Ανοιχτό Πανεπιστήμιο Κύπρου

Σχολή θετικών και εφαρμοσμένων επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Συστήματα Ασύρματης Επικοινωνίας

Μεταπτυχιακή Διατριβή

«Ανάπτυξη συστήματος Ταυτοποίησης και εντοπισμού συσκευών 802.11»

Μιχάλης Μαντούβαλος

Επιβλέπων Καθηγητής

Δρ. Σταύρος Σταύρου

Δεκέμβριος 2018

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται το θέμα της απεικόνισης των ασύρματων συσκευών και δικτύων ενός χώρου που αξιοποιούν το πρωτόκολλο 802.11, χρησιμοποιώντας ως αναγνωριστικό τις MAC διευθύνσεις τους . Σε πρώτο επίπεδο ορίζεται η πανταχού παρούσα υπολογιστική ως το τελευταίο κύμα εξέλιξης της τεχνολογίας στον τομέα της χρήσης πολλαπλών φορητών συσκευών από ένα άτομο ή οργανισμό και διερευνάται η σημασία των ασύρματων δικτύων στη λειτουργία τους. Στη συνέχεια, παρατίθενται οι θεωρητικές αρχές των δικτύων και ο τρόπος με τον οποίο αυτά εξελίχθηκαν με τέτοιο τρόπο ώστε να αποτελούν αναπόσπαστο κομμάτι της καθημερινής ζωής των ανθρώπων σε προσωπικό ή επαγγελματικό επίπεδο. Έπειτα εξετάζεται το πλαίσιο της διασφάλισης της πληροφορίας που μεταφέρεται μέσω αυτών και η ανάγκη που αναδύεται για την παρακολούθηση της μη εξουσιοδοτημένης πρόσβασης. Επιπρόσθετα, υπογραμμίζεται η συσχέτιση της ασφάλειας με την εμφάνιση των εμπορικών drones, τα οποία καθιστούν τον έλεγχο της φυσικής παρουσίας ενός κακόβουλου ατόμου, ακόμα δυσχερέστερη. Τέλος, μέσα από παραδείγματα παρουσιάζεται η ανάπτυξη εφαρμογής, κατάλληλης ώστε να ανιχνεύει και να απεικονίζει την παρουσία ασύρματων συσκευών οι οποίες λειτουργούν κάτω από το πρίσμα του 802.11 πρωτοκόλλου. Ο διαχειριστής της εφαρμογής θα έχει στη διάθεσή του τέσσερις διαφορετικές επιλογές, μέσα από τις οποίες θα μπορεί να επιβλέπει και να προστατεύει τον χώρο που επιθυμεί από την μη εξουσιοδοτημένη παρουσία ασύρματων συσκευών.

Abstract

This diploma deals with the monitoring of wireless devices and networks of a certain area, that uses the 802.11 protocol, exploiting their MAC addresses, as their identifier. At first, ubiquitous computing is defined as the last wave of technology advances, in the use of multiple portable devices by an individual or an organization, and the use of wireless communications for their advance. Subsequently, the theoretical principles of networks are being presented, and how they evolved in such a way that they are an integral part of our personal and professional life. The following sections discuss the importance of securing the information that is being transferred through these wireless networks with the need of monitoring unauthorized acces. Additionally, the association of security with the emergence of commercial drone use, is underlined, giving security a harder time to deal with the defence of this transparent threat. Finally, with the use of examples, the project's monitoring device that is able to detect 802.11 wireless devices, is being introduced. Users of the following application can examine four different options, allowing them to detect, recognise and prevent unauthorized access of wireless devices, in a given space.

Ευχαριστίες

Στο σημείο αυτό, αισθάνομαι την ανάγκη να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου και νυν ακαδημαϊκό υπεύθυνο και αναπληρωτή, κύριο Σταύρου Σταύρο, για την εμπιστοσύνη που μου έδειξε ως προς την ανάθεση αυτής της διπλωματικής εργασίας, καθώς και για την πολύτιμη βοήθεια του, ως προς την ολοκλήρωση της. Ακόμα, θα ήθελα να ευχαριστήσω ιδιαίτερα τον Νίκο Θωμαδάκη, για την πολύτιμη και άρτια καθοδήγησή του. Θερμές ευχαριστίες θα ήθελα να εκφράσω επίσης στους φίλους μου, στους συναδέλφους μου, καθώς και στην οικογένεια μου, για την αμέριστη υπομονή και ψυχολογική στήριξη που μου παρείχαν, καθ' όλη τη διάρκεια ολοκλήρωσης του παρόντος κύκλου σπουδών.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ραγδαία ανάπτυξη των συσκευών με επίγνωση πλαισίου έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο αλληλοεπιδρούμε καθημερινά με το περιβάλλον. Η γενιά της πανταχού παρούσας υπολογιστικής έχει μετατρέψει κάθε είδους πληροφορία σε ψηφιακή μορφή, η οποία ανταλλάσσεται καθημερινά από δισεκατομμύρια ανθρώπους μέσω τοπικών ασύρματων δικτύων και συσκευών όπως φορητοί υπολογιστές, αισθητήρες και έξυπνα τηλέφωνα. Το internet πλέον αποτελεί αναγκαίο εργαλείο όχι μόνο για τις επιχειρήσεις αλλά και σε προσωπικό επίπεδο. Η καθημερινή χρήση του για σκοπούς μετάδοσης πληροφορίας σε τομείς, όπως η επικοινωνία, το εμπόριο, η ψυχαγωγία και η ασφάλεια έχει καταστήσει τη χρήση του αναγκαία και αποτελεί αναπόσπαστο πλέον κομμάτι στις ζωές των ανθρώπων. Σε κάθε άνθρωπο ή οργανισμό αντιστοιχούν δεκάδες συσκευές συλλογής πληροφοριών, οι οποίες αξιοποιούν το ασύρματο μέσο προκειμένου να συνδεθούν και να επικοινωνήσουν μεταξύ τους. Αμέτρητες συσκευές σε κάθε επίπεδο ανταλλάσσουν πληροφορίες σε διάφορους τομείς, οι οποίες περιέχουν δεδομένα υψίστης σημασίας για τους ανθρώπους ή τους οργανισμούς που εξυπηρετούν. Το πρωτόκολλο ασύρματης επικοινωνίας IEEE 802.11 αποτελεί τον πιο διαδεδομένο τρόπο ανταλλαγής αυτής της πληροφορίας με αμέτρητες δυνατότητες, αλλά και αρκετούς κινδύνους. Το ερευνητικό ερώτημα που καλείται να απαντηθεί είναι « πώς γνωρίζει κανείς πως ο προσωπικός του χώρος δεν παραβιάζεται από την αδιάκριτη παρουσία συσκευών με επίγνωση πλαισίου; Πώς μπορεί κανείς να είναι σίγουρος πως οι κινήσεις του δεν παρακολουθούνται και δεν καταγράφονται από τρίτους;» Παρά τις τεχνικές διασφάλισης τους, η φύση των ασύρματων δικτύων καθιστά πολύ εύκολη την εισβολή και την απόσπαση της κίνησης τους, πράγμα που θα μπορούσε να επιφέρει δραματικές επιπτώσεις. Η ακεραιότητα και η ιδιωτικότητα της πληροφορίας είναι καθοριστικής σημασίας για οποιονδήποτε άνθρωπο ή οργανισμό. Ο φυσικός έλεγχος της ασφάλειας αποτελεί το πρώτο επίπεδο

προστασίας ενάντια σε μη εξουσιοδοτημένη παρουσία ή ενέργεια. Λόγω της φύσης και του μεγέθους τους, οι ασύρματες συσκευές στην εποχή που διανύουμε είναι αρκετά δύσκολο να γίνουν αισθητές σε ένα χώρο χωρίς την χρήση κατάλληλου εξοπλισμού, κάτι που μπορεί να τις καταστήσει αδιάκριτες ή επικίνδυνες. Δεδομένης της πλήρους ενσωμάτωσης της ανταλλαγής της πληροφορίας μέσω των ασύρματων συσκευών που περιβάλλουν έναν άνθρωπο ή έναν οργανισμό, είναι αναγκαία και η ύπαρξη ενός συστήματος για την παρακολούθηση και την αποτροπή της παρουσίας μη εξουσιοδοτημένων συσκευών στον χώρο. Ταυτόχρονα με την εμφάνιση των εμπορικά διαθέσιμων μη επανδρωμένων αεροσκαφών, ο τομέας της φυσικής ασφάλειας δέχεται ακόμα ένα πλήγμα όσον αφορά στη διαφύλαξη της πληροφορίας σε φυσικό κυρίως επίπεδο, καθιστώντας την παρουσία ενός συστήματος παρακολούθησης και καταγραφής της δραστηριότητάς τους αναγκαία. Η παρούσα διατριβή στοχεύει αρχικά στην βιβλιογραφική ανασκόπηση της πανταχού παρούσας υπολογιστικής και των ασύρματων δικτύων με έμφαση στο 802.11 πρωτόκολλο, καθώς και την διαφύλαξη της ασφάλειας σε φυσικό επίπεδο από την εμφάνιση πιθανών κινδύνων που προκύπτουν από την μαζική εμπορικοποίηση των εναέριων μη επανδρωμένων αεροσκαφών. Σε δεύτερο επίπεδο γίνεται αναφορά στην ανάπτυξη της εφαρμογής για την καταγραφή και απεικόνιση συσκευών που αξιοποιούν το πρωτόκολλο επικοινωνίας 802.11, καταγράφοντας τις μοναδικές MAC διευθύνσεις τους. Η εφαρμογή θα αποτελείται από τέσσερις λειτουργίες καταγραφής, αναζήτησης και προειδοποίησης των χρηστών για μη εξουσιοδοτημένη ή κακόβουλη ενέργεια.

Κεφάλαιο 2

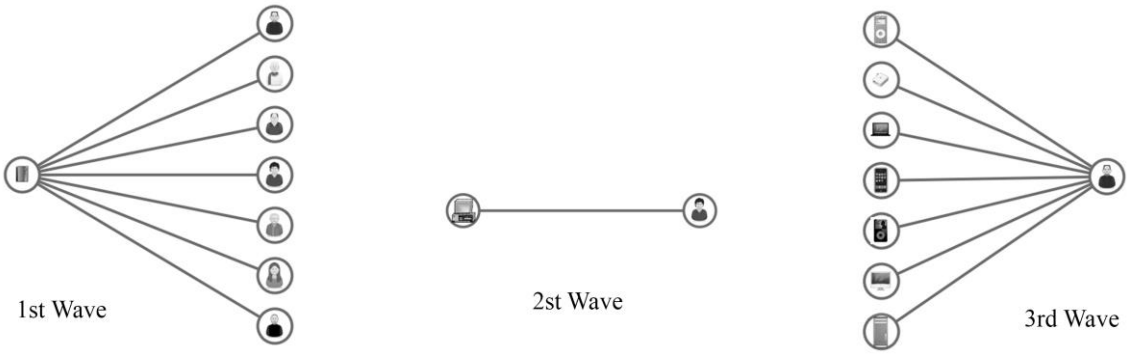
Πανταχού παρούσα υπολογιστική

Η βιολογική ανάγκη του ανθρώπου για επέκταση των δυνατοτήτων του στην επικοινωνία, συνετέλεσε στη σταδιακή από αυτόν συγκέντρωση των τελευταίων τεχνολογικών πόρων και τη διαμόρφωσή τους με τέτοιο τρόπο, ώστε να προσαρμόζονται στο φυσικό του περιβάλλον. Η εξέλιξη των ασύρματων τεχνολογιών, καθώς και του διαδικτύου αποτέλεσε καθοριστικό παράγοντα για την εμφάνιση του τρίτου σε σειρά κύματος στην ανάπτυξη των πληροφοριακών συστημάτων, την εποχή της πανταχού παρούσας υπολογιστικής [1].

Ο όρος αυτός συνιστά μία έννοια ευρέως αναπτυσσόμενη στον τομέα της τεχνολογίας των Πληροφοριών και των Επικοινωνιών, καθώς προορίζεται να συνδέει διάφορες και διαφορετικές μεταξύ τους εφαρμογές σε πολλές πτυχές της ανθρώπινης δραστηριότητας, όπως είναι η απομακρυσμένη υγεία, οι ευφυείς μεταφορές, η ευρεία καταγραφή των γεγονότων του περιβάλλοντος [2].

Οι απαρχές εμφάνισης των πρώτων υπολογιστών θα μπορούσαν να επονομαστούν ως εποχή του κεντρικού υπολογιστή (πρώτο κύμα). Πρόκειται για τη χρήση ενός ενιαίου υπολογιστή (mainframe) μέσω του οποίου πολλοί άνθρωποι επιτελούσαν τις διάφορες εργασίες τους με σημείο αναφοράς τους έναν ορισμένο σταθμό εργασίας (workstation). Με το πέρασμα των δεκαετιών επήλθε η μετάβαση στην εποχή του προσωπικού υπολογιστή (δεύτερο κύμα), κατά την οποία προβλεπόταν η χρήση ενός υπολογιστή κατά άτομο – χειριστή (personal computer). Στην προκειμένη περίπτωση προϋποτίθεται συνειδητή αλληλεπίδραση με τον χρήστη, ο οποίος κατά κύριο λόγο δεσμεύεται στην επιφάνεια εργασίας του υπολογιστικού του περιβάλλοντος [3].

Τις τελευταίες δεκαετίες, η σχέση μεταξύ ανθρώπου και υπολογιστή διαμορφώθηκε με τέτοιο τρόπο ώστε να αντιστοιχούν περισσότεροι υπολογιστές σε έναν χρήστη. Πρόκειται για μία σχέση πολλά προς ένα και για την εποχή της διάχυτης ή αλλιώς πανταχού παρούσας υπολογιστικής. Εκατομμύρια από αυτούς τους υπολογιστές βρίσκονται πλέον ενσωματωμένοι στο περιβάλλον, επιτρέποντας στην τεχνολογία να μην είναι εμφανής σε πρώτο επίπεδο, υποχωρώντας σταδιακά στο παρασκήνιο. Η σύγχρονη εποχή πληροφορικής είναι πλέον γνωστή σε διεθνές επίπεδο ως " Ubiquitous Computing" [4].



Εικόνα 2.1

Η Πανταχού παρούσα υπολογιστική είναι μια ιδέα στη βάση της οποίας, οι υπολογιστικές δυνατότητες είναι διάσπαρτες παντού και ο υπολογισμός της πληροφορίας μπορεί να εμφανίζεται οπουδήποτε, χρησιμοποιώντας οποιαδήποτε συσκευή, σε οποιαδήποτε θέση και σε οποιαδήποτε μορφή. Ο υπολογισμός και η κατανόηση του περιβάλλοντος στα πανταχού παρόντα συστήματα παίζει καθοριστικό ρόλο σε αυτά. Οι εξελίξεις στην επιστήμη των υπολογιστών παρέχουν πλέον την δυνατότητα στη τεχνολογία να ενσωματώνεται άψογα στην καθημερινότητά μας [5].

Οι συσκευές λειτουργούν σε δικτυωμένο και αυτόνομο περιβάλλον και είναι ικανές να επικοινωνούν με τον άνθρωπο, αλλά και μεταξύ τους. Αυτές οι συσκευές υποστηρίζουν εφαρμογές με γνώμονα το περιβάλλον, νομαδικούς χρήστες, υπηρεσίες γνωστοποίησης θέσης και πρόσβαση σε κινητά δεδομένα. Τα πανταχού παρόντα

συστήματα παρέχουν οπουδήποτε και οποτεδήποτε πρόσβαση σε πληροφορίες και διάφορες υπηρεσίες, ενώ ταυτόχρονα καθιστούν την παρουσία του συστήματος "αόρατη" στο χρήστη (Poslad, 2009)[6].

Για τη στήριξη της πανταχού παρούσας υπολογιστικής απαιτείται η χρήση ορισμένων βασικών τεχνολογιών, όπως το διαδίκτυο, το ενδιάμεσο λογισμικό (middleware), το λειτουργικό σύστημα, οι αισθητήρες, οι μικροεπεξεργαστές, οι διεπαφές εισόδου – εξόδου (I/O interfaces), οι διεπαφές χρήστης (user interfaces), τα δίκτυα, τα διάφορα πρωτόκολλα, οι κινητοί πράκτορες (Mobile agents) και οι υπηρεσίες τοποθεσίας [6].

Μία κοινά αποδεκτή εννοιολογική αποσαφήνιση διατυπωμένη από τον M. Weiser (1991) [7], ο οποίος επινόησε τον όρο ως επικεφαλής τεχνολόγος της Xexor Palo Alto Research Center (PARC), ορίζει την πανταχού παρούσα υπολογιστική ως τη μέθοδο που αποσκοπεί στην αύξηση της χρήσης των ηλεκτρονικών υπολογιστών και υπάρχει διαθέσιμη σε όλο το φυσικό περιβάλλον. Όπως χαρακτηριστικά ανέφερε ο ίδιος, οι πιο εμβριθείς τεχνολογίες είναι εκείνες που εξαφανίζονται, δεδομένου ότι συνυπάρχουν στον ιστό της καθημερινής ζωής έως ότου δεν μπορούν να διακριθούν πλέον από αυτό.

Παρόλο που ο Weiser (1991) [7] οραματίστηκε τον όρο “Πανταχού παρούσα υπολογιστική” ως μια πιο ακαδημαϊκή και ιδεαλιστική έννοια και ως ένα διακριτικό – ανθρωποκεντρικό τεχνολογικό όραμα που η ανάπτυξη και η εφαρμογή του αφορά μία μελλοντική πραγματικότητα, η βιομηχανία του σήμερα έχει προσεγγίσει τον όρο αυτόν με διαφορετική κλίση, αποδίδοντας τον ως “διάχυτη υπολογιστική“. Αν και ο όρος αυτός σχετίζεται με την πανταχού παρούσα επεξεργασία πληροφοριών, ο πρωταρχικός της στόχος είναι να εκμεταλλευτεί αυτή την επεξεργασία δεδομένων στο εγγύς μέλλον σε τομείς, όπως το ηλεκτρονικό εμπόριο και τις web-based επιχειρησιακές διαδικασίες.

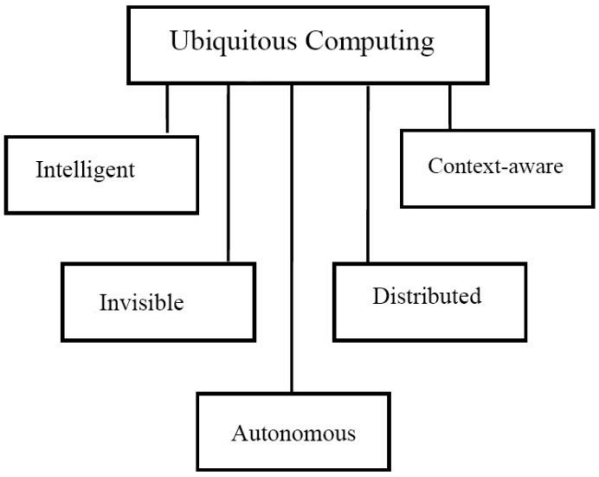
Σε αυτή την πραγματική παραλλαγή, όπου η ασύρματη τεχνολογία αποτελεί σημαντικό παράγοντα σε συνδυασμό με την ανάπτυξη των ασύρματων συσκευών, η εφαρμογή της πανταχού παρούσας υπολογιστικής εδραιώνεται ολοένα και περισσότερο στις καθημερινές ζωές των ανθρώπων. Το όραμα της πανταχού παρούσας υπολογιστικής στηρίζεται στη πεποίθηση της επιστημονικής κοινότητας, πως ο νόμος του [8]Moore (1965) θα ισχύει για τουλάχιστον 10 με 15 χρόνια ακόμη. Ο Moore διαπίστωσε πως ο αριθμός των τρανζίστορ ανά τσιπ και κατά συνέπεια η ισχύς των μικροεπεξεργαστών, διπλασιάζονται κάθε 18 μήνες. Αυτό σημαίνει ότι στα επόμενα χρόνια οι μικροεπεξεργαστές θα μειώσουν το κόστος και το μέγεθός τους σε τόσο

μεγάλο βαθμό, ώστε να μπορούν να ενσωματωθούν όχι μόνο σε ηλεκτρονικές συσκευές, αυτοκίνητα, παιχνίδια και εργαλεία, αλλά και σε κοσμικά αντικείμενα όπως μολύβια, ρούχα ή βιβλία. Στην πραγματικότητα η τεχνολογία αναμένεται να επιφέρει περαιτέρω δραματικές βελτιώσεις, κάτι που σημαίνει ότι τελικά δισεκατομμύρια μικρών και κινητών επεξεργαστών, θα καταλάβουν το περιβάλλον και θα ενσωματωθούν σε πολλά αντικείμενα του φυσικού μας κόσμου, συνδεδεμένες μεταξύ τους μέσω του ασύρματου μέσου.

Σύμφωνα με τον Zhang (2005) [9], η πανταχού παρούσα υπολογιστική ορίζεται ως well defined περιοχή, με την έννοια του περιβάλλοντος το οποίο περιλαμβάνει μία σειρά από ενσωματωμένα συστήματα όπως υπολογιστές, αισθητήρες, διεπαφές χρηστών και της υποδομής των υπηρεσιών που με τη σειρά τους ενισχύεται από τις ΤΠΕ (τεχνολογίες της πληροφορίας και των επικοινωνιών).

Πρώτος ο Weiser [7] εντόπισε τις τρεις κυριότερες ιδιότητες της διάχυτης υπολογιστικής, αυτή του κατανεμημένου υπολογισμού (distributed computation), αυτή της μη ορατής παρουσίας (invisibility), και αυτής της επίγνωσης πλαισίου (context-awareness). Ο όρος του κατανεμημένου υπολογισμού υπαγορεύει ότι τα υπολογιστικά συστήματα πρέπει να είναι δικτυωμένα, διανεμημένα και διαφανή, δηλαδή να μπορούν να αλληλεπιδρούν με τους ανθρώπους καθώς και μεταξύ τους. Η έννοια της αόρατης παρουσίας υπονοεί την διάφανη αλληλεπίδραση των συσκευών με τον χρήστη και τέλος η τρίτη ιδιότητα, αυτή της επίγνωσης πλαισίου, υποδηλώνει πως προκειμένου οι συσκευές να αξιοποιηθούν με τον βέλτιστο τρόπο από τον άνθρωπο, στο φυσικό του χώρο, χρειάζεται να έχουν επίγνωση του περιβάλλοντός που τους περιβάλλει [10].

Σύμφωνα με τους Abowd και Mynatt (2000) [11], οι συσκευές πανταχού παρούσας υπολογιστικής έχουν ως σκοπό την διευκόλυνση των χρηστών στην καθημερινή τους ζωή. Παράλληλα, οι Kang and Pisan (2006) [12]υποστήριξαν πως η βασική αρχή της διάχυτης υπολογιστικής αποσκοπεί στην προσανατολισμένη γύρω από τον άνθρωπο χρήση των συσκευών με φυσικό και μη παρεμβατικό τρόπο. Στο σχήμα που ακολουθεί ο [6] Poslad (2009), απεικονίζει της βασικότερες κατηγοριοποιήσεις της πανταχού παρούσας υπολογιστικής :



Εικόνα 2.2 [6]

2.1 Αρχές σχεδιασμού συστημάτων με επίγνωση πλαισίου.

Η χρήση των εφαρμογών σε υπολογιστικά συστήματα με επίγνωση πλαισίου συνεχώς αυξάνεται κυρίως λόγω της αύξησης και τις εξέλιξης των ασύρματων συσκευών. Ένα τέτοιο παράδειγμα αποτελούν οι εφαρμογές που εξυπηρετούν στον προσανατολισμό των χρηστών βασιζόμενες στην εκάστοτε τοποθεσία τους. Προκειμένου να συλληφθούν οι συντεταγμένες του χρήστη, δίνοντάς του την ανάλογη πληροφορία, συνεργάζεται ένα πλήθος τεχνολογιών και αισθητήρων, όπως GPS δέκτες και δορυφόροι, σταθμοί βάσης εκπομπής και λήψεως σημάτων, αισθητήρες ανίχνευσης εγγύτητας (Proximity sensors) , μικρο-κάμερες, μαγνητικά card readers κ.α. [13].

Οι εφαρμογές που αξιοποιούν τα συστήματα επίγνωσης πλαισίου δεν επικεντρώνονται μονάχα στην καταγραφή της τοποθεσίας ενός χρήστη, αλλά επεκτείνονται, με την χρήση διαφορετικών μηχανισμών και καινοτομιών, όπως ανιχνευτές ήχου, κίνησης, φωτός ή καπνού. Ο συνδυασμός των πληροφοριών που μπορούν να καταγραφούν με τα παραπάνω, επιτρέπει τον σχεδιασμό και την ανάπτυξη εφαρμογών με μεγαλύτερη χρησιμότητα, αποδοτικότητα, προσαρμοστικότητα και χρηστικότητα [13].

Ο Chen (2004) [14] παρουσίασε τρεις διαφορετικές μεθόδους συλλογής δεδομένων περιβάλλοντος: την άμεση πρόσβαση αισθητήρα, το ενδιάμεσο λογισμικό μεταξύ συσκευών, καθώς και τον διακομιστή περιβάλλοντος. Οι Munoz et al. (2003) [15] ανέπτυξαν μία υποδομή συστημάτων με επίγνωση πλαισίου η οποία στηρίζει την άμεση ανταλλαγή μηνυμάτων με σκοπό την βελτιστοποίηση της διαχείρισης πληροφοριών στα νοσοκομεία.

Επιπλέον οι Devaraju et al (2007) [16] πρότειναν μία δομή εφαρμογής για την συλλογή πληροφοριών περιβάλλοντος, με επίγνωση πλαισίου, η οποία αξιοποιεί την τεχνολογία άμεσης αποστολής και λήψης μηνυμάτων, σε συνδυασμό με δεδομένα αισθητήρων, πρωτόκολλα επικοινωνίας καθώς και την διεπαφή προγραμματισμού εφαρμογών.

Διερευνώντας τη σημασία της έννοιας του πλαισίου, συμπεραίνουμε ότι αφορά στις προτιμήσεις των χρηστών, την τοποθεσία τους και την γενικότερη επίγνωση του περιβάλλοντα χώρου στον οποίο βρίσκονται. Η επίγνωση του πλαισίου προκύπτει από πληροφορίες που σχετίζονται με τον καιρό, το κλίμα, την κυκλοφοριακή συμφόρηση, την ώρα ή τη φυσική τοποθεσία ενός χρήστη. Άλλες πληροφορίες θα μπορούσαν να σχετίζονται με την συσκευή αυτή καθ' εαυτή, όπως με το επίπεδο της μπαταρίας της, το διαθέσιμο εύρος ζώνης του δικτύου στο οποίο συνδέεται ή τις διαθέσιμες WiFi υποδομές του χώρου στον οποίο βρίσκεται [17].

Μεταβαίνοντας από την ευρύτερη έννοια της επίγνωσης πλαισίου στην υπολογιστική επίγνωση πλαισίου διαπιστώνουμε ότι αυτή αφορά στο υπολογιστικό περιβάλλον, το οποίο έχει ενσωματωμένες πληροφορίες για το πλαίσιο της υπολογιστικής συσκευής, της υπολογιστικής υποδομής ή του χρήστη. Υπολογιστική συσκευή θεωρείται οποιαδήποτε συσκευή, συμπεριλαμβανομένων των έξυπνων κινητών τηλεφώνων (Smartphones), Tablets, Wearables, drones ή παραδοσιακές συσκευές όπως φορητοί υπολογιστές ή υπολογιστές γραφείου. Μία υπολογιστική υποδομή μπορεί να περιλαμβάνει Hardware, software, εφαρμογές εύρος ζώνης δικτύου WiFi bandwidth profiles ή πληροφορίες όπως τα επίπεδα της μπαταρίας της [18].

Ένα έξυπνο τηλέφωνο για παράδειγμα είναι μία υπολογιστική συσκευή που έχει επίγνωση του περιβάλλοντός του. Η υπολογιστική υποδομή του, που αποτελεί το λειτουργικό του σύστημα, αποκτά αυτό το πλαίσιο, το αποθηκεύει και το επεξεργάζεται. Στη συνέχεια, αλληλοεπιδρά με αυτό, μεταβάλλοντας και προσαρμόζοντας είτε τη λειτουργικότητα του. είτε τη συμπεριφορά του. Ακόμα μπορεί να λάβει κάποιες αποφάσεις έχοντας την επίγνωση του πλαισίου [17].

Η υπολογιστική υποδομή μπορεί να επεξεργαστεί την πληροφορία αυτή και να ανταποκριθεί στο περιβάλλον με ελάχιστες παρεμβάσεις από το χρήστη. Μερικά παραδείγματα αυτής της συμπεριφοράς είναι τα ακόλουθα:

- Ένα έξυπνο κινητό τηλέφωνο μπορεί να εντοπίσει ότι βρίσκεται σε ένα πολυσύχναστο μέρος, όπως ένα αεροδρόμιο, ένας σιδηροδρομικός σταθμός ή ένα εμπορικό κέντρο και αυτόματα να αλλάξει την συμπεριφορά της συσκευής εφαρμόζοντας αλγορίθμους μείωσης θορύβου, έτσι ώστε να μπορεί να ανταποκριθεί καλύτερα σε ενδεχόμενες φωνητικές εντολές του χρήστη.
- Ένα έξυπνο κινητό τηλέφωνο λαμβάνοντας υπόψιν την τοποθεσία ενός χρήστη μπορεί να εφαρμόσει αλλαγή στη λειτουργικότητα του, όπως για παράδειγμα την αυτόματη μείωση ή αύξηση της έντασης του ηχείου ή τη μεταβολή στην αθόρυβη λειτουργία ανάλογα με το αν είναι στο γραφείο ή στο σπίτι ή αν ταξιδεύει με αυτοκίνητο.
- Τα κινητά τηλέφωνα μπορούν αυτόματα να ανταποκριθούν σε συγκεκριμένες κλήσεις, στέλνοντας για παράδειγμα ένα μήνυμα ανάλογα με το αν ο χρήστης βρίσκεται στον χώρο εργασίας του ή οδηγεί. Θα μπορούσε επίσης να απορρίψει κάποιες κλήσεις βασισμένο στην εκάστοτε τοποθεσία του χρήστη.
- Τα έξυπνα ρολόγια χρησιμοποιώντας τον αισθητήρα εγγύτητας, σε περίπτωση που αντιληφθούν πτώση του χρήστη συνοδευόμενη από την απουσία άλλων κινήσεων από την πλευρά του, ειδοποιούν σε συνεργασία με το κινητό του τηλέφωνο και την τοποθεσία του, την κοντινότερη αρμόδια υπηρεσία.
- Παραδοσιακές ή σύγχρονες έξυπνες συσκευές μπορούν να χρησιμοποιήσουν υπηρεσίες τοποθεσίας προκειμένου να προτείνουν στον χρήστη εστιατόρια, κέντρα ψυχαγωγίας ή ακόμα και πλησιέστερα νοσοκομεία σε επείγουσες περιπτώσεις [18].

Στην υπολογιστική με επίγνωση πλαισίου εντοπίζονται τρία διαφορετικά επίπεδα αλληλεπίδρασης:

- Εξατομικευμένη επίγνωση πλαισίου : Οι χρήστες μπορούν να καθορίσουν τις δικές τους προτιμήσεις προκειμένου να μπορούν να ελέγχουν τη συμπεριφορά της εφαρμογής με επίγνωση πλαισίου, ανάλογα την περίσταση.

- Παθητική επίγνωση πλαισίου: Σε αυτή την περίπτωση η υποδομή επίγνωσης πλαισίου παρέχει στον χρήστη πληροφορίες από τους αισθητήρες ή αλλαγές που έχουν παρέλθει από προηγούμενο περιβάλλον χωρίς να δρα η να αλλάζει τη συμπεριφορά της συσκευής ανάλογα με αυτές. Ο χρήστης αποφασίζει για τις ενέργειες στις οποίες θα προβεί ανάλογα με τις πληροφορίες πλαισίου που έχει λάβει.
- Ενεργητική επίγνωση περιβάλλοντος Εν προκειμένω η υποδομή επίγνωσης περιβάλλοντος συλλέγει επεξεργάζεται και λαμβάνει όλες τις απαιτούμενες ενέργειες, βάσει των πληροφοριών που έχει δεχτεί. Ο χρήστης δεν απαιτείται να πραγματοποιήσει καμία ενέργεια, καθώς όλες οι λογικές αποφάσεις καθορίζονται από αυτήν [18].

Παρατηρήσαμε πως ο στόχος της πανταχού παρούσας υπολογιστικής είναι να ενισχύσει και να βοηθήσει την καθημερινότητα των ανθρώπων. Δυστυχώς, όμως, οι συσκευές με επίγνωση περιβάλλοντος ενός ατόμου ή οργανισμού μπορούν να χρησιμοποιηθούν για την εξαγωγή εξαιρετικά ιδιωτικών πληροφοριών. Ως εκ τούτου, οι συσκευές αυτές πρέπει να σχεδιαστούν προσεκτικά, διαφορετικά αυτή η ιδέα μπορεί να μετατραπεί σε ένα πανταχού παρόν σύστημα επιτήρησης. Κατά συνέπεια, τα υφιστάμενα υπερσύγχρονα συστήματα πρέπει να εξεταστούν υπό το πρίσμα επιθέσεων που μπορούν πιθανόν να δεχτούν τα ίδια, αλλά και να προξενήσουν σε οντότητες και οργανισμούς του περιβάλλοντός τους.

Κεφάλαιο 3

Η εξέλιξη των ασύρματων δικτύων

Δεδομένης της σημαντικότητας της πανταχού παρούσας υπολογιστικής στον αιώνα που διανύουμε, η ασύρματη επικοινωνία είναι μια εφαρμογή της επιστήμης και της τεχνολογίας που έχει καταστεί ζωτικής σημασίας για την λειτουργία της στην σύγχρονη ύπαρξη. Από το πρώιμο ραδιόφωνο και το τηλέφωνο μέχρι τις σύγχρονες συσκευές όπως τα κινητά τηλέφωνα και τους φορητούς υπολογιστές, η ανάγκη των ανθρώπων για ασύρματη πρόσβαση στο παγκόσμιο δίκτυο έχει μετατραπεί σε ουσιαστικό και αναπόσπαστο κομμάτι της ζωής τους. Τα ασύρματα δίκτυα αποτελούν ένα συνεχώς αναπτυσσόμενο πεδίο και χάρη σ' αυτά οι δυνατότητες των ανθρώπων συνεχώς διευρύνονται. Μία από τις κύριες επιφυλάξεις του μέλλοντος στον τομέα των ασύρματων δικτύων είναι η δυνατότητα ανταλλαγής μεγαλύτερου όγκου δεδομένων με μεγαλύτερη ασφάλεια [19].

Οι ασύρματες επικοινωνίες είναι αδιαμφισβήτητα το ταχύτερα αναπτυσσόμενο τμήμα της βιομηχανίας των Επικοινωνιών και αυτό είναι ο λόγος για τον οποίο έχει τραβήξει την προσοχή των μέσων ενημέρωσης και της φαντασίας του κοινού. Τα κυψελοειδή συστήματα γνώρισαν εκθετική αύξηση κατά την τελευταία δεκαετία και σήμερα υπάρχουν περίπου 2 δισεκατομμύρια χρήστες παγκοσμίως που χρησιμοποιούν τις υπηρεσίες τους. Πράγματι, οι κινητές και ασύρματες συσκευές, αποτελούν ένα κρίσιμο επιχειρηματικό εργαλείο και μέρος της καθημερινής ζωής στις περισσότερες ανεπτυγμένες χώρες, καθιστώντας γρήγορα τα απαρχαιωμένα πλέον καλωδιακά συστήματα. Επιπλέον τα ασύρματα τοπικά δίκτυα συμπληρώνουν ή αντικαθιστούν τα ενσύρματα σε πολλά σπίτια, επιχειρήσεις ή πανεπιστημιακούς χώρους. Πολλές νέες εφαρμογές συμπεριλαμβανομένων των ασύρματων δικτύων αισθητήρων, των αυτόνομων αυτοκινητοδρόμων και εργοστασίων, των έξυπνων κατοικιών καθώς και της εξ αποστάσεως τηλεϊατρικής αναδύονται από ερευνητικές ιδέες και εφαρμόζονται

σε πολλούς τομείς της καθημερινής ζωής [20].

Τα πρώτα ασύρματα δίκτυα αναπτύχθηκαν στην Προ-βιομηχανική εποχή. Αυτά τα συστήματα μεταδίδουν πληροφορίες μέσω των ορατών αποστάσεων (που επεκτάθηκαν αργότερα με τηλεσκόπια) χρησιμοποιώντας σήματα καπνού, σηματοδότηση πυρσού, κάτοπτρα που αναβοσβήνουν, σηματοδότες σήματος ή σημαίες σηματοφόρου. Ένα περίπλοκο σύνολο συνδυασμών σημάτων αναπτύχθηκε για να μεταφέρει σύνθετα μηνύματα με αυτά τα στοιχειώδη σήματα. Οι σταθμοί παρατήρησης χτίστηκαν σε λόφους και κατά μήκος δρόμων για να μεταδίδουν αυτά τα μηνύματα σε μεγάλες αποστάσεις. Αυτά τα πρώτα δίκτυα επικοινωνίας αντικαταστάθηκαν πρώτα από το τηλεγραφικό δίκτυο (που εφευρέθηκε από τον Samuel Morse το 1838) και αργότερα από το τηλέφωνο. Το 1895, λίγες δεκαετίες μετά την εφεύρεση του τηλεφώνου, ο Marconi παρουσίασε την πρώτη μετάδοση από το Isle of Wight σε ένα ρυμουλκό 18 χιλιόμετρα μακριά και γεννήθηκαν ραδιοεπικοινωνίες. Το πρώτο δίκτυο που βασίζεται στο ραδιόφωνο πακέτων, το ALOHANET, αναπτύχθηκε στο Πανεπιστήμιο της Χαβάης το 1971. Το δίκτυο αυτό επέτρεψε τη χρήση ηλεκτρονικών υπολογιστών σε επτά πανεπιστημιουπόλεις σε τέσσερα νησιά για επικοινωνία με κεντρικό υπολογιστή στο Oahu μέσω ραδιοφωνικής μετάδοσης. Η αρχιτεκτονική δικτύου χρησιμοποίησε μια τοπολογία αστέρα με τον κεντρικό υπολογιστή στο κέντρο της. Ο στρατός των Η.Π.Α. ενδιαφέρθηκε εξαιρετικά για το συνδυασμό πακέτων δεδομένων και ραδιοφωνικών εκπομπών που ενυπάρχουν στην ALOHANET. Καθ' όλη τη δεκαετία του 1970 και στις αρχές της δεκαετίας του 1980, η Υπηρεσία Προηγμένων Έργων Έρευνας για την Άμυνα (DARPA) επένδυσε σημαντικούς πόρους για την ανάπτυξη δικτύων χρησιμοποιώντας ραδιόφωνα πακέτων για τακτικές επικοινωνίες στο πεδίο της μάχης [21].

Τα δίκτυα ραδιοσυχνοτήτων πακέτων βρήκαν επίσης εμπορική εφαρμογή για την υποστήριξη ασύρματων υπηρεσιών δεδομένων ευρείας περιοχής. Αυτές οι υπηρεσίες, που εισήχθησαν για πρώτη φορά στις αρχές της δεκαετίας του 1990, επιτρέπουν την ασύρματη πρόσβαση σε δεδομένα (συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου, της μεταφοράς αρχείων και της περιήγησης στο διαδίκτυο) με σχετικά χαμηλές ταχύτητες, της τάξης των 20 Kbps. Η εισαγωγή της ενσύρματης τεχνολογίας Ethernet στη δεκαετία του '70 οδήγησε πολλές εμπορικές εταιρείες μακριά από τη ραδιοφωνική δικτύωση [22].

Το 1985, η Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) επέτρεψε την εμπορική ανάπτυξη ασύρματων τοπικών δικτύων, κάνοντας αποδεκτή τη δημόσια

χρήση των ζωνών συχνοτήτων βιομηχανικών, επιστημονικών και ιατρικών (ISM) για προϊόντα ασύρματου LAN. Η μπάντα ISM ήταν πολύ ελκυστική για τους πωλητές ασύρματου LAN, δεδομένου ότι δεν χρειάστηκε να αποκτήσουν άδεια FCC για να λειτουργήσουν σε αυτή τη μπάντα. Επιπλέον, η παρεμβολή από τους πρωτογενείς χρήστες εντός αυτής της ζώνης συχνοτήτων ήταν αρκετά υψηλή. Ως αποτέλεσμα, αυτά τα αρχικά ασύρματα δίκτυα LAN είχαν πολύ χαμηλή απόδοση όσον αφορά στα ποσοστά δεδομένων και την κάλυψη [21].

Η τρέχουσα γενιά ασύρματων τοπικών δικτύων, βασισμένη στην οικογένεια των προτύπων IEEE 802.11., προσφέρουν ταχύτητες δεδομένων 100 Mbps και το χάσμα απόδοσης μεταξύ ενσύρματων και ασύρματων τοπικών δικτύων είναι πιθανό να αυξηθεί με την πάροδο του χρόνου χωρίς πρόσθετη κατανομή φάσματος. Παρά τις μεγάλες διαφορές των ποσοστών δεδομένων, τα ασύρματα δίκτυα LAN καθίστανται η προτιμώμενη μέθοδος πρόσβασης στο Διαδίκτυο σε πολλά περιβάλλοντα κατοικιών, γραφείων και πανεπιστημιουπόλεων λόγω της ευκολίας και της ελευθερίας τους από τα καλώδια. Ωστόσο, τα περισσότερα ασύρματα δίκτυα LAN υποστηρίζουν εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο και η περιήγηση στο Web που δεν απαιτούν εύρος ζώνης [23].

Η πιο επιτυχημένη εφαρμογή της ασύρματης δικτύωσης είναι το κινητό τηλεφωνικό σύστημα. Οι ρίζες αυτού του συστήματος ξεκίνησαν το 1915, όταν εγκαταστάθηκε για πρώτη φορά η ασύρματη μετάδοση φωνής μεταξύ Νέας Υόρκης και στο Σαν Φρανσίσκο. Το 1946, η δημόσια υπηρεσία κινητής τηλεφωνίας εισήχθη σε 25 πόλεις στις Ηνωμένες Πολιτείες: τριάντα χρόνια μετά την εισαγωγή της υπηρεσίας κινητής τηλεφωνίας το σύστημα της Νέας Υόρκης μπορούσε να υποστηρίξει μόνο 543 χρήστες. Μια λύση σε αυτό το πρόβλημα χωρητικότητας προέκυψε κατά τη δεκαετία του '50 και του '60, όταν οι ερευνητές της AT & T Bell Laboratories ανέπτυξαν την κυτταρική έννοια. Το 1947 η AT & T ζήτησε φάσμα για κυψελοειδή υπηρεσία από την FCC. Ο σχεδιασμός ολοκληρώθηκε ως επί το πλείστον μέχρι τα τέλη της δεκαετίας του 1960, η πρώτη δοκιμή πεδίου ήταν το 1978 και η FCC χορήγησε άδεια λειτουργίας το 1982 [22].

Το όραμα των ασύρματων επικοινωνιών που υποστηρίζουν την ανταλλαγή πληροφοριών μεταξύ ανθρώπων ή συσκευών είναι τα σύνορα επικοινωνίας των επόμενων δεκαετιών και πολλά από αυτά ήδη υπάρχουν με κάποια μορφή. Αυτό το όραμα θα επιτρέψει την επικοινωνία πολυμέσων από οπουδήποτε στον κόσμο χρησιμοποιώντας μια μικρή φορητή συσκευή ή έναν φορητό υπολογιστή. Τα ασύρματα

δίκτυα θα συνδέουν palmtop, φορητό υπολογιστή και επιτραπέζιους υπολογιστές οπουδήποτε μέσα σε ένα κτίριο γραφείων ή πανεπιστημιούπολη, καθώς και από το γωνιακό καφέ. Στο σπίτι αυτά τα δίκτυα θα επιτρέψουν μια νέα κατηγορία ευφυών ηλεκτρονικών συσκευών που μπορούν να αλληλεπιδρούν μεταξύ τους και με το Διαδίκτυο, πέρα από την παροχή σύνδεσης μεταξύ υπολογιστών, τηλεφώνων και συστημάτων ασφαλείας παρακολούθησης. Τέτοια έξυπνα σπίτια μπορούν επίσης να βοηθήσουν τους ηλικιωμένους και τα άτομα με αναπηρία με υποβοηθούμενη διαβίωση, παρακολούθηση ασθενών και αντιμετώπιση έκτακτης ανάγκης. Η ασύρματη ψυχαγωγία θα διαπεράσει το σπίτι και οπουδήποτε συγκεντρωθούν οι άνθρωποι. Η τηλεδιάσκεψη βίντεο θα πραγματοποιηθεί ανάμεσα σε κτήρια που είναι χωριστά ή σε διαφορετικές ηπείρους και αυτά τα συνέδρια μπορούν να περιλαμβάνουν και τους ταξιδιώτες, από τον πωλητή που έχασε τη σύνδεση αεροσκάφους με τον διευθύνοντα σύμβουλο από την ιστιοπλοΐα στην Καραϊβική. Το ασύρματο βίντεο θα επιτρέψει σε απομακρυσμένες αίθουσες διδασκαλίας, απομακρυσμένες εγκαταστάσεις εκπαίδευσης και απομακρυσμένα νοσοκομεία οπουδήποτε στον κόσμο. Οι ασύρματες αισθητήρες διαθέτουν ένα τεράστιο φάσμα εμπορικών και στρατιωτικών εφαρμογών. Οι εμπορικές εφαρμογές περιλαμβάνουν την παρακολούθηση των κινδύνων πυρκαγιάς, των χώρων επικίνδυνων αποβλήτων, το άγχος και την τάση σε κτίρια και γέφυρες, την κίνηση του διοξειδίου του άνθρακα και την εξάπλωση χημικών ουσιών και αερίων σε χώρο καταστροφής. Αυτοί οι ασύρματοι αισθητήρες αυτο-διαμορφώνονται σε ένα δίκτυο για να επεξεργάζονται και να ερμηνεύουν τις μετρήσεις των αισθητήρων και στη συνέχεια να μεταφέρουν αυτές τις πληροφορίες σε μια κεντρική θέση ελέγχου. Οι στρατιωτικές εφαρμογές περιλαμβάνουν τον εντοπισμό στόχων του εχθρού, τον εντοπισμό χημικών και βιολογικών επιθέσεων, την υποστήριξη μη επανδρωμένων ρομποτικών οχημάτων και την καταπολέμηση της τρομοκρατίας. Τέλος, τα ασύρματα δίκτυα επιτρέπουν κατανεμημένα συστήματα ελέγχου, με απομακρυσμένες συσκευές και αισθητήρες συνδεδεμένους μεταξύ τους μέσω ασύρματων καναλιών επικοινωνίας. Τέτοια δίκτυα επιτρέπουν αυτοματοποιημένους αυτοκινητόδρομους, κινητά ρομπότ και βιομηχανικά αυτοματισμούς που μπορούν εύκολα να αναδιαμορφωθούν [24].

Προκειμένου να αναλυθεί η σημασία των ασύρματων δικτύων είναι σημαντικό να αποσαφηνιστεί εννοιολογικά ο όρος δίκτυο υπολογιστών. Το δίκτυο υπολογιστών ή τηλεπικοινωνιακό δίκτυο αποτελεί τη διασύνδεση αυτόνομων ή μη αυτόνομων υπολογιστικών συστημάτων μεταξύ τους. Προκειμένου ένας υπολογιστής να θεωρείται συνδεδεμένος με κάποιον άλλον αρκεί να μπορεί να ανταλλάσσει πληροφορία με

αυτόν, και βασική προϋπόθεση για να θεωρηθεί αυτόνομος είναι να μην επιτρέπεται σε κανέναν άλλον υπολογιστή να τον ελέγχει. Ένα ενσύρματο δίκτυο αποτελείται από τη διασύνδεση δύο ή περισσότερων υπολογιστών, εκτυπωτών, και άλλων μηχανημάτων μέσω Ethernet καλωδίων. Το πρωτόκολλο ethernet είναι το γρηγορότερο πρωτόκολλο ενσύρματης ζεύξης με ταχύτητες από 10 megabits το δευτερόλεπτο μέχρι 1 Gigabit το δευτερόλεπτο. Βασική προϋπόθεση των συσκευών που συνδέονται στο δίκτυο χρησιμοποιώντας αυτή τη τεχνολογία, είναι η ενσωματωμένης σ ε αυτά κάρτας δικτύου Ethernet [25].

Η έννοια της δικτύωσης συσκευών, ήρθε στο φως με τον πρωταρχικό σκοπό της μείωση των υπολογιστικών πόρων και της προώθησης της αποτελεσματικότερης χρήσης των ήδη υπαρχόντων και περιορισμένων πόρων. Με την έννοια των υπολογιστικών πόρων εννοούνται οι πληροφορίες δεδομένων, το hardware των υπολογιστικών συστημάτων όπως οι σκληροί δίσκοι η μνήμες, οι εκτυπωτές κ.α. Πριν την εμφάνιση των δικτύων δεν υπήρχε ανταλλαγή δεδομένων μεταξύ των Συστημάτων και κάθε αυτόνομο υπολογιστικό σύστημα χρησιμοποιούσε τους δικούς του υπολογιστικούς πόρους με τους οποίους ήταν άμεσα συνδεδεμένο, κάτι που οδηγούσε σε μη αποτελεσματική χρήση αυτών. Όταν ο συγκεκριμένος υπολογιστής δεν χρησιμοποιούσε τους πόρους αυτούς, αυτοί παρέμεναν σε κατάσταση αναμονής, παρόλο που κάποιος άλλος υπολογιστής στον χώρο ενδεχομένως να μπορούσε να τους χρησιμοποιήσει. Προκειμένου να αναληφθεί αυτή η μη αποτελεσματική χρήση των πόρων, παρουσιάστηκε η έννοια του διαμοιρασμού τους, μεταξύ πολλαπλών συστημάτων για την αποτελεσματική πλέον χρήση τους μεταξύ διαφορετικών υπολογιστών. Η έννοια αυτή επιτεύχθηκε μέσω της δικτύωσης ή της διασύνδεσης των Συστημάτων μεταξύ τους, βασιζόμενη σε διαφορετικές αρχιτεκτονικές δικτύου[26].

Τα δίκτυα κατηγοριοποιούνται με βάση κάποια ειδικά χαρακτηριστικά τους, σε δημόσια ή ιδιωτικά, ανάλογα με τον τρόπο πρόσβασης σε αυτά, σε τοπικά, μητροπολιτικά ευρείας κάλυψης και προσωπικά, ανάλογα με τη γεωγραφική εμβέλεια που μπορούν να καλύψουν και τέλος στα ενσύρματα ή ασύρματα όπου η κατηγοριοποίηση γίνεται ανάλογα με το φυσικό μέσο που αξιοποιείται για τηλεδιασύνδεσής τους [27].

Ένα τοπικό δίκτυο αποτελείται από τον Διακομιστή (Server) και τους Πελάτες (Clients). Σαν διακομιστής χρησιμοποιείται ένας υπολογιστής ισχυρών τεχνικών χαρακτηριστικών, επειδή ουσιαστικά είναι ο εγκέφαλος του δικτύου. Ειδικότερα, σε αυτόν συνδέονται όλες οι συσκευές που απαρτίζουν το εκάστοτε δίκτυο,

εγκαθίστασντε όλες οι εφαρμογές και τα προγράμματα που χρησιμοποιούνται στο δίκτυο, και αποθηκεύονται όλα τα αρχεία του δικτύου. Ένας Server συνήθως δουλεύει αδιάκοπα, ώστε να βρίσκεται ανά πάσα στιγμή στη θέση να εξυπηρετήσει τους Clients. Γι' αυτό, το λόγο είναι τοποθετημένος σε ένα ειδικό μεταλλικό κουτί, το Rack, το οποίο διαθέτει πολύ καλή παροχή εξαερισμού και ψύξης. Τέλος, είναι συνδεδεμένος πάντα σε μια συσκευή αδιάλειπτης παροχής ρεύματος, το UPS, ώστε να είναι σε θέση να εξυπηρετήσει σε περίπτωση διακοπής ρεύματος. Οι Clients είναι υπολογιστές ανεξαρτήτου ισχύος και απόδοσης και συνδέονται με τον Server για να τρέξουν προγράμματα, να μεταφέρουν αρχεία, για να συνδεθούν στο διαδίκτυο και για όποιο άλλο λόγο χρειαστούν [27].

Είναι προφανές ότι για να μεταδοθεί η κάθε πληροφορία από την Πηγή στον προορισμό της απαιτείται κάποιο μέσο μετάδοσης που δίνει τη δυνατότητα να σταλεί η οποιαδήποτε πληροφορία. Τα ενσύρματα μέσα διάδοσης έβρισκαν αποκλειστική χρησιμότητα στα τηλεπικοινωνιακά δίκτυα μέχρι να κάνουν την εμφάνισή τους τα ασύρματα μέσα μετάδοσης. Τα ασύρματα δίκτυα αξιοποιούν όλες τις παραπάνω ιδιότητες των απλών δικτύων, χωρίς τους περιορισμούς των καλωδίων. Ο Clark et al, 1998 όρισε το ασύρματο δίκτυο ως ένα κλειστό δίκτυο, γεωγραφικά περιορισμένο. Ένα τοπικό ασύρματο δίκτυο παρέχει υψηλού εύρους ζώνης επικοινωνία μέσω του φτηνού ασύρματου μέσου. Η ερμηνεία που δόθηκε από τον Flickengen το 2005 είναι πως το ασύρματο δίκτυο αποτελεί μία ομάδα από ασύρματα σημεία πρόσβασης και τις σχετικής με αυτά υποδομής σε μία περιορισμένη γεωγραφική έκταση όπως ένα κτήριο ή έναν οργανισμό κτηρίων. Το τοπικό ασύρματο δίκτυο (wlan) συνδέει μεταξύ τους δύο ή περισσότερες συσκευές που χρησιμοποιούν την μέθοδο της ασύρματης επικοινωνίας. Αυτό δίνει την δυνατότητα στους χρήστες να κινούνται με ευελιξία στο χώρο κάλυψης του δικτύου παραμένοντας συνδεδεμένοι σε αυτό. Ακριβώς με τον ίδιο τρόπο που ένα έξυπνο κινητό τηλέφωνο παρέχει στους χρήστες του τη δυνατότητα να επικοινωνούν οπουδήποτε και αν βρίσκονται στον κόσμο, έτσι και το τοπικό ασύρματο δίκτυο επιτρέπει στους χρήστες του να χρησιμοποιούν την συσκευή τους σε οποιοδήποτε σημείο της περιοχής κάλυψης [28].

3.1 Ασύρματη έναντι ενσύρματης δικτύωσης

Στην ορολογία των υπολογιστών, ο όρος ενσύρματο χρησιμοποιείται για να διαφοροποιήσει της ασύρματες συνδέσεις με αυτές που χρησιμοποιούν καλώδια. Μία ενσύρματη εγκατάσταση χρησιμοποιεί φυσικά καλώδια για την μεταφορά της πληροφορίας μεταξύ διαφορετικών συσκευών και υπολογιστικών συστημάτων. Τα περισσότερα ενσύρματα δίκτυα χρησιμοποιούν Ethernet καλώδια για να μεταφέρουν την πληροφορία μεταξύ συνδεδεμένων υπολογιστών. Σε ένα μικρό ενσύρματο δίκτυο ένας μοναδικός διαμοιραστής Router χρησιμοποιείται για να συνδέσει όλους τους υπολογιστές μεταξύ τους, ενώ μεγαλύτερα δίκτυα συνήθως χρησιμοποιούνται πολλαπλοί Routers ή Switches που συνδέονται μεταξύ τους. Μία από όλες αυτές τις συσκευές δικτύου, συνδέεται με ένα modem το οποίο παρέχει σε όλο το δίκτυο πρόσβαση στον ευρύτερο κοινό δίκτυο (Internet) [29].

Ως σύγχρονο ασύρματο δίκτυο εννοούμε την χρήση σημάτων υπέρυθρης ακτινοβολίας η ραδιοκυμάτων για τον διαμοιρασμό της πληροφορίας και των πόρων, μεταξύ των συσκευών ενός χώρου. Πολλοί τύποι ασύρματων συσκευών είναι διαθέσιμοι σήμερα, όπως ασύρματα κινητά τηλέφωνα, υπολογιστές τσέπης, υπολογιστές χειρός, tablets, ασύρματοι αισθητήρες, δορυφορική δέκτες κ.α. Τα πέμπτης γενιάς δίκτυα κινητής τηλεφωνίας έχουν εξελίξει σε μεγάλο βαθμό την ταχύτητα μεταφοράς δεδομένων κάτι που επιτρέπει την ανάπτυξη μίας νέας εποχής εφαρμογών όπου η ταχύτητα μεταφοράς δεδομένων εφαρμόζει καθοριστικό ρόλο. Εντωμεταξύ standards όπως το 802.11 πρωτόκολλο, το bluetooth, το hyperplane και η υπέρυθρη μετάδοση, συνεπάγονται τη δημιουργία ενός ευρέος δικτύου με νέες εφαρμογές για οικιακή ή εταιρική χρήση επιτρέποντας τις ασύρματες υπηρεσίες πολυμέσων και μεταφοράς δεδομένων[30].

Τα ενσύρματα δίκτυα χωρίζονται σε δύο κατηγορίες, σε Δίκτυο Τοπικής Εμβέλειας (LAN – Local Area Network), και σε Δίκτυο Εκτεταμένης Εμβέλειας (WAN – Wide Area Network). Το τοπικό δίκτυο (LAN) συντελείται από μία μικρή ομάδα υπολογιστών, οι οποίοι είναι συνδεδεμένοι με ειδικά καλώδια δικτύου, τα λεγόμενα UTP (Unshielded Twisted Pair) και έχουν περιορισμένη γεωγραφική εμβέλεια λειτουργίας. Τα δίκτυα αυτά είναι ιδιωτικά και χρησιμοποιούνται κυρίως για να

συνδέσουν προσωπικούς υπολογιστές με σκοπό την ανταλλαγή πληροφοριών ή την κοινή χρήση συσκευών, για παράδειγμα εκτυπωτών. Τα κλασσικά LAN λειτουργούν συνήθως σε ταχύτητες των 10 έως 100 Mbps και παρουσιάζουν πολύ καλή ποιότητα στη μετάδοση πληροφορίας. Τα πιο προηγμένα LAN έχουν τη δυνατότητα να λειτουργήσουν σε υψηλότερες ταχύτητες, καθώς έχουν βελτιωθεί τα μέσα μετάδοσής τους [31].

Είναι αντιληπτό πως οι περισσότερες επιχειρήσεις επιθυμούν να παραμείνουν πιστές στη χρήση της ενσύρματης διασύνδεσης των υπολογιστών του δικτύου τους. Ο λόγος είναι πως τα ενσύρματα δίκτυα παρέχουν μεγαλύτερο έλεγχο, ασφάλεια και αξιοπιστία. Αυτό οφείλεται στο γεγονός ότι στην καλωδιακή δικτύωση, προκειμένου να συνδεθεί κάποιος στο δίκτυο απαιτείται φυσική πρόσβαση, κάτι το οποίο μπορεί εύκολα να αποτραπεί στο πρώτο επίπεδο ασφαλείας ενός οργανισμού. Παράλληλα, το κόστος του εξοπλισμού των ενσύρματων δικτύων είναι αρκετά μειωμένο συγκριτικά με παλαιότερα, κάτι που καθιστά τα ενσύρματα δίκτυα ως την πιο συμφέρουσα επιλογή ενός οργανισμού [32].

Ανεξάρτητα από τα πλεονεκτήματα τον ενσύρματων δικτύων στον διαχειριστικό τομέα, η παρουσία του μεγάλου όγκου καλωδίων απαιτεί πολύ χρόνο και κόστος προκειμένου να συντηρηθεί ή να επεκταθεί, όπως σε σενάρια ενίσχυσης εργατικού δυναμικού ή επιδιόρθωση τυχόν φθαρμένων καλωδίων. Τα κύρια πλεονεκτήματα των ασύρματων δικτύων συγκριτικά με τα ενσύρματα είναι η κινητικότητα, η ευκαμψία, και η ευκολία εγκατάστασης και συντήρησης τους. Σύμφωνα με την (Symantec, 2002) τα ασύρματα δίκτυα είναι σε γενικότερο πλαίσιο φθηνότερα και λιγότερο "ενοχλητικά" στην εφαρμογή και συντήρησή τους. Η απλή υλοποίηση, η εύκολη συντήρηση, καθώς και η επεκτασιμότητά τους, αυξάνουν την κινητικότητα των χρηστών τους καθώς μειώνουν το κόστος ιδιοκτησίας και λειτουργίας τους [33].

Σύμφωνα με τον Ibrahim Al Shourbaji τα ακόλουθα αποτελούν τα κυριότερα σημεία στα οποία τα ασύρματα δίκτυα υπερισχύουν έναντι των ενσύρματων :

1. Ο ολοένα και αυξανόμενος αριθμός των χρηστών που επιθυμούν πρόσβαση στο ενιαίο δίκτυο αυξάνεται. Δεδομένου της νέας πραγματικότητας της, ολοένα και περισσότερες συσκευές θα χρειάζονται συνεχή πρόσβαση στο ευρύ δίκτυο. Στο κοντινό μέλλον, κάθε άνθρωπος θα διαθέτει και θα χρησιμοποιεί

δεκάδες συσκευές ταυτόχρονα εξυπηρετώντας διαφορετικό σκοπό, ενώ αυτές θα απαιτούν την ταυτόχρονη σύνδεσή τους στο διαδίκτυο, κάτι που με την χρήση ενσύρματης τεχνολογίας είναι μη πρακτικό έως αδύνατο.

2. Η εγκατάσταση των ασύρματων δικτύων καθίσταται ευκολότερη δεδομένης της απουσίας καλωδίων και συνδέσμων μεταξύ των κόμβων. Αν και η εγκατάσταση ενός ασύρματου τοπικού δικτύου προϋποθέτει μεγαλύτερους οικονομικούς πόρους, η χρήση τους θεωρείται βέλτιστη σε περιπτώσεις όπου οι κόμβοι ενός δικτύου διευρύνονται σε μεγάλη γεωγραφική έκταση. Η παρουσία καλωδίων στην περίπτωση αυτή θα αποτελούσε μία αρκετά δαπανηρή και επίπονη εργασία προκειμένου να επιτευχθεί.
3. Στις περιπτώσεις δικτύων τα οποία ενδέχεται να επεκτείνονται συνεχώς, η χρήση ενσύρματων μέσων θα αποτελούσε μη αποδοτική διαδικασία για έναν οργανισμό. Η μελέτη και αρχιτεκτονική στην προσθήκη νέων κόμβων με την χρήση ασύρματων δικτύων είναι μία αρκετά απλούστερη διαδικασία συγκριτικά με την εγκατάσταση μεγάλης έκτασης καλωδιακού δικτύου.
4. Η καλωδιακή εγκατάσταση δυσπρόσιτων περιοχών συνήθως καθίσταται αδύνατη λόγω της κοστοβόρας μελέτης και εγκατάστασης καλωδίων μεταξύ των κόμβων. Η ασύρματη ζεύξη στις περιπτώσεις αυτές είναι αναγκαία καθώς με το ίδιο κόστος μπορεί να επιτευχθεί πολύ μεγαλύτερης έκτασης δικτυακή κάλυψη [34].
5. Σε περιοχές όπου η εγκατάσταση νέων καλωδιακών γραμμών δεν είναι δυνατή λόγω της γεωγραφικής ιδιαιτερότητας, η χρήση των ασύρματων δικτύων μπορεί να αποτελέσει μία αξιόπιστη εναλλακτική. Η διασύνδεση μεταξύ των κόμβων μπορεί να επιτευχθεί ανεξαρτήτως της γεωγραφικής ανωμαλίας του χώρου, συνδέοντας μεγάλες γεωγραφικές περιοχές μεταξύ τους [32].
6. Μολονότι το αρχικό κόστος εγκατάστασης ενός ασύρματου δικτύου μπορεί να είναι μεγαλύτερο από αυτό ενός ενσύρματου, εντούτοις η συντήρηση ενός ασύρματου είναι αισθητά μικρότερη και αυτό οφείλεται στην απουσία των φυσικών καλωδίων τα οποία λόγω της επαφής τους με το έδαφος σταδιακά διαβρώνονται [32].

Τα μακροχρόνια οφέλη της ασύρματης δικτύωσης την ανάγουν να είναι μία σημαντική και ουσιαστική αντικατάσταση των ήδη υπαρχόντων ενσύρματων δικτύων.

Αν και τα ασύρματα δίκτυα είναι ακριβά, όχι τόσο αξιόπιστα και πιο αργά σε σχέση με τα ενσύρματα, η μετάβαση στα ασύρματα είναι μεγάλης σημασίας για τους οργανισμούς όπου ο αριθμός των κόμβων ή των συμμετεχόντων ενός δικτύου δεν μπορεί προηγουμένως να υπολογιστεί. Η ευελιξία της προσθήκης νέων κόμβων χωρίς αισθητό επιπλέον κόστος για την εγκατάσταση και την σύνδεση του, αποτελεί τους βασικότερους λόγους που τα ασύρματα δίκτυα υπερισχύουν έναντι των ενσύρματων. [35].

3.2 Τεχνολογίες Ασύρματων δικτύων.

Οι εφαρμογές των συσκευών που χαρακτηρίζουν την πανταχού παρούσα υπολογιστική, προϋποθέτουν την ενσωμάτωση σε αυτές τεχνολογιών ασύρματης επικοινωνίας για την ανταλλαγή πληροφοριών στο διαδίκτυο. Το γεγονός της ύπαρξής τους δημιουργεί αμέτρητες επιχειρησιακές προοπτικές σε αρκετούς τομείς, όπως η ηλεκτρονικά καθοδηγούμενη περίθαλψη (e-health), τα έξυπνα σπίτια, η αυτόνομη οδήγηση κ.α. Υπάρχουν πολλές διαθέσιμες τεχνολογίες ασύρματου lan σήμερα, με διαφορετικά επίπεδα τυποποίησης και διαλειτουργικότητας πολλές εκδοχές αυτών που αξιοποιούνται από τη σημερινή βιομηχανία. Μερικές από τις πιο σημαντικές και διαδεδομένες είναι το ZigBee, το Bluetooth, καθώς και τις διαφορετικές εκδόσεις Wi-Fi συμπεριλαμβανομένου της 802.11ah έκδοσης. Συνδυαστικά, οι παραπάνω τεχνολογίες αποτελούν τη βάση για τον σχεδιασμό και την υλοποίηση εφαρμογών στα πλαίσια της πανταχού παρούσας [36].

- **IEEE 802.15.1 Bluetooth**

Το Bluetooth χαρακτηρίστηκε από τον οργανισμό Bluetooth Special Interest Group (Bluetooth SIG) ως μία τεχνολογία ασύρματης μεταξύ ασύρματων προσωπικών συσκευών σε μικρή εμβέλεια. Ανακοινώθηκε το 1999 και χρησιμοποιεί την ελεύθερη από τον νόμο ISM μπάντα συχνοτήτων των 2,45 Ghz και λόγω αυτού μπορεί να χρησιμοποιηθεί σε παγκόσμιο επίπεδο. Ο κύριος σκοπός του πρωτοκόλλου αυτού είναι να επιτρέπει την άμεση διασύνδεση δύο συσκευών κυρίως για την

ανταλλαγή δεδομένων μεταξύ τους. Η απόσταση στην οποία μπορεί να λειτουργήσει ποικίλει ανάλογα με την έκδοση του Bluetooth και στις σύγχρονες εφαρμογές αυτή δεν ξεπερνάει τα 10 μέτρα σε εξωτερικό χώρο, ενώ σε περιπτώσεις υψηλής ισχύος η απόσταση μπορεί φτάσει τα 100 μέτρα [37].

- **IEEE 802.15.4 Zigbee**

Το Zigbee είναι το πρωτόκολλο επικοινωνίας, ευρέως διαδεδομένο για την εφαρμογή του σε αισθητήρες ασύρματης επικοινωνίας. Αναπτύχθηκε από την ZigBee Alliance και τα χαρακτηριστικά του είναι η χαμηλή κατανάλωση ενέργειας, ο χαμηλός ρυθμός μετάδοσης δεδομένων, το χαμηλό κόστος αγοράς, η υψηλή απόκριση. Ταυτόχρονα είναι από στην κατασκευή του και παρέχει πολύ υψηλή ασφάλεια και αξιοπιστία δεδομένων. Το όνομά του προήλθε από τα Zigzagg μονοπάτια που ακολουθούν οι μέλισσες μεταξύ των λουλουδιών, πράγμα που αντιπροσωπεύει την επικοινωνία μεταξύ των κόμβων ενός δικτύου σε ένα mesh network (δίκτυο τύπου πλέγματος). Η ισχύς όπου απαιτείται για την λειτουργία του ZigBee είναι πολύ χαμηλή. Στις περισσότερες περιπτώσεις χρησιμοποιεί χαμηλότερη των 1mW ισχύ, αλλά εξακολουθεί να παρέχει επικοινωνία σε εμβέλεια έως και 150 μέτρα σε εξωτερικούς χώρους. Το μεγάλο μέγεθος της γεωγραφικής έκτασης στην οποία λειτουργεί επιτυγχάνεται με την μέθοδο διασποράς φάσματος DSSS η οποία καταναλώνει λιγότερη ισχύ σε σύγκριση με την FHSS. Οι συχνότητες λειτουργίας του είναι για την Ευρώπη τα 915 Mhz, ενώ για την Αμερική και την Αυστραλία λειτουργεί στα 868 Mhz. Ακόμα, μπορεί να λειτουργήσει παγκόσμια στις ISM συχνότητες των 2.4 Ghz με μέγιστη ταχύτητα μεταφοράς δεδομένων τα 250 Kbps. Λόγω της διαφορετική ζώνης κύματος που χρησιμοποιεί εν συγκρίσει με τα διαδεδομένα σημερινά ασύρματα δίκτυα, το ZigBee μπορεί λειτουργήσει παράλληλα με αυτά χωρίς την ύπαρξη αμοιβαίων παρεμβολών μεταξύ τους [38].

- **IEEE 802.11 (WiFi)**

Ενώ υπάρχουν αρκετές τεχνολογίες και πρωτόκολλα ασύρματης διασύνδεσης των φορητών συσκευών, με τα σημερινά δεδομένα το πρωτόκολλο 802.11 είναι το πιο ευρέως διαδεδομένο και εφαρμοσμένο μεταξύ αυτών . Τα τελευταία χρόνια η χρήση

του WLAN ως η προέκταση των ήδη υπαρχόντων. Το πρωτόκολλο αυτό χαρακτηρίζει δύο αρχιτεκτονικές δομές, την iBSS και τη BSS. Το iBSS αποτελείται από ένα σύστημα όπου ένας σταθμός βάσης αποτελεί την ομοιοκατευθυντική γέφυρα που ενώνει και καθοδηγεί τους σταθμούς (clients), δηλαδή της κινητές συσκευές να ανταλλάξουν πληροφορία με υπόλοιπο ενσύρματο δίκτυο και κατ' επέκταση το διαδίκτυο. Η πληροφορία αυτή αρχικά μεταδίδεται από τις κινητές μέσω του ασύρματου μέσου και σε δεύτερο χρόνο μέσω των σταθμών βάσεων προωθούνται στον ευρύ ιστό. Ως BSS ορίζεται το σύνολο των κινητών σταθμών μαζί με τον σταθμό βάσης με τον οποίο συσχετίζονται. Η ικανότητα των BSSs να συσχετίζονται μεταξύ τους (Distribution systems), παρέχει την δυνατότητα της ανάπτυξη μεγάλων ασύρματων δικτύων τα οποία μπορούν να επεκτείνουν γεωγραφικά τη δυνατότητα ασύρματης δικτύωσης συσκευών και στη συνέχεια την πρόσβασή τους στο ίντερνετ. Η WiFi τεχνολογία χρησιμοποιεί υψηλότερη ισχύ σήματος αλλά και πολλαπλές κεραίες συγκριτικά με άλλες παρόμοιες τεχνολογίες, κυρίως γιατί βασική της ανάγκη είναι να παρέχει όσο το δυνατόν μεγαλύτερη κάλυψη στον περιβάλλοντα χώρο. Οι κύριες μπάντες που αξιοποιεί η τεχνολογία αυτή είναι αυτή των 2.4 Ghz και των 5 Ghz. Οι κύριες διαφορές περιορίζονται στη χωρητικότητα της πληροφορίας που μπορεί να μεταφέρεται σε συνάρτηση με τον χρόνο και στην φυσική απόσταση που μπορεί να διανύσει ένα ραδιοκύμα σε συνάρτηση με την ισχύ εκπομπής του. Όσο λιγότερα είναι τα Hz της μετάδοσης τόσο λιγότερη και η πληροφορία που μπορεί να διαδοθεί ανά δευτερόλεπτο και αντίστοιχα τόσο μεγαλύτερη και η απόσταση που μπορεί να διανύσει το σήμα [39].

Κεφάλαιο 4
Το πρωτόκολλο 802.11

Οι δικτυακές τεχνολογίες ως επί το πλείστον εστιάζουν στις ενσύρματες λύσεις δικτύωσης. Ωστόσο, με την εισαγωγή των 802.11 προτύπων στην αγορά, συσκευές όπως, φορητοί υπολογιστές, tablets, και κινητά τηλέφωνα, γνώρισαν μεγάλη ανάπτυξη και εφαρμογή σε οικιακούς, εργασιακούς ή και δημόσιους χώρους, ενσωματώνοντας στο έπακρον την τεχνολογία της ασύρματης δικτύωσης. Το 802.11 αποτελεί την απαρχή μίας νέας εποχής στις ασύρματες επικοινωνίες και δημοσιεύτηκε τον Ιούνιο του 1997 από τον οργανισμό Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE), ως το πρώτο πρότυπο ασύρματων τοπικών δικτύων με συχνότητα εκπομπής σημάτων τα 2,4 Ghz και ρυθμούς μετάδοσης από 1 μέχρι 2 Mbps (Megabits per second). Το IEEE 802, αποτελεί την επιτροπή του IEEE, η οποία διερευνά την δικτύωση LAN (local area networks) και MAN (Metropolitan area networks) Το .11 αποτελεί ένα σύνολο από standards της ομάδας αυτής, υπεύθυνο για την ασύρματη δικτύωση των LAN δικτύων ή αλλιώς WLAN (wilress locan area Networks). Η ορολογία Wi-Fi (Wireless Fidelity) αποτελεί την εμπορική ονομασία που εξέλαβε το πρωτόκολλο και κύριος σκοπός του είναι η ασύρματη δικτύωση των συσκευών μεταξύ τους σε τοπικά ή μητροπολιτικά δίκτυα, καθώς και η πρόσβαση τους, μέσω αυτού, στο Internet [39].

Το 802.11, ως το πλέον ευρέως ανεπτυγμένο πρότυπο ασύρματης δικτύωσης, επεκτείνεται από την αρχή της εμφάνισής του σε διάφορες εκδοχές, με τα αρχικά πρότυπα να παρέχουν μέγιστο ρυθμό μεταφοράς δεδομένων της τάξης των 2Mpbs ανά Access Point. Προκειμένου να καλύψει τις συνεχώς αυξανόμενες ανάγκες για μεγαλύτερο ρυθμό μετάδοσης δεδομένων, το ινστιτούτο παρουσίασε το 802.11b το οποίο κάτω από το ίδιο φάσμα συχνοτήτων, επιτρέπει την ανταλλαγή πληροφορίας με ρυθμούς έως 11Mpbs. Τα προηγμένα πρότυπα IEEE 802.11a και 802.11b χρησιμοποιούν πιο πρόσφατες τεχνικές διαμόρφωσης, πετυχαίνοντας ακόμη μεγαλύτερους ρυθμούς μετάδοσης [40 -42].

Η πρώτη και πλέον απαρχαιωμένη εκδοχή του IEEE 802.11, ανακοινώθηκε το

1997 και είναι γνωστή ως 802.11 Legacy. Προβλέπει δύο ρυθμούς μετάδοσης, αυτούς των 1 και 2 Mpbs σε συχνότητες των 2.4 Ghz. Η εκπομπή της πληροφορίας ολοκληρωνόταν με την χρήση υπέρυθρων σημάτων τα οποία, όμως, απορρίφθηκαν στα πρότυπα που ακολούθησαν. Σε φυσικό επίπεδο ακολουθεί την τεχνική FHSS ή DSSS σε ζώνες συχνοτήτων 915MHz, 2.4MHz, 5.2MHz ή την υπέρυθρη μετάδοση στα 850nm ως 900nm. Υποστηρίζει δυνατότητες, όπως κατανομή προτεραιοτήτων της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής

- **IEEE 802.11a**

Το πρότυπο 802.11a έκανε την εμφάνισή του στην αγορά, ενώ το 802.11b είχε ήδη ένα μεγάλο μερίδιο αυτής. Ωστόσο, η τεχνολογία που χρησιμοποιεί προσφέρει αρκετά πλεονεκτήματα σε σχέση με αυτή του 802.11b. Συγκεκριμένα, χρησιμοποιεί τις μπάντες UNII στα 5 Ghz για μετάδοση που είναι γενικά πολύ λιγότερο χρησιμοποιούμενες από αυτές των 2,4 Ghz, οπότε και με λιγότερες παρεμβολές. Οι τρεις μπάντες UNII χωρίζονται με τρόπο ανάλογο της καταλληλόλητάς τους για μετάδοση σε εσωτερικά ή εξωτερικά περιβάλλοντα και επιτρέπουν την δημιουργία μακρινών ασύρματων ζεύξεων σε μεγάλες ταχύτητες. Το 802.11a παρέχει ταχύτητες μέχρι 54 mpbs, ωστόσο, είναι ωφέλιμο περί τα 25 mpbs, μια σημαντική αύξηση στην ταχύτητα πέντε φορές από το 802.11b. Αυτό καθίσταται δυνατό λόγω μιας ανώτερης τεχνικής διαμόρφωσης των ραδιοκυμάτων που λέγεται OFDM (Orthogonal Frequency Division Multiplexing). Παρόλα αυτά οι υψηλότερες ραδιοσυχνότητες μειώνουν κατά πολύ την απόσταση κάλυψης, καθώς και την διεισδυτική δύναμη του 802.11a, ειδικά σε εσωτερικούς χώρους. Εκεί που μια μετάδοση 802.11b θα περνούσε έναν τοίχο, μια μετάδοση 802.11a μπορεί να εμποδιστεί. Το γεγονός αυτό μπορεί να εμποδίσει την εγκατάσταση σε μεγάλη κλίμακα ενός δικτύου 802.11a, καθώς απαιτούνται πιο πολλοί σταθμοί βάσης για την κάλυψη του χώρου [43].

- **IEEE 802.11b**

Το 802.11b παρουσιάστηκε, όπως και το 802.11a, το 1999. Αποτελεί τον διάδοχο του 802.11 legacy και λειτουργεί στην μπάντα των 2.4 Ghz με την χρήση χαμηλής ισχύος (low gain) omnidirectional κεραία, με διαχωρισμό στο εύρος των

συχνοτήτων του σε τρία μη αλληλοκαλυπτόμενα κανάλια των 22Mhz. Η έκδοση αυτή παρέχει ταχύτητες μεταφοράς δεδομένων έως και 11 Mbps, χρησιμοποιώντας την DSSS (Direct Sequence Spread Spectrum) τεχνική διαμόρφωσης σε halfduplex μέθοδο. Λόγω της εκτεταμένης χρήσης της συχνότητας των 2.4 Ghz, στο 802.11b πρωτόκολλο ενδέχεται να υπάρχουν παρεμβολές από άλλες συσκευές στη μεταδιδόμενη πληροφορία, οδηγώντας σε σημαντική μείωση του ωφέλιμου bandwidth. Η τυπική απόσταση επικοινωνίας μεταξύ του σταθμού βάσης και των σταθμών, συνήθως δεν υπερβαίνει τα 34 μέτρα σε εσωτερικό χώρο και τα 140 μέτρα σε εξωτερικό χώρο[44].

- **IEEE 802.11g**

Το πιο πρόσφατο επικυρωμένο πρότυπο για την ασύρματη δικτύωση είναι το 802.11g, που στην ουσία συνιστά μία τροποποίηση του προτύπου 802.11b. Η έκδοση αυτή λειτουργεί σε ένα σύνολο 14άρων καναλιών, διαθέσιμα στην μπάντα των 2,4 Ghz τα οποία αριθμούνται από το 1 μέχρι το 14 και η χωρητικότητα του κάθε καναλιού είναι τα 22 Mhz, με 5 Mhz απόσταση μεταξύ τους. Από τα παραπάνω κανάλια μόνο τρία είναι μη επικαλυπτόμενα και μπορούν να χρησιμοποιηθούν χωρίς παρεμβολές μεταξύ διαφορετικών σταθμών βάσεων. Η τυπική ισχύς των σταθμών βάσεων κυμαίνεται στα 20dBm και το εύρος παροχής σήματος τους παραμένει ίδιο με αυτό του προκάτοχού του. Το 802.11g χρησιμοποιεί μία επιπλέον μέθοδο κωδικοποίησης OFDM η οποία δαπουσίαζε από το αρχικό 802.11 standart. Το παραπάνω επιτρέπει την αύξηση του μέγιστου ρυθμού bit ανά δευτερόλεπτο έως τα 54 Mbps, χρησιμοποιώντας μέθοδο διαμόρφωσης DSSS. Το 802.11g χρησιμοποιείται σε Single Input Single Output συστήματα, δηλαδή στην χρήση μονής κεραίας για την λήψη και εκπομπή σημάτων. Ακόμα, αντιμετωπίζει τους ίδιους περιορισμούς σε bandwidth με αυτές του 802.11b χωρίς να έχει καταφέρει να περιορίσει το πρόβλημα που υπάρχει με τη συμφόρηση στη συγκεκριμένη πάντα στην οποία λειτουργούν πολλές συσκευές συγχρόνως. Ωστόσο χαρακτηρίζεται από την διεισδυτική δύναμη της μικροκυμματικής μπάντας καθώς και την ικανότητα της για μετάδοση σε μακρινές αποστάσεις [45].

- **IEEE 802.11n**

Η 802.11n έκδοση του WiFi πρωτοκόλλου η οποία παρουσιάστηκε το 2009, αξιοποιεί την ορθογώνια πολυπλεξία διαίρεσης συχνότητας OFDM, όπως και οι 802.11a/g εκδόσεις, προσθέτοντας πολλαπλές κεραίες εκπομπής και λήψης σήματος. Το γεγονός αυτό αξιοποιεί τις πολλαπλές χωρικές διαδρομές που προσφέρουν οι πολλαπλές κεραίες στο φυσικό περιβάλλον των ραδιοσυχνοτήτων. Η τεχνική αυτή ονομάζεται MIMO (Multiple Input Multiple Output) και προσφέρει ταχύτητες μεταφοράς δεδομένων έως και 600 Mbps σε κανάλια εύρους 40 Mhz. Η έκδοση αυτή είναι συμβατή με εξοπλισμούς των 2,4 Ghz και 5 Ghz με μέγιστη ισχύ τα 2.1 Watt [46].

- **IEEE 802.11ac**

Το συγκεκριμένο πρότυπο είχε ξεκινήσει την ανάπτυξή του το 2008 και έλαβε τέλος το 2013. Το πρότυπο αυτό παρέχει τριπλάσιες ταχύτητες μεταφοράς δεδομένων συγκριτικά με τον προκάτοχό του. Αυτό επιτυγχάνεται χάρη στον διπλασιασμό των καναλιών συγκριτικά με τα 40 MHz κανάλια του 802.11n, στα 80 Mhz ή ακόμα και 160 Mhz, αυξάνοντας τις ταχύτητες από 117% μέχρι 333%). Σημαντικό ρόλο στην βελτιστοποίηση του ρυθμού αποστολής και λήψης δεδομένων καθιστά η ανεπτυγμένη μέθοδος κωδικοποίησης 256 Quadrature Amplitude Modulation (QAM), συγκριτικά με την 64QAM του 802.11n, αυξάνοντας κατά 33% τις ταχύτητες μετάδοσης. Ακόμα, ο μεγαλύτερος αριθμός ταυτόχρονων ζεύξεων μεταξύ κεραιών (MIMO) διπλασιάζεται, προσφέροντας 8 Spartial Streams σε αντίθεση με τα 4 του 802.11n. Το γεγονός αυτό αυξάνει περαιτέρω τις ταχύτητες επικοινωνίας κατά 100%. Η πρώτη έκδοση του 802.11ac στα 40 Mhz κανάλια παράγει ταχύτητες μετάδοσης από 433 Mbps μέχρι 1.3 Gbps στο φυσικό επίπεδο, ενώ μεταγενέστερες εκδόσεις αναπαράγουν ταχύτητες έως τα 3.47 Gbps. Το πρωτόκολλο 802.11 λειτουργεί στα 5Ghz, γεγονός που από την μία αξιοποιεί την λιγότερο συνωστισμένη μπάντα συχνοτήτων αλλά από την άλλη αδυνατεί να συνεργαστεί με τους ήδη υπάρχοντες εξοπλισμούς των 2.4 Ghz [47].

- **IEEE 802.11ah**

Είναι ευρέως γνωστό πως το πρωτόκολλο 802.11 είναι η κυρίαρχη ασύρματη τεχνολογία για τη διασύνδεση των περισσότερων συσκευών εσωτερικού χώρου με το

διαδίκτυο. Με συχνότητες λειτουργίας τα 2.4 και 5 GHz και με τις τροποποιήσεις (802.11 a/b/g/n/ac), επιτρέπει την χωρίς άδεια πρόσβαση στο ISM band (industrial, Scientific και Medical) κάνοντας εύκολη την δημιουργία ιδιωτικών ασύρματων δικτύων για τους χρήστες του. Η τεράστια αξιοποίηση της τεχνολογίας βασισμένη στο 802.11, έχει οδηγήσει σε δραματική συμφόρηση δικτύου μειώνοντας σε μεγάλο βαθμό την ταχύτητα και την αξιοπιστία των χρηστών απέναντι στη χρήση των ασύρματων συσκευών. Εκτός από την χρήση του 802.11 σε εσωτερικούς χώρους πλέον συναντάται σε συσκευές, όπως φορητούς υπολογιστές, κινητά τηλέφωνα, drones, αυξάνοντας ολοένα τον αριθμό των συσκευών στις ISM μπάντες. Η πανταχού παρούσα υπολογιστική, ενδέχεται να προκαλέσει μεγαλύτερο κορεσμό στο φάσμα συχνοτήτων που χρησιμοποιείται στις WiFi τεχνολογίες. Με έμπνευση τεχνολογιών που λειτουργούν σε χαμηλότερες συχνότητες, όπως αυτή των RFID οδήγησε την έρευνα γύρω από την ανάπτυξη ασύρματων δικτύων με την λιγότερο παρεμβάλουσα συχνότητα κάτω του 1Ghz. Στις περισσότερες χώρες οι συχνότητες αυτές είναι διαθέσιμες για αξιοποίηση, όμως ακόμα δεν έχει αναπτυχθεί κάποιο πρότυπο για την μοντελοποίησή τους [48].

Προκειμένου, λοιπόν, να καλυφθεί η απαίτηση για νέο φάσμα συχνοτήτων αλλά και για χαμηλότερης υπολογιστικής ισχύς ασύρματων συσκευών, η IEEE 802 LAN/MAN standards committee(LMSC) διαμόρφωσε το πρωτόκολλο IEEE 802.11ah Task Group (Tgah). Κύριος στόχος της επιτροπής είναι ο σχεδιασμός μίας ενεργειακά αποδοτική τεχνολογίας, επιτρέποντας σε χιλιάδες συσκευές εξωτερικού και εσωτερικού χώρου να λειτουργούν χωρίς περιορισμούς στον ίδιο χώρο. Το 802.11ac στοχεύει στην ταυτόχρονη λειτουργία πάνω από 8 χιλιάδων συσκευών σε ακτίνα ενός χιλιομέτρου. Οι ταχύτητες μετάδοσης της πληροφορίας θα κυμαίνονται από 150 Kbps μέχρι 40 Mbps. Λόγω της χαμηλότερης συχνότητας μετάδοσης της πληροφορίας οι συσκευές θα μπορούν μεταφέρουν την πληροφορίας σε αποστάσεις ίσες με ένα χιλιόμετρο σε εξωτερικό περιβάλλον [49].

Το πρωτόκολλο 802.11ah προσφέρει μία ποικιλία πλεονεκτημάτων, όπως η ευκολία χρήσης του σε εξωτερικά περιβάλλοντα σε συνάρτηση με την χαμηλή συχνότητα εκπομπής της πληροφορίας η οποία επιφέρει χαμηλή κατανάλωση ενέργειας και μεγάλο εύρος διάδοσης σήματος. Τα κυριότερα πλεονεκτήματα της αναπτυσσόμενης αυτής τεχνολογίας είναι :

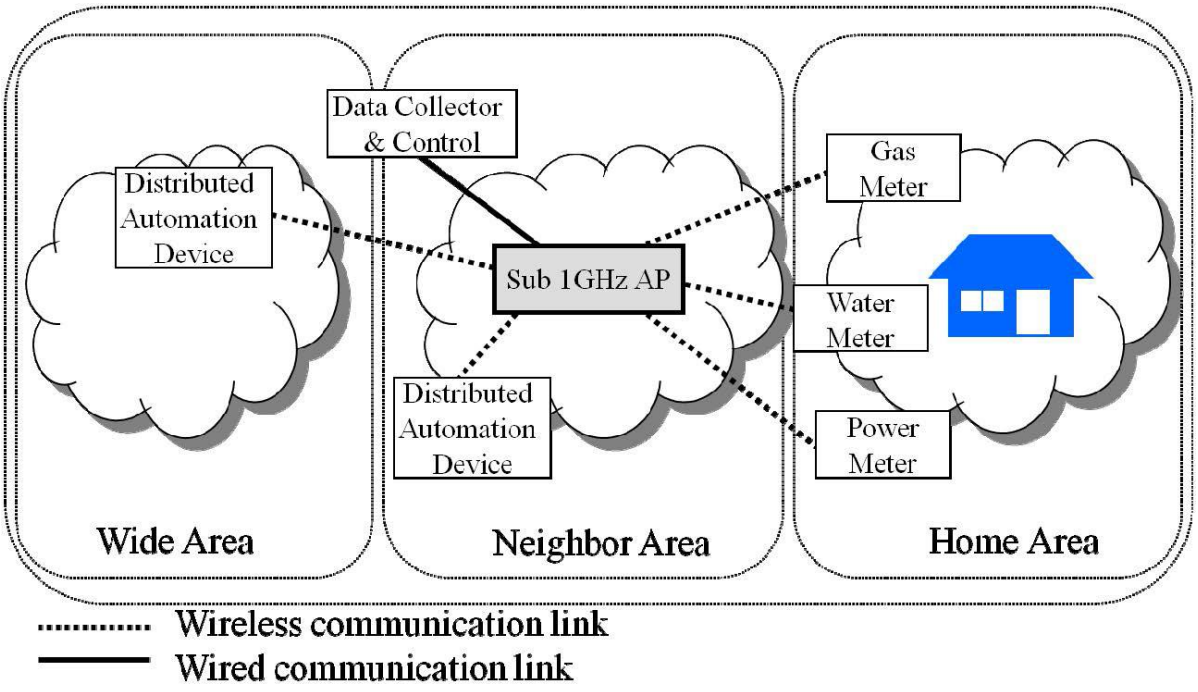
- Τα βελτιωμένα χαρακτηριστικά διάδοσης, με συχνότητες κάτω των 1Ghz

- Χρήση των ISM συχνοτήτων
- Μη αδειοδοτούμενο εύρος ζώνης συχνοτήτων στις περισσότερες χώρες.
- Ευκολία στην ενσωμάτωση σε νέες συσκευές, δεδομένου τις ήδη πολυχρησιμοποιημένης τεχνολογίας WiFi.
- Μεγαλύτερη απόσταση κάλυψης δικτύου με την χρήση λιγότερης ενέργειες

Παρακάτω αναφέρονται πιθανοί τρόποι χρήσης του νέου αυτού πρωτοκόλλου αξιοποιώντας τα πλεονεκτήματα της SUB 1 Ghz μπάντας.

A. Sensor Networks

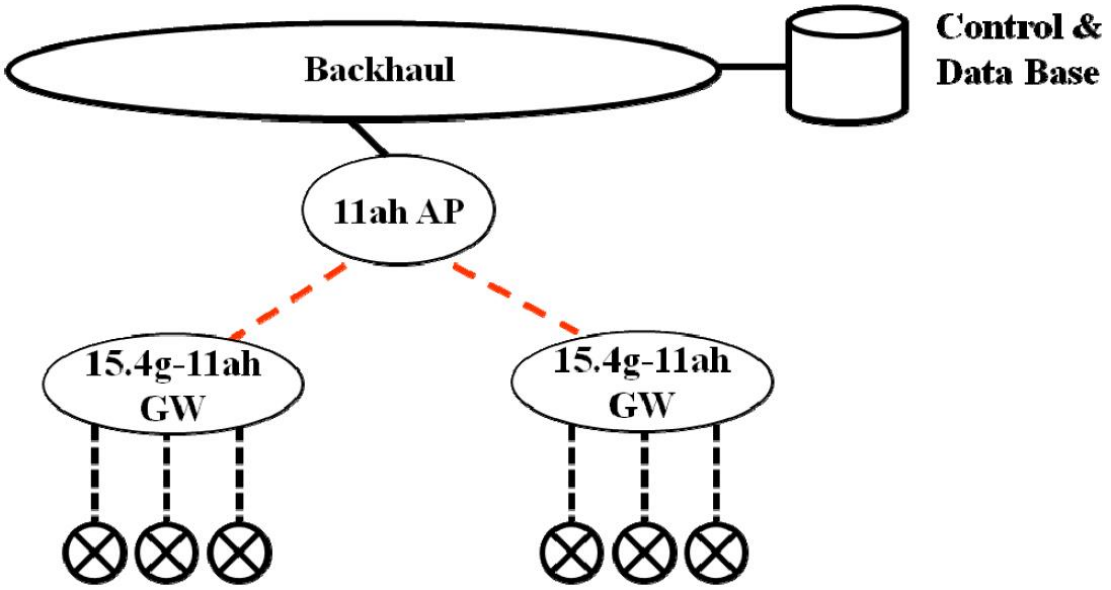
Δεδομένης της χαμηλής συχνότητας λειτουργίας των συσκευών μπορεί να επιτευχθεί μεγάλη διεισδυτικότητα του σήματος, γεγονός που εξυπηρετεί στην ταυτόχρονη λειτουργία περισσότερων συσκευών σε μεγαλύτερη απόσταση. Ανάλογα δίκτυα αποτελούν τα δίκτυα αισθητήρων (Sensor networks). Τα δίκτυα αυτά αποτελούνται από συσκευές με επίγνωση του περιβάλλοντος σε διαφορετικούς το καθένα τομείς. Οι αποκαλούμενοι αισθητήρες έχουν την δυνατότητα να αποσπούν πληροφορία, όπως νερό, φωτιά, κίνηση και να τη μεταφέρουν σε μικρής διάρκειας εκπομπές προς τον σταθμό βάσης που τους εξυπηρετεί. Στο παρακάτω σχήμα δίνεται ένα παράδειγμα δικτύων αισθητήρων [50].



Εικόνα 4.1 [11]

B. Backhaul δίκτυα για αισθητήρες

Καθώς η ανάγκη για μεγαλύτερη ταχύτητα μεταφοράς δεδομένων αυξάνεται, η κάλυψη του δικτύου ολοένα και μειώνεται, αυξάνοντας αρκετά το κόστος εγκατάστασης νέων σταθμών βάσεων για την κάλυψη των περιοχών που το έχουν ανάγκη. Λόγω της μεγάλης γεωγραφικής κάλυψης που παρέχουν οι Sub 1Ghz συχνότητες, δύναται να κατασκευαστούν Backhaul δίκτυα τα οποία θα μπορούν να διευρύνουν την κάλυψη δικτύου συνδέοντας σε σειρά διαφορετικούς 802.11ah σταθμούς μεταξύ τους, δημιουργώντας mesh δίκτυα ή αλλιώς δίκτυα μορφής πλέγματος. Με τα δίκτυα αυτά, οι σταθμοί βάσης συνδέονται μεταξύ τους ασύρματα και ανταλλάσσουν δεδομένα προκειμένου να τα προωθήσουν προς ή από την πύλη δικτύου (gateway point) στο ευρύ δίκτυο. Στο παρακάτω σχήμα απεικονίζεται ένα backhaul δίκτυο αισθητήρων το οποίο περιέχει 802.11 σταθμούς βάσης και διαμοιραστές / πύλες για τη σύνδεση δικτύων αισθητήρων μεταξύ τους [48].



Εικόνα 4.2 [11]

c. Επεκτάσιμα wifi ασύρματα δίκτυα με εκφόρτωση (offloading) δικτύου.

Το offloading στα ασύρματα δίκτυα θεωρείται η χρήση συμπληρωματικών τεχνολογιών δικτύου για την αποστολή και λήψη δεδομένων κυρίως στα κυψελωτά δίκτυα κινητής τηλεφωνίας. Η εκφόρτωση μειώνει τον όγκο των δεδομένων που μεταφέρονται στις κυψελοειδείς ζώνες, απελευθερώνοντας το γύρος ζώνης για άλλους χρήστες. Επιπρόσθετα, μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπου η τοπική λήψη σήματος από το κοντινότερο κελί είναι ασθενής. Στο 802.11 ah offloading είναι σημαντικό η τεχνολογία της εκφόρτωσης να είναι παρεμφερής με αυτή του κυψελωτού δικτύου που εξυπηρετεί και για τον λόγο αυτό πρέπει να ληφθεί αρχικά υπόψιν ποια είναι η υπάρχουσα φασματική αποδοτικότητα του συστήματος σε συνάρτηση με την ταχύτητα ανταλλαγής δεδομένων και το ήδη υπάρχον φορτίο του συστήματος [48].

D. Machine-to-Machine (M2M) Communication

Η εξέλιξη του 802.11 ah αποτελεί υποψήφια τεχνολογία για την χρήση σε machine to machine επικοινωνία μεταξύ των συσκευών. Η τεχνολογία αυτή επιτρέπει την αυτόνομη μεταφορά δεδομένων και μετρήσεων μεταξύ συσκευών που μοιράζονται κοινές τεχνολογίες ασύρματης δικτύωσης, σε αντίθεση με τα σημερινά δεδομένα όπου η μεταφορά της πληροφορίας μεταξύ των συσκευών απαιτεί την παρουσία του ανθρώπινου παράγοντα (Human to Human communications). Δεδομένου της μεγάλης διαφορετικότητας μεταξύ πρωτοκόλλων για M2M μεταφοράς πληροφορίας, το πρωτόκολλο 802.11 ah μπορεί να αποτελέσει βασικό παράγοντα για την δημιουργία ενός παγκόσμιου και ενιαίου standart για την M2M επικοινωνία, όπου μέχρι σήμερα θεωρείται ως cloud computing. Διαδικασίες όπως : η έξυπνη διαχείριση στόλου, η διαίσθηση κινδύνου, ή οι χρηματοοικονομικές συναλλαγές μεταξύ συσκευών [48].

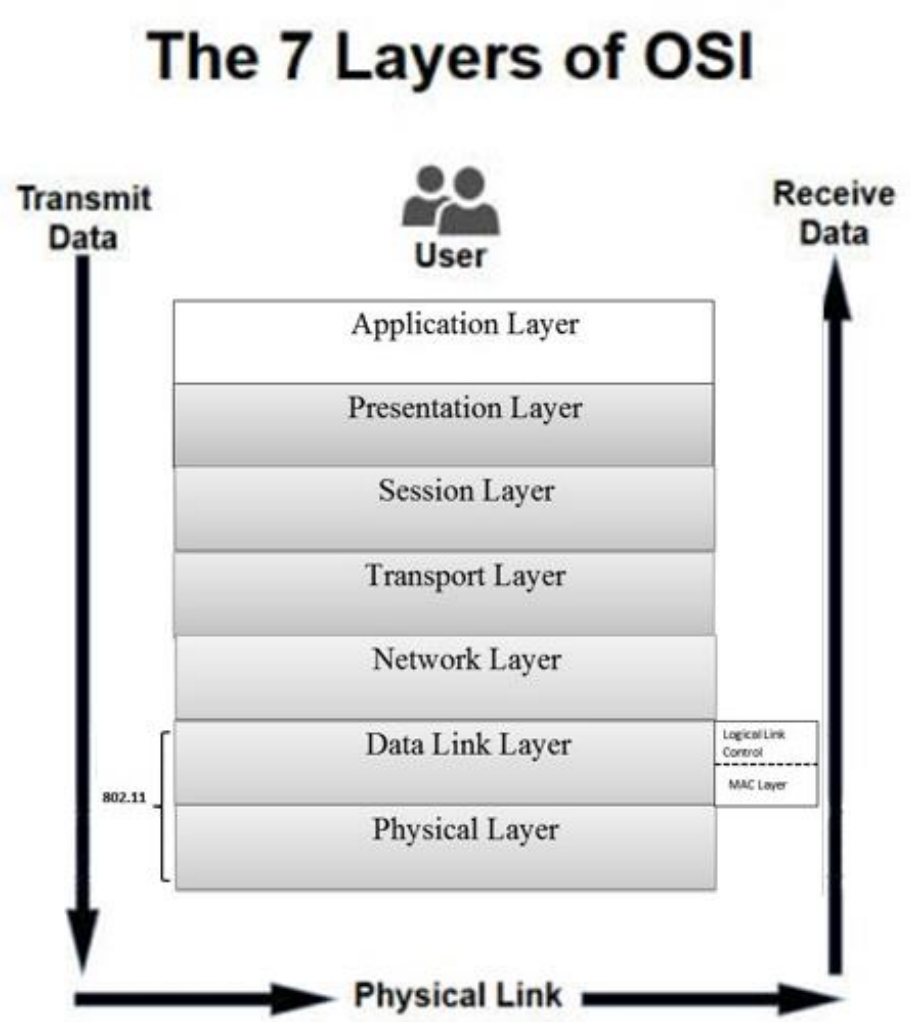
E. Rural communication (connecting the unconnected)

Η παροχή δικτύου σε απομακρυσμένες περιοχές όπου μέχρι πρότινος θεωρούταν αδύνατο, με την εξέλιξη των SUB 1 Ghz συχνοτήτων λόγω της μεγάλης

εμβέλειας μετάδοσης σήματος. Κύριες εφαρμογές αυτού είναι το E-learing και το E-health [48].

4.1 Ο ρόλος του IEEE 802.11 στο μοντέλο OSI

Όπως όλα τα 802.x πρότυπα έτσι και το 802.11 επικεντρώνεται στα δύο τελευταία στρώματα του μοντέλου OSI (Open systems Interconnection), καθώς περιέχει στοιχεία από το φυσικό (Physical Layer) και το δικτυακό επίπεδο(data layer). Το μοντέλο OSI είναι ένα εργαλείο αναφοράς για την κατανόηση των κανόνων επικοινωνίας, ανάμεσα σε δύο ή περισσότερα συστήματα. Διαχωρίζει την διαδικασία επικοινωνίας σε 7 στρώματα, όπου κάθε ένα από αυτά εκτελεί κατάλληλες διαδικασίες για να υποστηρίξει τα υψηλότερα στρώματά του, καθώς και να εξυπηρετήσει τα κατώτερα. Τα πρώτα τρία στρώματα είναι υπεύθυνα για την μεταφορά της πληροφορίας μέσω του δικτύου στα αντίστοιχα τερματικά συστήματα, ενώ τα τέσσερα πρώτα ολοκληρώνουν την διαδικασία επεξεργασίας και απεικόνισης. Εικόνα 4.1.1 [39].



Εικόνα 4.1.1

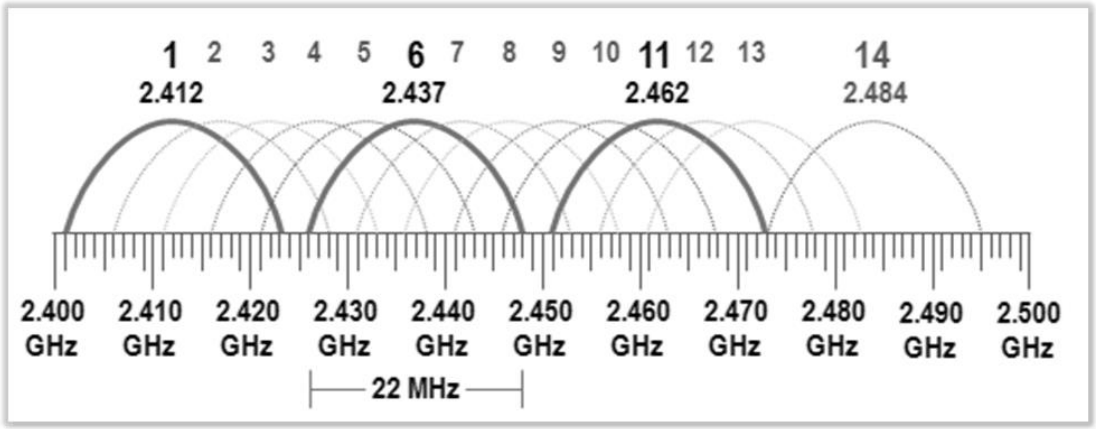
Physical layer (PHY) θεωρείται το φυσικό μέσο πάνω στο οποίο πραγματοποιείται η επικοινωνία. . Στις ασύρματες τεχνολογίες, χρησιμοποιείται ένας πομποδέκτης σε κάθε συσκευή, ο οποίος στέλνει και λαμβάνει σήματα πληροφορίας στη μορφή ραδιοκυμάτων και τα αποστέλλει μέσω του ασύρματου μέσου. Η συχνότητα εκπομπής και λήψης σημάτων, οι διαδικασίες εντοπισμού και διόρθωσης σφαλμάτων καθώς και οι τεχνικές διαμόρφωσης σημάτων, αποτελούν διαδικασίες και μεθόδους του φυσικού επιπέδου. Η πληροφορία που εκπέμπεται μέσω του επιπέδου αυτού, ενσωματώνει πληροφορίες από το PHY επίπεδο σε συνδυασμό με πληροφορίες από τα ανώτερα στρώματα δημιουργώντας πακέτα, τα οποία αντίστοιχα μόλις ληφθούν από

τον δέκτη διαχωρίζονται από αυτά του PHY, μεταφέροντας την πληροφορία στα ανώτερα επίπεδα [39].

Το PHY επίπεδο διαχωρίζεται σε δύο υπό-επίπεδα το : Physical Layer Convergence Procedure (PLCP) και το Physical Medium Dependent (PMD). Το πρώτο είναι η διασύνδεση των στοιχείων MAC και των ασύρματων μεταδόσεων στο ασύρματο μέσο, προσθέτοντας την δική του επικεφαλίδα. Τα πακέτα χρησιμοποιούν μία εισαγωγική πληροφορία προκειμένου να καθοδηγήσουν τον συγχρονισμό των ληφθέντων σημάτων, η οποία εξαρτάται από τον τρόπο διαμόρφωσης τους. Το δεύτερο υπό-επίπεδο αναλαμβάνει την μετάδοση των bits της πληροφορίας που λαμβάνει από το PLCP με την χρήση κεραιών, στον αέρα. Επιπρόσθετα, το φυσικό επίπεδο ενσωματώνει ακόμα μία διαδικασία (CCA) η οποία είναι υπεύθυνη για την υπόδειξη της πληροφορίας στο ανώτερο από αυτό επίπεδο. Αρχικά το πρότυπο 802.11 καθόρισε τρία φυσικά πρότυπα για το PHY επίπεδο. Πρόκειται για ένα σύστημα υπέρυθρων ακτινών καθώς και δύο συστημάτων διαμόρφωσης φάσματος, Το φάσμα διασποράς συχνότητας (FHSS) και το φάσμα εξάπλωσης άμεσης αλληλουχίας (DSSS). Το πρότυπο των υπερύθρων δεν εφαρμόστηκε κυρίως λόγω της περιορισμένης χρήστης του καθώς επηρεάζεται άμεσα από στερεά αντικείμενα και πηγές φωτός. Οι παραπάνω τεχνικές σε συνάρτηση με την ανάπτυξη των 802.11 πρωτοκόλλων, κατέστησαν δυνατή την περαιτέρω εξέλιξη των τεχνικών διαμόρφωσης [51].

Το 802.11 πρότυπο χρησιμοποιεί την εξελιγμένη τεχνική διαμόρφωσης High Rate DSSS, ενώ το 802.11a και 802.11g την ορθογωνική πολυπλεξία διαίρεσης συχνότητας OFDM (Orthogonal Frequency Division Multiplexing), αυξάνοντας σε μεγάλο βαθμό τη συνολική ταχύτητα διακίνησης της πληροφορίας. Το 802.11n εφαρμόζει και αυτό την τεχνική διαμόρφωσης OFDM συνδυάζοντάς την με το σύστημα πολλαπλών εισόδων – πολλαπλών εξόδων MIMO (Multiple Input Multiple Output). αυξάνοντας σε μεγαλύτερο βαθμό τις θεωρητικές ταχύτητες μεταφοράς. Οι περισσότεροι 802.11 σταθμοί αξιοποιούν την μπάντα συχνοτήτων των 2.4 Ghz, διαχωρίζοντας τα κανάλια επικοινωνίας τους σε 14, η χρήση των οποίων διαφέρει ανάλογα με την νομοθεσία κάθε χώρας. Το 802.11a αξιοποιεί τα κανάλια από το 36 μέχρι το 161, ανάλογα με την συχνότητα λειτουργίας του (από 5.15 – 5.825 GHz) και το εύρος των καναλιών. Στις περισσότερες περιπτώσεις η κεντρική συχνότητα λειτουργίας είναι αυτή των 5Ghz δημιουργώντας 12 μη επικαλυπτόμενα κανάλια επικοινωνίας (U.S.) και 19 μη επικαλυπτόμενα κανάλια (EU). Αντιθέτως τα 802.11

b/g/n δίκτυα τα οποία αξιοποιούν την 2.4 Ghz μπάντα συχνοτήτων, διαθέτουν 14 κανάλια εκ των οποίων τα 3 είναι μη επικαλυπτόμενα [39].



Εικόνα 4.1.2

Το Data link Layer αποτελεί το προτελευταίο επίπεδο κατηγοριοποίησης της μεταφοράς της πληροφορίας στο OSI μοντέλο. Αποτελείται από δύο υπό στρώματα, το LLC (Logical Link Control) sublayer και το MAC (Media access Control) sublayer. Η παρουσία του LLC καθιστά δυνατή την συνύπαρξη διαφορετικών δικτυακών πρωτοκόλλων όπως το Ethernet, το IEEE 802.11, ή το token ring. Το MAC sublayer στα 802.11 συστήματα, είναι υπεύθυνο για τον συντονισμό των πακέτων που λαμβάνονται και εκπέμπονται από το κοινόχρηστο φυσικό μέσο, με δίκαιο και αποδεκτό τρόπο. Επιτρέπει την αποτελεσματική επικοινωνία μεταξύ διαφορετικών συσκευών του δικτύου με τον σταθμό βάσης τους. Όταν μεταδίδεται η πληροφορία τοπικού δικτύου μεταξύ μίας συσκευής σε μια άλλη, στην πρώτη, το MAC υπόστρωμα λαμβάνει πακέτα από το LLC και τα μετατρέπει σε πακέτα έτοιμα προς εκπομπή μέσω του ασύρματου μέσου, προσθέτοντας μια ακολουθία ελέγχου πλαισίου για τον εντοπισμό σφαλμάτων μετάδοσης. Έπειτα προωθεί τα δεδομένα στο PHY επίπεδο μόλις το επιτρέπει η κατάλληλη μέθοδος πρόσβασης καναλιού. Το MAC layer στο πρωτόκολλο 802.11 αξιοποιεί την τεχνική PCF (Point coordination function) την οποία αξιοποιεί ο σταθμός βάσης του συστήματος και είναι υπεύθυνη για τον συντονισμό της επικοινωνίας του δικτύου. Το Data link Layer προκειμένου να ακολουθήσει τις παραπάνω διαδικασίες, χρησιμοποιεί τις διευθύνσεις MAC (MAC addresses) οι οποίες αποτυπώνονται σε κάθε συσκευή του δικτύου, ως μοναδικό αναγνωριστικό. Ως εκ

τούτου, κάθε συσκευή που ακολουθεί το πρότυπο 802.11 ενσωματώνει μία 48-bit MAC διεύθυνση [52].

4.2 IEEE 802.11 MAC Address

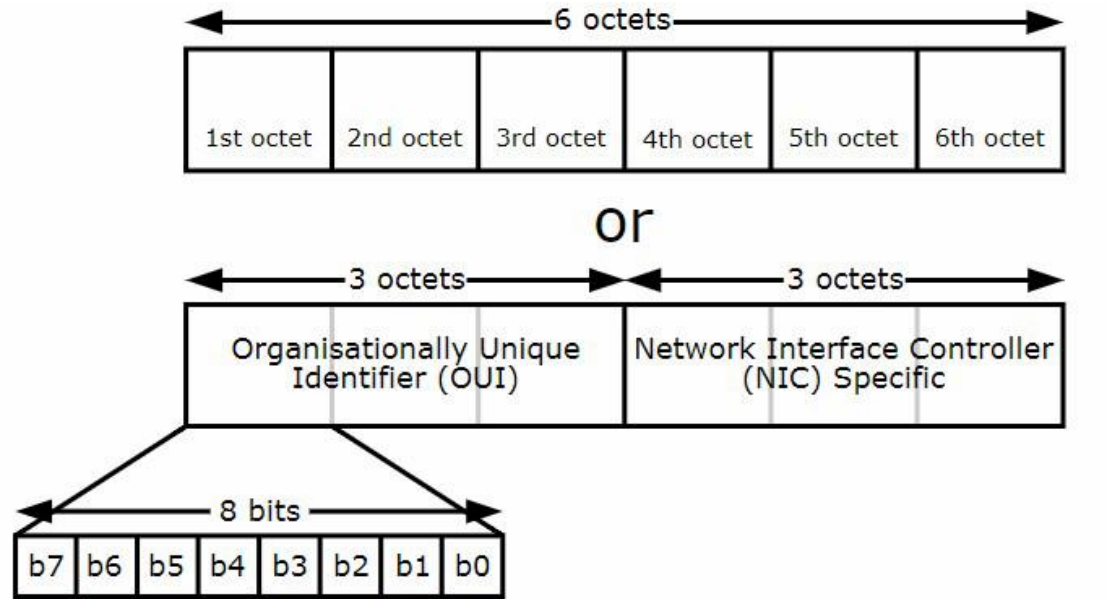
Οι MAC διευθύνσεις των διαφόρων εξοπλισμών ενός δικτύου, είναι σχεδιασμένες για να παραμένουν αμετάβλητες και να είναι μοναδικές για κάθε συσκευή παγκοσμίως. Για να επιτευχθεί αυτό κάθε εταιρία ή οργανισμός ο οποίος επιθυμεί την παραγωγή συσκευών για ασύρματη δικτυακή χρήση, κατοχυρώνει έναντι πληρωμής από το Ινστιτούτο ηλεκτρολόγων μηχανικών και ηλεκτρονικών μηχανικών (IEEE) ένα πρόθεμα τριών Bytes, το οποίο παραμένει αμετάβλητο μεταξύ των παραχθέντων συσκευών του οργανισμού αυτού. Αυτό χαρακτηρίζεται ως MAC address Block Large (MA-L) ή Organization Unique Identifier (OUI) και παρέχει στον οργανισμό/κατασκευαστή την πλήρη ευθύνη και έλεγχο για όλες τις MAC διευθύνσεις που εντάσσονται σε αυτό. Ο κατασκευαστής μετά είναι αρμόδιος να διαμορφώσει την κάθε διεύθυνση όπως αυτός επιθυμεί, με την βασική προϋπόθεση κάθε μία από αυτές να είναι διαφορετικές μεταξύ τους. Το ινστιτούτο IEEE επισημαίνει πως εάν κάποιος γνωρίζει την MAC address μίας δεδομένης συσκευής, δεν μπορεί με κάποιο τρόπο να βλάψει ή να αποσπάσει πληροφορίες μέσω αυτής. Οι Mac διευθύνσεις σχεδόν σε όλες τις περιπτώσεις χρησιμοποιούνται εσωτερικά του δικτύου μεταξύ της συσκευής και της αμέσως επόμενης από αυτό πύλης δικτύου. Παρόλα αυτά κάθε ένας ο οποίος «ακούει» την κίνηση των γειτονικών ασύρματων συσκευών, μπορεί να έχει πρόσβαση στην Mac διεύθυνση κάθε μίας από αυτές με αποτέλεσμα να γνωρίζει βασικές πληροφορίες για τον κατασκευαστή της. Σαν άμυνα προς αυτό, το IEEE ινστιτούτο παρέχει «ιδιωτικά» OUI τα οποία αποκρύπτουν την ταυτότητα του κατασκευαστή. Αυτή η δυνατότητα βέβαια δεν χρησιμοποιείται την δεδομένη χρονική περίοδο από κανέναν γνωστό κατασκευαστή [53].

Αντίστοιχα όμως με την μοναδική, δημόσια και χαρακτηριστική για κάθε κατασκευαστή MAC διεύθυνση, οι σύγχρονες δικτυακές συσκευές παράγουν δικές τους τοπικά καθορισμένες MAC διευθύνσεις η οποίες όπως και οι Private ips

(10.0.0.0/8, 172.16.0.0/12, και 192.168.0.0/16), μπορούν να χρησιμοποιηθούν με την βεβαιότητα πως δεν θα συγκρούονται με καμία άλλη MAC (τοπική ή δημόσια) εσωτερικά ενός δικτύου. Ο συγκεκριμένος τύπος MAC διευθύνσεων χρησιμοποιείται σε διάφορα περιβάλλοντα όπως σε multi-Service Set Identifier (SSID), ιδιωτικά WiFi hotspots, peer-to-peer (P2P) services και γενικότερα στην δικτύωση ψηφιακών εικονικών μηχανημάτων (virtual machines) [54].

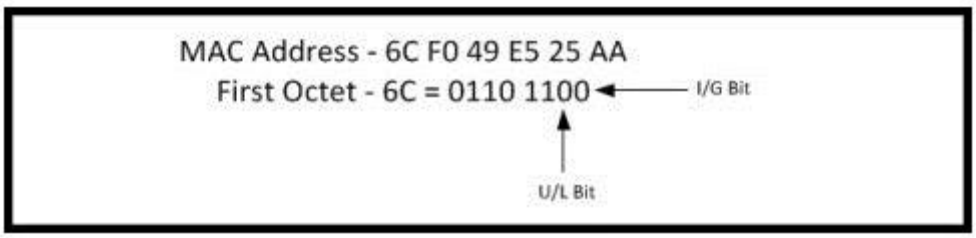
4.2.1 Μορφολογία MAC Address.

Μία Ethernet hardware address ή MAC Address αποτελείται από μία διαδοχική σειρά 12 χαρακτήρων και είναι αποτυπωμένη στη μνήμη ROM της δικτυακής κάρτας ενός μηχανήματος, δηλαδή στον εξοπλισμού που υπάρχει στο PHY layer του μοντέλου OSI Αυτή χωρίζεται συνήθως σε 2 μέλη. Το πρώτο 24bit μέλος αποτελεί το OUI και το δεύτερο 24bit μέλος, το NIC. Το συνολικό μέγεθος της MAC διεύθυνσης είναι 48 bits. Κάθε χαρακτήρας μπορεί να έχει 16 διαφορετικούς χαρακτήρες από 0-9 ή από A-F. Ο συνολικός αριθμός των πιθανών MAC διευθύνσεων που μπορεί να υποστηρίξει αυτή η αρχιτεκτονική είναι 16^{12} δηλαδή 281, 474 ,976, 710, 656 πιθανές Hardware διευθύνσεις. Η τυπική μορφή μίας 802.11 MAC-48bit διεύθυνσης διαφέρει μόνο ως προς την απεικόνιση και αποτελείται από έξι ομάδες των 8bit με δύο δεκαεξαδικά ψηφία η κάθε μία, Εικόνα 4.2.1.1**.** Οι ομάδες χωρίζονται από μία παύλα (-) ή κολώνα (:). Παράδειγμα MAC διεύθυνσης : 4C:66:41:93:1C:3E, 9A-A7-B7-47-11-B0. Η πρωτότυπη διεύθυνση MAC IEEE 802.11 προέρχεται από Ethernet Xerox σχήμα διευθύνσεων και μία 48bit MAC μπορεί να δημιουργήσει 2^{48} ή αλλιώς 281,474,976,710,656 δυνητικά πιθανές διευθύνσεις [54].



Εικόνα 4.2.1.1

Τα πρώτα 8 bits από μία MAC διεύθυνση, καθορίζουν τις πιο βασικές πληροφορίες για την ταυτότητα της. Το I/G αποτελεί το τελευταίο bit και εκφράζει το αν η πληροφορία θα προωθηθεί σε μία συγκεκριμένη συσκευή ή σε πολλαπλές συσκευές στο δίκτυο. Όταν αυτό είναι μηδέν η πληροφορία θα παραδοθεί συγκεκριμένα σε έναν παραλήπτη, ενώ αν είναι 1, η πληροφορία θα παραδοθεί σε πολλαπλούς παραλήπτες. Το U/L bit αποτελεί το bit στο οποίο υποδεικνύεται αν η MAC διεύθυνση είναι κατασκευασμένη από κάποιον οργανισμό, ή είναι ιδιωτική και έχει αποδοθεί εσωτερικά του δικτύου [54].



Εικόνα 4.2.1.2

Κεφάλαιο 5

Ασφάλεια δεδομένων στα ασύρματα δίκτυα

[51]I don't mean "poor" in an absolute sense. But the reliability of wireless transmission is really not comparable to the reliability of a wired network.

Παρόλο που οι ασύρματες τεχνολογίες αποτελούν καθοριστικό παράγοντα στην εξέλιξη της πανταχού παρούσας υπολογιστικής, η ασφάλειά τους αποτελεί βασικό μέλημα. Καθώς τα ενσύρματα δίκτυα αποτελούνται από συσκευές οι οποίες ανήκουν εντός του φυσικού χώρου ενός οργανισμού, δεν είναι άμεσα επιρρεπείς σε επιθέσεις. Επειδή η πρόσβαση στα δεδομένα που μεταφέρονται μεταξύ δύο υπολογιστών στο ενσύρματο δίκτυο απαιτούν τη φυσική πρόσβαση, είτε σε καθεμία από αυτές είτε στην θύρα ή το καλώδιο που χρησιμοποιούν για να επικοινωνήσουν, μόνος παράγοντας που μπορεί να αποτελέσει απειλή για ένα ενσύρματο δίκτυο είναι χρήστες οι οποίοι έχουν πρόσβαση στον χώρο του δικτύου αλλά μη εξουσιοδοτημένη χρήση αυτού [55].

Η σημασία της ασφάλειας στις αρχές της ανάπτυξης των ασύρματων δικτύων, περιοριζόταν στις ανάγκες για διαφύλαξη και απόκρυψη των πληροφοριών που ανταλλάσσονταν μεταξύ του στρατού, και σε μερικούς διάσπαρτους υπερασπιστές τις καθημερινής ιδιωτικής ζωής. Με την ανάπτυξη του διαδικτύου, όμως, τα δεδομένα μέχρι σήμερα έχουν διαφοροποιηθεί. Το διαδίκτυο πλέον αποτελεί καθρέφτη της κοινωνίας και όλες σχεδόν οι διαδικασίες που απαιτούν την ιδιωτικότητα προκειμένου να λειτουργήσουν, έχουν μεταφερθεί σε αυτό. Η διεξαγωγή ιδιωτικών συνομιλιών, η φύλαξη προσωπικών εγγράφων, η υπογραφή επιστολών και συμβάσεων, η ανώνυμη επικοινωνία, η ακεραιότητα της πληροφορίας, η ψήφος ή η δημοσίευση εγγράφων. Βασική προϋπόθεση των παραπάνω είναι η διαφύλαξη της ασφάλειας τους, προκειμένου να παραμείνουν ακέραια και ιδιωτικά. Οι εταιρίες σήμερα είναι άμεσα εμπλεκόμενες στην ανταλλαγή πληροφορίας στο διαδίκτυο, και μέρος αυτής της ανταλλαγής διεξάγεται μέσω ασύρματων δικτύων και φορητών συσκευών. Η ανάγκη

τους για επικοινωνία με τους πελάτες τους, τους προμηθευτές τους, τους συνεργάτες τους και τους ίδιους τους εργαζομένους τους, αποτελεί βασική προϋπόθεση για την υγιή λειτουργία της. Λόγω της ανάγκης αυτής όμως παρουσιάζεται μία σειρά από νέες απειλές όπως κακόβουλοι χάκερς, διαδικτυακοί εγκληματίες και βιομηχανικοί κατάσκοποι, οι οποίοι προκαλούν διακοπές στην λειτουργία, αποτυχίες του συστήματος και κλοπές προσωπικών και εταιρικών δεδομένων [56].

Εν προκειμένω, η πολιτική ασφαλείας των πληροφοριών πρέπει αρχικά να καλύπτεται φυσικά, όπως ο έλεγχος της φυσικής πρόσβασης και λογικά, όπως την ανίχνευση μη εξουσιοδοτημένης πρόσβασης στο δίκτυο, με έμφαση, μεταξύ άλλων, στον έλεγχο της εισαγωγής, πρόσβασης, καταγραφής, διαβίβασης και κοινοποίησης των δεδομένων, καθώς και στον έλεγχο των μέσων αποθήκευσης των δεδομένων. Τα τμήματα που διαχειρίζονται την τεχνολογία για αυτούς τους τύπους ασφαλείας είναι συνήθως εντελώς ξεχωριστά και σπάνια συνεργάζονται. Ο πολλαπλασιασμός της IP σύγκλισης της πληροφορίας μέσω του κοινού μέσου μεταφοράς μπορεί να επιφέρει δραματικές επιπτώσεις και στα δύο αυτά τμήματα, ενός οργανισμού. Στο κεφάλαιο αυτό θα εξεταστούν οι υπάρχουσες στρατηγικές για την διασφάλιση της πληροφορίας στους 2 αυτούς τομείς καθώς και τους νέους φυσικούς κινδύνους που αναπτύσσονται με την ανάπτυξη και την εξέλιξη της τεχνολογίας [57].

Η ύπαρξη ενός ατόμου ή τμήματος, υπεύθυνο για μια ολοκληρωμένη πολιτική ασφαλείας είτε πραγματική είτε εικονική, η οποία καλύπτει τόσο τη φυσική όσο και τη λογική ασφάλεια είναι πρωταρχικής σημασίας για την διασφάλιση των δεδομένων ενός οργανισμού. Παρέχοντας εκτελεστική χορηγία (Chief information officer) το τμήμα αυτό, ως διοικητικό όργανο με διαλειτουργικές ή διακλαδικές ομάδες για τη συγκέντρωση απαιτήσεων που αφορούν συγκεκριμένα τμήματα εξασφαλίζει ολοκληρωμένη παροχή ασφαλείας σε έναν οργανισμό. Πριν τη σύγκλιση των συσκευών , των εφαρμογών και των υπηρεσιών στο ip δίκτυο, τα μέτρα ασφαλείας ενός οργανισμού, διαχωρίζονταν σε κατηγορίες [57].

- Η παρακολούθηση μέσω βίντεο πραγματοποιούταν μέσω αποκλειστικών αναλογικών καλωδίων.
- Η φυσική πρόσβαση στα κτήρια διαχειριζόταν εξ ολοκλήρου σε απομονωμένο δίκτυα αντί για τοπικό δίκτυο, όπως συμβαίνει σήμερα.
- Η πρόληψη εισβολών έπαιρνε μέρος στο τείχος προστασίας.

- Ο εντοπισμός και η ανίχνευση ιών πραγματοποιούταν αποκλειστικά στους προσωπικούς υπολογιστές.
- Τα emails και η ασφάλεια στον κυβερνοχώρο περιορίζονταν στους χρήστες μέσα στα φυσικά όρια του οργανισμού.

Η σύγκλιση φωνής βίντεο και δεδομένων, επέφερε τις ακόλουθες αλλαγές σε κάθε έναν από αυτούς τους τομείς :

- Φωνή. Εκτός από την κυκλοφορία που δημιουργείται από την ανάπτυξη υπηρεσιών VoIP (Voice over IP), η φωνή τώρα αναφέρεται και σε άλλες πηγές ήχου, όπως την παρακολούθηση πλήθους, πυροβολισμός σε περιοχή υψηλής εγκληματικότητας, η ανίχνευση ήχου σε περιβάλλοντα που υποτίθεται είναι απομονωμένα για λόγους ασφαλείας.
- Βίντεο. Εκτός από τις βιντεοκλήσεις, τις τηλεοπτικές συνομιλίες, και την τηλεδιάσκεψη, το βίντεο αναφέρεται πλέον σε επιτήρηση χώρου, κάμερες κυκλοφορίας, ψηφιακή σήμανση και βίντεο συνεχούς ροής
- Δεδομένα. Η πρόσβαση στην πληροφορία δεν αποτελεί πλέον διαδικασία που λαμβάνει χώρα μόνο στο τοπικά ή ιδιωτικά δίκτυα. Με την ανάπτυξη των υπηρεσιών Cloud, η πρόσβαση στην πληροφορία μπορεί να επιτευχθεί από οπουδήποτε, οποιαδήποτε στιγμή, από οποιαδήποτε συσκευή.
- Δίκτυο. Πολλές ετερογενείς συσκευές συνδέονται στο δίκτυο όπως Smartphones, προσωπικοί φορητοί υπολογιστές κ.ο.κ. Δεν υπάρχει διάκριση μεταξύ μίας συσκευής και μίας συγκεκριμένης διαδικασίας.

Η διασφάλιση των δεδομένων περιλαμβάνει μία διαδικασία αρκετά πιο περίπλοκη από μία απλή αποτροπή πρόσβασης στη βάση δεδομένων ενός οργανισμού. Οι περισσότεροι οργανισμοί διαφυλάσσουν εκτός από τα ιδιωτικά τους δεδομένα και άλλου είδους δεδομένα πνευματικής ιδιοκτησίας όπως αιτήσεις για διπλώματα ευρεσιτεχνίας, πηγαίου κώδικα, εσωτερικών παρουσιάσεων και αναπτυξιακών σχεδίων. Η ανάπτυξη ενός σχεδίου ασφαλείας που λαμβάνει υπόψη όλους αυτούς τους διαφορετικούς τύπους δεδομένων οφείλει να προστατεύει όχι μόνο αυτά, αλλά και τα δεδομένα κα τις τεχνικές που αφορούν την ασφάλεια του οργανισμού, όπως η βάση δεδομένων ελέγχου πρόσβασης, αρχεία με βίντεο παρακολούθησης κ.α. Ένας μη εξουσιοδοτημένος χρήστης ο οποίος μπορεί να παρέμβει κα να αλλοιώσει τα δεδομένα αυτά, έχει την δυνατότητα ενδεχομένως να διαγράψει οποιαδήποτε ένδειξη παραβίασης

της ασφάλειας. Αυτή είναι μία περίπτωση όπου η φυσική και λογική πρόσβαση πρέπει να χρησιμοποιούνται από κοινού με σκοπό να δημιουργήσουν ένα ασφαλέστερο περιβάλλον. Για παράδειγμα, προτού δοθεί πρόσβαση σε ένα εξουσιοδοτημένο άτομο για την φυσική του πρόσβαση στον χώρο, θα πρέπει εκτός από τα στοιχεία που του επιτρέπουν την πρόσβαση, να ελεγχθούν και να ταυτοποιηθούν με αυτά, τα φυσικά του χαρακτηριστικά, προκειμένου να αποτραπεί η παραχώρηση σε άτομα χωρίς άδεια πρόσβασης. Η παραβίαση αυτή είναι μία από τις πιο συνηθισμένες παραβιάσεις εσωτερικής ασφαλείας [57].

Αν και η διασφάλιση μία εγκατάστασης θεωρείται συνήθως φυσική λειτουργία ασφαλείας, με την επέκταση των ασύρματων δικτύων η εγκατάσταση πλέον διαθέτει εικονική παρουσία, έξω από τα τοιχώματα του φυσικού της χώρου. Στο παρελθόν η απόκτηση πρόσβασης στο δίκτυο απαιτούσε την παρουσία ενός ανθρώπου ή υπολογιστή εντός της τοποθεσίας αυτού. Πλέον όμως αυτό δεν είναι απαραίτητο καθώς η ασύρματη δικτύωση διευρύνει την πρόσβαση εκτός του κτηρίου ή του λογικού του χώρου, και η σημασία που απαιτείται για την διασφάλισή της είναι εξίσου σημαντική. Με τα νέα αυτά δεδομένα της επέκτασης της λογικής πρόσβασης ενός δικτύου εκτός του κτιρίου, είναι αναγκαία η ανάπτυξη μηχανισμών για την αποτελεσματική παρακολούθηση και διαχείριση πιθανών απειλών ασφαλείας. Ένα παράδειγμα που θα μπορούσε να εξεταστεί είναι η περίπτωση ενός κακόβουλου ανθρώπου ο οποίος περιφέρεται, αναζητώντας μη κλειδωμένα Acess Points. Η ικανότητα εντοπισμού τόσο της απειλή όσο και του ίδιου του ατόμου είναι απαραίτητη για την αποτροπή της επίθεσης καθώς και την πιθανή δίωξη του [57].

Οι περισσότεροι οργανισμοί στεγάζονται σε πολυόροφρα κτήρια ή απομακρυσμένες βιομηχανικές περιοχές, όπου και στις δύο περιπτώσεις η φυσική παρουσία μη εξουσιοδοτημένων ατόμων δεν είναι εύκολη. Οι περισσότερες επιθέσεις στο ασύρματο μέσο χρειάζονται την πρόσβαση του δράστη εντός των ορίων του ασύρματου δικτύου κάτι που στις παραπάνω περιπτώσεις δεν είναι εφικτή. Με την εμφάνιση των drones αυτό δεν είναι πλέον εμπόδιο. Οποιοσδήποτε έχει πρόσβαση σε μία εμπορική συσκευή drone, μπορεί να ενσωματώσει σε αυτή τον κατάλληλο εξοπλισμό προκειμένου να αποκτήσει «φυσική πρόσβαση» στον ιδιωτικό χώρο ενός ανθρώπου ή οργανισμού [57].

5.1 Ασφάλεια και Drones

Τα drones ή αλλιώς μη επανδρωμένα εναέρια οχήματα UAV, καθίστανται γρήγορα δημοφιλή στον εμπορικό και μη εμπορικό τομέα για διάφορους σκοπούς όπως η παροχή πρόσβασης στο διαδίκτυο η λήψη φωτογραφιών σε απομακρυσμένες τοποθεσίες και η παράδοση φυσικών πακέτων. Η ομοσπονδιακή υπηρεσία Αεροπορίας FFA στις Ηνωμένες Πολιτείες προβλέπει ότι οι πωλήσεις εμπορικών μη επανδρωμένων αεροσκαφών θα φτάσουν μέχρι το 2020 τα 2,7 εκατομμύρια drones και η παραγωγή μη στρατιωτικών αεροσκαφών προβλέπεται να αυξηθεί από 2,6 σε 10,9 δισεκατομμύρια δολάρια μέχρι το 2025. Ωστόσο, οι κανονισμοί λειτουργίας των αεροσκαφών αργούν να αναπτυχθούν συγκριτικά με τον ρυθμό ανάπτυξής τον ίδιων των αεροσκαφών, λαμβάνοντας υπόψιν πως αυτά μπορεί να επηρεάσουν την ιδιωτική ζωή των ανθρώπων και την ασφάλειά τους, καθώς μπορούν να καταγράψουν τις κινήσεις τους ή ακόμα και να τους τραυματίσουν. Ακόμα και με τους κανόνες που θεσπίστηκαν πρόσφατα για τη λειτουργία των αεροσκαφών η FFA παρέχει Απλώς απροσδιόριστες κατευθυντήριες γραμμές σχετικά με την προστασία της ιδιωτικής ζωής όσον αφορά τη σωστή χρήση [58].

Ο ορισμός ενός drone είναι το αεροσκάφος το οποίο δεν φέρει πλήρωμα, αλλά λειτουργεί εξ αποστάσεως από τον χειριστή του ή αυτόνομα μέσω προγραμματισμένου λογισμικού. Αυτά ποικίλουν σε μεγάλο βαθμό ανάλογα με το μέγεθος τους, την διάρκεια μπαταρίας τους καθώς και τις τεχνολογίες που χρησιμοποιούν προκειμένου να ανταλλάξουν πληροφορία με τον χειριστή τους. Η χρήση τους τα τελευταία πέντε χρόνια αυξήθηκε εκθετικά για ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένης της χαρτογράφησης, της επιθεώρησης απομακρυσμένων ηλεκτρικών γραμμών και αγωγών, των υπηρεσιών παράδοσης φυσικών πακέτων, της επιτήρησης από τον στρατό και την αστυνομία, της παρακολούθησης της κυκλοφορίας, της περιπολίας, της αναγνώρισης συνόρων καθώς και της παρακολούθησης έκτακτων γεγονότων. Από στρατιωτικής απόψεως τα drones μπορούν να ανακτηθούν ή να αναλωθούν. Χρησιμοποιούνται συνήθως για τη χρήση τους σε επικίνδυνα ή εχθρικά εδάφη χωρίς να θέτουν σε κίνδυνο καμία ανθρώπινη ζωή. Η εμπορική διαθεσιμότητα μία νέας γενιάς μικρών drones ή αλλιώς quadcopters έχει καταστήσει την ανάπτυξή τους ιδιαίτερα ανησυχητική. Παρά το μικρό τους μέγεθος έχουν την δυνατότητα να μεταφέρουν ωφέλιμο φορτίο έως και μερικά κιλά, και επειδή το μέγεθός τους είναι αρκετά μικρό,

μπορούν πολύ εύκολα να αποφύγουν τις παραδοσιακές μεθόδους επιτήρησης και ασφάλειας. Ένα εμπορικά διαθέσιμο drone μπορεί να κοστίζει έως και μερικά εκατοντάδες δολάρια και μπορεί πολύ εύκολα να προξενήσει καταστροφές όπως μεταφορά εκρηκτικού υλικού, κατασκοπία, καταγραφή ιδιωτικών δεδομένων, εισβολή σε ασύρματα δίκτυα κ.α. [59].

5.1.1 Privacy issues

Μία σημαντική ανησυχία των εμπορικά διαθέσιμων μη επανδρωμένων αεροσκαφών είναι η ευκολία της χρήσης τους στην παραβίαση της ιδιωτικότητας, καθώς και της δυσκολίας τους να ανιχνευτούν από τα κοινά μέσα παρακολούθησης. Τα drones διαθέτουν ένα μοναδικό εύρος ευκίνητων τεχνικών πρόσβασης γεγονός που τα κάνει να υπερισχύουν σε δυνατότητες συγκριτικά με άλλες διεισδυτικές συσκευές απορρήτου. Στην πραγματικότητα, σήμερα, τα UAVs με ενσωματωμένες κάμερες μπορούν να χειρίζονται απομακρυσμένα με μεγαλύτερη ακρίβεια και κινητικότητα και ευελιξία από τις στατικές κάμερες παρακολούθησης [60].

5.1.2Κανονισμοί Drones

Οι μελετητές του νόμου εξετάζουν τους νόμους περί απορρήτου που διέπουν τη χρήση των μη επανδρωμένων εναέριων σκαφών και συμφωνούν πως οι ισχύοντες κανονισμοί της FAA θα πρέπει να περιλαμβάνουν κανόνες για τα δεδομένα που συλλέγονται από αυτά αντί για την ίδια τους τη λειτουργία. Συγκεκριμένα, επισημάνθηκαν ανησυχίες σχετικά με τη συλλογή πληροφοριών από ιδιώτες, από άτομα της κυβέρνησης ή τον βιομηχανικό τομέα καθώς και για τον τρόπο χρήσης αυτών των πληροφοριών. Το 2016 η FAA εξέδωσε έναν μικρό κανόνα λειτουργίας για τα μη επανδρωμένα εναέρια σκάφη. Ο κανόνας αυτός, ρυθμίζει τις λειτουργίες των drones για εμπορική ή ιδιωτική χρήση και περιέχει αυστηρές προϋποθέσεις για τον χειρισμό τους. Για παράδειγμα ένας ιδιοκτήτης drone από δω και στο εξής θα πρέπει να παρακολουθεί υποχρεωτικά ένα εκπαιδευτικό πρόγραμμα ως πιστοποιητικό της εγγραφής και της άδειάς τους, για τον χειρισμό της συσκευής, καθώς και να είναι τουλάχιστον 16 ετών. Η FFA δημιούργησε την εφαρμογή B4UFLY για να βοηθήσει

τους χρήστες να ελέγξουν εάν υπάρχουν περιορισμοί και ποιοι είναι αυτοί, στην περιοχή όπου βρίσκονται. Ωστόσο, αυτοί οι κανόνες εξακολουθούν να μην καθορίζουν ποια δεδομένα μπορεί να συλλέξει ένα drone ή τους περιορισμούς χρήσης της πληροφορίας αυτής από τους ιδιοκτήτες τους [58].

Η δημιουργία του προφίλ ενός ανθρώπου βασιζόμενο στη συμπεριφορά και τις προτιμήσεις του μπορεί να αποβεί μία πολύ κερδοφόρα στρατηγική καθώς είναι πολύ χρήσιμη για την αγορά. Αυτή η δραστηριότητα συχνά μπορεί να παρατηρηθεί στο διαδίκτυο με τη μορφή της στενευμένης διαφήμισης, βασισμένη στο ιστορικό της περιήγησης ενός ανθρώπου. Παρόλο που αυτή όμως η στρατηγική διαφήμισης είναι ασυνείδητα ανεκτική από όλους, μία παρόμοια τακτική στον πραγματικό κόσμο σπάνια θα μπορούσε να γίνει ανεκτή. Τα drones ενδέχεται να χρησιμοποιηθούν για την φυσική και στοχευμένη σάρωση και συλλογή δεδομένων σχετικά με τον τρόπο ζωής μας, εξυπηρετώντας τους σκοπούς της αγοράς. Με την πρόσθετη λειτουργία της οπτικής καταγραφής, εκτιμάται πως αυτή η στρατηγική πρόκειται να είναι περισσότερο πολύτιμη από αυτή που χρησιμοποιείται στις μέρες μας από ένα botnet. Δεδομένης της συνεχούς φυσικής και διαδικτυακής παρακολούθησης της συμπεριφοράς ενός ανθρώπου, μπορεί κανείς να αναμένει πως η εικόνα αυτού, όσον αφορά στις κινήσεις του, τις προτιμήσεις του καθώς και του κοινωνικού του κύκλου μπορούν να ανακατασκευαστούν [61].

Παρακάτω παρουσιάζονται μερικά παραδείγματα για την χρήση ενός drone, κακοβούλως :

- Snoopy. Το κακόβουλο αυτό λογισμικό μπορεί να εγκατασταθεί σε ένα drone προκειμένου να συλλέγει πληροφορίες και πόρους αλλά και να παρακολουθεί ανυποψίαστους χρήστες, εκμεταλλευόμενο το ανοιχτό WiFi στα έξυπνα κινητά τηλέφωνα τους. Ένα drone εξοπλισμένο με το λογισμικό Snoopy, εκμεταλλεύεται τις δυνατότητες του WiFi ενός smartphone και τα ωθεί στο να αναζητούν συνεχώς ασύρματα δίκτυα προκειμένου να συνδεθούν σε αυτά συμπεριλαμβανομένων δικτύων που έχουν συνδεθεί στο παρελθόν. Το Snoopy λαμβάνει πληροφορία που εκπέμπεται από το εκλαμβανόμενο κινητό τηλέφωνο σχετικά με τους σταθμούς βάσης που αυτό έχει συνδεθεί στο παρελθόν και παριστάνει έναν από αυτούς τους σταθμούς βάσης με αποτέλεσμα να ξεγελάει τη συσκευή του χρήστη η οποία συνδέεται σε αυτό. Με αυτόν τον τρόπο μπορεί να αποσπάσει πληροφορίες όπως την Mac address του κινητού,

με την οποία ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει για να εντοπίσει το κινητό σε πραγματικό χρόνο [62].

- Skynet ή αλλιώς Το "Stealth δίκτυο", χρησιμοποιώντας drones έχει την δυνατότητα να στρατολογήσει και να ελέγξει δυναμικά τους ιδιωτικούς υπολογιστές διαφόρων χρηστών. Τα drones χρησιμοποιούνται για να σαρώσουν μία συγκεκριμένη γεωγραφική έκταση και να θέσουν σε κίνδυνο τα τοπικά δίκτυα της περιοχής και τελικά τους υπολογιστές των χρηστών που είναι συνδεδεμένοι σε αυτά. Στη συνέχεια τα drones χρησιμοποιούνται τακτικά για να εκτελέσουν τις εντολές του κακόβουλου χρήστη (botmaster) στους υπολογιστές που έχουν μολύνει. Το Skynet εκμεταλλεύεται την μέτρια ασφάλεια των ιδιωτικών ασύρματων δικτύων, τα οποία θεωρούνται ως τα λιγότερα ασφαλή δίκτυα στο Internet. Τα δίκτυα αυτά συνήθως αφορούν δίκτυα τα οποία δεν χρησιμοποιούν κωδικό πρόσβασης, δίκτυα που δεν εφαρμόζουν πρωτόκολλα ασφαλείας, ή δίκτυα με προβλέψιμους κωδικούς πρόσβασης. Μόλις παραβιαστούν οι οικιακοί υπολογιστές, ο botmaster μπορεί να αποκτήσει πρόσβαση σε προσωπικά αρχεία όπως ευαίσθητα διαπιστευτήρια τραπεζικών λογαριασμών. Το Skynet ελεγχόμενο από drones ενισχύει την λειτουργία του botnet, παρακάμπτοντας την χρήση του διαδικτύου, αποφεύγοντας έτσι τους γνωστούς μηχανισμούς ασφαλείας, όπως firewalls και συστήματα ανίχνευσης εισβολής [63].

- The Iot done ή το drone του Ίντερνετ των πραγμάτων, είναι το κακόβουλο drone το οποίο μπορεί να επικοινωνήσει με τις ασύρματες συσκευές της περιοχής που βρίσκεται μέσα στην εμβέλειά του, χρησιμοποιώντας την τεχνολογία Zig-Bee. Το drone είναι εφοδιασμένο με πολλές Zig-Bee κεραίες η οποίες μπορούν να αλληλεπιδράσουν με συσκευές που χρησιμοποιούν το ίδιο πρωτόκολλο. Το drone που χρησιμοποιείται για αυτού του είδους την επίθεση είναι εξοπλισμένο με τεχνολογία GPS για τον προσδιορισμό της θέσης κάθε συσκευής. Λειτουργεί λαμβάνοντας και καταγράφοντας τη θέση καθώς και πληροφορίες για κάθε συσκευή σε ακτίνα 330 μέτρων. Η συλλογή πληροφοριών σχετικά με τον τύπο και ενδεχομένως τη χρήση των συσκευών στις ιδιωτικές οικίες μπορεί να χρησιμοποιηθεί για να προβλέψει το βιοτικό επίπεδο και τις ώρες που

βρίσκονται οι χρήστες αυτών εντός ή εκτός αυτών. Τέτοιες πληροφορίες δεν παραβιάζουν μόνο την ιδιωτικότητα των προσώπων που έχουν πληγεί, αλλά μπορούν επίσης να χρησιμοποιηθούν για σκοπούς κλοπής και βανδαλισμού [64].

Δεδομένης της ραγδαίας ανάπτυξης των drones σε συνδυασμό με τις αμέτρητες ικανότητες που διαθέτουν, το εύλογο ερώτημα που δημιουργείται είναι : Πως γνωρίζουμε πως δε θα χρησιμοποιηθούν με κακόβουλο σκοπό; Ο αριθμός των αναφορών των μέσων μαζικής ενημέρωσης σχετικά με τα δυσάρεστα περιστατικά όπου αυτά εμπλέκονται, αυξάνεται συνεχώς. Παραδείγματος χάριν, έχουν χρησιμοποιηθεί για να μεταφέρουν λαθραία προϊόντα σε φυλακές ή να πλήξουν περιοχές με χτυπήματα ηλεκτρομαγνητικών κυκλωμάτων, διακόπτοντας την ρευματοδότηση. Υπήρξε, επίσης, αναφορά από τον λευκό οίκο πως ένα Quadcopter DJI Phantom συνετρίβει εντός των εγκαταστάσεων του. Από τα παραπάνω είναι προφανές πως δεν μπορεί κανείς να πει με σιγουριά πως η χρήση των μη επανδρωμένων αυτών οχημάτων θα παραμείνει ασφαλής. Μπορούμε μόνο να φανταστούμε τι συνέπειες μπορεί να έχει η τεχνολογία αυτή στα χέρια των τρομοκρατών, ή ακόμα και την μη εξουσιοδοτημένη πτήση κοντά σε αεροδρόμια η οποία θα μπορούσε να προξενήσει πολύ σημαντικές υλικές ζημιές, ακόμα και θέσει σε κίνδυνο τη ζωή εκατοντάδων ανθρώπων. Η απόσπαση, επίσης, απόρρητων πληροφοριών από στρατιωτικές βάσεις θα μπορούσε να θέσει σε κίνδυνο τον θεσμό της ασφάλειας μία χώρας [65].

Προκειμένου να αντιμετωπιστούν αυτές οι απειλές κατά της ασφάλειας, απαιτείται η ανάπτυξη ενός μοντέλου παρακολούθησης της δραστηριότητας των οχημάτων αυτών και αναλόγως των παραβιάσεων που αυτά πράττουν να διενεργούνται και οι κατάλληλες δράσεις εναντίων τους. Η πιο σημαντική πτυχή της ανάπτυξης και εφαρμογής ενός τέτοιου μοντέλου Monitoring σχετίζεται με την αρχιτεκτονική της, διότι θα πρέπει να πράττει αυτόνομα ανάλογα με την περίπτωση, χωρίς την βοήθεια του κεντρικού σταθμού ελέγχου ασφαλείας ή του χειριστή του. Για τον λόγο αυτόν σε λιγότερο ευαίσθητες περιοχές σε θέματα ασφαλείας μπορεί να εφαρμοστεί η αρχιτεκτονική του Point to Point, η οποία διαθέτει μόνο ένα μηχανισμό ανίχνευσης, ο οποίος έχει την δυνατότητα να ανιχνεύσει εναέρια οχήματα μόνο σε κοντινή από αυτό απόσταση. Εναλλακτικά σε σενάρια όπου η ασφάλεια είναι ζωτικής σημασίας, προτείνεται η αρχιτεκτονική ad hoc για την πιο αξιόπιστη εκτίμηση της ενδεχόμενης απειλής και την αποτροπή οποιασδήποτε κακόβουλη ενέργειας. Το κίνητρο για την

ανάπτυξη αυτού του μοντέλου είναι η πανταχού και πλήρης παρακολούθηση κάθε ερασιτεχνικής κίνησης των drones ανεξαρτήτου γεωγραφικής περιοχής, προκειμένου να υπάρχει πλήρης εικόνα των κινήσεών τους, με σκοπό την αποφυγή κακόβουλων ενεργειών οι οποίες θα μπορούσαν να αποβούν καταστροφικές [65].

5.1.3 Προσέγγιση τεχνικών άμυνας

Ως απάντηση προς την κακόβουλη χρήση των drones για επιτήρηση, πρόσβαση σε ασύρματα δίκτυα, συλλογή πληροφορίων και πόρων, προέκυψαν διάφορες τεχνικές και προϊόντα για την υπεράσπιση και άμυνα ενάντια στην ανεπιθύμητη παρουσία των αιωρούμενων αυτών μηχανημάτων, σε ένα δεδομένο εναέριο χώρο. Στις μέρες μας ορισμένοι κατασκευαστές drones, περιλαμβάνουν μία λίστα μη επιτρεπτών GPS συντεταγμένων που καλύπτουν ευαίσθητες περιοχές όπως αεροδρόμια, στρατιωτικά κέντρα, εμπορικά κέντρα, στάδια και κυβερνητικές εγκαταστάσεις. Νέες καταχωρήσεις στην "no fly" αυτή λίστα καταχωρούνται στις υποχρεωτικές αναβαθμίσεις των συσκευών που κάθε χρήστης πρέπει να εφαρμόσει προκειμένου να μπορεί να λειτουργήσει η ιπτάμενη συσκευή του. Επίσης, κάθε χρήστης έχει το δικαίωμα να καταχωρήσει το σπίτι του ή την εταιρία του στη βάση δεδομένων - NoFlyZone 2016. ως νέα απαγορευτική περιοχή πτήσης, το οποίο επιτρέπει σε αυτούς να θέσουν κανόνες πτήσης γύρω από την περιοχή που τους ανήκει. Για παράδειγμα, οι ιδιοκτήτες διαφόρων ιδιωτικών περιοχών, μπορούν να έχουν τη δυνατότητα να καθορίσουν την επιθυμητή πολιτική πρόσβασης για τον ελεγχόμενο ιδιωτικό τους χώρο, συμπεριλαμβανομένης της διατήρησης των επιθυμητών αποστάσεων για κάθε ώρα ή ημέρα της εβδομάδας. Ως μέσον καταχώρησης τον ιδιωτικών αυτών νόμων μπορεί να χρησιμοποιηθεί το εκπεμπόμενο σήμα από τα ιδιωτικά ασύρματα δίκτυα, τα οποία λειτουργώντας ως φάροι θα μεταφέρουν στα drones του κανόνες σχετικά με την συγκεκριμένη περιοχή [66].

Ωστόσο, δεν υπάρχει κάποιος τρόπος προκειμένου να διασφαλιστεί πως αυτός ο κανόνας θα τηρηθεί και για τον λόγο αυτόν τεχνικές όπως η παρατήρηση, ανίχνευση και καταγραφή εναέριων μη επανδρωμένων αεροσκαφών είναι αναγκαίος και προτιμότερος. Τεχνικές που εμπίπτουν στην κατηγορία αυτή, αποσκοπούν στην ανίχνευση και πιθανή παρακολούθηση των αεροσκαφών σε μια δεδομένη περίμετρο

και στη συνέχεια στην ειδοποίηση του ιδιοκτήτη του χώρου προς επιτήρηση. Συστήματα τέτοιου είδους, όπως το σύστημα παρακολούθησης χρησιμοποιούν έναν συνδυασμό διαφορετικών αισθητήρων, υπέρυθρων καμερών και ανιχνευτών ραδιοεπικοινωνίας για να ανιχνεύσουν την παρουσία ενός αδιάκριτου drone, είτε από τον ήχο, το σχήμα του είτε την μεταξύ του επικοινωνία με τον χειριστή του. Μόλις αυτό αναγνωριστεί από το σύστημα παρακολούθησης μέθοδοι τριγωνισμού χρησιμοποιούνται προκειμένου να προσδιορίσουν την θέση του, καθώς και τεχνικές για την υπεξαίρεση ή την καταστροφή του [67].

Κεφάλαιο 6
Ανάπτυξη εφαρμογής

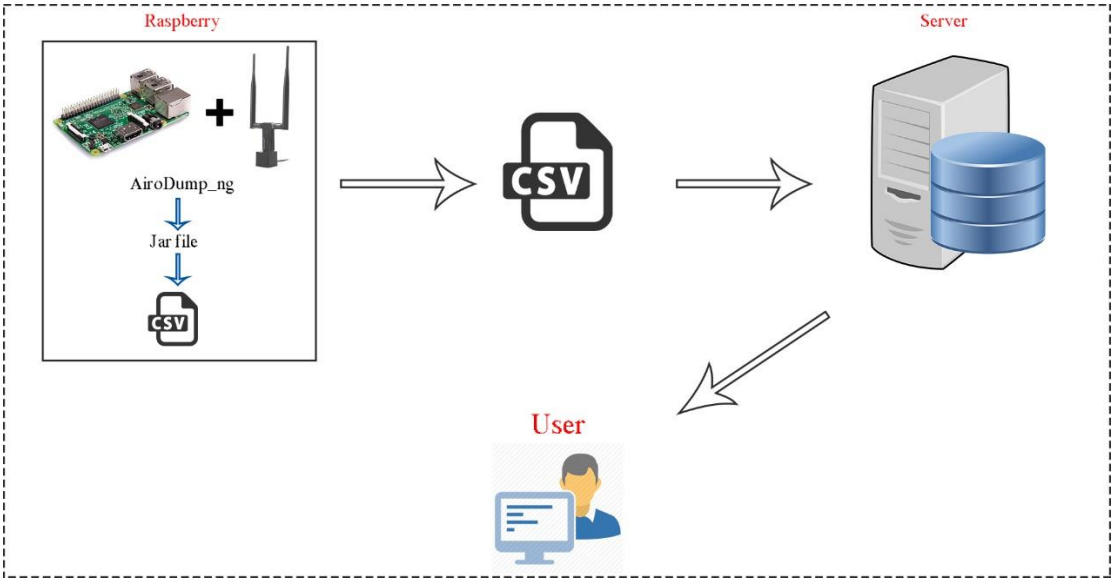
Το πρακτικό τμήμα της παρούσας διπλωματικής εργασίας πραγματεύεται την ανάπτυξη συστήματος με στόχο την καταγραφή και ταυτοποίηση γειτονικών συσκευών που αξιοποιούν το πρωτόκολλο IEEE 802.11. Η εφαρμογή εξειδικεύεται στην καταγραφή των Mac διευθύνσεων, οι οποίες συλλέγονται από την δικτυακή κίνηση των συσκευών που βρίσκονται στην ακτίνα εμβέλειας. Αποτελείται από έναν υπολογιστή μικρού μεγέθους Raspberry, συνδεδεμένο με ειδική κεραία, ικανή να τεθεί σε λειτουργία ανίχνευσης (Monitoring Mode). Για την κατασκευή της, χρησιμοποιήθηκε γλώσσα προγραμματισμού Java σε πλατφόρμα Linux με σκοπό την ανάπτυξη μιας φιλικής προς τον χρήστη εφαρμογής. Οι λειτουργίες που πραγματοποιούνται από την εφαρμογή είναι η καταγραφή των MAC διευθύνσεων που κάθε συσκευή χρησιμοποιεί για να αναγνωριστεί από το δίκτυο, και η καταχώρησή αυτών σε απομακρυσμένη βάση δεδομένων. Η εφαρμογή με αυτόν τον τρόπο μπορεί να αξιοποιεί την πληροφορία αυτή σε πραγματικό χρόνο, παρέχοντας στον χειριστή μία πρώτη εικόνα. Αξιοποιώντας, λοιπόν, τις δυνατότητες αυτές, ο χρήστης θα έχει μία πρώτη απεικόνιση της αόρατης στο ανθρώπινο μάτι παρουσίας συσκευών, αξιοποιώντας την με βάση τις ανάγκες του ή τις ανάγκες ενός θεσμού που αντιπροσωπεύει. Το παρόν έργο θα αναπτύξει την καταγραφή αυτής της πληροφορίας για σκοπούς άμυνας από εμπορικά, μη επανδρωμένα αεροσκάφη (drones), την αναζήτηση συσκευών κατά βούληση, καθώς και την προτροπή από "επίθεση" twin evil Access Point. Ακόμα, η εφαρμογή θα μπορεί να παρέχει στον χρήστη πλήρη εικόνα των γειτονικών ενεργών WiFi συσκευών μαζί με πληροφορίες, όπως την ισχύ σήματός του, το κανάλι λειτουργίας του, το όνομα του κατασκευαστή της κάρτας δικτύου του, κ.α. Η εφαρμογή είναι συμβατή με τα περισσότερα παραθυριακά προγράμματα περιήγησης (Browsers), επεκτάσιμη και μπορεί στο μέλλον να εξελιχθεί αξιοποιώντας το διαδίκτυο και άλλες νέες τεχνολογίες. Το σύστημα αυτό αναπτύχθηκε στα πλαίσια

μεταπτυχιακής διατριβής που έλαβε χώρα για το ανοιχτό πανεπιστήμιο Κύπρου.

Ως απώτερος σκοπός του project είναι η δημιουργία ενός ενιαίου δικτύου με πολλαπλές συσκευές το οποίο θα είναι σε θέση να καλύψει μεγαλύτερες και διαφορετικές μεταξύ τους γεωγραφικές περιοχές, αποστέλλοντας διαφορετικά δεδομένα σε κοινή βάση δεδομένων. Το όραμα του project είναι η δημιουργία φορητών συσκευών Raspberry οι οποίες θα εξυπηρετούν πάντα τον ίδιο σκοπό, την ανίχνευση και καταγραφή των γειτονικών ασύρματων συσκευών. Ο τρόπος δικτύωσης της κάθε συσκευής με την βάση δεδομένων, επιτρέπει την ταυτόχρονη συνεργασία πολλών συσκευών , καλύπτοντας μεγαλύτερες γεωγραφικές εκτάσεις και διαμορφώνοντας ένα ευρύτερο δίκτυο επιτήρησης. Δεδομένης της χαμηλής απαιτούμενης ενέργειας που καταναλώνει η συσκευή Raspberry, έχει την δυνατότητα να λειτουργήσει με την παροχή εξωτερικής μπαταρίας (Powerbank) σε συνδυασμό με αντάπτορα GSM σήματος, γεγονός που την καθιστά πλήρως φορητή. Το γεγονός αυτό μπορεί να ωφελήσει στην άμεση δημιουργία ενός δικτύου παρακολούθησης, παρέχοντας κάλυψη σε μεγάλες γεωγραφικές εκτάσεις ή σε πολυώροφα κτήρια. Με τον απαραίτητο προγραμματισμό η συσκευή θα είναι θέση να λειτουργεί αυτόνομα, θέτοντάς την σε λειτουργία ανίχνευσης και καταγραφής, αμέσως μετά την εκκίνησή της. Είναι σημαντικό να σημειωθεί πως η εφαρμογή διαμορφώθηκε έτσι ώστε να ανιχνεύει συσκευές που λειτουργούν με το WiFi πρωτόκολλο, για τις ανάγκες της παρούσας πτυχιακής εργασίας. Με τις κατάλληλες παραμετροποιήσεις και επιπλέον προσθήκες hardware, η συσκευή θα μπορεί να είναι σε θέσει να ανιχνεύει διαφορετικά πρωτόκολλα επικοινωνίας, ανάλογα με τις ανάγκες του κάθε οργανισμού.

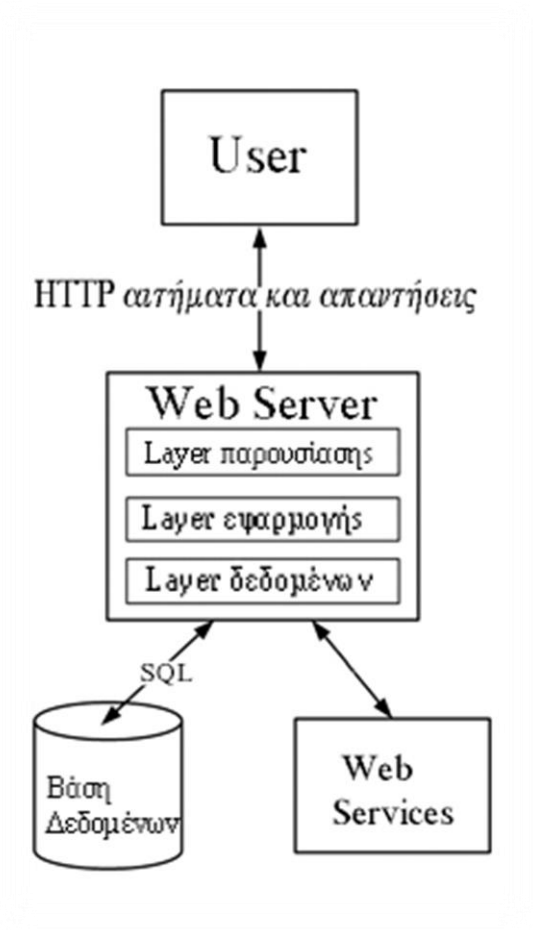
6.1 Σχεδιασμός Συστήματος

Το προτεινόμενο σύστημα αποτελείται κυρίως από την συσκευή Raspberry (Client) και τον εξυπηρετητή Server στον οποίον τρέχει η βάση δεδομένων και εκτελείται η web εφαρμογή. Η αρχιτεκτονική του συστήματος φαίνεται στο Σχήμα χ Στα πλαίσια της εκπόνησης της διδακτορικής αυτής διατριβής, η βάση δεδομένων του συστήματος έχει δομηθεί με τέτοιο τρόπο ώστε να μπορεί να φιλοξενεί τις πιο απαραίτητες πληροφορίες για τον έλεγχο και την παρακολούθηση του έργου. Ο διαχειριστής του συστήματος έχει πρόσβαση σε αυτό χρησιμοποιώντας φυλλομετρητές ιστού (Web Browsers). Η εφαρμογή αναπτύχθηκε σε web περιβάλλον προκειμένου να είναι αρκετά εύκολη η πρόσβασή του χρήστη σε αυτή. Δεν επιλέχθηκε η ένταξη διαφορετικών χρηστών, μη παρέχοντας δικλίδα ασφαλείας για την είσοδο στην εφαρμογή, αν και αυτό μπορεί να προστεθεί αν χρειαστεί μεταγενέστερα. Η εφαρμογή βρίσκεται σε πειραματικό στάδιο γι' αυτό και οι λειτουργίες της δεν είναι εντελώς αυτοματοποιημένες που σημαίνει πως ο διαχειριστής της εφαρμογής χρειάζεται να εγκαταστήσει και να παραμετροποιήσει τα συστατικά της μέρη, προκειμένου αυτή να λειτουργήσει . Η ηλεκτρονική ανταλλαγή των πληροφοριών μεταξύ των συμμετεχόντων στην κατασκευή του έργου επιτυγχάνεται με ένα σύνολο κατάλληλα σχεδιασμένων ιστοσελίδων, που αποτελούν τη διαδικτυακή εφαρμογή. Η βάση δεδομένων γεμίζει συνεχώς με πληροφορίες οι οποίες προέρχονται από ένα αρχείο το οποίο κατασκευάζεται στη συσκευή Raspberry.



Εικόνα 6.1. Αρχιτεκτονική συστήματος

Η ανάπτυξη της Web εφαρμογής περιλαμβάνει το σχεδιασμό ενός συνόλου δυναμικών ιστοσελίδων οδηγούμενων από δεδομένα (data driven dynamic web pages) οι οποίες θα επιτρέπουν στον χρήστη του συστήματος να αποκτήσει πρόσβαση σε συγκεκριμένες διαδικασίες. Μία ιστοσελίδα είναι δυναμική όταν το περιεχόμενό της είναι μερικώς ή πλήρως μεταβλητό. Δυναμική ιστοσελίδα είναι για παράδειγμα εκείνη που απεικονίζει την τρέχουσα ισχύ μίας κοντινής συσκευής, καθότι κάθε φορά που αυτή μετακινείται η σελίδα έχει διαφορετικό περιεχόμενο. Όταν το περιεχόμενο μίας ιστοσελίδας καθορίζεται από πληροφορίες που είναι καταχωρημένες σε βάση δεδομένων, τότε η ιστοσελίδα ονομάζεται οδηγούμενη από δεδομένα (data-driven). Το περιεχόμενο μιας τέτοιας σελίδας καθορίζεται κάθε φορά από τα κριτήρια που θέτει ο χρήστης για αναζήτηση πληροφορίας και τις καταχωρημένες στη βάση δεδομένων πληροφορίες. Οι δυναμικές οδηγούμενες από δεδομένα ιστοσελίδες επιτρέπουν την εισαγωγή, αναζήτηση, θέαση, ανάκτηση, τροποποίηση και διαγραφή δεδομένων από τη βάση δεδομένων. Στο σχήμα x διακρίνεται εποπτικά η διαδικασία ερώτησης μίας βάσης δεδομένων μέσω ιστοσελίδας και η επιστροφή των κατάλληλων δεδομένων στον φυλλομετρητή ιστού (browser). Η όλη διαδικασία αποτελείται από τα παρακάτω βήματα :



Εικόνα 6.2 Διάγραμμα φιλοσοφίας εφαρμογής

1. User : Ο χρήστης μέσω του web browser αιτείται από τον εξυπηρετητή ιστού την πληροφορία και στη συνέχεια λαμβάνει απάντηση χρησιμοποιώντας την τεχνολογία JavaServerFaces (JSF)

2. Web Server : Φιλοξενεί διάφορα επίπεδα της εφαρμογής :

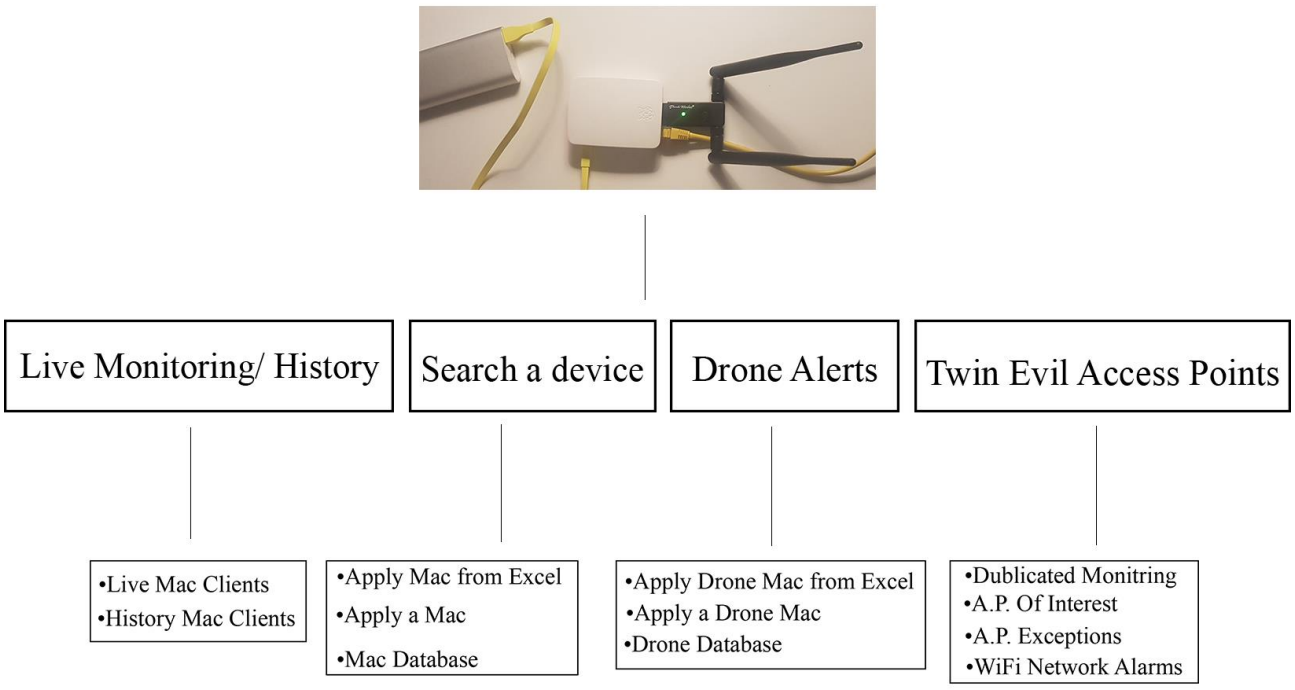
- Layer Παρουσίασης : Ο χρήστης αλληλοεπιδρά με την εφαρμογή μέσω HTTP αιτημάτων και ανταποκρίσεων που αποδίδονται στον φυλλομετρητή ιστού.
- Layer Εφαρμογής : Είναι υπεύθυνο για την ροή της εφαρμογής εφαρμόζοντας επιχειρηματική λογική. Συνεργάζεται με το επίπεδο δεδομένων (Layer δεδομένων) για να επεξεργάζεται τα αιτήματα του χρήστη και τις απαντήσεις τους. Προγράμματα third party και ανοιχτού λογισμικού, εδρεύουν στο επίπεδο αυτό.
- Layer Δεδομένων : Το επίπεδο αυτό είναι υπεύθυνο για την ανάκτηση των δεδομένων από τις πηγές του

4. Βάση δεδομένων : Το επίπεδο αυτό είναι υπεύθυνο για την ανάκτηση και αποθήκευση της πληροφορίας .

5. Web services : Η αλληλεπίδραση με άλλες διαδικτυακές εφαρμογές

6.2 Παρουσίαση Web εφαρμογής

Οι λειτουργίες της εφαρμογής Project_Monitoring κατηγοριοποιούνται ως εξής : Εικόνα 6.2



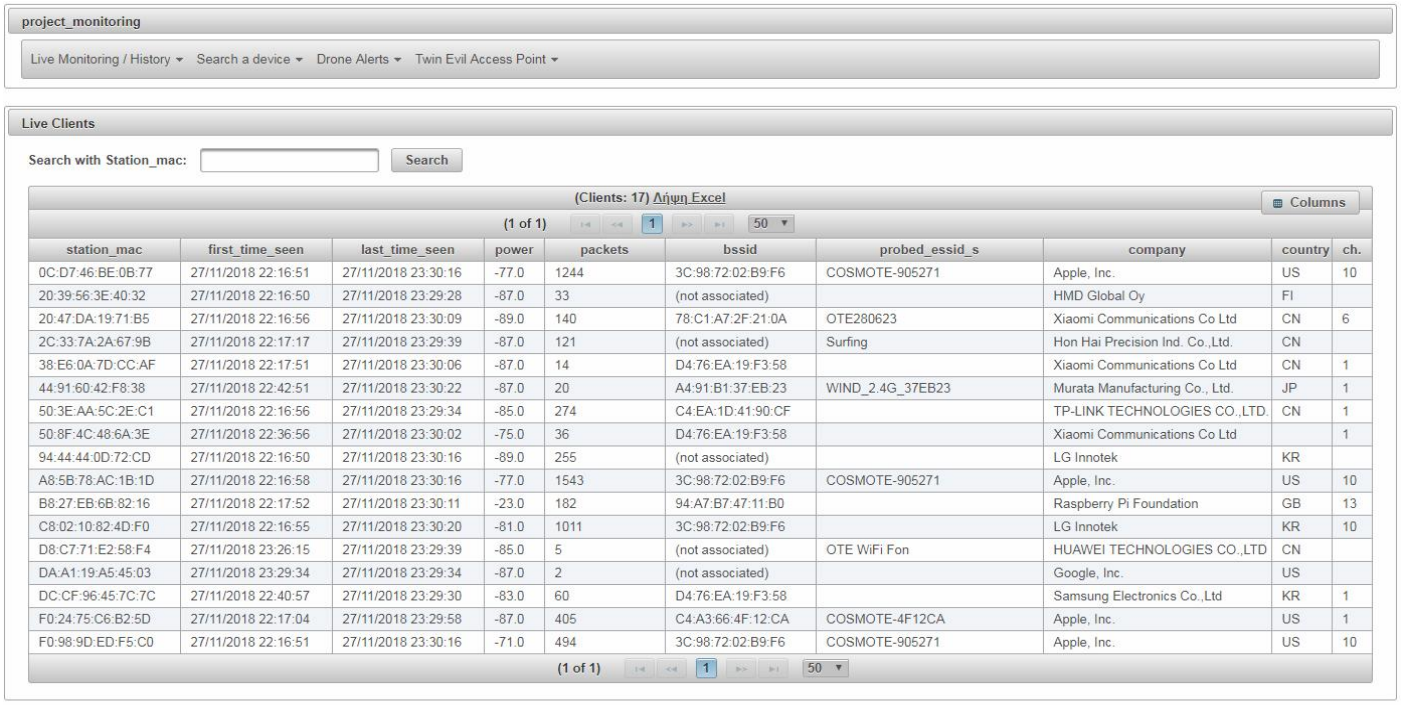
Εικόνα 6.2

6.2.1 Live Monitroing/ History

Η πρώτη κατηγορία της εφαρμογής περιέχει την λειτουργία της απεικόνισης των Client και Access Point που βρίσκονται σε λειτουργία στην ευρύτερη περιοχή. Επίσης παρέχει την δυνατότητα προβολής του ιστορικού των συσκευών που έχει ληφθεί ανά διαστήματα.

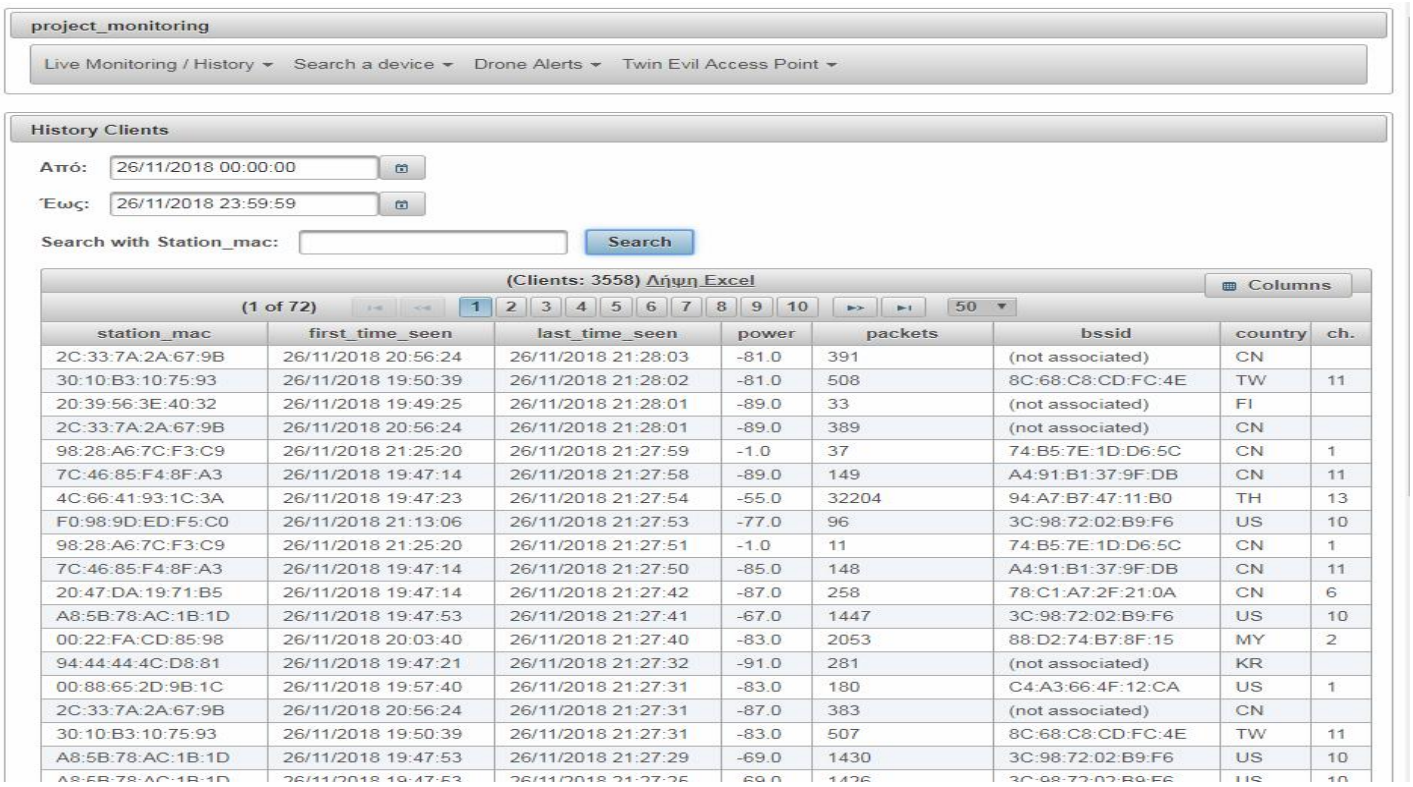
Με την Επιλογή **: Live Mac Clients** (Εικόνα 6.2.1.1) απεικονίζονται τα βασικά χαρακτηριστικά για της Clients συσκευές. Παρατηρούμε πως η πλειοψηφία των συσκευών αποτελούνται από smartphones και αυτό γίνεται αντιληπτό από τις εταιρίες κατασκευής των ασύρματων καρτών δικτύου τους (Apple INC , Samsung Electroincs CO LTD, Xiaomi). Οι κατηγορίες των χαρακτηριστικών που απεικονίζονται παροουσιάζονται ως εξής :

- Station mac : Η MAC διεύθυνση της ασύρματης κάρτας δικτύου της ασύρματης συσκευής.
- First time seen : Η ώρα και ημερομηνία που τέθηκε εντός εμβέλειας ή λειτουργίας η ασύρματη συσκευή.
- Last time seen : Η ώρα και ημερομηνία που η ασύρματη συσκευή προβλήθηκε για τελευταία φορά.
- Power : Η ισχύς σήματος εκπομπής της κεραίας της συσκευής.
- Packets : Ο αριθμός της συνολικής μετάδοσης των μεταδιδόμενων πακέτων. από ή προς την ασύρματη συσκευή.
- Bssid : Ο σταθμός βάσης με τον οποίο είναι συνδεδεμένη η ασύρματη συσκευή.
- Point.Bssid : Ο σταθμός βάσης στον οποίο είναι συνδεδεμένη η ασύρματη συσκευή.
- Probed_essid_s : Ο σταθμός βάσης που αναζητά μία ασύρματη συσκευή προκειμένου να συνδεθεί αυτόματα σε αυτή.
- Company : Πληροφορίες για την εταιρία παρασκευής της κάρτας δικτύου της συσκευής.
- Country : Η χώρα κατασκευής της κάρτας δικτύου.
- channel : Το κανάλι λειτουργίας του Access Point.



Εικόνα 6.2.1.1. Live Clients

Η επιλογή **History Mac Clients** (Εικόνα 6.2.1.2), Απεικονίζει το ιστορικό των Clients από μία δεδομένη χρονική στιγμή την οποία επιλέγει ο χρήστης.



station_mac	first_time_seen	last_time_seen	power	packets	bssid	country	ch.
2C:33:7A:2A:67:9B	26/11/2018 20:56:24	26/11/2018 21:28:03	-81.0	391	(not associated)	CN	
30:10:B3:10:75:93	26/11/2018 19:50:39	26/11/2018 21:28:02	-81.0	508	8C:68:C8:CD:FC:4E	TW	11
20:39:56:3E:40:32	26/11/2018 19:49:25	26/11/2018 21:28:01	-89.0	33	(not associated)	FI	
2C:33:7A:2A:67:9B	26/11/2018 20:56:24	26/11/2018 21:28:01	-89.0	389	(not associated)	CN	
98:28:A6:7C:F3:C9	26/11/2018 21:25:20	26/11/2018 21:27:59	-1.0	37	74:B5:7E:1D:D6:5C	CN	1
7C:46:85:F4:8F:A3	26/11/2018 19:47:14	26/11/2018 21:27:58	-89.0	149	A4:91:B1:37:9F:DB	CN	11
4C:66:41:93:1C:3A	26/11/2018 19:47:23	26/11/2018 21:27:54	-55.0	32204	94:A7:B7:47:11:B0	TH	13
F0:98:9D:ED:F5:C0	26/11/2018 21:13:06	26/11/2018 21:27:53	-77.0	96	3C:98:72:02:B9:F6	US	10
98:28:A6:7C:F3:C9	26/11/2018 21:25:20	26/11/2018 21:27:51	-1.0	11	74:B5:7E:1D:D6:5C	CN	1
7C:46:85:F4:8F:A3	26/11/2018 19:47:14	26/11/2018 21:27:50	-85.0	148	A4:91:B1:37:9F:DB	CN	11
20:47:DA:19:71:B5	26/11/2018 19:47:14	26/11/2018 21:27:42	-87.0	258	78:C1:A7:2F:21:0A	CN	6
A8:5B:78:AC:1B:1D	26/11/2018 19:47:53	26/11/2018 21:27:41	-67.0	1447	3C:98:72:02:B9:F6	US	10
00:22:FA:CD:85:98	26/11/2018 20:03:40	26/11/2018 21:27:40	-83.0	2053	88:D2:74:B7:8F:15	MY	2
94:44:44:4C:D8:81	26/11/2018 19:47:21	26/11/2018 21:27:32	-91.0	281	(not associated)	KR	
00:88:65:2D:9B:1C	26/11/2018 19:57:40	26/11/2018 21:27:31	-83.0	180	C4:A3:66:4F:12:CA	US	1
2C:33:7A:2A:67:9B	26/11/2018 20:56:24	26/11/2018 21:27:31	-87.0	383	(not associated)	CN	
30:10:B3:10:75:93	26/11/2018 19:50:39	26/11/2018 21:27:31	-83.0	507	8C:68:C8:CD:FC:4E	TW	11
A8:5B:78:AC:1B:1D	26/11/2018 19:47:53	26/11/2018 21:27:29	-69.0	1430	3C:98:72:02:B9:F6	US	10

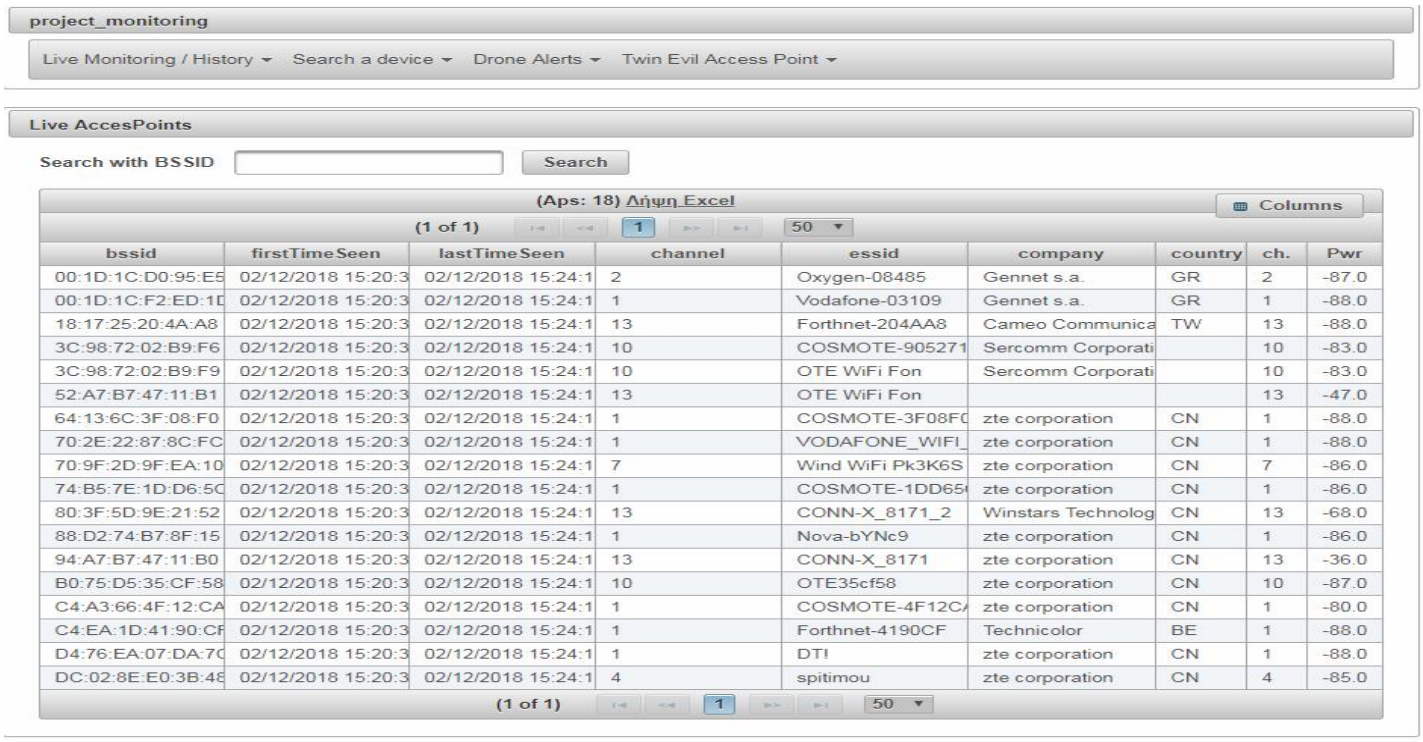
Εικόνα 6.2.1.2 History of Client

Με την επιλογή **Search with Station_Mac**, ο χρήστης μπορεί να αναζητήσει μία συσκευή εάν γνωρίζει τη MAC διεύθυνσή της.

Η επιλογή **Live Mac Access Points** (**Εικόνα 6.2.1.3**): απεικονίζει τα παρακάτω χαρακτηριστικά για τους σταθμούς βάσεις σε λειτουργία :

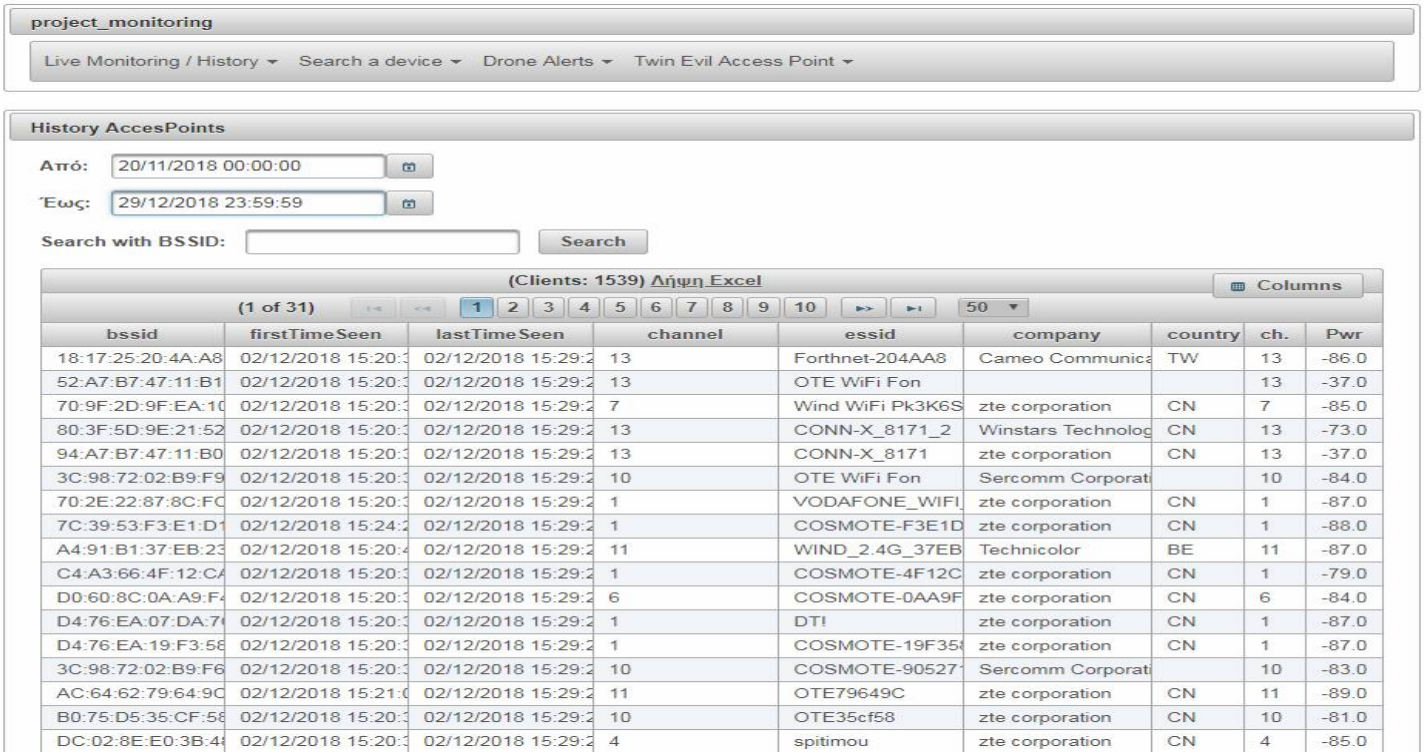
- Bssid : Την Mac διεύθυνση του σταθμού βάσης ή αλλιώς το BSSID.
- First time seen : Η ώρα και ημερομηνία που τέθηκε εντός εμβέλειας ή λειτουργίας ο κάθε σταθμός βάσης.
- Last time seen : Η ώρα και ημερομηνία όπου ο σταθμός βάσης προβλήθηκε για τελευταία φορά.
- channel : Το κανάλι λειτουργίας του σταθμού βάσης.

- essid : Το όνομα που έχει δοθεί στον σταθμό βάσης.
- Company : Η εταιρία κατασκευής της ασύρματης κάρτας δικτύου του σταθμού βάσης.
- Power : Η ισχύς σήματος εκπομπής της κεραίας του σταθμού βάσης.



Εικόνα 6.2.1.3. Live Access Points

Η επιλογή **History Access Points** (Εικόνα 6.2.1.4) : Απεικονίζει το ιστορικό των Access Point από μία δεδομένη χρονική στιγμή την οποία επιλέγει ο χρήστης.



Εικόνα 6.2.1.4 History of Access Points

Με την επιλογή **Search with BSSID**, ο χρήστης μπορεί να αναζητήσει ένα συγκεκριμένο Access Point εάν γνωρίζει τη MAC διεύθυνσή του.

Σενάρια χρήσης της Live πληροφορίας:

- **Monitoring ασύρματων συσκευών**

Ο σκοπός του Monitoring των συσκευών δίνει την δυνατότητα σε έναν οργανισμό να μπορεί να έχει πλήρη εικόνα των συσκευών που υπάρχουν στην περιοχή των εγκαταστάσεών του. Οι άνθρωποι που απαρτίζουν τον οργανισμό θα πρέπει να καταχωρούν τα στοιχεία κάθε συσκευής υπό την κατοχή τους, έτσι ώστε να θεωρείται εξουσιοδοτημένη η παρουσία τους στον χώρο. Κάθε νέα συσκευή που ανιχνεύεται και δεν έχει δηλωθεί θα θεωρείται μη εξουσιοδοτημένη και θα χρήζει περαιτέρω διερεύνησης. Δεδομένου πως ο οργανισμός θα είναι πλήρως δικτυωμένος με συσκευές Monitoring σε όλους τους χώρους της εγκατάστασης, θα έχει την δυνατότητα να εντοπίσει την μη εξουσιοδοτημένη συσκευή και να διερευνήσει την ύπαρξή της.

- **Ενέργειες με βάση τα ανιχνευόμενα MAC adresses.**

Δεδομένου πως κάθε μέλος ενός οργανισμού διαθέτει τουλάχιστον μία συσκευή η οποία λειτουργεί υπό το πρωτόκολλο 802.11, όπως ένα κινητό τηλέφωνο, η πληροφορία της παρουσίας του στον χώρο μέσω της Monitoring συσκευής μπορεί με τον κατάλληλο προγραμματισμό, να του προσφέρει την απαραίτητη εξουσιοδότηση για την πρόσβαση στους χώρους του κτηρίου όπου του αναλογούν, ή λειτουργίες όπως η ενεργοποίηση του υπολογιστή του κατά την άφιξη του, η ενεργοποίηση του φωτισμού ή της θέρμανσης στο γραφείο όπου εργάζεται, κ.α.

- **Έλεγχος μη εξουσιοδοτημένων Access Points στον εργασιακό Χώρο.**

Επειδή ένας σταθμός βάσης είναι αρκετά οικονομικός, οποιοσδήποτε εργαζόμενος ενός οργανισμού θα είναι σε θέση τοποθετήσει έναν σταθμό βάσης ως προέκταση του ενσύρματου δικτύου της εταιρίας, προκειμένου να διευρύνει χωρίς άδεια, πρόσβαση των προσωπικών του συσκευών στο δίκτυο. Η τοποθέτηση ερασιτεχνικού εξοπλισμού στο ήδη υπάρχον δίκτυο μπορεί να επιφέρει κενά ασφαλείας στον οργανισμό. Επειδή οι υπάλληλοι γενικώς δεν ενεργοποιούν σύνθετα πρωτόκολλα ασφαλείας, η ύπαρξη ενός τέτοιου δικτύου μπορεί να γίνει αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες οι οποίοι επιθυμούν να προσκομίσουν ευαίσθητες πληροφορίες προς όφελός τους. Επίσης, τα δίκτυα αυτά μπορούν να τοποθετηθούν σε μη ασφαλείς περιοχές του οργανισμού, επεκτείνοντας το δίκτυο εκτός των φυσικών συνόρων του οργανισμού.

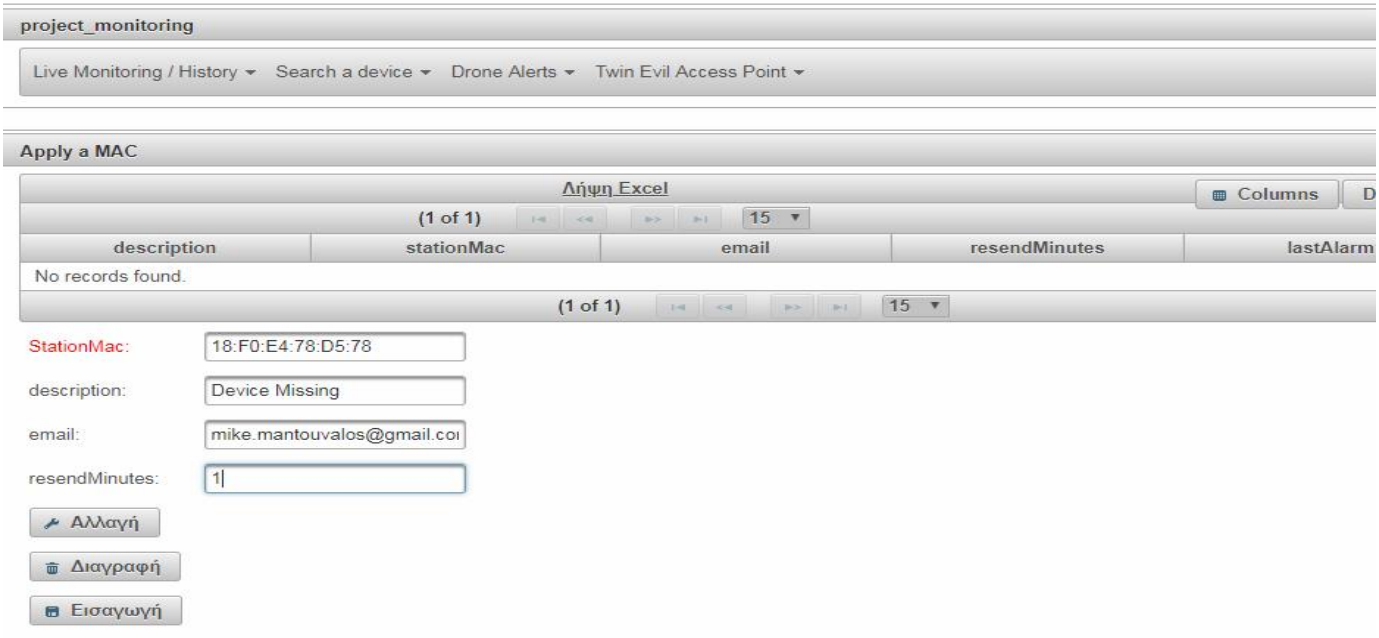
6.2.2 Search A device

Η δεύτερη κατηγορία της εφαρμογής περιέχει την λειτουργία της αναζήτησης στοχευμένων Client και Access Point. Μόλις η συσκευή εντοπιστεί ο διαχειριστής του Project_Monitoring λαμβάνει ειδοποίηση με e-mail.

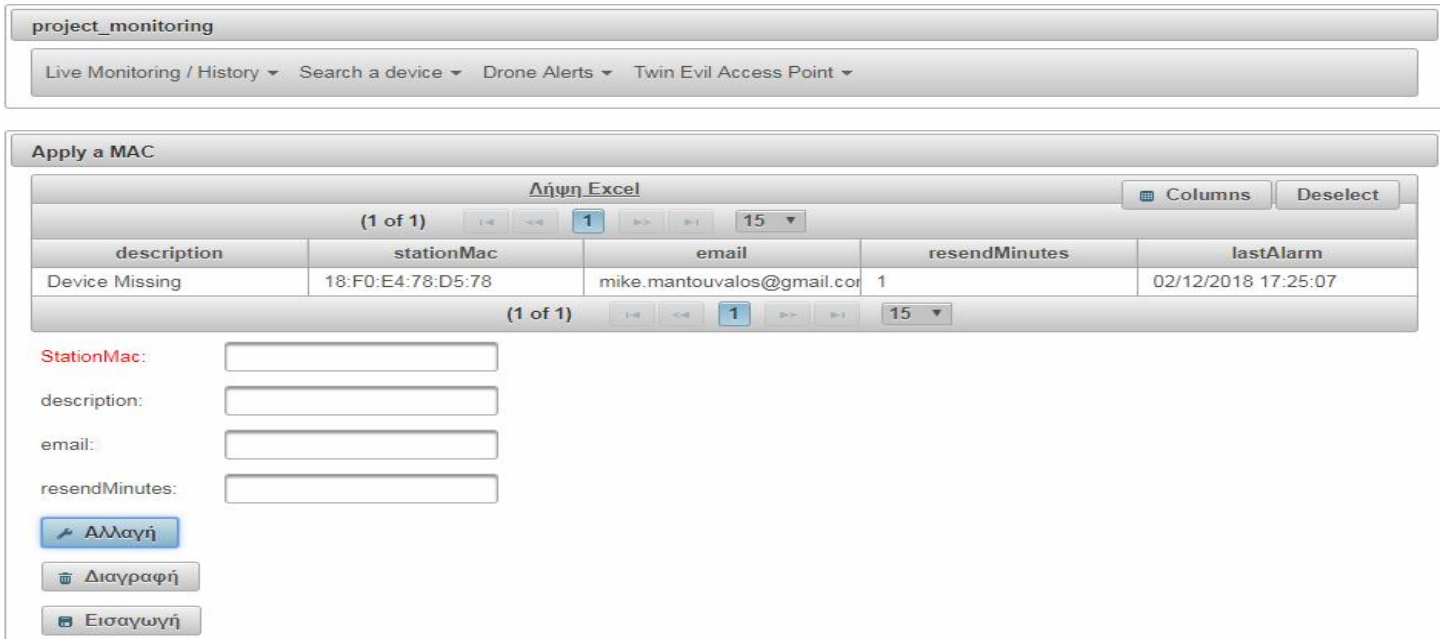
Σενάρια χρήσης :

- Αναζήτηση συσκευής που έχει χαθεί δεδομένης της φορητότητας της συσκευής Project_Monitoring
- Ειδοποίηση μόλις μία συσκευή εισέλθει στον χώρο.

Με την επιλογή **Apply a MAC** (εικόνα 6.2.2.1), ο χρήστης θέτει το MAC Address της συσκευής που τον ενδιαφέρει να αναζητήσει.

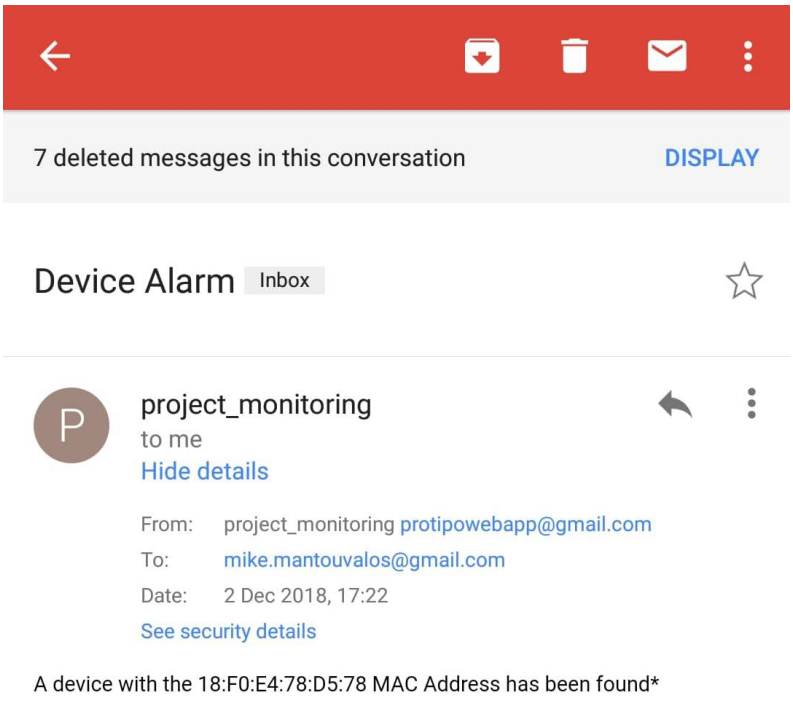


Εικόνα 6.2.2.1 Καταχώρηση Mac Διεύθυνσης συσκευής προς αναζήτηση.



Εικόνα 6.2.2.2 Ολοκλήρωση καταχώρησης.

Μόλις η εφαρμογή Project_Monitoring εντοπίσει την συσκευή, στέλνει email στον διαχειριστή όπως φαίνεται στην εικόνα 6.2.2.3.



Εικόνα 6.2.2.3 Ειδοποίηση Εύρεσης συσκευής

6.2.3 Drone Alerts

Η δεύτερη λειτουργία του Project_Monitoring αποσκοπεί στην ανίχνευση των γειτονικών από την συσκευή drones τα οποία αξιοποιούν το πρωτόκολλο IEEE 802.11 προκειμένου είτε να τα χειριστεί ο χρήστης τους, είτε να ανταλλάξουν live εικόνα μαζί του. Στο εμπόριο υπάρχουν διάφοροι τρόποι που οι παραπάνω λειτουργίες μπορούν να λάβουν χώρα, όμως στην παρούσα διπλωματική θα μελετηθούν τα drones που αξιοποιούν το δημοφιλέστερο πρωτόκολλο ασύρματης επικοινωνίας, καθώς είναι το εμπορικά πιο διαδεδομένο και οικονομικό. Στόχος είναι μέσω της συσκευής, ο παρατηρητής να μπορεί να εντοπίσει τα πλησιέστερα μη εξουσιοδοτημένα drones

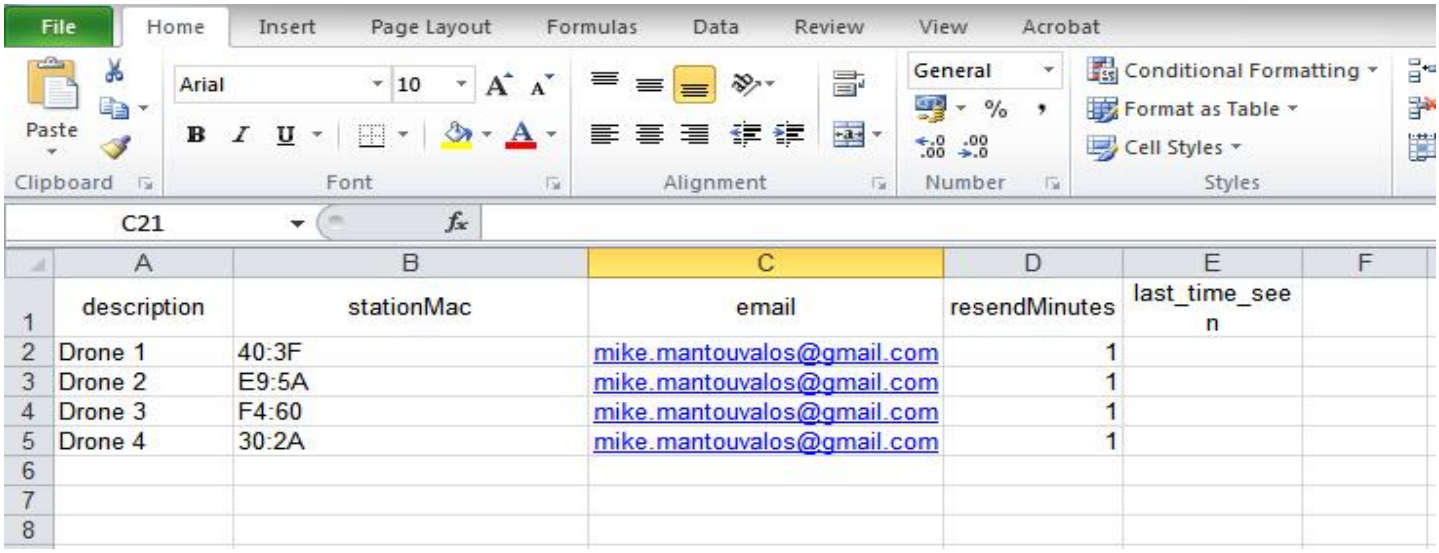
προκειμένου να αμυνθεί από τις ενδεχόμενες απειλές που αυτά μπορεί να προξενήσουν. Πηγή έμπνευσης για τη συγκεκριμένη λειτουργία αποτέλεσε το video στο Youtube του : Samy Kamkar ο οποίος δημιούργησε μία συσκευή Raspberry η οποία τοποθετημένη σε drone και κατάλληλα παραμετροποιημένη είναι σε θέση να ανιχνεύσει τα γειτονικά σε αυτή WiFi drones και να λάβει τον πλήρη έλεγχο της λειτουργίας τους. Πηγή : https://www.youtube.com/watch?v=EHKV01YQX_w&t=297s. Προκειμένου ο χειριστής ενός drone να έχει Live εικόνα από αυτό χρειάζεται να εγκαταστήσει σε αυτό FPV (First Person View) εξοπλισμό. Οι δημοφιλέστεροι τρόποι FPV που είναι διαθέσιμοι στο εμπόριο είναι :

- 2.4 Ghz ή 5 Ghz analog
- 2.4 Ghz ή 5 Ghz digtal (WiFi)

Με βάση τις παραπάνω διαφορετικές εκδοχές του FPV η ψηφιακή (WiFi) είναι η δημοφιλέστερη μεταξύ των "budget" drones. Σχεδόν κάθε FPV-enabled drone διαθέτει αυτού του είδους την επικοινωνία. Αυτό οφείλεται στο γεγονός ότι ο FPV πομπός που είναι συνδεδεμένος με την Camera του drone χρησιμοποιεί το πρωτόκολλο IEEE 802.11 το οποίο είναι ευρέως διαδομένο και δεν απαιτεί καμία αγορά επιπλέον εξοπλισμού, αφού μπορεί να χρησιμοποιηθεί από οποιαδήποτε συσκευή διαθέτει την τεχνολογία αυτή (smartphones, tablets, laptops). Επιπλέον, λόγω της ψηφιακής λειτουργίας της, παρέχει στον χρήστη πολύ πιο καθαρή εικόνα εν συγκρίσει με τις αναλογικές εκδοχές της. Προκειμένου να λειτουργήσει το WiFi FPV το drone δρα ως Access Point και η ασύρματη συσκευή του χειριστή ως Client ο οποίος συνδέεται με αυτόν. Δεδομένης της παραπάνω διαδικασίας, κάθε ασύρματη κάρτα δικτύου ενός drone διαθέτει και εκπέμπει μία μοναδική MAC address, παρόμοια με την λειτουργία ενός τοπικού ασύρματου Access Point. Ως εκ τούτου κάθε κατασκευαστής drone δεσμεύει το Organization Unique Identifier (OUI) της MAC διεύθυνσης που χρησιμοποιεί, και έτσι είναι δυνατή η ταυτοποίηση της, ως drone.

Στο διαδίκτυο υπάρχουν αρκετά sites τα οποία λειτουργούν ως βάσεις δεδομένων με όλα τα OUIs από τους διάφορους κατασκευαστές ασύρματων καρτών δικτύου και με την βοήθεια αυτόν η εφαρμογή Project_Monitoring μπορεί να αναγνωρίσει αν η συσκευή που ανίχνευσε αφορά μία από τις εμπορικές αυτές συσκευές μη επανδρωμένων αεροσκαφών. Μερικά από τα δημοφιλέστερα drones με WiFi FPV είναι τα : DJI Mavic Air, DJI Mavic 2 Pro, DJI Spark, DJI Phantom 4, Parrot Bebop 2, DJI Mavic Pro, Parrot Anafi, DJI Inspire 1, DJI Insipire 2, ZeroTech Dobby.

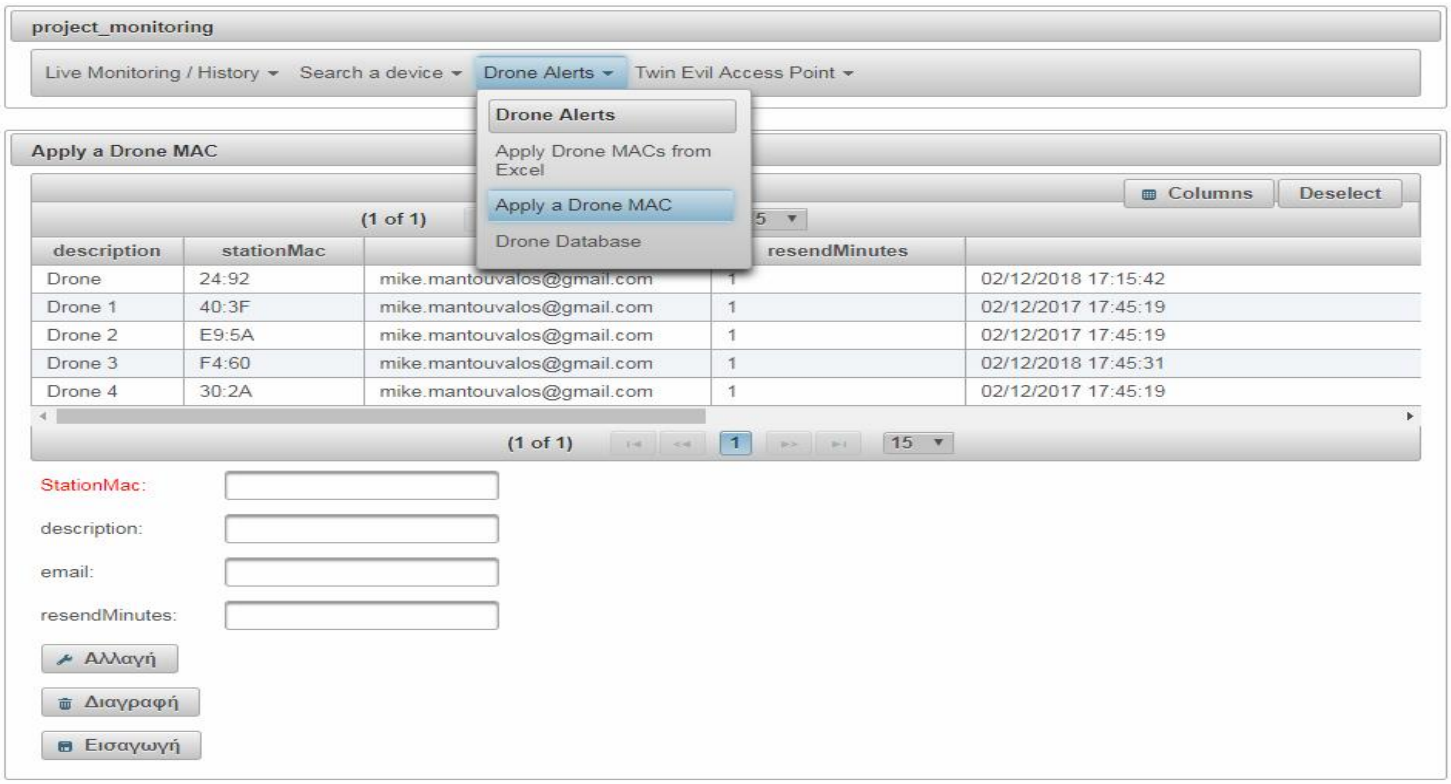
Η επιλογή **Apply Drone Macs from Excel**, παρέχει την δυνατότητα στον διαχειριστή της εφαρμογής να καταχωρήσει μαζικά τα Mac addresses της επιλογής του. Στην Εικόνα 6.2.3.1 δίνεται παράδειγμα της καταχώρησης τεσσάρων OUI Mac adresses.



	A	B	C	D	E	F
1	description	stationMac	email	resendMinutes	last_time_seen	
2	Drone 1	40:3F	mike.mantouvalos@gmail.com	1		
3	Drone 2	E9:5A	mike.mantouvalos@gmail.com	1		
4	Drone 3	F4:60	mike.mantouvalos@gmail.com	1		
5	Drone 4	30:2A	mike.mantouvalos@gmail.com	1		
6						
7						
8						

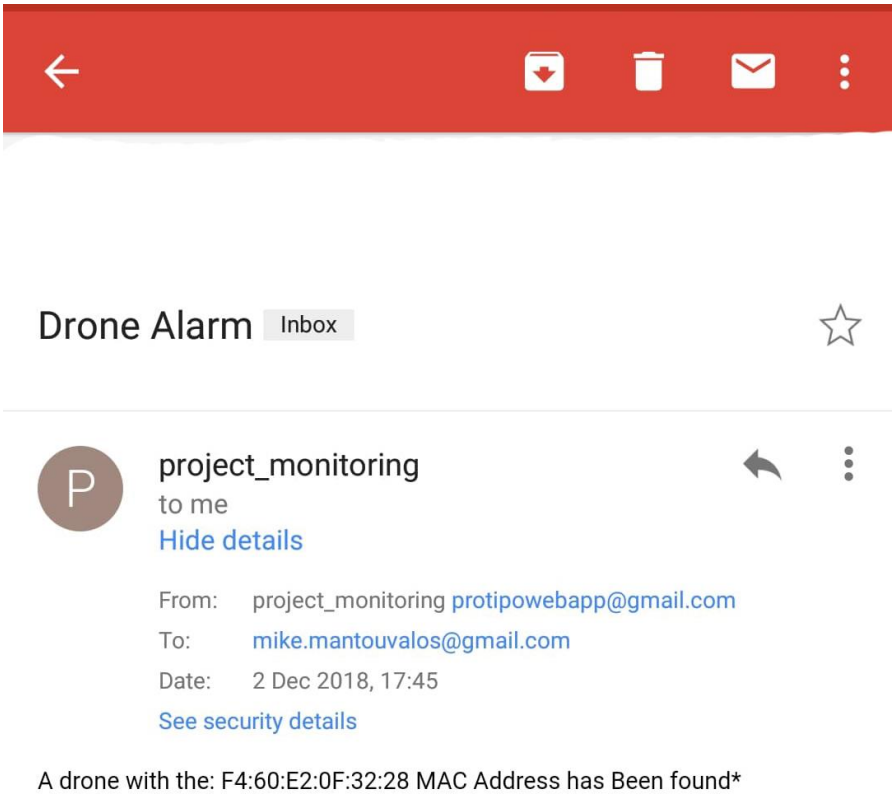
Εικόνα 6.2.3.1 Excel καταχώρησης Drone.

Αφού αυτά καταχωρηθούν επιτυχώς στο μενού : Apply a drone MAC θα έχουν καταχωρηθεί επιτυχώς. Να σημειωθεί πως εάν ο διαχειριστής το επιθυμεί, μπορεί και να καταχωρήσει και άλλες MAC διευθύνσεις ή OUI MAC διευθύνσεων χειροκίνητα από αυτή τη σελίδα από τις επιλογές που εμφανίζονται στην εικόνα 6.2.3.2.



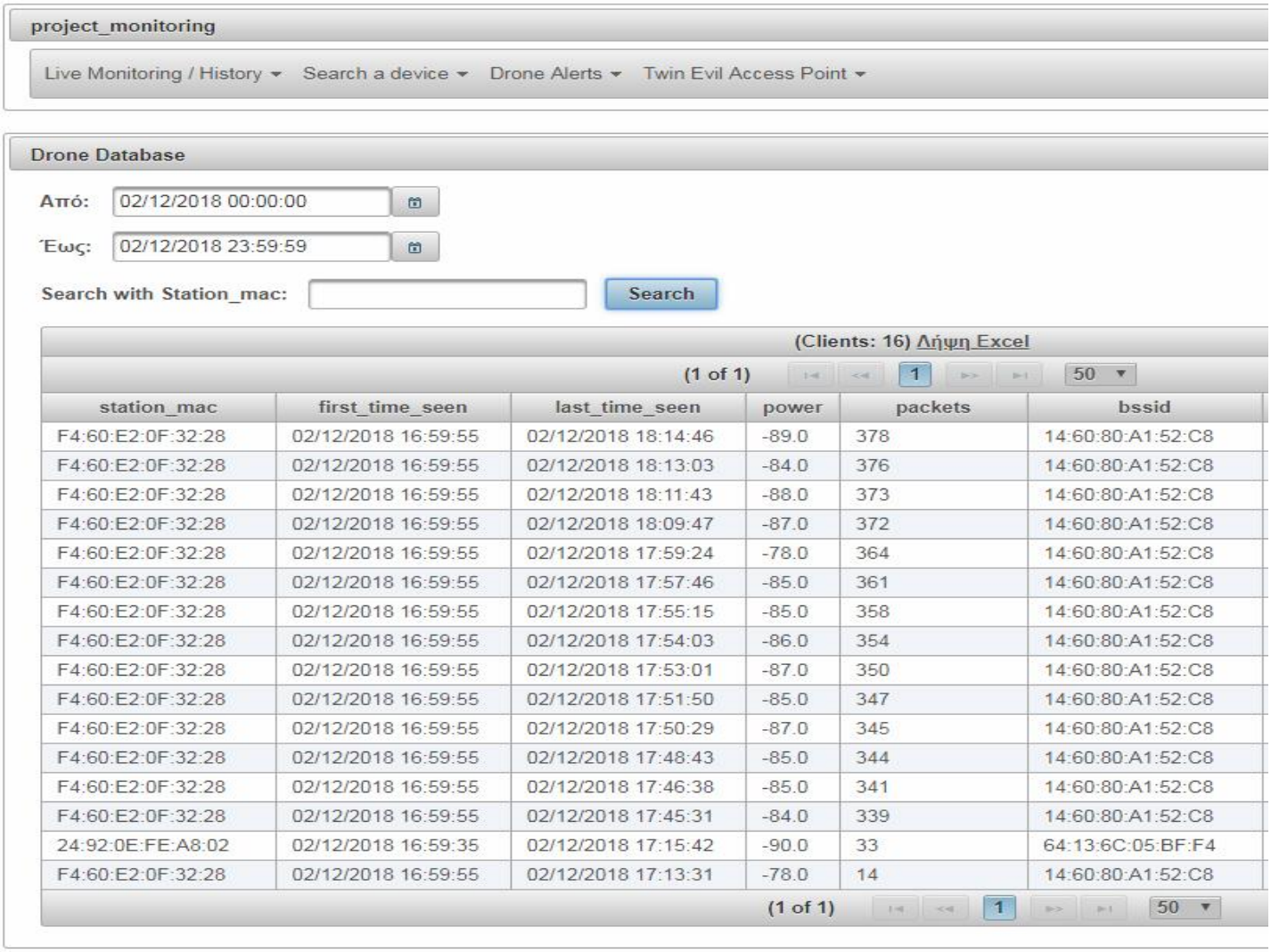
Εικόνα 6.2.3.2 Apply A Drone MAC

Με τη καταχώρηση των OUI των κατασκευαστών drones, η εφαρμογή Porject_Monitoring βρίσκεται σε αναμονή για την ειδοποίηση του διαχειριστή κατά την εμφάνισή τους. Μόλις εντοπιστεί κάποιο από αυτά, θα ληφθεί mail προειδοποίησης στο διαχειριστικό email. Εικόνα 6.2.3.3



Εικόνα 6.2.3.3 Drone alarm

Στη περίπτωση αυτή ο διαχειριστής έλαβε mail για εισερχόμενο Drone με OUI MAC διεύθυνση : F4:60 , και συγκεκριμένα το drone με MAC διεύθυνση : F4:60:E2:0F:32:28 Με την επιλογή Drone Database ο διαχειριστής έχει τη δυνατότητα να ανατρέξει στο ιστορικό των Drone που η συσκευή έχει εντοπίσει, επιλέγοντας την ημερομηνία που τον ενδιαφέρει. Εικόνα 6.2.3.4



Εικόνα 6.2.3.4 Drone Database

6.2.4 Twin Evil Access Points.

Η τρίτη λειτουργία της συσκευής έχει προγραμματιστεί για να μπορεί να ανιχνεύει επιθέσεις MAN IN THE MIDDLE (MITM) επιθέσεις με την χρήση κακόβουλου ενδιάμεσου Access Point (Twin Evil Access Point).

Τα ασύρματα δίκτυα αποτελούν την πύλη στο διαδίκτυο για συσκευές, όπως έξυπνα κινητά τηλέφωνα, φορητούς υπολογιστές ή tablets. Η ανάπτυξη και χρήση ασύρματων συσκευών έχει αυξήσει την κυκλοφορία δεδομένων εντός των ασύρματων δικτύων. Ορισμένες επιχειρήσεις όπως καφετέριες, εστιατόρια, αεροδρόμιο και εμπορικά κέντρα, παρέχουν στους πελάτες τους δωρεάν υπηρεσίες Wi-Fi. Εκτός από την εκφόρτωση δεδομένων από κυψελοειδή δίκτυα κινητής τηλεφωνία, τα WiFi Access Points παρέχουν μία γρήγορη, δωρεάν και φιλική προς τον χρήστη εναλλακτική για πρόσβαση στο διαδίκτυο[68].

Ωστόσο, για λόγους ευκολίας της πρόσβασης, τα περισσότερα δημόσια ασύρματα δίκτυα δεν περιέχουν εξιδεικευμένες τεχνικές προστασίας όσον αφορά στον έλεγχο ταυτότητας ή την κρυπτογράφηση των δεδομένων. Όταν ένας ασύρματος χρήστης επιθυμεί να αποκτήσει πρόσβαση σε ένα δημόσιο ασύρματο δίκτυο, συνήθως χρειάζεται να συμφωνήσει με τους όρους και τις προϋποθέσεις του δικτύου, στους οποίους ο πάροχος αναφέρει πως το δίκτυό του ενδέχεται να μην είναι ασφαλές και προτείνει στους χρήστες να αποφεύγουν να ανταλλάσσουν ευαίσθητες πληροφορίες μέσω αυτού. Δίκτυα όπως αυτά, προσφέρουν ένα δελεαστικό περιβάλλον για τους επιτιθέμενους προκειμένου αυτοί να εφαρμόσουν διάφορες επιθέσεις, μία εκ των οποίων είναι η επίθεση που αποκαλείται : Evil Twin Access Point (ETA). Ως ETA αποκαλείται η επίθεση με την οποία ένας κακόβουλος χρήστης δημιουργεί με τον κατάλληλο εξοπλισμό, ένα δίδυμο σημείο πρόσβασης το οποίο χρησιμοποιεί το ίδιο SSID με το εξουσιοδοτημένο. Δεδομένου πως στον χρήστη το μόνο αναγνωριστικό ενός ασύρματου δικτύου είναι το SSID και το MAC address, δεν υπάρχει τρόπος αυτός να αντιληφθεί την διαφορά μεταξύ των δύο δικτύων εάν αυτά μοιράζονται το ίδιο όνομα. Ο κακόβουλος χρήστης, μπορεί να στήσει το δικό του σημείο πρόσβασης, στην περιοχή εμβέλειας του εξουσιοδοτημένου και με διάφορες τεχνικές να τους αναγκάσει να συνδεθούν σε αυτό [68].

Ένα ETA χρησιμοποιεί αρκετά μεγάλη εκπομπή σήματος, κάτι που αναγκάζει τις συσκευές που είναι ήδη συνδεδεμένες στο εξουσιοδοτημένο Access Point, να αλλάξουν τη σύνδεσή τους με αυτή του κακόβουλου, καθώς αυτές συνδέονται αυτόματα στο δίκτυο με το μεγαλύτερο RSSI (Received signal strength indication). Κατά τη σύνδεση των χρηστών στο κακόβουλο δίκτυο, ο θύτης μπορεί να κατασκοπεύσει την κίνηση των θυμάτων, ξεκινώντας έτσι την MITM επίθεση. Βασική προϋπόθεση για την απόσπαση ευαίσθητων πληροφορίων, όπως κωδικοί πρόσβασης ή στοιχεία πιστωτικών καρτών είναι η πρόσβαση των χρηστών στο διαδίκτυο. Ο

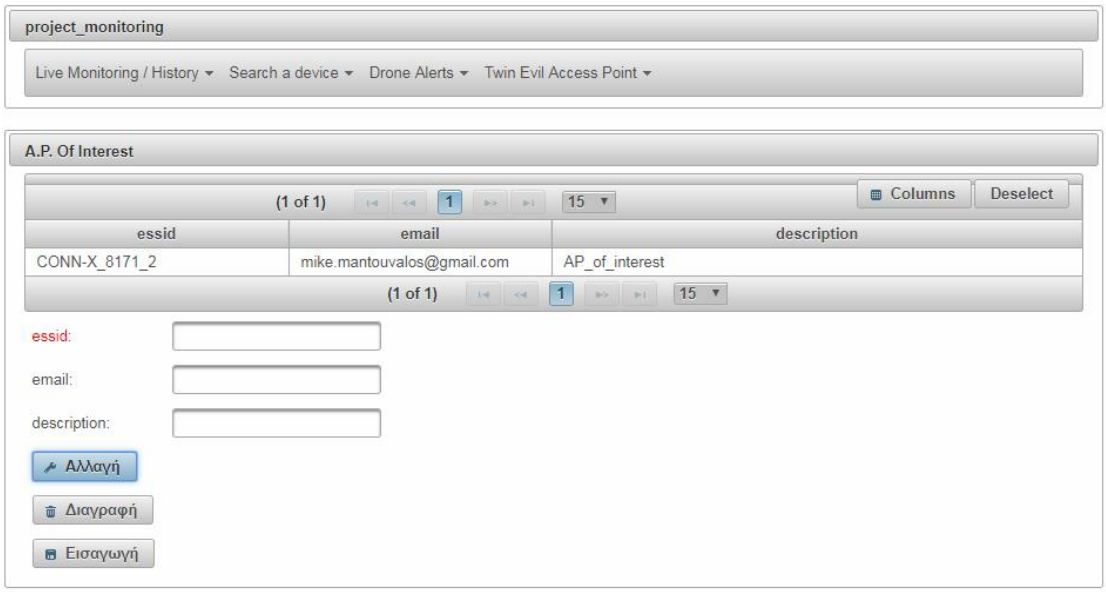
εισβολέας έχει δύο επιλογές για να κατευθύνει τα δεδομένα των ανυποψίαστων χρηστών στο διαδίκτυο. Μπορεί είτε να μεταβιβάσει την πρόσβαση από το κανονικό δίκτυο, είτε να χρησιμοποιήσει την δική του κυψελωτή ευρυζωνική σύνδεση 4G [68].

Η παραπάνω τεχνική αφορά μπορεί να εφαρμοστεί επιπλέον και σε περιπτώσεις όπου το ασύρματο δίκτυο είναι διασφαλισμένο με κωδικό προστασίας. Βασική προϋπόθεση είναι ο επιτιθέμενος να γνωρίζει το κλειδί εισόδου στο δίκτυο προκειμένου να μπορεί να καταχωρήσει το ίδιο και στον δίδυμο σταθμό βάσης του. Με τον τρόπο αυτόν και με την ενσωμάτωση του εξοπλισμού σε drone, μπορεί να στήσει απομακρυσμένα την συγκεκριμένη επίθεση, στοχεύοντας σε οργανισμούς και επιχειρήσεις [68].

Η εφαρμογή Project_Monitoring μπορεί να ρυθμιστεί κατάλληλα ώστε ο χειριστής της, να θέσει σε αυτήν τα Access Points που αναγνωρίζει ως εξουσιοδοτημένα. Όταν αυτή μετά από την ανίχνευση των γειτονικών Access Points διαπιστώσει πως υπάρχει ένα επιπλέον ασύρματο AP με το ίδιο SSID αλλά με διαφορετική MAC address, ειδοποιεί τον χειριστή ότι έχει ανιχνευτεί μη εξουσιοδοτημένος σταθμός βάσης.

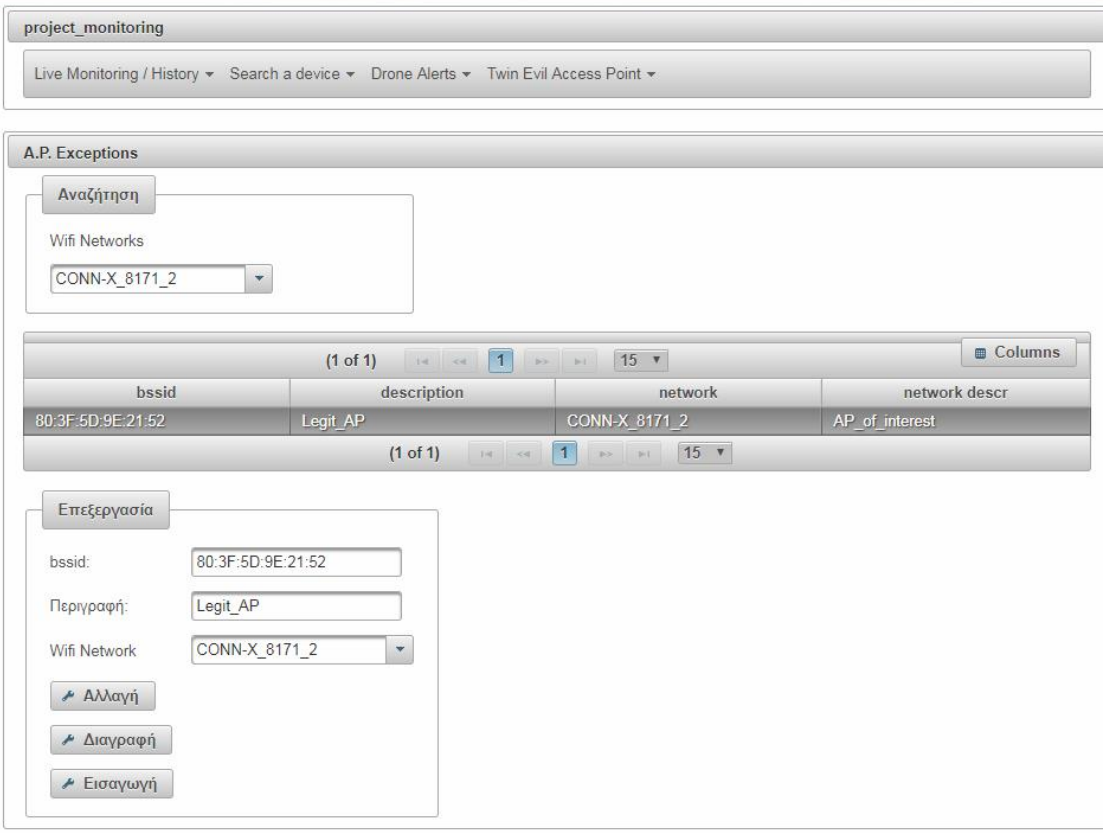
Παράδειγμα χρήσης :

Ο χρήστης θέτει την ονομασία του δικτύου που τον ενδιαφέρει να διασφαλίσει, το email στο οποίο επιθυμεί να γίνει η αποστολή της ειδοποίησης καθώς και μία περιγραφή. Στο παράδειγμα της εικόνας 6.2.4.1, ορίζουμε ως ενδιαφερόμενο δίκτυο το : CONN-X_8171_2 , ως email αποστολής το: mike.mantouvalos@gmail.com και ως περιγραφή το : AP_of_interest.



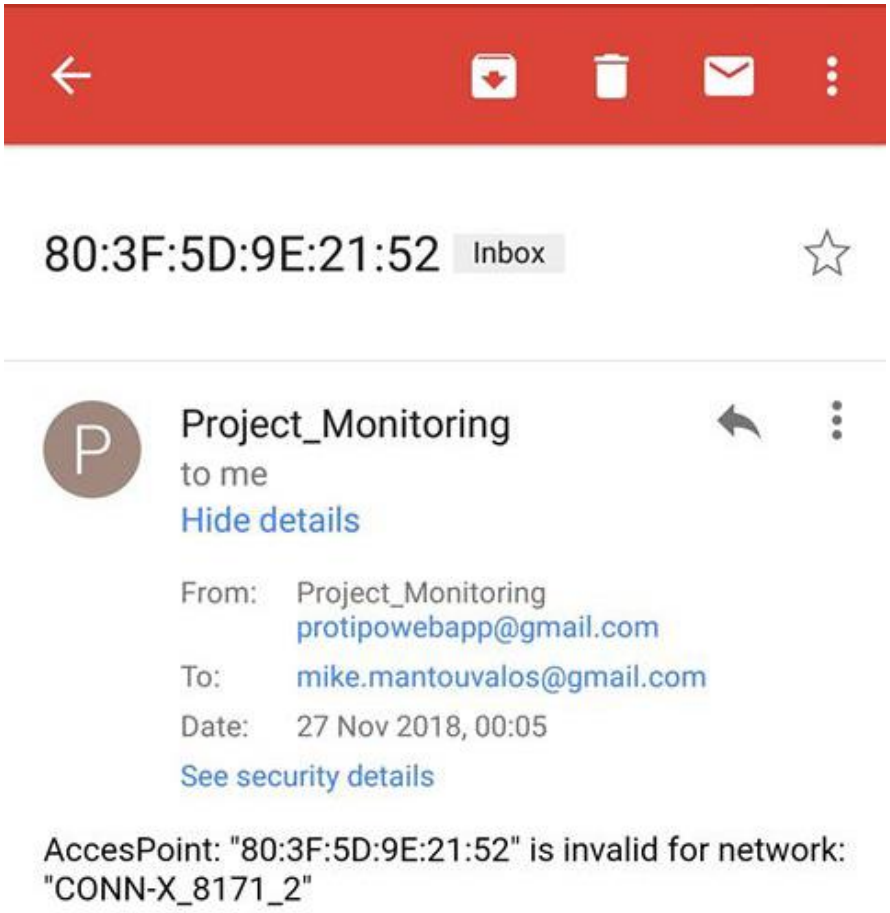
Εικόνα 6.2.4.1 Ορισμός AP ενδιαφέροντος

Στην επόμενη κατηγορία ο διαχειριστής αφού συμβουλευτεί την σελίδα : Live Access Points, βρίσκει την MAC διεύθυνση των Access Point που τον ενδιαφέρουν και την καταχωρεί στο πεδίο : bssid, προκειμένου να τα εξαιρέσει από την ειδοποίηση για Twin Evil Access Point. Στο συγκεκριμένο παράδειγμα το AP ενδιαφέροντος είναι το : CONN-X_8171_2 και η MAC address που εξαιρείται είναι η : 80:3F:50:9E:21:52. Για τους σκοπούς του παραδείγματος, δόθηκε σε δεύτερο AP η ίδια ονομασία, και τέθηκε σε λειτουργία.



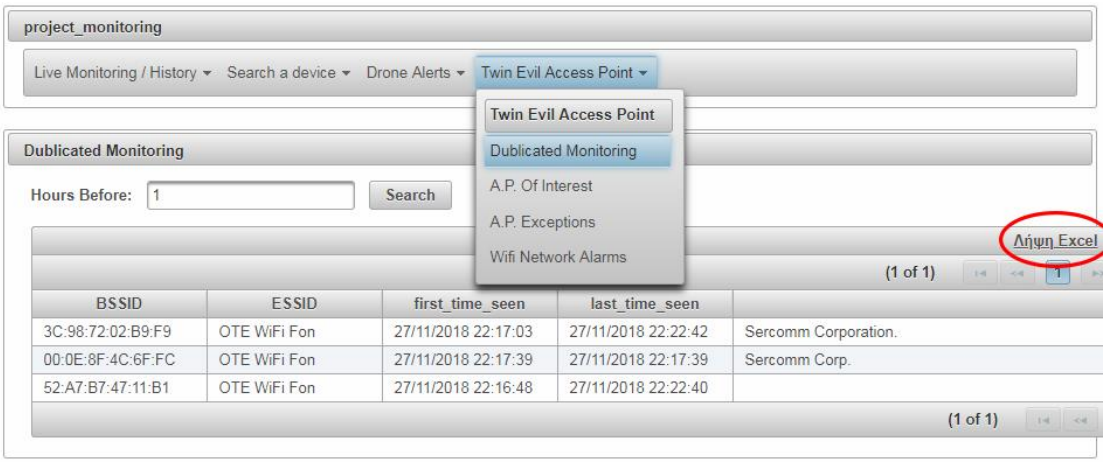
Εικόνα 6.2.4.2 Εξαίρεση Access Point που δεν αποτελούν απειλή.

Ο διαχειριστής στη συνέχεια λαμβάνει ειδοποίηση για την μη εξουσιοδοτημένη παρουσία του δεύτερου CONN-X_8171_2 router με MAC Address : 80:3F:5D:9E:21:52. Εικόνα 6.2.4.3



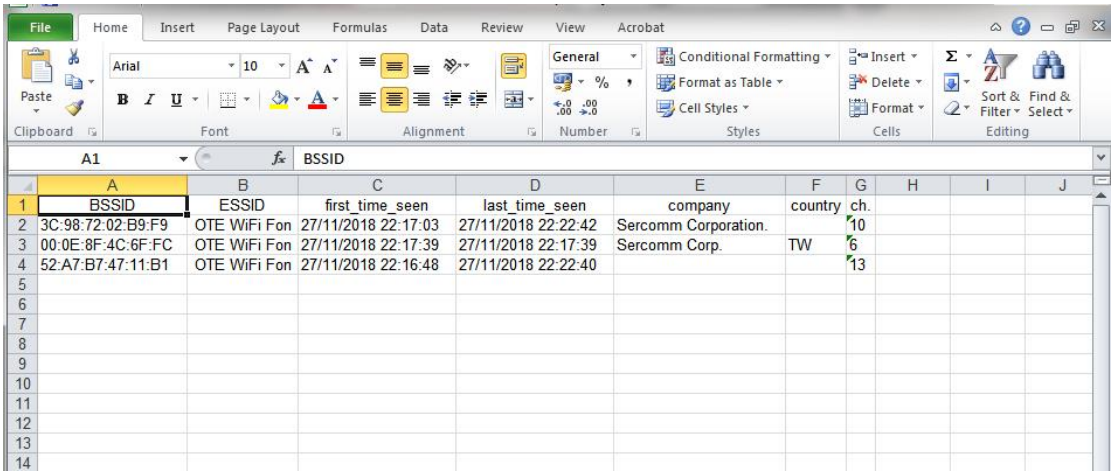
Εικόνα 6.2.4.3 Ειδοποίηση Twin Evil

Dublicated Monitoring : Δίνει στον χρήστη την επιλογή να δει πόσα δίδυμα Access Points υπάρχουν στον χώρο την δεδομένη στιγμή.



Εικόνα 6.2.4.4 Dublicated Monitoring

Με την λήψη excel ο διαχειριστής μπορεί να κατεβάσει το αρχείο Excel στο οποίο τα δίδυμα Access Points αποτυπώνονται.



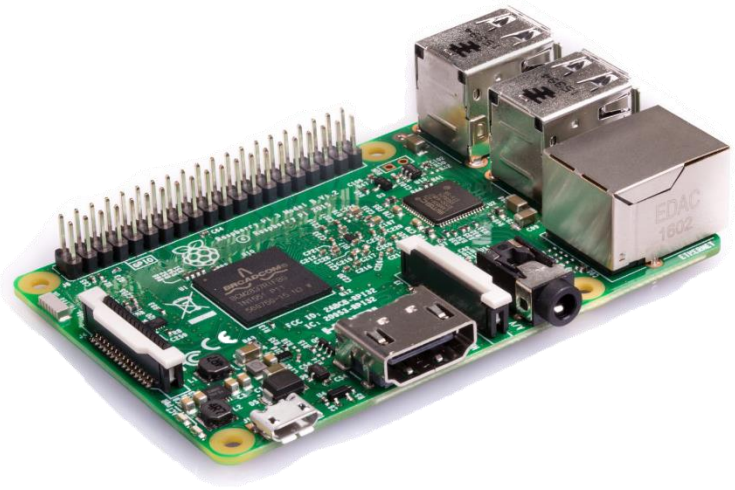
Εικόνα 6.2.4.5 Live Twin Excel

6.3 Hardware

Όπως αναφέρθηκε προηγουμένως, σε αυτή την εργασία πραγματοποιήθηκε ο σχεδιασμός και η υλοποίηση ενός συστήματος βασισμένο σε ένα σύγχρονο υπολογιστικό σύστημα. Σε πρώτο στάδιο έγινε η επιλογή του υλικού (hardware) που απαρτίζει το σύστημα. Το στάδιο αυτό είναι ιδιαίτερα σημαντικό, καθώς εδώ επιλέγονται όλα τα κομμάτια που θα πρέπει στη συνέχεια να προγραμματιστούν και να λειτουργήσουν μαζί. Η επιλογή του υλικού αποτελεί το πρώτο βήμα στην διαδικασία σχεδιασμού οποιουδήποτε συστήματος. Στις υπόλοιπες ενότητες αυτού του κεφαλαίου παρουσιάζονται τα κομμάτια του υλικού που χρησιμοποιήθηκαν στην εργασία αυτή και περιγράφεται ο τρόπος λειτουργίας τους, καθώς και βασικά στοιχεία γι' αυτά.

6.3.1 Raspberry Pi

Το ρόλο του ανιχνευτή των γειτονικών ασύρματων συσκευών στο συγκεκριμένο project διαδραματίζει το raspberry pi (Εικόνα 4.2) σε συνδυασμό με μία εξωτερική ασύρματη WIFI κάρτα PANDA PAU09 (Εικόνα 4.3) Αξίζει να σημειωθεί πως για τον ρόλο του ανιχνευτή δεν είναι απαραίτητο να χρησιμοποιηθεί Raspberry PI , αλλά οποιαδήποτε υπολογιστική μονάδα με δυνατότητα εκτέλεσης των προγραμμάτων που χρησιμοποιήθηκαν στο παρόν project.



Εικόνα 6.3.1 Raspberry Pi 3

Το Raspberry pi αποτελεί έναν υπολογιστή σε μέγεθος πιστωτικής κάρτας. Αναπτύχθηκε από την Raspberry Pi Foundation και σκοπό είχε την προώθηση της διδασκαλίας της επιστήμης των υπολογιστών σε σχολεία. Είναι μια συσκευή η οποία Κεφάλαιο 4 50 παρουσιάζει πολλές δυνατότητες και είναι ικανή για λειτουργίες που συνήθως της κάνει ένας προσωπικός υπολογιστής, όπως προβολή ταινιών, παιχνίδια, internet browsing κλπ. Λόγω του μεγέθους και των δυνατοτήτων του χρησιμοποιείται σε πολλά project.

6.3.2 Panda PAU09

Όσον αφορά στην ασύρματη κάρτα δικτύου, επιλέχθηκε η Panda PAU09 η οποία σε αντίθεση με την ενσωματωμένη ασύρματη κάρτα δικτύου του Raspberry, η οποία έχει την δυνατότητα να τεθεί σε λειτουργία : Monitor mode, καθώς και να ανιχνεύσει εκπομπές σημάτων τόσο στα 2.4 MHz όσο και στα 5 Mhz.

Εικόνα : 6.3.2 : Panda PAU09 external wireless WIFI card.

Το Monitor mode ή RFMON (Radio Frequency MONitor) mode, επιτρέπει σε έναν υπολογιστή με Wireless network interface controller (WNIC) να απεικονίζει (monitoring) όλη την κίνηση των ασύρματων συσκευών που χρησιμοποιούν το πρωτόκολλο IEEE 802.11 στο ασύρματο μέσο. Εν αντιθέσει με το Promiscuous mode, το οποίο χρησιμοποιείται επίσης για packet sniffing, το monitoring mode επιτρέπει την σύλληψη των πακέτων από τους κοντινούς χρήστες (Clients) χωρίς αυτοί να έχουν συνδεθεί πρώτα σε κάποιο σημείο πρόσβασης (Access Point).

6.4 Software

Το λογισμικό που χρησιμοποιήθηκε παρουσιάζεται παρακάτω :

- MySQL (βάση δεδομένων)
- JAVA (γλώσσα προγραμματισμού)
- Java Server Faces (Front End Framework)
- Kali Linux (διανομή linux με ενσωματωμένα εργαλεία ελέγχου ασφάλειας δικτύων)

- Apache Maven (εργαλείο διαχείρισης έργων λογισμικού)
- Apache Tomcat (Web Server)
- GIT (σύστημα ελέγχου εκδόσεων)
- Netbeans & Eclipse (εργαλεία ανάπτυξης κώδικα)
- Aircrack-ng (σουίτα εργαλείων για την αξιολόγηση της ασφάλειας δικτύου WiFi)

6.5 Αρχιτεκτονική βάσης δεδομένων

Ακολουθεί η αναλυτική περιγραφή των πινάκων της σχεσιακής βάσης δεδομένων.

- Πίνακας **macvendors**: σε αυτόν τον πίνακα αποθηκεύονται οι πληροφορίες σχετικά με το κάθε mac address που εντοπίζεται, είτε είναι client είτε Access Point είτε drone, αυτές οι πληροφορίες μας παρέχονται από την υπηρεσία https://macvendors.co/api/
- Πίνακας **user_permitions**: συστημικός πίνακας, δεν μας απασχολεί στην παρούσα εφαρμογή.
- Πίνακες **livemacclients** και **liveaccesspoints**: σε αυτούς τους πίνακες καταγράφεται η πιο πρόσφατη δικτυακή κίνηση των clients και Access Points αντίστοιχα. Τα περιεχόμενα τους εμφανίζονται στις σελίδες Live Mac Clients και Live AccessPoints.
- Πίνακες **historymacclients** και **historyaccesspoints**: καταγράφεται το αναλυτικό ιστορικό της δικτυακής κίνησης των clients και Access Points αντίστοιχα. Τα περιεχόμενα τους εμφανίζονται στις σελίδες History Mac Clients και History AccessPoints.
- Πίνακας **wifinetworks**: εδώ αποθηκεύονται τα δίκτυα που επίκεινται σε παρακολούθηση (βλέπε σελίδα A.P. Of Interest). Οι δύο επόμενοι πίνακες έχουν άμεση σύνδεση με αυτόν.

- Πίνακας **accesspoints**: Είναι τα routers που επιτρέπεται να εκπέμπουν wifi με essid τα οποία περιγράφονται στον πίνακα wifinetworks (βλέπε σελίδα A.P. Exceptions).
- Πίνακας **wifinetworksalarms**: εδώ καταγράφονται όσα routers εκπέμπουν wifi με καταχωρημένα essid στον πίνακα wifinetworks, αλλά δεν έχουν καταχωρηθεί τα bssid τους στον πίνακα accesspoints (βλέπε σελίδα Wifi Network Alarms).
- Πίνακες **dronesmacs** και **mac_detect_alarm**: Σε αυτούς τους πίνακες καταχωρούνται τα stationMacs των drones και απλών wifi clients που επίκεινται σε παρακολούθηση (βλέπε σελίδες Apply a Drone MAC και Apply a MAC).
- Πίνακες **drones_detect_alarm_history** και **detect_alarm_history**: Εδώ καταχωρούνται τα συμβάντα που καταγράφονται όταν εντοπίζονται τα stationMacs drones και απλών wifi clinets, που έχουν τεθεί σε παρακολούθηση από τους δύο παραπάνω πίνακες dronesmacs και mac_detect_alarm (βλέπε σελίδες Drone Database και Mac Database).

6.6 Αρχιτεκτονική εφαρμογής

Για την ανάπτυξη της εφαρμογής χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java. Ενώ η αρχιτεκτονική και η μεταγλώττιση του πηγαίου κώδικα σε εκτελέσιμο έγινε με το εργαλείο Maven. Το Project της εφαρμογής κατά τη μεταγλωττιστή μας παράγει δύο εκτελέσιμα αρχεία, ένα **jar** και ένα **war**.

Όσον αφορά στη μορφή του κώδικα, για να μπορέσει ο αναγνώστης να κατανοήσει το παρόν κεφάλαιο (Αρχιτεκτονική εφαρμογής), θα πρέπει να έχει μια βασική γνώση ανάπτυξης εφαρμογής βασισμένη στη γλώσσα προγραμματισμού Java. Όπως Προαναφέρθηκε το Project βασίζεται στην αρχιτεκτονική Maven, και όχι σε κάποια μορφή αποδεκτή μόνο από ένα συγκεκριμένο IDE, αυτό έχει σαν αποτέλεσμα να μπορούμε να κάνουμε Open το Project από οποιοδήποτε σχεδόν Java IDE, όπως Netbeans Eclipse κ.α.

Ας υποθέσουμε πως ανοίγουμε το project με το Netbeans, πρώτα απ' όλα θα παρατηρήσουμε ότι τα πακέτα χωρίζονται σε δυο βασικές κατηγορίες :

com.protipo.master και com.protipo.drones. Η πρώτη κατηγορία πακέτων είναι η γενική πλατφόρμα εφαρμογής στην οποία βασίστηκε η δεύτερη για να σχεδιαστεί συγκεκριμένα για τον σκοπό της πτυχιακής. Όπως είπαμε και παραπάνω το Project είναι ένα, αλλά κατά την μεταγλώττιση παράγονται δυο διαφορετικές εφαρμογές. Η πρώτη, είναι η εφαρμογή τύπου jar η οποία θα τρέξει στο raspberry σε συνεργασία με το Aircrack-ng.

6.6.1 Εφαρμογή Client

Σκοπός αυτής της εφαρμογής είναι να διαβάσει το παραγόμενο από το Aircrack csv αρχείο, και να το στείλει δικτυακά στον Server (εφαρμογή τύπου war). Ας δούμε, λοιπόν, στον κώδικα πως γίνεται αυτό. Η εκκίνηση της εφαρμογής jar γίνεται από την κλάση com.protipo.drones. Client.java . Ανοίγοντας αυτή με το Netbeans θα δούμε στην γραμμή 36 την εντολή :

DronesParameters.loadFromile();

Με αυτήν στην εντολή στήνεται η εφαρμογή με τις αρχικές παραμέτρους από το αρχείο /etc/Project_Monitoring/configuration_properties.txt, αυτές οι παράμετροι είναι απαραίτητες για την εκτέλεση της εφαρμογής, όπως για παράδειγμα το path του αρχείου csv που καταγράφεται από το Aircrack. Στις επόμενες γραμμές του κώδικα γίνεται ένα Loop αφού η διαδικασία ανάγνωσης και αποστολής θα πρέπει να είναι επαναλαμβανόμενη. Η πιο σημαντική συνάρτηση είναι η : readCSV_and_Send(args);

Σε αυτήν γίνεται η ανάγνωση του αρχείου csv, ο διαχωρισμός σε Wifi Clients και AccesPoints, το κατάλληλο πακετάρισμα όλων αυτών των πληροφοριών σε δικτυακό μήνυμα μορφής Json , και τέλος η αποστολή του στην εφαρμογή war (Server).

6.6.2 Εφαρμογή Server

Ακολουθώντας, λοιπόν, τη ροή των δεδομένων από τον client στον server, πηγαίνουμε στην κλάση com.protipo.drones.services. MacClientsServiceImpl, όπου εκεί ο Server λαμβάνει σε μορφή Json το δικτυακό πακέτο με τα Wifi clients και AccessPoints. Σε αυτήν την κλάση γίνεται η βασική επεξεργασία των δεδομένων, στις

γραμμές 55-69 γίνεται η αποθήκευση των πιο πρόσφατων Wifi Clients στον πίνακα livemacclients, αντιστοίχως στις γραμμές 83-94 γίνεται η αποθήκευση των πιο πρόσφατων AccessPoints. Στην συνέχεια της κλάσης γίνονται οι κατάλληλοι έλεγχοι εφόσον εντοπιστεί Wifi client ή AccesPoint, ενώ πραγματοποιείται και η κλήση της υπηρεσίας https://macvendors.co/api/ που μας παρέχει πληροφορίες για τα stationMacs.

Ο ρόλος της εφαρμογής war (Server) δεν είναι μόνο να καταγράφει και να επεξεργάζεται τις πληροφορίες του Aircrack, αλλά αναλαμβάνει και τον ρόλο της παρουσίασης τους. Για αυτό τον σκοπό στο Front End έχει χρησιμοποιηθεί η τεχνολογία JSF (Java Server Faces). Με την JSF κάθε κλάση της Java συνδέεται με μια συγκεκριμένη σελίδα, για παράδειγμα τα συστατικά της σελίδας Apply a Drone MAC αλληλεπιδρούν με την κλάση com.protipo.drones.jsfbeans. DronesMacsBean. Με την ίδια αντίστοιχη λογική, κάθε σελίδα της εφαρμογής έχει από πίσω της μια κλάση του πακέτου com.protipo.drones.jsfbeans.

6.7 Εγκατάσταση εφαρμογής

Σε αυτό το κεφάλαιο θα δούμε πώς θα γίνει η σωστή εγκατάσταση της εφαρμογής πριν τη χρήση της. Για αρχή θα πρέπει να στήσουμε το κατάλληλο περιβάλλον. Η εφαρμογή έχει τη δυνατότητα να εκτελείται και σε Linux και σε Windows, αφού βασίζεται στην Java η οποία είναι διαπλατφορμική, επομένως δεν μας απασχολεί το λειτουργικό σύστημα που θα χρησιμοποιήσουμε. Θα πρέπει να κάνουμε λοιπόν εγκατάσταση την Java8 και συγκεκριμένα το JDK8, αφού στο μηχάνημα μας θα πρέπει να μεταγλωττίσουμε τον κώδικα. Στην συνέχεια εγκαθιστούμε το Maven, επίσης, αν θέλουμε μπορούμε να κατεβάσουμε το Netbeans ή Eclipse, ώστε να δούμε και να πειραματιστούμε καλύτερα μέσα στον κώδικα. Έπειτα, θα πρέπει να εγκαταστήσουμε και τον κατάλληλο Web Server, ο οποίος είναι ο Apache Tomcat, και συγκεκριμένα για την ανάπτυξη και τις δοκιμές της εφαρμογής χρησιμοποιήθηκε ο Tomcat 7.0.55. Τέλος θα πρέπει να εγκαταστήσουμε και την βάση δεδομένων που θα χρησιμοποιήσει ο Server μας. Αυτή θα πρέπει να είναι MySQL5 και άνω ή MariaDB5.5 και άνω. Βάσει των προαναφερθέντων, το Project είναι αρχιτεκτονικής Maven, επομένως, για να παραγάγουμε από τον πηγαίο κώδικα το εκτελέσιμο πηγαίνουμε στον φάκελο του Project (Project_Monitoring) και γράφουμε την εξής εντολή mvn clean

install, αφού ολοκληρωθεί η εκτέλεση της θα εμφανιστεί ένας φάκελος /target/. Μέσα από αυτόν τον φάκελο θα χρειαστούμε δύο αρχεία Project_Monitoring-jar-with-dependencies.jar και Prokect_Monitoring.war τα οποία ουσιαστικά είναι οι εφαρμογές Client και Server.

6.7.1 Εγκατάσταση Server

Ο Server στην περίπτωση μας είναι ο υπολογιστής που εκτελεί την λήψη, την αποθήκευση, την επεξεργασία και την παρουσίαση των πληροφοριών. Το λειτουργικό σύστημα μπορεί να είναι είτε Windows είτε Linux, αφού όλες οι εφαρμογές που θα χρειαστούμε είναι συμβατές και με τα δύο λειτουργικά συστήματα. Υποθέτουμε ότι έχουμε εγκαταστήσει την Java-JRE8, την MySQL και τον Apache Tomcat.

6.7.1.1 Δημιουργία σχήματος βάσης δεδομένων

Το πρώτο βήμα είναι να δημιουργήσουμε μια βάση δεδομένων και τους πίνακες που χρειάζεται η εφαρμογή χωρίς δεδομένα, δηλαδή το σχήμα της βάσης. Τα αρχεία με το σχήμα της βάσης βρίσκονται μέσα στον φάκελο του project, υποθέτουμε ότι αυτός ο φάκελος είναι ο C:\Project_Monitoring Εκτελούμε λοιπόν με τη σειρά τα ακόλουθα βήματα:

- Σύνδεση στη βάση δεδομένων: ανοίγουμε ένα τερματικό ή αλλιώς κονσόλα και γράφουμε το εξής mysql -h 127.0.0.1 -u root –proot
- Δημιουργία κενής βάσης: create schema Project_Monitoring;
- Επιλογή της βάσης που δημιουργήσαμε: use Project Monitoring;
- Τρέχουμε το αρχείο που δημιουργεί το σχήμα της βάσης με την εντολή: source C:\Project_Monitoring\Protipo_Monitoring.sql;
-

6.7.1.2 Ρυθμίσεις Web Server

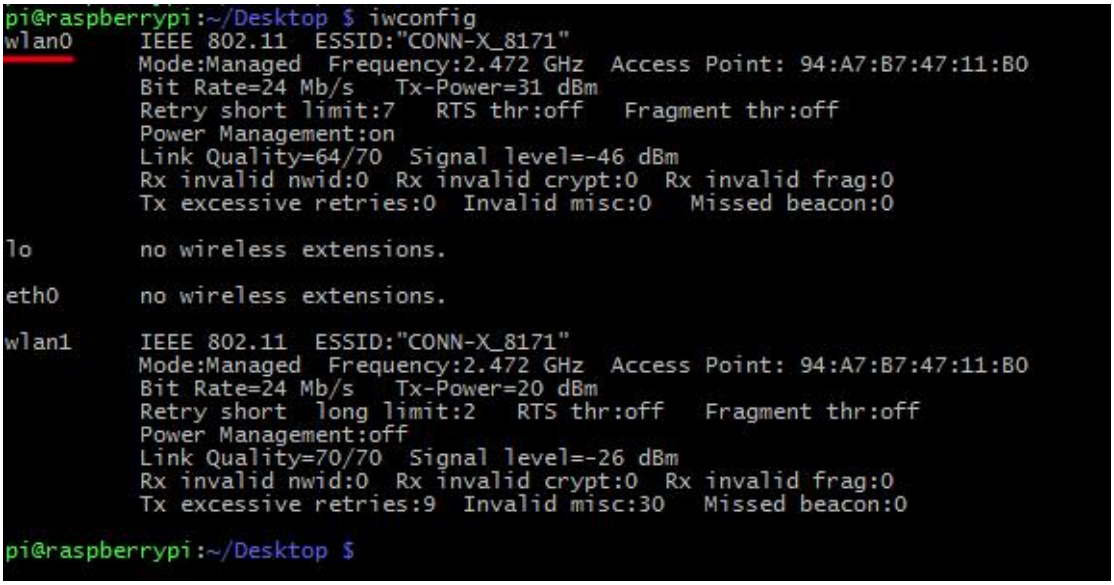
Αφού δημιουργήσουμε το σχήμα της βάσης στον Server, το επόμενο βήμα είναι να ρυθμίσουμε κατάλληλα τον Web Server δηλαδή τον Apache Tomcat ώστε κατά την εκκίνηση του να συνδέεται στην βάση. Ας υποθέσουμε ότι ο φάκελος που έχει εγκατασταθεί ο Apache Tomcat είναι ό C:\TOMCAT\apache-tomcat-7.0.55\, ανοίγουμε για επεξεργασία το αρχείο C:\TOMCAT\apache-tomcat-7.0.55\conf\context.xml και προσθέτουμε τις κατάλληλες ρυθμίσεις για την σύνδεση με τη βάση της εφαρμογής (βλέπε αρχείο context.xml). Όπως έχουμε ήδη αναφέρει στην ενότητα 6.6, κατά τη μεταγλώττιση της εφαρμογής παράγονται 2 αρχεία τύπου jar και war, μεταφέρουμε λοιπόν το αρχείο Project_Monitoring.war στον κατάλληλο φάκελο του Tomcat ώστε να το κάνει deploy και να ξεκινήσει την Server-Web εφαρμογή, αυτός είναι ό C:\TOMCAT\apache-tomcat-7.0.55\webapps\. Πριν, όμως, δώσουμε την εντολή εκκίνησης στον Tomcat θα χρειαστεί να μεταφέρουμε στο κατάλληλο path του server το απαραίτητο αρχείο ρυθμίσεων τύπου txt της εφαρμογής war. Αυτό είναι C:\etc\ \configuration_properties.txt για windows ή /etc/Project_Monitoring/configuration_properties.txt για Linux. Τέλος, δίνουμε την εντολή εκκίνησης του Apache Tomcat. Ο τρόπος εκκίνησης εξαρτάται από την μορφή εγκατάστασης που έχουμε κάνει. Για παράδειγμα, μπορούμε να τον εκκινήσουμε σαν Service από το μενού των Windows Services, ή μέσω της γραμμής εντολών π.χ. με την εντολή C:\TOMCAT\apache-tomcat-7.0.55\bin catalina.bat run. Αφού ξεκινήσει, λοιπόν, ο WebServer (Apache Tomcat), μπορούμε να δούμε την web εφαρμογή μέσω web browser π.χ. στην διεύθυνση http://127.0.0.1:7575/Project_Monitoring/ . Τέλος, όπως ήδη προαναφέρθηκε η εφαρμογή server έχει πολλαπλούς ρόλους, ένας από τους οποίους είναι η λήψη σημάτων από την εφαρμογή client. Επομένως, είναι αναγκαίο να κάνουμε τις κατάλληλες ρυθμίσεις στο Firewall του λειτουργικού συστήματος του Server ώστε να επιτρέπει την είσοδο των δικτυακών πακέτων από τον client. Για τα Windows μπορούμε να το πραγματοποιήσουμε από το Control Panel επιλέγοντας Control Panel → System and Maintenance → Administrative Tools → Windows Firewall with Advanced Security. Για τα Linux συστήματα εξαρτάται από τον τύπο Firewall της κάθε εφαρμογής. Η δικτυακή πόρτα που πρέπει να ανοίξουμε είναι η 22000 και είναι του πρωτοκόλλου TCP, η οποία ορίζεται από το αρχείο ρυθμίσεων της εφαρμογής configuration_properites.txt.

6.7.2 Εγκατάσταση Client

Η εφαρμογή client είναι το παραγόμενο από τη μεταγλώττιση αρχείο τύπου jar. Αυτό το αρχείο μπορεί να εκτελεστεί σε όποιο μηχάνημα έχει εγκατεστημένη την πλατφόρμα Java-JRE8 την σουίτα εργαλείων WiFi Aircrack-ng και μία κάρτα δικτύου με δυνατότητα λειτουργίας σε monitoring mode. Δεν χρειάζεται ούτε βάση δεδομένων ούτε WebServer, αφού είναι μια απλή εφαρμογή jar, της οποίας αποκλειστικός στόχος είναι να διαβάζει το αρχείο τύπου csv που δημιουργεί και να ανανεώνει το aircrack, αλλά και να στέλνει δικτυακά τα δεδομένα στον Server κάθε ορισμένα δευτερόλεπτα (βλέπε αρχείο ρυθμίσεων configuration_properties_txt). Το αρχείο ρυθμίσεων θα πρέπει να βρίσκεται στο ίδιο path με τον Server (βλέπε ενότητα 6.7.1.2). Στις παρακάτω ενότητες περιγράφονται διαδοχικά τα βήματα για να ξεκινήσουμε την εφαρμογή client.

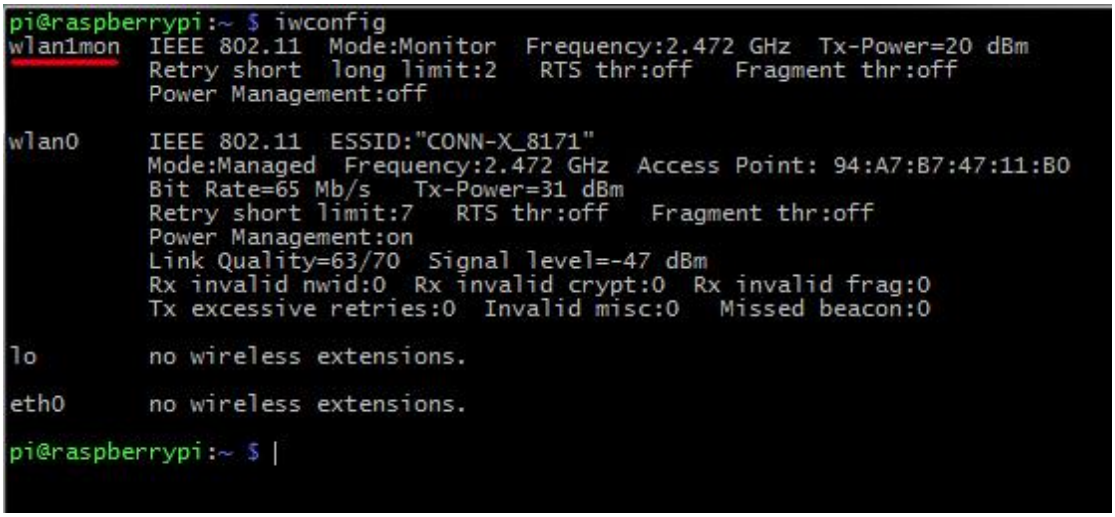
6.7.2.1 Ρυθμίσεις ασύρματης κάρτας δικτύου

Η εντολή iwconfig είναι μία cli (command line interface) εντολή, η οποία μπορεί να απεικονίσει τις παραμέτρους μίας ασύρματης κάρτας δικτύου. Στην εικόνα (χ) παρατηρούμε 2 wireless κάρτες ενεργές. Την wlan0 η οποία είναι η default ασύρματη κάρτα που χρησιμοποιεί το Raspberry. Την wlna1 η οποία είναι η εξωτερική κάρτα δικτύου που χρησιμοποιήθηκε για τους σκοπούς της εφαρμογής.



Εικόνα 6.7.2.2.2

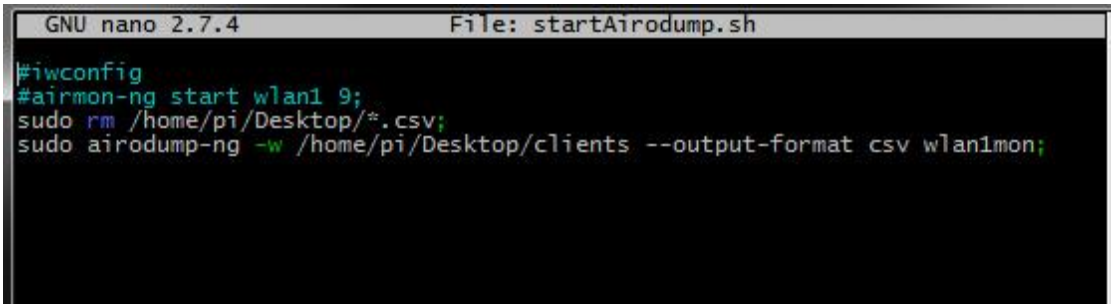
Όπως ήδη είπαμε δεν μπορούμε να χρησιμοποιήσουμε οποιαδήποτε ασύρματη κάρτα δικτύου, παρά μόνο αν έχει την δυνατότητα λειτουργίας σε monitoring mode. Για να γυρίσουμε την κάρτα σε monitoring mode χρειαζόμαστε την εφαρμογή airmon-ng της σουίτας Aircrack-ng. Αν υποθέσουμε ότι το λειτουργικό σύστημα βλέπει την ασύρματη κάρτα δικτύου με όνομα wlan1, τότε τρέχουμε την εντολή: airmon-ng start wlan1 9; η οποία θα γυρίσει την κάρτα μας σε monitoring mode και θα την μετονομάσει σε wlan1mon. Εικόνα 6.7.2.2.3



Εικόνα 6.7.2.2.3

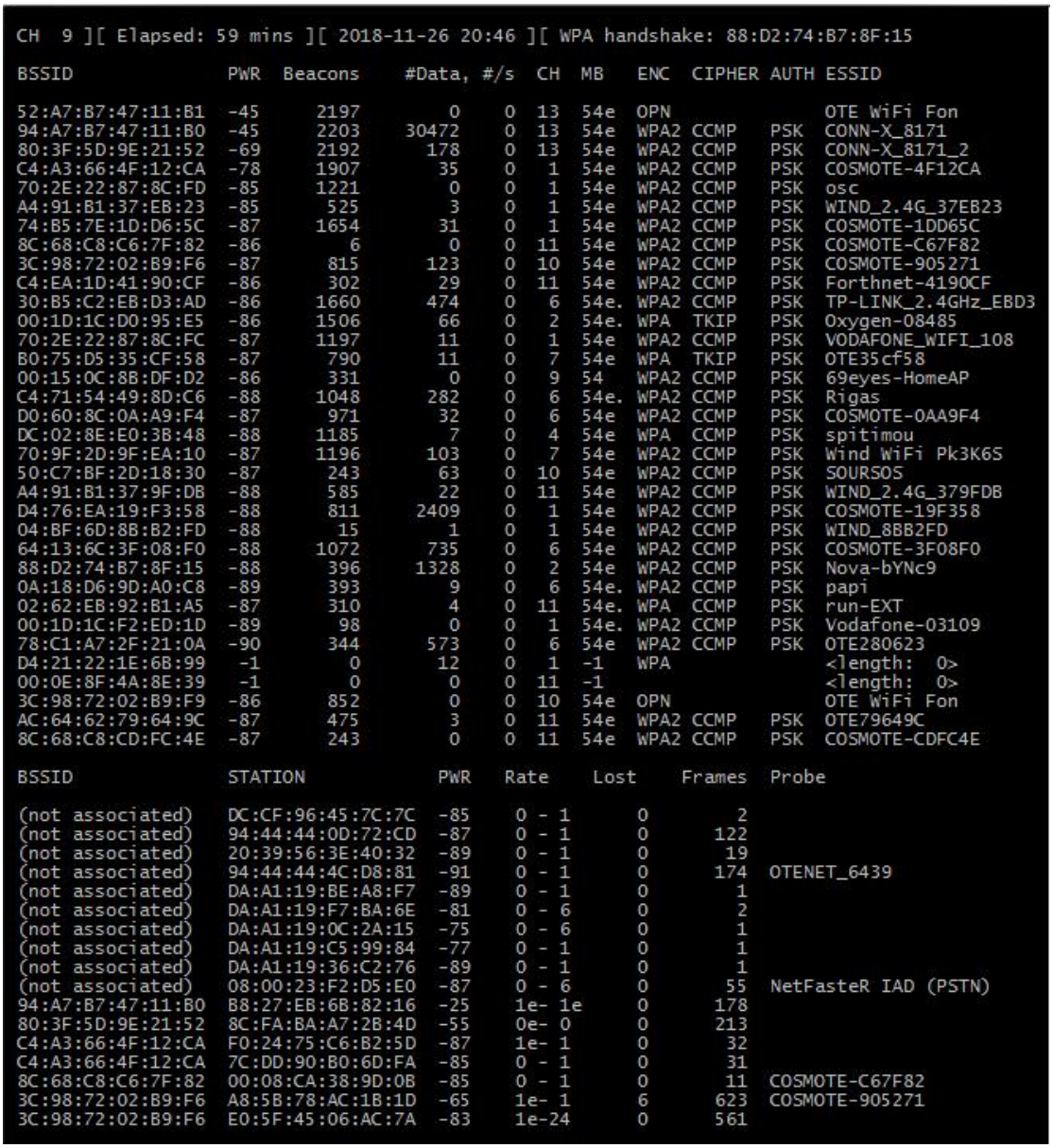
6.7.2.2 Ανίχνευση στατιστικών ασύρματων συσκευών

Με την εφαρμογή airodump-ng, επίσης της σουίτας Aircrack-ng, καταγράφουμε τα στατιστικά των ασύρματων δικτύων σε αρχείο τύπου csv, για την εκκίνηση της καταγραφής τρέχουμε την εντολή airodump-ng -w /home/pi/Desktop/clients --output-format csv wlan1mon; Μετά την παράμετρο –w ακολουθεί το path του αρχείου csv όπου θέλουμε να γίνεται η καταγραφή, πρέπει να είναι παρόμοιο με το path που έχει η παράμετρος CLIENTS_CSV_PATH του αρχείου ρυθμίσεων της jar εφαρμογής, ώστε να γνωρίζει από πού θα διαβάσει το αρχείο csv. Για λόγους ευκολίας στην επιφάνεια εργασίας του χρήστη pi στο Raspberry, δημιουργήθηκε το εκτελέσιμο αρχείο : startAirodump.sh το οποίο περιλαμβάνει μαζί με την παραπάνω εντολή, την : rm/home/pi/Desktop/*.csv η οποία διαγράφει τυχόν csv αρχεία που υπάρχουν στην επιφάνεια εργασίας έτσι ώστε να δημιουργηθεί εκ νέου το csv αρχείο στο οποίο θα καταγράφεται η παρουσία των ασύρματων συσκευών. Εικόνα 6.7.2.2.1



Εικόνα 6.7.2.2.1

Κατά την εκτέλεση του αρχείου startAirodump.sh, ξεκινάει η καταγραφή των client και Access Point που βρίσκονται εντός εμβέλειας . Εικόνα 6.7.2.2.4



```
CH  9 ][ Elapsed: 59 mins ][ 2018-11-26 20:46 ][ WPA handshake: 88:D2:74:B7:8F:15

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

52:A7:B7:47:11:B1  -45     2197        0    0  13  54e  OPN              OTE WiFi Fon
94:A7:B7:47:11:B0  -45     2203    30472    0  13  54e  WPA2 CCMP   PSK  CONN-X_8171
80:3F:5D:9E:21:52  -69     2192      178    0  13  54e  WPA2 CCMP   PSK  CONN-X_8171_2
C4:A3:66:4F:12:CA  -78     1907       35    0   1  54e  WPA2 CCMP   PSK  COSMOTE-4F12CA
70:2E:22:87:8C:FD  -85     1221        0    0   1  54e  WPA2 CCMP   PSK  osc
A4:91:B1:37:EB:23  -85      525        3    0   1  54e  WPA2 CCMP   PSK  WIND_2.4G_37EB23
74:B5:7E:1D:D6:5C  -87     1654       31    0   1  54e  WPA2 CCMP   PSK  COSMOTE-1DD65C
8C:68:C8:C6:7F:82  -86        6        0    0  11  54e  WPA2 CCMP   PSK  COSMOTE-C67F82
3C:98:72:02:B9:F6  -87      815      123    0  10  54e  WPA2 CCMP   PSK  COSMOTE-905271
C4:EA:1D:41:90:CF  -86      302       29    0  11  54e  WPA2 CCMP   PSK  Forthnet-4190CF
30:B5:C2:EB:D3:AD  -86     1660      474    0   6  54e. WPA2 CCMP   PSK  TP-LINK_2.4GHz_EBD3
00:1D:1C:D0:95:E5  -86     1506       66    0   2  54e. WPA  TKIP   PSK  Oxygen-08485
70:2E:22:87:8C:FC  -87     1197       11    0   1  54e  WPA2 CCMP   PSK  VODAFONE_WIFI_108
B0:75:D5:35:CF:58  -87      790       11    0   7  54e  WPA  TKIP   PSK  OTE35cf58
00:15:0C:8B:DF:D2  -86      331        0    0   9  54   WPA2 CCMP   PSK  69eyes-HomeAP
C4:71:54:49:8D:C6  -88     1048      282    0   6  54e. WPA2 CCMP   PSK  Rigas
D0:60:8C:0A:A9:F4  -87      971       32    0   6  54e  WPA2 CCMP   PSK  COSMOTE-0AA9F4
DC:02:8E:E0:3B:48  -88     1185        7    0   4  54e  WPA  CCMP   PSK  spitimou
70:9F:2D:9F:EA:10  -87     1196      103    0   7  54e  WPA2 CCMP   PSK  Wind WiFi Pk3K6S
50:C7:BF:2D:18:30  -87      243       63    0  10  54e  WPA2 CCMP   PSK  SOURSOS
A4:91:B1:37:9F:DB  -88      585       22    0  11  54e  WPA2 CCMP   PSK  WIND_2.4G_379FDB
D4:76:EA:19:F3:58  -88      811     2409    0   1  54e  WPA2 CCMP   PSK  COSMOTE-19F358
04:BF:6D:8B:B2:FD  -88       15        1    0   1  54e  WPA2 CCMP   PSK  WIND_8BB2FD
64:13:6C:3F:08:F0  -88     1072      735    0   6  54e  WPA2 CCMP   PSK  COSMOTE-3F08F0
88:D2:74:B7:8F:15  -88      396     1328    0   2  54e  WPA2 CCMP   PSK  Nova-bYNc9
0A:18:D6:9D:A0:C8  -89      393        9    0   6  54e. WPA2 CCMP   PSK  papi
02:62:EB:92:B1:A5  -87      310        4    0  11  54e. WPA  CCMP   PSK  run-EXT
00:1D:1C:F2:ED:1D  -89       98        0    0   1  54e. WPA2 CCMP   PSK  Vodafone-03109
78:C1:A7:2F:21:0A  -90      344      573    0   6  54e  WPA2 CCMP   PSK  OTE280623
D4:21:22:1E:6B:99   -1        0       12    0   1  -1   WPA              <length:  0>
00:0E:8F:4A:8E:39   -1        0        0    0  11  -1                    <length:  0>
3C:98:72:02:B9:F9  -86      852        0    0  10  54e  OPN              OTE WiFi Fon
AC:64:62:79:64:9C  -87      475        3    0  11  54e  WPA2 CCMP   PSK  OTE79649C
8C:68:C8:CD:FC:4E  -87      243        0    0  11  54e  WPA2 CCMP   PSK  COSMOTE-CDFC4E

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   DC:CF:96:45:7C:7C  -85    0 - 1      0         2
(not associated)   94:44:44:0D:72:CD  -87    0 - 1      0       122
(not associated)   20:39:56:3E:40:32  -89    0 - 1      0        19
(not associated)   94:44:44:4C:D8:81  -91    0 - 1      0       174  OTENET_6439
(not associated)   DA:A1:19:BE:A8:F7  -89    0 - 1      0         1
(not associated)   DA:A1:19:F7:BA:6E  -81    0 - 6      0         2
(not associated)   DA:A1:19:0C:2A:15  -75    0 - 6      0         1
(not associated)   DA:A1:19:C5:99:84  -77    0 - 1      0         1
(not associated)   DA:A1:19:36:C2:76  -89    0 - 1      0         1
(not associated)   08:00:23:F2:D5:E0  -87    0 - 6      0        55  NetFasteR IAD (PSTN)
94:A7:B7:47:11:B0  B8:27:EB:6B:82:16  -25   1e- 1e      0       178
80:3F:5D:9E:21:52  8C:FA:BA:A7:2B:4D  -55   0e- 0       0       213
C4:A3:66:4F:12:CA  F0:24:75:C6:B2:5D  -87   1e- 1       0        32
C4:A3:66:4F:12:CA  7C:DD:90:B0:6D:FA  -85    0 - 1      0        31
8C:68:C8:C6:7F:82  00:08:CA:38:9D:0B  -85    0 - 1      0        11  COSMOTE-C67F82
3C:98:72:02:B9:F6  A8:5B:78:AC:1B:1D  -65   1e- 1       6       623  COSMOTE-905271
3C:98:72:02:B9:F6  E0:5F:45:06:AC:7A  -83   1e-24       0       561
```

Εικόνα 6.7.2.2.4

6.7.2.4 Εκκίνηση της εφαρμογής Jar.

Πριν την την εφαρμογή πρέπει να βεβαιωθούμε ότι έχουμε κάνει τις κατάλληλες ρυθμίσεις στο αρχείο ρυθμίσεων configuration_properties.txt. Είναι απαραίτητο να θέσουμε σωστά την παράμετρο WS_SERVER_URL, την οποία διαβάζει η εφαρμογή jar, ώστε να γνωρίζει σε ποια IP και πόρτα βρίσκεται ο Server που θα στείλει τα δεδομένα του αρχείου csv. Για την εκκίνηση της εφαρμογής jar τρέχουμε την εντολή: java -jar Project_MonitoringApp-jar-with-dependencies.jar; Για λόγους ευκολίας, δημιουργήθηκε το εκτελέσιμο αρχείο sendJar.sh, το οποίο περιέχει την παραπάνω εντολή. Εικόνα 6.7.2.4.1

```
pi@raspberrypi:~/Desktop $ ./sendJar.sh
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
DEBUG: (26-11-2018 21:14:08,499) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):

DEBUG: (26-11-2018 21:14:08,507) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
::::System Parameters::::
DEBUG: (26-11-2018 21:14:08,510) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
ITEM_COLUMNS: 6
DEBUG: (26-11-2018 21:14:08,512) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
CSV_DATE_FORMAT:  yyyy-MM-dd HH:mm:ss
DEBUG: (26-11-2018 21:14:08,514) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
WS_SERICE_NAME: MacClientsServiceImplService
DEBUG: (26-11-2018 21:14:08,516) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
WS_SERVER_LINK: http://services.drones.protipo.com/
DEBUG: (26-11-2018 21:14:08,518) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
LOCK_TABLE_LIVE: false
DEBUG: (26-11-2018 21:14:08,520) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
LOCK_TABLE_LIVE_WAIT_MILLS: 100
DEBUG: (26-11-2018 21:14:08,522) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):

DEBUG: (26-11-2018 21:14:08,524) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
::::Client Parameters::::
DEBUG: (26-11-2018 21:14:08,525) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
CLIENTS_CSV_PATH: /home/pi/Desktop/clients-01.csv
DEBUG: (26-11-2018 21:14:08,528) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
WS_SERVER_URL: http://192.168.1.12:22000/ws/macclients?wsdl
DEBUG: (26-11-2018 21:14:08,530) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
READER_CSV_REFRESH_MILLS: 5000
DEBUG: (26-11-2018 21:14:08,532) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):

DEBUG: (26-11-2018 21:14:08,534) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
::::Server Parameters::::
DEBUG: (26-11-2018 21:14:08,536) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
WS_CLIENTS_URL: http://0.0.0.0:22000/ws/macclients
DEBUG: (26-11-2018 21:14:08,538) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
LIVE_PAGE_REFRESH_SECONDS: 5
DEBUG: (26-11-2018 21:14:08,541) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
LIVE_PAGE_RECENT_VIEW_SECONDS: 30
DEBUG: (26-11-2018 21:14:08,543) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):
DRONES_DETECT_ALARM_PATTERN: AB:CD
DEBUG: (26-11-2018 21:14:08,545) ::::  [com.protipo.drones.DronesParameters.loadFromile()]:::  (USER: n/a):

DEBUG: (26-11-2018 21:14:17,205) ::::  [com.protipo.drones.Client.main()]:::  (USER: n/a): readCSV_and_Send
DEBUG: (26-11-2018 21:14:23,976) ::::  [com.protipo.drones.Client.main()]:::  (USER: n/a): readCSV_and_Send
DEBUG: (26-11-2018 21:14:30,614) ::::  [com.protipo.drones.Client.main()]:::  (USER: n/a): readCSV_and_Send
DEBUG: (26-11-2018 21:14:37,261) ::::  [com.protipo.drones.Client.main()]:::  (USER: n/a): readCSV_and_Send
```

Εικόνα 6.7.2.4.1

Κεφάλαιο 7
Συμπεράσματα

Είναι γεγονός πως η πανταχού παρούσα υπολογιστική αποτελεί την νέα πραγματικότητα των ανθρώπων στις ανεπτυγμένες κοινωνίες του εικοστού πρώτου αιώνα. Δεκάδες συσκευές για κάθε άνθρωπο ή οργανισμό, μεταφέρουν καθημερινά έναν μεγάλο όγκο πληροφορίας σε τοπικό ή διαδικτυακό επίπεδο, αποτελούμενες κυρίως από ασύρματες συσκευές με επίγνωση του πλαισίου που εξυπηρετούν την μετάδοση πολύτιμων δεδομένων για σκοπούς επικοινωνίας, υγείας, ψυχαγωγίας, ευκολίας, εργασίας και ασφάλειας. Τα ασύρματα δίκτυα διαδραματίζουν καθοριστικό ρόλο στην επιτυχή επικοινωνία και συνεργασία των συσκευών αυτών, αξιοποιώντας τις τεχνικές των δικτύων των πληροφοριακών συστημάτων. Το πιο διαδεδομένο πρωτόκολλο μεταξύ άλλων για την ασύρματη επικοινωνία, αποτελεί το IEEE 802.11, το οποίο χρησιμοποιείται κατά κόρον για τη διασύνδεση συσκευών, όπως έξυπνα τηλέφωνα, φορητοί υπολογιστές, tablets, αισθητήρες. Ωστόσο πλέον ενσωματώνεται σε συσκευές που μέχρι τώρα εξυπηρετούσαν απλές καθημερινές ανάγκες των ανθρώπων. Για τον λόγο αυτό, είναι πρωταρχικής σημασίας η πληροφορία που ανταλλάσσεται μέσω των ασύρματων δικτύων να παραμένει ασφαλής και αμετάβλητη. Δεδομένης της φύσης των ασύρματων δικτύων όμως ο ρόλος της ασφάλειας διακυβεύεται. Τα δίκτυα αυτά λόγω της εκπομπής και λήψης ραδιοσυχνοτήτων, προσπερνούν τα φυσικά όρια ενός κτηρίου και οποιοσδήποτε κακόβουλος ενδιαφέρεται να αποσπάσει, ή να διαστρεβλώσει την πληροφορία που μεταδίδεται για δικό του όφελος, υπάρχουν αμέτρητες τεχνικές που θα μπορούσε να το καταφέρει. Επίσης, η εμπορική ανάπτυξη των μη επανδρωμένων εναέριων αεροσκαφών έχει καταστήσει ευκολότερη την πρόσβαση ενός πιθανού κακόβουλου χρήστη κοντά στις φυσικές εγκαταστάσεις και στον χώρο ραδιοκάλυψης ενός ασύρματου δικτύου, με αποτέλεσμα να μπορεί πολύ ευκολότερα να αποκτήσει πρόσβαση σε αυτό χωρίς να γίνει αντιληπτός. Δεδομένης της νέας αυτής κατάστασης είναι αναγκαίο για την

ασφάλεια κάθε οντότητας που αξιοποιεί και εξαρτάται από αυτού του είδους την δικτύωση, να ενσωματώνει κατάλληλο, ανάλογα με τις ανάγκες του, σύστημα ανίχνευσης και καταγραφής των ασύρματων συσκευών που τον περιβάλλει.

Για τους σκοπούς της συγκεκριμένης διατριβής, κατασκευάστηκε συσκευή, ικανή για την ανίχνευση και απεικόνιση της δικτυακής κίνησης των συσκευών (είτε χρηστών – clients είτε σταθμών βάσης – Access Points) που αξιοποιούν το πρωτόκολλο IEEE 802.11 προκειμένου να ανταλλάξουν πληροφορία. Η συσκευή αυτή ονομάστηκε Project_Monitoring και λειτουργεί μέσω της καταγραφής των μοναδικών MAC διευθύνσεων που βρίσκονται καταχωρημένες στις ασύρματες κάρτες δικτύου κάθε συσκευής. Βασική λειτουργία της, μεταξύ άλλων, είναι η ειδοποίηση της εμφάνισης συσκευών στο δίκτυο που έχουν οριστεί ως μη εξουσιοδοτημένες, όπως smartphones, WiFi controlled drones, αλλά και η προειδοποίηση της πιθανής επίθεσης Man-In-The-Middle Attack με την χρήση κακόβουλου Twin Access Point. Η πρώτη δυσκολία που αντιμετωπίστηκε κατά τον σχεδιασμό της εφαρμογής είναι η εύρεση σχετικού Online Service για την πλήρη εισαγωγή του Organization Unique Identifier (OUI) των MAC διευθύνσεων για όλα τα drones του εμπορίου, με αποτέλεσμα η εφαρμογή να μην είναι σε θέση να μπορεί να αναγνωρίσει την πλήρη γκάμα των μη επανδρωμένων αεροσκαφών που κυκλοφορούν. Ως αποτέλεσμα, η εφαρμογή μπορεί να ειδοποιήσει τον ενδιαφερόμενο μόνο αν τα OUI καταχωρηθούν χειροκίνητα. Ταυτόχρονα, αντιμετωπίστηκε δυσκολία κατά την προσπάθεια της πλήρους ανεξαρτητοποίησης της συσκευής λόγω της αδυναμίας ενσωμάτωσης κατάλληλου εξοπλισμού GSM στο Raspbbery PC, έτσι ώστε να μπορεί να στείλει τα δεδομένα στη βάση, ανεξάρτητα από την τοποθεσίας του.

Βιβλιογραφία

[1] Fluhrer S., Mantin I., Shamir A., (2001) Weaknesses in the Key Scheduling Algorithm of RC4, *8th International Workshop*, SAC 2001, Toronto, Ontario, Canada, August, 2001.

[2] Mohammed L.A., (2008)Towards Pervasive Computing Security, *In the Proceedings of the World Congress on Engineering 2008* Vol I, WCE 2008, July 2008, London, UK..

[3] Ranga K. (2015) Ubiquitous computing : Fastest emerging technology. *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. 2015 New Delhi, India 1(1). ISBN 978-9-3805-4416-8

[4] Greenfield A. (2010), Everyware: The Dawning Age of Ubiquitous Computing, New Riders.

[5]Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005).Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. Ambient intelligence, pp. 5-29.

[6]Stefan Poslad, (2009) Ubiquitous Computing: Smart Devices, Environments and Interactions, Wiley-Blackwell, 2009.

[7]Mark Weiser, (1991)The Computer for the 21st Century, *Scientific American,* Vol. 265, No. 3, pp. 66-75, 1991.

[8]Moore, G.. (1965): Cramming more components onto integrated circuits. Electronics, Vol. 38, pp. 114-117.

[9] Zhang, G., Jin, Q., & Lin, M. (2005). A framework of social interaction support for ubiquitous learning. In Proceedings - International Conference on Advanced *Information Networking and Applications, AINA (Vol. 2, pp. 639-643).* https://doi.org/10.1109/AINA.2005.26.

[10] Mark Weiser, (1994)The World is not a Desktop", Interactions, Vol. 1, No. 1, pp. 7-8, 1994.

[11] Gregory D. Abowd and Elizabeth D. Mynatt, (2000)Charting Past, Present, and Future Research in Ubiquitous Computing, *ACM Transactions on Computer-Human Interaction*, Vol. 7, No. 1, pp. 29-58, 2000.

[12] Kang T., Pisan Y., (2006) A survey of major challenges and future directions for next generation pervasive computing. *University of Technology. Instabul, Turkey* p.755-745. 1(1) doi 10.1007/11902140_79

[13] Meshram V., Patil K., (2016) A SURVEY ON UBIQUITOUS COMPUTING", 2016, DOI: 10.21917/ijsc.2016.0157.

[14] Chen H., (2004) An Intelligent Broker Architecture for Pervasive Context-Aware Systems*", Ph.D Thesis, University of Maryland, 2004.*

[15] Muñoz, M. A., Rodriguez, M., Favela, J., Martinez-Garcia, A. I., & González, V. M. (2003). Context-aware mobile communication in hospitals. I*EEE Computer Society*, 36(9), 38–46

[16] Devaraju A., Hoh S., Hartley M., (2007) A Context gathering Framework for Context-Aware Mobile Solutions", *Proceedings of the 4th International Conference*

on Mobile Technology, Applications, and Systems and the 1st International
Symposium on Computer Human Interaction in Mobile Technology, pp. 39-46, 2007.

[17] Spreitzer M.,Theimer M. (1993) Providing location information in a ubiquitous computing environment. *InProceedings of the Fourteenth ACMSymposium on Operating System Principles*, pages 270–283, Asheville, NC,
Dec 1993. SIGOPS, ACM.

[18] Gajjar, M. J. (2017). Mobile Sensors and Context-Aware Computing. Morgan Kaufmann (2017). ISBN: 9780128017982 (elektronic bk.), 0128017988 (elektronic bk.), 9780128016602.

[19] L. Wang, B. Srinivasan, N. Bhattacharjee, (2011) Security Analysis and Improvements on WLANs", *Journal of Networks*, vol. 6, no. 3, March 2011.

[20] Seymour T. & Shabeen A. (2011). History of Wireless Communication. *Review of Business Infrormation Systems* , 15(2).

[21] Rappaport T. S. Wireless Communications: Principles and Practice, 2nd ed. Prentice Hall.

[22] Stallings W., Wireless Communications and Networks, 2nd Ed., Prentice Hall.

[23] V.H. McDonald, ―The Cellular Concept,‖ Bell System Tech. J.

[24] Bantz, D., and Bauchot, F. (1994) Wireless LAN Design Alternatives." IEEE Network, March/April,1994.

[25] Robertazzi T.G. (2007) Networks and Grids: Technology and Theory, Springer, New York NY, 2007.

[26] Priyanka Radja (2015) The overview of wired and wireless networks and the need for the transition from wired to wireless networks, *International Journal of Industrial Electronics and Electrical Engineering*, ISSN: 2347-6982, Volume-3, Issue-8, Aug. – 2015.

[27] Comer D., Droms R. (2003) Computer Networks and Internets. *Prentice-Hall*, Inc. Upper Saddle River, NJ, USA ©2003. ISBN:0131433512

[28] Hiertz, G., et al. (2010) The IEEE 802.11 universe. *Communications Magazine*, IEEE48.1 (2010).

[29] Joshua Muscatello, Joshua Martin, (2005) Wireless Networks Security, Prepared for Dr. Wibowo IFMG 250, April 20, 2005.

[30] Stefano B., Marco C.,Silvia G., Stojmenovic I. (2010) Mobile Ad Hoc Networking" , IEEE Press, India , 2010.

[31] Collier, M. (1988). "Telecommunications for Information Management and Transfer," Proceedings of the First International Conference, Leicester Polytechnic. London: Gower.

[32] Clark, David, Pogran, Kenneth T. & Wed, David P. (1978). An Introduction to Local Area Networks. Proceedings of the IEEE, Vol. 66, 11, November 1978.

[33] Wireless LAN Security. Symantec Corporation, 2002.

[34] An Overview of Wireless Local Area Networks(WLAN)Ibrahim Al ShourbajiComputer Networks DepartmentJazan UniversityJazan 82822-6649, Saudi Arabia.

[35] Priyanka R. (2015). The overview of wired and wireless networks and the need for the transition from wired to wireless networks. International Journal of Industrial Electronics and Electrical Engineering. 3(8) , ISSN: 2347-6982.

[36] R. Want, B. N. Schilit, and S. Jenson, (2015) "Enabling the internet of things," Computer.

[37] Goldsmith C., (2004). Wireless Local Area Networking
For Device Monitoring, Master thesis, University of
Rochester Rochester, New York.

[38] Muthu Ramya. C, Shanmugaraj M., Prabakaran R. (2011) Study on Zigbee Technology. 1(1), DOI: 10.1109/ICECTECH.2011.5942102.

[39] Banerji S. & Chowdhury R. (2013) On IEEE 802.11: Wireless Lan Technology. International Journal of Mobile Network Communications & Telematics. 3(4) doi : 10.5121/ijmnct.2013.3405.

[40] IEEE 802.11b-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications High Speed Physical Layer Extension in the 2.4 GHz Band, September 16, 1999.

[41] IEEE 802.11a-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications High Speed Physical Layer in the 5 GHz Band, 1999.

[42] IEEE 802.11g-2003, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and

Physical Layer (PHY) Specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 27, 2003.

[43] Chen J. (2001) Measured Performance of 5-Ghz 802.11a Wireless Lan Systems. Atheros Communication, Inc.

[44] Wallett T. (2009) A Brief Survey of Media Access Control, Data Link Layer, and Protocol Technologies for Lunar SurfaceCommunications/ Nasa/Tm2009-215295

[45] Masood Haani S. (2013) Performace comparison of IEEE 802.11g and IEEE 802.11n in the presence of interference from 802.15.4 networks. 1(1). Department of Electrical Engineering, McGill University.

[46] Halperin D. , Greenstein B. , Sheth A., Wetherall D. (2010) Demystifying 802.11n Power Consumption. University of Washington and Intel Labs Seattle 1(1).

[47] Kelly V. (2014) New IEEE 802.11ac™ Specification Driven by Evolving Market Need for Higher, Multi-User Throughput in Wireless LANs". IEEE. Retrieved 2014-01-11.

[48] Aust S., Prasad V. (2012) IEEE 802.11 ah : Advantages in Standards and Further Challenges for Sub 1 Ghz Wi-Fi 1(1) DOI: 10.1109/ICC.2012.6364903.

[49] Elkhord M., Shahrestani S. & Cheung H. (2016) Emerging Wireless Technologies In The Internet OF things : A Comparative Study. International Journal of Wireless & Mobile Networks (IJWMN) 8(5).

[50] NIST Priority Action Plan 2, Guidelines for Assessing Wireless Standards for Smart Grid Applications, ver. 1.0, December 31, 2010.

[51] Gast M. (2002). 802.11 Wireles Networks : The Definitive Guide.(1st ed.) San Francisco, California ISBN: 0-596-00183-5.

[52] Wallett T. (2009) A Brief Survey of Media Access Control, Data Link Layer, and Protocol Technologies for Lunar Surface Communications. Ανακτήθηκε από https://ntrs.nasa.gov/search.jsp?R=20090019005.

[53] Martin J. & Mayberry T. & Donahue C. (2017) A study of MAC Address Randomization in Mobile Devices and When it Fails. Proceedings on Privacy Enchancing Technologies.

[54] Garg U., Verma P & Moudgil Y., Sharma S. (2012) MAC and Logical addressing (A Review Study). International Journal of Engineering Research and Applications. 2(3) ISSN : 2248-9622.

[55] Waliullah Md., Diane Gan, (2014) Wireless Lan Secutiry Threats & Vulnerabilities : A Literature Review. (IJACSA) International Journal of Advanced Computer Science and Applicatio, 5(1).

[56] Schneier Bruce. (2001) Managed Security Monitoring : Network Security for the 21st Century. Computers & Security Elsevier Science Ltd, 1(1) 491-503

[57] Carney John. (2011) Why Integrate Physical and Logical Security? Cisco and/or its affiliates.

[58] Chang V., Chundury Pr., Chetty Mar., (2017) “Spiders in the Sky” : User Perceptions of Drones, Privacy, and Security. Denver, CO, USA 1(1) DOI: http://dx.doi.org/10.1145/3025453.3025632

[59] Sathyamoorrthy D. (2015) A Review of Security Threats of Unmanned Aerial Vehicles and Mitigation Steps. Science & Technology Research Institute for Defence, Ministry of Defence, Malaysia. 1(1).

[60] Cratty C. (2013). FBI uses drones for surveillance in U.S. Ανακτήθηκε από : https://edition.cnn.com/2013/06/19/politics/fbi-drones/index.html

[61] Lea R. (2013). Drones and the Digital Panopticon. XRDS: Crossroads, The ACM magazine for students scientific computing 19, 3 (March 2013), 10–10.

[62] Gittleson K. (2014). Data-stealing Snoopy drone unveiled at Black Hat - BBC News. (2014). http://www.bbc.com/news/technology-26762198

[63] Reed T., Geis J., Dietrich S. (2011). SkyNET: A 3G-enabled mobile attack drone and stealth botmaster. In Proceedings of the 5th USENIX conference on Offensive technologies. 28–36. 1(1).

[64] Jongho W., Seung-Hyun S., and Bertino E. (2015) A Secure Communication Protocol for Drones and Smart Objects. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 249–260. 1(1).

[65] Altawy R., Youssef Arm M. (2016) Security, Privacy, and Safety Aspects of Civilian Drones : A survey. Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada. 1(1).

[66] Tavish Vaidya and Micah Sherr. (2015). Mind Your (R,_)s: Location-Based Privacy Controls for Consumer Drones. In Security Protocols XXIII (LNCS), Bruce Christianson, Petr ˇ Svenda, Vashek Maty´aˇs, James Malcolm, Frank Stajano, and Jonathan Anderson (Eds.), Vol. 9379. Springer International Publishing, 80–90.

[67] Martyn Williams. (2015). NEC's surveillance system will detect, track drones. (2015). http://www.pcworld.com/article/2990525/necs-surveillance-system-will-detect-track-drones.html

[68] Nakhila O., Zou C. (2016) User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring. MILCOM 2016 - 2016 IEEE Military Communications Conference. 10.1109/MILCOM.2016.7795501