Ανοικτό Πανεπιστήμιο Κύπρου
Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών Στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Κρυπτογραφικές Επιθέσεις Παράπλευρου Καναλιού: Εφαρμογή σε Ασύρματα Δίκτυα Αισθητήρων.

Αχιλλέας Κωσταγιάννης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Δεκέμβριος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Στα Πληροφοριακά και Επικοινωνιακά Συστήματα*

Μεταπτυχιακή Διατριβή

Κρυπτογραφικές Επιθέσεις Παράπλευρου Καναλιού: Εφαρμογή σε Ασύρματα Δίκτυα Αισθητήρων.

Αχιλλέας Κωσταγιάννης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

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

Δεκέμβριος 2015

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η ραγδαία τεχνολογική πρόοδος έδωσε το έναυσμα για την παραγωγή αυτών των λύσεων όπου έχουν ως κύριο σκοπό την βελτίωση της ποιότητας ζωής του ανθρώπου. Ένα από τα τεχνολογικά επιτεύγματα τα οποία υλοποιήθηκαν είναι και οι ασύρματοι αισθητήρες. Οι αισθητήρες έχουν κάνει την εμφάνισή τους σε ένα τεράστιο πλαίσιο εφαρμογών. Το μικρό τους μέγεθος, το χαμηλό τους κόστος και η ανεξαρτησία που προσφέρουν αποτελούν τους κυριότερους παράγοντες που συνετέλεσαν για την προώθησή τους. Όπως και κάθε συσκευή η οποία ανταλλάσσει δεδομένα, έτσι και οι ασύρματοι αισθητήρες για την μετάδοση των δεδομένων τους χρησιμοποιούν κάποια κρυπτογραφική τεχνική για να κρυπτογραφήσουν τα δεδομένα τους.

Ωστόσο υπάρχουν πολλές τεχνικές επίθεσης οι οποίες είναι σε θέση να αποκρυπτογραφήσουν το κρυπτογραφημένο κείμενο, αν υπάρχει κάποια ευπάθεια κατά τη σχεδίαση του κρυπτογραφικού αλγορίθμου. Μια από αυτές τις τεχνικές κάνει χρήση του ενεργειακού αποτυπώματος μιας κρυπτογραφικής συσκευής. Η τεχνική αυτή υπάγεται στην ευρύτερη κατηγορία των κρυπτογραφικών επιθέσεων παράπλευρου καναλιού, οι οποίες αποσκοπούν στην εύρεση του μυστικού κλειδιού κρυπτογράφησης όχι εκμεταλλευόμενες κάποιες μαθηματικές ιδιότητες άλλα μέσω παρατηρήσεων φυσικών μεγεθών που εκπέμπονται από την κρυπτογραφική συσκευή – όπως είναι η κατανάλωση ενέργειας. Αν και οι τεχνικές αυτές μπορούν να εφαρμοστούν σε οποιοδήποτε περιβάλλον, είναι πιο εύκολα εφαρμόσιμες σε ασύρματα δίκτυα αισθητήρων.

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να παρουσιάσει και να αναδείξει όλα τα θέματα ασφάλειας που αφορούν τα ασύρματα δίκτυα αισθητήρων αλλά και, ειδικότερα, να πραγματοποιήσει μια προσπάθεια ανάκτησης του μυστικού κλειδιού κάνοντας χρήση απλά των ενεργειακών αποτυπωμάτων μίας συσκευής. Καταδεικνύεται ότι για τη σχεδίαση ενός κρυπτογραφικού αλγορίθμου πρέπει να λαμβάνονται υπόψη και τέτοιου τύπου επιθέσεις – κάτι το οποίο δεν φαίνεται ότι συμβαίνει πάντοτε.

Summary

Rapid technological progress has stimulated the production of these solutions which are primarily aimed at improving the quality of human life. One of the technological advancements that have been implemented is the so-called Wireless Sensors Networks (WSN). Sensors are being used in a huge frame of applications; small size, low cost and the independence they offer are their main advantages. Like any device that exchange data so the wireless are using a cryptographic technique to encrypt the transmitting data.

However there are several cryptanalytic techniques that are able to recover the initial message or the secret key. One of these techniques makes use of the energy footprint of a cryptographic device. Such a technique lies in a general class of attacks, namely the so-called side channel attacks. This type of attacks aims at recovering secret information of the devices via simple measurements of physical phenomena, such as their power dissipation. Although side channel attacks can be applied to any cryptographic device in any context, they become extremely dangerous especially to wireless sensor networks.

The aim of this master thesis is to present and highlight all the security issues relating to WSNs; emphasis is given to the side channel attacks, where a specific approach is fully described, via a realistic scenario, to recover the secret key of a contemporary cipher by using the energy fingerprint of a cryptographic device. By this way, we show that such attacks should be always considered when designing a cryptographic algorithm – which unfortunately is not always the case.

Ευχαριστίες

Από του βήματος τούτου, θα ήθελα να ευχαριστήσω των επιβλέποντα καθηγητή μου, κύριο Λιμνιώτη Κωνσταντίνο, για τις παραγωγικές συμβουλές του, αλλά την άρτια καθοδήγηση του, χωρίς την οποία δεν θα ήταν εφικτό να περατωθεί η παρούσα μεταπτυχιακή διατριβή.

Επιπρόσθετα θα ήθελα να ευχαριστήσω την ομάδα των διδασκόντων με τους οποίους είχα την χαρά να συνεργαστώ, τον κ. Γκουμόπουλο, τον κ. Βερύκιο, την κ Ιωάννου, τον κ. Φασουλιώτη, τον κ. Βαζιργιάννη την κ. Κλεάνθους, τον κ. Βασιλείου, τον κ. Γκρίτζαλη και τον επιβλέποντα καθηγητή μου κύριο Λιμνιώτη, χωρίς τους οποίους δεν θα είχα αποκομίσει το πλήθος των γνώσεων που απέκτησα.

Επιπρόσθετα θα ήθελα να ευχαριστήσω την οικογένεια μου και την Μαρία, που με «στερήθηκαν» όλο αυτό το χρονικό διάστημα, αλλά και για την υπομονή και επιμονή που έδειξαν ώστε να περατωθεί ο στόχος που έθεσα.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή.

1 Εισαγωγή.

Η ασφάλεια στις επικοινωνίες είναι μία «εύθραυστη» και σχετική έννοια: συνήθως περιγράφεται με βάση τους στόχους που αυτή καλύπτει, όπως η εμπιστευτικότητα της μεταδιδόμενης πληροφορίας, η ακεραιότητα των δεδομένων και η διαθεσιμότητα των υπηρεσιών. Για την επίτευξη των στόχων αυτών υπάρχει σύνολο διαφορετικών προσεγγίσεων, οι οποίες βασίζονται σε συγκεκριμένους «πυλώνες»: για παράδειγμα, για την εμπιστευτικότητα της μετάδοσης χρησιμοποιείται κρυπτογράφηση δεδομένων, η οποία κρυπτογράφηση μπορεί να γίνει είτε στο φυσικό επίπεδο, είτε στο επίπεδο δικτύου είτε σε επίπεδο εφαρμογής. Προς τούτο, υπάρχει μια πλειάδα σχετικών εμπορικών προϊόντων, που το κάθε ένα καλύπτει ένα πλήθος αναγκών. Ο γνώμονας με τον οποίο πρέπει να γίνεται η επιλογή της αγορά ενός προϊόντος, άπτεται των αναγκών που θα εξυπηρετεί, της ευελιξίας της οποίας μπορεί να προσφέρει αλλά και της πραγματικής ασφάλειας την οποία παρέχει στο σύγχρονο περιβάλλον απειλών.

Ουδείς μπορεί να πει με απόλυτη βεβαιότητα ότι έχει δημιουργηθεί κάποιο σύστημα το οποίοι να παρέχει απόλυτη ασφάλεια. Αυτό το οποίο μπορεί να ειπωθεί όμως με απόλυτη βεβαιότητα είναι ότι, υπάρχουν αρκετά συστήματα τα οποία παρέχουν αυτό το πλήθος παραμετροποιήσεων, ώστε να μετριαστεί ο κίνδυνος μιας ανεπιθύμητης επίθεσης.

Στο λυκαυγές του εικοστού πρώτου αιώνα, μεγάλο μερίδιο της αγοράς καταλαμβάνουν πλέων τα προϊόντα ασύρματης δικτύωσης. Τα προϊόντα ασύρματης δικτύωσης, όπου για τη σχετική τεχνολογία υπάρχει πλέον καταιγισμός ιδεών, αποτελούν ορόσημο για την κατασκευή λύσεων, που θα βελτιώσουν πλήθος τομέων της σύγχρονης ζωής του ανθρώπου, τόσο στην καθημερινότητα του όσο και στο πεδίο της επιστήμης και της ιατρικής (Παρακολούθηση ασθενών, παρακολούθηση περιβάλλοντος πόλεων).

Είναι γεγονός πως η βάση του διαδικτύου αρχίζει να μετακινείται από την παραδοσιακή αρχιτεκτονική, στην λεγόμενη αρχιτεκτονική του λεγόμενου Διαδικτύου των Πραγμάτων (Internet of Things – IoT). Ακρογωνιαίος λίθος στην υλοποίηση αυτού του τύπου αρχιτεκτονικής είναι και τα δίκτυα ασύρματων αισθητήρων (Wireless Sensor Networks - WSN). Ως εκ τούτου, η έννοια της ασφάλειας στις συναφείς τεχνολογίες αποκτά ιδιαίτερη βαρύτητα και σημασία.

Για να μπορέσει να στοιχειοποιηθεί η έννοια της ασφάλειας πρέπει να αναλυθεί και να επεξηγηθεί ένα πλήθος από έννοιες: επίσης θα πρέπει να γίνει μια σαφής ανάλυση ορισμένων από τα βασικά χαρακτηριστικά τα οποία υπάρχουν στα ασύρματα δίκτυα αισθητήρων. Ένα δεύτερο βήμα ανάλυσης το οποίο θα πρέπει να γίνει, είναι αυτό της χρησιμότητας των ασύρματων δικτύων αισθητήρων στο σύγχρονο τρόπο ζωής.

1.1 Εν Δυνάμει Κίνδυνοι.

Όπως αναφέρθηκε πιο πάνω, τα δίκτυα αισθητήρων αποτελούν ακρογωνιαίο τρόπο τεχνολογικής λύσης στο σύγχρονο τεχνοκρατικό τρόπο ζωής. Ωστόσο η αθρόα χρήση τους ελλοχεύει και αρκετούς κινδύνους για την ελευθερία του ατόμου. Ελλοχεύει κινδύνους άρσης της ιδιωτικότητάς του - π.χ. μέσω παρακολούθησης των κινήσεών του («tracking») ή δημιουργίας προφίλ συμπεριφοράς του («profiling»), όπως επίσης και διοχέτευσης προσωπικών δεδομένων σε κοινή χρήση. Στο οικονομικό επίπεδο η διαρροή ευαίσθητων πληροφοριών μπορεί να προκαλέσει ανεπανόρθωτη οικονομική βλάβη σε έναν οργανισμό, ο οποίος δεν έχει λάβει τα απαραίτητα μέτρα για να προστατεύσει τα οικονομικά του συμφέροντα.

Πρέπει να σημειωθεί ότι τα ανωτέρω αποτελούν κινδύνους οι οποίοι είναι παρόντες σχεδόν σε οποιοδήποτε πληροφοριακό σύστημα (δηλ. όχι μόνο σε ασύρματες επικοινωνίες): σε ασύρματα δίκτυα όμως αποκτούν ακόμη μεγαλύτερη σημασία, γιατί οι κίνδυνοι αυτοί είναι πιο εύκολο να πραγματοποιηθούν. Αυτό οφείλεται στο ότι αφενός το ασύρματο μέσο μετάδοσης είναι ακόμα περισσότερο επιρρεπές σε επιθέσεις ασφαλείας – συγκρινόμενο πάντα με οποιοδήποτε ενσύρματο μέσο μετάδοσης – ενώ επίσης και οι κόμβοι ενός τέτοιου δικτύου κατά κανόνα δεν έχουν την υπολογιστική ισχύ

αλλά και τα λοιπά τεχνολογικά χαρακτηριστικά που απαιτούνται προκειμένου να υιοθετηθούν απευθείας οι υπάρχουσες βέλτιστες λύσεις ασφαλείας.

Αντικειμενικός σκοπός είναι η παροχή υπηρεσιών οι οποίες θα ικανοποιούν τις ανάγκες του ανθρώπου, αλλά ταυτόχρονα θα εξασφαλίζουν το μέγιστο δυνατό επίπεδο ασφαλείας. Για να επιτευχθεί η μέγιστη δυνατή ασφάλεια, απαραίτητη προϋπόθεση – μεταξύ άλλων – είναι η κρυπτογράφηση των δεδομένων και την αποστολή τους. Σκοπός αυτής της διαδικασίας είναι να μεταφέρονται τα δεδομένα (τόσο ενσύρματα όσο και ασύρματα) μέσω δημόσιων δικτύων μετάδοσης, χωρίς αυτά να είναι αναγνώσιμα σε μη εξουσιοδοτημένους χρήστες.

1.2 Αντίμετρα Κινδύνων – Χρήση κρυπτογραφίας.

Η κρυπτογραφία είναι μια επιστήμη η οποία αν και έχει αρκετά πρόσφατα αναπτυχθεί, οι ρίζες της προέρχονται από τα βάθη των αιώνων. Σκοπός της είναι να μετατρέψει ένα κείμενο το οποίο είναι σε κανονική μορφή σε μία μορφή η οποία δεν είναι εύκολα κατανοητή από έναν τρίτο ο οποίος δεν είναι εξουσιοδοτημένος χρήστης για τη συγκεκριμένη κρυπτογραφική επικοινωνία. Το κύριο πλεονέκτημα της κρυπτογράφησης είναι η μεταφορά δεδομένων σε ελεύθερο (δηλαδή δημόσιο, και όχι ιδιωτικό) κανάλι μετάδοσης, χωρίς ωστόσο να είναι κατανοητά στο ευρύ κοινό. Για να επιτευχθεί αυτό γίνεται χρήση ορισμένων κρυπτογραφικών αλγορίθμων. Οι αλγόριθμοι αυτοί πραγματοποιούν την μετατροπή του αρχικού κειμένου σε ένα κρυπτοκείμενο με τη βοήθεια ενός μυστικού κλειδιού. Οι κρυπτογραφικοί αλγόριθμοι δεν είναι τίποτα άλλο παρά ένα σύνολο μαθηματικών τεχνικών, με τις οποίες κρυπτογραφούνται τα μηνύματα κατά τρόπο τέτοιο ώστε μόνο όποιος διαθέτει το κλειδί αποκρυπτογράφησης είναι σε θέση να ανακτήσει τα αρχικά μηνύματα. Άρα, με χρήση μαθηματικών τεχνικών, διασφαλίζεται ότι: α) χωρίς γνώση του κλειδιού αποκρυπτογράφησης, δεν είναι εφικτή η αποκρυπτογράφηση, ακόμα και αν ο ίδιος ο κρυπτογραφικός αλγόριθμος που έχει χρησιμοποιηθεί είναι γνωστός, β) το μυστικό κλειδί προστατεύεται κατάλληλα, είναι μη προβλέψιμο, και ανταλλάσσεται με ασφάλεια μεταξύ των συνδιαλεγομένων εξουσιοδοτημένων μελών.

Επιθέσεις (attacks) οι οποίες εφαρμόζονται σε κρυπτογραφικούς αλγορίθμους έχουν ως σκοπό, πάλι με χρήση μαθηματικών τεχνικών, είτε να ανακαλύψουν το μυστικό κλειδί είτε να ανακτήσουν απευθείας το αρχικό μήνυμα. Για παράδειγμα, έχουν υπάρξει επιτυχείς επιθέσεις σε κρυπτογραφικούς αλγορίθμους οι οποίες βασίστηκαν στο ότι δεν είχε καλά χαρακτηριστικά τυχαιότητας η ακολουθία του κλειδιού (κλειδοροή – keystream). Έτσι κλειδοροές οι οποίες έχουν συγκεκριμένα καλά χαρακτηριστικά είναι αναγκαία προϋπόθεση για την ασφάλεια, χωρίς ωστόσο να μπορεί να ειπωθεί με απόλυτη βεβαιότητα ότι αυτό αρκεί για να χαρακτηριστεί ο κρυπτογραφικός αλγόριθμος ως απόλυτα ασφαλής.

Κάθε τεχνική που παραβιάζει την ασφάλεια ενός κρυπτογραφικού αλγορίθμου καλείται κρυπταναλυτική επίθεση ή, απλά, επίθεση.

1.3 Η Έννοια των Επιθέσεων Παράπλευρου Καναλιού.

Με βάση τα όσα αναφέρθηκαν ανωτέρω, το να πλήξει κανείς την ασφάλεια ενός κρυπτογραφικού αλγορίθμου απαιτεί τη χρήση «έξυπνων» μαθηματικών τεχνικών, που θα εκμεταλλευθούν μία παράμετρο που δεν λήφθηκε υπόψη κατά τη σχεδίαση του αλγορίθμου. Ωστόσο, δεν είναι δυστυχώς αυτή η μόνη δυνατότητα που έχει ένας επίδοξος υποκλοπέας. Για παράδειγμα, κάνοντας κανείς απλές φυσικές μετρήσεις (π.χ. κατανάλωση ενέργειας συσκευής που επιτελεί κρυπτογράφηση ή χρόνος εκτέλεσης της κρυπτογράφησης) μπορεί να του επιτρέψει να εξάγει συμπεράσματα για το μυστικό κλειδί της κρυπτογράφησης. Μία τέτοια επίθεση αποκαλείται με τον όρο κρυπτογραφική επίθεση παράπλευρου καναλιού (side channel attack). Ουσιαστικά, οι επιθέσεις αυτές αποτελούν μία ιδιαίτερη κατηγορία επιθέσεων: αποσκοπούν στο να πλήξουν την ασφάλεια ενός κρυπτογραφικού αλγορίθμου όχι εκμεταλλευόμενοι κάποια μαθηματική αδυναμία αυτού, αλλά αξιοποιώντας μετρήσιμα μεγέθη που σχετίζονται με την υλοποίηση και τη λειτουργία του αλγορίθμου. Υπό αυτήν την έννοια, θεωρούνται από πολλούς οι πιο δύσκολα αντιμετωπίσιμες κρυπταναλυτικές επιθέσεις.

Επιθέσεις παράπλευρου καναλιού μπορούν να πραγματοποιηθούν σε οποιοδήποτε τηλεπικοινωνιακό σύστημα – και πράγματι, έχουν καταγραφεί επιτυχείς τέτοιες

επιθέσεις σε διάφορα περιβάλλοντα. Ωστόσο, το πρόβλημα αντιμετώπισης αυτών των επιθέσεων είναι ιδιαίτερα έκδηλο σε ασύρματα δίκτυα ή/και σε δίκτυα αισθητήρων, ακριβώς λόγω των ιδιαίτερων χαρακτηριστικών τους.

1.4 Δομή της Διατριβής.

Η παρούσα μεταπτυχιακή διατριβή ως κύριο στόχο έχει να αναλύσει την ιδιαίτερη κατηγορία επιθέσεων παράπλευρου καναλιού, υπό το πρίσμα κυρίως της μελέτης της ασφάλειας ασύρματων δικτύων αισθητήρων, μιας και τα δίκτυα αυτά τείνουν να είναι πιο ευάλωτα σε τέτοιου είδους προσπάθειες διείσδυσης. Αντικειμενικός σκοπός κατά την διάρκεια της συγγραφής υπήρξε να αποδοθούν οι βασικές έννοιες αλλά και να επεξηγηθούν όλες οι παράμετροι απλά και συνοπτικά, ώστε να είναι εύκολο στον αναγνώστη να αφομοιώσει τις έννοιες οι οποίες συνοδεύουν την ασφάλεια των πληροφοριών. Με γνώμονα τα παραπάνω, η δομή την οποία φέρει η παρούσα μεταπτυχιακή διατριβή είναι η ακόλουθη.

Στο δεύτερο κεφάλαιο αναλύονται οι βασικές έννοιες ασφάλειας τις οποίες θα πρέπει να γνωρίζει ο μελετητής των θεμάτων που άπτονται της ασφάλειας των πληροφοριών, καθώς επίσης και η βασική ορολογία η οποία χρησιμοποιείται για να αποδοθούν οι παράμετροι της ασφάλειας – όπως είναι η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικοποίηση και η μη αποποίηση. Γίνεται αναφορά στις βασικές επιλογές τις οποίες μπορεί να έχει ένας χρήστης ώστε να καταστήσει το σύστημα του ασφαλές. Τέλος αναφέρονται οι παράμετροι και οι τεχνικές που διέπουν κάθε κρυπτογραφική διαδικασία.

Στο τρίτο κεφάλαιο της παρούσας μεταπτυχιακής διατριβής γίνεται μια περιγραφή των συμμετρικών κρυπτογραφικών αλγορίθμων και, ιδίως, των κρυπταλγορίθμων ροής (stream ciphers), λόγω του ότι αποτελούν την κατηγορία αλγορίθμων που συναντάται συχνότερα σε ασύρματα δίκτυα αισθητήρων. Καταδεικνύεται ότι κρίσιμο σχεδιαστικό ζήτημα για τους κρυπταλγόριθμους ροής είναι οι τεχνικές παραγωγής διαφόρων ακολουθιών με καλά χαρακτηριστικά τυχαιότητας για την κρυπτογραφική διαδικασία,

όπου και γίνεται μια εκτενής ανάλυση των δυνατοτήτων και των τεχνικών παραγωγής τυχαίων κλειδοροών.

Στο τέταρτο κεφάλαιο αναλύονται οι πτυχές των επιθέσεων παράπλευρου καναλιού. Όπως θα εξηγηθεί, οι επιθέσεις παράπλευρου καναλιού δεν πραγματοποιούν μαθηματική ανάλυση του υποκείμενου κρυπτογραφικού αλγορίθμου αλλά κάνουν χρήση των παραμέτρων κάποιας πληροφορίας που «εκπέμπεται» και μπορεί να μετρηθεί κατά την κρυπτογραφική λειτουργία. Εξετάζονται όλα τα πιθανά είδη επιθέσεων παράπλευρου καναλιού, καθώς και τρόποι αντιμετώπισής τους.

Στη συνέχεια, στο πέμπτο κεφάλαιο γίνεται μία προσπάθεια να αναλυθούν οι βασικές κατηγορίες των ασύρματων δικτύων αισθητήρων όπως επίσης και να αναφερθούν απλά και περιεκτικά τα χαρακτηριστικά τα οποία διέπουν τα ασύρματα δίκτυα αισθητήρων. Εν συνεχεία αναλύονται οι εφαρμογές στις οποίες γίνεται χρήση δικτύων αισθητήρων. Οι εφαρμογές αυτές τείνουν να καλύπτουν μεγάλο φάσμα της ανθρώπινης δραστηριότητας, από την καθημερινότητα, στην παραγωγική διαδικασία και στις ανάγκες των τεχνικών βιομηχανικής παραγωγής, όπως επίσης και σε εξειδικευμένες και αρκετά πολύπλοκες περιπτώσεις, όπως η χρήση σε στρατιωτικές επιχειρήσεις.

Στο έκτο κεφάλαιο γίνεται μια αναφορά στις επιθέσεις οι οποίες πραγματοποιούνται στα ασύρματα δίκτυα αισθητήρων. Γίνεται ρητή αναφορά στο είδος των επιθέσεων που μπορούν να πραγματοποιηθούν στα δίκτυα αυτά εκμεταλλευόμενες τα ιδιαίτερα χαρακτηριστικά τους. Πέραν αυτών των ειδικών επιθέσεων, επεξηγείται η σημαντικότητα των κρυπτογραφικών επιθέσεων παράπλευρου καναλιού ειδικά σε αυτά τα δίκτυα, κυρίως λόγω του ότι είναι εφικτή η φυσική πρόσβαση στους κόμβους του δικτύου (που επιτρέπει τη λήψη μετρήσεων που χρειάζονται για μία τέτοια επίθεση) αλλά και γιατί οι περιορισμοί σε κατανάλωση ενέργειας, υπολογιστική ισχύ και μνήμη δεν επιτρέπουν την άμεση υιοθέτηση οποιουδήποτε κρυπτογραφικού μηχανισμού.

Στο έβδομο κεφάλαιο πραγματοποιείται μια προσπάθεια υλοποίησης μίας τέτοιας επίθεσης μέσω ανάπτυξης κατάλληλης πειραματικής εφαρμογής που θα επιτυγχάνει επιτυχή κρυπτανάλυση παράπλευρου καναλιού. Σκοπός της είναι να αποδειχθεί πόσο εύκολο είναι να εκμεταλλευθεί κάποιος επίδοξος εισβολέας μία όχι σωστή υλοποίηση του κρυπτογραφικού αλγορίθμου έτσι ώστε να μπορέσει να ανακτήσει το μυστικό κλειδί που

χρησιμοποιήθηκε στη διαδικασία μιας κρυπτογράφησης. Στο πλαίσιο αυτό, επεξηγείται αναλυτικά μία ειδική επίθεση παράπλευρου καναλιού που μπορεί να πραγματοποιηθεί σε συγκεκριμένου τύπου κρυπταλγορίθμους ροής και, ακολούθως, η τεχνική αυτή επίθεσης εφαρμόζεται σε έναν κρυπτογραφικό αλγόριθμο που έχει πρόσφατα προταθεί ως μία καλή εναλλακτική για χρησιμοποίησή του σε ασύρματα δίκτυα αισθητήρων. Με τη χρήση κατάλληλων προγραμμάτων λογισμικού που αναπτύχθηκαν για το σκοπό αυτό, πραγματοποιήθηκε επιτυχής επίθεση στον εν λόγω αλγόριθμο, υπό την υπόθεση ότι ο εισβολέας είναι σε θέση να μετρήσει καταναλώσεις ενέργειας της κρυπτοσυσκευής αυτό (το μοντέλο μετρήσεων καταναλώσεων ενέργειας προσομοιώθηκε κατάλληλα με ειδική εφαρμογή). Περιγράφεται επίσης με ποιον τρόπο ο σχεδιαστής του αλγορίθμου μπορεί να καταστήσει το σύστημα ασφαλές έναντι αυτής της επίθεσης

Τέλος, συμπεράσματα και συζήτηση πάνω σε λοιπά ανοικτά θέματα πραγματοποιείται στο Κεφάλαιο 8.

Κεφάλαιο 2
Βασικές Έννοιες.

2 Βασικές Έννοιες.

Η εξασφάλιση της απρόσκοπτης επικοινωνίας και ανταλλαγής δεδομένων αποτελεί το βασικό επιδιωκόμενο στοιχείο σε οποιοδήποτε δίκτυο επικοινωνίας. Για την απρόσκοπτη επικοινωνία, πέρα των αμιγώς τηλεπικοινωνιακών ζητημάτων (μετάδοση απαλλαγμένη σφαλμάτων που εισάγονται από το θόρυβο του καναλιού, χωρίς καθυστερήσεις κτλ.), ιδιαίτερα κρίσιμα είναι τα ζητήματα που αφορούν την προστασία και την διαθεσιμότητα των πληροφοριών. Ειδική μνημεία, ως παράδειγμα, μπορεί να γίνει σε ευαίσθητα θέματα τα οποία άπτονται στρατιωτικών ή πολιτικών σκοπών και για τα οποία, τυχόν υποκλοπή των δεδομένων θα επιφέρει εξαιρετικά δυσμενείς συνέπειες. Συνεπώς, για να λειτουργεί σωστά και αξιόπιστα ένας οργανισμός, η ασφάλειά του αποτελεί απαραίτητο συστατικό (σε συνδυασμό φυσικά και με λοιπές βασικές παραμέτρους όπως η ποιότητα και η απόδοση).

Προς επίρρωση των παραπάνω, μπορεί κανείς να πει ότι βασικός σκοπός για τον οποίο πραγματοποιείται μία πολιτική ασφάλειας στα δίκτυα, έγκειται στην προσπάθεια ανίχνευσης δραστηριοτήτων, και δη ανεπιθύμητων εντός ενός δικτύου, όπως επίσης και στην εφαρμογή των κατάλληλων μέτρων για την αντιμετώπιση τους. Η έννοια της ασφάλειας στα δίκτυα είναι στενά συνυφασμένη με την πρόληψη, δηλαδή τη λήψη εκ των προτέρων μέτρων, προκειμένου να προληφθούν προβλήματα εντός του δικτύου.

2.1 Βασικές Έννοιες Ασφαλείας.

Θα πρέπει να τονιστεί ότι το σημαντικότερο τμήμα ενός δικτύου τόσο στην σχεδίασή του, όσο και στην υλοποίησή του αποτελεί η ασφάλεια. Το γεγονός αυτό αποτελεί και βασική παράμετρο ώστε τα δίκτυα να κατασκευάζονται με γνώμονα κάποιες προδιαγραφές. Οι προδιαγραφές αυτές θα εγγυώνται την απρόσκοπτη και απροβλημάτιστη λειτουργία του δικτύου, αλλά και τη σφυρηλάτησή του, ώστε να είναι ικανό να αντιμετωπίσει ένα πλήθος πιθανών επιθέσεων -πάντα με γνώμονα τις απαιτήσεις, τις ιδιαιτερότητες, αλλά και τις προδιαγραφές κατασκευής. Οι προδιαγραφές αυτές, οι οποίες καλούνται απαιτήσεις ασφάλειας, αποτελούν τον αρωγό ώστε να επιτευχθεί το υψηλότερο επίπεδο ασφάλειας. Επιχειρώντας κάποιος μία αρχική ταξινόμηση μπορεί να πει ότι αυτές είναι, η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικοποίηση και η μη αποποίηση.

2.1.1 Διαθεσιμότητα.

Προσπαθώντας κανείς να δώσει έναν αρκετά ικανοποιητικό ορισμό της διαθεσιμότητας, θα μπορούσε να πει ότι αναφέρεται στην ιδιότητα ενός αγαθού να είναι διαθέσιμο προς χρήση όταν αυτό ζητείται, από μία εξουσιοδοτημένη οντότητα. Κάνοντας μία πιο εκτενέστερη ανάλυση του ορισμού, μπορεί να ειπωθεί, ότι με τη διαθεσιμότητα, επιδιώκεται τα δεδομένα και οι πληροφορίες να είναι συνεχώς διαθέσιμα. Επίσης απαιτείται οι υπηρεσίες που στηρίζονται πάνω τους, να είναι λειτουργικές, παρά τις όποιες τυχόν διαταραχές, που μπορούν να ανακύψουν, όπως η διακοπή τροφοδοσίας πηγής ενέργειας, οι φυσικές καταστροφές και οι τυχόν επιθέσεις. Στην περίπτωση αυτή μπορεί να ειπωθεί ότι είναι επιθυμητό να αποφεύγονται τυχόν προβλήματα άρνησης υπηρεσίας (Denial of Service - DoS). Αυτό είναι βέλτιστο να αποφεύγεται, ειδικά όταν αιτούνται υπηρεσίες από εξουσιοδοτημένους χρήστες και κόμβους του δικτύου, και στην πιθανότητα που αυτοί ζητούν να προσπελάσουν πόρους του δικτύου (Czarnowski 2014: 4-7).

Η απόδοση των αλγορίθμων δικτύωσης βασίζεται πάνω στη διαθεσιμότητα και την ακρίβεια της κατάστασης της πληροφορίας. Υπάρχουν ωστόσο ειδικές κατηγορίες

δικτύων, όπως τα δίκτυα των αισθητήρων, τα οποία έχουν μία δυναμική φύση που καθιστά τη διαθεσιμότητα εξαιρετικά κρίσιμη, για την οποία πρέπει να ληφθεί ειδική μέριμνα. Οι κόμβοι στα δίκτυα αισθητήρων ενδέχεται να εισέλθουν ή να αποχωρήσουν και οι συνδέσεις να διακοπούν ανά πάσα στιγμή. Ως εκ τούτου, η συντήρηση και η επανίδρυση των δεδομένων της σύνδεσης δυναμικά, αποτελούν τεράστιο πρόβλημα στα ασύρματα δίκτυα αισθητήρων (Gowrishankar 2009: 177-178).

2.1.2 Εμπιστευτικότητα.

Ως εμπιστευτικότητα μπορεί να οριστεί η διαδικασία εκείνη, με την οποία τα κρίσιμα (σημαντικά) δεδομένα είναι δυνατόν, να διακινηθούν μέσα σε ένα δίκτυο, χωρίς να ελλοχεύει ο κίνδυνος αυτά να γνωστοποιηθούν σε μη εξουσιοδοτημένους χρήστες. Αντίθετα, τα δεδομένα που διακινούνται μέσα στο δίκτυο αποκαλύπτονται μόνο σε εξουσιοδοτημένες οντότητες. Τούτο όχι μόνο για την προστασία των δεδομένων από μη εξουσιοδοτημένη αποκάλυψη, αλλά και για να προστατευθεί αυτή καθ' αυτή η ύπαρξή τους εντός του δικτύου (Kumar 2011:.63-64).

Κατά συνέπεια, για κάθε κόμβο ενός δικτύου είναι κρίσιμη η διαφύλαξη των δεδομένων του, δίχως να υπάρχει πιθανότητα κινδύνου αυτά να είναι προσβάσιμα σε γειτονικούς κόμβους. Τούτο γίνεται πασιφανές στην περίπτωση που οι κόμβοι χρησιμοποιούνται για στρατιωτικές εφαρμογές. Για την ειδικότερη δε περίπτωση των δικτύων αισθητήρων (που περιγράφονται σε επόμενο κεφάλαιο), η εμπιστευτικότητα είναι στενά συνυφασμένη με την επικοινωνία που εγκαθίσταται μεταξύ των γειτονικών κόμβων. Για να επιτευχθεί μία ασφαλής επικοινωνία μεταξύ των κόμβων του δικτύου στο πλείστο των περιπτώσεων, γίνεται χρήση κρυπτογραφικών μεθόδων κρυπτογράφηση των δεδομένων με τη χρήση μυστικού κλειδιού κρυπτογράφησης, όπου αποτελεί και τη συνηθέστερη μέθοδο. Η μέθοδος αυτή βασίζεται στο γεγονός ότι το μυστικό κλειδί κρυπτογράφησης θα είναι διαθέσιμο μόνο στους επίδοξους αποδέκτες– παραλήπτες του μηνύματος. Ωστόσο μιας και η χρήση κρυπτογράφησης δημόσιου κλειδιού, αν και αρκετά ασφαλής, είναι αρκετά ενεργοβόρα και κοστοβόρα (όπως εξηγείται στη συνέχεια), έως τώρα γίνεται χρήση πρωτοκόλλων κρυπτογράφησης τα οποία χρησιμοποιούν μεθόδους συμμετρικού κλειδιού.

2.1.3 Ακεραιότητα.

Κάνοντας μία προσπάθεια να γίνει μία εισαγωγική τοποθέτηση στον ορισμό της ακεραιότητας, μπορεί να πει κανείς ότι γίνεται λόγος για την ουσιαστική επιβεβαίωση των δεδομένων, που είτε έχουν αποσταλεί, είτε παραληφθεί, ή έχουν αποθηκευτεί, δηλαδή να διασφαλίζεται ότι δεν έχουν κατά οποιονδήποτε τρόπο υποστεί τροποποίηση– αλλοίωση. Ουσιαστικά μπορεί να ειπωθεί ότι δεν πρέπει να υπάρχει διαφοροποίηση των δεδομένων από τον εισβολέα κατά τη μετάδοσή τους στον παραλήπτη (Kumar 2011:.63-64).

Για να επιτευχθεί μια σύνοδος μεταξύ δύο μερών τα οποία την επιθυμούν, θα πρέπει συνεπώς, κατά το ελάχιστο, να πληρούν το κριτήριο της ακεραιότητας. Όπως και για την εμπιστευτικότητα, και για τη διασφάλιση της ακεραιότητας αναμένεται να γίνει χρήση κατάλληλων μηχανισμών κρυπτογράφησης. Σαφώς και δεν είναι αναγκαίο να επικεντρωνόμαστε μόνο στην επικοινωνία των δύο μελών. Τούτο γιατί θα πρέπει να αναλογιστεί κανείς το μέγεθος του προβλήματος που θα δημιουργηθεί αν κατά την υποκλοπή προστεθούν επιπλέον κομμάτια ή διαγραφούν τμήματα. Για παράδειγμα, η τροποποίηση της διεύθυνσης του παραλήπτη, αποτελεί ένα σημαντικό πρόβλημα. Από τα παραπάνω, μπορεί να γίνει εύκολα αντιληπτό ότι πρέπει να αντιμετωπιστεί ένα ζήτημα το οποίο έχει πολύπλευρες διαστάσεις. Επιπρόσθετα πρέπει να γίνει αναφορά στο γεγονός ότι, η αλλοίωση των δεδομένων δεν μπορεί να επιτευχθεί μόνο από ένα επίδοξο υποκλοπέα, αλλά μπορεί να προκληθεί και από μη βέλτιστες συνθήκες επικοινωνίας οι οποίες μπορεί να άπτονται σε φυσικούς περιορισμούς.

Από τα παραπάνω μπορεί να γίνει αντιληπτό ότι για να χαρακτηριστεί ένα σύστημα ως ασφαλές, θα πρέπει να είναι ικανό να διαπιστώσει οποιοδήποτε πρόβλημα ακεραιότητας προκύψει. Εν κατακλείδι μπορεί να ειπωθεί ότι ο τακτικός έλεγχος ακεραιότητας παρέχει τα εχέγγυα, πως καμία μεταβολή δεν έχει προκληθεί στα δεδομένα και ότι αυτά παραδόθηκαν στον προορισμό τους χωρίς καμία τροποποίηση.

2.1.4 Αυθεντικοποίηση.

Η μέχρι τώρα ανάλυση έκανε λόγο για την ανάγκη που υπάρχει να διασφαλιστεί ότι τα δεδομένα θα μεταδοθούν με ορθό τρόπο από τον αποστολέα πληρώντας το κριτήριο της εμπιστευτικότητας. Έκανε λόγο επίσης, ότι τα δεδομένα πρέπει να είναι αναγνώσιμα μόνο από τον παραλήπτη, πληρώντας το κριτήριο, πέραν της εμπιστευτικότητας, και της ακεραιότητας.

Αυτό το οποίο στερείται η παρούσα ανάλυση είναι η εξέταση του πιθανού σεναρίου τα δεδομένα που αποστέλλονται να μην προέρχονται πράγματι από την πηγή που ο παραλήπτης τους πιστεύει. Με την διαδικασία της αυθεντικοποίησης απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση εντός ενός δικτύου, ενώ ταυτόχρονα γίνεται επιτρεπτό στους υπόλοιπους κόμβους να ανιχνεύσουν, εάν και κατά πόσο τα πακέτα προέρχονται από τον πραγματικό αποστολέα ή κάποιον κακόβουλο αποστολέα – οπότε και, στην περίπτωση αυτή, θα πρέπει να τα απορρίψουν. Ως εκ τούτου, μπορεί να ειπωθεί, ότι η αυθεντικοποίηση αποτελεί σημαντικό συστατικό στοιχείο και αποτελεί απαραίτητο τμήμα για πολλούς εκτελεστικούς σκοπούς, όπως τον εκ νέου προγραμματισμού του δικτύου, ή τον έλεγχο ασφάλειας σε ένα κόμβο και ούτω καθ' εξής (Kumar 2011:.63-64).

Στην διαδικασία της επικοινωνίας δύο μερών, η αυθεντικοποίηση είναι δυνατό να επιτευχθεί με έναν αμφίπλευρο μηχανισμό πιστοποίησης ταυτότητας. Κατά την έναρξη της επικοινωνίας ανάμεσα σε δύο κόμβους πραγματοποιείται μία αυθεντικοποίηση της ταυτότητας των συνομιλητών. Εν συνεχεία ακολουθεί ένας επιπρόσθετος έλεγχος προκειμένου να διαπιστωθεί κατά πόσο δεν υπάρχει ενδιάμεσος τρίτος χρήστης, ο οποίος έχει ως σκοπό να υποκλέψει τα δεδομένα τα οποία ανταλλάσσονται μεταξύ των δύο πλευρών που έχουν εγκαταστήσει επικοινωνία. Στην περίπτωση αυτή τόσο ο αποστολέας όσο και ο παραλήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο γίνεται ο υπολογισμός του λεγόμενου κώδικα αυθνετικοποίησης του μηνύματος (Message Authentication Code - MAC) για να αποστείλουν τα δεδομένα. Όταν το μήνυμα φτάσει στον παραλήπτη με το σωστό MAC, τότε ο λήπτης θα είναι σε θέση να αποφανθεί ότι αυτό στάλθηκε από τον σωστό αποστολέα.

2.1.5 Μη Αποποίηση.

Θέτοντας τον ορισμό της μη αποποίησης, μπορεί στο γενικό του πλαίσιο να ειπωθεί ότι γίνεται λόγος, για μία υπηρεσία η οποία παρέχει αυτού του τύπου τις αποδείξεις που επιβεβαιώνουν την ακεραιότητα αλλά και την ταυτότητα προέλευσης των δεδομένων. Αποτελεί σημαντική παράμετρο ασφαλείας να μπορεί να αποδειχθεί η πατρότητα αποστολής ενός μηνύματος και να πιστωθεί σε κάποιον χρήστη η ιδιοκτησία του. Με απλά λόγια, αν ένα μήνυμα πιστοποιηθεί ως γνήσιο σε κάποιο στάδιο της επικοινωνίας, δεν θα πρέπει να μπορεί ο αποστολέας του μελλοντικά να μπορεί να αποποιηθεί ότι το έστειλε (Gowrishankar 2009: 177-178).

Ειδικά στο πεδίο της ασύρματης δικτύωσης τούτο είναι αρκετά χρήσιμο, μιας και παρέχεται η δυνατότητα να απομονωθούν κόμβοι που έχουν εκτεθεί σε ορισμένης μορφής κίνδυνο. Ως τρόπο αντιμετώπισης των προβλημάτων μη αποποίησης, μπορεί να προτείνει κανείς την χρήση ψηφιακών υπογραφών: με την τεχνική αυτή γίνεται αρκετά δύσκολο να αποποιηθεί κανείς την πατρότητα ενός κειμένου, Μιας και η ψηφιακή υπογραφή αποτελεί στοιχείο το οποίο βρίσκεται στην αποκλειστική και μόνο κατοχή του αποστολέα.

2.2 Επιλογές Ασφαλείας.

Για να επιτευχθεί η μέγιστη δυνατή ασφάλεια σε ένα δίκτυο γίνεται χρήση όχι μίας και μόνο μεθόδου ασφαλείας, αλλά μίας υβριδικής διάταξης ασφαλείας. Με τον όρο υβριδική ασφάλεια, νοείται η χρήση δύο ή περισσότερων μεθόδων οι οποίες σε ένα πλαίσιο αγαστής συνεργασίας είναι σε θέση να προασπίσουν ένα δίκτυο, ανεξάρτητου του μεγέθους το οποίο αυτό καλύπτει.

Η υιοθέτηση του μοντέλου αυτού είναι συνειδητή μιας και επιτυγχάνεται με αυτόν τον τρόπο ένα δεύτερο ή και τρίτο επίπεδο ασφάλειας και ούτω καθ' εξής. Η φιλοσοφία κατασκευής βασίζεται στην υπόθεση ότι, ακόμα και αν πληγεί ένα επίπεδο ασφαλείας, θα υπάρχει ένα επιπρόσθετο επίπεδο ασφάλειας αμέσως μετά. Για να επιτευχθεί όμως η βέλτιστη πολιτική ασφάλειας θα πρέπει να τεθούν ορισμένες προδιαγραφές. Οι

προδιαγραφές αυτές επιτάσσουν ότι το δίκτυο θα πρέπει να είναι σε θέση να προστατεύσει τον εαυτό του τόσο από εξωτερικές όσο και από εσωτερικές απειλές – και τούτο γιατί δεν μπορεί να προεξοφλήσει κανείς ότι οι απειλές θα προέρχονται μόνο από εξωγενείς παράγοντες.

Επιπρόσθετα θα πρέπει να γίνεται σαφές ότι η κάθε πληροφορία η οποία διακινείται μέσα στο δίκτυο θα πρέπει να χαρακτηρίζεται ως άκρως διαφυλασσόμενη. Τα δεδομένα τα οποία διακινούνται και αποθηκεύονται εντός του δικτύου πρέπει να θεωρούνται εξασφαλισμένα. Επιπρόσθετα η πολιτική πρόσβασης σε αυτά θα πρέπει να επιβάλει ότι η δυνατότητα επεξεργασίας και πρόσβασης σε αυτά θα πρέπει να κατέχεται μόνο από εξουσιοδοτημένους χρήστες.

Εάν και εφόσον κάποιος χρήστης εκδηλώσει το ενδιαφέρον να αποκτήσει πρόσβαση σε δεδομένα του δικτυακού χώρου τότε θα πρέπει να υπάρξει ένας προκαταρκτικός έλεγχος, δηλαδή μια πιστοποίηση, ότι ο αιτούμενος έχει την απαραίτητη εξουσιοδότηση να προσπελάσει τα δεδομένα. Σε διαφορετική περίπτωση, εφόσον ο προκαταρτικός έλεγχος διαπιστώσει την μη ύπαρξη δικαιωμάτων πρόσβασης, τότε η πρόσβαση θα πρέπει να απορρίπτεται.

2.3 Τρόποι Ασφάλειας Δικτύων.

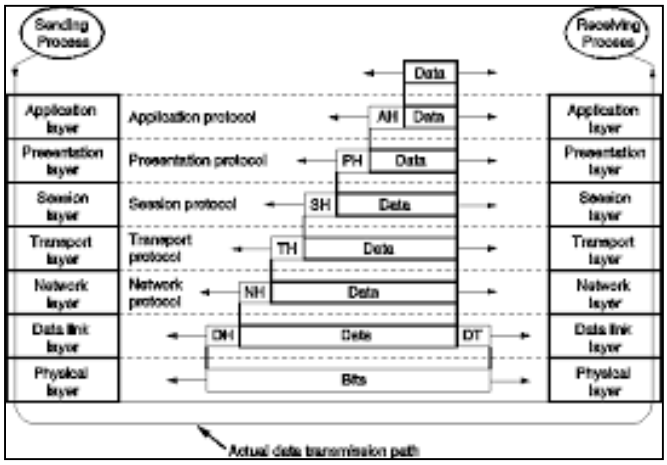
Για να γίνει επίτευξη των απαιτήσεων για συστήματα με υψηλό δείκτη ασφαλείας, ένα πρώτο χαρακτηριστικό το οποίο θα πρέπει να λαμβάνεται σοβαρά υπόψη από τους μηχανικούς σχεδίασης συστημάτων ασφαλείας είναι η παράλληλη συμπόρευση των στόχων που πρέπει να καλύπτει το δίκτυο και των στόχων ασφαλείας που θα πρέπει να πληροί.

Πλήθος επιθέσεων πραγματοποιούνται σε κάθε είδους δίκτυα (π.χ. σε κινητά ad-hoc δίκτυα, όσο και σε δίκτυα τα οποία έχουν άμεση σχέση και σύνδεση με το Διαδίκτυο κτλ.). Υπάρχει ένα πλήθος τεχνικών και μηχανισμών που έχουν αναπτυχθεί για να προλαμβάνουν ή/και να τις αντιμετωπίζουν, λαμβάνοντας υπόψη ότι η πλήρης εξάλειψη της πραγματοποίησης επιθέσεων ασφαλείας αποτελεί μη ρεαλιστικό στόχο. Σε κάθε

περίπτωση, για την επίτευξη του συγκεκριμένου στόχου, σαφώς και δεν μπορεί να γίνει χρήση μίας μόνο μεθόδου ή ενός μόνου εργαλείου, αλλά χρήση ενός μείγματος μεθόδων και εργαλείων. Το μείγμα αυτό μπορεί να περιέχει διάφορα χαρακτηριστικά, κάποια εκ των οποίων περιγράφονται συνοπτικά στη συνέχεια.

2.3.1 Τείχος Προστασίας.

Ως τείχη προστασίας (firewall) μπορούν να οριστούν διαδικτυακές συσκευές και λογισμικά τα οποία επιβάλουν την πολιτική ασφάλειας ενός οργανισμού. Οι μέθοδοι αυτοί φιλτράρουν την κίνηση δεδομένων σε ένα ή περισσότερα από τα επίπεδα του μοντέλου δικτύωσης OSI, συνηθέστερα όμως έχουν εφαρμογή στα επίπεδα εφαρμογών μεταφοράς και δικτύων (Ingram, Forrest 2002: 1-5).



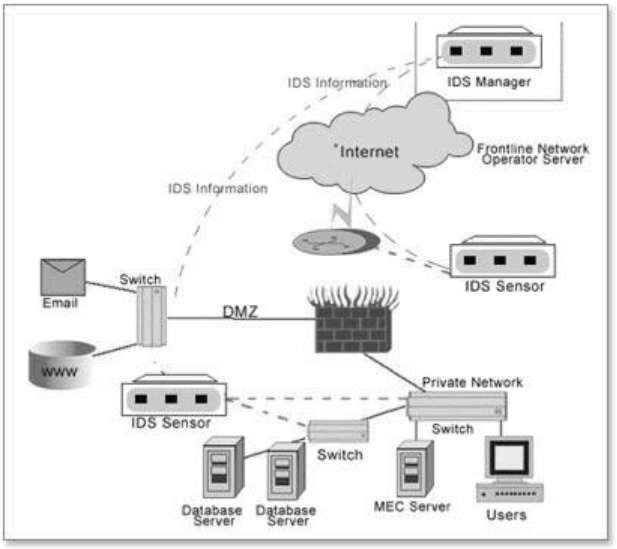
Εικόνα 1.Μοντέλο OSI

Η βασική ιδέα είναι η κατασκευή ενός «τείχους» οποίο θα περιορίζει τους εισβολείς εκτός του χώρου προστασίας του, κάτι εφάμιλλο δηλαδή με το μεγάλο Σινικό τείχος που κατασκευάστηκε από τους κινέζους αυτοκράτορες για να περιορίζουν τους εχθρούς έξω από τα όρια της αυτοκρατορίας τους. Η πολιτική ασφάλειας αποτελείται από ένα πλήθος από κανόνες οι οποίοι έχουν υλοποιηθεί με τη χρήση προγραμματισμού σε γλώσσες υψηλού επιπέδου. Εφόσον η πολιτική ασφαλείας έχει καθοριστεί και προγραμματιστεί, αντικειμενικός στόχος του τοίχους προστασίας είναι να ελέγξει και να διαπιστώσει αν η πολιτική ασφάλειας και οι περιορισμοί της έχουν υλοποιηθεί με ορθό τρόπο. Τούτο γιατί

ορισμένα δεδομένα θα πρέπει να διαπεράσουν το δίκτυο μέσω του τείχους προστασίας μιας και το προστατευόμενο δίκτυο δεν θα πρέπει να είναι πλήρως απομονωμένο αλλά προστατευμένο και χρήσιμο.

2.3.2 Συστήματα Ανίχνευσης Εισβολέων.

Η ανίχνευση εισβολέων (Intrusion detection) είναι η διαδικασία παρακολούθησης των γεγονότων που συμβαίνουν σε ένα σύστημα ηλεκτρονικού υπολογιστή, ή σε ένα δίκτυο, καθώς επίσης και η ανάλυσή τους, για τυχόν ενδείξεις "γεγονότων μη αποδεκτής πρόσβασης" ή επαπειλούμενης παραβίασης των πολιτικών ασφαλείας.



Εικόνα 2. Γενικό μοντέλο ανίχνευσης εισβολών.

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection System - IDS) είναι λογισμικά τα οποία αυτοματοποιούν τη διαδικασία ανίχνευσης απειλών. Επίσης έχουν τις δυνατότητες να σταματήσουν τις επιθέσεις που ανιχνεύουν. Κύριος προσανατολισμός είναι η αναγνώριση πιθανών απειλών, δηλαδή εάν ένα IDS ή ένα IDPS (Intrusion Detection Protection System) είναι σε θέση να ανιχνεύσει αν ένας επιτιθέμενος έχει επιτυχημένα θέσει σε κίνδυνο ένα σύστημα με την ανακάλυψη μιας ευπάθειας (Vulnerability) του συστήματος. Η ανακάλυψη της ευπάθειας αυτής θα επισημανθεί τους

διαχειριστές του συστήματος οι οποίοι με την σειρά τους θα κάνουν όλες τις απαραίτητες ενέργειες για τον περιορισμό των πιθανών αρνητικών συνεπειών- αποτελεσμάτων.

Επιπρόσθετα σε πολλά συστήματα ανίχνευσης απειλών δίνεται η δυνατότητα της διαμόρφωσης ώστε να αναγνωρίζουν παραβιάσεις σε πολιτικές ασφαλείας. Επιπρόσθετα έχουν τη δυνατότητα να αναγνωρίσουν δραστηριότητες, οι οποίες μπορεί να υποδεικνύουν ότι μία επίθεση βρίσκεται σε εξέλιξη. Μιας και οι δραστηριότητες αναγνώρισης είναι συνηθέστερες στο διαδίκτυο, η ανίχνευση αναγνωρίσεων συχνά διενεργείται, πρωτίστως, για την προστασία των εσωτερικών δικτύων, όπως αυτό ενός ασύρματου δικτύου αισθητήρων (Scarfone, Mell, 2007: 19-21).

2.4 Κρυπτογραφία – Συστήματα Κρυπτογράφησης.

Με τον όρο κρυπτογραφία αναφερόμαστε στο σύνολο τεχνικών οι οποίες μελετούν και υλοποιούν τον τρόπο με τον οποίο ένα μήνυμα θα λάβει μορφή ακατάληπτη για τον μη εξουσιοδοτημένο αναγνώστη.

Στις σύγχρονες μορφές κρυπτογραφίας ακολουθείται ο κανόνας του Kerchcoff. Ο κανόνας αυτός προστάζει ότι η δύναμη του αλγορίθμου κρυπτογράφησης και κατ' επέκταση η ασφάλειά του, θα πρέπει να βασίζεται αποκλειστικά μόνο στο μυστικό του κλειδί (δηλαδή οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι γνωστοί, χωρίς να υπάρχει απαίτηση να μένουν κρυφοί). Αν και τούτο δε μας προσδίδει απόλυτη ασφάλεια, μιας και ουδείς μπορεί να εγγυηθεί ότι η διαρροή μέρος του κλειδιού ή του αρχικού κειμένου δεν θα αποκαλύψει το μήνυμα– συνεπώς, οι κρυπτογραφικοί αλγόριθμοι θα πρέπει να σχεδιάζονται με τέτοιο τρόπο ώστε, παρόλο που η κρυπτογραφική τους λειτουργία (στην οποία υπεισέρχεται ένα μυστικό κλειδί) είναι πλήρως γνωστή, εν τούτοις η μη γνώση του κλειδιού θα πρέπει να είναι αρκετή για να μην είναι δυνατή η ανάκτηση του αρχικού μηνύματος

Μπορούμε να πούμε ότι οι ορισμοί των Katz και Lindell, αποτελούν πιο σαφή προσέγγιση της κρυπτογράφησης. Οι ορισμοί αυτοί διατυπώνουν ότι ένας αλγόριθμος θεωρείται ασφαλής αν κανείς άλλος, πλην των ατόμων που έχουν εξουσιοδότηση, δεν μπορεί να

υπολογίσει οποιαδήποτε μορφή του αρχικού κειμένου από οποιαδήποτε ζεύγος αρχικού κειμένου και κρυπτογραφημένου κειμένου, ή μόνο κρυπτογραφημένου κείμενου, όση υπολογιστική ισχύ και αν έχει στην κατοχή του (Πατσάκης, Φούντας, 2009: 99-101).

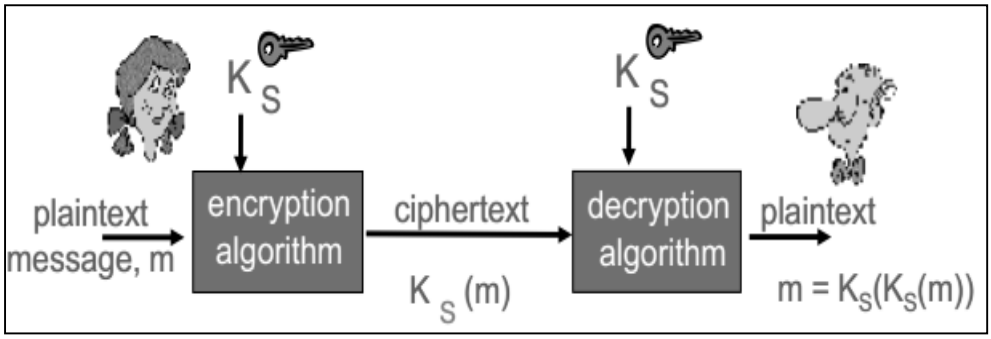
Η σημασία της κρυπτογράφησης έχει υπάρξει ένα αρκετά σημαντικό στοιχείο στο ρου της ανθρώπινης επικοινωνίας, ειδικότερα δε μετά την εφεύρεση του τηλέγραφου αλλά και του ραδιοφωνικού τηλεγραφικού σήματος. Τούτο γιατί η τηλεπικοινωνία επιτρέπει την υποκλοπή του σήματος με πολύ πιο εύκολο τρόπο από ό,τι γινόταν στο παρελθόν. Για να προστατευτεί η εμπιστευτικότητα των τηλεπικοινωνιών, ιδίως δε σε στρατιωτικές, διπλωματικές και άλλου είδους ευαίσθητης υπηρεσίες, γίνεται κατά κόρον χρήση της κρυπτογράφησης. Αναπόφευκτα, στο πλαίσιο διερεύνησης ευπαθειών σε κρυπτογραφικούς αλγορίθμους, αναπτύχθηκαν και βελτιώνονται συνεχώς οι κρυπταναλυτικές τεχνικές, δηλαδή οι τεχνικές που αποσκοπούν στο να πλήξουν την ασφάλεια που παρέχουν οι κρυπτογραφικοί αλγόριθμοι.

Κάνοντας μία μικρή ιστορική αναδρομή μπορεί να υπενθυμίσει κανείς ότι κατά τη διάρκεια του δεύτερού παγκοσμίου πολέμου, τόσο ο γερμανικός κώδικας Enigma, όσο και ο ιαπωνικός "Μωβ κώδικας" (purple code) αποκαλύφθηκαν (δηλαδή υπέστησαν επιτυχή κρυπτανάλυση) από τις συμμαχικές δυνάμεις, και αυτό διαδραμάτισε σημαντικό ρόλο στην εξέλιξη του Β’ παγκοσμίου πολέμου (Van Brussel 2008: 8-12).

Η σύγχρονη κρυπτογραφία έχει αναπτυχθεί με τέτοιο τρόπο, ώστε να προστατεύει όχι μόνο την εμπιστευτικότητα, αλλά και την ακεραιότητα της πληροφορίας, ενώ επίσης μέσω της κρυπτογραφίας παρέχεται και η δυνατότητα της αυθεντικοποίησης.

2.4.1 Κρυπτογράφηση Συμμετρικού Κλειδιού.

Στη σύγχρονη κρυπτογραφία, οι αλγόριθμοι συμμετρικού κλειδιού είναι ουσιώδεις για την προστασία της εμπιστευτικότητας των πληροφοριών.



Εικόνα 3. Συμμετρική Κρυπτογράφηση.

Το ερώτημα το οποίο γεννάται είναι πώς λειτουργεί η κρυπτογραφία συμμετρικού κλειδιού. Στην περίπτωση αυτή, πρέπει να αναφερθεί ότι τα δύο μέρη της επικοινωνίας, τόσο ο αποστολέας όσο και ο παραλήπτης για να ανταλλάξουν το μήνυμα κρυπτογραφημένο, έτσι ώστε ο παραλήπτης να μπορεί να το αποκρυπτογραφήσει (δηλ. να το ανακτήσει στην αρχική του μορφή) τους θα πρέπει έχουν προσυμφωνήσει για το μυστικό κλειδί το οποίο θα χρησιμοποιηθεί κατά την διάρκεια της κρυπτογράφησης και αποκρυπτογράφησης. Το κλειδί αυτό θα πρέπει να είναι εις γνώσιν μόνο αυτών των δύο – συνεπώς είναι κρίσιμο ζήτημα η ασφαλής ανταλλαγή ή προ-συμφωνία του κλειδιού αυτού. Κατά την διαδικασία της κρυπτογράφησης, ο αποστολέας κρυπτογραφεί το μυστικό κείμενο (Plaintext) με ένα αλγόριθμο κρυπτογράφησης και το κλειδί της κρυπτογράφησης για να δημιουργήσει το κρυπτοκείμενο (Ciphertext). Το κρυπτοκείμενο μεταδίδεται πάνω σε ένα μέσο μετάδοσης, που στις περισσότερες φορές είναι μη ασφαλές. Ο παραλήπτης αποκρυπτογραφεί το μυστικό κείμενο ώστε να ανακτήσει το αρχικό μήνυμα. Ένας επιτιθέμενος ή ένας αντίπαλος είναι και σε αυτήν την περίπτωση σε θέση να υποκλέψει (δηλαδή να παρακολουθήσει και να καταγράψει) το κρυπτοκείμενο. Ωστόσο δεν θα είναι εύκολο να αποκρυπτογραφήσει το κείμενο λόγω του γεγονότος ότι δεν θα έχει επίγνωση του μυστικού κλειδιού κρυπτογράφησης.

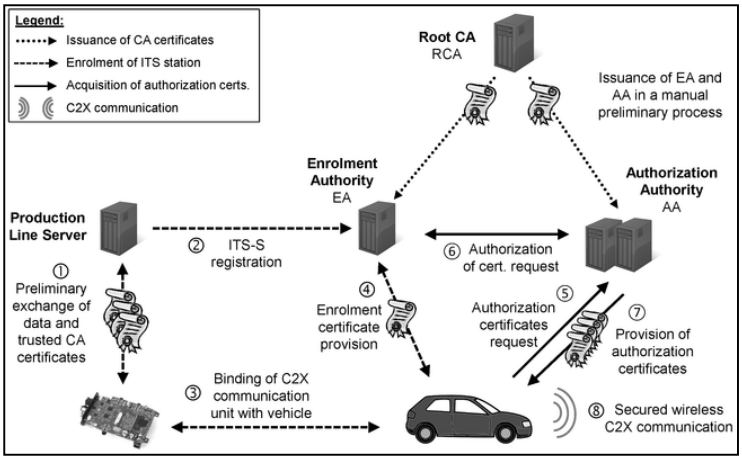
Οι βασικές αρχές που διέπουν τη λειτουργία των συμμετρικών αλγορίθμων κρυπτογράφησης είναι οι έννοιες της αντικατάστασης και της αντιμετάθεσης. Γνωστοί αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού είναι ο 3DES (βελτίωση του παλαιότερου πρότυπου κρυπτογράφησης DES), ο AES (το νέο πρότυπο κρυπτογράφησης) κ.α.

Προσπαθώντας να γίνει ένας απολογισμός των πλεονεκτημάτων και των μειονεκτημάτων των συμμετρικών αλγόριθμων κρυπτογράφησης μπορεί να ειπωθεί ότι είναι ένας μηχανισμός κρυπτογράφησης ο οποίος είναι αρκετά απλός και αρκετά γρήγορος, σε αυτό το βαθμό που τείνει να είναι 1.000 έως 10.000 φορές ταχύτερος από τους ασύμμετρους κρυπτογραφικούς αλγορίθμους (που περιγράφονται στη συνέχεια). Στον αντίποδα των παραπάνω, ως μειονεκτήματα μπορούν να πιστωθούν: Α) το γεγονός ότι πρέπει να πραγματοποιηθεί ένα προσύμφωνο για το κλειδί το οποίο θα πρέπει να χρησιμοποιηθεί από τα δυο μέρη για την μεταξύ τους κρυπτογράφηση. Β) Απόρροια του παραπάνω μειονεκτήματος είναι ο τρόπος και η μεθοδολογία την οποία πρέπει να χρησιμοποιήσουν τα δύο μέρη ώστε να ανταλλάξουν με ασφάλεια το κλειδί κρυπτογράφησης μεταξύ τους. Τούτο αποτελεί ύψιστης σημασίας παράμετρο μιας και οποιοσδήποτε μπορεί να ισχυριστεί ότι είναι ο εξουσιοδοτημένος παραλήπτης ενός μηνύματος και να συμφωνήσει με τον αποστολέα για το μυστικό κλειδί. Έτσι θα είναι σε θέση να λάβει μηνύματα τα οποία δεν προορίζονται για αυτόν και να λάβει πληροφορίες για τις οποίες δεν έχει εξουσιοδότηση να δει.

2.4.2 Κρυπτογράφηση Δημοσίου Κλειδιού.

Τα ερωτήματα τα οποία θέτει η προηγούμενη ενότητα βρίσκουν εν μέρει απάντηση στις γραμμές της παρούσας ενότητας. Το βασικό πρόβλημα στην κρυπτογραφία συμμετρικού κλειδιού, όπως ειπώθηκε, είναι ο τρόπος με τον οποίο θα γίνει η ανταλλαγή του μυστικού κλειδιού κρυπτογράφησης στους συμμετέχοντας. Το πρόβλημα αυτό έρχεται να επιλυθεί με την μέθοδο κρυπτογραφίας δημοσίου κλειδιού ή, ισοδύναμα, ασύμμετρης κρυπτογράφησης.

Γενικότερα, με μία υποδομή δημόσιου κλειδιού (Public Key Infrastructure - PKI) που θα είναι σε θέση να υποστηρίξει την εγκαθίδρυση κατάλληλων πρωτοκόλλων και μηχανισμών, δύο μέρη μπορούν να μοιράζονται ένα μυστικό κλειδί και να διενεργούν κρυπτογράφηση συμμετρικού κλειδιού με ένα αρκετά εύκολο τρόπο (Van Brussel 2008: 21-25).



Εικόνα 4. Παράδειγμα λειτουργιών μιας υποδομής PKI.

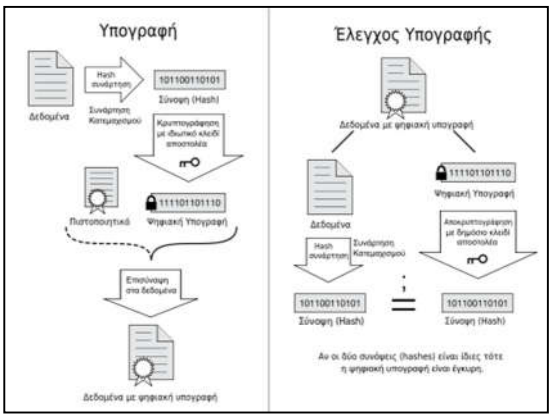
Η κρυπτογράφηση δημόσιου κλειδιού είναι μια αρκετά σημαντική διαδικασία για την μετάδοση μυστικών πληροφοριών. Κατά την διαδικασία της κρυπτογράφησης δημοσίου κλειδιού γίνεται χρήση δύο τύπων κλειδιών, ενός δημοσίου και ενός ιδιωτικού. Το δημόσιο κλειδί ενός χρήστη είναι γνωστό σε όλους, ενώ το ιδιωτικό του κλειδί είναι γνωστό μονό στον κάτοχό του. Τα δύο κλειδιά έχουν την ικανότητα αυτό-αντιστροφής, δηλαδή αν κρυπτογραφηθεί ένα μήνυμα με το δημόσιο κλειδί ενός χρήστη, τότε αποκρυπτογράφηση αυτού με το ιδιωτικό θα επιστρέψει το αρχικό μήνυμα. Έτσι, η κρυπτογράφηση του αρχικού κειμένου πραγματοποιείται με το δημόσιο κλειδί του παραλήπτη, ενώ η αποκρυπτογράφηση του με το ιδιωτικό του κλειδί. Κρίσιμο θέμα για την ασφάλεια των αλγορίθμων αυτής της κατηγορίας είναι το ότι η γνώση του δημόσιου κλειδιού δεν πρέπει να επιτρέπει τον υπολογισμό του ιδιωτικού κλειδιού. Αλγόριθμοι οι οποίοι υλοποιούν κρυπτογράφηση δημοσίου κλειδιού είναι ο RSA (Rivest-Shamir-Adleman algorithm), ο Diffie-Helman κ.α. Για να διασφαλιστεί ότι ο επιτιθέμενος ή ο αντίπαλος δεν θα λάβουν οποιαδήποτε μορφή πληροφορίας από την διαρροή, ισχυροί αλγόριθμοι και ισχυρά κλειδιά θα πρέπει να χρησιμοποιηθούν για την κρυπτογράφηση (Van Brussel 2008: 22).

Όπως κάθε μέθοδος, έτσι και η κρυπτογραφική μέθοδος δημοσίου κλειδιού έχει τα πλεονεκτήματα και τα μειονεκτήματά της. Στα μειονεκτήματά της μπορούν να λογιστούν η τεράστια καθυστέρηση η οποία παρατηρείται στην κρυπτογραφική διαδικασία, η σχετική ευπάθεια που παρατηρείται σε επιθέσεις γνώσης μέρους του κρυπτοκειμένου

(known ciphertext attack), αλλά και προβλήματα εμπιστοσύνης που υπάρχουν ως προς τη γνησιότητα του δημοσίου κλειδιού. Αντίθετα με τα παραπάνω, στα θετικά χαρακτηριστικά της μεθόδου δημοσίου κλειδιού μπορούν να πιστωθούν η επίλυση του προβλήματος του διαμοιρασμού του κλειδιού μεταξύ αποστολέα και παραλήπτη (δεν απαιτείται η προ-συμφωνία για κάποιο κλειδί). Επιπρόσθετα επιτρέπεται η δημιουργία πλαισίου εμπιστοσύνης μεταξύ των μερών. Σε κάθε περίπτωση, οι καθυστερήσεις που εισάγει η κρυπτογράφηση δημοσίου κλειδιού είναι και ο λόγος που δεν χρησιμοποιείται στα τηλεπικοινωνιακά δίκτυα για την ανταλλαγή πληροφοριών (πολύ δε περισσότερο δεν χρησιμοποιείται σε ασύρματα δίκτυα): ωστόσο, επιλύει σε πολλές περιπτώσεις το πρόβλημα ασφαλούς ανταλλαγής του συμμετρικού κλειδιού κρυπτογράφησης.

2.4.3 Ψηφιακές Υπογραφές.

Η ψηφιακή υπογραφή είναι μια μεθοδολογία η οποία κάνει χρήση κατάλληλων μαθηματικών τεχνικών ι για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Η ψηφιακή υπογραφή παρέχει στον παραλήπτη του μηνύματος ή εγγράφου την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα. Το απεσταλμένο μήνυμα έχει υπογραφεί ψηφιακά και αυτό πιστοποιεί ότι δεν αλλοιώθηκε/παραποιήθηκε κατά την μεταφορά του προς τον παραλήπτη.



Εικόνα 5. Ψηφιακή Υπογραφή

Οι ψηφιακές υπογραφές κάνουν ένα συνδυασμό μιας κρυπτογραφικής συνάρτησης κατακερματισμού (hash function) για δημιουργία της λεγόμενης σύνοψης του μηνύματος

(hash). Η έννοια της συνάρτησης κατακερματισμού και της σύνοψης εκφεύγει του αντικειμένου της παρούσας διατριβής – θα αναφέρουμε απλά ότι η σύνοψη ενός μηνύματος είναι μοναδική για το μήνυμα, μη αντιστρεπτή (δηλαδή γνωρίζοντας τη σύνοψη ενός μηνύματος δεν μπορούμε να ανακτήσουμε το αρχικό μήνυμα), καθώς επίσης και ότι δεν μπορούμε να βρούμε δύο διαφορετικά μηνύματα με την ίδια σύνοψη. Το αποτέλεσμα της σύνοψης σε συνδυασμό με κατάλληλη χρήση ασύμμετρης κρυπτογράφησης παρέχει την ψηφιακή υπογραφή, δηλαδή τα εχέγγυα τόσο για την ακεραιότητα του εγγράφου όσο και για την πιστοποίηση της ταυτότητας του αποστολέα.

Σε ορισμένες χώρες, οι ψηφιακές υπογραφές έχουν – υπό συγκεκριμένες προϋποθέσεις και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες, ως προς τη σημασία τους, με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές εφαρμόζονται παράλληλα με τη χρήση ασφαλών κρυπτογραφικών αλγορίθμων, είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επιπρόσθετα το φυσικό ή νομικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε για όσο χρονικό διάστημα το ιδιωτικό του κλειδί που χρησιμοποιήθηκε για τη δημιουργία της ψηφιακής υπογραφής δεν υποκλάπηκε. Ορισμένες υλοποιήσεις των ψηφιακών υπογραφών, προσθέτουν και επιπρόσθετες πληροφορίες όπως για παράδειγμα την ημερομηνία υπογραφής του εγγράφου. Με τον τρόπο αυτό αποφεύγεται ο κίνδυνος ακόμα και τον ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από δεδομένα (bits) όπως για παράδειγμα στα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα και μηνύματα που στέλνονται στο Διαδίκτυο.

2.4.4 Ψηφιακά Πιστοποιητικά.

Το ψηφιακό πιστοποιητικό αποτελεί ένα είδος ηλεκτρονικής ταυτότητας που το εκδίδεται από μια αρχή πιστοποίησης (Certification Authority - CA) και εγγυάται την εγκυρότητα των στοιχείων του κατόχου του. Ο παραλήπτης ενός μηνύματος, για την επαλήθευση της ηλεκτρονικής υπογραφής αυτού, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με απόλυτη

βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Κάνοντας την θεώρηση ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι καθώς και την υπόθεση ότι η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί, ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε.

Εικόνα 6. Ψηφιακό Πιστοποιητικό.

Συνέπεια αυτού είναι η απαίτηση να διασφαλιστεί ότι ο κάτοχος του ιδιωτικού κλειδιού, και αποκλειστικά αυτός, δημιούργησε την ηλεκτρονική υπογραφή, όπως επίσης ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιείται από την παραλήπτη για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι βέβαιος για την ταυτότητα του αποστολέα που κατέχει το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

Ο πάροχος υπηρεσιών πιστοποίησης (Certification Authority) είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι μέσω της έκδοσης ενός πιστοποιητικού (Certificate) στο οποίο ο πάροχος υπηρεσιών πιστοποίησης, πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Εν κατακλείδι, πρέπει να σημειωθεί ότι το σύνολο όλων των ανωτέρω κρυπτογραφικών μηχανισμών αποτελεί ένα πλούσιο σύνολο για τη διασφάλιση όλων των απαιτήσεων της ασφάλειας: εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση, μη αποποίηση. Αυτός είναι και ο λόγος που εφαρμόζονται στην πλειοψηφία των μεγάλων τηλεπικοινωνιακών δικτύων. Ωστόσο, υπάρχουν περιπτώσεις δικτύων με ιδιαίτερες απαιτήσεις ως προς την ταχύτητα μετάδοσης, τη χαμηλή κατανάλωση ενέργειας και τη χαμηλή υπολογιστική ισχύ (π.χ. ασύρματα δίκτυα αισθητήρων), που καθιστούν πολλές εκ των ανωτέρω ασύμφορες: ακόμα και η χρήση του συμμετρικού κρυπτογραφικού αλγορίθμου που θα επιλεγεί για τη διασφάλιση της εμπιστευτικότητας δεν μπορεί να είναι αυθαίρετη, ακριβώς λόγω των παραπάνω περιορισμών. Ως εκ τούτου, το ζήτημα της επιλογής των κατάλληλων κρυπτογραφικών μηχανισμών παραμένει στη γενική περίπτωση ανοιχτό.

Κεφάλαιο 3
Συμμετρικοί Κρυπταλγόριθμοι.

3 Συμμετρικοί Κρυπταλγόριθμοι.

Στην παρούσα ενότητα αντικειμενικός σκοπός είναι να επεξηγηθούν λιτά και περιεκτικά τα βασικά χαρακτηριστικά μιας σημαντικής κατηγορίας συμμετρικών κρυπτογραφικών αλγορίθμων, των λεγόμενων κρυπταλγορίθμων ροής (stream ciphers). Θα γίνει μία σαφής και ρητή αναφορά στις τεχνικές παραγωγής των ακολουθιών των κλειδιών ή αλλιώς των κλειδοροών (keystreams), αλλά και στις ιδιότητες που πρέπει να πληροί μια κλειδοροή ώστε να χαρακτηριστεί κατάλληλη για χρήση σε κρυπτογραφικό αλγόριθμο. Ο κύριος λόγος που επικεντρωνόμαστε σε αυτήν την κατηγορία αλγορίθμων είναι γιατί συναντώνται σε εφαρμογές ασύρματων δικτύων αισθητήρων, στις οποία δίκτυα θα εστιάσει η παρούσα διατριβή στο πλαίσιο ανάδειξης των κινδύνων από επιθέσεις παράπλευρου καναλιού.

3.1 Αλγόριθμοι Κρυπτογράφησης.

Οι αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού, που αναφέρθηκαν στο προηγούμενο κεφάλαιο, περιλαμβάνουν τόσο τους κρυπταλγόριθμους τμήματος (Block Ciphers) όσο και τους κρυπταλγόριθμους ροής (Stream Ciphers). Ένας κρυπταλγόριθμος τμήματος επεξεργάζεται τμήματα του αρχικού μηνύματος σταθερού μεγέθους, το οποίο

καλείται μπλοκ: μπορεί να θεωρηθεί ως ένας τεράστιος και σταθερός, για κάθε κλειδί, μυστικός πίνακας αντικατάστασης που μετατρέπει ένα τμήμα (μπλοκ) κειμένου σε κάποιο τμήμα (μπλοκ) κρυπτοκειμένου. Η ίδια συνάρτηση κρυπτογράφησης χρησιμοποιείται για την κρυπτογράφηση διαδοχικών τμημάτων. Έτσι, οι κρυπταλγόριθμοι τμήματος μπορεί να ειπωθεί ότι είναι κατ' αρχάς αλγόριθμοι "άνευ μνήμης" (memoryless). Ωστόσο, η προσθήκη «μνήμης» σε έναν κρυπταλγόριθμο τμήματος είναι εφικτή – ήτοι ένα τμήμα του αρχικού μηνύματος να επηρεάζει την κρυπτογράφηση κατοπινών τμημάτων - με κατάλληλο τρόπο λειτουργίας (που είναι και η συνηθέστερη περίπτωση). Γενικά, ένας οποιοσδήποτε κρυπταλγόριθμος τμήματος επιτελεί κρυπτογράφηση μέσω σύνθετων λειτουργιών (πολλαπλές αντικαταστάσεις και αντιμεταθέσεις των bits, οι οποίες εξαρτώνται από το μυστικό κλειδί). Οι αλγόριθμοι DES, 3DES και AES που αναφέρθηκαν στο προηγούμενο κεφάλαιο, ανήκουν στην κατηγορία των κρυπταλγορίθμων τμήματος.

Ένας συμμετρικός κρυπταλγόριθμος τμήματος (stream cipher) έχει ως είσοδο ένα μήνυμα μεταβλητού μήκους και μπορεί να θεωρηθεί ως ένα μικρός αλλά μεταβλητός πίνακα αντικατάστασης ο οποίος μετατρέπει τα bits του κειμένου σε νέα bits κρυπτοκειμένου. Ωστόσο υπάρχει κάποιο είδος σύνδεσης μεταξύ των αλγορίθμων τμήματος και αλγορίθμων ροής. Ένας κρυπταλγόριθμος τμήματος σε συγκεκριμένους τρόπους λειτουργίας, όπως σε τρόπο λειτουργίας μετρητή (Counter Mode- CTR) ή σε τρόπο λειτουργίας ανάδρασης εξόδου (Output feedback-CFB) είναι ένας – όχι ιδιαίτερα αποδοτικός - συμμετρικός κρυπταλγόριθμος ροής (Van Brussel, et al 2008: 35).

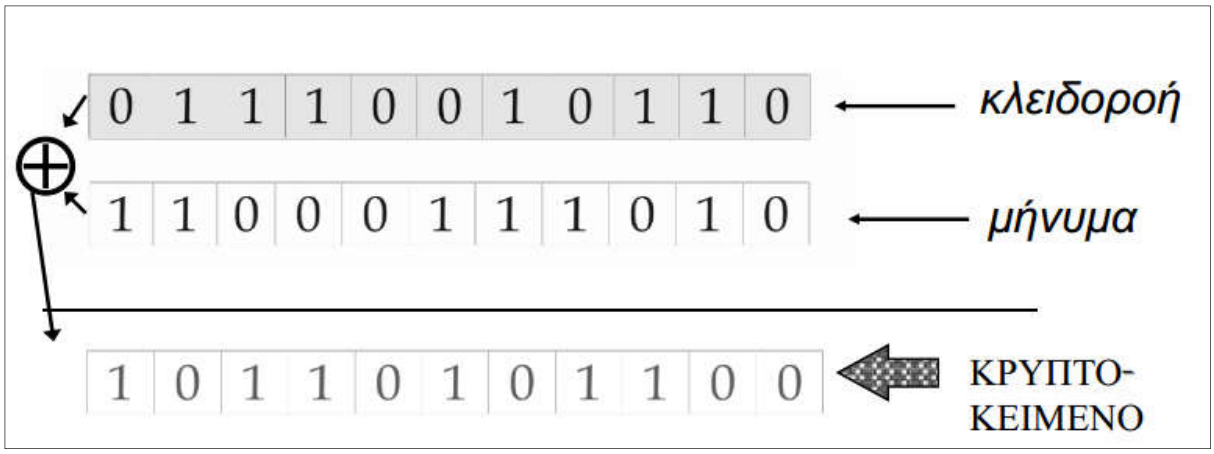
Σε πολλές εφαρμογές ένας κρυπταλγόριθμος τμήματος είναι προτιμότερος για χρήση του σε σύγκριση με έναν κρυπταλγόριθμο ροής. Πέραν των χαρακτηριστικών ασφαλείας (υπάρχει πρότυπος αλγόριθμος κρυπτογράφησης τμήματος, ενώ δεν υπάρχει πρότυπος αλγόριθμος κρυπτογράφησης ροής), ένας συμμετρικός κρυπταλγόριθμος τμήματος είναι επίσης χρήσιμος στην κατασκευή άλλων θεμελιωδών κρυπτογραφικών λειτουργιών, όπως οι συναρτήσεις κατακερματισμού και οι κώδικες αυθεντικοποίησης μηνύματος (MAC).

Από την άλλη πλευρά, ένας κρυπταλγόριθμος ροής εμφανίζει πλεονεκτήματα έναντι του κρυπταλγόριθμου τμήματος. Το πρώτο πλεονέκτημα είναι ότι για να επιτευχθεί το ίδιο επίπεδο ασφάλειας, με όρους πολυπλοκότητας υπολογισμού του μυστικού κλειδιού

(βάσει του μεγέθους του κλειδιού), ένας συμμετρικός κρυπταλγόριθμος ροής (stream cipher) πραγματοποιεί λιγότερους υπολογισμούς από ότι ένας συμμετρικός κρυπταλγόριθμος τμήματος, (Van Brussel, et al 2008: 2-3). Το κύριο πλεονέκτημα, το οποίο είναι και απόρροια και του προαναφερθέντος, είναι ότι η κρυπτογράφηση και η αποκρυπτογράφηση του συμμετρικού κρυπταλγόριθμου ροής μπορεί να είναι εξαιρετικά γρήγορη. Επίσης, σε σχέση με τους κρυπταλγόριθμους τμήματος, έχουν λιγότερο πολύπλοκη κυκλωματική υλοποίηση (δηλαδή απλούστερο υλικό (hardware), ενώ είναι πιο κατάλληλοι και σε περιπτώσεις όπου χαρακτήρες του μηνύματος θα πρέπει να υποβάλλονται σε επεξεργασία ξεχωριστά καθώς λαμβάνονται. Περαιτέρω, επειδή έχουν περιορισμένη ή μηδενική διάδοση σφαλμάτων, οι συμμετρικοί κρυπταλγόριθμοι ροής είναι σε πλεονεκτική θέση σε καταστάσεις όπου οι μεταδόσεις σφαλμάτων είναι μία πολύ υψηλή πιθανότητα (Menezes, et al 1996: 197). Τα ανωτέρω καθιστούν τους κρυπτογραφικούς αλγορίθμους ροής ως πρώτη επιλογή σε περιπτώσεις όπου υπάρχει απαίτηση για υψηλή ταχύτητα μετάδοσης, χαμηλή κατανάλωση ενέργειας και χρησιμοποίηση

3.1.1 Συμμετρικοί Κρυπταλγόριθμοι Ροής.

Οι συμμετρικοί κρυπταλγόριθμοι ροής είναι, όπως περιγράφηκε ανωτέρω, μια πολύ σημαντική κατηγορία αλγορίθμων κρυπτογράφησης. Κατά την διάρκεια της κρυπτογράφησης, κρυπτογραφούνται ξεχωριστά οι χαρακτήρες ενός κειμένου, ένας κάθε φορά, κάνοντας χρήση ενός κρυπτογραφικού μετασχηματισμού ο οποίος ποικίλοι προϊ όντος του χρόνου. Η λειτουργία της κρυπτογράφησης που συντελούν οι κρυπταλγόριθμοι ροής είναι τελικά μία πρόσθεση (αποκλειστική διάζευξη – τελεστής XOR) των bits του μηνύματος με τα bits της ακολουθίας κλειδιού, που ονομάζεται κλειδοροή. Με άλλα λόγια, ισχύει $m_i \oplus k_i = c_i$, όπου m_i, k_i και c_i είναι τα i-ιοστά bit του μηνύματος, της κλειδοροής και του κρυπτοκειμένου αντίστοιχα. Κρίσιμο ζήτημα εδώ είναι τα χαρακτηριστικά της κλειδοροής, τα οποία με τη σειρά τους είναι στενά συνυφασμένα με τη γεννήτρια της κλειδοροής (keystream generator).



Εικόνα 7 Παράδειγμα Κρυπτογράφησης.

Πριν προχωρήσουμε στη λογική που διέπει την κατασκευή των κρυπταλγορίθμων ροής, θα εξηγήσουμε τους λόγους που αυτή η απλή λειτουργία κρυπτογράφησης που επιτελούν (πρόσθεση XOR) μπορεί, υπό κατάλληλες προϋ ποθέσεις, να παρέχει επαρκή ασφάλεια.

3.1.2 Σημειωματάριο Μιας Χρήσης.

Ο αλγόριθμος του σημειωματάριου μιας χρήσης (One Time Pad) χρησιμοποιεί ένα κλειδί το οποίο παράγεται τελείως τυχαία και έχει μέγεθος όσο ακριβώς και το μήνυμα το οποίο θα πρέπει να κρυπτογραφήσει. Στο κλειδί του σημειωματάριου μιας χρήσης πραγματοποιείται η πράξη XOR (πρόσθεση modulo 2) με το αρχικό κείμενο για την κρυπτογράφηση. Για την αποκρυπτογράφηση στο κλειδί του σημειωματάριου μιας χρήσης πραγματοποιείται η πράξη XOR αυτή τη φορά με το κρυτοκείμενο (Van Brussel, et al 2008: 58).

Ο αλγόριθμος του σημειωματάριου μιας χρήσης αποτελεί το μόνο – μέχρι σήμερα - αλγόριθμο ο οποίος είναι απεριόριστα ασφαλής. Πρακτικά αυτό σημαίνει ότι ο αλγόριθμος παραμένει ασφαλής παρόλη την υπολογιστική δύναμη την οποία μπορεί να έχει ένας επιτιθέμενος. Η απόλυτη ασφάλεια του σημειωματάριου μιας χρήσης έχει αποδειχτεί από τον Claude Shannon, τον πατέρα και θεμελιωτή της επιστήμης της κρυπτογραφίας (Shannon C. 1949: 15). Συγκεκριμένα, ο Shannon όρισε την απεριόριστη

ασφάλεια (unconditional security) ως εκείνη την ιδιότητα ενός κρυπτογραφικού συστήματος στο οποίο η γνώση του κρυπτοκειμένου δεν αποκαλύπτει απολύτως καμία πληροφορία για το αρχικό μήνυμα.

Ο Shannon απέδειξε ότι μία απαραίτητη συνθήκη για μία κρυπτογράφηση συμμετρικού κλειδιού ώστε να είναι απόλυτα ασφαλής είναι ότι το μέγεθος του κλειδιού πρέπει να είναι τουλάχιστον όσο και το μέγεθος του μηνύματος. Αυτό μεταφράζεται στο ότι, η αβεβαιότητα του μυστικού κλειδιού θα πρέπει να είναι τουλάχιστον τόση όση η αβεβαιότητα του κειμένου προς κρυπτογράφηση. Αυτό προφανώς ισχύει στο σημειωματάριο μιας χρήσης (Menezes, et al 1996: 42-43).

Παρόλο που το σημειωματάριο μιας χρήσης παρέχει απόλυτη ασφάλεια, είναι ωστόσο μη πρακτικό να γίνει η χρήση του σε πολλές εφαρμογές: τούτο λόγω του περιορισμού ότι το κλειδί που χρησιμοποιείται για την κρυπτογράφηση έχει τόσο μεγάλο μήκος όσο και το κείμενο το οποίο πρόκειται να κρυπτογραφηθεί - άρα αποτελεί αρκετά σοβαρό πρόβλημα η παραγωγή κλειδοροής χωρίς καμία επανάληψη και μεγέθους τόσο, όσο το προς κρυπτογράφηση κείμενο. Επίσης ένας άλλος λόγος που καθιστά μη πρακτικό το σημειωματάριο μιας χρήσης είναι το ότι καμία κλειδοροή που παράγεται από υπολογιστική μηχανή δεν μπορεί να είναι τελείως τυχαία (η τυχαιότητα αυτή είναι κρίσιμη για την απόδειξη της απόλυτης ασφάλειας του σημειωματαρίου μιας χρήσης). Ωστόσο, ένας ισχυρός συμμετρικός κρυπταλγόριθμος ροής (stream cipher) αποτελεί καλό αντικαταστάτη αντί του σημειωματάριου μιας χρήσης. Στους συμμετρικούς κρυπταλγόριθμους ροής παράγεται μία ψευδοτυχαία κλειδοροή (δηλαδή μία κλειδοροή με καλά χαρακτηριστικά που να προσομοιάζει μία τυχαία ακολουθία) από ένα μικρότερο μυστικό κλειδί, μαζί με την προϋ πόθεση ότι η κλειδοροή έχει μεγάλη περίοδο ώστε πρακτικά να μην εμφανίζονται, για ρεαλιστικού μεγέθους μηνύματα, επαναλήψεις αυτής. Οι συμμετρικοί κρυπταλγόριθμοι ροής δεν παρέχουν ωστόσο απόλυτη ασφάλεια (το πλήθος των πιθανών κλειδιών είναι πάντα μικρότερο του πλήθους των μηνυμάτων), αλλά ωστόσο με κατάλληλη σχεδίαση θεωρούνται (ή, υπάρχει η ελπίδα) ότι είναι υπολογιστικά ασφαλείς (Menezes, et al 1996: 195).

3.1.3 Σχεδιασμός Συμμετρικού Κρυπταλγόριθμου Ροής.

Το πιο βασικό δομικό συστατικό ενός συμμετρικού κρυπταλγορίθμου ροής είναι η γεννήτρια κλειδοροής, η οποία περιγράφεται από τη συνάρτηση που ενημερώνει (μεταβάλλει) την κατάστασή της, καθώς και τη συνάρτηση παραγωγής της ακολουθίας εξόδου. Η κατάσταση (state) του συμμετρικού κρυπταλγόριθμου ροής ανανεώνεται αυτόματα κατά τη διάρκεια της κρυπτογράφησης, έτσι ώστε τα bits σε διαφορετικές θέσεις σε ένα μήνυμα, να κρυπτογραφούνται με διαφορετικές καταστάσεις της γεννήτριας. Η συνάρτηση εξόδου δημιουργεί bits κλειδοροής από την τρέχουσα κατάσταση και πραγματοποιεί κρυπτογράφηση ή αποκρυπτογράφηση. Εάν η αρχική κατάσταση ενός συμμετρικού κρυπταλγόριθμου ροής δεν είναι όμοια όπως το κλειδί, τότε μία διαδικασία εγκαθίδρυσης κλειδιού εγκατάστασης απαιτείται για να παραχθεί η αρχική κατάσταση από το κλειδί. Εάν το κλειδί χρησιμοποιείται με διαφορετικό διάνυσμα αρχικοποίησης (Initialization Vector - IV) για την παραγωγή της κλειδοροής, τότε μία διαδικασία εγκαθίδρυσης κλειδιού βασισμένη στο διάνυσμα αρχικοποίησης απαιτείται για να παραχθεί η αρχική κατάσταση από το κλειδί και το διάνυσμα αρχικοποίησης (Van Brussel, et al 2008: 3).

Οι συμμετρικοί κρυπταλγόριθμοι ροής μπορούν να ταξινομηθούν με βάση το αν η γεννήτρια κλειδοροής έχει «μνήμη». Εάν η κατάστασή τους είναι ανεξάρτητη από το μήνυμα, τότε ο αλγόριθμος κρυπτογράφησης ονομάζεται "σύγχρονος" συμμετρικός κρυπταλγόριθμος ροής (synchronous stream cipher), μιας και απαιτεί συγχρονισμό μεταξύ του αποστολέα και του παραλήπτη. Εάν η κατάσταση εξαρτάται από τα προηγούμενα bits του κρυπτοκειμένου, τότε ο αλγόριθμος κρυπτογράφησης καλείται ασύγχρονος ή αυτοσυγχρονιζόμενος συμμετρικός κρυπταλγόριθμος ροής. Ορισμένοι συμμετρικοί κρυπταλγόριθμοι ροής, δεν είναι ούτε σε σύγχρονη ούτε σε ασύγχρονη κατάσταση, δεδομένου ότι η κατάσταση επηρεάζεται από όλα τα προηγούμενα bits του μηνύματος.

Η βασική απαίτηση σχετικά με τη γεννήτρια κλειδοροής είναι να παράγει ακολουθίες (κλειδοροές) πολύ μεγάλης περιόδου. Υπάρχουν αρκετοί τρόποι για να επιτευχθεί αυτό: Ο απλούστερος τρόπος είναι να γίνει η χρήση ενός συμμετρικού κρυπταλγόριθμου τμήματος σε κατάλληλο τρόπο λειτουργίας – π.χ. σε τρόπο λειτουργίας μετρητή. Ωστόσο υπάρχουν δύο προβλήματα που προκύπτουν με τη χρήση κρυπταλγόριθμου τμήματος

ως γεννήτρια κλειδοροής. Ένα πρόβλημα είναι ότι η διάχυση μέσα σε ένα μετρητή είναι πολύ αργή, ένα άλλο πρόβλημα είναι ότι τα πιο σημαντικά bits δεν θα επηρεάσουν τα λιγότερα σημαντικά bits, έτσι ένας αλγόριθμος κρυπτογράφησης με τη χρήση μετρητή, απαιτεί ένα μεγάλο πλήθος υπολογισμών έτσι ώστε να επιτευχθεί ένα επίπεδο υψηλής ασφαλείας (Van Brussel, et al 2008: 55).

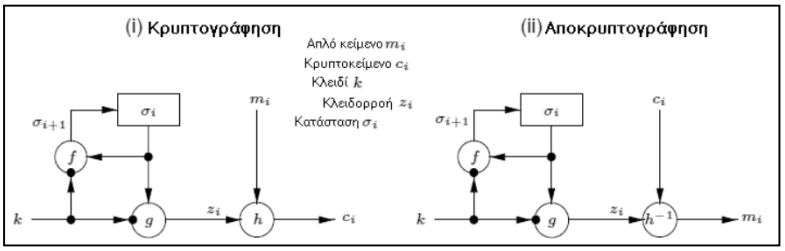
3.1.4 Σύγχρονοι Κρυπταλγόριθμοι Ροής.

Ένας σύγχρονος συμμετρικός κρυπταλγόριθμος ροής (Stream Cipher) είναι αυτός στον οποίο η κλειδοροή παράγεται ανεξάρτητα από το κείμενο προς κρυπτογράφηση (plaintext) και το κρυπτοκείμενο (ciphertext).

Η διαδικασία κρυπτογράφησης ενός σύγχρονου συμμετρικού κρυπταλγόριθμου ροής μπορεί να περιγραφεί από τις εξισώσεις:

$$\sigma_i + 1 = f(\sigma_i, k),$$
$$z_i = g(\sigma_i, k),$$
$$c_i = h(z_i, m_i),$$

όπου σ_0 είναι η αρχική κατάσταση και μπορεί να καθοριστεί από το κλειδί k, f είναι η συνάρτηση "επόμενης κατάστασης", g είναι η συνάρτηση η οποία παράγει την κλειδοροή z_i, και h είναι η συνάρτηση εξόδου η οποία συνδυάζει την κλειδοροή και το κείμενο προς κρυπτογράφηση m_i ώστε να παραχθεί το κρυπτοκείμενο c_i. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζεται στην Εικόνα 8.



Εικόνα 8. Συμμετρική Κρυπτογράφηση και Αποκρυπτογράφηση με κρυπταλγόριθμο ροής.

3.1.5 Ιδιότητες Σύγχρονων Κρυπταλγόριθμών Ροής.

Οι ιδιότητες που καλείται να έχει ένας σύγχρονος συμμετρικός κρυπταλγόριθμος ροής (Menezes, et al 1996: 202) είναι οι ακόλουθες:

I. **Απαιτήσεις συγχρονισμού**. Σε ένα σύγχρονο συμμετρικό κρυπταλγόριθμο ροής, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να συγχρονίζονται, κάνοντας χρήση του ίδιου κλειδιού και έχοντας την ίδια αρχική κατάσταση που προκύπτει από αυτό το κλειδί, έτσι ώστε να είναι εφικτή η αποκρυπτογράφηση. Εάν ο συγχρονισμός απολεσθεί είτε διότι εισαχθούν είτε διότι διαγραφούν ψηφία κρυπτοκειμένου κατά τη διάρκεια της μετάδοσης, τότε η αποκρυπτογράφηση αποτυγχάνει και μπορεί να αποκατασταθεί διαμέσου πρόσθετων τεχνικών επανασυνδέσεων. Οι τεχνικές επανασυγχρονισμού περιλαμβάνουν την επανα-αρχικοποίηση, καθώς και την τοποθέτηση ειδικών δεικτών ανά τακτά χρονικά διαστήματα στο κρυπτοκείμενο.

II. **Μη διάδοση σφαλμάτων**. Ένα ψηφίο κρυπτοκειμένου το οποίο τροποποιείται (δηλαδή αλλάζει τιμή), αλλά δεν διαγράφεται, κατά τη διάρκεια της μετάδοσης δεν επηρεάζει την κρυπτογράφηση άλλων δυαδικών ψηφίων.

III. **Ενεργητικές Επιθέσεις**. Ως απόρροια της πρώτης ιδιότητας που περιγράφηκε πιο πάνω, η εισαγωγή, διαγραφή ή η επανάληψης των ψηφίων του κρυπτοκειμένου από ένα ενεργό επιτιθέμενο, προκαλεί άμεση απώλεια συγχρονισμού και ως εκ τούτου είναι πολύ πιθανό να ανιχνευθεί από τον παραλήπτη. Ως συνέπεια της δεύτερης ιδιότητας, ένας ενεργός επιτιθέμενος μπορεί να είναι σε θέση να κάνει αλλαγές σε επιλεγμένα ψηφιά κρυπτοκειμένου και να ξέρει επακριβώς τα αποτέλεσμα που αυτές οι αλλαγές θα έχουν στο αρχικό κείμενο.

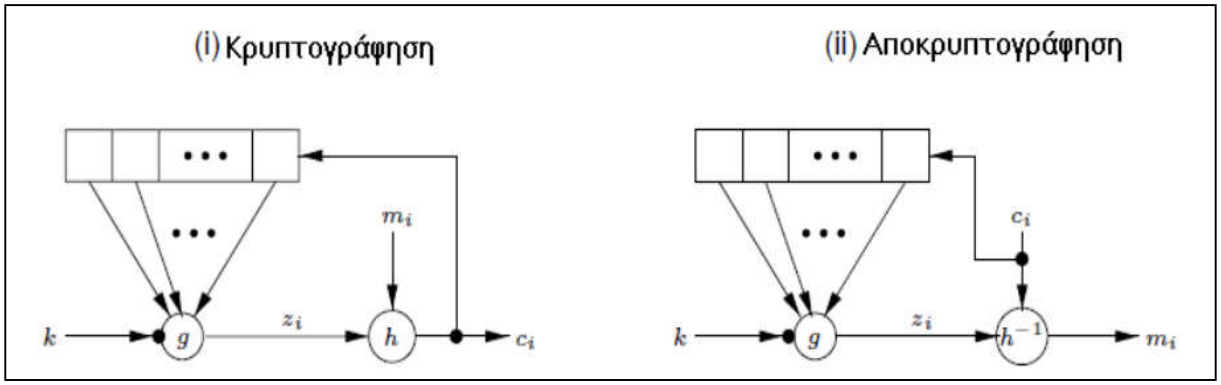
3.1.6 Αυτοσυγχρονιζόμενοι Κρυπταλγόριθμοι ροής.

Ένας αυτό-συγχρονιζόμενος ή ασύγχρονος συμμετρικός κρυπταλγόριθμος ροής είναι ένας αλγόριθμος στον οποίο η κλειδοροή παράγεται ως συνάρτηση του κλειδιού και ενός σταθερού πλήθους των προηγούμενων ψηφίων κρυπτοκειμένου.

Η συνάρτηση κρυπτογράφησης του αυτό-συγχρονιζόμενου κρυπταλγόριθμου ροής μπορεί να περιγραφεί από τις συναρτήσεις:

$$\sigma_i = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}),$$
$$z_i = g(\sigma_i, k),$$
$$c_i = h(z_i, m_i),$$

Όπου $\sigma_0 = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1})$ είναι η αρχική κατάσταση, k είναι το κλειδί, g είναι η συνάρτηση οποία παράγει την κλειδοροή z_i, και h είναι η συνάρτηση εξόδου όπου συνδυάζει την κλειδοροή και το κείμενο m_i, για να παράξει κρυπτοκείμενο c_i. Η κρυπτογράφηση και η αποκρυπτογράφηση εμφανίζονται στην εικόνα.



Εικόνα 9. Αυτοσυχρονιζόμενη Κρυπτογράφηση και Αποκρυπτογράφηση σε κρυπταλγόριθμο ροής.

Οι ιδιότητες των αυτό-συγχρονιζόμενων κρυπταλγόριθμων ροής είναι:

I. **Αυτό-συγχρονισμός**. Αυτό-συγχρονισμός είναι πλέον εφικτός σε περίπτωση που ψηφία του κρυπτοκειμένου διαγράφουν ή εισαχθούν, και αυτό γιατί η αποκρυπτογράφηση ενός χαρακτήρα του κρυπτοκειμένου εξαρτάται μόνο από ένα σταθερό αριθμό των προηγούμενων χαρακτήρων του κρυπτοκείμενο.
II. **Περιορισμός διάδοσης σφαλμάτων**. Εάν ένα μόνο ψηφίο κρυπτοκειμένου τροποποιηθεί (διαγραφεί ή εισαχθεί) κατά την διάρκεια της μετάδοσης, τότε κατά την αποκρυπτογράφηση *t* ψηφία κρυπτοκειμένου μπορεί να είναι εσφαλμένα. Το πλήθος *t* εξαρτάται από το πλήθος *t* των προηγούμενων ψηφίων κρυπτοκειμένου.

Μετά το πέρας των *t* εσφαλμένων ψηφίων συνεχίζεται η σωστή αποκρυπτογράφηση.

III. **Ενεργείς επιθέσεις.** Η ιδιότητα (ii) συνεπάγεται ότι οποιαδήποτε τροποποίηση στα ψηφία του κρυπτοκειμένου από ένα ενεργό επιτιθέμενο προκαλεί την λανθασμένη αποκρυπτογράφηση πολλών άλλων ψηφίων κρυπτοκειμένου, βελτιώνοντας έτσι την πιθανότητα να ανιχνευθεί από τον παραλήπτη. Ως απόρροια της ιδιότητας (i) είναι πολύ δύσκολη η ανίχνευση, διαγραφή, ή επανάληψη των ψηφίων κρυπτοκειμένου από ένα ενεργό επιτιθέμενο.

IV. **Διάχυση στατιστικών του κειμένου (plaintext).** Μιας και κάθε ψηφίο του κειμένου προς κρυπτογράφηση επηρεάζει, ολόκληρο το ακολουθούμενο κρυπτοκείμενο, οι στατιστικές ιδιότητες του αρχικού κειμένου (plaintext) διαχέονται μέσα στο κρυπτοκείμενο. Έτσι οι αυτοσυγχρονιζόμενοι κρυπταλγόριθμοι ροής μπορεί να είναι πιο ανθεκτικοί έναντι των σύγχρονων συμμετρικών κρυπταλγόριθμων ροής σε επιθέσεις που βασίζονται στον πλεονασμό αρχικού κειμένου.

3.2 Καταχωρητές Ολίσθησης Γραμμικής Ανάδρασης (LFSR).

Οι γραμμικοί καταχωρητές ολίσθησης με ανάδραση (LFSR) είναι στη φυσική τους δομή ψηφιακά κυκλώματα τα οποία αποτελούνται από N βαθμίδες (θέσεις μνήμης), όπου το περιεχόμενο την κάθε βαθμίδας δύναται να είναι είτε το δυαδικό μηδέν είτε το δυαδικό ένα. Σε κάθε γραμμικό καταχωρητή υπάρχει μια πύλη αποκλειστικής διάζευξης (XOR) στην οποία εκτελείται η πράξη της πρόσθεσης (modulo 2). Η είσοδος που δέχεται η πύλη XOR (πράξη ανάδρασης) είναι κάποιες από τις βαθμίδες του LFSR, οι οποίες ποικίλουν και δεν είναι συγκεκριμένες, αλλά μπορεί να είναι οποιεσδήποτε: στην πράξη, όπως θα δούμε στη συνέχεια, η ανάδραση πρέπει να είναι όχι αυθαίρετη αλλά τέτοια ώστε η παραγόμενη ακολουθία να έχει τη μέγιστη δυνατή περίοδο. Το σύνολο των τιμών των βαθμίδων που αποτελούν τον LFSR ονομάζεται κατάσταση (State) του LFSR για την τρέχουσα χρονική στιγμή.

Ένας LFSR μήκους N είναι σε θέση να διέλθει το πολύ από 2^N-1 διαφορετικές καταστάσεις, όπου πιθανές είναι όλες οι N-άδες έκτος της μηδενικής. Απόρροια του

παραπάνω είναι ό,τι είναι σε θέση να παράγει ακολουθίες με μέγιστη τη δυνατή περίοδο 2^N-1 (δηλαδή η ακολουθία αρχίζει να επαναλαμβάνεται μετά από την παραγωγή 2^N-1 ψηφίων αυτής και όχι νωρίτερα). Οι LFSR που παράγουν την μέγιστη δυνατή περίοδο καλούνται πρωταρχικοί (primitive) και οι ακολουθίες που παράγονται από τέτοιους LFSR ονομάζονται ακολουθίες μέγιστου μήκους (*m-sequences*). Το αν ένας LFSR είναι πρωταρχικός εξαρτάται αποκλειστικά από την ανάδρασή του και όχι από την αρχική του κατάσταση.

Στη γενική περίπτωση ωστόσο, θα πρέπει να ειπωθεί ότι η ακολουθία εξόδου ενός LFSR εξαρτάται τόσο από την ανάδρασή του, δηλαδή το ποιες βαθμίδες λαμβάνουν μέρος στην πρόσθεση XOR, όσο και από την αρχική του κατάσταση.

Για να χαρακτηριστεί ένας LFSR πρωταρχικός θα πρέπει το χαρακτηριστικό του πολυώνυμο να είναι έχει μία συγκεκριμένη μαθηματική ιδιότητα, ήτοι να είναι πρωταρχικό στο πεπερασμένο σώμα $GF(2^N)$ (Menezes, et al 1996: 196-197). Το χαρακτηριστικό πολυώνυμο είναι ένα συγκεκριμένο πολυώνυμο μιας μεταβλητής (με συντελεστές 0 και 1) που περιγράφει κάθε LFSR ανάλογα με την ανάδρασή του. Από τα παραπάνω εξάγεται το συμπέρασμα ότι οι πρωταρχικοί LFSR παράγουν ακολουθίες με τη μέγιστη δυνατή περίοδο, έτσι η κλειδοροή δεν θα είναι επαναλαμβανόμενη – κάτι που είναι απόλυτα επιθυμητό στις κρυπτογραφικές εφαρμογές. Ωστόσο, ένα άλλο πλεονέκτημα των ακολουθιών μεγίστου μήκους που παράγονται από πρωταρχικούς LFSR είναι ότι παρουσιάζουν κάποια καλά χαρακτηριστικά τυχαιότητας. Τα χαρακτηριστικά τυχαιότητας της κλειδοροής θα πρέπει να ικανοποιούν και τα λεγόμενα τρία κριτήρια τυχαιότητας του Golomb που εξετάζονται πιο κάτω.

Ως μαθηματικό μοντέλο, ένας LFSR μεγέθους N πάνω σε ένα σώμα F_2 (πεπερασμένο σώμα με στοιχεία) είναι μια μηχανή πεπερασμένων καταστάσεων (πεπερασμένο αυτόματο) η οποία παράγει μια ακολουθία στοιχείων του σώματος F_2, ικανοποιώντας μια γραμμική αναδρομική σχέση βαθμού N στο πεπερασμένο σώμα F_2 (Van Tilborg 2011: 274).

Οι καταχωρητές ολίσθησης με ανάδραση και συγκεκριμένα οι γραμμικοί καταχωρητές ολίσθησης με ανάδραση (LFSR) αποτελούν τα βασικά δομικά στοιχεία πολλών γεννητριών κλειδοροής. Το γεγονός αυτό βασίζεται σε πολλούς λόγους, όπως:

(i) Οι LFSR έχουν εύκολη υλοποίηση σε hardware.

(ii) Είναι σε θέση να παράγουν ακολουθίες με τη μέγιστη δυνατή περίοδο.

(iii) Είναι σε θέση να παράγουν ακολουθίες με καλές στατιστικές ιδιότητες.

(iv) Λόγω της δομής τους μπορούν να αναλυθούν εύκολα χρησιμοποιώντας αλγεβρικές τεχνικές.

Ένας LFSR μεγέθους *L* περιλαμβάνει *L* καταστάσεις, που αριθμούνται από *0,1,…,L-1,* για κάθε μία από τις οποίες είναι ικανή να αποθηκεύσει ένα bit και να έχει μία έξοδο και μία είσοδο καθώς και ένα ρολόι που ελέγχει την κίνηση των δεδομένων.

Σε μια μηχανή πεπερασμένων καταστάσεων η οποία πραγματοποιείται σε μια υλοποίηση με την βοήθεια υλικού (όπως αναφέρετε στο σημείο(i) που παρατίθεται πιο πάνω) είναι πιο αποδοτική και ταυτόχρονα πιο ελκυστική η χρήση ακολουθιακών κυκλωμάτων *flip-flop* για την αποθήκευση της εσωτερικής κατάστασης του LFSR. Σε ένα αλγόριθμο που αποτελείται από *n* ακολουθιακά κυκλώματα μπορούμε να χρησιμοποιήσουμε μια μηχανή με 2^n καταστάσεις (Klein 2013: 25).

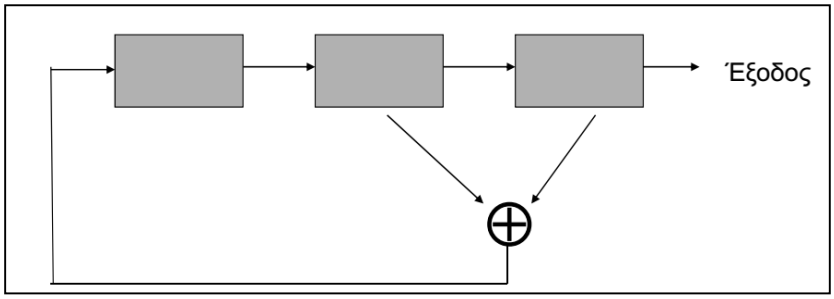
Κατά τη διάρκεια κάθε μονάδας χρόνου (κάθε αλλαγής κατάστασης) στην υλοποίηση ενός LFSR εκτελούνται οι ακόλουθες λειτουργίες:

1. Η τιμή της πρώτης βαθμίδας του LFSR προκύπτει από τις τιμές της προηγούμενης κατάστασης, βάσει της πρόσθεσης XOR που υλοποιεί ο LFSR. Το περιεχόμενο της θέσης *i* μετακινείται προς τα δεξιά στη θέση *i-1* για κάθε i, *1≤i≤L-1*, και

$$s_t = \sum_{i=0}^{N-1} c_i s_{t-N+i,} \qquad \text{t} \geq \text{N}$$

όπου η πρόσθεση στον ανωτέρω τύπο είναι πράξη XOR (πρόσθεση στο πεπερασμένο σώμα F_2) και οι συντελεστές c_i, που στην ουσία είναι οι συντελεστές του πολυωνύμου ανάδρασης του LFSR (βλ. συνέχεια), είναι είτε 0 είτε 1. $S_{t+L} = \sum_{i=1}^{L} C_i S_{t+L-1} \quad \forall t \geq 0$

2. Οι τιμές των άλλων βαθμίδων προκύπτουν από ολίσθηση προς τα δεξιά όλων των βαθμίδων της προηγούμενης κατάστασης. (Menezes, et al 1996: 204).

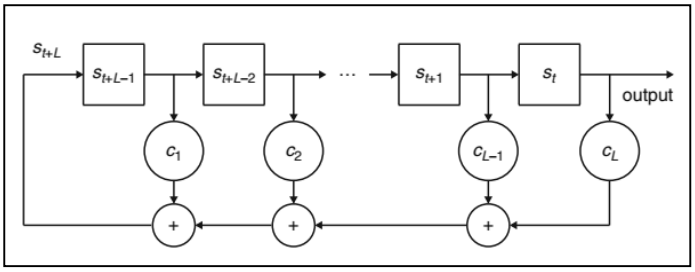


Εικόνα 10 Παράδειγμα πρωταρχικού LFSR τριών βαθμίδων.

Παράδειγμα: Ο LFSR της Εικόνας 10 (για λόγους απλότητας, δεν εμφανίζεται το σήμα του ρολογιού) υλοποιεί τη γραμμική ανάδραση $s_t = s_{t-2} + s_{t-3}$ για t≥3 (θεωρούμε την αρχική κατάσταση του LFSR ως (s_2, s_1, s_0) από δεξιά προς τα αριστερά, και η παραγόμενη ακολουθία στην έξοδο θα είναι η $s_0 s_1 s_2 s_3 s_4$…….

3.2.1 Πολυώνυμο Ανάδρασης και Χαρακτηριστικό Πολυώνυμο.

Το πολυώνυμο ανάδρασης αποτελεί την εξίσωση που καθορίζει τους συντελεστές ανάδρασης ενός LFSR. Η ακολουθία εξόδου ενός LFSR είναι μοναδική και είναι παράγωγο της αρχικής κατάστασης και των συντελεστών ανάδρασης. Στην εικόνα που ακολουθεί (Εικόνα 11) οι τελεστές $c_1,\ldots,c_L$, είναι στοιχεία του πεπερασμένου σώματος F_2. Οι τελεστές αυτοί καλούνται και ως τελεστές ανάδρασης του LFSR. Ένας LFSR μεγέθους L στο πεπερασμένου σώματος F_2 έχει σχηματικά την ακόλουθη δομή:



Εικόνα 11. Δομή LFSR.

Οι καταχωρητές ολίσθησης ελέγχονται από ένα εξωτερικό ρολόι. Κάθε χρονική στιγμή, κάθε δυαδικό ψηφίο της κατάστασης ολισθαίνει κατά μία θέση προς στα δεξιά. Το περιεχόμενο της δεξιότερης κατάστασης S_t αποτελεί και την έξοδο του καταχωρητή ολίσθησης. Το νέο περιεχόμενο της αριστερότερης κατάστασης είναι το *bit* ανάδρασης, S_{t+L}. Το *bit* ανάδρασης παράγεται από ορισμένες από τις βαθμίδες του καταχωρητή οι οποίες λαμβάνονται τυχαία και μπορεί να είναι στη γενική περίπτωση, όπως ειπώθηκε, οποιεσδήποτε από τις βαθμίδες του.

Η ακολουθία εξόδου ενός LFSR , όπως έχει ήδη ειπωθεί, καθορίζεται μοναδικά από την ανάδραση των βαθμίδων του και την αρχική του κατάσταση. Οι τελεστές ανάδρασης $C_1,\ldots,C_L$ ενός LFSR μεγέθους L, συνήθως αναπαριστώνται από το πολυώνυμο ανάδρασης του LFSR το οποίο καθορίζεται από τον τύπο (Van Tilborg 2011: 727):

$$P(X) = 1 - \sum_{i=1}^{L} c_i X^i$$

Ένας LFSR ονομάζεται *μη-ιδιάζων* (non singular) εάν ο βαθμός του πολυωνύμου ανάδρασης είναι ίσος με το μήκος του LFSR. Κάθε ακολουθία η οποία παράγεται από *μη-ιδιάζοντα* LFSR με μέγεθος L είναι περιοδικός και η περίοδος του δεν ξεπερνά το $2^L - 1$. Είναι γεγονός ό,τι ο LFSR έχει το πολύ 2^L διαφορετικές καταστάσεις και η μηδενική κατάσταση (all-zero) ακολουθείται πάντα από μηδενική κατάσταση. Επιπλέον εάν ένας LFSR είναι *ιδιάζων* (singular), όλες οι παραγόμενες ακολουθίες δεν είναι περιοδικές αλλά «τελικά περιοδικές» - δηλαδή πρώτα παράγονται κάποια ψηφία μη περιοδικά και μετά ξεκινά η περιοδικότητα (Van Tilborg 2011: 727).

3.2.2 Χαρακτηρισμός της Ακολουθίας Εξόδου του LFSR.

Ένας LFSR μεγέθους L πάνω στο πεπερασμένο σώμα F_2 μπορεί να παράξει 2^L διαφορετικές καταστάσεις που αντιστοιχούν στις διαφορετικές 2^L αρχικές καταστάσεις. Το σύνολο όλων των ακολουθιών που παράγονται από έναν LFSR με πολυώνυμο ανάδρασης χαρακτηρίζεται από την ακόλουθη ιδιότητα (Van Tilborg 2011: 727) – η οποία διατυπώνεται εδώ στη γενική της περίπτωση για οποιοδήποτε πεπερασμένο σώμα F_q:

- Μία ακολουθία $(S_t)_{t\geq 0}$ παράγεται από ένα LFSR μεγέθους L πάνω σε ένα πεπερασμένο σώμα F_q με πολυώνυμο ανάδρασης P μόνο αν και μόνο υπάρχει πολυώνυμο: $Q \in F_q[X]$ βαθμού $deg(Q)=L$ τέτοιο ώστε η συνάρτηση παραγωγής του $(S_t)_{t\geq 0}$ να ικανοποιεί την ακόλουθη σχέση:

$$\sum_{t\geq 0}^{n} s_i X^t = \frac{Q(X)}{P(X)}$$

Όπου το πολυώνυμο Q καθορίζεται πλήρως από τους συντελεστές του P και από την αρχική κατάσταση του LFSR.

$$Q(X) = -\sum_{i=0}^{L-1} X^i \left(\sum_{j=0}^{i} c_i - \quad {}_J s_j \right)$$

Το αποτέλεσμα αυτό, συμπεραίνει ότι υπάρχει μια αντιστοιχία "ένα-προς-ένα" μεταξύ των παραγόμενων ακολουθιών που παράγονται από ένα LFSR μεγέθους L με πολυώνυμο ανάδρασης P και το κλάσμα $\frac{Q(X)}{P(X)}$, και με βαθμό $deg(Q)<L$. Αυτή η "ένα-προς-ένα" αντιστοιχία έχει δύο κύριες συνέπειες (Van Tilborg 2011: 727).

- Κάθε ακολουθία που παράγεται από ένα LFSR, του οποίου το πολυώνυμο ανάδρασης είναι το P, παράγεται επίσης από έναν LFSR του οποίου το πολυώνυμο ανάδρασης, είναι πολλαπλάσιο του P. Αυτή η ιδιότητα χρησιμοποιείται πολλές φορές σε κάποιες επιθέσεις στις γεννήτριες κλειδοροής που βασίζονται στη χρήση του LFSR.

- Αν μια ακολουθία παράγεται από έναν LFSR με πολυώνυμο ανάδρασης P', τότε το αντίστοιχο κλάσμα είναι τέτοιο ώστε ο μέγιστος κοινός διαιρέτης των P και Q να είναι διάφορος του ένα $(gcd(P,Q)\neq 1)$.

Έτσι, ανάμεσα σε όλες τις ακολουθίες που παράγονται από ένα LFSR με πολυώνυμο ανάδρασης P, υπάρχει μια ακολουθία η οποία μπορεί να παράγεται από ένα μικρότερο

LFSR αν και μόνο αν, το P δεν είναι σε θέση να περιοριστεί ή να απλουστευθεί πάνω στο πεπερασμένο σώμα F_q.

3.2.3 Κριτήρια Τυχαιότητας του Golomb.

Οι γραμμικοί καταχωρητές ολίσθησης με ανάδραση (LFSR) έχουν αρκετές επιθυμητές στατιστικές ιδιότητες. Η πιο γνωστή από αυτές τις ιδιότητες είναι ότι ικανοποιούν τα λεγόμενα κριτήρια τυχαιότητας του Golomb για τις ψευδοτυχαίες ακολουθίες (Klein 2013: 33).

Πριν περιγράψουμε τα κριτήρια τυχαιότητας του Golomb, θα δώσουμε έναν χρήσιμο ορισμό. Μια διαδρομή (run) σε μια δυαδική ακολουθία είναι ένα σύνολο διαδοχικών άσων και μηδενικών. Μία διαδρομή που περιέχει μόνο μηδέν δηλώνεται ως ″κενό″ και μία διαδρομή από άσσους δηλώνεται ως «μπλοκ». Ένα ″κενό″ μεγέθους Κ είναι ένας σύνολο από Κ συνεχόμενα μηδενικά πλαισιωμένα από άσσους. Ένα «μπλοκ» με μέγεθος Κ είναι ένα σύνολο από Κ διαδοχικούς άσσους πλαισιωμένα από μηδενικά. Μια διαδρομή μεγέθους Κ είναι ένα ″κενό″ μεγέθους Κ ή ένα «μπλοκ» μέγεθος Κ. Ουσιαστικά μια διαδρομή είναι ένα τμήμα της ακολουθίας που αποτελείται μόνο από μηδενικά ή μόνο από άσσους και αμέσως πριν και μετά από αυτά βρίσκονται διαφορετικά bit από αυτά που απαρτίζουν το τμήμα (Van Tilborg 2011: 516).

Καμιά πεπερασμένη ακολουθία που κατασκευάζεται από ένα γραμμικό καταχωρητή ολίσθησης με ανάδραση δεν είναι στην πραγματικότητα μια τυχαία ακολουθία. Ο *Golomb* εισήγαγε την έννοια της ψευδο-τυχαίας ακολουθίας για τις περιοδικές δυαδικές ακολουθίες που ικανοποιούν τρία αξιώματα τυχαιότητας. Τα τρία αυτά αξιώματα αντανακλούν τις ιδιότητες που θα ανέμενε κανείς να βρεις σε μια τυχαία σειρά. Έτσι για να χαρακτηριστεί μια ακολουθία (περιόδου 2^N-1 για κάποιο N) ως τυχαία θα πρέπει να περιέχει τις ακόλουθες ιδιότητες.

- **Ισο-κατανεμημένο πλήθος (Balance Property):** Σε μία περίοδο μιας ακολουθίας, το πλήθος των άσων και το πλήθος των μηδενικών πρέπει να διαφέρουν κατά ένα.

- **Run Property**: Σε μία περίοδο της ακολουθίας, οι μισές διαδρομές έχουν μήκος ένα (1), το εν τέταρτο των διαδρομών έχουν μήκος δύο (2), το ένα όγδοο των διαδρομών έχουν μήκος τρία (3) κ.ο.κ. Η ισχύς της συνθήκης εξετάζεται όσο ο αριθμός των διαδρομών είναι μεγαλύτερος ή ίσος από 2^l, όπου ως l ορίζεται το μήκος της διαδρομής.
- Για τη **συνάρτηση αυτοσυσχέτισης** (auto- correlation) της ακολουθίας, η οποία είναι η:

$$\boldsymbol{C(\tau) = \sum_{i=0}^{p-1} (-1)^{a_i} (-1)^{a_{i+r}}}$$

όπου $a_0 a_1 \ldots$ η ακολουθία, θα πρέπει να ισχύει ότι μπορεί να πάρει μόνο δυο τιμές: να είναι σταθερή (ίση με K) για τ≠0 και τιμή N για τ=0.

Θα πρέπει να σημειωθεί ότι κάθε ακολουθία μεγίστου μήκους – δηλαδή ακολουθία που παράγεται από πρωταρχικό LFSR – ικανοποιεί πάντα και τα τρία κριτήρια τυχαιότητας του *Golomb*. Αυτό καταδεικνύει ότι οι LFSR έχουν μία ιδιαίτερη κρυπτογραφική αξία και χρησιμότητα: ωστόσο, από μόνοι τους δεν μπορούν να θεωρηθούν ως ασφαλείς γεννήτριες κλειδοροής για έναν κρυπταλγόριθμο ροής, όπως εξηγείται στη συνέχεια.

3.2.4 Γραμμική Πολυπλοκότητα.

Η γραμμική πολυπλοκότητα (Linear Complexity) μίας ακολουθίας $S(S_t)_{t\geq 0}$, ορίζεται ως το μέγεθος του μικρότερου LFSR που την παράγει. Για λόγους σύμβασης μπορεί να ειπωθεί ότι η γραμμική πολυπλοκότητα μιας ακολουθίας που περιέχει μόνο μηδενικά είναι μηδέν. Η γραμμική πολυπλοκότητα μιας γραμμικής επαναλαμβανόμενης ακολουθίας ισούται με το βαθμό του μικρότερου πολυωνύμου ανάδρασης που την παράγει.

Ειδικότερα, η γραμμική πολυπλοκότητα $\Lambda(S^N)$ μίας πεπερασμένης ακολουθίας $S_N=S_0S_1\ldots S_{n-1}$, με n στοιχεία του πεπερασμένου σώματος F_q αποτελείται από το μέγεθος του μικρότερου LFSR ο οποίος παράγει την ακολουθία S^N για κάποια κατάλληλη αρχική

κατάσταση. Η γραμμική πολυπλοκότητα κάθε πεπερασμένης ακολουθίας μπορεί να καθοριστεί από το γνωστό αλγόριθμο Berlekamp-Massey. Ο αλγόριθμος αυτός, δοθείσης μιας ακολουθίας (με τιμές σε οποιοδήποτε πεπερασμένο σώμα και όχι μόνο στο F_2 που εξετάζουμε εδώ) υπολογίζει όχι μόνο τη γραμμική της πολυπλοκότητα, αλλά και τον μικρότερο LFSR που την παράγει. Αν η περίοδος μιας ακολουθίας είναι N και η γραμμική της πολυπλοκότητα είναι μικρότερη από το ήμισυ της περιόδου ($L<N/2$) τότε ο μικρότερος LFSR μήκους L που την παράγει είναι ***μοναδικός***. Για να υπολογιστεί ο μοναδικός αυτός LFSR με το μικρότερο μέγεθος αρκεί να είναι σε γνώση μας οποιαδήποτε διπλάσια διαδοχικά bits (2L) της μικρότερης ακολουθίας (Van Tilborg 2011: 276).

Η τυχόν χαμηλή γραμμική πολυπλοκότητα μιας ακολουθίας έχει ως αποτέλεσμα η ακολουθία αυτή να είναι μια αρκετά προβλέψιμη ακολουθία. Όπως έχει αναφερθεί ήδη αν η γραμμική πολυπλοκότητα μιας ακολουθίας είναι L τότε ο αλγόριθμος Berrlekamp Massey χρειάζεται μόνο ένα πλήθος 2L διαδοχικών bits για να υπολογίσει των LFSR ελάχιστου μήκους που την παράγει. Αν ένας LFSR είναι *μοναδικός* τότε στην ουσία έχουμε βρει μια γεννήτρια όλης της ακολουθίας. Συμπερασματικά μπορεί να ειπωθεί ότι μια ακολουθία για να χρησιμοποιηθεί ως κλειδί στην κρυπτογραφική διαδικασία θα πρέπει να έχει όσο το δυνατόν υψηλότερη γραμμική πολυπλοκότητα (Van Tilborg 2011: 276).

3.2.5 Αλγόριθμος Berlekamp Massey

Ο Αλγόριθμος Berlekamp-Massey είναι ένας αποδοτικός αλγόριθμος για τον προσδιορισμό της γραμμικής πολυπλοκότητας μιας πεπερασμένης δυαδικής ακολουθίας S^n μήκους n. Ο αλγόριθμος κάνει n επαναλήψεις, με τη i-οστή επανάληψη να υπολογίζει τη γραμμική πολυπλοκότητα της υπο-ακολουθίας S^i που αποτελείται από τους πρώτους i όρους της S^n. Επίσης, όπως προαναφέρθηκε, ο αλγόριθμος είναι κατάλληλος και για τον καθορισμό του μικρότερου δυνατού πολυωνύμου ανάδρασης ενός γραμμικού καταχωρητή ολίσθησης με ανάδραση (LFSR) που παράγει την ακολουθία (Van Tilborg 2011: 274).

Ο χρόνος εκτέλεσης του αλγορίθμου Berlekamp-Massey για τον υπολογισμό της γραμμικής πολυπλοκότητας μιας δυαδικής ακολουθίας δυαδικού μήκους n είναι $O(n^2)$ πράξεις bit (Menezes, et al 1996: 204).

Μία περιγραφή του αλγορίθμου Berlekamp Massey είναι η εξής: (Klein 2013: 34).

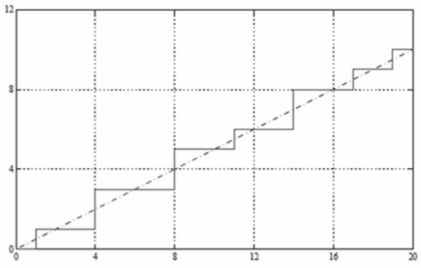
1: {initialization}
2: f0 ← 1, L0 ← 0
3: f−1 ← 1, L−1 ← 0
4: {Compute linear complexity}
5: ***for*** *i* ***from*** *0* ***to*** *n − 1* ***do***
6: Li = degfi
7: di ← L j= i 0 coeff(fi,Li − j)xi−j
8: ***if*** *di = 0* ***then***
9: fi+1 ← fi
10: ***else***
11: m ← max −1 if {j | Lj < Lj+1} if { {j j || L Lj j < L < Lj j+ +1 1} = ∅ } = ∅
12: ***if*** *m − L*
m ≥ i − Li ***then***
13: fi+1 ← fi + X(m−Lm)−(i−Li)fm
14: ***else***
15: fi+1 ← X(i−Li)−(m−Lm)fi + fm
16: ***end if***
17: ***end if***
18: ***end for***

Το σημαντικό συμπέρασμα από τα ανωτέρω είναι ότι ένας LFSR δεν μπορεί να χρησιμοποιηθεί αυτούσιος ως γεννήτρια κλειδοροής, γιατί παράγει ακολουθίες χαμηλής γραμμικής πολυπλοκότητας (δηλαδή προβλέψιμες): πράγματι, για μία ακολουθία μεγίστου μήκους περιόδου 2^N-1, παρόλο η περίοδός της μπορεί να είναι εξαιρετικά μεγάλη για κατάλληλη τιμή του N και, επιπροσθέτως, θα ικανοποιεί και τα κριτήρια τυχαιότητας του Golomb, εν τούτοις έχει γραμμική πολυπλοκότητα μόλις N και άρα, αν ο επιτιθέμενος γνωρίζει μόνο ένα τμήμα αυτής μεγέθους 2N μπορεί, χρησιμοποιώντας τον αλγόριθμο Berlekamp-Massey, να την υπολογίσει ολόκληρη. Ως εκ τούτου, με κάποιον

τρόπο πρέπει να «εμφυτεύσουμε» μη γραμμικές λειτουργίες σε έναν LFSR, για να παραχθούν ακολουθίες υψηλής γραμμικής πολυπλοκότητας.

3.2.6 Προφίλ Γραμμικής Πολυπλοκότητας.

Το προφίλ γραμμικής πολυπλοκότητας είναι μια έκφραση του πως μεταβάλλεται η τιμή της γραμμικής πολυπλοκότητας καθώς η ακολουθία διατρέχεται bit προς bit. Έχει αποδειχθεί ότι το αναμενόμενο προφίλ μια τυχαίας ακολουθίας πρέπει να είναι κοντά στη τιμή $\frac{n}{2}$, αλλά και ότι οι τιμές γύρω από αυτή την τιμή να είναι ακανόνιστες.



Εικόνα 12 Προφίλ Γραμμικής Πολυπλοκότητας

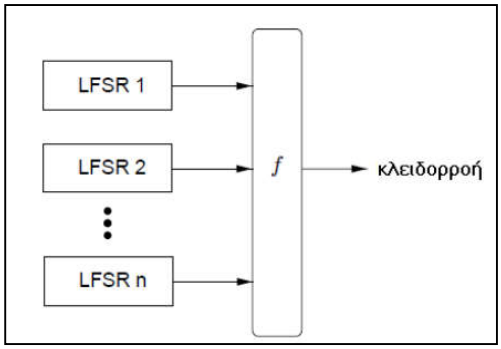
Έτσι σε οποιοδήποτε υπο-τμήμα της ακολουθίας και αν εστιάσουμε (Εικόνα 12), η γραμμική της πολυπλοκότητα θα έχει τιμή κοντά στο μισό του μήκους του τμήματος αυτού.

Συνεπώς, η υψηλή γραμμική πολυπλοκότητα είναι αναγκαία προϋ πόθεση για την ασφάλεια της κλειδοροής – ωστόσο, δεν αρκεί από μόνη της μία μεγάλη τιμή γραμμικής πολυπλοκότητας για να χαρακτηριστεί μία ακολουθία ως φέρουσα καλά χαρακτηριστικά τυχαιότητας.

3.2.7 Γεννήτριες μη Γραμμικού Συνδυασμού.

Για την καταστροφή της γραμμικότητας που υπάρχει στους LFSR, η οποία είναι απαραίτητη προκειμένου να διασφαλιστεί υψηλή γραμμική πολυπλοκότητα, γίνεται

συχνά χρήση μιας τεχνικής η οποία επιτάσσει να χρησιμοποιούνται αρκετοί LFSR τοποθετημένοι μεταξύ τους παράλληλα. Η κλειδοροή που παράγεται στην περίπτωση αυτή εμφανίζεται ως μια μη γραμμική συνάρτηση *f* των εξόδων των διαφόρων LFSRs. Αυτού του είδους οι γεννήτριες κλειδοροών καλούνται ως γεννήτριες μη γραμμικών συνδυασμών και σε αυτήν την περίπτωση η *f* λέγεται *συνάρτηση-συνδυαστής* (Van Tilborg 2011: 274).



Εικόνα 13. Γεννήτρια μη γραμμικού συνδυασμού.

Η ασφάλεια του κρυπτοσυστήματος εξαρτάται σε μεγάλο βαθμό από τις ιδιότητες της μη γραμμικής συνάρτησης συνδυαστή *f*. Κατ' αρχάς, πρέπει να οριστεί η λεγόμενη Αλγεβρική Κανονική Μορφή (Algebraic Normal Form – ANF) μίας λογικής (Boolean) συνάρτησης. Κάνοντας μια προσπάθεια να αποδώσει κάποιος έναν ορισμό της αλγεβρικής κανονικής μορφής της *f* πρέπει να αναφέρει τα ακόλουθα: ένα γινόμενο *m* μεταβλητών λέγεται *m*-οστής τάξης γινόμενο των μεταβλητών. Κάθε λογική συνάρτηση $f(x_1, x_2, \dots, x_n)$ με *n* μεταβλητές μπορεί να γραφτεί ως άθροισμα *modulo 2* διαφορετικών *m*-οστής τάξης γινομένων των μεταβλητών της (για διάφορα m): αυτή η έκφραση λέγεται *αλγεβρική κανονική μορφή* της *f*. Ο *βαθμός* (degree) της *f* είναι το πλήθος των μεταβλητών στο μεγαλύτερο γινόμενο που εμφανίζεται στην αλγεβρική κανονική μορφή της.

Για παράδειγμα η συνάρτηση $f(x_1, x_2, x_3, x_4, x_5)=1 \oplus x_1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3x_4x_5$ έχει βαθμό 4. Θα πρέπει να τονιστεί ότι ο μέγιστος δυνατός βαθμός μιας λογικής συνάρτησης *n* μεταβλητών είναι *n*. Το γεγονός ότι, ένας *n* LFSR μέγιστου μήκους, των οποίων τα μήκη $L_1, L_2, \dots, L_n$ είναι διαφορετικά μεταξύ τους και μεγαλύτερα του 2, συνδυάζονται με μια γραμμική συνάρτηση $f(x_1, x_2, \dots, x_n)$ (όπως στην Εικόνα 13), επιτρέπει την παραγωγή ακολουθιών εγγυημένα υψηλής γραμμικής πολυπλοκότητας, με την προϋ πόθεση ότι έχει

εφαρμοστεί σε αυτή τη γεννήτρια μια συνάρτηση f υψηλού βαθμού. Άρα, ο υψηλός βαθμός είναι απαραίτητη προϋπόθεση για μία τέτοια λογική συνάρτηση, ωστόσο, για την αντιμετώπιση επιθέσεων ασφαλείας πρέπει να λαμβάνονται υπόψη και άλλα κριτήρια, όπως καταδεικνύεται στη συνέχεια.

Στη γενική περίπτωση, οι επιθέσεις συσχέτισης σε τέτοιου τύπου γεννήτριες μπορούν να περιγραφούν ως εξής. Κατ' αρχάς, γίνεται η υπόθεση ότι υπάρχουν n πρωταρχικοί *LFSR* με μήκη $L_1, L_2, \ldots, L_n$, αντίστοιχα, οι οποίοι χρησιμοποιούνται σε μια γεννήτρια μη γραμμικού συνδυασμού. Αν τα πολυώνυμα των LFSR και η συνδυάζουσα συνάρτηση f είναι γνωστά, τότε το πλήθος των διαφορετικών κλειδιών της γεννήτριας ισούνται με τον τύπο $\prod_{i=1}^{n} 2^{L_i-1}$ όπου το κλειδί αποτελείται από τις αρχικές καταστάσεις των LFSR.

Επιπρόσθετα γίνεται η υπόθεση ότι υπάρχει μια συσχέτιση μεταξύ της κλειδοροής και της ακολουθίας εξόδου του R_1, με πιθανότητα συσχέτισης $p > 1/2$. Αν ένα αρκετά μεγάλο τμήμα της κλειδοροής είναι γνωστό, το οποίο είναι δυνατό να συμβεί στα πλαίσια μιας επίθεσης γνώσης τμήματος αρχικού μηνύματος (known-plaintext attack) σε έναν κρυπταλγόριθμο ροής, τότε η αρχική κατάσταση του R_1 μπορεί να βρεθεί μετρώντας τον αριθμό των συμπτώσεων μεταξύ της κλειδοροής και όλων των δυνατών μετατοπίσεων της ακολουθίας εξόδου R_1, μέχρι να συμφωνήσει ο αριθμός αυτός με την πιθανότητα συσχέτισης p. Υπό αυτές τις προϋποθέσεις και υπό από αυτές τις συνθήκες, η εύρεση της αρχικής κατάστασης του R_1 θα απαιτήσει το πολύ $2^{L1} - 1$ δοκιμές (Van Tilborg 2011: 275).

Στην περίπτωση που υπάρχει μια συσχέτιση μεταξύ της κλειδοροής και των ακολουθιών εξόδου καθενός από τους $R_1, R_2, \ldots, R_n$, η αρχική κατάσταση καθενός από τους LFSR μπορεί να προσδιοριστεί ανεξάρτητα, με ένα πλήθος από $\sum_{i=1}^{n} 2^{L_i-1}$ δοκιμές συνολικά. Ο αριθμός αυτός ωστόσο είναι σημαντικά μικρότερος από το συνολικό πλήθος των διαφορετικών κλειδιών. Με παρόμοιο τρόπο είναι δυνατόν να γίνει εκμετάλλευση των συσχετίσεων μεταξύ των ακολουθιών εξόδου συγκεκριμένων υποσυνόλων των LFSR και της κλειδοροής. Στο σημείο αυτό πρέπει να τονιστεί ότι η συνδυάζουσα συνάρτηση f θα πρέπει να επιλεγεί προσεκτικά έτσι, ώστε να μην υπάρχει στατιστική εξάρτηση μεταξύ οποιουδήποτε μικρού υποσυνόλου των ακολουθιών των LFSR.

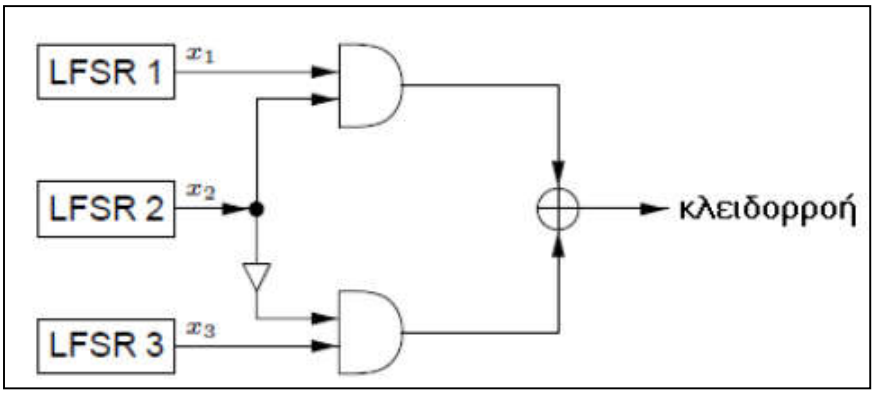
Γενικότερα, η ανωτέρω περιγραφεί μια τεχνική κρυπτανάλυσης είναι ενδεικτικά μόνο μία από διάφορες που μπορούν να εφαρμοστούν: περιγράφηκε απλά για να καταδείξει το πόσο σημαντική είναι η επιλογή της εκάστοτε κρυπτογραφικής συνάρτησης για την κατασκευή της γεννήτριας κλειδοροής.

3.2.7.1 Επιθέσεις Συσχέτισης - Γεννήτρια Geffe.

Για να καταδείξουμε την κρισιμότητα των ιδιοτήτων που πρέπει να έχει μία συνάρτηση *f*, θα αναλογιστούμε ένα κλασικό παράδειγμα, τη λεγόμενη γεννήτρια *Geffe*. Μια γεννήτρια *Geffe*, όπως αυτή στην Εικόνα 14, αποτελείται από τρεις πρωταρχικούς LFSR των οποίων τα μήκη L_1, L_2, L_3 είναι ανά δύο πρώτοι μεταξύ τους και παράγουν, προφανώς, ακολουθίες με μέγιστη περίοδο. Η γραμμική τους συνάρτηση είναι η

$$f(x_1, x_2, x_3) = x_1x_2 \oplus (1 \oplus x_2)x_3 = x_1x_2 \oplus x_2x_3 \oplus x_3.$$

Η παραγόμενη κλειδοροή έχει περίοδο $(2^{L1} - 1)(2^{L2} - 1)(2^{L3} - 1)$ και γραμμική πολυπλοκότητα $L = L_1L_2 + L_2L_3 + L_3$. Για κατάλληλα επιλεγμένους LFSR, παράγονται ακολουθίες μεγάλης περιόδου και μεγάλης γραμμικής πολυπλοκότητας (Van Tilborg 2011: 273).



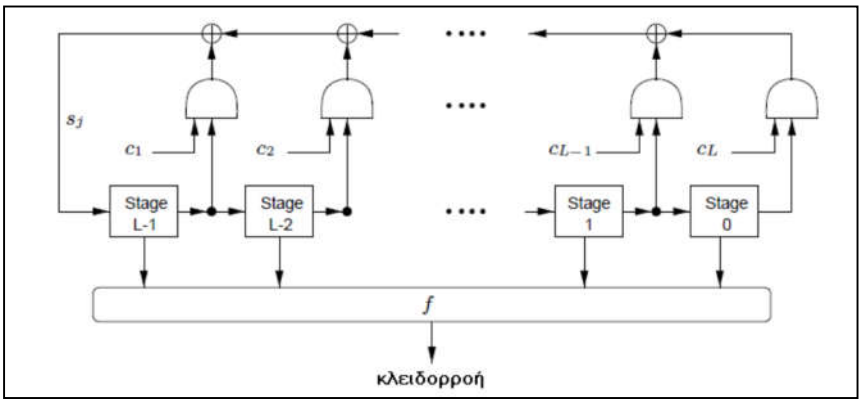
Εικόνα 14. Γεννήτρια Geffe.

Η γεννήτρια *Geffe* είναι ωστόσο κρυπτογραφικά ασθενής επειδή «διαρρέει» πληροφορίες για τις εσωτερικές καταστάσεις των LFSR1 και LFSR2 μέσα στην ακολουθία εξόδου.

Πράγματι, μπορεί κανείς εύκολα να δει ότι η πιθανότητα η κλειδοροή να ταυτίζεται με την έξοδο, π.χ. του LFSR 1 είναι ¾ (δηλαδή, αρκετά υψηλή). Υπάρχει λοιπόν μία συσχέτιση της εξόδου της *f* με τις εισόδους της. Για τον λόγο αυτό, παρότι έχει υψηλή περίοδο και υψηλή γραμμική πολυπλοκότητα, η γεννήτρια *Geffe* υποκύπτει σε επιθέσεις συσχέτισης.

3.2.8 Γεννήτριες μη Γραμμικού Φίλτρου.

Μια άλλη γενική τεχνική για την καταστροφή της γραμμικότητας που υπάρχει στους LFSR είναι να παράγουμε την κλειδοροή εφαρμόζοντας κάποια μη γραμμική συνάρτηση στις βαθμίδες ενός μεμονωμένου LFSR. Η κατασκευή αυτή είναι παρόμοια με αυτή που παρουσιάζεται πιο κάτω. Αυτού του είδους οι γεννήτριες κλειδοροών λέγονται γεννήτριες μη γραμμικού φίλτρου και η *f* στην περίπτωση αυτή ονομάζεται συνάρτηση φίλτρου (*filtering function*) (Van Tilborg 2011: 276).



Εικόνα 15. Γεννήτρια μη γραμμικού φίλτρου.

Στην περίπτωση αυτή ο LFSR λειτουργεί όπως ένας κανονικός LFSR, δηλαδή πραγματοποιείται μετάβαση από κατάσταση σε κατάσταση, μονό που στην περίπτωση αυτή η κλειδοροή δεν προκύπτει ως έξοδος του LFSR αλλά ως έξοδος της συνάρτησης *f*. Στην περίπτωση αυτή η συνάρτηση *f* πρέπει να είναι κατά το δυνατόν ισοβαρής, δηλαδή στην κλειδοροή να είναι ισο-μοιρασμένα τα μηδενικά (0) και οι άσοι (1) έτσι ώστε να εξασφαλίζει ομοιόμορφη κατανομή των bits 0 και 1. Το αποτέλεσμα που επιτυγχάνεται με αυτή την διάταξη είναι, με κατάλληλη επιλογή της συνάρτησης φίλτρου *f*, να

εξασφαλιστεί η μέγιστη δυνατή περίοδος και υψηλή γραμμική πολυπλοκότητα, ως απόρροια του πρωταρχικού LFSR και της χρήσης φίλτρου μεγάλου βαθμού.

3.2.8.1 Γραμμική Πολυπλοκότητα Μη Γραμμικών Φίλτρων.

Αν το μέγεθος ενός LFSR είναι N και ο βαθμός της είναι *deg(f)=d,* τότε η μέγιστη τιμή που μπορεί να έχει η γραμμική πολυπλοκότητα της κλειδοροής είναι $\sum_{i=0}^{d}\binom{N}{i}$. Με γνώμονα τον πιο πάνω τύπο μπορούμε να υποθέσουμε ότι η *f* πρέπει να έχει αρκετά υψηλό βαθμό. Ωστόσο δεν μπορεί να προσδιοριστεί, δοθείσης μιας *f* ,η ακριβής τιμή της γραμμικής πολυπλοκότητας μιας κλειδοροής που παράγεται από μία τέτοια διάταξη. Υπάρχουν όμως συγκεκριμένες κατασκευές συναρτήσεων που αν χρησιμοποιηθούν ως μη γραμμικά φίλτρα παράγουν κλειδοροές πολύ υψηλής γραμμικής πολυπλοκότητας.

Και σε αυτήν την περίπτωση πάντως, η μη σωστή επιλογή της συνάρτησης *f* μπορεί να καταστήσει το σύστημα ευάλωτο σε συγκεκριμένες κρυπταναλυτικές επιθέσεις.

3.2.9 Χρήση μη Γραμμικών Καταχωρητών.

Στα τελευταία έτη, μία νέα προσέγγιση για την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας είναι η χρήση μη γραμμικών καταχωρητών ολίσθησης με ανάδραση (NLFSR) – δηλαδή, σε σχέση με τους LFSR, η συνάρτηση ανάδρασης είναι μη γραμμική. Σε πολλές περιπτώσεις, συναντώνται τόσο LFSR όσο και NLFSR, προκειμένου να αξιοποιηθούν τα πλεονεκτήματα και των δύο (π.χ. αλγόριθμος Grain). Θα πρέπει ωστόσο να σημειωθεί ότι οι NLFSR δεν έχουν μελετηθεί στον ίδιο βαθμό με τους LFSR: για παράδειγμα, δεν είναι γνωστό με ποιον τρόπο μπορούμε να κατασκευάσουμε NLFSR που να παράγει ακολουθίες με τη μέγιστη δυνατή περίοδο.

Κεφάλαιο 4
Επιθέσεις Παράπλευρου Καναλιού.

4 Επιθέσεις Παράπλευρου Καναλιού.

Η ασφάλεια των κρυπτογραφικών αλγορίθμων, κυρίως εξαρτάται στην αντίστασή τους πάνω σε όλους τους τύπους επιθέσεων. Ενώ οι μαθηματικές κρυπταναλυτικές επιθέσεις (όπως αυτές που ενδεικτικά περιγράφηκαν στο προηγούμενο κεφάλαιο ερευνούν κενά ασφαλείας στον κρυπτογραφικό αλγόριθμο, οι επιθέσεις υλοποίησης επικεντρώνονται σε ευπάθειες που προκύπτουν από την υλοποίηση του αλγόριθμου. Οι επιθέσεις υλοποίησης χωρίζονται σε δύο κατηγορίες, τις επιθέσεις παράπλευρου καναλιού και τις ψευδείς επιθέσεις (fault attack), δηλαδή τις επιθέσεις που παρουσιάζονται με σφάλματα υλικού, που συνήθως προκαλούνται από κάποια μη αναμενόμενη κατάσταση ή ελάττωμα της συσκευής (Batina, et al 2005: 118).

Οι επιθέσεις παράπλευρου καναλιού (side-channel attacks) είναι επιθέσεις οι οποίες στηρίζονται στις λεγόμενες πληροφορίες παράπλευρου καναλιού. Οι πληροφορίες παράπλευρου καναλιού είναι οι πληροφορίες οι οποίες μπορούν να «διαρρεύσουν» από οποιαδήποτε κρυπτογραφική συσκευή στην οποία είτε το κείμενο πρόκειται να κρυπτογραφηθεί είτε το κείμενο πρόκειται να αποκρυπτογραφηθεί (Bar–El 2011: 3-4).

Κατά το παρελθόν, μία κρυπτογραφική συσκευή εκλαμβάνονταν ως μία μονάδα η οποία δεχόταν το κείμενο προς κρυπτογράφηση ως είσοδο και παρήγαγε στην έξοδο το κρυπτοκείμενο, καθώς επίσης και το αντίστροφο. Ως εκ τούτου, αναπτύχθηκαν διάφορα είδη επιθέσεων: αυτές οι οποίες στηρίζονται στην γνώση μόνο του κρυπτοκειμένου (Ciphertext only attack), στη γνώση τόσο του κρυπτοκειμένου όσο και τμήματος του

αρχικού μηνύματος (Known plaintext attack), στη δυνατότητα να καθοριστεί ποιο κείμενο πρόκειται να κρυπτογραφηθεί και στη συνέχεια να παρατηρήσει κανείς το αποτέλεσμα της κρυπτογράφησης (Chosen plaintext attack), και τέλος στη δυνατότητα να καθοριστεί ποιο κρυπτοκείμενο πρόκειται να αποκρυπτογραφηθεί και στη συνέχεια να παρατηρήσει κανείς το αποτέλεσμα της αποκρυπτογράφησης (Chosen ciphertext attack).

Στη σημερινή εποχή, είναι γνωστό ότι οι κρυπτογραφικές συσκευές έχουν επιπρόσθετες πληροφορίες, τόσο εξερχόμενες όσο και εισερχόμενες, πέρα από το αρχικό κείμενο και το κρυπτοκείμενο. Οι πληροφορίες αυτές είναι εύκολο να ποσοτικοποιηθούν και να μετρηθούν. Πληροφορίες αυτού του τύπου μπορεί να είναι ο χρόνος που απαιτείται για να λειτουργήσει μία κρυπτογραφική συσκευή, η εκπομπή ραδιοσυχνοτήτων διαφόρων τύπων και η κατανάλωση ενέργειας. Συχνά οι κρυπτογραφικές συσκευές έχουν ακούσιες εισόδους όπως η τάση ρεύματος, οι οποίες μπορούν να τροποποιηθούν ώστε να προκαλέσουν προβλέψιμα αποτελέσματα. Οι επιθέσεις παράπλευρου καναλιού κάνουν χρήση μερικών από αυτές τις πληροφορίες, σε συνδυασμό με άλλες γνωστές τεχνικές κρυπτανάλυσης για να ανακτήσουν το κλειδί που έχει χρησιμοποιηθεί.

Οι επιθέσεις παράπλευρου καναλιού είναι ιδιαίτερα ανησυχητικές, διότι μπορούν να πραγματοποιηθούν εύκολα και πολλές φορές μπορούν να υλοποιηθούν κάνοντας χρήση ήδη διαθέσιμων πόρων υλικού. Αυτό περιορίζει το κόστος υλοποίησής τους. Ο χρόνος ο οποίος θα απαιτηθεί για την ανάλυση και την εκτέλεση της επίθεσης διαφέρει ανάλογα τον τύπο της επίθεσης.

Με μία γενική και ακαδημαϊ κή οπτική γωνία θεωρείται ότι ολόκληρη η εσωτερική διεργασία ενός συμμετρικού κρυπταλγορίθμου αποτελείται από εσωτερικά αποτελέσματα και τιμές οι οποίες υπό φυσιολογικές συνθήκες δεν περιλαμβάνονται στο τελικό εξερχόμενο αποτέλεσμα. Προς επίρρωση αυτού μπορεί να τονιστεί ότι ο αλγόριθμος AES διατρέχεται, στην τυπική περίπτωση, από δέκα (10) γύρους, ενώ θεωρούμε ως ενδιάμεσες καταστάσεις τις εξόδους των γύρων ένα (1) έως εννέα (9). Οι επιθέσεις παράπλευρου καναλιού δίνουν πληροφορίες σχετικά με αυτές τις εσωτερικές διεργασίες ή για τις λειτουργίες που πραγματοποιούνται κατά τη μετάβαση από τη μία εσωτερική κατάσταση σε μία άλλη. Ο τύπος της επίθεσης θα καθορίσει σαφώς τον τύπο και την ποιότητα της πληροφορίας που θα είναι διαθέσιμη στον επιτιθέμενο. Το τυπικό

σενάριο μιας τέτοιας επίθεσης είναι η αποκάλυψη γνώσης για την εσωτερική κατάσταση της κρυπτογραφικής διαδικασίας, η οποία μπορεί να αποκτηθεί τόσο με την υπόθεση μέρους του κλειδιού και μετέπειτα δοκιμές, όσο και με χρήση στατιστικών ιδιοτήτων του αλγορίθμου οι οποίες καθιστούν την ελέγξιμη τιμή όχι τελείως τυχαία.

4.1 Παθητικές Επιθέσεις Παράπλευρου Καναλιού.

Οι επιθέσεις παράπλευρου καναλιού είναι στενά συνδεδεμένες με την ύπαρξη φυσικών παρατηρούμενων φαινομένων, τα οποία πραγματοποιούνται από την εκτέλεση των εργασιών υπολογισμού στις τρέχουσες μικρό-ηλεκτρικές συσκευές - όπως λόγου χάρη η κατανάλωση χρόνου και ενέργειας. Οι επιθέσεις που εκμεταλλεύονται αυτές τις μετρήσεις ονομάζονται παθητικές (passive attacks), διότι δεν επηρεάζουν την κρυπτογραφική λειτουργία – δηλαδή ο επιτιθέμενος απλά παρατηρεί, χωρίς να εισάγει ή να τροποποιεί κάποια πληροφορία. Αυτές οι επιθέσεις είναι και οι πιο δύσκολα ανιχνεύσιμες.

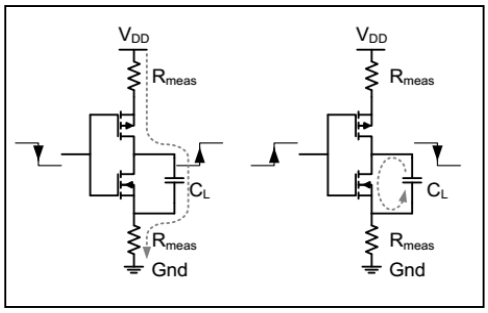
Επίσης οι μικροσυσκευές εκπέμπουν ηλεκτρομαγνητικό πεδίο, διαχέουν θερμότητα, αλλά ακόμα παρουσιάζουν και κάποιας μορφής θόρυβο. Είναι κοινός τόπος ότι υπάρχει αρκετό πλήθος από πληροφορίες οι οποίες διαρρέουν από τα υπολογιστικά συστήματα και τα οποία, συνέπεια αυτού, μπορούν να ανιχνευθούν από κακόβουλα προγράμματα. Δύο σημαντικές πηγές διαρροής πληροφοριών στις επιθέσεις παράπλευρου είναι η κατανάλωση ρεύματος και η ηλεκτρονική ακτινοβολία (Standaert 2012: 3).

4.1.1 Πηγές Της Διαρροής.

Πρέπει να εξηγηθεί όμως ποιες μετρήσεις εκμεταλλεύονται οι επιθέσεις προκειμένου να αποκτήσουν πρόσβαση σε ένα σύστημα.

4.1.1.1 Κατανάλωση Ρεύματος σε Συσκευές CMOS.

Οι στατικές πύλες CMOS έχουν τρεις διαφορετικές αιτίες κατανάλωσης ρεύματος. Η πρώτη είναι διαμέσου της διάθεσης ρεύματος σε τρανζίστορ. Η δεύτερη είναι λόγω του λεγόμενου βραχυκυκλώματος ρεύματος, όπου υπάρχει μια μικρή περίοδος στην οποία πραγματοποιείται το κλείσιμο της θύρας ενώ το NMOS και το PMOS είναι ταυτόχρονα ενεργά. Τέλος, η δυναμική κατανάλωση ενέργειας οφείλεται στη φόρτιση και στην αποφόρτιση των παρασιτικών χωρητικοτήτων κατά τη διάρκεια μεταβάσεων της τάσης στους κόμβους ενός κυκλώματος.



Εικόνα 16. Φόρτιση & αποφόρτιση CMOS.

Η αντίστοιχη σημασία αυτών των πηγών απαγωγής συνήθως εξαρτάται από την τεχνολογία ταξινόμησης. Αλλά η δυναμική κατανάλωση ενέργειας είναι ιδιαίτερα σημαντική από την πλευρά των επιθέσεων παράπλευρου καναλιού, διότι καθορίζει μια απλή σχέση μεταξύ των εσωτερικών δεδομένων μιας συσκευής και την εξωτερικά παρατηρήσιμη κατανάλωση ρεύματος.

4.1.1.2 Ηλεκτρομαγνητική Ακτινοβολία Συσκευών CMOS.

Όπως η κατανάλωση ρεύματος στις κρυπτογραφικές συσκευές είναι ανάλογη των δεδομένων που επεξεργάζονται, μπορεί να ειπωθεί ότι ανάλογη είναι και η ηλεκτρομαγνητική ακτινοβολία αυτών (Standaert 2012: 4.) Στο θεωρητικό πεδίο η ηλεκτρομαγνητική ακτινοβολία δίνεται από τον τύπο:

$$dM = \frac{\mu * I * dI * \hat{r}}{4\pi r^2}$$

που ως $\boldsymbol{\mu}$ είναι η μαγνητική διαπερατότητα, $\boldsymbol{I}$ είναι η τρέχουσα φέρουσα του αγωγού με απειροελάχιστο μήκος dl, $\hat{\boldsymbol{r}}$ είναι η μονάδα φορέας που προσδιορίζει την απόσταση μεταξύ του τρέχοντος στοιχείου και του πεδίου του σημείου. Παρόλο που η εξίσωση είναι αρκετά απλή και δεν περιγράφει την ακριβή ακτινοβολία ενός ολοκληρωμένου κυκλώματος, δίνει έμφαση σε δύο σημαντικές παραμέτρους: (1) το πεδίο είναι εξαρτώμενο από τα δεδομένα και την τρέχουσα ένταση ρεύματος και (2) ο προσανατολισμός του πεδίου εξαρτάται από την τρέχουσα κατεύθυνση. Αυτή η ακτινοβολία, εξαρτώμενη από τα δεδομένα, είναι ξανά η πηγή των διαρροών για εφαρμογή επιθέσεων παράπλευρου καναλιού. Σε γενικές γραμμές ένα οποιοδήποτε φυσικά παρατηρούμενο φαινόμενο το οποίο μπορεί να συσχετιστεί με την εσωτερική διαμόρφωση η δραστηριότητα μίας κρυπτογραφικής συσκευής μπορεί να είναι πηγή χρήσιμων πληροφοριών κακόβουλων χρηστών.

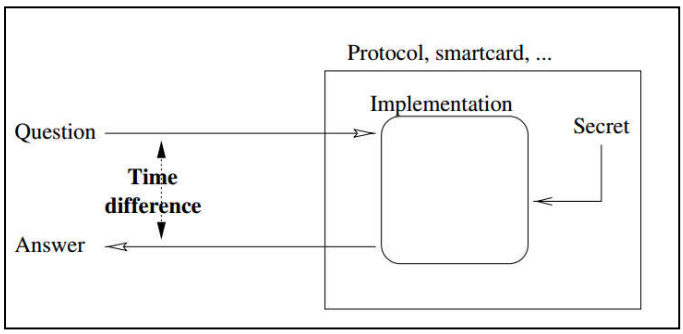
4.1.1.3 Χρόνος Εκτέλεσης.

Μία άλλη ποσότητα που μπορεί να «διαρρεύσει» από μία κρυπτογραφική συσκευή και να μετρηθεί είναι ο χρόνος εκτέλεσης της κρυπτογραφικής λειτουργίας. Και σε αυτήν την περίπτωση, παράμετροι του αλγορίθμου όπως οι τιμές του μυστικού κλειδιού, μπορεί να επηρεάζουν το χρόνο εκτέλεσης, με αποτέλεσμα απλή παρατήρηση του χρόνου αυτού να οδηγεί σε συμπεράσματα σχετικά με τις παραμέτρους αυτές. Έχουν παρατηρηθεί επιτυχείς τέτοιες επιθέσεις κατά το παρελθόν, με χαρακτηριστικότερο παράδειγμα επίθεση στον αλγόριθμο δημοσίου κλειδιού RSA.

4.1.2 Επιθέσεις Χρονισμού.

Όταν ο χρόνος εκτέλεσης ενός αλγορίθμου είναι μη σταθερός, τότε ένα διάγραμμα των χρόνων εκτέλεσής του μπορεί να διαρρεύσει πληροφορίες σχετικά με το μυστικό κλειδί. Για τους κρυπτογραφικούς αλγορίθμους, ο χρόνος εκτέλεσής τους κατά κανόνα δεν είναι σταθερός, λόγω επιλογών ως προς την απόδοση που έχουν υιοθετηθεί σε αυτού του είδους τις διαδικασίες, οι οποίες περιέχουν μυστικές παραμέτρους. Αυτές οι χρονικές παραλλαγές μπορεί να οδηγήσουν στην διαρροή ορισμένων πληροφοριών και να

προσφέρουν επαρκή γνώση για την υλοποίηση επιθέσεων στα χέρια του επιτιθέμενου. Επιπλέον μία αρκετά προσεκτική στατιστική ανάλυση είναι εφικτό να οδηγήσει ακόμα και στην ολοκληρωτική ανάκτηση αυτών των παραμέτρων (Dhem, et al 2000: 169). Κάθε τέτοια επίθεση αποκαλείται επίθεση χρονισμού (timing attack).



Εικόνα 17. Λογική μίας επίθεσης χρονισμού.

Επιπλέον ο επιτιθέμενος έχει μια αρκετά λεπτομερή γνώση για την υλοποίηση του συστήματος στο οποίο επιτίθεται. Επίσης είναι σε θέση να υπολογίσει το μερικό χρονισμό, μιας και γνωρίζει ένα μέρος του κλειδιού. Εάν όμως ο επιτιθέμενος έχει στην κατοχή του ένα μέρος του μηνύματος και του χρόνου που απαιτήθηκε για να παραχθεί η υπογραφή του μηνύματος με το κλειδί. Τότε θα είναι σε θέση να υπολογίσει το κλειδί. Αυτό μπορεί να επιτευχθεί με την δημιουργία δύο υποσυνόλων του μηνύματος, καθώς και δύο συναρτήσεων των οποίων η στατιστική συμπεριφορά θα εξαρτάται από την πραγματική τιμή του κλειδιού (Song, et al 2007: 125).

Σημαντικά στοιχεία στις επιθέσεις χρονισμού τα οποία δεν πρέπει να παραλειφθούν να τονιστούν είναι: Μέτρηση χρόνου και Αναγέννηση χρόνου.

4.1.2.1 Μέτρηση Χρόνου.

Για τη διεξαγωγή μίας επίθεσης, ο επιτιθέμενος θα πρέπει να κάνει μια συλλογή δειγμάτων από τα μηνύματα, καθώς και τον χρόνο που απαιτήθηκε για να επεξεργαστούν τα μηνύματα αυτά από την κρυπτογραφική συσκευή. Ο τρέχων χρόνος εκτέλεσης είναι δυνατόν να ληφθεί με την μέτρηση της καθυστέρησης στις ερωτο-

απαντήσεις, με την παρακολούθηση της δραστηριότητας επεξεργασίας και ούτω καθεξής.

Ένας αρκετά προνομιακός στόχος για τους επιτιθέμενους στις επιθέσεις τύπου χρονισμού, είναι οι έξυπνες κάρτες (Koeune 2005: 622). Η διαμόρφωση μιας κλασικής έξυπνης κάρτας δεν περιλαμβάνει ένα εσωτερικό ρολόι χρονισμού, αλλά λαμβάνει τους χτύπους του ρολογιού χρονισμού από το τερματικό στο οποίο εισέρχεται για να εκτελέσει τον υπολογισμό. Ως εκ τούτου, για ένα τερματικό που είναι υπό τον έλεγχο επιτιθέμενου καθίσταται εύκολο να λάβει μία πολύ ακριβή μέτρηση του χρόνου λειτουργίας.

4.1.2.2 Αναγέννηση Χρόνου.

Οι επιθέσεις χρονισμού, για την πραγματοποίησή τους, κάνουν χρήση του δόγματος στρατηγικής "Διαίρει και βασίλευε" (Koeune 2005: 622). Εδώ το μυστικό κλειδί αποκαλύπτεται ανά τμήματα κάνοντας προβλέψεις βάσει κάποιου είδους συσχετίσεων μεταξύ ενός τμήματος του κλειδιού και του αναμενόμενου χρόνου εκτέλεσης.

Για το κάθε τμήμα του κλειδιού ο επιτιθέμενος ενεργεί ως ακολούθως. Κατ' αρχάς, ανάλογα με την εικασία για τη μερική γνώση του κλειδιού, μπορεί να καθοριστεί ένα κριτήριο για τον αναμενόμενο χρόνο εκτέλεσης. Στη συνέχεια γίνεται ο έλεγχος εάν οι χρόνοι που απαιτήθηκαν για την εκτέλεση της κρυπτογραφικής λειτουργίας ταιριάζουν με το κριτήριο που καθορίστηκε. Αν ταιριάζουν, τότε εξάγεται το συμπέρασμα ότι η εικασία του μερικού κλειδιού είναι σωστή. Αν όμως δεν ταιριάζουν τότε τεκμηριώνεται το συμπέρασμα ότι η εικασία του μερικού κλειδιού είναι λανθασμένη και θα πρέπει να εκτελεστεί ξανά η διαδικασία, κάνοντας μία νέα.

Οι επιθέσεις χρονισμού έχουν εφαρμογή τόσο σε συμμετρικούς αλγορίθμους κρυπτογραφίας, όσο και σε ασύμμετρους.

4.1.2.3 Αντίμετρα.

Δύο τύποι αντίδρασης μπορούν να χρησιμοποιηθούν για να αντιμετωπιστούν επιθέσεις χρονισμού. Η πρώτη περιλαμβάνει την εξάλειψη των διαφορετικοτήτων στις μεταβλητές χρόνου, ενώ η δεύτερη καθιστά τις μεταβλητές αυτές άχρηστες για τον επιτιθέμενο εισβολέα.

Ο μόνος αποδεκτός τρόπος για την πρόληψη των επιθέσεων χρονισμού είναι να γίνεται η κρυπτογραφική λειτουργία σε αυστηρά συγκεκριμένο και σταθερό χρόνο και ανεξάρτητα από τις υπεισερχόμενες μεταβλητές. Ωστόσο αυτό θα σήμαινε ένα αρκετά σοβαρό μειονέκτημα απόδοσης, ειδικά δε για τα συμμετρικά συστήματα, δεδομένου ότι η σταθερά χρόνου θα είναι αυτή που θα καθορίζει την βραδύτερη πιθανή περίπτωση υπολογισμού (Koeune 2005: 623). Ένα τέτοιο αντίμετρο τελικά δεν θα είναι αρκετά πρακτικό. Ένα πιο αποδοτικό, αν και λιγότερο γενικό, αντίμετρο θα είναι η αντιμετώπιση συγκεκριμένων μόνο επιθέσεων χρονισμού.

Προσθέτοντας τυχαία καθυστερήσεις στον αλγόριθμο προκειμένου να «κρύψει» τον πραγματικό χρόνο εκτέλεσης αποτελεί ένα μέτρο που διαισθητικά μοιάζει αρκετά καλό, αλλά τελικά δεν είναι αρκετά αποτελεσματικό αντίμετρο, δεδομένου ότι είναι ισοδύναμο με την προσθήκη "λευκού" θορύβου σε μία πηγή. Τέτοιος θόρυβος μπορεί εύκολα να φιλτραριστεί, αν αυξήσουμε το μέγεθος του δείγματος.

Ο δεύτερος τύπος αντιμέτρων περιλαμβάνει το να αποκρύπτεται η εσωτερική κατάσταση, έτσι ώστε ο επιτιθέμενος να μην είναι σε θέση να προσομοιώσει πλέον τους υπολογισμούς που διενεργούνται εσωτερικά. Αν και οι επιλογές αυτές δεν είναι σε θέση να εγγυηθούν στις πιθανές επιθέσεις χρονισμού, τα αντίμετρα αυτά είναι αρκετά ικανοποιητικά. Επιπρόσθετα οι τεχνικές τύφλωσης (blinding techniques) έχουν επίσης αποδειχθεί αποτελεσματικές εναντίον επιθέσεων παράπλευρου καναλιού (Koeune 2005: 623) – πρόκειται για τεχνικές που μετατρέπουν τις ποσότητες που πρόκειται να υπεισέλθουν στους κρυπτογραφικούς υπολογισμούς σε άλλες, εντελώς διαφορετικές, «συσκοτίζοντας» τις πραγματικές τους τιμές.

4.1.3 Επίθεση Ανάλυσης Παρακολούθησης Ενέργειας.

Οι επιθέσεις που βασίζονται στην ανάλυση της ενέργειας που καταναλώνεται κατά την υλοποίηση της κρυπτογράφησης (Power monitor analysis attack), έχουν καταστεί εξαιρετικά επικίνδυνες για την ασφάλεια των δεδομένων που αποθηκεύονται στις κρυπτογραφικές συσκευές, όπως λόγου χάρη οι έξυπνες κάρτες. Αυτές οι επιθέσεις εκμεταλλεύονται την εξάρτηση που υπάρχει μεταξύ της δυναμικής κατανάλωσης ενέργειας με τις ποσότητες που υπεισέρχονται στο εσωτερικό των κρυπτογραφικών αλγορίθμων: τέτοιες ποσότητες μπορεί να είναι το κρυπτοκείμενο το οποίο θα πρέπει να αποκρυπτογραφηθεί και το μυστικό κλειδί για την αποκρυπτογράφηση. Το υπολογιστικό κόστος είναι αρκετά χαμηλό, ως εκ τούτου οι επιθέσεις αυτές είναι εύκολο να πραγματοποιηθούν.

Στις επιθέσεις ανάλυσης ενέργειας, εφαρμόζεται μία αλληλουχία εισόδων και η στιγμιαία ισχύς που καταναλώνεται κατά τη διάρκεια μιας αποκρυπτογράφησης (ή κρυπτογράφησης) της κάθε εισόδου μετράται και στη συνέχεια αποθηκεύεται. Έπειτα, τεχνικές που έχουν σχέση με την ανάλυση της ενέργειας χρησιμοποιούνται για να ανακαλύψουν το μυστικό κλειδί, το οποίο είναι εσωτερικά αποθηκευμένο και χρησιμοποιείται στη φάση της αποκρυπτογράφησης (ή κρυπτογράφησης). Μία αρκετά γνωστή τεχνική ανίχνευσης μετά την επεξεργασία είναι η ανάλυση συσχέτισης ενέργειας CPA (Correlation power analysis).

Στην ανάλυση CPA, ένα μοντέλο ενέργειας υιοθετείται για την εκτίμηση της δυναμικής κατανάλωσης ενέργειας που απαιτείται. Επίσης χρησιμοποιείται για την εκτίμηση του σήματος που παράγεται εντός του κρυπτογραφικού μικροελεγκτή ως συνάρτηση εισόδου του μυστικού κλειδιού (Alioto, et al 2010: 356). Στη συνέχεια ένα τμήμα του μυστικού κλειδιού μπορεί να μαντευθεί. Επίσης το αποτέλεσμα της δυναμικής κατανάλωσης ενέργειας μπορεί να εκτιμηθεί με αυτό το μοντέλο. Ακολούθως ο συντελεστής συσχέτισης μεταξύ αυτής της εκτίμησης και της μετρούμενης ενέργειας αξιολογείται. Τελικά, το σωστό κλειδί αναγνωρίζεται/ ταυτοποιείται, κάνοντας μία εικασία του κλειδιού που οδηγεί στην υψηλότερη τιμή του συντελεστή συσχέτισης. Πράγματι όσο πιο κοντά είναι στο να μαντέψει κανείς το κλειδί που αντιστοιχεί στο πραγματικό κλειδί, τόσο μεγαλύτερη είναι η συσχέτιση μεταξύ της εκτιμώμενης και της μετρούμενης ισχυρής ενέργειας (Alioto, et al 2010: 357).

Από την άλλη οπτική γωνία υπάρχουν επιπλέον δύο τύποι επιθέσεων. Η επίθεση απλής αναλύσεις ενέργειας SPA (Simple Power Analysis) και η διαφορική ανάλυση ενέργειας DPA (Differential Power Analysis). Μία επίθεση απλής ανάλυσης μπορεί να περιγραφεί ως μια επίθεση στην οποία ο επιτιθέμενος μπορεί απευθείας να χρησιμοποιήσει μια απλή μέτρηση κατανάλωσης ενέργειας για να «σπάσει το κρυπτοσύστημα. Για παράδειγμα, η ενέργεια που καταναλώνεται μπορεί να είναι ανάλογη του βάρους Hamming – δηλαδή του πλήθους των '1' – του μυστικού κλειδιού, και από τις μετρήσεις της ενέργειας να εξάγονται συμπεράσματα για το πραγματικό βάρος Hamming αυτού. Οι πληροφορίες για τα σήματα ενέργειας είναι συνήθως μικρές, ως εκ τούτου διαδικασίες όπως η εκτέλεση τυχαίου κώδικα, ή η αποφυγή προσπέλασης μνήμης με την επεξεργασία των δεδομένων στους καταχωρητές, μπορούν να αποτελέσουν σημαντικά εργαλεία για την προστασία εναντίον των SPA απειλών (Messerges 2001: 150).

Οι επιθέσεις διαφορικής ανάλυσης DPA, από την άλλη, αποτελούν πολύ πιο δύσκολες επιθέσεις ως προς το να αμυνθεί κάποιος. Μια επίθεση διαφορικής ανάλυσης κάνει χρήση στατιστικής ανάλυσης για να εξάγει πληροφορίες για την ανάλυση της ενέργειας. Πληροφορίες οι οποίες μπορεί να είναι ανεπαίσθητης σημασίας για την ανάλυση SPA, μπορούν να εξαχθούν και να έχουν αρκετή σημασία κάνοντας χρήση της DPA. Στην μινιμαλιστική της προσέγγιση, η DPA μειώνει την πιθανότητα ανάλυσης κατανομών των σημείων στο σήμα κατανάλωσης ενέργειας (Messerges 2001: 151).

Για την αντιμετώπιση επιθέσεων DPA έχουν προταθεί ορισμένα αντίμετρα. Τα αντίμετρα αυτά περιλαμβάνουν την υιοθέτηση ενός εικονικού κώδικα τυχαιοποίησης της κατανάλωσης ενέργειας και την «εξισορρόπηση» (κατάλληλη τροποποίηση) των δεδομένων. Αυτές οι μέθοδοι θα μειώσουν την δύναμη της DPA επίθεσης. Δεν είναι ικανές όμως να την αποτρέψουν πλήρως. Επίσης τα ad-hoc αντίμετρα δεν είναι αρκετά, δεδομένου ότι οι επιθέσεις μπορούν θεωρητικά να χρησιμοποιήσουν τεχνικές επεξεργασίας σήματος, για να απομακρύνουν τον εικονικό κώδικα και, ως εκ τούτου, να είναι σε θέση να αναλύσουν περισσότερα δεδομένα και να ξεπεράσουν τις επιπτώσεις της τυχαιοποίησης και της εξισορρόπησης των δεδομένων.

Έχει ωστόσο προταθεί μία καλύτερη προσέγγιση, η οποία «επιβαρύνει» τον διαμοιρασμό των ενδιάμεσων αποτελεσμάτων των δεδομένων κάνοντας χρήση ενός μυστικού σχήματος διαμοίρασης. Ως εκ τούτου, οι επιτιθέμενοι θα πρέπει πλέον να αναλύσουν, ως

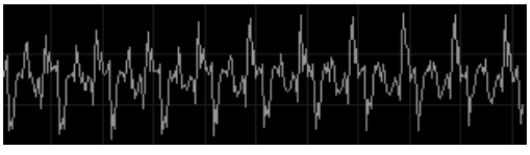
προς την ενέργεια, κοινά διανεμημένες συναρτήσεις σε πολλαπλά σημεία (Messerges 2001: 152).

4.1.4 Επίθεση Ηλεκτρομαγνητικής Ανάλυσης.

Όπως ήδη αναφέρθηκε νωρίτερα, η μέτρηση της κατανάλωσης ενέργειας ενός κρυπτογραφικού επεξεργαστή, παρέχει πληροφορίες για τις κρυπτογραφικές πράξεις που υλοποιεί του (Quisquater, Samyde 2001: 202). Πρόκειται για μία περίπτωση παθητικών επιθέσεων παράπλευρου καναλιού. Αντίστοιχου κινδύνου επιθέσεις όμως είναι και οι λεγόμενες επιθέσεις ηλεκτρομαγνητικής ανάλυσης, που αποτελούν μεγάλο και σοβαρό κίνδυνο.

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν καταχωρητές για να διατηρούν τις τιμές των δεδομένων οι οποίες διανέμονται στο ενσωματωμένο κύκλωμα. Οι τιμές των καταχωρητών (π.χ. οι LFSR σε έναν κρυπταλγόριθμο ροής) αλλάζουν τιμή με κάθε παλμό ρολογιού, και βάσει της νέας τιμής μεταβάλλεται κατάλληλα η λειτουργία του κυκλώματος. Όλες οι εμπλεκόμενες λογικές πύλες επεξεργάζονται την αλλαγή της δυναμικής κατανάλωσης από το δίκτυο διανομής, η οποία μπορεί να μετρηθεί.

Ένας καταχωρητής ο οποίος δεν ενημερώνεται, διατηρεί την τρέχουσα τιμή της ανατροφοδότησής του και ως εκ τούτου δεν καταναλώνει δυναμικά ενέργεια. Κρυπτογραφικοί αλγόριθμοι οι οποίοι χρησιμοποιούν τους καταχωρητές τους διαφορετικά, εξαρτώμενοι από την τιμή του μυστικού που φέρουν, ρέπουν προς «διαρροή», διότι η ίδια διαρροή πληροφοριών που διατηρούν οι καταχωρητές οδηγούν σε διαρροές για το μυστικό που αυτοί φέρουν (Heyszl, et al 2012: 232).



Εικόνα 18. Φάσμα.

Όλες οι ηλεκτρονικές συσκευές περιλαμβάνουν ηλεκτρονικά συστήματα, τα οποία είναι ευαίσθητα σε εξωτερικές διαταραχές. Ωστόσο πολλές φορές διαταράσσουν στοιχεία από μόνες τους. Έτσι, ένας ηλεκτρονικός υπολογιστής μπορεί να παρεμβαίνει σε ένα δέκτη. Φαίνεται ότι αυτή η ακτινοβολία είναι ευθέως συνδεδεμένη με την τρέχουσα κατανάλωση του επεξεργαστή. Το ηλεκτρομαγνητικό πεδίο επιτρέπει πληροφορίες από τις διεργασίες του ολοκληρωμένου κυκλώματος να «βγουν» προς τα έξω. Η μορφή του φάσματος όμως είναι στενά εξαρτώμενη από την αρχιτεκτονική που χρησιμοποιείται στο ενσωματωμένο ολοκληρωμένο κύκλωμα. Ωστόσο ορισμένες συμπεριφορές είναι πανομοιότυπες από ένα επεξεργαστή σε ένα άλλο (Quisquater, Samyde 2001: 203).

Επιθέσεις οι οποίες μπορούν να πραγματοποιηθούν με αρωγό το ηλεκτρομαγνητικό φάσμα είναι οι επιθέσεις σύγκρουσης βασισμένες σε παράπλευρο κανάλι (Side Channel Base Collision Attacks), οι επιθέσεις πρότυπου (Template Attacks) και η εύρεση της τοποθεσίας εξαρτώμενα από την διαρροή (Finding Location Dependent Leakage).

4.1.4.1 Αντίμετρα.

Τα αντίμετρα τα οποία μπορούν να καθυστερήσουν ή να σταματήσουν την ηλεκτρομαγνητική ανάλυση είναι ποικίλα και μπορούν να τοποθετηθούν κάτω από αρκετές οπτικές γωνίες. Ο σχεδιασμός του συστήματος μπορεί να προσπαθήσει να σταματήσει τη διαρροή πληροφορίας. Μπορεί επίσης να τη μειώσει σε μη μετρήσιμη μορφή, όπως μπορεί να τροποποιήσει τις πιθανότητες συσχέτισης ή μπορεί πολύ απλά να τροποποιήσει την αρχιτεκτονική. Επίσης οι σχεδιαστές μπορούν να χρησιμοποιήσουν ίχνη με γνωστούς εκθέτες ή βαθμίδα για να εκτελέσουν διάφορες δοκιμές ώστε να εξετάσουν τις διαρροές πληροφοριών (Heyszl, et al 2012: 233).

4.1.5 Ακουστική Κρυπτανάλυση.

Πολλοί υπολογιστές εκπέμπουν ένα υψίσυχνο θόρυβο κατά την λειτουργία τους, λόγω κραδασμών σε μερικά από τα ηλεκτρονικά τους στοιχεία. Αυτές οι ακουστικές εκπομπές παρέχουν τη δυνατότητα διαρροής του μυστικού κλειδιού που χρησιμοποιείται στην

λειτουργία κρυπτογράφησης. Αυτό αποτελεί εκπληκτικό στοιχείο, δεδομένου ότι η ακουστική πληροφορία έχει πολύ χαμηλό εύρος ζώνης το οποίο κυμαίνεται κάτω των 20 kHz, κάνοντας χρήση κοινών μικροφώνων και μερικές εκατοντάδες kHz χρησιμοποιώντας μικρόφωνα υπερήχων.

Οι δονήσεις των ηλεκτρονικών εξαρτημάτων σε ένα υπολογιστή ακούγονται σαν ένα αμυδρό υψίσυχνο ήχο ή σφύριγμα, ο οποίος ονομάζεται "σπείρα κλαυθμυρισμού" (coil whine) και είναι φαινόμενο δημιουργίας της λειτουργίας των πυκνωτών.

Αυτές οι ακουστικές εκπομπές, που προκαλούνται συνήθως από κυκλώματα ρύθμισης της τάσης, σχετίζονται με τη δραστηριότητα του συστήματος εφόσον η κεντρική μονάδα επεξεργασίας αλλάζει δραστικά το ενεργειακό σχήμα, ανάλογα με τις λειτουργίες που εκτελούν. Αλλά αυτό επιτυγχάνεται με έναν αρκετά "χονδροειδή" τρόπο. Τούτο λόγω του χαμηλού εύρους ζώνης, που δεν επιτρέπει στον εισβολέα να ακούσει μεμονωμένες εντολές, που εκτελούνται σε ένα υπολογιστή με επεξεργαστές πολλών Ghz (Genkin, et al 2014: 444). Το γεγονός ότι η ακουστική εκπομπή από ηλεκτρονικούς υπολογιστές έχει κρυπτογραφικό ενδιαφέρον προκύπτει από την παρατήρηση ότι τα διαφορετικά κρυπτογραφικά κλειδιά έχουν διακριτά ακουστικά αποτυπώματα.

Αυτό το οποίο μπορεί να αποδειχθεί είναι ότι μερική ανάκτηση του μυστικού κλειδιού μπορεί να επιτευχθεί διαμέσου της ακουστικής κρυπτανάλυσης, από μη εξειδικευμένες διατάξεις λογισμικού και υλικού. Τα διαφορετικά μυστικά κλειδιά μπορούν να διακριθούν από το φάσμα του ήχου που παράγουν όταν χρησιμοποιούνται. Αυτό είναι ιδιαίτερα έντονο σε κρυπτογραφήσεις δημοσίου κλειδιού. Αν και οι παραπάνω γραμμές περιγράφουν την εξειδικευμένη περίπτωση, που γίνεται ανάλυση του ακουστικού κύματος εντός του συστήματος, θα πρέπει να γίνει αναφορά και σε ακουστικά κύματα τα οποία υπάρχουν εκτός υπολογιστικού συστήματος.

Αναντίρρητα συσκευές όπως εκτυπωτές αλλά και πληκτρολόγια παράγουν ήχο και κατ' επέκταση ακουστικό κύμα, όταν χρησιμοποιούνται. Στην περίπτωση αυτή, ο επιτιθέμενος είναι σε θέση να συλλέξει τον παραγόμενο ήχο και με ένα πλήθος δοκιμών, να προσπαθήσει να παράξει το ακουστικό κύμα. Εφόσον έχει ταυτοποιήσει ότι το κάθε κύμα αντιστοιχεί στο πάτημα ενός πλήκτρου, με αντίστροφη διαδικασία θα είναι σε θέση να αναπαράγει με αρκετή πιστότητα το μυστικό κλειδί.

Κάνοντας χρήση της ίδιας φιλοσοφίας, μπορεί επίσης να είναι σε θέση να αποκαλύψει το αρχικό μήνυμα, όταν αυτό αποτυπώνεται με την βοήθεια μηχανής εκτύπωσης. Επίσης και σε αυτή την περίπτωση γίνεται καταγραφή του ακουστικού φάσματος το οποίο παράγει ένας χαρακτήρας κατά την αποτύπωσή του και στη συνέχεια, με σύγκριση, γίνεται απόπειρα να αποκαλυφθεί ο χαρακτήρας ο οποίος αποτυπώθηκε. (Backes et al, 2012: 2).

Κύριο αντίμετρο το οποίο μπορεί να προταθεί για τον περιορισμό του κινδύνου είναι, το προφανές: μείωση του ακουστικού σήματος το οποίο παράγουν οι διάφορες συσκευές. Αυτό μπορεί να επιτευχθεί με την χρήση νέων υλικών τα οποία θα είναι σε θέση να απορροφούν τον παραγόμενο θόρυβο, ώστε να ελαχιστοποιείται η πιθανότητα υποκλοπής. Ως άλλο αντίμετρο θα ήταν η εσκεμμένη δημιουργία θορύβου, πράγμα το οποίο θα δυσχέραινε τον επιδέξιο υποκλοπέα να αφουγκραστεί τον παραγόμενο θόρυβο των κρυπτογραφικών συσκευών. Τέλος δεν πρέπει να παραμελούνται άλλες τεχνικές όπως η χρήση μόνωσης στο χώρο όπου είναι εγκατεστημένες οι συσκευές. Αλλά και το πιο απλό, που δεν είναι άλλο από το κλείσιμο της πόρτας του χώρου που είναι εγκατεστημένες οι συσκευές (Genkin 2014: 444, Backes, 2012: 3)

4.1.6 Επίθεση Παραμένουσας Μαγνήτισης.

Η παραμένουσα μαγνήτιση είναι υπόλοιπο της φυσικής αναπαράστασης των δεδομένων τα οποία έχουν σβηστεί ή έχουν επανεγγραφεί (overwritte)/αντικατασταθεί σε μη πτητικές προγραμματιζόμενες συσκευές, όπως συσκευές που έχουν μνήμες τύπου EPROM, EEPROM ή Flash.

Σε αυτές τις μνήμες τα δεδομένα αποθηκεύονται ως φορτίο στις αιωρούμενες θύρες ενός τρανζίστορ. Μετά από κάθε λειτουργία διαγραφής, ένα μέρος της προηγούμενης φόρτισης παραμένει. Η προστασία στους μικροελεγκτές και στις συσκευές που στηρίζονται στην χρήση μνήμης EEPROM βασίζεται στην παραδοχή ότι οι πληροφορίες από τη μνήμη εξαφανίζονται εντελώς μετά τον τερματισμό της συσκευής.

Ενώ έχει γίνει τεράστια προσπάθεια από τους κατασκευαστές λογισμικού να χαλυβδώσουν τα προϊόντα τους έναντι μίας σειράς επιθέσεων, εντούτοις εξακολουθούν να αντιμετωπίζουν προβλήματα με τρανζίστορ που βασίζονται στην τεχνολογία των αιωρούμενων θυρών (*floating gate*). Τούτο γιατί ακόμα και μετά τη διαγραφή των λειτουργιών που γίνονται σε αυτό, το τρανζίστορ δεν επιστρέφει πλήρως στην αρχική του κατάσταση. Έτσι, επιτρέπει στον επιτιθέμενο να μπορεί να κάνει την διάκριση μεταξύ της προηγούμενης κατάστασης που είχε προγραμματιστεί, ανακτώντας κατ' αυτόν τον τρόπο πληροφορίες από την μνήμη που είχαν θεωρητικά διαγραφεί (Skorobogatov 2005: 339).

Η παραμένουσα μαγνήτιση αποτελεί ένα πρόβλημα το οποίο εμφανίζεται, προφανώς, στα μαγνητικά μέσα. Όπως έχει αναφερθεί ήδη, πληροφορίες οι οποίες έχουν αντικατασταθεί πολλές φορές σε μαγνητικά μέσα, είναι σε θέση να ανακτηθούν στην αρχική τους μορφή. Η παραμένουσα μαγνήτιση δεν επηρεάζει μνήμες όπως η SDRAM, αλλά και μνήμες όπως η DRAM, EPROM, EEPROM και η Flash. Αποτέλεσμα αυτού θα είναι η πιθανότητα εξαγωγής πληροφοριών, από μνήμες που έχουν ήδη διαγραφεί. Αυτό σαφώς και δημιουργεί προβλήματα με ορισμένες συσκευές ασφαλείας στις οποίες οι κατασκευαστές τους υποθέτουν ότι όλες οι ευαίσθητες πληροφορίες έχουν χαθεί μόλις διαγραφεί η μνήμη (Skorobogatov 2005: 340).

Σε ορισμένους μικροελεγκτές, περιορισμοί στην προστασία του κώδικα δεν επιτρέπουν στο firmware να αναβαθμιστεί. Επίσης επιτρέπουν την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες. Συνήθως συστήματα τα οποία έχουν ενσωματωμένο το ολοκληρωμένο κύκλωμα, διαγράφουν τόσο τον κωδικό όσο και τη μνήμη των δεδομένων πριν φορτώσουν τον νέο κωδικό. Με αυτό τον τρόπο απαγορεύει σε κάθε νέα εφαρμογή από το να αποκτήσει την πλήρη πρόσβαση. Εάν το συνθηματικό ή το μυστικό κλειδί μπορεί να εξαχθεί στη συνέχεια, τότε εγείρονται σοβαρά προβλήματα για την εμπιστευτικότητα των προηγούμενων κρυπτογραφημένων πληροφοριών (Skorobogatov 2005: 340).

Μνήμες όπως η EPROM, η EEPROM και η Flash αποθηκεύουν την πληροφορία τους σε μορφή ηλεκτρικού φορτίου πάνω στην αιωρούμενη πύλη από το ολοκληρωμένο κύκλωμα. Η αιωρούμενη πύλη μετατοπίζει την τάση κατωφλίου του κελιού/κυττάρου του ολοκληρωμένου κυκλώματος. Αυτή η ενέργεια ανιχνεύεται με ένα ενισχυτή αίσθησης

όταν το κελί/ κύτταρο διαβάζεται. Το μέγιστο φορτίο το οποίο η αιωρούμενη πύλη μπορεί να συσσωρεύσει κυμαίνεται από τεχνολογία σε τεχνολογία. Αλλά στην τυπική της διάταξη είναι μεταξύ 10^3 και 10^5 ηλεκτρόνια. Έτσι μία εισαγωγή 5V θα προκαλέσει μετατόπιση κατωφλίου στα 3,5 V.

Υπάρχουν δύο τεχνικές οι οποίες τοποθετούν τα ηλεκτρόνια στις αιωρούμενες πύλες, ωστόσο οι τεχνικές αυτές δεν θα επεξηγηθούν μιας και το χωρίο αυτό είναι σαφώς εισαγωγικό. Πρέπει να τονιστεί ότι και οι δύο τεχνικές είναι καταστρεπτικές στον λεπτό διηλεκτρικό επίπεδο μεταξύ της αιωρούμενης πύλης και του δίαυλου του ολοκληρωμένου κυκλώματος. Αυτό το στρώμα είναι υπεύθυνο για την διατήρηση του φορτίου στην αιωρούμενη πύλη.

Αποτέλεσμα αυτού είναι ο αριθμός των πιθανών κύκλων επανεγγραφών να είναι περιορισμένος. Διότι οι αιωρούμενες πύλες αρχίζουν σιγά σιγά να συσσωρεύουν ηλεκτρόνια. Προκαλώντας την βαθμιαία αύξηση στο κατώφλι αποθήκευσης του ολοκληρωμένου κυκλώματος, αλλά και στον χρόνο προγραμματισμού. Μετά από ένα συγκεκριμένο πλήθος κύκλων διαγραφής δεν είναι επιπλέον εφικτό να διαγραφεί ή να προγραμματιστεί ένα κελί. Ένα άλλο αρνητικό σημείο είναι η αρνητική φόρτιση στην θύρα (Skorobogatov 2005: 341).

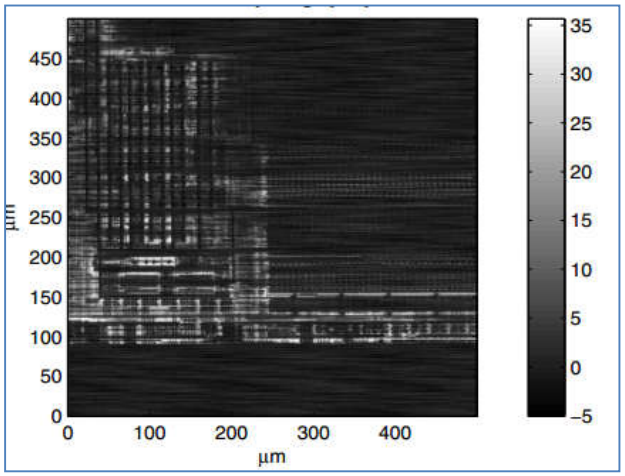
Το πλήθος της εγκλωβισμένης φόρτισης μπορεί να εντοπιστεί και να μετρηθεί, με την μέτρηση της διαρροής του επαγωγικού ρεύματος του κελιού. Η παρατήρηση της μέτρησης γίνεται από την τάση κατωφλίου του κελιού/κύτταρου. Σε συσκευές παλαιότερου τύπου, η τάση αναφοράς για τον ενισχυτή ήταν συνδεδεμένη με την τάση τροφοδοσίας της συσκευής. Σε νεότερες συσκευές είναι απαραίτητο να αλλάξουν οι παράμετροι του κέντρου αναφοράς που χρησιμοποιείται στη διαδικασία ανάγνωσης. Αυτό μπορεί να πραγματοποιηθεί είτε με τμήματα επανά-καλωδίωσής του κυκλώματος ή με την χρήση αχαρτογράφητων δοκιμών Οι οποίες ενδέχεται να είναι ενσωματωμένες στην συσκευή από τους κατασκευαστές.

Επιπρόσθετα στην παραμένουσα μαγνήτιση, οι μνήμες SRAM υπόκειται σε ένα λιγότερο γνωστό φαινόμενο το οποίο καλείται "Burn-in". Εδώ αν ένα κύτταρο μνήμης χρησιμοποιείται για την αποθήκευση της ίδιας τιμής για ένα παρατεταμένο χρονικό διάστημα, η τιμή θα καεί (Burn-in) πάνω σε αυτό το κελί. Δηλαδή το κύτταρο μνήμης θα

εισάγει αυτήν την τιμή όταν θα τροφοδοτείται με ρεύμα. Όπως και η παραμένουσα μαγνήτιση, έτσι και το "Burn-in" έχει σοβαρούς κινδύνους για τις κρυπτογραφικές διαδικασίες (Saxena, Voris 2011: 213). Εάν ένα κλειδί αποθηκεύεται στην ίδια θέση μνήμης για ένα μεγάλο χρονικό διάστημα, τότε μπορεί να είναι πιθανό να ανακτηθεί ακόμα και αν το ρεύμα θα έχει αφαιρεθεί από το κύκλωμα της μνήμης RAM (Saxena, Voris 2011: 213).

Το "κάψιμο" (Burn-in) είναι επίσης προβληματικό και σε γεννήτριες τυχαίων αριθμών που βασίζονται στη μνήμη. Ένα κύτταρο μνήμης το οποίο ″καίγεται″ γίνεται προβλέψιμο και έτσι δεν μπορεί να συμμετέχει στην εντροπία ακόμα και αν προηγούμενα έχει εκτεθεί σε απρόβλεπτη συμπεριφορά. Από την άλλη οπτική, "καμένα" κύτταρα είναι χρήσιμα για να αφήσουν τα αποτυπώματά τους. Τούτο διότι είναι αξιόπιστα στην εισαγωγή της ίδιας κατάστασης πάνω στην έλλειψη της ενέργειας ρεύματος (Saxena, Voris 2011: 214).

Για να αποφευχθούν επιθέσεις παραμένουσας μαγνήτισης είναι καλό να γίνει η υιοθέτηση ορισμένων μέτρων (Skorobogatov 2005: 339).



Εικόνα 19. Σκανάρισμα μνήμης EEPROM με laser.

- Φόρτιση της μνήμης EEPROM/Flash 10 έως 100 φορές με τυχαία δεδομένα πριν να τοποθετούν σε αυτή ευαίσθητα δεδομένα.
- Προγραμματισμός όλων των EEPROM/Flash κυττάρων πριν την διαγραφή τους για να εξαλειφθούν ανιχνεύσιμες επιδράσεις του υπολειπομένου φορτίου.

- Χρήση του τελευταίου τύπου συσκευών αποθήκευσης με την υψηλότερη πυκνότητα, καθώς οι νέες τεχνολογίες σε γενικές γραμμές κάνουν την ανάκτηση δεδομένων πολύ δύσκολη.

4.1.7 Επίθεση Αποκαλυπτικών Εκπομπών.

Τόσο οι υπολογιστές όσο και οι συσκευές επικοινωνίας εκπέμπουν ένα πλήθος από μορφές ενέργειας. Πολλές από αυτές τις εκπομπές παράγονται ως ακούσιες παράπλευρες εκπομπές της κανονικής λειτουργίας. Προς επίρρωση αυτού μπορεί να ειπωθεί ότι, όταν οι εκπομπές αυτές λαμβάνουν την μορφή ραδιοκυμάτων, τότε μπορούν εύκολα να ανιχνευθούν και να παρατηρηθούν, από παρακείμενους δέκτες ραδιοσυχνοτήτων. Ήδη άλλωστε νωρίτερα περιγράψαμε την περίπτωση των ακουστικών κυμάτων. Μερικές από τις ακούσιες εκπεμπόμενες μορφές ενέργειας μεταφέρουν πληροφορίες για τα δεδομένα των διεργασιών. Κάτω από ιδανικές συνθήκες ένας εξειδικευμένος και καλά εξοπλισμένος ωτακουστής είναι σε θέση να υποκλέψει και να αναγνωρίσει εκπεμπόμενες μορφές ενέργειας που έχουν τρωθεί, ώστε να εξάγει και να υποκλέψει πληροφορίες, ακόμα και σε εκπομπές που είναι προορισμένες για συγκεκριμένο σκοπό (όπως στην περίπτωση του αναμεταδότη και του δέκτη της οθόνης της τηλεόρασης, όπου μόνο ένα μικρό κλάσμα από την όλη ενέργεια και τις περιλαμβανόμενες πληροφορίες που εκπέμφθηκαν θα φτάσουν στον παραλήπτη που προορίζονται). Οι επίδοξοι ωτακουστές μπορούν να είναι σε θέση με την χρήση πιο εξειδικευμένων και ευαίσθητων αισθητήρων να αξιοποιήσουν το υπόλοιπο φάσμα και να αποκτήσουν πρόσβαση σε εμπιστευτικές πληροφορίες, συνήθως με πολύ ανορθόδοξους τρόπους, όπως μερικοί που έπονται στις επόμενες γραμμές (Van Tilborg, Jajodia 2011: 273).

Η περισσότερη γνώση που έχει εξαχθεί σε αυτόν τον τομέα έχει αντληθεί από την έρευνα πάνω σε στρατιωτικούς σκοπούς. Ορισμένοι τύποι εκπομπών που έχουν τρωθεί και αναφέρονται στην διεθνή βιβλιογραφία είναι οι:

- Κύματα ραδιοσυχνοτήτων που εκπέμπονται στον ελεύθερο χώρο.
- Κύματα ραδιοσυχνοτήτων που πραγματοποιούνται κατά μήκος των καλωδίων.
- Δονήσεις, ακουστικές και υπερηχητικές εκπομπές.
- Οπτικά σήματα υψηλών συχνοτήτων.

Η γνώση αυτή συλλέγεται στο πλείστο των περιπτώσεων παθητικά, χρησιμοποιώντας κατευθυντικές κεραίες, μικρόφωνα, υψηλής συχνότητας συνδέσεις γραμμών ηλεκτρικής ενέργειας, τηλεσκόπια, ραδιοφωνικούς δέκτες, παλμογράφους και παρόμοιο εξοπλισμό ανίχνευσης και επεξεργασίας σήματος. Σε πολλές περιπτώσεις οι επίδοξοι ωτακουστές – υποκλοπείς μπορούν να λάβουν πρόσθετες πληροφορίες, με ενεργή καθοδήγηση των ραδιοκυμάτων ή ακτίνων φωτός προς μία συσκευή και εν συνεχεία με την ανάλυση της ανακλώμενης ενέργειας.

Προς επίρρωση των παραπάνω μπορούν να δοθούν ορισμένα παραδείγματα. Οι ηλεκτρομαγνητικοί εκτυπωτές μπορούν να παράξουν σήματα χαμηλής ακουστικής συχνότητας, μαγνητικά σήματα και σήματα τροφοδοσίας ρεύματος που είναι χαρακτηριστικά για κάθε τυπωμένο χαρακτήρα. Ως αποτέλεσμα, όπως έχει τονιστεί και σε προηγούμενο χωρίο, το τυπωμένο κείμενο θα μπορούσε να ανακατασκευαστεί με την αρωγή των συνδέσεων ηλεκτρικών γραμμών, μικροφώνων ή κεραιών ραδιοφώνου. Οι πηγές σήματος είναι οι μαγνητικοί ενεργοποιητές στον εκτυπωτή και τα ηλεκτρονικά κυκλώματα που τους οδηγούν.

Ως δεύτερο παράδειγμα επίρρωσης μπορεί να ειπωθεί η τεχνολογία που βρίσκεται πίσω από τις, παρωχημένες πλέον, οθόνες καθοδικού διαύλου. Οι οθόνες καθοδικού διαύλου (CRT), τροφοδοτούνται με μια τάση αναλογικού σήματος, η οποία ενισχύεται με έναν συντελεστή τάξεως 100 μονάδων και εφαρμόζεται σε ένα πλέγμα ελέγχου που διαμορφώνει τη δέσμη ηλεκτρονίων. Αυτή η διευθέτηση επενεργεί μαζί με το καλώδιο της εισερχόμενης εικόνας (βίντεο), σαν ένα είδος κεραίας παρασιτικής μετάδοσης.

Ως απόρροια αυτού, οι οθόνες CRT εκπέμπουν το σήμα του video ως ηλεκτρομαγνητικό κύμα, συνήθως στο εύρος των συχνοτήτων VHF και UHF, από τα 30 MHz έως τα 3 GHz. Στους ραδιοφωνικούς δείκτες AM με εύρος ζώνης συχνότητας συγκρίσιμα με το ρολόι συχνοτήτων του σήματος video μπορεί να μετατραπεί σε μία από τις αρμονικές του μεταδιδόμενου σήματος. Το αποτέλεσμα θα είναι ένα υψιπερατό, φιλτραρισμένο και διορθωμένο σήμα κατά προσέγγιση του αρχικού σήματος, το οποίο όμως, θα στερείται πληροφοριών χρώματος και κάθε κατακόρυφο άκρο του θα εμφανίζεται ως απλή γραμμή. Η εικόνα που έπεται παρουσιάζει την παραμένουσα μορφή των χαρακτήρων του κειμένου μετά την παραμόρφωση.

Εικόνα 20. Παραμόρφωση.

Στις οθόνες CRT μπορεί επίσης να διερευνήσει το σήμα video ως υψηλή διακύμανση του εκπεμπόμενου φωτός. Σε αυτό το κανάλι, το σήμα video διαστρεβλώνεται από την υστερολαμπή των στοιχείων φωσφόρου στην οθόνη, αλλά και από τον θόρυβο τον οποίο το φόντο του φωτός συμβάλει. Είναι επίσης δυνατόν να ανακατασκευαστεί αναγνώσιμο κείμενο από το φως της οθόνης ακόμα και μετά από διάχυτη ανάκλαση, για παράδειγμα, από το πρόσωπο του χρήστη ή από ένα τοίχο.

Σε ορισμένες επίπεδες οθόνες μπορεί να γίνει υποκλοπή των στοιχείων μετάδοσης μέσω της συχνότητας UHF. Ειδικά όταν υψηλής ταχύτητας ψηφιακή σειριακοί σύνδεσμοι χρησιμοποιούνται μεταξύ του ελεγκτή βίντεο και της οθόνης. Αυτού του είδους οι συνδέσεις είναι μια τυπική περίπτωση οθονών φορητών υπολογιστών με σύγχρονες κάρτες γραφικών που έχουν ενσωματωμένο ένα ψηφιακό εικονικό σύνδεσμο (DVI). Με μια πρώτη προσέγγιση μπορεί να ειπωθεί ότι ο επίδοξος υποκλοπέας μπορεί να λάβει το σήμα από ένα καλώδιο βίντεο τεχνολογίας Gbit/s το οποίο θα παρουσιάζει το πλήθος των συναλλαγών bits στις λέξεις των δεδομένων που αντιπροσωπεύονται από το χρώμα του κάθε pixel της οθόνης.

4.2 Ενεργητικές Επιθέσεις Παράπλευρου Καναλιού.

Πέρα από τις ανωτέρω περιγραφείσες παθητικές επιθέσεις, υπάρχουν και ενεργές επιθέσεις παράπλευρου καναλιού. Αυτές οι επιθέσεις συναντώνται συνήθως με το όνομα «ανάλυση σφάλματος» (fault analysis), υπό την έννοια ότι ο επιτιθέμενος επηρεάζει τη λειτουργία της κρυπτογραφικής συσκευής, αναγκάζοντάς την να παράγει λανθασμένα αποτελέσματα στην έξοδό της, από τα οποία μπορεί να αποκαλύψει πληροφορία που θα

έπρεπε να μείνει μυστική. Για παράδειγμα, μπορεί να αυξηθεί η θερμοκρασία στην οποία λειτουργεί η κρυπτογραφική συσκευή, έτσι ώστε τα ηλεκτρικά της κυκλώματα να «αναγκαστούν» να λειτουργήσουν έξω από τις ανεκτές προδιαγραφές θερμοκρασίας τους. Τέτοιες επιθέσεις είναι επίσης, συνήθως, σχετικά εύκολο να πραγματοποιηθούν, χωρίς υψηλό κόστος. Και σε αυτήν την περίπτωση πάντως, η αντιμετώπιση των επιθέσεων αυτών έχει να κάνει με τη σωστή υλοποίηση των κρυπτογραφικών συσκευών.

4.2.1 Επίθεση Διαφορικής Ανάλυσης Σφαλμάτων.

Η διαφορική ανάλυση σφαλμάτων είναι μία αρκετά ισχυρή κρυπτοαναλυτική τεχνική, που διαταράσσει κρυπτογραφικούς υπολογισμούς και εκμεταλλεύεται λανθασμένα αποτελέσματα για να συμπεράνει ποιά μπορεί να είναι τα μυστικά κλειδιά.

Η ανάλυση σφαλμάτων γενικά είναι μια κατηγορία επιθέσεων εφαρμογής που εστιάζει στη χρήση «ενοχλητικών» κρυπτογραφικών υπολογισμών για να ανακαλύψει τα μυστικά κλειδιά. Μεταξύ αυτών των επιθέσεων η διαφορική, η οποία εκμεταλλεύεται τη διαφορά μεταξύ αληθούς και ψευδούς αποτελέσματος, ενώ άλλες επιθέσεις επικεντρώνονται στη συμπεριφορά του κατεστραμμένου υπολογισμού (δηλαδή στο γεγονός κατά πόσο η προκληθείσα βλάβη, προκαλεί αποτελεσματικά ένα λανθασμένο αποτέλεσμα ή όχι). Έτσι, εάν το αποτέλεσμα είναι εσφαλμένο ή αν εντοπιστεί ένα σφάλμα, τότε ο επιτιθέμενος γνωρίζει ότι η ενδιάμεση μεταβλητή είχε διαφορετική τιμή από την εικαζόμενη . Η έλλειψη αυτής της πληροφορίας για αρκετές κρυπτογραφήσεις επιτρέπει την ανάκτηση του κλειδιού.

Ένας απλός τρόπος για να αντιμετωπιστεί αυτό το είδος της επίθεσης είναι η χρήση δεδομένων συγκάλυψης, η οποία εφαρμόζεται συχνά για την προστασία των υλοποιήσεων έναντι και της ανάλυσης ενέργειας. Επίσης ένας άλλος τρόπος για να προστατευθεί ένας αλγόριθμος έναντι της διαφορικής ανάλυσης σφαλμάτων, είναι να προβεί στον υπολογισμό δύο φορές και να ελέγξει εάν τα αποτελέσματα που λαμβάνονται είναι τα ίδια ή όχι. Μία άλλη παρόμοια λύση είναι να επαληθευτεί η ακεραιότητα της κρυπτογράφησης από ένα σύστημα αποκρυπτογράφησης αλλά και το

αντίστροφο. Είναι επίσης πιθανό να υπάρχουν και έλεγχοι πλεονασμού και συνοχής ως μέτρο αντιμετώπισης.

Ένας άλλος τρόπος για να ματαιώσει κανείς αυτές τις επιθέσεις είναι να διπλασιάσει τον υπολογισμό των τελευταίων γύρων κρυπτογράφησης, εξοικονομώντας έτσι χρόνο υπολογισμού. Ωστόσο ένα κρίσιμο και δύσκολο ερώτημα είναι, ποιο θα πρέπει να είναι το πλήθος των γύρων που θα επιτάσσεται να προστατεύονται, για να αποκτηθεί ένα άρτιο επίπεδο ασφάλειας (Rivain 2009: 457). Ο δείκτης πολυπλοκότητας της ασφάλειας σε τέτοια σχήματα είναι συνήθως της ίδιας τάξης με εκείνη του υπολογισμού διπλασιασμού. Ένα μειονέκτημα του υπολογισμού διπλασιασμού, είναι η επεκτασιμότητα σχετικά με το πλήθος των γύρων που θα προστατεύουν.

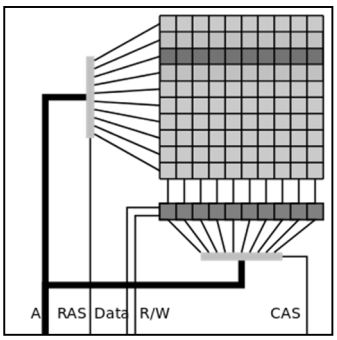
4.2.2 Row Hammer.

Στις δυναμικές μνήμες RAM (DRAM), κάθε δυαδικό ψηφίο από αποθηκευμένα δεδομένα καταλαμβάνει ένα ξεχωριστό κελί μηνύματος το οποίο ηλεκτρονικά υλοποιείται είτε με ένα πυκνωτή είτε με ένα ολοκληρωμένο κύκλωμα. Η κατάσταση φόρτισης ενός πυκνωτή είναι αυτή η οποία καθαρίζει εάν η δυναμική μνήμη DRAM αποθηκεύει την κατάσταση 1 ή την κατάσταση 0 σε κάθε ένα από τα κελιά μνήμης ως δυαδική τιμή. Ένα τεράστιο πλήθος από τέτοια κελιά «στοιβάζονται» στα ολοκληρωμένα κυκλώματα. (Kim, et al 2014: 362).

Τα κελιά μνήμης οργανώνονται σε πίνακες και λαμβάνουν διεύθυνση από τις στήλες και τις γραμμές του πίνακα που βρίσκονται. Η διεύθυνση της μνήμης χωρίζεται σε διεύθυνση στήλης και διεύθυνση γραμμής, οι οποίες υπόκεινται σε επεξεργασία από τους αποκωδικοποιητές. Με αυτή τη διαδικασία γίνεται η προσπέλαση στα δεδομένα, που είναι αποθηκευμένα σε κάθε κελί μνήμης.

Ωστόσο οι διαδικασίες ανάγνωσης μπορεί να έχουν καταστροφικά αποτελέσματα, με την έννοια του ότι τα κύτταρα μνήμης αρχίζουν να αποφορτίζονται και θα πρέπει να γίνει μία διαδικασία επανεγγραφής τους, ώστε τα δεδομένα τους να παραμείνουν αναλλοίωτα. Οι διαδικασίες επανεγγραφής είναι κοινές για όλα τα κελιά μνήμης. Ως αποτέλεσμα του

σχεδιασμού τους ολόκληρες γραμμές δεδομένων ξαναγράφονται εάν έστω μόνο η τιμή ενός δυαδικού ψηφίου αλλάξει.



Εικόνα 21. Επανεγγραφή Δεδομένων.

Η επίθεση Row Hammer είναι μία παρενέργεια στη δυναμική μνήμη τυχαίας προσπέλασης DRAM, που προκαλεί στα κύτταρα μνήμης διαρροή της φόρτισης που έχουν. Απόρροια αυτού είναι να αλληλεπιδρούν ηλεκτρικά μεταξύ τους, κάνοντας πιθανή μία αλλαγή του περιεχομένου των κοντινών σειρών μνήμης, που στην πραγματικότητα δεν απευθύνεται στην αρχική τιμή του κελιού μνήμης. Αυτή η καταστρατήγηση της απομόνωσης την οποία θα πρέπει να έχουν τα δεδομένα των κελιών στις μνήμες DRAM, είναι αποτέλεσμα της υψηλής πυκνότητας στις σύγχρονες DRAM μνήμες. Η πυροδότησή τους μπορεί να γίνει από ειδικά δημιουργημένα πρότυπα πρόσβασης μνήμης που ενεργοποιούν ταχέως τις ίδιες σειρές μνήμης πολλές φορές (Kim, et al 2014: 363).

Τα ολοκληρωμένα κυκλώματα DRAM τα οποία τείνουν να σχεδιάζονται με υψηλότερη συχνότητα, έχουν οδηγήσει στην κατασκευή μικρότερων κελιών μνήμης σε φυσικό επίπεδο. Τα οποία κελιά είναι σε θέση να αποθηκεύσουν μικρότερα φορτία. Με αποτέλεσμα την μείωση των περιθωρίων θορύβου, την αύξηση των ποσοστών των ηλεκτρομαγνητικών αλληλεπιδράσεων μεταξύ των κυττάρων μνήμης και υψηλότερες δυνατότητες για την απώλεια δεδομένων.

Απόρροια αυτού είναι η παρατήρηση διαταρακτικών σφαλμάτων, που προκαλείται από τα ίδια τα κελιά μνήμης, προκαλώντας την παρέμβαση της λειτουργίας μεταξύ τους. Η εκδήλωση γίνεται με τυχαίες αλλαγές στις τιμές των bits που αποθηκεύονται στα κύτταρα μνήμης που επηρεάζονται (Kim, et al 2014: 364).

Επιπρόσθετα η τεχνική Row Hammer έχει επηρεάσει και τις δυναμικές μνήμες τρίτης γενιάς (DDR3), στις οποίες η συχνή ενεργοποίηση των γραμμών μνήμης προκαλεί διακυμάνσεις τάσης στις συσχετισμένες επιλεγμένες γραμμές μνήμης. Έτσι, στην περίπτωση αυτή, αν τα κελιά μνήμης τα οποία έχουν προσβληθεί δεν ανανεώνονται πριν χάσουν πάρα πολύ από την φόρτισή τους, τότε πραγματοποιούνται σφάλματα διαταραχής (Kim, et al 2014: 364).

Υπάρχουν αρκετοί τρόποι για να μετριαστεί το φαινόμενο Row Hammer, ορισμένοι από αυτούς επιτάσσουν την καθιέρωση πιο συχνών ανανεώσεων μνήμης, με διάστημα ανανέωσης μικρότερο των 64ms, η οποία θα επιφέρει μεγαλύτερη κατανάλωση ενέργειας αλλά και περισσότερη επιβάρυνση στην επεξεργασία. Αυτό από μόνο του αποτελεί μία λιγότερο αποτελεσματική κίνηση, μιας και όπως έχει ήδη αναφερθεί τα ασύρματα δίκτυα αισθητήρων στερούνται τόσο μνήμης όσο και υπολογιστικής ισχύς.

Οι επιπτώσεις από μια επίθεση του τύπου Row Hammer είναι πολλές και ποικίλες. Τούτο γιατί η προστασία της μνήμης, ως ένας τρόπος για την πρόληψη από πρόσβαση σε μνήμη που δεν έχει εκχωρηθεί, είναι μία αρκετά σημαντική έννοια. Έτσι κακόβουλα προγράμματα λογισμικού θα είναι σε θέση να ενεργοποιούν συχνά μία συγκεκριμένη σειρά μνήμης - γεγονός το οποίο μπορεί να προκαλέσει απώλεια δεδομένων. Δυστυχώς η πρακτική έχει δείξει ότι τέτοια προγράμματα είναι αρκετά εύκολο να γραφούν. Έτσι σε μέλλοντα χρόνο και σε μελλοντικής κατασκευής μνήμες DRAM, η επίθεση Row Hammer όχι μόνο θέτει ένα ζήτημα αξιοπιστίας, αλλά επίσης θα παρουσιάσει ένα ζήτημα ασφάλειας. Το ζήτημα αυτό θα επιτάσσει εάν ένα κακόβουλο πρόγραμμα θα μπορεί να προκαλέσει απώλεια δεδομένων τη στιγμή που θα τρέχει παράλληλα με ένα άλλο πρόγραμμα (Kim, et al 2014: 9).

4.2.3 Επίθεση Ψυχρής Εκκίνησης.

Η επίθεση ψυχρής εκκίνησης (Cold-Boot) αποτελεί ένα τύπο επίθεσης παράπλευρου καναλιού, στην οποία ο επιτιθέμενος κάνει χρήση του φαινομένου της παραμένουσας μαγνήτισης στις μνήμες DRAM και SDRAM, έτσι ώστε να αναγνώσει τα δεδομένα από τις

μνήμες που υπάρχουν εγκατεστημένες σε ένα υπολογιστικό σύστημα όταν αυτό τερματίσει την λειτουργία του (Van Tilborg, Jajodia 2011: 274).

Οι δυναμικές μνήμες RAM (DRAM) οι οποίες χρησιμοποιούνται στους περισσότερους σύγχρονους υπολογιστές διατηρούν τα περιεχόμενά τους για αρκετό χρονικό διάστημα μετά την διακοπή της τροφοδοσίας τους με ενέργεια, ακόμα και αν η διακοπή τροφοδοσίας πραγματοποιείται σε θερμοκρασία δωματίου, αλλά και ακόμα, αν το στοιχείο της μνήμης έχει αφαιρεθεί από τη μητρική κάρτα. Αν και οι μνήμες DRAM γίνονται λιγότερο αξιόπιστες όταν δεν προχωρούν σε συνεχή ανανέωση των δεδομένων τους (Refresh), εν τούτοις δεν διαγράφουν αμέσως τα δεδομένα που περιέχουν και τα δεδομένα τους γίνονται εν δυνάμει, απόκτημα επίδοξων υποκλοπέων οι οποίοι μπορούν να θέσουν υπό τον έλεγχό τους τμήματα μνήμης του συστήματος (Halderman, et al 2008: 52).

Ένας υπολογιστής ο οποίος εκτελεί κρυπτογραφικό λογισμικό, βασίζεται πάνω στο λειτουργικό σύστημα για την ασφάλεια οποιουδήποτε κλειδιού πρέπει να προστατεύσει, το οποίο βρίσκεται στη μνήμη κατά την διάρκεια των υπολογισμών. Σε μια επίθεση Cold-Boot ο επιτιθέμενος καταστρέφει την προστασία του λειτουργικού συστήματος, κάνοντας μία ανάγνωση του περιεχομένου της μνήμης απευθείας από τα στοιχεία των RAM. Αυτό μπορεί να επιτευχθεί με φυσική πρόσβαση, αφαιρώντας την ενέργεια του υπολογιστικού συστήματος είτε επαν-εκκινώντας το σε ένα συνήθως μικρό πυρήνα (Cold- Boot) ή μεταφυτεύοντας τα φυσικά στοιχεία της μνήμης RAM σε ένα διαφορετικό υπολογιστή για να διαβαστούν. Στην τελευταία αυτή περίπτωση, το chip της μνήμης ενδέχεται να ψυχθεί για να αυξηθεί η διατήρηση των δεδομένων κάνοντας χρήση ενός φιαλιδίου "ψυχρού πάγου", ψεκάζοντας απευθείας πάνω στο chip μνήμης ή κάνοντας χρήση υγρού αζώτου ώστε να διατηρηθεί το στοιχείο της μνήμης ψυχρό για μεγάλο χρονικό διάστημα. Σε θερμοκρασία δωματίου τα σύγχρονα chips είναι σε θέση να διατηρήσουν τα δεδομένα τους για αρκετά δευτερόλεπτα. Κάτω από τη θερμοκρασία δωματίου είναι σε θέση να διατηρήσουν τα δεδομένα τους για αρκετές ώρες ακόμα και για μέρες (Van Tilborg, Jajodia 2011: 273).

Μία επίθεση cold-boot μπορεί να χρησιμοποιηθεί εναντίον τόσο κρυπτογραφίας συμμετρικού κλειδιού, όσο και κρυπτογραφίας δημοσίου κλειδιού. Στις δύο περιπτώσεις, επιπρόσθετες πληροφορίες, όπως το σχέδιο του κλειδιού μπορούν να χρησιμοποιηθούν

για τον αυτοματισμό της έρευνας των κλειδιού στη μνήμη και για την ανακατασκευή ενός κλειδιού που λήφθηκε από την εικόνα του κλειδιού που βρίσκεται σε αποσύνθεση στο στοιχείο μνήμης που έχει δεχθεί την επίθεση (Van Tilborg, Jajodia 2011: 273).

Τόσο η μνήμη DRAM όσο και η μνήμη RAM είναι πτητικές μνήμες αποθήκευσης, αλλά και οι δύο μπορούν να διατηρούν τα δεδομένα χωρίς ρεύμα για μερικά δευτερόλεπτα σε θερμοκρασία δωματίου και ακόμα περισσότερο όταν ψύχεται. Οι δύο μνήμες παρουσιάζουν διαφορετικά πρότυπα φθοράς δεδομένων χωρίς την ύπαρξη ρεύματος κατά την πάροδο του χρόνου.

Η μνήμη SDRAM αποθηκεύει κάθε bit σε τέσσερα transistors σε μια σταθερή διαμόρφωση η οποία δεν χρειάζεται να ανανεώνεται ενώ η πηγή της ενέργειας είναι ανοικτή. Όταν η πηγή ενέργειας αφαιρεθεί και αποκατασταθεί, ένα κελί μνήμης SDRAM το οποίο έχει χάσει τα δεδομένα του μπορεί να εκκινήσει στην ίδια με πριν κατάσταση, παρόλο που το κελί το οποίο έχει αποθηκεύσει την ίδια τιμή για πάρα πολύ χρονικό διάστημα τείνει να βρεθεί σε κατάσταση "εγγραφής" δεδομένων της αυτής τιμής (Van Tilborg, Jajodia 2011: 274).

Η μνήμη DRAM αποθηκεύει κάθε bit σε ένα πυκνωτή. Ο πυκνωτής διαρρέει φόρτιση με την πάροδο του χρόνου και χρειάζεται περιοδικά να επαναφορτίζεται για να ανανεώσει την κατάστασή του. Έτσι, ένα κελί RAM το οποίο έχει χάσει τα δεδομένα του θα διαβαστεί σε γενικό πλαίσιο ως γείωση, η οποία μπορεί να είναι συνδεδεμένη είτε ως μηδέν (0) είτε ως ένα (1) (Van Tilborg, Jajodia 2011: 274).

4.2.4 Ροή Πληροφοριών και Μη Παρεμβολές.

Οι μη παρεμβολές (Non- Interference) είναι μια ιδιότητα η οποία απαγορεύει- περιορίζει τη ροή δεδομένων διαμέσου ενός συστήματος. Μπορεί να χρησιμοποιηθεί για να εκφράσει πτυχές της εμπιστευτικότητας και της ακεραιότητας.

Μία διαδικασία A μπορεί να ειπωθεί ότι είναι μη παρεμβατική με μία άλλη διαδικασία B σε ένα σύστημα M, εάν οι είσοδοι του A στο M δεν έχουν καμία συνέπεια στις εξόδους του

Μ προς τη διαδικασία Β. Η μη παρεμβατικότητα εξασφαλίζει μια εγγύηση ως προς την εμπιστευτικότητα: τούτο γιατί εάν οι παρατηρήσεις της διαδικασίας Β είναι απόλυτα ανεξάρτητες από τις ενέργειες της διαδικασίας Α, τότε το σύστημα Μ δεν έχει διαρροές προς την διεργασία Β για τις εισόδους της διεργασίας Α, και η διεργασία Α δεν μπορεί να αποκαλύψει μυστικά στη διεργασία Β διαμέσου του συστήματος Μ.

Οι μη παρεμβολές εξασφαλίζουν επίσης μια εγγύηση ακεραιότητας: τούτο διότι εάν καθόλου πληροφορίες δεν ρέουν από τη διεργασία Α στη Β, διαμέσου του Μ, τότε η Β δεν μπορεί να καταστραφεί από την Α διαμέσου του Μ.

Η μη παρεμβολή μπορεί να υιοθετηθεί και από άλλα μοντέλα υπολογισμού πέραν των ντετερμινιστικών μηχανών. Ωστόσο αυτή η υιοθέτηση έχει αποτελέσματα σε περισσότερες από μία λογικές ιδιότητες, ιδιαίτερα, εάν ένα μοντέλο κάνει την παραδοχή μιας μη παρεμβολικής συμπεριφοράς. Στην λεγόμενη ντετερμιστική προσέγγιση για τον καθορισμό της μη παρεμβολής στα μη παρεμβολικά μοντέλα υπάρχει μια απαίτηση, για κάθε δοθείσα είσοδο από το Β, η έξοδος του Μ στο Β πρέπει να είναι παρόμοια προς όλες τις πιθανές εισόδους του Α σε όλες τις εκτελέσεις οι οποίες είναι πιθανές για τις δοθείσες του Μ εισόδους Α και Β. Σε αντίθεση με τα παραπάνω, η μη παρεμβολή καθορίζεται ως μία κλειστή ειδικότητα σε κάθε σετ/ ομάδας πιθανών εκτελέσεων του Μ συστήματος, στη λεγόμενη πιθανολογική προσέγγιση.

Η μη παρεμβολή μπορεί να χρησιμοποιηθεί για την εγγύηση της έκφρασης της εμπιστευτικότητας και της ακεραιότητας. Ως εκ τούτου, αυτές οι ιδιότητες μπορούν να χρησιμοποιηθούν για την πιστοποίηση ασφάλειας που απαιτείται σε ένα επίσημο μοντέλο ασφάλειας. Οι ιδιότητες της μη παρεμβολής δεν περιορίζονται σε ένα συγκεκριμένο στρώμα του συστήματος, ειδικότερα μπορούν να χρησιμοποιηθούν για τα προγράμματα, τις εφαρμογές καθώς και για το λογισμικό σε επίπεδο συστήματος.

Το λεγόμενο ξετύλιγμα (Unwinding) είναι μία τεχνική επαλήθευσης που μπορεί να χρησιμοποιηθεί για την απλοποίηση της απόδειξης ότι ένα δοθέν σύστημα ικανοποιεί την ικανότητα της μη παρεμβολής κάτω από μία δοθείσα πολιτική ασφάλειας. Η ανάλυση της σύστασης είναι πιθανή, αλλά μόνο μερικές μεταβλητές της μη παρεμβολής διατηρούνται σε σύνθεση, σε γενικές γραμμές.

Μια σημαντική πρόκληση είναι να κατασκευαστούν συστήματα λογισμικού, έτσι ώστε να έχουν ασφαλή ροή πληροφορίας από την κατασκευή. Αυτό απαιτεί μία πιο βαθιά κατανόηση της διασύνδεσης μεταξύ της κατασκευής λογισμικού και της ασφάλειας στη ροή δεδομένων. θεμελιώδη ζητήματα που απαιτούν πρόσθετες διερευνήσεις είναι:

Πρώτο, χρειάζεται μια διευκρίνιση για το πώς ένας δοθέν μηχανισμός ασφαλείας συμβάλει στην επιβολή ενός ευρέος συστήματος, ανακηρύσσοντας συγκεκριμένες ιδιότητες ασφάλειας όπως η μη παρεμβολή. Επί του παρόντος, υπάρχει μία σημαντική εννοιολογική διαφορά μεταξύ των εγγυήσεων που παρέχονται από τους μηχανισμούς ασφαλείας και τους μηχανισμούς ασφαλείας σε ολόκληρο το σύστημα ασφαλείας της ροής πληροφοριών.

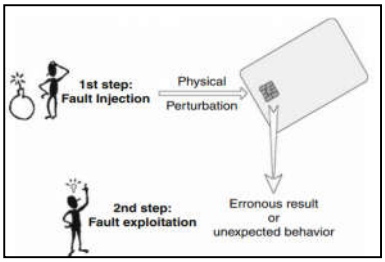
Δεύτερο, χρήσιμα κριτήρια μπορεί να χρησιμοποιηθούν για να επιτρέψουν ότι ο προσδιορισμός πολλαπλών μηχανισμών ασφάλειας είναι επαρκής για να εγγυηθεί ότι η ολότητα του συστήματος έχει μια ασφαλή ροή δεδομένων. Δηλαδή, η παραδοσιακή μηχανισμό-κεντρική προσέγγιση για την ασφάλεια πρέπει να σημειωθεί από μία προσέγγιση ιδιοτήτο-κεντρική.

Τρίτο, οι έννοιες της αφαίρεσης, της σύνθεσης, της αποσύνθεσης και της διακίνησης, πρέπει να αναπτυχθούν ώστε να είναι κατάλληλα εργαλεία σκέψεις για την τεχνολογία λογισμικού, καθώς και για την επίτευξη της ασφάλειας της ροής πληροφοριών. Επί του παρόντος η μηχανική κατασκευής λογισμικού δεν σέβεται την ασφάλεια της ροής πληροφοριών, οδηγώντας σε απαραίτητες πιθανότητες αθέμιτης ροής δεδομένων διαμέσου μυστικών καναλιών και παράπλευρων καναλιών.

Τέταρτο, επίσημα πιστοποιημένες εγγυήσεις για την ασφάλεια πληροφοριών πρέπει να χρησιμοποιηθούν στα πιστοποιητικά ασφαλείας ώστε να παρέχεται μία αξιόπιστη διαβεβαίωση ασφαλείας, αλλά και το ότι να είναι επίσης κατανοητή. Σε αντίθετη περίπτωση οι εν δυνάμει πελάτες ενός συστήματος δεν θα είναι σε θέση να εκτιμήσουν τα πλεονεκτήματα της ασφάλειας του ενός συστήματος ενάντια του άλλου.

4.2.5 Επίθεση Σφάλματος.

Μια επίθεση σφάλματος (Fault Attack) είναι μία επίθεση πάνω σε μια φυσική ηλεκτρονική συσκευή, η οποία «αναγκάζει» μια συσκευή να περιέλθει σε μία όχι επιθυμητή κατάσταση με ένα εξωτερικό τρόπο όπως, π.χ., χρησιμοποιώντας τάση ρεύματος, ή το φως. Απώτερο σκοπό έχει να παράξει λάθη με τέτοιο τρόπο ώστε τα λάθη αυτά να οδηγήσουν σε μία επίθεση ασφαλείας του συστήματος. Η επίθεση αυτή μπορεί να έχει ως αποτέλεσμα την ανάκτηση του κλειδιού.



Εικόνα 22. Επίθεση σφάλματος σε κάρτα

Θα εστιάσουμε, για την περιγραφή των επιθέσεων αυτών, στη περίπτωση μίας κάρτας που περιέχει ενσωματωμένο ολοκληρωμένο κύκλωμα (ICC), αν και πρέπει να σημειωθεί ότι αντίστοιχες τεχνικές αυτής της επίθεσης μπορούν να εφαρμοστούν και σε άλλα περιβάλλοντα.

Μια επιτυχής επίθεση σφάλματος πάνω σε ένα ενσωματωμένο κύκλωμα μίας κάρτας (ICC) προϋποθέτει δύο βήματα, την έγχυση σφάλματος και την εκμετάλλευση σφάλματος (Van Tilborg, Jajodia 2011: 274).

4.2.5.1 Έγχυση Σφάλματος.

Το πρώτο βήμα περιέχει την έγχυση του σφάλματος στον κατάλληλο χρόνο κατά την διάρκεια της διαδικασίας. Η έγχυση σφάλματος είναι εξαρτώμενη σε μεγάλο βαθμό από το υλικό και κατ' επέκταση από το ενσωματωμένο ολοκληρωμένο κύκλωμα (ICC). Το δεύτερο βήμα έχει να κάνει με την αξιοποίηση του λανθασμένου αποτελέσματος ή της απροσδόκητης συμπεριφοράς. Η εκμετάλλευση του σφάλματος εξαρτάται από τον

σχεδιασμό του λογισμικού και από την υλοποίησή του. Έτσι, στην περίπτωση ενός αλγορίθμου, θα εξαρτηθεί από τις προδιαγραφές των δεδομένων του, δεδομένου ότι η εκμετάλλευση σφάλματος θα βρίσκεται σε συνδυασμό, τις περισσότερες φορές, με κλασικές τεχνικές κρυπτανάλυσης. Ανάλογα με τον τύπο της ανάλυσης που πραγματοποιήθηκε, η έγχυση σφάλματος θα πρέπει να πραγματοποιηθεί σε μια συγκεκριμένη στιγμή ή περίπου σε μια δεδομένη χρονική περίοδο (Van Tilborg, Jajodia 2011: 275)

Υπάρχουν πολλοί τρόποι για να παράγει κανείς ένα σφάλμα σε ένα ενσωματωμένο κύκλωμα. Έως τώρα υπάρχουν τρεις κύριοι τρόποι ψευδούς έγχυσης που μπορούν να διακριθούν:

- Ηλεκτρική διαταραχή στο πρότυπο ISO της επαφής της κάρτας.
  - VCC (Video Capture Card) δυσλειτουργία.
  - Κύκλοι ρολογιού ή/ και αλλαγή συχνότητας.
- Διατάραξη ακτίνας φωτός
  - Σφαιρική/ καθολική ακτίνα φωτός. (Ευρύ φάσμα)
  - Εστιασμένη ακτίνα φωτός. (Ευρύ φάσμα)
  - Ακτίνα Laser. (Μονή δέσμη)
- Ηλεκτρομαγνητική διαταραχή τομέα.

Η αποτελεσματικότητα της κάθε μεθόδου ψευδούς έγχυσης εξαρτάται σε μεγάλο βαθμό από τον σχεδιασμό του υλικού, την μέθοδο κατασκευής και την τεχνολογία υλοποίησης της κατασκευής. Η συμπεριφορά του chip πάνω από την πίεση της ψευδούς έκχυσης μπορεί να είναι τεσσάρων τύπων:

- Μη επίδρασης.
- Λάθος αποτελέσματος ή απροσδόκητης συμπεριφοράς.
- Καμιάς απάντησης από την κάρτα.
- Νεκρής κάρτας.

Προφανώς, μόνο μία από τις τέσσερις περιπτώσεις που παρατίθενται στην πιο πάνω λίστα μπορεί να είναι προς εκμετάλλευση. Επιπλέον, η διαταραχή μπορεί να έχει μια παροδική επίδραση ή μόνιμη επίδραση, ή ένα ενδιάμεσο στάδιο μεταξύ των καταστάσεων:

- Παροδικό αποτέλεσμα.
- Ημι-μόνιμη επίδραση.
- Μόνιμη επίδραση.

Η κυρία δυσκολία στην έγχυση σφάλματος είναι η ανεύρεση των κατάλληλων παραμέτρων της διατάραξης για το ολοκληρωμένο κύκλωμα που αποτελεί στόχο. Ακατάλληλες παράμετροι δεν θα οδηγήσουν σε εκμεταλλεύσιμα σφάλματα, όπως ένα λάθος αποτέλεσμα ή μία απροσδόκητη συμπεριφορά. Ως εκ τούτου, υπάρχει κίνδυνος το τσιπ να εκτεθεί σε ανεπανόρθωτα σφάλματα. Εκτός αυτού, εάν το υλικό υλοποιεί κάποιους αισθητήρες ασφαλείας ή και μηχανισμούς προστασίας, θα είναι ακόμα πιο δύσκολο να εγχυθεί ένα εκμεταλλεύσιμο σφάλμα χωρίς να ενεργοποιηθεί ένας μηχανισμός ασφάλειας.

4.2.5.2 Εκμετάλλευση Σφαλμάτων.

Η εκμετάλλευση σφαλμάτων είναι το υποχρεωτικό δεύτερο βήμα για μια επιτυχημένη επίθεση σφάλματος. Η εκμετάλλευση σφαλμάτων εξαρτάται άμεσα από το αποτέλεσμα σφαλμάτων, τον εντοπισμό σφαλμάτων στο χρόνο, καθώς και το στόχο της επίθεσης. Δύο βασικοί τύποι του στόχου μπορούν να διακριθούν για μία επίθεση σφάλματος:

- Το λειτουργικό σύστημα και η ευαίσθητη εφαρμογή.
- Ο κρυπτογραφικός αλγόριθμος.

Η ευαίσθητη εφαρμογή μπορεί να καθοριστεί ως ένα τμήμα κώδικα το οποίο επεξεργάζεται δεδομένα τα οποία είναι γνωστά στον εξωτερικό κόσμο αλλά θα πρέπει να τροποποιηθούν. Η ψευδής έγχυση θα τροποποιήσει ακριβώς αυτά τα δεδομένα. Από

τα παραπάνω γίνεται σαφές ότι τα δεδομένα δεν θα πρέπει τροποποιηθούν, και αυτό γιατί. η τροποποίησή τους θα υπονομεύσει το σύστημα ασφαλείας σε κάποιο βαθμό.

Η διαφορική ανίχνευση σφάλματος (DFA, Differential Fault Analysis) συνίσταται κυρίως στην ανάλυση του αποτελέσματος ενός αλγορίθμου, υπό κανονική κατάσταση και σε μη κανονικές συνθήκες, για την ίδια είσοδο. Η ανώμαλη κατάσταση επιτυγχάνεται συνήθως με την έγχυση σφαλμάτων κατά τη διάρκεια της διαδικασίας (παροδική βλάβη) ή πριν από τη διαδικασία (μόνιμη βλάβη).

Εν κατακλείδι, μία επίθεση σφαλμάτων είναι μια απειλή για οποιοδήποτε κρίσιμο σημείο και θα πρέπει να λαμβάνεται υπόψη σε όλα τα στάδια του σχεδιασμού των προϊ όντων, αλλά και τις προδιαγραφές. Αντίμετρα και προστασία μπορούν να υλοποιηθούν τόσο με παρεμβάσεις υλικού όσο και με παρεμβάσεις λογισμικού για να ματαιωθούν τέτοιες επιθέσεις.

4.3 Τρόποι αντιμετώπισης – Λοιπά θέματα.

Οι παθητικές επιθέσεις παράπλευρου καναλιού μπορούν, όπως ειπώθηκε, να αντιμετωπιστούν με κατάλληλη υλοποίηση των κρυπτογραφικών διαδικασιών, έτσι ώστε τα μετρήσιμα μεγέθη που περιγράφονται ανωτέρω να μην εξαρτώνται από τα δεδομένα που επεξεργάζεται ο αλγόριθμος. Με άλλα λόγια, η αντιμετώπιση των επιθέσεων άπτεται κυρίως στην υλοποίηση της κρυπτογραφικής συσκευής και λειτουργίας – για αυτό και ονομάζονται και επιθέσεις υλοποίησης (implementation attacks). Ωστόσο, εξακολουθούν να παραμένουν επικίνδυνες, ακριβώς γιατί στην πράξη τα σχετικά θέματα υλοποίησης δεν λαμβάνονται σωστά υπόψη. Εξάλλου, το γεγονός ότι αυτές οι επιθέσεις είναι μη ανιχνεύσιμες (ο επιτιθέμενος δεν επεμβαίνει καθόλου στο σύστημα, ούτε καν εισάγοντας δεδομένα για να παρατηρήσει το πώς θα τα επεξεργαστεί η κρυπτογραφική συσκευή) τις καθιστά εξαιρετικά επικίνδυνες ως προς την ασφάλεια και εύκολα εφαρμόσιμες.

Πέρα από τις παθητικές επιθέσεις, περιγράφηκαν νωρίτερα και οι ενεργές επιθέσεις παράπλευρου καναλιού. Αυτές οι επιθέσεις συναντώνται συνήθως με το όνομα «ανάλυση

σφάλματος» (fault analysis), υπό την έννοια ότι ο επιτιθέμενος επηρεάζει τη λειτουργία της κρυπτογραφικής συσκευής, αναγκάζοντάς την να παράγει λανθασμένα αποτελέσματα στην έξοδό της, από τα οποία μπορεί να αποκαλύψει πληροφορία που θα έπρεπε να μείνει μυστική. Τέτοιες επιθέσεις είναι επίσης, συνήθως, σχετικά εύκολο να πραγματοποιηθούν, χωρίς υψηλό κόστος. Και σε αυτήν την περίπτωση πάντως, η αντιμετώπιση των επιθέσεων αυτών έχει να κάνει με τη σωστή υλοποίηση των κρυπτογραφικών συσκευών.

Όλα τα ανωτέρω μπορούν να εφαρμοστούν σε οποιαδήποτε κρυπτογραφική συσκευή, σε οποιοδήποτε περιβάλλον. Ωστόσο, οι επιθέσεις αυτές καθίστανται πιο εύκολα εφαρμόσιμες σε ασύρματα δίκτυα αισθητήρων, ακριβώς γιατί η φυσική πρόσβαση στους κόμβους ενός τέτοιου δικτύου (προκειμένου να γίνουν οι σχετικές μετρήσεις) είναι πιο εύκολο να πραγματοποιηθεί. Για αυτό το λόγο, στο υπόλοιπο της παρούσας διατριβής εστιάζουμε σε ασύρματα δίκτυα αισθητήρων.

Κεφάλαιο 5
Ασύρματα Δίκτυα Αισθητήρων.

5 Ασύρματα Δίκτυα Αισθητήρων.

Στο παρόν κεφάλαιο γίνεται μία περιγραφή των βασικών χαρακτηριστικών των ασύρματων δικτύων αισθητήρων, μέσω μιας ταξινόμησής τους με ορισμένα κριτήρια. Στο πρώτο τμήμα του τρέχοντος κεφαλαίου γίνεται μια ταξινόμηση με γνώμονα την φυσική τους υλοποίηση, ενώ στο δεύτερο τμήμα πραγματοποιείται μια παράθεση των χαρακτηριστικών των δικτύων αισθητήρων.

5.1 Κατηγορίες.

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks - WSN) αποτελούν δικτυακή τεχνολογία με αρκετή πρόοδο στην χρηστικότητά τους και αρκετή διείσδυση σε αρκετούς τομείς τις σύγχρονης τεχνολογίας, των επιστημών και της βιομηχανίας. Η δομή τους αποτελείται από ένα πλήθος μικροσκοπικών συσκευών, το μέγεθος των οποίων μπορεί να μην ξεπερνά αυτό του ενός νομίσματος, οι οποίες μπορεί στο πλήθος τους να αποτελούνται από μία ντουζίνα έως αρκετές χιλιάδες. Έχουν ενσωματωμένες υπολογιστικές δυνατότητες μέσω μιας μονάδας επεξεργασίας, περιορισμένες δυνατότητες μνήμης της τάξεως των ορισμένων δεκάδων Kb, μικρή πηγή τάσης ενέργειας (μπαταρία), όπως και ένα πλήθος αισθητήρων όπως αυτών της κίνησης, του

φωτός, της υγρασίας, της θερμοκρασίας, της δόνησης, της ταχύτητας του ανέμου κ.α. (Gay, et all 2002: 4).

Mote Type	WeC	rene2	rene2	dot	mica
					
Date	9/99	10/00	6/01	8/01	2/02
Microcontroller					
Type	AT90LS8535		ATMega163		ATMega103
Prog. mem. (KB)	8		16		128
RAM (KB)	0.5		1		4
Communication					
Radio	RFM TR1000				
Rate (Kbps)	10	10	10	10	10/40
Modulation type	OOK				OOK/ASK

Εικόνα 23. Χαρακτηριστικά ενός WSN

Ταυτόχρονα με το σχετικά μικρό μέγεθός τους, οι αισθητήρες ασύρματων δικτύων υπόκεινται και σε περιορισμούς ως προς τις δυνατότητές τους. Τούτο είναι εύλογο αν αναλογιστεί κανείς αυτά που αποτυπώθηκαν στην προηγούμενη παράγραφο, περί των σχετικά μικρών δυνατοτήτων σε επεξεργαστική ισχύ αλλά και σε ενέργεια.

Πέραν τούτων, τα ασύρματα δίκτυα αισθητήρων, αντιμετωπίζουν προβλήματα τα οποία άπτονται των δυνατοτήτων που έχουν στα θέματα συνεργασίας με όμορους αισθητήρες, μιας και η τοπολογία ή η δομή σε ένα δίκτυο ασύρματων δικτύων αισθητήρων προσεγγίζει το χαρακτηρισμό του αδόμητου δικτύου. Ωστόσο τείνουν να είναι σε θέση να πραγματοποιήσουν «ανιχνεύσεις» (όπως περιγράφονται στη συνέχεια) σε μεγάλη κλίμακα.

Αντικειμενικός τους σκοπός είναι να «πυροδοτήσουν» όλα τα απαραίτητα συστήματα ενημέρωσης, μόλις ο αισθητήρας ο οποίος φέρουν, ανιχνεύσει μεταβολές εκτός των ορισθέντων φυσιολογικών τιμών. Εν συνεχεία το μήνυμα «πυροδότησης», είτε από τον ίδιο αισθητήρα είτε με την αρωγή των υπολοίπων αισθητήρων, μεταφέρεται στο κέντρο ελέγχου. Πρέπει να τονιστεί ότι τα ασύρματα δίκτυα αισθητήρων δεν χρησιμοποιούνται αποκλειστικά ως εργαλείο συναγερμού, αλλά και ως βοηθήματα παρατήρησης και καταγραφής δεδομένων και καταστάσεων, τόσο στον πολιτικό όσο και στον αμυντικό τομέα.

Αρκεί κανείς να σταθεί στο πλήθος και τη σημασία των εφαρμογών που κάνουν χρήση ασύρματων δικτύων αισθητήρων για να μπορέσει να αντιληφθεί τη σημασία τους. Ενδεικτικά μπορεί να παρατεθούν επιγραμματικά οι ακόλουθες εφαρμογές: α) η παρακολούθηση απομακρυσμένων περιοχών για ακραία φυσικά φαινόμενα, όπως οι πυρκαγιές, οι πλημμύρες, ή ακόμα η ηφαιστειακή δραστηριότητα και η σεισμικότητα μιας περιοχής, β) εφαρμογές που έχουν άμεση σχέση με τη βιομηχανία ή την οικονομική ανάπτυξη όπως η "καλλιέργεια ακριβείας", γ) η παρακολούθηση των καταπονήσεων των δομικών υλικών τόσο στον κατασκευαστικό κλάδο όσο και στο βιομηχανικό κλάδο, δ) εφαρμογές στην ιατρική και στην κτηνιατρική, ε) σε εφαρμογές καθημερινότητας, όπως στο πλαίσιο υλοποίησης του Διαδικτύου των Πραγμάτων (Internet of Things). Σαφώς το πλήθος των εφαρμογών δεν εξαντλείται εδώ, στο εισαγωγικό όμως αυτό χωρίο αποτελεί πλεονασμό η οποιαδήποτε περαιτέρω ανάλυση.

5.1.1 Κατηγοριοποίηση Ασύρματων Δικτύων Αισθητήρων.

Ανάλογα με το χώρο, τη χρήση ενός δικτύου, αλλά και το περιβάλλον εγκατάστασης, τα ασύρματα δίκτυα αισθητήρων μπορούν να ταξινομηθούν σε: υπέργεια, υπόγεια, υποθαλάσσια, δίκτυα πολυμέσων και κινητά ασύρματα δίκτυα αισθητήρων (Yick, et al 2008: 2292).

5.1.2 Υπέργεια.

Τα υπέργεια ασύρματα δίκτυα αισθητήρων στην τυπική τους διαμόρφωση περιλαμβάνουν από μερικές δεκάδες έως ορισμένες χιλιάδες ασύρματους κόμβους οι οποίοι είναι εγκατεστημένοι σε μία δοθείσα γεωγραφική περιοχή, είτε ως ad-hoc δίκτυα είτε με τρόπο ο οποίος έχει προεπιλεγεί για την τοποθέτησή τους. Στην ad-hoc διάταξη, οι κόμβοι μπορούν να τοποθετούνται στη σχεδιαζόμενη τοποθεσία τους ακόμα και με εναέρια μέσα, είτε μπορούν να τοποθετηθούν τυχαία στο χώρο χωρίς καμία διάταξη. Κατά την προσχεδιασμένη διευθέτηση των κόμβων, υπάρχει ένα προαποφασισμένο πλέγμα ανάπτυξης των κόμβων το οποίο στηρίζεται είτε στην βέλτιστη δυνατή τοποθέτηση, είτε σε δισδιάστατο μοντέλο, είτε σε τρισδιάστατο μοντέλο τοποθέτησης.

Σε κάθε υπέργειο ασύρματο δίκτυο αισθητήρων, η αξιόπιστη επικοινωνία είναι ιδιαίτερα σημαντική, ειδικά όταν έχει να αντιμετωπίσει ένα πυκνό πλέγμα επικοινωνίας. Οι κόμβοι επικοινωνίας θα πρέπει να είναι σε θέση να στείλουν τα δεδομένα τους πίσω στο σταθμό βάσης, επομένως θα πρέπει να είναι σε θέση να επικοινωνούν με το σταθμό της βάσης σε ικανοποιητικό βαθμό. Παρά το γεγονός ότι υπόκεινται σε περιορισμούς, όσον αφορά την πηγή ενέργειας την οποία μπορούν να φέρουν, έχουν τη δυνατότητα να εφοδιαστούν με δευτερεύουσα πηγή ενέργειας, όπως παραδείγματος χάριν, έναν ηλιακό συλλέκτη. Σε κάθε περίπτωση είναι αρκετά σημαντικό οι κόμβοι να μπορούν να διατηρήσουν την ενέργεια. Τα υπέργεια ασύρματα δίκτυα αισθητήρων έχουν την ικανότητα να διατηρήσουν ενέργεια κάνοντας εφαρμογή ορισμένων μεθόδων όπως η χρήση δρομολόγησης δεδομένων με πολλαπλά άλματα (multi hop), και η χρήση μικρής εμβέλειας μετάδοσης - εξαλείφοντας έτσι τον πλεονασμό δεδομένων και ελαχιστοποιώντας τις καθυστερήσεις που τυχόν μπορεί να συμβούν.

5.1.3 Υπόγεια.

Τα υπόγεια ασύρματα δίκτυα αισθητήρων (Yick et al, 2008: 2295) περιλαμβάνουν ένα πλήθος αισθητήρων οι οποίοι είναι ενταφιασμένοι. Σε ορισμένες περιπτώσεις ενδέχεται να συναντηθούν είτε σε σπηλαιώσεις είτε σε ορυχεία. Ωστόσο ο βασικός σκοπός παραμένει ο ίδιος, δηλαδή παρακολούθηση της υπόγειας δραστηριότητας (Akyildiz, Stuntebeck, 2006: 674). Επιπρόσθετα οι ενδιάμεσοι κόμβοι (Κόμβοι καταποντισμένοι-"νεροχύτης"), τοποθετούνται άνω του εδάφους (υπέργεια) έχοντας ως αντικειμενικό σκοπό να αναμεταδώσουν το σήμα από τους υπόγειους κόμβους στο σταθμό βάσης.

Με όρους κόστους εξοπλισμού ανάπτυξης, ένα υπόγειο ασύρματου δικτύου αισθητήρων είναι σαφώς πιο ακριβό από ένα υπέργειο ασύρματο δίκτυο αισθητήρων. Τούτο γιατί για να δημιουργηθεί μία αξιόπιστη επικοινωνία διαμέσου των πετρωμάτων και των διαφόρων υλικών που τυχόν θα συναντήσουν, θα πρέπει να γίνει χρήση ειδικού εξοπλισμού. Το υπόγειο περιβάλλον αποτελεί μία πρόκληση για τη μεταφορά των ασύρματων δεδομένων και εν γένει την ασύρματη επικοινωνία, τούτο διότι υπάρχει υψηλό ποσοστό απωλειών σήματος και υψηλό ποσοστό εξασθένησης σήματος.

Σε αντίθεση με τα υπέργεια ασύρματα δίκτυα αισθητήρων, η ανάπτυξη των υπόγειων ασύρματων δικτύων αισθητήρων προϋ ποθέτει προσεκτικό σχεδιασμάώστε να προσεχθεί το κόστος υλοποίησης, αλλά και η απαιτούμενη ενέργεια για την λειτουργία τους. Όπως και με όλους τους τύπους ασύρματων δικτύων αισθητήρων, έτσι και στα υπόγεια ασύρματα δίκτυα αισθητήρων οι κόμβοι είναι εξοπλισμένοι με περιορισμένους ενεργειακούς πόρους (μπαταρία). Επιπρόσθετα, εφόσον αναπτυχθούν, είναι εξαιρετικά δύσκολο να επαναφορτιστούν ή να αντικατασταθεί το στοιχείο ενέργειας που φέρουν.

Όπως και σε όλα τα ασύρματα δίκτυα αισθητήρων, η ενεργειακή επάρκεια είναι σημαντικό στοιχείο το οποίο πρέπει να λαμβάνεται σοβαρά υπόψη. Έτσι μπορεί να ειπωθεί ότι ένας αντικειμενικός σκοπός στην υλοποίηση των ασύρματων δικτύων αισθητήρων, είναι η ενεργειακή επάρκεια, έτσι ώστε να καταστεί δυνατή η αύξηση της ζωής του δικτύου. Αυτό μπορεί να επιτευχθεί με την συνεπικουρία πρωτοκόλλων επικοινωνίας με τα οποία θα πραγματοποιείται καλύτερη διαχείριση της ενέργειας.

5.1.4 Υποθαλάσσια.

Όταν γίνεται λόγος για τα υποθαλάσσια ασύρματα δίκτυα αισθητήρων, θα πρέπει να συμπεριλαμβάνει κανείς στη σκέψη του, ότι η δομή τους περιλαμβάνει ένα πλήθος από κόμβους και οχήματα τα οποία έχουν αναπτυχθεί στον υποθαλάσσιο χώρο. Κάνοντας μια αντιπαραβολή με τα υπέργεια ασύρματα δίκτυα αισθητήρων, τα οποία περιγράφηκαν ανωτέρω, μπορεί να εξαχθεί το συμπέρασμα ότι οι υποθαλάσσιοι κόμβοι, είναι πιο ακριβοί σε όρους χρηματικών μονάδων. Ωστόσο, για να υλοποιηθεί ένα υποθαλάσσιο δίκτυο απαιτούνται λιγότεροι κόμβοι (Akyildiz, Pompili, Melodia, 2004: 5).

Σε αντιδιαστολή με τα υπέργεια ασύρματα δίκτυα αισθητήρων, τα οποία ακολουθούν μια πυκνή διάταξη αισθητήρων, τα υποθαλάσσια δίκτυα αισθητήρων έχουν μια αραιή διάταξη κόμβων. Σε μία τυπική διάταξη, τα υποθαλάσσια δίκτυα κάνουν χρήση της μετάδοσης ακουστικών κυμάτων και να εγκαθιδρύσουν μία επικοινωνία. Αυτός ο τρόπος μετάδοσης όμως έχει ορισμένες προκλήσεις που συνάδουν με τον περιορισμό του εύρους ζώνης μετάδοσης, τη μεγάλη καθυστέρηση μετάδοσης αλλά και θέματα εξασθένησης του σήματος.

Σημείο πρόκλησης για τους υποθαλάσσιους αισθητήρες είναι οι αστοχίες λόγω των περιβαλλοντικών συνθηκών. Οι υποθαλάσσιοι κόμβοι θα πρέπει να είναι σε θέση να αυτορυθμίζονται και να προσαρμόζονται στις απαιτητικές συνθήκες του υποθαλάσσιου περιβάλλοντος. Όπως και με τους υπόγειους κόμβους, έτσι και με τους υποθαλάσσιους κόμβους, οι αισθητήρες είναι εξοπλισμένοι με μπαταρία περιορισμένης διάρκειας ζωής, η οποία δεν μπορεί ούτε να αντικατασταθεί αλλά είναι και αρκετά δύσκολο να επαναφορτιστεί. Αυτό αποτελεί αρκετά σημαντικό ζήτημα, μιας και απαιτείται υψηλή ενέργεια στην υποθαλάσσια επικοινωνία λόγω των μεγάλων αποστάσεων που πρέπει να διανύσει το ακουστικό σήμα, αλλά και της πιο περίπλοκης διεργασίας των σημάτων που πρέπει να εφαρμοστούν στο δέκτη λόγο του υποθαλάσσιου χώρου.

5.1.5 Ασύρματα Δίκτυα Αισθητήρων Δικτύου Πολυμέσων.

Τα ασύρματα δίκτυα αισθητήρων δικτύων πολυμέσων έχουν προταθεί για την παρακολούθηση και τον έλεγχο κάθε μορφής πολυμέσων όπως ήχου, εικόνας και βίντεο. Τα δίκτυα πολυμέσων περιέχουν ένα πλήθος από αρκετά οικονομικούς κόμβους οι οποίοι είναι εξοπλισμένοι με κάμερες και μικρόφωνα. Αυτού του είδους οι κόμβοι αισθητήρων διασυνδέονται μεταξύ τους κάνοντας χρήση ασύρματης σύνδεσης για την ανάκτηση των δεδομένων, τη συσχέτιση και τη συμπίεση των δεδομένων. Οι κόμβοι αισθητήρων πολυμέσων, έχουν αναπτυχθεί με ένα προσχεδιασμένο τρόπο στο περιβάλλον ανάπτυξης τους για να εξασφαλίσουν την απαραίτητη γεωγραφική κάλυψη (Sohraby, Minoli, Znati, 2007: 21).

Σαφώς, όπως και στις προηγούμενες περιπτώσεις, υπάρχουν ορισμένες προκλήσεις για τα πολυμεσικά ασύρματα δίκτυα αισθητήρων, όπως οι απαιτήσεις ως προς το εύρος ζώνης που πρέπει να χρησιμοποιηθεί, ως προς την κατανάλωση ενέργειας, ως προς την ποιότητα των υπηρεσιών (Quality of service), ενώ πρόκληση αποτελεί επίσης η χρήση τεχνικών συμπίεσης. Για παράδειγμα, το πολυμεσικό περιεχόμενο, όπως λόγου χάρη το βίντεο, απαιτεί υψηλό εύρος ζώνης για να γίνει εφικτή η μετάδοσή του. Αποτέλεσμα αυτού είναι η απαίτηση για υψηλή κατανάλωση ρεύματος. Αυτό όπως έχει ήδη ειπωθεί, αποτελεί μια σημαντική τροχοπέδη στην ανάπτυξη των ασυρμάτων δικτύων αισθητήρων (Sohraby, Minoli, Znati, 2007: 23).

5.1.6 Κινητά Ασύρματα Δίκτυα Αισθητήρων.

Τα κινητά ασύρματα δίκτυα αισθητηριακών, αποτελούνται από μία συλλογή από αισθητήρες οι οποίοι είναι σε θέση να μετακινηθούν με ιδία μέσα από την αρχική τους τοποθέτηση. Επίσης είναι σε θέση να αλληλοεπιδρούν με το φυσικό περιβάλλον στο οποίο βρίσκονται. Όπως και στους στατικούς κόμβους (υπέργειους, υποθαλάσσιους, υπόγειους, πολυμεσικούς) έτσι και οι κινητοί κόμβοι είναι σε θέση να εκτελέσουν κάποιες λειτουργίες, όπως η δυνατότητα να αισθανθούν, να κάνουν υπολογισμούς αλλά και να διεξάγουν επικοινωνία. Ωστόσο μια αρκετά σημαντική δομική διαφορά είναι η δυνατότητα να επανατοποθετηθούν στο χώρο και να οργανώσουν από μόνοι τους το δίκτυο (Sohraby, Minoli, Znati, 2007: 23).

Η αρχιτεκτονική των κινητών ασύρματων δικτύων αισθητήρων προτάσσει μία αρχική τοποθέτηση των κόμβων στο χώρο. Στη συνέχεια οι κόμβοι αυτοί μπορούν να αναδιαταχθούν όπου κρίνεται απαραίτητο, συλλέγοντας πληροφορίες για το χώρο τον οποίο βρίσκονται. Οι πληροφορίες που έχουν συλλεχθεί από τους κόμβους είναι σε θέση να προωθηθούν σε γειτονικούς κόμβους, πραγματοποιώντας έτσι μια διαδικασία αυτό-ενημέρωσης. Σημαντικό στοιχείο διαφοροποίησης είναι η διανομή των δεδομένων. Στα στατικά δίκτυα γίνεται χρήση στατικών και προκαθορισμένων διαδρόμων, ενώ στα κινητά δίκτυα γίνεται χρήση δυναμικής δρομολόγησης των δεδομένων (Sohraby, Minoli, Znati, 2007: 24).

5.2 Χαρακτηριστικά.

Ανάλογα με τη χρήση τα δίκτυα αισθητήρων κατασκευάζονται με διαφορετική αρχιτεκτονική, έτσι ώστε να μπορούν να ανταπεξέλθουν με το βέλτιστο δυνατό τρόπο στις απαιτήσεις του σχεδιασμού τους. Η πυκνότητα αλλά και η ποσότητα των κόμβων άπτονται της χρήσης τους. Επιπρόσθετα, κρίσιμο στοιχείο για την αρχιτεκτονική του δικτύου είναι η συνεργασία των κόμβων, η οποία πραγματοποιείται με τη χρήση πολλαπλών αλμάτων (Multi Hop). Κάνοντας μια εισαγωγική προσέγγιση μπορεί να γίνει

η κατηγοριοποίηση των κόμβων σε δύο βασικές κατηγορίες, την πηγή δεδομένων και τον δρομολογητή δεδομένων.

Με τον όρο πηγή δεδομένων (source) μπορούμε να κατατάξουμε οποιαδήποτε συσκευή η οποία είναι σε θέση να αντιλαμβάνεται («αισθάνεται») δεδομένα από το χώρο. Με άλλα λόγια, να έχει τη δυνατότητα να λαμβάνει δεδομένα και να τα επεξεργάζεται, αλλά και να τα μεταδίδει, δηλαδή να επικοινωνεί με άλλους σταθμούς. Ουσιαστικά τα δεδομένα λαμβάνονται κάνοντας μετρήσεις στο φυσικό περιβάλλον όπου έχει εγκατασταθεί το δίκτυο.

Ως δρομολογητή δεδομένων, μπορεί να ειπωθεί ότι πρόκειται για μια συσκευή η οποία αναλαμβάνει να διαβιβάσει τα δεδομένα τα οποία λαμβάνει από ένα κόμβο. Συνήθως ο κόμβος αυτός βρίσκεται γεωγραφικά κοντά του, σε ένα σταθμό βάσης, όπου και πραγματοποιείται η τελική επεξεργασία και ανάλυση των δεδομένων που συλλέχτηκαν από τους περιφερειακούς κόμβους.

Πέραν των ως άνω αναφερθέντων, υπάρχουν και άλλες τμηματοποιήσεις οι οποίες μπορούν να πραγματοποιηθούν για την ανάλυση των ασύρματων δικτύων αισθητήρων. Έτσι μπορεί να ειπωθεί ότι μία επιπρόσθετη τμηματοποίηση είναι με γνώμονα την αρχιτεκτονική που χρησιμοποιούν για την κατασκευή τους. Επίσης ένα ασύρματο δίκτυο αισθητήρων μπορεί να κατηγοριοποιηθεί με βάση το υλικό και το λογισμικό το οποίο χρησιμοποιείται.

5.2.1 Υλικό Ασύρματων Δικτύων Αισθητήρων.

Για να μπορέσει να υπάρξει ως οντότητα ένας κόμβος, θα πρέπει κατ' ελάχιστο το υλικό από το οποίο αποτελείται (Hardware) να έχει ένα σύστημα αισθητήρων, ένα σύστημα επεξεργασίας, ένα σύστημα επικοινωνίας και να σύστημα τροφοδοσίας.

Στο σύστημα αισθητήρων θα πρέπει να υπάρχει εκείνο το τεχνολογικό τμήμα το οποίο θα βοηθά να μετατρέπεται το ερέθισμα το οποίο λαμβάνεται από το φυσικό περιβάλλον σε μονάδα μετρήσιμη από ηλεκτρικές συσκευές - δηλαδή σε ηλεκτρικό ρεύμα.

Το σύστημα επεξεργασίας αποτελεί το τμήμα εκείνο το οποίο ως είσοδο λαμβάνει τα δεδομένα τα οποία λήφθηκαν από το σύστημα αισθητήρων και, ακολούθως, επεξεργάζεται δεδομένα αυτά. Επειδή κρίσιμο σημείο για την επιβίωση ενός κόμβου αισθητήρα είναι η ενεργειακή αυτονομία του, είναι κρίσιμης σημασίας η επιλογή επεξεργαστή ο οποίος στην ουσία θα πρέπει να είναι ένας μικροελεγκτής, ο οποίος θα απαρτίζεται από μνήμες τύπου Flash και Nand και επιπρόσθετα θα πρέπει να έχει εγκατεστημένους μετατροπείς αναλογικού σε ψηφιακό σήμα. Οι επιλογές αυτές κρίνονται ως ορθές με όρους μείωσης κόστους, αφού εξασφαλίζουν οικονομία τόσο στην κατανάλωση ενέργειας όσο και στον τελικό κόστος του μικρό-ελεγκτή του αισθητήρα. Τούτο γιατί αντικειμενικός σκοπός είναι η παραγωγή αισθητήρων οι οποίοι μπορούν εύκολα (από πλευράς κόστους) να αντικατασταθούν όταν αυτό απαιτηθεί.

Το σύστημα επικοινωνιών, όπως και όλα τα συστήματα επικοινωνιών τα οποία κάνουν χρήση ραδιοσυχνοτήτων, αποτελείται από έναν πομπό και έναν δέκτη: ο μεν πομπός μεταδίδει τα δεδομένα προς το περιβάλλον, ενώ ο δέκτης λαμβάνει τα δεδομένα από το περιβάλλον. Πρέπει να τονιστεί ότι το σύστημα επικοινωνιών είναι αυτό το οποίο καταναλώνει την περισσότερη ενέργεια. Συνέπεια αυτού είναι να επηρεάζεται η συνολική λειτουργία του αισθητήρα αλλά και η απόδοσή του.

Η λειτουργία του συστήματος τροφοδοσίας είναι η τροφοδότηση του αισθητήρα με ενέργεια. Η ενέργεια λαμβάνεται είτε από εσωτερική μπαταρία ιόντων λιθίου, είτε από μία εξωτερική πηγή, όπως ηλιακός συλλέκτης ή ένας αιολικός μετατροπέας. Ανάλογα με τη χρήση και το περιβάλλον ανάπτυξης, γίνεται και η αντίστοιχη επιλογή: τούτο γιατί, όπως έχει τονιστεί σε αρκετά σημεία της παρούσας μεταπτυχιακής διατριβής, αποτελεί αρκετά δύσκολο εγχείρημα η αντικατάσταση του συστήματος ενέργειας (μπαταρία) ενός αισθητήρα όταν αυτός διαταχθεί στο περιβάλλον. Με βάση όλα αυτά, μπορεί να δικαιολογηθεί η φιλοσοφία σχεδίασης ενός αισθητήρα κατά τρόπο τέτοιο ώστε να καταναλώνει την ελάχιστη δυνατή ενέργεια.

5.2.2 Λογισμικό Ασυρμάτων Δικτύων Αισθητήρων.

Επιπρόσθετα ένας αισθητήρας θα πρέπει να έχει κατ' ελάχιστο και ορισμένες μονάδες λογισμικού (Software) για να μπορέσει να συσταθεί σε ανεξάρτητη οντότητα. Τα τμήματα λογισμικού τα οποία απαιτείται να έχει ένας αισθητήρας πρέπει να είναι το λειτουργικό σύστημα, τα προγράμματα-οδηγοί (Drivers), οι επεξεργαστές επικοινωνίας και οι επιπρόσθετες εφαρμογές. Στις πιο κάτω γραμμές γίνεται μια επεξήγηση των ανωτέρω.

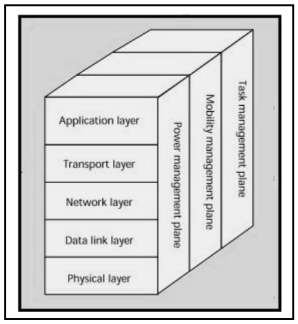
Το λειτουργικό σύστημα αποτελεί το κομβικό σημείο επικοινωνίας μεταξύ του μηχανικού επιπέδου και των πρόσθετων λογισμικών. Επίσης αποτελεί το τμήμα αυτό το οποίο επιτρέπει την διεπαφή με το χρήστη, δηλαδή την ανταλλαγή δεδομένων και την εξαγωγή πληροφοριών. Συνήθως αποτελείται από κώδικα ανοικτής αρχιτεκτονικής, πράγμα το οποίο σημαίνει ότι είναι αρκετά παραμετροποιήσιμο.

Τα προγράμματα οδήγησης (Drivers) είναι τα τμήματα λογισμικού τα οποία αναλαμβάνουν να διαχειριστούν τις βασικές λειτουργίες τόσο του πομπού όσο και του δέκτη. Επιπλέον, διαχειρίζονται και τη διαμόρφωση του σήματος, όπως επίσης και την αποκωδικοποίηση. Πρέπει να γίνει γνωστό ότι το φάσμα των ενεργειών που γίνονται στο φυσικό επίπεδο επίσης διαχειρίζονται από τα προγράμματα οδήγησης.

Οι επιπρόσθετες εφαρμογές είναι επιπρόσθετα τμήματα λογισμικού (συνήθως αρκετά μικρού μεγέθους), τα οποία έχουν ως κύρια λειτουργία την επεξεργασία των δεδομένων τα οποία λαμβάνει ένας αισθητήρας. Η επεξεργασία αυτή έχει ως αντικειμενικό σκοπό την εξαγωγή χρήσιμων συμπερασμάτων έτσι ώστε αυτά να αποτυπωθούν με μορφή χρήσιμη στον τελικό χρήστη ή στον ενδιάμεσο χρήστη του συστήματος.

5.2.3 Στοίβα Πρωτοκόλλου.

Η στοίβα πρωτοκόλλων που υλοποιούν οι κόμβοι ενός ασύρματου δικτύου αισθητήρων ενσωματώνουν όλα όσα εκφράστηκαν ως ανησυχίες που αναφέρονται για την ενέργεια, καθώς επίσης και ζητήματα δρομολόγησης (Rahman 2010 :78).



Εικόνα 24. Στοίβα πρωτοκόλλων WSN.

Τα επίπεδα, στα οποία είναι τμηματοποιημένη η στοίβα πρωτοκόλλων, είναι το φυσικό επίπεδο, το επίπεδο ζεύξης δεδομένων, το επίπεδο δικτύου, το επίπεδο μεταφοράς και το επίπεδο εφαρμογής. Από τα παραπάνω μπορεί να ειπωθεί ότι η στοίβα των πρωτοκόλλων στα ασύρματα δίκτυα αισθητήρων προσομοιάζει με αυτή του μοντέλου OSI.

5.2.4 Φυσικό Επίπεδο

Το φυσικό επίπεδο είναι υπεύθυνο για την επιλογή της συχνότητας που θα χρησιμοποιηθεί, την απλή και ισχυρή διαμόρφωση του σήματος, την ανίχνευσή του, την κρυπτογράφηση δεδομένων, την μετάδοση και τελικά την λήψη του σήματος. Αυτό το επίπεδο επίσης εξετάζει τις ανάγκες των τεχνικών διαμόρφωσης ώστε να επηρεάσει τις απαιτήσεις της ισχύος, αν και αυτό ακόμα θεωρείται περιοχή μη εξερευνημένη.

Ωστόσο υπάρχουν ανοιχτά ζητήματα για την υλοποίησή του. Τα ζητήματα αυτά άπτονται του σχεδιασμού των διαμορφωτών οι οποίοι θα πρέπει να είναι μικρού μεγέθους και χαμηλής κατανάλωσης, καθώς επίσης και ζητήματα στρατηγικών οι οποίες θα πρέπει να υιοθετηθούν για να αντιμετωπίσουν τα προβλήματα που ανακύπτουν κατά τη μετάδοση – διάδοσης του σήματος.

Όπως έγινε αναφορά και σε πιο πάνω γραμμές, σημαντικό στοιχείο προβληματισμού και «πεδίο δόξης λαμπρό» είναι το να επιτευχθεί αυτές οι εφαρμογές, όσον αφορά τις

απαιτήσεις υλικού, να υλοποιηθούν με τρόπο τέτοιο ώστε να καταλαμβάνουν τον ελάχιστο δυνατό χώρο.

5.2.4.1 Επίπεδο Ζεύξης Δεδομένων.

Το επίπεδο αυτό είναι υπεύθυνο για την δημιουργία της δικτυακής υποδομής, του διαμοιρασμού και της πρόσβασης στο μέσο επικοινωνίας μεταξύ των κόμβων αισθητήρων. Επίσης στο επίπεδο αυτό πραγματοποιείται η πολυπλεξία των ροών δεδομένων, η ανίχνευση πλαισίου δεδομένων και ο έλεγχος σφαλμάτων (Sohraby 2007: 24, Angel 2008: 8, Rahman 2010:78).

5.2.4.2 Επίπεδο Δικτύου.

Οι κόμβοι αισθητήρων είναι διασκορπισμένοι σε ένα πυκνό πεδίο και απαιτούνται πολύ-επίπεδα ασύρματα πρωτόκολλα δρομολόγησης ώστε να επικοινωνήσουν. Τα παραδοσιακά ad-hoc πρωτόκολλα δρομολόγησης δεν μπορούν να χρησιμοποιηθούν τόσο αποτελεσματικά στα δίκτυα αισθητήρων (Sohraby 2007: 24, Angel 2008: 8, Rahman 2010:78).

Θέματα σχεδιασμού που συναντώνται στο επίπεδο δικτύου των δικτύων αισθητήρων και πρέπει να αντιμετωπίζονται είναι: 1) αποδοτικότητα ενέργειας, 2) συνάθροιση δεδομένων, 3) συμπεριφορές που άπτονται της διεύθυνσης και γνώσεις τοποθεσίας του κόμβου, 4) δεδομένο-κεντρική δρομολόγηση (Rahman 2010 :78).

5.2.4.3 Επίπεδο Μεταφοράς.

Το επίπεδο αυτό είναι επιτακτικό και αναγκαίο όταν το σύστημα πρέπει να προσπελασθεί διαμέσου του διαδικτύου. Το πρωτόκολλο TCP, με τους μηχανισμούς διάδοσής του, πληροί τα χαρακτηριστικά του περιβάλλοντος ασύρματων αισθητήρων. Η

χρήση του TCP χρειάζεται προκειμένου το ασύρματο δίκτυο αισθητήρων να διαδράσει με τα άλλα δίκτυα, όπως το Διαδίκτυο.

Οι συνδέσεις TCP δημιουργούνται μεταξύ της βάσης και του κόμβου αισθητήρα. Η σύνδεση μεταξύ του χρήστη και το σταθμού βάσης πραγματοποιείται με τη χρήση του UDP και του TCP διαμέσου διαδικτύου ή σε άλλες περιπτώσεις διαμέσου δορυφόρου. Λόγω του ότι ένας κόμβος έχει ελάχιστη εσωτερική μνήμη, η σύνδεση μεταξύ του χρήστη και του σταθμού βάσης μπορεί να είναι αρκετά φτωχή με τη χρήση UDP πρωτοκόλλου (Sohraby 2007: 24, Angel 2008: 9, Rahman 2010:79).

Στον αντίποδα αυτού, στο TCP πρωτόκολλο, το οποίο κάνει χρήση παγκοσμίας διευθυνσιοδότησης, οι κόμβοι αισθητήρα χρησιμοποιεί ονοματοδοσία βάσει γνωρισμάτων (attribute-based naming) για να υποδείξουν τον προορισμό των πακέτων δεδομένων. Επιπρόσθετα, στους κόμβους του αισθητήρα, το επίπεδο μεταφοράς πρέπει να χειριστεί διαφορετικά παράγοντες όπως η κατανάλωση ενέργειας και η επεκτασιμότητα (Rahman 2010:79).

5.2.4.4 Επίπεδο Εφαρμογών.

Για τα δίκτυα αισθητήρων, τρία πιθανά πρωτόκολλα επιπέδου εφαρμογής μπορεί να χρησιμοποιηθούν. 1) Πρωτόκολλο διαχείρισης αισθητήρα (Sensor Management Protocol SMP), 2) Πρωτόκολλο ανάθεσης εργασίας και διάδοσης δεδομένων (Task assignment and Data Advertisement protocol TADAP) και 3) Πρωτόκολλο ερώτησης αισθητήρα και διάδοσης δεδομένων (Sensor Query and Data Dissemination Protocol SQDDP). (Sohraby 2007: 25, Angel 2008: 8, Rahman 2010:78)

5.2.4.5 Πρωτόκολλα Δρομολόγησης.

Σε γενικές γραμμές, η δρομολόγηση στα ασύρματα δίκτυα αισθητήρων μπορεί να διαιρεθεί σε ορισμένα πρωτοκόλλα: τα πρωτοκόλλα αυτά είναι: α) η δρομολόγηση διαμέρισης (flat base) η οποία χρησιμοποιείται όταν σε ένα μεγάλο πλήθος κόμβων κάθε

κόμβος έχει τον ίδιο ρόλο, β) Τοποθέτησης (routing), όταν οι κόμβοι αισθητήρων είναι διάσπαρτοι τυχαία σε μια περιοχή ενδιαφέροντος και κυρίως γνωστοί από τη γεωγραφική θέση όπου έχουν αναπτυχθεί, γ) Ιεραρχική δρομολόγηση (Hierarchical), όταν απαιτείται επεκτασιμότητα του δικτύου και αποτελεσματική επικοινωνία μεταξύ των κόμβων.

Επίσης ανάλογα με την τεχνική λειτουργίας του πρωτοκόλλου, τα πρωτόκολλα μπορούν να ταξινομηθούν σε: α) πολλαπλών διαδρομών, όπου πολλαπλά μονοπάτια επιλέγονται για την αποστολή των πακέτων του μηνύματος, β) ερωτημάτων όπου σε αυτήν την κατηγορία οι κόμβοι στέλνουν ερωτήματα στο δίκτυο για να λάβουν τα δεδομένα που χρειάζονται, γ) διαπραγμάτευσης, όπου το πρωτόκολλο χρησιμοποιεί υψηλού επιπέδου περιγραφή δεδομένων ώστε να αποφύγει περιττές μεταδόσεις δεδομένων, δ) Συνεκτικής δρομολόγησης, όπου στο πρωτόκολλο χρησιμοποιείται η επεξεργασία των δεδομένων όταν απαιτείται ενεργειακά αποδοτική δρομολόγηση. Επιπρόσθετα, ανάλογα με τη δυνατότητα η πηγή να βρίσκει μία διαδρομή προς τον προορισμό, μπορούν να κατηγοριοποιηθούν σε τρεις κατηγορίες, ήτοι: προληπτικά, αντιδραστικά και υβριδικά πρωτόκολλα (Rahman 2010: 81).

5.2.4.6 Πρωτόκολλο Προσπέλασης Κόμβων Ασύρματου Δικτύου.

Στο χωρίο αυτό θα γίνει προσπάθεια να αναλυθεί το πρωτόκολλο προσπέλασης μέσου (πρωτόκολλο MAC), το οποίο σχεδιάζεται για τους ασύρματους αισθητήρες. Το MAC πρωτόκολλο ελέγχει πώς ο κάθε αισθητήρας θα πρέπει να προσπελάσει ένα διαμοιραζόμενο ραδιοφωνικό κανάλι για να επικοινωνήσει με τους γειτονικούς του κόμβους. Παραδοσιακά το πρόβλημα είναι γνωστό ως «κατανομή καναλιού» ή ως «πρόβλημα πολλαπλής πρόσβασης» (Angel 2008: 8).

Αν και το MAC πρωτόκολλο έχει μελετηθεί εκτεταμένα σε παραδοσιακές μορφές ασύρματης μετάδοσης φωνής και επικοινωνίας δεδομένων, όπως η πολλαπλή πρόσβαση διαίρεσης χρόνου (TDMA), η πολλαπλή πρόσβαση διαίρεσης συχνότητας (FDMA) και η πολλαπλή πρόσβασης διαίρεσης κώδικα (CDMA), εν τούτοις οι απαιτήσεις του MAC πρωτοκόλλου στα δίκτυα αισθητήρων διαφέρουν από αυτά των παραδοσιακών

ασύρματων δικτύων φωνής και δεδομένων σε πολλούς παραμέτρους. Πρώτα από όλα, όπως έχει ήδη αναφερθεί, οι ασύρματοι αισθητήρες κάνουν χρήση μπαταρίας για την τροφοδότησή τους με ενέργεια και συνήθως είναι αρκετά δύσκολο να αντικατασταθεί η πηγή ενέργειας σε όλους τους αισθητήρας όταν αυτό απαιτηθεί. Σε δεύτερο χρόνο, οι κόμβοι συνήθως αναπτύσσονται σε μία ad-hoc διάταξη παρά με μια πιο προσεκτική και κατανεμημένη διάταξη. Ως εκ τούτου, μετά την αρχική τοποθέτηση, οι αισθητήρες πρέπει σε σύντομο χρονικό διάστημα να αυτό-οργανωθούν σε ένα δίκτυο επικοινωνίας. Σε τρίτο επίπεδο, πολλές εφαρμογές απασχολούν μεγάλο αριθμό κόμβων. Τέλος, η μεγαλύτερη κυκλοφορία στο δίκτυο «πυροδοτείται» από γεγονότα που ανιχνεύονται στο χώρο όπου βρίσκονται εγκατεστημένα τα δίκτυα και μπορεί να γίνονται πολύ συχνά σε ορισμένες χρονικές στιγμές. Τα χαρακτηριστικά που αναφέρθηκαν πιο πάνω, συνηγορούν ότι τα έως τώρα MAC πρωτόκολλα, δεν είναι κατάλληλα χωρίς τροποποιήσεις για τα δίκτυα ασύρματων αισθητήρων.

Η σχεδίαση των MAC πρωτόκολλων στα ασύρματα δίκτυα αισθητήρων εξαρτάται από το αναμενόμενο μοτίβο για το φορτίο (κίνηση), με βάση τις εκάστοτε εφαρμογές. Για παράδειγμα εάν ένας κόμβος έχει αναπτυχθεί για να παρατηρεί συνέχεια φυσικά φαινόμενα, όπως την θερμοκρασία σε ένα δάσος, αναμένεται να ανιχνεύεται ένα συνεχές και χαμηλού φορτίου σήμα, με σημαντικό βαθμό περιοδικότητας.

Από την άλλη πλευρά, εάν αντικειμενικός σκοπός είναι το δίκτυο να είναι σε αναμονή μέχρι να συμβεί ένα σημαντικό γεγονός, οπότε και θα καταγράψει όσο το δυνατόν περισσότερα δεδομένα, τότε το δίκτυο τείνει να είναι σε αδράνεια τον περισσότερο καιρό και στη συνέχεια αντιμετωπίζει ένα όγκο από πακέτα, τα οποία θα πρέπει να παραδοθούν σε σύντομο χρονικό διάστημα στον παραλήπτη. Όταν μια πλημμύρα δεδομένων ανιχνευθεί, τότε τα δεδομένα αυτά πρέπει να προωθηθούν στο διαχειριστή του συστήματος με ταχύτητα και ασφάλεια. Λόγω των απαιτήσεων αυτών, τα πρωτόκολλα MAC τα οποία βασίζονται σε CSMA (Carrier sense multiple access).τεχνικές, είναι καταλληλότερα, σε σύγκριση με τις τεχνικές TDMA (Angel 2008: 9). Στη CSMA τεχνική κάθε κόμβος ανιχνεύει το μέσο μετάδοσης και όταν διαπιστώσει απουσία κίνησης στο μέσο τότε πραγματοποιεί την αποστολή των πακέτων που διαθέτει.

Τα βασισμένα σε TDMA πρωτόκολλα, χρειάζεται να ελέγξουν το κανάλι για να στείλουν προσχεδιασμένα μηνύματα σε κάθε αισθητήρα του κόμβου, με σκοπό ο κάθε κόμβος να

έχει την κατάλληλη χρονοθυρίδα. Ο χρονικός έλεγχος του μηνύματος με αυτό τον τρόπο είναι αρκετά υψηλότερος πράγμα που μεταφράζεται σε αρκετή κατανάλωση ενέργειας. Επίσης σε ένα μικρό και φθηνό κόμβο, είναι πολύ δύσκολο να εφαρμοστούν ξεχωριστά κανάλια επικοινωνίας.

Επιπρόσθετα οι απαιτήσεις στα βασισμένα σε TDMA πρωτόκολλο απαιτούν υψηλό χρόνο ώθησης συγχρονισμού. Σε μικρούς και φθηνούς κόμβους είναι επίσης πολύ δύσκολο να επιτευχθεί πολύ υψηλός χρόνος ώθησης συγχρονισμού μεταξύ των γειτονικών κόμβων. Από την άλλη οπτική γωνία, από την οπτική του CSMA δεν απαιτούνται προϋ ποθέσεις ώθησης συγχρονισμού μεταξύ των κόμβων.

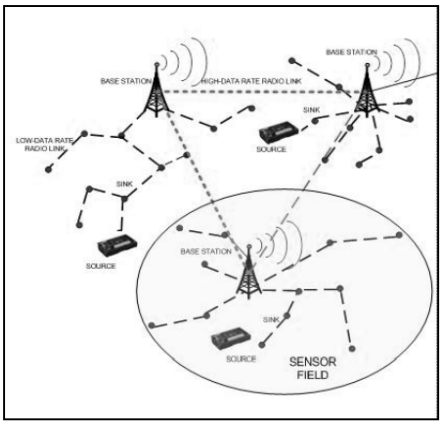
5.2.4.7 CSMA MAC Πρωτόκολλο.

Στα πρωτόκολλα MAC τα οποία βασίζονται στην τεχνική CSMA οι κόμβοι στο δίκτυο είναι γενικά ασυντόνιστοι. Στην κατηγορία των CSMA πρωτοκόλλων, οι κόμβοι που μεταδίδουν έχουν πάντα "σεβασμό" στις εξερχόμενες μεταδόσεις. Στην αρχή της επικοινωνίας ο κόμβος απαιτεί να ακουστεί το μέσο μετάδοσης: η διαδικασία αυτή καλείται "ανίχνευση φέροντος". Εάν κατά την ακρόασή το μέσο είναι αδρανές, τότε ο κόμβος ξεκινά την μετάδοσή του. Εάν το μέσο είναι απασχολημένο τότε ο κόμβος αναβάλλει την μετάδοσή του για χρονικό διάστημα που καθορίζεται από έναν ή περισσότερους πιθανούς αλγορίθμους. Έτσι, ο κόμβος χρησιμοποιεί ένα τυχαίο χρόνο αναμονής, μετά τον οποίο το μέσο αρχίζει να ανιχνεύεται και πάλι. Πριν από αυτή την κατάσταση, δεν υπάρχει ενδιαφέρον για την κατάσταση του μέσου (Angel 2008: 8).

Αν και το CSMA έχει αρκετά πλεονεκτήματα, έχει εν τούτοις και ορισμένα μειονεκτήματα. Λόγου χάρη το CSMA έχει δυνατότητα σύγκρουσης πακέτων και αναμετάδοσής τους αργότερα. Κατά αυτό τον τρόπο η ενέργεια που δαπανάται για να αποσταλούν ξανά τα πακέτα που έχουν συγκρουστεί είναι αρκετά μεγάλη, επίσης η χρονική καθυστέρηση στη μετάδοση είναι αρκετή σημαντική παράμετρος, πράγμα που επενεργεί αρνητικά στην απόδοση του δικτύου.

5.2.5 Συντήρηση.

Ως όρος, στα ασύρματα δίκτυα, η συντήρηση αναφέρεται σε αυτά τα δίκτυα τα οποία είναι σε θέση να εκτελέσουν απαραίτητες λειτουργίες, όπως αυτή του αυτοπροσδιορισμού, της αυτοπροστασίας, αλλά και της επαναφοράς, χωρίς να απαιτείται η συμμετοχή του ανθρώπου.



Εικόνα 25. Συντήρηση Δικτύου.

Στη διαδικασία της συντήρησης εντάσσονται και οι ενέργειες της ανίχνευσης πιθανών αποτυχιών ή ακόμα της μείωσης της απόδοσης του δικτύου. Επίσης εντάσσονται όλες οι διαδικασίες που απαιτούνται για την διάγνωση προβλημάτων αλλά και την επαναφορά.

Τύποι συντήρησης που μπορούν να συναντηθούν είναι η διορθωτική (corrective), όταν ένα δίκτυο έχει την δυνατότητα να επανορθώσει τις αστοχίες, η προσαρμοστική (adaptive), όταν το δίκτυο αισθητήρων έχει την δυνατότητα να προσαρμόζεται στις τυχόν μεταβολές που προκύπτουν, η αποτρεπτική (preventive), όταν το δίκτυο είναι σε θέση να μπει σε μαθησιακή κατάσταση, όπου και αναμένει την πιθανή επίδραση που έχουν οι αλλαγές, και τέλος η προληπτική (proactive) όπου σε αυτή το δίκτυο μπορεί προληπτικά να επεμβαίνει για την αντιμετώπιση αποτυχιών (Ilyas, Mahgoub 2005: 36).

5.2.6 Ενεργειακή Απόδοση.

Η ενεργειακή απόδοση είναι κρίσιμος παράγοντας για τα δίκτυα αισθητήρων, γιατί οι κόμβοι έχουν μικρούς και περιορισμένους φορείς ενέργειας. Πολλές λύσεις έχουν προταθεί για την αντιμετώπιση της στρέβλωσης αυτής: οι λύσεις αυτές κατευθύνονται τόσο σε προσανατολισμό υλικού όσο και λογισμικού.

Οι αισθητήρες είναι χρήσιμο να παραμένουν σε αδράνεια, κατ' αυτό τον τρόπο εξοικονομούν ενέργεια ανάμεσα σε ενδιαφέροντα γεγονότα που πυροδοτούν τη λειτουργία τους. Επίσης είναι σε θέση να περιορίσουν την κατανάλωση ενέργειας με τον περιορισμό του χρόνου αναμονής για τον ενεργό χρόνο του δικτύου σύμφωνα με τις συγκεκριμένες απαιτήσεις του χρήστη. Με την εξέταση του δικτύου ως μία ενιαία οντότητα και με τα συνεργατικά πρωτόκολλο επικοινωνίας να αφαιρούν τον πλεονασμό από τους υπολογισμούς και την επικοινωνία. Κατ’ αυτό τον τρόπο το δίκτυο διατηρεί και καταναλώνει "χωρική ταξινόμηση" ενέργειας (Sohraby, Minoli, Znati, 2007: 23).

Κόμβοι με άπειρη διάρκεια ζωής μπορούν να κατασκευαστούν και να χρησιμοποιούνται: η χρήση τέτοιων κόμβων καθίσταται εφικτή με τη μετατροπή των περιβαλλοντολογικών φαινομένων σε ενέργεια ηλεκτρική. Αυτές οι τεχνικές συγκομιδής ενέργειας κάνουν χρήση συγκέντρωσης ενέργειας από διάφορες πηγές. Οι πηγές αυτές μπορεί να είναι: δονήσεις του εδάφους, εκρήξεις ραδιοφωνικής ενέργειας, κυματισμό της θάλασσας και άλλα πιθανά σενάρια. Αποτέλεσμα αυτού θα είναι η ύπαρξη μιας πηγής ενέργειας (μπαταρία) με τη μικρότερη δυνατή χρήση, πράγμα που θα εκτοξεύσει την διάρκεια της ζωής της και θα δώσει μεγαλύτερο εύρος ζωής στον ίδιο τον κόμβο.

5.2.7 Ασφάλεια.

Αναντίρρητα ο τομέας της ασφάλειας είναι το κυριότερο στοιχείο ανησυχίας σε ένα ασύρματο δίκτυο ασφαλείας, μιας και τα δεδομένα που μεταφέρει είναι πολλές φορές βαρύνουσας σημασίας τόσο για ίδιο δίκτυο, όσο και για τον οργανισμό που το διαχειρίζεται.

Το γεγονός ότι είναι επιτακτική η ανάγκη ύπαρξης ασφαλείας, αλλά και το γεγονός, το πως υλοποιείται αυτή, με τη χρήση πολύπλοκων αλγορίθμων αυθεντικοποίησης και κρυπτογράφησης, επιβαρύνει με πολλούς πόρους την λειτουργία των κόμβων. Το να υποκλαπούν τα δεδομένα τα οποία μεταδίδονται, ή να πραγματοποιηθεί μία παρεμβολή στο κανάλι μετάδοσης, στο οποίο πρέπει να γίνει υπενθύμιση ότι είναι ασύρματο, είναι αρκετά εύκολο. Άρα προκύπτει η ανάγκη τα δεδομένα να κρυπτογραφούνται ώστε αυτά να παραδοθούν αναλλοίωτα στους παραλήπτες. Ακόμα πρέπει να γίνεται πρόνοια κατά την κατασκευή και τοποθέτηση των κόμβων ώστε να επιτυγχάνεται η σχετική αντοχή στα φαινόμενα φυσικής παραβίασης.

Οι τεχνικές όμως οι οποίες χρησιμοποιούνται για να επιτευχθεί κρυπτογράφηση των δεδομένων και αυθεντικοποίηση έχουν και ορισμένες επιδράσεις οι οποίες στο πλείστο των περιπτώσεων έχουν αρνητικό αντίκτυπο για την κατανάλωση ενέργειας αλλά και στον περιορισμό της διαθεσιμότητας του εύρος ζώνης του μέσου μεταφοράς. Επιπλέον τα πακέτα δεδομένων επιβαρύνονται με πρόσθετα δυαδικά ψηφία, τα οποία είναι απαραίτητα για την κρυπτογράφηση και την αυθεντικοποίηση, πράγμα που είχε ως συνέπεια να μειωθούν αρκετά τα διαθέσιμα δυαδικά ψηφία πληροφορίας στα μεταδιδόμενα πακέτα.

Εν κατακλείδι, η ασφάλεια στα ασύρματα δίκτυα αισθητήρων αποκτά ιδιάζουσα σημασία για δύο λόγους: α) είναι περισσότερο εύκολο, σε σχέση με άλλα δίκτυα, να πραγματοποιηθεί μία επίθεση ασφάλειας, β) πολλές από τις κλασικές τεχνικές ενίσχυσης της ασφάλειας δεν μπορούν να υλοποιηθούν, λόγω των περιορισμών που υπάρχουν από τις απαιτήσεις για χαμηλή κατανάλωση ενέργειας και χαμηλή μνήμη. Οι επιθέσεις ασφάλειας στα δίκτυα αυτά μελετώνται αναλυτικά στο επόμενο Κεφάλαιο.

5.2.8 Διάταξη των Κόμβων και Αρχιτεκτονική.

Όπως είναι ήδη γνωστό στα ασύρματα δίκτυα αισθητήρων η φιλοσοφία αλλά και η υλοποίηση της σχεδίασής τους βασίζεται στο γεγονός της πυκνής και τυχαίας διάταξης των κόμβων, οι οποίοι πολλές φορές είναι τοποθετημένοι σε περιοχές όχι εύκολα προσιτές. Οι κόμβοι του δικτύου δεν βρίσκονται σε διαρκή επικοινωνία με τους

γειτονικούς κόμβους λόγω των ενεργειακών περιορισμών που υπάρχουν, αλλά βρίσκονται σε διάφορα στάδια κατάστασης. Τα στάδια αυτά μπορεί να είναι είτε ανενεργά, είτε σε αναμονή, είτε σε αδράνεια, είτε σε κατάσταση εκπομπής, είτε σε κατάσταση λήψης.

Η επικοινωνία αυτών των καταστάσεων αναγκάζει το δίκτυο να δημιουργεί συνδέσεις συχνά και πολλές φορές χωρίς να είναι σε θέση να γνωρίζει την κατάσταση του κόμβου ώστε να μπορέσει να αντιληφθεί σε ποια κατάσταση λειτουργίας βρίσκεται. Οι ενέργειες αυτές νοούνται και ως ενέργειες αυτοπροσδιορισμού του δικτύου (Sohraby, Minoli, Znati, 2007: 25).

Ως αυτοπροσδιορισμός του δικτύου μπορούν να λογιστούν όλες οι ενέργειες οι οποίες γίνονται για την ανακατεύθυνση των πακέτων μέσω των κόμβων οι οποίοι διαθέτουν πλεονάσματα ενέργειας. Κατ' αυτό τον τρόπο επιτυγχάνεται μια συμμετρικότητα στην εξάντληση της ενέργειας που υπάρχει στο δίκτυο. Η ad-hoc αρχιτεκτονική πάνω στην οποία δομείται ένα ασύρματο δίκτυο αισθητήρων επιτάσσει την κατά το δυνατόν λιγότερη ανθρώπινη παρέμβαση, αλλά και την μη ύπαρξη σταθερής δομής. Με αυτόν τον τρόπο εξαναγκάζει το δίκτυο να πραγματοποιεί συνδέσεις αυτούσιο αλλά και να τις συντηρεί επίσης αυτούσιο.

5.2.9 Περιορισμοί Σχεδίασης.

Αναντίρρητα, κατά τον σχεδιασμό ενός δικτύου επικοινωνίας, ένα από τα βασικά στοιχεία τα οποία τίθενται υπόψη του κατασκευαστή είναι οι περιορισμοί που θα αντιμετωπίσει κατά τη διάρκεια της σχεδίασης. Οι περιορισμοί αυτοί μπορεί να είναι περιορισμοί της φιλοσοφίας σχεδίασης, της τεχνολογίας σχεδίασης ή ακόμα και των απαιτήσεων σχεδίασης.

Οι περιορισμοί αυτοί, αν και επιγραμματικά έχουν επισημανθεί στα ανωτέρω, παρατίθενται συγκεντρωτικά στη συνέχεια – και αυτό γιατί οι περιορισμοί αυτοί καθορίζουν τελικά, σε μεγάλο βαθμό, και τις δυνατότητες που υπάρχουν για υλοποίηση κατάλληλων κρυπτογραφικών λειτουργιών. Κατ’ αρχάς, όπως αναφέρθηκε πολλές

φορές έως τώρα, οι κόμβοι από τους οποίους είναι κατασκευασμένο το δίκτυο έχουν περιορισμούς όσον αφορά την απόδοση τους. Οι περιορισμοί αυτοί έγκεινται στην πλειονότητα των περιπτώσεων στο γεγονός ότι η πηγή ενέργειάς τους έχει συγκεκριμένες δυνατότητες. Περαιτέρω, πέραν του περιορισμού της ενεργειακής αυτονομίας, οι κόμβοι στα ασύρματα δίκτυα αισθητήρων από την σχεδίασή τους στερούνται ορισμένων προδιαγραφών, όπως είναι η υπολογιστική ισχύς, η εγκατεστημένη μνήμη, αλλά και το εύρος ζώνης του μέσου μετάδοσης.

Η συνήθης τοποθέτηση των κόμβων είναι σε απομακρυσμένες περιοχές, μη εύκολα προσβάσιμες, οπότε η διάρκεια ζωής ενός κόμβου άπτεται από τον χρόνο που του επιτρέπει το σύστημα τροφοδοσίας ενέργειας που διαθέτει. Η ενέργεια που καταναλώνει ένας κόμβος συνήθως δαπανάται στην αποστολή και λήψη δεδομένων, άρα είναι επιτακτική η χρήση πρωτοκόλλων τα οποία ρυθμίζουν μία αποδοτική αποστολή πακέτων. Για να επιτευχθεί αυτό κρίνεται αναγκαία η χρήση αλγορίθμων χαμηλής πολυπλοκότητας.

Το ασύρματο μέσο πάνω στο οποίο στηρίζεται η μετάδοση των δεδομένων υπόκειται σε περιορισμούς μετάδοσης. Οι περιορισμοί αυτοί έχουν να κάνουν με το φυσικό περιβάλλον το οποίο επενεργεί αρνητικά, αλλά και τον υψηλό θόρυβο στην μετάδοση. Απότοκος αυτών είναι η εξασθένηση του σήματος αλλά πολλές φορές και η αξιοπιστία του. Πέραν τούτων, μιας και οι κόμβοι έχουν περιορισμένες δυνατότητες υπολογισμού αλλά και εύρους ζώνης, τα δεδομένα συχνά μεταδίδονται απροστάτευτα χωρίς κρυπτογράφηση. Αυτό το γεγονός εγείρει θέματα αξιοπιστίας και ασφάλειας του μεταδιδόμενου σήματος.

5.3 Πλεονεκτήματα.

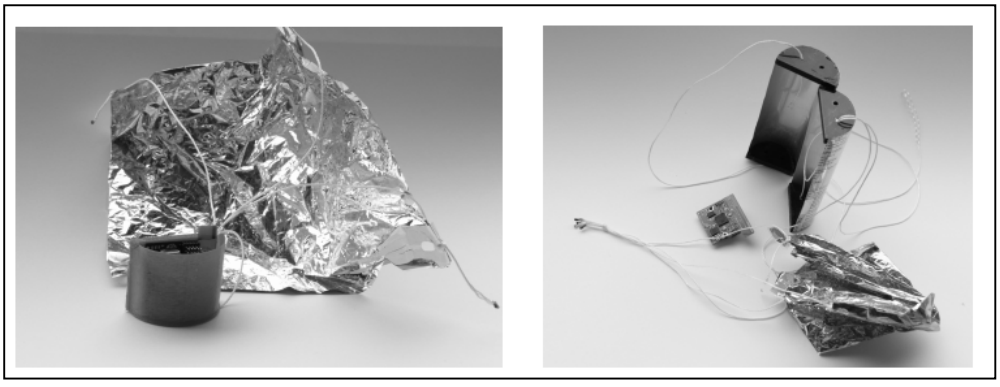
Κάνοντας μια απόπειρα να αναφερθεί κανείς στα συγκριτικά πλεονεκτήματα των ασύρματων δικτύων αισθητήρων, θα πρέπει να αναφέρει τη δυνατότητα την οποία προσφέρουν να αυτο-οργανώνονται δίχως να απαιτούν ή να αναμένουν τον ανθρώπινο παρεμβατισμό. Η έλλειψη παρεμβατισμού έδωσε τη δυνατότητα να αναπτυχθούν σε περιβάλλοντα αρκετά δυσπρόσιτα. Συγκριτικό πλεονέκτημα έναντι άλλων υλοποιήσεων

είναι η έλλειψη δομημένης καλωδίωσης, κάτι που προσφέρει τη δυνατότητα ανάπτυξης χωρίς γεωγραφικούς περιορισμούς και κολλήματα.

Στην επιθυμία να παρουσιαστούν συνοπτικά τα πλεονεκτήματά τους, θα ήταν άδικο να λησμονήσει κανείς να αναφέρει ότι έχουν την δυνατότητα να εργαστούν σε συνθήκες οι οποίες μπορούν να χαρακτηριστούν ως ακραίες. Δεν μπορεί να ειπωθεί ότι υπάρχει περιορισμός στο πλήθος των αισθητήρων οι οποίοι είναι ενταγμένοι σε ένα δίκτυο. Η δυνατότητα αυτή επιτρέπει στη συλλογή περισσότερων δειγμάτων πληροφορίας αλλά και στην αύξηση της ποιότητας των δειγμάτων.

Η σχεδιαστική τους φιλοσοφία αλλά και ο χώρος διάταξής τους επιτάσσει τη χρήση πηγών ενέργειας σε στοιχεία (μπαταρία) ή την χρήση ανανεώσιμων πηγών ενέργειας. Λόγω του ότι τα συστήματα αισθητήρων πολλές φορές βρίσκονται σε κατάσταση αδράνειας - άρα μη λειτουργίας - για εξοικονόμηση ενέργειας, η ενέργεια η οποία εξοικονομείται είναι τεράστια σε σχέση με μία φιλοσοφία αδιάλειπτης λειτουργίας.

Το πλήθος των αισθητήρων που έχουν παραχθεί είναι αρκετά μεγάλο και το πλήθος των μετρήσεων που μπορούν να πραγματοποιήσουν είναι αρκετά μεγαλύτερο. Τα φαινόμενα τα οποία «πυροδοτούν» την ενεργοποίηση ενός αισθητήρα, στην πλειοψηφία των περιπτώσεων, είναι φυσικά φαινόμενα και καταστάσεις. Τέτοια φυσικά φαινόμενα είναι η θερμοκρασία, η υγρασία, η κίνηση, η δόνηση, η ατμοσφαιρική πίεσή, η ένταση του φωτός, η σύσταση του εδάφους, η ένταση του θορύβου, η επιτάχυνση του ανέμου και πλήθος άλλων περιπτώσεων φυσικών φαινομένων.



Εικόνα 26. Βαλλιστική ανάπτυξη μέσω Drones.

Επιπρόσθετα ο τρόπος ανάπτυξης των αισθητήρων μπορεί να ποικίλει ανάλογα την περίσταση (Kulau, et al 2014: 2), το περιβάλλον ανάπτυξης, το μέγεθος της επιθυμητής ανάπτυξης, αλλά και τον αναγκαίο εξοπλισμό. Οι μέθοδοι αυτοί μπορεί να είναι είτε αμιγώς παραδοσιακοί κάνοντας χρήση της ανθρώπινης παρέμβασης, είτε με την χρήση εξοπλισμού ή μηχανικής υποβοήθησης, όπως η χρήση αυτοκινήτων, θαλάσσιων μέσων και εναέριων μέσων. Η υποβοήθηση στην τοποθέτηση πλεονεκτεί εναντίον άλλων εφαρμογών στον τομέα της επεκτασιμότητας, της ταχύτητας στην ανάπτυξη, της χρηστικότητας, αλλά και της ανάπτυξης σε μη φιλικά περιβάλλοντα. Αυτό που έχει αξία σημαντική να τονιστεί είναι η επικρατούσα τάση να γίνεται χρήση drones για την ανάπτυξη των αισθητήρων. Το γεγονός αυτό, πέραν των πλεονεκτημάτων που έχουν αναλυθεί, δίνει και το επιπλέον πλεονέκτημα της επαναχρησιμοποίησης του εξοπλισμού, μειώνοντας έτσι το κόστος εγκατάστασης μιας και το κόστος ανάκτησης του εξοπλισμού είναι σχετικά μικρό κάνοντας χρήση αυτοματοποιημένων διαδικασιών.

5.4 Εφαρμογές Ασύρματων Δικτύων Αισθητήρων.

Κατά το πρόσφατο παρελθόν, αλλά και στο ρου της ιστορίας τους, τα ασύρματα δίκτυα αισθητήρων έχουν βρει το δρόμο τους για μία ευρεία ποικιλία εφαρμογών καθώς και ευρεία εφαρμογή σε συστήματα με διαφορετικές απαιτήσεις και χαρακτηριστικά (García-Hernández, et al 2007: 265). Πολλές εφαρμογές επίσης βασίζονται σε αυτά για την άντληση πληροφοριών.

Η ενσωμάτωση πολλαπλών τύπων αισθητήρων όπως σεισμικοί, ακουστικοί, οπτικοί κ.α. σε μία πλατφόρμα δίνει τεράστια ώθηση στην άντληση πληροφοριών από την επιστημονική και όχι μόνο κοινότητα. Μια κατηγοριοποίηση των εφαρμογών που κάνουν χρήση δικτύων αισθητήρων μπορεί να γίνει με γνώμονα την κινητικότητα, τους πόρους, το κόστος, την ενέργεια, την ετερογένεια, την υποδομή, την τοπολογία, την γεωγραφική κάλυψη, την συνδεσιμότητα, το μέγεθος, την διάρκεια ζωής και την ποιότητα υπηρεσιών (Quality of Service) των αισθητήρων που χρησιμοποιούν (García-Hernández, et al 2007: 266).

Το φάσμα των εφαρμογών στις οποίες μπορούν να χρησιμοποιηθούν είναι πολύ μεγάλο, αλλά με μια πιο προσεκτική ματιά μπορεί κανείς να κάνει μια πρωταρχική ταξινόμηση σε δύο βασικές κατηγορίες: αυτή της επίβλεψης και αυτή της ανίχνευσης. Πέραν των βασικών κατηγοριών είναι δυνατό να πραγματοποιηθούν και υποδιαιρέσεις που έχουν να κάνουν με την παρατήρηση του χώρου και των αντικειμένων, καθώς και με την παρακολούθηση της αλληλεπίδρασης των αντικειμένων και του χώρου που τα περιβάλλουν.

Με βάση τα όσα αναφέρθηκαν έως τώρα, κάνοντας μία εισαγωγική προσέγγιση (Sohraby, Minoli, Znati, 2007: 16) μπορούμε να αναφέρουμε ως πεδίο χρήσης και εφαρμογής των δικτύων αισθητήρων τον τομέα του περιβάλλοντος, τον στρατιωτικό τομέα, τον γεωργικό τομέα, την υγεία, την βιομηχανία, τις συγκοινωνίες, τον τομέα της επιτήρησης, της πολιτικής προστασίας αλλά και τον τομέα της οικιακής χρήσης.

5.4.1 Περιβαλλοντολογικός Τομέας.

Η περιβαλλοντολογική παρακολούθηση είναι ένας τομέας όπου χρήση ασύρματων δικτύων αισθητήρων βρίσκει εφαρμογή, έχοντας ως σκοπό την παρακολούθηση φυσικών μεταβλητών, οι οποίες πρέπει να μετρηθούν και να ποσοτικοποιηθούν, όπως λόγου χάρη η θερμοκρασία και η υγρασία, σε ένα γεωγραφικό εύρος (Martinez, Hart, Ong 2004: 2).

Οι εφαρμογές περιβαλλοντολογικής παρακολούθησης μπορούν να ταξινομηθούν σε δύο κύριες κατηγορίες: του εσωτερικού και εξωτερικού χώρου (Oliveira, Rodrigues 2011: 145). Οι εφαρμογές εσωτερικού χώρου συνήθως περιλαμβάνουν την παρακολούθηση γραφείων και οικιακών χώρων. Οι εφαρμογές αυτές ανιχνεύουν θερμοκρασία, φως, υγρασία και την ποιότητα του αέρα. Επιπρόσθετα εσωτερικές εφαρμογές ενδέχεται να περιλαμβάνουν την δυνατότητα της ανίχνευσης πυρκαγιών σε κτίρια, καθώς επίσης και την ανίχνευση παραμορφώσεων αστικών δομών.

Οι εξωτερικού χώρου εφαρμογές περιλαμβάνουν την ανίχνευση χημικών καταστροφών, την παρακολούθηση του φυσικού περιβάλλοντος, την παρακολούθηση της

κυκλοφορίας, την ανίχνευση της σεισμικής δραστηριότητας, την δραστηριότητα των ηφαιστείων (εκρήξεις), την ανίχνευση πλημμυρών, την πρόγνωση του καιρού και πλήθος άλλων εφαρμογών (Oliveira, Rodrigues 2011: 145).

Τα πεδία παρακολούθησης τα οποία αναφέρθηκαν πιο πάνω συνέβαλαν αποφασιστικά στη βελτίωση της ποιότητας ζωής του ανθρώπου αλλά και στην προστασία του περιβάλλοντος. Οι μετρήσεις οι οποίες πραγματοποιήθηκαν στις εσωτερικές εφαρμογές ώθησαν την αρχιτεκτονική στο να βελτιωθεί, κάνοντας χρήση πιο οικολογικών και φιλικών υλικών (García-Hernández, et al 2007: 262) αλλά και στην υιοθέτηση αρχιτεκτονικών προσανατολισμένων στη χρηστικότητα και την άνεση.

Στον τομέα των εξωτερικών παρατηρήσεων τέθηκαν οι βάσεις για την παρακολούθηση του φυσικού περιβάλλοντος και του βιότοπου διαμονής ειδών προς εξαφάνιση. Δόθηκε η δυνατότητα στην επιστημονική κοινότητα να ανιχνεύσει μεταβλητές και να προστατεύσει το περιβάλλον από οικολογικές καταστροφές. Για παράδειγμα, μια μεταβλητή η οποία είναι δυνατόν να μετρηθεί και να ποσοτικοποιηθεί είναι η ποσότητα πετρελαίου στο θαλάσσιο νερό, γεγονός που συνέβαλλε στην προσπάθεια για την εκ των προτέρων προσπαθειών πρόληψης και μετρίασης των επιπτώσεων των οικολογικών καταστροφών (Corke, et al 2010: 19014).

Οι οικολογικές καταστροφές οι οποίες είναι σε θέση να ελεγχθούν είναι οι πετρελαϊ κές κηλίδες, οι δασικές πυρκαγιές, οι εκρήξεις ηφαιστείων, οι ανεμοστρόβιλοι και οι σεισμικές εξάρσεις.

Ενδεικτικά, μπορούν επίσης να παρατεθούν το πρόγραμμα Great Duck (García-Hernández, et al 2007: 271) που αντικειμενικός του στόχος ήταν η παρακολούθηση αποδημητικών πουλιών, όπως επίσης και το πρόγραμμα ZebraNet το οποίο ως αντικείμενο μελέτης εξετάζει τις παραμέτρους μετανάστευσης των πληθυσμών ζέβρας στην Αφρική καθώς και την νυχτερινή τους συμπεριφορά, επίσης πραγματεύεται την συνύπαρξη τους με άλλα είδη (García-Hernández, et al 2007: 261).

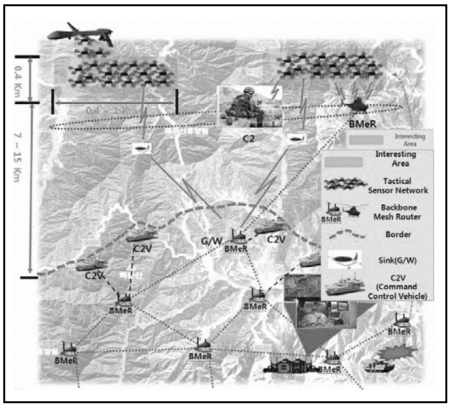
5.4.2 Στρατιωτικός – Αμυντικός Τομέας.

Τα ασύρματα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν για στρατιωτικές εφαρμογές και για ένα πλήθος ειδικών σκοπών (Lee, et al 2009: 3), όπως η παρακολούθηση και η επίβλεψη των εχθρικών δυνάμεων, αλλά και η προστασία φίλιων δυνάμεων. Σε αντίθεση με τα δίκτυα αισθητήρων που έχουν προσανατολισμό στην πολιτική χρήση, τα τακτικά στρατιωτικά συστήματα αισθητήρων έχουν διαφορετικές προτεραιότητες και απαιτήσεις.

Στην εποχή της πληροφορίας, τα τακτικά στρατιωτικά δίκτυα αισθητήρων αποτελούν την ραχοκοκαλιά του δίκτυο-κεντρικού πολέμου σε πολλές Ένοπλες Δυνάμεις ανά την υφήλιο. Ο δίκτυο-κεντρικός πόλεμος είναι ένα αρκετά ενορχηστρωμένο, δυναμικά αυτόνομο, ψηφιακό πεδίο μάχης επικοινωνιών. Όπου η διοίκηση και ο έλεγχος σε ένα δίκτυο επίγνωσης της κατάστασης επιτρέπει στον ηγήτορα να μπορεί να δει, να αποφασίσει και να επιλέξει το στόχο του με αρκετή σαφήνεια. Τούτο επιτυγχάνεται λόγω της προηγμένης επίγνωσης της κατάστασης στο πεδίο της μάχης.

Οι Ένοπλες Δυνάμεις αρκετών αναπτυγμένων χωρών στα αντίστοιχα τους προγράμματα για το μελλοντικό σύστημα μάχης που αναπτύσσουν, κάνουν χρήση επιγείων αισθητήρων, με σκοπό να ανιχνεύσουν, να εντοπίσουν και να αναγνωρίσουν εχθρικούς στόχους. Οι αισθητήρες αυτοί αναπτύσσονται είτε με τη χρήση μη επανδρωμένων σκαφών (UAV) είτε με εξειδικευμένες βολές πυροβολικού (Lee, et al 2009: 4).

Υπάρχουν πλήθος σεναρίων χρήσης ασύρματων δικτύων αισθητήρων για τακτικές στρατιωτικές εφαρμογές. Αναφορικά μπορεί να προταθεί η χρήση για την προστασία φίλιων δυνάμεων. Όπου με την επικουρία των ασύρματων δικτύων αισθητήρων, οι φίλιες δυνάμεις είναι σε θέση να προστατεύσουν τις προκεχωρημένες βάσεις τους, τις θωρακισμένες μονάδες τους και τα κέντρα επικοινωνιών. Όλα τα απαραίτητα στοιχεία δηλαδή που είναι απαραίτητα για την διεξαγωγή ενός πολέμου σε ένα σύγχρονο πεδίο μάχης.



Εικόνα 27. Ψηφιακό Πεδίο Μάχης.

Μια επιπρόσθετη εφαρμογή, είναι συστήματα προειδοποίησης με στρατιώτες φέροντες συστήματα αισθητήρων. Στην φιλοσοφία αυτή έχει εξελιχθεί το πρόγραμμα ASSIST του Υπουργείου Αμύνης των ΗΠΑ, όπου αντικειμενικός του σκοπός είναι η παροχή αναφορών και ενημερώσεων. Οι οποίες θα καταγράφουν και θα περιγράφουν πιθανά γεγονότα τα οποία αντιμετωπίστηκαν κατά τη διάρκεια μιας επιχείρησης, ώστε να προβλεφθούν αστοχίες σε μελλοντικές επιχειρήσεις.

Αναντίρρητα η χρήση ασύρματων δικτύων αισθητήρων σε απομακρυσμένες γεωγραφικές περιοχές αποτελεί ένα σημαντικό πλεονέκτημα σε στρατιωτικές επιχειρήσεις. Στην φιλοσοφία αυτής της εφαρμογής, χιλιάδες αισθητήρες αναπτύσσονται σε περιοχές εχθρικές με σκοπό να παρακολουθούν την εχθρική δραστηριότητα. Αυτό θα επιτρέψει την πρόβλεψη των στρατιωτικών κινήσεων των στόχων με βάση μοντέλα κίνηση στόχων που έχουν ήδη αναπτυχθεί (Raza, et al 2007: 3).

5.4.3 Γεωργικές Κτηνοτροφικές Εφαρμογές.

Λαμβάνοντας υπόψη την ταχεία αύξηση του πληθυσμού σε παγκόσμιο επίπεδο και ιδιαίτερα στην νοτιοανατολική Ασία, αποτελεί εγχείρημα-πρόκληση για την ανθρωπότητα να παράξει τα απαραίτητα για την συντήρηση του πληθυσμού ενός τέτοιου μεγάλου μεγέθους. Για να υπερπηδηθεί το εμπόδιο αυτό χρειάζεται αύξηση της παραγωγικότητας στη γεωργία τόσο στην ποσότητα αλλά και στην ποιότητα του παραγόμενου προϊόντος (Patil, Dawande 2014: 404). Για να επιτευχθεί αυτό κρίνεται

επιτακτική η παρακολούθηση των περιβαλλοντολογικών συνθηκών όπως η θερμοκρασία, το φως, η υγρασία, η ταχύτητα του ανέμου. Οι παράμετροι αυτοί και η επεξεργασία τους θα βοηθήσουν ώστε να διατηρηθεί το υγιές κλίμα που απαιτείται για την ενίσχυση των καλλιεργειών. Ένα υγιές κλίμα ωθεί στην αύξηση της παραγωγικότητας με στοχευμένες παρεμβάσεις όταν αυτές απαιτηθούν (Barrenetxea, et al 2008: 99).

Πέραν των γεωργικών εφαρμογών υπάρχουν κι οι κτηνοτροφικές εφαρμογές. Όπως οι γεωργικές έτσι και οι κτηνοτροφικές εφαρμογές, έχουν ως απώτερο σκοπό την αύξηση της παραγωγικότητας. Ενδεικτικά μπορεί να αναφερθεί η παρακολούθηση των βοοειδών. Σε πρώτο στάδιο περιλαμβάνεται η παρακολούθηση τους σε βάθος χρόνου και η μέτρηση της υγρασίας του εδάφους εντός της μάντρας διαμονής. Η υγρασία του εδάφους αποτελεί σημαντικό δείκτη για την ταχύτητα αύξησης του βοσκότοπου και επομένως σημαντική παράμετρο για τον σχεδιασμό τοποθέτησης του αριθμού ζώων ανά μονάδα επιφάνειας.

Τέλος, γίνεται χρήση του λεγόμενου εικονικού φράκτη, όπου μπορεί να μετακινηθεί και να ωθήσει πληθυσμούς ζώων από περιοχή σε περιοχή. Επιτυγχάνοντας έτσι μία ελεγχόμενη μετανάστευση, αλλά και μία ελεγχόμενη διαδικασία μετακίνησης βοσκοτόπων.

5.4.4 Εφαρμογές στην Υγεία.

Αποτελεί σημαντικό σημείο αναφοράς κάθε προσπάθεια η οποία πραγματοποιείται, και έχει ως σκοπό την βελτίωση της ανθρώπινης ποιότητας ζωής και την παροχή υπηρεσιών υγείας.

Τα ασύρματα δίκτυα αισθητήρων παρέχουν τη δυνατότητα, τόσο στις μεμονωμένες οικίες ασθενών όσο και στους οίκους ευγηρίας, να βοηθήσουν τους ασθενείς αλλά και τους φροντιστές τους, παρέχοντάς τους συνεχή ιατρική παρακολούθηση. Επιπρόσθετα έχουν ρόλο καθοριστικής σημασίας στον έλεγχο των οικιακών συσκευών που βρίσκονται εντός του χώρου διαμονής τους, όπως επίσης παρέχουν την δυνατότητα πρόσβασης

ιατρικών δεδομένων σε εξειδικευμένο προσωπικό όταν αυτό απαιτηθεί. Τέλος καθίστανται αρωγοί στην δυνατότητα επικοινωνίας έκτακτης ανάγκης όταν ο αισθητήρας τεθεί σε κατάσταση συναγερμού, συνεπεία των δεδομένων των οποίων λαμβάνει (Junnila, et al 2010: 449).

Επιπλέον γίνεται λόγος για μία ξεχωριστή κατηγορία ασύρματων αισθητήρων που καλούνται ως BSN (Body Sensor Networ). Οι BSN αισθητήρες καλούνται να εκτελέσουν μετρήσεις στο ανθρώπινο σώμα, αυτό αποτελεί και το εγχείρημα πρόκληση το οποίο πρέπει να αντιμετωπίσουν (Virone, et al 2006: 2). Οι προκλήσεις έγκειται στο γεγονός της πολυπλοκότητας της δομής του ανθρώπινου σώματος αλλά και στην ανάγκη οι ληφθείσες μετρήσεις να είναι κατά το μέγιστο δυνατό ακριβείς. Παράδειγμα εφαρμογής αποτελεί το πρόγραμμα κινητής ιατρικής το οποίο εφαρμόζει ιδιωτικό νοσοκομείο στην Ελληνική επικράτεια με την αρωγή ενός τηλεπικοινωνιακού παρόχου κινητής τηλεφωνίας.

Επιπρόσθετες εφαρμογές αποτελούν η παρακολούθηση ασθενών οι οποίοι βρίσκονται σε μονάδες εντατικής θεραπείας κατά την μετά-εγχειρητική τους περίοδο. Αλλά ακόμα και η παρακολούθηση τόσο ασθενών στα νοσηλευτικά ιδρύματα όσο και στην διαδικασία ανάρρωσης κατ' οίκων. Ακόμη ο ιατρικός έλεγχος ασθενών με χρόνιες παθήσεις ή ατόμων ηλικιωμένων, οι οποίοι χρήζουν συνεχής παρακολούθησης. Η πρόκληση που πρέπει να αντιμετωπιστεί και να υπερκεραστεί είναι ο έλεγχος σε συνθήκες πλήρους κινητικότητας του ατόμου με διακριτικότητα και αποτελεσματικότητα, αλλά και ταυτόχρονα να προσδώσουν αισθήματα ασφάλειας στους παρακολουθούμενους ασθενείς.

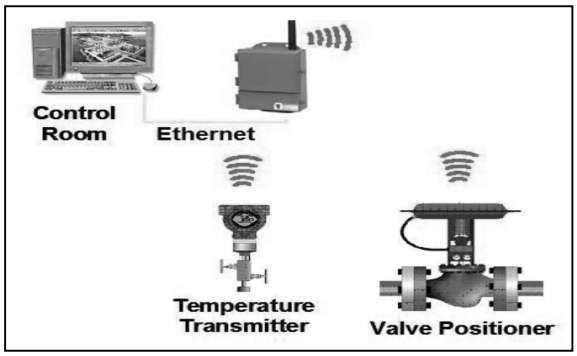
Πλεονεκτήματα τα οποία μπορούν να πιστωθούν σε κάθε τέτοιου είδους προσπάθεια είναι η διαρκής και διακριτική παρακολούθηση των ασθενών, απελευθερώνοντας έτσι πόρους πρωτοβάθμιας και δευτεροβάθμιας υγείας (νοσοκομείο) – πάντα με τη σαφή και ρητή συγκατάθεσή τους. Η συλλογή, επεξεργασία, αξιολόγηση και αποθήκευση πληροφοριών και ιατρικών δεδομένων είναι ένα σημαντικό στοιχείο το οποίο δεν πρέπει να παραβλεφθεί να αναφερθεί. Η δημιουργία βάσεων δεδομένων ιατρικών δεδομένων, όπου βοηθά στο να μειωθεί το κόστος περίθαλψης αλλά και να βελτιωθεί το επίπεδο ζωής είναι ένας επιπρόσθετο σημαντικό πλεονέκτημα. Τούτο γιατί η συγκέντρωση

γνώσης ωθεί στη δημιουργία στοχευόμενων παρεμβάσεων, ελαχιστοποιώντας έτσι τις δυσάρεστες καταστάσεις (Junnila 2010: 451, Virone 2006: 3).

5.4.5 Βιομηχανικές Εφαρμογές.

Τα ασύρματα δίκτυα αισθητήρων έχουνε επιδείξει πολλές δυνατότητες στη χρήση και εφαρμογή σε πολλούς τομείς την ανθρώπινης δραστηριότητας, όπως στη βιομηχανία, στο εμπόριο και στις εφαρμογές καταναλωτών. Συγκεκριμένα γίνεται χρήση τους στη διαδικασία παρακολούθησης και ελέγχου, στην επεξεργασία δεδομένων όπως η πίεση, η υγρασία, η θερμοκρασία, η ροή υγρών, το ιξώδες, η πυκνότητα, καθώς και οι μέτρησης έντασης των δονήσεων. Οι μετρήσεις αυτές στην τυπική τους διαχείριση συλλέγονται από μία μονάδα ανίχνευσης και στη συνέχεια μεταφέρονται ασύρματα σε ένα σύστημα ελέγχου για την επεξεργασία και τη διαχείριση τους.

Η υιοθέτηση των ασύρματων δικτύων αισθητήρων για την παρακολούθηση και τον έλεγχο της διαδικασίας παραγωγής παρέχει αρκετά πλεονεκτήματα σε σύγκριση με τον παραδοσιακό τρόπο συλλογής δεδομένων. Ως τεχνολογική επιλογή πανταχού παρούσα, προσφέρει συνεχή και αδιάλειπτη λειτουργία. Η ερευνητική κοινότητα έχει εξερευνήσει διάφορες πτυχές σχετικά με τις εφαρμογές των δικτύων αισθητήρων στη βιομηχανία. Επίσης έχουν γίνει τεράστιες προσπάθειες για την έρευνα και την ανάπτυξη των προϊ όντων της βιομηχανίας.



Εικόνα 28. Σύστημα Ελέγχου Υδρόψυξης.

Η παρακολούθηση της διαδικασίας παραγωγής και ο έλεγχος είναι ένας συνδυασμός αρχιτεκτονικών, μηχανισμών και αλγορίθμων που χρησιμοποιούνται στη βιομηχανική παραγωγή, ώστε να ελέγχουν συγκεκριμένες ενέργειες για να επιτευχθεί ο απαιτούμενος στόχος παραγωγής. Για να γίνει αντιληπτό αυτό καλό θα ήταν να γίνει η παράθεση ενός παραδείγματος. Η ψύξη ενός πυρηνικού αντιδραστήρα γίνεται με τη ρύθμιση του ρυθμού ροής του ψυκτικού υγρού διαμέσου του μανδύα ψύξης. Επιθυμητό αποτέλεσμα είναι η διατήρηση μιας σταθερής και προκαθορισμένης θερμοκρασίας σε συνάρτηση του χρόνου. Στην ίδια χρονική στιγμή η μεταβλητή θερμοκρασίας μετριέται με ένα μετρητή θερμότητας και χρησιμοποιείται από μία διαδικασία ή μια συνάρτηση για να ληφθεί η απόφαση εάν η βαλβίδα έλεγχού θα πρέπει να αυξήσει ή όχι τη ροή ψυκτικού υγρού ώστε ο πυρήνας να διατηρηθεί στα επιθυμητά πλαίσια θερμοκρασίας (Zhao 2010: 46).

Αναντίρρητα η χρήση των δικτύων αισθητήρων έχει συνεισφέρει καθοριστικό ρόλο στον τρόπο διαχείρισης της ηλεκτρικής ενέργειας. Τούτο γιατί οι εμπορικές εφαρμογές τείνουν προς μία εντελώς απελευθέρωση του σχεδιασμού των μονάδων λειτουργίας στα πεδία των εφαρμογών της επαγωγικής μεταφοράς του ηλεκτρικού ρεύματος. Επίσης η σύγχρονη έρευνα στην τεχνολογία της αυτόνομης λειτουργίας των RFID συστημάτων οδήγησε σε σημαντικό ενδιαφέρον για τη μεταφορά ενέργειας για μεσαίου επιπέδου εφαρμογές (Pukish 2010: 6317).

5.4.5.1 Πλεονεκτήματα Βιομηχανικών Αισθητήρων.

Οι ασύρματοι αισθητήρες έχουν ένα μεγάλο πλήθος πλεονεκτημάτων τα οποία πρέπει να παρατεθούν.

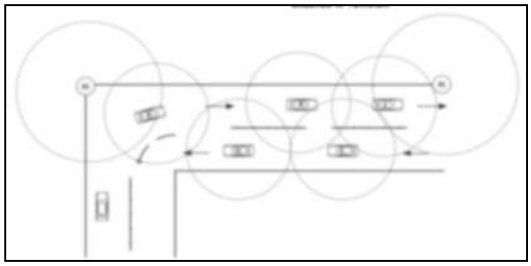
- Δεν υπάρχουν περιορισμοί καλωδίων: Τα ασύρματα δίκτυα αισθητήρων τοποθετούνται σε βιομηχανικές περιοχές για να μετρήσουν μεγέθη όπως η εγγύτητα, η θερμοκρασία, πίεση, οι σταθμοί και η ποιότητα ισχύος. Δίχως τον περιορισμό της καλωδίωσης, οι συσκευές μπορούν να χρησιμοποιηθούν σε εφαρμογές που προηγούμενα είτε ήταν φυσικά απρόσιτες είτε το κόστος υλοποίησης των απαγορευτικό.

- Συντήρηση: Μετά την εγκατάσταση των ενσύρματων συσκευών, οι μηχανικοί ελέγχου έχουν να αντιμετωπίσουν διάφορα προβλήματα συντήρησης της καλωδίωσης, όπως η διάβρωσή και η φυσική φθορά που προκαλείται από τη συχνή μετακίνηση των οργάνων. Οι ασύρματες συσκευές είναι σχεδόν αδιάφορες για τέτοιου είδους προβλήματα, αυτό το οποίο θα πρέπει να αντιμετωπίσουν είναι η πηγή ενέργειας την οποία φέρουν και η αυτονομία αυτής της πηγής.

- Μείωση κόστους: Η καλωδίωση και η εγκατάσταση για ένα σχέδιο αυτοματισμού μπορεί να αγγίξει το 80% του συνολικού κόστους (Zhao 2010: 47) του συστήματος. Με τη χρήση ασύρματων μέσων εξαλείφεται η καλωδίωση και το κόστος εγκατάστασης.

5.4.6 Εφαρμογές Συγκοινωνιών.

Ένα από τα κύρια σημεία-κλειδιά τα οποία τα ασύρματα δίκτυα αισθητήρων έχουν εφαρμογή είναι οι εφαρμογές διαχείρισης κίνησης, ο έλεγχος οχημάτων και κίνησης, η γνώση της θέσης και της ταχύτητας των οχημάτων στο οδικό δίκτυο, σε πραγματικό χρόνο. Τα ασύρματα δίκτυα αισθητήρων έχουν λάβει σημαντική προσοχή κατά την τελευταία δεκαετία και τα επιτυχημένα αποτελέσματα της ερευνητικής δραστηριότητας τα τοποθετούν ως μέσο επίλυσης του προβλήματος αυτού (Katiyar, et al 2010: 23). Τούτο γιατί η τεχνολογία των ασύρματων δικτύων αισθητήρων μπορεί να βοηθήσει στην υποδομή για την ανάπτυξη έξυπνων συστημάτων μεταφορών (ITS).



Εικόνα 29. Μοντέλο Επικοινωνίας Μεταξύ Οχημάτων.

Τα οχήματα είναι συνήθως εξοπλισμένα με ένα πλήθος βοηθημάτων όπως το bluetooth, με το οποίο διαμέσου ραδιοσυχνότητας μπορούν να επικοινωνήσουν μεταξύ τους. Στα

ITS το πιο σημαντικό στοιχείο είναι η κατάσταση του οχήματος, η οποία περιλαμβάνει την θέση του, την ταχύτητα και την διεύθυνσή του. Ορισμένοι πιθανοί αισθητήρες που μπορούν να χρησιμοποιηθούν για τα ITS είναι αυτοί της μαγνητικής αντίστασης, του φωτός, της πίεσης και του βίντεο το οποίο είναι ορατό ή υπέρυθρο (Katiyar, et al 2010: 24). Όσον αφορά τη μετάδοση των δεδομένων αυτών, υπάρχει συνήθως ασύρματων τεχνολογιών ή οποίες είναι διαθέσιμες όπως το Bluetooth, το ZigBee, το Wlan, το W max και το 3G (Chen 2009: 2).

Η χρήση αισθητήρων που είναι εγκατεστημένοι στα οχήματα δεν αντιμετωπίζει τους περιορισμούς ενέργειας, μιας και τροφοδοτούνται από την πηγή ενέργειας του αυτοκινήτου. Αυτό από μόνο του αποτελεί συγκριτικό πλεονέκτημα σε σχέση με άλλες υλοποιήσεις. Ωστόσο για να λειτουργήσει πιο αποδοτικά ένα σύστημα διαχείρισης κυκλοφορίας είναι σημαντικό να υπάρχουν και ορισμένοι σταθμοί βάσης όπου θα συλλέγουν ή θα εκπέμπουν ζωτικής σημασίας πληροφορίες.

Προς επίρρωση αυτού του σεναρίου, μπορεί να ειπωθεί ότι υπάρχει η δυνατότητα οχήματα τα οποία συναντούν ακραίες συνθήκες κατά τη διαδρομή τους, όπως το χιόνι, ή ολισθηρό οδόστρωμα, να μεταδώσουν τις πληροφορίες αυτές σε σταθμούς βάσης και αυτοί με τη σειρά τους στα επερχόμενα οχήματα, έτσι ώστε με αυτό τον τρόπο να προειδοποιήσουν τους χειριστές τους για τα επερχόμενα εμπόδια.

Επίσης με την μέτρηση του χρόνου που απαιτείται για την διάνυση μίας μονάδας απόστασης, μπορεί να αποφευχθεί η κυκλοφοριακή συμφόρηση και να οδηγηθούν τα οχήματα σε οδούς με λιγότερη κυκλοφορία. Απότοκος αυτού είναι η αποσυμφόρηση κύριων και νευραλγικών οδικών αρτηριών. Εφαρμογή των ασύρματων δικτύων αισθητήρων μπορεί να γίνει και στην προσπάθεια ενημέρωσης για έργα ή για κακή ποιότητα οδοστρώματος, ακόμα και για ενημέρωση ατυχημάτων που ενδέχεται να συναντήσει ένας οδηγός στα προπορευόμενα χιλιόμετρα. Οι πληροφορίες αυτές αποτελούν σημαντικό αρωγό στην ταχύτερη επέμβαση των υπηρεσιών έτσι ώστε να αποκατασταθεί η δυσλειτουργία στις υποδομές, αλλά και στην ταχύτερη αντιμετώπιση των ατυχημάτων από τις υπηρεσίες πρωτοβάθμιας υγείας (ασθενοφόρα).

Όλες οι επισημάνσεις οι οποίες τονίστηκαν πιο πάνω έχουν ως αντικειμενικό στόχο ένα μόνο γεγονός, την προώθηση της ασφαλούς οδήγησης, την ελαχιστοποίηση των

ατυχημάτων, την αρτιότερη διαχείριση του συγκοινωνιακού φόρου, αλλά και την επίτευξη καλύτερων συνθηκών οδήγησης. Τα επιτεύγματα αυτά έχουν ως αποτέλεσμα τη μείωση του κόστους, την μετακίνηση με καλύτερους όρους οικολογίας, αλλά και σε βάθος χρόνου την δημιουργία υποδομών και προϋ ποθέσεων ώστε κάθε όχημα να μετακινείται αυτόνομα χωρίς την ανθρώπινη παρέμβαση.

5.4.7 Εφαρμογές Επιτήρησης Χώρων.

Επιπρόσθετες εφαρμογές είναι η επιτήρηση χώρων κρίσιμης σημασίας. Σε αυτούς τους χώρους γίνεται η χρήση αισθητήρων κίνησης, κάτι το οποίο αποτελεί συχνά και λύση-μονόδρομο. Τέτοιοι χώροι μπορεί να είναι χώροι υψίστης σημασίας, όπως διοικητικά κέντρα πολιτικού και στρατιωτικού ενδιαφέροντος, ή χώροι αποθήκευσης υλικού, όπως χώροι στάθμευσης οχημάτων πολιτικής και στρατιωτικής χρήσης. Επιπρόσθετα η επιτήρηση χερσαίων και θαλάσσιων χώρων είναι μια εφαρμογή που στη σημερινή εποχή έχει τεράστιο πεδίο δράσης. (Chen 2009: 3).

5.4.8 Πολιτική Προστασία.

Στο πλαίσιο των εφαρμογών που συναντάμε στα ασύρματα δίκτυα αισθητήρων, άξια αναφοράς είναι και τα θέματα που άπτονται της πολιτικής προστασίας. Το πλαίσιο των εφαρμογών που μπορούν να υλοποιηθούν είναι ευρύ και έχει να κάνει τόσο με επείγουσες καταστάσεις, όσο και με την εποπτεία περιοχών που βρίσκονται σε αυξημένο κίνδυνο να εκδηλωθεί κάποια καταστροφή. Εξειδικεύοντας τα παραπάνω, ως παράδειγμα τεκμηρίωσης μπορούν να αναφερθούν ο έλεγχος πλημμυρών και η ανίχνευση πυρκαγιών.

Το φαινόμενο της πλημμύρας αποτελεί ένα φυσικό φαινόμενο το οποίο μπορεί να προκληθεί από πληθώρα αιτιών. Τα αίτια αυτά μπορεί να είναι είτε η παρατεταμένη βροχόπτωση, είτε η τήξη υπερβολικών ποσοτήτων πάγου, συνέπεια της κλιματικής αλλαγής. Είτε από υπερχείλιση κύριων ή δευτερευόντων ποταμών συνέπεια εξαιρετικά υπερβολικής βροχόπτωσης. Καθώς και καταστροφή τεχνικών μέσων όπως αναχώματα

ή φράγματα. Σε αντιστοιχία με το αίτιο το οποίο προκάλεσε την καταστροφή μπορεί να προταθεί το αντίστοιχο δίκτυο αισθητήρων το οποίο θα παρακολουθεί τις κρίσιμες μεταβλητές του συστήματος και θα ενημερώνει την εποπτεύουσα αρχή για την επερχόμενη καταστροφή. Ως τέτοιου είδους συστήματα προστασίας έχουν προταθεί τα συστήματα CYCLOPS και DORII (Esteves 2009: 3) τα οποία έχουν υλοποιηθεί επ' ωφελεία για τις ανάγκες της Πορτογαλικής πολιτικής προστασίας.

Τόσο το πρόγραμμα CYCLOPS όσο και το DORII έχουν πρόβλεψη και για τον τομέα της δασικής αστυνόμευσης και της πρόκλησης πυρκαγιών. Στον τομέα αυτό τα ασύρματα δίκτυα αισθητήρων είναι δυνατό να αναπτυχθούν σε τεράστιες γεωγραφικές περιοχές και να επιτηρούν περιοχές που βρίσκονται σε υψηλό δείκτη επικινδυνότητας. Οι μεταβλητές που δύναται να μετρηθούν είναι η ατμοσφαιρική πίεση, η θερμοκρασία, η ταχύτητα του ανέμου και η υγρασία. Μεταβλητές που μπορούν να προκαλέσουν ή να επιταχύνουν την εξάπλωση πυρκαγιών.

Τα οφέλη τα οποία αποκομίζονται από την επιτήρηση περιοχών είναι πολλά και ποικίλα, τόσο σε βραχυπρόθεσμο όσο και σε μακροπρόθεσμο χρόνο (προστασία περιοχών, διατήρηση χλωρίδας και πανίδας κα.).

Τέλος ως παράδειγμα τεκμηρίωσης μπορεί να αναφερθεί η επιτήρηση δημόσιων υποδομών στρατηγικής σημασίας. Ως τέτοιου είδους υποδομές μπορεί να αναφέρει κανείς μεγάλα εργοστάσια ηλεκτρικής ενέργειας που για την παραγωγή ενέργειας κάνουν χρήση φυσικών πόρων, όπως τα υδροηλεκτρικά φράγματα και τα αιολικά πάρκα. Αλλά και έργα υποδομών όπως γέφυρες, οδικά δίκτυα και σήραγγες υποθαλάσσιες ή μη. Οι τεχνικές επιτήρησης βοηθούν στο να εντοπιστούν παθογένειες και να αντιμετωπιστούν στοχευμένα. Οι τεχνικές αυτές αποσκοπούν στη διατήρηση των υποδομών για το μέγιστο δυνατό χρονικό διάστημα και στη μείωση του κόστους συντήρησης τους.

5.4.9 Οικιακές Εφαρμογές.

Οι έννοιες οικιακός αυτοματισμός, έξυπνο σπίτι, αυτοματοποιημένο οικιακό περιβάλλον η αυτοματισμός οικιακών λειτουργιών, συγκλίνουν σε ένα μόνο σκοπό: στην επιθυμία του ανθρώπου να δημιουργήσει και να εξοπλίσει μία οικία με αυτά τα μέσα, τα οποία θα εξασφαλίσουν όλες τις ανέσεις που είναι απαραίτητες για την αυτονομία της οικίας του.

Για να δημιουργηθεί ένα σύστημα αυτονομίας, θα πρέπει να υπάρχουν κάποια υποσυστήματα τα οποία να το υποστηρίζουν (El-Basioni 2013: 414). Τέτοια συστήματα είναι το σύστημα εισόδου, το σύστημα ανίχνευσης εισβολέα, το σύστημα εξαπάτησης εισβολέα, το σύστημα παρακολούθησης και ελέγχου συστατικών στοιχείων, η παρακολούθηση της υγείας της δομής της κατασκευής και το σύστημα περιποίησης των φυτών (El-Basioni 2013: 414).

Τα παραπάνω με την επικουρία των δυνατοτήτων τις οποίες προσδίδουν οι οικιακές μικροσυσκευές (ψυγείο κ.α.) αποτελούν άριστη υλοποίηση του λεγόμενου Διαδίκτυου των Πραγμάτων (Internet of Things), προσφέροντας αυτονομία και αυτοτέλεια στο χώρο που είναι εγκατεστημένες.

Κεφάλαιο 6
Επιθέσεις Ασφαλείας σε Ασύρματα Δίκτυα Αισθητήρων.

6 Επιθέσεις Ασφαλείας σε Ασύρματα Δίκτυα Αισθητήρων.

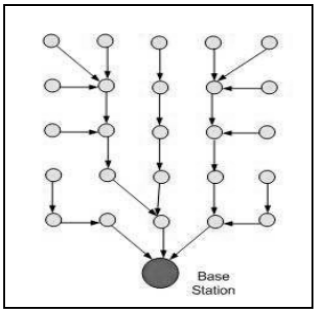
Η ασφάλεια στα ασύρματα δίκτυα αισθητήρων έχει ένα πλήθος από προκλήσεις, μερικές από τις οποίες είναι: η ασύρματη επικοινωνία μεταξύ των κόμβων, η έλλειψη προϋπάρχουσας υποδομής, η αλλαγή δυναμικά της τοπολογίας και οι περιορισμοί που υπεισέρχονται στους πόρους του δικτύου αναφορικά με τη μνήμης η διαχείριση της ενέργειας και το μικρό εύρος ζώνης επικοινωνίας.

Στο παρόν κεφάλαιο, θα δώσουμε μια γενική περιγραφή των επιθέσεων ασφαλείας που μπορούν να πραγματοποιηθούν σε ένα ασύρματο δίκτυο αισθητήρων. Θα εστιάσουμε αρχικά σε ειδικού τύπου επιθέσεις, οι οποίες μπορούν να εφαρμοστούν ακριβώς λόγω της ειδικής φύσης των ασύρματων δικτύων αισθητήρων.

6.1 Επίθεση Ανάλυσης Κυκλοφορίας .

Από τη φύση τους στα ασύρματα δίκτυα αισθητήρων η κίνηση διαμέσου των κόμβων έχει μία συγκεκριμένη μορφή, όπως πολλά-προς-ένα, ή πολλά προς-λίγα. Οι περισσότεροι

κόμβοι σε ένα δίκτυο στέλνουν τις παρατηρήσεις τους στο σταθμό βάσης (Βλέπε Εικόνα 30). Ο επίδοξος υποκλοπέας είναι σε θέση να συγκεντρώσει ένα πλήθος από πληροφορίες για την τοπολογία του δικτύου, όπως επίσης και για την τοποθεσία του σταθμού της βάσης. Είναι σε θέση να συγκεντρώσει και άλλες στρατηγικής σημασίας πληροφορίες για τους κόμβους, με μία παρατήρηση του όγκου της κίνησης και της διάρθρωσης της κίνησης (Roosta, Shieh, Sastry 2006: 5).



Εικόνα 30. Πρότυπο κυκλοφορίας σε ασύρματα δίκτυα.

Για την κατανόηση αυτού θέτουμε το ακόλουθο παράδειγμα. Ο αντίπαλος ενδέχεται να παρατηρεί την κίνηση και να συμπεραίνει ότι οι κόμβοι μπορεί να αποτελούν συνδετικούς κρίκους μεταξύ δύο τμημάτων του δικτύου. Τότε είναι σε θέση να επιτεθεί σε αυτούς τους κόμβους που βρίσκονται στα όρια, πράγμα που θα έχει ως αποτέλεσμα το διαχωρισμό του δικτύου σε δύο ασύνδετα τμήματα. Οποιαδήποτε διαδρομή από το ένα τμήμα στο άλλο θα πρέπει να διαπεράσει διαμέσου των κόμβων που έχουν παραβιαστεί. Εναλλακτικά ο επιτιθέμενος είναι σε θέση να εκτελέσει μια επίθεση άρνησης υπηρεσίας (DoS) εναντίον των κόμβων που βρίσκονται στην κορυφή της περικοπής, έχοντας ως στόχο να εξαντλήσει την φέρουσα ενέργεια τους. Απότοκος αυτού θα είναι η μείωση της διάρκειας ζωής του δικτύου.

Υπάρχουν κυρίως δύο τρόποι με τους οποίους ένας αντίπαλος μπορεί να πραγματοποιήσει ανάλυση κίνησης. Κατά τον πρώτο τύπο επίθεσης ο επιτιθέμενος παρατηρεί το ρυθμό αποστολής των πακέτων από τους κόμβους οι οποίοι βρίσκονται αρκετά κοντά σε αυτόν, και στη συνέχεια μετακινείται προς κόμβους που έχουν υψηλότερο βαθμό αποστολής πακέτων.

Κατά τον δεύτερο τύπο επίθεσης, ο επιτιθέμενος παρατηρεί τον χρόνο μεταξύ διαδοχικών αποστολών πακέτων μεταξύ γειτονικών κόμβων. Στη συνέχεια προσπαθεί να ακολουθήσει το μονοπάτι του πακέτου που έχει προωθηθεί μέχρι να φτάσει στο σταθμό βάσης.

Ένας τρόπος αντιμετώπισης των επιθέσεων ανάλυσης κυκλοφορίας είναι η χρήση πολλαπλών διαδρομών κατά την δρομολόγηση, κάνοντας χρήση πιθανολογικής διαδρομής, καθώς και την εισαγωγή ψευδών μηνυμάτων στο δίκτυο. Η χρήση ψευδών μηνυμάτων θα προκαλέσει ωστόσο πρόσθετη επιβάρυνση με όρους ενεργειακής κατανάλωσης και εσωτερικής κίνησης δεδομένων. Για να μπορέσουν ωστόσο τα ψευδή μηνύματα να είναι αποτελεσματικά στο να αποτρέψουν τους επιτιθέμενους από την γνώση οποιασδήποτε πληροφορίας, θα πρέπει να μοιάζουν με πραγματικά μηνύματα.

6.2 Επιθέσεις σε Πρωτόκολλα Διαχείρισης Κλειδιού.

Οι κόμβοι σε ένα δίκτυο αισθητήρων κάνουν χρήση είτε προδιανεμημένων κλειδιών, είτε κάποιας μορφής υλικού το οποίο θα παράγει ζεύγη κλειδιών δυναμικά. Τα κρυπτογραφικά κλειδιά είναι ταξινομημένα είτε σε ομάδες είτε σε ζεύγη. Επιπρόσθετα κάθε κόμβος θα πρέπει να ανακαλύψει τους γειτονικούς του κόμβους με τους οποίους μοιράζεται το ίδιο μυστικό κλειδί. Εάν δυο κόμβοι δεν μοιράζονται το ίδιο κλειδί απευθείας, τότε θα πρέπει να βρούνε μία διαδρομή η οποία θα συνδέει αυτούς τους κόμβους με αρκετά ασφαλή τρόπο.

Σκοπός του πρωτοκόλλου διαχείρισης κλειδιού είναι να προ-διανείμει τα κρυπτογραφικά κλειδιά μεταξύ των κόμβων πριν από την ανάπτυξή τους, καθώς επίσης και να ανακαλέσει τα κλειδιά εάν οι κόμβοι εγκαταλείψουν το δίκτυο. Επίσης, το πρωτόκολλο αυτό είναι υπεύθυνο να αναθέσει νέα ζεύγη κλειδιών στους κόμβους που θα ενταχθούν στο δίκτυο ή όταν κάποια ζεύγη κλειδιών θα έχουν λήξει (Roosta, Shieh, Sastry 2006: 4).

Υπάρχουν δύο κύριες προτάσεις σχημάτων διαχείρισης των ίδιων στα ad-hoc δίκτυα: τα ντετερμινιστικά (Deterministic) και τα πιθανολογικά (Probabilistic). Ένας τυπικός

ντετερμινιστικός αλγόριθμος εγκαθιστά σε κάθε κόμβο ένα κοινό απλό κλειδί, ενώ στην πιθανολογική προσέγγιση ένα κλειδί μακράς διάρκειας ισχύος σε κάθε κόμβο επιλέγεται τυχαία από μία δεξαμενή κλειδιών (Dwoskin, et al 2007: 168). Εφόσον τα κλειδιά μακράς διάρκειας θα έχουν αναπτυχθεί στο κινητό δίκτυο,. χρησιμοποιούνται για αμοιβαία αυθεντικοποίηση μεταξύ των ζευγών των κόμβων (που βρίσκονται στην ίδια επικοινωνιακή ακτίνα), προκειμένου να εγκαθιδρύσουν ζεύγη συμμετρικών κλειδιών κρυπτογράφησης για μελλοντική επικοινωνία.

Όταν οι γειτονικοί κόμβοι δεν διαμοιράζονται μακροπρόθεσμα κλειδιά, θα πρέπει να βασίζονται για την επικοινωνία τους σε άλλους κόμβους οι οποίοι βρίσκονται εντός της επικοινωνιακής τους ακτίνας για να εγκαθιδρύσουν ζεύγη κλειδιών. Η εγκαθίδρυση ζευγών κλειδιών και οι μελλοντικές επικοινωνίες είναι δυνατόν να υποκλαπούν από άλλους κόμβους που βρίσκονται εντός της επικοινωνιακής ακτίνας, υπό την προϋ πόθεση ότι οι εν λόγω κόμβοι έχουν τα αντίστοιχα μακροπρόθεσμα ζεύγη κλειδιών.

Στα αστικά δίκτυα, όπου οι κόμβοι δεν είναι εφικτό να μετακινηθούν μετά από την αρχική εγκατάσταση, τόσο η ντετερμινιστική όσο και η πιθανολογική προσέγγιση μπορούν να προσφέρουν ασφάλεια. Με την ανταλλαγή μηνυμάτων κρυπτογραφημένων με τα αρχικά κοινά κλειδιά ή τα διανεμημένα κλειδιά, δύο γειτονικοί κόμβοι μπορούν να παράγουν τυχαία ζεύγη κλειδιών, τα οποία θα είναι γνωστά μόνο σε αυτούς. Τα ζεύγη κλειδιών δεν είναι εφικτό να αποκαλυφθούν, ακόμα και αν τα αρχικά μακροπρόθεσμα κλειδιά αργότερα αποκαλυφθούν.

Αντίθετα, στα κινητά δίκτυα, οι κόμβοι συνεχώς βρίσκονται σε κίνηση και πρέπει. Σε αυτήν την περίπτωση, σε ένα ντετερμινιστικό σύστημα κλειδιού, η πιθανότητα επιτυχούς επίθεσης μπορεί να είναι της τάξης του 100%. Ωστόσο και το πιθανολογικό σχήμα είναι επίσης αρκετά ευάλωτο, Το ποσοστό του αγγίζει την πιθανότητα του 60% για μια επιτυχή επίθεση (Dwoskin, et al 2007: 169). Αιτία αυτού είναι ότι, σε μία πιθανολογική προσέγγιση, για να αυξηθεί η συνδεσιμότητα, απαιτείται η αναμετάδοση του κλειδιού. Με την αναχαίτιση/υποκλοπή των πληροφοριών κλειδιού τα οποία αναμεταδίδονται, ένας κόμβος ο οποίος είναι υπό τον έλεγχο του επιτιθέμενου/εισβολέα, είναι σε θέση να αναγνωρίσει το κλειδί το οποίο δύο εξουσιοδοτημένοι κόμβοι θα χρησιμοποιήσουν για μια μελλοντική επικοινωνία. Αυτή η «man in the middle» εφαρμογή για επίθεση, μπορεί να αυξήσει σημαντικά την επιτυχή πιθανότητα επίθεσης για μία

πιθανολογική προσέγγιση, δεδομένου ότι υπάρχει υψηλή πιθανότητα της χρησιμοποίησης της αναμετάδοσης για την εγκατάσταση μιας σύνδεσης σε ένα κινητό περιβάλλον. Αν ο υποκλοπέας έχει υπό τον έλεγχό του πολλούς κόμβους, η πιθανότητα επιτυχούς επίθεσης αυξάνεται περισσότερο (Dwoskin, et al 2007: 169).

Στο σημείο αυτό πρέπει να τονιστεί ότι υπάρχει και η υβριδική (Hybridic) προσέγγιση στην οποία γίνεται ένας συνδυασμός ντετερμινιστικής και πιθανολογικής προσέγγισης με τα πλεονεκτήματα και τα μειονεκτήματα της κάθε μιας.

Πιθανή λύση στο πρόβλημα αυτό μπορεί να είναι η υλοποίηση πρωτοκόλλων δημόσιου κλειδιού στους κόμβους. Ωστόσο η λύση αυτή ελλοχεύει αρκετούς κινδύνους μιας και η υλοποίηση πρωτόκολλου δημόσιου κλειδιού στους ασύρματους κόμβους, με τους γνωστούς περιορισμούς ως προς την κατανάλωση ενέργειας και στους πόρους μνήμης, δεν μπορεί να χαρακτηριστεί ως μία εφικτή επιλογή.

6.3 Σιβυλλικές Επιθέσεις.

Στην σιβυλλική επίθεση (Sybil Attack), η οποία αποτελεί μία αρκετά σημαντική επίθεση, ένας κακόβουλος κόμβος συμπεριφέρεται σαν να είναι ένα μεγάλο πλήθος κόμβων. Για παράδειγμα μιμείται άλλους κόμβους ή ακόμα διεκδικεί ψευδείς ταυτότητες. Στο χειρότερο δυνατό σενάριο, ο επιτιθέμενος είναι δυνατό να δημιουργήσει ένα αυθαίρετο αριθμό από επιπρόσθετες ταυτότητες κόμβων, κάνοντας χρήση μόνο μιας φυσικής συσκευής (Newsome, et al 2004: 3). Η σιβυλλική επίθεση αναφέρεται στο σενάριο όπου ένας κακόβουλος κόμβος προσποιείται ότι έχει πλήθος ψευδών ταυτοτήτων.

Το πλήθος των πρωτοκόλλων που μία σιβυλλική επίθεση μπορεί να πλήξει είναι αρκετά ευρύ. Μερικά από αυτά είναι: α) το κατανεμημένης αποθήκευσης, όπου κανονικά το σύστημα αναπαράγει δεδομένα σε συγκεκριμένους κόμβους, και μέσω της επίθεσης μπορεί να τα αναπαράγει σε «σιβυλλικού» κόμβους, β) το πρωτόκολλο δρομολόγησης, όπου φαινομενικά ασύνδετες διαδρομές θα μπορούσαν στην πραγματικότητα να φαίνεται ότι είναι συνδεόμενες λόγω ενός «σιβυλλικού» κόμβου, γ) στη συγκέντρωση δεδομένων (data aggregation), όπου τα πρωτόκολλα συγκεντρώνουν τα διάφορα

δεδομένα στο δίκτυο για λόγους εξοικονόμησης ενέργειας (αντί να διαμοιράζονται μεταξύ πολλών κόμβων), και με την επίθεση αυτή ο επιτιθέμενος μπορεί να προσθέσει δεδομένα αλλοιώνοντας το σύνολο, δ) σε πρωτόκολλο «ψηφοφορίας», όπου η σιβυλλική επίθεση μπορεί να χρησιμοποιηθεί για να "γεμίσει την κάλπη" σε κάποια ψηφοφορία (πρωτόκολλα ψηφοφορίας, για διάφορα θέματα, υλοποιούνται σε δίκτυα αισθητήρων), ε) στο πρωτόκολλο κατανομής πόρων, έτσι ώστε να προκαλέσει ο επιτιθέμενος μη δίκαιη κατανομή των πόρων και στ) στην ανίχνευση ανάρμοστης συμπεριφοράς, όπου ο επιτιθέμενος μπορεί να δρα κατά τρόπο τέτοιο ώστε συμπεριφορές που θα ήταν ανιχνεύσιμες ως ύποπτες να μην ανιχνεύονται και αντίστροφα. (Newsome, et al 2004: 3-4).

Οι προτεινόμενες λύσεις για την αντιμετώπιση των σιβυλλικών επιθέσεων περιλαμβάνουν ορισμένες διαδικασίες. Οι διαδικασίες αυτές επιτάσσουν τον έλεγχο του μέσου μετάδοσης. Ο έλεγχος αυτός βασίζεται στην παραδοχή ότι κάθε συσκευή έχει μόνο μία συχνότητα μετάδοσης.

Ως δεύτερη λύση μπορεί να χρησιμοποιηθεί η προδιανομή του κλειδιού που να συνδέει την ταυτότητα του κόμβου με το κλειδί το οποίο έχει προ διανεμηθεί, έτσι ώστε να μπορεί να εξακριβωθεί ότι ο κόμβος είναι πραγματικά αυτός ο οποίος ισχυρίζεται ότι είναι (Roosta, Shieh, Sastry 2006: 5).

Επίσης προτείνεται η καταχώρηση της ταυτότητας του κόμβου στον κεντρικό σταθμό βάσης. Τέλος μπορεί να προταθεί η επαλήθευση της θέσης, αλλά αυτό μπορεί να επιτευχθεί μόνο αν γίνει η υπόθεση ότι η τοπολογία του δικτύου είναι στατική.

Οι λύσεις οι οποίες προτείνονται σαφώς και έχουν τα μειονεκτήματά τους. Δεν μπορεί να δοθεί κανενός τύπου εγγύηση ότι οι χρησιμοποιούμενες συσκευές θα φέρουν μόνο μία συχνότητα. Στην πραγματικότητα ορισμένα πρωτόκολλα MAC βασίζονται στο ότι κάθε κόμβος θα έχει πάνω από μια ραδιοσυχνότητα. Η χρήση προ διανεμημένου κλειδιού και η χρήση κρυπτογράφησης δημόσιου κλειδιού, συναντά τους περιορισμούς ισχύος και ενέργειας που έχουν οι ασύρματοι κόμβοι. Τέλος, δεν μπορεί επίσης να δοθεί καμιά εγγύηση ότι η τοπολογία του δικτύου θα είναι στατική και ότι οι κόμβοι δεν θα επανατοποθετούνται.

6.4 Επιθέσεις σε Συστήματα Φήμης.

Τα συστήματα φήμης (Reputation Schemes) αποτελούν άριστα εργαλεία στους μηχανισμούς αυτοελέγχου, ώστε να αντιμετωπίζουν τις απειλές από κόμβους που έχουν παραβιαστεί (Roosta, Shieh, Sastry 2006: 5). Λειτουργούν κάνοντας τακτοποίηση ποιοι κόμβοι κρίνονται ως «εγωιστές» (δηλαδή συμπεριφέρονται με μη συνεργατικό τρόπο), και αυτούς τους κόμβους τους θέτουν σε απομόνωση από το υπόλοιπο δίκτυο. Κατά αυτόν τον τρόπο βοηθούν τους χρήστες αλλά και τους κόμβους του δικτύου να αποφασίσουν ποιοι κόμβοι είναι αξιόπιστοι, ώστε να ξεκαθαριστεί ποιους μπορούν να εμπιστευτούν και να επικοινωνήσουν μαζί τους.

Τα συστήματα φήμης τα οποία είναι κεντρικοποιημένα είναι αρκετά γνωστά σε εφαρμογές διαδικτύου, ενώ τα αποκεντροποιημένα είναι ευρύτατα γνωστά για την εφαρμογή τους σε ad-hoc συστήματα. Ορισμένα συστήματα φήμης και τα σχετικά τους πρωτόκολλα αναγκάζουν τον κάθε κόμβο να κάνει πρόσθετες ενέργειες, για να παρατηρήσουν και ακολούθως να αξιολογήσουν τη συμπεριφορά τους. Εάν ο κόμβος δεν προωθεί το μήνυμα, τότε η φήμη του μειώνεται και η πληροφορία της κακής φήμης πολλαπλασιάζεται διαμέσου του δικτύου.

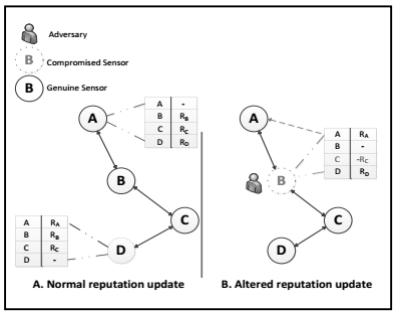
Επίσης κάθε κόμβος κάνει χρήση πληροφοριών από άλλους κόμβους ώστε να μπορέσει να υπολογίσει την συνολική φήμη ενός κόμβου. Σε βάθος χρόνου, κόμβοι με κακή συμπεριφορά έχουν κακή αξιοπιστία και δεν αξιοποιούνται για τον σχεδιασμό αξιόπιστων διαδρομών.

Ένα πλαίσιο για την εισαγωγή αξιοπιστίας στα δίκτυα αισθητήρων υιοθετεί την λύση μηχανισμών "φρουρών" (Watchdog). Σκοπός των μηχανισμών φρουρών, είναι η παρακολούθηση των γειτονικών κόμβων και ο καθορισμός εάν κάποιος από αυτούς τους κόμβους αποκλίνει της μέχρι εκείνη τη στιγμή αναμενόμενης συμπεριφοράς.

Οι επιθέσεις συστημάτων φήμης είναι η εξής: επίθεση κακής τοποθέτησης (Bad mounting attack), επίθεση Ψηφοφορίας Στελέχωσης (Ballot Stuffing Attack), επίθεση On-Off (On - off Attack), επίθεση Νεοεισερχόμενου (Newcomer Attack).

6.4.1 Επίθεση κακής Τοποθέτησης.

Αυτού του είδους η επίθεση στοχεύει στο να χορηγήσει (άδικα) αρνητική βαθμολογία σε αξιόπιστους κόμβους. Μόλις ο αντίπαλος έχει υπό τον έλεγχό του ένα κόμβο, μπορεί να επηρεάσει την φήμη του συστήματος θέτοντας, ψευδώς, αρνητική ανατροφοδότηση σε άρτια συμπεριφερόμενους κόμβους.

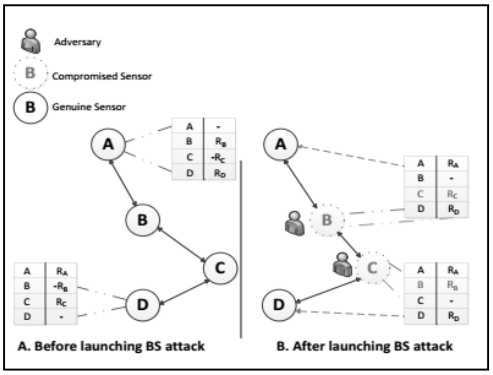


Εικόνα 31. Επίθεση Κακής Τοποθέτησης.

Όταν αυτές οι λανθασμένες παρατηρήσεις μεταδοθούν σε άλλους κόμβους, θα χρησιμοποιηθούν από τους γειτονικούς κόμβους στη φάση υπολογισμού της φήμης, εάν μέχρι εκείνη την στιγμή δεν υπάρξει κατάλληλη επαλήθευση. Απόρροια αυτού θα είναι η δημιουργία αρνητικής τιμής για τους κόμβους με ορθή συμπεριφορά που έχουν γίνει «θύματα» της επίθεσης (Alzaid 2013: 66).

6.4.2 Επίθεση Ψηφοφορίας.

Οι επιθέσεις ψηφοφορίας (Ballot Stuffing Attack) είναι αρκετά όμοιες με τις επιθέσεις τύπου bad mounting που περιγράφηκαν νωρίτερα. Ωστόσο η ειδοποιός τους διαφορά είναι ότι σε αυτή την περίπτωση ο επιτιθέμενος προσπαθεί να κάνει ακριβώς το αντίθετο, δηλαδή να παράσχει άδικα θετικές βαθμολογίες. Η αξιοπιστία των κόμβων με κακή φήμη επηρεάζεται κάνοντας ανάθεση σε αυτούς τους κακόβουλους κόμβους θετική ανατροφοδότηση.

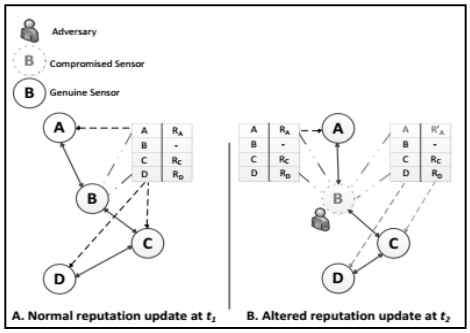


Εικόνα 32. Επίθεση Ψηφοφορίας.

Η επίθεση αυτή είναι ορατή σε σενάρια που λαμβάνονται υπόψη οι έμμεσες παρατηρήσεις και οι συμβαλλόμενοι μπορούν να μοιραστούν τις θετικές τους τιμές ανατροφοδότησης με τους γειτονικούς τους κόμβους (Alzaid 2013: 67).

6.4.3 Επίθεση ON-OFF.

Σε αυτού του είδους τις επιθέσεις, ο επιτιθέμενος στοχεύει να απασχολήσει το σύστημα στην ολότητά του για να περιορίσει την απόδοσή του, ελπίζοντας με αυτή την κίνηση ότι δεν θα εντοπιστεί ή θα αποκλειστεί από το δίκτυο. Ο επιτιθέμενος διαφοροποιεί τη φαινομενικά φυσιολογική και μη φυσιολογική του συμπεριφορά με σκοπό να επεκτείνει τον χρόνο που απαιτείται για να ανιχνευτούν οι μη κανονικότητες στην συμπεριφορά του. Αυτό του είδους οι επιθέσεις συνήθως εξαπολύονται εναντίον των δραστηριοτήτων φήμης ή των γενικών δραστηριοτήτων στα ασύρματα δίκτυα αισθητήρων (Alzaid 2013: 67).



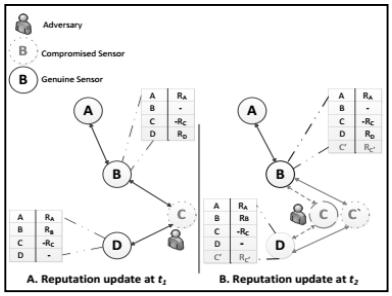
Εικόνα 33. Επίθεση ON-OFF

6.5 Επίθεση Νεοεισερχόμενου.

Στην επίθεση αυτή μόλις η τιμή του επιτιθέμενου αρχίζει να φθίνει και να τοποθετείται κάτω από μία τιμή αξιοπιστίας, πράγμα το οποίο έχει ως συνέπεια τη μετακίνησή του από την ζώνη της αξιοπιστίας στην ζώνη της αναξιοπιστίας, τότε ο επιτιθέμενος βρίσκει μεθόδους ώστε να μετακινηθεί ξανά στη ζώνη της αξιοπιστίας, αυξάνοντας την τιμή της αξιοπιστίας του. Ένας τρόπος για να το πετύχει αυτό είναι να αλλάξει την ταυτότητά του και να ενταχθεί ξανά στο δίκτυο με τη νέα ταυτότητα, «εκκαθαρίζοντας» το κακό του ιστορικό. Αυτή η επίθεση είναι γνωστή ως η επίθεση του νεοεισερχόμενου (Newcomer) εάν ο επιτιθέμενος έχει την ικανότητα να πραγματοποιεί αυτού του είδους τις επιθέσεις. Η ανίχνευση των ανωμαλιών στην συμπεριφορά του δεν είναι κάτι το οποίο θα πρέπει να απασχολεί τον επιτιθέμενο το ιστορικό του μπορεί να διαγραφεί ανά πάσα στιγμή (Alzaid 2013: 67).

Επιπρόσθετα, εγείρονται και άλλα ζητήματα αναφορικά με το πλαίσιο της φήμης των συστημάτων. Εφόσον το μέσο μετάδοσης είναι ασύρματο, οι κόμβοι σε γειτονικούς χώρους είναι σε θέση να ακούσουν την επικοινωνία του κόμβου μετάδοσης. Η ιδιότητα της πολυακρόασης χρησιμοποιείται από το μηχανισμό φύλαξης για να καθορίσει την ανάρμοστη συμπεριφορά. Ωστόσο, σε ένα πλήθος εφαρμογών στα δίκτυα αισθητήρων, δεν είναι εφικτό να γίνει χρήση της ιδιότητας της πολυακρόασης. Με γνώμονα τα προβλήματα ασφαλείας τα οποία αντιμετωπίζουν τα συστήματα φήμης, μαζί με την έλλειψη μεθόδων για την ανάπτυξη μηχανισμού φύλαξης, η δημιουργία ενός αξιόπιστου

συστήματος φύλαξης, αποτελεί ένα πρόβλημα, που μπορεί να χαρακτηριστεί ως μεγάλη πρόκληση.



Εικόνα 34. Επίθεση Νεοεισερχόμενου.

6.6 Επίθεση Συνάθροισης Εσωτερικών Δεδομένων Δικτύου.

Κατά το τελευταίο χρονικό διάστημα, τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται ευρέως σε εφαρμογές του πραγματικού φυσικού κόσμου και των απαιτήσεών του. Στις περισσότερες των περιπτώσεων, όπως έχει ήδη ειπωθεί και σε άλλα χωρία της παρούσας διατριβής, οι κόμβοι δημιουργούν ένα πολύ-βηματικό δίκτυο, ενώ ο σταθμός βάσης τους ενεργεί ως το κεντρικό σημείο ελέγχου. Στην τυπική τους διαμόρφωση οι κόμβοι έχουν περιορισμούς όσον αφορά τις υπολογιστικές τους δυνατότητες και τα αποθέματα ενέργειας, τη στιγμή που ο σταθμός βάσης επιθυμεί να συλλέξει τις πληροφορίες που έχει ανιχνεύσει ο κάθε κόμβος του δικτύου (Sankardas, et al 2014: 683). Δεδομένων των περιορισμών σε πόρους που έχει ένας κόμβος αισθητήρων, είναι δυνατό για όλους τους κόμβους να στείλουν πίσω στο σταθμό βάσης όλα τα δεδομένα τους.

Επιπλέον ο αριθμός της σύγκρουσης πακέτων θα αυξηθεί σημαντικά εάν οι κόμβοι αναφέρουν τις παρατηρήσεις τους στο σταθμό βάσης. Ως εκ τούτου, ορισμένοι από τους ενδιάμεσους κόμβους συγχωνεύουν τα δεδομένα τους με αυτά των γειτονικών τους κόμβων και τα στέλνουν συγκεντρωτικά (συναθροισμένα) πίσω στο σταθμό βάσης τους – το λεγόμενο φαινόμενο της συνάθροισης ή συγκέντρωσης δεδομένων. Είναι επίσης πιθανό, να υπάρχει μία ιεραρχία μεταξύ των κόμβων και στο κάθε επίπεδο ένας κόμβος

να συγχωνεύει τα δεδομένα, από τους κόμβους που βρίσκονται στο επίπεδο ακριβώς από κάτω.

Η συνάθροιση δεδομένων στο εσωτερικό δίκτυο μπορεί να μειώσει την ποσότητα της επικοινωνίας και ως εκ τούτου την κατανάλωση ενέργειας στα ασύρματα δίκτυα αισθητήρων - ιδιαίτερα σε αυτά που έχουν μεγάλο γεωγραφικό εύρος. Όπως έχει ήδη αναφερθεί, η κύρια ιδέα είναι ο συνδυασμός μερικών αποτελεσμάτων στους ενδιάμεσους κόμβους κατά την διαδρομή του μηνύματος. Η μία προσέγγιση προτάσσει την δημιουργία ενός συνδετικού δέντρου το οποίο θα είναι συνδεδεμένο με το σταθμό βάσης και στη συνέχεια να προβεί σε συνάθροιση δεδομένων εσωτερικά του δικτύου κατά μήκος του δέντρου. Οι σημαντικές συναθροίσεις, κατά την επιστημονική κοινότητα, περιλαμβάνουν την μέτρηση δεδομένων και το άθροισμά τους. Είναι απλό να γενικεύονται αυτές οι συναθροίσεις για να δηλώσουν το σύνολο (Sankardas, et al 2014: 683).

Εύκολα γίνεται αντιληπτό είναι ότι εάν ορισμένοι κόμβοι έχουν παραβιαστεί τότε μπορούν να εγχέουν ψευδή δεδομένα στο δίκτυα. Απόρροια αυτού θα είναι μία κατεστραμμένη συνάθροιση δεδομένων.

Στην ιεραρχική προσέγγιση, υπάρχουν ιεραρχίες κόμβων. Στο κάθε επίπεδο, ένας αρχηγικός κόμβος επιλέγεται, και οι υπόλοιποι κόμβοι στέλνουν τις παρατηρήσεις τους στον κόμβο-αρχηγό. Οι αρχηγοί κάνουν χρήση ενός συστήματος στάθμισης για τη σύντηξη των παρατηρήσεών τους. Οι κόμβοι-αρχηγοί, στη συνέχεια, στέλνουν τις συντηγμένες παρατηρήσεις τους στο σταθμό βάσης. Ο σταθμός βάσης δημιουργεί τη διαδρομή του αντικειμένου με βάση τα συγκεντρωτικά στοιχεία που έλαβε. Ωστόσο εάν ένα ποσοστό των κόμβων έχει παραβιαστεί και έχει στείλει ψευδείς παρατηρήσεις στους κόμβους-αρχηγούς, οι παρατηρήσεις που θα γίνουν θα οδηγήσουν σε εσφαλμένα συμπεράσματα. Απόρροια αυτού θα είναι η διαδρομή που έχει σχηματιστεί από το σταθμό της βάσης να είναι είτε λανθασμένη ή σε ορισμένες περιπτώσεις μη υπαρκτή. Η η απώλεια επικοινωνίας η οποία θα προέλθει ως απόρροια αστοχιών κόμβων και της μετάδοσης μπορεί να επηρεάσει δυσμενώς τις τεχνικές συνάθροισης. Για να αντιμετωπιστεί το πρόβλημα αυτό, μπορεί να γίνει χρήση τεχνικών πολλαπλών διαδρομών δρομολόγησης για την προώθηση των υποσυνόλων (Sankardas, et al 2014: 684).

Η πιθανότητα της «υπονόμευσης» κόμβων – δηλαδή του να τεθεί ένας κόμβος υπό τον πλήρη έλεγχο του εισβολέα - εισαγάγει πολλές προκλήσεις. Τούτο γιατί οι περισσότεροι αλγόριθμοι στη συνάθροιση του εσωτερικού δικτύου δεν κάνουν πρόβλεψη για την ασφάλεια. Ένας υπονομευμένος κόμβος είναι πιθανό να προσπαθήσει να ματαιώσει την διαδικασία συνάθροισης με τη δημιουργία πολλών επιθέσεων.

Στο ακαδημαϊ κό πεδίο έχουν προταθεί ορισμένες λύσεις για τις διαδικασίεστο εσωτερικό του δικτύου. Οι προτάσεις που έχουν δοθεί είναι η χρήση στατιστικών δεδομένων– ιδιοτήτων, για να μειωθεί το αποτέλεσμα των επιθέσεων στη διαδικασία συνάθροισης.

Δεύτερη μέθοδος είναι η δημιουργία ασθενούς ιεραρχίας από συστάδες κόμβων. Η χρήση κρυπτογραφικών κλειδιών σε κάθε επίπεδο της ιεραρχίας χρησιμοποιείται για την εγκαθίδρυση ασφαλούς επικοινωνίας μεταξύ των κόμβων-συστάδων. Επιπλέον γίνεται αναφορά στην εγκαθίδρυση κρυπτογραφικού κλειδιού για να διασφαλιστεί η ασφάλεια στα συγχωνευμένα δεδομένα (Roosta, Shieh, Sastry 2006: 5).

Μία πιθανότητα για να εξασφαλιστεί η ασφάλεια σε ένα δίκτυο άθροισης δεδομένων είναι η χρήση ενός συστήματος φήμης. Τα δεδομένα ενός κόμβου λαμβάνονται υπόψη εάν η φήμη του κόμβου είναι αρκετά υψηλή, διαφορετικά απορρίπτεται. Ωστόσο η χρήση αυτής της λύσης απαιτεί την ύπαρξη ενός ισχυρού και ανθεκτικού σε επιθέσεις συστήματος φήμης. Επιπρόσθετη πιθανότητα είναι χρήση ισχυρών στατιστικών μεθόδων για την εκτίμηση ενός μέσου όρου, που δεν είναι τόσο επιρρεπής σε σφάλματα (Roosta, Shieh, Sastry 2006: 5).

6.7 Επιθέσεις σε Πρωτόκολλα Συγχρονισμού Χρόνου.

Πολλές εφαρμογές αισθητήρων δικτύου απαιτούν χρόνο για να συγχρονιστούν εντός του δικτύου. Τέτοιου είδους εφαρμογές περιλαμβάνουν, κινητό εντοπισμό αντικειμένων, συγχώνευση δεδομένων, πρωτόκολλα πολλαπλής ταυτότητας κ.α. Ας λάβουμε υπόψη τις εφαρμογές για την ανίχνευση των κινητών αντικειμένων, στην οποία ένα δίκτυο αισθητήρων έχει αναπτυχθεί στην περιοχή του ενδιαφέροντος με σκοπό την ανίχνευση

των διερχόμενων, περαστικών κόμβων. Όταν ένα αντικείμενο εμφανιστεί, ο κόμβος ανίχνευσης καταγράφει την ανιχνευθείσα τοποθεσία και την ανιχνευθείσα ώρα. Στη συνέχεια αυτές οι πληροφορίες τοποθεσίας και χρόνου αποστέλλονται στον κόμβο ανίχνευσης ο οποίος υπολογίζει την τροχιά κίνησης του αντικειμένου. Χωρίς έναν ακριβή χρόνο συγχρονισμού, η εκτιμώμενη τροχιά του ανιχνευθέντος αντικείμενου μπορεί να διαφέρει αρκετά από το πραγματικό (Song, et al 2007: 124).

Τα πρωτόκολλα συγχρονισμού παρέχουν μηχανισμούς για τον συγχρονισμό των τοπικών ρολογιών του κόμβου σε ένα δίκτυο αισθητήρων. Όλοι οι μηχανισμοί συγχρονισμού κόμβων βασίζονται σε κάποιο βαθμό ανταλλαγής μηνυμάτων μεταξύ των κόμβων. Η διεθνής βιβλιογραφία (Roosta 2006: 4, Song, 2007: 124) έχει προτείνει αρκετά σχηματικά μοντέλα για την αντιμετώπιση του προβλήματος συγχρονισμού χρόνου. Τα σχήματα αυτά περιλαμβάνουν την ανταλλαγή μηνυμάτων συγχρονισμού πολλαπλού χρόνου, είτε μεταξύ των πολλαπλών κόμβων ανίχνευσης είτε μεταξύ δύο κόμβων αισθητήρων που πρέπει να συγχρονιστούν.

Ωστόσο κανένα από αυτά δεν έχει σχεδιαστεί με γνώμονα την ασφάλεια, αν και η ασφάλεια αποτελεί σημαντικό συστατικό στοιχείο στα ασύρματα δίκτυα αισθητήρων. Εάν ένας επιτιθέμενος είναι σε θέση να καταστρέψει ορισμένους κόμβους, μπορεί να προτιμήσει ακόμη πιο σοβαρές επιθέσεις από το να εξολοθρεύσει τελείως ένα κόμβο, μιας και είναι πιο επικίνδυνο να αναλάβει δράση πάνω σε δεδομένα, παρά σε κόμβους με καθόλου δεδομένα.

Υπάρχει συνεπώς ο κίνδυνος, εάν ένας επιτιθέμενος επιτεθεί σε πρωτόκολλα, συγχρονισμού, η θέση συγχρονισμού ενός κινητού αντικείμενου να είναι αντίθετη από την κανονική θέση. Ως εκ τούτου, μια λανθασμένη ή υψηλής επικινδυνότητας ενέργεια μπορεί να λάβει χώρα.

Η εκ των υστέρων (Post Facto) μέθοδος συγχρονισμού αποτελεί την πρώτη μέθοδο για θέματα συγχρονισμού στα ασύρματα δίκτυα. Σε αυτήν τη μέθοδο, τα ρολόγια των κόμβων δεν είναι συγχρονισμένα. Όταν ένα γεγονός συμβαίνει, τότε κάθε κόμβος καταγράφει την ώρα του γεγονότος με βάση το δικό του ρολόι. Μετά το γεγονός αυτό, ένας τρίτος κόμβος, ο οποίος επενεργεί ως φάρος, μεταδίδει ένα παλμό συγχρονισμού σε όλους τους κόμβους που βρίσκονται στην περιοχή. Όλοι οι κόμβοι οι οποίοι έχουν λάβει

αυτόν τον παλμό θα τον χρησιμοποιήσουν ως αναφορά ώστε να ομαλοποιήσουν την χρονοσήμανση του γεγονότος.

Οι τεχνικές συγχρονισμού οι οποίες έχουν προταθεί για τα ασύρματα δίκτυα αισθητήρων είναι βασισμένες σε δύο μοντέλα, το μοντέλο δέκτης – δέκτης και το μοντέλο αποστολέας – δέκτης. Υπάρχει και μία άλλη εναλλακτική, το σχήμα συγχρονισμού βασισμένο στην αναμετάδοσή RBS (Reference Broadcast Synchronization), που είναι βασισμένο σε μία απλή ιδέα: τη χρήση μίας τρίτης εξωτερικής οντότητας για τον συγχρονισμό. Εδώ ένας τρίτος κόμβος χρησιμοποιείται ως κόμβος αναφοράς. Στην περίπτωση αυτή ο χρόνος συγχρονισμού είναι η διαφορά μεταξύ του χρόνου του κόμβου αναφοράς και των τοπικών κόμβων. Ωστόσο, στην περίπτωση αυτή ο επιτιθέμενος σκόπιμα μπορεί στον κόμβο αναφοράς να καθυστερήσει ορισμένα από τα μηνύματα χρόνου, ώστε στο σήμα RBS να υπάρξει μία αποτυχία στη διαδικασία συγχρονισμού (Song, et al 2007: 124). Η επίθεση αυτή ονομάζεται επίθεση καθυστέρησης (Delay attack)

Τα πρωτόκολλα αποστολέα–παραλήπτη είναι και αυτά ευάλωτα σε επιθέσεις συγχρονισμού. Σε αυτό το μοντέλο ο αποστολέας και ο παραλήπτης ανταλλάσσουν πακέτα συγχρονισμού, εκτιμώντας το χρόνο επιστροφής της μετάδοσης μεταξύ τους. Δεδομένου ότι μόνο δύο κόμβοι εμπλέκονται στη διαδικασία, επιτρέπει σε αυτό το μοντέλο να μην υποφέρει από τις επιθέσεις που εισαγάγει ένας κακόβουλος κόμβος αναφοράς. Ωστόσο ένας κόμβος μπορεί να εξαπατηθεί εάν ο κόμβος με τον οποίο διενεργεί την διαδικασία του συγχρονισμού είναι κακόβουλος. Ως εκ τούτου τα συστήματα αυτά υπόκεινται επίσης στους περιορισμούς επιθέσεων καθυστέρησης.

Η γενική ιδέα για την αντιμετώπιση επιθέσεων συγχρονισμού υιοθετεί την ακόλουθη λογική. Μετά την συλλογή ενός συνόλου μετατοπίσεων από κόμβους που έχουν εμπλακεί στη διαδικασία, γίνεται η ανάγνωση των κακόβουλων χρονικών μετατοπίσεων που βρίσκονται κάτω από την επίθεση καθυστέρησης. Οι αναγνωρισμένες κακόβουλες χρονικές μετατοπίσεις θα αποκλειστούν και οι υπόλοιπες χρονικές μετατοπίσεις θα χρησιμοποιηθούν για τον υπολογισμό της πραγματικής χρονικής μετατόπισης.

6.8 Επιθέσεις Παράπλευρου Καναλιού στα Ασύρματα Δίκτυα Αισθητήρων

Οι προηγούμενες επιθέσεις είναι ειδικού τύπου επιθέσεις που μπορούν να πλήξουν την ασφάλεια σε ασύρματα δίκτυα αισθητήρων. Οι εν λόγω επιθέσεις, όπως είδαμε, βασίζονται σε συγκεκριμένες ιδιότητες των πρωτοκόλλων και της δομής των ασύρματων δικτύων αισθητήρων. Ωστόσο, όλες οι επιθέσεις παράπλευρου καναλιού (και ιδιαίτερα οι παθητικές επιθέσεις) που περιγράφηκαν αναλυτικά σε προηγούμενο κεφάλαιο μπορούν επίσης να πλήξουν σημαντικά την ασφάλεια των δικτύων αυτών. Και αυτό γιατί οι κόμβοι ενός τέτοιου δικτύου είναι εύκολα προσπελάσιμοι και, ως εκ τούτου, καθίσταται εφικτό να γίνει π.χ. ανάλυση της ενέργειας που καταναλώνεται από αυτούς. Αν συνδυαστεί αυτό με το γεγονός ότι υπάρχουν περιορισμοί στην υπολογιστική ισχύ, στη χωρητικότητα μνήμης και στη μέγιστη δυνατή κατανάλωση για τους κόμβους ενός τέτοιου δικτύου, το ανωτέρω πρόβλημα επιτείνεται.

Γενικότερα, με όρους ασύρματων δικτύων αισθητήρων, τέτοιες επιθέσεις απαντώνται στη βιβλιογραφία και με τον όρο «φυσικές επιθέσεις».

6.8.1 Φυσικές Επιθέσεις.

Το τρέχον υλικό στην υλοποίηση των ασύρματων δικτύων αισθητήρων δεν παρέχει κανενός τύπου αντίσταση στη φυσική αλλοίωση. Εάν ένας επιτιθέμενος αντίπαλος συλλάβει ένα κόμβο, τότε μπορεί αρκετά εύκολα να εξάγει τις κρυπτογραφικές του ιδιότητες. Επίσης είναι σε θέση να συμπεράνει τα αποτελέσματα της υλοποίησης σχεδιασμού (Roosta, Shieh, Sastry 2006: 4).

Στο λεγόμενο "βασίλειο" των ασύρματων δικτύων υπάρχουν δύο κατηγορίες στις οποίες μια φυσική επίθεση μπορεί να διαιρεθεί. Οι κατηγορίες αυτές είναι οι *επιδρομικές* και οι *μη επιδρομικές*.

Οι επιδρομικές είναι ένας τύπος επίθεσης ο οποίος περιλαμβάνει τεχνικές που απαιτούν πρόσβαση στα συστήματα των συσκευών. Τα συστατικά πρόσβασης είναι σε επίπεδο μικροελεγκτή (τσιπ).

Οι μη επιδρομικές επιθέσεις, είναι τεχνικές όπου οι συσκευές είναι ενσωματωμένες και ως εκ τούτου δεν μπορούν να παραβιαστούν, οπότε δεν είναι δυνατόν να αλλοιωθούν. Προφανώς, μία επίθεση αυτού του είδους είναι η επίθεση παράπλευρου καναλιού. Όπου, όπως έχει αναφερθεί, οι επιθέσεις παράπλευρου καναλιού αναφέρονται στις επιθέσεις που βασίζεται σε πληροφορίες που συγκεντρώθηκαν από τη φυσική εφαρμογή ενός κρυπτογραφικού συστήματος, σε αντίθεση με μία ευπάθεια που αναφέρεται στην υλοποίηση του αλγορίθμου.

Προς επίρρωση αυτού μπορεί να ειπωθεί, ότι ένας εισβολέας μπορεί να αναλύσει ορισμένες παραμέτρους όπως την κατανάλωση ενέργειας, το χρονοδιάγραμμα της εκτέλεσης λειτουργίας του λογισμικού ή τη συχνότητα των ήλεκτρο-μαγνητικών κυμάτων (Roosta, Shieh, Sastry 2006: 4).

Και οι δύο τύποι επιθέσεων στοχεύουν απευθείας στην κτήση των κόμβων αισθητήρων. Η επιδρομική επίθεση είναι εφικτή μέσω της φυσικής σύλληψης ενός κόμβου αισθητήρα. Ωστόσο ακόμα δεν υπάρχει διαθέσιμη ανάλυση η οποία να καταστήσει τους κόμβους αυτούς με περισσότερη αντίσταση στις φυσικές αλλοιώσεις. Οι κόμβων αισθητήρων, πρέπει να τονιστεί ότι, στερούνται οποιασδήποτε προστασίας μνήμης βασισμένη στην υλοποίηση μνήμης.

Στα ενσωματωμένα συστήματα, οι κρυπτο-επεξεργαστές, όπως για παράδειγμα οι ασφαλείς επεξεργαστές βασισμένοι στο φυσικό επίπεδο, έχουν χρησιμοποιηθεί για να παράσχουν κάποιου επιπέδου αντίσταση από την φυσική παραβίαση. Ακόμα και αν υπάρχουν γνωστές επιθέσεις σε κρυπτο-επεξεργαστές, αυτοί παρέχουν μια πρώτη γραμμή άμυνας έναντι των φυσικών παραβιάσεων. Ως εκ τούτου υπάρχει ανάγκη να αναπτυχθούν βελτιστοποιημένοι επεξεργαστές οι οποίοι θα ικανοποιούν τις απαιτήσεις για κατασκευή χαμηλού κόστους, χαμηλής ενέργειας απαιτήσεις των δικτύων αισθητήρων.

Οι μη επιδρομικές επιθέσεις όπως αυτή του παράπλευρου καναλιού είναι αρκετά πιθανές στα δίκτυα αισθητήρων. Προς επίρρωση αυτού μπορεί να αναφερθεί κανείς σε μία μελέτη η οποία κατέδειξε ότι οι επιθέσεις παράπλευρου καναλιού στο MAC (Message Authentication Protocol) με τη χρήση ανάλυσης ισχύος ή διαφορικής ανάλυσης ισχύος είναι δυνατή σε δίκτυα αισθητήρων (Okeya, Iwata 2005: 208). Τα αποτελέσματα της μελέτης αυτής κατέδειξαν ότι αρκετά bits κλειδιών μπορούν να εξαχθούν διαμέσου της επίθεσης ανάλυσης ισχύος (Power Analysis).

Κεφάλαιο 7
Πρακτική Εφαρμογή.

7 Εισαγωγή.

Σκοπός του τρέχοντος κεφαλαίου είναι να καταδείξουμε σε ένα ασύρματο δίκτυο αισθητήρων (WSN) μια επίθεση παράπλευρου καναλιού. Κύριο άξονα για την προσέγγιση που θα ακολουθήσουμε αποτελεί το γεγονός ότι στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται για την κρυπτογράφηση των μεταδιδόμενων δεδομένων, όπως ήδη αναφέρθηκε, κρυπταλγόριθμοι ροής (stream ciphers), λόγω του ότι οι αλγόριθμοι αυτοί έχουν καλύτερη απόδοση στην ταχύτητα κρυπτογράφησης / αποκρυπτογράφησης αλλά και χαμηλότερη κατανάλωση ενέργειας. Για το λόγο αυτό, θα αξιοποιήσουμε μία έξυπνη τεχνική επίθεσης παράπλευρου καναλιού που μπορεί να εφαρμοστεί σε οποιονδήποτε κρυπταλγόριθμο ροής βασίζει τη λειτουργία του σε χρήση LFSR (π.χ. σε μη γραμμικό φίλτρο εφαρμοζόμενο σε LFSR). Θα περιγράψουμε επακριβώς τη λογική της επίθεσης αυτής και, ακολούθως, θα γίνει εφαρμογή της σε ένα σύγχρονο κρυπτογραφικό αλγόριθμο που έχει προταθεί πρόσφατα για χρήση σε ασύρματα δίκτυα αισθητήρων. Η επίθεση που θα υλοποιηθεί και περιγράφεται στο τρέχον κεφάλαιο ανήκει στην κατηγορία SPA (Simple Power Analysis) που επεξηγήθηκε στην Ενότητα 4.1.3

7.1 Περιγραφή της Επίθεσης.

Οι αλγόριθμοι κρυπτογράφησης, όπως αναλυτικά εξηγήθηκε στο Κεφάλαιο 2, χρησιμοποιούνται για να προστατεύσουν τις πληροφορίες από μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη και χρησιμοποιούν για την κατασκευή τους ένα κλειδί

κρυπτογράφησης το οποίο χρησιμοποιείται από τους κρυπτογραφικούς αλγόριθμους. Η ανθεκτικότητα της ασφάλειας των κρυπτογραφικών αλγορίθμων έχει παραδοσιακά μετρηθεί κάτω από τρία μαθηματικά μοντέλα, τα οποία ονομαστικά είναι, (Burman, Mukhopadhyay, Veezhinathan 2007: 387).

I. απεριόριστη ασφάλεια: Όταν το σύστημα είναι ασφαλές ακόμα και υπό την υπόθεση ότι ο επιτιθέμενος διαθέτει απεριόριστη υπολογιστική ισχύ

II. ευαπόδεικτη ασφάλεια: Όταν μπορεί να αποδειχτεί ότι εάν ένας επιτιθέμενος έχει επιτυχώς «σπάσει» (κρυπταναλύσει) τον κρυπτογραφικό αλγόριθμο με μία επίθεση, τότε θα μπορεί να επιλύσει ένα γνωστό δύσκολο μαθηματικό πρόβλημα για το οποίο εικάζεται ότι είναι αρκετά δύσκολο να επιλυθεί

III. υπολογιστική ασφάλεια: Όταν η προσπάθεια η οποία απαιτείται για να «σπάσει» (κρυπταναλυθεί) ένας κρυπτογραφικός αλγόριθμος είναι τόσο μεγάλη, ώστε ο κρυπτογραφικός αλγόριθμος να μπορεί να θεωρηθεί πρακτικά ως απαραβίαστος.

Τα ανωτέρω μοντέλα ασφάλειας αναφέρονται σε τεχνικές κρυπτανάλυσης, δηλαδή σε τεχνικές που προσπαθούν να εκμεταλλευτούν κάποιες μαθηματικές ιδιότητες του αλγορίθμου για να υπάρξει παραβίασή του. Για παράδειγμα, η επίθεση συσχέτισης που περιγράφηκε ενδεικτικά στο Κεφάλαιο 3 είναι μία τεχνική κρυπτανάλυσης, και για τη γεννήτρια Geffe που εφαρμόστηκε προκύπτει ότι η συγκεκριμένη γεννήτρια δεν παρέχει υπολογιστική ασφάλεια (άρα και καμία άλλη ασφάλεια). Από την άλλη πλευρά, το σημειωματάριο μιας χρήσης (one-time pad), που επίσης παρουσιάστηκε στο Κεφάλαιο 3, έχει αποδειχθεί ότι παρέχει απεριόριστη ασφάλεια (αλλά δεν μπορεί πρακτικά να υλοποιηθεί).

Ωστόσο, όπως ήδη αναφέρθηκε στην παρούσα διατριβή, οι επιθέσεις παράπλευρου καναλιού έχουν τελείως διαφορετική φιλοσοφία, με αποτέλεσμα η ασφάλεια ενός κρυπτογραφικού αλγορίθμου έναντι αυτών να μην εντάσσεται στις ανωτέρω κατηγορίες. Στο άρθρο των (Burman, Mukhopadhyay, Veezhinathan 2007: 387), αποδείχθηκε ότι αν μετρηθεί η κατανάλωση ενέργειας μεταξύ διαδοχικών καταστάσεων ενός LFSR είναι δυνατόν να οδηγηθούμε στην ανακάλυψη του μυστικού κλειδιού (για πολλές τέτοιες μετρήσεις). Ο επιτιθέμενος σε αυτήν την περίπτωση εκμεταλλεύεται, για

να επιτεθεί στον αλγόριθμο κρυπτογράφησης, τις πληροφορίες που διέρρευσαν κατά λάθος στο περιβάλλον από το σύστημα το οποίο εκτελεί τον κρυπτογραφικό αλγόριθμο, γεγονός που συχνά οδηγεί σε καταστροφική αποτυχία της ασφάλειας. Αυτό είναι εφικτό, ακόμη και σε ένα σύστημα του οποίου η θεωρητική ανθεκτικότητα έναντι επιθέσεων κρυπτανάλυσης εντάσσεται σε κάποιο από τα μαθηματικά μοντέλα που αναφέρθηκαν πιο πάνω.

Η δυναμική ενέργεια που καταναλώνεται από ένα ψηφιακό κύκλωμα είναι ευθέως ανάλογη προς τη δραστηριότητα μεταγωγής (switching activity). δηλαδή με τον αριθμό των βαθμίδων στο κύκλωμα που έχουν μια μετάβαση κατάστασης από μηδέν σε ένα ή αντίστροφα. Στην περίπτωση των LFSR, η δυναμική ενέργεια που καταναλώνεται κατά τη διάρκεια της μετάβασης από τη χρονική στιγμή t στη χρονική στιγμή *t+1* είναι ανάλογη με HD_t, όπου το HD_t είναι η απόσταση Hamming μεταξύ των n-bit διανυσμάτων ST_t και ST_{t+1} (δηλαδή το βάρος Hamming (HW) του διανύσματος $ST_t \oplus ST_{t+1}$) και ST_i είναι η κατάσταση του LFSR τη χρονική στιγμή i. Αν s(0), s(1), ..., s(n-1) είναι η αρχική κατάσταση του LFSR, τότε τα ανωτέρω βάρη Hamming, δίνονται από τα ακόλουθα (Burman, Mukhopadhyay, Veezhinathan 2007: 387).

$$HD_0 = HW((S(n) \oplus S(n-1)), (S(n-1) \oplus S(n-2)), \cdots, (S(1) \oplus S(0))) \quad (1)$$

$$HD_1 = HW((S(n+1) \oplus S(n)), (S(n) \oplus S(n-1)), \cdots, (S(2) \oplus S(1))) \quad (2)$$

και, γενικότερα,

$$HD_t = HW((S(n+t) \oplus S(n+t\text{-}1)), (S(n+t\text{-}1) \oplus S(n+t-2)), \cdots, (S(t+1) \oplus S(t))) \quad (3)$$

Αυτό αποτελεί την υπολογιζόμενη απόσταση Hamming και είναι ένα μέτρο του συνολικού αριθμού των εντολών της κατάστασης του LFSR κατά τη διάρκεια του χρονικού διαστήματος *t* έως *t+1*. Αυτό σημαίνει ότι η διαφορά στην ισχύ που καταναλώνεται από τον LFSR μεταξύ του κύκλου *t* και κύκλου *t+1* είναι ανάλογη προς το PD_t.

Από τις εξισώσεις (1) και (2), όπως γενικεύονται μέσω της (3), έχουμε:

$$\begin{aligned} PD_t &= HD_t - HD_{t+1} \\ &= HW((S(t) \oplus S(t+1)) - HW((S(n+t+1) \oplus S(n+t))) \\ &= \{0, 1\} - \{0, 1\} \\ &= \{-1, 0, 1\} \end{aligned}$$

Δηλαδή, η ποσότητα PD_t μπορεί να πάρει τρεις μόνο πιθανές τιμές: -1, 0 και 1.

Ας γίνει η υπόθεση ότι το PD'_t, καθορίζεται ως ακολούθως: είναι μηδέν όταν $HD_t = HD_{t+1}$, ενώ είναι ένα όταν $HD_t \neq HD_{t+1}$.

Δοθέντος ενός συνόλου $S(n+t+1)$, $S(n+t)$, $S(t+1)$ και $S(t)$ τότε αποδεικνύεται εύκολα (η απόδειξη υπάρχει στο ανωτέρω άρθρο) ότι:

$PD't = S(n + t+ 1) \oplus S(n+t) \oplus S(t+1) \oplus S(t)$.

Από το παραπάνω προκύπτει:

$$S_{(n+1)} \oplus S_{(n)} \oplus S_{(1)} \oplus S_{(0)} = PD'_0 \quad (4)$$

$$S_{(n+2)} \oplus S_{(n+1)} \oplus S_{(2)} \oplus S_{(1)} = PD'_1 \quad (5)$$

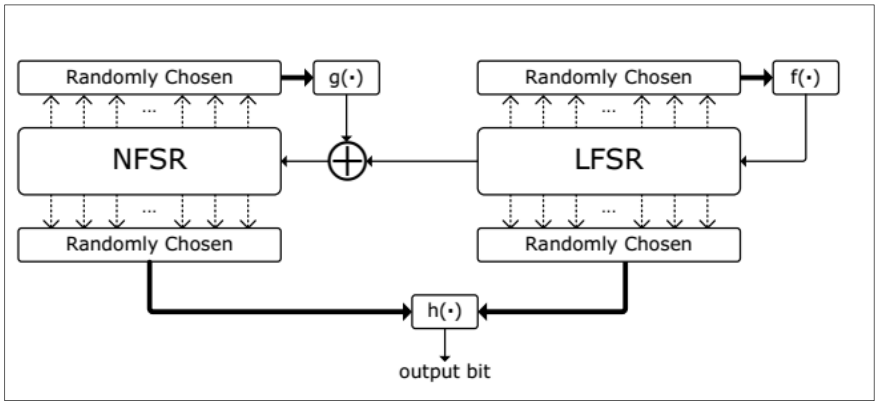
και ούτω καθ' εξής.

Εάν ο αριθμός των εναλλαγών τιμών σε μια κατάσταση ενός LFSR σε ένα κύκλο t είναι διαφορετικός από εκείνον του κύκλου $t+1$, με άλλα λόγια $HD_t \neq HD_{t+1}$, τότε η ισχύς που καταναλώνεται από τον LFSR στους δύο κύκλους είναι επίσης διαφορετική: σε διαφορετική περίπτωση θα είναι η ίδια. Ως εκ τούτου, με τη μέτρηση της κατανάλωσης ισχύος σε κάθε κύκλο, η τιμή της PD'_t, μπορεί να υπολογιστεί. Εφόσον είμαστε σε θέση να μετρήσουμε τα PD'_t θα μπορέσουμε να λύσουμε ένα γραμμικό σύστημα της μορφής των

εξισώσεων (4)-(5). Η κρίσιμη παρατήρηση εδώ είναι ότι, το αριστερό μέλος κάθε εξίσωσης, μπορεί να γραφεί ως γραμμική συνάρτηση μόνο των S(0),S(1),…,S(n-1), δηλαδή ως συνάρτηση της αρχικής κατάστασης του LFSR (που, πρακτικά, ισοδυναμεί με το μυστικό κλειδί): και αυτό γιατί κάθε στοιχείο S(t) της ακολουθίας γράφεται ως άθροισμα κάποιων εκ των n προηγούμενων στοιχείων (βλ. Κεφ. 3), οπότε αναδρομικά μπορεί εύκολα να δει κανείς ότι γράφεται ως άθροισμα των πρώτων n στοιχείων της ακολουθίας. Άρα, με μετρήσεις κατανάλωσης ενέργειας μπορούμε να κατασκευάσουμε ένα γραμμικό σύστημα εξισώσεων με αγνώστους μόνο την αρχική κατάσταση του LFSR – το οποίο μπορεί να επιλυθεί.

7.2 Περιγραφή του Αλγορίθμου.

Σε πρόσφατο άρθρο (Zeng, 2013: 559-562) προτάθηκε ένας νέος κρυπταλγόριθμος ροής για χρήση του σε ασύρματα δίκτυα αισθητήρων. Ο προτεινόμενος αλγόριθμος επιλέχθηκε με γνώμονα τη χαμηλή υπολογιστική πολυπλοκότητα και ενεργειακή απόδοση ενός αναπροσαρμόσιμου καταχωρητή (κρυπτογράφησης ροής) ολίσθησης με ανάδραση (RFSR). Ο προτεινόμενος αλγόριθμος κρυπτογράφησης, αποτελείται από τρία βασικά δομικά στοιχεία: ένα γραμμικό καταχωριστή ολίσθησης με ανάδραση (LFSR) με γραμμική συνάρτηση ανάδρασης *f,* έναν μη γραμμικό καταχωρητή (NFSR) με μη γραμμική συνάρτηση ανάδρασης *g* και μια συνάρτηση εξόδου *h*. Οι θέσεις μνήμης του LFSR συμβολίζονται ως: $y_1, y_2, y_3, y_4, y_5, \ldots, y_{32}$, ενώ οι θέσεις μνήμης του NFSR ως: $z_1, z_2, z_3, z_4, z_5, \ldots, z_{32}$. Η βασική καινοτομία των σχεδιαστών του αλγορίθμου ήταν ότι οι συναρτήσεις ανάδρασης f και g μπορούν να αλλάζουν δυναμικά (αναπροσαρμόζονται) ενώ ο αλγόριθμος είναι σε εξέλιξη. Η αναπροσαρμόσιμη γραμμική συνάρτηση εξόδου για τον LFSR είναι η: $f: y_0=y_{\alpha 1}+y_{\alpha 2}+y_{\alpha 3}+y_{\alpha 4}+y_{\alpha 5}+y_3$, όπου τα a_1 έως a_5 επιλέγονται προσεκτικά, έτσι ώστε η f να είναι ένα πρωταρχικό πολυώνυμο βαθμού τριάντα δύο (32).



Εικόνα 35 Δομή του αλγορίθμου.

Το πρωταρχικό πολυώνυμο, όπως αναλύθηκε και στο Κεφάλαιο 3, εγγυάται ότι οι εσωτερικές καταστάσεις του LFSR θα οδηγήσουν στην παραγωγή ακολουθίας με τη μέγιστη περίοδο 2^n-1, όπου $n=32$ είναι το μέγεθος του LFSR. Οι σχεδιαστές του αλγορίθμου αναφέρουν ότι, για την επιλογή του *f*, υπάρχει ένα σύνολο 5.039 πρωταρχικών πολυώνυμων βαθμού 32, τα οποία αποτελούν μια «δεξαμενή» για να επιλέξει κανείς. Προφανώς, η εναλλαγή της συνάρτησης ανάδρασης θα εξαρτάται με κάποιον τρόπο από το κλειδί. (Zeng 2013: 560).

7.3 Κρυπτανάλυση Αλγορίθμου.

Στο σημείο αυτό θα γίνει εφαρμογή της τεχνικής που επεξηγήθηκε στην παράγραφο 7.1 στον αλγόριθμο που αναλύθηκε στην παράγραφο 7.2. Για να επιτευχθεί αυτό κάνουμε τις εξής υποθέσεις:

α) Η γραμμική συνάρτηση ανάδρασης *f*, η οποία είναι δυναμικά μεταβαλλόμενη, μένει σταθερή για 32 περιόδους του ρολογιού (οι σχεδιαστές του αλγορίθμου δεν προσδιορίζουν το ρυθμό μεταβολής της συνάρτησης ανάδρασης, ενώ περαιτέρω σημειώνεται ότι το 32 είναι πολύ μικρότερο από το 2^{32} -1 που είναι η συνολική περίοδος),

β) Είμαστε σε θέση να μετρήσουμε την κατανάλωση ενέργειας ειδικά στον LFSR.

Για λόγους προσομοίωσης του πειράματος, μιας και δεν έχουμε τη δυνατότητα να κάνουμε προσομοίωση σε hardware ώστε να μετρήσουμε την κατανάλωση ενέργειας, έγινε ανάπτυξη κατάλληλου λογισμικού που να εκτελεί τις λειτουργίες του συγκεκριμένου LFSR και υπολογίσαμε τα PD΄ με βάση τις μαθηματικές εξισώσεις που τα διέπουν. Όπως αναφέρθηκε ήδη, για του υπολογισμό του PD_t' γίνεται ο έλεγχος μεταξύ των αποστάσεων Hamming, εάν η απόσταση Hamming μεταξύ των καταστάσεων *t* και *t+1* είναι ίδια τότε το αποτέλεσμα είναι μηδέν (0) διαφορετικά το αποτέλεσμα είναι ένα (1).

X1	X2	X3	X4	X5	X6	X7	X8	X9	Έξοδος	HD	PD΄
0	0	0	0	0	0	1	1	1	1		
1	0	0	0	0	0	0	1	1	1	2	
1	1	0	0	0	0	0	0	1	1	2	0
1	1	1	0	0	0	0	0	0	0	2	0
0	1	1	1	0	0	0	0	0	0	2	0
0	0	1	1	1	0	0	0	0	0	2	0
1	0	0	1	1	1	0	0	0	0	3	1
1	1	0	0	1	1	1	0	0	0	3	0
1	1	1	0	0	1	1	1	0	0	3	0
0	1	1	1	0	0	1	1	1	1	4	1
1	0	1	1	1	0	0	1	1	1	4	0

Πίνακας 1. Παράδειγμα LFSR εννέα βαθμίδων.

Στο πιο πάνω παράδειγμα εμφανίζεται ένας πίνακας ενός LFSR εννέα (9) βαθμίδων όπου στην ανάδρασή του υπεισέρχονται οι βαθμίδες X_5, X_9. Στον πίνακα παρατηρούνται οι ολισθήσεις που έχουν συμβεί στον LFSR καθώς και οι έξοδος του LFSR . Επιπρόσθετα απεικονίζεται και η απόσταση Hamming (HD) κάθε κατάστασης με την επόμενή της, όπως επίσης και το αντίστοιχο PD'. Μπορούμε επίσης να ανακαλέσουμε ότι η απόσταση Hamming ορίζεται ως το πλήθος θέσεων στις οποίες οι αντίστοιχοι χαρακτήρες/αριθμοί είναι διαφορετικοί.

Για τον αλγόριθμο που εξετάζουμε, λόγω της ανωτέρω υπόθεσης (α) μπορούμε να θεωρήσουμε οποιαδήποτε συγκεκριμένη συνάρτηση ανάδρασης *f* (προφανώς, η διαδικασία που θα ακολουθήσουμε για μία τέτοια συνάρτηση μπορεί να επαναληφθεί για

κάθε μία, εκ του συνόλου των 5.039 πιθανών, άλλων συναρτήσεων). Ο LFSR που επιλέχτηκε για την πειραματική διαδικασία είχε ανάδραση που περιγράφεται από την εξίσωση: *y_{32}=y_{0}+y_{1}+y_{2}+y_{3}+y_{5}+y_{7},* όπου το *y_{0}* είναι το δεξιότερο *bit*. Η συνάρτηση αυτή υπάγεται σε αυτές που περιγράφουν οι σχεδιαστές του αλγορίθμου. Επίσης η αρχική κατάσταση του *LFSR* που επιλέχθηκε ήταν η: *LFSR={1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}*, όπου η θέση μηδέν (0) είναι το δεξιότερο bit. Στόχος της επίθεσης είναι η ανακάλυψη αυτής της αρχικής κατάστασης, μετρώντας απλά καταναλώσεις ενέργειας του LFSR.

7.3.1 Γραμμικές Εξισώσεις.

Έχοντας κατά νου της σχέσεις (3) και (4) που αναφέρθηκαν πιο πάνω όπως επίσης ότι η ανάδραση του LFSR είναι η: *S_{32}=S_{0}+S_{1}+S_{2}+S_{3}+S_{5}+S_{7},* δημιουργήθηκε ένα γραμμικό σύστημα εξισώσεων τριάντα δύο αγνώστων, αντικαθιστώντας όπου *S_{32}=S_{0}+S_{1}+S_{2}+S_{3}+S_{5}+S_{7}*.

Ενδεικτικά παρατίθεται η επίλυση της πρώτης εξίσωσης PD'_0

$PD'_0=S_0+S_1+S_n+S_{(n+1)}$, *όπου n=32 και* $S_{(32)}=S_0+S_1+S_2+S_3+S_5+S_7$, *άρα*

Για n=32

$PD'_0=S_0+S_1+S_{32}+S_{(32+1)}$

$PD'_0=S_0+S_1+[S_0+S_1+S_2+S_3+S_5+S_7]+[S_{0+1}+S_{1+1}+S_{2+1}+S_{3+1}+S_{5+1}+S_{7+1}]$

$PD'_0=S_0+S_1+[S_0+S_1+S_2+S_3+S_5+S_7]+[S_1+S_2+S_3+S_4+S_6+S_8]$

$PD'_0=S_0+S_1+S_0+S_1+S_2+S_3+S_5+S_7+S_1+S_2+S_3+S_4+S_6+S_8$

(Διαγραφή όμοιων ανά ζεύγη στοιχείων)

$\boldsymbol{PD'_0=S_1+S_4+S_5+S_6+S_7+S_8}$	Όπου {+} η πράξη XOR.

Με γνώμονα την πιο πάνω διαδικασία οι εξισώσεις που δημιουργήθηκαν ήταν οι:

$PD'_0 = S_1 + S_4 + S_5 + S_6 + S_7 + S_8$

$PD'_1 = S_2 + S_5 + S_6 + S_7 + S_8 + S_9$

$PD'_2 = S_3 + S_6 + S_7 + S_8 + S_9 + S_{10}$

$PD'_3 = S_4 + S_7 + S_8 + S_9 + S_{10} + S_{11}$

$PD'_4 = S_5 + S_8 + S_9 + S_{10} + S_{11} + S_{12}$

$PD'_5 = S_6 + S_9 + S_{10} + S_{11} + S_{12} + S_{13}$

$PD'_6 = S_7 + S_{10} + S_{11} + S_{12} + S_{13} + S_{14}$

$PD'_7 = S_8 + S_{11} + S_{12} + S_{13} + S_{14} + S_{15}$

$PD'_8 = S_9 + S_{12} + S_{13} + S_{14} + S_{15} + S_{16}$

$PD'_9 = S_{10} + S_{13} + S_{14} + S_{15} + S_{16} + S_{17}$

$PD'_{10} = S_{11} + S_{14} + S_{15} + S_{16} + S_{17} + S_{18}$

$PD'_{11} = S_{12} + S_{15} + S_6 + S_{17} + S_{18} + S_{19}$

$PD'_{12} = S_{13} + S_{16} + S_{17} + S_{18} + S_{19} + S_{20}$

$PD'_{13} = S_{14} + S_{17} + S_{18} + S_{19} + S_{20} + S_{21}$

$PD'_{14} = S_{15} + S_{18} + S_{19} + S_{20} + S_{21} + S_{22}$

$PD'_{15} = S_{16} + S_{19} + S_{20} + S_{21} + S_{22} + S_{23}$

$PD'_{16} = S_{17} + S_{20} + S_{21} + S_{22} + S_{23} + S_{24}$

$PD'_{17} = S_{18} + S_{21} + S_{22} + S_{23} + S_{24} + S_{25}$

$PD'_{18} = S_{19} + S_{22} + S_{23} + S_{24} + S_{25} + S_{26}$

$PD'_{19} = S_{20} + S_{23} + S_{24} + S_{25} + S_{26} + S_{27}$

$PD'_{20} = S_{21} + S_{24} + S_{25} + S_{26} + S_{27} + S_{28}$

$PD'_{21} = S_{22} + S_{25} + S_{26} + S_{27} + S_{28} + S_{29}$

$PD'_{22} = S_{23} + S_{26} + S_{27} + S_{28} + S_{29.} + S_{30}$

$PD'_{23} = S_{24} + S_{27} + S_{28} + S_{29.} + S_{30} + S_{31}$

$PD'_{24} = S_0 + S_1 + S_2 + S_{3.} + S_5 + S_7 + S_{25} + S_{28} + S_{29} + S_{30.} + S_{31}$

$PD'_{25} = S_0 + S_4 + S_5 + S_6 + S_7 + S_8 + S_{26} + S_{29} + S_{30} + S_{31}$

$PD'_{26} = S_0 + S_2 + S_3 + S_6 + S_8 + S_9 + S_{27} + S_{30} + S_{31.}$

$PD'_{27} = S_0 + S_2 + S_4 + S_5 + S_9 + S_{10} + S_{28} + S_{31}$

$PD'_{28} = S_{29} + S_0 + S_2 + S_{10} + S_{11}$

$PD'_{29} = S_{30} + S_3 + S_7 + S_8 + S_{11} + S_{12}$

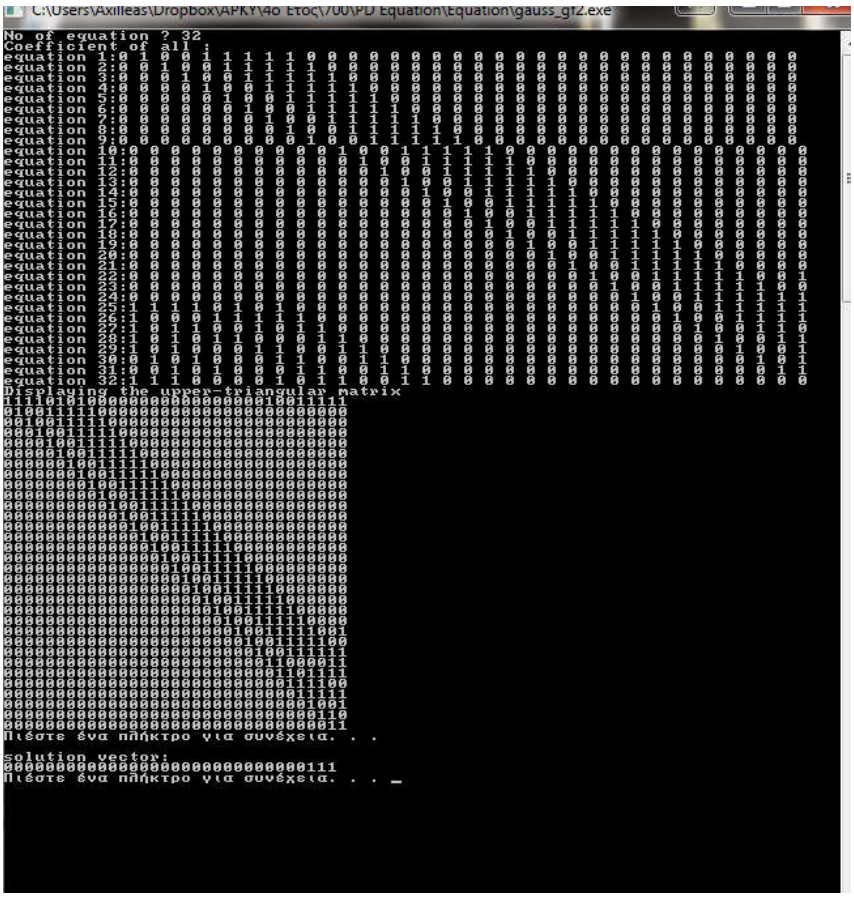
$PD'_{30} = S_{31} + S_2 + S_4 + S_8 + S_9 + S_{12} + S_{13}$

$PD'_{31} = S_{31} + S_0 + S_1 + S_{2.} + S_6 + S_7 + S_9 + S_{10} + S_{13} + S_{14.}$

Όπου {+} η πράξη XOR.

Μιας και το κλειδί είναι μεγέθους 32 χρειαζόμαστε 32 εξισώσεις, οπότε ο επιτιθέμενος χρειάζεται να κάνει 32 μετρήσεις και, συνεπώς, θα έχει στην κατοχή του 32 PD'. Σημειώνεται ότι οι ανωτέρω εξισώσεις αντιστοιχούν στη συγκεκριμένη *f* που επιλέξαμε: για κάθε άλλη *f* κατασκευάζουμε αντίστοιχα ένα άλλο σύστημα εξισώσεων. Για τις διάφορες τιμές PD', χρησιμοποιήσαμε την εφαρμογή που αναπτύξαμε για σκοπούς προσομοίωσης της λειτουργίας του LFSR (βλ. Παράρτημα Α.1).

Για να επιλύσουμε τις εξισώσεις αναπτύξαμε ένα αλγόριθμο επίλυσης του γραμμικού συστήματος με την μέθοδο απαλοιφής του Gauss (Gauss elimination). Οι πράξεις οι οποίες εκτελούνται στον αλγόριθμο που αναπτύχτηκε είναι στο πεπερασμένο σώμα $F_2=\{0,1\}$ (δηλαδή 1+1=0 κ.ο.κ.), και όχι στους πραγματικούς αριθμούς το οποίο είναι η συνήθης περίπτωση όπου χρησιμοποιείται η μέθοδος απαλοιφής Gauss. Για να επιτευχθεί αυτό, ο αλγόριθμος που αναπτύχθηκε αποτελεί τροποποίηση της κλασικής μεθόδου απαλοιφής του Gauss, έτσι ώστε να μπορεί να εκτελέσει πράξεις στο σώμα {0,1}.



Εικόνα 36 Λειτουργία Αλγόριθμου Gauss.

Από την επίλυση του γραμμικού συστήματος, μέσω της εφαρμογής που αναπτύχθηκε (βλ. Παράρτημα Α.2)_παρατηρήθηκε ότι είμαστε σε θέση να υπολογίσουμε το μυστικό κλειδί μιας και το αποτέλεσμα το οποία εξάχθηκε ήταν όμοιο με την αρχική κατάσταση του LFSR που επιλέχθηκε, *{1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}.*

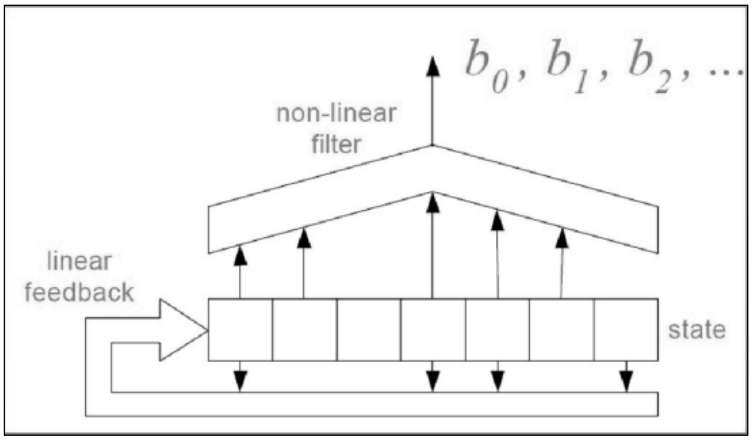
Εικόνα 37 Αποτέλεσμα Αλγόριθμου.

Άρα, καταφέραμε πράγματι, με τις υποθέσεις α) και β) ανωτέρω, να προσδιορίσουμε την αρχική κατάσταση του LFSR απλά μετρώντας την κατανάλωση ενέργειας αυτού.

7.4 Αντιμετώπιση της Επίθεσης

Οι σχεδιαστές του εν λόγω αλγορίθμου δεν περιλαμβάνουν στην ανάλυσή τους καμία περιγραφή για αντιμετώπιση επιθέσεων παράπλευρου καναλιού. Προφανώς, η επίθεση που περιγράφηκε και καταδείξαμε θα μπορεί να αντιμετωπιστεί εάν η συνάρτηση ανάδρασης του LFSR μεταβάλλεται πάρα πολύ συχνά - κάτι που θα πρέπει να τεθεί ως απαραίτητη σχεδιαστική παράμετρος του αλγορίθμου. Σε κάθε περίπτωση, το γεγονός ότι ο αλγόριθμος δεν βασίζεται μόνο στον LFSR αλλά και σε NLFR δυσχεραίνει πράγματι την πραγματοποίηση της επίθεσης, ακριβώς γιατί η μέτρηση της κατανάλωσης ενέργειας μόνο του LFSR πιθανώς να μην είναι πρακτικά εφικτή: παρόλα αυτά, είναι «επικίνδυνο» να επαφίεται η ασφάλεια μόνο στο ότι πιθανότατα δεν θα μπορέσει ο υποκλοπέας να μετρήσει τις καταναλώσεις ενέργειας του LFSR, και θα πρέπει ο αλγόριθμος να είναι ανθεκτικός σε κάθε περίπτωση έναντι αυτών των επιθέσεων. Εξάλλου, προς επίρρωση των ανωτέρω, σημειώνουμε ότι υπάρχουν και άλλοι κρυπταλγόριθμοι ροής οι οποίοι δεν κάνουν χρήση NLFSR και, ως εκ τούτου, είναι πιο άμεσα επιρρεπείς στην εν λόγω επίθεση

(π.χ. αλγόριθμος Toyocrypt, ο οποίος ωστόσο έχει ούτως ή άλλως υποστεί επιτυχή μαθηματική κρυπτανάλυση αλγεβρικών επιθέσεων).



Εικόνα 38 Γενική μορφή του αλγόριθμου Toyocrypt, που είναι προφανώς επιρρεπής στην επίθεση παράπλευρου καναλιού που περιγράφηκε.

Για τη γενική και συνολική αντιμετώπιση της επίθεσης που υλοποιήθηκε προτείνεται η κατάλληλη τροποποίηση της δομής του LFSR ώστε κατά την μετάβαση των καταστάσεων να μην αποκαλύπτεται κάποια πληροφορία. Μία τέτοια υλοποίηση περιγράφεται από τους εμπνευστές αυτής της επίθεσης (Burman, Mukhopadhyay, Veezhinathan 2007: 387). Αυτό πρέπει να λαμβάνεται υπόψη κατά την υλοποίηση ενός κρυπταλγορίθμου ροής που χρησιμοποιεί LFSR και είναι μια παράμερος την οποία οι εμπνευστές του αλγορίθμου που περιγράφηκε ανωτέρω δεν την αναφέρουν στο άρθρο τους.

Κεφάλαιο 8
Επίλογος.

8 Σύνοψη.

Η παρούσα μεταπτυχιακή διατριβή πραγματεύτηκε θέματα που άπτονται της ειδικής κατηγορίας επιθέσεων ασφάλειας που περιγράφονται με τον όρο κρυπτογραφικές επιθέσεις παράπλευρου καναλιού, εστιασμένες ιδίως στον τομέα της ασφάλειας των ασύρματων δικτύων αισθητήρων. Ειδικότερα έγινε ανάλυση και περιγραφή της βασικής ορολογίας ασφάλειας που απαντάται στα εγχειρίδια ασφάλειας, ενώ επίσης μελετήθηκαν επιθέσεις που κάνουν χρήση των παθογενειών των ιδιοτήτων των φυσικών μέσων μετάδοσης αλλά και των συναφών συσκευών (παράπλευρες επιθέσεις), όπως και άλλες επιθέσεις που επικεντρώνονται στα ασύρματα δίκτυα αισθητήρων. Πραγματοποιήθηκε εκτενής περιγραφή των τύπων των επιθέσεων παράπλευρου καναλιού, με τεκμηρίωση της ιδιαίτερης βαρύτητάς τους ως προς την ασφάλεια των ασύρματων δικτύων αισθητήρων. Στο πλαίσιο αυτό, αναφέρθηκαν τα βασικότερα είδη δικτύων αισθητήρων και παρατέθηκαν τόσο τα πλεονεκτήματά τους όσο και τα χαρακτηριστικά τους.

Επιπλέον, δεδομένου ότι στα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται κυρίως, για την κρυπτογράφηση της μεταδιδόμενης πληροφορίας, κρυπταλγόριθμοι ροής, έγινε μια περιγραφή των εν λόγω τεχνικών κρυπτογράφησης και των σχεδιαστικών τους παραμέτρους. Η επιλογή των αλγορίθμων αυτών για τα εν λόγω δίκτυα γίνεται με γνώμονα τα ποιοτικά τους χαρακτηριστικά μιας και έχουν καλύτερη απόδοση στην ταχύτατα κρυπτογράφησης αλλά και χαμηλότερη κατανάλωση ενέργειας.

Τέλος έγινε προσπάθεια να πραγματοποιηθεί μια προσομοίωση επίθεσης παράπλευρου καναλιού σε ένα ασύρματο δίκτυο αισθητήρων (WSN) με εφαρμογή μίας γνωστής τέτοιας επίθεσης σε ένα σύγχρονο κρυπτογραφικό αλγόριθμο ροής που έχει προταθεί για χρήση σε ασύρματα δίκτυα αισθητήρων. Για να επιτευχθεί αυτό έγινε η υπόθεση ότι

είμαστε σε θέση να μετρήσουμε την κατανάλωση ενέργειας του LFSR που υπεισέρχεται στη λειτουργία του κρυπτογραφικού αλγορίθμου: για λόγους προσομοίωσης του πειράματος, αναπτύχθηκε εφαρμογή που υλοποιεί τη λειτουργία του συγκεκριμένου LFSR, ενώ αντίστοιχα, για την περαιτέρω ανακάλυψη του μυστικού κλειδιού, αναπτύχθηκε εφαρμογή που επιλύει ένα κατάλληλα κατασκευασμένο γραμμικό σύστημα εξισώσεων στο πεπερασμένο σώμα $F_2=\{0,1\}$.

Από την πειραματική διαδικασία η οποία διενεργήθηκε με την χρήση κώδικα προσομοίωσης αποδείχτηκε ότι είναι εύκολο να ανευρεθεί το μυστικό κλειδί που χρησιμοποιήθηκε κατά την κρυπτογράφηση. Για να αντιμετωπιστεί η παθογένεια αυτή προτείνεται να γίνει η τροποποίηση της δομής του LFSR ώστε κατά την μετάβαση των καταστάσεων να μην αποκαλύπτει κάποια πληροφορία περί των πλήθος bits της κατάστασής του που αλλάζουν τιμή.

8.1 Συμπεράσματα – Μελλοντική Έρευνα.

Η μελέτη που πραγματοποιήθηκε στο πλαίσιο της παρούσας διατριβής οδηγεί στο συμπέρασμα ότι οι κρυπτογραφικές επιθέσεις παράπλευρου καναλιού μπορούν να γίνουν ιδιαίτερα επικίνδυνες. Ο κίνδυνος αυτός επιτείνεται από το γεγονός ότι οι σχεδιαστές των κρυπτογραφικών αλγορίθμων δεν δείχνουν πάντα ότι τις λαμβάνουν υπόψη τους, καθώς επικεντρώνονται στην αντιμετώπιση μόνο των αμιγώς μαθηματικών επιθέσεων κρυπτανάλυσης. Το πρόβλημα γίνεται περισσότερο εμφανές σε ασύρματα δίκτυα αισθητήρων, όπου αφενός δεν υπάρχει η «απόλυτη ελευθερία» στην επιλογή του κρυπτογραφικού αλγορίθμου που θα υιοθετηθεί, και αφετέρου είναι εύκολο για τον επιτιθέμενο να αποκτήσει φυσική πρόσβαση στους κόμβους του δικτύου. Άρα, ειδικά για αυτά τα δίκτυα, πρέπει οπωσδήποτε να λαμβάνονται υπόψη εκείνα τα σχεδιαστικά κριτήρια που καθιστούν τους αλγορίθμους ανθεκτικούς και σε αυτές τις επιθέσεις.

Ως μελλοντική έρευνα, υπάρχουν ακόμα πολλά ανοιχτά θέματα που χρήζουν διερεύνησης. Ενδεικτικά αναφέρουμε, σε άμεση συνάφεια με τα όσα αναλύθηκαν στην παρούσα διατριβή, ότι θα πρέπει να μελετηθεί ενδελεχώς τυχόν επίθεση παράπλευρου καναλιού που θα εκμεταλλεύεται διαρροή πληροφορίας από την εναλλαγή καταστάσεων

ενός NLFSR (αντί για LFSR), μια που οι NLFSR δείχνουν ότι αρχίζουν να αποτελούν κύρια σχεδιαστική επιλογή σε κρυπταλγορίθμους ροής. Αυτό το εγχείρημα έχει σαφώς μεγαλύτερο βαθμό δυσκολίας, δεδομένου ότι η μη γραμμικότητα των NLFSR δεν επιτρέπει την άμεση κατασκευή συστήματος γραμμικών εξισώσεων: ωστόσο, ενδεχομένως να μπορούν να εφαρμοστούν συνδυαστικά με άλλες επιθέσεις κρυπτανάλυσης που εστιάζουν στην επίλυση μη γραμμικών συστημάτων.

Βιβλιογραφία

9 Βιβλιογραφία.

Akyildiz I.F., Pompili D., Melodia T. (2004) «Challenges for Efficient Communication in Underwater Acoustic Sensor Networks». ACM Sigbed, Special issue on embedded sensor networks and wireless computing, Vol 1, Issue 2, pp 3-8.

Akyildiz I.F., Stuntebeck E.P. (2006) «Wireless Underground Sensor Network: Research Challenges». Elsevier, Ad-Hoc Networks, Vol 4, Issue 6, pp 669–686.

Alioto M., Giancane L., Scotti G., Trifiletti A. (2010) «Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits». IEEE, Transactions on Circuits and Systems, Regular Papers Col 57, No 2, pp 355-367.

Alzaid H. et al, (2013) «Reputation-Based Trust Systems for WSNs: A Comprehensive Review». Springer, IFIP International Federation for Information Processing, Vol 401, pp. 66–82.

Angel M., Tang S. Y., Qian Y. (2008) «Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring». Technical Report TR-NCIG-0501, University of Puerto Rico at Mayagüez, pp 7-12.

Backes M. et al, (2012) «Acoustic Side-Channel Attacks on Printers». Saarland University, Computer Science Department, Saarbrücken, USENIX Security Symposium pp 307-322.

Bar–El Hagai. (2011) «Introduction to side Chanel Attacks». Discretix, White paper, Netanya, Israel, pp 1-12.

Barrenetxea G., Ingelrest F., Schaefer G., Vetterli M. (2008) «Wireless Sensor Networks for Environmental Monitoring: The SensorScope Experience». IEEE, Communications, 2008 IEEE International Zurich Seminar, pp 98-101.

Batina L., Mentens N., Verbauwhede I. (2005) «Side-Channel Issues for Designing Secure Hardware Implementations». Proceedings of 11th IEEE International On-Line Testing Symposium, Washington, DC, USA, pp. 118–121.

Burman S., Mukhopadhyay D., Veezhinathan K. (2007) «LFSR Based Stream Ciphers Are Vulnerable to Power Attacks», Springer, Indocrypt 2007, Lecture Notes in Computer Science, Vol 4859, pp. 384–392.

Carlet C., Goubin L., Prouff E., Quisquarter M., Rivain M., (2012) «Higher- Order Masking Schemes for S-boxes». Springer, Lecture Notes in Computer Science, Vol 7549, pp. 366—384.

Chen Y., Cheng L., Chen C., Ma J. (2009) «Wireless Sensor Network for Data Sensing in Intelligent Transportation System». IEEE, 69th Vehicular Technology Conference, E-ISDN: 978-1-4244-2517-4, pp: 1-5.

Corke P., Wark T., Jurdak R., Hu W., Valencia P., Moore D. (2010) «Environmental Wireless Sensor Networks». IEEE, Proceedings of the IEEE, Vol. 98, No. 11, pp 1903- 1917.

Czarnowski A. P. (2014) «Service Availability (In the Clouds) ». AVET INS/EuroCloud Polska, pp 3-16.

Dhem Jean-François, et al. (2000) «A Practical Implementation of the Timing Attack». Springer, Lecture Notes in Computer Science, Volume 1820, pp 167-182.

Dwoskin J., Xu D., Huang J., Chiang M., Lee R. (2007) «Secure Key Management Architecture against Sensor-node Fabrication Attacks». IEEE GLOBECOM, Department of Electrical Engineering, Princeton University, NJ 08544, USA, pp 166-171.

Dyka Z., Langendorfer P. (2013) «Improving the Security of Wireless Sensor Networks by Protecting the Sensor Nodes against Side Channel Attacks». Springer, Wireless Networks and Security, SCT, pp. 303-328.

El-Basioni B. M., Abd El-kader S. M., Fakhreldin M. A. (2013) «Smart Home Design using Wireless Sensor Network and Biometric Technologies». IJAIEM Egypt, Volume 2, Issue 3, pp: 413-429.

Esteves António, et al. (2009) «A Prototype to Integrate a Wireless Sensor Network with Civil Protection Grid Applications». Department of Informatics, University of Minho. Portugal, pp 1-11.

García-Hernández F. C., Ibargüengoytia-González P. H., García-Hernández J., Pérez-Díaz, J. A. (2007) «Wireless Sensor Networks and Applications: a Survey». Electric Research Institute, (IIE), ITESM, Cuernavaca Campus, Mexico, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, pp 264-273.

Gay D., Levis P., Behren R.v. (2003) «The nesC language: A Holistic Approach To Networked Embedded Systems». PLDI '03 Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation, pp 1-11.

Genkin D., Shamir A., Tromer E. (2014) «RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis». Springer, CRYPTO 2014, Part I, LNCS 8616, pp. 444–461.

Gowrishankar S. (2008) «Issues in Wireless Sensor Networks».IAENG, Proceedings of the World Congress on Engineering, Vol I, pp 176-187.

Halderman A., et al. (2008) «Lest We Remember: Cold Boot Attacks on Encryption Keys». USENIX, 17th USENIX Security Symposium, pp 45-60.

Heyszl J., Mangard S., Heinz B., Stumpf F., Sigl G. (2012)« Localized Electromagnetic Analysis of Cryptographic Implementations». Springer, Topics in Cryptology–CT-RSA 2012, Lecture Notes in Computer Science, Volume 7178, pp 231-244.

Ilyas M, Mahgoub M. (2005) «Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems», CRC Press, pp 12-47

Ingram K., Forrest S. (2002) «A History and Survey of Network Firewalls». The University of New Mexico Computer Science Department Technical Report 2002-37, pp 1-42.

Junnila S., et al, (2010) «Wireless, Multipurpose In-Home Health Monitoring Platform: Two Case Trials».IEEE, IEEE Transactions of Information Technology in Biomedicine, Vol 14, No 2, pp 447-455.

Katiyar V., Kumar P., Chand N. (2011) «An Intelligent Transportation Systems Architecture Using Wireless Sensor Networks». International Journal of Computer Applications (0975- 8887), Volume 14, No.2, pp: 22 – 26.

Kim D., Nair P.J., Quereshi M.K. (2014) «Architectural Support for Mitigating Row Hammering in DRAM Memories». IEEE, Computer Architecture Letters, Vol.: 14 Issue: 1, pp 9-12.

Kim Y., et al. (2014) «Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors». IEEE, Computer Architecture (ISCA), pp 361-372.

Klein A. (2013) «Stream Ciphers». Springer, ISBN: 978-1-4471-5078-7, pp 15-58.

Koeune F. (2005) «Timing Attack». Springer, Encyclopedia of Cryptography and Security, pp 620-621.

Kulau U., Schildt S., Von Zengen G., Rottmann S., Wolf L. (2014) « Ballistic Deployment of WSN Nodes Using Model Rockets». ACM, Institute for Operating Systems and Computer Networks Technische Universität Braunschweig, Braunschweig, ExtremeCom '14, Germany, pp 1 -6.

Kumar M. (2011) «Wireless Sensor Networks: Security Issues and Challenges», IJCIT, ISSN 2078-5828, Vol 02, Issue 01, pp 62- 67.

Lee S.H., Lee S., Song H., Lee H.S., (2009) «Wireless Sensor Network Design for Tactical Military Applications: Remote large-scale environments». IEEE, Military Communications Conference, 2009. MILCOM 2009, pp1 -7.

Martinez K., Hart J. K., Ong R. (2004) «Environmental Sensor Networks». IEEE, Computer Manuscript, Vol. 34, Issue 8, pp 1-6.

Menezes A., Van Oorschot P., Vanstone S. (1996) «Handbook of Applied Cryptography». CRC Press, pp 191-222.

Messerges T. S. (2001) «Securing the AES Finalists against Power Analysis Attacks». Springer, Fast Software Encryption Lecture Notes in Computer Science, Vol 1978, pp 150-164.

Newsome J., Shi E., Song D., Perrig A. (2004) «The Sybil Attack in Sensor Networks: Analysis & Defenses». IEEE, Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium, pp 1–10.

Okeya K., Iwata T. (2005) «Side Channel Attacks on Message Authentication Codes». Springer, 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, pp 205-207.

Oliveira L. M. L., Rodrigues J. J. P. C. (2011) «Wireless Sensor Networks: a Survey on Environmental Monitoring». Journal of Communications, Portugal, Vol. 6, No. 2, pp 143-151.

Patil P.D., Dawande N.A. (2014) «WNS for Agricultural Monitoring & Development». International Journal of Engineering Research and General Science (IJERGS) Vol 2, Issue 4, pp 403-407.

Pukish M. S., et al. (2010) «Recent Developments in Wireless Hardware Design, Modeling, and Analysis for Industrial Applications». IEEE, IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society, pp: 6315 – 6319.

Quisquater J., Samyde D. (2001) «ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards». Springer, Smart Card Programming and Security Lecture Notes in Computer Science, Volume 2140, pp 200-210.

Rahman K. C. (2010) «A Survey on Sensor Network». IEEE, Communications magazine, ,Vol 40, Issue), pp 102-114.

Raza Muhammad Taqi, et al. (2007) «A Yaw Rate Aware Sensor Wakeup Protocol (YAP) for Target Prediction and Tracking in Sensor Networks». Department of Information and Communication Engineering Ajou University, Republic of Korea, pp 1-7.

Rivain M. (2009) «Differential Fault Analysis on DES Middle Rounds». Springer, Cryptographic Hardware and Embedded Systems - CHES 2009, Lecture Notes in Computer Science, Volume 5747, pp 457-469.

Roosta T., Shieh S., Sastry S. (2006) «Taxonomy of Security Attacks in Sensor Networks and Countermeasures». IEEE, First IEEE Int. Conf. on System Integration and Reliability Improvements, Vol 25, pp 1-11.

Sankardas R., Conti M., Sanjeev S., Sushil J. (2014) «Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact». IEEE, Transactions on Information Forensic and Security, Vol. 9, No. 4, pp 681-694.

Saxena N., Voris J. (2011) «Data Remanence Effects on Memory-based Entropy Collection for RFID Systems». Springer, International Journal Information Security, Volume 10, Issue 4, pp 213-222.

Scarfone K., Mell P. (2007) «Guide to Intrusion Detection and Prevention Systems». NIST, NIST special publication 800.2007, pp 14-28.

Shannon C. (1949) «Communication Theory of Secrecy Systems», pp 1-60.

Skorobogatov S. (2005) «Data Remanence in Flash Memory Devices». Springer, Lecture Notes in Computer Science, CHES, Vol 3659, pp 339–353.

Sohraby K., Minoli D., Znati T. (2007) «Wireless Sensor Networks: Technology Protocols and Applications». Willey, ISBN: 978-0-471-74300-2, pp 15- 26.

Song H., Zhu S., Cao G. (2007) «Attack-Resilient Time Synchronization for Wireless Sensor Networks». Elsevier, Ad hoc networks, Vol 5, Issue 1, pp 112–125.

Standaert F. X. (2012) «Introduction to Side Chanel Attacks». Belgian Fund for Scientific Research (FNRS), BCRYPT Course on Embedded Security, Belgium, pp 1-15.

Van Brussel H., et al. (2008) «Cryptanalysis and Design of Stream Ciphers». Katholieke Universiteit Leuven, Belgium, Thesis ISBN 978-90-5682-000-8, pp 1-151.

Van Tilborg H., Jajodia S. (2011) «Encyclopedia of Cryptography and Security». Springer Science & Business Media, pp 272- 275.

Virone G. et al. (2006) «An Advanced Wireless Sensor Network for Health Monitoring». Department of Computer Science, University of Virginia, pp 1-4.

Yick et al, (2008) «Wireless sensor network survey». Elsevier, Computer networks, Vol 52, Issue12 pp 2292-2330.

Zeng G, Dong X. (2013) «Reconfigurable Feedback Shift Register Based Stream Cipher for Wireless Sensor Networks», IEEE, IEEE Wireless Communication Letters, Vol 2, No. 5, pp. 559-562.

Zhao G. (2010) «Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey».Macrothink, Network Protocols and Algorithms, ISSN 1943-35812011, Vol. 3, No. 1, pp 46-63.

Πατσάκης Κ., Φούντας Ε. (2009) «Κρυπτογραφία και Εφαρμογές 1». Εκδόσεις Βαρβαρήγου, σελ. 97-105.

Παράρτημα Α
Κώδικες Υλοποίησης.

Α.1 Κώδικας Υλοποίησης LFSR

```
#include <iostream>
#include <iomanip>
using std::cout;
using std::cin;
using std::setw;
using std::endl;
using std::string;
using std::stringstream;


void printArray(int initalLFSRdata[])
{
    for(int i=0; i<32; ++i)
    {
        cout<<initalLFSRdata[i]<<" ";
    }
    cout<<endl;
}


int main()
{

int initalLFSR[32]={1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0};
int LFSR[512][32];
int HD[512];
int PD[512];
int length;
int count=0;

cout<<" Gia tin arxiki katastasi  "; printArray(initalLFSR); cout<<" LFSR"<<endl;
cout<<endl;
cout<<"Eisagete to plithos ton grammon"<<endl
        <<"pou Thelete na exei o pinakas"<<endl
        <<"PROSOXI oxi megalitero apo 501"<<endl;
cout<<endl;
cin>>length;
cout<<endl;

/********** Transfer of initial state into Array LFSR**********/
  for(int i=0; i<32; i++)
         {
                LFSR[0][i]=initalLFSR[i];
         }
```

```
/*********** Creation of LFSR Array***********/
  for(int i=0; i<length; i++)
         for (int j=0; j<32; j++)
         {
        LFSR[i+1][0]=LFSR[i][0]^LFSR[i][1]^LFSR[i][2]^LFSR[i][3]^LFSR[i][4]^LFSR[i][31];
        LFSR[i+1][j+1]=LFSR[i][j];
         }

/*********** Print of LFSR Array ***********/
  for(int i=0; i<length; i++)
          {
                for (int j=0; j<32; j++)
                 {
                 cout<<setw(2)<<LFSR[i][j]<<setw(2);
                 }
                 cout<<endl;
          }
          cout<<endl;

/*********** Creation of HD Array ***********/
  for(int i=0; i<length; i++)
  {count=0;
        for (int j=0; j<32; j++)
        //computes Hamming Distanse
        {
        if(LFSR[i][j]!=LFSR[i+1][j])
                {
                count++;
                HD[i]=count;
                }
         }
  }

/********** Print HD Array *****************/
          for(int i=0; i<length-1; i++)
          {
        out<<setw(2)<<"Hamming Distance  "<<i<<" kai "<<i+1<<" = "<<HD[i]<<setw(2)<<endl;
          }
          cout<<endl;


/**********Creation of PD Array ***********/
          for(int i=0; i<length-1; i++)
          {
                  if(HD[i]==HD[i+1])
                          PD[i]=0;
                  else
                          PD[i]=1;
        }
cout<<endl;
                  //
/**********Print Of PD Array**********/
          cout<<"To PD einai to :";
           for(int i=0; i<length-1; i++)
          {
                  cout<<setw(2)<<PD[i]<<setw(2);
          }
 cout<<endl;
 cout<<endl;
 cout<<"Press Enter For Exit";
 cout<<endl;
 system("pause");
return 0;
}
```

A.2 Κώδικας Υλοποίησης Μεθόδου Απαλοιφής του Gauss

```
/************* Gauss elimination for solving linear equations *************/
#include<stdio.h>
#include<conio.h>
#include<math.h>
#include<stdlib.h>

#define N 40

int xor_add(int a, int b);

FILE *fp;

int main()
{
    int n,i,j,k,temp,m,counter;
    int a[N][N],c,d[N]={0},v1[N],v2[N];


    fp=fopen("input.txt","r");

    printf("No of equation ? ");
    scanf("%d",&n);;
    printf("Coefficient of all : \n");
    for(i=0;i<n;i++)
    {
        printf("equation %d:", i+1);
        for(j=0;j<=n;j++)
        {
            fscanf(fp,"%d", &a[i][j]);
            printf("%d ", a[i][j]);
        }
        printf("\n");
    }

  counter=-1;

  for(i=0;i<n;i++)
  {
        k=i;
        while ((k<n) && (a[k][i]!=1))
          k++;


        if (k<n) //Switch the i-th row with the k-th row
        {
                for(j=0;j<=n;j++)
                {
                  c=a[i][j];
                  a[i][j]=a[k][j];
                   a[k][j]=c;
                  }
          }
          else  // there is no row with a[i][i]=1, so we will switch columns
          {
                k=i+1;
                while ((k<n) && (a[i][k]!=1))
                  k++;
                if (k<n) //Switch the i-th column with the k-th column
            {
              counter++;
              v1[counter]=i;
              v2[counter]=k;

                  for(j=0;j<n;j++)
                  {
                    c=a[j][i];
                    a[j][i]=a[j][k];
                     a[j][k]=c;
                    }
```

```
            }
          else
          {
                printf("The coefficient matrix is non-singular\n");
                system("pause");
                return 0;
          }
          }

          //Now a[i][i]=1
          for(m=i+1;m<n;m++)
            if (a[m][i]==1)
            {
             for(j=0;j<=n;j++)
                   a[m][j]=xor_add(a[m][j],a[i][j]);
                }

    }

    //*************** DISPLAY UPPER TRIANGULAR MATRIX*************//
    printf("Displaying the upper-triangular matrix\n");
        for(i=0;i<n;i++)
    {
        for(j=0;j<=n;j++)
            printf("%d",a[i][j]);
        printf("\n");
    }

    system("pause");



    //***************** Backward Substitution method***************//

    d[n-1]=a[n-1][n];
    for(i=n-2;i>=0;i--)
    {
        c=0;
        for (k=n-1;k>i;k--)
        {
          c=xor_add(c,a[i][k]*d[k]);
                }
        d[i]=xor_add(c,a[i][n]);
    }

     if (counter>0) //columns swapped
                for(i=counter;counter>0;counter--)
                {
                  c=d[v2[counter]];
                  d[v2[counter]]=d[v1[counter]];
                  d[v1[counter]]=c;
                 }


    //******** RESULT DISPLAY *********//
    printf("\nsolution vector:\n");
    for(i=0;i<n;i++)
     printf("%d",d[i]);
    printf("\n");

    fclose(fp);
    system("pause");
    return 0;
}

int xor_add(int a, int b)
{
        if (a==b)
          return 0;
          else
          return 1;
}
```