ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Χαρτογράφηση Ασύρματων Δικτύων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μπουγιατιώτης Βαγγέλης

Α.Μ. ΜΕ/0648

Πειραιάς, Σεπτέμβριος 2008

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος ***Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα*** στην κατεύθυνση ***Ψηφιακών Επικοινωνιών και Δικτύων*** του τμήματος ***Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων*** του ***Πανεπιστημίου Πειραιώς.***

Ο κύριος σκοπός της συγκεκριμένης διπλωματικής εργασίας είναι η χαρτογράφηση ασυρμάτων δικτύων σε αστικές περιοχές προκειμένου να γίνει έρευνα σε θέματα ασφάλειας.

Αρχικά παρουσιάζονται γενικές πληροφορίες σχετικές με τα ασύρματα δίκτυα καθώς και με τα θέματα ασφάλειάς τους. Στη συνέχεια ακολουθεί περιληπτική αναφορά του εξοπλισμού που χρειάζεται κάποιος για να εντοπίσει και να καταγράψει την ύπαρξη ασύρματων δικτύων και παραθέτονται τα αποτελέσματα από την προσωπική έρευνα σχετικά με την αναζήτηση και καταγραφή ασύρματων δικτύων σε κάποιες υπο-περιοχές της Αττικής παρέχοντας στους αναγνώστες στατιστικές πληροφορίες σχετικές με θέματα κρυπτογράφησης. Τέλος γίνεται αναφορά στους κινδύνους και στους τρόπους διαφύλαξης της ασφάλειας των ασύρματων δικτύων, καθώς και στις μελλοντικές τάσεις-τεχνολογίες που πρόκειται να επικρατήσουν.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1 Ασύρματα Δίκτυα

1.1 Εισαγωγή στην Ασύρματη Τεχνολογία

Οι ασύρματες τεχνολογίες καθιστούν δυνατή την επικοινωνία δύο ή περισσοτέρων συσκευών, χωρίς να απαιτείται η χρήση δικτύου ή κάποιας περιφερειακής καλωδίωσης. Αυτό που ξεχωρίζει τις τεχνολογίες ασύρματης διάδοσης από εκείνες της ενσύρματης είναι η χρήση πομπών ραδιοκυμάτων, ως μέσα μετάδοσης δεδομένων, σε αντίθεση με τις δεύτερες, οι οποίες χρησιμοποιούν καλώδια.

Οι ασύρματες τεχνολογίες ποικίλουν από πολύπλοκα συστήματα, όπως τα ασύρματα δίκτυα (Wireless Local Area Networks – WLANs) και τα κινητά τηλέφωνα, σε απλές συσκευές, όπως τα ασύρματα τηλέφωνα και μικρόφωνα, καθώς και άλλες συσκευές οι οποίες δεν επεξεργάζονται ή αποθηκεύουν πληροφορίες. Επιπλέον, αυτές οι τεχνολογίες χρησιμοποιούν και συσκευές υπερύθρων (IR), όπως ασύρματα τηλεχειριστήρια, ασύρματα πληκτρολόγια και ποντίκια υπολογιστών, καθώς και ασύρματα ακουστικά στερεοφωνικών, τα οποία απαιτούν άμεση οπτική επαφή και μικρή απόσταση μεταξύ του πομπού και του δέκτη.

Στο κεφάλαιο αυτό θα κάνουμε μία διεξοδική ανάλυση των ασύρματων δικτύων, συσκευών και κριτηρίων που απαρτίζουν μία ασύρματη τεχνολογία, καθώς και των θεμάτων ασφάλειας που προβληματίζουν τους κατασκευαστές και διαχειριστές μίας τέτοιας τεχνολογίας.

1.2 Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα (Wireless Networks) εξυπηρετούν ως μηχανισμοί μετάδοσης μεταξύ δύο συσκευών, και μεταξύ συσκευών και των παραδοσιακών ενσύρματων δικτύων. Τα ασύρματα δίκτυα μπορεί να ποικίλουν αλλά χωρίζονται κυρίως σε τρεις κατηγορίες, ανάλογα με την περιοχή κάλυψής τους :

- Τα ***Ασύρματα Δίκτυα Ευρείας Περιοχής*** (Wireless Wide Area Networks – WWANs), τα οποία περιλαμβάνουν τεχνολογίες ευρείας κάλυψης όπως το CDPD, το GSM, και το Mobitex.
- Τα ***Ασύρματα Τοπικά Δίκτυα*** (Wireless Local Area Networks – WLANs), τα οποία περιλαμβάνουν τα 802.11, τα HiperLANs και πολλά άλλα.
- Τα ***Ασύρματα Ιδιωτικά Δίκτυα*** (Wireless Personal Area Networks – WPANs), τα οποία αντιπροσωπεύουν τεχνολογίες όπως τα Bluetooth και τις IR.

1.2.1 Ασύρματα Τοπικά Δίκτυα (WLANs)

Τα WLANs παρέχουν μεγαλύτερη ευελιξία και φορητότητα, λόγω της χρήσης των σημείων πρόσβασης (Access Points – APs) για την σύνδεση των υπολογιστών ή άλλων εξαρτημάτων στο δίκτυο, αναλογικά με τα παραδοσιακά τοπικά ενσύρματα δίκτυα (Local Area Networks - LANs), τα οποία χρησιμοποιούν καλώδια.

Η τεχνολογία WLAN χρονολογείται από τα μέσα της δεκαετίας του ’80, όταν η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (Federal Communications Commission – FCC) κατέστησε για πρώτη φορά διαθέσιμο το φάσμα RF στην βιομηχανία. Από τότε έως και τις αρχές της δεκαετίας του ’90 η ανάπτυξή της ήταν σχετικά αργή, ενώ σήμερα η τεχνολογία WLAN υπόκειται σε εκπληκτικά μεγάλη ανάπτυξη. Το κλειδί για αυτήν την ανάπτυξη είναι η αυξανόμενο εύρος ζώνης το οποίο κατέστη εφικτό από το πρότυπο IEEE 802.11.

1.2.1.1 Κατανομές Συχνότητας και Δεδομένων

Ο οργανισμός IEEE έχει ορίσει πολλά πρότυπα για τα WLANs, μερικά από τα οποία συνοψίζονται στον παρακάτω πίνακα (Πίνακας 1-1) .

Το πρότυπο 802.11a είναι το πιο διαδεδομένο από την οικογένεια των 802.11. Λειτουργεί στην περιοχή συχνοτήτων των 5 GHz και χρησιμοποιεί OFDM πολυπλεξία (Orthogonal Frequency Division Multiplexing) για μείωση των παρεμβολών. Το 802.11b λειτουργεί στην περιοχή συχνοτήτων 2,4 – 2,5 GHz και χρησιμοποιεί την τεχνολογία απευθείας διάδοσης φάσματος (direct sequence spread – spectrum).

Πρότυπο	Περιγραφή	Διαθεσιμότητα
IEEE 802.11	Ρυθμοί δεδομένων μέχρι 2Mbps στην 2.4GHz ISM μπάντα.	Ιούλιος 1997
IEEE 802.11a	Ρυθμοί δεδομένων μέχρι 54Mbps στην 5GHz UNII μπάντα.	Σεπτέμβριος 1999
IEEE 802.11b	Ρυθμοί δεδομένων μέχρι 11Mbps στην 2.4 ISM μπάντα.	Σεπτέμβριος 1999

Πίνακας 1-1 Πρότυπα Ασύρματων Δικτύων

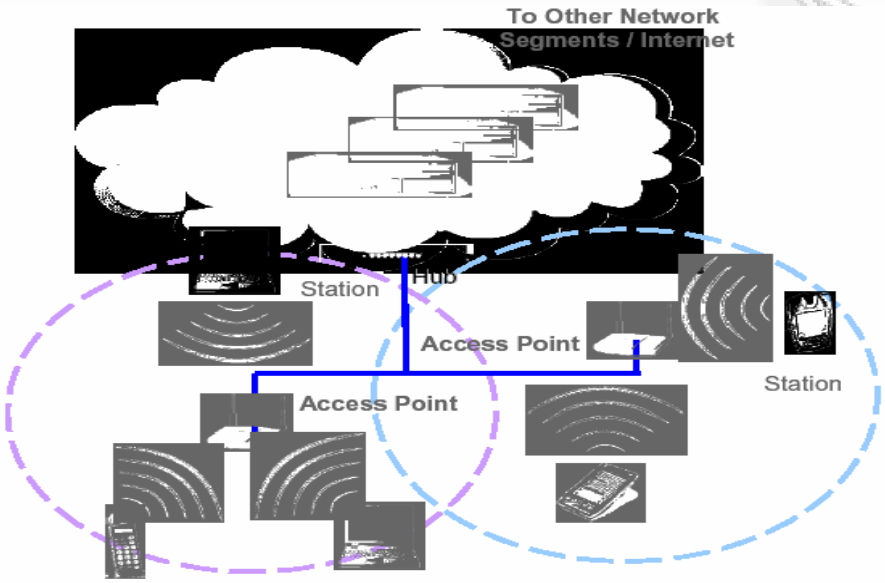
1.2.1.2 Αρχιτεκτονική ενός 802.11

Το πρότυπο IEEE 802.11 επιτρέπει την κατασκευή είτε από σημείο σε σημείο (peer-to-peer) δικτύων είτε δικτύων βασισμένων σε σταθερά access points (AP), με τα οποία μπορούν να επικοινωνήσουν οι κινητοί κόμβοι. Για το λόγο αυτόν, το δεδομένο πρότυπο καθορίζει δύο βασικές τοπολογίες δικτύου: το δίκτυο υποδομής (infrastructure network) και το δίκτυο συγκεκριμένου σκοπού (ad hoc network) .

1.2.1.2.1 Δίκτυο Υποδομής

Το **δίκτυο υποδομής (infrastructure network)** είναι φτιαγμένο για να επεκτείνει την εμβέλεια του ενσύρματου LAN σε ασύρματες κυψέλες. Ένας φορητός υπολογιστής ή άλλη κινητή συσκευή μπορεί να κινείται από κυψέλη σε κυψέλη (από AP σε AP) διατηρώντας ταυτόχρονα πρόσβαση στους πόρους του LAN. Μια κυψέλη είναι η περιοχή που καλύπτεται από ένα AP και καλείται **BSS** (*Basic Service Set*). Το σύνολο όλων των κυψελών ενός δικτύου υποδομής λέγεται **ESS** (*Extended Service Set*). Αυτή η τοπολογία είναι χρήσιμη για την παροχή ασύρματης κάλυψης κτιρίων ή πανεπιστημιουπόλεων. Παρατάσσοντας πολλά APs με επικαλυπτόμενες περιοχές κάλυψης, οι οργανισμοί μπορούν να πετύχουν κάλυψη ευρείας περιοχής (WLAN). Η τεχνολογία WLAN μπορεί να χρησιμοποιηθεί για να αντικαταστήσει ολοκληρωτικά τα ενσύρματα LANs και να επεκτείνει την υποδομή τους. Ένα περιβάλλον WLAN έχει ασύρματους σταθμούς – πελάτες (clients) που χρησιμοποιούν ασύρματα μόντεμ για την επικοινωνία τους με ένα AP. Οι σταθμοί αυτοί είναι εξοπλισμένοι με μια ασύρματη κάρτα δικτύου (*Network Interface Card* - **NIC**) που αποτελείται από έναν ασύρματο πομποδέκτη και την λογική ώστε να αλληλεπιδρά με την μηχανή και το λογισμικό του client. Ένα AP, το οποίο καλύπτει τυπικά περιοχές μεγαλύτερες από περίπου 100 μέτρα, αποτελείται από έναν ασύρματο πομποδέκτη από τη μια πλευρά και μια γέφυρα στο ενσύρματο backbone από την άλλη. Το AP, μια στατική συσκευή που αποτελεί μέρος της ενσύρματης υποδομής, είναι το ανάλογο του σταθμού βάσης στις κυψελοειδείς επικοινωνίες. Όλες οι μεταδόσεις μεταξύ των σταθμών πελατών και των σταθμών και ενσύρματου δικτύου περνούν μέσα από το AP.

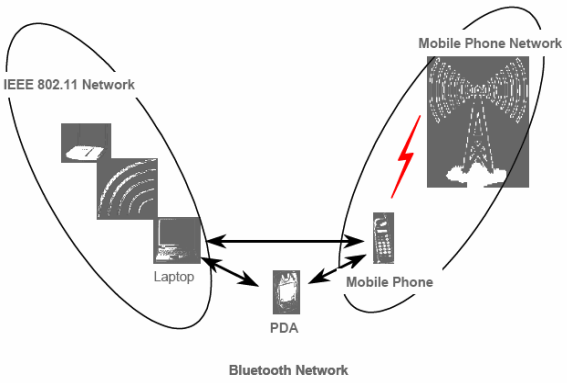
Η βασική τοπολογία ενός WLAN απεικονίζεται στην Εικόνα 1.1.



Εικόνα 1.1 ***Βασική Τοπολογία ενός 802.11 Ασύρματου LAN***

1.2.1.2.2 Ad Hoc Δίκτυο

Τα Ad hoc δίκτυα, όπως τα Bluetooth, είναι δίκτυα σχεδιασμένα ώστε να συνδέουν δυναμικά απομακρυσμένες συσκευές όπως κινητά τηλέφωνα, φορητούς υπολογιστές (laptops), και PDAs. Αυτά τα δίκτυα ονομάζονται "ad hoc" εξαιτίας των ευέλικτων δικτυακών τοπολογιών τους. Ενώ τα WLANs χρησιμοποιούν μία σταθερή δικτυακή υποδομή, τα ad hoc δίκτυα υποστηρίζουν τυχαίους δικτυακούς σχηματισμούς, στηριζόμενα σε ένα master-slave σύστημα το οποίο είναι συνδεδεμένο ασύρματα, ώστε να καθιστά τις συσκευές ικανές να επικοινωνήσουν.



Εικόνα 1.2 **Ενδεικτικό Ad Hoc Δίκτυο**

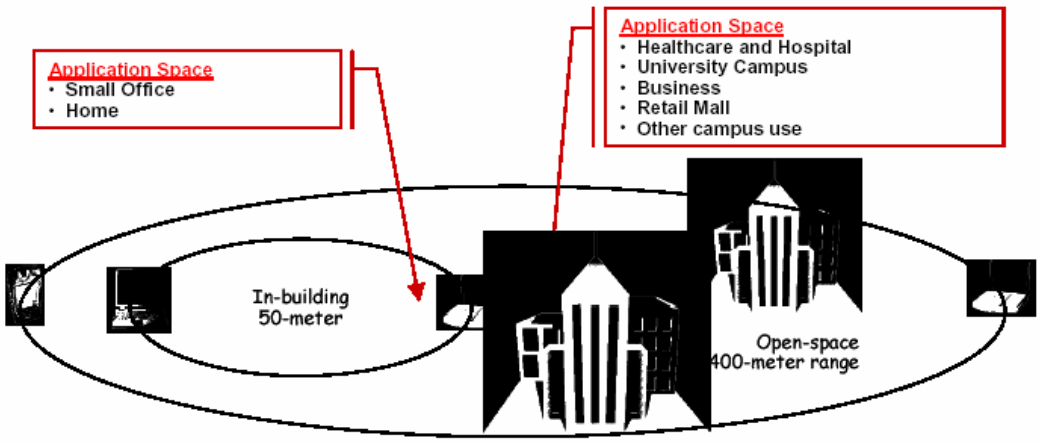
1.2.1.3 Συστατικά ενός Ασύρματου LAN

Ένα WLAN συνίσταται από δύο τύπους εξοπλισμού: έναν **ασύρματο σταθμό** και ένα **access point**. Ο ασύρματος σταθμός, ή πελάτης, είναι τυπικά ένας φορητός υπολογιστής εξοπλισμένος με μία ασύρματη κάρτα δικτύου NIC. Οι κάρτες δικτύου χρησιμοποιούν ραδιοσήματα για την δημιουργία συνδέσεων στο WLAN. Το AP, το οποίο δρα ως γέφυρα μεταξύ των ασύρματων και ενσύρματων δικτύων, αποτελείται από ένα ραδιοπομπό, από μία διεπαφή ενσύρματου δικτύου τύπου 802.3, και από ένα λογισμικό γεφυροποίησης. Το AP λειτουργεί ως βασικός σταθμός για το ασύρματο δίκτυο, συγκεντρώνοντας πολλαπλούς ασύρματους σταθμούς στο ενσύρματο δίκτυο.

1.2.1.4 Εμβέλεια

Η αξιόπιστη κάλυψη για τα 802.11 WLANs εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του απαιτούμενου ρυθμού δεδομένων και της χωρητικότητας, των πηγών παρεμβολών των ραδιοσυχνοτήτων, της φυσικής περιοχής και των χαρακτηριστικών της, και την ισχύ, την συνδετικότητα, και χρήση της κεραίας. Θεωρητικά, οι εμβέλειες κυμαίνονται από **29 μέτρα (για 11 Mbps),** σε μια κλειστή περιοχή, έως και **485 μέτρα (για 1 Mbps)** σε μια ανοιχτή περιοχή. Εντούτοις, σύμφωνα με εμπειρικές αναλύσεις, η τυπική εμβέλεια για την διασύνδεση του εξοπλισμού ενός 802.11 είναι περίπου **50 μέτρα,** για εσωτερικούς χώρους. Μία εμβέλεια **400 μέτρων** καθιστά τα WLANs την ιδανική τεχνολογία για πολλές εφαρμογές σε πανεπιστημιουπόλεις. Είναι σημαντικό να σημειωθεί ότι η χρήση

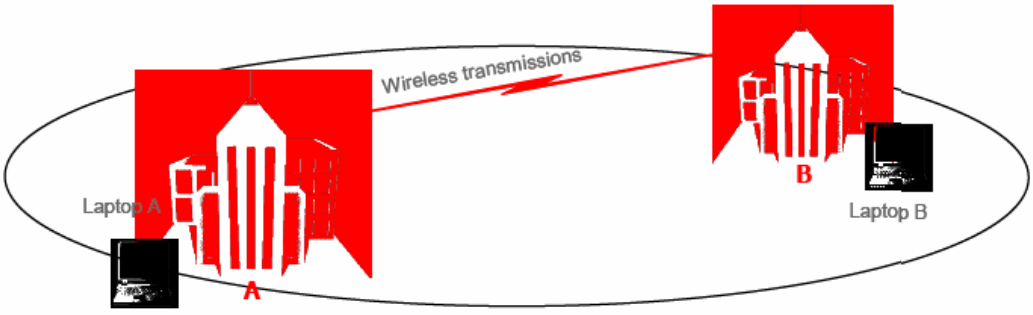
ειδικών κεραιών με αυξημένο κέρδος είναι δυνατόν να συντελέσει στην αύξηση της εμβέλειας.



Εικόνα 1.3 ***Τυπική εμβέλεια ενός 802.11 WLAN***

Τα APs μπορούν επίσης να παρέχουν την λειτουργία "γεφυροποίησης". Η γεφυροποίηση συνδέει δύο ή περισσότερα δίκτυα με τέτοιο τρόπο, ώστε να μπορούν να επικοινωνούν μεταξύ τους και να ανταλλάσσουν την κίνηση του δικτύου. Η λειτουργία αυτή εμπεριέχει είτε μία από σημείο σε σημείο (point-to-point) είτε από ένα σημείο προς πολλά (point-to-multipoint) αρχιτεκτονική. Σύμφωνα με την point-to-point αρχιτεκτονική, δύο LANs συνδέονται μεταξύ τους δια μέσου των αντίστοιχων APs των LANs. Όσον αφορά την multipoint γεφυροποίηση, το υποδίκτυο ενός LAN συνδέεται με άλλα υποδίκτυα ενός άλλου LAN μέσω του AP κάθε υποδικτύου.

Το Εικόνα 1.4 απεικονίζει την point-to-point γεφυροποίηση μεταξύ δύο LAN.



Εικόνα 1.4 ***Γεφυροποίηση των Access Points***

1.2.2 Πλεονεκτήματα Ασύρματων Δικτύων

Τα WLANs διαθέτουν τέσσερα θεμελιώδη πλεονεκτήματα:

- **Κινητικότητα Χρήστη:** Οι χρήστες μπορούν να έχουν πρόσβαση σε αρχεία, στους πόρους του δικτύου και στο διαδίκτυο, χωρίς την ύπαρξη σύνδεσης τους με καλώδια.
- **Γρήγορη Εγκατάσταση:** Ο απαιτούμενος χρόνος εγκατάστασης ενός δικτύου έχει μειωθεί διότι οι συνδέσεις στο δίκτυο γίνονται πλέον χωρίς την χρήση καλωδίων και την προσαρμογή τους ανάμεσα από τοίχους και οροφές.
- **Ευελιξία:** Τα ασύρματα δίκτυα διαθέτουν, επίσης, μεγάλη ευελιξία εξαιτίας της ευκολίας με την οποία εγκαθίστανται ή γκρεμίζονται, ανάλογα με τις ανάγκες κάθε οργανισμού.
- **Ευκολία Κλιμάκωσης:** Οι τοπολογίες WLAN δικτύων μπορούν να κλιμακώνονται, από μικρά peer-to-peer δίκτυα σε πολύ μεγάλα δίκτυα επιχειρήσεων, έτσι ώστε να ικανοποιούν συγκεκριμένες ανάγκες ως προς την εγκατάσταση και την εφαρμογή τους.
- Σε αντίθεση με τα συστήματα packet radio το Wi-Fi χρησιμοποιεί μη κατοχυρωμένο ραδιοφάσμα και δεν χρειάζεται έγκριση των αρχών για ιδιωτική ανάπτυξη .
- Επιτρέπει στα LANs να αναπτυχθούν χωρίς καλωδίωση , πιθανώς μειώνοντας το κόστος της ανάπτυξης και επέκτασης του δικτύου . Μέρη όπου τα καλώδια δεν μπορούν να υπάρχουν όπως εξωτερικές περιοχές και ιστορικά κτίρια , μπορούν να φιλοξενήσουν ασύρματα δίκτυα .
- Προ'ι'όντα Wi-Fi χρησιμοποιούνται μαζικά στην αγορά . Διαφορετικές μάρκες σημείων πρόσβασης και διεπαφών δικτύου πελατών συνεργάζονται σε ένα βασικό επίπεδο της υπηρεσίας .
- Ο ανταγωνισμός μεταξύ των πωλητών έχει μειώσει τις τιμές σημαντικά από την κυκλοφορία τους .
- Πολλά δίκτυα Wi-Fi υποστηρίζουν το roaming , στο οποίο μία φορητή συσκευή πελάτη όπως ένας φορητός υπολογιστής , μπορεί να μετακινηθεί από ένα σημείο πρόσβασης σε ένα άλλο καθώς ο χρήστης μετακινείται σε ένα κτίριο ή σε μια περιοχή .

- Πολλά σημεία πρόσβασης και διεπαφές δικτύων υποστηρίζουν διάφορα επίπεδα κρυπτογράφησης για να προστατέψουν τα δεδομένα από υποκλοπή.
- Το Wi-Fi είναι ένα παγκόσμιο σετ από στάνταρς . Αντίθετα με τους πελάτες δικτύου κυψελών , ο ίδιος Wi-Fi πελάτης μπορεί να δουλέψει σε διαφορετικές χώρες ανά τον κόσμο (αν και μπορεί να χρειαστεί κάποιες ρυθμίσεις στο λογισμικό) .

1.2.3 Μειονεκτήματα Ασύρματων Δικτύων

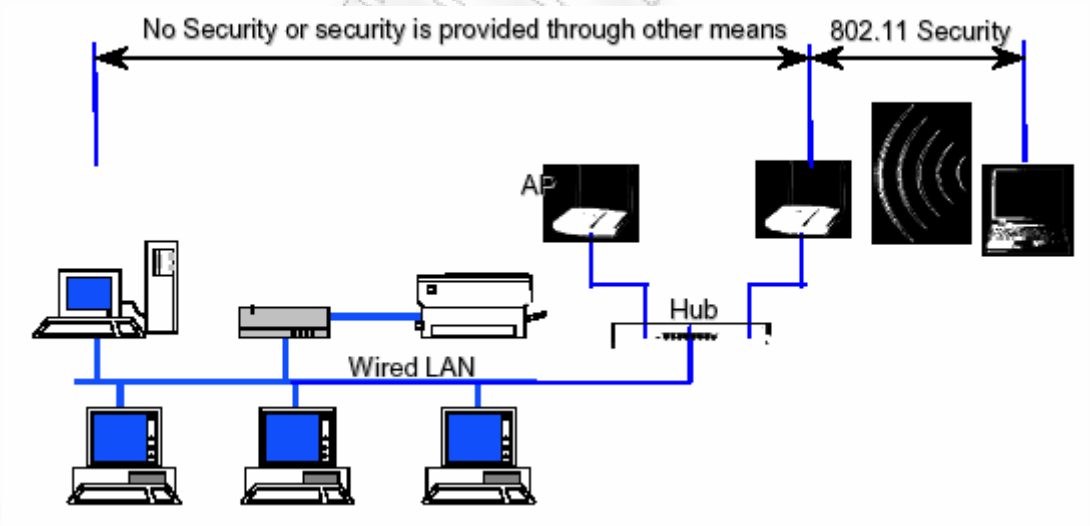
- Η χρησιμοποίηση της συχνότητας των 2.4GHz από το Wi-Fi δεν απαιτεί άδεια από τον περισσότερο κόσμο με την προϋπόθεση ότι κάποιος μένει κάτω από τα θεσμοθετημένα τυπικά όρια και με την προϋπόθεση ότι κάποιος δέχεται παρεμβολές από άλλες πηγές , συμπεριλαμβανομένων παρεμβολές που προκαλούν την δυσλειτουργία των συσκευών του .
- Η νομοθεσία δεν είναι ίδια παντού . Οι περισσότερες ευρωπα'ι'κές χώρες επιτρέπουν 2 κανάλια παραπάνω από αυτά των προδιαγραφών b , g . Η Ιαπωνία έχει και ένα ακόμα κανάλι , και χώρες όπως η Ισπανία απαγορεύουν την χρήση καναλιών με μικρότερους αριθμούς . Επιπλέον κάποιες χώρες όπως η Ιταλία συνήθιζε να ζητά μία «γενική άδεια» για οποιοδήποτε Wi-Fi που χρησιμοποιούνταν έξω από τα επιτρεπτά όρια ή ζητούσε κάτι παρόμοιο με εγγραφή χειριστή .
- Το 802.11b και το 802.11g χρησιμοποιούν το φάσμα των 2.4GHz , στο οποίο υπάρχει συνωστισμός από άλλες συσκευές όπως το Bluetooth , φούρνων μικροκυμάτων , ασύρματα τηλέφωνα (τα 900MHz ή τα 5.8GHz είναι εναλλακτικές συχνότητες τηλεφωνικές που μπορούν να χρησιμοποιηθούν για αποφυγή παρεμβολών με ένα Wi-Fi δίκτυο) και συσκευές αποστολής βίντεο ανάμεσασε πολλές άλλες . Αυτό μπορεί να προκαλέσει μία στατική μείωση στην απόδοση. Άλλες συσκευές που χρησιμοποιούν αυτές τις συχνότητες μικροκυμάτων μπορούν επίσης να προκαλέσουν σταδιακή μείωση στην απόδοση .
- Κλειστά σημεία πρόσβασης μπορούν να παρεμβάλλονται με σωστά ρυθμισμένα ανοιχτά σημεία πρόσβασης στην ίδια συχνότητα , εμποδίζοντας την λειτουργία των ανοιχτών σημείων πρόσβασης από άλλους .

- Η κατανάλωση ενέργειας είναι συγκριτικά πολύ μεγαλύτερη σε σχέση με άλλα στάνταρ κάνοντας την διάρκεια ζωής της μπαταρίας και την εκπεμπόμενη θερμότητα πρόβλημα.

2 Ασφάλεια

2.1 Ασφάλεια των 802.11 Ασύρματων LAN

Η ασφάλεια του προτύπου IEEE 802.11 εξασφαλίζεται κατά κύριο λόγο από το πρωτόκολλο WEP (Wired Equivalence Protocol) για την προστασία της ασύρματης μετάδοσης πακέτων μεταξύ των πελατών (clients) και των σημείων πρόσβασης (Access Points - APs). Το μειονέκτημα του WEP είναι ότι προσφέρει από σημείο σε σημείο (end–to–end) ασφάλεια μόνο για το ασύρματο κομμάτι της μετάδοσης, όπως παρουσιάζεται στην Εικόνα 2.1 .



Εικόνα 2.1 ***Ασφάλεια του 802.11 σε ένα τυπικό Ασύρματο Δίκτυο***

2.2 Χαρακτηριστικά της Ασφάλειας των 802.11 Ασύρματων LAN σύμφωνα με το Πρότυπο

Οι τρεις βασικές υπηρεσίες ασφάλειας, οι οποίες καθορίζονται από την επιτροπή IEEE για το WLAN, εξασφαλίζονται, όπως αναφέρθηκε, από το πρωτόκολλο WEP και είναι οι ακόλουθες:

- **Εμπιστευτικότητα (Confidentiality):** Η εμπιστευτικότητα, ή ιδιωτικότητα (privacy), αναπτύχθηκαν ώστε να εξασφαλίζουν την αποκάλυψη δεδομένων μόνο σε εξουσιοδοτημένους χρήστες.
- **Ακεραιότητα (Integrity):** Η ακεραιότητα διαβεβαιώνει ότι τα μηνύματα δεν τροποποιήθηκαν κατά την μεταφορά τους από τους ασύρματους πελάτες στο σημείο πρόσβασης.
- **Αυθεντικοποίηση (Authentication):** Ένας από τους πρωτεύοντες σκοπούς του WEP ήταν να παρέχει μία υπηρεσία ασφάλειας για την επαλήθευση της ταυτότητας των επικοινωνούντων πελατών. Η δεδομένη υπηρεσία εξασφαλίζει τον έλεγχο πρόσβασης στο δίκτυο, με την άρνηση της προσπέλασης του δικτύου από μη αυθεντικοποιημένους χρήστες.

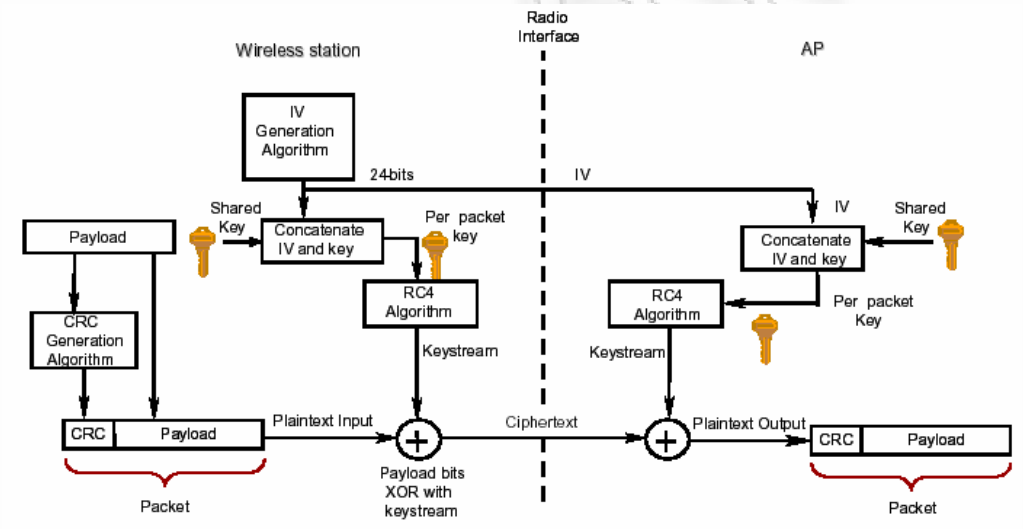
2.2.1 Εμπιστευτικότητα

Το πρότυπο 802.11 υποστηρίζει την εμπιστευτικότητα (ιδιωτικότητα) μέσω της χρήσης τεχνικών κρυπτογράφησης για την ασύρματη διεπαφή. Συγκεκριμένα χρησιμοποιείται η τεχνική του WEP, η οποία κάνει χρήση του αλγορίθμου συμμετρικού κλειδιού RC4 για τη δημιουργία μιας τυχαίας ακολουθίας χαρακτήρων. Αυτή η ακολουθία προστίθεται στα προς μετάδοση δεδομένα με χρήση της λογικής πράξης XOR. Μέσω της τεχνικής αυτής, τα δεδομένα μπορούν να προστατευθούν από τυχόν αποκάλυψή τους κατά τη διάρκεια της μετάδοσής τους στην ασύρματη ζεύξη.

Η τεχνική WEP, σύμφωνα με το πρότυπο 802.11, υποστηρίζει κλειδιά μεγέθους 40 bits, ως διαμοιραζόμενα κλειδιά. Εντούτοις, κάποιοι κατασκευαστές έχουν προσφέρει

κατά καιρούς επεκτάσεις του WEP οι οποίες υποστηρίζουν μεγέθη κλειδιών από 40 bits έως 104 bits, εκ των οποίων τα τελευταία μπορούν να φτάσουν και τα 128 bits, συμπεριλαμβανομένου του διανύσματος αρχικοποίησης (Initialization Vector-IV). Είναι γνωστό ότι καθώς μεγαλώνει το μήκος του κλειδιού, αυξάνεται αντίστοιχα και η ασφάλεια της κρυπτογραφικής τεχνικής, παρόλο που τυχόν υποτιθέμενες εσφαλμένες υλοποιήσεις ή κατασκευές κλειδιών είναι πιθανό να εμποδίσουν την αύξηση αυτή. Έρευνες έχουν δείξει ότι κλειδιά μήκους από 80 bits και πάνω κάνουν την κρυπτανάλυση με τη μέθοδο brute force ένα σχεδόν αδύνατο εγχείρημα. Για ένα κλειδί μήκους 80 bits ο αριθμός των δυνατών κλειδιών είναι μεγαλύτερος από 10^{26}!!!

Στην Εικόνα 2.2 παρουσιάζεται η θεμελίωση της εμπιστευτικότητας με την χρήση του WEP.



Εικόνα 2.2 Εμπιστευτικότητα κατά WEP με χρήση του Αλγορίθμου RC4

2.2.2 Ακεραιότητα

Το πρότυπο 802.11 παρέχει μια υπηρεσία για να εξασφαλίσει την ακεραιότητα, στα μηνύματα που μεταδίδονται μεταξύ των πελατών του ασύρματου δικτύου και των σημείων πρόσβασης. Αυτή η υπηρεσία έχει σχεδιασθεί για να απορρίπτει μηνύματα τα οποία έχουν τροποποιηθεί από ένα κακόβουλο τρίτο άτομο (man-in-the-middle).

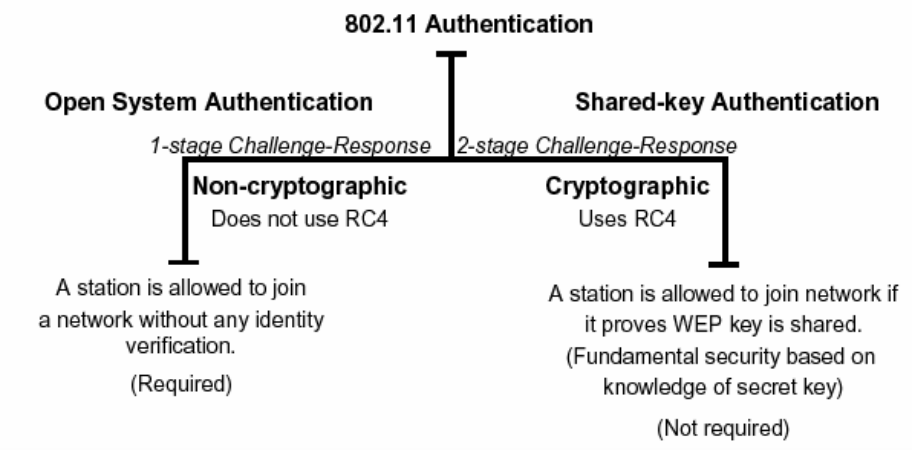
Γίνεται χρήση ενός απλού κρυπτογραφημένου κώδικα **CRC** (*Cyclic Redundancy Check* – Έλεγχος Κυκλικού Πλεονασμού). Όπως φαίνεται και στην Εικόνα 2.2, υπολογίζεται μια ακολουθία ελέγχου πλαισίου (**CRC - 32**) για κάθε πακέτο (payload) πριν την μετάδοση. Το πακέτο κρυπτογραφείται, έπειτα, με την τυχαία ακολουθία του RC4 και παρέχεται το κρυπτογραφημένο κείμενο (cipher-text). Στο άκρο της λήψης γίνεται αποκρυπτογράφηση και υπολογίζεται η ακολουθία ελέγχου πλαισίου (CRC) του ληφθέντος μηνύματος. Αν οι δύο ακολουθίες ελέγχου πλαισίου δεν είναι ίδιες, έχουμε παραβίαση της ακεραιότητας και το πακέτο απορρίπτεται.

Παρόλα αυτά η υπηρεσία είναι ευάλωτη σε διάφορες επιθέσεις, κυρίως γιατί ο έλεγχος κυκλικού πλεονασμού δεν είναι αρκετά ασφαλής κρυπτογραφική τεχνική όπως είναι μια συνάρτηση κατακερματισμού ή ένας MAC (Message Authentication Code).

2.2.3 Αυθεντικοποίηση

Το πρότυπο IEEE 802.11 χρησιμοποιεί δύο τεχνικές για την επαλήθευση της ταυτότητας των ασύρματων χρηστών που επιθυμούν να προσπελάσουν το ενσύρματο δίκτυο: την αυθεντικοποίηση ανοιχτού συστήματος (**open system authentication)** και την αυθεντικοποίηση διαμοιραζόμενου κλειδιού (**shared-key authentication)**, εκ των οποίων η δεύτερη βασίζεται στην κρυπτογραφία ενώ η πρώτη όχι.

Στην Εικόνα 2.3 παρατίθενται οι δύο τεχνικές αυθεντικοποίησης.

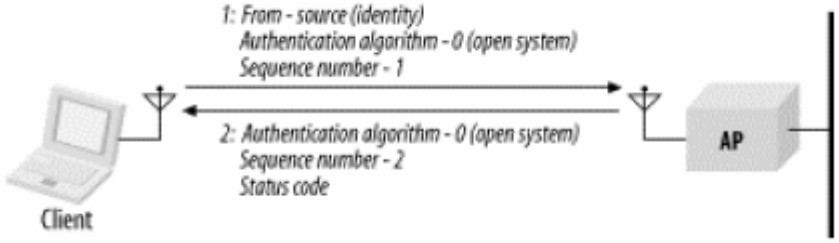


Εικόνα 2.3 ***Ταξινόμηση των τεχνικών Αυθεντικοποίησης του προτύπου 802.11***

2.2.3.1 Τεχνική Αυθεντικοποίησης Ανοιχτού Συστήματος

Η **τεχνική αυθεντικοποίησης ανοιχτού συστήματος** δεν είναι στην πραγματικότητα αυθεντικοποίηση, διότι ο κινητός σταθμός προσπελάζει το σημείο πρόσβασης χωρίς να εξακριβωθεί η ταυτότητά του. Επιπλέον, θα πρέπει να σημειωθεί ότι η αυθεντικοποίηση είναι μονόδρομη, δηλαδή μόνο ο κινητός σταθμός μπορεί να αυθεντικοποιηθεί, και πρέπει αυτός να θεωρήσει ότι επικοινωνεί με ένα πραγματικό σημείο πρόσβασης. Ο πελάτης αυθεντικοποιείται απλά ανταποκρινόμενος με μια MAC διεύθυνση κατά την ανταλλαγή των δύο μηνυμάτων με ένα σημείο πρόσβασης. Κατά τη διάρκεια της ανταλλαγής ο πελάτης δεν επικυρώνεται πραγματικά αλλά απλά απαντά με τα σωστά πεδία στην ανταλλαγή μηνυμάτων. Είναι φανερό ότι, χωρίς την χρήση κάποιας μεθόδου κρυπτογράφησης, η δεδομένη τεχνική είναι εξαιρετικά ευάλωτη στις επιθέσεις από μη εξουσιοδοτημένους χρήστες .

Η διαδικασία ανταλλαγής μιας αυθεντικοποίησης ανοιχτού συστήματος αποτελείται από δύο πλαίσια, τα οποία παρουσιάζονται στην Εικόνα 2.4 .



Εικόνα 2.4 ***Αυθεντικοποίηση Ανοιχτού Συστήματος***

Το πρώτο πλαίσιο, το οποίο προέρχεται από τον κινητό σταθμό, είναι ουσιαστικά ένα πλαίσιο διαχείρισης μιας υποκατηγορίας αυθεντικοποίησης. Το πρότυπο 802.11 δεν αναφέρει επισήμως αυτό το πλαίσιο ως αίτηση (request) αυθεντικοποίησης, αλλά αυτός είναι και ο πρακτικός του σκοπός. Κατά το 802.11, η ταυτότητα του κάθε σταθμού είναι η MAC διεύθυνσή του. Όπως και στα δίκτυα Ethernet, οι διευθύνσεις MAC πρέπει να είναι μοναδικές σε κάθε σημείο του δικτύου και μπορούν εύκολα να παίξουν και τον ρόλο των αναγνωριστικών των κινητών σταθμών. Τα σημεία πρόσβασης χρησιμοποιούν την πηγαία διεύθυνση των πλαισίων ως ταυτότητα του αποστολέα, χωρίς την χρήση πεδίων εντός του πλαισίου, για την επιπλέον

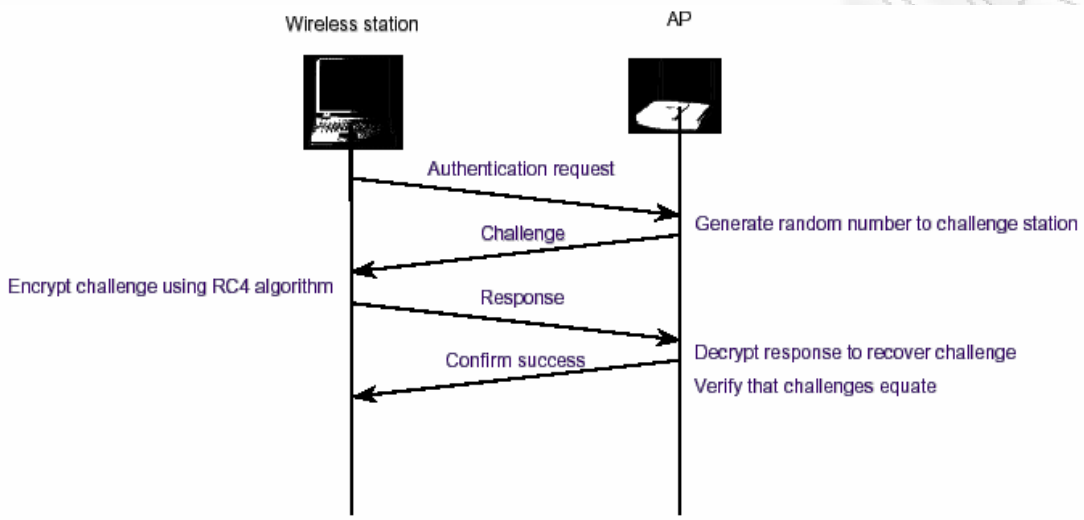
ταυτοποίηση του αποστολέα. Υπάρχουν δύο πληροφοριακά στοιχεία στο κύριο μέρος της αίτησης αυθεντικοποίησης. Πρώτον, το στοιχείο αναγνώρισης του αλγορίθμου αυθεντικοποίησης (Authentication Algorithm Identification), το οποίο είναι ρυθμισμένο στο 0 ώστε να δείχνει ότι η μέθοδος ανοιχτού συστήματος είναι σε λειτουργία. Δεύτερον, ο αριθμός της ακολουθίας ανταλλαγής της αυθεντικοποίησης (Authentication Transaction Sequence number), ο οποίος είναι ρυθμισμένος στο 1, ώστε να δείχνει ότι το πρώτο πλαίσιο είναι ουσιαστικά το πρώτο πλαίσιο της ακολουθίας.

Στην συνέχεια, το σημείο πρόσβασης επεξεργάζεται την αίτηση αυθεντικοποίησης και επιστρέφει την απόκριση (response) του. Όμοια με το πρώτο πλαίσιο, το πλαίσιο απόκρισης είναι ένα πλαίσιο διαχείρισης μιας υποκατηγορίας αυθεντικοποίησης. Τρία πληροφοριακά στοιχεία είναι παρόντα: Το πεδίο του στοιχείου αναγνώρισης του αλγορίθμου αυθεντικοποίησης (Authentication Algorithm Identification), το οποίο είναι ρυθμισμένο στο 0 ώστε να δείχνει την ύπαρξη αυθεντικοποίησης ανοιχτού συστήματος, ο αριθμός ακολουθίας (Sequence Number) που είναι 2, και ο κώδικας κατάστασης (Status Code), ο οποίος δείχνει την έκβαση της αίτησης αυθεντικοποίησης.

2.2.3.2 Τεχνική Αυθεντικοποίησης Διαμοιραζόμενου κλειδιού

Η **τεχνική αυθεντικοποίησης διαμοιραζόμενου κλειδιού**, όπως αναφέρθηκε και παραπάνω, χρησιμοποιεί την κρυπτογραφία και βασίζεται στη γνώση του διαμοιραζόμενου κλειδιού από τον πελάτη (ο αλγόριθμος που χρησιμοποιείται είναι συμμετρικός και είναι ο RC4). Αρχικά το AP δημιουργεί και στέλνει στον πελάτη μια τυχαία ακολουθία χαρακτήρων μήκους 128 bits (***challenge***). Ο πελάτης, χρησιμοποιώντας το μυστικό κλειδί (που μοιράζεται με το AP), κρυπτογραφεί την ακολουθία αυτή και στέλνει το αποτέλεσμα της κρυπτογράφησης στο AP (***response***). Το AP αποκρυπτογραφεί την ακολουθία που μόλις στάλθηκε από τον πελάτη και του επιτρέπει την πρόσβαση μόνο αν είναι ίδια με την ακολουθία που είχε σταλεί αρχικά. Πρέπει να σημειωθεί ότι και αυτή η τεχνική πάσχει αμοιβαίας αυθεντικοποίησης. Επομένως, είναι ευπαθής σε διαφόρων ειδών επιθέσεις, συμπεριλαμβανομένης και της γνωστής man-in-the-middle .

Η Εικόνα 2.5 είναι ένα διάγραμμα ροής το οποίο αναπαριστά την διαδικασία αυθεντικοποίησης με τη χρήση της τεχνικής διαμοιραζόμενου κλειδιού.



Εικόνα 2.5 ***Αυθεντικοποίηση Μηνύματος με την χρήση Διαμοιραζόμενου κλειδιού***

2.3 Βασικοί Μηχανισμοί Ασφάλειας

Έχουν αναπτυχθεί τρεις βασικοί μηχανισμοί για την ασφάλιση ενός σημείου πρόσβασης (Access Point) στα 802.11 δίκτυα :

- Το **SSID** (Service set identifier)
- Το **MAC** (Media Access Control) address filtering
- Το **WEP** (Wired Equivalent Privacy)

Σε ένα ασύρματο δίκτυο μπορεί να εφαρμοστεί ένας ή και περισσότεροι από τους παραπάνω μηχανισμούς. Εντούτοις, θα πρέπει να γνωρίζουμε ότι η καλύτερη ασφάλεια επιτυγχάνεται όταν εφαρμόζονται και οι τρεις μηχανισμοί μαζί.

2.3.1 SSID (Service Set Identifier)

Ο έλεγχος πρόσβασης σε ένα δίκτυο μπορεί να εφαρμοστεί χρησιμοποιώντας ένα SSID σε συνδυασμό, είτε με ένα είτε με μία ομάδα από Access Points. Το SSID, δρώντας ως αναγνωριστικό ενός WLAN, παρέχει ένα μηχανισμό ο οποίος "τεμαχίζει" ένα ασύρματο δίκτυο σε μία υπηρεσία πολλαπλών δικτύων αποτελούμενων από ένα ή περισσότερα APs. Κάθε AP είναι εφοδιασμένο με ένα SSID, το οποίο ανταποκρίνεται σε ένα συγκεκριμένο ασύρματο δίκτυο. Επομένως, για να προσπελάσει ένας υπολογιστής το δίκτυο, θα πρέπει να είναι ρυθμισμένος με το σωστό SSID, το οποίο προστίθεται στην επικεφαλίδα (header) κάθε πακέτου που στέλνεται μέσω του WLAN και, έπειτα, επαληθεύεται από το AP .

Η πιστοποίηση ενός υπολογιστή σε ένα AP μέσω του SSID καθιστά το AP ικανό να δρα ως κωδικός πρόσβασης, πράγμα το οποίο παρέχει ένα μέτρο ασφάλειας σε ένα WLAN. Εντούτοις, η εν λόγω υποτυπώδης ασφάλεια ενδέχεται να παραβιαστεί στην περίπτωση κατά την οποία το AP είναι ρυθμισμένο ώστε να γνωστοποιεί το SSID του.

2.3.2 MAC Address Filtering

Ενώ ένα AP, ή ένα σύνολο από APs, μπορούν να πιστοποιηθούν μέσω ενός SSID, ένας υπολογιστής είναι δυνατόν να πιστοποιηθεί μέσω της μοναδικής διεύθυνσης MAC που διαθέτει η κάρτα δικτύου του σύμφωνα με το πρότυπο 802.11. Για να επιτευχθεί αύξηση της ασφάλειας ενός 802.11 δικτύου, κάθε AP μπορεί να εφοδιαστεί με μία λίστα η οποία περιλαμβάνει τις διευθύνσεις MAC που συσχετίζονται με τους υπολογιστές που επιτρέπεται να προσπελάσουν το AP. Σε περίπτωση που η διεύθυνση MAC ενός υπολογιστή δεν περιέχεται στην λίστα, τότε δεν θα του επιτραπεί η σύνδεση με το AP .

Η προκείμενη ασφάλεια παρέχει υψηλό επίπεδο ασφάλειας, αλλά ενδείκνυται για μικρά μόνο δίκτυα. Η δημιουργία της λίστας των διευθύνσεων MAC πρέπει να γίνεται χειροκίνητα σε κάθε AP, και, επιπλέον, η λίστα θα πρέπει να ενημερώνεται

συνεχώς, με αποτέλεσμα η υπερκείμενη διαχειριστικότητα να περιορίζει την κλιμάκωση αυτής της προσέγγισης .

2.3.3 WEP (Wired Equivalent Privacy)

Το WEP παρέχει κρυπτογραφημένη επικοινωνία, χρησιμοποιώντας ένα κλειδί κρυπτογράφησης για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων. Το δεδομένο κλειδί υπάρχει και στον client αλλά και σε κάθε AP, ώστε και τα δύο μέρη να πιστοποιούν την ταυτότητά τους προτού προχωρήσουν σε επικοινωνία .

Το πρόβλημα της χρήσης WEP είναι ότι το πρότυπο 802.11 δεν υποστηρίζει κάποιο πρωτόκολλο διαχείρισης για ηλεκτρονική διαχείριση κλειδιών, με αποτέλεσμα όλα τα κλειδιά να εισάγονται χειροκίνητα στα APs από τους διαχειριστές. Επομένως, η διαδικασία αυτή καθιστά πολύ δύσκολη την χρήση WEP στα μεγάλα σε αριθμό συσκευών ασύρματα δίκτυα .

2.3.4 Wi-Fi Προστατευμένη Πρόσβαση (Wi-Fi Protected Access, WPA)

Το πρότυπο IEEE 802.11i αποτελεί μια νεότερη έκδοση του αρχικού 802.11, που ενσωματώνει ένα καινούριο σύστημα ασφάλειας, το οποίο αναπτύχθηκε από την ομάδα εργασίας i του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE TGi). Με το νέο πρότυπο επιδιώκεται να αντιμετωπιστούν οι αδυναμίες του πρωτοκόλλου Ενσύρματου Ισοδύναμου Απόρρητου (WEP).

Για να το επιτύχει αυτό περιλαμβάνει το πλαίσιο εργασίας της διαδικασίας πιστοποίησης του προτύπου IEEE 802.1X, το Πρωτόκολλο Χρονικού Κλειδιού Ακεραιότητας (Temporal Key Integrity Protocol, TKIP), το Πρότυπο Προηγμένης Κρυπτογράφησης (Advanced Encryption Standard,AES), ιεραρχία κλειδιών και νέα χαρακτηριστικά διαχείρισής τους καθώς και διαδικασίες διαπραγμάτευσης για την κρυπτογράφηση των δεδομένων και την πιστοποίηση της ταυτότητας του

σταθμού. Στο μμεταξύ εξαιτίας των όλο και αυξανόμενων απαιτήσεων ασφάλειας από το 802.11 η WECA (Wireless Ethernet Compatibility Alliance), γνωστή και ως Συμμαχία Wi-Fi, υιοθέτησε κάποια κομμάτια του 802.11i και δημιούργησε ένα καινούριο πρότυπο ασφάλειας, γνωστό ως Wi-Fi Προστατευμένη Πρόσβαση (Wi-Fi Protected Access, WPA), το οποίο μπορεί να ενσωματωθεί στο 802.11 με απλή

αναβάθμιση του λογισμικού. Ουσιαστικά το μόνο κομμάτι του 802.11i που δεν ενσωματώθηκε είναι αυτό που αναφέρεται στην κρυπτογράφηση των δεδομένων, αφού κάτι τέτοιο απαιτεί την αναβάθμιση του υπάρχοντος εξοπλισμού. Έτσι τα τμήματα που αποτελούν την Wi-Fi Προστατευμένη Πρόσβαση είναι:

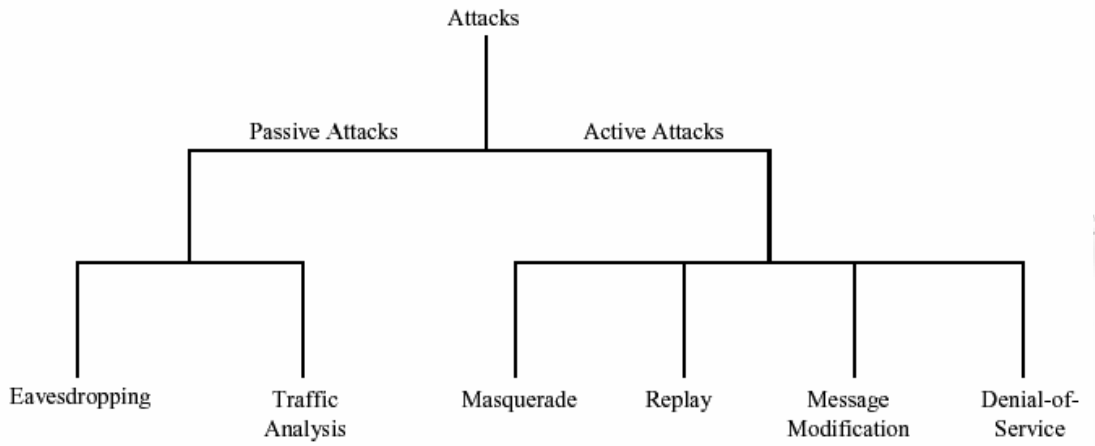
- Το πλαίσιο εργασίας της διαδικασίας πιστοποίησης του πρότυπου 802.1X.
- Το Πρωτόκολλο Χρονικού Κλειδιού Ακεραιότητας (TKIP).
- Η ιεραρχία των κλειδιών και τα νέα χαρακτηριστικά διαχείρισής τους.
- Οι διαδικασίες διαπραγμάτευσης για την κρυπτογράφηση των δεδομένων και την πιστοποίηση της ταυτότητας του σταθμού.

2.4 Ευπάθειες των 802.11 WLANs

Αν και η πορεία των 802.11 WLANs είναι εξελικτική, παρατηρήθηκε το γεγονός ότι τα δίκτυα αυτά αντιμετωπίζουν τρομερά προβλήματα ασφάλειας. Πολλές αναφορές σχετικές με τα 802.11 WLANs περιγράφουν τις επιθέσεις που γίνονται συνεχώς και αναφέρουν τους κινδύνους στους οποίους εκτίθενται οι οργανισμοί.

2.4.1 Ευπάθειες ενός Ασύρματου Δικτύου

Η Εικόνα 2.6 παρουσιάζει μία γενική ταξινομία των επιθέσεων κατά της ασφάλειας ώστε να βοηθήσει τους οργανισμούς και τους χρήστες να αντιληφθούν το είδος και τον τύπο της καθεμιάς.



<u>Εικόνα 2.6</u> Ταξινόμηση των Επιθέσεων κατά της Ασφάλειας

Οι επιθέσεις κατά της ασφάλειας των δικτύων χωρίζονται τυπικά σε δύο κατηγορίες, τις ακούσιες και τις εκούσιες. Αυτές οι δύο μεγάλες κατηγορίες μπορούν να υποδιαιρεθούν και σε άλλους τύπους επιθέσεων. Όλοι αυτοί οι τύποι επιθέσεων περιγράφονται ακολούθως :

- **Ακούσια Επίθεση (Passive Attack)** – Είναι η επίθεση κατά την οποία ένα μη εξουσιοδοτημένο μέλος αποκτά το πλεονέκτημα πρόσβασης σε έναν πόρο, χωρίς όμως να αλλάζει το περιεχόμενο του (π.χ., παρακολούθηση συνόδου ή ανάλυση της κίνησης).
    - **Παρακολούθηση συνόδου (Eavesdropping)** – Ο επιτιθέμενος παρακολουθεί τις μεταδόσεις για να δει το περιεχόμενο του μηνύματος.
    - **Ανάλυση της Κίνησης (Traffic analysis)** – Ο επιτιθέμενος αποκτά πληροφορίες, με πιο επιδέξιο τρόπο, παρακολουθώντας τις μεταδόσεις και συμπεραίνοντας τον τρόπο επικοινωνίας.
- **Εκούσια Επίθεση (Active Attack)** – Κατά την εκούσια επίθεση, ένα μη εξουσιοδοτημένο μέλος κάνει τροποποιήσεις σε ένα μήνυμα, μία ακολουθία δεδομένων, ή ένα αρχείο. Είναι πιθανό η επίθεση αυτή να ανιχνευθεί, αλλά δυστυχώς δεν είναι δυνατόν να εξαλειφθεί. Οι τύποι των εκούσιων επιθέσεων αναλύονται ακολούθως .

- **Προσποίηση (Masquerading)** – Ο επιτιθέμενος προσποιείται έναν εξουσιοδοτημένο χρήστη, με αποτέλεσμα να κερδίζει συγκεκριμένα προνόμια τα οποία δεν του ανήκουν.
- **Επανάληψη (Replay)** – Ο επιτιθέμενος παρακολουθεί τις μεταδόσεις και αναμεταδίδει μηνύματα σαν νόμιμος χρήστης.
- **Τροποποίηση μηνύματος (Message modification)** – Ο επιτιθέμενος αλλάζει το κανονικό μήνυμα, διαγράφοντας, προσθέτοντας, αλλάζοντας, ή αναδιατάσσοντας το περιεχόμενό του.
- **Άρνηση Εξυπηρέτησης (Denial-of-Service)** – Ο επιτιθέμενος εμποδίζει την κανονική χρήση ή διαχείριση των υπηρεσιών από τους νόμιμους χρήστες.
- **Ανακατεύθυνση της Κίνησης (Traffic Redirection)** − Ένας εισβολέας μπορεί να αλλάξει την πορεία της κίνησης, με αποτέλεσμα, τα πακέτα που προορίζονταν αρχικά για έναν συγκεκριμένο προορισμό, να ανακατευθύνονται στον επιτιθέμενο σταθμό.
- **Παράνομα Σημεία Πρόσβασης (Rogue Access Points)** − Ένα τέτοιο AP εγκαθίσταται από κάποιον επιτιθέμενο (συνήθως σε δημόσιες περιοχές όπως κοινόχρηστους εργασιακούς χώρους, αεροδρόμια κτλ.), ώστε να προσποιείται μία έγκυρη συσκευή αυθεντικοποίησης και να δέχεται την κίνηση από τους clients. Με αυτόν τον τρόπο είναι δυνατόν να αποσπώνται ευαίσθητες πληροφορίες από τα πακέτα, ή ακόμα και να τροποποιείται το περιεχόμενό τους.
- **Εισβολή και υποκλοπή των πόρων ενός δικτύου (Intrusion & Resource Stealing)** − Οι πόροι ενός δικτύου περιλαμβάνουν την πρόσβαση σε ποικίλες συσκευές (όπως για παράδειγμα εκτυπωτές και εξυπηρετητές) και υπηρεσίες (όπως η επικοινωνία σε ένα εσωτερικό δίκτυο ή στο Internet). Για την εισβολή σε ένα δίκτυο, ο επιτιθέμενος αποκτά αρχικά γνώση των παραμέτρων πρόσβασης για το συγκεκριμένο δίκτυο. Για παράδειγμα, εάν το υποκείμενο δίκτυο χρησιμοποιεί φιλτράρισμα των clients βάσει των MAC διευθύνσεων τους, τότε το μόνο που χρειάζεται να κάνει ο εισβολέας είναι να μάθει την MAC και την IP διεύθυνση ενός client και να χρησιμοποιεί το δίκτυο, και τους πόρους του γενικότερα, ως έγκυρος χρήστης όταν ο client θα είναι αποσυνδεδεμένος.

2.4.2 Ευπάθειες του Προτύπου IEEE 802.11

Έχουν παρουσιαστεί κατά καιρούς πολλά προβλήματα σχετικά με την ασφάλεια των WLANs, τα οποία επιτρέπουν σε κακόβουλους χρήστες να βλάπτουν την ασφάλεια των δικτύων αυτών. Συνέπεια των παραπάνω είναι οι επιθέσεις ανάλυσης της κίνησης, αποκρυπτογράφησης της κίνησης, ο φόρτος της κίνησης από μη εξουσιοδοτημένους χρήστες και οι επιθέσεις λεξικού .

Οι ευπάθειες που αναφέρθηκαν παραπάνω σχετίζονταν με τα ασύρματα δίκτυα γενικότερα. Το μεγαλύτερο ενδιαφέρον για την ασφάλεια όμως επικεντρώνεται περισσότερο στο πρότυπο IEEE 802.11 δίκτυο, όσον αφορά τα ακόλουθα :

1. **Αυθεντικοποίηση βάσει των διευθύνσεων MAC (MAC Address Authentication):** Αυτού του είδους η αυθεντικοποίηση επαληθεύει την ταυτότητα ενός μηχανήματος και όχι του χρήστη του. Επομένως, ένας επιτιθέμενος, ο οποίος καταφέρει να κλέψει έναν φορητό υπολογιστή, εμφανίζεται στο δίκτυο ως νόμιμος χρήστης.
2. **Μονόδρομη Αυθεντικοποίηση (One-way Authentication):** Η αυθεντικοποίηση με βάση το WEP είναι μονόδρομη. Αυτό σημαίνει ότι ο χρήστης αποδεικνύει την ταυτότητα του σε ένα AP αλλά όχι το αντίστροφο. Επομένως, ένα παράνομο AP θα μπορούσε να αυθεντικοποιήσει επιτυχώς έναν χρήστη και στην συνέχεια να υποκλέψει όλα τα πακέτα που προορίζονται στον νόμιμο σταθμό.
3. **SSID:** Εφόσον το SSID προστίθεται στην επικεφαλίδα του πακέτου και μεταφέρεται σε καθαρή μορφή κειμένου, παρέχει, τελικώς, πολύ μικρή ασφάλεια. Επομένως, μπορεί να θεωρηθεί πιο πολύ ως ένας αναγνωριστής δικτύου παρά χαρακτηριστικό ασφάλειας.
4. **Χρήση στατικών κλειδιών WEP:** Η χρήση κοινού κλειδιού από όλους τους σταθμούς είναι μεγάλη ευπάθεια του συστήματος, διότι μπορεί να οδηγήσει στην έκθεση ενός μεγάλου ποσού της κίνησης σε έναν υποτιθέμενο hacker ή ακόμα και την έκθεση του ίδιου κλειδιού σε περίπτωση κλοπής του φορητού

υπολογιστή. Επιπλέον, όπως αναφέρθηκε και παραπάνω, η εισαγωγή των κλειδιών χειροκίνητα δημιουργεί ζητήματα διαχειριστικότητας.

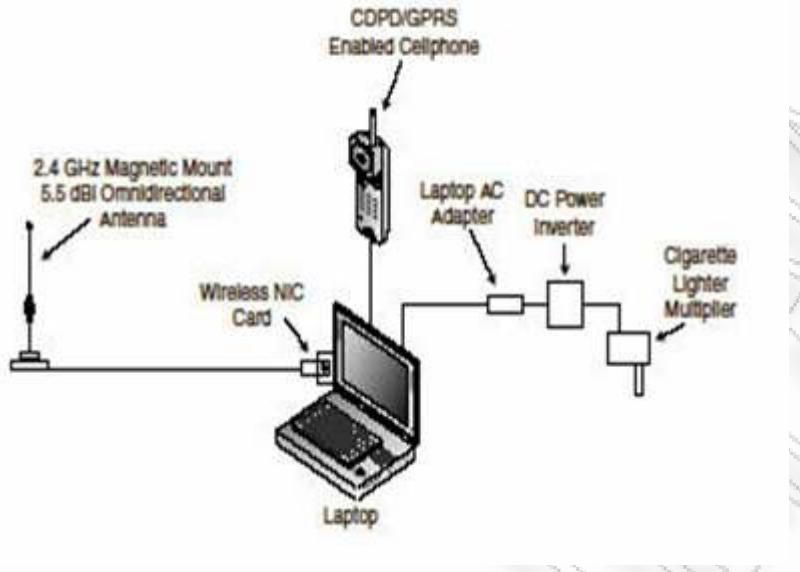
5. **Ευπάθεια του κλειδιού WEP:** Η κρυπτογράφηση βάσει του κλειδιού WEP δημιουργήθηκε ώστε να προσφέρει ίδιο επίπεδο ασφάλειας με εκείνο των ενσύρματων δικτύων. Εντούτοις, προέκυψαν αργότερα πολλές ανησυχίες όσον αφορά την ασφάλεια του WEP . Μερικά από αυτά περιγράφονται εκτενέστερα παρακάτω :
    - **Το IV (Initialization Vector) στο WEP:** Το μήκος των 24 bits ενός IV θεωρείται πολύ μικρό όταν χρησιμοποιείται για κρυπτογραφικούς σκοπούς, με αποτέλεσμα να υπάρχει πιθανότητα επαναχρησιμοποίησης του και, επομένως, παραγωγής της ίδιας ακολουθίας χαρακτήρων.
    - **Το IV είναι μέρος του κλειδιού RC4:** Το γεγονός ότι ένας επιτιθέμενος είναι δυνατόν να γνωρίζει τα 24 bits κάθε πακέτου, σε συνδυασμό με την αδυναμία του αλγορίθμου RC4, οδηγεί σε μία επιτυχή επίθεση ανάλυσης, κατά την οποία ανακτάται το κλειδί, μετά την αναχαίτιση και την ανάλυση ενός μόνο μικρού μέρους της κίνησης.
    - **Το WEP δεν παρέχει καμία προστασία της ακεραιότητας:** Το πρωτόκολλο MAC του 802.11 χρησιμοποιεί τον αλγόριθμο CRC, ο οποίος είναι ένας μη κρυπτογραφικός αλγόριθμος, για τον έλεγχο της ακεραιότητας των πακέτων και την επιβεβαίωση λήψης τους με τον σωστό έλεγχο αθροίσματος. Ο συνδυασμός των μη κρυπτογραφικών ελέγχων αθροίσματος, με τους stream αλγορίθμους κρυπτογράφησης είναι επικίνδυνος και συχνά συνιστά στην δημιουργία ευπαθειών, όπως συμβαίνει και στην περίπτωση του WEP.

3 Wardriving

Ο όρος «Wardriving» χρησιμοποιείται για να περιγράψει την πρακτική εκείνη κατά την οποία ένας χρήστης του Διαδικτύου περιπλανιέται στους δρόμους συνοικιών εφοδιασμένος με συσκευή που έχει δυνατότητα ασύρματης πρόσβασης στο Διαδίκτυο με σκοπό να εντοπίσει ασύρματα δίκτυα πρόσβασης στο Διαδίκτυο οικιακής ή επαγγελματικής χρήσης και να χαρτογραφήσει την ύπαρξή τους για στατιστικούς ή άλλους λόγους.

Το Wardriving αναφέρθηκε για πρώτη φορά στις ΗΠΑ όταν ο σύμβουλος ασφαλείας τηλεπικοινωνιακών δικτύων Peter M. Shipley έκανε, το 2000, έρευνα για τα ασύρματα δίκτυα στην πόλη Berkeley της California και δημοσιοποίησε τα αποτελέσματα των ερευνών του στο ετήσιο DefCon συνέδριο hackers τον Ιούλιο του 2001. Η έρευνα του Shipley αποσκοπούσε να δείξει τα κενά ασφαλείας των ασύρματων δικτύων που αναπτύσσονταν ραγδαία στο Berkeley, και να προκαλέσει την προσοχή των καθ' ύλη αρμοδίων φορέων για την βελτίωση της ασύρματης τεχνολογίας δικτύων αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων. Με την έρευνά του ο Shipley απέδειξε ότι είναι δυνατή η πρόσβαση σε ασύρματο δίκτυο, κάνοντας χρήση απλών εργαλείων, ακόμη και από απόσταση σαράντα χιλιομέτρων μακριά από την κορυφή του κτιρίου όπου έχει τοποθετηθεί πομπός ασύρματης δικτύωσης. Το Wardriving δεν απαιτεί τη χρήση ακριβού ή δυσεύρετου εξοπλισμού για την διενέργειά του. Μπορεί να γίνει με χρήση είτε φορητού ηλεκτρονικού υπολογιστή είτε προσωπικού ψηφιακού βοηθού (PDA).

Η παρακάτω απεικόνιση δείχνει τη συνδεσμολογία των εργαλείων του Wardriving με χρήση φορητού ηλεκτρονικού υπολογιστή που έχει παροχή ρεύματος από τον αναπτήρα του αυτοκινήτου.



Εικόνα 3.1

3.1 Προέλευση του Wardriving

Το Wardriving πήρε την ονομασία του κατά παράφραση μίας συνήθους πρακτικής στη δεκαετία του 1980 γνωστής ως **«Wardialing»** κατά την οποία οι δράστες καλούσαν τηλεφωνικούς αριθμούς επιλεγμένους στην τύχη με σκοπό να εντοπίσουν dial-up modems σε λειτουργία και στη συνέχεια να επιχειρήσουν την παράνομη χρήση αυτών των modems για την παράνομη πρόσβαση των δραστών σε τηλεφωνικά δίκτυα, αλλά αργότερα και στο Διαδίκτυο. Η διενέργεια του Wardriving έλαβε, σχεδόν αμέσως, διαστάσεις μαζικού κινήματος και προβλήθηκε από τα αμερικανικά media ως λαμπρή ιδέα. Αλλά και στην Ευρώπη, το Wardriving εμφάνισε από νωρίς συμπτώματα μαζικού κινήματος. Σε έρευνα που διενήργησε η εταιρία KPMG Λονδίνου το 2003 με σκοπό να καταγράψει το Wardriving στο Λονδίνο, προέκυψε ότι κατά μέσον όρο γίνονταν 3,4 προσπάθειες σύνδεσης ημερησίως με συγκεκριμένα σημεία πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο που έστησε η KPMG σε κεντρικά σημεία του Λονδίνου από Wardrivers. Η έρευνα της KPMG κατέγραψε ένα σημαντικό ποσοστό προσπαθειών hacking από τους Wardrivers του Λονδίνου. Σε μεταγενέστερη έρευνα του 2004 που έγινε στο Λονδίνο από την εταιρία RSA Security, βρέθηκε ότι μόνο το 66% των ιδιωτικών εταιρικών ασύρματων δικτύων

χρησιμοποιούσαν στοιχειώδη συστήματα προστασίας από τους Wardrivers και hackers. Υπόψη, δε, του γεγονότος ότι κατά τη διάρκεια του 2004 στο Λονδίνο εμφανίστηκε αύξηση της χρήσης ασύρματων δικτύων κατά 235%, αντιλαμβάνεται κανείς ότι το 34% των μη φυλασσόμενων ή προστατευμένων ασύρματων δικτύων, βάσει των στοιχείων της έρευνας αυτής, αντιστοιχούσε σε εξαιρετικά μεγάλο αριθμό ασύρματων δικτύων. Αξίζει, επίσης, να σημειωθεί ότι με αφορμή τη δημοσιότητα και τη μαζικότητα του Wardriving, το hacking των ασύρματων συστημάτων δικτύωσης βασισμένων στο πρωτόκολλο επικοινωνίας 802.11 (Wi-Fi συστήματα) έγινε αντικείμενο και ακαδημαϊκής διδαχής σε προβεβλημένα πανεπιστήμια όπως το Massachusetts Institute of Technology.

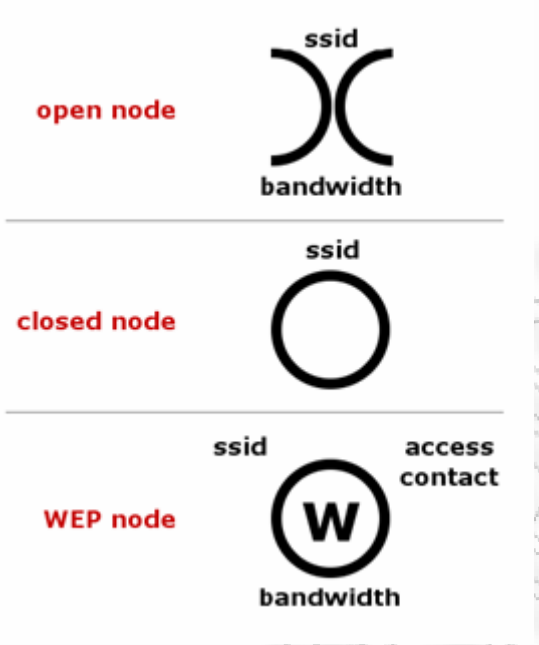
Phreaking

Η έννοια του Phreaking είναι παρόμοια με αυτήν του Wardialing από το οποίο έλκει τις ρίζες του το Wardriving. Το Phreaking αναφέρεται στις προσβολές του τηλεφωνικού δικτύου δια των οποίων ο δράστης επιδιώκει ν' αποφύγει τη χρέωσή του για τις τηλεφωνικές του κλήσεις. Το Phreaking «άνθισε» πριν από την μετατροπή του τηλεφωνικού δικτύου από αναλογικό σε ψηφιακό. Υπ' αυτή την έννοια, το Phreaking είναι προγενέστερο του hacking. Οι κυριότερες περιπτώσεις Phreaking αφορούσαν στη χρήση «red boxes» με τη χρήση των οποίων ο δράστης έκανε δωρεάν τηλεφωνικές κλήσεις από τηλεφωνικούς θαλάμους. Επίσης, στη χρήση «blue boxes» με τη χρήση των οποίων ο δράστης έκανε τηλεφωνικές κλήσεις παραπλανώντας την τηλεφωνική εταιρία η οποία αντιλαμβανόταν την τηλεφωνική κλήση σαν να είχε γίνει από το τηλεφωνικό της κέντρο—operator. Στην πραγματικότητα, ο δράστης προκαλούσε την μετάδοση ηχητικού τόνου μέσω του τηλεφωνικού δικτύου που ήταν ίδιος με αυτόν που δημιουργείται σε περίπτωση λειτουργίας του operator. Επίσης, στη χρήση «black boxes» με τη χρήση των οποίων ο δράστης έκανε τηλεφωνικές κλήσεις παραπλανώντας την τηλεφωνική εταιρία η οποία αντιλαμβανόταν την τηλεφωνική κλήση ως γενομένη χωρίς χρέωση του καλούντος. Και στη χρήση «silver boxes» με τη χρήση των οποίων ο δράστης έκανε τηλεφωνικές κλήσεις παραπλανώντας την τηλεφωνική εταιρία η οποία αντιλαμβανόταν την τηλεφωνική κλήση σαν να είχε γίνει από συγκεκριμένο PBX τηλεφωνικό κέντρο. Στην πραγματικότητα, ο δράστης προκαλούσε την μετάδοση ηχητικού τόνου μέσω του

τηλεφωνικού δικτύου που ήταν ίδιος με αυτόν που δημιουργείται σε περίπτωση λειτουργίας του PBX τηλεφωνικού κέντρου, για ειδικές περιπτώσεις κλήσεων όπως κλήσεις προτεραιότητας, επείγουσας ανάγκης κλπ. Η ψηφιοποίηση του αναλογικού τηλεφωνικού δικτύου και η χρήση ψηφιακών πληροφοριακών συστημάτων για τη λειτουργία του κατέστησε δυσχερή και ίσως άνευ νομικής σημασίας πλέον τη διάκριση μεταξύ Phreaking και hacking. Ο γνωστότερος δράστης Phreaking, ο Ian Arthur Murphy, καταδικάστηκε το 1981 για hacking και έγινε έτσι ο πρώτος καταδικαστείς hacker στη ιστορία του ηλεκτρονικού εγκλήματος.

Warchalking

Συχνά, οι Wardrivers, αφού εντοπίσουν ασύρματα δίκτυα, οικιακής ή επαγγελματικής χρήσης, για την πρόσβαση στο Διαδίκτυο δημοσιοποιούν κάθε σχετικό στοιχείο σε διαδικτυακούς τόπους μέσω των οποίων έρχονται σε επικοινωνία με ομοϊδεάτες τους. Για τη δημοσιοποίηση στοιχείων που αφορούν σε ασύρματα δίκτυα πρόσβασης στο Διαδίκτυο, χρησιμοποιείται ο όρος «Warchalking». Το Warchalking κυρίως περιγράφει τη σήμανση με σημειωτικούς χαρακτήρες συνήθως επί ακινήτων που βρίσκονται στην περιοχή στην οποία επιτυγχάνεται η κτήση πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο με σκοπό να επωφεληθούν και άλλοι που ενδεχόμενα θελήσουν να κάνουν χρήση της εντοπισμένης ασύρματης πρόσβασης στο δίκτυο ή Διαδίκτυο. Το Warchalking πήρε την ονομασία του κατά παράφραση μίας συνήθους πρακτικής στη δεκαετία του ’30 στην Αμερική, με την οποία συνήθιζαν οι άστεγοι να μαρκάρουν σπίτια ή περιοχές στα οποία μπορούσαν να βρουν καταφύγιο. Οι Warchalkers χρησιμοποιούν τους παρακάτω σημειωτικούς χαρακτήρες που έχουν ήδη γίνει γνωστοί για να γνωστοποιήσουν το είδος και την ευρυζωνικότητα του εντοπισμένου ασύρματου σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένο με το Διαδίκτυο.



Εικόνα 3.2

Από τα παραπάνω χρησιμοποιούμενα σύμβολα, το πρώτο γνωστοποιεί την ύπαρξη ενός ανοιχτού σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένου στο Διαδίκτυο. Στο πάνω μέρος του συμβόλου σημειώνονται στοιχεία του Service Set Identifier (SSID) ή το όνομα του δικτύου, ενώ στο κάτω μέρος σημειώνονται στοιχεία που αφορούν στην ευρυζωνικότητα του δικτύου. Στο δεύτερο από τα παραπάνω σύμβολα, που γνωστοποιεί την ύπαρξη μη προσβάσιμου σε τρίτους ασύρματου δικτύου, σημειώνεται στο πάνω μέρος του συμβόλου στοιχεία του Service Set Identifier (SSID), ενώ στο κάτω μέρος αυτού δεν γίνεται καμία αναγραφή. Στο τρίτο από τα παραπάνω σύμβολα, που γνωστοποιεί την ύπαρξη σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένου στο Διαδίκτυο με WEP κρυπτογραφικό λογισμικό κώδικα, σημειώνονται στο πάνω αριστερό μέρος στοιχεία του Service Set Identifier (SSID), στο πάνω δεξιό μέρος στοιχεία επικοινωνίας για τη λήψη άδειας πρόσβασης στο εν λόγω δίκτυο, και στο κάτω μέρος στοιχεία που αφορούν στην ευρυζωνικότητα του δικτύου.

Οι παρακάτω φωτογραφικές απεικονίσεις είναι ενδεικτικές του συνήθους τρόπου χρήσης των Warchalking σημάνσεων.

Εικόνα 3.3

Εικόνα 3.4

3.2 Ασφάλεια των ασύρματων δικτύων και επικινδυνότητα διάρρηξης τους

Μετά την υιοθέτηση του 802.11 standard από το Institute of Electrical and Electronics Engineers (IEEE), το ενδιαφέρον των τεχνολόγων αναφορικά με την ασύρματη τεχνολογία δικτύωσης διερεύνησε διεξοδικά τις δυνατότητες διάρρηξης

της ασφάλειας των ασύρματων συστημάτων, και κατά συνέπεια, την επικινδυνότητα των εν λόγω συστημάτων σχετικά με την προστασία της ιδιωτικότητας. Από νωρίς διαπιστώθηκε ότι το 802.11 standard που χρησιμοποιείται στα ασύρματα δίκτυα τύπου Wi-Fi εμπεριέχει το τεχνολογικό πρωτόκολλο WEP (Wireless Equivalent Protocol), το οποίο, όμως, υστερεί στο ζήτημα της θωράκισης της ασφάλειας των

ασύρματων συστημάτων δικτύωσης. Ειδικότερα, στο ζήτημα της διασφάλισης της ελεγχόμενης πρόσβασης ή αυθεντικοποίησης (authentication), δηλαδή αναφορικά με τις αυτοματοποιημένες

και τυποποιημένες μεθόδους για την πιστοποίηση της ταυτότητας του χρήστη στο ασύρματο δίκτυο, το 802.11 standard που χρησιμοποιείται στα ασύρματα δίκτυα τύπου Wi-Fi επιτρέπει την επαλήθευση ταυτότητας με δύο τρόπους:

(α) open-system authentication

(β) shared-key authentication.

Open-system authentication

Δεν συνιστά στην πραγματικότητα έλεγχο πρόσβασης. Το ασύρματο σημείο πρόσβασης (Access Point, ή AP) εντοπίζει και αποδέχεται τη συσκευή ασύρματης δικτύωσης χωρίς να επιβεβαιώνει την ταυτότητα της συσκευής αυτής. Ο εντοπισμός και η αποδοχή της συσκευής ασύρματης δικτύωσης γίνεται από το AP. Το AP αναζητά τη MAC διεύθυνση της συσκευής ασύρματης δικτύωσης την οποία η συσκευή αυτή, π.χ. ένας φορητός ηλεκτρονικός υπολογιστής, μεταβιβάζει προς το AP. Η επικοινωνία αυτή μεταξύ AP και φορητού η/υ γίνεται χωρίς καμία κρυπτογράφηση. Κατά συνέπεια, το open-system authentication δεν προσφέρει καμία ουσιαστική διασφάλιση της ελεγχόμενης πρόσβασης στο ασύρματο δίκτυο.

Shared-key authentication

Είναι μια τεχνική επικοινωνίας μεταξύ AP και συσκευής ασύρματης δικτύωσης που κάνει χρήσης κρυπτογράφησης. Στο shared-key authentication, το AP εκπέμπει κρυπτογραφημένο μήνυμα προς οποιαδήποτε συσκευή ασύρματης δικτύωσης βρίσκεται εντός της εμβέλειάς του. Ωστόσο, η κρυπτογραφημένη επικοινωνία του AP προς τη συσκευή ασύρματης δικτύωσης δεν εξασφαλίζει αμοιβαίο έλεγχο της πρόσβασης στο ασύρματο δίκτυο (mutual authentication). Δηλαδή, η συσκευή ασύρματης δικτύωσης δεν ελέγχει το AP, και κατά συνέπεια, δεν διασφαλίζεται ότι η

πρόσβαση στο ασύρματο δίκτυο γίνεται από ελεγχόμενο σημείο πρόσβασης (AP). Επιπλέον, η κρυπτογραφημένη επικοινωνία του AP με την συσκευή ασύρματης δικτύωσης είναι στοιχειώδης (rudimentary) και όχι προηγμένη (advanced), με αποτέλεσμα, ο τρόπος του shared-key authentication να υστερεί στο ζήτημα της θωράκισης της ασφάλειας των ασύρματων συστημάτων.

Confidentiality

Στο ζήτημα της διασφάλισης της εμπιστευτικότητας (confidentiality), δηλαδή αναφορικά με τη διαδικασία ασφάλειας με την οποία αποτρέπεται η διάθεση ή η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα, οντότητες ή διεργασίες το ασύρματο δίκτυο, το 802.11 standard που χρησιμοποιείται στα ασύρματα δίκτυα τύπου Wi-Fi επέτρεπε αρχικά τη λειτουργία κρυπτογράφησης στο πρωτόκολλο WEP με χρήση μόνο 40-bit κλείδων κρυπτογράφησης. Το μέγεθος των 40-bit κλείδων αποδείχθηκε ανεπαρκές για τη διασφάλιση της εμπιστευτικότητας. Θεωρητικά, η διασφάλιση της εμπιστευτικότητας μπορεί να επιτευχθεί με κρυπτογράφηση τουλάχιστον 80-bit κλείδων.

Integrity

Στο ζήτημα της διασφάλισης της ακεραιότητας των πληροφοριών (integrity) στο ασύρματο δίκτυο, το 802.11 standard που χρησιμοποιείται στα ασύρματα δίκτυα τύπου Wi-Fi επέτρεπε αρχικά τη λειτουργία κρυπτογράφησης στο πρωτόκολλο WEP με την τεχνική Cyclic Rudimentary Check (CRC) η οποία, όμως, αποδείχθηκε ανεπαρκής ή τουλάχιστον υποδεέστερη από την κρυπτογραφική τεχνική hash για τη διασφάλιση της ακεραιότητας των πληροφοριών. Τα πολλαπλά και εγνωσμένα προβλήματα ασφάλειας του WEP και η συνεχής προσπάθεια επίλυσης τους οδήγησαν στη διαμόρφωση του νέου πρωτόκολλου TKIP (Temporal Key Integrity Protocol) που αρχικά έγινε γνωστό και ως πρωτόκολλο WEP2. Το TKIP διαμορφώθηκε ως μια προσωρινή λύση για την επίλυση ενός βασικού προβλήματος του WEP, δηλαδή της χρησιμοποίησης περιοδικά του ίδιου κλειδιού κρυπτογράφησης στοιχείων και λειτούργησε σε συνδυασμό με το πρωτόκολλο WPA που αναπτύχθηκε με σκοπό την επίλυση των προβλημάτων ασφάλειας του WEP. Ακολούθησαν προσπάθειες

περαιτέρω ενίσχυσης της ασφάλειας των ασύρματων δικτύων οι οποίες οδήγησαν στη διαμόρφωση του νέου πρωτοκόλλου WPA2 (Wi-Fi Protected Access 2) που βασίζεται στο 802.11i standard του IEEE και χρησιμοποιεί την προηγμένη τεχνική κρυπτογράφησης AES (Advanced Encryption Standard) η οποία είναι συμβατή με τις προδιαγραφές ασφαλείας FIPS (Federal Information Processing Standards) 140-2 του National Institute of Standards & Technology (NIST) των Η.Π.Α. Το πρωτόκολλο WPA2 λειτουργεί σε ασύρματη τεχνολογία δικτύωσης είτε αυτή χρησιμοποιείται σε επιχειρησιακό περιβάλλον (WPA2 Enterprise) είτε σε επίπεδο απλού οικιακού χρήστη (WPA2 Personal). Πολλά από τα προβλήματα ασφάλειας του WEP λύθηκαν ικανοποιητικά με το νέο πρωτόκολλο ασφαλείας WPA2. Ωστόσο, στο ζήτημα της θωράκισης της ασφάλειας των ασύρματων συστημάτων δικτύωσης υπάρχει μεγάλο περιθώριο ανάπτυξης νέων ή βελτίωσης των υπαρχόντων πρωτοκόλλων. Το hacking των ασύρματων δικτύων εξακολουθεί να υφίσταται ως αγαπημένη ενασχόληση των απανταχού hackers.

3.3 Επιθέσεις κατά των ασύρματων δικτύων

Σε γενικές γραμμές, οι δυνατές επιθέσεις hacking κατά των ασύρματων συστημάτων ταξινομούνται σε:

(α) Παθητικές (passive attacks)

(β) Ενεργητικές (active attacks).

Οι **παθητικές επιθέσεις** είναι επιθέσεις στις οποίες ο δράστης αποκτά πρόσβαση στο ασύρματο δίκτυο χωρίς, όμως, ν' αλλάζει κάτι σ' αυτό ή στα πληροφοριακά δεδομένα που διακινούνται σ' αυτό. Αντίθετα, στις **ενεργητικές επιθέσεις**, ο δράστης προβαίνει σε αλλοιώσεις είτε του ασύρματου δικτύου είτε των πληροφοριακών δεδομένων που διακινούνται σ' αυτό.

Πέραν αυτής της γενικής διάκρισης των επιθέσεων, ειδικότερες μορφές hacking κατά ασυρμάτων δικτύων μπορεί να είναι:

- το Eavesdropping ή Wireless Network Sniffing
- Traffic Analysis
- Passive Scanning
- Masquerading
- Replay
- Message Modification
- Denial-of-Service
- Wireless Spoofing
- MAC Address Spoofing
- IP Spoofing
- Frame Spoofing
- Wireless Network Probing
- Detection of SSID
- Detection of APs
- Wireless Man-In-The-Middle (MITM) επιθέσεις
- Session Hijacking επιθέσεις κλπ.

Το **Eavesdropping ή Wireless Network Sniffing** είναι μέθοδος παρακολούθησης και υποκλοπής του περιεχομένου επικοινωνίας που μεταδίδεται μέσω ασύρματων δικτύων. Για τη μέθοδο αυτή χρησιμοποιείται το Sniffer, δηλαδή λογισμικό πρόγραμμα που διεισδύει και αποκωδικοποιεί μεταδιδόμενο περιεχόμενο μέσω ασύρματων δικτύων. Το Sniffer δημιουργεί σ' έναν ηλεκτρονικό υπολογιστή του δράστη αντίγραφα του μεταδιδόμενου περιεχομένου από έναν ηλεκτρονικό υπολογιστή *A* σ' έναν υπολογιστή *B* του θύματος. Η μέθοδος του Sniffing συχνά χρησιμοποιείται για να διαπιστωθεί ο βαθμός της υφιστάμενης επικινδυνότητας για τη διάρρηξη της ασφάλειας ενός δικτύου υπολογιστικών συστημάτων. Το Eavesdropping ή Wireless Network Sniffing χρησιμοποιείται κυρίως για τον εντοπισμό των ανοικτών σημείων πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένο στο Διαδίκτυο ή για τον προσδιορισμό στοιχείων ελεγχόμενης πρόσβασης, π.χ. τα Passwords, που χρησιμοποιούνται σε σύνδεση με το ασύρματο

δίκτυο που ενδεχομένως είναι διαφορετική από προσβάσεις στο δίκτυο μέσω συνδέσεων τύπου WEP, telnet, FTP, rlogin.

Με το **Traffic Analysis** ο δράστης αποκτά γνώση για τον τρόπο λειτουργίας και διακίνησης του περιεχομένου ενός ασύρματου δικτύου. Η γνώση αυτή μπορεί να χρησιμοποιηθεί από τον δράστη για περαιτέρω επιθέσεις κατά του παρακολουθούμενου ασύρματου δικτύου.

Το **Passive Scanning** είναι μια μέθοδος Sniffing. Ο δράστης του Passive Scanning χρησιμοποιεί μια κάρτα ασύρματης δικτυακής πρόσβασης (hardware) για να συντονιστεί στις ραδιοσυχνότητες μεταξύ 2.4 GHz και 2.5 GHz τις οποίες χρησιμοποιούν τ' ασύρματα σημεία πρόσβασης. Ο συντονισμός του Passive Scanner στις εν λόγω ραδιοσυχνότητες μπορεί να γίνει χωρίς καμία αναγνώριση του δράστη από το δίκτυο. Αυτό μπορεί να συμβεί με χρήση μίας κάρτας ασύρματης διαδικτυακής πρόσβασης που επιτρέπει τη ρύθμιση της λειτουργίας της σε RF monitor mode. Με το Passive Scanning μπορεί να εντοπιστεί και το SSID, δηλαδή το Service Set Identifier. Το SSID εμφανίζεται στα Beacon frames65 που μεταδίδουν τα ασύρματα σημεία πρόσβασης, εφόσον η λειτουργία των Beacon frames δεν έχει απενεργοποιηθεί ή δεν έχει προηγηθεί κατάλληλη ρύθμιση απόκρυψης των SIDs.

Με το **Masquerading** ο δράστης «μεταμφιέζεται» σε νόμιμο χρήστη του ασύρματου δικτύου, έχοντας ενδεχομένως κλέψει τα χαρακτηριστικά του νόμιμου χρήστη με διάπραξη παθητικής επίθεσης κατά του ασύρματου δικτύου. Ο συνήθης λόγος για τον οποίο ένας δράστης εμφανίζεται μεταμφιεσμένος σαν νόμιμος χρήστης είναι για να κάνει χρήση των προνομίων που μπορεί να έχει ο νόμιμος χρήστης στο ασύρματο δίκτυο.

Με το **Replay** ο δράστης αναμεταδίδει στο ασύρματο δίκτυο μηνύματα σαν να ήταν νόμιμος χρήστης αυτού.

Με το **Message Modification** ο δράστης προβαίνει σε πράξεις αλλοίωσης των μεταδιδόμενων μηνυμάτων μέσω του ασύρματου δικτύου.

Με το **Denial-of-Service** ο δράστης προκαλεί την αδυναμία εύρυθμης λειτουργίας του ασύρματου τηλεπικοινωνιακού δικτύου. Με hacking σε ασύρματο δίκτυο μπορεί να γίνει πλαστογράφηση των Media Access Control (MAC) Addresses. Η πλαστογράφηση αυτή συνήθως γίνεται από τον δράστη που επιδιώκει να παραπλανά ή να παραμένει απαρατήρητος κάθε φορά που προβαίνει σε παράνομη χρήση ασύρματου τηλεπικοινωνιακού δικτύου τρίτων. Επίσης, ο δράστης μπορεί να προβεί για τους ίδιους λόγους και σε η πλαστογράφηση των **Internet Protocol (IP) Addresses** ή και σε **Frame Spoofing** με τη βοήθεια πληροφοριακών δεδομένων του στοχοποιημένου ασύρματου δικτύου πρόσβασης τρίτων, τα οποία έχει συλλέξει ο δράστης με μεθόδους **Sniffing** και έχει ενδεχομένως συνδυάσει με άλλα δεδομένα που έχει βρει.

Το **Wireless Network Probing**, γνωστό και ως **Active Scanning**, αφορά σε διαδραστική μέθοδο hacking ασύρματων δικτύων. Με τη μέθοδο αυτή ο δράστης αποστέλλει μη γνήσια πληροφοριακά δεδομένα στο στοχοποιημένο ασύρματο δίκτυο επιδιώκοντας τη διαδραστική επικοινωνία του με το δίκτυο αυτό, με απώτερο σκοπό ν' αντλήσει πληροφοριακά δεδομένα περί του εν λόγω δικτύου που ενδεχομένως δεν έχει καταφέρει να συγκεντρώσει με ενέργειές του τύπου Passive Scanning.

Στις **Wireless Man-In-The-Middle (MITM)** επιθέσεις, ο δράστης διεισδύει μεταξύ δύο επικοινωνούντων σημείων ασύρματης πρόσβασης (AP) ενός δικτύου εξαναγκάζοντας καθένα από αυτά να εξουσιοδοτήσει και πιστοποιηθεί με το σημείο ή συσκευή ασύρματης πρόσβασης του δράστη. Έτσι, το περιεχόμενο της επικοινωνίας των δύο σημείων ασύρματης πρόσβασης στο δίκτυο κατευθύνεται από τον αποστολέα στον λήπτη μέσω του ασύρματου σημείου ή συσκευής πρόσβασης του δράστη, ο οποίος φυσικά υποκλέπτει πλήρως το περιεχόμενο της επικοινωνίας. Για την

αυτοματοποίηση της ασύρματης MITM επίθεσης, κυκλοφορεί στην αγορά, ήδη από το 2003, κατάλληλο hardware και Linux-based software, το λεγόμενο AirJack, καθώς και άλλα προϊόντα όπως το AirSnort, το WEPcrack, το Aerosol.

Στις **Session Hijacking** επιθέσεις, ο δράστης προκαλεί στιγμιαία, ή τουλάχιστον προσωρινή, απώλεια σύνδεσης ενός χρήστη με τον διακομιστή του δικτύου στο οποίο είναι συνδεδεμένος. Κατά τη διάρκεια της διακοπής, ο δράστης ιδιοποιείται παράνομα την ταυτότητα του χρήστη για να επιτύχει τη σύνδεσή του με τον διακομιστή του δικτύου με τα προνόμια που είχε ο χρήστης. Αφού, ο δράστης, εμφανιζόμενος με την ταυτότητα του νόμιμου χρήστη, αντλήσει από τον διακομιστή του δικτύου τα πληροφοριακά δεδομένα που τον ενδιαφέρουν, επαναφέρει τον νόμιμο χρήστη σε σύνδεση με τον διακομιστή, συνήθως χωρίς ο χρήστης ν' αντιληφθεί την πραγματική αιτία της προσωρινής διακοπής της σύνδεσής του. Οι διαγνωσθείσες ελλείψεις στο ζήτημα της θωράκισης της ασφάλειας των ασύρματων συστημάτων και η συστηματική έρευνα, καταγραφή και ταξινόμηση των δυνατών επιθέσεων hacking κατά των εν λόγω συστημάτων οδήγησε στη λήψη πρόσθετων τεχνολογικών μέτρων, αλλά και στη χάραξη πολιτικής ασφαλείας (συνήθως αποκαλούμενη «Wireless Local Area Network» ή WLAN πολιτική ασφαλείας) για τη διασφάλιση των ασύρματων συστημάτων από οποιοδήποτε είδος hacking κατ' αυτών.

Ειδικότερα, η WLAN πολιτική ασφαλείας, στα πλαίσια του εργασιακού περιβάλλοντος ενός φορέα, π.χ. μίας εταιρίας, μπορεί να προβλέπει και ρυθμίζει πληθώρα ζητημάτων όπως:

1. Τον προσδιορισμό των προσώπων που νομιμοποιούνται να χρησιμοποιούν τεχνολογία ασύρματης δικτύωσης εντός του εργασιακού περιβάλλοντος του φορέα στον οποίο ανήκουν.

2. Την επιτρεπόμενη ή απαγορευμένη χρήση τεχνολογίας ασύρματης δικτύωσης για την πρόσβαση στο Διαδίκτυο.

3. Τον προσδιορισμό των προσώπων που έχουν την αποκλειστική αρμοδιότητα για την εγκατάσταση σημείων πρόσβασης (AP) και εν γένει κάθε τεχνολογίας ασύρματης δικτύωσης.

4. Τους χωροταξικούς ή άλλους περιορισμούς που αφορούν στην εγκατάσταση σημείων πρόσβασης (AP) ή άλλης τεχνολογίας ασύρματης δικτύωσης.

5. Το είδος των πληροφοριακών δεδομένων που επιτρέπεται ή απαγορεύεται να διακινηθούν μέσω ασύρματου δικτύου.

6. Τις προϋποθέσεις υπό τις οποίες επιτρέπεται η χρήση ασύρματων συσκευών εντός του εργασιακού περιβάλλοντος της εταιρίας.

7. Τον προσδιορισμό των standard security settings για τα ασύρματα σημεία πρόσβασης (APs).

8. Τον προσδιορισμό του hardware και software configuration για όλες τις ασύρματες συσκευές.

9. Τον προσδιορισμό λεπτομερών οδηγιών και διαδικασιών για την αναφορά κλοπής ασύρματων συσκευών.

10. Τον προσδιορισμό οδηγιών για τη χρήση κρυπτογράφησης ή άλλων τεχνικών ασφαλείας.

11. Τον προσδιορισμό περιοδικών ασκήσεων ελέγχου της ασφάλειας του ασύρματου δικτύου της εταιρίας.

Εκτός, όμως, από την WLAN πολιτική ασφάλειας και την οποιαδήποτε άλλη κωδικοποίηση ή θέσπιση ρυθμιστικού πλαισίου υπό μορφή εσωτερικού κανονισμού για την αυτορρύθμιση της ασφάλειας των ασύρματων συστημάτων (soft law), που κερδίζει όλο και περισσότερο έδαφος στην καθημερινή πρακτική χρήσης τεχνολογιών

της πληροφορικής επιστήμης,77 υπάρχει στην Ελλάδα εν ισχύ νομοθετικό πλαίσιο (hard law) που ρυθμίζει ζητήματα σχετικά με την προστασία της ιδιωτικότητας αφενός και τον ποινικό και αστικό κολασμό πράξεων hacking αφετέρου.

3.4 Εργαλεία για Wardriving

Αυτή η ενότητα θα σας παρουσιάσει όλα τα εργαλεία που χρειάζονται για την επίτευξή του WarDrive. Υπάρχουν πολλά διαφορετικά configurations που μπορούν αποτελεσματικά να χρησιμοποιηθούν για WarDriving, τα οποία έχουν να κάνουν με:

(α) Το hardware

(β) Την wireless network κάρτα

(γ) Την επιλογή μιας εξωτερικής κεραίας και την σύνδεση της κεραίας στο wireless NIC

(α) Hardware

1. Laptop
2. PDA

1. Laptop

Ένα επιτυχημένο laptop WarDriving setup περιλαμβάνει:

- Ένα laptop computer
- Μία wireless NIC κάρτα
- Μία εξωτερική κεραία
- Ένα pigtail για να συνδεθεί η εξωτερική κεραία με την wireless NIC
- Ένα handheld global positioning system (GPS) unit
- Ένα GPS data cable
- Ένα WarDriving software program

- Έναν cigarette lighter or AC adapter power inverter

Εάν χρησιμοποιηθεί laptop πρέπει να καθοριστεί το WarDriving software που πρόκειται να χρησιμοποιηθεί. Σε περίπτωση που χρησιμοποιήσουμε ως operating system το Linux, πρέπει να γίνει χρήση του Kismet (το οποίο τρέχει σε Linux), αλλιώς αν ως operating system είναι το Microsoft Windows, πρέπει να γίνει χρήση του NetStumbler, το οποίο είναι συμβατό με το περιβάλλον Microsoft Windows. Γενικά η επιλογή του software που θα χρησιμοποιηθεί, είναι περιορισμένη.

2. The Personal Digital Assistant (PDA)

Τα PDAs είναι το ιδανικό αξεσουάρ για έναν WarDriver επειδή είναι "highly portable".Το Compaq iPAQ, ή όποιο άλλο PDA, το οποίο έχει ARM, MIPS, ή SH3 επεξεργαστή, μπορεί να χρησιμοποιήσει κοινά WarDriving software packages.

Όπως και με το laptop, το PDA απαιτεί επιπρόσθετο εξοπλισμό:

- Ένα PDA με ένα data cable
- Μία wireless NIC κάρτα
- Μία εξωτερική κεραία
- Ένα pigtail για να συνδεθεί η εξωτερική κεραία με το wireless NIC
- Ένα handheld global positioning system (GPS) unit
- Ένα GPS data cable
- Ένα null modem connector
- Ένα WarDriving software program

Παρόμοια με το laptop configuration, το software package που θα επιλεχθεί θα παίξει ρόλο στην επιλογή του PDA. Το MiniStumbler, είναι το PDA version του NetStumbler, δουλεύει σε PDAs τα οποία λειτουργούν το Microsoft Pocket PC operating system.Το HP/Compaq iPAQ είναι ένα από τα πιο δημοφιλή PDA στους WarDrivers που προτιμούν το MiniStumbler.Οι WarDrivers οι οποίοι επιλέγουν να

χρησιμοποιούν το Kismet επιλέγουν το PDA Sharp Zaurus, το οποίο τρέχει μία PDA version του Linux.Υπάρχουν επίσης Kismet packages τα οποία έχουν σχεδιαστεί για το Zaurus.

(β)Επιλογή της Wireless Network Interface κάρτας

Όταν το Kismet και το NetStumbler πρωτοεμφανιστήκαν, υπήρχαν μόνο δύο βασικά chipsets διαθέσιμα σε wireless NICs:

- Το Hermes chipset
- Και το Prism2 chipset.

Αν και τώρα υπάρχουν πολλά άλλα chipsets διαθέσιμα, τα περισσότερα WarDriving software σχεδιάζονται προκειμένου να χρησιμοποιούν μόνο αυτά τα δύο. Συγκεκριμένα το NetStumbler δουλεύει με κάρτες που βασίζονται στο Hermes chipset, ενώ το Kismet, με κάρτες που βασίζονται στο Prism2 chipset.

Για να γίνει εφικτό το WarDrive, χρειάζεται ένα wireless NIC. Προτού γίνει η αγορά της wireless κάρτας, πρέπει να καθοριστεί το software και το configuration το οποίο σκοπεύουμε να χρησιμοποιήσουμε. Το NetStumbler προσφέρει το ευκολότερο configuration για κάρτες που βασίζονται στο Hermes chipset. Το Kismet είναι συμβατό και με Prism2- και με Hermes-based κάρτες. Παρόλα αυτά οι περισσότερες Linux και BSD distributions απαιτούν αλλαγές στον kernel καθώς και κάποια driver patch προκειμένου κάποιες Hermes-based κάρτες να λειτουργήσουν με το Kismet.

(γ)Εξωτερικές Κεραίες

Προκειμένου να μεγιστοποιηθούν τα αποτελέσματα του WarDrive, μία εξωτερική κεραία πρέπει να χρησιμοποιηθεί. Η κεραία είναι η συσκευή για την εκπομπή ή λήψη ραδιοκυμάτων. Οι περισσότερες wireless network κάρτες έχουν μια "low power"

κεραία μέσα τους. Μία εξωτερική κεραία θα αυξήσει το εύρος του ραδιοσήματος το οποίο ανιχνεύεται από την wireless network κάρτα.

Πολλά διαφορετικά είδη κεραιών μπορούν να χρησιμοποιηθούν με τα wireless NICs:

(α) Parabolic antennas (παραβολικές)

(β) Directional antennas (κατευθυντικές)

(γ) Omni-directional antennas (παγκατευθυντικές)

4 Χαρτογράφηση ασύρματων δικτύων

4.1 Ο εξοπλισμός που χρησιμοποιήθηκε

Hardware

Τεχνικά Χαρακτηριστικά

- Acer Aspire 5630
- PC Notebook Intel Core 2 Duo Mobile T5200, 1.60GHz
- 2048MB RAM
- 120GB HD
- Λειτουργικό Microsoft Windows XP SP2
- Ασύρματη κάρτα την 3Com 11a/b/g Wireless PC Card με XJACK Antenna 3CRPAG175

Εικόνα 4.1 Acer Aspire 5630

WiFi Card

3Com 11a/b/g Wireless PC Card με XJACK Antenna 3CRPAG175

Εικόνα 4.2 Η ασύρματη κάρτα που χρησιμοποιήθηκε

Τεχνικά Χαρακτηριστικά

- **Πρότυπο**: IEEE 802.11b (11 Mbps) / IEEE 802.11g (54 Mbps)
- **Τοποθέτηση**: Type II ή Type III 32-bit ή PC Card (PCMCIA)
- **Ασφάλεια**: WEP (40/64, 128 και 154-bit), 802.1x, WPA, AES 128-bit, EAP-MD5/EAP-TLS/PEAP, MD5
- **Εμβέλεια**: Έως 100m (σε εσωτερικό χώρο), έως 300m (σε εξωτερικό χώρο)
- **Τύπος Κεραίας**: XJACK
- **Άλλα Χαρακτηριστικά**: Ρυθμός μεταφοράς δεδομένων: 802.11b: 11, 5.5, 2 και 1Mbps / 802.11g: 54, 48, 36, 24, 18, 12, 9 και 6Mbps

Software

NetStumbler 0.4.0

Το NetStumbler (γνωστό και ως Network Stumbler) είναι ένα εργαλείο για Windows που εντοπίζει και αναλύει ασύρματα δίκτυα που κάνουν χρήση των πρωτοκόλλων 802.11b, 802.11a και 802.11g.

Χρήση του NetStumbler:

* Verifying network configurations
* Finding locations with poor coverage in one’s WLAN
* Detecting causes of wireless interference
* Detecting unauthorized (”rogue”) access points
* Aiming directional antennas for long-haul WLAN links

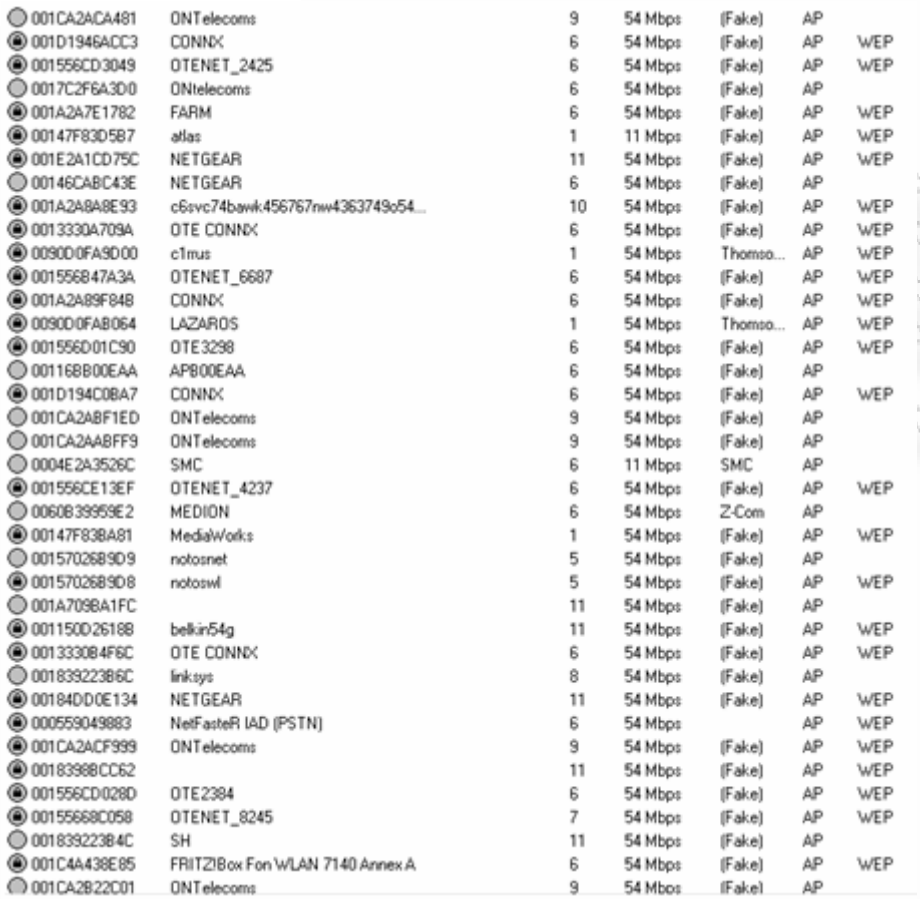
4.2 Χαρτογράφηση ασύρματων δικτύων

4.2.1 Προσωπική έρευνα ασύρματων δικτύων στην περιοχή του Πειραιά

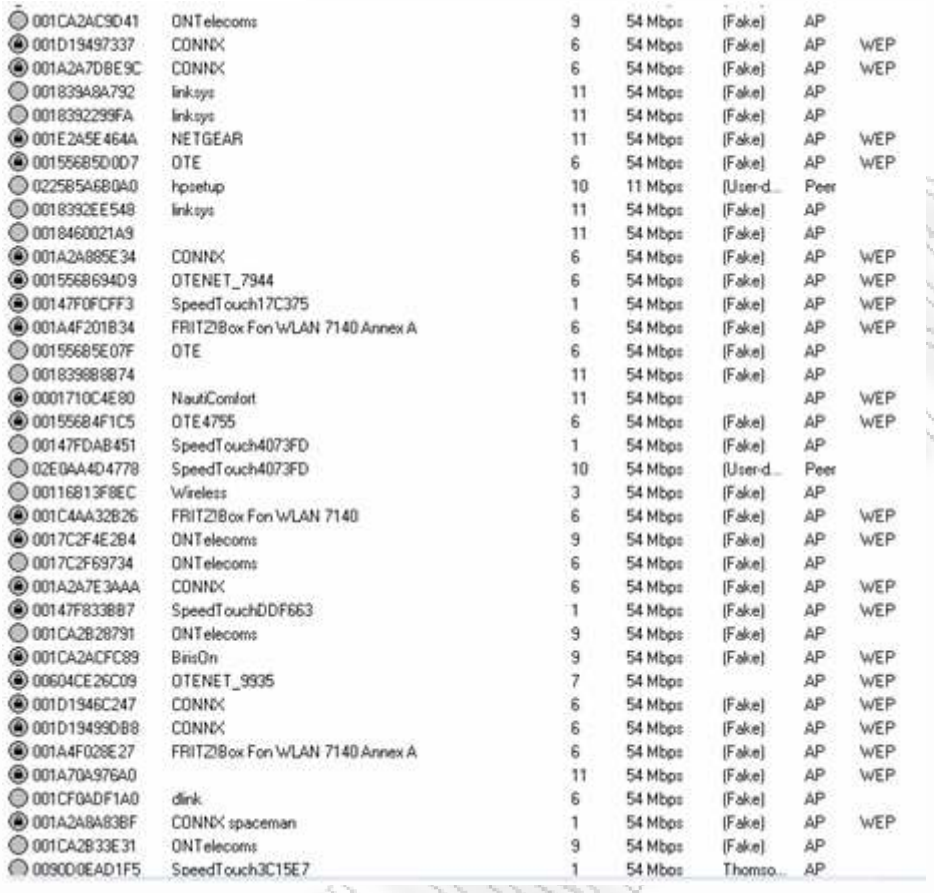
Εικόνα 4.3 Περιοχή Πειραιά

4.2.1.1 Συγκέντρωση αποτελεσμάτων

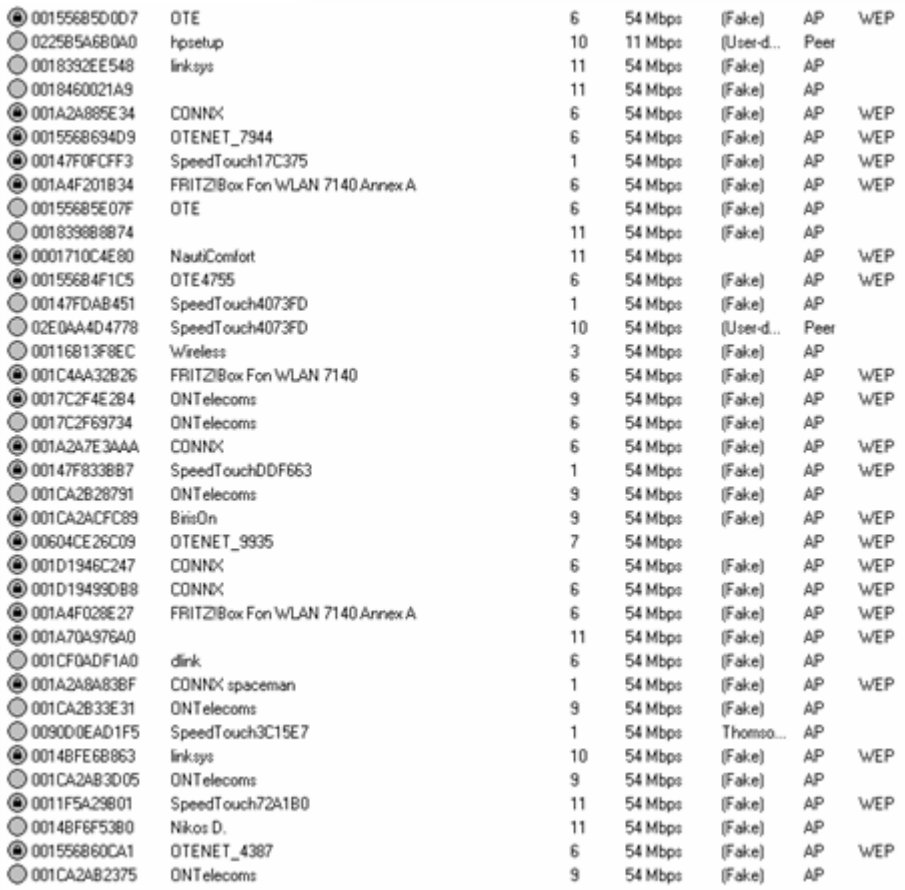
001556B68504	OTENET_6735	6	54 Mbps	(Fake)	AP	WEP
001CA2ACA56D	ONTelecoms	9	54 Mbps	(Fake)	AP	
001A709D3518	linksys	11	54 Mbps	(Fake)	AP	WEP
0080C8AC714A	johnhack	6	22 Mbps	D-Link	AP	WEP
001CA2B23A7D	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
001CA2AB5F79	ONTelecoms	9	54 Mbps	(Fake)	AP	
001A2A8A10FC	CONNX	6	54 Mbps	(Fake)	AP	WEP
001D197072C7	CONNX	6	54 Mbps	(Fake)	AP	WEP
0015568754CA	OTENET_2776	6	54 Mbps	(Fake)	AP	WEP
001556D003E2	OTE4498	6	54 Mbps	(Fake)	AP	WEP
001CA2ACA31D	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
001556685CCE	OTENET_2832	7	54 Mbps	(Fake)	AP	WEP
001D19469C5E	CONNX	6	54 Mbps	(Fake)	AP	WEP
001D1949AA24	CONNX	6	54 Mbps	(Fake)	AP	WEP
00147F6A92A5	SpeedTouch84BF9A	1	54 Mbps	(Fake)	AP	
001CA2AB4E3D	ONTelecoms	9	54 Mbps	(Fake)	AP	
00186E081C7B	3Com	11	54 Mbps	(Fake)	AP	
001556CDA07E	OTE5873	6	54 Mbps	(Fake)	AP	WEP
001A2A88977C	CONNX	6	54 Mbps	(Fake)	AP	WEP
0013330A77DC	OTE CONNX	6	54 Mbps	(Fake)	AP	WEP
0090D0F6510C	SpeedTouchCFCBFB	1	54 Mbps	Thomso...	AP	WEP
001B2FF2BF2C	NETGEAR	11	54 Mbps	(Fake)	AP	
00193EE88D39	goal	11	54 Mbps	(Fake)	AP	WEP
001556CDCC01	OTE6958	6	54 Mbps	(Fake)	AP	WEP
001556CDAC81	OTE3993	6	54 Mbps	(Fake)	AP	WEP
0013330A7C2A	home	6	54 Mbps	(Fake)	AP	WEP
001A68EAECBF	Livebox-1618	10	54 Mbps	(Fake)	AP	WEP
001333068706	OTE CONNX	6	54 Mbps	(Fake)	AP	WEP
0019DB91B56A	wlan-ap	1	54 Mbps	(Fake)	AP	
001CA2AB60A9	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
001CA2ABEC71	ONTelecoms	9	54 Mbps	(Fake)	AP	
001CA2ABE4E9	ONTelecoms	9	54 Mbps	(Fake)	AP	
001B113FD856	VigoRulez	6	54 Mbps	(Fake)	AP	WEP
001CA2AC535D	ONTelecoms	9	54 Mbps	(Fake)	AP	
0002611184D2	Tilgin-tAD452W	11	54 Mbps		AP	
0090D0FA3619	SpeedTouchA6A3C8	1	54 Mbps	Thomso...	AP	
001D1949DBA1	CONNX	6	54 Mbps	(Fake)	AP	WEP
00133307D6E6	OTE CONNX	6	54 Mbps	(Fake)	AP	WEP



001CA2ACA481	ONTelecoms	9	54 Mbps	(Fake)	AP	
001D1946ACC3	CONNX	6	54 Mbps	(Fake)	AP	WEP
001556CD3049	OTENET_2425	6	54 Mbps	(Fake)	AP	WEP
0017C2F6A3D0	ONtelecoms	6	54 Mbps	(Fake)	AP	
001A2A7E1782	FARM	6	54 Mbps	(Fake)	AP	WEP
00147F83D5B7	atlas	1	11 Mbps	(Fake)	AP	WEP
001E2A1CD75C	NETGEAR	11	54 Mbps	(Fake)	AP	WEP
00146CABC43E	NETGEAR	6	54 Mbps	(Fake)	AP	
001A2A8A8E93	c6svc74bawk456767nw4363749c54...	10	54 Mbps	(Fake)	AP	WEP
0013330A709A	OTE CONNX	6	54 Mbps	(Fake)	AP	WEP
0090D0FA9D00	c1rrus	1	54 Mbps	Thomso...	AP	WEP
001556847A3A	OTENET_6687	6	54 Mbps	(Fake)	AP	WEP
001A2A89F84B	CONNX	6	54 Mbps	(Fake)	AP	WEP
0090D0FAB064	LAZAROS	1	54 Mbps	Thomso...	AP	WEP
001556D01C90	OTE3298	6	54 Mbps	(Fake)	AP	WEP
00116BB00EAA	APB00EAA	6	54 Mbps	(Fake)	AP	
001D194C0BA7	CONNX	6	54 Mbps	(Fake)	AP	WEP
001CA2ABF1ED	ONTelecoms	9	54 Mbps	(Fake)	AP	
001CA2AABFF9	ONTelecoms	9	54 Mbps	(Fake)	AP	
0004E2A3526C	SMC	6	11 Mbps	SMC	AP	
001556CE13EF	OTENET_4237	6	54 Mbps	(Fake)	AP	WEP
0060B39959E2	MEDION	6	54 Mbps	Z-Com	AP	
00147F83BA81	MediaWorks	1	54 Mbps	(Fake)	AP	WEP
00157026B9D9	notosnet	5	54 Mbps	(Fake)	AP	
00157026B9D8	notoswl	5	54 Mbps	(Fake)	AP	WEP
001A709BA1FC		11	54 Mbps	(Fake)	AP	
001150D2618B	belkin54g	11	54 Mbps	(Fake)	AP	WEP
0013330B4F6C	OTE CONNX	6	54 Mbps	(Fake)	AP	WEP
0018392236C	linksys	8	54 Mbps	(Fake)	AP	
00184DD0E134	NETGEAR	11	54 Mbps	(Fake)	AP	WEP
000559049883	NetFasteR IAD (PSTN)	6	54 Mbps		AP	WEP
001CA2ACF999	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
0018398BCC62		11	54 Mbps	(Fake)	AP	WEP
001556CD028D	OTE2384	6	54 Mbps	(Fake)	AP	WEP
00155668C058	OTENET_8245	7	54 Mbps	(Fake)	AP	WEP
0018392236AC	SH	11	54 Mbps	(Fake)	AP	
001C4A438E85	FRITZ!Box Fon WLAN 7140 Annex A	6	54 Mbps	(Fake)	AP	WEP
001CA2B22C01	ONTelecoms	9	54 Mbps	(Fake)	AP	



001CA2AC9D41	ONTelecoms	9	54 Mbps	(Fake)	AP	
001D19497337	CONNX	6	54 Mbps	(Fake)	AP	WEP
001A2A7DBE9C	CONNX	6	54 Mbps	(Fake)	AP	WEP
001839A8A792	linksys	11	54 Mbps	(Fake)	AP	
0018392299FA	linksys	11	54 Mbps	(Fake)	AP	
001E2A5E464A	NETGEAR	11	54 Mbps	(Fake)	AP	WEP
00155685D0D7	OTE	6	54 Mbps	(Fake)	AP	WEP
0225B5A6B0A0	hpsetup	10	11 Mbps	(User-d...	Peer	
0018392EE548	linksys	11	54 Mbps	(Fake)	AP	
0018460021A9		11	54 Mbps	(Fake)	AP	
001A2A885E34	CONNX	6	54 Mbps	(Fake)	AP	WEP
001556B694D9	OTENET_7944	6	54 Mbps	(Fake)	AP	WEP
00147F0FCFF3	SpeedTouch17C375	1	54 Mbps	(Fake)	AP	WEP
001A4F201B34	FRITZ!Box Fon WLAN 7140 Annex A	6	54 Mbps	(Fake)	AP	WEP
00155685E07F	OTE	6	54 Mbps	(Fake)	AP	
001839B89B74		11	54 Mbps	(Fake)	AP	
0001710C4E80	NautiComfort	11	54 Mbps		AP	WEP
00155684F1C5	OTE4755	6	54 Mbps	(Fake)	AP	WEP
00147FDAB451	SpeedTouch4073FD	1	54 Mbps	(Fake)	AP	
02E0AA4D4778	SpeedTouch4073FD	10	54 Mbps	(User-d...	Peer	
00116B13F8EC	Wireless	3	54 Mbps	(Fake)	AP	
001C4AA32B26	FRITZ!Box Fon WLAN 7140	6	54 Mbps	(Fake)	AP	WEP
0017C2F4E2B4	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
0017C2F69734	ONTelecoms	6	54 Mbps	(Fake)	AP	
001A2A7E3AAA	CONNX	6	54 Mbps	(Fake)	AP	WEP
00147F833B87	SpeedTouchDDF663	1	54 Mbps	(Fake)	AP	WEP
001CA2B28791	ONTelecoms	9	54 Mbps	(Fake)	AP	
001CA2ACFC89	BirisOn	9	54 Mbps	(Fake)	AP	WEP
00604CE26C09	OTENET_9935	7	54 Mbps		AP	WEP
001D1946C247	CONNX	6	54 Mbps	(Fake)	AP	WEP
001D19499D88	CONNX	6	54 Mbps	(Fake)	AP	WEP
001A4F028E27	FRITZ!Box Fon WLAN 7140 Annex A	6	54 Mbps	(Fake)	AP	WEP
001A70A976A0		11	54 Mbps	(Fake)	AP	WEP
001CF0ADF1A0	dlink	6	54 Mbps	(Fake)	AP	
001A2A8A83BF	CONNX spaceman	1	54 Mbps	(Fake)	AP	WEP
001CA2B33E31	ONTelecoms	9	54 Mbps	(Fake)	AP	
0090D0EAD1F5	SpeedTouch3C15E7	1	54 Mbps	Thomso...	AP	



00155685D0D7	OTE	6	54 Mbps	(Fake)	AP	WEP
0225B5A6B0A0	hpsetup	10	11 Mbps	(User-d...	Peer	
0018392EE548	linksys	11	54 Mbps	(Fake)	AP	
0018460021A9		11	54 Mbps	(Fake)	AP	
001A2A885E34	CONNX	6	54 Mbps	(Fake)	AP	WEP
0015568694D9	OTENET_7944	6	54 Mbps	(Fake)	AP	WEP
00147F0FCFF3	SpeedTouch17C375	1	54 Mbps	(Fake)	AP	WEP
001A4F201B34	FRITZ!Box Fon WLAN 7140 Annex A	6	54 Mbps	(Fake)	AP	WEP
00155685E07F	OTE	6	54 Mbps	(Fake)	AP	
0018396B8B74		11	54 Mbps	(Fake)	AP	
0001710C4E80	NautiComfort	11	54 Mbps		AP	WEP
00155684F1C5	OTE4755	6	54 Mbps	(Fake)	AP	WEP
00147FDAB451	SpeedTouch4073FD	1	54 Mbps	(Fake)	AP	
02E0AA4D4778	SpeedTouch4073FD	10	54 Mbps	(User-d...	Peer	
00116B13F8EC	Wireless	3	54 Mbps	(Fake)	AP	
001C4AA32B26	FRITZ!Box Fon WLAN 7140	6	54 Mbps	(Fake)	AP	WEP
0017C2F4E2B4	ONTelecoms	9	54 Mbps	(Fake)	AP	WEP
0017C2F69734	ONTelecoms	6	54 Mbps	(Fake)	AP	
001A2A7E3AAA	CONNX	6	54 Mbps	(Fake)	AP	WEP
00147F833BB7	SpeedTouchDDF663	1	54 Mbps	(Fake)	AP	WEP
001CA2B28791	ONTelecoms	9	54 Mbps	(Fake)	AP	
001CA2ACFC89	BirisOn	9	54 Mbps	(Fake)	AP	WEP
00604CE26C09	OTENET_9935	7	54 Mbps		AP	WEP
001D1946C247	CONNX	6	54 Mbps	(Fake)	AP	WEP
001D19499DB8	CONNX	6	54 Mbps	(Fake)	AP	WEP
001A4F028E27	FRITZ!Box Fon WLAN 7140 Annex A	6	54 Mbps	(Fake)	AP	WEP
001A70A976A0		11	54 Mbps	(Fake)	AP	WEP
001CF0ADF1A0	dlink	6	54 Mbps	(Fake)	AP	
001A2A8A83BF	CONNX spaceman	1	54 Mbps	(Fake)	AP	WEP
001CA2B33E31	ONTelecoms	9	54 Mbps	(Fake)	AP	
0090D0EAD1F5	SpeedTouch3C15E7	1	54 Mbps	Thomso...	AP	
0014BFE6B863	linksys	10	54 Mbps	(Fake)	AP	WEP
001CA2AB3D05	ONTelecoms	9	54 Mbps	(Fake)	AP	
0011F5A29B01	SpeedTouch72A1B0	11	54 Mbps	(Fake)	AP	WEP
0014BF6F53B0	Nikos D.	11	54 Mbps	(Fake)	AP	
001556860CA1	OTENET_4387	6	54 Mbps	(Fake)	AP	WEP
001CA2AB2375	ONTelecoms	9	54 Mbps	(Fake)	AP	

4.2.1.2 Στατιστική έρευνα αποτελεσμάτων

Έπειτα από ανάλυση των παραπάνω πληροφοριών, καταλήξαμε στα ακόλουθα αποτελέσματα.

Αριθμός συνολικών δικτύων που εντοπίστηκαν: 119

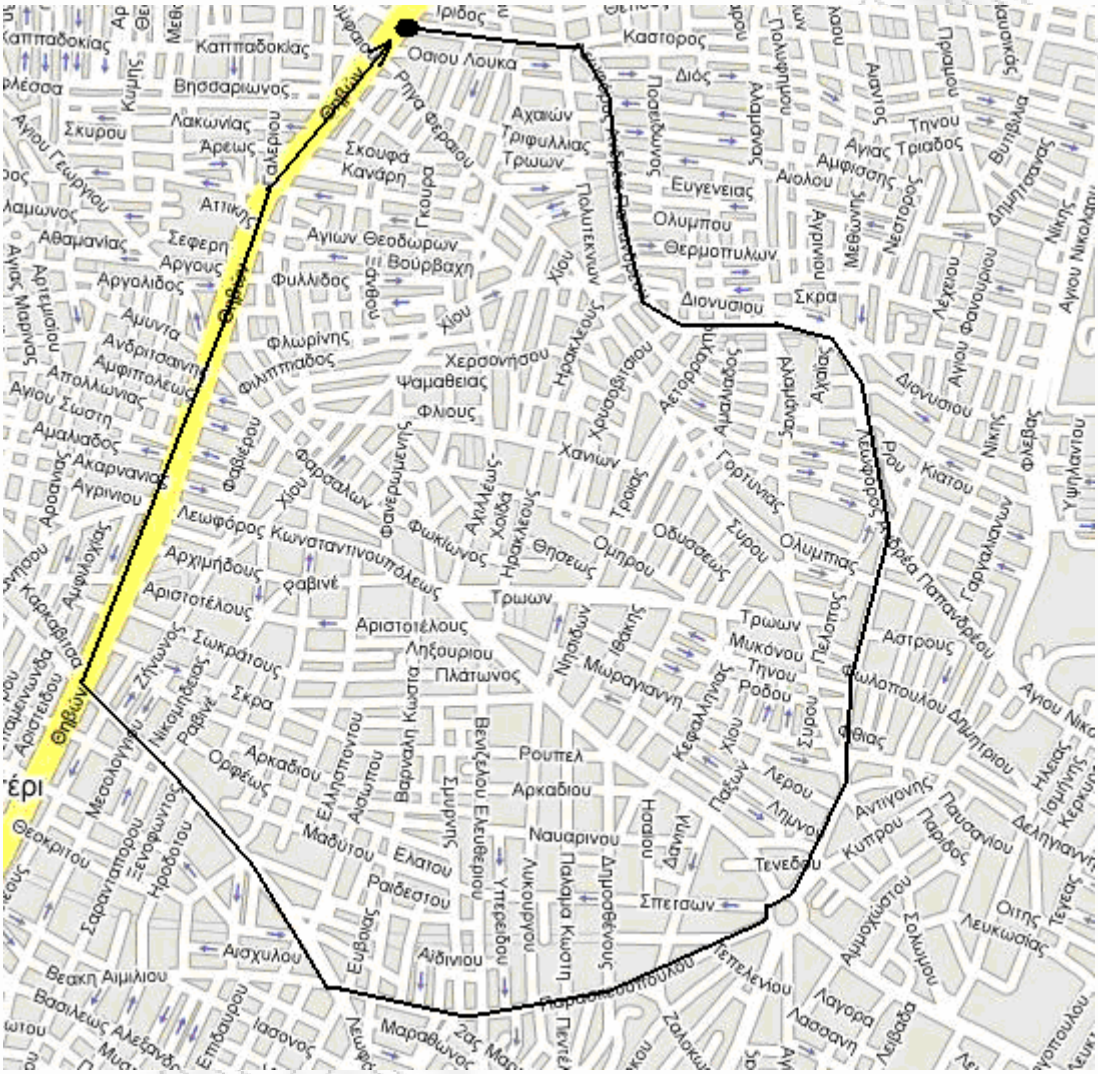
Αριθμός δικτύων τα οποία ήταν κλειδωμένα: 75/119

Αριθμός δικτύων τα οποία **δεν** ήταν κλειδωμένα: 44/119

Αριθμός δικτύων από τα οποία δεν υπήρχε εκπομπή του SSID: 8/119

(4 ανοιχτά - 4 κλειδωμένα)

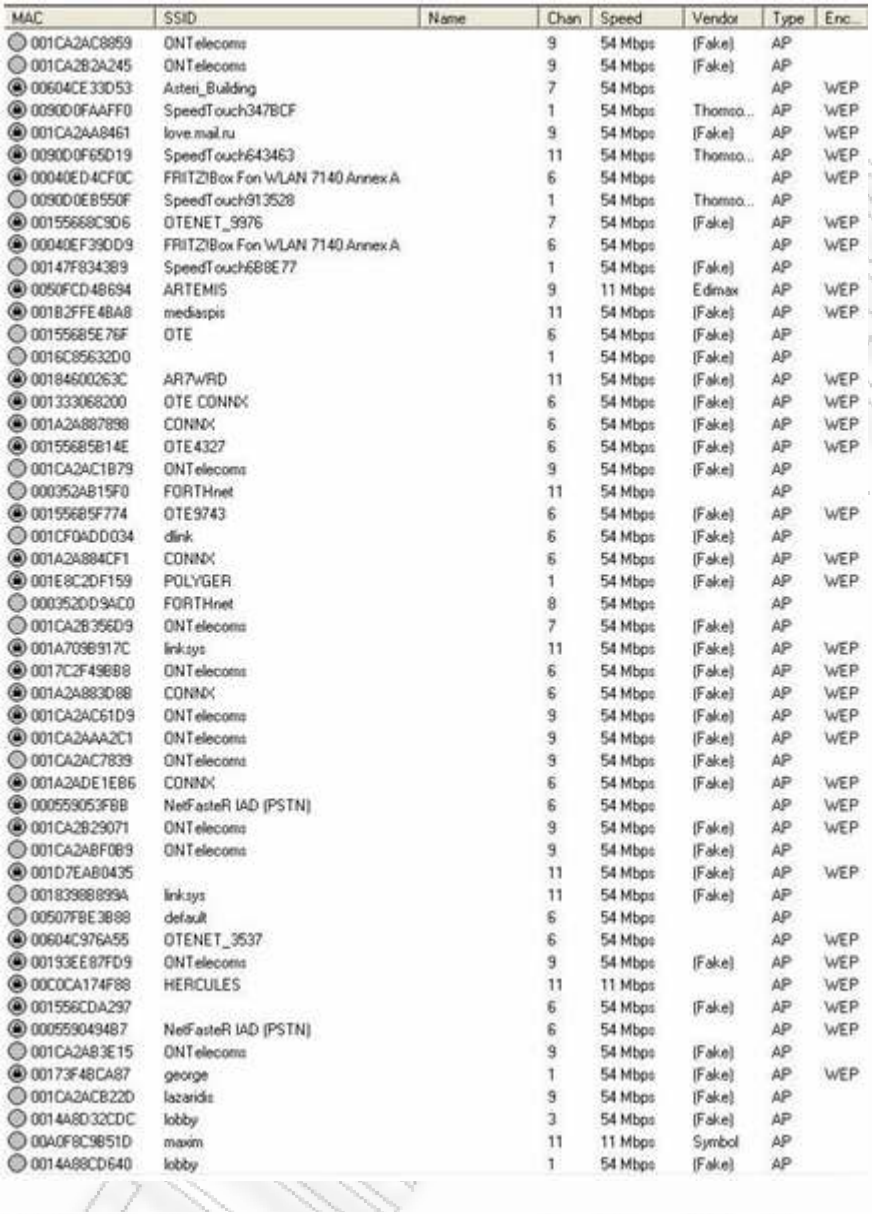
4.2.2 Προσωπική έρευνα ασύρματων δικτύων στην περιοχή του Περιστερίου



Εικόνα 4.4 Περιοχή Περιστερίου

4.2.2.1 Συγκέντρωση αποτελεσμάτων

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
00146CAA6F84	NETGEAR2		11	54 Mbps	(Fake)	AP	WEP
0001710C504A	Ixokinisi		11	54 Mbps		AP	WEP
0015568SCE6D	LOGIS		6	54 Mbps	(Fake)	AP	
00146C581C7E	homewireless		11	54 Mbps	(Fake)	AP	WEP
001556CD8A04	OTENET_9557		6	54 Mbps	(Fake)	AP	WEP
001C4A411D9C	KAVATZA		6	54 Mbps	(Fake)	AP	WEP
0017C2F6A0C4	NETFORTH		9	54 Mbps	(Fake)	AP	WEP
001A2A7DBE8A	Panag-Litsa		6	54 Mbps	(Fake)	AP	WEP
001A6BEBC251	Livebox-1ce6		10	54 Mbps	(Fake)	AP	WEP
00193EE880C9	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2AB3655	ONTelecom		4	54 Mbps	(Fake)	AP	
0014C146002C	Motorsport		11	54 Mbps	(Fake)	AP	WEP
001D1948DD36	CONNX		6	54 Mbps	(Fake)	AP	WEP
0013330ED26A	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2AAFB61	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2ACDC29	ONTelecoms		9	54 Mbps	(Fake)	AP	
001556B66D85	OTENET_7747		6	54 Mbps	(Fake)	AP	WEP
0002CF5A75DA	sk		6	54 Mbps		AP	WEP
001349EAE33C			11	54 Mbps	(Fake)	AP	WEP
0017C2F48918	ONTelecoms		6	54 Mbps	(Fake)	AP	WEP
0013330CB62E	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001AA1E013E6	ELX_WiFi2		1	54 Mbps	(Fake)	AP	WEP
001A30BA3590	ELX_WiFi2		1	54 Mbps	(Fake)	AP	WEP
001CA2B276D9	ONTelecoms		9	54 Mbps	(Fake)	AP	
00604CE24254	OTENET_9286		7	54 Mbps		AP	WEP
001B2FA29A46	NETGEAR		11	54 Mbps	(Fake)	AP	WEP
001CA2AC5A41	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B33E51	ONTelecoms		9	54 Mbps	(Fake)	AP	
001839223982	linksys		11	54 Mbps	(Fake)	AP	
001333094002	TZEPETO		6	54 Mbps	(Fake)	AP	WEP
001A2A8CACAD	CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2AC865D	ONTelecoms		9	54 Mbps	(Fake)	AP	
00604CE252EF	OTENET_2588		7	54 Mbps		AP	
0011F5858BEC	SpeedTouch5E7C22		1	54 Mbps	(Fake)	AP	
001A2A8875A1	CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568764JC	OTE2726		6	54 Mbps	(Fake)	AP	WEP
001CA2B2AB8D	ONTelecoms		9	54 Mbps	(Fake)	AP	
001C4A462962	FRITZIBox Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
0090D0F6724F	SpeedTouch785E72		1	54 Mbps	Thomso...	AP	
0017C2F6C2AC	PIRELLI		6	54 Mbps	(Fake)	AP	
00147FB240FB	SpeedTouch43C395		1	54 Mbps	(Fake)	AP	
001B2FE4113C	NETGEAR		11	54 Mbps	(Fake)	AP	
000559048893	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
0013330B42FE	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
0016B65C43EC	DA_PANT95		11	54 Mbps	(Fake)	AP	WEP
001556CD9865	OTE4392		6	54 Mbps	(Fake)	AP	WEP
001556B52042	OTE8483		6	54 Mbps	(Fake)	AP	WEP
0013330956AE	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001A2A8A4F45	CONNX		6	54 Mbps	(Fake)	AP	WEP
00147F83BDB9	SpeedTouchB10B36		1	54 Mbps	(Fake)	AP	
001C4AD0A7EF	FRITZIBox Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
001CA2AC8859	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B2A245	ONTelecoms		9	54 Mbps	(Fake)	AP	
00604CE33D53	Asteri_Building		7	54 Mbps		AP	WEP
0090D0FAAFF0	SpeedTouch347BCF		1	54 Mbps	Thomso...	AP	WEP
001CA2AA8461	love.mail.ru		9	54 Mbps	(Fake)	AP	WEP
0090D0F65D19	SpeedTouch643463		11	54 Mbps	Thomso...	AP	WEP
00040ED4CF0C	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps		AP	WEP
0090D0EB550F	SpeedTouch913528		1	54 Mbps	Thomso...	AP	
00155668C9D6	OTENET_9976		7	54 Mbps	(Fake)	AP	WEP
00040EF39DD9	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps		AP	WEP
00147F8343B9	SpeedTouch6B8E77		1	54 Mbps	(Fake)	AP	
0050FCD4B694	ARTEMIS		9	11 Mbps	Edimax	AP	WEP
001B2FFE4BA8	mediaspis		11	54 Mbps	(Fake)	AP	WEP
00155685E76F	OTE		6	54 Mbps	(Fake)	AP	
0016C85632D0			1	54 Mbps	(Fake)	AP	
00184600263C	AR7WRD		11	54 Mbps	(Fake)	AP	WEP
00133068200	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001A2A887898	CONNX		6	54 Mbps	(Fake)	AP	WEP
00155685B14E	OTE4327		6	54 Mbps	(Fake)	AP	WEP
001CA2AC1B79	ONTelecoms		9	54 Mbps	(Fake)	AP	
000352AB15F0	FORTHnet		11	54 Mbps		AP	
00155685F774	OTE9743		6	54 Mbps	(Fake)	AP	WEP
001CF0ADD034	dlink		6	54 Mbps	(Fake)	AP	
001A2A884CF1	CONNX		6	54 Mbps	(Fake)	AP	WEP
001E8C2DF159	POLYGER		1	54 Mbps	(Fake)	AP	WEP
000352DD9AC0	FORTHnet		8	54 Mbps		AP	
001CA2B356D9	ONTelecoms		7	54 Mbps	(Fake)	AP	
001A709B917C	linksys		11	54 Mbps	(Fake)	AP	WEP
0017C2F49BB8	ONTelecoms		6	54 Mbps	(Fake)	AP	WEP
001A2A883D88	CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2AC61D9	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2AAA2C1	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2AC7839	ONTelecoms		9	54 Mbps	(Fake)	AP	
001A2ADE1EB6	CONNX		6	54 Mbps	(Fake)	AP	WEP
000559053FBB	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
001CA2B29071	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2ABF0B9	ONTelecoms		9	54 Mbps	(Fake)	AP	
001D7EAB0435			11	54 Mbps	(Fake)	AP	WEP
0018388B899A	linksys		11	54 Mbps	(Fake)	AP	
00507FBE3B88	default		6	54 Mbps		AP	
00604C976A55	OTENET_3537		6	54 Mbps		AP	WEP
00193EE87FD9	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
00C0CA174F88	HERCULES		11	11 Mbps		AP	WEP
001556CDA297			6	54 Mbps	(Fake)	AP	WEP
000559049487	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
001CA2AB3E15	ONTelecoms		9	54 Mbps	(Fake)	AP	
00173F4BCA87	george		1	54 Mbps	(Fake)	AP	WEP
001CA2ACB22D	lazaridis		9	54 Mbps	(Fake)	AP	
0014A8D32CDC	lobby		3	54 Mbps	(Fake)	AP	
00A0F8C9B51D	maxim		11	11 Mbps	Symbol	AP	
0014A88CD640	lobby		1	54 Mbps	(Fake)	AP	
0014A8D32CDC	lobby		3	54 Mbps	(Fake)	AP	
00A0F8C9B51D	maxim		11	11 Mbps	Symbol	AP	
0014A88CD640	lobby		1	54 Mbps	(Fake)	AP	
00507FDEF580	Draytek		9	54 Mbps		AP	
0017597C6640			5	54 Mbps	(Fake)	AP	WEP
0016B65C04C9	accpagoto		11	54 Mbps	(Fake)	AP	
0013330EC382	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568775A0	Segafredo-velvet		6	54 Mbps	(Fake)	AP	WEP
001570726AB0			1	11 Mbps	(Fake)	AP	
001A2A7D9D33	CONNX		6	54 Mbps	(Fake)	AP	WEP
001B11383084	Tellas		6	54 Mbps	(Fake)	AP	WEP
00147F0FCA7B	SpeedTouch8FF342		1	54 Mbps	(Fake)	AP	WEP
001CA2B224D5	ONTelecoms		9	54 Mbps	(Fake)	AP	
0090D0E0F360	SpeedTouch62F810		1	54 Mbps	Thomso...	AP	WEP
001CA2B2210D	ONTelecoms		9	54 Mbps	(Fake)	AP	
001D19491EAA	CONNX		6	54 Mbps	(Fake)	AP	WEP
0013330FC3DC	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2ACA7BD	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
0001710C5240	Tornado		7	54 Mbps		AP	WEP
00507FDA9BB0			6	54 Mbps		AP	WEP
0019DB0E99AD	wlan-ap		1	54 Mbps	(Fake)	AP	
0090D0FB1668	SpeedTouch2378B3		1	54 Mbps	Thomso...	AP	WEP
00147FB48535	SpeedTouch9C8874		1	54 Mbps	(Fake)	AP	WEP
00147F6A9233	SpeedTouch728887		11	54 Mbps	(Fake)	AP	
001E2A1C3ADE	NETGEAR		11	54 Mbps	(Fake)	AP	WEP
001A2A8CAE24	CONNX		6	54 Mbps	(Fake)	AP	WEP

4.2.2.2 Στατιστική έρευνα αποτελεσμάτων

Έπειτα από ανάλυση των παραπάνω πληροφοριών, καταλήξαμε στα ακόλουθα αποτελέσματα.

Αριθμός συνολικών δικτύων που εντοπίστηκαν: 125

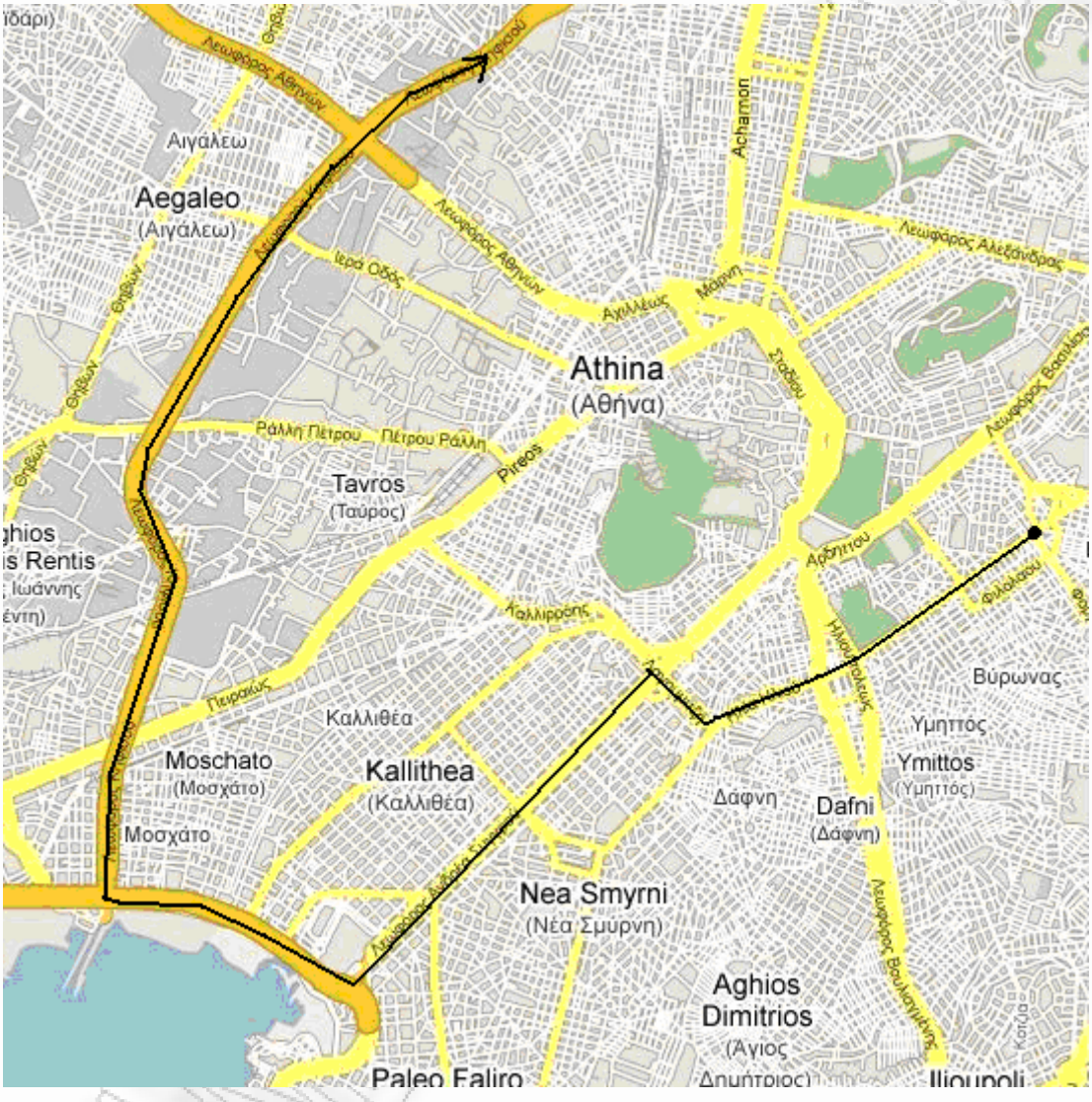
Αριθμός δικτύων τα οποία ήταν κλειδωμένα: 81 /125

Αριθμός δικτύων τα οποία **δεν** ήταν κλειδωμένα: 44/125

Αριθμός δικτύων από τα οποία δεν υπήρχε εκπομπή του SSID: 7/125

(2 ανοιχτά - 5 κλειδωμένα)

4.2.3 Προσωπική έρευνα ασύρματων δικτύων στη διαδρομή Παγκράτι - Περιστέρι μέσω της λ.Συγγρού και της Εθνικής οδού



Εικόνα 4.5 Διαδρομή Παγκράτι - Περιστέρι (μέσω λ.Συγγρού)

4.2.3.1 Συγκέντρωση αποτελεσμάτων

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.
0018392A1086			11	54 Mbps	(Fake)	AP	
00160A0E003F	Sweex_MD251		1	54 Mbps	(Fake)	AP	WEP
001556B68612	OTENET_9637		6	54 Mbps	(Fake)	AP	WEP
001556B5DAD6	OTE		6	54 Mbps	(Fake)	AP	
0201710DB166	Tropical		6	54 Mbps	(User-d...	AP	
00147F20AAD1	SpeedTouch27E6FE		1	54 Mbps	(Fake)	AP	
00C0CA174F88	HERCULES		11	11 Mbps		AP	WEP
00A0F8AE3887	2211		1	11 Mbps	Symbol	AP	WEP
00195B807F53	LionAir		11	54 Mbps	(Fake)	AP	WEP
001839ABDDCC	AERA		11	54 Mbps	(Fake)	AP	WEP
000FCBAF403D	TOTEM		10	54 Mbps		AP	
000F3DDFC8A9	komv1		6	54 Mbps		AP	WEP
0015AF2337D8	panagiotis-PC_AP		1	54 Mbps	(Fake)	AP	WEP
001CA2B345A5	PIRELLI		9	54 Mbps	(Fake)	AP	WEP
001CA2ABF0E1	ONTelecoms		1	54 Mbps	(Fake)	AP	
0600F0F49B64	HOUSEMAR-WLAN		1	54 Mbps	(User-d...	AP	WEP
0000F0F49B64	ACS-WLAN		1	54 Mbps	Samsung	AP	WEP
000B6B35CBE9	awmn-588-3210			54 Mbps		AP	
00156D102090	awmn-3210-6496			54 Mbps	(Fake)	AP	
000B6B349631	awmn-TEI_PEIREA-3210		11	11 Mbps		AP	
00147CB96C66	Budget		9	54 Mbps	(Fake)	AP	
0014C13EC5A5	USR9108		11	54 Mbps	(Fake)	AP	WEP
0015706E9DA0			11	54 Mbps	(Fake)	AP	WEP
0018390BDC3A	Jaguar		1	54 Mbps	(Fake)	AP	
0018194C8C90			1	54 Mbps	(Fake)	AP	
0014BFE6B8A7	10-4comms1		2	54 Mbps	(Fake)	AP	WEP
001C4AA31073	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001556B47E18	OTE		7	54 Mbps	(Fake)	AP	WEP
000E8E0A8311	awmn-jako-ap		8	11 Mbps		AP	
00186EC48CFF	AICom		11	54 Mbps	(Fake)	AP	WEP
00195B7F9CC5	ESRD		6	54 Mbps	(Fake)	AP	WEP
000FCBFDAE35	easyCruise		1	54 Mbps		AP	WEP
001C10666356	easyCruise		1	54 Mbps	(Fake)	AP	WEP
00179A7BD6E9	ESRD		1	54 Mbps	(Fake)	AP	WEP
021CBF000029	hpsetup		1	54 Mbps	(User-d...	Peer	
0019CB0C56F0			6	11 Mbps	(Fake)	AP	WEP
00026F4FA8F2	locnet_ath		1	54 Mbps	Senao Intl	AP	WEP
001C4A439755	Chris-office		11	54 Mbps	(Fake)	AP	WEP
00147F281BE5	SpeedTouch1BD32B		1	54 Mbps	(Fake)	AP	WEP
001E526C0AFF	Airport		1	54 Mbps	(Fake)	AP	WEP
001E2AD98C84	JGS		11	54 Mbps	(Fake)	AP	WEP
0015703B9CD0	101		11	54 Mbps	(Fake)	AP	WEP
00032F255217	KFC96		6	54 Mbps	GST (Li...	AP	WEP
001556B5CBCD	OTE1		6	54 Mbps	(Fake)	AP	WEP
001A2A7E0E01	soulandmate		6	54 Mbps	(Fake)	AP	WEP
00040EF3E339	LAB		6	54 Mbps		AP	WEP
0011502462F0	Griffin Athens		1	54 Mbps	(Fake)	AP	WEP
001839A9AA98	linksys		11	54 Mbps	(Fake)	AP	WEP
001556CDDEB8	Techzone		6	54 Mbps	(Fake)	AP	WEP
00134693F7FC	panos		6	54 Mbps	(Fake)	AP	WEP
001556B735B3	AEEGA_WLESS		6	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
001A2A7DACCF	CONNX		5	54 Mbps	(Fake)	AP	WEP
001556873883	OTENET_2633		6	54 Mbps	(Fake)	AP	WEP
0019CB567852	INLIFE		6	11 Mbps	(Fake)	AP	WEP
0015568 4984F	Glosec		8	54 Mbps	(Fake)	AP	WEP
00184D82917C	NETGEAR		11	54 Mbps	(Fake)	AP	WEP
10168FDE0A01	lady_1			54 Mbps	(Fake)	AP	WEP
001C10669183	Franman.wifi		11	54 Mbps	(Fake)	AP	WEP
0200025442A1			10	11 Mbps	Xerox	Peer	
00184D98A47A			6	54 Mbps	(Fake)	AP	WEP
001A2A8CAC3E	CONNX		6	54 Mbps	(Fake)	AP	WEP
0018F86799CD	mortaz		11	54 Mbps	(Fake)	AP	
0018841EEC71	FON_FREE_INTERNET		3	54 Mbps	(Fake)	AP	
0018841EEC72	MyPlace		3	54 Mbps	(Fake)	AP	WEP
001A2ADE3320	Wan601		7	54 Mbps	(Fake)	AP	WEP
0014C11E5EBE	tree_T2		11	54 Mbps	(Fake)	AP	WEP
0013330B8EEE	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
0017597C6630	flocale		7	54 Mbps	(Fake)	AP	
00146CA964FA	Netgear ADSL Router		5	54 Mbps	(Fake)	AP	WEP
001A2AB02C22	lotus		11	54 Mbps	(Fake)	AP	WEP
0014C13E42B0	segas epya		11	54 Mbps	(Fake)	AP	WEP
001A2A8A00BB	CONNX		6	54 Mbps	(Fake)	AP	WEP
000352F1DEC0	FORTHnet		6	54 Mbps		AP	
001E2A04F320	Makos Kentavros		11	54 Mbps	(Fake)	AP	WEP
00409656FB6C			6	11 Mbps	Cisco	AP	
00409655BC5E			1	11 Mbps	Cisco	AP	
00116B80B1DE	SV1fw_AP		4	54 Mbps	(Fake)	AP	WEP
00116B628513	HACI_2		7		(Fake)	AP	WEP
001A2A8A7162	mywifi		9	54 Mbps	(Fake)	AP	WEP
001839224F84	Gratia		11	54 Mbps	(Fake)	AP	WEP
0013330B4844	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
00026F409FA6	awmn-11350		4	1 Mbps	Senao Intl	AP	
00184D7A9A10	TYHQ		11	54 Mbps	(Fake)	AP	WEP
001A709EA9FA	transel		11	54 Mbps	(Fake)	AP	WEP
001CF0E3148A	STRUDECON		6	54 Mbps	(Fake)	AP	WEP
00A0C5C049D0	EK_SALES01		6	54 Mbps	Zyxel	AP	WEP
00115041EAAF			10	54 Mbps	(Fake)	AP	WEP
001D194976AC	CONNX		6	54 Mbps	(Fake)	AP	WEP
00195B4FBE5F	Network Virus Inside!		1	54 Mbps	(Fake)	AP	WEP
000FCBF96BF5	3Com		11	54 Mbps		AP	
00147F6C4C8D	SpeedTouch500F00		1	54 Mbps	(Fake)	AP	
001A2A8832C6	CONNX		6	54 Mbps	(Fake)	AP	WEP
0090D0F6373E	SpeedTouch40D581		11	54 Mbps	Thomso...	AP	WEP
00409656DC0A			6	11 Mbps	Cisco	AP	
001A2A72322C	CONNX		6	54 Mbps	(Fake)	AP	WEP
001A2A7E21E7	CONNX		6	54 Mbps	(Fake)	AP	WEP
001349CC2D46	PHARMAPLACE		6	54 Mbps	(Fake)	AP	WEP
0019DB929D76	wlan-ap		1	54 Mbps	(Fake)	AP	
00147FAFBEE9	Tomais Weeless		1	54 Mbps	(Fake)	AP	WEP
00147F6AA45F	SpeedTouch4E98A6		1	54 Mbps	(Fake)	AP	
00194BA02D6B	OTE6787		6	54 Mbps	(Fake)	AP	WEP
00409654ECA5			1	11 Mbps	Cisco	AP	

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
00409654ECA5			1	11 Mbps	Cisco	AP	
0015568532BD	OTENET_2483		6	54 Mbps	(Fake)	AP	WEP
00507FDC01A8	EMST		6	54 Mbps		AP	
00147F6E839F	SpeedTouchD0E742		1	54 Mbps	(Fake)	AP	WEP
001A70A96EF4	TA		11	54 Mbps	(Fake)	AP	
001A7094D0DC			11	54 Mbps	(Fake)	AP	
00131092AB5A	sub		11	54 Mbps	(Fake)	AP	WEP
001556B58403	OTE9396		6	54 Mbps	(Fake)	AP	WEP
001839D4219E	Apopsis		6	54 Mbps	(Fake)	AP	
0018393C3F50	linksys		11	54 Mbps	(Fake)	AP	
001A2ADE369E	CONNX		6	54 Mbps	(Fake)	AP	WEP
00301A092B8B	AWMN-434		6	11 Mbps	Smartbri...	AP	
001D1970A765	CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568B31A	OTENET_6769		7	54 Mbps	(Fake)	AP	WEP
001CA2B3253D	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B2A9E5	test		9	54 Mbps	(Fake)	AP	
001CA2B2662D	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2AB3431	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CF0AE7726	fotis		6	54 Mbps	(Fake)	AP	WEP
000FB5DA4FDE	NETGEAR		11	54 Mbps		AP	
0090D0FAAEFA	Drew's Net		1	54 Mbps	Thomso...	AP	
001A4F029BC2	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001CA2B35111	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B35981	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2AC5A4D	AGAHARIOYT		6	54 Mbps	(Fake)	AP	WEP
001CA2AC8665	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2AB2E55	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
00055905DD73	OREGANO FOODS		7	54 Mbps		AP	WEP
001CA2B2D6C5	On Telecoms		9	54 Mbps	(Fake)	AP	WEP
0017C2F68674	ONTelecoms		6	54 Mbps	(Fake)	AP	
0002CF53D8EE	Myriam		6	54 Mbps		AP	WEP
001CA2B28AFD	ONTelecoms		9	54 Mbps	(Fake)	AP	
0018392F36E4	zervos		8	54 Mbps	(Fake)	AP	WEP
00604CE21C17	OTENET_2726		7	54 Mbps		AP	WEP
001A703AE8DC	LinoHotSpot		9	54 Mbps	(Fake)	AP	WEP
00604CE3387C	OTENET_6887		7	54 Mbps		AP	WEP
0018393852AA	VISION_TANK		11	54 Mbps	(Fake)	AP	WEP
001A709B22F4	ESS		11	54 Mbps	(Fake)	AP	WEP
001556B60317	OTE		6	54 Mbps	(Fake)	AP	WEP
0004E266E736	linohotspot1		6	11 Mbps	SMC	AP	WEP
001A2A7E2D21	CONNX		6	54 Mbps	(Fake)	AP	WEP
000E2EA9B586	Topcom		3	54 Mbps		AP	WEP
00507FB49630	Euromotors		5	54 Mbps		AP	WEP
001CA2AAEA05	CSTATH		9	54 Mbps	(Fake)	AP	WEP
001CA2ACC43D	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001CA2B2D409	ONTelecoms		9	54 Mbps	(Fake)	AP	
00147F6AA8B3	GALINOS		1	54 Mbps	(Fake)	AP	WEP
001CA2B25795	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001556CFF095	courier center		6	54 Mbps	(Fake)	AP	WEP
001556CD9A69	AGEL_HAIR		6	54 Mbps	(Fake)	AP	WEP
0011F58075B3	SpeedTouch497C7Bhome		1	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.
0014C141E3EB	25jan3sko9b		11	54 Mbps	(Fake)	AP	WEP
001333069D0	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
00147F73D401	SpeedTouchD468CD		1	54 Mbps	(Fake)	AP	WEP
00147F65FFA7	Speed		1	54 Mbps	(Fake)	AP	WEP
001CA2ACA631	ONTELECOMS		9	54 Mbps	(Fake)	AP	WEP
001A4F21D3DD	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001CA2ACBE21	ONTelecoms		9	54 Mbps	(Fake)	AP	
0017C2F6EB88	danai		6	54 Mbps	(Fake)	AP	
001A4F22A0F8	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001CA2ABF4B5	JOHN TODL		9	54 Mbps	(Fake)	AP	WEP
001CA2B3DAF1	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2AB2ABD	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2AA7985	Viktoria		9	54 Mbps	(Fake)	AP	WEP
001CA2B30B19	ONTelecoms		9	54 Mbps	(Fake)	AP	
001E2A1D7ABC	NETGEAR		11	54 Mbps	(Fake)	AP	WEP
00150C37745D	xyn		6	54 Mbps	(Fake)	AP	WEP
001D197073B1	CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2B249D9	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001B2F4786A0	Tsourouflis		8	54 Mbps	(Fake)	AP	WEP
00604CE26ABC	CONNX		7	54 Mbps		AP	WEP
0019E096175E	TP-LINK		6	54 Mbps	(Fake)	AP	WEP
001CA2AAA67D	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
00147C5073B4	mes		11	54 Mbps	(Fake)	AP	WEP
001D1988A188	CONNX		6	54 Mbps	(Fake)	AP	WEP
001D1949C8ED	CONNX		6	54 Mbps	(Fake)	AP	WEP
00147F8498C9	SpeedTouch387954		1	54 Mbps	(Fake)	AP	WEP
000559049E43	NetFasteR_IAD		6	54 Mbps		AP	WEP
001556B5948C	OTENET_5862		6	54 Mbps	(Fake)	AP	WEP
001CA2B32C31	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B2A205	PIRELLI		9	54 Mbps	(Fake)	AP	WEP
0014C1390787	giristroula		11	54 Mbps	(Fake)	AP	WEP
00193EE8BF89	ONTelecoms		9	54 Mbps	(Fake)	AP	
001A2AD4A6E7	CONNX		6	54 Mbps	(Fake)	AP	WEP
00147FAF94C7	SpeedTouch8436E8		1	54 Mbps	(Fake)	AP	WEP
0013496AD8D6			6	54 Mbps	(Fake)	AP	
001CA2B26601	ONTelecoms		9	54 Mbps	(Fake)	AP	
001CA2B3D4D9	ONTelecoms		9	54 Mbps	(Fake)	AP	
001556B75038	AEEGA_WLESS		6	54 Mbps	(Fake)	AP	WEP
001CA2AC96B1	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001D1970A12C	CONNX		6	54 Mbps	(Fake)	AP	WEP
001D1970A6C0	CONNX		6	54 Mbps	(Fake)	AP	WEP
000352F02890	FORTHnet		6	54 Mbps		AP	
0014C13481C3	USR-9108		11	54 Mbps	(Fake)	AP	
001A2A8825A0	CONNX		6	54 Mbps	(Fake)	AP	WEP
001839384C20	PAGRATID		10	54 Mbps	(Fake)	AP	WEP
00137F532CB0	QUINTA		3	54 Mbps	(Fake)	AP	
001556CDD5A3	OTE9484		6	54 Mbps	(Fake)	AP	WEP
001556CDFA60	OTE4366		6	54 Mbps	(Fake)	AP	WEP
001839908142	linksys		11	54 Mbps	(Fake)	AP	
00186E0AD854	swan		11	54 Mbps	(Fake)	AP	WEP
00155668E497	OTENET_8242		7	54 Mbps	(Fake)	AP	WEP
001A2ADE2DF8	CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2AC5B45	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
0014BFCB7546	Helicon		11	54 Mbps	(Fake)	AP	WEP
00604CE33891	OTENET_7558		7	54 Mbps		AP	WEP
0014BFA93643	linksys		11	54 Mbps	(Fake)	AP	
00147F73DF19	SpeedTouchF09CB1		1	54 Mbps	(Fake)	AP	WEP

4.2.3.2 Στατιστική έρευνα αποτελεσμάτων

Έπειτα από ανάλυση των παραπάνω πληροφοριών, καταλήξαμε στα ακόλουθα αποτελέσματα.

Αριθμός συνολικών δικτύων που εντοπίστηκαν: 209

Αριθμός δικτύων τα οποία ήταν κλειδωμένα: 150/209

Αριθμός δικτύων τα οποία **δεν** ήταν κλειδωμένα: 59/209

Αριθμός δικτύων από τα οποία δεν υπήρχε εκπομπή του SSID: 14/209

(9 ανοιχτά - 5 κλειδωμένα)

4.2.4 Προσωπική έρευνα ασύρματων δικτύων στη διαδρομή Πλ.Αττικής - Παγκράτι

__Εικόνα 4.6__ Διαδρομή πλ.Αττικής - Παγκράτι

4.2.4.1 Συγκέντρωση αποτελεσμάτων

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encry...
001839384C20	PAGRATIO		10	54 Mbps	(Fake)	AP	WEP
00147F73DF19	SpeedTouchF09CB1		1	54 Mbps	(Fake)	AP	WEP
00604CE33891	OTENET_7558		7	54 Mbps		AP	WEP
00148FCB7546	Helicon		11	54 Mbps	(Fake)	AP	WEP
00137F532CB0	QUINTA		3	54 Mbps	(Fake)	AP	
001CA2AC5B45	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001A2ADE2DF8	CONNX		6	54 Mbps	(Fake)	AP	WEP
00155668E497	OTENET_8242		7	54 Mbps	(Fake)	AP	WEP
00183990B142	linksys		11	54 Mbps	(Fake)	AP	
001556CDFA60	OTE4366		6	54 Mbps	(Fake)	AP	WEP
00186E0AD854	swan		11	54 Mbps	(Fake)	AP	WEP
0014BFA93643	linksys		11	54 Mbps	(Fake)	AP	
001556CDD5A3	OTE9484		6	54 Mbps	(Fake)	AP	WEP
001A2A8825A0	CONNX		6	54 Mbps	(Fake)	AP	WEP
001A2ADE6881	CONNX		6	54 Mbps	(Fake)	AP	WEP
001E2A254D90	NETGEAR		11	54 Mbps	(Fake)	AP	
00116B16EECC	saconis		11	54 Mbps	(Fake)	AP	WEP
001D194991F7	CONNX		6	54 Mbps	(Fake)	AP	WEP
00507FBF2C40	default		6	54 Mbps		AP	
0015568B5C47A	OTE9786		6	54 Mbps	(Fake)	AP	WEP
00604CE254D8	dmos		7	54 Mbps		AP	WEP
001556D01162	Isis		6	54 Mbps	(Fake)	AP	
0014C119F134	NEWGEN		6	54 Mbps	(Fake)	AP	WEP
000FB50FD488	NETGEAR		11	54 Mbps		AP	
001CA2ABE5D1	ONTelecoms		9	54 Mbps	(Fake)	AP	
0017C2F49D50	ONTelecoms		6	54 Mbps	(Fake)	AP	WEP
0090D0F815DE	SpeedTouch21CDD4		1	54 Mbps	Thomso...	AP	WEP
001A4F01A7D9	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
0015568481D5	OTE		7	54 Mbps	(Fake)	AP	WEP
0016B6202E87	linksys		11	54 Mbps	(Fake)	AP	WEP
0017C2F4C55C	Paros		6	54 Mbps	(Fake)	AP	WEP
000FB5CD12BE	NETGEAR		11	54 Mbps		AP	
00116B147848	MarvelWood		3	54 Mbps	(Fake)	AP	WEP
001C4A4112D9	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001D19498798	CONNX		6	54 Mbps	(Fake)	AP	WEP
00026F409F19	awmn-8949-ne		11	11 Mbps	Senao Intl	AP	
001CF0E2E150	gati		11	54 Mbps	(Fake)	AP	WEP
001CA2B241B1	ONTelecoms		9	54 Mbps	(Fake)	AP	
001B2F4A9192	NETGEAR		11	54 Mbps	(Fake)	AP	WEP
00194BA0079D	OTE8552		6	54 Mbps	(Fake)	AP	WEP
00147F73F3BD	SpeedTouch3AE34A		1	54 Mbps	(Fake)	AP	
001CF0E2F598	dlink		6	54 Mbps	(Fake)	AP	
001A2A883FDD	CONNX		6	54 Mbps	(Fake)	AP	WEP
001CA2B2BD95	ONTelecoms		9	54 Mbps	(Fake)	AP	
00026F409F11	awmn-8949		5	11 Mbps	Senao Intl	AP	
00147F0FCAAD	SpeedTouch7107A8		1	54 Mbps	(Fake)	AP	WEP
00155668B18B	GP		7	54 Mbps	(Fake)	AP	WEP
000559048488	NetFasteR_IAD		6	54 Mbps		AP	WEP
000559062053	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
00116B12B9D4	LAW_WIFI		6	54 Mbps	(Fake)	AP	WEP
001D19496F56	CONNX		6	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encry...
00195B8BDA12	dlink		6	54 Mbps	(Fake)	AP	WEP
000FB5B08C20	NETGEAR		11	54 Mbps		AP	WEP
0013197BF440	wlan@802.11b		1	54 Mbps	(Fake)	AP	WEP
0018F8D27FC8	Cyclades		6	54 Mbps	(Fake)	AP	WEP
001A7096FCCA	SISY		6	54 Mbps	(Fake)	AP	WEP
001556CD5F02	conet		6	54 Mbps	(Fake)	AP	WEP
0013309456C	ConnX 2008		6	54 Mbps	(Fake)	AP	WEP
001D194983D8	Geo		11	54 Mbps	(Fake)	AP	WEP
00507F88CF00	med6		6	54 Mbps		AP	WEP
001C4AD0DCC2	MELIA		6	54 Mbps	(Fake)	AP	WEP
001556861EDA	degus		6	54 Mbps	(Fake)	AP	WEP
00155668C313	OTENET_9579		7	54 Mbps	(Fake)	AP	WEP
00117C0A1BC2	wgs2b		3	11 Mbps	(Fake)	AP	
00116B275EB4	SANTOGUSTO		2	54 Mbps	(Fake)	AP	WEP
001C4A4BCECC	FRITZ!Box Fon WLAN 7140		1	54 Mbps	(Fake)	AP	WEP
00604CE24380	OTENET_4745		2	54 Mbps		AP	WEP
0019060D32E1	ebea-guest		2	54 Mbps	(Fake)	AP	WEP
0018392299BC	minos		11	54 Mbps	(Fake)	AP	WEP
00116B1092CA	Wireless		2	54 Mbps	(Fake)	AP	WEP
001556B56A80	OTE2473		6	54 Mbps	(Fake)	AP	WEP
000AE90A5342	SMC		1	54 Mbps	AirVast	AP	WEP
00194BA01571	KALNET		6	54 Mbps	(Fake)	AP	WEP
0013330A739E	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
000E6ACC5DC6	3Com		4	54 Mbps		AP	WEP
001AC137971A	Ghizzoni		10	54 Mbps	(Fake)	AP	WEP
001D1970769C	CONNX		6	54 Mbps	(Fake)	AP	WEP
00183922C3A2	localw		11	54 Mbps	(Fake)	AP	WEP
0014692D6DD0			1	5.5 Mbps	(Fake)	AP	WEP
00116B60CED2	FaropAP		6	54 Mbps	(Fake)	AP	WEP
00186E066F88	3Com		11	54 Mbps	(Fake)	AP	WEP
0014C1050050	Kafros		11	54 Mbps	(Fake)	AP	WEP
00131ABED920			2	54 Mbps	(Fake)	AP	WEP
001556D00775	OTE3589		6	54 Mbps	(Fake)	AP	WEP
00040ED39C2E	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps		AP	WEP
000FB53E3A10			11	54 Mbps		AP	WEP
02130201FCD7	Jet Blue hot spot		11	54 Mbps	(User-d...	Peer	
0014C138F737	USR5455		11	54 Mbps	(Fake)	AP	WEP
0015C66A2C10			1	54 Mbps	(Fake)	AP	WEP
001D197076AE	CONNX		6	54 Mbps	(Fake)	AP	WEP
0014BF940B55	linksys		3	54 Mbps	(Fake)	AP	WEP
00147FAFAACF	SpeedTouch3C00E1		1	54 Mbps	(Fake)	AP	WEP
00183931010A	tsb		11	54 Mbps	(Fake)	AP	WEP
001D1946A43E	CONNX		6	54 Mbps	(Fake)	AP	WEP
00304F4E318D	gi		6	54 Mbps	PLANE...	AP	WEP
001D197074AA	CONNX		6	54 Mbps	(Fake)	AP	WEP
00133068782	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
00147F226DCB	Soutzoglou		1	54 Mbps	(Fake)	AP	WEP
0015568681F5	OTENET_9556		6	54 Mbps	(Fake)	AP	WEP
001D198CCEE2	CONNX		6	54 Mbps	(Fake)	AP	WEP
00184D930A54	AFCO2		11	54 Mbps	(Fake)	AP	WEP
00121768 2092	linksys		11	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encry...
00155668E70A	OTENET_3742		7	54 Mbps	(Fake)	AP	WEP
0015568SD899	OTE3773		6	54 Mbps	(Fake)	AP	WEP
001556878632	OTE4347		6	54 Mbps	(Fake)	AP	WEP
001A2A7DB569	CONNX		6	54 Mbps	(Fake)	AP	WEP
001556CE210F	adsl-ktenas		6	54 Mbps	(Fake)	AP	WEP
00A0C5D0E396	myOfficeWlan		6	54 Mbps	Zyxel	AP	WEP
0015568SECC4	OTE8325		6	54 Mbps	(Fake)	AP	WEP
00183925EE52	linksys-tee		11	54 Mbps	(Fake)	AP	WEP
00184DE001DF			11	54 Mbps	(Fake)	AP	WEP
0016B65BF98F	ZAN		11	54 Mbps	(Fake)	AP	WEP
00116B39B2D2	BIGAPPLE1		11	11 Mbps	(Fake)	AP	WEP
00032F255556	AP255556		6	54 Mbps	GST (Li...	AP	WEP
001A2A888C0F	CONNX		6	54 Mbps	(Fake)	AP	WEP
001556688332	OTENET_2946		7	54 Mbps	(Fake)	AP	WEP
000D937FF9E8	yolanda hotspot		10	54 Mbps	Apple	AP	WEP
001C10683243	ToBakaliko		2	54 Mbps	(Fake)	AP	WEP
00150C8B8032	SFRAG_WLAN		11	54 Mbps	(Fake)	AP	WEP
001A2A886A01	CONNX		6	54 Mbps	(Fake)	AP	WEP
001556CE20EE	OTE8329		6	54 Mbps	(Fake)	AP	WEP
001556CD6C40	OTE3352		6	54 Mbps	(Fake)	AP	WEP
00186ECD5FAA	ts_lw		11	54 Mbps	(Fake)	AP	
00155684FB13	OTENET_7728		6	54 Mbps	(Fake)	AP	WEP
00184D5099F8	PHOTOPOULOS		6	54 Mbps	(Fake)	AP	WEP
001556CD153D	OTENET_3839		6	54 Mbps	(Fake)	AP	WEP
0002CF640152	TT		6	54 Mbps		AP	WEP
001A2A8AA489	CONNX		6	54 Mbps	(Fake)	AP	WEP
001A2A7E2DFF	CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568781E2	OTE7282		6	54 Mbps	(Fake)	AP	WEP
00147F6E94EF	Dalne		11	54 Mbps	(Fake)	AP	WEP
001556CD92B3	OTE3848		6	54 Mbps	(Fake)	AP	WEP
001217DF17E1	linksys		11	54 Mbps	(Fake)	AP	WEP
0014C13566EE	TOURIST		11	54 Mbps	(Fake)	AP	WEP
00147FAFAFD5	SpeedTouch279330		1	54 Mbps	(Fake)	AP	WEP
00147FB4C72B	SpeedTouch16B2B0		1	54 Mbps	(Fake)	AP	WEP
00155668FFE	OTENET_8744		7	54 Mbps	(Fake)	AP	WEP
0018395C133F	linksys		11	54 Mbps	(Fake)	AP	WEP
004F621A11FE	Anelixis		9	54 Mbps	(Fake)	AP	WEP
001B2F79B03A	PAPAPOLITIS		11	54 Mbps	(Fake)	AP	WEP
001B2F473C3C	Argyropoulos		6	54 Mbps	(Fake)	AP	WEP
001CA2AC7D4D	ONTelecoms		9	54 Mbps	(Fake)	AP	
004096541C59	@c@d3mi		7	11 Mbps	Cisco	AP	
00147C4D2259	nemesis		11	54 Mbps	(Fake)	AP	WEP
00193EE89AE5	ONTelecoms		9	54 Mbps	(Fake)	AP	
0014C119BF8C	KLOUDAS		11	54 Mbps	(Fake)	AP	WEP
001A2A7E1BC6	CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568SCA4D	OTE		10	54 Mbps	(Fake)	AP	WEP
00184D93208C	loukou		3	54 Mbps	(Fake)	AP	WEP
000FCBB4E71D	3Com		11	54 Mbps		AP	WEP
001A4F20C08E	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
000559060837	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
0013330EC3C4	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encry...
001556B5C2C7	RIGOPOYLOSWIFI		6	54 Mbps	(Fake)	AP	WEP
001556873793	Ilias		6	54 Mbps	(Fake)	AP	WEP
0090D0E0F981	Hydria Wireless		1	54 Mbps	Thomso...	AP	WEP
00186E0E5387	3Com		11	54 Mbps	(Fake)	AP	WEP
001D7EACECB8	linksys		11	54 Mbps	(Fake)	AP	WEP
000C2002F33F	Lan_1		6	48 Mbps		AP	WEP
00147FB252A5	SpeedTouch0179A3		1	54 Mbps	(Fake)	AP	WEP
0014BF6F95D6	domain		11	54 Mbps	(Fake)	AP	
000C46F2FF8C	allied		52	54 Mbps		AP	
001E2A1D3F2C	Solon		8	54 Mbps	(Fake)	AP	WEP
0015568F033	Satan's net		6	54 Mbps	(Fake)	AP	
001556CD91AB	highpromogroup		6	54 Mbps	(Fake)	AP	WEP
001556B5C921	EIET		6	54 Mbps	(Fake)	AP	WEP
001AC115C52C	13L564BW004BB		11	54 Mbps	(Fake)	AP	WEP
000FCBFC8475	3Com		11	54 Mbps		AP	WEP
001AC1159022	3Com		11	54 Mbps	(Fake)	AP	
0012BF236909	celt		11	54 Mbps	(Fake)	AP	WEP
00147F834769	SpeedTouchD1742C		11	54 Mbps	(Fake)	AP	
001CA2B24E89	ONTelecoms		9	54 Mbps	(Fake)	AP	
0012A90A79AF	XROADS		4	54 Mbps	(Fake)	AP	WEP
001839392E38	linksys		11	54 Mbps	(Fake)	AP	
000352DAD100	FORTHnet		11	54 Mbps		AP	
001A2AD49958	CONNX		6	54 Mbps	(Fake)	AP	WEP
001556CDD90C	darbin		6	54 Mbps	(Fake)	AP	WEP
001CA2AADAF9	ONTelecoms		9	54 Mbps	(Fake)	AP	
00604C992F3C	OTENET_8492		7	54 Mbps		AP	WEP
00147FAFA2AF	SpeedTouchLocked		1	54 Mbps	(Fake)	AP	WEP
001556B7716E	OTE6475		6	54 Mbps	(Fake)	AP	WEP
001556CDD267			6	54 Mbps	(Fake)	AP	
001A2A7D95E9	CONNX		6	54 Mbps	(Fake)	AP	WEP
000F3D34C4DC	RIGpool		1	54 Mbps		AP	
001D197078B5	CONNX		6	54 Mbps	(Fake)	AP	WEP
00147F20A7E9	SpeedTouch6CE165		1	54 Mbps	(Fake)	AP	WEP
000FCBFA00F7	3Com		11	11 Mbps		AP	
001556B49303	MiOu_NeT		6	54 Mbps	(Fake)	AP	WEP
000F3D34C08E	RIGlobby		6	54 Mbps		AP	
0014C1287153	USR		11	54 Mbps	(Fake)	AP	WEP
0016E63CB811			7	54 Mbps	(Fake)	AP	WEP
00121770F60E	linksys		11	54 Mbps	(Fake)	AP	WEP
001556CDF670	DEAL		6	54 Mbps	(Fake)	AP	
00116B13D4F2	Matrix		3	54 Mbps	(Fake)	AP	WEP
001556CD3FAC	QP		6	54 Mbps	(Fake)	AP	
001333095B82	HATZIPIENET		6	54 Mbps	(Fake)	AP	WEP
00116B10F7EA	Wireless		6	54 Mbps	(Fake)	AP	WEP
0015568C4A7	DOULIS LAW FIRM		6	54 Mbps	(Fake)	AP	WEP
001556B61CD0	OTE4834		6	54 Mbps	(Fake)	AP	
001195DA4CDB	VZV		8	54 Mbps	(Fake)	AP	
00116B60CD1C	extra		7	54 Mbps	(Fake)	AP	WEP
000559048AC3	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
001CA2B2B081	ONTelecoms		9	54 Mbps	(Fake)	AP	
001333078F2A	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP

MAC	SSID	Name	Chan	Speed	Vendor	Type	Encry...
001B2FAC6108	HATPAN		11	54 Mbps	(Fake)	AP	WEP
001556B5BFA3	OTE6956		6	54 Mbps	(Fake)	AP	WEP
001884257C15	FON_Photodesmos		2	54 Mbps	(Fake)	AP	
001884257C16	Photodigital		2	54 Mbps	(Fake)	AP	WEP
0014BFBB3232	olficeG		11	54 Mbps	(Fake)	AP	WEP
0050F1121210	TI-AR7WRD		11	54 Mbps		AP	
00147F35DBA9	ANSWER-ATHENS		6	54 Mbps	(Fake)	AP	WEP
00116BB0842F	APB0B42F		6	54 Mbps	(Fake)	AP	
00116B10EA44	Wireless		6	54 Mbps	(Fake)	AP	WEP
00156D543FF8			4	11 Mbps	(Fake)	AP	WEP
001839F7ABAF	linksys4		11		(Fake)	AP	WEP
001A2A7DA96C	CONNX		11	54 Mbps	(Fake)	AP	WEP
00150CFE7AB9	FRITZ!Box Fon WLAN 7140		6	54 Mbps	(Fake)	AP	WEP
0005590460AB	NetFasteR_IAD		6	54 Mbps		AP	WEP
001556CE2028	jkap		6	54 Mbps	(Fake)	AP	WEP
0001710C5B36	Tornado		6	54 Mbps		AP	
0014BF9E3C93	cris580		2	54 Mbps	(Fake)	AP	WEP
0001710C5B46	Elysium 2		6	54 Mbps		AP	WEP
001D1988B121	MEEST_HELLAS_TOURS		6	54 Mbps	(Fake)	AP	WEP
001556B56F78	OTENET_4847		6	54 Mbps	(Fake)	AP	WEP
00147FB242BF	AbdslaWiFi		11	54 Mbps	(Fake)	AP	WEP
001839373B9B	ELENCO		11	54 Mbps	(Fake)	AP	WEP
000B6B80B1F7			1	11 Mbps		AP	WEP
001CA2B3607D	ONTelecoms		9	54 Mbps	(Fake)	AP	
00147F209D73	SpeedTouch8598BC		1	54 Mbps	(Fake)	AP	
0227B788BC80	loswn		6	11 Mbps	(User-d...	Peer	
001A2A882F8A	CONNX		6	54 Mbps	(Fake)	AP	WEP
001D19496203	Hronis		6	54 Mbps	(Fake)	AP	WEP
001A4F02950B	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001A4F01B097	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001D68711065	SpeedTouchFAFE39		1	54 Mbps	(Fake)	AP	
000958CD106E	MAGER		11	54 Mbps	Netgear	AP	WEP
001D19887B93	CONNX		6	54 Mbps	(Fake)	AP	WEP
0015568486A	otenet		6	54 Mbps	(Fake)	AP	
001A2A7E0FFF	programalistes		6	54 Mbps	(Fake)	AP	WEP
001556CFBB3A	daem_computer_room		6	54 Mbps	(Fake)	AP	WEP
00C049FBB835	smartboynet		11	54 Mbps	US Rob...	AP	WEP
00193EE88449	ONTelecoms		9	54 Mbps	(Fake)	AP	
001E2A0D61B4	CARPE NOCTEM		6	54 Mbps	(Fake)	AP	WEP
0005590629D7	NetFasteR IAD (PSTN)		6	54 Mbps		AP	
00193EE87C2D	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
0005590446F3	NetFasteR_IAD		6	54 Mbps		AP	WEP
000F667750AD	novotel		11	54 Mbps	Linksys	AP	
001CA2B22D29	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
0014C10423FA	USR5451		11	54 Mbps	(Fake)	AP	
001556CFEAC2	OTE6639		6	54 Mbps	(Fake)	AP	WEP
001C4AD0B786	FRITZ!Box Fon WLAN 7140 Annex A		6	54 Mbps	(Fake)	AP	WEP
001A4F016F1F	FRITZ!Box Fon WLAN 7140 Annex B		6	54 Mbps	(Fake)	AP	WEP
00147F6A93A3	SpeedTouchD75C41		1	54 Mbps	(Fake)	AP	
001A2A7DE161	CONNX		6	54 Mbps	(Fake)	AP	WEP
00055904A53F	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
00055905FEC3	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
0013330BE162	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
001556D01939	OTE9479		6	54 Mbps	(Fake)	AP	WEP
001D19499362	CONNX		6	54 Mbps	(Fake)	AP	WEP
000559049337	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
001556D0105A	loucas		6	54 Mbps	(Fake)	AP	WEP
000559043FAB	NetFasteR IAD (PSTN)		6	54 Mbps		AP	WEP
0013330B46C8	OTE CONNX		6	54 Mbps	(Fake)	AP	WEP
AA986DC29FA9	print server 103570		11	11 Mbps	(User-d...	Peer	
00193EE894D9	ONTelecoms		9	54 Mbps	(Fake)	AP	WEP
001D19469C1F	CONNX		6	54 Mbps	(Fake)	AP	WEP

4.2.4.2 Στατιστική έρευνα αποτελεσμάτων

Έπειτα από ανάλυση των παραπάνω πληροφοριών, καταλήξαμε στα ακόλουθα αποτελέσματα.

Αριθμός συνολικών δικτύων που εντοπίστηκαν: 268

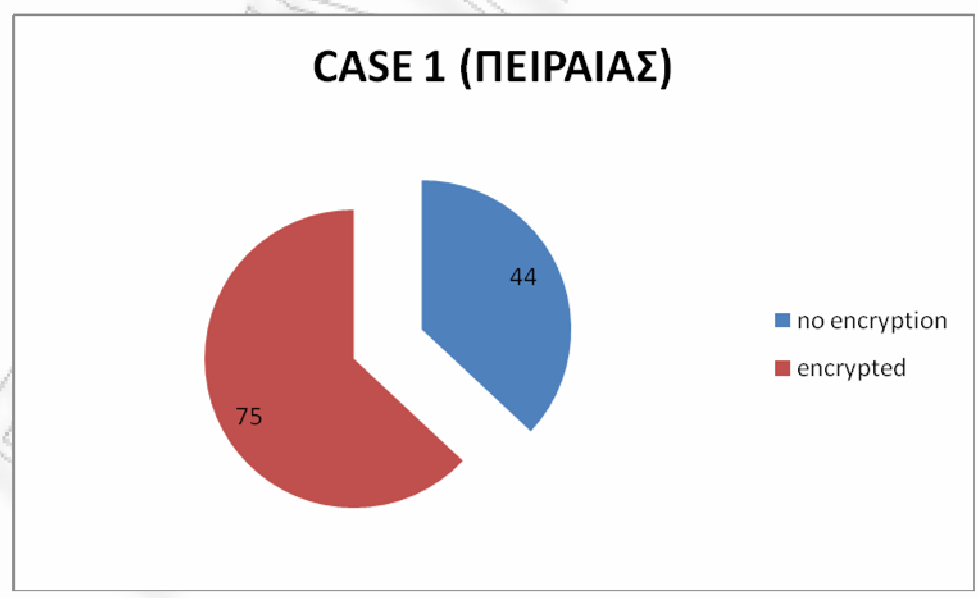
Αριθμός δικτύων τα οποία ήταν κλειδωμένα: 213/268

Αριθμός δικτύων τα οποία **δεν** ήταν κλειδωμένα: 55/268

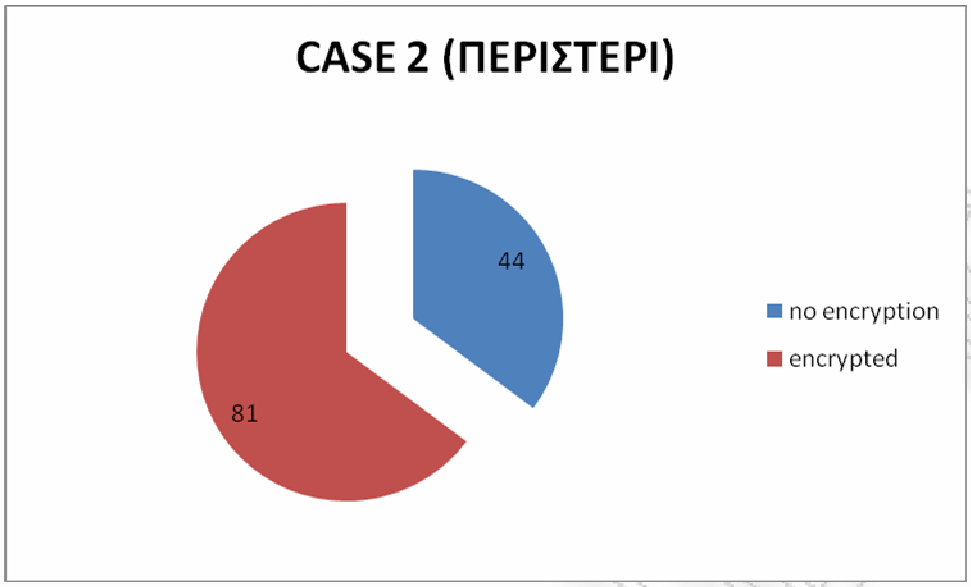
Αριθμός δικτύων από τα οποία δεν υπήρχε εκπομπή του SSID:9/268

(1 ανοιχτό - 8 κλειδωμένα)

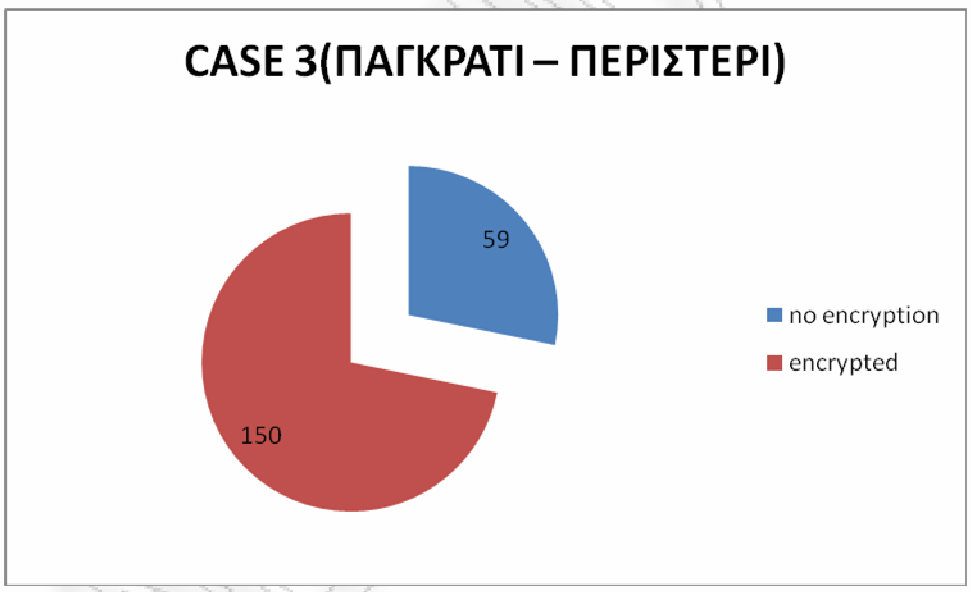
4.3 Συγκέντρωση Στατιστικών



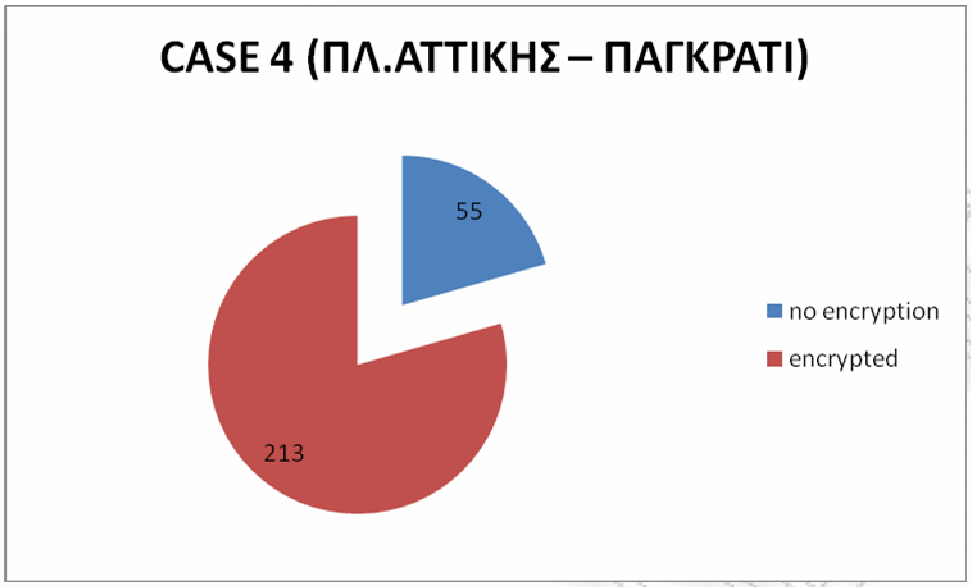
Εικόνα 4.7



Εικόνα 4.8



Εικόνα 4.9

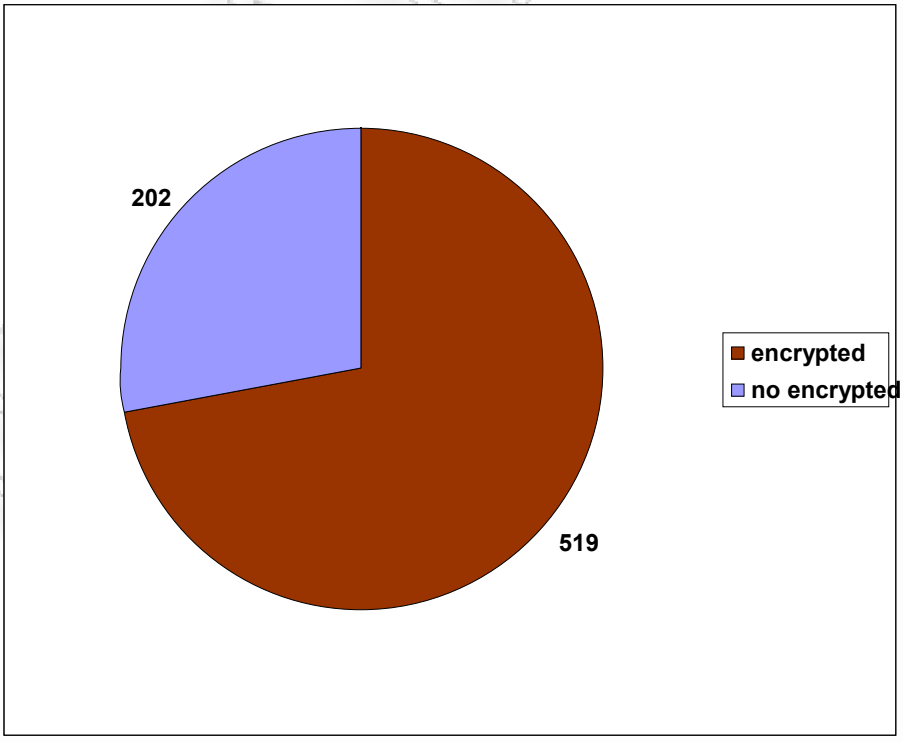


Εικόνα 4.10

Συνολικά αποτελέσματα

Συνολικός αριθμός ασύρματων δικτύων: 721

Συνολικός αριθμός **μη κλειδωμένων** ασύρματων δικτύων: 202



Εικόνα 4.11

5.1 Μετρίαση των Κινδύνων

Οι συνέπειες των επιθέσεων είναι καθοριστικές για τα 802.11 WLANs διότι επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. Για τον λόγο αυτόν, έχουν παρθεί κάποια αντίμετρα για την μετρίαση των κινδύνων και των ευπαθειών. Τα αντίμετρα διαχείρισης, σε συνδυασμό με τα λειτουργικά και τεχνικά αντίμετρα, μπορούν να μειώσουν αποτελεσματικά τους κινδύνους που σχετίζονται με τα WLANs.

Οι παρακάτω οδηγίες δεν εξαλείφουν ολοκληρωτικά τους κινδύνους σε ένα τέτοιο σύστημα, δίνουν όμως τις κατευθυντήριες γραμμές για την μετρίαση και την εξάλειψη πολλών, αν όχι όλων, από τους κινδύνους αυτούς. Θα πρέπει επίσης να σημειωθεί ότι δεν υπάρχει κανένα συγκεκριμένο σύνολο οδηγιών το οποίο να μπορεί να ταιριάξει στις ανάγκες όλων των συστημάτων όταν έχουμε να κάνουμε με θέματα ασφάλειας.

5.2 Αντίμετρα Διαχείρισης

Τα αντίμετρα διαχείρισης ξεκινούν με μία περιεκτική πολιτική, ώστε να εξασφαλίσουν την ασφάλεια σε ένα ασύρματο δίκτυο. Στην πολιτική αυτή θα στηριχτεί η λογική και υλοποίηση και των άλλων αντιμέτρων, των λειτουργικών και των τεχνικών. Μία πολιτική ασφάλειας θα πρέπει, λοιπόν, να εφαρμόζει τα ακόλουθα:

- Αναγνώριση του ποιος θα χρησιμοποιεί την τεχνολογία WLAN σε έναν οργανισμό.
- Αναγνώριση του αν απαιτείται πρόσβαση στο Internet.
- Περιγραφή του ποιος θα εγκαθιστά σημεία πρόσβασης και άλλον ασύρματο εξοπλισμό.
- Εξασφάλιση περιορισμών όσον αφορά την τοποθεσία και τη φυσική ασφάλεια των σημείων πρόσβασης.
- Περιγραφή του τύπου των πληροφοριών που μπορούν να μεταδίδονται μέσω της ασύρματης ζεύξης.

- Περιγραφή των συνθηκών, σύμφωνα με τις οποίες θα επιτρέπονται ασύρματες συσκευές.
- Καθορισμός συγκεκριμένων ρυθμίσεων ασφαλείας για τα σημεία πρόσβασης.
- Καθορισμός περιορισμών, σύμφωνα με τους οποίους θα χρησιμοποιείται η ασύρματη συσκευή.
- Περιγραφή των ρυθμίσεων υλικού (hardware) και λογισμικού (software) για όλες τις ασύρματες συσκευές.
- Παροχή οδηγιών για την αναφορά απωλειών όσον αφορά τις ασύρματες συσκευές, την προστασία ασύρματων πελατών, την χρήση κρυπτογράφησης και διαχείρισης κλειδιών, και τα περιστατικά ασφάλειας.
- Καθορισμός της συχνότητας και του εύρους των εκτιμήσεων ασφάλειας, ώστε να περιλαμβάνουν την εύρεση όλων των σημείων πρόσβασης

5.2.1 Λειτουργικά Αντίμετρα

Η φυσική ασφάλεια είναι το πιο θεμελιώδες βήμα για την εξασφάλιση της πρόσβασης μόνο εξουσιοδοτημένων χρηστών στον ασύρματο εξοπλισμό. Η φυσική ασφάλεια συνδυάζει τον έλεγχο πρόσβασης, την αυθεντικοποίηση χρηστών, και την εξωτερική περιοριστική προστασία.

Πολύ σημαντική είναι η γνώση της ακτίνας που καλύπτει ένα σημείο πρόσβασης, ώστε αυτή να μην ξεπερνά το χώρο των εγκαταστάσεων του δικτύου. Αν κάτι τέτοιο συμβεί (δηλαδή η εμβέλεια ενός σημείου πρόσβασης καλύπτει και χώρο εκτός των εγκαταστάσεων), τότε κάποιος μπορεί να το εκμεταλλευτεί για να κερδίσει πρόσβαση στο δίκτυο. Για να αποφευχθεί, λοιπόν, μια τέτοια ευπάθεια, κάποια σημεία πρόσβασης έχουν ειδικές λειτουργίες που ρυθμίζουν την ισχύ του σήματος τους, ώστε να ρυθμίζεται η ακτίνα κάλυψης τους σύμφωνα με τις ανάγκες σε κάθε περίπτωση.

5.2.2 Τεχνικά Αντίμετρα

Τα τεχνικά αντίμετρα περιλαμβάνουν λύσεις λογισμικού και υλικού που βοηθούν στην ασφάλεια του ασύρματου περιβάλλοντος.

5.2.3 Λύσεις λογισμικού

Οι λύσεις λογισμικού συμπεριλαμβάνουν την ρύθμιση των σημείων πρόσβασης, την τακτική ενημέρωση του λογισμικού, την εκτέλεση κάποιων λεπτομερών εξετάσεων και την υιοθέτηση αποτελεσματικής κρυπτογράφησης. Οι λύσεις αυτές αναλύονται διεξοδικά στην παρακάτω παράγραφο.

5.2.3.1 Ρύθμιση των σημείων πρόσβασης

Οι διαχειριστές των δικτύων πρέπει να ρυθμίζουν τα σημεία πρόσβασης, σύμφωνα με τις πολιτικές ασφάλειας και τις απαιτήσεις του κάθε συστήματος. Οι ενέργειες που θα πρέπει να εκτελούν κάθε φορά είναι οι εξής :

- **Αλλαγή των προκαθορισμένων συνθηματικών:** Κάθε συσκευή ασύρματου δικτύου έρχεται με τις προκαθορισμένες ρυθμίσεις της, μερικές από τις οποίες περιέχουν ευπάθειες ασφάλειας. Για παράδειγμα σε μερικά σημεία πρόσβασης δεν απαιτείται password (το πεδίο του password είναι κενό). Ο ρόλος ενός διαχειριστή είναι να αντικαθιστά την ρύθμιση αυτή με ένα "δυνατό" συνθηματικό (ένα τέτοιο συνθηματικό αποτελείται από 8 χαρακτήρες και άνω, και απαρτίζεται από έναν συνδυασμό γραμμάτων, αριθμών, ειδικών χαρακτήρων, κ.τ.λ.). Εάν οι απαιτήσεις ασφάλειας είναι ιδιαίτερα υψηλές, θα μπορούσε να χρησιμοποιηθεί μια γεννήτρια τυχαίων συνθηματικών.
- **Καθορισμός κατάλληλων κρυπτογραφικών ρυθμίσεων:** Οι ρυθμίσεις αυτές θα πρέπει να επιτρέπουν τη μέγιστη δυνατή κρυπτογράφηση που υποστηρίζει το προϊόν, και να εξαρτώνται από τις απαιτήσεις ασφάλειας του οργανισμού. Τυπικά, τα σημεία πρόσβασης έχουν μόνο μερικές κρυπτογραφικές ρυθμίσεις διαθέσιμες: είτε καμία, είτε κάποιο κοινό κλειδί μήκους 40 bits είτε κάποιο κοινό κλειδί μήκους 104 bits, με αυτή την κρυπτογράφηση να είναι η δυνατότερη. Η κρυπτογράφηση WEP, δεν παρουσιάζει προβλήματα απόδοσης στους υπολογιστές που πραγματοποιούν αυτή τη λειτουργία. Θα πρέπει όμως

να αναφερθεί ότι προϊόντα που χρησιμοποιούν κλειδιά μήκους 128 bits δεν είναι εφικτό να λειτουργούν με εκείνα που χρησιμοποιούν κλειδιά μήκους 104 bits.

- **Έλεγχος της επαναφοράς των λειτουργιών:** Αυτή η λειτουργία θέτει ένα σοβαρό πρόβλημα ασφάλειας, διότι επιτρέπει σε έναν κακόβουλο χρήστη να ακυρώσει τις ρυθμίσεις που έχουν γίνει από τους διαχειριστές του σημείου πρόσβασης, επιστρέφοντας το σημείο πρόσβασης στις αρχικές του ρυθμίσεις, οι οποίες μπορεί να είναι, για παράδειγμα, χωρίς κρυπτογράφηση ή χωρίς password κ.τ.λ. Η επαναφορά των αρχικών ρυθμίσεων του σημείου πρόσβασης μπορεί να επιτευχθεί με την τοποθέτηση και πίεση ενός αιχμηρού αντικειμένου στην τρύπα που χρησιμεύει για την λειτουργία αυτή. Κάτι τέτοιο θα μπορούσε να προκαλέσει ακόμα και την άρνηση εξυπηρέτησης, γιατί τα σημεία πρόσβασης μπορεί να τεθούν εκτός λειτουργίας, αφού στην περίπτωση της επαναφοράς μπορεί να χαθούν πληροφορίες όπως IP διευθύνσεις ή κλειδιά. Επομένως, για να αποφευχθούν τέτοιες ενέργειες από κακόβουλους χρήστες, τα σημεία πρόσβασης χρειάζονται φυσική προστασία.
- **Χρήση λιστών ελέγχου πρόσβασης με MAC διευθύνσεις:** Όπως γνωρίζουμε, μια MAC διεύθυνση είναι μια διεύθυνση υλικού που αναγνωρίζει μοναδικά κάθε υπολογιστή σε ένα δίκτυο. Πολλά σημεία πρόσβασης παρέχουν τη δυνατότητα πρόσβασης στο δίκτυο, συσκευών με συγκεκριμένες MAC διευθύνσεις, μέσω λιστών (MAC Access Control Lists - ACLs) οι οποίες είναι αποθηκευμένες σε αυτά. Αυτή η μέθοδος όμως δεν είναι ασφαλής, γιατί η MAC διεύθυνση μεταδίδεται στο δίκτυο μη κρυπτογραφημένη και, κάποιος μπορεί να την χρησιμοποιήσει ώστε να αποκτήσει πρόσβαση στο δίκτυο. Επομένως, η λύση αυτή θα πρέπει να χρησιμοποιείται σε συνδυασμό με άλλες και θα πρέπει μάλιστα να σημειωθεί ότι δεν προσφέρεται για μεσαίου και μεγάλου μεγέθους δίκτυα, εξ' αιτίας των πολλών συσκευών και της πολυπλοκότητας τους.
- **Αλλαγή του SSID:** Οι προκαθορισμένες ρυθμίσεις του SSID του σημείου πρόσβασης θα πρέπει να αλλάζουν, για την αποφυγή της εύκολης πρόσβασης. Αν και ένας καλά εξοπλισμένος αντίπαλος μπορεί να το βρει με διάφορους τρόπους, θα αποθαρρυνθούν με τον τρόπο αυτόν κακόβουλα άτομα με ελλιπείς γνώσεις.

- **Μεγιστοποίηση του διαστήματος μεταξύ των ραδιοσημάτων:** Τα πλαίσια ραδιοσημάτων (beacon frames) ανακοινώνουν την ύπαρξη του ασύρματου δικτύου. Αυτά μεταδίδονται από τα σημεία πρόσβασης σε κανονικά διαστήματα και επιτρέπουν σε έναν ασύρματο πελάτη να ρυθμίσει τις παραμέτρους που απαιτούνται για την πρόσβαση του σε ένα ασύρματο δίκτυο. Ρυθμίζοντας το διάστημα στη μεγαλύτερη τιμή του (συνήθως 67 δευτερόλεπτα), γίνεται πιο δύσκολη η ακούσια ανίχνευση ενός ασύρματου δικτύου, εφόσον το σημείο πρόσβασης δεν εκπέμπει πλέον το ίδιο συχνά.
- **Αλλαγή των προκαθορισμένων κρυπτογραφικών κλειδιών:** Ο κατασκευαστής του σημείου πρόσβασης μπορεί να παρέχει ένα ή περισσότερα κλειδιά για shared-key αυθεντικοποίηση, μεταξύ μιας συσκευής που θέλει να αποκτήσει πρόσβαση στο δίκτυο και του σημείου πρόσβασης. Οι προκαθορισμένες τιμές πρέπει να αλλαχθούν, και μια καλή πολιτική είναι να αλλάζουν συχνά και ιδιαίτερα όταν συμβαίνουν αλλαγές προσωπικού στον οργανισμό.
- **Χρήση SNMP:** Εάν δεν απαιτείται η χρήση του SNMP σε ένα δίκτυο καλό είναι να απενεργοποιείται η λειτουργία του. Αν αυτό πρέπει να χρησιμοποιηθεί συνιστάται η χρήση της έκδοσης 3, SNMPv3, η οποία περιέχει μηχανισμούς που παρέχουν ενισχυμένη ασφάλεια, σε αντίθεση με τις προηγούμενες δύο εκδόσεις που παρέχουν ελαφρά αυθεντικοποίηση. Η προκαθορισμένη τιμή του community string που έχουν οι πράκτορες του SNMP είναι συνήθως **"public"** με δικαιώματα **"read"** ή **"read and write"**. Εάν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση στο σημείο πρόσβασης με δικαιώματα "read and write" θα μπορούσε να γράψει δεδομένα σε αυτό, προκαλώντας προβλήματα. Γι' αυτό, καλό είναι τα δικαιώματα να είναι σε τιμή **"read only"**, όπου και αν αυτό απαιτείται.
- **Αλλαγή του προκαθορισμένου καναλιού:** Οι κατασκευαστές χρησιμοποιούν συνήθως προκαθορισμένα κανάλια στα σημεία πρόσβασης, με αποτέλεσμα να υπάρξει η πιθανότητα παρεμβολής μεταξύ δύο σημείων πρόσβασης δύο διαφορετικών δικτύων που βρίσκονται σε κοντινές τοποθεσίες. Επειδή η παρεμβολή αυτή μπορεί να προκαλέσει άρνηση εξυπηρέτησης, οι διαχειριστές θα πρέπει να εξετάζουν εάν υπάρχουν τυχόν πηγές ραδιοπαρεμβολών, και να αποφασίζουν για την τοποθεσία και την ακτίνα κάλυψης των σημείων

πρόσβασης, καθώς και για την ανάθεση των κατάλληλων ραδιοκαναλιών σε κάθε σημείο πρόσβασης.

- **Χρήση DHCP:** Ένας DHCP (Dynamic Host Control Protocol) server αναθέτει αυτόματα IP διευθύνσεις σε κάθε σταθμό εργασίας. Το πρόβλημα είναι ότι ένας κακόβουλος χρήστης με ένα φορητό υπολογιστή εξοπλισμένο με μια ασύρματη κάρτα, θα μπορούσε εύκολα να κερδίσει πρόσβαση στο δίκτυο, αφού ο DHCP server δε θα ξέρει απαραίτητα ποιες συσκευές έχουν πρόσβαση σε αυτό. Έτσι θα του ανέθετε μια έγκυρη IP διεύθυνση. Σε τέτοιες περιπτώσεις καλό θα ήταν να απενεργοποιηθεί το πρωτόκολλο DHCP και να χρησιμοποιηθούν στατικές διευθύνσεις στο ασύρματο δίκτυο, αν αυτό είναι δυνατό εξ' αιτίας του μεγέθους του.

5.2.3.2 Αναβαθμίσεις και Διορθώσεις Λογισμικού

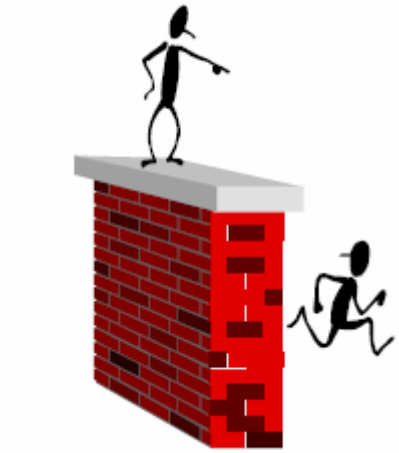
Οι προμηθευτές προσπαθούν διαρκώς να διορθώσουν τυχόν ευπάθειες, όταν αυτές εντοπιστούν, σε υλικό και λογισμικό. Οι διαχειριστές των δικτύων πρέπει να επικοινωνούν τακτικά με τους προμηθευτές για να ελέγχουν εάν υπάρχουν διαθέσιμες διορθώσεις ή αναβαθμίσεις οι οποίες θα πρέπει να εφαρμοστούν κατάλληλα. Επιπλέον, οι διαχειριστές πρέπει να γραφτούν στις λίστες με τα e-mail πελατών που διαθέτουν οι προμηθευτές, μέσω των οποίων θα ενημερώνονται και θα καθοδηγούνται για γνωστές ευπάθειες και επιθέσεις.

5.2.3.3 Αυθεντικοποίηση

Γενικά, οι αποτελεσματικές μέθοδοι αυθεντικοποίησης είναι ένας τρόπος να εμποδίζονται οι μη εξουσιοδοτημένοι χρήστες να προσπελάζουν ένα δίκτυο. Οι τεχνικές αυθεντικοποίησης περιλαμβάνουν την χρήση ονόματος χρήστη (user name) και κωδικού πρόσβασης (password), έξυπνων καρτών (smart cards), βιομετρίας, υποδομής δημοσίου κλειδιού (public key infrastructure – PKI), ή έναν συνδυασμό από όλα τα παραπάνω.

Όταν η αυθεντικοποίηση βασίζεται στην χρήση ονόματος χρήστη και κωδικού πρόσβασης, είναι σημαντικό να καθορίζεται, το ελάχιστο μήκος, οι απαιτούμενοι χαρακτήρες, και η λήξη του κωδικού πρόσβασης. Οι έξυπνες κάρτες, η βιομετρία και το PKI θα αναλυθούν περισσότερο σε παρακάτω παραγράφους.

5.2.3.4 Τείχη Ασφαλείας (Firewalls)



Τα προσωπικά firewalls προσφέρουν ένα είδος προστασίας εναντίον ορισμένων επιθέσεων. Είναι λύσεις λογισμικού στο μηχάνημα ενός πελάτη και διαχειρίζονται από αυτόν, προσδιορίζοντας την επιθυμητή πολιτική ασφάλειας. Συνήθως χρησιμοποιούνται από χρήστες, οι οποίοι έχουν πρόσβαση σε δημόσια δίκτυα όπως αεροδρόμια, ξενοδοχεία κ.τ.λ, όπου μπορεί να υπάρχουν, για παράδειγμα, μη νόμιμα σημεία πρόσβασης εγκατεστημένα.

5.2.3.5 Συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems – IDS)

Ένα τέτοιο σύστημα αποτελεί ένα καλό εργαλείο για να προσδιορισθεί αν κάποιος μη εξουσιοδοτημένος χρήστης προσπαθεί να κερδίσει πρόσβαση σε ένα δίκτυο. Μπορεί να είναι τριών ειδών: **host-based, network-based και hybrid** (υβριδικά, τα οποία συνδυάζουν τις δυνατότητες των δύο προηγούμενων ειδών). Ένα **host-based** σύστημα μπορεί να είναι εγκατεστημένο, για παράδειγμα, σε έναν server βάσης δεδομένων και να παρακολουθεί το σύστημα για ύποπτη συμπεριφορά, όπως επαναλαμβανόμενες αποτυχημένες απόπειρες εισόδου ενός χρήστη, ή αλλαγές στα δικαιώματα κάποιων αρχείων. Ένα **network-based** σύστημα παρακολουθεί, σε ένα τοπικό δίκτυο, την κίνηση των πακέτων σε πραγματικό χρόνο για να προσδιορίσει αν η κίνηση συμφωνεί με κάποια ήδη γνωστή επίθεση, που υπάρχει στη βάση δεδομένων του συστήματος.

5.2.3.6 Εκτιμήσεις Ασφάλειας

Οι εκτιμήσεις ασφάλειας είναι σημαντικό εργαλείο για να ελέγχεται η εικόνα της ασφάλειας ενός ασύρματου δικτύου. Οι διαχειριστές του δικτύου μπορούν, με τη χρήση προγραμμάτων παρακολούθησης της κίνησής του, να ελέγξουν αν οι ασύρματες συσκευές εκπέμπουν σωστά, να δουν αν υπάρχουν εγκατεστημένα μη εξουσιοδοτημένα σημεία πρόσβασης, κ.τ.λ.

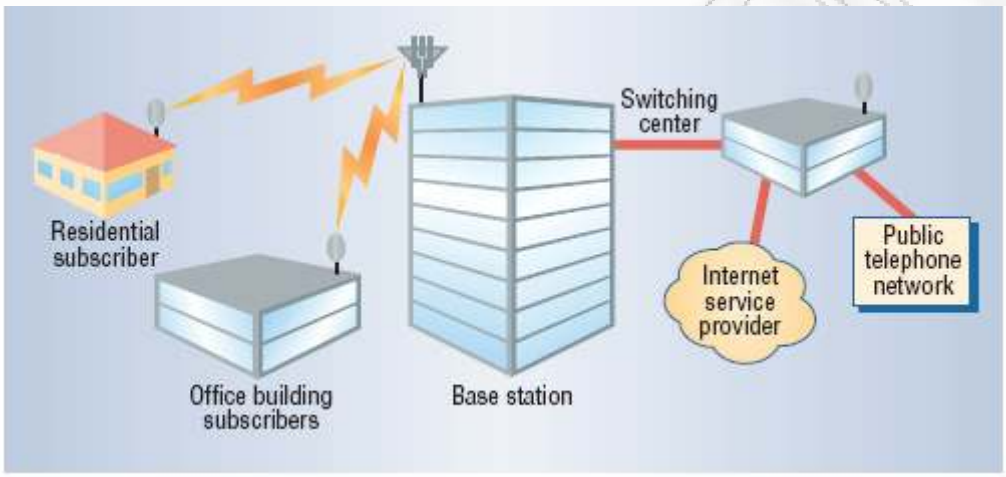
6. Μελλοντικές τάσεις - Το πρότυπο IEEE 802.16 (WiMax)

6.1 Τι είναι το WiMax

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16 γνωστό και σαν WiMAX, ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση (με σταθερούς ρυθμούς) ευρείας ζώνης. Όπως συμβαίνει με τα πρότυπα της σειράς 802 για ασύρματα τοπικά δίκτυα, έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες ρυθμίσεις. Το WiMax είναι μια νέα τεχνολογία, ένα βήμα μπροστά από το Wi-Fi, που παρέχει ασύρματη ευρυζωνική πρόσβαση υψηλών ταχυτήτων σε μεγάλες αποστάσεις. Είναι σαφώς καλύτερο από το Wi-Fi και μπορεί να καλύψει μεγαλύτερες αποστάσεις μετάδοσης. Πλέον ένας φορητός υπολογιστής μπορεί να συνδυάζει τις ιδιότητες κινητού τηλεφώνου και ραδιοφωνικού πομπού: θα πιάνει «παντού» και θα εξασφαλίζει επικοινωνία με και από κάθε γωνιά του πλανήτη.

Τα αρχικά της λέξης WiMax προκύπτουν από τις λέξεις World Interoperability for Microwave Access και είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ταυτοποιεί συγκεκριμένο εξοπλισμό υποστηριζόμενος από εταιρίες (Intel…) προσπαθώντας να προωθήσει το πρότυπο 802.16 σε κάθε ευρυζωνικής ασύρματης πρόσβασης σύστημα. Για να γίνουμε λίγο πιο σαφής το WiMAX δεν είναι ένα πρότυπο αλλά ένα εμπορικό όνομα που αναφέρεται σε κάθε σύστημα και εφαρμογή που χρησιμοποιεί το πρότυπο 802.16.Το να ταυτοποιείται λοιπόν ένα προϊόν με το όνομα WiMAX σημαίνει ότι έχει κατασκευαστεί με βάση το πρότυπο 802.16 και έτσι εξασφαλίζεται η συμβατότητα και η διαλειτουργικότητα (interoperability) στον BWA εξοπλισμό.

Αρχικά, το όραμα των υπερασπιστών του WiMax, όπως φαίνεται και στην παρακάτω εικόνα, ήταν ότι οι μεταφορείς θα εγκαταστήσουν πομποδέκτες στεγών ως σταθμούς βάσεων συνδεδεμένους με το Διαδίκτυο. Κάθε ένας σταθμός βάσεων θα μπορούσε να χρησιμοποιήσει την τεχνολογία WiMax για να στείλει και να λάβει δεδομένα από και προς τις σταθερές κεραίες συνδρομητών, που είναι τοποθετημένες στις στέγες ή στους εξωτερικούς τοίχους.



Εικόνα 6.1

Αντίθετα με άλλα ασύρματα δίκτυα, τα οποία επιτρέπουν μεταδόσεις μόνο με ένα φάσμα συχνότητας, το WiMax επιτρέπει τη μεταφορά δεδομένων με πολλαπλά, ευρέα φάσματα συχνότητας. Αυτό βοηθάει πάρα πολύ, γιατί το να υπάρχουν πολλά φάσματα, μεγιστοποιεί τη δυνατότητα της τεχνολογίας να μεταδώσει πέρα από τις συχνότητες άλλων ασύρματων εφαρμογών.

Το WiMax αναμένεται να επιτρέψει αληθινές ευρυζωνικές ταχύτητες πέρα από τα ασύρματα δίκτυα με κόστος που θα καταστήσει ενεργή την υιοθέτηση μαζικής αγοράς. Το WiMax είναι το μόνο ασύρματο πρότυπο που σήμερα έχει τη δυνατότητα να παραδώσει τις αληθινές ευρυζωνικές ταχύτητες και βοηθάει στο να γίνει το όραμα της κυρίαρχης συνδετικότητας μια πραγματικότητα.

Τα *βασικά πλεονεκτήματα* των συστημάτων που βασίζονται στο πρότυπο 802.16 είναι τα εξής:

•Η ικανότητα γρήγορης παροχής υπηρεσιών ακόμα και σε περιοχές πολύ απομακρυσμένες όπου η εγκατάσταση ενσύρματων δικτύων θα ήταν εξαιρετικά δύσκολη.

•Αποφυγή μεγάλου κόστους εγκατάστασης.

•Η ικανότητα υπέρβασης των φυσικών περιορισμών που υπάρχουν στην ενσύρματη δικτύωση.

Συνοψίζοντας τα παραπάνω θα μπορούσαμε να πούμε ότι το 802.16 συνιστά ένα πολύ ευέλικτο και οικονομικό πρότυπο το οποίο μπορεί να καλύψει τις αδυναμίες της ενσύρματης δικτύωσης και επιπλέον να παρέχει νέες υπηρεσίες και προϊόντα.

6.1.1 Τα κύρια χαρακτηριστικά του

Αρχικά βασικό χαρακτηριστικό του προτύπου είναι η **διεκπαιρεωτική ικανότητα (throughput).** Το πρότυπο IEEE 802.16 επιτυγχάνει πολύ μεγάλη διεκπαιρεωτική ικανότητα, ακόμα και σε μεγάλες αποστάσεις αφού έχει ένα πολύ μεγάλο φάσμα εκπομπής που είναι ιδιαίτερα ανθεκτικό σε αντανακλάσεις του σήματος κατά τη διάρκεια της διαδρομής του.

Επίσης πολύ σημαντικό για τη διάδοση του είναι η **κλιμακοσιμότητα (scalability)** ή καλύτερα επεκτασιμότητα. Για να μπορεί να γίνει εύκολος και επεκτάσιμος σχεδιασμός κυψελών (cells) επικοινωνίας σε επιτρεπόμενες και μη συχνοτικές μπάντες ,το πρότυπο IEEE 802.16 υποστηρίζει ευέλικτα από την άποψη εύρους ζώνης κανάλια επικοινωνίας. Για παράδειγμα αν σε κάποιο χειριστή ανατεθεί συχνοτικό φάσμα τον 20 MHz, τότε αυτός μπορεί να χωρίσει το φάσμα σε δύο κομμάτια των 10 MHz ή ακόμα σε τέσσερα κομμάτια των 5 MHz. Συγκεντρώνοντας έτσι όλη την ενέργεια σε ένα πολύ μικρό φάσμα συχνοτήτων ο χειριστής μπορεί να αυξήσει τον αριθμό των χρηστών επιτυγχάνοντας παράλληλα μεγάλο βεληνεκές και

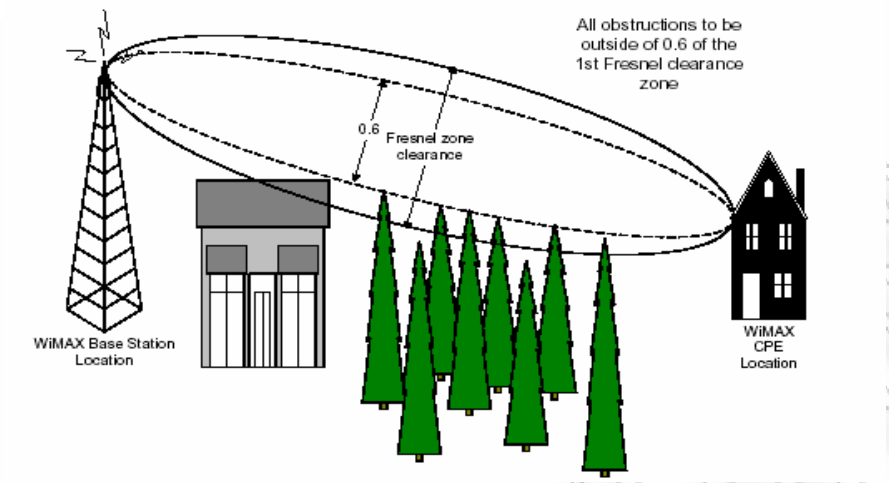
throughput. Για να κλιμακώσει ακόμα περισσότερο την εμβέλεια του σήματος, ο χειριστής μπορεί να χωρίσει ακόμα περισσότερο το φάσμα συχνοτήτων δημιουργώντας απομόνωση μεταξύ των κεραιών των σταθμών βάσης.

Ένα άλλο εξίσου σημαντικό χαρακτηριστικό του WiMax είναι η **εμβέλεια (coverage).** Το πρότυπο IEEE 802.16 κατασκευάζεται έτσι ώστε να υποστηρίζει τεχνολογίες που αυξάνουν την εμβέλεια του σήματος όπως *mesh τοπολογίες* και έξυπνες κεραίες. Αξίζει να σημειώσουμε ότι *mesh τοπολογίες* είναι αυτές οι τοπολογίες δικτύου όπου κάθε κόμβος συνδέεται άμεσα με κάθε άλλο κόμβο του δικτύου. Όσο λοιπόν η ράδιο-τεχνολογίες βελτιώνονται και το κόστος μειώνεται, μεγαλώνει και η δυνατότητα αύξησης της εμβέλειας και του throughput με τη χρήση πολλαπλών κεραιών καθώς ενθαρρύνεται και η εξάπλωση της εμβέλειας σε περιοχές που παλαιότερα ήταν αδύνατο να εξαπλωθεί.

Η **παροχή υψηλής ποιότητας υπηρεσιών (QoS ή Quality of service)** όπως είναι η μεταφορά φωνής, είναι εξαιρετικά σημαντική για την υιοθέτηση και εξάπλωση του προτύπου. Για αυτό ακριβώς το λόγο το υποπρότυπο 802.16a συμπεριλαμβάνει κάποια ιδιαίτερα χαρακτηριστικά που κάνουν δυνατή τη μεταφορά φωνής και βίντεο αφού για να είναι εφικτή αυτή η μεταφορά χρειάζεται ένα χαμηλού φόρτου δίκτυο.

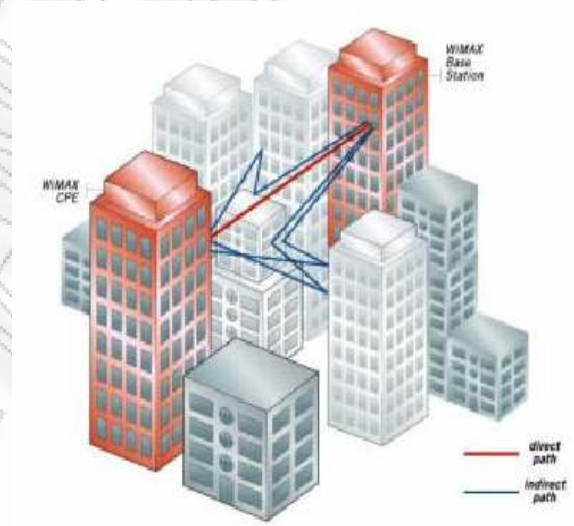
Επίσης κάτι άλλο που χαρακτηρίζει το πρότυπο IEEE 802.16 είναι τα κανάλια ραδιοκυμάτων ασύρματης επικοινωνίας, στα οποία εκπέμπονται οι συχνότητες. Αυτά διαχωρίζονται σε LOS (Line of sight) και σε NLOS (Non line of sight).

Σε μια σύνδεση LOS ένα σήμα ταξιδεύει σε μία άμεση και χωρίς εμπόδια διαδρομή από το πομπό στο δέκτη. Μια σύνδεση LOS, απαιτεί το περισσότερο μέρος της ζώνης Frensel να μην παρεμποδίζεται από κάτι. Αν δεν ισχύει αυτό ο παράγοντας τότε η ισχύς του σήματος ελαττώνεται σημαντικά. Γενικά, γνωρίζουμε ότι η ζώνη Frensel καλύπτει τη ζώνη οπτικής επαφής μεταξύ πομπού και δέκτη. Τα παραπάνω φαίνονται καλύτερα στην παρακάτω εικόνα. Αξίζει να σημειώσουμε ότι η Frensel zone clearance που αναφέρεται στο Εικόνα, εξαρτάται από τη συχνότητα του σήματος και βέβαια από την απόσταση μεταξύ πομπού και δέκτη.



Εικόνα 6.2

Σε μια NLOS σύνδεση ένα σήμα φθάνει στο δέκτη μέσω αντανακλάσεων και διασποράς . Το σήμα αυτό που φτάνει στο δέκτη αποτελείται από σήμα που έφτασε άμεσα από το πομπό, σήμα που έφτασε από πολλαπλά μονοπάτια μέσω αντανάκλασης, διασπαρμένη ενέργεια και μονοπάτια όπου συνέβη περίθλαση. Αυτά τα σήματα έχουν διαφορετική καθυστέρηση διάδοσης, πολώσεις, και σταθερότητα σχετικά με το σήμα που φτάνει άμεσα. Το φαινόμενο αυτό του πολλαπλού μονοπατιού που περιγράφουμε μπορεί να ευθύνεται και για την αλλαγή της πολικότητας του σήματος. Στην παρακάτω εικόνα φαίνεται ένα παράδειγμα μιας NLOS μετάδοσης.



Εικόνα 6.3

Γενικά, αν και υπάρχουν προβλήματα, η NLOS μετάδοση έχει αρκετά πλεονεκτήματα έναντι της LOS αφού είναι πιο ευέλικτη, απαιτεί πολύ μικρότερες κεραίες. Η ύπαρξη μικρών κεραιών είναι πολύ μεγάλης σημασία σε ασύρματα δίκτυα με κυψελοειδής δομές και αυτό συμβαίνει γιατί με μικρές κεραίες μειώνονται οι παρεμβολές μεταξύ των γειτονικών κυψελών. Βέβαια η NLOS μετάδοση μειώνει το κόστος εγκατάσταση σε απομακρυσμένες περιοχές όπου η εγκατάσταση πολλών κεραιών είναι αρκετά δύσκολη.

6.1.2 Χρήσεις του WiMax, τοπολογίες και ρυθμοί μετάδοσης

Λόγω των μεγάλων αποστάσεων που καλύπτει και ταυτόχρονα τους υψηλούς ρυθμούς μετάδοσης που μπορεί να παρέχει, το πρότυπο WiMAX βρίσκει πολλές εφαρμογές, λύνοντας σημαντικά προβλήματα που απασχολούσαν του τεχνικούς δικτύων σήμερα. Τρεις είναι οι βασικότερες χρήσεις του:

Δίκτυο κορμού στα κυψελωτά συστήματα κινητής τηλεφωνίας. Η εισαγωγή του προτύπου αυτού αναμένεται να μειώσει σημαντικά το κόστος εξάπλωσης των δικτύων κινητής τηλεφωνίας μιας και αποτελεί μια οικονομικότερη πρόταση, αν συγκριθεί με την οπτική ίνα, για τις εταιρίες κινητής τηλεφωνίας. Εξασφαλίζει ταυτόχρονα αξιοπιστία και υψηλούς ρυθμούς μετάδοσης που απαιτούν τα δίκτυα κορμού των κινητών δικτύων επικοινωνιών.

Broadband on Demand. Παρέχει υψηλούς ρυθμούς μετάδοσης κάνοντας εφικτή τη χρήση της τεχνολογίας για εφαρμογές πραγματικού χρόνου κάτι που με το πρότυπο IEEE 802.11 σε μεγάλες αποστάσεις δεν ήταν εφικτό.

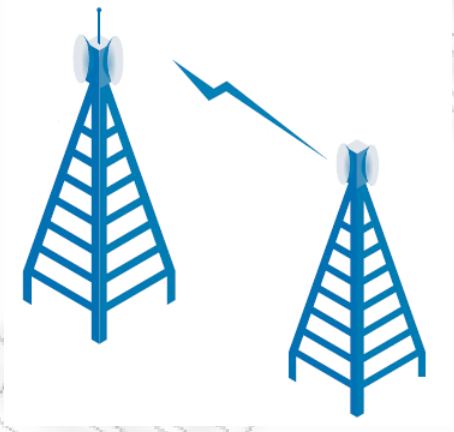
Παρέχει κάλυψη σε περιοχές που είναι αδύνατο τα καλυφθούν με χρήση χαλκού ή οπτικής ίνας. Μπορεί να χρησιμοποιηθεί σαν συμπλήρωμα δικτύων οπτικών ινών σε τμήματα του εδάφους στα οποία το κόστος εγκατάστασης και συντήρησης δικτύων οπτικών ινών είναι απαγορευτικό.

Το WiMAX έχει δύο κύριες εφαρμογές: οι σταθερές εφαρμογές WiMAX είναι **Point-to-Multipoint** επιτρέποντας την ευρυζωνική πρόσβαση στα σπίτια και τις επιχειρήσεις, ενώ κινητό WiMax προσφέρει την πλήρη κινητικότητα των

κυψελοειδών δικτύων με τις αληθινές ευρυζωνικές ταχύτητες. Το WiMAX σχεδιάστηκε κατά βάση ώστε να καλύπτει κυρίως Point-to-Multipoint (PTM) συνδέσεις χωρίς ωστόσο να αποκλείεται και η χρήση του για point to point συνδέσεις. Η διαμόρφωση η οποία χρησιμοποιείται ονομάζεται OFDM (Orthogonal Frequency Division Multiplexing). Πρόκειται για μια πολύ ανθεκτική διαμόρφωση σε ότι αφορά το φαινόμενο της πολυδιόδευσης ειδικότερα στις συχνότητες πάνω των 2 GHz όπου το πρότυπο χρησιμοποιεί. Συγκεκριμένα, αυτή η διαμόρφωση έχει πλεονεκτήματα στη ρυθμοαπόδοση, στη λανθάνουσα κατάσταση, τη φασματική αποδοτικότητα και την προηγμένη υποστήριξη κεραιών κάνοντάς το ικανό να παρέχει την υψηλότερη απόδοση από τις σημερινές ευρείες ασύρματες τεχνολογίες περιοχής.

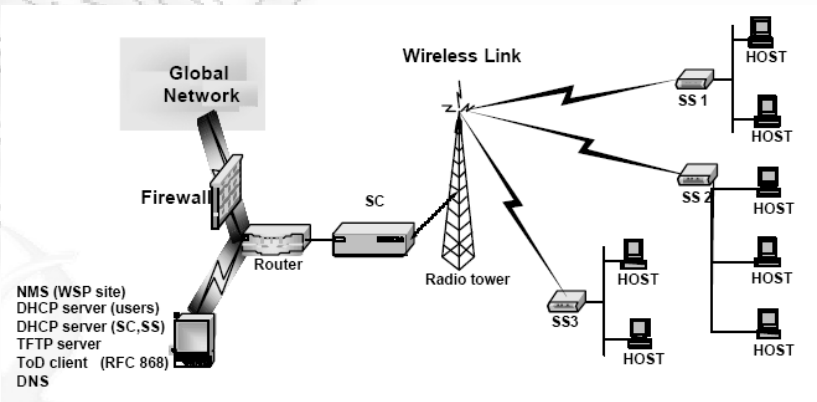
Παρακάτω παρουσιάζονται γραφικά οι point to point και οι Point-to-Multipoint συδέσεις:

Point-to-Point



Εικόνα 6.5

Point-to-Multipoint



Εικόνα 6.6

Το πρότυπο IEEE 802.16 σχεδιάστηκε ώστε να λειτουργεί σε μια ευρεία μπάντα συχνοτήτων η οποία εκτείνεται από 2 ως 66 GHz. Υποστηρίζει ταχύτητες μετάδοσης ως και 72 Mbps στον αέρα ενώ η πραγματική ταχύτητα στο Ethernet υπολογίζεται στα 50 Mbps. Οι αποστάσεις που μπορεί να καλυφθούν ξεπερνούν τα 50 Km σε συνθήκες οπτικής επαφής. Οι ταχύτητες μετάδοσης του προτύπου εξαρτώνται από την εκάστοτε ψηφιακή διαμόρφωση που χρησιμοποιείται. Συνήθεις διαμορφώσεις είναι η 64 QAM η οποία μπορεί να εξασφαλίσει και τη μεγαλύτερη ταχύτητα μετάδοσης, η 16 QAM και η QPSK η οποία μπορεί να εξασφαλίσει μεγάλη κάλυψη του συστήματος.

6.2 Ασφάλεια του WiMax

Την **ασφαλή μετάδοση** των δεδομένων στο WiMAX αναλαμβάνει ο αλγόριθμος κρυπτογράφησης DES (Data Encryption Standard, Πρότυπο Κωδικοποίησης Δεδομένων) και συγκεκριμένα μια παραλλαγή του αλγορίθμου ο Triple DES. Το DES αναπτύχθηκε το 1970 από το Αμερικανικό Εθνικό Γραφείο Προτύπων. Η βασική ιδέα ήταν η ανάπτυξη ενός αλγόριθμου κρυπτογράφησης που θα μπορούσε να χρησιμοποιηθεί (και να βελτιωθεί) από διάφορες εταιρείες ή οργανισμούς. Το DES ανήκει στην οικογένεια των συμμετρικών αλγόριθμων και κάνει χρήση κλειδιών με μήκος 56 bit. Ο "κλασικός" αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, μπορούμε να αυξήσουμε σημαντικά την ασφάλειά του. Με τη μέθοδο Triple - DES, για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά κατά συνέπεια αυτό το πρότυπο αυξάνει την ασφάλεια του DES, καθώς χρησιμοποιεί τρία κλειδιά κρυπτογράφησης.

6.3 Εφαρμογές του WiMax

Γενικά υπάρχουν δύο κύριες κατηγορίες εφαρμογών του WiMax: οι σταθερές εφαρμογές, οι οποίες επιτρέπουν την ευρυζωνική πρόσβαση στα σπίτια και τις επιχειρήσεις και οι κινητές εφαρμογές WiMax που προσφέρουν την πλήρη κινητικότητα των κυψελοειδών δικτύων στις αληθινές ευρυζωνικές ταχύτητες.

Πιο συγκεκριμένα, όμως, το πρότυπο 802.16 έχει εξαιρετικές εφαρμογές και θα δώσει πολλές λύσεις σε υπάρχοντα προβλήματα της βιομηχανίας, μερικές από τις οποίες αναφέρονται περιληπτικά παρακάτω:

Κυψελοειδής μετάδοση (backhaul): Οι παροχείς της κύριας αρτηρίας (backbone) του internet στην Αμερική είναι αναγκασμένοι να μισθώσουν σε τρίτους παροχείς υπηρεσιών (ISP's) γραμμές του δικτύου μια συμφωνία που κάνει την ενσύρματη σύνδεση στο internet για τους χρήστες αρκετά προσιτή. Αυτό έχει ως αποτέλεσμα το 20% των κυψελών που εξυπηρετούν την ασύρματη επικοινωνία να μένουν αχρησιμοποίητες. Στην Ευρώπη όμως δεν συμβαίνει αυτό, πράγμα που σημαίνει ότι πρέπει να βρεθούν εναλλακτικές λύσεις. Το 802.16a αποτελεί μία εξαιρετική λύση σε εταιρίες παροχής τέτοιων υπηρεσιών που τώρα δε θα είναι αναγκασμένες να μισθώνουν ενσύρματες γραμμές αλλά μπορούν με τη χρήση των ασύρματων κυψελών να παρέχουν φτηνό internet στους χρήστες.

Άρση των περιορισμών των καλωδίων: Υπάρχουν κάποιοι φυσικοί περιορισμοί στις καλωδιακές και DSL τεχνολογίες οι οποίοι αποτρέπουν πολλούς πελάτες να συνδεθούν με το δίκτυο. Η γνωστή DSL σύνδεση μπορεί να φτάσει μέχρι περίπου τρία μίλια μακριά από το κεντρικό δρομολογητή πράγμα που σημαίνει ότι πολλές αστικές και προαστιακές περιοχές δεν μπορούν να εξυπηρετηθούν από DSL τεχνολογία. Η χρήση του καλωδίου έχει επίσης και τους περιορισμούς της. Πολλά παλιά ενσύρματα δίκτυα δεν είναι εξοπλισμένα με κανάλι επιστροφής και έτσι ο εκσυγχρονισμός αυτών μπορεί να είναι ιδιαίτερα ακριβός. Επίσης η επέκταση της

καλωδιακής εγκατάστασης είναι αρκετά δύσκολη και ακριβή ειδικά σε περιοχές στις οποίες δεν υπάρχει μεγάλη «πυκνότητα» χρηστών. Η προτυποποίηση της ασύρματης δικτύωσης με τη δημιουργία του 802.16 μπορεί να λύσει όλα τα παραπάνω προβλήματα. Επίσης μπορεί να παρέχει επιπλέον μεγάλο bandwidth, ευελιξία και χαμηλό κόστος.

Επέκταση της ασύρματης ευρυζωνικότητας: Το πρότυπο 802.16 μπορεί να χρησιμοποιηθεί στη μεγαλύτερη αξιοποίηση του 802.11 . Τα σπίτια ή τα γραφεία τα οποία έχουν μικρά LAN τα οποία χρησιμοποιούν το 802.11 μπορεί να γίνουν σταθμοί για ένα 802.16 WAN ειδικότερα σε περιοχές που η χρήση καλωδίων είναι εξαιρετικά δύσκολη. Εδώ μπαίνει ξανά το θέμα σύνδεσης στο internet ειδικότερα για εταιρίες οι οποίες χρειάζεται να μετακινούνται. Επίσης, η χρήση του 802.16 μας απαλλάσσει από το πρόβλημα της εγκατάστασης καλωδιώσεων σε κτίρια τα οποία δεν είχε γίνει καμία προηγούμενη τέτοια εγκατάσταση και με πολύ χαμηλό κόστος. Επιπλέον μας δίνεται το πλεονέκτημα να διαμορφώσουμε τη σύνδεση μας σε πιο αργή ή πιο γρήγορη χωρίς καμία επιπλέον εγκατάσταση.

*Απομακρυσμένες περιοχές:*Η ασύρματη τεχνολογία internet με τη χρήση του 802.16 είναι μία φυσική επιλογή για απομακρυσμένες περιοχές. Σε αυτή τη κατεύθυνση έχουν αρχίσει να δουλεύουν πολλές κυβερνήσεις σε συνεργασία με WISP. Σύμφωνα με πρόσφατα στατιστικά περισσότεροι από 2.500 WISPs που εκμεταλλεύονται το χωρίς άδεια φάσμα (exempt-licensed spectrum) έχουν ανοιχτεί σε περισσότερες από 6.000 αγορές στις Ηνωμένες Πολιτείες Αμερικής. Γενικά όμως σε διεθνές επίπεδο οι περισσότερες επεκτάσεις γίνονται στο νόμιμο φάσμα συχνοτήτων σε πελάτες που απαιτούν καλή ποιότητα μεταφοράς φωνής παρά δεδομένων. Αυτό συμβαίνει κυρίως σε κάποιες περιοχές που δεν υπάρχει ενσύρματο δίκτυο.

6.4. Υποπρότυπα IEEE 802.16

IEEE 802.16 a

Η ανάγκη για επικοινωνία μεταξύ σταθμών που δεν βρίσκονται σε οπτική επαφή ήταν το κίνητρο για τη δημιουργία του υποπροτύπου IEEE 802.16 a. Τον Ιανουάριο του 2003 το πρότυπο επεκτάθηκε ώστε να λειτουργεί και στις συχνότητες από 2-11 GHz όπου στις συχνότητες αυτές ήταν δυνατή η δημιουργία συνδέσεων χωρίς οπτική επαφή πομπού - δέκτη. Το υποπρότυπο το οποίο περιγράφει τη διαδικασία αυτή ονομάστηκε IEEE 802.16 a. Τα πρώτα προϊόντα WiMAX τα οποία σήμερα είναι διαθέσιμα στην αγορά ακολουθούν στην μεγαλύτερή τους πλειοψηφία το υποπρότυπο αυτό

IEEE 802.16 b

Το πρότυπο 802.16b ήταν από τα πρώτα που δημιουργήθηκαν. Η δημιουργία του υποπροτύπου αυτού στόχευε στις εφαρμογές εκτός νόμιμης (licensed) περιοχής στις συχνότητες 5-6GHz.Το 802.16b παρέχει QoS διαβεβαιώντας ότι θα υπάρχει προτεραιότητα στη μετάβαση πραγματικού χρόνου εικόνας και ήχου καθώς επίσης παρέχει διαφοροποιημένα επίπεδα υπηρεσίας σε διαφορετικού τύπου μετακίνησης δεδομένων.

IEEE 802.11 c

Όπως έχει ήδη αναφερθεί, στην αρχική του έκδοση το πρότυπο IEEE 802.16 λειτουργούσε στην ζώνη συχνοτήτων 10-66 GHz. Στις παραπάνω συχνότητες η επικοινωνία μεταξύ δύο σταθμών επιτυγχάνεται μόνο όταν οι σταθμοί αυτοί βρίσκονται σε συνθήκες οπτικής επαφής. Η παραπάνω διαδικασία περιγράφεται στο υποπρότυπο IEEE 802.11 c.

IEEE 802.16 d.

Καθώς η πολυπλοκότητα των εφαρμογών που διαδίδονται πάνω από ένα ασύρματο δίκτυο ολοένα και αυξάνει, η ποιότητα υπηρεσίας πάνω από τέτοια δίκτυα γίνεται ένας πολύ καθοριστικός παράγοντας για την ποιότητα της επικοινωνίας. Για παράδειγμα, η μετάδοση video σε πραγματικό χρόνο απαιτεί από το δίκτυο συνθήκες πολύ χαμηλής καθυστέρησης μετάδοσης. Για αυτό το λόγο, προκειμένου να ικανοποιηθεί η ανάγκη για ποιότητα υπηρεσίας ορίστηκε το υποπρότυπο IEEE 802.16 d.

IEEE 802.16 e

Το υποπρότυπο **IEEE 802.16 e** εισάγει και περιγράφει την έννοια της κινητικότητας των χρηστών από ένα base station σε άλλο. Στο υποπρότυπο αυτό ορίζεται ότι ένας κινητός χρήστης μπορεί να συνεχίσει να εξυπηρετείται από το δίκτυο ακόμα και αν κινείται με ταχύτητες οι οποίες προσεγγίζουν τα 120 Km / h . Ωστόσο η παραπάνω τιμή είναι ενδεικτική - πειραματική, καθώς μέχρι τη στιγμή αυτή δεν υπάρχει κάποιο διαθέσιμο προϊόν στην αγορά συμβατό με το IEEE 802.16 e υποπρότυπο που να πιστοποιεί την προαναφερθείσα τιμή.

IEEE 802.16-2004

Η ένωση των υποπροτύπων IEEE 802.11 a, c, d όρισε το πρότυπο IEEE 802.16-2004 το οποίο περιγράφει τη συνολική λειτουργικότητα των επιμέρους υποπροτύπων που προαναφέρθηκαν για συχνότητες λειτουργίας 2-66 GHz.

Το πρότυπο IEEE 802.26-2004 ορίζει την επικοινωνία χρηστών οι οποίοι βρίσκονται μέσα σε ένα κελί το οποίο καλύπτεται από ένα base station . Όταν κάποιος χρήστης κινηθεί σε περιοχή που βρίσκεται εκτός περιοχής κάλυψης του base station η σύνδεση χάνεται.

6.5 Σύγκριση WiMax με άλλες ασύρματες τεχνολογίες

	Ταχύτητα (Mbps)	Εμβέλεια	Συχνότητα	Διασύνδεση	Κατάσταση	Υποστ.
Bluetooth	1 Mbps	10 m	2.4 GHz	Καμία	Διαθέσιμο	Erricson IBM, Intel, Toshiba, Nokia, Motorola
HomeRF	2 Mbps	50 m	2.4 GHz	Ethernet	Διαθέσιμο	Promix, Intel,HP, 3COM, Motorola
HiperLAN Type 1	24 Mbps	50 m	5 GHz	Ethernet	Διαθέσιμο	ETSI, Promix, HP,IBM, Xircom, Nokia
HiperLAN Type 2	54 Mbps	<150m	5 GHz	Ethernet, ATM,IP, UMTS, Firewire, PPP		ETSI, Promix, HP,IBM, Xircom, Nokia, Erricson, Dell,TI
IEEE 802.11	2 Mbps	100m-2Km	2.4 GHz	Ethernet	Διαθέσιμο	Cisco, Lucent, 3Com,
802.11b	11 Mbps	-//-	2.4 GHz	Ethernet	Διαθέσιμο	Apple,
802.11a	54 Mbps	-//-	5 GHz	Ethernet	Διαθέσιμο	Nokia,
802.11g	54 Mbps	-//-	2.4 GHz		Διαθέσιμο	Compaq
Wi-Max	70 Mbps	70 Km	2-11 GHz		Διαθέσιμο	RedLine

Πίνακας 6-1

6.5.1 Προκλήσεις του WiMax έναντι του IEEE 802.11

Αν και τα δύο πρότυπα μοιράζονται κάποια θεμελιώδη βασικά χαρακτηριστικά προσεγγίζουν το θέμα της ασύρματης δικτύωσης από δύο διαφορετικές οπτικές γωνίες. Τα δύο πρότυπα σχεδιάστηκαν για να εξυπηρετήσουν διαφορετικούς σκοπούς πράγμα που κάνει τη σύγκρουση τους σχεδόν αδύνατη.

Μια σημαντική διαφορά του προτύπου IEEE 802.16 σε σχέση με το IEEE 802.11 είναι ότι το πρώτο μπορεί να χρησιμοποιηθεί και σε συνθήκες μη οπτικής επαφής φυσικά με ρυθμούς μετάδοσης πολύ χαμηλότερους των 50 Mbps.

Το πρότυπο IEEE 802.16 παρέχει υψηλού επιπέδου **ποιότητα υπηρεσίας**. Το επίπεδο MAC του προτύπου είναι σχεδιασμένο κατά τέτοιο τρόπο ώστε να παρέχει στους χρήστες, όταν οι ίδιοι το επιθυμούν, εγγυημένο ρυθμό μετάδοσης και ταυτόχρονα κίνηση best effort σε χρήστες που καλύπτονται από το ίδιο base station κάτι που το πρότυπο IEEE 802.11 δεν μπορούσε να εξασφαλίσει. Δηλαδή, αν υποθέσουμε ότι δύο χρήστες καλύπτονται από το ίδιο base station, είναι δυνατό ο ένας χρήστης να έχει εγγυημένη ποιότητα υπηρεσίας και ο δεύτερος χρήστης να δέχεται και να στέλνει απλή IP κίνηση best effort κάτι που με το πρότυπο 802.11 δεν ήταν δυνατό. Δηλαδή χρήστες που βρισκόταν στην κάλυψη ενός Access Point είχαν την ίδια ποιότητα υπηρεσίας.

Η πιο θεμελιώδης διαφορά είναι ότι το WiFi είναι μια τεχνολογία για τοπική δικτύωση και σχεδιάστηκε για να δώσει μια κινητικότητα σε ιδιωτικά ενσύρματα LAN ενώ το WiMAX σχεδιάστηκε για να παρέχει BWA υπηρεσίες. Η ιδέα πίσω από τις BWA υπηρεσίες είναι η ασύρματη πρόσβαση στο internet χωρίς καλώδια και DSL τεχνολογίες. Έτσι λοιπόν ενώ το WiFi υποστηρίζει εύρος μετάδοσης μερικών εκατοντάδων μέτρων, τα WiMAX συστήματα μπορούν να υποστηρίξουν υπηρεσίες μεγαλύτερες των 30 μιλίων. Το παραπάνω επιχείρημα μπορεί μάλιστα να δικαιολογήσει γιατί δεν γίνεται τόσο μεγάλος λόγος στην αγορά για το WiMAX όσο για το WiFi, αφού το WiFi στοχεύει στο χρήστη ενώ το WiMAX χρησιμοποιείται σαν η κύρια αρτηρία μεταφοράς δεδομένων σε μακρινές αποστάσεις.

Μια άλλη διαφορά έγκειται στο γεγονός ότι το WiMax παρέχει συμμετρικό εύρος ζώνης για πολλά χιλιόμετρα και σειρά με την ισχυρότερη κρυπτογράφηση (3DES or AES) και συγκεκριμένα με τη λιγότερη παρέμβαση. Αντίθετα το πρότυπο IEEE 802.11 έχει την κρυπτογράφηση WEP ή WPA και δεν μπορεί να υπάρχει μεγάλη παρέμβαση σε περιοχές όπως αυτές όπου υπάρχουν πολλοί συνδεδεμένοι χρήστες.

Επίσης οι δυναμικές ζώνες του προτύπου IEEE 802.11 είναι backhauled στο ADSL, επομένως η πρόσβαση WiFi είναι τυπικά υποστηριζόμενη και έχει πολύ μικρές upload ταχύτητες μεταξύ του δρομολογητή και του Διαδικτύου.

Εκτός από αυτές τις διαφορές σχετικά με το εύρος μετάδοσης των δύο προτύπων, υπάρχουν αρκετές διαφορές στη ραδιοτεχνολογία που διακρίνουν τα δύο πρότυπα. Από τη μια πλευρά το WiMax αποτελείται από ένα πολύ μεγάλο εύρος πιθανών υλοποιήσεων για να μπορεί να παίξει το ρόλο του μεταφορέα σήματος σε ολόκληρο τον κόσμο και από την άλλη το WiFi περιγράφει $4^{ων}$ τύπων ραδιοσυνδέσεις οι οποίες δουλεύουν στις συχνότητες 2.4 ή 5 GHz στη μη νόμιμη περιοχή. Και αυτό που είναι αξιόλογο να σημειωθεί εδώ, είναι ότι ενώ όλες οι υλοποιήσεις του WiFi χρησιμοποιούν μη νόμιμες συχνοτικές μπάντες, το WiMAX δουλεύει σε νόμιμες και μη, συχνοτικές μπάντες.

Επίσης τα πρότυπα WiFi καιWiMAX έχουν και μία σημαντική διαφορά στο εύρος ζώνης των καναλιών. Το WiFi καθορίζει ένα σταθερό εύρος ζώνης καναλιού που είναι 25MHz για το 802.11b και 20MHz για τα 802.11a και 802.11g.Αντίθετα στο WiMAX, το εύρος ζώνης του καναλιού είναι προσαρμοστικό και κυμαίνεται από το 1.25MHz μέχρι τα 20MHz .

7. Βιβλιογραφία

1) WARDRIVING MANUAL Version 1.0
www.autistici.org/emdel/documents/wardriving.pdf

2) Wardriving, Warchalking & Wireless Hacking Μαρίνος Παπαδόπουλος
http://www.marinos.com.gr

3) WLAN War Driving DA Sna 02/6 8. September 2002 - 28. Oktober 2002
Studierende: Alain Girardet, Dominik Blunk Dozent:Prof. Dr. Andreas Steffen

4) Wireless Network Security 802.11, Bluetooth and Handheld Devices (National Institute of Standards and Security - NIST)

5) Ασφάλεια Πληροφοριακών Συστημάτων, Σωκράτης Κ. Κατσίκας – Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης (Εκδόσεις Νέων Τεχνολογιών)

6) 802.11 Wireless Networks: The Definitive Guide (By Matthew Gast)

7) 802.12 WiFi Security –Stewart S. Miller

8) Wi-Fi for the Enterprise- Nathan J. Muller – 2003

1) 10) Wireless Hacking. Projects for Wi-Fi Enthusiasts - Lee Barken with Eric Bermel, John Eder, Matthew Fanady Michael Mee, Marc Palumbo, Alan Koebrick

9) Hacking the Invisible Network Insecurities in 802.11x By Michael Sutton iDEFENSE Labs July 10, 2002

10) Hacking Wireless Networks for Dummies, Kevin Beaver and Peter T. Davis

11) Wireless Hacking. Projects for Wi-Fi Enthusiasts, By the SoCalFreeNet.org WirelessUsers Group Lee Barken with Eric Bermel, John Eder, Matthew Fanady Michael Mee, Marc Palumbo, Alan Koebrick

12) ERNST & YANG – Wireless Penetration Testing and Countermeasures for WiFi (802.11b/g) Technology, Matt Hynes , Senior Manager, Ernst & Young Technology & Security Risk Services

13) Computer Networks, 4th Edition, Prentice Hall, 2002, A. S. Tanenbaum.

14) "Your 802.11 Wireless Network has No Clothes." Arbaugh, William, Narendar Shankar and Justin Wan. http://downloads.securityfocus.com/library/wireless.pdf.

15) Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities." Information Systems Control Journal,Volume 2 (2002). http://www.isaca.org/wirelesswhitepaper.pdf

16) 802.11 IEEE standard http://standards.ieee.org/getieee802/download/802.11-1999.pdf

17) 802.11i IEEE standard http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

18) N.Borisov ,I.Goldberg and D.Wagner , "802.11 Security " , http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

19) B.Furht,Ph.D,M.Ilyas, "Wireless Internet Handbook , Technologies,Standards and Applications" , Publications CRC Press ,2003

Αναφορές από το Διαδίκτυο(WWW):

1) **www.worldwidewardrive.org**
2) **www.wardrive.net**
3) **en.wikipedia.org/wiki/Wi-Fi**
   Ιστοσελίδα Wikipedia με πληροφορίες σχετικές για το Wi-Fi
4) **en.wikipedia.org/wiki/WiMAX**
   Ιστοσελίδα Wikipedia με πληροφορίες σχετικές για το WiMax
5) **www.tutorial-reports.com/wireless/wlanwifi**
   Ιστοσελίδα με πληροφορίες σχετικές για το Wi-Fi καθώς επίσης και σχετικά βοηθήματα.
6) **www.freenetworks.org**
   Το FreeNetworks.org είναι μια εθελοντική συνεργατική κοινότητα, αφοσιωμένη στην εκπαίδευση, την συνεργασία και την δημιουργία των FreeNetworks (Ελεύθερα δίκτυα σε όλο τον κόσμο, τα οποία ακολουθούν συγκεκριμένα πρότυπα)
7) **www.wifi-forum.com**
   Wi-Fi forum
8) **ieee802.org /16/**
   Ιστοσελίδα με πληροφορίες για το συγκεκριμένο πρότυπο
9) **www.wimaxforum.org**
   WiMax forum
10) **computer.howstuffworks.com/wimax.htm/printable**
    Ιστοσελίδα με σχετικές πληροφορίες για την τεχνολογία WiMax
11) **www.wardriving.com**
    Ιστοσελίδα σχετική με το Wardriving
12) **en.wikipedia.org/wiki/Wardriving**
    Ιστοσελίδα Wikipedia με πληροφορίες σχετικές για το Wardriving
13) **www.kismetwireless.net**
    Επίσημη ιστοσελίδα του Kismet
14) **www.netstumbler.com**
    Επίσημη ιστοσελίδα του netstumbler

15) www.macstumbler.com

Επίσημη ιστοσελίδα του macstumbler

16) www.warchalking.org

Ιστοσελίδα σχετική με το Wardriving

17) www.wimax.com

Ιστοσελίδα της WiMax Community

18) ru6.cti.gr/broadband/el/wimax.php

Ιστοσελίδα σχετικά με την προώθηση της ευρυζωνικότητας στην περιφέρεια της Δυτικής Ελλάδας. Στη συγκεκριμένη γίνεται αναφορά στην τεχνολογία wimax.

19) www.eng.ucy.ac.cy/toumpis/courses/ECE453/papers/wimax.ppt

Ιστοσελίδα του "School of Engineering" από το Πανεπιστήμιο Κύπρου.

20) home.no.net/coverage/SecurityinWLAN.htm

Wireless Security

APPENDIX A: AUDITING TOOLS

WLAN Scanners

Name	Platform	Vendor website
NetStumbler	Windows	http://www.NetStumbler.org/
Dstumbler	BSD	http://www.dachb0den.com/projects/dstumbler.html
MacStumbler	Macintosh	http://homepage.mac.com/macstumbler/
MiniStumbler	Pocket PC	http://www.NetStumbler.org/download.php?op=getit&lid=21
SSIDSniff	Unix	http://www.bastard.net/~kos/wifi/
Airosniff	Unix	http://gravitino.net/~bind/code/airosniff/
AP Scanner	Macintosh	http://homepage.mac.com/typexi/Personal1.html
wavemon	Linux	http://www.jm-music.de/projects.html
WLAN Expert	Windows	http://www.vector.kharkov.ua/download/WLAN/wlanexpert.zip
wavelan-tools	Linux	http://sourceforge.net/projects/wavelan-tools/
Kismet	Linux, iPaq, Zaurus	http://www.kismetwireless.net/
AiroPeek	Windows	http://www.wildpackets.com/products/airopeek/
Sniffer Wireless	Windows	http://www.sniffer.com/products/sniffer-wireless/
THC-WarDrive	Linux	http://www.thehackerschoice.com/download.php?t=r&d=wardrive-2.3.tar.gz
APSniff	Windows	http://www.bretmounet.com/ApSniff/
Wellenreiter	Linux	http://www.remote-exploit.org/
PrismStumbler	Linux	http://prismstumbler.sourceforge.net/
AirTraf	Linux	http://airtraf.sourceforge.net/

WLAN Sniffers

Name	Platform	Vendor website
Mognet	Java VM	http://chocobospore.org/mognet/
Kismet	Linux, Ipaq, Zaurus	http://www.kismetwireless.net/
Ethereal	Unix, Windows	http://www.ethereal.com/
TCPDump	Unix	http://www.tcpdump.org/
Prismdump	Unix	http://developer.axis.com/download/tools/
prism2dump	BSD	http://www.dachb0den.com/projects/prism2dump.html
AiroPeek	Windows	http://www.wildpackets.com/products/airopeek/
Sniffer Wireless	Windows	http://www.sniffer.com/products/sniffer-wireless/

WEP Key Crackers

Name	Platform	Vendor website
WEPCracker	Perl	http://sourceforge.net/projects/wepcrack/
AirSnort	Linux	http://www.be-secure.com/airsnort.html
AirSnort for BSD	BSD	http://www.dachb0den.com/projects/bsd-airsnort.html

Other

Name	Platform	Vendor website
APTools	Windows, Unix	http://aptools.sourceforge.net/
Note: Identify APs based on MAC addresses by querying routers and switches		
Wireless Tools	Linux	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
Note: Tools allowing for the manipulation of Wireless Extensions		
THC-Rut	Unix	http://www.thehackerschoice.com/download.php?t=r&d=thcrut-0.1.tar.gz
Note: Local network discovery tool developed to brute force its way into WLAN access points		
AirMagnet	PocketPC	http://www.airmagnet.com/products.htm
Note: This commercial product is a wireless vulnerability scanner that attempts to identify rogue access points, denial of service attacks, unencrypted traffic, default SSIDs and MAC address spoofing, along with functionality to troubleshoot connectivity issues.		

APPENDIX B: IEEE TASK GROUPS

802.11 Task Group	Name
802.11a	**High-speed Physical Layer in the 5GHz Band**
IEEE description	The family of specifications for wireless, Ethernet local area networks in 5-gigahertz bandwidth space.
URL	http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
802.11b	**Higher-Speed Physical Layer Extension in the 2.4GHz Band**
IEEE description	The family of specifications for wireless, Ethernet local area networks in 2.4-gigahertz bandwidth space.
URL	http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
802.11d	**Specification for Operation in Additional Regulatory Domains**
IEEE description	Define the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains, or countries).
URL	http://standards.ieee.org/getieee802/download/802.11d-2001.pdf
802.11e	**MAC Enhancements for Quality of Service**
IEEE description	Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
URL	http://grouper.ieee.org/groups/802/11/Reports/tge_update.htm
802.11f	**Recommended Practice for Inter Access Point Protocol**
IEEE description	Develop recommended practices for an Inter-Access Point Protocol (IAPP), which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgf_update.htm
802.11g	**Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band**
IEEE description	Develop a higher speed(s) physical layer extension to the 802.11b standard. The new standard shall be compatible with the IEEE 802.11 MAC. The maximum physical layer data rate targeted by this project shall be at least 20 Mbit/s. The new extension shall implement all mandatory portions of the IEEE 802.11b physical layer standard.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm
802.11h	**SMa - Spectrum Managed 802.11a**
IEEE description	Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz Band supplement to the standard; to add indoor and outdoor channel selection for 5GHz license exempt bands in Europe; and to enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management (per CEPT and subsequent EU committee or body ruling incorporating CEPT Recommendation ERC 99/23).
URL	http://grouper.ieee.org/groups/802/11/Reports/tgh_update.htm
802.11i	**MAC Enhancements for Enhanced Security**
IEEE description	Enhance the current 802.11 MAC to provide improvements in security.
URL	http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm