το μοντέλο κινητικότητας ομάδας αυτό-παλινδρόμησης κατατάσσεται στην κατηγορία: ομογενή μοντέλα ελεγχόμενης κινητικότητας. Είναι ένα σύνθετο μοντέλο που η αρχιτεκτονική του στηρίζεται σε δύο επίπεδα (2-tier composite model). Στο 1^ο επίπεδο (tier) οι μεμονωμένοι κινητοί κόμβοι έχουν μία κίνηση που μοντελοποιείται με βάση το μοντέλο αυτό-παλινδρόμησης.

Στο 2^ο επίπεδο (tier) συλλαμβάνεται μία συμπεριφορά κινητικότητας ομάδας. Η κινητικότητα ομάδας βασίζεται στην συσχέτιση (correlation) της κινητικότητας των κόμβων. Η παρουσία μιας ομάδας ανιχνεύεται αν εκτελεστεί ένας έλεγχος του δείκτη συσχέτισης (correlation index test) στις καταστάσεις κινητικότητας (mobility states) των κόμβων (nodes).

Σε αυτό το μοντέλο παρέχεται και μία μορφή ελέγχου για να γίνει εκτίμηση της κινητικότητας σε μία ομάδα (group based mobility).

Από μία ομάδα επιλέγεται ένας αντιπροσωπευτικός κόμβος (representative node) και ελέγχεται η κατάσταση κινητικότητας του (mobility state).

Αυτή η κατάσταση κινητικότητας των αντιπροσωπευτικών κόμβων χρησιμοποιείται για να γίνει εκτίμηση της κατάστασης κινητικότητας όλων των μελών της ομάδας.

4.2.3.12 Μοντέλο Κινητικότητας με βάση την κάλυψη (Coverage Oriented Mobility Model)

Το μοντέλο κινητικότητας με βάση την κάλυψη ανήκει στην κατηγορία: ομογενή μοντέλα ελεγχόμενης κινητικότητας.

Σε αυτό το μοντέλο ελέγχεται ποια περιοχή έχει την χαμηλότερη κάλυψη (lowest coverage) μέσα στη γειτονιά του κάθε κόμβου. Μετά οι κινητοί κόμβοι κινούνται προς την περιοχή με την χαμηλότερη κάλυψη.

4.2.3.13 Μοντέλο κινητικότητας Τυχαίων σημείων διαδρομής (Random Way Point Mobility Model)

Αυτό το μοντέλο ανήκει στην κατηγορία: ετερογενή μοντέλα τυχαίας κινητικότητας.

Στο μοντέλο κινητικότητας τυχαίων σημείων διαδρομής (Random Waypoint Mobility Model) γίνεται κίνηση των κόμβων με αλλαγές στην κατεύθυνση τους και στην ταχύτητά τους. Για κάποιους χρόνους ο κινητός κόμβος σταματά (pause times). Η συνολική κίνηση του κόμβου διαιρείται σε περιόδους κίνησης (motion periods) και σε περιόδους παύσης (pause periods).

Στην περίοδο κίνησης ο κινητός κόμβος (Mobile Node) (MN) επιλέγει μία τυχαία κατεύθυνση (direction) και κινείται προς αυτή με μία τυχαία ταχύτητα (velocity) για να φτάσει σε μία συγκεκριμένη θέση (location).

Όταν φτάσει εκεί ο κινητός κόμβος σταματάει και παραμένει σε αυτή την τοποθεσία (location) για κάποιο χρονικό διάστημα που λέγεται περίοδος παύσης (pause period). Μετά ο κινητός κόμβος MN επιλέγει τυχαία έναν νέο προορισμό.

προορισμό destination(x, y) στην περιοχή προσομοίωσης με παραμέτρους όπως είναι μία ταχύτητα speed με τιμές στο διάστημα $[0, V_{max}]$, χρόνο παύσης pause time με τιμές στο διάστημα $[P_{min}, P_{max}]$ οι οποίες είναι κατανομημένες ομοιόμορφα. Ο κινητός κόμβος MN μετά κινείται προς τον νέο προορισμό που έχει επιλέξει με την επιλεγμένη ταχύτητα. Όταν φτάσει στον προορισμό του, ο κινητός κόμβος MN κάνει μία παύση και σταματάει για συγκεκριμένο χρονικό διάστημα που είναι ίδιο με το χρόνο που είχε σταματήσει στην προηγούμενη θέση του. Μετά ξαναρχίζει την ίδια διαδικασία. Η τιμή του χρόνου παύσης (pause time) και η τιμή της ταχύτητας (velocity) σχετίζονται μεταξύ τους. Ο κόμβοι που έχουν γρήγορη ταχύτητα και μεγάλους χρόνους παύσης δημιουργούν ένα πιο σταθερό δίκτυο. Αν οι κόμβοι κινούνται με μικρές ταχύτητες και έχουν μικρούς χρόνους παύσης τότε το δίκτυο είναι λιγότερο σταθερό. Το ζήτημα που προκύπτει είναι αν οι κόμβοι πρέπει να κινηθούν περισσότερο στην κεντρική περιοχή της τοπολογίας του δικτύου ή αν θα πρέπει να κινηθούν κοντά στα σύνορα της περιοχής. Παρόλο που το μοντέλο τυχαίων σημείων διαδρομής χρησιμοποιείται σε μελέτες προσομοιώσεων, λείπει μία βασική κατανόηση για τα θεωρητικά του χαρακτηριστικά. Οι ερευνητές ερευνούν τις στοχαστικές του ιδιότητες όπως την κατανομή πιθανότητας ή το μέγεθος χρόνου μεταβάσεων (transition length) και του χρόνου μετάβασης για κάθε χρονική περίοδο epoch. Άλλο πρόβλημα του μοντέλου αυτού είναι ότι έχει μία κακή επιλογή στην κατανομή της ταχύτητας και στην ομοιόμορφη κατανομή.

4.2.3.14 Μοντέλο Κινητικότητας Τυχαίας Κατεύθυνσης (Random Direction Mobility Model)

Αυτό το μοντέλο ανήκει στην κατηγορία: ετερογενή μοντέλα τυχαίας κινητικότητας. Το μοντέλο κινητικότητας τυχαίας κατεύθυνσης θεωρείται ότι είναι το πιο διαδεδομένο στην έρευνα που γίνεται για τις κινητές επικοινωνίες. Και σε αυτό το μοντέλο η συνολική κίνηση του κινητού κόμβου (Mobile Node) (MN) χωρίζεται σε περιόδους κίνησης (motion periods) και σε περιόδους παύσης (pause periods), αλλά οι περίοδοι παύσης είναι προαιρετικές. Η διαφορά του μοντέλου αυτού από το προηγούμενο μοντέλο, είναι ότι ο

κινητός κόμβος, στην περίοδο κίνησης του κινείται μόνο πάνω σε ευθύγραμμα τμήματα και με σταθερή ταχύτητα. Μόλις ο κινητός κόμβος φτάσει στον προορισμό του, κάνει προαιρετικά μία στάση, για ένα συγκεκριμένο χρονικό διάστημα. Μετά επιλέγει έναν νέο προορισμό (destination). Υπάρχουν διάφορες παραλλαγές αυτού του μοντέλου. Σε μία παραλλαγή, ο κινητός κόμβος, μετακινείται μεταξύ κυψελίδων (cells) σε μία τροχιά ευθείας γραμμής και όταν φτάσει στα σύνορα των κυψελίδων μπορεί να αλλάζει την κατεύθυνσή του. Σε άλλη παραλλαγή ο κινητός κόμβος μπορεί να αλλάξει την κατεύθυνσή του οπουδήποτε μέσα στην περιοχή που μετακινείται.

4.2.3.15 Μοντέλο Κινητικότητας Τυχαίου Περιπάτου (Random Walk Mobility Model)

Αυτό το μοντέλο ανήκει στην κατηγορία: ετερογενή μοντέλα τυχαίας κινητικότητας.

Το μοντέλο κινητικότητας τυχαίου περιπάτου (random walk mobility model), είναι βασισμένο σε έναν κινητό κόμβο, mobility mode, που κινείται τυχαία μέσα στην περιοχή εφαρμογής. Το μοντέλο αυτό μιμείται την κίνηση πραγματικών κινητών οντοτήτων στον πραγματικό κόσμο που είναι μη προβλέψιμη.

Ο κινητός κόμβος, επιλέγει μία κατεύθυνση (direction) και κινείται σε αυτή την κατεύθυνση με τυχαία ταχύτητα. Μετά από ένα συγκεκριμένο χρονικό διάστημα, ή όταν έχει διανύσει κάποια συγκεκριμένη απόσταση από την αρχική του θέση, ενώ κινείται προς την επιλεγμένη κατεύθυνση, υπολογίζεται μία νέα κατεύθυνση (direction), με μία νέα ταχύτητα. Η νέα κατεύθυνση και η νέα ταχύτητα υπολογίζονται μέσα από προκαθορισμένα εύρη τιμών. Όταν ο κινητός κόμβος που ακολουθεί μία κατεύθυνση, φτάσει στα σύνορα της περιοχής που πρέπει να κινείται, τότε ανακλάται με μία γωνία που καθορίζεται από την κατεύθυνση που έχει όταν εισέρχεται.

Έχουν γίνει προτάσεις και για άλλα μοντέλα παραλλαγές που βασίζονται σε αυτό το μοντέλο, όπως είναι οι περίπατοι 1-D και 2-D.

4.2.3.16 Μοντέλο Κινητικότητας των Data MULEs

Αυτό το μοντέλο ανήκει στην κατηγορία: ετερογενή μοντέλα τυχαίας κινητικότητας. Βασίζεται σε Data MULES που είναι κινητές οντότητες (mobile entities), που ονομάζονται mobile ubiquitous LAN extensions (MULE). Γενικότερα, οι κινητοί κόμβοι αυτής της περίπτωσης, λέγονται και κινητοί συλλέκτες δεδομένων (Mobile Data Collectors ,MDC).

Οι Data MULEs είναι κινητοί κόμβοι, που κινούνται μέσα στο δίκτυο αισθητήρων με τυχαίο τρόπο. Όταν ένας κινητός κόμβος data MULE φτάσει στην εμβέλεια επικοινωνίας ενός στατικού κόμβου αισθητήρα (sensor node), τότε ο αισθητήρας, στέλνει στον data MULE τα δεδομένα του. Ο data MULE συλλέγει τα δεδομένα από διαφορετικούς κόμβους αισθητήρες και τα μεταφέρει στον κεντρικό κόμβο sink.

Σε κάποια σενάρια κινητικότητας, οι data MULEs κινούνται σε ευθείες γραμμές, και ο κάθε data MULE βρίσκεται στην εμβέλεια μιας ομάδας στατικών κόμβων, και συλλέγει δεδομένα μόνο από αυτούς. Η αρχιτεκτονική των MULEs είναι μία αρχιτεκτονική 3 επιπέδων (three-tier architecture).

α) Το επίπεδο βάση (bottom layer)

περιέχει στατικούς ασύρματους αισθητήρες (static wireless sensors) που ευθύνονται για συλλογή δεδομένων από το περιβάλλον. Οι αισθητήρες αυτοί μπορεί να είναι διάσπαρτα τοποθετημένοι στο χώρο με τυχαίο τρόπο, ή να είναι τοποθετημένοι σε συγκεκριμένα σημεία. Αποθηκεύουν τα δεδομένα τους σε μία ενδιάμεση μνήμη απομόνωσης (buffer) και είναι αποθηκευμένα σε μία ουρά queue.

β) Το μεσαίο επίπεδο (middle layer)

έχει κινητές οντότητες (mobile entities) που είναι τα (MULEs) που μετακινούνται στο πεδίο αισθητήρων (sensor field) και συλλέγουν τα δεδομένα αισθητήρων (sensed data) από τους αισθητήρες πηγής (source sensors) όταν βρίσκονται σε εγγύτητα (proximity) και τα παραδίδουν σε σημεία πρόσβασης (access points) όταν βρίσκεται σε κοντινή εμβέλεια (close range). Τα MULEs κινούνται τυχαία ανάμεσα στους αισθητήρες και συλλέγουν τα δεδομένα ευκαιριακά όταν φτάνουν στην εμβέλεια των επικοινωνιών τους. Όταν η τροχιά των MULEs είναι τυχαία υπάρχουν κάποια μειονεκτήματα όπως είναι η καθυστέρηση latency που μπορεί να είναι μεγάλη διότι δεν έχει κάποιο ανώτερο όριο.

Λόγω της καθυστέρησης μπορεί να υπάρχει απώλεια δεδομένων διότι ο MULE δεν προλαβαίνει να συλλέξει τα δεδομένα πριν γεμίσει η ενδιάμεση μνήμη του κόμβου αισθητήρα και έτσι γίνεται μία υπερχείλιση και χάνονται δεδομένα.

γ) Το επίπεδο κορυφή (top layer)

περιλαμβάνει συνδεδεμένες συσκευές που συνδέονται με δίκτυο WAN και σημεία πρόσβασης (access points) και κεντρικά αποθετήρια (central repositories) για ανάλυση των δεδομένων από αισθητήρες (sensed data). Αυτά τα σημεία πρόσβασης (access points) επικοινωνούν με ένα κεντρικό αποθετήριο δεδομένων (central data warehouse) που επιτρέπει να συγχρονιστούν τα δεδομένα που συλλέχθηκαν, να προσδιοριστούν τα δεδομένα πλεονασμού (redundant data) και να έρθει μήνυμα αναγνώρισης (acknowledge) ως απόδειξη λήψης (receipt) για τα δεδομένα που έχουν σταλεί από τα MULEs, ώστε να υπάρχει μία αξιόπιστη μετάδοση δεδομένων (reliable data transmission). Η αρχιτεκτονική των MULE βοηθάει τους αισθητήρες (sensors) να εξοικονομούν την ενέργεια τους όσο περισσότερο γίνεται και έτσι να επεκτείνουν την διάρκεια ζωής τους (lifetime). Επειδή οι αισθητήρες (sensors) επικοινωνούν άμεσα με τους MULEs μέσω διαδρομών χαμηλής εμβέλειας (short-range paths), εξαντλούν την ενέργεια τους αργά και ομοιόμορφα (slowly and uniformly). Επιπλέον η αρχιτεκτονική των MULE έχει χαμηλό κόστος υποδομής (infrastructure cost). Επειδή η επικοινωνία είναι άμεση ανάμεσα στους αισθητήρες πηγές (source sensors) και στους MULEs, δεν υπάρχει routing overhead που μπορεί να εξαντλήσει την ενέργεια των αισθητήρων sensors. Η αρχιτεκτονική MULE architecture είναι ανθεκτική σε σφάλματα (fault tolerant) και πολύ ισχυρή robustness και επεκτάσιμη scalable. Όμως αν αποτύχει ένας κόμβος MULE fails, θα υποβαθμιστεί η απόδοση σε ένα αραιό δίκτυο (sparse network) διότι θα μειωθεί ο ρυθμός επιτυχών δεδομένων decreasing its data success rate και θα αυξηθεί η καθυστέρηση (latency). Για κρίσιμες εφαρμογές ως προς το χρόνο (time-critical applications), η αρχιτεκτονική των MULE μπορεί να εισάγει ανεπιθύμητη καθυστέρηση (undesirable delay) στην αναφορά των δεδομένων από τους αισθητήρες (reporting the sensed data) από τους κόμβους πηγές (source sensors) και έτσι να μην είναι πρακτικοί practical. Ένας τρόπος για να λυθεί αυτό το πρόβλημα είναι να εξοπλίζονται οι MULEs με μία σύνδεση πάντα ανοιχτή (always-on connection) ώστε να δρουν σαν κινητοί sinks (mobile sinks) (δηλ., MULEs και access points).

4.2.3.17 Μοντέλο Κινητικότητας Gauss Markov Mobility Model

Το μοντέλο Gauss Markov ανήκει στα ετερογενή μοντέλα με τυχαία κινητικότητα.

Η κινητικότητα ενός κόμβου (node) χαρακτηρίζεται από την επιτάχυνση (acceleration), την ταχύτητα (velocity) και το ρυθμό αλλαγών κατεύθυνσης (direction) του κόμβου. Οι τιμές σε αυτές τις παραμέτρους επηρεάζονται από διάφορους περιορισμούς. Έτσι ο κάθε κινητός κόμβος (mobile node) έχει μία τρέχουσα ταχύτητα που ενδεχομένως να εξαρτάται από την ταχύτητα που είχε την προηγούμενη χρονική στιγμή. Για αυτό, οι τιμές ταχύτητας ενός κινητού κόμβου σε διαφορετικές χρονικές σχισμές (time slots) συσχετίζονται μεταξύ τους ('correlated'). Μερικά μοντέλα κινητικότητας, όπως είναι το μοντέλο τυχαίου περιπάτου (Random Walk model), το μοντέλο τυχαίων σημείων διαδρομής (Random Way point model) και διάφορες άλλες παραλλαγές τους, δεν έχουν καθόλου χαρακτηριστικά μνήμης για να θυμούνται τις προηγούμενες τιμές ταχύτητας των κινητών κόμβων. Έτσι, τα μοντέλα αυτά είναι ανεπαρκή να συλλάβουν την συμπεριφορά χρονικής εξάρτησης των τιμών ταχύτητας από προηγούμενες τιμές. Στο μοντέλο κινητικότητας Gauss-Markov, η χρονική εξάρτηση (temporal dependency) παίζει έναν σημαντικό ρόλο για να καθορίσει την συμπεριφορά κινητικότητας. Σε αυτό το μοντέλο, υπάρχει μία φάση αρχικοποίησης, στην οποία, σε κάθε κινητό κόμβο (mobile node), δίδεται μία κατεύθυνση (direction) και μία ταχύτητα (speed). Μετά ο χρόνος διαιρείται σε σταθερά χρονικά διαστήματα (fixed time intervals). Σε κάθε χρονικό διάστημα, η κατεύθυνση της κίνησης (direction) και η ταχύτητα (speed) αλλάζουν και ενημερώνονται με νέες τιμές. Ο καθορισμός των νέων τιμών γίνεται με χρήση μίας τυχαίας μεταβλητής και επιπλέον με χρήση της προηγούμενης τιμής που είχαν η κατεύθυνση και η ταχύτητα αντίστοιχα.

Έτσι η τιμή που έχουν η ταχύτητα και η διεύθυνση για τρέχων χρονικό διάστημα n εξαρτώνται από την τιμή που είχε η διεύθυνση και η ταχύτητα για το προηγούμενο χρονικό διάστημα $n-1$.

Ο υπολογισμός γίνεται με χρήση κάποιων εξισώσεων.

Το μοντέλο Gauss Markov προσαρμόζεται σε διαφορετικά επίπεδα τυχειότητας (randomness). Το μοντέλο Gauss Markov έχει χρονική εξάρτηση (temporal dependency) με μία παράμετρο σε επίπεδο μνήμης που ονομάζεται α . Το α είναι μία παράμετρος που αντικατοπτρίζει την τυχειότητα της διεργασίας Gauss-Markov. Η ταχύτητα (velocity) του κινητού κόμβου (mobile node) θεωρείται ότι είναι συσχετισμένη (correlated) στη διάρκεια του χρόνου και μοντελοποιείται ως μία στοχαστική διεργασία (stochastic

process) Gauss Markov. Όταν ο κόμβος πρόκειται να κινηθεί πέρα από τα σύνορα (boundaries) του πεδίου προσομοίωσης, τότε η κατεύθυνση της κίνησης αναγκάζεται να αλλάξει με αναστροφή 180 μοιρών για να παραμείνει ο κινητός κόμβος μέσα στην περιοχή εξομοίωσης.

4.2.3.18 Μοντέλο Κινητικότητας με Κινητούς Πράκτορες (Mobile Agents)

Το μοντέλο αυτό ανήκει στα ετερογενή μοντέλα με ελεγχόμενη κινητικότητα.

Σε ένα μοντέλο με κινητούς πράκτορες όπως είναι το μοντέλο SENMA (Sensor Network with Mobile Agents), υπάρχει ένα σύνολο από στατικούς κόμβους αισθητήρες, ένα σύνολο από κινητούς κόμβους και ένα σύνολο από κινητούς κόμβους με περισσότερους πόρους (resource rich nodes) και μεγαλύτερη επεξεργαστική ισχύ, που λέγονται κινητοί πράκτορες (mobile agents). Η επιβάρυνση των υπολογισμών πηγαίνει στους κινητούς πράκτορες (mobile agents) και όχι στους στατικούς κόμβους. Αυτό συμβαίνει διότι οι κινητοί πράκτορες έχουν μεγαλύτερη επεξεργαστική ισχύ από ότι οι απλοί στατικοί κόμβοι αισθητήρες.

Τέτοιοι κινητοί πράκτορες μπορεί να βρίσκονται πάνω σε οχήματα όπως είναι τα αυτόνομα οχήματα (Unmanned Vehicles) που δεν οδηγούνται από άνθρωπο. Επίσης μπορούν να τοποθετηθούν σε οχήματα που οδηγούνται από ανθρώπους ή σε ρομπότ.

Οι κινητοί πράκτορες συνήθως δεν είναι συνεχώς παρόντες στο δίκτυο αλλά μπαίνουν σε λειτουργία όταν υπάρξει μία ανάγκη.

Ο ρόλος των απλών στατικών κόμβων είναι να καταγράφουν δεδομένα και ο ρόλος των κινητών πρακτόρων είναι να συλλέγουν τα δεδομένα από τους στατικούς κόμβους.

4.2.3.19 Μοντέλα Πρόβλεψης Κινητικότητας (Predictable Mobility Models)

Τα μοντέλα πρόβλεψης κινητικότητας έχουν στόχο να υπολογίζουν από πριν την επόμενη θέση του κινητού κόμβου ή χρησιμοποιούν άλλες μεθόδους ώστε να γνωρίζουν πότε πρέπει να παραδοθούν τα δεδομένα από έναν στατικό κόμβο στον κινητό κόμβο που είναι ο κινητός συλλέκτης δεδομένων (Mobile Data Collector MDC). Τα δεδομένα του

στατικού κόμβου είναι αποθηκευμένα σε μία ουρά queue. Οι στατικοί κόμβοι μπορεί να γνωρίζουν την τροχιά του κινητού κόμβου MDC. Η προβλεπτική συλλογή δεδομένων είναι μία μέθοδος που εφαρμόζεται όταν είναι γνωστή η τροχιά του κινητού κόμβου και γνωρίζουμε ότι θα περάσει από συγκεκριμένα σημεία σε αναμενόμενες χρονικές στιγμές. Οι στατικοί κόμβοι δεν είναι συνεχώς ενεργοποιημένοι για να μην εξαντλούν την ενέργεια της μπαταρίας τους, αλλά βρίσκονται σε κατάσταση sleep και ενεργοποιούνται όταν αναμένεται να περάσει ο κινητός κόμβος από ένα σημείο που είναι στην εμβέλεια τους για να γίνει μεταφορά δεδομένων από τον στατικό στον κινητό κόμβο.

4.2.3.20 Μοντέλο Pathway Mobility Model

Το μοντέλο αυτό ανήκει στην κατηγορία ετερογενή μοντέλα με γεωγραφική κινητικότητα.

Ένας τρόπος για να ενσωματωθούν στο μοντέλο κινητικότητας οι γεωγραφικοί περιορισμοί είναι να περιοριστεί η κίνηση των κόμβων σε διαδρομές που υπάρχουν σε έναν χάρτη. Ο χάρτης είναι προκαθορισμένος στο πεδίο της προσομοίωσης. Σε κάποιες περιπτώσεις χρησιμοποιείται ένα τυχαίο γράφημα για να μοντελοποιηθεί ένας χάρτης πόλης. Το γράφημα αυτό είτε δημιουργείται με έναν τυχαίο τρόπο, είτε καθορίζεται προσεκτικά με βάση το χάρτη από μία πραγματική πόλη. Τότε για τον κάθε κινητό κόμβο ο προορισμός επιλέγεται τυχαία και ο κινητός κόμβος κινείται προς αυτόν τον προορισμό με τη μέθοδο ελάχιστης διαδρομής κατά μήκος των ακμών του γραφήματος (edges). Μόλις φτάσει στον προορισμό, ο κόμβος σταματάει για χρόνο Trause και μετά επιλέγει έναν νέο προορισμό για την επόμενη κίνησή του. Αυτή η διαδικασία επαναλαμβάνεται μέχρι το τέλος της προσομοίωσης. Αντίθετα με το μοντέλο Random Way point model όπου οι κόμβοι μπορούν να κινούνται ελεύθερα, σε αυτό το μοντέλο οι κινητοί κόμβοι επιτρέπεται να ταξιδεύουν μόνο πάνω στις διαδρομές. Όμως, επειδή ο προορισμός σε κάθε φάση της κίνησης επιλέγεται τυχαία, υπάρχει ένας βαθμός τυχαιότητας. Έτσι σε αυτό το μοντέλο κινητικότητας που βασίζεται σε γραφήματα, οι κόμβοι ταξιδεύουν με έναν ψευδοτυχαίο τρόπο στις διαδρομές.

4.2.3.21 Free Way Mobility Model

Είναι ένα μοντέλο που ανήκει στην κατηγορία ετερογενή μοντέλα και γεωγραφικά μοντέλα κινητικότητας.

Αυτό το μοντέλο, υποθέτει ότι οι ελεύθερες διαδρομές που κινούνται οι κόμβοι, έχουν μία ή περισσότερες λωρίδες κυκλοφορίας (lanes). Ο κάθε κινητός κόμβος (mobile node) περιορίζεται μόνο σε μία λωρίδα κυκλοφορίας και δεν μπορεί να αλλάξει λωρίδα. Ο κινητός κόμβος μπορεί να κινείται και προς τις δύο κατευθύνσεις της λωρίδας. Η ταχύτητα που έχει ο κινητός κόμβος τη χρονική στιγμή t υπολογίζεται με βάση την ταχύτητα που έχει ο ίδιος κόμβος τη χρονική στιγμή $t-1$. Αν υπάρχει μία λωρίδα στην οποία κινούνται 2 κόμβοι και ο κόμβος A βρίσκεται μπροστά από τον κόμβο B, τότε ο κόμβος B μειώνει την ταχύτητά του, ώστε να είναι μικρότερη από την ταχύτητα του κόμβου A, για να διατηρείται μία απόσταση ασφαλείας μεταξύ των δύο κόμβων και να μη συγκρουστούν.

4.2.3.22 Μοντέλο Manhattan mobility model

Το μοντέλο αυτό ανήκει στην κατηγορία ετερογενή μοντέλα και γεωγραφικά μοντέλα κινητικότητας. Το μοντέλο κινητικότητας Manhattan mobility model είναι παρόμοιο με το προηγούμενο μοντέλο διότι ο κινητός κόμβος κινείται σε δρόμους. Το μοντέλο Manhattan βασίζεται σε μία τοπολογία δρόμων σε μορφή ορθογώνιου πλέγματος (grid), όπου όλοι οι δρόμοι είναι οργανωμένοι οριζόντια και κάθετα και έτσι η κίνηση γίνεται μόνο σε οριζόντιες και κάθετες ευθείες στην περιοχή. Αυτό χρησιμοποιεί μία προσέγγιση πιθανοκρατική, διότι, η επιλογή της κίνησης του κόμβου γίνεται σε κάθε διασταύρωση. Ο κινητός κόμβος μπορεί να αλλάξει την κατεύθυνση του μόνο στα σημεία διασταυρώσεων των δρόμων. Ένας κόμβος μπορεί να στρίψει δεξιά, αριστερά, ή να προχωρήσει ευθεία διατηρώντας την κατεύθυνση που έχει. Σε κάθε περίπτωση η πιθανότητα να στρίψει αριστερά είναι $1/2$ ενώ η πιθανότητα να στρίψει δεξιά είναι $1/4$. Στον κινητό κόμβο επιτρέπεται να κινηθεί μέσα στο πλέγμα είτε σε οριζόντια είτε σε κάθετη διαδρομή μέσα στην περιοχή.

Η ταχύτητα του κινητού κόμβου τη χρονική στιγμή t εξαρτάται από την ταχύτητα που είχε την προηγούμενη χρονική στιγμή $t-1$.

Ισχύει ότι και στο προηγούμενο μοντέλο δηλαδή αν δύο κινητοί κόμβοι κινούνται ο ένας πίσω από τον άλλο, τότε αυτός που ακολουθεί μειώνει την ταχύτητα του ώστε να είναι μικρότερη από την ταχύτητα του προπορευόμενου κόμβου και έτσι να υπάρχει μία απόσταση ασφαλείας.

Σε μία αποθήκη που κινούνται αυτόματα οχήματα φόρτωσης μέσα σε ευθείς κάθετους και οριζόντιους διαδρόμους για να φορτώσουν ή να ξεφορτώσουν εμπορεύματα και κιβώτια, το μοντέλο Manhattan θα μπορούσε να εφαρμοστεί.

Όμως μοντέλο Manhattan δεν είναι κατάλληλο για περιπτώσεις όπου ένας κινητός κόμβος βρίσκεται σε ένα ρομπότ το οποίο κινείται κατά μήκος ενός αγωγού για να ανιχνεύσει σφάλματα στον αγωγό. διότι οι δρόμοι στο μοντέλο Manhattan είναι ευθείες κάθετες και οριζόντιες διαδρομές.

4.2.3.23 Μοντέλο Κινητικότητας Εμποδίων (Obstacle Mobility Model)

Το μοντέλο αυτό ανήκει στην κατηγορία ετερογενή μοντέλα και γεωγραφικά μοντέλα κινητικότητας.

Το μοντέλο κινητικότητας εμποδίων είναι ένα μοντέλο που λαμβάνει υπόψη την παρουσία των εμποδίων σε μία διαδρομή κίνησης που κυκλοφορεί ο κινητός κόμβος (mobile node). Όταν υπάρχουν εμπόδια, στη διαδρομή τότε ο κινητός κόμβος πρέπει να αλλάξει την κίνηση του για να τα παρακάμψει.

Για αυτό πρέπει να σχεδιάσει μία νέα τροχιά κίνησης που περνάει ανάμεσα από τα εμπόδια. Ένα άλλο πρόβλημα που προκαλούν τα εμπόδια είναι ότι μπορεί το σήμα του ασύρματου δικτύου να έχει σημαντική εξασθένιση στην περιοχή κοντά στο εμπόδιο και έτσι χάνεται η σύνδεση του κινητού κόμβου από το δίκτυο.

Συνεπώς τα εμπόδια επηρεάζουν και την διάδοση του ασύρματου σήματος και την προσχεδιασμένη διαδρομή που ακολουθεί ο κινητός κόμβος σε ένα γεωγραφικό χάρτη. Για τη λύση του προβλήματος προτάθηκαν διάφορα σενάρια όπως είναι το σενάριο συνεδρίου, το σενάριο κάλυψης συμβάντων και το σενάριο αντιμετώπισης καταστροφών.

4.2.3.24 Μοντέλο Κινητικότητας Με Χρονοπρογραμματισμό (scheduling) του κινητού στοιχείου (Mobile Element)

Το μοντέλο αυτό ανήκει στην κατηγορία κινητικότητας με χρήση κινητού συλλέκτη δεδομένων (Mobile Data Collector, MDC). Βασίζεται σε ένα χρονοδιάγραμμα επισκέψεων του κινητού κόμβου στους στατικούς κόμβους.

Σε ένα ασύρματο δίκτυο αισθητήρων, υπάρχουν οι στατικοί κόμβοι αισθητήρες οι οποίοι μετρούν ένα φυσικό μέγεθος και παράγουν δεδομένα που τα αποθηκεύουν σε μία ουρά queue, στην ενδιάμεση μνήμη απομόνωσης τους (buffer).

Όταν παράγονται τα δεδομένα, οι ρυθμοί δειγματοληψίας μπορούν να καθορίζονται με βάση το ρυθμό που συμβαίνουν αλλαγές στο φαινόμενο που παρατηρείται.

Ένας κινητός κόμβος που ονομάζεται κινητός συλλέκτης δεδομένων (Mobile Data Collector, MDC), η κινητό στοιχείο (Mobile Element) ακολουθεί μία διαδρομή και επισκέπτεται κάποιες χρονικές στιγμές τους στατικούς κόμβους και συλλέγει τα δεδομένα.

Ένας τρόπος συλλογής δεδομένων είναι η μορφή συμβάντων (events).

Σύμφωνα με αυτή τη μέθοδο δεν αποθηκεύονται τα δεδομένα όταν η μετρούμενη τιμή διατηρείται σταθερή, αλλά κάθε φορά που γίνεται αύξηση ή μείωση της τιμής ή όταν φτάσει η τιμή σε κάποια όρια, τότε μόνο γίνεται η λήψη δεδομένων.

Αυτό γίνεται για μία εξοικονόμηση αποθηκευτικού χώρου ο οποίος είναι περιορισμένος.

Όμως η απώλεια δεδομένων (Data Loss) μπορεί να συμβεί όταν καθυστερήσει αρκετά ο κινητός συλλέκτης δεδομένων ME να φτάσει στον στατικό κόμβο και τότε γεμίζει πλήρως η ενδιάμεση μνήμη (buffer) του στατικού κόμβου ώστε χάνονται τα επόμενα δεδομένα που παράγονται και δεν μπορούν να αποθηκευτούν. Έτσι, για όλους τους στατικούς κόμβους καθορίζεται μία παράμετρος χρόνου t_{ov} που ονομάζεται χρόνος υπερχείλισης ενδιάμεσης μνήμης και θεωρείται ότι μόλις ξεπεραστεί αυτό το όριο χρόνου συμβαίνει υπερχείλιση ενδιάμεσης μνήμης στον στατικό κόμβο.

Ο κινητός κόμβος ME πρέπει να περάσει από όλους τους στατικούς κόμβους εγκαίρως, πριν γεμίσει πλήρως η ενδιάμεση μνήμη τους, δηλαδή πριν να περάσει ο χρόνος υπερχείλισης ενδιάμεσης μνήμης t_{ov} για κάθε στατικό κόμβο.

Τότε απαιτείται ένας χρονοπρογραμματισμός (scheduling) σε πραγματικό χρόνο (real-time) για την κίνηση του κινητού στοιχείου ΜΕ, ώστε να προλάβει να επισκεφτεί όλους τους στατικούς κόμβους πριν να λήξει ο χρόνος υπερχείλισης τους. Έτσι δημιουργείται ένα χρονοδιάγραμμα επισκέψεων (visiting schedule).

Διάφοροι αλγόριθμοι έχουν σχεδιαστεί ώστε να επιτευχθεί ο στόχος αυτός.

Οι περισσότεροι αλγόριθμοι λαμβάνουν υπόψη το χρόνο υπερχείλισης t_{ov} κάθε κόμβου, και την απόσταση s μεταξύ των στατικών κόμβων.

Αν υπάρχουν δύο στατικοί κόμβοι αισθητήρες που βρίσκονται τοποθετημένοι μακριά μεταξύ τους και έχουν παραπλήσιους χρόνους υπερχείλισης, τότε υπάρχει ο κίνδυνος για το κινητό στοιχείο ΜΕ να επισκεφτεί μόνο τον ένα κόμβο πριν γίνει υπερχείλιση, αλλά να μην προλάβει να φτάσει στον άλλον και έτσι να γίνει υπερχείλιση και να χαθούν τα δεδομένα. Για αυτό στο χρονικό πρόγραμμα επισκέψεων λαμβάνονται υπόψη, οι χρόνοι υπερχείλισης των στατικών κόμβων, και οι αποστάσεις μεταξύ τους. Πρέπει ο κινητός κόμβος ΜΕ να βρίσκει ποιοι είναι οι κοντινοί στατικοί κόμβοι που έχουν παραπλήσιους χρόνους υπερχείλισης και να επισκέπτεται πρώτα αυτούς και μετά να πηγαίνει σε απομακρυσμένους κόμβους. Πολλές φορές όμως δεν είναι εφικτό, όσο σωστός και αν είναι ο χρονοπρογραμματισμός, να δεχτούν όλοι οι απομακρυσμένοι κόμβοι επίσκεψη, πριν συμβεί υπερχείλιση, ούτε είναι δυνατόν να εξαλειφθούν πλήρως τα πισωγυρίσματα και οι επισκέψεις μπρος πίσω ανάμεσα σε δύο κόμβους. Τότε θα υπάρξει σίγουρα απώλεια δεδομένων, αλλά θέλουμε να μην ξεπεράσει κάποια όρια. Επίσης γίνονται επαναληπτικές μεταδόσεις περιοδικά.

4.2.3.25 Μοντέλο Κινητικότητας με Ραντεβού (Rendezvous-Based Mobility Model)

Αυτό το μοντέλο κινητικότητας χρησιμοποιεί λύσεις υβριδικές που βασίζονται στις ιδιότητες του κινητού συλλέκτη δεδομένων (Mobile Data Collector, MDC) αλλά και στις ιδιότητες του κινητού σταθμού βάσης (Mobile Base Station, MBS). Τα «ραντεβού» είναι προκαθορισμένες χρονικές στιγμές, στις οποίες ο κινητός κόμβος πρέπει να επισκεφτεί έναν στατικό κόμβο, και οι στιγμές αυτές είναι γνωστές από πριν.

Σε κάποια ασύρματα δίκτυα αισθητήρων WSNs, οι στατικοί κόμβοι κατανέμονται σε διάφορες μεγάλες γεωγραφικές περιοχές, με τέτοιο τρόπο, ώστε ένα σύνολο κόμβων να

είναι συγκεντρωμένο σε μία απομακρυσμένη περιοχή, ενώ παράλληλα, να συμβαίνει το ίδιο και σε πολλές άλλες μικρές περιοχές του δικτύου. Έτσι δημιουργούνται διάφορα απομονωμένα τμήματα του δικτύου σε απομακρυσμένες περιοχές. Αυτά τα τμήματα δικτύου μπορεί να θεωρηθούν σαν ξεχωριστές νησίδες που δεν βρίσκονται κοντά στο κυρίως δίκτυο.

Τότε, αν ένας κινητός κόμβος ME, επιχειρήσει να επισκεφτεί όλα αυτά τα απομακρυσμένα τμήματα του δικτύου, θα υπάρξει το μειονέκτημα ότι ο κινητός κόμβος θα καθυστερήσει να διανύσει όλες τις μακρινές αποστάσεις και να πάει σε όλους τους στατικούς κόμβους. Δεύτερο μειονέκτημα, είναι ότι θα δαπανήσει ενέργεια μπαταρίας για την μετακίνηση του καθώς και για τη συλλογή δεδομένων μέσω ασύρματου δικτύου, από τους απομακρυσμένους κόμβους.

Για να μη συμβεί αυτό, σε κάθε απομακρυσμένη περιοχή, υπάρχουν κάποιοι συγκεκριμένοι στατικοί κόμβοι, που ορίζονται ως κεντρικοί, ώστε όλοι οι υπόλοιποι γειτονικοί κόμβοι να στέλνουν τα δεδομένα τους σε αυτούς τους κεντρικούς κόμβους. Ένας κεντρικός κόμβος, συγκεντρώνει όλα τα δεδομένα από πολλούς άλλους γειτονικούς κόμβους, σε μία περιοχή, και για αυτό, έχει μεγαλύτερο χώρο στην ενδιάμεση μνήμη απομόνωσης του (buffer), ώστε να μπορεί να διατηρήσει τα δεδομένα για αρκετό χρόνο χωρίς να συμβεί υπερχείλιση.

Τότε, ο κινητός συλλέκτης δεδομένων (Mobile Data Collector, MDC) δεν απαιτείται να επισκεφτεί ξεχωριστά κάθε στατικό κόμβο στην απομακρυσμένη περιοχή του δικτύου, αλλά επισκέπτεται μόνο τους κεντρικούς κόμβους. Οι επισκέψεις γίνονται σε συγκεκριμένες χρονικές στιγμές. Η χρονική στιγμή που ο κινητός κόμβος MDC, θα πρέπει να επισκεφτεί έναν κεντρικό κόμβο, της απομακρυσμένης περιοχής, είναι μια στιγμή προκαθορισμένη και γνωστή από πριν, ώστε λέμε ότι γίνεται ένα «ραντεβού». Τότε ο στατικός κόμβος αναμεταδίδει (relay) στον κινητό κόμβο όλα τα δεδομένα που έχει συλλέξει.

Όμοια λύση μπορεί να χρησιμοποιηθεί όταν υπάρχουν δύο ή περισσότερα διαφορετικά ασύρματα δίκτυα αισθητήρων, που είναι συνδεδεμένα μεταξύ τους.

Τότε ο κεντρικός κόμβος σε κάθε δίκτυο είναι ο sink.

Ο κινητός συλλέκτης δεδομένων τότε θα μπορεί να επισκέπτεται μόνο τους sinks με «ραντεβού». Με αυτό τον τρόπο υπάρχει εξοικονόμηση ενέργειας και επίσης μειώνεται και το φορτίο επικοινωνιών (communication load) συνολικά στο δίκτυο.

Τα δεδομένα σε ένα ασύρματο δίκτυο αισθητήρων στατικό παραδίδονται από τους απομακρυσμένους κόμβους στον sink με διαδρομές πολλαπλών αλμάτων (multiple hops). Αυτό έχει ομοιότητα με την περίπτωση που υπήρχε ο κινητός σταθμός βάσης (mobile base station, MBS). Επιπλέον τα δεδομένα παραμένουν αρκετό χρόνο στο sink, μέχρι να έρθει ο κινητός κόμβος για να τα συλλέξει.

4.2.3.26 Μοντέλο Κινητικότητας με κινητό Δρομολογητή (Mobile Router) και αναμετάδοση δεδομένων (relayed data).

Το μοντέλο αυτό ανήκει στην κατηγορία κινητικότητας με χρήση κινητού συλλέκτη δεδομένων (Mobile Data Collector, MDC), και ανήκει στα γεωγραφικά μοντέλα κινητικότητας.

Σε αυτή την λύση κινητικότητας, υπάρχει ένας κινητός συλλέκτης δεδομένων MDC ο οποίος κινείται σε μία γραμμική διαδρομή (linear path) ακολουθώντας κάποιο φυσικό μονοπάτι που είναι περιορισμένο γεωγραφικά. Για παράδειγμα, μπορεί να ακολουθεί έναν αγωγό αερίου.

Επιπλέον στο δίκτυο υπάρχουν οι στατικοί κόμβοι. Η εμβέλεια μεταδόσεων (transmission range) των στατικών κόμβων είναι σχετικά μικρή. Έτσι ο κινητός κόμβος όταν ακολουθήσει την γραμμική τροχιά του, θα βρεθεί στην εμβέλεια ορισμένων στατικών κόμβων που βρίσκονται κοντά στη διαδρομή του και θα συλλέξει τα δεδομένα από αυτούς.

Οι υπόλοιποι στατικοί κόμβοι που δεν βρίσκονται κοντά στην διαδρομή του κινητού κόμβου, στέλνουν τα δεδομένα τους σε άλλους κόμβους στατικούς που βρίσκονται κοντά στη διαδρομή του. Αυτή η προώθηση πακέτων γίνεται με μία μετάδοση πολλαπλών αλμάτων (multi-hop transmission).

Χρησιμοποιούνται διάφοροι αλγόριθμοι. Σε μία φάση αρχικοποίησης γίνεται ένας έλεγχος για να διαπιστωθεί ποιοι στατικοί κόμβοι βρίσκονται κοντά στη διαδρομή από όπου θα περάσει ο κινητός κόμβος. Όταν κάποιος στατικός κόμβος ανακαλύψει ότι ο κινητός κόμβος δεν θα περάσει ποτέ από την δική του εμβέλεια επικοινωνίας, τότε επιλέγει να προωθήσει τα δεδομένα του σε άλλο ενδιάμεσο κόμβο που βρίσκεται πλησιέστερα στη διαδρομή του κινητού κόμβου.

Η προώθηση των δεδομένων από τον αρχικό στατικό κόμβο στον στατικό κόμβο προορισμού μπορεί να γίνει με βάση τη συντομότερη διαδρομή. Τα δεδομένα αποθηκεύονται και παραμένουν στην ενδιάμεση μνήμη απομόνωσης (buffer) του στατικού κόμβου προορισμού, μέχρι να τα συλλέξει ο κινητός κόμβος.

Σε άλλες μορφές του ίδιου μοντέλου κινητικότητας, μπορεί να υπάρχουν περισσότεροι από ένας κινητοί κόμβοι που είναι συλλέκτες δεδομένων MDC.

Αυτό συμβαίνει όταν θέλουμε να καλύψει μεγαλύτερη γεωγραφική περιοχή και γενικότερα όταν υπάρχουν πολλές παράλληλες γραμμικές διαδρομές, όπως για παράδειγμα όταν υπάρχουν αγωγοί υγρών ή αερίων που οδεύουν παράλληλα μεταξύ τους. Τότε εφαρμόζεται το ίδιο μοντέλο όπου οι κινητοί συλλέκτες δεδομένων κινούνται σε παράλληλες γραμμικές διαδρομές.

Σε άλλη μορφή του μοντέλου αυτού, ο κινητός κόμβος αυξομειώνει την ταχύτητά του ανάλογα με το πόσοι στατικοί κόμβοι υπάρχουν στην εμβέλεια μεταδόσεων του. Αν υπάρχουν πολλοί στατικοί κόμβοι τότε μειώνει την ταχύτητά του και προχωράει με χαμηλή ταχύτητα για να συλλέξει όσο το δυνατόν γίνεται περισσότερα δεδομένα από αυτούς.

Αν όμως οι στατικοί κόμβοι είναι πολύ λίγοι ή κανένας δεν βρίσκεται κοντά στη διαδρομή του, τότε ο κινητός συλλέκτης δεδομένων αυξάνει την ταχύτητά του και τρέχει γρήγορα ώστε να φτάσει σε μέρος με περισσότερους στατικούς κόμβους.

Με αυτή τη μέθοδο, υπάρχει το μειονέκτημα ότι ο κινητός κόμβος μπορεί να μην συλλέγει όλα τα δεδομένα αλλά να υπάρχουν απώλειες. Όμως γίνονται επαναληπτικές προσπάθειες μετάδοσης και για αυτό περιορίζονται οι απώλειες, χωρίς να είναι εγγυημένο ότι δεν θα εξαλειφθούν πλήρως.

4.3 Κινητικότητα στο Επίπεδο DLL (Στρώμα MAC)

Η κινητικότητα στο επίπεδο ζεύξης δεδομένων (Data Link Layer) (DLL), καθορίζεται στο στρώμα MAC, που είναι το υπό-επίπεδο ελέγχου πρόσβασης μέσου (Medium Access Control sub-layer) και βρίσκεται ακριβώς πάνω από το φυσικό στρώμα. Το μέσο είναι το ασύρματο κανάλι επικοινωνίας. Σε ένα ασύρματο δίκτυο αισθητήρων, χρησιμοποιούνται διάφορα κανάλια επικοινωνίας και το στρώμα MAC είναι υπεύθυνο για να ελέγξει την πρόσβαση στο κάθε ασύρματο κανάλι που χρησιμοποιείται. Οι κόμβοι αισθητήρες, που θέλουν να χρησιμοποιήσουν ταυτόχρονα ένα κανάλι επικοινωνίας για να στείλουν τα δεδομένα τους, ελέγχονται από το πρωτόκολλο MAC, που καθορίζει ποιοι κόμβοι θα αποκτήσουν την πρόσβαση στο κανάλι, με τέτοιο τρόπο, ώστε όσο το δυνατόν περισσότεροι κόμβοι να μπορούν στείλουν ταυτόχρονα τα δεδομένα τους με αξιοπιστία, για να διαμοιραστούν από κοινού, τα διαθέσιμα κανάλια, χωρίς να δημιουργηθούν σφάλματα στα δεδομένα που φτάνουν στον κόμβο προορισμό. Η τεχνική που χρησιμοποιείται, συνήθως, για να επιτευχθεί η κοινή χρήση καναλιού, από διαφορετικούς κόμβους, είναι η πολυπλεξία με διαίρεση χρόνου TDMA.

Τα συνηθισμένα πρωτόκολλα MAC που είχαν σχεδιαστεί παλαιότερα, δεν ήταν κατάλληλα για χρήση στα ασύρματα δίκτυα αισθητήρων (WSN), διότι θεωρούσαν πως οι κόμβοι είναι διαρκώς ενεργοποιημένοι, τον περισσότερο χρόνο λειτουργίας του δικτύου και δεν υπέθεταν ότι εξαντλείται γρήγορα η ενέργεια τροφοδοσίας. Αυτό ίσχυε, επειδή οι κόμβοι συνέχιζαν να τροφοδοτούνται διαρκώς, με επαναφορτίσεις των μπαταριών τους και έτσι δεν υπήρχε σημαντικός περιορισμός στην ενέργεια τροφοδοσίας τους.

Στα ασύρματα δίκτυα αισθητήρων, όμως, υπάρχει περιορισμός στην ενέργεια τροφοδοσίας. Για την εξοικονόμηση ενέργειας των κόμβων, πολλές φορές, οι κόμβοι διατηρούνται περιοδικά σε μία κατάσταση ύπνου (sleep mode) και σε άλλες χρονικές περιόδους ξυπνούν (wake up mode) και μεταβαίνουν σε κατάσταση ακοής (listening state) και «ακούν» τα σήματα που μεταφέρονται μέσα στο δίκτυο, για να εντοπίσουν τα εισερχόμενα πακέτα δεδομένων. Τότε, αν εντοπίσουν πακέτα δεδομένων, δημιουργούν μία ζεύξη με έναν κόμβο που στέλνει τα πακέτα, ειδάλλως, αν δεν εντοπίσουν πακέτα

δεδομένων, μετά από κάποιο χρονικό διάστημα μεταβαίνουν και πάλι στην κατάσταση ύπνου (sleep mode).

Δηλαδή κατά την λειτουργία του δικτύου, υπάρχει ένας κύκλος λειτουργίας (duty cycle) που επαναλαμβάνεται περιοδικά, και οι κόμβοι μεταβαίνουν διαδοχικά σε διαφορετικές καταστάσεις, και στην συνέχεια ένας νέος κύκλος αρχίζει πάλι από την αρχή.

Έτσι, ο χρόνος λειτουργίας των κόμβων στο δίκτυο, διαιρείται σε χρονικές περιόδους που οι κόμβοι είναι στην κατάσταση ύπνου (sleep mode), σε χρονικές περιόδους που οι κόμβοι είναι στην κατάσταση ξυπνήματος (awake mode), (δηλαδή προετοιμασία πριν την πλήρη ενεργοποίηση) και σε χρονικές περιόδους που οι κόμβοι είναι πλήρως ενεργοί (active state) και συμμετέχουν σε επικοινωνία δεδομένων με άλλους κόμβους.

Σε ένα σενάριο κινητικότητας, οι πολλαπλοί κόμβοι που στέλνουν τα δεδομένα, είναι κινητοί. Διάφορα είδη πρωτοκόλλων MAC και πρωτοκόλλων δρομολόγησης (routing protocols) σχεδιάζονται για τα ασύρματα δίκτυα αισθητήρων (WSN) ώστε να εγγραφούν την παράδοση δεδομένων από τους κόμβους-πηγές (source nodes) προς τον κεντρικό κόμβο (sink), ο οποίος ονομάζεται και κεντρικός σταθμός βάσης [40]. Οι συγγραφείς στο [40] αφού εξέτασαν διάφορα πρωτόκολλα MAC, κατέληξαν στο συμπέρασμα ότι τα περισσότερα πρωτόκολλα MAC που υπάρχουν, χρειάζονται βελτιώσεις για να λειτουργήσουν σε εφαρμογές πραγματικού χρόνου. Για αυτό το λόγο υπάρχουν πολλά διαφορετικά πρωτόκολλα MAC, τα οποία συχνά, είναι παραλλαγές άλλων και περιέχουν διάφορες βελτιώσεις σε σχέση με τα αρχικά. Στη μελέτη τους, οι συγγραφείς παρουσιάζουν προτεινόμενα πρωτόκολλα MAC, αναλύουν τα πλεονεκτήματα και τα μειονεκτήματα τους και εξετάζουν πόσο κατάλληλα είναι για εφαρμογές πραγματικού χρόνου.

Σε αυτή την παράγραφο, αναφέρονται ενδεικτικά μερικά πρωτόκολλα MAC, από τα πολλά που υπάρχουν, ώστε να φανεί ο μηχανισμός λειτουργίας κάποιων πρωτοκόλλων και ασφαλώς δεν είναι δυνατόν να αναφερθούν όλα.

4.3.1 Διάφορα είδη πρωτοκόλλων MAC

Για την περίπτωση που υπάρχουν πολλοί κινητοί κόμβοι που θέλουν να επικοινωνήσουν ταυτόχρονα με άλλους κόμβους σε ασύρματο δίκτυο αισθητήρων με στατικούς κόμβους,

έχει προταθεί ένα πρωτόκολλο για το στρώμα MAC, που είναι υβριδικό και ονομάζεται RI-MAC [41]. Αυτό το πρωτόκολλο, έχει λιγότερες καθυστερήσεις από άλλα πρωτόκολλα MAC, διότι στα πακέτα δεδομένων του, δεν χρησιμοποιείται το πεδίο preamble bits, ούτε τα πεδία ελέγχου και έτσι είναι πιο γρήγορο από τα άλλα πρωτόκολλα MAC, που χρησιμοποιούν τα συγκεκριμένα πεδία δεδομένων. Το RI-MAC μπορεί να χρησιμοποιηθεί και ως ένα μέτρο σύγκρισης για την ταχύτητα των άλλων πρωτοκόλλων MAC, που έχουν περισσότερα πεδία δεδομένων, διότι είναι πιο γρήγορο από τα πρωτόκολλα αυτά.

Το RI-MAC περιγράφεται εν συντομία και στο επόμενο κεφάλαιο, στην παράγραφο 5.1.1.4, όταν αναφερόμαστε στον ανταγωνισμό μεταξύ των κόμβων για να κερδίσουν τη χρήση του μέσου.

Στα ασύρματα δίκτυα αισθητήρων, οι εφαρμογές που συλλέγουν τα δεδομένα στο δίκτυο από τους κόμβους αισθητήρες και τα παραδίδουν στον κεντρικό κόμβο Sink, διακρίνονται σε 3 κατηγορίες, που είναι οι εξής:

- α) Ανίχνευση συμβάντων (event detection),
- β) Περιοδική ανίχνευση δεδομένων (periodic sensed)
- γ) Βασισμένες σε Ερωτήματα (query based).

Οι εφαρμογές που βασίζονται σε ανίχνευση συμβάντων συλλέγουν και αποστέλλουν τα δεδομένα από τους κόμβους αισθητήρες μόνο όταν υπάρχει κάποιο συμβάν, π.χ. μία αλλαγή θερμοκρασίας.

Οι εφαρμογές που εκτελούν περιοδική ανίχνευση δεδομένων, συλλέγουν και στέλνουν τα δεδομένα σε τακτά χρονικά διαστήματα.

Οι εφαρμογές που βασίζονται σε ερωτήματα (queries) συλλέγουν και στέλνουν τα δεδομένα στον κεντρικό κόμβο μόνο όταν τα ζητήσει ο κεντρικός κόμβος με κάποιο ερώτημα (query) και τότε στέλνουν μόνο τα δεδομένα που ζητούνται στο συγκεκριμένο ερώτημα (π.χ.: ποιες είναι οι τιμές πίεσης υγρών σε μία περιοχή της εγκατάστασης;) Τότε, τα δεδομένα συλλέγονται μόνο από συγκεκριμένους κόμβους οι οποίοι βρίσκονται στην περιοχή που αφορά το ερώτημα.

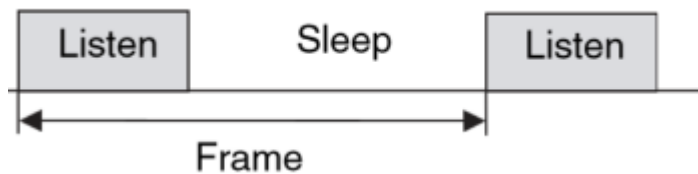
Κάθε μία από αυτές τις εφαρμογές έχει δικές τις τεχνικές για να συλλέγει τα δεδομένα από έναν ή περισσότερους κόμβους αισθητήρες (sensor nodes) και να τα αποστέλλει στον κεντρικό κόμβο (sink). Οι μέθοδοι αυτές, είναι διαφορετικές για κάθε κατηγορία εφαρμογών. Σε αντιστοιχία με τις εφαρμογές, έχουν προταθεί τα αντίστοιχα

πρωτόκολλα MAC, για κάθε τύπο εφαρμογής, με στόχο να υπάρξει αποτελεσματικότητα στη χρήση ενέργειας και στην καθυστέρηση (latency) για τις συγκεκριμένες κατηγορίες εφαρμογών.

Μερικά πρωτόκολλα MAC αναφέρονται συνοπτικά παρακάτω:

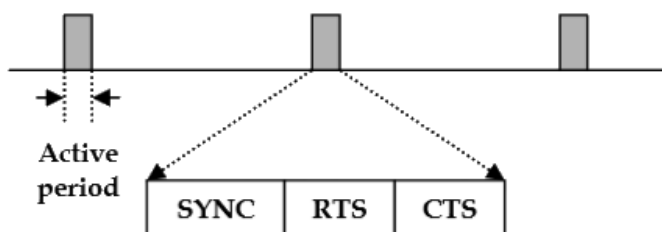
4.3.1.1 Sensor MAC (S-MAC)

Το πρωτόκολλο Sensor-MAC (S-MAC) χρησιμοποιεί την περιοδική κατάσταση «ύπνου» των κόμβων (periodic sleep) και τα χαρακτηριστικά των εικονικών συστοιχιών (virtual cluster) [42]. Αυτό το πρωτόκολλο MAC, σχεδιάστηκε κυρίως για τα ασύρματα δίκτυα αισθητήρων (WSN) και ο βασικός στόχος του ήταν να υπάρχει εξοικονόμηση ενέργειας [40]. Σχεδιάστηκε για να μειώσει την άσκοπη δαπάνη ενέργειας που οφείλεται σε καταστάσεις όπως είναι οι συγκρούσεις (collisions), οι αδρανείς κόμβοι στην κατάσταση ακοής (idle listening), το overhead από πακέτα ελέγχου που στέλνει ο διαχειριστής δικτύου και το overhearing που είναι η υπερβολική αναμονή του ενεργοποιημένου κόμβου για να λάβει πακέτα που δεν προορίζονται για αυτόν. [1]. Το S-MAC χρησιμοποιεί μόνο ένα κανάλι συχνότητας για επικοινωνία για να διαμορφωθεί ένα δίκτυο με μία τοπολογία επίπεδη, με ένα μόνο άλμα (single-hop). Περιοδικά οι κόμβοι, μεταβαίνουν στην κατάσταση «ύπνου» (sleep state) και στη διάρκειά της, το υποσύστημα ασύρματης επικοινωνίας τους είναι τελείως απενεργοποιημένο. Οι κόμβοι γίνονται ενεργοί, όταν υπάρχει κυκλοφορία δεδομένων στο δίκτυο. Κάθε κόμβος έχει έναν μετρητή χρόνου «ξυπνήματος» (wake-up timer) και βρίσκεται στην κατάσταση ύπνου για μία ορισμένη χρονική περίοδο. Μόλις έρθει ο χρόνος ξυπνήματος, ο κόμβος μπαίνει σε κατάσταση ξυπνήματος (wakes up) και αρχίζει να ακούει το κανάλι (listens) για να καθοριστεί αν θα επικοινωνήσει με άλλους κόμβους. Ο συνολικός κύκλος: χρόνος ακοής συν χρόνος ύπνου, ονομάζεται πλαίσιο (frame). Κάθε πλαίσιο (frame) χαρακτηρίζεται από τον κύκλο λειτουργίας (duty cycle), και ορίζεται ο λόγος χρόνου ακοής προς συνολικό χρόνο πλαισίου (interval-to-frame length ratio). Αν και το μήκος το χρόνου ακοής μπορεί να επιλεγεί με ανεξαρτησία από τους κόμβους αισθητήρες και να διαφέρει από κόμβο σε κόμβο, για απλότητα, το πρωτόκολλο υποθέτει ότι είναι το ίδιο για όλους τους κόμβους.



Εικόνα 116 Οι χρονικές περίοδοι λειτουργίας listen και sleep του πρωτοκόλλου S-MAC . Πηγή [1].

Για μία σταθερή χρονική περίοδο, που έχει διάρκεια 115 ms, οι κόμβοι παραμένουν πλήρως ενεργοποιημένοι, και αυτή η περίοδος ονομάζεται active period. Πριν από την περίοδο πλήρους ενεργοποίησης, προηγείται μία άλλη χρονική περίοδος, στην διάρκεια της οποίας, οι κόμβοι βρίσκονται στην κατάσταση «ξυπνήματος» και ονομάζεται wake-up period. Αυτή η περίοδος, δηλαδή, είναι η περίοδος πριν ενεργοποιηθούν πλήρως οι κόμβοι, και είναι μεταβλητή, ώστε μπορεί να διαρκέσει μέχρι και 100-άδες ms. Για αυτό, η περίοδος ύπνου (sleep period) μπορεί να μην είναι σταθερή αλλά να είναι άλλοτε μεγαλύτερη και άλλοτε μικρότερη.



Εικόνα 117. Οι χρονικές περίοδοι του πρωτοκόλλου S-MAC όταν οι κόμβοι είναι συγχρονισμένοι. Πηγή [42].

Μέσα σε μία συστοιχία (cluster), όλοι οι κόμβοι είναι συγχρονισμένοι, έτσι ώστε όλοι μαζί μπορούν να ξυπνήσουν (wake up) την ίδια χρονική στιγμή. Οι γειτονικοί κόμβοι συντονίζουν στο πρόγραμμα τους χρόνους ακοής (listen) και ύπνου (sleep) έτσι ώστε να ακούν όλοι την ίδια χρονική στιγμή, και να είναι σε ύπνο όλοι την ίδια χρονική στιγμή. Η περίοδος που το δίκτυο είναι ενεργό (active period) διαίρεείται σε 3 φάσεις :

α) Συγχρονισμός SYNC, β) Αρχή χειραψίας RTS, γ)Ολοκλήρωση χειραψίας CTS.

α) SYNC συγχρονισμός.

Για να γίνει ο συγχρονισμός, ο κάθε κόμβος επιλέγει ένα χρονικό πρόγραμμα (schedule) και το ανταλλάσσει με τους γείτονές του στην περίοδο συγχρονισμού. Κάθε κόμβος διατηρεί έναν πίνακα χρονικού προγραμματισμού (schedule table) που περιέχει το πρόγραμμα όλων των γνωστών γειτόνων του. Για να επιλέξει ένα πρόγραμμα, ο κόμβος πρώτα ακούει στο κανάλι για σταθερό χρονικό διάστημα, τουλάχιστον ίσο με την περίοδο συγχρονισμού. Όταν τελειώσει αυτός ο χρόνος αναμονής, αν ο κόμβος δεν ακούσει ένα πρόγραμμα schedule από άλλον γειτονικό κόμβο, αμέσως επιλέγει το δικό του πρόγραμμα schedule. Ο κόμβος ανακοινώνει το πρόγραμμα που επέλεξε στέλνοντας προς όλους τους γείτονες κόμβους (broadcast) ένα πακέτο συγχρονισμού (SYNC packet). Ο κόμβος πριν να εκπέμψει το πακέτο SYNC packet, πρέπει πρώτα να εκτελέσει ανίχνευση φέροντος (carrier sensing). Αυτό μειώνει την πιθανότητα συγκρούσεων ανάμεσα σε κόμβους που ανταγωνίζονται για τη χρήση του καναλιού. Αν κατά την περίοδο συγχρονισμού, ο κόμβος λάβει ένα άλλο χρονικό πρόγραμμα από γείτονα κόμβο, πριν να επιλέξει το δικό του πρόγραμμα schedule, τότε ο κόμβος αλλάζει το δικό του χρονικό πρόγραμμα schedule ώστε να γίνει το ίδιο με εκείνο το πρόγραμμα που λήφθηκε από τον γειτονικό κόμβο. Ο κόμβος περιμένει μέχρι να έρθει η επόμενη περίοδος συγχρονισμού, για να ανακοινώσει το πρόγραμμα schedule στους γειτονικούς κόμβους. Όμως υπάρχει περίπτωση, ένας κόμβος να λάβει ένα διαφορετικό πρόγραμμα schedule κάποια στιγμή αργότερα, από το χρόνο που επέλεξε και είχε ανακοινώσει το δικό του πρόγραμμα. Αυτό μπορεί να συμβεί αν το πακέτο SYNC packet που έστειλε ο γειτονικός κόμβος είχε καταστραφεί, είτε από συγκρούσεις είτε από παρεμβολές στο κανάλι. Αν ο κόμβος δεν έχει άλλον γείτονα με τον οποίο να μοιράζονται το ίδιο πρόγραμμα schedule, τότε μόλις ο κόμβος λάβει το νέο πρόγραμμα, απορρίπτει το παλιό πρόγραμμα και υιοθετεί το νέο. Αντίθετα, αν ο κόμβος γνωρίζει άλλους κόμβους που ήδη υιοθέτησαν το δικό του πρόγραμμα, τότε ο κόμβος υιοθετεί ταυτόχρονα και τα δύο προγράμματα schedules. Δηλαδή, ο κόμβος απαιτείται να ξυπνήσει (wake up) στις χρονικές περιόδους listen και των δύο προγραμμάτων schedules που υιοθέτησε. Πλεονέκτημα αυτής της αποδοχής των δύο προγραμμάτων από έναν κόμβο, είναι ότι κάποιοι κόμβοι που βρίσκονται στα σύνορα μεταξύ των δύο γειτονικών συστοιχιών και υιοθετούν τα δύο προγράμματα, απαιτείται να εκπέμψουν προς όλους (broadcast) τους άλλους κόμβους μόνο ένα πακέτο SYNC packet. Μειονέκτημα αυτής της προσέγγισης είναι ότι οι ίδιοι κόμβοι που βρίσκονται στα σύνορα, καταναλώνουν περισσότερη ενέργεια διότι βρίσκονται για λιγότερο χρόνο στην κατάσταση ύπνου. Όμως, οι γειτονικοί κόμβοι

μπορεί να αποτύχουν να ανακαλύψουν ό ένας τον άλλο αν υπάρξει μια απώλεια ενός πακέτου SYNC ή μία καθυστέρηση του πακέτου SYNC. Για να λυθεί αυτό το πρόβλημα, οι κόμβοι στο S-MAC απαιτείται να εκτελούν συχνά τη διαδικασία ανακάλυψης γειτόνων (neighbor discovery). Στη διαδικασία αυτή, ο κόμβος ακούει περιοδικά για όλη την περίοδο συγχρονισμού. Οι κόμβοι που δεν έχουν άλλους γείτονες την τρέχουσα περίοδο, αναμένεται ότι θα εκτελούν πιο συχνά τη διαδικασία ανακάλυψης των γειτόνων.

β) RTS Request to Send.

Αρχή χειραψίας.

γ) CTS Clear to Send.

Ολοκλήρωση χειραψίας.

Οι δύο παραπάνω φάσεις RTS, CTS χρησιμοποιούνται για την χειραψία (handshake) για την αποφυγή συγκρούσεων στην επικοινωνία με το CSMA/CA. (πολυπλεξία με ανίχνευση φέροντος/αποφυγή συγκρούσεων). Με αυτή τη διαδικασία, οι κόμβοι εφαρμόζουν έναν μηχανισμό πολύπλεξης. Επειδή ο κάθε κόμβος δεν μπορεί να ανιχνεύσει αν έγινε μία σύγκρουση, προσπαθεί να αποφύγει τις συγκρούσεις περιμένοντας να ελευθερωθεί το κανάλι. Ο χρόνος που περιμένει, είναι ίσος με τη χρονική διάρκεια που απαιτείται ώστε ένα πακέτο να διαδοθεί στους πιο απομακρυσμένους κόμβους του δικτύου. Όταν ο κόμβος θέλει να εκπέμψει πακέτο δεδομένων, κάνει ανίχνευση (senses) του φέροντος για να δει αν εκπέμπει ή όχι κάποιος άλλος κόμβος. Αν δεν υπάρχουν άλλες μεταδόσεις, τότε ο κόμβος στέλνει ένα πακέτο RTS στον κόμβο προορισμού που πρόκειται να στείλει αργότερα το πακέτο δεδομένων. Αν ο λήπτης είναι αδρανής (idle) και ανιχνεύει το κανάλι για να δει αν είναι ελεύθερο, στέλνει ως απάντηση ένα πακέτο CTS. Μόλις ο αρχικός κόμβος λάβει το πακέτο CTS στέλνει τα πραγματικά δεδομένα στον κόμβο προορισμού. Αν όμως ο κόμβος που έστειλε το RTS μετά από ένα χρονικό διάστημα δεν λάβει το πακέτο CTS, περιμένει για μία τυχαία χρονική περίοδο και μετά επαναλαμβάνει τη διαδικασία RTS/CTS που ονομάζεται χειραψία.

Κάθε φάση SYNC, RTS, CTS, διαιρείται σε σχισμές χρόνου (time slots) και κάθε κόμβος χρησιμοποιεί το μηχανισμό CSMA (πολυπλεξία με ανίχνευση φέροντος) με μία τυχαία υποχώρηση (random back-off) για να στείλει τα πακέτα SYNC, RTS και CTS στους

γείτονές του και στον δέκτη προορισμού (intended receiver). Επίσης κάθε κόμβος μαθαίνει το πρόγραμμα ύπνου (sleep schedule) που έχουν οι γείτονές του.

Μετά από τη φάση SYNC, κάθε κόμβος που θέλει να μεταδώσει ένα πακέτο δεδομένων πρέπει να κάνει ανταγωνισμό για τη χρήση του καναλιού (contend for the channel) με τους άλλους κόμβους που επιθυμούν να χρησιμοποιήσουν το ίδιο κανάλι. Ένας κόμβος (node) ακούει (listens) στο κανάλι και λαμβάνει ένα πακέτο RTS ή CTS και αν ο ίδιος δεν είναι ο δέκτης προορισμού (target receiver) αυτού του πακέτου, εξάγει από το πακέτο και μαθαίνει τις πληροφορίες για τη διάρκεια μετάδοσης δεδομένων από το πεδίο Network Allocation Vector (NAV), και μετά μεταβαίνει στην κατάσταση ύπνου (sleep mode). Επιπλέον, ο κόμβος (node) μπορεί να εκτελεί και μετάδοση και λήψη κατά τη διάρκεια των φάσεων RTS και CTS.

Υπάρχει όμως μία καθυστέρηση (latency) που προκύπτει από αυτή την τεχνική. Στον κύκλο λειτουργίας, το πρωτόκολλο S-MAC επιτρέπει στους κόμβους να μπαίνουν περιοδικά σε κατάσταση ύπνου (sleep). Αυτό έχει το πλεονέκτημα ότι μειώνεται η ενέργεια που καταναλώνεται στους κόμβους, αλλά ένα μειονέκτημα είναι, πως αυξάνεται η καθυστέρηση από σημείο σε σημείο (end to end delay).

Αυτό ισχύει, διότι ο πομπός που στέλνει τα δεδομένα, πρέπει να περιμένει μέχρι ο δέκτης να μεταβεί στην κατάσταση ξυπνήματος (wake up) για να λάβει τα δεδομένα, δηλαδή ο πομπός θα περιμένει να έρθει ο επόμενος κύκλος (cycle) για να μπορέσει να στείλει τα δεδομένα του. Επομένως αυτή η καθυστέρηση εισάγεται από το μηχανισμό του κύκλου λειτουργίας (duty cycle) του S-MAC.

Για την μείωση της καθυστέρησης αυτής, έγινε μία βελτίωση στο S-MAC, που επιτρέπει στους κόμβους (nodes) να πηγαίνουν από το χρόνο ακοής (listening time) στην κατάσταση ύπνου (sleep), σε προσαρμοσμένο χρόνο (adaptively) όταν δεν υπάρχει καμία επικοινωνία. Αυτή η μέθοδος ονομάζεται προσαρμογή του χρόνου που βρίσκεται ο κόμβος σε κατάσταση ακοής (adaptive listening). Σύμφωνα με αυτή τη μέθοδο, οι κόμβοι που έχουν τις πληροφορίες NAV information του πακέτου, ξυπνούν (wake up) περίπου κοντά στο χρόνο που αναμένεται ότι θα έχει τελειώσει η μετάδοση δεδομένων (data transmission) και έτσι οι κόμβοι παραμένουν για μικρότερο χρονικό διάστημα σε κατάσταση ακοής (listening), για να δουν αν έρχονται εισερχόμενα πακέτα. Με αυτό τον τρόπο μειώνονται οι μεγάλοι χρόνοι που οι ενεργοί κόμβοι μένουν αδρανείς (idle times).

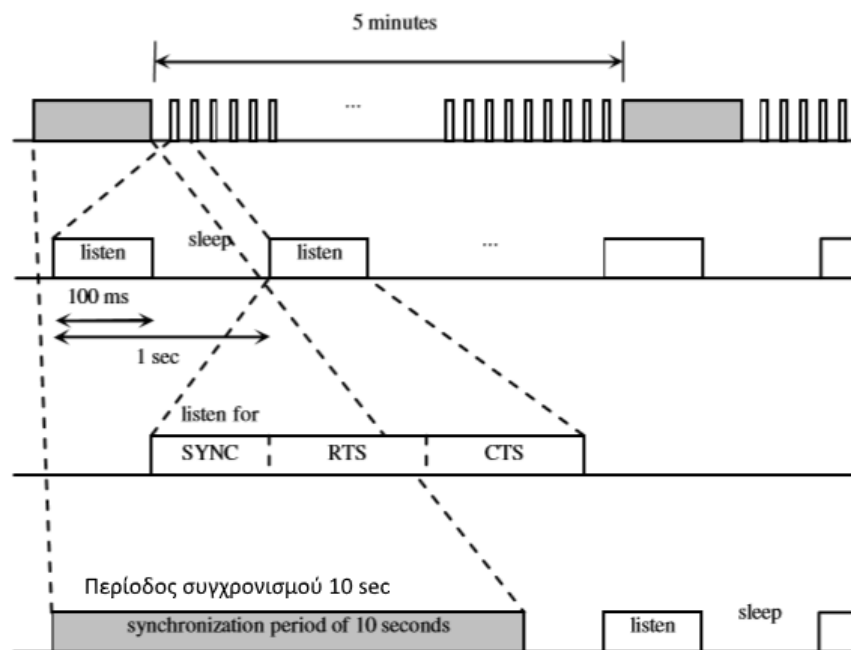
Χρησιμοποιώντας την μέθοδο αυτή, η καθυστέρηση (latency) μειώθηκε στο μισό [42]. Όμως και τότε, ξοδεύεται πάλι σημαντική ποσότητα ενέργειας, στη χρονική διάρκεια που οι κόμβοι είναι ενεργοποιημένοι (active part). Αυτό συμβαίνει είτε όταν οι κόμβοι παραμένουν ενεργοποιημένοι, αλλά αδρανείς (idle) επειδή δεν υπάρχει κάποια δραστηριότητα στο δίκτυο, είτε όταν οι κόμβοι περιμένουν σε κατάσταση ακοής (listening state) για να «ακούσουν» στο δίκτυο να κινούνται κάποια πακέτα δεδομένων και εμφανιστούν πακέτα δεδομένων που δεν προορίζονται για τους συγκεκριμένους κόμβους. Έτσι, χάνεται επιπρόσθετος χρόνος, καθώς οι κόμβοι παραμένουν στην κατάσταση ακοής (overhearing) ο οποίος όμως δεν ήταν απαραίτητος [42].

Οι κόμβοι στα ασύρματα δίκτυα αισθητήρων (WSN) χρειάζεται να απενεργοποιούνται (turned off) για όσο το δυνατόν για περισσότερο χρόνο, ώστε να αυξηθεί η διάρκεια ζωής ολόκληρου του δικτύου. Το πρωτόκολλο S-MAC βασίζεται στο πρότυπο 802.15 IEEE standard, και χρησιμοποιεί τις ίδιες τεχνικές για το διαμοιρασμό του μέσου. Το πρωτόκολλο S-MAC μειώνει την άσκοπη κατανάλωση ενέργειας επειδή εκτελεί διεργασίες με χαμηλό κύκλο λειτουργίας (low duty cycle operations) για όλους τους κόμβους στα ασύρματα δίκτυα αισθητήρων.

Στα ασύρματα δίκτυα αισθητήρων (WSN) συμβαίνει συχνά να υπάρξουν κάποιοι κόμβοι που πρέπει να παραδώσουν ή να λάβουν περισσότερα δεδομένα από άλλους κόμβους. Για αυτές τις περιπτώσεις, το S-MAC χρησιμοποιεί μία τεχνική αποστολής μηνυμάτων που διαιρεί τα μεγάλα μηνύματα (long messages) σε μικρότερα πακέτα και τα μεταδίδει με έναν καταιγισμό (burst). Αυτό γίνεται ώστε αν αποτύχει να παραδώσει ένα μεγάλο μήνυμα, να μη χρειάζεται να ξαναστείλει από την αρχή ολόκληρο το μήνυμα, αλλά να ξαναστείλει μόνο το μικρότερο πακέτο που απέτυχε να παραδοθεί την πρώτη φορά.

Περίληπτική επισκόπηση του S-MAC

Το S-MAC περιγράφεται παρακάτω περιληπτικά, όπου συνοψίζεται ο μηχανισμός λειτουργίας του.



Εικόνα 118. Ο κύκλος συγχρονισμού στο S-MAC, φαίνονται οι περίοδοι Listen, Sleep, Sync. Πηγή: [43]

Όπως είδαμε, στο S-MAC υπάρχουν περιοδικοί κύκλοι λειτουργίας (duty cycles) όπου οι κόμβοι αισθητήρες μεταβαίνουν στις καταστάσεις ύπνου/ξυπνήματος (sleep/wakeup) με ένα συντονισμένο τρόπο. Οι κόμβοι ομαδοποιούνται σε συστοιχίες που ονομάζονται virtual clusters, και σε κάθε συστοιχία όλοι οι κόμβοι ακολουθούν το ίδιο πρόγραμμα schedule. Όμως οι διαφορετικές συστοιχίες σε όλο το δίκτυο δεν χρησιμοποιούν όλες το ίδιο πρόγραμμα schedule για να μεταβαίνουν στις καταστάσεις ύπνου ξυπνήματος (sleep/wakeup). Σε κάθε μία συστοιχία virtual cluster οι κόμβοι την ίδια στιγμή μεταβαίνουν στην κατάσταση ξυπνήματος για να εκπέμψουν ή να λάβουν δεδομένα. Η μετάδοση ακολουθεί την διαδικασία χειραψίας RTS/CTS. Αν ένας κόμβος δεν έχει να μεταδώσει ούτε να λάβει κανένα πακέτο δεδομένων, τότε μεταβαίνει ξανά στην κατάσταση ύπνου.

Η δημιουργία μίας συστοιχίας virtual cluster είναι μία τυχαία διαδικασία που εξαρτάται από τη στιγμή που ξυπνούν πρώτη φορά οι κόμβοι. Όποιος κόμβος ξυπνήσει πρώτος, υιοθετεί ένα αρχικό πρόγραμμα, ενώ ύστερα, όποιος κόμβος ξυπνήσει αργότερα θα υιοθετήσει το ίδιο πρόγραμμα schedule του πρώτου γείτονά του ως το κύριο πρόγραμμα (primary schedule). Καθώς ενεργοποιούνται περισσότεροι κόμβοι, το μέγεθος των συστοιχιών virtual clusters συνεχώς αυξάνεται. Αν ένας κόμβος που έχει το ίδιο πρόγραμμα με γειτονικούς κόμβους ξαφνικά δει έναν νέο γείτονα με άλλο πρόγραμμα, τότε γίνεται συνοριακός κόμβος (border node) και διατηρεί και τα δύο διαφορετικά

προγράμματα. Ο συνοριακός κόμβος χρησιμοποιεί το δευτερεύον πρόγραμμα για να επικοινωνήσει με κόμβους από άλλη συστοιχία virtual cluster.

Για να αποφευχθεί η μετατόπιση χρόνου (time drift), πρέπει περιοδικά να γίνεται ένας επανασυγχρονισμός του κάθε κόμβου. Μετά από έναν προκαθορισμένο αριθμό κύκλων, έστω 10, κάθε κόμβος εκπέμπει το πρόγραμμά του προς τους άλλους κόμβους. Οι γείτονες του ενημερώνουν τις πληροφορίες τους στους δικούς τους πίνακες με προγράμματα (schedule tables) [43].

Ο κάθε κόμβος περιοδικά εκτελεί τη διαδικασία ανακάλυψης γειτόνων (neighbor discovery), για να μην υπάρξει η περίπτωση που δύο γειτονικοί κόμβοι δεν μπορούν να δουν ο ένας τον άλλον, είτε λόγω καταστροφής ενός πακέτου SYNC, είτε λόγω παρεμβολών, είτε επειδή το κανάλι είναι απασχολημένο και αργούν να φτάσουν στην ώρα τους τα πακέτα SYNC. Στη διαδικασία ανακάλυψης γειτόνων η περίοδος συγχρονισμού είναι 10 sec και επαναλαμβάνεται κάθε 5 min αν ο κόμβος έχει ένα γείτονα τουλάχιστον. Επαναλαμβάνεται πιο συχνά αν ο κόμβος δεν έχει καθόλου γείτονες για παράδειγμα κάθε 30 sec αντί για κάθε 5 min. Η περίοδος συγχρονισμού φαίνεται με σκουρο γκρι χρώμα στην παραπάνω εικόνα.

Καταλήγουμε λοιπόν στο συμπέρασμα ότι το S-MAC είναι ένα πρωτόκολλο κατάλληλο για χρήση σε ασύρματα δίκτυα αισθητήρων, που έχουν περιορισμένες δυνατότητες τροφοδοσίας ενέργειας και στατικούς κόμβους. Για να μειωθούν οι απαιτήσεις ενέργειας που δαπανάται άσκοπα στους κόμβους, όταν αυτοί παραμένουν για πολλή ώρα αδρανείς (idle) ενώ βρίσκονται σε κατάσταση ακοής (listening time), οι κόμβοι μεταβαίνουν στην κατάσταση ύπνου (sleep mode) αν δεν χρειάζεται να παραμείνουν ενεργοί (active), δηλαδή, όταν την τρέχουσα χρονική στιγμή, δεν υπάρχουν καθόλου δεδομένα για αποστολή ή λήψη. Υπάρχουν πολλά άλλα πρωτόκολλα MAC που βασίζονται πάνω στο S-MAC. Το κάθε πρωτόκολλο από αυτά δημιουργήθηκε ως μία βελτίωση, για να δώσει κάποιες λύσεις σε διάφορα προβλήματα που αντιμετώπιζε το πρωτόκολλο S-MAC.

4.3.1.2 Timeout-MAC (T-MAC)

Το πρωτόκολλο Timeout MAC (T-MAC) είναι και αυτό μία παραλλαγή του πρωτοκόλλου S-MAC. Χρησιμοποιεί έναν μηχανισμό προσαρμογής του χρόνου που οι κόμβοι βρίσκονται στην κατάσταση ακοής (adaptive listening). Η ιδέα στην οποία βασίζεται το T-MAC είναι να ρυθμίζεται ή να μειώνεται η περίοδος που το δίκτυο είναι πλήρως ενεργό (active period), ανάλογα με τις συνθήκες κυκλοφορίας που επικρατούν στο δίκτυο. Για να διατηρείται μία βέλτιστη διάρκεια για την ενεργή περίοδο (active period), σε συνθήκες που το φορτίο κυκλοφορίας είναι μεταβαλλόμενο, το T-MAC καθορίζει δυναμικά τη διάρκεια της ενεργής περιόδου, κάνοντας απλώς μία παύση (time out) όταν δεν «ακούγονται» πακέτα δεδομένων στο δίκτυο. Έτσι, όταν τελειώσει η φάση συγχρονισμού SYNC, κάθε κόμβος δεν χρειάζεται να παραμένει σε κατάσταση αδράνειας (idle) για όλη την υπόλοιπη διάρκεια της χρονικής περιόδου που το δίκτυο είναι ενεργό (active period), αν δεν υπάρχει καμία δραστηριότητα στο δίκτυο. Το T-MAC για να μειώσει την ακοή σε αδράνεια (idle listening) εισάγει έναν δυναμικό κύκλο λειτουργίας (duty cycle) και η εκπομπή όλων των μηνυμάτων γίνεται με ριπές καταιγισμού (bursts), μεταβλητού μεγέθους, στις ενεργές χρονικές περιόδους (active periods). Στα χρονικά διαστήματα, που μεσολαβούν ανάμεσα στις ενεργές περιόδους, οι κόμβοι παραμένουν στην κατάσταση ύπνου. Στο T-MAC, ο κάθε κόμβος ξυπνάει περιοδικά (wakes up) για να επικοινωνήσει με τους γείτονές του. Μετά, μεταβαίνει ξανά στην κατάσταση ύπνου, μέχρι το επόμενο πλαίσιο (frame).

Τοπολογία. Το δίκτυο διαμορφώνεται με μία τοπολογία που είναι επίπεδη (flat) και είναι ενός άλματος (single-hop). Το πρωτόκολλο T-MAC χρησιμοποιεί μόνο ένα κανάλι συχνότητας για την επικοινωνία.

Επικοινωνία κόμβων. Οι κόμβοι, για να επικοινωνήσουν μεταξύ τους, μεταβαίνουν διαδοχικά, σε μία ακολουθία καταστάσεων : αρχή χειραψίας RTS - τέλος χειραψίας CTS - αποστολή δεδομένων Data - αποστολή πακέτου αναγνώρισης ACK. Με αυτό τον τρόπο, επιτυγχάνεται η αποφυγή συγκρούσεων και η αξιόπιστη μετάδοση.

Χρόνος Ευαισθησίας T_h (threshold time). Ένας κόμβος συνεχίζει να ακούει στο δίκτυο (listening) και πιθανώς να εκπέμπει δεδομένα, για όσο χρόνο βρίσκεται στην ενεργή περίοδο (active period). Αν δεν υπάρχει κάποιο συμβάν ενεργοποίησης (activation event) για ένα χρονικό διάστημα T_h , που είναι ένας χρόνος ευαισθησίας, τότε σταματάει η ενεργή περίοδος (active period). Τότε ο κόμβος μεταβαίνει στην κατάσταση ύπνου. Ο χρόνος ευαισθησίας T_h , καθορίζει μία ελάχιστη διάρκεια χρόνου, που επιτρέπεται να υπάρχει ακοή σε αδράνεια (idle listening) για ένα πλαίσιο (frame). Αυτό έχει ως

αποτέλεσμα, όλοι οι κόμβοι να εκπέμπουν στην αρχή κάθε ενεργής περιόδου (active period).

Συμβάν ενεργοποίησης. Ένα συμβάν ενεργοποίησης (activation event) μπορεί να είναι

α) Η λήξη χρόνου ενός περιοδικού χρονοδιακόπτη timer για τα πλαίσια (frame).

β) Η λήψη ενός πακέτου δεδομένων στην μονάδα ασύρματης επικοινωνίας radio της συσκευής.

γ) Ανίχνευση σήματος επικοινωνίας στη μονάδα ασύρματης επικοινωνίας radio του κόμβου.

δ) Το τέλος μετάδοσης (end of transmission) ενός πακέτου δεδομένων ή ενός πακέτου επιβεβαίωσης λήψης (acknowledgment) που στέλνει ο ίδιος ο κόμβος.

ε) Το τέλος μετάδοσης (end of transmission) ενός πακέτου δεδομένων που στέλνει ένας γειτονικός κόμβος.

Παράθυρο παύσης. Μετά από την φάση τέλους χειραψίας CTS, μόλις ένας κόμβος λάβει ένα πλαίσιο (frame), περιμένει για ένα σύντομο χρονικό διάστημα που ονομάζεται παράθυρο παύσης (timeout window). Αν περάσει ο χρόνος που ορίζει το παράθυρο παύσης (timeout window) και ο κόμβος δεν ανιχνεύσει καμία δραστηριότητα στο δίκτυο τότε ο κόμβος μεταβαίνει στην κατάσταση ύπνου (sleep mode).

Μέγιστος χρόνος πλαισίου. Επειδή οι κόμβοι μεταβαίνουν σε κατάσταση ύπνου, στα χρονικά διαστήματα που μεσολαβούν ανάμεσα στις ενεργές περιόδους (active periods), τότε τα πακέτα δεδομένων θα πρέπει να αποθηκεύονται προσωρινά σε μία μνήμη απομόνωσης (buffered). Η μέγιστη χωρητικότητα της μνήμης απομόνωσης (buffer capacity) που χρησιμοποιείται, καθορίζει ένα ανώτατο όριο για το μέγιστο χρόνο ενός πλαισίου (frame).

Σύγκριση με το S-MAC. Σε σύγκριση με το S-MAC, το T-MAC αφήνει για περισσότερο χρόνο τους κόμβους στην κατάσταση ύπνου (sleep mode) και έτσι η ενέργεια που καταναλώνεται στο T-MAC είναι περίπου το 1/5 της ενέργειας που καταναλώνεται στο S-MAC.

Το T-MAC και το S-MAC έχουν περίπου το ίδιο μεγάλη μείωση στην κατανάλωση ενέργειας, που φτάνει στ 98%, σε σύγκριση με το CSMA. Όμως το T-MAC έχει πιο καλή απόδοση από το S-MAC σε μεταβλητό φορτίο κυκλοφορίας. Αλλά όπως είναι αναμενόμενο, η καθυστέρηση (latency) στο T-MAC είναι αυξημένη, σε σχέση με το S-MAC

επειδή το T-MAC αφήνει τους κόμβους περισσότερο χρόνο σε κατάσταση ύπνου από ότι το S-MAC.

Μειονέκτημα. Επομένως, ένα μειονέκτημα του T-MAC είναι ότι δεν μπορεί να χρησιμοποιηθεί σε δίκτυα που έχουν υψηλό φορτίο κυκλοφορίας δεδομένων, επειδή σε τέτοια δίκτυα υπάρχει απαίτηση για μικρή καθυστέρηση (low latency) και το T-MAC εμφανίζει μεγάλη καθυστέρηση. Επιπλέον, επειδή στο T-MAC η περίοδος που το δίκτυο είναι ενεργό (active period) είναι μικρή, αυτό δεν επιτρέπει στο T-MAC να προσαρμόζεται άμεσα σε ξαφνικές αλλαγές συνθηκών του δικτύου, όταν συμβαίνουν πάρα πολύ γρήγορα.

4.3.1.3 Q-MAC

Το πρωτόκολλο Q-MAC, αφορά την 3^η κατηγορία, από τις τρεις κατηγορίες, που αναφέρθηκαν προηγουμένως, στα είδη των εφαρμογών για τα ασύρματα δίκτυα αισθητήρων (WSN), δηλαδή, αφορά τις εφαρμογές που συλλέγουν τα δεδομένα από τους κόμβους αισθητήρες, με βάση τα ερωτήματα (query based applications).

Σε αυτή την κατηγορία εφαρμογών, οι χρήστες δημιουργούν ένα ερώτημα που λέγεται query και μέσα σε αυτό ζητούν κάποια δεδομένα που τους ενδιαφέρουν (π.χ. Ερώτημα: Ποιες είναι οι τιμές θερμοκρασίας του υγρού στις 3 δεξαμενές που βρίσκονται στην περιοχή A;). Μετά στέλνουν αυτό το ερώτημα (query), στο συγκεκριμένο τμήμα της περιοχής που είναι εγκατεστημένοι οι αντίστοιχοι κόμβοι αισθητήρες (sensor nodes) (π.χ. στο χώρο που βρίσκονται οι 3 δεξαμενές της περιοχής A). Αυτές οι εφαρμογές, μπορούν να έχουν μία αποτελεσματική χρήση της ενέργειας τροφοδοσίας και να ελαχιστοποιήσουν την καθυστέρηση από σημείο σε σημείο (end to end delay latency). Αν δεν υπάρχουν καθόλου ερωτήματα (queries) στο δίκτυο, τότε όλοι οι κόμβοι απενεργοποιούν το υποσύστημα της ασύρματης επικοινωνίας τους (radio) και έτσι εξοικονομούν ενέργεια.

Όμως, αν ένας χρήστης δημιουργήσει ένα ερώτημα (query) και το στείλει στο δίκτυο, τότε αυτόματα θα εκπεμφθούν προς όλους τους κόμβους (broadcast) τα πακέτα για χρονοπρογραμματισμό (scheduling) και για συγχρονισμό (SYNCH). Η επικοινωνία δεδομένων, θα γίνει με βάση τις τοποθεσίες που βρίσκονται οι συγκεκριμένοι κόμβοι τους οποίους αφορά το ερώτημα (query) (π.χ. μόνο οι κόμβοι που βρίσκονται στην περιοχή A και όσοι ενδιάμεσοι κόμβοι απαιτούνται για τη δρομολόγηση στη διαδρομή

που οδηγεί από την περιοχή A προς τον κεντρικό κόμβο sink). Έτσι θα ενεργοποιηθούν μόνο οι κόμβοι που βρίσκονται στην συγκεκριμένη περιοχή και όσοι άλλοι ενδιαμέσοι κόμβοι απαιτούνται για να γίνει η επικοινωνία δεδομένων, ενώ όλοι οι υπόλοιποι κόμβοι του δικτύου θα παραμείνουν στην κατάσταση ύπνου (sleep mode). Με αυτό τον τρόπο αυξάνεται η διάρκεια ζωής του δικτύου (lifetime) επειδή μόνο ένα μέρος του δικτύου παραμένει ενεργό για να εκτελέσει την αντίστοιχη επικοινωνία δεδομένων, ενώ το υπόλοιπο μέρος του δικτύου δεν είναι ενεργό.

Το πρωτόκολλο Q-MAC έχει δύο βασικούς στόχους που είναι οι εξής:

(α) Να μειώσει την καθυστέρηση από άκρο σε άκρο (end to end delay) δίνοντας στους ενδιαμέσους κόμβους (intermediate nodes) εκ των προτέρων πληροφορίες για την κυκλοφορία που υπάρχει στο δίκτυο, χρησιμοποιώντας έναν δυναμικό χρονοπρογραμματισμό (dynamic scheduling).

(β) Να βελτιώσει τη διάρκεια ζωής όλου του δικτύου, ενεργοποιώντας μόνο όσους κόμβους απαιτούνται για μία επικοινωνία δεδομένων, οι οποίοι είναι προκαθορισμένοι σε ένα ερώτημα (query).

Το Q-MAC είναι πολύ γρηγορότερο σε σύγκριση με το S-MAC δηλαδή έχει πολύ μικρότερη καθυστέρηση από σημείο σε σημείο (end to end latency).

Μερικά πλεονεκτήματα του Q-MAC είναι τα παρακάτω:

Το Q-MAC εξοικονομεί ενέργεια επειδή βασίζεται στα ερωτήματα (query based) και ενεργοποιεί μόνο συγκεκριμένους κόμβους που αφορά το κάθε ερώτημα.

Το Q-MAC αυξάνει την απόδοση (throughput) όταν υπάρχουν συνθήκες μεγάλης κυκλοφορίας στο δίκτυο, ενώ το S-MAC έχει μικρότερη απόδοση σε παρόμοιες συνθήκες.

Η καθυστέρηση από σημείο σε σημείο (end to end) είναι μειωμένη στο Q-MAC ενώ είναι μεγαλύτερη στο S-MAC.

Το Q-MAC υποστηρίζει πολλαπλούς προορισμούς (destinations).

Το Q-MAC έχει και μερικά μειονεκτήματα, όπως είναι:

Η αξιοπιστία για την παράδοση δεδομένων από σημείο σε σημείο (end to end) δεν είναι μεγάλη.

Δεν υποστηρίζει τη μη διαστρωματωμένη αρχιτεκτονική (cross layer).

Δεν παρέχει κάποια εγγύηση για την καθυστέρηση από σημείο σε σημείο (end to end) και έτσι δεν μπορεί να χρησιμοποιηθεί άμεσα σε εφαρμογές πραγματικού χρόνου χωρίς να γίνουν κάποιες αλλαγές στο πρωτόκολλο.

4.3.1.4 PEDAMACS

Ένα προτεινόμενο πρωτόκολλο MAC που βασίζεται στο TDMA, είναι το πρωτόκολλο PEDAMACS. Το πρωτόκολλο αυτό, αφορά τα ασύρματα δίκτυα αισθητήρων (WSN) πολλαπλών αλμάτων (multi hop). Σκοπός του είναι να μειώσει την καθυστέρηση από άκρο σε άκρο (end to end delay) και παράλληλα να εξοικονομήσει ενέργεια.

Το PEDAMACS παρέχει μία επέκταση στην πολυπλεξία με διαίρεση χρόνου TDMA ενός άλματος (single hop TDMA) για να χρησιμοποιηθεί σε TDMA πολλαπλών αλμάτων (multi-hop TDMA).

Σύμφωνα με το PEDAMACS, υπάρχει ένα κεντρικό σημείο πρόσβασης Access Point (AP) που επιτρέπει την μετάδοση σημάτων με υψηλή ενέργεια (high power transmission). Αυτό το σημείο πρόσβασης Access Point (AP) στέλνει εξειδικευμένα πακέτα δεδομένων ειδικού σκοπού, σε όλους τους κόμβους του δικτύου, για να συγχρονίσει τις πληροφορίες χρονοπρογραμματισμού (scheduling) των κόμβων, με γειτονικούς κόμβους που βρίσκονται σε απόσταση ενός άλματος (one hop). Αυτό σημαίνει, ότι το PEDAMACS χρησιμοποιεί διαφορετικές μεταδόσεις ειδικών πακέτων που περιέχουν εξειδικευμένες πληροφορίες, για να συλλέγει τα δεδομένα και για να οργανώνει τις πληροφορίες του χρονοπρογραμματισμού ανάμεσα στους κόμβους αισθητήρες.

Το σημείο πρόσβασης (Access Point) (AP) μπορεί να φτάσει σε οποιονδήποτε κόμβο μέσα στο δίκτυο επειδή δεν έχει περιορισμό στην ποσότητα ενέργειας τροφοδοσίας και επίσης επειδή είναι ο προορισμός για όλους τους κόμβους του δικτύου.

Το πρωτόκολλο PEDAMACS χρησιμοποιεί τρεις διαφορετικές εμβέλεις μετάδοσης. Αυτές είναι:

A) Η μέγιστη εμβέλεια μετάδοσης,

Το σημείο πρόσβασης (Access Point) AP χρησιμοποιεί τη μέγιστη εμβέλεια μετάδοσης για να στείλει μήνυμα προς όλους τους κόμβους (broadcast) που περιέχει πληροφορίες της τοπολογίας και χρονοπρογραμματισμού, με ένα άλμα στο δίκτυο (one hop).

Β) Η μεσαία εμβέλεια μετάδοσης

Η μεσαία εμβέλεια μετάδοσης, χρησιμοποιείται για να ανακαλυφθούν πληροφορίες σχετικά με την τοπολογία του δικτύου, τοπικά σε κάποιες περιοχές του δικτύου.

Γ) Η ελάχιστη εμβέλεια μετάδοσης.

Οι κόμβοι αισθητήρες χρησιμοποιούν την ελάχιστη εμβέλεια μετάδοσης για να συλλέξουν δεδομένα στο δίκτυο.

Το πρωτόκολλο PEDAMACS στηρίζεται στις πληροφορίες ανακάλυψης της τοπολογίας του δικτύου, για να οργανώσει τους κόμβους. Χρησιμοποιεί 4 φάσεις με στόχο να ανακαλύψει την τοπολογία του δικτύου, να στείλει μηνύματα (broadcast) σε όλους τους κόμβους και να συλλέξει δεδομένα ανάμεσα στους κόμβους του δικτύου.

Αυτές οι 4 φάσεις περιγράφονται παρακάτω:

Α) Φάση εκμάθησης της τοπολογίας

Το σημείο πρόσβασης AP, χρησιμοποιεί τη φάση εκμάθησης της τοπολογίας για να εκπέμψει προς όλους τους κόμβους (broadcast) κάποια ειδικά πακέτα δεδομένων συντονισμού (coordination packets) που χρησιμοποιούνται για την εκμάθηση της τοπολογίας (topology learning) του δικτύου. Αυτά τα πακέτα εκμάθησης τοπολογίας, αποστέλλονται προς όλους τους κόμβους αισθητήρες ή/και προς άλλους κόμβους μέσα στο δίκτυο, ώστε με βάση τα πακέτα αυτά, να οργανωθούν τα ζητήματα του χρονοπρογραμματισμού (scheduling). Ένα πακέτο δεδομένων εκμάθησης τοπολογίας (Topology learning packet) περιέχει δύο σχισμές χρόνου (time slots), που περιλαμβάνουν τον τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time). Ο τρέχων χρόνος (current time), είναι για τους κόμβους αισθητήρες και πρέπει να ρυθμίσουν τον χρονοπρογραμματισμό (scheduling) τους σύμφωνα με αυτόν τον τρέχοντα χρόνο. Ο

επόμενος χρόνος (next time), είναι χρόνος διακοπής της μετάδοσης σημάτων από τους κόμβους. Σε αυτό το χρόνο, οι κόμβοι σταματούν τη μετάδοσή τους και περιμένουν από το σημείο πρόσβασης (Access Point)(AP) να λάβει 2 νέες διαφορετικές τιμές για τους ίδιους 2 παραπάνω χρόνους, δηλαδή για τον τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time), αντίστοιχα, και αυτές τις νέες τιμές να τις αναθέσει εκ νέου στους κόμβους. Μόλις οι κόμβοι λάβουν ξανά τις καινούργιες τιμές για τον τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time), τότε το σημείο πρόσβασης AP πρέπει να στείλει σε όλους τους κόμβους (broadcast) ένα άλλο πακέτο για να δημιουργήσει την δομή της τοπολογίας, που είναι ένα πακέτο δημιουργίας δέντρου (a tree construction packet). Κάθε κόμβος λαμβάνει αυτό το πακέτο. Το πακέτο ακολουθεί τη διαδρομή (path) από το σημείο πρόσβασης (AP) μέχρι τον κόμβο αισθητήρα. Η διαδρομή αυτή περιλαμβάνει ένα σύνολο ενδιάμεσων κόμβων και προσδιορίζει το βάθος γειτόνων του κάθε κόμβου και δημιουργείται μία τοπολογία δέντρου. Μόλις αυτή η τοπολογία δέντρου δημιουργηθεί, οι κόμβοι πρέπει να στείλουν προς όλους τους κόμβους (broadcast) τις ενημερωμένες πληροφορίες για τον χρονοπρογραμματισμό τους (scheduling) και να φτάσουν σε όλο το δίκτυο.

B) Φάση Συλλογής τοπολογιών

Μόλις το σημείο πρόσβασης (AP) εκπέμπει προς όλους τους κόμβους την φάση εκμάθησης τοπολογίας, μετά πρέπει να μπει στη φάση συλλογής τοπολογιών. Δηλαδή, πρέπει να στείλει προς όλους τους κόμβους (broadcast) κάποια άλλα ειδικά πακέτα δεδομένων, που ονομάζονται πακέτα συλλογής τοπολογιών (topology collection packets), τα οποία θα τα εκπέμπει στην χρονική σχισμή του επόμενου χρόνου (next time slot) από το πακέτο εκμάθησης τοπολογίας (topology learning packet). Μετά, ο κάθε κόμβος θα οργανώσει τη δική του τοπική τοπολογία (local topology) σε μορφή δέντρου, χρησιμοποιώντας τις πληροφορίες που περιέχονται στο πακέτο συλλογής τοπολογιών (topology collecting packet). Αυτές οι πληροφορίες αναφέρουν πως θα δομηθεί το δέντρο της τοπολογίας σε κάθε τμήμα του δικτύου. Μετά οι κόμβοι, θα ακούσουν τους κόμβους-γονείς τους και θα εκπέμψουν προς αυτούς πακέτα με πληροφορίες για την τοπική τοπολογία τους (local topology). Οι κόμβοι για να εκπέμψουν σε άλλους κόμβους πακέτα, πάντα χρησιμοποιούν την ελάχιστη εμβέλεια μετάδοσης (lowest transmission range).

Σε αυτή τη φάση, οι κόμβοι χρησιμοποιούν το CSMA για να ακούν τους γονείς τους και να λάβουν τους 2 χρόνους που αναφέρθηκαν παραπάνω δηλαδή τον τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time), από τα πακέτα τοπολογίας (topology packets) που λαμβάνουν.

Γ) Φάση χρονοπρογραμματισμού

Η φάση του χρονοπρογραμματισμού (Scheduling) αφορά τη δημιουργία πινάκων χρονοπρογραμματισμού (scheduling tables). Οι πίνακες αυτοί δημιουργούνται για όλους τους κόμβους του δικτύου. Το σημείο πρόσβασης AP στέλνει προς όλους τους κόμβους (broadcasts) πακέτα δεδομένων χρονοπρογραμματισμού (scheduling packets) με βάση τις γνώσεις που έχει για τη συνολική τοπολογία του δικτύου, για να ρυθμίσει τους πίνακες χρονοπρογραμματισμού (schedule tables) για κάθε κόμβο του δικτύου. Το κάθε πακέτο χρονοπρογραμματισμού (scheduling packet) περιέχει τον τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time) όπως ισχύει και στις προηγούμενες φάσεις. Αυτό επιτρέπει στους κόμβους να οργανώσουν τους δικούς τους χρόνους και αργότερα, να διαιρέσουν αυτούς τους χρόνους σε σχισμές χρόνου (slots) με βάση τα δεδομένα που πρέπει να μεταδώσει ο κάθε κόμβος στο δίκτυο.

Δ) Φάση αυξομειώσεων

Η φάση αυξομειώσεων (Adjustment Phase) χρησιμοποιείται από το πρωτόκολλο PEDAMACS στο τέλος της φάσης χρονοπρογραμματισμού, για να ολοκληρώσει την τοπολογία του δικτύου, και να προσθέσει κάποιες τροποποιήσεις που απαιτούνται. Τέτοιες τροποποιήσεις είναι η κινητικότητα των κόμβων, η προσθήκη νέων κόμβων, ή άλλες. Αυτές οι τροποποιήσεις εξαρτώνται από την κάθε εφαρμογή. Το σημείο πρόσβασης AP στέλνει προς όλους τους κόμβους (broadcasts) το πακέτο τροποποιήσεων (adjustment packet) για να εξαπλωθούν οι υπόλοιπες πληροφορίες χρησιμοποιώντας τους χρόνους τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time) όπως έγινε και στις προηγούμενες περιπτώσεις. Για την αποστολή χρησιμοποιεί την μεσαία εμβέλεια μετάδοσης. Οι κόμβοι πρέπει να έχουν πρόσβαση σε αυτό το πακέτο για να ανακαλύψουν πως θα οργανώσουν τον χρονοπρογραμματισμό τους (scheduling times) με βάση τους χρόνους τρέχοντα χρόνο (current time) και τον επόμενο χρόνο (next time). Το πακέτο αυξομειώσεων περιλαμβάνει επίσης πληροφορίες που επιτρέπουν

στους κόμβους να αποκτήσουν πρόσβαση στο επόμενο πακέτο αυξομειώσεων. Αυτό το πακέτο το στέλνουν πίσω στο σημείο πρόσβασης AP στον επόμενο χρόνο του τρέχοντος πακέτου. Με αυτό τον τρόπο, όλοι οι κόμβοι μπορούν μετά να δεχτούν πρόσβαση από το σημείο πρόσβασης AP.

Μερικά πλεονεκτήματα του πρωτοκόλλου PEDAMACS είναι:

Επειδή έχει 3 τύπους εμβέλειας μετάδοσης, στην χαμηλότερη εμβέλεια μετάδοσης που χρησιμοποιείται από τους κόμβους του δικτύου, εξοικονομείται ενέργεια κατά την αποστολή και τη λήψη δεδομένων.

Αυξάνεται η απόδοση (throughput) όταν υπάρχει μεγάλη κυκλοφορία στο δίκτυο και τότε γίνεται καλύτερη από την απόδοση του πρωτοκόλλου S-MAC.

Υπάρχει εγγύηση για την καθυστέρηση από σημείο σε σημείο (End to end delay)

Υποστηρίζει τη μη διαστρωματωμένη αρχιτεκτονική (cross layer), σε διάφορα πρωτόκολλα δρομολόγησης.

Ένα μειονέκτημα του PEDAMACS είναι ότι δεν παρέχει εγγύηση για την αξιοπιστία. Έτσι αυτό το πρωτόκολλο δεν μπορεί να χρησιμοποιηθεί σε εφαρμογές πραγματικού χρόνου που απαιτούν εγγυημένη αξιοπιστία.

4.3.1.5 Data gathering MAC (D-MAC)

Το πρωτόκολλο D-MAC είχε τρεις βασικούς στόχους: α) να παρέχει λειτουργία με χαμηλή κατανάλωση ενέργειας β) να παρέχει χαμηλή καθυστέρηση (latency) και γ) να μην υπάρχουν διακοπές στη μετάδοση δεδομένων. Το D-MAC προτάθηκε για να διευθετηθεί το πρόβλημα προώθησης δεδομένων σε διαδρομές πολλαπλών αλμάτων (multihop) που παρουσίαζε διακοπές στην παράδοση δεδομένων [2].

Το πρόβλημα διακοπών στη μετάδοση δεδομένων. Επειδή πολλά πρωτόκολλα MAC χρησιμοποιούν τους κύκλους λειτουργίας (duty cycles) με τους κόμβους του δικτύου για κάποιες χρονικές περιόδους να παραμένουν ενεργοποιημένοι και για άλλες χρονικές περιόδους να παραμένουν σε κατάσταση ύπνου, συχνά εμφανίζεται το πρόβλημα διακοπών στην παράδοση δεδομένων. Το πρόβλημα δημιουργείται, όταν ένας κόμβος που βρίσκεται σε μία διαδρομή δρομολόγησης που κινούνται πακέτα, αντί να μεταδίδει

τα δεδομένα, μεταβαίνει αυτόματα σε κατάσταση ύπνου και ξυπνά στον επόμενο κύκλο, ώστε τα δεδομένα καθυστερούν να μεταδοθούν για έναν κύκλο. Το πρόβλημα του S-MAC ήταν οι διακοπές. Το πρωτόκολλο D-MAC σχεδιάστηκε με στόχο να μειώσει την κατανάλωση ενέργειας και την καθυστέρηση που υπήρχε στο S-MAC. Το D-MAC χρησιμοποιεί ένα κλιμακωτό πρόγραμμα ξυπνήματος (wake-up schedule) για τους κόμβους μιας διαδρομής πολλαπλών αλμάτων, ώστε να επιτρέψει τη συνεχή προώθηση δεδομένων σε μία διαδρομή και να μη γίνονται διακοπές.

Η τοπολογία Δέντρου στο D-MAC. Όπως ισχύει και σε άλλα πρωτόκολλα MAC, έτσι και στο D-MAC χρησιμοποιείται μία τοπολογία δέντρου, για τη συλλογή δεδομένων (data gathering). Αυτή η τοπολογία δομής δέντρου, επιλέγεται σε πολλά πρωτόκολλα MAC, διότι είναι χρήσιμη για τον έλεγχο της κυκλοφορίας των πακέτων δεδομένων στο δίκτυο. Στα ασύρματα δίκτυα αισθητήρων WSN συχνά η κυκλοφορία στο δίκτυο αναπαρίσταται με την τοπολογία ενός δέντρου, ώστε να επιτρέπει στις εφαρμογές να συλλέγουν δεδομένα από πολλαπλούς κόμβους-πηγές (δηλαδή κόμβους που στέλνουν πακέτα δεδομένων) και να προωθούνται όλα τα πακέτα προς έναν μόνο κεντρικό κόμβο sink. Σε αυτή την περίπτωση, ο κεντρικός κόμβος sink θα είναι η ρίζα του δέντρου (root) και όλοι οι κόμβοι αισθητήρες του δικτύου θα είναι τα παιδιά του (children). Με αυτό το είδος τοπολογίας, η κυκλοφορία στο δίκτυο μπορεί να ελεγχθεί πιο εύκολα, από ότι με άλλες τοπολογίες. Η κύρια κυκλοφορία σε ένα ασύρματο δίκτυο αισθητήρων, είναι η συλλογή δεδομένων από τους κόμβους αισθητήρες στον κεντρικό κόμβο sink. Οι διαδρομές από πολλαπλούς κόμβους πηγές, προς έναν κεντρικό κόμβο sink, αποτελούν ένα δέντρο συλλογής δεδομένων (data gathering) που οι ροές είναι μονής κατεύθυνσης και όλοι οι κόμβοι (εκτός από τον sink) προωθούν τα δεδομένα που λαμβάνουν προς το επόμενο άλμα. Για να επιτρέψει την συνεχή προώθηση δεδομένων, σε μία διαδρομή πολλαπλών αλμάτων, το D-MAC δημιουργεί κλιμακωτά το χρονικό πρόγραμμα (schedule) των κόμβων σε μία διαδρομή πολλαπλών αλμάτων (multihop) και επιτρέπει στους κόμβους να ξυπνούν διαδοχικά σαν μία αλυσιδωτή αντίδραση.

Ο χρονοπρογραμματισμός στο D-MAC. Ο Χρονοπρογραμματισμός κύκλου λειτουργίας (duty cycle schedule) είναι ένα πρόγραμμα χρόνου (schedule) που καθορίζει για ποιες χρονικές περιόδους οι κόμβοι θα βρίσκονται σε κατάσταση ύπνου (sleep) και για ποιες περιόδους θα βρίσκονται στην κατάσταση ενεργοποίησης (active state). Στο D-MAC, στο χρονικό πρόγραμμα (schedule), ισχύει ότι ένα σταθερό χρονικό διάστημα (interval) διαιρείται σε τρεις διαφορετικές καταστάσεις ή χρονικές περιόδους :

α) Περίοδος λήψης (receiving), όπου ο κόμβος αναμένεται να λάβει ένα πακέτο δεδομένων και να στείλει ένα πακέτο αναγνώρισης ACK πίσω στον αποστολέα.

β) Περίοδος αποστολής (sending), όπου ο κόμβος προσπαθεί να στείλει ένα πακέτο στο επόμενο άλμα, και να λάβει ένα πακέτο αναγνώρισης ACK.

γ) Περίοδος ύπνου (sleeping), όπου ο κόμβος απενεργοποιεί την ασύρματη μονάδα επικοινωνίας του, για εξοικονόμηση ενέργειας.

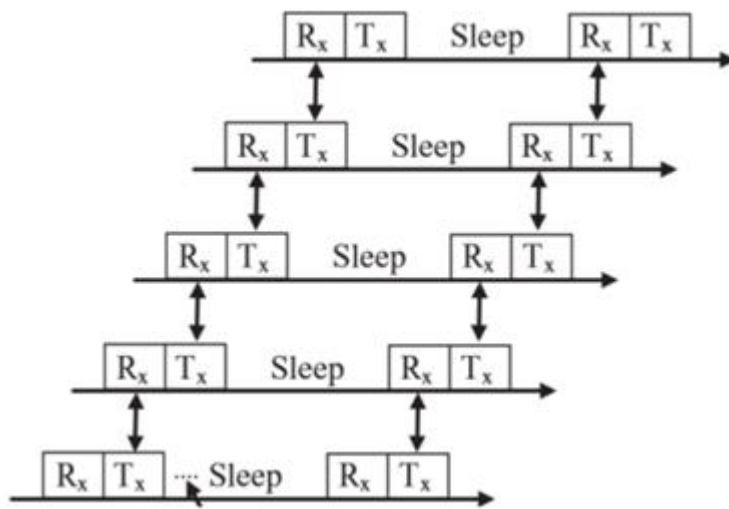
Η περίοδος αποστολής και η περίοδος λήψης έχουν το ίδιο μήκος μ που είναι αρκετό για τη μετάδοση και τη λήψη ενός πακέτου.

Σε αυτή τη δομή δέντρου, κάθε κόμβος έχει διαφορετικό χρονοπρογραμματισμό στον κύκλο λειτουργίας (duty cycle schedule), ανάλογα με το πόσο είναι το βάθος του κόμβου στη δομή του δέντρου. Έστω ότι ο κόμβος στη δομή του δέντρου συλλογής δεδομένων (data gathering tree) βρίσκεται σε ένα βάθος d . Τότε το χρονικό πρόγραμμα ξυπνήματος του κόμβου είναι πιο μπροστά κατά $d \cdot \mu$ από το χρονικό πρόγραμμα του sink, όπου το μ είναι η διάρκεια της περιόδου ύπνου αλλά και η διάρκεια περιόδου ενεργοποίησης.

Οι κόμβοι που βρίσκονται στο ίδιο βάθος του δέντρου d , έχουν τον ίδιο χρονοπρογραμματισμό στον κύκλο λειτουργίας τους (duty cycle schedule).

Έτσι, οι κόμβοι που βρίσκονται στο χαμηλότερο επίπεδο του δέντρου, θα έχουν μεγαλύτερο d και θα είναι σε κατάσταση ύπνου (sleep period) για την μεγαλύτερη χρονική περίοδο σε σύγκριση με άλλους κόμβους επειδή το $d \cdot \mu$ είναι μεγαλύτερο.

Ο κάθε κόμβος, ανάλογα με το βάθος δέντρου που βρίσκεται, πηγαίνει διαδοχικά στις καταστάσεις λήψης, αποστολής, ύπνου, κλιμακωτά. Με αυτή τη μέθοδο, όταν δεν υπάρχουν συγκρούσεις, το πακέτο προωθείται διαδοχικά σε μία διαδρομή πολλαπλών αλμάτων χωρίς να υπάρξει καθυστέρηση (latency) λόγω της κατάστασης ύπνου κάποιων κόμβων.



Εικόνα 119. Κλιμακωτή ενεργοποίηση κόμβων στο D-MAC. Πηγή [2].

Στην εικόνα φαίνονται οι σχισμές χρόνου για τους κόμβους σε κάθε επίπεδο του δέντρου. Κάθε κόμβος, διαδοχικά μεταβαίνει στις περιόδους λήψης, εκπομπής, ύπνου στις αντίστοιχες σχισμές (Rx,Tx,Sleep). Η λύση που δόθηκε με το πρωτόκολλο D-MAC ήταν να δημιουργηθεί ένας χρονοπρογραμματισμός (schedule) στον οποίο η χρονική περίοδος που ένας κόμβος παραμένει σε κατάσταση ύπνου, καθορίζεται από το βάθος που βρίσκεται αυτός ο κόμβος μέσα στο δέντρο. Το D-MAC κάνει προσαρμογές στον κύκλο λειτουργίας και τον αλλάζει ανάλογα με το τρέχον φορτίο κυκλοφορίας στο δίκτυο.

Η πρόσβαση στο κανάλι εκτελείται μέσω CSMA. Το D-MAC χρησιμοποιεί μόνο μία συχνότητα καναλιού για επικοινωνία. Όταν το φορτίο κυκλοφορίας είναι χαμηλό, τότε το πρωτόκολλο D-MAC είναι αποτελεσματικό ως προς την κατανάλωση ενέργειας τροφοδοσίας. Αν όμως το φορτίο κυκλοφορίας γίνει υψηλότερο, τότε στο πρωτόκολλο D-MAC θα προκύψει μία μεγάλη καθυστέρηση (latency) επειδή θα υπάρξει συμφόρηση κυκλοφορίας στους ενδιάμεσους κόμβους.

Η μέθοδος πρόβλεψης (data prediction).

Η έλλειψη πρόβλεψης στο S-MAC. Αυτό που ισχύει στο πρωτόκολλο S-MAC είναι ότι όλοι οι κόμβοι που εκπέμπουν παρεμβολές για τον τρέχοντα κόμβο, μεταβαίνουν στην κατάσταση ύπνου (sleep), και έτσι δεν επιτρέπεται σε κόμβους που βρίσκονται σε απόσταση δύο αλμάτων από τον τρέχοντα κόμβο να του στείλουν ειδοποίηση σχετικά με την κυκλοφορία που υπάρχει στο δίκτυο. Το μειονέκτημα σε αυτή την περίπτωση, είναι ότι κάποιοι κόμβοι που βρίσκονται σε κατάσταση ύπνου (sleep), αν αργότερα χρειαστεί να ενταχθούν στην διαδρομή (path), τότε θα προκληθεί μία καθυστέρηση (delay), διότι θα πρέπει πρώτα να ξυπνήσουν και μετά να ενεργοποιηθούν αυτοί οι κόμβοι. Αυτή η

διαδικασία απαιτεί κάποιο χρόνο. Με την καθυστέρηση θα δημιουργηθούν προβλήματα στην προώθηση των δεδομένων και θα υπάρξουν διακοπές. Επειδή στο S-MAC παρουσιαζόταν αυτό το πρόβλημα με διακοπές στην προώθηση πακέτων δεδομένων, λόγω της έλλειψης πρόβλεψης, το πρωτόκολλο D-MAC, όταν σχεδιάστηκε, είχε ως στόχο του να φέρει βελτίωση και να λύσει αυτό το πρόβλημα. Για αυτό, το D-MAC χρησιμοποίησε μία μέθοδο, πρόβλεψης, στην οποία οι κόμβοι που βρίσκονται σε μία διαδρομή μπορούν να επικοινωνούν μεταξύ τους. Το D-MAC χρησιμοποιεί τεχνικές πρόβλεψης δεδομένων για να συλλέξει τα δεδομένα από τους κόμβους και να τα μεταφέρει προς τον κεντρικό κόμβο sink. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί στην περίπτωση που η κυκλοφορία στο δίκτυο είναι χαμηλή αλλά υπάρχει συγκεντρωμένη μια μεγάλη ποσότητα δεδομένων που πρέπει να προωθηθεί στους ενδιαμέσους κόμβους. Αν ο τρέχων κύκλος λειτουργίας (duty cycle) δεν μπορεί να χειριστεί αυτή τη μετάδοση, τότε ενδέχεται να αυξηθούν τα δεδομένα και να δημιουργηθεί πρόβλημα με ορισμένους κόμβους που θα μεταβούν σε κατάσταση ύπνου. Το D-MAC χρησιμοποιεί ένα μηχανισμό πρόβλεψης για να λύσει το πρόβλημα που παρουσιάζεται, όταν κάθε μεμονωμένος κόμβος πηγή έχει έναν ρυθμό κυκλοφορίας αρκετά χαμηλό για να τον χειριστεί ο βασικός κύκλος λειτουργίας (basic duty cycle), αλλά σε έναν ενδιαμέσο κόμβο ο συγκεντρωμένος ρυθμός κυκλοφορίας είναι μεγαλύτερος από ότι μπορεί να χειριστεί ο βασικός κύκλος λειτουργίας (basic duty cycle). Οι τεχνικές πρόβλεψης δεδομένων θα επιτρέψουν στους κόμβους να παραμείνουν ενεργοποιημένοι για όσο χρόνο χρειάζεται.

Η μέθοδος More to Send (MTS). Το πρωτόκολλο D-MAC χρησιμοποιεί την τεχνική MTS για τους κόμβους στις πολλαπλές διαδρομές (multi paths) για να παραμείνουν ενεργοί όταν ένας κόμβος αποτύχει να στείλει ένα πακέτο δεδομένων στο γονέα του, επειδή πολλά παιδιά ενός κόμβου έχουν να στείλουν πακέτα στην ίδια σχισμή χρόνου. Όταν υπάρχουν πολλοί κόμβοι στο ίδιο επίπεδο του δέντρου συλλογής δεδομένων (data gathering tree) με διαφορετικούς κόμβους γονείς που ανταγωνίζονται μεταξύ τους για τη χρήση του καναλιού, ο μηχανισμός πρόβλεψης δεδομένων δεν έχει τη δυνατότητα να χειριστεί τις παρεμβολές. Σε αυτή την περίπτωση ένα ειδικό πακέτο ελέγχου που ονομάζεται More-to-Send χρησιμοποιείται για να αυξομειώσει τον κύκλο λειτουργίας (duty cycle) στη διάρκεια που γίνονται αυτές οι παρεμβολές.

Ο μηχανισμός ανανέωσης «σχισμή προς σχισμή». Αν ένας κόμβος έχει να στείλει πολλά πακέτα σε μία σχισμή χρόνου sending slot Tx, σχισμή αποστολής, απαιτείται να αυξήσει το δικό του κύκλο λειτουργίας (duty cycle), και θα πρέπει να ζητήσει και από τους άλλους

κόμβους της διαδρομής πολλαπλών αλμάτων να αυξήσουν αναλόγως τους δικούς τους κύκλους λειτουργίας (duty cycles). Για να επιτευχθεί αυτό, το D-MAC έχει ένα μηχανισμό ανανέωσης, σχισμή προς σχισμή (slot by slot) όπου υπάρχει μία μεταβλητή flag που ονομάζεται more data flag στην επικεφαλίδα MAC header και δείχνει την αίτηση για μία επιπρόσθετη περίοδο ενεργοποίησης των κομβών. Αυτό το flag προσθέτει μικρό overhead. Πριν ο κόμβος να μεταδώσει ένα πακέτο, πρώτα θέτει μία τιμή set στην μεταβλητή more data flag στο πακέτο, αν η ενδιάμεση μνήμη του buffer δεν είναι άδεια, ή αν έλαβε ένα πακέτο που έχει τη μεταβλητή more data flag από ένα προηγούμενο άλμα. Ο δέκτης θα ελέγξει την μεταβλητή more data flag αν είναι set στο πακέτο που έλαβε, και αν είναι set, θα θέσει και αυτός τιμή set στη μεταβλητή more data flag στο πακέτο ACK που θα στείλει στον αποστολέα (sender). Με αυτό το μηχανισμό ανανέωσης σχισμή προς σχισμή το D - MAC μπορεί προσαρμοστικά να αυξομειώνει τους κύκλους λειτουργίας (duty cycles) ανάλογα με το φορτίο κυκλοφορίας (traffic load).

Πλεονεκτήματα. Μερικά πλεονεκτήματα του πρωτοκόλλου D-MAC είναι:

Η εξοικονόμηση της ενέργειας χρησιμοποιώντας κατάλληλες τεχνικές του κύκλου λειτουργίας (duty cycling).

Η καθυστέρηση από σημείο σε σημείο (end to end delay) είναι σχετικά μειωμένη.

Οι τεχνικές πρόβλεψης δεδομένων και η συλλογή δεδομένων μειώνουν την καθυστέρηση (delay), ενώ αντιθέτως, στο πρωτόκολλο S-MAC, που δεν χρησιμοποιεί ανάλογες τεχνικές, υπάρχει μεγαλύτερη καθυστέρηση.

Αν συγκρίνουμε το D-MAC με το S-MAC, σε συνθήκες μεγάλης κυκλοφορίας, η απόδοση (throughput) είναι μεγαλύτερη στο D-MAC.

Επίσης, κατά την προώθηση δεδομένων, δεν παρουσιάζονται διακοπές στο D-MAC αλλά στο S-MAC μπορεί να παρουσιαστούν.

Μειονεκτήματα. Το πρωτόκολλο D-MAC έχει και μερικά μειονεκτήματα όπως είναι :

Δεν παρέχει αξιοπιστία για την παράδοση δεδομένων από σημείο σε σημείο (end to end).

Το πρωτόκολλο D-MAC πρέπει να προβλέπει ποιοι κόμβοι θα είναι ενεργοί αργότερα στο ασύρματο δίκτυο αισθητήρων WSN και έτσι, σε κάθε επίπεδο κυκλοφορίας πρέπει να ανακοινώνει ένα επιπλέον πακέτο SYNC, που χρειάζεται, για να μπορέσει να γίνει αυτή η πρόβλεψη. Έτσι, υπάρχει ένα μεγαλύτερο overhead, που δεν υπάρχει σε άλλα πρωτόκολλα τα οποία δεν χρησιμοποιούν αυτή την τεχνική.

Το D-MAC δεν υποστηρίζει την μη-διαστρωματωμένη αρχιτεκτονική (cross layer).

Το πρωτόκολλο D-MAC μπορεί να αντιμετωπίσει προβλήματα αν χρειαστεί να συλλέξει δεδομένα από τυχαίους κόμβους (arbitrary nodes), διότι συλλέγει πάντα τα δεδομένα με συγκεκριμένο τρόπο, που βασίζεται στην τοπολογία δέντρου.

Η καθυστέρηση (delay) από σημείο σε σημείο (end to end) δεν είναι εγγυημένη και συνεπώς αυτό το πρωτόκολλο δεν γίνεται να χρησιμοποιηθεί σε εφαρμογές πραγματικού χρόνου αλλά απαιτείται να γίνουν κάποιες βελτιώσεις.

4.3.1.6 Πρωτόκολλο LEACH

Το πρωτόκολλο LEACH είναι τα αρχικά των λέξεων Προσαρμοστική Ιεραρχία Συστοιχιών με Χαμηλή Κατανάλωση Ενέργειας (Low-Energy Adaptive Clustering Hierarchy). Το πρωτόκολλο LEACH είναι ένα πρωτόκολλο MAC που στηρίζεται στην πολυπλεξία με διαίρεση χρόνου (Time Division Multiple Access) (TDMA) και διαθέτει τα χαρακτηριστικά των συστοιχιών (clustering). Ένα δίκτυο διαμορφώνεται με τοπολογία αστέρα (star) και έχει δύο ιεραρχικά επίπεδα. Το LEACH έχει μία ιεραρχική προσέγγιση και οργανώνει τους κόμβους σε συστοιχίες.

Μία συστοιχία (cluster) είναι μία ομάδα κόμβων που αποτελείται από την κεφαλή της συστοιχίας (cluster head) δηλαδή έναν κόμβο σε ρόλο κεντρικού κόμβου, και τους κανονικούς κόμβους (ordinary nodes). Όλοι οι κανονικοί κόμβοι επικοινωνούν άμεσα με την κεφαλή της δικής τους συστοιχίας. Από την άλλη πλευρά, υπάρχει μόνο ένας σταθμός βάσης που επικοινωνεί άμεσα με όλες τις κεφαλές συστοιχιών (cluster heads). Η άμεση επικοινωνία με μεγάλη ισχύ μετάδοσης, χρησιμοποιείται ώστε να εξασφαλιστεί πως οι κεφαλές συστοιχίας θα μπορούν να στείλουν δεδομένα στον σταθμό βάσης (base station).

Η επικοινωνία ανάμεσα στους κανονικούς κόμβους και την κεφαλή συστοιχίας.

Το LEACH χρησιμοποιεί το TDMA για την επικοινωνία ανάμεσα στους κόμβους και στην κεφαλή συστοιχίας. Ο κόμβος κεφαλή συστοιχίας (cluster head) δημιουργεί ένα πρόγραμμα χρόνου TDMA schedule και μεταδίδει αυτό το πρόγραμμα σε όλους τους κόμβους που ανήκουν στη δική του συστοιχία. Το πρόγραμμα (schedule) επιτρέπει να αποφεύγονται συγκρούσεις στα μηνύματα δεδομένων και επιπλέον επιτρέπει στους

κόμβους να καθορίζουν σε ποιες χρονικές σχισμές slots θα παραμένουν ενεργοί και σε ποιες θα μένουν ανενεργοί. Έτσι ο κάθε κόμβος της συστοιχίας, (εκτός από την κεφαλή συστοιχίας) διατηρεί απενεργοποιημένο το υποσύστημα ασύρματης επικοινωνίας του, μέχρι να έρθουν οι σχισμές χρόνου slots που έχουν κατενεμηθεί σε αυτόν (allocated).

Το πρόγραμμα είναι οργανωμένο σε κύκλους που επαναλαμβάνονται περιοδικά (rounds) και ο κάθε κύκλος διαιρείται σε δύο φάσεις:

α) Τη φάση αρχικής ρύθμισης (setup phase)

β) Τη φάση σταθερής κατάστασης (steady-state phase).

α) Το LEACH υποθέτει ότι οι κόμβοι μιας συστοιχίας ξεκινούν την φάση αρχικής ρύθμισης (setup phase) την ίδια χρονική στιγμή, και στη συνέχεια παραμένουν συγχρονισμένοι. Ένας μηχανισμός συγχρονισμού, είναι να στείλει ο σταθμός βάσης παλμούς (pulses) συγχρονισμού σε όλους τους κόμβους. Η φάση αρχικής ρύθμισης (setup phase) ξεκινάει με τους κόμβους που επιλέγονται από μόνοι τους για να γίνουν κεφαλές συστοιχίας. Μόλις ένας κόμβος ρυθμιστεί κανονικά, για να γίνει κεφαλή συστοιχίας, κάνει έναν ανταγωνισμό με άλλους κόμβους για τη χρήση του καναλιού χρησιμοποιώντας ένα μηχανισμό πολυπλεξίας με ανίχνευση φέροντος (Carrier Sense Multiple Access) (CSMA).

Μετά, αν το κανάλι είναι ανενεργό (idle), ο κόμβος αυτός καταλαμβάνει το κανάλι και εκπέμπει προς όλους τους γείτονές του (broadcasts) ένα πακέτο διαφήμισης (advertisement packet). Όταν ένας κανονικός κόμβος (ordinary node), λαμβάνει διάφορα πακέτα διαφήμισης, από διαφορετικούς κόμβους, που ανταγωνίζονται για να γίνουν κεφαλές συστοιχίας, τότε ο κανονικός κόμβος, επιλέγει μία κεφαλή συστοιχίας, με βάση την ισχύ του σήματος που λαμβάνει.

Στη συνέχεια, κάνει ανταγωνισμό με άλλους κόμβους, για τη χρήση του καναλιού με CSMA και απαντάει στην κεφαλή συστοιχίας που διάλεξε, στέλνοντας της ένα σήμα αναγνώρισης λήψης πακέτου (acknowledgment). Με αυτό τον τρόπο, ζητάει να συνδεθεί στη συστοιχία. Τότε άμεσα η κεφαλή συστοιχίας στέλνει ένα χρονικό πρόγραμμα (schedule) TDMA προς όλους τους κόμβους που είναι μέλη της συστοιχίας. Η συστοιχία διαμορφώνεται πλήρως όταν όλα τα μέλη της συγχρονίζονται στο χρονικό πρόγραμμα

(schedule) TDMA. Η κεφαλή συστοιχίας δημιουργεί και διατηρεί το χρονικό πρόγραμμα (schedule) TDMA.

β) στη φάση της σταθερής κατάστασης, υπάρχουν δύο περιπτώσεις επικοινωνίας:

1. η επικοινωνία μεταξύ των κανονικών κόμβων και της κεφαλής συστοιχίας,
2. η επικοινωνία της κεφαλής συστοιχίας με τον σταθμό βάσης.

1. Επικοινωνία κανονικών κόμβων και της κεφαλής συστοιχίας.

Για την επικοινωνία των κόμβων με την κεφαλή της συστοιχίας τους, πρέπει να υπάρχει μείωση των παρεμβολών μεταξύ των διαφορετικών γειτονικών συστοιχιών (intercluster interference). Για αυτό το σκοπό, το LEACH χρησιμοποιεί μία μορφή ανάθεσης διαφορετικών κωδικών στους πομπούς. Οι επικοινωνίες ανάμεσα σε έναν κόμβο και στην κεφαλή συστοιχίας γίνονται με τη μορφή ευθείας ακολουθίας με εξάπλωση φάσματος (direct-sequence spread spectrum) (DSSS). Σύμφωνα με αυτή την διαμόρφωση, σε κάθε συστοιχία ανατίθεται ένας μοναδικός κώδικας εξάπλωσης (spreading code), που χρησιμοποιείται από όλους τους κόμβους της ίδιας συστοιχίας για να εκπέμψουν δεδομένα προς την κεφαλή συστοιχίας τους. Οι κώδικες εξάπλωσης (spreading codes) είναι διαφορετικοί μεταξύ τους και ανατίθενται στις κεφαλές συστοιχίας με τη μέθοδο «πρώτη έρχεται, πρώτη εξυπηρετείται» και ξεκινάει από την πρώτη κεφαλή συστοιχίας που ανακοινώνει τη θέση της και ακολουθείται διαδοχικά από τις επόμενες κεφαλές συστοιχίας. Οι κόμβοι απαιτείται επίσης να αυξομειώνουν την ισχύ του πομπού τους για να μειωθούν οι παρεμβολές με τις γειτονικές συστοιχίες.

2. Η επικοινωνία της κεφαλής συστοιχίας με το σταθμό βάσης

Όταν μία κεφαλή συστοιχίας λάβει πακέτα δεδομένων από τους κόμβους της, τότε η κεφαλή συστοιχίας συναθροίζει (aggregates) τα δεδομένα πριν να τα στείλει στο σταθμό βάσης. Η επικοινωνία ανάμεσα στην κεφαλή συστοιχίας και στο σταθμό βάσης επιτυγχάνεται με έναν σταθερό κώδικα εξάπλωσης (spreading code) του σταθμού βάσης και με διαμόρφωση CSMA.

Πριν να εκπέμψει δεδομένα προς τον σταθμό βάσης, η κεφαλή συστοιχίας πρέπει να ανιχνεύσει (sense) το κανάλι ώστε να βεβαιωθεί ότι την ίδια στιγμή δεν υπάρχει άλλη κεφαλή συστοιχίας που να εκπέμπει δεδομένα με τον ίδιο κώδικα εξάπλωσης του σταθμού βάσης (base station). Αν το κανάλι είναι απασχολημένο, η κεφαλή συστοιχίας καθυστερεί τη μετάδοση δεδομένων μέχρι το κανάλι να γίνει ανενεργό (idle). Όταν

συμβεί αυτό τότε η κεφαλή συστοιχίας στέλνει τα δεδομένα στο σταθμό βάσης χρησιμοποιώντας τον δικό του κώδικα εξάπλωσης.

3. Η εξοικονόμηση ενέργειας

Το πρωτόκολλο LEACH υλοποιεί δύο μεθόδους, για να εξασφαλιστεί ότι θα υπάρξει μία εξοικονόμηση ενέργειας, κατά τη λειτουργία του δικτύου.

Η πρώτη μέθοδος, είναι να εναλλάσσεται ο κόμβος που έχει ρόλο κεφαλής συστοιχίας, διαδοχικά με άλλους κόμβους από την ίδια συστοιχία. Το LEACH αναθέτει το ρόλο κεφαλής συστοιχίας, με τη σειρά, σε άλλους κόμβους, ώστε να μην είναι πάντα ο ίδιος κόμβος κεφαλή συστοιχίας και να αλλάζει κατά ίσα χρονικά διαστήματα με μία κυκλική εναλλαγή (rotating). Ο λόγος που το κάνει αυτό, είναι διότι η κεφαλή συστοιχίας καταναλώνει περισσότερη ενέργεια για να λάβει δεδομένα, ενώ οι κανονικοί κόμβοι καταναλώνουν λιγότερη ενέργεια. Αν παραμείνει ένας κόμβος κεφαλή συστοιχίας για περισσότερο χρόνο, τότε η ενέργεια του κόμβου αυτού θα εξαντληθεί πολύ γρήγορα ενώ οι υπόλοιποι κόμβοι, θα έχουν ακόμη αρκετή εναπομένουσα ενέργεια. Για να μη συμβεί αυτό, το πρωτόκολλο LEACH αναθέτει το ρόλο της κεφαλής συστοιχίας διαδοχικά σε όλους τους κόμβους και έτσι μετατοπίζεται το συνολικό φορτίο κατανάλωσης ενέργειας, από έναν μόνο κόμβο, σε όλους τους κόμβους. Έτσι οι κόμβοι σε μία συστοιχία εξαντλούν την ενέργειά τους όλοι μαζί ομοιόμορφα στη διάρκεια του χρόνου και όλα τα μέλη της συστοιχίας έχουν περίπου την ίδια απομένουσα ενέργεια.

Μια άλλη μέθοδος εξοικονόμησης ενέργειας, που χρησιμοποιείται από το LEACH, είναι ότι θέτει τους κανονικούς κόμβους (ordinary nodes) σε κατάσταση ύπνου (sleep mode) σε κάποιες σχισμές χρόνου (slots) του TDMA που είναι ανενεργές. Με αυτό τον τρόπο, στο TDMA, δημιουργείται ένας χαμηλός κύκλος λειτουργίας (low duty cycle) που βασίζεται σε ένα χρονικό πρόγραμμα (schedule), το οποίο περιλαμβάνει κάποιες ενεργές σχισμές χρόνου (active slots) και κάποιες ανενεργές σχισμές χρόνου (inactive slots) του TDMA. Με αυτό τον τρόπο αποφεύγεται το overhearing και αυξάνεται αρκετά ο χρόνος διάρκειας ζωής του δικτύου.

Όμως κατά την άμεση επικοινωνία που έχουν όλες οι κεφαλές συστοιχίας με τον σταθμό βάσης, απαιτείται μια μεγάλη ισχύς μετάδοσης (high transmission power). Τότε για ολόκληρο το δίκτυο αυτή η ενέργεια, είναι το μεγαλύτερο μέρος της συνολικής ενέργειας που καταναλώνεται.

Επιπλέον, η δομή με συστοιχίες που είναι σταθερές, απαιτεί έναν γενικό συγχρονισμό και έτσι η επεκτασιμότητα του δικτύου γίνεται πολύ δύσκολα, είτε όταν εισάγονται νέοι κόμβοι στο δίκτυο, είτε όταν αποσυνδέονται κάποιοι κόμβοι. Έτσι όταν οι κόμβοι είναι κινητοί, υπάρχουν πολλά προβλήματα και το πρωτόκολλο LEACH δεν μπορεί να τους διαχειριστεί σωστά.

Συνήθως τα πρωτόκολλα που βασίζονται σε ένα πρόγραμμα χρονικό (schedule) δεν έχουν συγκρούσεις και έτσι δεν έχουν απώλεια ενέργειας που να οφείλεται σε συγκρούσεις.

4.3.1.7 Το πρωτόκολλο SRSA

Αυτό το πρωτόκολλο ονομάζεται έτσι από τα αρχικά Αυτό-οργανωμένη Ανακατανομή Σχισμών Χρόνου (Self-Organising Slot Allocation) (SRSA) και είναι ένα πρωτόκολλο MAC το οποίο σχεδιάστηκε με στόχο να βελτιώσει το πρωτόκολλο LEACH που αναφέρθηκε προηγουμένως. Οι βελτιώσεις που έγιναν, αφορούσαν την εξοικονόμηση ενέργειας και την επεκτασιμότητα του δικτύου.

Το πρωτόκολλο SRSA βασίζεται στο TDMA και έχει την ίδια τοπολογία δικτύου που έχει και το LEACH.

Η μέθοδος που εφαρμόζει το πρωτόκολλο SRSA για να εξοικονομήσει ενέργεια, είναι να χρησιμοποιεί πολλαπλούς σταθμούς βάσης σε αντίθεση με το πρωτόκολλο LEACH που χρησιμοποιούσε μόνο έναν σταθμό βάσης για όλες τις κεφαλές συστοιχίας. Έτσι, στο SRSA οι κεφαλές συστοιχίας μπορούν να επικοινωνούν άμεσα με τον κοντινότερο σταθμό βάσης. Αυτό έχει ως αποτέλεσμα να μην απαιτούν πολύ μεγάλη ισχύ μετάδοσης διότι ο σταθμός βάσης βρίσκεται σχετικά κοντά στους κόμβους. Με αυτό τον τρόπο, μειώνεται σημαντικά η κατανάλωση ενέργειας για την επικοινωνία των κεφαλών συστοιχίας με τους σταθμούς βάσης. Για να δώσει μια λύση στο πρόβλημα επεκτασιμότητας του δικτύου, το πρωτόκολλο SRSA, παρέχει έναν τοπικό συγχρονισμό. Για τον τοπικό συγχρονισμό, κάθε συστοιχία διατηρεί ένα δικό της τοπικό πλαίσιο δεδομένων MAC, που βασίζεται στο TDMA, και ονομάζεται local TDMA MAC frame.

Σε αυτή τη μέθοδο, όταν ξεκινά μία επικοινωνία, αρχικά γίνεται μία τυχαία ανακατανομή σχισμών TDMA. Στη συνέχεια όμως, αυτή η ανακατανομή αλλάζει προσαρμοστικά, σε κάθε συστοιχία και δημιουργείται, τοπικά μέσα στην συστοιχία, ένα νέο χρονικό

πρόγραμμα ανακατανομής των σχισμών (slot allocation schedule). Το τοπικό πρόγραμμα ανακατανομής σχισμών, βασίζεται σε πληροφορίες που λαμβάνονται για τις συγκρούσεις πακέτων δεδομένων ανάμεσα σε τοπικούς κόμβους που βρίσκονται μέσα στην συστοιχία. Έτσι σε κάθε συστοιχία, γίνεται ένας διαφορετικός τοπικός συγχρονισμός (local synchronisation) και δεν γίνεται ένας γενικός συγχρονισμός (global synchronisation), ίδιος για όλες τις συστοιχίες, όπως ισχύει στο πρωτόκολλο LEACH.

Για αυτό τον λόγο, όταν πρόκειται να δημιουργηθούν μεγάλα δίκτυα, η επεκτασιμότητα που επιτυγχάνεται με το πρωτόκολλο SRSA, βασίζεται μόνο στον τοπικό συγχρονισμό μέσα σε μία μεμονωμένη συστοιχία (cluster).

Όμως αν συνδεθούν πολλοί νέοι κόμβοι στο δίκτυο, θα πρέπει να γίνεται συχνά ένας τοπικός συγχρονισμός. Αυτό είναι μειονέκτημα της μεθόδου, διότι με συχνούς τοπικούς συγχρονισμούς καταναλώνεται μεγάλη ποσότητα ενέργειας στους κόμβους. Έτσι η συνολική ενέργεια του δικτύου μπορεί να μειωθεί, και το κέρδος που υπήρχε αρχικά από την εξοικονόμηση ενέργειας, να μειωθεί σημαντικά λόγω της την κατανάλωσης ενέργειας που προκαλούν οι συχνοί τοπικοί συγχρονισμοί.

4.3.1.8 Zebra MAC (Z-MAC)

Το πρωτόκολλο Z-MAC συνδυάζει τα πλεονεκτήματα και του CSMA και του TDMA, για αυτό λέγεται υβριδικό. Το Z-MAC χρησιμοποιεί το CSMA ως το βασικό μηχανισμό για το στρώμα MAC και χρησιμοποιεί ένα πρόγραμμα TDMA (schedule) ως ένα βοήθημα για να βελτιώσει την επίλυση συγκρούσεων.

Τοπολογία. Το δίκτυο διαμορφώνεται με μία τοπολογία που είναι επίπεδη και πολλαπλών αλμάτων (multi-hop). Οι κόμβοι είναι σταθεροί στις θέσεις τους.

Φάση Αρχικής ρύθμισης. Η φάση αρχικής ρύθμισης (setup phase) είναι η πιο κρίσιμη φάση για το πρωτόκολλο και περιλαμβάνει τις παρακάτω διαδικασίες:

Ανακάλυψη των γειτονικών κόμβων (neighbors) .

Τοπική ανταλλαγή πλαισίων (frame exchange) για τις λίστες των γειτόνων.

Ανάθεση των σχισμών χρόνου (slots) σε κόμβους.

Όλοι οι κόμβοι είναι συγχρονισμένοι με βάση ένα γενικό χρόνο (global time) που είναι μία παράμετρος συγχρονισμού.

Σε κάθε κόμβο ανατίθεται μία σχισμή χρόνου (slot) αλλά αυτή δεν είναι σταθερή. Οποιοσδήποτε κόμβος μπορεί να ανταγωνιστεί με άλλους κόμβους για τη χρήση του καναλιού (contend for the channel) μέσα σε οποιαδήποτε σχισμή (slot) για μετάδοση δεδομένων, αλλά πάντα την υψηλότερη προτεραιότητα θα την έχει εκείνος ο κόμβος στον οποίον ανατέθηκε η σχισμή (slot).

Σε μία κατάσταση υπάρχει υψηλός ανταγωνισμός (high contention), η ανάθεση των σχισμών (slots) γίνεται εξαναγκασμένη ώστε να μειωθούν οι συγκρούσεις (collisions).

Η ανάθεση των σχισμών (slot assignment) βασίζεται σε έναν αλγόριθμο χρονοπρογραμματισμού που ονομάζεται DRAND. Αφότου γίνει η ανάθεση των σχισμών, ο κάθε κόμβος περιοδικά επαναχρησιμοποιεί τη σχισμή που του ανατέθηκε σε κάθε προκαθορισμένη περίοδο που ονομάζεται πλαίσιο. Ένας κόμβος που έχει ανατεθεί σε μία σχισμή slot, ονομάζεται ιδιοκτήτης (owner) της σχισμής slot και οι άλλοι ονομάζονται μη ιδιοκτήτες (non-owners) της ίδιας σχισμής. Ο αλγόριθμος DRAND επιτρέπει σε δύο κόμβους γείτονες που απέχουν πάνω από δύο άλματα (2-hop) να γίνουν ιδιοκτήτες της ίδιας χρονικής σχισμής slot και έτσι μία σχισμή slot μπορεί να έχει περισσότερους από έναν ιδιοκτήτες. Αντίθετα με ότι ισχύει στο TDMA, ένας κόμβος μπορεί να εκπέμψει δεδομένα σε οποιαδήποτε χρονική σχισμή στο Z-MAC.

Ο κόμβος δεν είναι απαραίτητο να εκπέμψει τα δεδομένα του στην αρχή μίας σχισμής slot, αλλά σε οποιοδήποτε σημείο της διάρκειάς της. Πριν ο κόμβος να εκπέμψει δεδομένα στη διάρκεια μίας σχισμής slot, πάντα εκτελεί μία ανίχνευση φέροντος (carrier sensing) και εκπέμπει ένα πακέτο όταν το κανάλι είναι αδρανές. Όμως, ένας κόμβος που είναι ιδιοκτήτης (owner) εκείνης της σχισμής πάντοτε έχει μεγαλύτερη προτεραιότητα από τους μη ιδιοκτήτες (non-owners) για την πρόσβαση στο κανάλι.

Για να υλοποιηθεί η προτεραιότητα, το Z-MAC αυξομειώνει το μέγεθος του αρχικού παράθυρου συγκρούσεων (initial contention window), ώστε πάντα οι ιδιοκτήτες (owners) να έχουν πιθανότητες να εκπέμψουν τα δεδομένα τους νωρίτερα από ότι οι μη ιδιοκτήτες (non-owners). Με τον τρόπο αυτό, το Z-MAC μειώνει τις πιθανότητες συγκρούσεων στις σχισμές slots όταν οι ιδιοκτήτες (owners) έχουν δεδομένα για να μεταδώσουν. Αν σε μία σχισμή slot, οι ιδιοκτήτες (owners) δεν έχουν να μεταδώσουν δεδομένα, τότε οι μη ιδιοκτήτες (non-owners) μπορούν να την χρησιμοποιήσουν. Για αυτό

το Z-MAC αυξομειώνει δυναμικά τη συμπεριφορά του MAC ανάμεσα στο CSMA και στο TDMA, με βάση το πλήθος συγκρούσεων που υπάρχουν στο δίκτυο.

Πεδίο preamble. Οποιαδήποτε μετάδοση πακέτου δεδομένων (data transmission) που γίνεται με το πρωτόκολλο Z-MAC, περιλαμβάνει στην αρχή του πακέτου δεδομένων ένα επιπρόσθετο πεδίο δεδομένων preamble, που είναι αρκετά μεγάλο. Ο λόγος που υπάρχει τόσο μεγάλο πεδίο preamble είναι, ότι με αυτό τον τρόπο το πακέτο δεδομένων θα διαρκεί περισσότερο χρόνο και έτσι θα αυξηθεί η πιθανότητα να φτάσει στο δέκτη, στην χρονική περίοδο που ο δέκτης είναι πλήρως ενεργός (receiver's active period).

Συγχρονισμός. Επειδή το Z-MAC απαιτεί μόνο τοπικό συντονισμό ανάμεσα στους γειτονικούς κόμβους που στέλνουν δεδομένα και βρίσκονται σε απόσταση δύο αλμάτων (2- hop), χρησιμοποιείται ένας απλός μηχανισμός τοπικού συγχρονισμού, στον οποίο κάθε κόμβος που στέλνει δεδομένα αυξομειώνει τη συχνότητα συγχρονισμού του με βάση τον τρέχοντα ρυθμό δεδομένων του και τους πόρους που διαθέτει (resource budget).

Μεγάλο Overhead. Στο Z-MAC, η ανάθεση (assignment) σχισμών slot εκτελείται στον αρχικό χρόνο που γίνεται η ανάπτυξη του δικτύου και αυτό έχει το μειονέκτημα του μεγάλου overhead. Το σκεπτικό στο οποίο βασίστηκε αυτή η σχεδίαση, ήταν ότι το αρχικό overhead, που είναι μεγάλο, κατανέμεται σε μία μεγάλη χρονική περίοδο λειτουργίας του δικτύου και σταδιακά αντισταθμίζεται από την βελτιωμένη απόδοση throughput και από την χαμηλή κατανάλωση ενέργειας.

Πλεονεκτήματα. Το βασικό χαρακτηριστικό του Z-MAC είναι ότι προσαρμόζεται σε δυναμικές μεταβολές του πλήθους συγκρούσεων στο δίκτυο. Όταν υπάρχουν λίγες συγκρούσεις, συμπεριφέρεται όπως το CSMA και μπορεί να επιτύχει υψηλό βαθμό χρήσης του καναλιού και μικρή καθυστέρηση. Όταν υπάρχουν πολλές συγκρούσεις συμπεριφέρεται όπως το TDMA και μπορεί να επιτύχει έναν υψηλό βαθμό χρήσης καναλιού και να μειώσει τις συγκρούσεις ανάμεσα σε γείτονες που βρίσκονται σε απόσταση δύο αλμάτων (2 - hop) και με χαμηλό κόστος. Επιπλέον είναι και ανθεκτικό σε λάθη συγχρονισμού στο χρόνο, σε αποτυχίες ανάθεσης σχισμών (slot assignment failures), μεταβαλλόμενες συνθήκες του καναλιού και δυναμικές αλλαγές στην τοπολογία του δικτύου. Έτσι ένα σύστημα Z-MAC έχει καλύτερη απόδοση από ότι ένα σύστημα που είναι μόνο TDMA. Στη χειρότερη περίπτωση, επιστρέφει πάλι στο CSMA.

Μειονεκτήματα. Το πρωτόκολλο Z-MAC έχει διάφορα μειονεκτήματα όπως είναι η μεγάλη καθυστέρηση (latency), και η μεγάλη σπατάλη ενέργειας που απαιτείται για τη μετάδοση ενός μεγάλου πεδίου preamble στα πακέτα δεδομένων.

Ένα άλλο μειονέκτημα είναι ότι οι κόμβοι πρέπει να είναι σταθεροί. Αυτό περιορίζει την επεκτασιμότητα του δικτύου.

Αν συνδεθούν νέοι κόμβοι στο δίκτυο, η φάση αρχικής ρύθμισης θα πρέπει να επαναλαμβάνεται διαρκώς.

4.3.1.9 Το πρωτόκολλο RMAC

Το πρωτόκολλο RMAC έλαβε αυτή την ονομασία από τα αρχικά των λέξεων Βελτιωμένος Κύκλος Λειτουργίας ως προς τη Δρομολόγηση (Routing Enhanced Duty Cycle MAC). Το RMAC είναι ένα πρωτόκολλο MAC που υποστηρίζει την μη διαστρωματωμένη αρχιτεκτονική (cross layer). Αυτό το πρωτόκολλο σχεδιάστηκε για να γίνουν κάποιες βελτιώσεις σε άλλα πρωτόκολλα που αναφέρθηκαν προηγουμένως, όπως είναι τα S-MAC, D-MAC, έτσι ώστε να μειωθεί η κατανάλωση ενέργειας, και οι καθυστερήσεις στη μετάδοση δεδομένων.

Το RMAC, επιτρέπει στους κόμβους που βρίσκονται στην διαδρομή (path) που οδηγεί από τους κόμβους πηγές προς τον κεντρικό κόμβο sink να μεταβούν στην κατάσταση ύπνου (sleep) και να ξυπνούν με έναν έξυπνο τρόπο (intelligently wake up) όταν χρειαστεί να στείλουν ή να λάβουν δεδομένα, στα δίκτυα πολλαπλών αλμάτων (multi-hop).

Επιπλέον, το RMAC επιτυγχάνει σημαντικές βελτιώσεις για την παράδοση δεδομένων από άκρο σε άκρο (end to end), σε έναν μόνο κύκλο στα δίκτυα πολλαπλών αλμάτων. Το RMAC μειώνει περισσότερο τις συγκρούσεις από ότι το πρωτόκολλο S-MAC. Το RMAC στέλνει ένα πλαίσιο ελέγχου (control frame) κατά μήκος της διαδρομής (path) και αυτό επιτρέπει στους κόμβους που βρίσκονται στην επιλεγμένη διαδρομή να γνωρίζουν την κυκλοφορία του δικτύου πριν να μεταδοθούν τα πραγματικά πακέτα δεδομένων. Μερικά πλεονεκτήματα του RMAC είναι:

Το RMAC εξοικονομεί ενέργεια διότι χρησιμοποιεί έναν μόνο κύκλο λειτουργίας (single duty cycle).

Σε περιπτώσεις που η κυκλοφορία στο δίκτυο είναι μεγάλη, το RMAC έχει αυξημένη απόδοση (throughput) που είναι μεγαλύτερη από αυτήν που επιτυγχάνεται με το S-MAC.

Υποστηρίζει ένα επίπεδο δρομολόγησης (routing layer) που επιτρέπει τη μη διαστρωματωμένη αρχιτεκτονική (cross layer).

Η καθυστέρηση από σημείο σε σημείο είναι μειωμένη.

Ένα μειονέκτημα του πρωτοκόλλου R-MAC είναι ότι δεν παρέχει εγγύηση για την καθυστέρηση και για την αξιοπιστία στην παράδοση δεδομένων από σημείο σε σημείο και έτσι δεν είναι κατάλληλο για τις εφαρμογές πραγματικού χρόνου.

4.3.2 Η Επέκταση στο S-MAC για Εισαγωγή Κινητικότητας

Για την εισαγωγή κινητικότητας στα ασύρματα δίκτυα αισθητήρων, προτάθηκε για το SMAC μία επέκταση που ονομάστηκε MS-MAC (Mobility Sensor MAC). [43]. Οι συγγραφείς, είχαν στόχο να σχεδιάσουν ένα πρωτόκολλο MAC που θα λειτουργούσε αποτελεσματικά και για στατικά δίκτυα και για σενάρια κινητικότητας. Με βάση το S-MAC έκαναν μία επέκταση του πρωτοκόλλου με στόχο να υποστηριχθούν οι κινητοί κόμβοι αισθητήρες. Το MS-MAC για τα στατικά δίκτυα έχει προταθεί να έχει ακριβώς την ίδια λειτουργία όπως και το S-MAC. Όταν υπάρχουν πολλοί κινητοί κόμβοι μπορούν οι κόμβοι να παρεμένουν «ξύπνιοι» (awake) για μεγαλύτερο χρονικό διάστημα από ότι στα στατικά δίκτυα. Στο πρωτόκολλο MS-MAC ορίστηκε η έννοια της ενεργής ζώνης (active zone) που είναι ένα σύνολο κόμβων γύρω από τον κινητό κόμβο οι οποίοι έχουν μία μεγαλύτερη επανάληψη συχνότητας της περιόδου συγχρονισμού, για να βοηθήσουν τον κινητό κόμβο να κάνει γρήγορα νέες συνδέσεις με τους γειτονικούς κόμβους και να μην αποσυνδεθεί από το δίκτυο. Οι κόμβοι που δεν βρίσκονται στην ενεργή ζώνη, έχουν την κανονική λειτουργία και οι περίοδοι συγχρονισμού τους επαναλαμβάνονται πιο αργά. Αυτή η διαδικασία εξηγείται παρακάτω στις επόμενες παραγράφους.

4.3.2.1 Μειονεκτήματα του S-MAC για Κινητούς Κόμβους

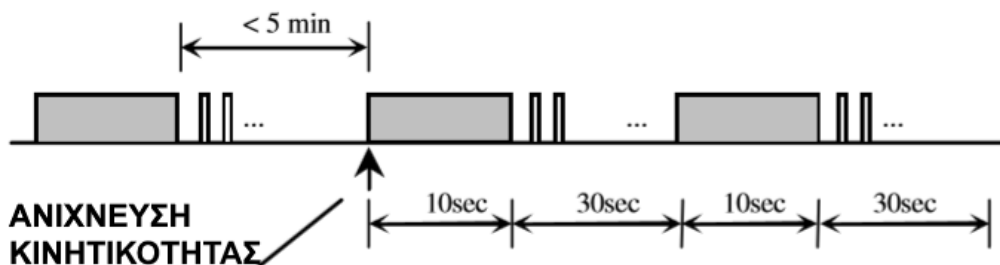
Το S-MAC λειτουργεί καλά στα στατικά δίκτυα, διότι οι διαμορφώσεις συνδέσεων και οι διακοπές συνδέσεων (brake-ups) δεν συμβαίνουν συχνά.

Αν ένας κινητός κόμβος θέλει να κάνει μία νέα σύνδεση με έναν άλλο κόμβο από διαφορετική συστοιχία, θα πρέπει πρώτα να περιμένει να έρθει η νέα περίοδος συγχρονισμού (που διαρκεί για 10 sec κάθε 5 min), ώστε να μπορέσει να ανιχνεύσει το μήνυμα SYNC message από το νέο κόμβο. Το S-MAC προτείνει να αυξηθεί η συχνότητα της περιόδου συγχρονισμού ενός κινητού κόμβου (mobile node) δύο φορές το λεπτό μόνο όταν ο κινητός κόμβος δεν έχει καμία σύνδεση με άλλους γειτονικούς κόμβους. Αυτή η πρόταση συντομεύει το χρόνο που απαιτείται για τον κινητό κόμβο να κάνει συνδέσεις με τους νέους γειτονικούς κόμβους. Όμως, αυτό είναι μία παθητική μορφή και αντιδραστική ("reactive") που ενεργοποιείται μόνο όταν χάνονται όλες οι συνδέσεις των γειτόνων με τον κινητό κόμβο. Ο χρόνος που απαιτείται για να δημιουργηθεί μία νέα σύνδεση είναι αρκετά μεγάλος και φτάνει ως και τα 30 sec (όταν περιμένει την νέα περίοδο συγχρονισμού) και προστίθεται κάθε περίοδος χρόνου λήξης timeout period (που διαρκεί για αρκετά min) μέχρι ένας κόμβος να ανακαλύψει ότι δεν έχει άλλους γείτονες. Σε αυτό το χρόνο ο κινητός κόμβος είναι αποσυνδεδεμένος από το δίκτυο και έτσι υπάρχει ένας μεγάλος ρυθμός απώλειας πακέτων (packet loss rate) ή μία κατάσταση εκτός λειτουργίας. Αν γίνει μία αλλαγή στο σύστημα ανακάλυψης γειτόνων του S-MAC ώστε να γίνεται η ανακάλυψη γειτόνων με πιο ενεργητική μορφή ("proactive"), δηλαδή η συχνότητα της περιόδου επανασυγχρονισμού, να αυξάνεται καθώς το πλήθος γειτόνων μειώνεται, τότε θα μειωθεί ο χρόνος που χρειάζεται για έναν κινητό κόμβο να βρει νέους γείτονες. Όμως αυτό σημαίνει ότι σε ένα αραιό τμήμα του δικτύου, οι κόμβοι θα αναγκαστούν να παραμένουν ενεργοί χωρίς να χρειάζεται, ακόμη και αν αυτός ο ενεργητικός μηχανισμός για αναζήτηση γειτόνων δεν οδηγήσει σε καλύτερες συνδέσεις στο δίκτυο.

Επιπλέον η πρόταση του S-MAC να αυξηθεί η συχνότητα της περιόδου συγχρονισμού αν ένας κόμβος δεν έχει καμία σύνδεση, δεν λειτουργεί σωστά σε μία μεμονωμένη συστοιχία virtual cluster. Αυτό συμβαίνει διότι οι κόμβοι σε μία συστοιχία όλοι μαζί ακολουθούν το ίδιο πρόγραμμα (schedule). Αν αυξηθεί η συχνότητα της περιόδου συγχρονισμού θα αυξηθεί και η κατανάλωση της ενέργειας, αλλά δεν θα αυξηθεί η πιθανότητα να βρεθούν νέοι γείτονες.

4.3.2.2 Η επέκταση MS-MAC για κινητούς κόμβους

Για αυτούς τους λόγους, οι συγγραφείς προτείνουν το πρωτόκολλο MS-MAC [43] που είναι μία επέκταση του S-MAC και είναι περισσότερο κατάλληλο για τους κινητούς κόμβους στα ασύρματα δίκτυα αισθητήρων. Αντί να περιμένουν παθητικά οι κινητοί κόμβοι να χάσουν όλες τις συνδέσεις τους με τους γείτονές τους μέχρι να αρχίσουν την ενεργή αναζήτηση νέων γειτόνων, στο MS-MAC μόλις ανιχνευθούν πληροφορίες κινητικότητας, τότε ο μηχανισμός για ανακάλυψη γειτόνων ενεργοποιείται αμέσως, με έναν ενεργητικό τρόπο (proactively).



Εικόνα 120. Μόλις ανιχνευθεί κινητικότητα, το MS-MAC μπαίνει σε περίοδο συγχρονισμού. Πηγή: [43].

Το πρωτόκολλο MS-MAC [43] προτάθηκε από τους συγγραφείς με τρεις στόχους.

Ένας στόχος ήταν η αποτελεσματική κατανάλωση ενέργειας, ο δεύτερος στόχος ήταν το πρωτόκολλο να λειτουργήσει στα στατικά δίκτυα με τον ίδιο τρόπο που λειτουργεί το S-MAC και τρίτος στόχος ήταν να λειτουργήσει αποτελεσματικά στα δίκτυα με κινητούς κόμβους.

Για το σκοπό αυτό, χρειαζόταν το πρωτόκολλο MS-MAC να έχει δυνατότητες να ανιχνεύσει την κινητικότητα. Πρέπει το πρωτόκολλο για τους κινητούς κόμβους να δημιουργεί νέες συνδέσεις πριν καταργηθούν οι παλιές ("make before break") [43]. Δηλαδή οι κόμβοι πρέπει να μπορούν να ανιχνεύσουν την παρουσία των κινητών κόμβων που βρίσκονται κοντά τους και να αναζητούν τους νέους γείτονες πιο εντατικά σε σύγκριση με τους στατικούς κόμβους. Για να ανιχνευθεί η κινητικότητα, χρησιμοποιούνται διάφοροι τρόποι. Μπορούν να βασίζονται σε σήματα ασύρματα, υπέρυθρη ακτινοβολία, ακουστικά κύματα, υπερήχους ή διάφορους συνδυασμούς των παραπάνω σημάτων.

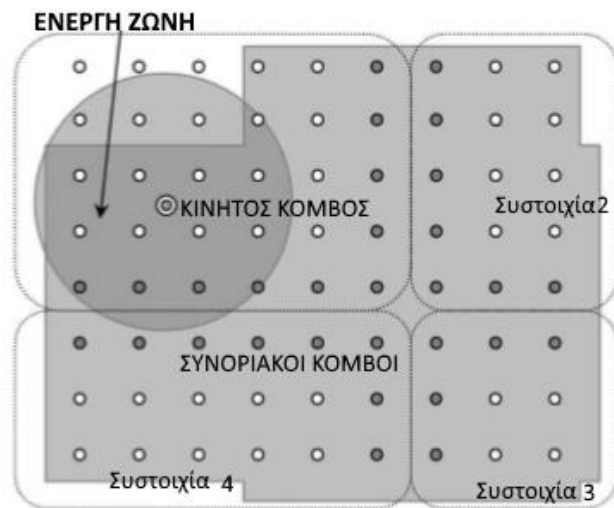
Επίσης, από το επίπεδο εφαρμογών (application layer), μπορούν να ανιχνευθούν πληροφορίες κινητικότητας με διάφορες μεθόδους, όπως με χρήση ενός αισθητήρα ανίχνευσης κίνησης (motion sensor) ή ενός μετρητή ταχύτητας (speed meter).

Στο πρωτόκολλο MS-MAC, χρησιμοποιήθηκε ως ένδειξη της παρουσίας κινητών κόμβων, το φαινόμενο ότι παρατηρήθηκε μία αλλαγή στο επίπεδο ισχύος του ασύρματου ραδιοσήματος κατά τη λήψη μηνυμάτων SYNC από κινητούς κόμβους. Αυτή η μέθοδος για ανίχνευση κινητικότητας δεν ήταν πολύ ακριβής. Παρόλα αυτά, λειτούργησε σωστά στο προτεινόμενο πρωτόκολλο MS-MAC.

Αν συμβεί μία λάθος ανίχνευση κινητού κόμβου, χωρίς να υπάρχει κινητός κόμβος στην πραγματικότητα, τότε θα ενεργοποιηθεί μία αναζήτηση γειτόνων χωρίς να χρειάζεται. Αυτό όμως δεν θα μειώσει την απόδοση του δικτύου.

Άλλες μέθοδοι ήταν η υπέρυθρη ακτινοβολία, ή τα ακουστικά σήματα ή οι υπερήχοι. Αυτές όμως οι μέθοδοι θα είχαν επιπλέον κόστος σε κατανάλωση ενέργειας. Αντίθετα με αυτές τις μεθόδους, το ασύρματο σήμα των μηνυμάτων SYNC είναι διαθέσιμο από το ίδιο το δίκτυο και δεν καταναλώνει επιπλέον ενέργεια, συνεπώς, δεν υπάρχει επιπλέον κόστος. Σε μία μεμονωμένη συστοιχία virtual cluster, όλοι οι κόμβοι ακολουθούν το ίδιο χρονικό πρόγραμμα ξυπνήματος/ύπνου (wakeup/sleep). Αν δύο κόμβοι βρεθούν ό ένας στην ασύρματη εμβέλεια του άλλου, τότε μπορεί ό ένας να βρει τον άλλον γρήγορα, μόλις ο ένας κόμβος θα λάβει το επόμενο μήνυμα SYNC message (που μεταφέρει τις πληροφορίες του προγράμματος schedule) από τον άλλο κόμβο. Αυτή η διαδικασία σύνδεσης, συνήθως γίνεται μέσα σε χρόνο λιγότερο από 10 sec.

Αντίθετα, αν ο κινητός κόμβος φτάσει σε μία νέα συστοιχία virtual cluster χωρίς να γνωρίζει το νέο πρόγραμμα, αυτό θα ήταν μία ανεπιθυμητή κατάσταση. Τότε θα έπρεπε ο κινητός κόμβος να περιμένει για αρκετό χρόνο μέχρι να έρθει η επόμενη περίοδος συγχρονισμού (που είναι προκαθορισμένη στα 5 min) και σε αυτό το χρονικό διάστημα ο κινητός κόμβος θα είναι αποσυνδεδεμένος από όλο το δίκτυο. Για να μειωθεί η πιθανότητα ο κινητός κόμβος να περάσει από τα σύνορα μίας συστοιχίας χωρίς να έχει ανιχνεύσει πρώτα το νέο πρόγραμμα schedule της νέας συστοιχίας cluster, πρέπει όλοι οι κόμβοι που βρίσκονται σε απόσταση R αλμάτων (hops) από τον κινητό κόμβο και όλοι οι κόμβοι σε απόσταση R αλμάτων (hops) από τους συνοριακούς κόμβους (border nodes) να διαμορφώνουν μία ενεργή ζώνη (active zone) γύρω από τον κινητό κόμβο. Δηλαδή, αυτή η ενεργή ζώνη είναι μια επικάλυψη της περιοχής γύρω από τον κινητό κόμβο και της περιοχής των συνόρων, όπως φαίνεται και στο παρακάτω σχήμα.



Εικόνα 121. Γύρω από τον κινητό κόμβο καθορίζεται η ενεργή ζώνη που είναι οι κόμβοι σε απόσταση R hops από τον κινητό κόμβο και R hops από τους συνοριακούς κόμβους Πηγή: [43].

Το R είναι μία παράμετρος μεταβίβασης ("hand-off"). Η προκαθορισμένη τιμή του R ορίστηκε να είναι το 2. Αν το R έχει μία μεγαλύτερη τιμή, τότε θα αυξηθεί το μέγεθος της ενεργού ζώνης. Αυτό θα υποστηρίξει καλύτερα την κινητικότητα, αλλά από την άλλη πλευρά, είναι πιθανόν να αυξήσει την πιθανότητα για περισσότερους κόμβους να μεταβούν σε ενεργή κατάσταση, χωρίς να χρειάζεται και έτσι θα καταναλώσουν άσκοπα περισσότερη ενέργεια. Στην ενεργή ζώνη, οι κόμβοι μπαίνουν άμεσα σε περίοδο συγχρονισμού, χωρίς να περιμένουν την επόμενη περίοδο συγχρονισμού, που είναι προγραμματισμένη.

Επιπλέον οι κόμβοι που βρίσκονται στην ενεργή ζώνη, επαναλαμβάνουν αυτή την περίοδο συγχρονισμού πιο συχνά (δηλαδή κάθε 30 sec), ενώ αντίθετα στην κανονική λειτουργία τους την επαναλαμβάνουν κάθε 5 min.

Αυτοί οι κόμβοι που βρίσκονται στην ενεργή ζώνη στοχεύουν να επισπεύσουν τις νέες συνδέσεις του κινητού κόμβου με νέους γείτονες με διαφάνεια για τον κινητό κόμβο καθώς ο κινητός κόμβος κινείται ανάμεσα σε διαφορετικές συστοιχίες (clusters).

Για να δημιουργηθεί αυτή η ενεργή ζώνη, οι κόμβοι που στέλνουν το πρόγραμμα schedule, στα μηνύματα SYNC του MS-MAC, επίσης στέλνουν και την πληροφορία για αποστάσεις (distances) σε μετρήσεις αλμάτων (hop counts) για το πόσα άλματα απέχει ο κόμβος αποστολέας από τον πλησιέστερο κινητό κόμβο και πόσα άλματα απέχει από τους πλησιέστερους συνοριακούς κόμβους (border nodes).

Όταν ένας τρέχων κόμβος λάβει μηνύματα SYNC messages από τους γειτονικούς κόμβους, τότε ο τρέχων κόμβος υπολογίζει τη δική του απόσταση από τον πλησιέστερο κινητό κόμβο και τον πλησιέστερο συνοριακό κόμβο (border node) και βρίσκει αν ανήκει ή όχι στην ενεργή ζώνη. Επιπλέον, αν πλησιάζει ο κινητός κόμβος, δηλαδή αν μειώνεται ο αριθμός αλμάτων από τον τρέχοντα κομβο προς τον κινητό κόμβο, τότε ο τρέχων κόμβος ανανεώνει την ενεργή κατάστασή του (active status) και αμέσως ξεκινά την περίοδο συγχρονισμού ενώ θέτει στο reset έναν χρονομετρητή της ενεργού κατάστασής του (active status timer).

Αν δεν ανήκει στην ενεργή ζώνη, ο κόμβος επιστρέφει στην κανονική λειτουργία του μετά από μία περίοδο λήξης χρόνου που διαρκεί 5 min.

Αυτός ο μηχανισμός του MS-MAC επιτρέπει στους κόμβους να λειτουργούν αποτελεσματικά και στα στατικά δίκτυα και στα σενάρια κινητικότητας. Είτε σε ένα σενάριο που όλοι οι κόμβοι είναι στατικοί είτε σε ένα σενάριο που ο κινητός κόμβος κινείται μόνο μέσα στην ίδια συστοιχία virtual cluster, όλοι οι κόμβοι έχουν αποτελεσματική κατανάλωση ενέργειας. Όπως ισχύει και στο S-MAC, εκτός από το ξύπνημα για ένα μικρό χρονικό διάστημα στην αρχή του κάθε κύκλου, ο κάθε κόμβος παραμένει ξύπνιος για μια περίοδο συγχρονισμού 10 sec κάθε 5 min. Όταν ένας κινητός κόμβος διασχίζει τα σύνορα δύο συστοιχιών clusters, τότε οι κινητός κόμβος και οι κόμβοι που τον περιβάλλουν διαμορφώνουν την ενεργή ζώνη ("active zone") σε μία απόσταση R αλμάτων (hops) γύρω από τον κινητό κόμβο. Οι κόμβοι που βρίσκονται στην ενεργή ζώνη λειτουργούν με έναν κύκλο λειτουργίας (duty cycle) υψηλότερο. Οι κόμβοι αυτοί πηγαίνουν στην περίοδο συγχρονισμού πιο γρήγορα από ότι στην κανονική λειτουργία τους και οι περίοδοι συγχρονισμού επαναλαμβάνονται πιο συχνά. Αυτή η περίοδος συγχρονισμού πλήρους κύκλου λειτουργίας (full duty cycle) επιτρέπει να κάνουν εγκαίρως συνδέσεις οι κόμβοι με του νέους γείτονες.

Κεφάλαιο 5

Η Δική μας Πρόταση

Η συνηθισμένη τοπολογία με την οποία ένα δίκτυο WirelessHART εγκαθίσταται σε μία βιομηχανική εγκατάσταση, είναι η τοπολογία πλέγματος (mesh) στην οποία όλοι οι κόμβοι αισθητήρες είναι στατικοί και αποτελούν τα έξυπνα όργανα μετρήσεων WirelessHART, ενώ υπάρχει ένας κεντρικός κόμβος που λέγεται sink και βρίσκεται τοποθετημένος σε μία κεντρική περιοχή της βιομηχανικής εγκατάστασης, ο οποίος συγκεντρώνει όλα τα δεδομένα από τους στατικούς κόμβους αισθητήρες που είναι διάσπαρτοι σε διάφορα σημεία στο χώρο της βιομηχανικής εγκατάστασης. Τότε η αποστολή δεδομένων από τους κόμβους αισθητήρες στον sink ή από τον sink στους κόμβους γίνεται με μία διαδρομή πολλαπλών αλμάτων (multi-hop routing) μέσω του ασύρματου δικτύου.

Η εισαγωγή κινητικότητας στο δίκτυο WirelessHART δεν σημαίνει απαραίτητα ότι πρόκειται να αλλάξει η τοπολογία δικτύου πλέγματος με τους στατικούς κόμβους αισθητήρων και τον στατικό κόμβο sink, αλλά σημαίνει ότι στο σύνολο των στατικών κόμβων αισθητήρων θα προστεθεί και ένα σύνολο κινητών κόμβων αισθητήρων. Οι στατικοί κόμβοι μπορούν να συνεχίσουν να στέλνουν τα δεδομένα τους με διαδρομή πολλαπλών αλμάτων στον sink. Όμως, οι κινητοί κόμβοι θα μπορούν επιπλέον να κινούνται διαγράφοντας μία τροχιά ανάμεσα στους στατικούς κόμβους, ή κοντά σε αυτούς, να συλλέγουν δεδομένα από τους στατικούς κόμβους και να τα μεταφέρουν στο sink.

Ένας από τους στόχους της εισαγωγής κινητικότητας είναι η ασφάλεια του προσωπικού που εργάζεται στις βιομηχανικές εγκαταστάσεις. Το εργατικό δυναμικό δεν πρέπει να εισέρχεται σε επικίνδυνους χώρους με επικίνδυνα χημικά ή αέρια ή εύφλεκτα υλικά. Έτσι, στις επικίνδυνες περιοχές, αντί να πάει κάποιος εργάτης, μπορεί να εισέλθει ένα ρομπότ ή ένα αυτόνομο όχημα UAV. Οι κινητοί κόμβοι αισθητήρες μπορεί να είναι τοποθετημένοι πάνω στο όχημα. Μόλις το όχημα εισέλθει στην εμβέλεια των στατικών αισθητήρων, αυτοί του στέλνουν τα δεδομένα τους μέσω ασύρματου δικτύου. Στη συνέχεια το όχημα επιστρέφει στον κεντρικό κόμβο sink και παραδίδει τα δεδομένα.

5.1 Η δική μας πρόταση

Η δική μας πρόταση, βασίστηκε στο πρότυπο WirelessHART, το οποίο, όπως είναι στην τρέχουσα μορφή του, περιλαμβάνει μόνο στατικούς κόμβους τοποθετημένους σε μία τοπολογία δικτύου πλέγματος (mesh).

Πριν παρουσιάσουμε το δικό μας σενάριο, κρίνεται σκόπιμο να γίνει περιληπτικά, μία γενική θεώρηση που καταδεικνύει τον τρόπο σκέψης που μας οδήγησε στο συγκεκριμένο σενάριο εισαγωγής κινητικότητας στο WirelessHART και έτσι, εδώ παρουσιάζονται πρώτα κάποιες αρχικές θεωρητικές εκτιμήσεις και γενικά ερωτήματα και έπειτα παρουσιάζεται το δικό μας σενάριο κινητικότητας. Παρακάτω, στην παράγραφο 5.1.1, εισαγωγικά γίνεται μία γενική ανάλυση απαιτήσεων και ιδεών, καθώς και διάφορων γενικών παραδειγμάτων από πιθανά σενάρια, ενώ στην παράγραφο 5.1.2 παρουσιάζεται το δικό μας σενάριο κινητικότητας που αναφέρεται στον καθαρισμό δεξαμενών σε ένα διυλιστήριο πετρελαίου. Θα χρησιμοποιήσουμε το σενάριο κινητικότητας για τους εργάτες που μετακινούνται ανάμεσα στις δεξαμενές και αναλαμβάνουν τον καθαρισμό των δεξαμενών.

Ο στόχος που τέθηκε, ήταν να γίνει μία επέκταση του προτύπου, ώστε να εισαχθούν επιπλέον και κινητοί κόμβοι στα δίκτυα WirelessHART. Συνεπώς, επιχειρήσαμε να δημιουργήσουμε μια «νέα» παραλλαγή του προτύπου, η οποία όμως θα έπρεπε να στηρίζεται και σε άλλες δοκιμασμένες υλοποιήσεις που έχουν γίνει σε διαφορετικά συστήματα. Ήταν όμως παράλληλα επιθυμητό, να μην απομακρυνθούμε πολύ από την υπάρχουσα λειτουργία του WirelessHART και να εισάγουμε όσο το δυνατόν, ελάχιστες τροποποιήσεις.

Για να προτείνουμε μία υλοποίηση εφαρμογής κινητικότητας με το πρότυπο WirelessHART, ήταν αναγκαίο να ληφθούν υπόψη ορισμένα σενάρια μιας πραγματικής βιομηχανικής εγκατάστασης, στην οποία θεωρείται ότι υπάρχει ένα σύνολο στατικών κόμβων αισθητήρων (static sensor nodes) και ένα σύνολο κινητών κόμβων αισθητήρων (mobile sensor nodes) οι οποίοι συνδέονται σε ένα ασύρματο δίκτυο αισθητήρων.

Οι συνθήκες κινητικότητας είναι μία πρόκληση για τα ασύρματα δίκτυα αισθητήρων σε βιομηχανικά περιβάλλοντα. Κινητικότητα είναι η περίπτωση που υπάρχουν κινητοί κόμβοι αισθητήρες, χαμηλού κόστους και μικρού μεγέθους, που ονομάζονται motes και

μεταφέρονται από έναν εργάτη, ένα ρομπότ, ένα κινητό όχημα, ή με άλλο τρόπο μέσα στους χώρους της βιομηχανικής εγκατάστασης, με στόχο είτε να συλλέξουν δεδομένα από άλλους κόμβους, είτε να βοηθήσουν να γίνουν συντηρήσεις και ρυθμίσεις στα όργανα μέτρησης. Επίσης, κινητός κόμβος μπορεί να είναι και μία συσκευή χειρός (handheld communicator) που συνδέεται στο δίκτυο για να γίνουν ρυθμίσεις και για παρακολούθηση της κατάστασης του δικτύου.

Πολλά διαφορετικά σενάρια μπορούν να δημιουργηθούν, ανάλογα με το πλήθος των σταθερών και των κινητών κόμβων, που θέλουμε να υπάρχουν στο δίκτυο WirelessHART. Διαφορετικά σενάρια επίσης μπορούν να δημιουργηθούν από το πλήθος δικτύων WirelessHART που θα σχηματιστούν στους χώρους της βιομηχανικής εγκατάστασης. Τέτοια σενάρια θα μπορούσαν να είναι, η περίπτωση να υπάρχει ένα μόνο δίκτυο, ή να υπάρχουν περισσότερα δίκτυα του ίδιου μεγέθους, ή να υπάρχει ένα κεντρικό δίκτυο μεγάλου μεγέθους το οποίο να συνδέεται με μικρότερα επιμέρους δίκτυα που βρίσκονται διάσπαρτα σε περιοχές γύρω από το κεντρικό δίκτυο.

Σε τέτοια σενάρια, ένας κινητός κόμβος, μπορεί να είναι μία συσκευή χειρός (Handheld Communicator) ή να είναι μία κινητή μηχανή.

Οι αισθητήρες καταγράφουν τιμές μεταβλητών όπως είναι η θερμοκρασία, η υγρασία, ο ήχος, το φως, η ακτινοβολία, η πίεση και συνήθως οι απομακρυσμένοι στατικοί αισθητήρες στέλνουν τα δεδομένα τους στον κινητό κόμβο όταν αυτός φτάσει μέσα στην εμβέλειά τους. Ο κινητός κόμβος μπορεί να αναφέρει στον κεντρικό κόμβο sink πχ κάθε 5 λεπτά τις τιμές που συλλέγει από τους στατικούς κόμβους. Σε άλλες περιπτώσεις, ο κινητός κόμβος δεν αναφέρει συνεχώς στον κεντρικό κόμβο sink, αλλά μόνο κατά απαίτηση, δηλαδή μόνο όταν ο κεντρικός κόμβος sink ζητήσει τα δεδομένα με αίτηση (request). Άλλες φορές πάλι μπορεί το σύστημα να βασίζεται σε συμβάντα (events) και τότε ο κινητός κόμβος μπορεί να μην στέλνει δεδομένα στον κεντρικό κόμβο όταν οι συνθήκες είναι κανονικές αλλά να στέλνει μόνο όταν γίνει κάποιο συμβάν (event). Για παράδειγμα αν γίνει μία αλλαγή στην ροή ή στη θερμοκρασία τότε ο κινητός κόμβος να στείλει τα δεδομένα στον σταθερό κόμβο για να υπάρξουν οι κατάλληλες διορθωτικές ενέργειες στο σύστημα.

Η εισαγωγή κινητικότητας έχει και πλεονεκτήματα και μειονεκτήματα. Τα πλεονεκτήματα είναι φανερά, αλλά το βασικό μειονέκτημα της είναι ότι εισάγει μία επιπλέον καθυστέρηση (latency) στην παράδοση των δεδομένων από τις συσκευές

πεδίου στον κεντρικό κόμβο sink και για αυτό σε πολλές λύσεις, αποφεύγεται η εφαρμογή της κινητικότητας. Η δυσκολία της εισαγωγής κινητικότητας σε ένα ασύρματο δίκτυο αισθητήρων με στατικούς κόμβους, όπως είναι το WirelessHART, είναι ότι εισάγοντας στο δίκτυο περισσότερους κινητούς κόμβους, τότε εισάγουμε συγχρόνως και μία μεγαλύτερη καθυστέρηση (latency) στις επικοινωνίες δεδομένων του δικτύου. Οι συσκευές Gateways έχουν δυνατότητα να υποστηρίξουν ένα ορισμένο πλήθος κόμβων δικτύου και σε δίκτυα που έχουν π.χ. 15 κόμβους η καθυστέρηση είναι μικρή (2 sec), ενώ σε δίκτυα με 100 κόμβους, η καθυστέρηση είναι μεγαλύτερη (10 sec), αλλά πάντοτε παραμένει στην τάξη των δευτερολέπτων.

Όταν υπάρχει ήδη μία αρχική ζεύξη (link) μεταξύ ενός κινητού κόμβου και ενός σταθερού κόμβου και ανταλλάσσονται δεδομένα μεταξύ τους, ενδέχεται στην διάρκεια επικοινωνίας δεδομένων να υποβαθμιστεί η ποιότητα της ζεύξης ή και να διακοπεί η ζεύξη. Τότε ο κινητός κόμβος θα αναγκαστεί να ψάξει για άλλους γειτονικούς κόμβους και θα επιχειρήσει επανειλημμένα να δημιουργήσει νέες ζεύξεις για να κάνει επαναληπτικές μεταδόσεις των πακέτων και να στείλει στον προορισμό τους, τα υπόλοιπα πακέτα που έχουν απομείνει από την προηγούμενη ζεύξη. Αυτό θα προκαλέσει ένα κόστος στο χρόνο και θα αυξηθεί η καθυστέρηση στις εφαρμογές.

Επίσης μια υποβαθμισμένη ζεύξη θα οδηγήσει σε πολλές αλλαγές στη διαδρομή δρομολόγησης (route) διότι οι κόμβοι που διέκοψαν τη ζεύξη τους θα αναζητήσουν να βρουν καλύτερες διαδρομές και έτσι θα εισαχθεί μία ακόμη μεγαλύτερη καθυστέρηση στο δίκτυο.

Ένας στόχος σχεδιασμού είναι να δημιουργηθεί ένας ενιαίος μηχανισμός για μεταβιβάσεις των ζεύξεων (handover), ο οποίος θα επιτρέπει σε έναν κινητό κόμβο που βρίσκεται σε μία ζεύξη, να μπορεί να μεταφέρει την επικοινωνία του σε μία καλύτερη ζεύξη με έναν άλλο κόμβο του δικτύου, πριν γίνει διακοπή της τρέχουσας ζεύξης, ώστε τα πακέτα δεδομένων να φτάνουν στον προορισμό χωρίς διακοπή, ακόμα και αν ο κινητός κόμβος κινείται διαρκώς και διακόπτει τις ζεύξεις του και δημιουργεί νέες, με άλλους γειτονικούς κόμβους.

5.1.1 Αρχικές θεωρητικές εκτιμήσεις και ερωτήματα

Μπορούν να δημιουργηθούν διάφορα σενάρια κινητικότητας στο πρότυπο WirelessHART. Κάθε σενάριο βασίζεται σε στόχους αυτοματοποίησης των βιομηχανικών διεργασιών και αφορά μία συγκεκριμένη βιομηχανία. Παρακάτω αναφέρεται μία γενική περιγραφή για το σχεδιασμό ενός σεναρίου κινητικότητας. Αρκετά παραδείγματα που αναφέρονται εδώ, δεν χρησιμοποιήθηκαν τελικά στη δική μας πρόταση, αλλά παρουσιάζονται γενικά για να φανεί τρόπος ανάλυσης που θα οδηγήσει στην δημιουργία ενός συγκεκριμένου σεναρίου κινητικότητας.

Ένας στόχος είναι να δημιουργηθούν τα αυτοματοποιημένα εργοστάσια, όπου αντί να μετακινούν οι άνθρωποι τα κιβώτια και τα βαριά αντικείμενα, να τα μετακινούν τα ρομπότ που κινούνται στο χώρο, ενώ παράλληλα, με τους ενσωματωμένους κινητούς αισθητήρες, τα ρομπότ να λαμβάνουν πληροφορίες από τους στατικούς αισθητήρες του χώρου, όπως είναι π.χ. πληροφορίες για την τοποθεσία που βρίσκεται ένα αντικείμενο, πληροφορίες για το βάρος του, κλπ.

Με βάση αυτά τα σενάρια, πρέπει να τεθούν διάφορα ερωτήματα σχετικά με το πώς θα αντιμετωπίζονται στο δίκτυο WirelessHART, όλοι οι κινητοί κόμβοι. Αυτά τα ερωτήματα θα πρέπει να απαντηθούν είτε με τη λογική, είτε λαμβάνοντας υπόψη διάφορες σχετικές προτάσεις που έγιναν από άλλους ερευνητές και προσαρμόζοντας την ίδια φιλοσοφία και στην δική μας υλοποίηση.

Ένα θέμα που είναι επιθυμητό να εξεταστεί, σε μία λύση κινητικότητας, είναι να τεθεί ένα υποθετικό σενάριο, στο οποίο θα υπάρχουν δύο κεντρικοί κόμβοι sink που υποστηρίζουν δύο διαφορετικά δίκτυα WirelessHART. Ας υποθέσουμε ότι 2 διαφορετικά δίκτυα WirelessHART, είναι τοποθετημένα σε 2 διαφορετικούς χώρους της βιομηχανικής εγκατάστασης.

5.1.1.1 Αρχικά βήματα δημιουργίας ενός υποθετικού σεναρίου

Ξεκινώντας να δημιουργούμε το σενάριο, κάνουμε κάποιες υποθέσεις, που είναι στην αρχή γενικές και αφηρημένες. Μετά θέτουμε διάφορους περιορισμούς ώσπου στο τέλος καταλήγουμε σε ένα πιο συγκεκριμένο σενάριο.

Η υλοποίηση ενός σεναρίου μπορεί να σχεδιαστεί με τα παρακάτω βήματα:

- 1) Πήγαμε σε ένα πραγματικό εργοστάσιο.
- 2) Τοποθετήσαμε 2 Gateways σε δύο θέσεις του εργοστασίου, την Gateway1 και Gateway2.
- 3) Τοποθετήσαμε τόσους κόμβους σταθερούς (π.χ 25 σε κάθε δίκτυο).
- 4) Τοποθετήσαμε τόσους κόμβους κινητούς. (π.χ. 5 εργάτες με ενσωματωμένους κόβους).
- 5) Χρησιμοποιήσαμε αυτό το μοντέλο κινητικότητας.
- 6) Κάποιοι κόμβοι κινούνται μόνο στο δίκτυο 1
- 7) Κάποιοι κόμβοι κινούνται μόνο στο δίκτυο 2
- 8) Κάποιοι κόμβοι κινούνται και στα δύο δίκτυα
- 9) Συγκεντρώθηκαν όλα τα δεδομένα από το δίκτυο 1
- 10) Συγκεντρώθηκαν όλα τα δεδομένα από το δίκτυο 2
- 11) Θέλουμε να λειτουργήσουν σωστά οι κινητοί κόμβοι που κινούνται και στα δύο δίκτυα.
- 12) Κάνουμε μία αλλαγή στο Header του πακέτου δεδομένων του στρώματος MAC ώστε ο κάθε κινητός κόμβος ME να μπορεί να «βλέπει» και τις δύο Gateways.

5.1.1.2 Κοινά στοιχεία στην ανάλυση των υποθετικών σεναρίων

Μολονότι μπορούν να προταθούν πολλά σενάρια περιπτώσεων χρήσης, διαφορετικά μεταξύ τους, όλα αυτά τα σενάρια διαθέτουν κάποια κοινά στοιχεία που πρέπει να ληφθούν υπόψη στην ανάλυση. Δηλαδή, για όλα τα σενάρια που μπορούν να προταθούν ως λύσεις, θα πρέπει να υπάρχει ένας κοινός τρόπος σκέψης και ανάλυσης. Αυτός ο τρόπος σκέψης περιλαμβάνει:

- α) τις ονομασίες που θα δώσουμε στα διάφορα μέρη του συστήματος.
- β) διάφορες παραμέτρους που αφορούν τους κόμβους.

π.χ. τύπος κόμβου, διαθέσιμη μνήμη, χρόνος αυτονομίας, εμβέλεια κόμβων, κ.α.

γ) Μοντέλο κινητικότητας που θα χρησιμοποιήσουν οι κινητοί κόμβοι ανάλογα με το σύστημα που εξετάζεται, ο χρόνος στάσης σε κάθε σταθερό κόμβο, η τροχιά του κινητού κόμβου.

δ) Τοπολογία δικτύου σταθερών κόμβων.

ε) Τρόπος σύνδεσης και αποσύνδεσης των κόμβων στα δίκτυα.

στ) Ο μηχανισμός μεταβίβασης (handover) πριν αποσυνδεθεί ένας κόμβος από μία ζεύξη λόγω απομάκρυνσης από έναν κόμβο, να μεταφέρει όλα τα στοιχεία της ζεύξης σε έναν άλλον κόμβο στον οποίο πλησιάζει, ώστε να συνεχίσει η μετάδοση πακέτων δεδομένων.

ζ) Ο Τρόπος ανάθεσης των σχισμών χρόνου (time slots) στα πλαίσια, που καθορίζει ποιοι είναι οι κόμβοι που θα εκπέμπουν δεδομένα σε κάθε χρονική σχισμή και ποια δεδομένα θα είναι αυτά.

Επίσης, για να υπάρξει μία συγκεκριμένη μεθοδολογία, θα πρέπει να γίνει μία τυποποιημένη περιγραφή του σεναρίου στην οποία να αναφέρονται:

α) Η συνολική Επισκόπηση,

είναι μια γενική παρουσίαση του σεναρίου.

β) Η περιγραφή του σεναρίου,

είναι μία συνοπτική περιγραφή που εξηγεί τις βασικές πλευρές του σεναρίου

γ) Διάγραμμα του σεναρίου.

Ένα σχεδιάγραμμα που φαίνονται τα στοιχεία του σεναρίου

δ) Αντικείμενα που συμμετέχουν στο σενάριο.

Είναι τα διάφορα αντικείμενα που χρησιμοποιούνται στο σενάριο και οι λειτουργίες τους.

ε) Οι απαιτήσεις του συστήματος,

είναι διάφορες τεχνικές απαιτήσεις που πρέπει να εκπληρωθούν από το σύστημα, οι οποίες βοηθούν στο σχεδιασμό μιας αρχιτεκτονικής.

στ) υποθέσεις για τη λύση

Είναι κάποιες υποθέσεις για τα στοιχεία του σεναρίου ώστε να κατασκευαστεί ένα τελικό σύστημα που δίνει λύσεις στις απαιτήσεις του σεναρίου.

Με βάση τις υποθέσεις για τη λύση, μπορούν να ελεγχθούν διαφορετικά σενάρια και να συγκριθούν μεταξύ τους ως προς τις λύσεις που προτείνουν.

ζ) Ορισμός,

είναι μία συνοπτική εξήγηση για κάθε απαίτηση

η) Επίπεδο,

είναι μία τιμή μεταβλητής ή ενός δείκτη μέτρησης για μία απαίτηση σε ένα συγκεκριμένο σενάριο.

Παρακάτω αναφέρονται μερικά παραδείγματα από πιθανά σενάρια για να δείξουμε ότι γίνονται συγκεκριμένες υποθέσεις για τους κόμβους. Τα σενάρια αυτά δεν χρησιμοποιήθηκαν στη δική μας λύση, αλλά παρουσιάζονται εδώ για να εξηγήσουν τα κοινά στοιχεία που πρέπει να ληφθούν υπόψη γενικά στην ανάλυση διαφορετικών σεναρίων.

Σενάριο 1: έστω ότι έχουμε 2 χώρους με 2 διαφορετικά δίκτυα WirelessHART.

Για παράδειγμα, έστω ότι ο 1^{ος} χώρος είναι χώρος συναρμολόγησης προϊόντων

και ο 2^{ος} χώρος είναι χώρος συσκευασίας προϊόντων και αποστολής τους στην αποθήκη.

Κάνουμε την υπόθεση ότι υπάρχει ένα σύνολο κινητών κόμβων, που μεταφέρονται από το ένα δίκτυο WirelessHART στο άλλο δίκτυο WirelessHART.

Ο κεντρικός κόμβος sink, είναι η πύλη (Gateway) στο δίκτυο WirelessHART, ενώ γενικότερα λέγεται Controller σε άλλα δίκτυα.

Υποθέτουμε ότι οι δύο κεντρικοί κόμβοι είναι στατικοί και ονομάζονται sink1 και sink2, ενώ υπάρχει ένας άλλος κινητός κόμβος που ονομάζεται ME (mobile element). Δεχόμαστε ότι το δίκτυο του sink1 έχει 10 αισθητήρες στατικούς ενώ το δίκτυο του sink2 έχει 6 αισθητήρες στατικούς (τυχαίο πλήθος στατικών αισθητήρων).

Είναι επιθυμητό, ο κινητός κόμβος ME που απομακρύνεται από τον sink1 και προσεγγίζει τον sink2 να αποσυνδέεται από το δίκτυο του sink1 και να συνδέεται στο δίκτυο του sink2, αλλά η επικοινωνία να είναι συνεχής και να καταλαβαίνουν οι 2 sinks ότι πρόκειται για τον ίδιο κινητό κόμβο ME.

Παράδειγμα λειτουργίας αυτού του σεναρίου:

Υπάρχει ένα ρομπότ που κινείται στους δύο χώρους και φεύγει από τον 1ο sink, και πηγαίνει στον 2ο sink.

Το ρομπότ έχει ενσωματωμένο πάνω του έναν αισθητήρα θερμοκρασίας και στέλνει συνεχώς κάθε 10 sec, την τιμή της θερμοκρασίας του χώρου, σε μία εφαρμογή (application) που λαμβάνει αυτές τις τιμές θερμοκρασίας για κάποιο σκοπό. Θα πρέπει τότε να υπάρχει συνεχώς από το ρομπότ, η ίδια ροή δεδομένων και να φαίνεται στην εφαρμογή (application) ότι είναι ο ίδιος κόμβος που στέλνει τα δεδομένα, παρόλο που συνδέεται και αποσυνδέεται στους 2 διαφορετικούς sinks.

Η ταυτότητα ID του κινητού κόμβου ME πρέπει να γίνεται γνωστή σε διάφορες περιπτώσεις.

Η καλύτερη περίπτωση είναι ο κινητός κόμβος να έχει ένα μοναδικό Global ID, γιατί τότε θα φαίνεται και στους 2 sinks ότι είναι ο ίδιος κόμβος είτε βρίσκεται στο δίκτυο του sink1 είτε βρίσκεται στο δίκτυο του sink2.

Η άλλη περίπτωση όμως, είναι ο κόμβος να μην έχει το ίδιο ID και στα δύο δίκτυα.

Τότε θα έχει ένα τοπικό Local ID1 στο ένα δίκτυο και ένα διαφορετικό Local ID2 στο 2ο δίκτυο.

Όμως ο κινητός κόμβος θα έχει και ένα ατομικό δικό του ID 3.

Ίσως τότε θα πρέπει να υπάρχει ένας πίνακας αντιστοιχίας table πάνω στον κινητό κόμβο, που θα λέει ότι το ID1 που είχε στον 1ο sink, αντιστοιχεί στο δικό του ID3 και ομοίως το ID 2 που είχε στον 2ο sink αντιστοιχεί στο δικό του ID3,

ώστε να τον αναγνωρίζει η εφαρμογή. Αυτός ο πίνακας όμως θα εισάγει μία καθυστέρηση για να γίνουν οι αντιστοιχίες και έτσι δεν είναι και τόσο καλή λύση για ένα δίκτυο WirelessHART.

Επίσης, ένας πίνακας αντιστοιχίας θα μπορούσε να ελέγχεται από τον διαχειριστή δικτύου.

Μπορούν να δοθούν λύσεις σε επίπεδο MAC ή σε επίπεδο δικτύου.

Για να είναι πλήρης η περιγραφή της λύσης κινητικότητας θα πρέπει να συγκεκριμενοποιηθεί μια λύση κινητικότητας που περιγράφει τα διάφορα IDs, Tables, Headers, slots.

Όταν εμφανίζεται ένας κινητός κόμβος πρέπει να ανατεθούν σε αυτόν (assign) κάποιες χρονικές σχισμές (slots).

Αυτές τις χρονικές σχισμές (slots) πρέπει να τις αναθέσει, ο κεντρικός sink που βρίσκεται πιο κοντά στον κινητό κόμβο. Θα μπορούσε να βρεθεί η απόσταση που απέχει ο κινητός κόμβος από κάθε στατικό sink.

Καθώς κινείται όμως ο κόμβος αλλάζουν οι αποστάσεις και πρέπει να γίνει μία μεταβίβαση (handoff) από τον sink1 στον sink2.

Επίσης, πρέπει να καθοριστεί ποιες χρονικές σχισμές (slots) θα ανατεθούν στον κινητό κόμβο ME από το πλαίσιο TDMA frame που θα χρησιμοποιήσουμε.

Μπορούμε να χρησιμοποιήσουμε ένα ίδιο υπερπλαίσιο superframe του TDMA, που χρησιμοποιείται στο WirelessHART, ή αλλιώς μπορεί να αλλάξει το υπερπλαίσιο και να υπάρξει ένα διαφορετικό πλαίσιο (frame) με περισσότερες σχισμές. Αν κάθε σχισμή έχει διάρκεια 10 msec, και το πλαίσιο έχει N σχισμές χρόνου, τότε ο συνολικός χρόνος του πλαισίου θα είναι $N \cdot 10 \text{ ms}$.

Πρέπει να αποφασιστεί από ποιο μέρος του υπερπλαισίου θα πάρει τις σχισμές χρόνου (slots).

Μία σκέψη είναι από την αρχή να διαστασιοποιηθεί το δίκτυο για πιο πολλούς κόμβους. Έτσι στο πλαίσιο θα υπάρχουν πολλές κενές σχισμές χρόνου slots που λέγονται unused slots και θα μπορούν να ανατίθενται σε νέους κινητούς κόμβους που εισέρχονται στο δίκτυο.

Θα χρειαστεί να υπάρξει ένα αίτημα request από τον κινητό κόμβο, ή εναλλακτικά θα γίνει αυτόματα η ανάθεση σχισμών μόλις ο κόμβος πλησιάσει στην εμβέλεια ενός άλλου κόμβου που ανήκει στο δίκτυο.

Η απάντηση σε αυτά τα ερωτήματα, θα μπορέσει να οδηγήσει σε μία προτεινόμενη λύση. Πρέπει όμως όσο το δυνατόν η λύση αυτή να βρίσκεται κοντά στο αρχικό πρότυπο διότι δεν πρέπει να χαθεί η φιλοσοφία του WirelessHART και η αρχική λειτουργία του, δηλαδή να γίνουν όσο το δυνατόν λιγότερες τροποποιήσεις.

5.1.1.3 Περιπτώσεις κίνησης ενός κινητού κόμβου μεταξύ δύο σταθερών κόμβων sinks

Με βάση τις συνθήκες που περιεγράφηκαν προηγουμένως, θα πρέπει να οριστούν οι διάφορες περιπτώσεις του κινητού κόμβου σε σχέση με τους 2 κεντρικούς στατικούς κόμβους Sinks.

Όταν ο κινητός κόμβος ME κινείται εσωτερικά μέσα στην εμβέλεια του ίδιου sink, τότε έχουμε εσωτερική κινητικότητα στο ίδιο δίκτυο (intra-mobility)

Όταν ο κινητός κόμβος ME κινείται εξωτερικά μέσα στην εμβέλεια δύο διαφορετικών στατικών sinks, τότε έχουμε εξωτερική κίνηση σε δύο δίκτυα (inter-mobility).

Διακρίνονται οι παρακάτω περιπτώσεις κατά την κίνηση του κινητού κόμβου.

Περίπτωση 1η

Όταν ο κινητός κόμβος ME απομακρύνεται από το δίκτυο του sink1 αποσυνδέεται και εισέρχεται στην εμβέλεια του δικτύου του sink2.

Τότε ο κινητός κόμβος είναι μία καινούργια συσκευή και παίρνει κάποιες νέες slots στο πλαίσιο TDMA του κόμβου sink 2. Αλλά η ροή πρέπει να είναι συνεχόμενη.

Περίπτωση 2^η

Όταν ο κινητός κόμβος ME απομακρύνεται από το δίκτυο του sink2 τότε ο κινητός κόμβος πρέπει να αποσυνδεθεί.

Περίπτωση 3^η

Ο κόμβος ME αποσυνδέεται από τον sink1 και μετά από κάποιο χρόνο ξανασυνδέεται στον sink1.

Ο sink1 πρέπει να μπορεί να δει αν ο κόμβος που συνδέθηκε είναι ένας ξένος πράκτορας (foreign agent) ή αν είναι ένας κόμβος του δικού του δικτύου και τότε είναι οικιακός πράκτορας (home agent).

5.1.1.4 πολλοί κινητοί κόμβοι που ανταγωνίζονται για να στείλουν δεδομένα

Για την περίπτωση που υπάρχουν πολλοί κινητοί κόμβοι που θέλουν να επικοινωνήσουν ταυτόχρονα με ένα ασύρματο δίκτυο αισθητήρων με στατικούς κόμβους, έχει προταθεί ένα πρωτόκολλο [41] για το στρώμα MAC που είναι υβριδικό και ονομάζεται RI-MAC. Στο RI-MAC στέλνονται σήματα beacons για να οριστούν χρόνοι ραντεβού (rendezvous times) στους οποίους μπορεί να γίνει η ανταλλαγή δεδομένων του κινητού κόμβου με έναν στατικό κόμβο του δικτύου [41].

Αυτό το πρωτόκολλο αναφέρεται εδώ, ως ένα παράδειγμα που δείχνει μια τεχνική που χρησιμοποιήθηκε για την μείωση της καθυστέρησης.

Για να μειωθεί η καθυστέρηση (latency) στο πρωτόκολλο RI-MAC, δεν υπάρχουν πακέτα ελέγχου και αρχικά πεδία preambles στα πακέτα δεδομένων. Όταν δεν έχουν να μεταδώσουν ή να λάβουν καθόλου δεδομένα, οι στατικοί κόμβοι, βρίσκονται για κάποιες χρονικές περιόδους στην κατάσταση ύπνου (sleep state) για να μην εξαντλούν την ενέργειά τους, ενώ ενεργοποιούνται περιοδικά για να ανιχνεύσουν αν υπάρχουν κινητοί κόμβοι που έχουν δεδομένα προς αποστολή στο δίκτυο. Όταν ένας δέκτης τελειώσει τη φάση ύπνου (sleep time), ενεργοποιείται για ένα χρονικό διάστημα που ονομάζεται χρόνος αναμονής (dwell time) και εκπέμπει ένα σήμα προς όλους τους κόμβους (broadcast), το οποίο είναι σήμα beacon που περιέχει μόνο πληροφορίες για τη διεύθυνση πηγής (source address information) SRC. Όλοι οι κόμβοι που έχουν δεδομένα προς αποστολή, μόλις λάβουν αυτό το σήμα ξεκινούν μετάδοση πακέτων δεδομένων (data transmission). Σε αυτή τη μετάδοση γίνεται ανταγωνισμός (competition) μεταξύ των κινητών κόμβων για το ποιος θα κερδίσει πρώτος το κανάλι επικοινωνίας για να δημιουργήσει μία ζεύξη με τον δέκτη. Όταν δύο ή περισσότεροι κόμβοι στέλνουν πακέτα δεδομένων ταυτόχρονα, τότε γίνεται μία σύγκρουση (collision). Ο δέκτης τότε θα στείλει

ένα νέο σήμα beacon στο οποίο θα έχει προστεθεί ένα πεδίο δεδομένων που λέγεται back-off window field (BW) δηλαδή παράθυρο υποχώρησης. Οι πομποί θα υποχωρήσουν και θα ξαναστείλουν δεδομένα λίγο αργότερα ώστε κάποιο πακέτο δεδομένων θα κερδίσει το κανάλι. Τότε ο δέκτης θα απαντήσει με ένα σήμα ACK beacon (DST), το οποίο λειτουργεί ως αναγνώριση λήψης πακέτου (ACK). Αν όμως λήξει ο χρόνος αναμονής (dwell time) του δέκτη και στο δέκτη δεν φτάσει κανένα πακέτο, τότε ο δέκτης θα μεταβεί ξανά στην κατάσταση ύπνου (sleep). Η τιμή στο πεδίο παράθυρο υποχώρησης (BW) που υπάρχει στα σήματα beacon που στέλνει ο δέκτης, καθορίζει και ποιος θα είναι ο χρόνος αναμονής (dwell time). Έτσι όταν υπάρχουν πολλές συγκρούσεις, τότε αυξάνεται το μέγεθος του παραθύρου υποχώρησης (BW) και παράλληλα αυξάνεται ο χρόνος αναμονής (dwell time). Αντίθετα, όταν δεν υπάρχουν πολλές συγκρούσεις το παράθυρο υποχώρησης (BW) παραμένει μικρό και έτσι είναι μικρότερος και ο χρόνος αναμονής dwell time.

5.1.1.5 Αρχικές Εκτιμήσεις για επιλογή μοντέλου κινητικότητας

Τα είδη κινητικότητας που μπορούν να χρησιμοποιηθούν, εξαρτώνται από την εφαρμογή, από το περιβάλλον και από την τοπολογία του δικτύου WirelessHART.

Γενικά υπάρχουν 3 είδη. Κινητικότητα κόμβου, κινητικότητα γεγονότος και κινητικότητα του sink.

Το μοντέλο κινητικότητας Manhattan μπορεί να εφαρμοστεί μόνο σε ένα περιβάλλον που οι διάδρομοι κίνησης είναι ευθείες και κάθετες γραμμές.

Ένα τέτοιο περιβάλλον για παράδειγμα, είναι μία αυτοματοποιημένη αποθήκη όπου διάφορα αυτόματα οχήματα, ή ρομπότ κινούνται μέσα σε ευθείς διαδρόμους, οριζόντια και κάθετα. Ο ρόλος των οχημάτων είναι να μεταφέρουν προϊόντα από το ένα σημείο της αποθήκης σε ένα άλλο. Διακρίνουμε τι εξής περιπτώσεις κίνησης:

α) Το όχημα μεταφέρει τα κιβώτια από την είσοδο της αποθήκης στη θέση που πρόκειται να αποθηκευτούν.

β) Το όχημα αλλάζει θέσεις στα κιβώτια μέσα στην αποθήκη για να εξοικονομήσει χώρο για νέα κιβώτια.

γ) Το όχημα περιφέρεται ανάμεσα στα κιβώτια και καταγράφει το πλήθος κιβωτίων.

δ) Το όχημα κάνει αναζήτηση ενός κιβωτίου

ε) Το όχημα μεταφέρει ένα κιβώτιο μέσα από την αποθήκη προς την έξοδο της αποθήκης για να το παραδώσει στον πελάτη.

Σε ένα περιβάλλον εργοστασίου που οι διάδρομοι δεν είναι ευθείες κάθετες και οριζόντιες, δεν μπορεί να εφαρμοστεί το μοντέλο κινητικότητας Manhattan. Τότε μπορεί να εφαρμοστεί το μοντέλο τυχαίας κινητικότητας Random Way Point Mobility Model.

Επίσης μπορεί να χρησιμοποιηθεί το μοντέλο κινητικότητας Gauss Markov. Όμως αυτά τα δύο μοντέλα δεν είναι κατάλληλα για οποιαδήποτε περίπτωση.

Για παράδειγμα, αν υπάρχει ένα διυλιστήριο, που ένα ρομπότ ανιχνεύει σφάλματα σε έναν αγωγό, τότε το ρομπότ κινείται κατά μήκος του αγωγού. Έτσι εκτελεί μία γραμμική κίνηση που δεν είναι τυχαία όπως στο Random Way Point Mobility Model αλλά ακολουθεί μία γραμμική κίνηση που είναι περιορισμένη γεωγραφικά και ακολουθεί τη διαδρομή του αγωγού. Δεν μπορεί να κινηθεί σε άλλη πορεία μακριά από τον αγωγό, παρά μόνο όταν συναντήσει κάποια εμπόδια στην τροχιά του και τότε θα πρέπει να απομακρυνθεί για λίγο από τον αγωγό.

Έτσι εδώ ταιριάζει καλύτερα ένα γεωγραφικό μοντέλο κινητικότητας με εμπόδια.

5.1.2 Σενάριο κινητικότητας στο χώρο δεξαμενών διυλιστηρίου, για καθαρισμό, στο οποίο βασίστηκε η δική μας λύση

Μία βιομηχανία στην οποία θα μπορούσε να χρησιμοποιηθεί το WirelessHART, είναι η βιομηχανική εγκατάσταση ενός διυλιστηρίου πετρελαίου.

Σε ένα διυλιστήριο γίνονται πολλές διεργασίες. Μία σημαντική διεργασία είναι ο καθαρισμός των δεξαμενών του διυλιστηρίου που γίνεται τακτικά.

Εμείς επιλέξαμε να χρησιμοποιήσουμε το WirelessHART σε ένα σενάριο κινητικότητας που αφορά τους εργάτες οι οποίοι κινούνται στο χώρο των δεξαμενών για να εκτελέσουν διαδικασίες καθαρισμού των δεξαμενών. Ένα κριτήριο για να επιλέξουμε την εισαγωγή κινητικότητας, είναι πως θα θέλαμε να σχεδιαστεί μία δυναμική ανάθεση, όπου θα αλλάζει το πλήθος των χρονικών σχισμών slots ή των πλαισίων frames.

Καταλήξαμε στο συγκεκριμένο σενάριο διότι στο παρελθόν χρησιμοποιήθηκαν και άλλα διαφορετικά πρότυπα που έχουν κοινούς στόχους με το WirelessHART και είχαν σχεδιαστεί για να χρησιμοποιηθούν σε όμοια βιομηχανική εγκατάσταση, και έτσι, το περιβάλλον του διυλιστηρίου πετρελαίου ήταν ένα περιβάλλον δοκιμασμένο ώστε ήταν γνωστά πολλά από τα προβλήματα που αντιμετωπίζονται. Επίσης άλλος στόχος του σεναρίου, ήταν η ασφάλεια των εργατών που κινούνται στις εγκαταστάσεις, μέσα σε ένα επικίνδυνο περιβάλλον για την υγεία.

5.1.2.1 Σενάριο όπου ένας εργάτης κινείται ανάμεσα σε 2 δεξαμενές (tanks) είναι η δική μας λύση

Οι δεξαμενές αποθήκευσης σε ένα διυλιστήριο, πρέπει να καθαρίζονται περιοδικά σε κάποιες προγραμματισμένες συντηρήσεις, ώστε να εντοπίζονται διάφορα προβλήματα που μπορεί να υπάρχουν στις δεξαμενές και να γίνεται μία εκτίμηση της κατάστασης για κάθε δεξαμενή, για να λαμβάνονται μέτρα διόρθωσης των προβλημάτων.

Τα υλικά που υπάρχουν μέσα στις δεξαμενές είναι εξαιρετικά τοξικά και έτσι στο χώρο των δεξαμενών δημιουργείται μία τοξική ατμόσφαιρα που είναι πολύ επικίνδυνη για την υγεία των εργαζομένων. Επίσης συχνά υπάρχουν αναθυμιάσεις τοξικών αερίων, τα οποία δεν πρέπει να τα εισπνεύσει ο άνθρωπος, και μπορεί να υπάρχουν ακόμη και εκρηκτικά αέρια που θα προκαλέσουν εκρήξεις ή πυρκαγιά σε υψηλές θερμοκρασίες.

Γύρω από τις δεξαμενές μπορούν να τοποθετηθούν στατικοί αισθητήρες που ελέγχουν τα αέρια της ατμόσφαιρας και να στέλνουν συναγερμούς (alarms), σε μία κεντρική περιοχή ελέγχου, αν οι τιμές συγκέντρωσης επιβλαβών αερίων ξεπεράσουν ένα επιτρεπτό όριο ευαισθησίας (threshold). Έτσι θα υπάρχουν ενδείξεις για το αν μπορεί να εισέλθει άνθρωπος ή όχι στον χώρο, σε μία δεδομένη χρονική στιγμή. Μια ομάδα εργατών του προσωπικού αναλαμβάνει τον καθαρισμό των δεξαμενών χρησιμοποιώντας διάφορα υγρά και χημικά υλικά.

Το προσωπικό που βρίσκεται στις δεξαμενές κινδυνεύει από τις αναθυμιάσεις των τοξικών αερίων. Για αυτό χρησιμοποιούνται ειδικοί αισθητήρες που λέγονται trip sensors και μπορούν να τοποθετηθούν πάνω στη στολή του εργαζόμενου, και δείχνουν τον προσανατολισμό του εργαζομένου (orientation) αν είναι κάθετος ή οριζόντιος. Αν κάποιος εργαζόμενος λιποθυμήσει από αναθυμιάσεις των αερίων, (κάτι που είναι πιθανό να συμβεί λόγω της μεγάλης τοξικότητας), τότε ο αισθητήρας trip sensor αντιλαμβάνεται ότι ο εργαζόμενος βρίσκεται σε οριζόντια θέση για ένα μεγάλο χρονικό διάστημα και τότε θα μπορεί να ενεργοποιεί συναγερμούς (alarms) που στέλνουν μηνύματα σε μία κεντρική περιοχή όπου βρίσκονται οι υπεύθυνοι υγείας και ασφάλειας του προσωπικού, ή κάποιοι νοσηλευτές. Στην περίπτωση αυτή το προσωπικό ασφάλειας στέλνει τους νοσηλευτές να απομακρύνουν τον εργαζόμενο από την επικίνδυνη περιοχή και να του χορηγήσουν πρώτες βοήθειες και τα κατάλληλα φάρμακα ή αντίδοτα κατά της δηλητηρίασης από τις τοξικές ουσίες.

Μαζί με τους αισθητήρες trip sensors, οι εργάτες μπορεί να φέρουν αναρτημένους στην στολή τους, και άλλους αισθητήρες, όπως π.χ. αισθητήρες που μετρούν τους παλμούς της καρδιάς του εργαζόμενου για να υπάρχουν πληροφορίες για την φυσική του κατάσταση.

Ένα άλλο στοιχείο που πρέπει να ληφθεί υπόψη σε αυτό το σενάριο, είναι πόσους κεντρικούς κόμβους sinks θα τοποθετήσουμε για να δημιουργήσουν ένα αντίστοιχο σύνολο από δίκτυα WirelessHART.

Ας υποθέσουμε ότι στην περιοχή δεξαμενών υπάρχουν δύο δεξαμενές.

Μπορούν να τοποθετηθούν στο πεδίο δύο πύλες Gateways μία κοντά σε κάθε δεξαμενή

Έτσι θα έχουμε ένα δίκτυο WirelessHART γύρω από την πρώτη δεξαμενή και ένα δεύτερο δίκτυο WirelessHART γύρω από την δεύτερη δεξαμενή.

Ο εργάτης που κινείται μεταξύ των δύο δεξαμενών έχει τους κινητούς κόμβους αισθητήρες είτε προσαρτημένους πάνω στη στολή του, είτε σε μία κινητή συσκευή

που κρατάει. Ή εναλλακτικά, οι κινητοί αισθητήρες μπορεί να βρίσκονται τοποθετημένοι σε ένα κινητό όχημα, με το οποίο κινείται ο εργάτης στους χώρους. Επίσης ο εργάτης δεν κινείται συνεχώς μέσα στους χώρους των δεξαμενών, αλλά μόνο όταν πρέπει να γίνει μία συντήρηση, ή ένας καθαρισμός. Παραμένει στο χώρο για όσο χρόνο διαρκούν οι εργασίες που κάνει. Στην υπόλοιπη περίοδο του χρόνου, που δεν γίνονται καθόλου συντηρήσεις, τα δύο δίκτυα WirelessHART έχουν μόνο τους στατικούς κόμβους ενώ οι κινητοί κόμβοι απουσιάζουν.

5.1.2.2 Απαιτήσεις του σεναρίου

Οι απαιτήσεις του σεναρίου αφορούν:

- α) την καθυστέρηση (latency),
- β) την ασφάλεια (security)
- γ) την αξιοπιστία (reliability),
- δ) την κινητικότητα (mobility)
- ε) τα χρονικά διαστήματα που μεσολαβούν μεταξύ των διαδοχικών συντηρήσεων.

Όσον αφορά την καθυστέρηση (latency), πρέπει να καθοριστεί ένα όριο χρόνου που είναι τα 5 sec μέσα στο οποίο ο κεντρικός κόμβος sink που τοποθετήθηκε σε μια δεξαμενή και ο κινούμενος εργάτης βρίσκεται κοντά της, θα λαμβάνει τα μηνύματα που στέλνουν οι αισθητήρες του κινούμενου εργάτη. Αν υπάρξει μεγαλύτερη καθυστέρηση από 5 sec ενδέχεται να αργήσει να φτάσει ο συναγερμός στον κεντρικό χώρο ελέγχου και έτσι να κινδυνέψει η ζωή του εργάτη.

Η ασφάλεια δηλώνει πόσο ασφαλές πρέπει να είναι το σύστημα από υποκλοπές δεδομένων από άλλους κόμβους που δεν ανήκουν στο σύστημα. Το σύστημα πρέπει να κάνει πιστοποίηση, να προσέχει την ακεραιότητα δεδομένων, να υπάρχει εμπιστευτικότητα και να μην επιτρέπει αποστολή δεδομένων σε κόμβους που δεν ανήκουν στο σύστημα.

Η αξιοπιστία δηλώνει πόσο σημαντικά είναι τα δεδομένα που μεταφέρει ο εργάτης. Όλα τα δεδομένα είναι σημαντικά για να μην υπάρξει πρόβλημα στην υγεία του εργάτη, επομένως δεν πρέπει να χάνονται τα πακέτα δεδομένων.

Η κινητικότητα είναι βασική απαίτηση του σεναρίου διότι ο εργάτης είναι κινούμενος μέσα στο χώρο των δεξαμενών και έχει προσαρτημένους πάνω του κινητούς κόμβους αισθητήρες.

Τα χρονικά διαστήματα που μεσολαβούν μεταξύ των διαδοχικών συντηρήσεων στο πρόγραμμα, λέγονται maintenance intervals. Αυτά τα χρονικά διαστήματα θέλουμε να είναι όσο το δυνατόν μεγαλύτερα για να μην διακόπτεται η παραγωγή. Όταν διακόπτεται η παραγωγή για μεγάλο χρόνο, τότε έχουμε απώλειες οικονομικές που είναι ανεπιθύμητες, καθώς και καθυστερήσεις παράδοσης παραγγελιών στους πελάτες. Σε αυτή την περίπτωση, ένα όριο που μπορεί να τεθεί είναι να υπάρχει λειτουργία για μεγαλύτερο χρονικό διάστημα από 6 μήνες, ώστε να συνεχίζεται κανονικά η παραγωγή πριν την επόμενη διακοπή της.

Μία 2^η αιτία συντήρησης είναι όταν τελειώνει η ενέργεια στις μπαταρίες των κόμβων αισθητήρων και χρειάζεται να γίνει μία αντικατάσταση μπαταριών ή επαναφόρτιση τους. Αυτή η διακοπή δεν αφορά όλους τους κόμβους αλλά μόνο όσους έχουν εξαντλήσει την ενέργεια της μπαταρίας τους. Τότε γίνονται κάποιες διακοπές τοπικά χωρίς να διακοπεί η παραγωγή, αλλά ενδέχεται να υπάρχει μικρότερη παραγωγή από την κανονική, μόνο για όση ώρα διαρκούν οι διαδικασίες αντικατάστασης μπαταριών ή επαναφόρτισης.

Για αυτό θέλουμε, σε αυτή την περίπτωση, ο χρόνος λειτουργίας που μεσολαβεί μεταξύ δύο διαδοχικών διακοπών για αλλαγή μπαταριών, να είναι μεγάλος, κατά προτίμηση πάνω από μία εβδομάδα. Αυτό βέβαια εξαρτάται και από το είδος των μπαταριών των αισθητήρων αλλά και από την μορφή κινητικότητας των κινητών κόμβων που αναγκάζουν τους στατικούς κόμβους να στέλνουν με ασύρματο δίκτυο τα δεδομένα τους. Όσο περισσότερο εκπέμπουν οι κόμβοι τα δεδομένα στο ασύρματο δίκτυο τόσο πιο γρήγορα εξαντλούν τη μπαταρία τους.

5.1.2.3. Συνολική επισκόπηση για το σενάριο Δεξαμενών Διυλιστηρίου πετρελαίου

Τοπολογία δικτύου: 2 δίκτυα πλέγματος WirelessHART με στατικούς κόμβους, ένα γύρω από κάθε δεξαμενή.

Πρωτόκολλο επικοινωνίας: WirelessHART.

Εύρος ζώνης (bandwidth): 2.4 GHz ως 2.4835 GHz

Διαμόρφωση ευθείας ακολουθίας με εξάπλωση φάσματος (Direct Sequence Spread Spectrum) (DSSS).

Πρότυπο IEC 62591.

Δύο Πύλες Gateways:

Οι δύο στατικοί κεντρικοί κόμβοι sinks που είναι οι πύλες Gateways του WirelessHART, είναι τοποθετημένες κάθε μία κοντά σε κάθε δεξαμενή και βρίσκονται μέσα στο πεδίο της βιομηχανικής εγκατάστασης (in-field).

Συσκευές πύλης (Gateway) που μπορούν να χρησιμοποιηθούν:

Για παράδειγμα, μία συσκευή Gateway, που υπάρχει στο εμπόριο, μπορεί να υποστηρίξει από 15 μέχρι και 100 συσκευές πεδίου (field devices). Όμως, όσο περισσότερες συσκευές πεδίου υπάρχουν σε ένα δίκτυο WirelessHART, τόσο περισσότερο αυξάνεται η καθυστέρηση (latency) για να φτάσουν τα δεδομένα στην πύλη (Gateway). Παρόλα αυτά η καθυστέρηση είναι σχετικά μικρή, της τάξεως δευτερολέπτων. Αν όμως το σύστημα είναι κρίσιμο ως προς το χρόνο, ακόμα και μία μικρή καθυστέρηση μπορεί να προκαλέσει προβλήματα.

Καθυστέρηση: (Latency)

Αν χρησιμοποιηθούν συγκεκριμένες συσκευές του εμπορίου, ως πύλες, υπάρχουν οι παρακάτω περιπτώσεις καθυστέρησης (latency).

Όταν το δίκτυο έχει μέχρι 100 συσκευές, τότε η καθυστέρηση είναι μέχρι 10 sec.

Όταν το δίκτυο έχει μέχρι 50 συσκευές, τότε η καθυστέρηση είναι μέχρι 5 sec.

Όταν το δίκτυο έχει μέχρι 15 συσκευές, τότε η καθυστέρηση είναι μέχρι 2 sec.

Στο δικό μας σύστημα το κάθε μεμονωμένο δίκτυο WirelessHART έχει 25 συσκευές επομένως είμαστε στην περίπτωση που η πιθανή καθυστέρηση (latency) είναι μέσα στα 5 sec.

Σταθεροί κόμβοι: Οι κόμβοι που είναι τοποθετημένοι γύρω από κάθε δεξαμενή. Γύρω από κάθε δεξαμενή υπάρχει ένα δίκτυο από συσκευές πεδίου που αποτελείται έστω από 25 κόμβους. Έτσι δημιουργούνται δύο δίκτυα WirelessHART, από 25 κόμβους, ένα γύρω από κάθε πύλη (Gateway).

Κινητοί κόμβοι: Ο εργάτης φέρει αισθητήρες κόμβους πάνω στη στολή του ή σε μία κινητή συσκευή ή σε ένα όχημα.

5.1.2.4. Υποθέσεις για να γίνει μία υλοποίηση

Για να γίνει μία υλοποίηση ενός συστήματος που υποστηρίζει τις παραπάνω απαιτήσεις, κάνουμε κάποιες υποθέσεις για το πώς θα λειτουργήσει ένα τέτοιο σύστημα.

Μερικές υποθέσεις είναι:

Ο τύπος συσκευών: Το είδος συσκευών που θα χρησιμοποιηθούν είναι κόμβοι αισθητήρες.

Η κινητικότητα: Οι κινητοί κόμβοι βρίσκονται στους κινούμενους εργάτες και υπάρχουν στο δίκτυο μόνο σε κάποιες περιπτώσεις, ενώ σε άλλες περιπτώσεις υπάρχουν μόνο οι στατικοί κόμβοι.

Το μέγεθος του δικτύου: Θα χρησιμοποιήσουμε 2 δίκτυα που το καθένα έχει 25 κόμβους.

Το είδος της τοπολογίας. Για τους στατικούς κόμβους θα έχουμε τοπολογία δικτύου πλέγματος στο ένα δίκτυο και τοπολογία δικτύου πλέγματος και στο άλλο δίκτυο.

Ο αριθμός αλμάτων: Το δίκτυο είναι πολλαπλών αλμάτων (multihop).

Το είδος της κυκλοφορίας: Υπάρχει μόνο ένα είδος κυκλοφορίας που είναι η κανονική κυκλοφορία.

Πλήθος ροών κυκλοφορίας: Μία ροή upstream για κάθε κινητό κόμβο.

Μία ροή downstream από τον κεντρικό κόμβο προς τους κινητούς κόμβους.

Μία ροή από τον ένα κεντρικό κόμβο στον άλλον κεντρικό κόμβο.

Τύπος της κυκλοφορίας: Η κυκλοφορία είναι περιοδική.

Συχνότητα της κυκλοφορίας: Είναι το πόσο συχνά κάθε κόμβος δημιουργεί ένα νέο πακέτο δεδομένων. Έστω ότι ένας κόμβος μπορεί να δημιουργεί νέο πακέτο δεδομένων κάθε 1 sec.

Όριο καθυστέρησης στην κυκλοφορία: Το όριο καθυστέρησης στην κυκλοφορία πρέπει να είναι 5sec για τη δική μας εφαρμογή.

5.1.2.5. Σύνδεση ενός εισερχόμενου κόμβου στο ένα δίκτυο WirelessHART

Στο δικό μας σενάριο έχουμε δύο δίκτυα WirelessHART. Έστω ότι ένας νέος κόμβος πρέπει να συνδεθεί στο ένα δίκτυο. Για να συνδεθεί θα πρέπει να βρει κάποιον κόμβο που βρίσκεται κοντά του και είναι ήδη συνδεδεμένος. Θα ανταλλάξει μηνύματα με τον κόμβο αυτόν.

Τότε θα υπάρχει ένα διάγραμμα ακολουθίας με τα μηνύματα που θα στείλει ο νέος κόμβος στο δίκτυο.

Ο μηχανισμός TDMA του WirelessHART βρίσκεται στο στρώμα MAC.

Ο χρόνος διαιρείται σε σχισμές (slots). Κάθε σχισμή έχει διάρκεια $10\text{ ms} = 1/100\text{ sec}$

Ένα υπερπλαίσιο διαχείρισης (management superframe) περιλαμβάνει 6400 σχισμές.

Άρα η διάρκεια ενός υπερπλαισίου διαχείρισης θα είναι $6400 / 100\text{ sec} = 64\text{ sec}$.

Ο διαχειριστής δικτύου Network Manager (NM) θα χειριστεί τη διαδικασία σύνδεσης του νέου κόμβου στο δίκτυο.

Στο διάγραμμα ακολουθίας φαίνονται 3 στοιχεία: ο νέος κόμβος (new node) που θα συνδεθεί στο δίκτυο, ο κόμβος (node) που είναι ήδη συνδεδεμένος στο δίκτυο, και ο διαχειριστής δικτύου (Network Manager) που διαχειρίζεται την σύνδεση του νέου κόμβου.

Η σύνδεση του νέου κόμβου απαιτεί να γίνουν τα παρακάτω βήματα:

1. Ο νέος κόμβος ενεργοποιεί τη σύνδεσή του και μπαίνει αρχικά σε λειτουργία λήψης (reception mode). Από τον συνδεδεμένο κόμβο λαμβάνει το μήνυμα

διαφήμισης (advertise message) που τον πληροφορεί ότι υπάρχει διαθέσιμο το δίκτυο WirelessHART. Το μήνυμα advertise message το έστειλε ο διαχειριστής δικτύου, και προωθήθηκε μέσω του κόμβου στον οποίο θα συνδεθεί ο νέος κόμβος.

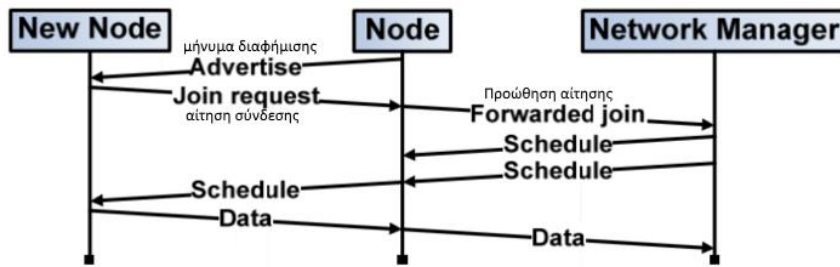
Το μήνυμα advertise περιέχει πληροφορίες για τον νέο κόμβο και καθορίζει μία σχισμή slot που λέγεται join slot, και μόνο σε αυτή τη χρονική στιγμή θα στείλει μήνυμα αίτησης σύνδεσης ο νέος κόμβος.

2. Ο νέος κόμβος θα στείλει το μήνυμα αίτησης σύνδεσης (join request message) όταν έρθει η σχισμή join slot.

Το μήνυμα σύνδεσης πάει στον συνδεδεμένο κόμβο και μετά ο συνδεδεμένος κόμβος το προωθεί σε επόμενο κόμβο για να ακολουθήσει μία διαδρομή πολλαπλών αλμάτων (multi hop) και τελικά να φτάσει στον διαχειριστή δικτύου (Network Manager).

3. Ο διαχειριστής δικτύου αποδέχεται τον νέο κόμβο και τότε ο διαχειριστής δικτύου (Network Manager) δημιουργεί έναν χρονοπρογραμματισμό (schedule) που περιλαμβάνει κατανομές σχισμών (slot allocations) σε διάφορους κόμβους. Μπορεί επίσης να αλλάξει τις κατανομές σχισμών που υπήρχαν προηγουμένως, ώστε να δημιουργήσει νέες διαδρομές δρομολόγησης δεδομένων. Ο διαχειριστής δικτύου (Network Manager) θα στείλει ένα μήνυμα με το χρονοπρογραμματισμό (schedule) προς τον κόμβο που ήταν ήδη συνδεδεμένος και μετά αυτός ο κόμβος θα προωθήσει το μήνυμα με το χρονοπρογραμματισμό στον νέο κόμβο που θέλει να συνδεθεί. Επίσης υπάρχουν και κάποια άλλα μηνύματα ασφαλείας αλλά δεν εμφανίζονται εδώ.
4. Μόλις ο νέος κόμβος λάβει τον χρονοπρογραμματισμό (schedule) τότε γίνεται η σύνδεσή του στο δίκτυο και μπορεί να κάνει και αυτός μετάδοση δεδομένων σε κατάλληλες χρονικές σχισμές (time slots), που τις έχει καθορίσει ο χρονοπρογραμματισμός.

Ο χρόνος που απαιτείται συνολικά για τα βήματα 1 ως 4, ονομάζεται χρόνος πρόσβασης (access time) και συμβολίζεται ως t_a .



Εικόνα 122. Διάγραμμα ακολουθίας για τη σύνδεση του νέου κόμβου στο δίκτυο WirelessHART. Πηγή [44]

Επιπλέον από αυτά τα μηνύματα, που φαίνονται στην παραπάνω εικόνα, υπάρχουν και τα μηνύματα ασφάλειας που ανταλλάσσουν με το διαχειριστή δικτύου οι συσκευές που πρόκειται να συνδεθούν, τα οποία δεν εμφανίζονται στο σχήμα. Τα μηνύματα αυτά περιλαμβάνουν κλειδιά δικτύου και άλλες τεχνικές πιστοποίησης.

5.1.2.6 Δείκτες μέτρησης απόδοσης (Performance Metrics)

Ως δείκτες μέτρησης της απόδοσης θεωρούνται οι προτεινόμενοι δείκτες από τους συγγραφείς στο [44].

Οι συγγραφείς για λόγους απλότητας στην περιγραφή, λαμβάνουν υπόψη την περίπτωση όπου υπάρχει στο δίκτυο μόνο ένας κινητός κόμβος, ο οποίος χρησιμοποιεί μόνο ένα κανάλι συχνότητας για να εκπέμψει τα δεδομένα του. Με βάση αυτή τη θεώρηση, μπορεί να γίνει έπειτα μία επέκταση αυτού του σεναρίου, ώστε να συμπεριλάβει πολλαπλούς κινητούς κόμβους που εκπέμπουν δεδομένα σε διαφορετικές συχνότητες.

Οι δείκτες μέτρησης απόδοσης είναι οι παρακάτω:

t_s είναι η διάρκεια (duration) μίας χρονικής σχισμής (time slot).

Υπερπλαίσιο διαχείρισης (Management Superframe):

N είναι το συνολικό πλήθος χρονικών σχισμών (time slots) του υπερπλαισίου διαχείρισης (Management Superframe).

$T_N = N \cdot t_s$ είναι η συνολική διάρκεια του υπερπλαισίου διαχείρισης (Management Superframe).

M είναι το πλήθος δεσμευμένων χρονικών σχισμών που χρησιμοποιούνται για τις λειτουργίες διαχείρισης (Management functions).

$T_M = M \cdot t_s$ είναι η διάρκεια των δεσμευμένων σχισμών διαχείρισης μέσα στο υπερπλαίσιο διαχείρισης (Management Superframe).

N-M είναι οι ελεύθερες σχισμές (free slots) που χρησιμοποιούνται από τους κόμβους για μετάδοση δεδομένων (data transmission) και για λήψη δεδομένων (data reception) μέσα στο υπερπλαίσιο διαχείρισης (Management Superframe).

t_e είναι ο χρόνος που ο κινητός κόμβος βρίσκεται μέσα στην κάλυψη ενός δικτύου WirelessHART.

N_h είναι το πλήθος αλμάτων (hops) που απαιτούνται για να φτάσουν τα δεδομένα από έναν κόμβο-πηγή σε έναν κόμβο προορισμό.

Ο βαθμός χρήσης καναλιού (Data_Ch_Usage):

είναι μία παράμετρος που δηλώνει αν υπάρχουν διαθέσιμες ελεύθερες σχισμές που μπορεί να τις δεσμεύσει ένας κόμβος για να εκπέμψει δεδομένα και υπολογίζεται με διαφορετικό τρόπο για στατικό κόμβο και για διαφορετικό τρόπο για κινητό κόμβο.

Είναι ένα κλάσμα που αριθμητής είναι το μέγιστο πλήθος διαθέσιμων σχισμών που μπορούν να ανατεθούν σε έναν κόμβο για να εκπέμψει δεδομένα, και ο παρονομαστής είναι το συνολικό πλήθος σχισμών του superframe.

Στο δίκτυο WirelessHART αν ένας κόμβος δεσμεύσει μία σχισμή (slot) δεν επιτρέπεται να ξαναχρησιμοποιηθεί η ίδια σχισμή slot για να μεταδώσει δεδομένα του και ένας άλλος κόμβος. Τελικά, προκύπτει ότι ο μέγιστος αριθμός σχισμών που μπορούν να ανατεθούν σε ένα κόμβο είναι:

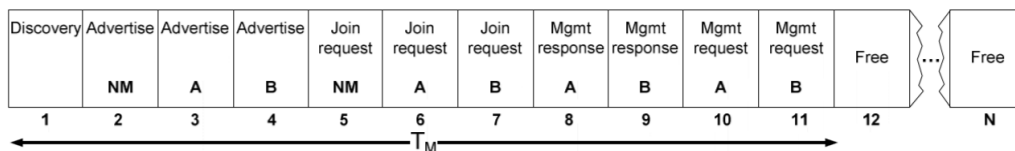
$$(N-M)/N_h$$

Έτσι, για έναν στατικό κόμβο, ο βαθμός χρήσης καναλιού θα είναι

$$\text{Data\_Ch\_Usage} = (N-M) / (N \cdot N_h).$$

Αν ο κόμβος είναι κινητός πρέπει να χρησιμοποιηθεί ένας διαφορετικός τύπος υπολογισμού του βαθμού χρήσης καναλιού.

t_a είναι ο χρόνος πρόσβασης (access time): Ο χρόνος που απαιτείται από τη στιγμή που ο κινητός κόμβος μπαίνει σε κατάσταση λήψης για να λάβει το μήνυμα advertise message, μέχρι να ολοκληρωθούν όλα τα βήματα σύνδεσης στο δίκτυο και να μπορεί να στείλει δεδομένα.



Εικόνα 123. Υπερπλαίσιο διαχείρισης (management superframe) στο WirelessHART. Πηγή [44]

Στην εικόνα φαίνονται ότι οι σχισμές slots από 1 ως 11 είναι δεσμευμένες για λειτουργίες διαχείρισης, ενώ οι σχισμές από 12 ως N είναι ελεύθερες για να μεταδοθούν δεδομένα από τους κόμβους.

5.1.2.7 Περιπτώσεις σύνδεσης κινητού κόμβου και βαθμός χρήσης καναλιού

Οι συγγραφείς στο [44], ορίζουν έναν διαφορετικό τύπο για τον βαθμό χρήσης καναλιού στην περίπτωση που ο κόμβος είναι κινητός.

Στον τύπο αυτό περιέχεται και ο χρόνος πρόσβασης t_a και παρουσιάζεται αργότερα σε αυτή την παράγραφο.

Ο κινητός κόμβος συνδέεται για κάποιο χρόνο στο δίκτυο, αλλά καθώς κινείται, μπορεί να γίνει μία υποβάθμιση της ζεύξης και να χάσει τη σύνδεσή του από το δίκτυο. Τότε λίγο πριν χάσει τη σύνδεσή του, ψάχνει έναν άλλο κόμβο του δικτύου για να συνδεθεί μέσω εκείνου στο δίκτυο.

Κατά την κίνηση του κινητού κόμβου μέσα σε μία τροχιά στο δίκτυο, πριν χαθεί η σύνδεσή του με τον τρέχοντα κόμβο, οι συγγραφείς στο [44] διακρίνουν δύο περιπτώσεις:

α) Η αποσύνδεση του κινητού κόμβου και η επανασύνδεση (Rejoin), συμβαίνει όταν δεν βρίσκει κανένα νέο κόμβο δικτύου για να διατηρήσει τη σύνδεση του στο δίκτυο, λίγο πριν χάσει τη σύνδεση με τον τρέχοντα κόμβο.

α) Η μεταβίβαση (handover), συμβαίνει όταν ο κινητός κόμβος βρει έναν νέο κόμβο δικτύου για να διατηρήσει τη σύνδεση του στο δίκτυο, λίγο πριν χαθεί η σύνδεση με τον τρέχοντα κόμβο.

Η επανασύνδεση:

Αποσύνδεση και επανασύνδεση γίνεται αν ο κινητός κόμβος, καθώς κινείται σε μία τροχιά, απομακρυνθεί από την εμβέλεια του στατικού κόμβου, που συνδέεται, αλλά δεν βρει κανέναν νέο κόμβο δικτύου για να διατηρήσει τη σύνδεσή του με το δίκτυο. Τότε πριν χάσει τελείως τη σύνδεσή του στο δίκτυο, θα πρέπει να ξεκινήσει διαδικασία επανασύνδεσης (Rejoin process). Όσο χρόνο διαρκεί αυτή η διαδικασία, ο κινητός κόμβος (mobile node) δεν θα δεσμεύσει καθόλου σχισμές (slots) για επικοινωνία. Έτσι δεν θα έχει δυνατότητα να στείλει δεδομένα στο δίκτυο. Τότε όμως υποβαθμίζεται η ποιότητα υπηρεσιών QoS.

Για να γίνει μία επανασύνδεση Rejoin, γίνονται ακριβώς τα βήματα σύνδεσης νέου κόμβου που αναφέρθηκαν προηγουμένως.

Και η διάρκεια αυτών των βημάτων είναι ο χρόνος πρόσβασης t_a

Ο χρόνος αυτός, όπως αναφέρθηκε, είναι ο χρόνος που απαιτείται από τη στιγμή που ο κινητός κόμβος μπαίνει σε κατάσταση λήψης για να λάβει το μήνυμα διαφήμισης (advertise message), μέχρι τη στιγμή που τελειώνει η διαδικασία σύνδεσης, συνδέεται πλήρως στο δίκτυο και μπορεί να στείλει δεδομένα.

Σε έναν κινητό κόμβο γίνεται συχνά η διαδικασία της αποσύνδεσης και της επανασύνδεσης (Rejoin process) διότι απομακρύνεται από την εμβέλεια των στατικών κόμβων και έτσι χάνεται η ποιότητα της ζεύξης και προσπαθεί να δημιουργήσει νέες ζεύξεις με άλλους κόμβους.

Ο χρόνος πρόσβασης t_a εμφανίζεται πολλές φορές συνολικά, στη διάρκεια κίνησης του κινητού κόμβου, εντός δικτύου, ώστε εισάγεται μία καθυστέρηση που είναι το άθροισμα των χρόνων t_a .

Ο χρόνος t_e είναι ο συνολικός χρόνος που ο κινητός κόμβος βρίσκεται μέσα στην κάλυψη του δικτύου. Στον χρόνο t_e θεωρούμε ότι θα συμβεί ένα πλήθος επανασυνδέσεων (Rejoins) που κάθε μία διαρκεί χρόνο t_a .

Όλες οι επανασυνδέσεις συνολικά διαρκούν τόσο χρόνο όσο είναι το άθροισμα των χρόνων t_a που συμβολίζεται ως Σt_a .

Αν αφαιρέσουμε από τον χρόνο t_e όλους τους χρόνους t_a τότε θα έχουμε το χρόνο $t_x = t_e - \Sigma t_a$.

Σε αυτό το χρόνο $t_x = t_e - \Sigma t_a$, ο κινητός κόμβος είναι μέσα στο δίκτυο, είναι συνδεδεμένος και μπορεί να στείλει δεδομένα κανονικά.

Όπως είδαμε, στο χρόνο t_e ο κινητός κόμβος είναι μέσα στο δίκτυο,

Ενώ στο χρόνο Σt_a είναι μέσα στο δίκτυο αλλά προσπαθεί να κάνει επανασύνδεση και δεν μπορεί να στείλει δεδομένα.

Οι συγγραφείς στο [44] δίνουν ένα διαφορετικό τύπο για το βαθμό χρήσης καναλιού σε αυτή την περίπτωση που είναι ο εξής:

$$\text{Data\_Ch\_Usage} = \left(\frac{N-M}{N*N_h} \right) * \left(\frac{t_e - \Sigma t_a}{t_e} \right)$$

Η μεταβίβαση:

Η δεύτερη περίπτωση είναι όταν ο κινητός κόμβος, λίγο πριν χάσει τη σύνδεση με τον τρέχοντα κόμβο του δικτύου, βρει έναν άλλο κόμβο για να συνδεθεί και τότε γίνεται η λειτουργία της μεταβίβασης (handover). (Αυτή δεν ορίζεται στο πρότυπο WirelessHART).

Η μεταβίβαση (handover) πρέπει να γίνει μέσω του διαχειριστή δικτύου Network Manager (NM). Ο διαχειριστής δικτύου θα αναθέσει νέες ανακατανομές στις σχισμές (slots) ώστε να μεταβιβάσει την επικοινωνία στον νέο κόμβο του δικτύου πριν αποσυνδεθεί ο κινητός κόμβος από τον τρέχοντα κόμβο που είναι συνδεδεμένος. Έτσι ο κινητός κόμβος δεν θα αποσυνδεθεί καθόλου από το δίκτυο αλλά θα συνεχίσει να στέλνει τα δεδομένα του χωρίς διακοπή καθώς κινείται. Πρέπει όμως ο διαχειριστής δικτύου να κάνει γρήγορα την μεταβίβαση πριν προλάβει να αποσυνδεθεί ο κινητός κόμβος από τον τρέχοντα κόμβο, για αυτό η διαδικασία είναι κρίσιμη ως προς το χρόνο και δεν πρέπει να συμβεί καθυστέρηση.

Κεφάλαιο 6

Συμπεράσματα και Μελλοντική Εργασία

Εδώ περιγράφονται ορισμένα συμπεράσματα και εισηγήσεις για το τι και πως θα μπορούσε να γίνει σαν συνέχεια αυτής της εργασίας. Τα συμπεράσματα αφορούν γενικά το πρότυπο WirelessHART, τα χαρακτηριστικά του και τις δυνατότητές του. Οι προτάσεις για μελλοντική εργασία αναφέρουν διάφορα παραδείγματα από βιομηχανίες και προτείνεται για αυτές η εισαγωγή του WirelessHART, για την επέκτασή τους και για τη βελτίωση των λειτουργιών τους.

6.1 Συμπεράσματα

Σε αυτή την παράγραφο, αναφέρονται μερικά γενικά συμπεράσματα για τα χαρακτηριστικά που υποστηρίζονται από το πρωτόκολλο WirelessHART και γίνεται μία γενική συζήτηση ως επίλογος της Μεταπτυχιακής Διατριβής.

Τα συμπεράσματα είναι απλώς κάποια σημεία που τονίζονται σε σχέση με τα θέματα που αναφέρθηκαν προηγουμένως και έχουν αναλυθεί με περισσότερες λεπτομέρειες στις προηγούμενες παραγράφους. Έτσι σε αυτή την παράγραφο, αναφέρονται πιο συνοπτικά

6.1.1 Το WirelessHART είναι πλήρως συμβατό με το παλαιότερο πρότυπο HART.

Το WirelessHART είναι πρωτόκολλο ασύρματων επικοινωνιών για δίκτυα πλέγματος (Mesh) που σχεδιάστηκε για να καλύψει τις απαιτήσεις εφαρμογών για αυτοματισμό διεργασιών και βασίστηκε στο πρωτόκολλο HART που χρησιμοποιείται αρκετά χρόνια στις βιομηχανίες αυτοματισμού διεργασιών.

Το WirelessHART είναι συμβατό προς τα πίσω με τις ήδη υπάρχουσες συσκευές και εφαρμογές HART χωρίς την ανάγκη αναβαθμίσεων λογισμικού. Αυτό είναι ίσως μία από τις αιτίες που επιλέγεται το WirelessHART σε πολλές βιομηχανίες έναντι άλλων προτύπων που έχουν τους ίδιους στόχους. Λόγω της συμβατότητας, οι παλαιότερες βιομηχανίες που χρησιμοποιούσαν πάνω από 20 χρόνια το HART και είχαν αναπτύξει βέλτιστες πρακτικές από την εμπειρία τους, θέλουν να κάνουν μικρές αλλαγές και να συνεχίσουν να χρησιμοποιούν τις προηγούμενες συσκευές ώστε να μην εγκαταλείψουν τις πρακτικές που είχαν συνηθίσει στο παρελθόν. Έτσι το WirelessHART, τους παρέχει την ευελιξία που χρειάζονται. Από την άλλη πλευρά, υπάρχουν άλλα πρότυπα που δεν συνεργάζονται τόσο καλά με το HART και απαιτούν περισσότερες τροποποιήσεις και προσαρμογές για να επικοινωνήσουν με το HART και ακόμα και τότε η υποστήριξη που παρέχουν δεν είναι πλήρης. Έτσι οι βιομηχανίες που χρησιμοποιούν το πρωτόκολλο HART είναι φυσικό σε κάθε επέκταση που σχεδιάζουν, να επιλέξουν το WirelessHART.

Η σύνδεση στο ασύρματο δίκτυο WirelessHART των παλαιότερων συσκευών HART γίνεται με τους προσαρμογείς (Adapters).

α) Οι συσκευές HART που είναι συνδεδεμένες από σημείο σε σημείο (Point-point) και οι συσκευές HART που είναι συνδεδεμένες με συνδεσμολογία πολλαπλών σημείων (multi-dropped) μπορούν να συνδεθούν με ένα προσαρμογέα (adapter) και έτσι να παρέχεται πρόσβαση σε όλες τις συσκευές που συνδέονται και λέγονται sub-devices

β) Οι προσαρμογείς WirelessHART Adapters παρέχουν υπηρεσίες δημοσίευσης δεδομένων εκ μέρους των συσκευών στις οποίες συνδέονται και λέγονται sub-devices.

Ακόμα και αν οι συσκευές sub-devices δεν υποστηρίζουν λειτουργία καταιγισμού Burst Mode ο Adapter επιτρέπει να χρησιμοποιούν και αυτή τη λειτουργία.

γ) Επειδή υπάρχουν ήδη τα εργαλεία HART, οι adapters πρέπει να έχουν ικανότητα για δύο διαφορετικές λειτουργίες, που είναι η κύρια συσκευή Token-Passing Master και η εξαρτώμενη συσκευή Slave στο δίκτυο των συνδεδεμένων συσκευών (sub-device)

δ) Στο WirelessHART οι πύλες (Gateways) απαιτείται να υποστηρίζουν τους προσαρμογείς (Adapters) και να συνεργάζονται μεταξύ τους ώστε να υπάρχει διαφανής δρομολόγηση μηνυμάτων για τις συνδεδεμένες συσκευές HART.

ε) Ο προσαρμογέας WirelessHART Adapter μπορεί να περιλαμβάνει και επιπλέον συνδέσεις σε αισθητήρες και επενεργητές πέρα από αυτούς που έχουν οι συσκευές HART.

6.1.2 Το WirelessHART είναι απλή και ανθεκτική τεχνολογία για δίκτυα πλέγματος (mesh).

Η αρχιτεκτονική του WirelessHART σχεδιάστηκε έτσι ώστε το πρωτόκολλο να είναι εύκολο στη χρήση και αξιόπιστο (reliable). Το WirelessHART δημιουργεί πολύ αξιόπιστα, αυτό-οργανωμένα και αυτό-θεραπευόμενα (self healing), δίκτυα πλέγματος (mesh) με πλεονασμό διαδρομών (redundant path). Αυτά τα δίκτυα πλέγματος είναι εύκολο να εγκατασταθούν και να λειτουργήσουν.

Το δίκτυο WirelessHART, λειτουργεί στη ζώνη συχνοτήτων 2.4GHz ISM και χρησιμοποιεί σήματα ασύρματης μετάδοσης που είναι συμβατά με το πρότυπο IEEE 802.15.4. Τα σήματα έχουν διαμόρφωση DSSS, με μεταπήδηση συχνότητας καναλιού (channel hopping) και μεταδίδονται με την μορφή πακέτων δεδομένων στα ασύρματα δίκτυα αισθητήρων σε τοπολογία πλέγματος.

6.1.3 Το WirelessHART έχει σχεδιαστεί με στόχο την διαλειτουργικότητα

Για να υπάρχει η διαλειτουργικότητα (interoperability), δηλαδή η δυνατότητα ώστε οι ασύρματες συσκευές που παρέχονται από διαφορετικούς κατασκευαστές, να χρησιμοποιούνται εναλλακτικά χωρίς να υπάρξουν οποιοδήποτε συμβιβασμοί που θα οδηγήσουν σε προβλήματα στη λειτουργία του συστήματος, το WirelessHART έχει καθορίσει τις υποχρεωτικές απαιτήσεις τις οποίες οι συμβατές συσκευές εξοπλισμού (compatible equipment) θα πρέπει να τις υποστηρίζουν.

6.1.4 Οι συσκευές WirelessHART υποστηρίζουν τη γλώσσα DDL

Ένα κοινό χαρακτηριστικό που υπάρχει στο HART και στο WirelessHART είναι ότι όλες οι συσκευές HART όπως είναι οι διαχειριστές δικτύου (network managers), οι πύλες (gateways), συσκευές πεδίου (field devices), πρέπει να υποστηρίζουν τη γλώσσα DDL.

Με αυτόν τον τρόπο μπορούν να εξάγουν αρχεία σε γλώσσα DDL με πληροφορίες που αφορούν τις διαγνώσεις κάθε συσκευής

6.1.5 Η επικοινωνία στο δίκτυο WirelessHART βασίζεται στο TDMA με superframes

Η επικοινωνία στο δίκτυο WirelessHART ανάμεσα στις δικτυακές συσκευές είναι βασισμένη στην τεχνολογία Time Division Multiple Access (TDMA).

Με τη μέθοδο TDMA το WirelessHART εκτελεί συντονισμό (coordinate) των επικοινωνιών και διαιτησία (arbitrate) ώστε να καθορίζει ποιος σταθμός θα μπορεί να εκπέμψει δεδομένα σε κάθε χρονική στιγμή. Το επίπεδο ζεύξης δεδομένων (Data-Link Layer) δημιουργεί ζεύξεις (links) που βασίζονται στο TDMA. Στις ζεύξεις καθορίζεται ποια σχισμή χρόνου (timeslot) και ποια συχνότητα (frequency) πρέπει να χρησιμοποιηθεί για την επικοινωνία ανάμεσα στις συσκευές. Αυτές οι ζεύξεις οργανώνονται σε υπερπλαίσια (superframes) που επαναλαμβάνονται περιοδικά. Τα υπερπλαίσια είναι ένα σύνολο από σχισμές χρόνου. 100 σχισμές χρόνου αντιστοιχούν σε 1 sec. Καθορίζονται διαφορετικά είδη υπερπλαισίων για διάφορες λειτουργίες.

Υπερπλαίσια (Superframes) μπορεί να επιτρέπονται (enabled) ή να απενεργοποιούνται (disabled) ανάλογα με τη ζήτηση ευρους ζώνης (bandwidth demand) που υπάρχει στο δίκτυο.

6.1.6 Το WirelessHART δημιουργεί δύο διαφορετικούς τύπους ζεύξεων

Οι ζεύξεις διακρίνονται σε δύο διαφορετικούς τύπους:

α) διαμοιραζόμενη (shared) ζεύξη. Είναι μία μορφή ζεύξης που επιτρέπει ελαστική χρήση στο εύρος ζώνης τηλεπικοινωνιών. Η επικοινωνία μεταξύ δύο κόμβων γίνεται μέσω πολλαπλών αλμάτων.

β) αφιερωμένη (dedicated) ζεύξη

Είναι μία ζεύξη που διασφαλίζει ότι τα δεδομένα της διεργασίας (process data) θα φτάσουν με ελάχιστη καθυστέρηση (latency). Η συσκευή για ένα διάστημα εκπέμπει δεδομένα καταιγισμού σε υψηλότερο ρυθμό από ότι στην κανονική λειτουργία.

6.1.7. Δεδομένα κυκλικά και Δεδομένα ακυκλικά.

Η κυκλοφορία δεδομένων που υποστηρίζεται, είναι και η κυκλική , και η ακυκλική. Όταν λέγονται τα δεδομένα κυκλικά (Cyclic data), στη βιομηχανία , αυτό αναφέρεται στο ότι τα δεδομένα πρέπει να παραδίδονται με κάποιο χρονικό πρόγραμμα (schedule) το οποίο είναι γνωστό ή προβλέψιμο. Η παράδοση δεδομένων οφείλει να γίνεται με κάποια εγγύηση ως προς το χρόνο που θα φτάσουν στον προορισμό και με περιορισμένη καθυστέρηση σε όρια που είναι από πριν γνωστά. Τα δίκτυα που μεταφέρουν κυκλικά δεδομένα, συνήθως έχουν μορφή κύριου σταθμού / εξαρτώμενου σταθμού (master/slave). Μόνο μία συσκευή επιτρέπεται να στέλνει δεδομένα κάθε φορά και κάθε φορά που στέλνεται ένα μήνυμα, η συσκευή προορισμού στέλνει πίσω στον αποστολέα ένα μήνυμα για επιβεβαίωση λήψης. Έτσι πάντα τα μηνύματα που στέλνονται είναι της μορφής αίτησης/απόκρισης (request/response). Συνήθως σε μία κυκλική κυκλοφορία δεδομένων τα δεδομένα που μεταφέρονται είναι μεγάλες ποσότητες αλλά με πιο αργούς ρυθμούς.

Τα ακυκλικά δεδομένα (Acyclic data) είναι επίσης αξιόπιστα, αλλά δεν παραδίδονται με τόσο αυστηρές εγγυήσεις και παραδίδονται με έναν τρόπο λιγότερο ντετερμινιστικό, δηλαδή ο χρόνος που φτάνουν τα δεδομένα στον προορισμό κυμαίνεται από milliseconds, μέχρι seconds. Τα δίκτυα που μεταφέρουν τα ακυκλικά δεδομένα συνήθως είναι μεγαλύτερα. Αυτά τα δίκτυα παραλείπουν την μέθοδο της χειραψίας (handshaking) πριν την επικοινωνία και μπορούν να στείλουν δεδομένα με πιο γρήγορες ταχύτητες για κάποιο χρονικό διάστημα. Όμως αυτό έχει το κόστος ότι υπάρχουν συχνά συγκρούσεις και συμφορήσεις στο δίκτυο και μπορεί να χαθούν πακέτα δεδομένων που είναι χρήσιμα επειδή ο προορισμός δεν στέλνει μήνυμα επιβεβαίωσης λήψης ή αποτυχίας λήψης πακέτου και έτσι μπορεί να υπάρξουν απώλειες δεδομένων και απαίτηση για συχνές επαναληπτικές μεταδόσεις.

Το WirelessHART, υποστηρίζει και τα κυκλικά δεδομένα και τα ακυκλικά με διαφορετικές λειτουργίες μηνυμάτων.

Όλες οι συσκευές (devices) υποστηρίζουν πολλαπλά υπερπλαίσια (superframes) με διαφορετικούς αριθμούς σχισμών χρόνου (differing numbers of timeslots) που επιτρέπουν μία μίξη κυκλοφορίας στο δίκτυο

δηλαδή κυκλοφορίας

γρήγορης (fast) (1 second),

αργής (slow) (minutes),

κυκλικής (cyclic),

άκυκλης (acyclic).

6.1.8 Το WirelessHART υποστηρίζει πολλαπλές λειτουργίες μηνυμάτων.

Οι πολλαπλές λειτουργίες μηνυμάτων (messaging modes) που υποστηρίζει το WirelessHART είναι :

α) Η μονόδρομη δημοσίευση των τιμών διεργασιών (process values) από τις συσκευές προς τον κεντρικό κόμβο sink καθώς και των τιμών ελέγχου (control values). Τα δεδομένα διεργασιών (process data) και τα σημεία ρύθμισης (setpoints) μπορούν να δημοσιεύονται περιοδικά (published periodically), όταν συμβεί σημαντική αλλαγή στην τιμή τους (significant change) ή όταν η τιμή τους ξεπεράσει ένα κρίσιμο όριο ευαισθησίας (crossing a critical threshold).

β) Μηνύματα με αυθόρμητες ειδοποιήσεις, κατ' εξαίρεση, για διάφορα συμβάντα. Όταν η κατάσταση μίας συσκευής (device status) ή η κατάσταση της διεργασίας (process status) αλλάζει, τότε αυτόματα δημιουργεί μήνυμα ειδοποίησης (notification message) στις εφαρμογές (applications).

γ) Επικοινωνία με Αιτήσεις /αποκρίσεις (request/response) μεταξύ ομότιμων κόμβων, επιπλέον αυτή η μορφή επικοινωνίας αιτήσεων/αποκρίσεων χρησιμοποιείται για

μεταφορά δεδομένων που αφορούν συντηρήσεις ρουτίνας, ρυθμίσεις, βαθμονομήσεις οργάνων.

δ) Αυτόματο τεμαχισμό μεγάλων μηνυμάτων (auto-segmented) σε μεταφορές μπλοκ δεδομένων (block transfers) για να μεταφέρονται μεγάλα σύνολα δεδομένων. Με αυτή την τεχνική μπορούν να μεταφερθούν δεδομένα όπως είναι κυματομορφές από φάσματα κραδασμών, ή δεδομένα από κυματομορφές ραντάρ.

ε) Όλα τα μηνύματα έχουν μία καλά ορισμένη προτεραιότητα (priority) που εξασφαλίζει την παράδοση μηνυμάτων με την κατάλληλη ποιότητα υπηρεσιών QoS. Το επίπεδο προτεραιότητας (Priority level) έχει 4 επίπεδα (levels):

- Command υψηλότερη προτεραιότητα (highest priority). Οποιοδήποτε πακέτο περιέχει δεδομένα στο πεδίο payload που τα στέλνει ο διαχειριστής δικτύου (Any packet containing Network Management payloads).
- Δεδομένα επεξεργασίας (Process Data) Οποιοδήποτε πακέτο περιέχει δεδομένα επεξεργασίας (process data) (π.χ., Command 3 ή 9).
- Κανονικό Normal. Τα υπόλοιπα πακέτα DLPDUs που δεν ανήκουν στις κατηγορίες "Command", "Process Data", ή "Alarm".
- Alarm συναγερμός χαμηλότερη προτεραιότητα (lowest priority). Τα πακέτα που περιέχουν στο πεδίο payload μόνο συναγερμούς alarm και συμβάντα (event) payload. Μόνο ένα πακέτο δεδομένων DLPDU με προτεραιότητα συναγερμού "Alarm" priority μπορεί να είναι αποθηκευμένο στην ενδιάμεση μνήμη (buffered) και όχι περισσότερα πακέτα ταυτόχρονα.

Τα μηνύματα χαμηλής προτεραιότητας (Low priority messages) απορρίπτονται (declined) καθώς γεμίζει η ενδιάμεση μνήμη της συσκευής (buffer).

στ) Το αφιερωμένο εύρος ζώνης (Dedicated bandwidth) χρησιμοποιείται για να υπάρχει υψηλή προτεραιότητα (priority) και περιοδικές επικοινωνίες.

ζ) Το διαμοιραζόμενο εύρος ζώνης (Shared bandwidth) παρέχει ελαστικότητα στην κυκλοφορία με βάση τα συμβάντα (event traffic) και στα μηνύματα (messages) που είναι μηνύματα αίτησης/απόκρισης (request/response) μηνύματα συντήρησης (maintenance messages) και διαγνωστικά μηνύματα (diagnostic messages).

6.1.9 Τα στρώματα στο WirelessHART δημιουργήθηκαν ως μία επέκταση των στρωμάτων του HART

Το πρωτόκολλο HART δημιουργεί ένα δίκτυο της κατηγορίας «token passing network». Το token είναι ένα μήνυμα δεδομένων ή μία σειρά από bits που δίνει άδεια στον κόμβο που έχει το token να ξεκινήσει την επικοινωνία του.

Το HART υποστηρίζει και την κυκλοφορία μηνυμάτων αίτησης/απόκρισης (request/response) και την δημοσίευση των δεδομένων μίας διεργασίας (process data).

Όταν συμπεριλήφθηκε στο HART το ασύρματο πρωτόκολλο WirelessHART, καθορίστηκε να υπάρχει ένα επιπρόσθετο φυσικό στρώμα (Physical Layer) και ένα στρώμα ζεύξης δεδομένων (Data Link Layer), για υποστηρίζεται το WirelessHART.

Αυτά τα στρώματα που καθορίστηκαν είναι:

το IEEE STD 802.15.4-2006 για το φυσικό επίπεδο (Physical Layer)

το TDMA για το επίπεδο ζεύξης δεδομένων (Data-Link Layer).

Επειδή το WirelessHART επιτρέπει την πλήρη δημιουργία των ασύρματων δικτύων πλέγματος (wireless mesh networks) δημιουργήθηκε μία πλήρης προδιαγραφή για το επίπεδο δικτύου (Network Layer).

Το WirelessHART υποστηρίζει το επίπεδο εφαρμογής HART (HART Application Layer).

6.1.10 Το WirelessHART είναι κατάλληλο εφαρμογές και σε μεγάλες βιομηχανικές εγκαταστάσεις και σε μικρότερες εγκαταστάσεις

Υποστηρίζονται οι εφαρμογές ευρείας περιοχής (Wide-area applications) για εγκαταστάσεις που καταλαμβάνουν μεγάλες εκτάσεις στο γεωγραφικό χώρο όπως π.χ.,

φάρμες δεξαμενών ή αγωγοί μεταφοράς πετρελαίου. Επίσης υποστηρίζονται εφαρμογές και για μικρές μονάδες, όπως είναι οι μικρές φαρμακευτικές μονάδες. Οι δυνατότητες του WirelessHART επιτρέπουν να σχεδιαστούν νέες εφαρμογές. Τυπικές εφαρμογές που υποστηρίζει το WirelessHART είναι: Παρακολούθηση του εξοπλισμού και των διεργασιών, παρακολούθηση του περιβαλλοντος, διαχείριση της ενέργειας, συμμόρφωση με τους κανονισμούς συμβατότητας, διαχείριση πόρων, προληπτική συντήρηση, προχωρημένες διαγνώσεις και Έλεγχο κλειστού βρόχου όπου μπορεί να γίνει αυτό. Μια βιομηχανία μπορεί να ξεκινήσει με μικρές αλλαγές και σταδιακά να προσθέσει νέες συσκευές στο δίκτυο WirelessHART. Αυτό βελτιώνει τη λειτουργία του δικτύου και αυξάνει την αξιοπιστία στις επικοινωνίες.

6.1.11 Το WirelessHART υποστηρίζει τη συνύπαρξη με άλλα ασύρματα δίκτυα

Το WirelessHART λειτουργεί στη ζώνη συχνοτήτων ISM και χρησιμοποιεί διάφορες μεθόδους που επιτρέπουν να μη γίνονται παρεμβολές στο WirelessHART από άλλα δίκτυα που υπάρχουν στην ίδια περιοχή και λειτουργούν στην ίδια ζώνη συχνοτήτων ISM, όπως είναι το WiFi. Οι μέθοδοι που υποστηρίζονται είναι:

α) ο έλεγχος ελεύθερου καναλιού, Clear Channel Assessment (CCA)

Για να μην υπάρχουν συγκρούσεις, κάθε συσκευή WirelessHART εκτελεί έλεγχο καθαρού καναλιού CCA και μετά εκπέμπει τα δεδομένα. Στο IEEE 802.15.4, ο έλεγχος CCA διαρκεί μία περίοδο 128μs και ελέγχεται αν το κανάλι είναι απασχολημένο (busy) ή αδρανές (idle) πριν μεταδώσει η συσκευή το μήνυμά της. Αυτός ο μηχανισμός μειώνει τις παρεμβολές και τις συγκρούσεις στο κανάλι.

β) η μεταπήδηση συχνότητας καναλιού (channel hopping).

Στο WirelessHART χρησιμοποιείται το πρότυπο IEEE 802.15.4 και η συχνότητα 2.4 GHz της ζώνης ISM διαιρείται σε 16 κανάλια συχνοτήτων που δεν επικαλύπτονται μεταξύ τους. Αντίθετα, ένα δίκτυο WiFi που ακολουθεί το πρότυπο IEEE 802.11b/g και λειτουργεί στη ίδια ζώνη συχνοτήτων, χρησιμοποιεί ένα από τρία διαφορετικά κανάλια και δεν εκπέμπει συνεχώς, αλλά περιοδικά. Το WirelessHART με μία ψευδοτυχαία ακολουθία χρησιμοποιεί διαφορετικά κανάλια με μεταπήδηση συχνότητας και διατηρεί τη χρήση κάθε καναλιού για ένα μικρό χρονικό διάστημα. Έτσι οι πιθανότητες να γίνει

μία σύγκρουση μεταξύ του δικτύου WirelessHART και του δικτύου WiFi στην ίδια συχνότητα, ελαχιστοποιούνται.

γ) Η μαύρη λίστα καναλιών (blacklisting), και η αξιολόγηση των καναλιών.

Το WirelessHART ρυθμίζεται για να αποφεύγει μερικά κανάλια, που χρησιμοποιούνται σε μεγάλο βαθμό από άλλα δίκτυα και έτσι επιτυγχάνει να μην υπάρχουν παρεμβολές. Αλλά επειδή τα περισσότερα δίκτυα δεν εκπέμπουν συνεχώς, αυτή η μέθοδος σπάνια απαιτείται. Επιπλέον, κάθε συσκευή WirelessHART πριν στείλει δεδομένα ακούει το κανάλι και αν ανιχνεύσει άλλες μεταδόσεις, αναβάλλει την δική της μετάδοση για μία άλλη σχισμή χρόνου time slot και σε μία διαφορετική συχνότητα.

δ) Η ρυθμιζόμενη ισχύς εκπομπής και η διαμόρφωση σήματος που επιτρέπει εκπομπή χαμηλής ισχύος. Οι πομποί συσκευών του WirelessHART ακολουθούν το πρότυπο IEEE 802.15.4, και το σήμα τους με ενίσχυση 10dB μπορεί να φτάσει στα 200m. Αλλά όταν δεν απαιτείται να εκπέμψουν στην πλήρη απόσταση, μπορούν να εκπέμψουν με χαμηλότερη ισχύ σήματος. Έτσι αποφεύγουν τις παρεμβολές σε δίκτυα WiFi που ακολουθούν το πρότυπο IEEE 802.11b/g.

ε) Η διαμόρφωση TDMA επιτρέπει να μεταβάλλεται ο χρόνος των επικοινωνιών μεταξύ δύο συσκευών. Διαιρείται ο χρόνος σε σχισμές 10 msec και έτσι εξασφαλίζεται ότι μόνο ένα ζεύγος συσκευών θα επικοινωνούν μεταξύ τους σε κάθε χρονική σχισμή στην ίδια συχνότητα και δεν θα υπάρχουν συγκρούσεις. Επιτρέπεται να επικοινωνούν ταυτόχρονα και άλλα ζεύγη συσκευών σε διαφορετικές συχνότητες.

στ) Η διαμόρφωση Ευθείας ακολουθίας με εξάπλωση φάσματος (Direct Sequence Spread Spectrum) DSSS.

Η διαμόρφωση DSSS έχει το πλεονέκτημα ότι χρησιμοποιεί μοναδικούς αλγόριθμους κωδικοποίησης. Η μετάδοση εξαπλώνεται σε όλο το φάσμα της ζώνης συχνοτήτων που αποτελεί ένα κανάλι. Οι συσκευές που λαμβάνουν τα δεδομένα πρέπει να έχουν τις σωστές πληροφορίες αποκωδικοποίησης. Αν οι συσκευές δεν έχουν τις σωστές πληροφορίες αποκωδικοποίησης, βλέπουν τα δεδομένα ως λευκό θόρυβο και τα απορρίπτουν. Για αυτό είναι εφικτό να στέλνονται ταυτόχρονα πολλά σήματα που επικαλύπτονται και μπορούν να τα αναγνωρίσουν μόνο οι συσκευές προορισμού.

ζ) Το δίκτυο πλέγματος (mesh) και η χρήση χαμηλής ισχύος εκπομπής μεταξύ των κόμβων, επιτρέπουν να στέλνονται τα δεδομένα σε διαδρομές πολλαπλών αλμάτων και

όχι απευθείας από έναν κόμβο σε έναν απομακρυσμένο κόμβο. Με αυτόν τον τρόπο μπορούν να υπάρξουν πολλαπλές διαδρομές πλεονασμού και έτσι να υπάρχει αξιοπιστία. Αν ένα δίκτυο wifi τοποθετηθεί έτσι ώστε οι συσκευές του να απέχουν πάνω από 1 m από τις συσκευές του WirelessHART, τότε τα σήματα WirelessHART δεν θα δημιουργούν παρεμβολές στις συσκευές WiFi και έτσι τα διαφορετικά δίκτυα θα λειτουργούν κανονικά και χωρίς προβλήματα.

Αυτές οι μέθοδοι μεγιστοποιούν τη συνύπαρξη (coexistence) ανάμεσα στα δίκτυα WirelessHART και σε άλλες συσκευές εξοπλισμού (equipment) που βρίσκονται στον ίδιο χώρο.

Επιπλέον, αν συμβούν παρεμβολές, και χαθούν κάποια δεδομένα, το WirelessHART υποστηρίζει την αναγνώριση πακέτου, στο στρώμα ζεύξης δεδομένων. Επειδή γίνονται αυτόματες επαναληπτικές μεταδόσεις, έτσι επιτυγχάνεται να μην υπάρχει απώλεια δεδομένων σε περίπτωση παρεμβολών.

6.2 Μελλοντική Εργασία

Υπάρχουν πολλές πιθανές εφαρμογές που μπορούν να σχεδιαστούν στη βιομηχανία με το πρότυπο WirelessHART. Στις παραγραφους που ακολουθούν, παρουσιάζονται ορισμένες προτάσεις για μελλοντικές εργασίες σε διάφορες περιπτώσεις βιομηχανιών όπου θα μπορούσε να γίνει εφαρμογή του προτύπου WirelessHART. Αυτές οι προτάσεις περιγράφονται με τη μορφή πιθανών σεναρίων και μπορούν να αποτελέσουν μία βάση για να προταθούν και άλλες εργασίες σχετικά με το πρότυπο WirelessHART, ή/και ως παραδείγματα για να μελετηθούν και να εξεταστεί η δυνατότητα υλοποίησής τους.

6.2.1. Επιτήρηση κατά μήκος ενός αγωγού Διυλιστηρίου πετρελαίου

Ένα πιθανό σενάριο για έρευνα, είναι ο έλεγχος ενός αγωγού πετρελαίου, για βλάβες ή σφάλματα που μπορεί να εμφανιστούν στον αγωγό με την πάροδο του χρόνου. Παρακάτω εξηγούμε μία μέθοδο που δείχνει πώς θα μπορούσε ένα ασύρματο δίκτυο αισθητήρων WirelessHART ή με κάποιο άλλο πρότυπο, να χρησιμοποιηθεί για τον έλεγχο ασφαλείας των αγωγών πετρελαίου.

Υποθέτουμε ότι υπάρχει ένας αγωγός πετρελαίου. Επίσης υπάρχει ο κεντρικός κόμβος sink, στον οποίο συγκεντρώνονται τα δεδομένα.

Άλλοι κόμβοι που υπάρχουν είναι οι στατικοί κόμβοι αισθητήρες οι οποίοι μετρούν ροή, θερμοκρασία, πίεση και είναι τοποθετημένοι σε κάποια διαστήματα κατά μήκος του αγωγού.

Ο σταθερός κόμβος sink βρίσκεται σε ένα κεντρικό σημείο του αγωγού πετρελαίου.

Εκατέρωθεν του sink, σε διάφορες αποστάσεις μεταξύ τους, βρίσκονται καταναμετημένοι πολλοί σταθεροί κόμβοι αισθητήρες, που μετρούν ροή, στάθμη, θερμοκρασία στον αγωγό. Ένα κινητό ρομπότ που έχει αισθητήρες κόμβους χρησιμοποιείται για να συλλέγει δεδομένα από σταθερούς κόμβους. Το ρομπότ ξεκινάει από τον sink και επισκέπτεται τους κόμβους αισθητήρες και καταλήγει σε ένα σημείο του αγωγού που είναι σε κάποια απόσταση από τον sink.

Το ρομπότ σταματάει σε κάθε κόμβο αισθητήρα για ένα χρονικό διάστημα και συλλέγει δεδομένα. Στη συνέχεια επιστρέφει στο sink και παραδίδει τα δεδομένα.

Επίσης εκεί μπορεί να φορτίζεται. Τα δεδομένα θα μπορούν να προωθούνται στον sink και με μία διαδρομή πολλαπλών αλμάτων αλλά η χρήση του ρομπότ θα βοηθήσει να συλλεχθούν κάποια δεδομένα από απομακρυσμένους κόμβους που θα ήθελαν πολλαπλά άλματα. Με τη χρήση του ρομπότ, θα μεταδοθούν τα δεδομένα με απόσταση ενός άλματος.

Ο sink θα λάβει τα δεδομένα και θα τα μεταφέρει στο κέντρο ελέγχου.

Στη συνέχεια το κέντρο ελέγχου θα στείλει εντολές σε επενεργητές. Που θα κλείσουν βαλβίδες αποκοπής (shutoff valves) οι οποίες θα κλείσουν με ερμητικό σφράγισμα και έτσι θα αποκόψουν τους αγωγούς πριν και μετά το σημείο της διαρροής και θα κάνουν μία απομόνωση. Υπάρχουν οι λεγόμενες τυφλές βάνες που τοποθετούνται κατά την απομόνωση τμημάτων της εγκατάστασης για να γίνουν διάφορες εργασίες. Με αυτό τον τρόπο το σημείο της διαρροής θα απομονωθεί και θα χαθεί όσο το δυνατόν λιγότερο από το υγρό που μεταφέρουν οι αγωγοί και έτσι θα υπάρχει μικρότερο πρόβλημα μόλυνσης στο περιβάλλον και λιγότερη απώλεια προϊόντος.

Ένα 2^ο ρομπότ όμοιο με το άλλο, ξεκινάει από τον sink και κινείται κατά μήκος του αγωγού προς την αντίθετη κατεύθυνση. Το ρομπότ σταματάει σε κάθε κόμβο και συλλέγει δεδομένα. Στη συνέχεια επιστρέφει στο sink και παραδίδει τα δεδομένα.

Παραλλαγή 1.

Αυτή η ίδια δομή μπορεί να επαναλαμβάνεται σε περισσότερα τμήματα του αγωγού και ο καθένας sink να έχει ένα δικό του δίκτυο WirelessHART που εκτείνεται εκατέρωθεν του.

Παραλλαγή 2.

Μια άλλη παραλλαγή του σεναρίου με χρήση κεφαλών συστοιχίας, είναι η παρακάτω:

Για να μειωθούν περισσότερο οι κινήσεις του ρομπότ προς κάποιους κόμβους, μπορεί να υπάρχει ένας κόμβος κεφαλή συστοιχίας που αντιστοιχεί σε κάποιο σύνολο κόμβων μιας περιοχής, όπου όλοι οι κόμβοι θα στέλνουν τα δεδομένα τους στην κεφαλή συστοιχίας, και στη συνέχεια το ρομπότ θα επισκέπτεται μόνο την κεφαλή συστοιχίας για να λάβει τα δεδομένα. Έτσι πρέπει να τοποθετηθούν κεφαλές συστοιχίας σε σταθερές αποστάσεις από τους sink κατά μήκος του αγωγού.

Το σύστημα έχει τους παρακάτω στόχους:

α) Ανιχνεύει σε έναν αγωγό πχ ροή υγρού μέσα στον αγωγό,

β) ατέλειες δομής του αγωγού,

γ) διαρροές σε συγκολλήσεις.

Το κάθε ρομπότ κινείται με μία γραμμική κίνηση που είναι κατά μήκος του αγωγού. Η κίνηση του ρομπότ ακολουθεί το μήκος του αγωγού για μία απόσταση

και μετά εκτελεί την αντίθετη κίνηση και επιστρέφει στον sink.

Οι απαιτήσεις για ανίχνευση σφαλμάτων και διαρροών στον αγωγό περιγράφονται ως εξής

Σενάριο: Διυλιστήριο πετρελαίου (αγωγοί)

Τύπος αισθητήρα: Ο στατικός: Ασύρματος, μετρητής ροής, μετρητής θερμοκρασίας, μετρητής στάθμης. Ο κινητός: ασύρματος.

Μοντέλο παράδοσης των δεδομένων: Συνεχές.

Κρίσιμες απαιτήσεις: Χαμηλή καθυστέρηση, χωρίς απώλειες πακέτων.

6.2.2. Αποθήκη

Κινητοί κόμβοι αισθητήρες πάνω σε UAV φορτηγάκια που μεταφέρουν τα προϊόντα σε κιβώτια.

Για αποθήκευση, από τις πόρτες εισόδου της αποθήκης προς τη θέση αποθήκευσης μεταφέρονται τα προϊόντα μέσω διαδρόμων.

Για παράδοση στον πελάτη, από τις θέσεις αποθήκευσης προς τις πόρτες εξόδου της αποθήκης μεταφέρονται τα προϊόντα.

Αν οι διάδρομοι είναι ευθείες και οριζόντιες γραμμές μπορεί να χρησιμοποιηθεί το μοντέλο κινητικότητας Manhattan.

Περιπτώσεις κίνησης:

α) Το όχημα μεταφέρει τα κιβώτια από την είσοδο της αποθήκης στη θέση που πρόκειται να αποθηκευτούν.

β) Το όχημα αλλάζει θέσεις στα κιβώτια μέσα στην αποθήκη για να εξοικονομήσει χώρο για νέα κιβώτια.

γ) Το όχημα περιφέρεται ανάμεσα στα κιβώτια και καταγράφει το πλήθος κιβωτίων.

δ) Το όχημα κάνει αναζήτηση ενός κιβωτίου

ε) Το όχημα μεταφέρει ένα κιβώτιο μέσα από την αποθήκη προς την έξοδο της αποθήκης για να το παραδώσει στον πελάτη.

Σε αυτό το σενάριο θα μπορούσε να χρησιμοποιηθεί το WirelessHART, ώστε να στέλνει δεδομένα σε πραγματικό χρόνο για όλα τα παραπάνω στοιχεία σε μία κεντρική εφαρμογή.

6.2.3 Εργοστάσιο παραγωγής αυτοκινήτων

Γραμμή παραγωγής οχημάτων που συναρμολογούνται.

Ρομποτικοί βραχίονες, κάνουν συγκολλήσεις σε διάφορα τμήματα του οχήματος υπό κατασκευή. Ο κινητός κόμβος αισθητήρας βρίσκεται στο ρομποτικό βραχίονα. Κινητός κόμβος αισθητήρας βρίσκεται και μέσα στο όχημα υπό κατασκευή.

Σε αυτό το σενάριο θα μπορούσε να χρησιμοποιηθεί το WirelessHART για να στέλνει δεδομένα σχετικά με τη θέση του βραχίονα σε πραγματικό χρόνο. Άλλα δεδομένα που θα μπορούσε να στέλνει, είναι: η κατάσταση υγείας, του βραχίονα, το πλήθος κομματιών που έχει συγκολλήσει ανάλογα με την ημερομηνία και την ώρα, το πλήθος κομματιών που δεν συναρμολόγησε επειδή υπήρξε κάποιο σφάλμα. Ο αισθητήρας μέσα στο όχημα μπορεί να στέλνει πληροφορίες σε πραγματικό χρόνο, για το πόσο μέρος των συγκολλήσεων έχει ολοκληρωθεί, τη θέση που βρίσκεται το κομμάτι και ποιος βραχίονας αναλαμβάνει τη συγκόλληση, πιο μέρος του κομματιού συγκολλήθηκε και ποιο δεν συγκολλήθηκε.

6.2.4 Βιομηχανία χαρτοποιίας

Δύο βασικές λειτουργίες που εκτελεί η χαρτοβιομηχανία είναι α) η παραγωγή χαρτοπολτού και χαρτιού και β) η λειτουργία επικάλυψης χαρτιού.

Σε ένα σενάριο βιομηχανίας έστω ότι υπάρχουν π.χ. 100 αισθητήρες μέτρησης ροής flow meters και 90 αισθητήρες μέτρησης πίεσης (pressure sensors).

Επίσης υπάρχουν αρκετές βαλβίδες ελέγχου (control valves).

Τα έξυπνα όργανα συνδέονται με ένα PLC.

Θα μπορούσε να γίνει χρήση του WirelessHART, ώστε να στέλνονται σε πραγματικό χρόνο πληροφορίες διάγνωσης για την υγεία των συσκευών. Επιπλέον θα μπορούσαν να καταγράφονται σε πραγματικό χρόνο οι τιμές μέτρησης πίεσης και ροής, όπως και η θέση των βαλβίδων ελέγχου και να παρέχονται συγκεντρωτικές αναφορές για την τρέχουσα κατάσταση.

6.2.5 Βιομηχανία με αγωγούς μεταφοράς πετρελαίου

Σε μία βιομηχανία αγωγών μεταφοράς πετρελαίου, στον αγωγό υπάρχουν έξυπνα όργανα μέτρησης, όπως είναι: Πομποί πίεσης, Πομποί θερμοκρασίας, Πομποί ροής.

Το πλήθος αυτών των πομπών μπορεί να είναι πολλές χιλιάδες, για έναν αγωγό πολύ μεγάλου μήκους και στέλνουν πάρα πολλά σήματα μετρήσεων. Η χρήση του WirelessHART, θα μπορούσε να έχει στόχο την μετάδοση δεδομένων σε πραγματικό χρόνο για την θερμοκρασία, την πίεση και την ροή του ρευστού στον αγωγό καθώς και την συγκέντρωση και οργάνωση αυτών των δεδομένων για χρήση από άλλες εφαρμογές. Επίσης, αν υπάρχουν σφάλματα διαρροών στον αγωγό θα μπορούν να ανιχνεύονται και να ενεργοποιούνται κατάλληλοι συναγερμοί. Στα θέματα που αφορούν έναν αγωγό πετρελαίου, δεν είναι μόνο η επιλογή ενός κατάλληλου συστήματος αυτοματισμού, αλλά και τα γεωγραφικά περιβάλλοντα, όπως και οι πολιτικές συμφωνίες του κάθε κράτους για τη χρήση ενός αγωγού. Έτσι ένα σύστημα αγωγού πετρελαίου θα πρέπει να έχει και άλλα τεχνικά συστήματα υποστήριξης όπως είναι συστήματα ηλεκτροδότησης, συστήματα ελέγχου, συστήματα οργάνων μέτρησης, δίκτυο κορμού επικοινωνιών, δορυφορική παρακολούθηση, δίκτυο υπολογιστών, σύστημα διαχείρισης πόρων, σύστημα ανίχνευσης διαρροών, συντήρηση από απόσταση, πληροφόρηση σε πραγματικό χρόνο για σφάλματα και άλλα.

Ενδεικτικά αναφέρουμε μερικά συστήματα που χρειάζονται σε αγωγούς μεταφοράς πετρελαίου.

Σύστημα ελέγχου διεργασιών (Process Control System), PCS. Αυτό μπορεί να βασιστεί στο WirelessHART.

Σύστημα ασφαλείας οργάνων (Safety Instrumented System), SIS. Αυτό μπορεί επίσης να βασιστεί στο WirelessHART επειδή όλα τα όργανα μέτρησης παρέχουν αναφορές διαγνώσεων για την υγεία τους.

Ελεγκτές φωτιάς και αερίων (fire & gas) για την παρακολούθηση της πυρκαγιάς και της διαρροής επικίνδυνων αερίων. Στο WirelessHART, με χρήση κατάλληλων αισθητήρων θερμοκρασίας και ανίχνευσης αερίων θα μπορούσαν να συγκεντρώνονται αυτές οι πληροφορίες. Αλλιώς, μπορούν να χρησιμοποιηθούν άλλα συστήματα παρόμοιου σκοπού.

Διακόπτες οπτικών ινών και πομποδέκτες χρησιμοποιούνται για να συνδεθεί το σύστημα σε άλλα δίκτυα. Και εδώ το WirelessHART μέσω της πύλης Gateway μπορεί να συνδέσει τα δίκτυα οργάνων μέτρησης σε άλλα δίκτυα.

6.2.6 Βιομηχανία με Πετροχημικά

Μια βιομηχανία με Πετροχημικά προϊόντα ασχολείται με τη δημιουργία και μεταφορά σε άλλες βιομηχανικές μονάδες του προϊόντατος PTA (καθαρό τερεφθαλικό οξύ) που είναι πρώτη ύλη για πλαστικά.

Σε μία τέτοια βιομηχανία υπάρχουν Βαλβίδες ελέγχου (control valves), positioners και οι έξυπνες βαλβίδες θέσης (valve position).

Στόχος είναι να υπάρχουν τα διαγνωστικά βαλβίδων σε πραγματικό χρόνο, ώστε να μην κλείνει η εγκατάσταση αλλά να απομονώνονται μόνο λίγες βαλβίδες και τα υπόλοιπα μέρη να λειτουργούν κανονικά, σε μία διακοπή λειτουργίας της εγκατάστασης. Ο χρόνος διακοπής λειτουργίας της εγκατάστασης ονομάζεται downtime και έχει σημαντικό κόστος. Για αυτό οι τεχνικοί προσπαθούν να περιορίζουν το τμήμα της εγκατάστασης που διακόπτει τη λειτουργία του, όσο το δυνατόν πιο κοντά στο σημείο της βλάβης, ενώ η υπόλοιπη εγκατάσταση να λειτουργεί ομαλά.

Πρίν την εφαρμογή του HART δεν υπήρχαν επαρκή διαγνωστικά για τις βαλβίδες και για τη θέση τους σε πραγματικό χρόνο, ώστε οι τεχνικοί δεν μπορούσαν να απομονώσουν

μόνο όσες βαλβίδες ήθελαν συντήρηση. Έτσι απομόνωναν μεγάλα τμήματα. Με την εισαγωγή του HART όμως, υπήρχαν τα διαγνωστικά των βαλβίδων σε πραγματικό χρόνο, οπότε γνώριζαν ποιες βαλβίδες παρουσίαζαν σφάλμα.

Το WirelessHART θα μπορούσε να χρησιμοποιηθεί στην επέκταση ενός τέτοιου συστήματος ώστε να συμπεριληφθούν περισσότερες βαλβίδες και να συνδεθούν μέσω WirelessHART χωρίς καλώδια για να παρέχουν διαγνώσεις των συσκευών σε πραγματικό χρόνο.

6.2.7 Βιομηχανία Κατασκευής Υαλικών και Πιάτων

Σε μία βιομηχανία κατασκευής υαλικών και πιάτων χρησιμοποιούνται βαλβίδες, και Positioners, π.χ. σε πραγματικό σενάριο υπάρχουν 64 Βαλβίδες με ελεγχόμενη θέση. Έτσι το σύστημα περιλαμβάνει πολλές μεταβλητές που περιγράφουν τις θέσεις των βαλβίδων.

Για τη διαχείριση των βαλβίδων συνολικά, χρειάζονται οι πληροφορίες για την κατάσταση και τη θέση των βαλβίδων σε πραγματικό χρόνο, και η μεταφορά των πληροφοριών σε ένα κεντρικό σημείο ελέγχου μέσω δικτύου. Έτσι όταν υπάρχουν συγκεντρωμένες οι πληροφορίες στο κέντρο ελέγχου, μπορεί να γίνεται απομακρυσμένη ρύθμιση της θέσης των βαλβίδων με εντολές που δίνονται από το κέντρο ελέγχου.

Το δίκτυο WirelessHART θα μπορούσε να χρησιμοποιηθεί και σε αυτή την περίπτωση, για να παρέχει διαγνώσεις σε πραγματικό χρόνο για την κατάσταση και τη θέση των βαλβίδων που μέσω της πύλης Gateway μπορούν να συγκεντρωθούν σε ένα κεντρικό σύστημα ελέγχου.

6.2.8 Βιομηχανία δημιουργίας αντιοξειδωτικών υλικών και πρόσθετων υλικών που χρησιμοποιούνται στην παραγωγή πλαστικών

Σε μία χημική βιομηχανία που κατασκευάζονται κάποια υλικά για χρήση στην κατασκευή πλαστικών, υπάρχουν πολλές συσκευές πεδίου, εγκατεστημένες σε

επικίνδυνες περιοχές με χημικά. Αυτές οι συσκευές μετά από κάποιο χρόνο λειτουργίας, πρέπει να ξαναρυθμίζονται κάθε φορά, λόγω της επίδρασης που ασκεί σε αυτές το περιβάλλον χημικών ουσιών.

Απαιτούνται ρυθμίσεις των συσκευών πεδίου εκ νέου μετά από κάθε παραγωγή, ώστε να προσαρμοστούν σε μία νέα παρτίδα παραγωγής.

Στόχος είναι η κεντρική παρακολούθηση διαγνώσεων των συσκευών πεδίου σε πραγματικό χρόνο και η μεταφορά των δεδομένων από τις συσκευές σε ένα κεντρικό σημείο μακριά από τις επικίνδυνες περιοχές με τα χημικά.

Τα δεδομένα που συγκεντρώνονται είναι οι τιμές από μετρήσεις διεργασιών και οι πληροφορίες ρυθμίσεων.

Το WirelessHART θα μπορούσε να χρησιμοποιηθεί με το σύστημα διαγνώσεων σε πραγματικό χρόνο για να μεταφέρει δεδομένα από τις συσκευές σε ένα κεντρικό σημείο ελέγχου.

6.2.9 Βιομηχανία επεξεργασίας και μεταφοράς με αγωγούς νερού και λυμάτων

Μία βιομηχανία επεξεργασίας λυμάτων, πριν να εισάγει το HART, είχε τα παλιότερα παραδοσιακά όργανα μετρήσεων, όπως μαγνητικά ροόμετρα, venture, μετρητές ροής νερού ή αέρα. Η καταγραφή μετρήσεων και ενδείξεων γινόταν με το χέρι σε χαρτιά.

Στη βιομηχανία αυτή υπήρχαν πολλές βαλβίδες και επενεργητές.

Μετά από την εισαγωγή του HART, αντικαταστάθηκαν τα παλαιότερα όργανα με τα όργανα HART και χρησιμοποιήθηκαν 750 έξυπνα όργανα μέτρησης πίεσης και ροής σε υπόγειες εγκαταστάσεις αγωγών μεταφοράς νερού.

Το πλεονέκτημα ήταν η μεταφορά δεδομένων μετρήσεων σε πραγματικό χρόνο, από τα σημεία που είναι τοποθετημένοι οι μετρητές προς τα σημεία πώλησης.

Με αυτό τον τρόπο, είναι εφικτό να υπολογίζεται η χρήση ποσοτήτων του νερού που διέρχεται από τους αγωγούς, ώστε να καθορίζεται ένας λογαριασμός χρεώσεων για την πώληση του νερού στους πελάτες χονδρικής πώλησης. Με την εισαγωγή του WirelessHART, τα ήδη υπάρχοντα συστήματα μπορούν να λειτουργούν στο ασύρματο

δίκτυο WirelessHART. Αν χρειαστεί να γίνουν επεκτάσεις, θα είναι πιο εύκολο να προστεθούν νέα όργανα μέτρησης χωρίς καλώδια. Η επέκταση θα είναι πιο εύκολη και έτσι η καταγραφή της ροής του νερού μπορεί να επιτευχθεί με έναν πιο αποτελεσματικό τρόπο χωρίς καθυστερήσεις.

6.2.10 Βιομηχανία επεξεργασίας ξυλείας, αγωγός που μεταφέρει πριονίδι

Σε μία βιομηχανία επεξεργασίας ξυλείας, το πριονίδι που παράγεται από τα επεξεργασμένα ξύλα, περνάει μέσα από ένα σύστημα αγωγών εξαερισμού και τελικά συγκεντρώνεται μέσα σε μία δεξαμενή. Αυτό γίνεται, με στόχο η ατμόσφαιρα στο περιβάλλον της βιομηχανίας, να μην γεμίζει από τη σκόνη πριονιδιού, ώστε όλοι όσοι βρίσκονται και εργάζονται μέσα σε εκείνο το χώρο, να μην εισπνεύσουν αυτή τη σκόνη και να μην δημιουργηθούν προβλήματα στην υγεία τους. Επιπλέον, το πριονίδι που συγκεντρώνεται στη δεξαμενή, μπορεί να αποθηκευθεί και να χρησιμοποιηθεί μελλοντικά ως μία καύσιμη ύλη ή για άλλους σκοπούς όπως, πχ, υλικό συσκευασίας εύθραυστων αντικειμένων. Για τη μεταφορά του πριονιδιού μέσα στον αγωγό, τίθενται σε λειτουργία διάφοροι ανεμιστήρες που δημιουργούν μία ροή αέρα μέσα στον αγωγό. Αν όμως η στάθμη το πριονιδιού μέσα στη δεξαμενή αυξηθεί αρκετά, τότε θα πρέπει να σταματήσουν για ένα διάστημα οι κινητήρες και να αδειάσει η δεξαμενή για να μην φράξει το πριονίδι τους αγωγούς ή να μην συγκεντρωθεί μεγάλη ποσότητα πριονιδιού σε έναν κινητήρα, και δημιουργηθούν προβλήματα ροής στο σύστημα εξαερισμού.

Σε ένα τέτοιο σύστημα, χρειάζονται πληροφορίες σε πραγματικό χρόνο για την ροή των αγωγών σε πριονίδι, τη στάθμη της δεξαμενής και άλλες παραμέτρους. Η στάθμη του πριονιδιού στη δεξαμενή και στους αγωγούς θα μπορούσε να ελέγχεται διαρκώς ώστε όταν υπερβεί κάποιο όριο, να αδειάζει η δεξαμενή, και το πριονίδι να τοποθετείται σε κάποιο σημείο για τη μεταφορά του και την αποθήκευσή του σε άλλους χώρους. Άλλος έλεγχος που μπορεί να γίνει είναι η εκκίνηση κινητήρων στους αγωγούς να γίνεται με μία συγκεκριμένη σειρά. Έτσι πρέπει να διασφαλίζεται ότι δεν θα εκκινεί ένας κινητήρας ανεμιστήρα που στέλνει πριονίδι, όταν υπάρχει ήδη πριονίδι μέσα στον αγωγό όταν είναι σταματημένος κάποιος άλλος κινητήρας που εξάγει το πριονίδι από τον αγωγό.

Ένα δίκτυο WirelessHART θα μπορούσε να χρησιμοποιηθεί για να συλλέγει τα δεδομένα της στάθμης της δεξαμενής πριονιδιού. Επίσης μπορεί να συλλέγει δεδομένα από την

πίεση και τη ροή πριονιδιού στους αγωγούς μεταφοράς και να δίνει πληροφορίες στο κέντρο ελέγχου όταν υπάρχουν σφάλματα ή όταν οι αγωγοί παρουσιάσουν φθορές και παρατηρηθούν αλλαγές στην πίεση και στη ροή.

Βιβλιογραφία

- [1] K. Sohrabi, D. Minoli και T. Znati, «Medium Access Control Protocols for Wireless Sensor Networks,» σε *Wireless Sensor Networks Technology, Protocols, and Applications*, New Jersey, John Wiley & Sons Inc., 2007, pp. 142-191.
- [2] Zheng, Jun; Jamalipour, Abbas; IEEE, «Medium Access Control,» σε *Wireless Sensor Networks A Networking Perspective*, New Jersey, John Wiley & Sons, Inc., 2009, pp. 35-61.
- [3] J. F. Kazienko, I. G. Ribeiro, I. M. Moraes και C. V. Albuquerque, «Practical Evaluation of a Secure Key-Distribution and Storage Scheme for Wireless Sensor Networks Using TinyOS,» *CLEI ELECTRONIC JOURNAL*, τόμ. 14, αρ. 1, April 2011.
- [4] W. Dargie και C. Poellabauer, *Fundamentals Of Wireless Sensor Networks Theory And Practice*, John Wiley & Sons Ltd, 2010.
- [5] M. O. Farooq και T. Kunz, «Operating Systems for Wireless Sensor Networks: A Survey,» *Sensors*, τόμ. 11, αρ. 6, pp. 5900-5930, 31 May 2011.
- [6] C. H. Ganan, «Energy Management Architecture for Wireless Sensor Networks,» Koninklijke Philips Electronics N.V., 2008.
- [7] A. Asperheim, S. F. Kaja and . S. V. Rune, "Design and Implementation of a Rudimentary WirelessHART Network," UNIVERSITY OF OSLO Department of Informatics, OSLO, 2012.
- [8] D. Chen, M. Nixon and A. Mok, *WirelessHART™ Real-Time Mesh Network for Industrial Automation*, 1 ed., New York; Dordrecht ;Heidelberg; London;: Springer US, 2010, pp. XXII, 276.
- [9] S. Basagni, A. Carossi και C. Petrioti, «Mobility in Wireless Sensor Networks,» σε *Algorithms And Protocols For Wireless Sensor Networks*, New Jersey, Ottawa, John Wiley & Sons, Inc, 2009, pp. 267-306.
- [10] I. Howitt και J. A. Gutierrez, «IEEE 802.15.4 Low Rate –Wireless Personal Area Network Coexistence Issues,» σε *Wireless Communications and Networking, 2003. WCNC 2003*, New Orleans, LA, 2003.
- [11] ATMEL, «IEEE 802.15.4 MAC User Guide,» ATMEL Corporation, San Jose, 2006.

- [12] S. Pollin , M. Ergen, L. V. d. Perre, L. Van der Perre, I. Moerman, A. Bahai και et.al., «Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer,» *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, τόμ. 7, αρ. 9, pp. 3359 - 3371, 19 September 2008.
- [13] NXP Laboratories UK, «IEEE 802.15.4 Stack User Guide,» NXP Laboratories UK, 2015.
- [14] J. Zheng και M. J. Lee, «A Comprehensive Performance Study of IEEE 802.15.4,» *Sensor Network Operations*, pp. 218-237, 2006.
- [15] D. J. Vergados, A. Sgora, D. D. Vergados, D. Vouyioukas και I. Anagnostopoulos, «Fair TDMA scheduling in wireless multihop networks,» *Telecommunication Systems*, τόμ. 50, αρ. 3, pp. 181-198, July 2012.
- [16] J. Tourrilhes, «Wireless LAN resources for Linux (5 The MAC Level),» Ιούλιος 2007. [Ηλεκτρονικό]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.mac.html. [Πρόσβαση 19 Αύγουστος 2015].
- [17] O. Khader, A. Willig και A. Wolisz, «WirelessHART TDMA Protocol Performance,» σε *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*, Barcelona, 2011.
- [18] S. Li, H. Wang, A. Xu και S. H. Hong, «Study of Time-sync for WirelessHART Networks,» *Information Technology Journal*, τόμ. 12, αρ. 23, pp. 7809-7814, 2013.
- [19] HART Communication Foundation, «HART COMMUNICATION PROTOCOL,» [Ηλεκτρονικό]. Available: <http://en.hartcomm.org/>. [Πρόσβαση 30 03 2015].
- [20] A. N. Kim, F. Hekland, S. Petersen και D. Paula, «When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard,» σε *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*, Hamburg, 2008.
- [21] www.pactrol.com, «hart protocol,» PAControl.com, 1999. [Ηλεκτρονικό]. Available: <http://www.pactrol.com/download/hart-protocol.pdf>. [Πρόσβαση 24 04 2014].
- [22] PEPPERL & FUCHS, «Access To Process Devices With HART Intrerface Solutions,» [Ηλεκτρονικό]. Available: http://files.pepperl-fuchs.com/selector_files/navi/productInfo/doct/tdoct0683d_eng.pdf.
- [23] HART Communication Foundation, "How HART Works," [Online]. Available: http://en.hartcomm.org/hcp/tech/aboutprotocol/aboutprotocol_how.html. [Accessed 25 04 2015].
- [24] V. S. Soto, I. Muller, J. M. Winter, C. E. Pereira και J. C. Netto, «Control over WirelessHART Network through a Host Application,» σε *Computing Systems Engineering (SBESC) Brazilian Symposium on*, Manaus, 2014.
- [25] Fuji Electric Instrumentation & Control, «Coulton.com,» [Ηλεκτρονικό]. Available: http://www.coulton.com/beginners_guide_to_differential_pressure_transmitters.html. [Πρόσβαση 4 May 2015].

- [26] I. Konovalov, «A Framework for WirelessHART Simulations,» SICS Tech. Rep. T2010:06 (1-39), Kista, 2010.
- [27] T. O'Donovan, J. Brown, U. Roedig, V. Vassiliou, C. J. Sreenan, J. doO, A. Dunkels, A. Klein, j. Sa Silva και L. Wolf, «GINSENG: Performance Control in Wireless Sensor Networks,» σε *Real-World Wireless Sensor Networks*, τόμ. 6511, Springer Berlin Heidelberg, 2010, pp. 166-169.
- [28] J. Brown, B. McCarthy, U. Roedig, T. Voigt και C. J. Sreenan, «Burstprobe: Debugging time-critical data delivery in wireless sensor networks.,» σε *Wireless Sensor Networks*, Berlin , Springer Berlin Heidelberg, 2011, pp. 195-210.
- [29] K. A. A. Somappa, M. L. Kristensen και K. Ovsthus, «A formal executable specification of the GinMAC protocol for Wireless Sensor Actuator Networks,» σε *Wireless and Pervasive Computing (ISWPC), 2013 International Symposium on*, Taipei, 2013.
- [30] Nixon, Mark; Emerson, *A comparison of WirelessHART and ISA100.11a*, TX,USA, 2012.
- [31] S. Petersen και S. Carlsen, «WirelessHART Versus ISA100.11a,» *Industrial Electronics Magazine, IEEE*, τόμ. 5, αρ. 4, pp. 23-34, 15 December 2011.
- [32] ARC Advisory Group, «Yokogawa's Wireless Solutions Show a Long- Term Commitment to ISA100 Standard,» February 2011. [Ηλεκτρονικό]. Available: <http://www.yokogawa.com/us/technical-library/white-papers/yokogawas-wireless-solutions-show-a-long-term-commitment-to-isa100-standard.htm>. [Πρόσβαση 21 Αύγουστος 2015].
- [33] G. Johnson, «Industrial wireless networks — comparing the standards: Part 2,» *Whats New in Process Technology (WNIPT)*, 13 July 2015.
- [34] Nivis wireless sensor networks, «ISA100.11a Technology Standard,» [Ηλεκτρονικό]. Available: <http://www.nivis.com/technology/ISA100.11a.php>. [Πρόσβαση 22 August 2015].
- [35] E. Ekici, Y. Gu και D. Bozdag, «Mobility-Based Communication in Wireless Sensor Networks,» *IEEE Communications Magazine*, τόμ. 44, αρ. 7, pp. 56-62, 14 August 2006.
- [36] S. Basagni, A. Carosi, E. Melachrinoudis, C. Petrioli και M. Z. Wang, «Controlled sink mobility for prolonging wireless sensor networks lifetime,» *Wireless Networks*, τόμ. 14, αρ. 6, pp. 831-858, 7 February 2007.
- [37] A. A. Taleb, T. Alhmiedat, O. A.-h. Hassan και N. M. Turab, «A Survey of Sink Mobility Models for Wireless Sensor Networks,» *Journal of Emerging Trends in Computing and Information Sciences*, τόμ. 4, αρ. 9, pp. 679-687, September 2013.
- [38] S. Basagni, A. Carosi και C. Petrioli, «Mobility in Wireless Sensor Networks,» σε *Algorithms And Protocols For Wireless Sensor Networks*, IEEE, Επιμ., Ottawa, John Wiley & Sons, Inc., 2008, pp. 267-301.

- [39] J. Rezazadeh, M. Moradi και S. A. Ismail, «Mobile Wireless Sensor Networks Overview,» *IJCCN International Journal of Computer Communications and Networks*, τόμ. 2, αρ. 1, pp. 17-22, February 2012.
- [40] M. Atto και C. Guy, «Wireless Sensor Networks: MAC Protocols and Real Time Applications,» Liverpool, 2012.
- [41] Q. Dong, W. Dargie και M. Lu, «Effects of Mobility on Latency in a WSN that Accommodates Mobile Nodes».
- [42] M. R. Ahmad, E. Dutkiewicz και X. Huang, «A Survey of Low Duty Cycle MAC Protocols in Wireless Sensor Networks,» σε *Emerging Communications for Wireless Sensor Networks*, Shangai, inTech, 2011, pp. 69-90.
- [43] H. Pham και S. Jha, «Addressing Mobility in Wireless Sensor Media Access Protocol,» σε *Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004. Proceedings of the 2004*, 2004.
- [44] S. Montero, J. Gozálvez, U. Sepúlcre και G. Prieto, «Impact of mobility on the management and performance of WirelessHART industrial communications,» σε *Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on*, Krakow, 2012.

Περισσότερες Πηγές

- [45] A. Dunkels, G. Bjorn και T. Voigt, «Contiki-a Lightweight and Flexible Operating System for Tiny Networked Sensors,» σε *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, 2004.
- [46] M. Nobre, I. Silva και A. Guedes, «Performance Evaluation of WirelessHART networks using a new network simulator 3 module,» *Computers and Electrical Engineering*, 2014.
- [47] S. K. Singh, M. P. Singh και D. K. Singh, «Routing Protocols in Wireless Sensor Networks-A Survey,» *International Journal of Computer Science & Engineering Survey (IJCSSES)*, τόμ. 1, αρ. 2, pp. 63-83, November 2010.
- [48] M. A. Labrador και P. M. Wightman, *Topology Control in Wireless Sensor Networks*, Tampa, South Florida: Springer, 2009.
- [49] N. Bulusu και S. Jha, *Wireless Sensor Networks*, London: Artech House, 2005.
- [50] H. Karl και A. Willig, *Protocols And Architectures For Wireless Sensor Networks*, John Wiley & Sons Ltd., 2005.

- [51] P. Santi, *Topology Control in Wireless Ad Hoc and Sensor Networks*, John Wiley & Sons Ltd., 2005.
- [52] R. Shorey, A. Anada, M. C. Chan και W. T. Ooi, *Mobile, Wireless, and Sensor Networks, Technology, Applications, and Future Directions*, P. IEEE, Επιμ., New Jersey: John Wiley & Sons, Inc., 2006.
- [53] P. Zand, E. Mathews, P. Havinga, S. Stojanovski, E. Sisinni και P. Ferrari, «Implementation of WirelessHART in the NS-2 Simulator and Validation of Its Correctness,» *Sensors*, τόμ. 14, pp. 8633-8668, 16 May 2014.
- [54] I. Konovalov, «A Framework for WirelessHART Simulations,» Kista, 2010.
- [55] P. Ferrari, A. Flammini, D. Marioli, S. Rinaldi και E. Sisinni, «On the Implementation and Performance Assessment of a WirelessHART Distributed Packet Analyzer,» *IEEE Transactions On Instrumentation And Measurement*, τόμ. 50, αρ. 5, 5 May 2010.
- [56] D. Roth, J. Montavont και T. Noel, «MOBINET: Mobility Management Across Different Wireless Sensor Networks,» σε *Wireless Communications and Networking Conference (WCNC)*, 2011 IEEE, Cancun, Quintana Roo, 2011.
- [57] S. Han, Z. Xiuming, A. K. Mok, M. Nixon, T. Blevins και D. Chen, «Control Over WirelessHART Network,» IEEE, 2010.
- [58] I. Muller, J. C. Netto και C. E. Pereira, «WirelessHART Field Devices,» *IEEE Instrumentation & Measurement Magazine*, pp. 20-25, December 2011.
- [59] P. Ferrari, A. Flammini, S. Rinaldi και E. Sisinni, «Performance Assesment of a WirelessHART network in real-world testbed,» IEEE, 2012.
- [60] J. Mao, Z. Wu και X. Wu, «A TDMA scheduling scheme for many-to-one communications in wireless sensor networks,» *Computer Communications*, αρ. 30, pp. 863-872, 15 November 2006.
- [61] P. Ferrari, A. Flammini, M. Rizzi και E. Sisinni, «Improving simulation of wireless networked control systems based on WirelessHART,» *Computer Standards & Interfaces*, τόμ. 35, pp. 605-615, 13 April 2013.
- [62] S. Gandham, Y. Zhang και Q. Huang, «Distributed time-optimal scheduling for convergecast in wireless sensor networks,» *Computer Networks*, τόμ. 52, pp. 610-629, 7 November 2007.
- [63] T. Rault, A. Bouabdallah και Y. Challal, «Energy efficiency in wireless sensor networks: A top-down survey,» *Computer Networks*, τόμ. 67, 5 April 2014.
- [64] M. Kohvakka, J. Suhonen, M. Kuorilehto, V. Kaseva, M. Hannikainen και T. D. Hamalainen, «Energy-efficient neighbor discovery protocol for mobile wireless sensor networks,» *Ad Hoc Networks*, τόμ. 7, pp. 24-41, 15 December 2007.

- [65] K. R. Chowdhury, N. Nandiraju, P. Chanda, D. P. Agrawal και Q. A. Zeng, «Channel allocation and medium access protocol for wireless sensor networks,» *Ad Hoc Networks*, αρ. 7, pp. 307-321, 11 April 2008.
- [66] D. Yang, M. Gidlund, W. Shen, Y. Xu, T. Zhang και H. Zhang, «CCA-Embedded TDMA enabling acyclic traffic in industrial wireless sensor networks,» *Ad Hoc Networks*, τόμ. 11, pp. 1105-1121, 23 December 2012.
- [23] Daniel Measurement and Control Inc., «HART Field Device Specification Guide,» Emerson, Houston, 2011.
- [67] S. I. Amiri, A. Shahidinejad, A. Nikoukar, J. Ranijbar, J. Ali και P. P. Yupapin, «Digital Binary Codes Transmission via TDMA Networks Communication System Using Dark and Bright Optical Soliton,» *GSTF Journal of Computing (JoC)*, τόμ. 2, αρ. 1, April 2012.
- [68] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, P. Varaiya και F. Catthoor, «Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer,» *IEEE Transactions on Wireless Communications*, τόμ. 7, αρ. 9, pp. 3359-3371, September 2008.
- [69] L. Ma, Leung Henry και D. Li, «Hybrid TDMA/CDMA MAC Protocol for Wireless Sensor Networks,» *Journal of Networks*, τόμ. 9, αρ. 10, pp. 2665-2673, October 2014.
- [70] S. Han, Y. H. Wei, A. K. Mok, D. Chen, M. Nixon και E. Rotvold, «Building Wireless Embedded Internet for Industrial Automation,» IEEE, 2013.
- [71] R. Zhang, X. Cheng, L. Yang, X. Shen και B. Jiao, «A Novel Centralized TDMA-Based Scheduling Protocol for Vehicular Networks,» *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, τόμ. 16, αρ. 1, pp. 411-416, February 2015.
- [72] T. Kelter, H. Falk, P. Marwedel, S. Chattopadhyay και A. Roychoudhury, «Static Analysis of Multi-Core TDMA Resource Arbitration,» *Springer Real-Time Systems*, pp. 1-38, 8 July 2013.
- [73] M. K. Marina, S. R. Das και A. P. Subramanian, «A topology control approach for utilizing multiple channels in multi-radio wireless mesh networks,» *Computer Networks*, τόμ. 54, pp. 241-256, 5 August 2009.
- [74] ARC Advisory Group, «Yokogawa's Wireless Solutions Show a Long-Term Commitment to ISA100 Standard,» Arc Advisory Group, 2011.
- [75] K. Dang, J. Z. Shen, L. D. Dong και Y. X. Xia, «A Graph Route-Based Superframe Scheduling Scheme in WirelesHART mesh networks for High Robustness,» *Wireless Personal Communications*, τόμ. 71, pp. 2431-2444, 5 December 2012.
- [76] D. Chen, M. Nixon, H. Song, A. K. Mok και Z. Xiuming, «WirelessHART and IEEE 802.15.4e,» σε *Industrial Technology (ICIT), 2013 IEEE International Conference on*, 2014.

- [77] softing : Krohn, ALbert; Hilz, Thomas; Suss, Georg;, «WirelessHART in Practice: Saving Power with Proper Network ans Field Device Configuration,» [Ηλεκτρονικό]. Available: industrial.softing.com.
- [78] P. Radmand, A. Talevski, S. Petersen και S. Carlsen, «Comparison of Industrial WSN Standards,» σε *4th IEEE International Confernece on Digital Ecosystems and Technologies (IEEE DEST 2010)*, 2010.
- [79] P. Zand, A. Dilo και P. Havinga, «D-MSR: A Distributed Network Management Scheme for Real Time Monitoring and Process Control Applications in Wireless Industrial Automation,» *Sensors*, τόμ. 13, 27 June 2013.
- [80] A. Saifullah, Y. Xu, C. Lu and Y. Chen, "Priority Assingnment for Real-Time Flows in WirelessHART Networks," in *Real-Time Systems (ECRTS),2011 23rd Euromicro Conference On*, Porto, 2011.
- [81] L. Tang, S. Yajun, O. Gurewitz and D. Johnson, "EM-MAC: A Dynamic Multichannel Energy-Efficient MAC," in *MobiHoc 2011*, France, 2011.
- [82] W. Ye, J. Heidemann and D. ESTRIN, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *Wireless Sensor Network*, vol. 1, pp. 1-69, June 2008.
- [83] S. Raza, T. Voigt, A. Slabbert and K. Landernas, "Design and implementation of a Security Manager for WirelessHART networks," in *Mobile Adhoc and Sensor Systems, 2009. MASS 09. IEEE 6th International Conference on*, Macau, 2009.
- [84] A. Hoiydi, "Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks," in *Computers and Communications, 2002. Proceedings.ISCC 2002.Seventh International Symposium on*, Neuhatel, 2002.
- [85] Schmidt, Garret; Phoenix Contact, "Getting the Most Out of your WirelessHART System," 2010. [Online]. Available: www.phoenixcontact.com.
- [86] S. e. Yoo, P. k. Chong, D. Kim, Y. Doh, M. L. Pham, E. Choi and J. Huh, "Guaranteeing Real-Time Services for Industrial Wireless Sensor Networks With IEEE 802.15.4," *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, vol. 57, no. 11, pp. 3868-3876, November 2010.
- [87] D. Gustafsson, *WirelessHART-Implementation and Evaluation on Wireless Sensors*, Stockholm: KTH Electrical Engineering, 2009.
- [88] M. Holland, T. Wang, B. Tavli, A. Seyedli and W. Heinzelman, "Optimizing Physical Layer Parameters for Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 7, no. 4, February 2011.
- [89] H. Shan, H. T. Cheng and W. Zhuang, "Cross-Layer Cooperative MAC Protocol in Distributed Wireless Networks," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 8, pp. 2603-2615, 18 August 2011.

- [90] P. K. Pal and P. Chatterjee, "A Survey on TDMA-based MAC Protocols for Wireless Sensor Network," *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 6, pp. 219-230, June 2014.
- [91] V. Sevani, B. Raman and P. Joshi, "Implementation Based Evaluation of a Full-Fledged Multi-Hop TDMA-MAC for WiFi Mesh Networks," *Mobile Computing, IEEE Transactions on*, vol. 13, no. 2, pp. 392-406, 19 December 2013.
- [92] Control Global Staff, "WirelessHART Takes Off," *CONTROL*, 12 September 2012.
- [93] S. Raza and T. Voigt, "Interconnecting WirelessHART and Legacy HART Networks," in *Distributed Computing in Sensor Systems Workshops, 2010 6th IEEE International Conference on*, Santa Barbara, 2010.
- [94] A. Richa, C. Scheideler, S. Schmid and J. Zhang, "A Jamming-Resistant MAC Protocol for Multi-Hop Wireless Networks," in *Distributed Computing*, Springer Berlin Heidelberg, 2010, pp. 179-193.
- [95] K. Kunert, "TDMA-based MAC Protocols for Wireless Sensor Networks: State of the Art and Important Research Issues," 2005.
- [96] G. Lu, K. Bhaskar and C. S. Raghavendra, "Performance Evaluation of the IEEE 802.15.4 MAC for Low-Rate Low-Power Wireless Networks," in *Performance, Computing, and Communications, 2004 IEEE International Conference on*, 2004.
- [97] P. Hurni and T. Braun, "MaxMAC: a Maximally Traffic-Adaptive MAC Protocol for Wireless Sensor Networks," in *Wireless Sensor Networks*, Springer Berlin Heidelberg, 2010, pp. 289-305.
- [98] O. D. Incel, L. van Hoesel, P. Jansen and P. Havinga, "MC-LMAC: A Multi-Channel MAC Protocol for Wireless Sensor Networks," *Ad Hoc Networks*, vol. 9, no. 1, pp. 73-94, January 2011.
- [99] I. Rhee, A. Warriar, M. Aia, M. Jeongki and M. Sichitiu, "Z-MAC: A Hybrid MAC for Wireless Sensor Networks," *IEEE/ACM TRANSACTIONS ON NETWORKING*, vol. 16, no. 3, pp. 511-524, 13 June 2008.
- [100] X. Mao, S. Liu, L. Zhang and V. O. Li, *Energy-Delay Region of Low Duty Cycle Wireless Sensor Networks for Critical Data Collection*, 2014.
- [101] S. Hulyalkar, C. Ngo and Y. Du, "Medium access control (MAC) protocol for wireless ATM". USA Patent US6198728 B1 , 6 March 2001.
- [102] S. Petersen and S. Carlsen, "Performance Evaluation of WirelessHART for Factory Automation," in *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, Mallorca, 2009.

- [103] S. Petersen, P. Doyle, S. Vatland, C. S. Aasland, T. M. Andersen and D. Sjong, "Requirements, drivers and analysis of wireless sensor network solutions for the Oil & Gas industry," in *Emerging Technologies and Factory Automation, 2007.ETFA. IEEE Conference on*, Patras, 2007.
- [104] W. Shen, T. Zhang, F. Barac and M. Gidlund, "PriorityMAC: A Priority-Enhanced MAC Protocol for Critical Traffic in Industrial Wireless Sensor and Actuator Networks," *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 1, pp. 824-835, 12 December 2013.
- [105] J. Blanckenstein, J. G. Jimenez, J. Klaue and H. Karl, "A Scalable Redundant TDMA Protocol for High-Density WSNs Inside an Aircraft," in *Real-World Wireless Sensor Networks*, Como, Springer International Publishing, 2013, pp. 165-177.
- [106] I. Silva, L. A. Guedes, P. Portugal and F. Vasques, "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," *Sensors*, pp. 806-838, 10 January 2012.
- [107] X. Zhu, P. C. Huang, S. Han, A. K. Mok, D. Chen και M. Nixon, «RoamingHART: A Collaborative Localization System on WirelessHART,» 2012.
- [108] A. Saifullah, Y. Xu, C. Lu και Y. Chen, «Real-Time Scheduling for WirelessHART Networks,» σε *Real-Time Systems Symposium (RTSS), 2010 IEEE 31st*, San Diego, 2010.
- [109] M. Nobre, I. Silva και L. A. Guedes, «Routing and Scheduling Algorithms for WirelessHART Networks: A Survey,» *Sensors*, τόμ. 15, pp. 9703-9740, 24 April 2015.
- [110] Q. Huang, A. Sikora, V. F. Groza και P. Zand, «Simulation & Analysis of WirelessHART Nodes for Real-Time Actuator Application,» σε *Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, 2014 IEEE International*, Montevideo, 2014.
- [111] P. Zand, «Decentralized management schemes for real-time and reliable communication in industrial wireless sensor and actuator networks,» Enschede, 2014.
- [112] J. H. Hauer, «TKN15.4: An IEEE 802.15.4 MAC Implementation for TinyOS 2,» Telecommunication Networks Group, Berlin, 2009.
- [113] Y. Tselishev, A. Boulis και L. Libman, «Experiences and Lessons from Implementing a Wireless Sensor Network MAC Protocol in the Castalia Simulator,» σε *Wireless Communications and Networking Conference (WCNC) 2010 IEEE*, Sydney, 2010.
- [114] N. Li και J. C. Hou, «Topology Control in Heterogeneous Wireless Networks: Problems and Solutions,» σε *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004.
- [115] H. Fujii, «DTM supporting a wide range of field instruments and field networks,» σε *SICE Annual Conference (SICE), 2012 Proceedings of*, Akita, 2012.

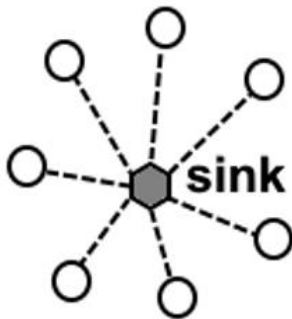
- [116] E. Toscano και L. Lo Bello, «A multichannel approach to avoid beacon collisions in IEEE 802.15.4 cluster-tree industrial networks,» σε Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on, Mallorca, 2009.
- [117] Z. Wang, F. Yu, J. Tian και Z. Zhang, «A fairness adaptive TDMA scheduling algorithm for wireless sensor networks with unreliable links,» International Journal of Communication Systems, τόμ. 27, αρ. 10, p. 1535–1552, 17 October 2014.
- [118] X. Wang, B. F. Raton, A. G. Marques και G. B. Giannakis, «Power-Efficient Resource Allocation and Quantization for TDMA Using Adaptive Transmission and Limited-Rate Feedback,» Signal Processing, IEEE Transactions on, τόμ. 56, αρ. 9, pp. 4470 - 4485, 12 August 2008.
- [119] S. Zhuo, Y.-Q. Song, Z. Wang και Z. Wang, «Queue-MAC: A queue-length aware hybrid CSMA/TDMA MAC protocol for providing dynamic adaptation to traffic and duty-cycle variation in wireless sensor networks,» σε Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on, Lemgo, 2012.
- [120] J. H. Sanchez, «WirelessHART Network Manager Software Design and Architecture,» KTH The Royal Institute of Technology, Stockholm, 2011.
- [121] T. Lennvall και F. Hekland, «A comparison of WirelessHART and ZigBee for industrial applications,» σε Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on, Dresden, 2008.
- [122] D. H. Chae, K. H. Han, K. H. Seo, W. D. Cho και S. S. An, «Power Saving Mobility Protocol for Sensor Network,» σε Software Technologies for Future Embedded and Ubiquitous Systems, 2004. Proceedings. Second IEEE Workshop on, 2004.
- [123] A. Osmani, M. Dehghan, H. Pourakbar και P. Emdadi, «Fuzzy-Based Movement-Assisted Sensor Deployment Method in Wireless Sensor Networks,» σε Computational Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference on, Indore, 2009.
- [124] A. Calhan και C. Ceken, «An adaptive neuro-fuzzy based vertical handoff decision algorithm for wireless heterogeneous networks,» σε Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on, Κωνσταντινούπολη, 2010.
- [125] Y. Li, Y. Pan και W. Ping, «Research and implementation of a mobility management mechanism for Wireless Sensor Networks based on IEEE 802.15.4,» σε Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011 IEEE International Conference on, Kunming, 2011.

Παράρτημα Α

Τοπολογίες Δικτύων

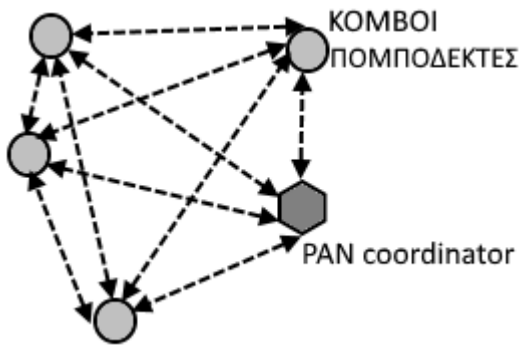
Σε αυτό το παράρτημα αναφέρονται συνοπτικά οι συνήθεις τοπολογίες δικτύων για τα ασύρματα δίκτυα αισθητήρων, καθώς και μορφές δρομολόγησης που χρησιμοποιούνται για την αποστολή σημάτων από τον κεντρικό κόμβο σε άλλους κόμβους του δικτύου.

A.1 Τοπολογία Αστέρα



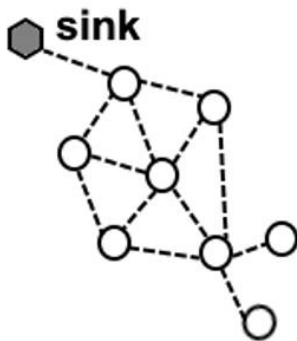
Στην τοπολογία αστέρα υπάρχει ένας κεντρικός κόμβος *sink* και οι τελικοί κόμβοι. Ο κεντρικός κόμβος *sink* συνδέεται με τους τελικούς κόμβους με απόσταση ενός άλματος (*one hop*). Οι τελικοί κόμβοι μπορούν να επικοινωνήσουν μόνο με τον κεντρικό κόμβο και όχι μεταξύ τους. Αν ένας τελικός κόμβος πρέπει να επικοινωνήσει με άλλο τελικό κόμβο, θα πρέπει πρώτα να στείλει το μήνυμά του στον κεντρικό κόμβο και μετά ο κεντρικός κόμβος να το προωθήσει στον τελικό κόμβο.

A.2 Τοπολογία *peer to peer*



Στην τοπολογία peer to peer (ομότιμοι κόμβοι), Ο κεντρικός κόμβος βρίσκεται σε ένα σημείο και συνδέεται με όλους τους τελικούς κόμβους με ένα άλμα (hop), όπως και ο αστέρας, αλλά υπάρχουν επιπλέον εναλλακτικές διαδρομές πολλαπλών αλμάτων (multi-hop), που συνδέουν όλους τους τελικούς κόμβους μεταξύ τους.

A.3 Τοπολογία Δικτύου Πλέγματος (Mesh)

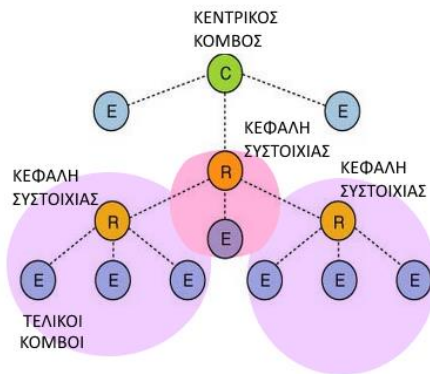


Η τοπολογία δικτύου πλέγματος (mesh network) μοιάζει με την τοπολογία peer to peer (ομότιμοι κόμβοι). Ο κεντρικός κόμβος sink βρίσκεται σε ένα σημείο και συνδέεται με όλους τους τελικούς κόμβους με διαδρομές πολλαπλών αλμάτων (multi-hop), οι οποίες συνδέουν τους τελικούς κόμβους μεταξύ τους. Η διαφορά από την τοπολογία peer to peer είναι ότι ο κεντρικός κόμβος sink δεν συνδέεται πάντοτε με όλους τους κόμβους με απόσταση ενός άλματος (single hop). Επιπλέον, ο κάθε τελικός κόμβος, δεν συνδέεται με όλους τους άλλους τελικούς κόμβους με απόσταση ενός άλματος, αλλά μόνο με κάποιους από αυτούς.

A.4 Τοπολογία Δέντρου Συστοιχιών

Η τοπολογία δέντρου ξεκινάει από έναν κεντρικό κόμβο root, ο οποίος έχει παιδιά, και τα παιδιά του έχουν άλλα παιδιά και έτσι σχηματίζεται ένα δέντρο με κλάδους που εκτείνεται σε ένα βάθος.

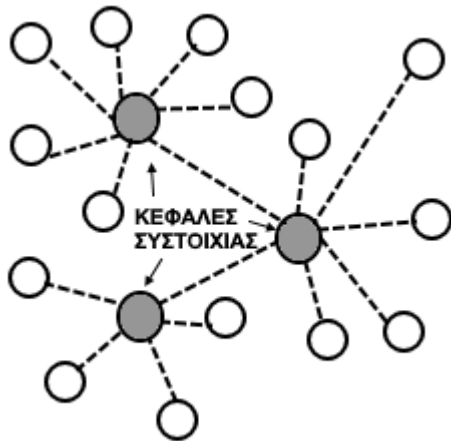
Οι κόμβοι έχουν μία ιεραρχία επιπέδων, δηλαδή κάθε κόμβος είναι παιδί άλλου κόμβου του προηγούμενου επιπέδου, γονέας άλλου κόμβου του επόμενου επιπέδου, ή φύλλο, δηλαδή κόμβος χωρίς παιδιά.



Η μορφή του δικτύου είναι ένα δέντρο όπου ο κεντρικός κόμβος sink είναι στην ρίζα (root) δηλαδή στην κορυφή. Μπορεί να θεωρηθεί και ως μία τοπολογία αστέρα με πολλούς κλάδους. Οι κλάδοι μπορούν να ομαδοποιηθούν σε συστοιχίες που περιέχουν ομάδες γονέων-παιδιών. Κάθε συστοιχία έχει έναν τοπικό κεντρικό κόμβο συστοιχίας που είναι η κεφαλή συστοιχίας. Για αυτό λέγεται δέντρο συστοιχιών (cluster tree). Σε κάθε συστοιχία δίνεται ένα μοναδικό αναγνωριστικό Cluster ID ώστε να ξεχωρίζει από τις άλλες συστοιχίες. Το δέντρο συστοιχιών είναι ειδική περίπτωση της τοπολογίας δέντρου.

A.5 Τοπολογία συστοιχιών με μορφή αστέρα

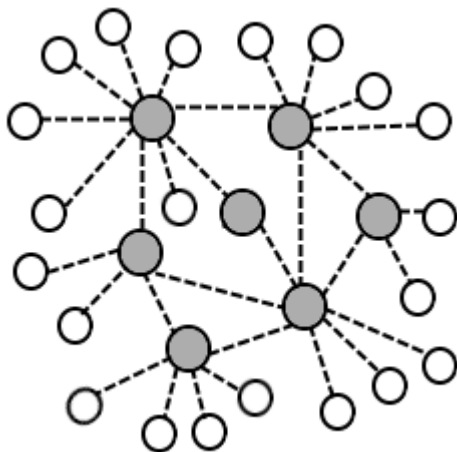
Είναι ένας συνδυασμός των συστοιχιών και του αστέρα και αποτελεί παραλλαγή της τοπολογίας δέντρου συστοιχιών.



Κάθε συστοιχία σχηματίζει τοπικά έναν αστέρα όπου στο κέντρο του αστέρα βρίσκεται μία κεφαλή συστοιχίας και συνδέεται με τους τελικούς κόμβους σε τοπολογία αστέρα. Η κάθε κεφαλή συστοιχίας συνδέεται μόνο με μία άλλη γειτονική κεφαλή συστοιχίας με απόσταση ενός άλματος (one hop).

A.6 Τοπολογία υβριδική αστέρα πλέγματος

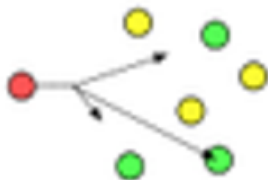
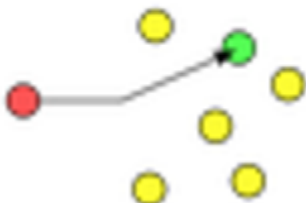
Η υβριδική τοπολογία αστέρα-πλέγματος, είναι ένας συνδυασμός του δικτύου πλέγματος και του αστέρα.



Στην υβριδική τοπολογία αστέρα-πλέγματος, υπάρχουν οι κεφαλές συστοιχίας και οι τελικοί κόμβοι. Κάθε κεφαλή συστοιχίας δημιουργεί τοπικά ένα δίκτυο με τους τελικούς κόμβους που συνδέονται σε αυτή σε τοπολογία αστέρα. Οι τελικοί κόμβοι δεν μπορούν να προωθούν μηνύματα, σε άλλους κόμβους, αλλά μόνο στη δική τους κεφαλή συστοιχίας. Κάθε τελικός κόμβος συνδέεται τοπικά με ένα άλμα (single hop) σε μία γειτονική του κεφαλή συστοιχίας, ώστε να

σχηματίζεται μία τοπολογία αστέρα για κάθε μία κεφαλή συστοιχίας. Όλες οι κεφαλές συστοιχίας συνδέονται μεταξύ τους με τοπολογία πλέγματος (mesh) ώστε μπορούν να στέλνουν δεδομένα η μία στην άλλη με διαδρομές πολλαπλών αλμάτων (multi hop). Με αυτή την τοπολογία το δίκτυο που δημιουργείται είναι ισχυρό και η κατανάλωση ενέργειας ελαχιστοποιείται για τους τελικούς κόμβους. Οι κεφαλές συστοιχίας μπορούν να προωθούν μηνύματα μέσω του δικτύου πλέγματος από τους τελικούς κόμβους προς άλλους τελικούς κόμβους. Συνήθως οι κεφαλές συστοιχίας είναι κόμβοι πιο ισχυροί σε πόρους και ενέργεια από ότι οι τελικοί κόμβοι. Σε μερικές περιπτώσεις οι κεφαλές συστοιχίας δημιουργούν ένα δίκτυο κορμού που είναι συνεχώς συνδεδεμένο σε παροχή τροφοδοσίας ενέργειας και έτσι δεν εξαντλείται η ενέργεια των κεντρικών κόμβων.

A.7 Μορφές Δρομολόγησης

anycast 	multicast 
broadcast 	unicast 
geocast 	

A.8 Διαμορφώσεις σήματος σε ασύρματες επικοινωνίες

Παρακάτω αναφέρονται, ενδεικτικά και σε συνοπτική περιγραφή, ορισμένες διαμορφώσεις σημάτων που χρησιμοποιούνται σε ασύρματα δίκτυα αισθητήρων ή/και σε ενσύρματα, αλλά δεν αναφέρονται όλες οι πιθανές διαμορφώσεις που μπορεί να υπάρχουν. Επίσης αναφέρονται διάφορες διαδικασίες ανάθεσης σχισμών στους κόμβους για τη χρήση ενός καναλιού από πολλούς κόμβους.

A.8.1 TDMA

Πολλαπλή πρόσβαση με διαίρεση χρόνου (Time Division Multiple Access). Το TDMA είναι μετάδοση ψηφιακής επικοινωνίας που επιτρέπει σε ένα σύνολο από κόμβους, που επικοινωνούν μεταξύ τους, να έχουν πρόσβαση σε ένα μόνο κανάλι συχνότητας, χωρίς παρεμβολές και συγκρούσεις. Αυτό επιτυγχάνεται αν διαιρεθεί η συχνότητα του καναλιού σε σχισμές χρόνου time slots, και μετά κατανέμονται μοναδικές σχισμές χρόνου σε κάθε κόμβο. Οι κόμβοι με τη σειρά εκπέμπουν και λαμβάνουν δεδομένα ο ένας μετά από τον άλλον, με βάση έναν χρονοπρογραμματισμό (Schedule). Αλλά κάθε φορά μόνο ένας κόμβος χρησιμοποιεί το κανάλι για όλο το χρονικό διάστημα που διαρκεί μία σχισμή χρόνου time slot. Αυτή η μέθοδος έχει το πλεονέκτημα ότι δεν γίνονται συγκρούσεις αλλά έχει το μειονέκτημα ότι αν ένας κόμβος δεν έχει να εκπέμψει δεδομένα καταλαμβάνει άσκοπα μία χρονική σχισμή slot του καναλιού χωρίς να χρειάζεται.

A.8.2 CDMA

Πολλαπλή πρόσβαση με διαίρεση κώδικα (Code Division Multiple Access). Το CDMA είναι μία διαμόρφωση εξαπλωμένου φάσματος (spread spectrum) (SS) που επιτρέπει σε πολλούς κόμβους που επικοινωνούν να εκπέμπουν ταυτόχρονα. Η εξαπλώση φάσματος (Spread spectrum) είναι μία τεχνική διαμόρφωσης των ραδιοεπικοινωνιών όπου η ενέργεια της ασύρματης μετάδοσης εξαπλώνεται σε ένα πολύ μεγαλύτερο εύρος ζώνης (bandwidth) από αυτό που απαιτείται πραγματικά για το ρυθμό δεδομένων (data rate). Τα συστήματα που βασίζονται στην εξάπλωση φάσματος, εκπέμπουν ένα σήμα πληροφοριών που συνδυάζεται με ένα σήμα ψευδο-θορύβου που έχει αρκετά μεγαλύτερο εύρος ζώνης, για να παραχθεί ένα σήμα ευρείας ζώνης wideband signal. Συνεπώς, το σήμα που εκπέμπεται καταλαμβάνει μεγαλύτερο εύρος ζώνης bandwidth από αυτό που απαιτείται για να μεταδοθεί το αρχικό σήμα πληροφορίας. Αυτό έχει το πλεονέκτημα ότι δεν είναι εύκολη η υποκλοπή του αρχικού σήματος και η αποδασμόρφωσή του από κάποιον υποκλοπέα, ενώ επιπλέον περιορίζονται οι επιδράσεις των παρεμβολών στο εξαπλωμένο σήμα διότι οι παρεμβολές περιορίζονται μόνο σε κάποιες συχνότητες και όχι σε όλο το φάσμα συχνοτήτων του εξαπλωμένου σήματος. Οι πιο κοινές τεχνικές εξάπλωσης φάσματος χρησιμοποιούν είτε την μεταπήδηση συχνοτήτων frequency hopping (FH) ή την ευθεία ακολουθία direct sequence (DS), ενώ υπάρχουν και τα υβριδικά συστήματα που χρησιμοποιούν έναν συνδυασμό των δύο τύπων.

Μεταπήδηση συχνοτήτων (Frequency Hopping).

Τα συστήματα εξάπλωσης φάσματος με μεταπήδηση συχνότητας Frequency-hopping spectrum systems (FHSS) διαμορφώνουν το σήμα δεδομένων με ένα σήμα φέροντος στενής ζώνης narrowband carrier signal που μεταπηδά hops στη διάρκεια του χρόνου από μία συχνότητα σε άλλη με ένα ψευδοτυχαίο αλλά προβλέψιμο σχήμα επιλέγοντας συχνότητες από τις συχνότητες ευρείας ζώνης (wideband of frequencies). Για να αποκωδικοποιηθεί σωστά το σήμα πρέπει να είναι συγχρονισμένα τα ασύρματα σχήματα μεταπήδησης συχνότητας (hopping patterns) από τον πομπό και από το δέκτη.

Ευθεία ακολουθία.

Τα συστήματα ευθείας ακολουθίας με εξάπλωση φάσματος Direct-sequence spread-spectrum systems (DSSS) διαιρούν τη ροή πληροφορίας που πρόκειται να μεταδοθεί, σε μικρά κομμάτια (small chunks) και το καθένα από αυτά κατανέμεται σε ένα κανάλι συχνότητας σε όλο το φάσμα. Ένα σήμα δεδομένων στον κόμβο αποστολέα συνδυάζεται με μία ακολουθία bit υψηλότερου ρυθμού δεδομένων, που ονομάζεται chipping code, που διαιρεί τα δεδομένα του χρήστη σύμφωνα με το λόγο εξάπλωσης spreading ratio. Ο κώδικας chipping code είναι ένα σχήμα bit πλεονασμού redundant bit pattern για κάθε bit του πραγματικού σήματος που μεταδίδεται. Αυτός ο πλεονασμός των bit αυξάνει την αντίσταση σε παρεμβολές στο σήμα που εκπέμπεται και βελτιώνει την πιθανότητα να αποκαλυφθούν τα αρχικά δεδομένα αν ένα ή περισσότερα bits του σχήματος έχουν καταστραφεί στην διάρκεια της μετάδοσης.

Polling

Μια μορφή ανάθεσης σχισμών σε κόμβους, που χρησιμοποιείται ευρέως, είναι η διαδικασία polling. Σε αυτή τη μορφή, μία κύρια συσκευή ελέγχου (master control device ή controller) εκτελεί αιτήσεις με ερωτήματα (queries), με κάποια προκαθορισμένη σειρά, σε κάθε εξαρτώμενο κόμβο (slave node) για το αν έχει να μεταδώσει δεδομένα. Αν ο κόμβος έχει να μεταδώσει δεδομένα, τότε πληροφορεί την κεντρική συσκευή ελέγχου (controller) για την πρόθεσή του να εκπέμψει τα δεδομένα. Σε απάντηση, η κεντρική συσκευή ελέγχου ανακατανέμει το κανάλι στον κόμβο αυτόν που είναι έτοιμος να στείλει δεδομένα, και τότε αυτός ο κόμβος χρησιμοποιεί τον πλήρη ρυθμό δεδομένων (data rate) για να μεταδώσει τα δεδομένα του.

Αν ο κόμβος που δέχεται το polling δεν έχει δεδομένα να εκπέμψει, τότε απορρίπτει την αίτηση της κεντρικής συσκευής ελέγχου (controller). Σε απάντηση, η συσκευή ελέγχου (controller) προχωράει στον επόμενο κόμβο και εκτελεί την ίδια διαδικασία polling.

Το βασικό πλεονέκτημα της διαδικασίας polling είναι ότι όλοι οι κόμβοι μπορούν να έχουν ίση πρόσβαση στο κανάλι. Όμως μπορεί να δοθεί προτίμηση σε κάποιους κόμβους υψηλής προτεραιότητας και να δέχονται πιο συχνά τη διαδικασία polling. Βασικό μειονέκτημα της διαδικασίας polling, είναι το μεγάλο overhead που προκαλείται από το μεγάλο πλήθος μηνυμάτων που παράγονται από την συσκευή ελέγχου (controller) όταν κάνει ερωτήσεις στους κόμβους. Επιπλέον η αποτελεσματικότητα της διαδικασίας polling εξαρτάται από την αξιοπιστία του controller.

A.8.4 CSMA

Πολλαπλή πρόσβαση με ανίχνευση φέροντος (Carrier Sense Multiple Access). Το CSMA λειτουργεί και σε λειτουργία συνεχούς χρόνου unslotted CSMA, και σε λειτουργία διακριτού χρόνου, slotted CSMA. Επιπλέον τα πρωτόκολλα CSMA διακρίνονται σε δύο κατηγορίες το μη επίμονο CSMA και το επίμονο CSMA, ανάλογα με την τεχνική που χρησιμοποιείται για να αποκτήσει ο κόμβος πρόσβαση σε ένα ελεύθερο κανάλι και την τεχνική που περιμένει να ελευθερωθεί ένα κανάλι που είναι απασχολημένο.

Μη επίμονο (Non-Persistent) CSMA.

Στο μη επίμονο CSMA όταν ο κόμβος είναι έτοιμος να μεταδώσει ένα πακέτο πρώτα ανιχνεύει (sense) το φέρον (carrier) για να διαπιστώσει αν γίνεται κάποια άλλη μετάδοση σήματος εκείνη τη στιγμή. Αν το κανάλι είναι αδρανές (idle), ο κόμβος εκπέμπει άμεσα το πακέτο δεδομένων του και περιμένει για ένα μήνυμα αναγνώρισης. Για να ρυθμίσει τον χρόνο λήξης για αναμονή αναγνώρισης (acknowledgment timeout value), ο κόμβος πρέπει να λάβει υπόψη του την καθυστέρηση διάδοσης (round-trip propagation delay) δηλαδή το χρονικό διάστημα που απαιτείται για να αποσταλεί το σήμα μαζί με το χρονικό διάστημα που απαιτείται για το μήνυμα αναγνώρισης acknowledgment αυτού του σήματος. Επιπλέον ισχύει το γεγονός ότι ο κόμβος δέκτης πρέπει επίσης να κάνει ανταγωνισμό στο κανάλι για να εκπέμψει το σήμα αναγνώρισης acknowledgment. Απαιτείται να γίνει μία εκτίμηση για το μέσο χρόνο συγκρούσεων, για μία επιτυχή μετάδοση αλλά αυτό είναι δύσκολο να γίνει και εξαρτάται από το φορτίο κυκλοφορίας και το πλήθος των σταθμών που ανταγωνίζονται μεταξύ τους. Όταν δεν λάβει κανένα μήνυμα αναγνώρισης acknowledgment, όση ώρα περιμένει ο κόμβος αποστολέας μέχρι το χρόνο λήξης, τότε ο κόμβος υποθέτει ότι χάθηκε το πακέτο δεδομένων, επειδή υπήρχαν συγκρούσεις ή παρεμβολές. Ο σταθμός προγραμματίζει χρονικά το πακέτο για να ξανά μεταδοθεί retransmission. Αν το κανάλι είναι απασχολημένο busy, ο κόμβος που εκπέμπει υποχωρεί “backs off” για ένα τυχαίο χρονικό διάστημα. Μετά από αυτό το διάστημα ανιχνεύει ξανά το κανάλι. Ανάλογα με την κατάσταση του καναλιού, αν το κανάλι είναι αδρανές idle ο κόμβος εκπέμπει το πακέτο, ενώ αν το κανάλι είναι απασχολημένο, ο κόμβος μπαίνει ξανά σε κατάσταση υποχώρησης back-off mode. Η ίδια διαδικασία επαναλαμβάνεται μέχρι το πακέτο δεδομένων να μεταδοθεί επιτυχώς. Το μη επίμονο CSMA ελαχιστοποιεί τις παρεμβολές interference ανάμεσα στις μεταδόσεις πακέτων και απαιτεί από τους σταθμούς που βλέπουν ότι το κανάλι είναι απασχολημένο, να ξανα προγραμματίσουν τις μεταδόσεις τους με έναν τυχαίο τρόπο. Το βασικό μειονέκτημα του μη επίμονου CSMA scheme, είναι ότι το κανάλι μπορεί να είναι αδρανές στο χρόνο υποχώρησης back-off time ενός σταθμού που ανταγωνίζεται με τους άλλους σταθμούς. Τότε υπάρχει μία σπατάλη στην χωρητικότητα του καναλιού που δεν είναι απαραίτητη και μπορεί να μειώσει σημαντικά την απόδοση throughput του δικτύου.

Η μορφή 1-persistent CSMA

Δημιουργήθηκε με στόχο να ξεπεραστούν τα προβλήματα του μη επίμονου CSMA. Αυτή η μορφή χρησιμοποιεί διαφορετικό αλγόριθμο για να αποκτήσουν πρόσβαση σε ένα

ελεύθερο κανάλι. Η μορφή 1-persistent scheme δεν επιτρέπει στο κανάλι να παραμείνει αδρανές (idle) αν ένας κόμβος είναι έτοιμος να εκπέμψει δεδομένα. Με βάση τη μορφή 1-persistent, ο κόμβος που είναι έτοιμος να εκπέμψει ένα πακέτο δεδομένων, πρώτα ανιχνεύει το κανάλι. Αν το κανάλι είναι ελεύθερο, ο κόμβος εκπέμπει το μήνυμά του αμέσως. Αν το κανάλι είναι απασχολημένο, ο κόμβος επίμονα συνεχίζει να ακούει μέχρι το κανάλι να γίνει αδρανές (idle). Μόλις το κανάλι ανιχνευτεί ότι είναι αδρανές (idle), τότε η μετάδοση ξεκινάει αμέσως.

Η μορφή p-persistent CSMA

Ο αλγόριθμος p-persistent αντιπροσωπεύει έναν συμβιβασμό ανάμεσα στα συστήματα μη επίμονου CSMA και 1-persistent CSMA. Με βάση αυτόν τον αλγόριθμο, ο κόμβος που ανιχνεύει ότι το κανάλι είναι αδρανές εκπέμπει το πακέτο του με πιθανότητα p . Με πιθανότητα $(1-p)$, ο σταθμός περιμένει για κάποιο συγκεκριμένο χρόνο πριν επιχειρήσει να εκπέμψει ξανά το πακέτο. Η τιμή του χρόνου που διαρκεί η αναμονή (waiting period) συνήθως τίθεται να είναι ίση με τη μέγιστη καθυστέρηση διάδοσης ανάμεσα στους πιο απομακρυσμένους κόμβους στο unslotted CSMA ή σε μία σχισμή χρόνου slot time στο slotted ALOHA. Στο τέλος της περιόδου αναμονής, ο κόμβος ανιχνεύει ξανά το κανάλι. Αν το κανάλι είναι απασχολημένο, ο κόμβος συνεχίζει να ακούει μέχρι το κανάλι να γίνει αδρανές. Μόλις το κανάλι γίνει αδρανές, ο κόμβος επαναλαμβάνει τον αλγόριθμο p-persistent για την απόκτηση πρόσβασης στο κανάλι. Αυτή η διαδικασία συνεχίζεται μέχρι ένα πακέτο να μεταδοθεί επιτυχώς. Η τιμή του p παίζει σημαντικό ρόλο για τη σταθερότητα του πρωτοκόλλου. Όταν υπάρχει μεγάλο φορτίο κυκλοφορίας, αν είναι μεγάλη η τιμή του p , τότε πολλαπλοί κόμβοι θα προσπαθήσουν να εκπέμψουν και έτσι θα αυξηθεί η πιθανότητα συγκρούσεων. Επειδή το p θα έχει μεγάλη τιμή, οι κόμβοι που συγκρούονται θα προσπαθήσουν πιθανόν να κάνουν επαναληπτική μετάδοση σχεδόν αμέσως μετά από τη στιγμή της σύγκρουσης. Σε χειρότερη περίπτωση, αυτές οι επαναληπτικές μεταδόσεις θα πρέπει να ανταγωνιστούν με τις νέες μεταδόσεις που κάνουν άλλοι κόμβοι και έτσι αυτό εγγυάται ότι θα συμβούν ακόμη περισσότερες συγκρούσεις. Σταδιακά καθώς θα αυξηθεί το πλήθος των σταθμών που ανταγωνίζονται, θα μειωθεί σημαντικά η απόδοση throughput. Για να μη συμβεί μια τέτοια κατάσταση θα πρέπει η τιμή του p να είναι μικρή. Αν στο p τεθεί μία τιμή που είναι μικρή, θα μειωθεί το πλήθος των συγκρούσεων. Σε ένα χαμηλό φορτίο κυκλοφορίας, όμως, αν η τιμή του p είναι μικρή μπορεί να προκαλέσει σε έναν σταθμό που ανταγωνίζεται με άλλους, να περιμένει για μεγάλες καθυστερήσεις, χωρίς να χρειάζεται, πριν να εκπέμψει τα πακέτα δεδομένων του. Για αυτό είναι απαραίτητο να ληφθεί υπόψη με προσοχή ο παρεχόμενος ρυθμός κυκλοφορίας για να επιλεγεί μία κατάλληλη τιμή του p .

CSMA/CD

Πολλαπλή πρόσβαση με ανίχνευση φέροντος (Carrier Sense Multiple Access) με ανίχνευση συγκρούσεων (collision detection). Στα δίκτυα, όταν η καθυστέρηση διάδοσης propagation delay είναι μικρή σχετικά με το χρόνο μετάδοσης του πακέτου, ένα πλεονέκτημα του CSMA είναι ότι η ανίχνευση φέροντος μειώνει το πλήθος συγκρούσεων και μειώνει και το χρονικό διάστημα συγκρούσεων που είναι το πιο σημαντικό.

Το βασικό μειονέκτημα του CSMA είναι ότι οι σταθμοί που ανταγωνίζονται συνεχίζουν να εκπέμπουν τα δεδομένα τους ακόμα και όταν συμβεί μία σύγκρουση. Για μεγάλα πακέτα δεδομένων, το εύρος ζώνης στο οποίο γίνεται άσκοπη χρήση είναι σημαντικό σε σύγκριση με το χρόνο διάδοσης πακέτων. Επιπλέον οι κόμβοι μπορεί να έχουν μεγάλες καθυστερήσεις που δεν χρειάζονται όταν περιμένουν για τη μετάδοση ολόκληρου του πακέτου να ολοκληρωθεί πριν κάνουν επαναληπτική προσπάθεια για να στείλουν ξανά το πακέτο. Για να μειωθεί αυτό το πρόβλημα χρησιμοποιείται η τεχνική CSMA/CD. Αλλά αυτή η μέθοδος είναι προτιμώμενη σε ενσύρματα δίκτυα και όχι σε ασύρματα. Η μέθοδος CSMA/CD επεκτείνει τις δυνατότητες του κόμβου ώστε του επιτρέπει να ακούει το κανάλι παράλληλα ενώ εκπέμπει τα δικά του δεδομένα. Ο κόμβος μπορεί να παρακολουθήσει το σήμα στο κανάλι και να ανιχνεύσει μία σύγκρουση αν συμβεί. Πιο συγκεκριμένα, αν ο κόμβος έχει να στείλει δεδομένα, πρώτα ακούει για να διαπιστώσει αν υπάρχει μία μετάδοση σε εξέλιξη στο κανάλι. Αν δεν υπάρχει καμία δραστηριότητα στο κανάλι, ο κόμβος αρχίζει να εκπέμπει τα δεδομένα του και συνεχίζει να παρακολουθεί το σήμα στο κανάλι καθώς τα εκπέμπει. Αν ανιχνευθεί ένα άλλο σήμα στο κανάλι, ο κόμβος που εκπέμπει αμέσως σταματά την μετάδοση του. Αυτό μειώνει μια ποσότητα του εύρους ζώνης που σπαταλιέται άσκοπα αν συμβεί μία σύγκρουση, μέχρι να ανιχνευθεί ότι έγινε αυτή η σύγκρουση.

Όταν συμβεί η σύγκρουση, κάθε σταθμός που ανταγωνίζεται τους άλλους και συμμετέχει στη σύγκρουση περιμένει για ένα τυχαίο χρονικό διάστημα και μετά προσπαθεί να μεταδώσει ξανά το πακέτο δεδομένων του. Το χρονικό διάστημα που περιμένει ο κόμβος πριν να προγραμματίσει την επαναληπτική μετάδοση του πακέτου, καθορίζεται από έναν αλγόριθμο πιθανολογικό (probabilistic algorithm) που ονομάζεται truncated binary exponential back-off algorithm. Ο αλγόριθμος παράγει το χρόνο αναμονής μετά από μία σύγκρουση, με βάση τη χρονική διάρκεια της σχισμής χρόνου slot και με βάση το τρέχον πλήθος προσπαθειών για επαναληπτικές μεταδόσεις.

Το μειονέκτημα του CSMA/CD είναι ότι απαιτεί να υπάρχουν κάποιοι κόμβοι αισθητήρες με επιπρόσθετες δυνατότητες για ανίχνευση συγκρούσεων. Οι κόμβοι αισθητήρες έχουν περιορισμένη μνήμη αποθήκευσης, επεξεργαστική ισχύ και πόρους ενέργειας. Αυτοί οι περιορισμοί περιορίζουν και το σχεδιασμό του στρώματος MAC layer. Η υποστήριξη για ανίχνευση συγκρούσεων σε ένα WSN δεν είναι εφικτή χωρίς πρόσθετα κυκλώματα. Συγκεκριμένα, οι ασύρματοι πομποδέκτες συνήθως είναι half-duplex δηλαδή τα δεδομένα μπορούν να μεταδίδονται και προς τις δύο κατευθύνσεις αλλά όχι την ίδια χρονική στιγμή. Για να ανιχνεύσει τη σύγκρουση ο κόμβος αισθητήρας πρέπει να είναι σε κατάσταση ακοής "listening" και ταυτόχρονα σε κατάσταση αποστολής "talking." Όμως η πολυπλοκότητα και το κόστος των αισθητήρων πρέπει να είναι σε χαμηλά επίπεδα, και να υπάρχει επεκτασιμότητα ώστε να υπάρξουν ευρείες προσαρμογές στην τεχνολογία σε εφαρμογές ευαίσθητες προς το κόστος στις οποίες χρησιμοποιείται ένα μεγάλο πλήθος αισθητήρων. Συνεπώς, ο σχεδιασμός του φυσικού επιπέδου πρέπει να είναι βελτιστοποιημένος ώστε να διατηρηθεί χαμηλό το κόστος. Άλλος σημαντικός παράγοντας που αποτρέπει τη χρήση του CSMA/CD είναι η δυσκολία ανίχνευσης των συγκρούσεων σε ασύρματο περιβάλλον. Στο ενσύρματο περιβάλλον δεν υπάρχει μεγάλη εξασθένιση και ο πομπός μπορεί να ανιχνεύσει μία σύγκρουση στο δέκτη. Στο ασύρματο

περιβάλλον όμως υπάρχει μεγάλη εξασθένιση με την απόσταση και ο πομπός δεν έχει δυνατότητα να ανιχνεύσει με βεβαιότητα αν έγινε ή όχι μία σύγκρουση στο δέκτη. Αυτό το μειονέκτημα περιορίζει την μέθοδο ανίχνευσης συγκρούσεων και δεν εφαρμόζεται σε ασύρματα δίκτυα αισθητήρων.

CSMA/CA

Πολλαπλή πρόσβαση με ανίχνευση φέροντος (Carrier Sense Multiple Access) με αποφυγή συγκρούσεων (Collision Avoidance). Αν το κανάλι μετάδοσης είναι απασχολημένο και αυτό ανιχνευθεί πριν από τη μετάδοση, τότε η μετάδοση αναβάλλεται για ένα τυχαίο χρονικό διάστημα. Με αυτό το τυχαίο χρονικό διάστημα μειώνεται η πιθανότητα να εκπέμψουν ταυτόχρονα δύο ή περισσότεροι κόμβοι μόλις τελειώσει η μετάδοση διότι κάθε κόμβος καθυστερεί για διαφορετικό χρονικό διάστημα να εκπέμψει. Με αυτή τη μέθοδο μειώνεται η πιθανότητα να γίνουν συγκρούσεις.

Ο λόγος που δημιουργήθηκε το CSMA/CA ήταν ότι υπήρχαν μειονεκτήματα στο CSMA που εξηγούνται στη συνέχεια. Η ανίχνευση φέροντος πριν από τη μετάδοση είναι μία αποτελεσματική μέθοδος για να αυξηθεί η απόδοση throughput στο διαμοιραζόμενο κανάλι. Αν και μπορεί να εφαρμοστεί στα ασύρματα δίκτυα αυτή η μορφή, είναι ευαίσθητη σε δύο προβλήματα που είναι το πρόβλημα του κρυμμένου κόμβου (hidden-node) και το πρόβλημα του εκτεθειμένου κόμβου (exposed-node). Τα προβλήματα του κρυμμένου κόμβου (hidden-node) και του εκτεθειμένου κόμβου (exposed-node) προκύπτουν έμμεσα από τις μεταβαλλόμενες ιδιότητες ως προς το χρόνο του ασύρματου καναλιού, που προκαλούνται από φυσικά φαινόμενα όπως είναι ο θόρυβος η εξασθένηση, η απόσβεση και η εξασθένηση λόγω απωλειών διαδρομών. Αυτά τα προβλήματα σε συνδυασμό με τη γρήγορη μείωση της ισχύος του λαμβανόμενου σήματος καθώς αυξάνεται η απόσταση ανάμεσα στον πομπό και στον δέκτη, περιορίζουν τη μέγιστη εμβέλεια που μπορεί να επιτευχθεί από έναν κόμβο αποστολέα. Αυτός ο περιορισμός και το ότι το CSMA σχεδιάστηκε για να αποφεύγει συγκρούσεις ανιχνεύοντας το σήμα στην γειτονιά του πομπού οδηγούν στα προβλήματα του κρυμμένου και του εκτεθειμένου κόμβου.

Κρυμμένος κόμβος

Ο κρυμμένος κόμβος (hidden node) ορίζεται ως ο κόμβος που είναι μέσα στην εμβέλεια του κόμβου προορισμού αλλά εκτός εμβέλειας του κόμβου που εκπέμπει. Τότε ενδέχεται να γίνει μία σύγκρουση στον δέκτη διότι θα επιχειρήσουν να στείλουν δεδομένα και ο κόμβος που εκπέμπει αλλά και ο κρυμμένος κόμβος ταυτόχρονα και δεν θα μπορεί να ανιχνεύσει ο ένας κόμβος τον άλλον για να υποχωρήσουν. Αυτό συχνά συμβαίνει στα ασύρματα δίκτυα. Αυτή είναι η διαφορά των συγκρούσεων στα ενσύρματα δίκτυα από τα ασύρματα δίκτυα.

Εκτεθειμένος Κόμβος

Ο εκτεθειμένος κόμβος είναι ένας κόμβος που βρίσκεται μέσα στην εμβέλεια του αποστολέα, αλλά έξω από την εμβέλεια του κόμβου προορισμού. Αυτό μπορεί να οδηγήσει σε κάποιες επιπλέον καθυστερήσεις, που δεν χρειάζονται, όταν ο αποστολέας

επιχειρήσει να στείλει δεδομένα στον εκτεθειμένο κόμβο. Η καθυστέρηση προκύπτει διότι όταν ο κόμβος αποστολέας ανιχνεύσει σήματα στο κανάλι που πηγαίνουν στον κόμβο προορισμού, θα θεωρήσει ότι το κανάλι είναι απασχολημένο και θα υποχωρήσει. Αλλά αφού ο εκτεθειμένος κόμβος δεν βρίσκεται εντός της εμβέλειας του κόμβου προορισμού, δεν χρειαζόταν να γίνει αυτή η υποχώρηση και μπορούσε να είχε λάβει τα δεδομένα.

Έτσι το πρόβλημα του κρυφού κόμβου είναι η σύγκρουση στον κόμβο δέκτη, ενώ το πρόβλημα του εκτεθειμένου κόμβου είναι η άσκοπη καθυστέρηση στη λήψη δεδομένων που προορίζονται για τον ίδιο τον κρυμμένο κόμβο.

Για τη λύση ή για τη μείωση των προβλημάτων εκτεθειμένου κόμβου και κρυμμένου κόμβου σχεδιάστηκαν διάφορες προσεγγίσεις αλλά ξεχωρίζουν δύο από αυτές.

Το σήμα busy tone

Η πρώτη προσέγγιση ήταν η χρήση ενός σήματος busy tone. Η χρήση του σήματος busy-tone έγινε με το σκεπτικό ότι οι συγκρούσεις συμβαίνουν στον κόμβο δέκτη, ενώ το CSMA εκτελείται στον κόμβο αποστολέα. Η μέθοδος busy-tone απαιτεί να χρησιμοποιούνται δύο ξεχωριστά κανάλια: ένα κανάλι δεδομένων (data channel) και ένα κανάλι ελέγχου (control channel). Το κανάλι δεδομένων (data channel) χρησιμοποιείται αποκλειστικά για μετάδοση δεδομένων (transmit data). Το κανάλι ελέγχου (control channel) χρησιμοποιείται από το δέκτη για να στείλει ένα σήμα σε όσους κόμβους στο δίκτυο είναι στη διαδικασία λήψης δεδομένων. Μόλις ένας κόμβος ξεκινά να λαμβάνει ένα πακέτο δεδομένων data packet που μεταφέρει τη διεύθυνση του κόμβου αυτού στο πεδίο διεύθυνση προορισμού, αμέσως ο κόμβος εκκινεί την εκπομπή ενός μη διαμορφωμένου σήματος στο κανάλι ελέγχου, που δείχνει ότι ο δέκτης είναι απασχολημένος. Ο κόμβος συνεχίζει να μεταδίδει το σήμα busy tone την ίδια στιγμή που λαμβάνει το πακέτο δεδομένων μέχρι να ολοκληρώσει τη λήψη αυτού του πακέτου. Πριν μεταδώσει ένα πακέτο δεδομένων ο κόμβος αποστολέας πρέπει πρώτα να ανιχνεύσει το κανάλι ελέγχου για την ύπαρξη ενός σήματος busy tone. Αν το κανάλι είναι ελεύθερο, τότε μόνο θα προχωρήσει ο κόμβος στην εκπομπή του πακέτου δεδομένων. Αλλιώς ο κόμβος αποστολέας θα αναβάλλει την μετάδοση μέχρι να ελευθερωθεί το κανάλι ελέγχου. Η μέθοδος busy-tone λύνει και τα δύο προβλήματα δηλαδή του κρυμμένου κόμβου και του εκτεθειμένου κόμβου. Το σήμα busy-tone πρέπει να έχει ένα επίπεδο ισχύος που δεν είναι πολύ ασθενές για να μπορεί να το ακούσει ένας κόμβος που βρίσκεται στην εμβέλεια του δέκτη, αλλά να μην είναι και πολύ ισχυρό για να μην το ακούσουν παραπάνω κόμβοι από όσους πρέπει και αρχίσουν να διακόπτουν τις μεταδόσεις τους.

Το βασικό μειονέκτημα του busy tone είναι ότι πρέπει ο κόμβος να λειτουργεί σε λειτουργία duplex mode, για να στέλνει και να λαμβάνει δεδομένα συγχρόνως. Με αυτή την απαίτηση η πολυπλοκότητα του κόμβου αυξάνεται σημαντικά και έχει αυξημένο κόστος και κατανάλωση ενέργειας.

Η αποφυγή συγκρούσεων

CSMA/CA

Η δεύτερη μέθοδος που είχε στόχο να αντιμετωπίσει το πρόβλημα του κρυμμένου κόμβου βασίστηκε στην αποφυγή συγκρούσεων. Αυτή η μέθοδος χρησιμοποιεί τη χειραψία (handshake) με τα πακέτα ready to-send (RTS), clear-to-send (CTS). Σε αυτή τη διαδικασία χειραψίας απαιτείται οι κόμβοι να εφαρμόζουν ένα τυπικό μηχανισμό για την αποφυγή συγκρούσεων στα μηνύματα που στέλνουν στο ασύρματο δίκτυο. Επειδή ένας κόμβος δεν μπορεί να ανιχνεύσει αν συμβεί μία σύγκρουση, προσπαθεί να αποφύγει τις συγκρούσεις. Για αυτό περιμένει να είναι ελεύθερο το ασύρματο κανάλι για το χρονικό διάστημα που χρειάζεται για να μεταδοθεί ένα πακέτο σε όλο το μέσο. Δηλαδή: ο χρόνος που απαιτείται για να αποσταλεί το πακέτο στους πιο απομακρυσμένους κόμβους του δικτύου. Όταν ο κόμβος θέλει να μεταδώσει ένα πακέτο δεδομένων, πρώτα ανιχνεύει το φέρον για να δει αν εκπέμπει ένας άλλος κόμβος. Αν δεν ανιχνεύσει άλλες μεταδόσεις, ο κόμβος στέλνει ένα μικρό πακέτο RTS στον προοριζόμενο δέκτη του πακέτου δεδομένων. Αν ο δέκτης είναι στην πραγματικότητα αδρανής και ανιχνεύσει ότι το μέσο είναι ελεύθερο, στέλνει ως απάντηση ένα μικρό πακέτο CTS. Μόλις λάβει το πακέτο CTS, ο κόμβος πομπός στέλνει το πραγματικό πακέτο δεδομένων στο δέκτη. Αν μετά από μία προκαθορισμένη περίοδο ο σταθμός που εκπέμπει δεν λάβει ένα πακέτο CTS ως απάντηση στο πακέτο RTS packet, περιμένει για τυχαίο χρονικό διάστημα και μετά επαναλαμβάνει την διαδικασία χειραψίας RTS/CTS. Παρόλο που δεν μπορεί να λύσει εντελώς το πρόβλημα του κρυμμένου κόμβου, η χειραψία RTS/CTS χρησιμοποιείται ευρέως στα ασύρματα δίκτυα για αποφυγή συγκρούσεων μεταξύ των πακέτων δεδομένων και βελτιώνει την απόδοση throughput στο δίκτυο.

A.8.5 Διαμοιρασμός ενός καναλιού σε πολλούς κόμβους

Υπάρχουν διάφορες μορφές ανάθεσης ενός καναλιού σε πολλαπλούς κόμβους που πρόκειται να στείλουν δεδομένα στο κανάλι. Μερικοί τρόποι αναφέρονται παρακάτω.

α) Η σταθερή ανάθεση πόρων του καναλιού σε κόμβους.

Στη διαδικασία σταθερής ανάθεσης πόρων του καναλιού στους κόμβους, σε κάθε κόμβο που θέλει να εκπέμψει τα δεδομένα του, κατανέμεται (allocated) μία προκαθορισμένη και σταθερή ποσότητα των πόρων του καναλιού. Οι πόροι του καναλιού είναι σχισμές χρόνου στο TDMA ή ζώνες συχνοτήτων σε συστήματα FDMA. Ο κάθε κόμβος χρησιμοποιεί τους πόρους που έχουν κατανεμηθεί σε αυτόν κατ' αποκλειστικότητα, χωρίς να ανταγωνίζεται με άλλους κόμβους για την πρόσβαση και χρήση αυτών των πόρων. Τυπικά πρωτόκολλα που ανήκουν σε αυτή την κατηγορία είναι η πολύπλεξη με διαίρεση συχνότητας frequency-division multiple access (FDMA), η πολύπλεξη με διαίρεση χρόνου time-division multiple access (TDMA) και η πολύπλεξη με διαίρεση κώδικα code-division multiple access (CDMA). Στις μορφές σταθερής ανάθεσης (fixed-assignment), η χωρητικότητα του καναλιού ανατίθεται αποκλειστικά στους κόμβους του δικτύου με έναν προκαθορισμένο τρόπο, ανεξάρτητα από το αν έχουν να εκπέμψουν ή όχι δεδομένα. Σε κάθε κόμβο που επικοινωνεί, ανατίθεται είτε μία ζώνη συχνοτήτων σε συστήματα FDMA είτε μία σχισμή χρόνου time slot στα συστήματα TDMA. Αυτή η

ανάθεση όμως είναι στατική και αν ο κόμβος δεν έχει δεδομένα για να στείλει, πάλι δεσμεύει τους πόρους του καναλιού, χωρίς να στέλνει δεδομένα και έτσι υπάρχει μία σπατάλη.

β) Η ανάθεση πόρων του καναλιού κατά απαίτηση στους κόμβους

Ο κύριος στόχος ανάθεσης κατά απαίτηση πόρων του καναλιού στους κόμβους είναι να βελτιωθεί ο βαθμός χρήσης καναλιού (channel utilization) κάνοντας μία ανακατανομή της χωρητικότητας του καναλιού σε κόμβους που ανταγωνίζονται μεταξύ τους, με έναν τρόπο βέλτιστο ή κοντά στο βέλτιστο για να χρησιμοποιήσουν τους πόρους του καναλιού. Στην ανάθεση πόρων κατ' απαίτηση, αγνοούνται οι κόμβοι που είναι αδρανείς και λαμβάνονται υπόψη μόνο εκείνοι οι κόμβοι που είναι έτοιμοι να εκπέμψουν τα δεδομένα τους. Για την ανάθεση κατ' απαίτηση, συνήθως απαιτείται να υπάρχει ένας μηχανισμός ελέγχου του δικτύου που θα έχει τη διαιτησία και θα δίνει πρόσβαση στο κανάλι σε κόμβους που ανταγωνίζονται για τη χρήση του καναλιού. Επιπλέον απαιτείται και ένα δεύτερο κανάλι λογικού ελέγχου (logical control channel) που είναι διαφορετικό από το κανάλι δεδομένων (data channel). Το κανάλι λογικού ελέγχου χρησιμοποιείται από τους σταθμούς ώστε να ζητούν δυναμικά την πρόσβαση από το μέσο επικοινωνιών.

Η ανάθεση κατά απαίτηση μπορεί να προκαλέσει κάποια καθυστέρηση στη μετάδοση δεδομένων, λόγω του ότι απαιτείται χρόνος για αίτηση πρόσβασης στο κανάλι από τους κόμβους. Μια άλλη κατηγοριοποίηση της ανάθεσης κατά απαίτηση είναι ο διαχωρισμός σε κεντρικού ελέγχου και σε κατανεμημένου ελέγχου.

γ) Η τυχαία ανάθεση πόρων του καναλιού στους κόμβους

Οι τεχνικές τυχαίας ανάθεσης Random assignment δεν έχουν προκαθορισμένη ανάθεση του εύρους ζώνης στους κόμβους και δεν εξασκούν κάποιο έλεγχο για να καθορίζουν ποιος κόμβος θα είναι ο επόμενος που θα έχει πρόσβαση στο κανάλι. Επιπλέον, αυτές οι τεχνικές δεν αναθέτουν κάποιο προβλέψιμο ή προκαθορισμένο χρόνο με πρόγραμμα schedule για οποιοδήποτε κόμβο θέλει να εκπέμψει δεδομένα. Όλοι οι κόμβοι πρέπει να ανταγωνίζονται μεταξύ τους για να έχουν πρόσβαση στο κανάλι. Οι συγκρούσεις συμβαίνουν όταν ένας οι περισσότεροι κόμβοι προσπαθούν να εκπέμψουν ταυτόχρονα τα δεδομένα τους. Για να ανιχνεύονται οι συγκρούσεις, απαιτείται ένας μηχανισμός για ανίχνευση συγκρούσεων και μία μορφή χρονοπρογραμματισμού των πακέτων που συγκρούονται, ώστε να γίνουν διαδοχικές επαναληπτικές μεταδόσεις τους (retransmissions). Οι τεχνικές αυτές ξεκίνησαν όταν χρησιμοποιήθηκαν αρχικά σε ζεύξεις ραδιοκυμάτων μακρινών αποστάσεων και στις δορυφορικές τηλεπικοινωνίες. Γνωστά πρωτόκολλα που χρησιμοποιούν αυτή την τεχνική είναι τα ALOHA, και CSMA.

