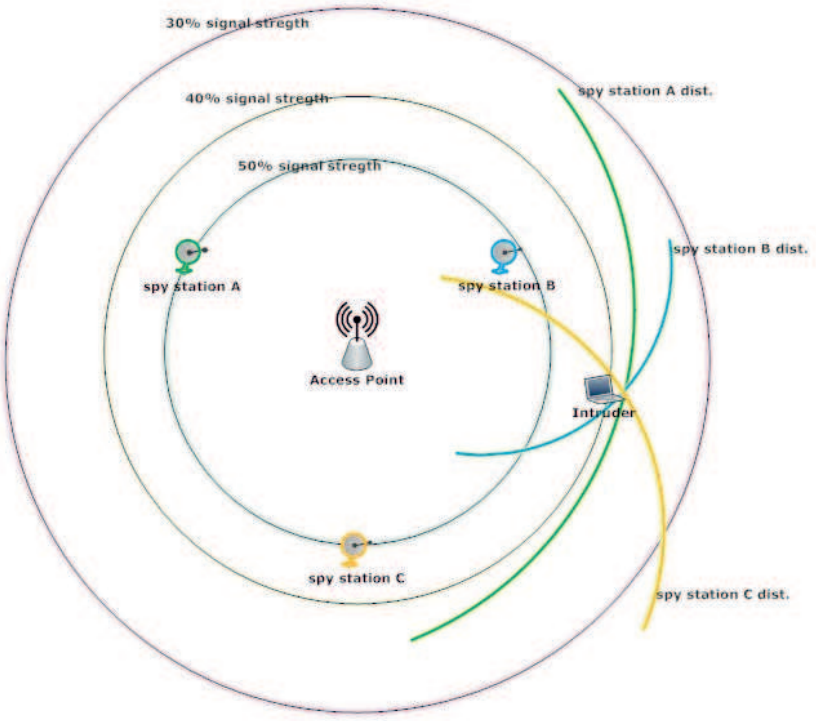
ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Μελέτη και ανάλυση της ασφάλειας ασύρματων δικτύων όταν τα χρησιμοποιούν χρήστες για κακόβουλες ενέργειες»



Του φοιτητή
Σταύρου Τζίκα
Αρ. Μητρώου: 00/1607

Επιβλέπων καθηγητής
Δημήτριος Αμανατιάδης

Θεσσαλονίκη 2012

ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Μελέτη και ανάλυση της ασφάλειας ασύρματων τοπικών δικτύων όταν τα χρησιμοποιούν χρήστες για κακόβουλες ενέργειες»

Του φοιτητή
Σταύρου Τζίκα
Α.Μ.: 00/1607

Επιβλέπων καθηγητής
Δημήτριος Αμανατιάδης

Θεσσαλονίκη 2012

ΠΡΟΛΟΓΟΣ

Τα τελευταία χρόνια τα ασύρματα τοπικά δίκτυα γνωρίζουν μεγάλη εξάπλωση. Τα συναντούμε σε διάφορους χώρους και χρησιμοποιούνται από πολλούς χρήστες που βρίσκονται σε κίνηση.

Ένα όμως μειονέκτημά τους θεωρείται πως είναι η ασφάλεια που παρέχουν. Έχουν γίνει κάποιες προτάσεις και υλοποιήσεις που δείχνουν να έχει ξεπεραστεί αυτό το μειονέκτημα.

Υπάρχουν όμως χρήστες που γνωρίζοντας τις αδυναμίες των ασύρματων τοπικών δικτύων τα χρησιμοποιούν για κακόβουλες ενέργειες.

Στόχος αυτής της μελέτης είναι η καταγραφή της υπάρχουσας κατάστασης από την οπτική της προστασίας που παρέχουν τα διάφορα προγράμματα ασφάλειας και οι αδυναμίες που εντοπίζονται καθώς και ένας οδηγός για τη διασφάλιση των χρηστών αλλά και των εξυπηρετητών από κακόβουλες επιθέσεις. Ένας ακόμη στόχος είναι η διαβάθμιση των επιθέσεων και οι αντίστοιχες αποκρούσεις που πρέπει να έχει προετοιμάσει ο διαχειριστής του ασύρματου τοπικού δικτύου.

Σκοπός της ανάλυσης που θα προκύψει είναι η εύρεση του στίγματος του χρήστη που προσπαθεί να επιτεθεί μέσα από τα στοιχεία που υπάρχουν στα χαμηλά επίπεδα (στα πακέτα και τα πλαίσια που ανταλλάσσονται) έτσι ώστε αν είναι δυνατόν να εντοπιστεί ο επίδοξος «τρομοκράτης» με μια σειρά από ίχνη που έχει αφήσει και δεν είναι δυνατόν να τα παραποιήσει ή να τα διαγράψει.

ΠΕΡΙΛΗΨΗ

Τα ασύρματα τοπικά δίκτυα άλλαξαν τον τρόπο επικοινωνίας και αύξησαν την κινητικότητα των χρηστών. Έφεραν την επανάσταση στον τρόπο που οι άνθρωποι χρησιμοποιούσαν τους ηλεκτρονικούς υπολογιστές για την επικοινωνία. Τα πιο δημοφιλή και εμπορικά ασύρματα δίκτυα είναι εκείνα που χρησιμοποιούν το πρότυπο 802.11.

Το 802.11, με τη γηγενή ασφάλεια που προσφέρουν, φαίνεται να είναι αποτελεσματικά. Στην πραγματικότητα, όπως αναλύεται στη παρούσα μελέτη, ακόμα και εφαρμόζοντας επιπρόσθετες δικλείδες ασφαλείας σε ένα ασύρματο δίκτυο, δεν είναι εφικτό να αποτραπεί η εισβολή ενός κακόβουλου χρήστη, παρά μόνο να τον καθυστερήσουν.

Γεννάτε λοιπόν η ανάγκη, για τους επαγγελματίες διαχειριστές δικτύων, να μπορεί να εντοπιστεί ο εισβολέας χωροταξικά. Στα ενσύρματα τοπικά δίκτυα το φυσικό μέσο είναι αυτό που προδίδει τη θέση του εισβολέα. Στα ασύρματα δίκτυα δεν έχουμε αυτό το πλεονέκτημα.

Αφού μελετηθούν οι μέθοδοι ασφάλειας ασύρματων δικτύων και παράλληλα οι μέθοδοι παράκαμψης αυτών θα παρατηρήσουμε πως και οι διαχειριστές αν εκμεταλλευτούν αυτές τις μεθόδους παράκαμψης κατά ένα μεγάλο ποσοστό θα αποτρέψουν τον εισβολέα να υποκλέψει τις πληροφορίες και τα δεδομένα που διακινούνται στον αέρα, αλλά και να τον εντοπίσει χωροταξικά.

ABSTRACT

The wireless local area networks changed the way users communicate and increased their mobility. Revolutionized the way people used to communicate using computers. The most popular and commercial wireless networks are those that use the 802.11 standard.

The 802.11 offers a native security, which appears to be effective in safe transfer of data. In fact, as analyzed in this study, applying additional safeguards to a wireless local area network, it is not possible to prevent the intrusion of a malicious user. Only to be delayed.

The need for professional network administrators, to be able to identify the attacker spatially, comes up. In wired LANs the physical medium is what betrays the position of the attacker. This advantage does not exist in wireless networks.

After studying the methods used for securing wireless local area networks and the methods used to bypass them, we will see how administrators could take advantage of these “bypassing methods”. They would have a large percentage of success of preventing attackers to intercept information and data travelling through the air and also to allocate them.

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω τους φίλους μου και συναδέλφους Πασχάλη Καμαργιάννη και Δημήτριο Στοϊμένο που μου στάθηκαν τα πρώτα χρόνια των σπουδών μου και με βοήθησαν να καλύψω τα κενά γνώσεων που είχα. Ειδικότερα τους οφείλω τις ευχαριστίες μου για τις γνώσεις που μου μετέδωσαν στον τομέα των δικτύων και για τον «πληροφορικό» τρόπο σκέψης που μου δίδαξαν.

Ευχαριστώ τον επιβλέποντα καθηγητή μου κύριο Δημήτριο Αμανατιάδη για την υπομονή του και την εμπιστοσύνη που έδειξε στο πρόσωπό μου. Τον ευχαριστώ επίσης για τη στήριξή του και τη βοήθειά του που μου πρόσφερε, όχι μόνο για την εκπόνηση της πτυχιακής εργασίας, αλλά και κατά τη διάρκεια των σπουδών μου.

Τέλος θέλω να εκφράσω τις ευχαριστίες μου στην οικογένειά μου για την πνευματική και φυσική συμπαράσταση και την υπομονή τους όλα αυτά τα χρόνια.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

ΣΥΝΤΜΗΣΕΙΣ

ACK	Acknowlendgement
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set ID
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct-Sequence Spread Spectrum
ESSID	Extended Service Set Identification
FHSS	Frequency-Hopping Spread Spectrum
GPS	Global Positioning System
HR-DSSS	High Rate DSSS
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP SEC	Internet Protocol Security
IR	Infrared
LAN	Local Area Network
LBS	Location Based System
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MB	Mega Byte
MB/s	Mega Byte per second
Mbps	Mega bite per second
NIC	Network Interface Card
OFDM	Orthogonal Frequency - Division Multiplexing
OSI	Open System Interconnection
PCF	Point Coordination Function
PPTP	Point -to-Point Tunneling Protocol
PSK	Pre-Shared Key
RF	Radio Frequency
RSN	Robust Secure Network
SSID	Service Set Identification
SYN	Synchronize (TCP)
TCP/IP	Transmission Control Program/Internet Protocol

TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WMAN	Wireless MAN
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WWAN	Wireless Wide Area Network

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία έχει ως σκοπό την θεωρητική προσέγγιση μιας εφαρμογής χωροταξικού εντοπισμού εισβολέων σε ασύρματα τοπικά δίκτυα. Στόχος, να ελαχιστοποιηθεί ή ακόμα και να μηδενιστεί το κενό ασφαλείας που υπάρχει στη φύση των ασύρματων τοπικών δικτύων. Η χαρτογράφηση της ισχύς του σήματος και η προσθήκη βοηθητικού υλικού στην υποδομή ενός ασύρματου δικτύου μπορεί να αποτελέσει την λύση στο υπάρχον πρόβλημα.

Στο Κεφάλαιο 1 γίνεται μία αναδρομή στα ασύρματα δίκτυα παραθέτοντας τα πλεονεκτήματα και τα μειονεκτήματα και τα δομικά στοιχεία. Δίνεται ιδιαίτερη έμφαση στο πρότυπο 802.11, στα χαρακτηριστικά του και τις τοπολογίες του. Επίσης γίνεται και μια σύντομη περιγραφή της τεχνικής μετάδοσης των δεδομένων.

Στο πρώτο μέρος στο Κεφάλαιο 2 αναλύεται η ασφάλεια των 802.11 ασύρματων δικτύων, περιγράφοντας και αναλύοντας χωρίς πολλές λεπτομέρειες τις ιδιότητες ασφαλούς επικοινωνίας. Στο δεύτερο μέρος περιγράφονται οι τύποι επιθέσεων, κάποιες μέθοδοι επιθέσεων και αντίστοιχα εργαλεία-λογισμικά που διευκολύνουν τέτοιου είδους τακτικές.

Στο Κεφάλαιο 3 εστιάζεται σε γνωστές τεχνικές ασφάλειας ενσύρματων δικτύων που εφαρμόζονται και στα ασύρματα. Με κάθε τεχνική περιγράφεται και μία μέθοδος παράκαμψης αντίστοιχα. Ιδιαίτερα το υποκεφάλαιο 3.2 θα μπορούσε να θεωρηθεί και ένας σύντομος οδηγός θωράκισης ασύρματου τοπικού δικτύου.

Στο Κεφάλαιο 4 γίνεται μία θεωρητική προσέγγιση για μία εφαρμογή για τον χωροταξικό εντοπισμό εισβολέα σε ασύρματο τοπικό δίκτυο. Η προσέγγιση γίνεται με μία χαρτογράφηση του ασύρματου δικτύου, με προσθήκη εξοπλισμού στο σύνολο του τοπικού δικτύου και η περιγραφή του πιθανού εντοπισμού του εισβολέα.

ΚΕΦΑΛΑΙΟ 1

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.1 ΕΙΣΑΓΩΓΗ

Ένα από τα χαρακτηριστικά της εποχής μας είναι ο εθισμός στην τεχνολογία της συλλογής, επεξεργασίας και αναδιανομής της πληροφορίας. Όλο και περισσότεροι άνθρωποι γίνονται τόσο παθητικά αλλά και ενεργητικά μέλη στο παγκόσμιο διαδίκτυο. Για αυτούς τους χρήστες που το διαδίκτυο είναι πλέον ζωτικής σημασίας τόσο σε επαγγελματικό αλλά και σε προσωπικό επίπεδο, τα καλώδια πλέον είναι δεσμευτικά. Οι χρήστες αυτοί χρειάζονται δεδομένα για το φορητό υπολογιστή, τον υπολογιστή τσέπης ή ακόμα και τον υπολογιστή γραφείου τους χωρίς να είναι προσδεμένοι στην ενσύρματη επικοινωνιακή δομή. Για τους χρήστες αυτούς η απάντηση είναι οι ασύρματες επικοινωνίες.

Ένας από τους ορισμούς που έχει επικρατήσει γενικότερα για τα δίκτυα υπολογιστών παρατίθεται πιο κάτω:

Ένα δίκτυο υπολογιστών είναι ένα σύνολο από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμός) κάποιου άλλου.

Θα πρέπει να τονιστεί ότι σύμφωνα με την λειτουργικότητά τους τα δίκτυα υπολογιστών καθορίζουν και την σημασία τους και χωρίζονται ως εξής:

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως «ενσύρματα» ή «ασύρματα».
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως «δημόσια» ή «ιδιωτικά» δίκτυα.
- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως «τοπικά» (LAN και WLAN), «μητροπολιτικά» (MAN και WMAN), «ευρείας κάλυψης» (WAN και WWAN).

Όπως αναφέρεται πιο πάνω, αυτό που μπορεί να διαφοροποιήσει ένα ενσύρματο από ένα ασύρματο δίκτυο είναι το φυσικό μέσο μετάδοσης της πληροφορίας. Όλα τα ασύρματα δίκτυα (WLAN, WMAN, WWAN) αντί για καλώδια, χρησιμοποιούν τον αέρα. Οι υπέρυθρες ακτίνες (IR) και ραδιοσυχνότητες (RF) ευθύνονται για την μετάδοση πληροφοριών μέσω του αέρα. Οι ραδιοσυχνότητες είναι πιο διαδεδομένες διότι είναι μεγαλύτερης εμβέλειας, εύρους ζώνης και κάλυψης. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα συνήθως 2,4 GHz και 5 GHz. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου.

Ο τομέας των ασύρματων δικτύων, ένας τομέας επανάσταση για το είδος του, είναι ένας από τους ταχύτερα αναπτυσσόμενους κλάδους των τηλεπικοινωνιών.

Τα ασύρματα δίκτυα υπολογιστών όμως, όπως και τα κλασσικά ενσύρματα δίκτυα, απαιτούν την χρήση αξιόπιστων πρωτοκόλλων μεταφοράς δεδομένων, τα οποία θα εξασφαλίζουν την ασφαλή μετάδοση των δεδομένων μεταξύ των χρηστών. Πρέπει να παρέχουν ασφάλεια από οποιαδήποτε ενέργεια παραβίασης, να δίνουν την δυνατότητα ταχείας πρόσβασης και μεταφοράς δεδομένων και τέλος να επιτρέπουν την διασύνδεση των ασύρματων δικτύων με τα ήδη υφιστάμενα ενσύρματα τοπικά δίκτυα.

Με δεδομένη την αποδοχή του κόσμου για αυτή τη νέα τεχνολογία, τις λύσεις των προμηθευτών και τα βιομηχανικά πρότυπα, η ασύρματη δικτύωση θα επικρατήσει στο μέλλον. Όμως πόσο ασφαλής είναι αυτή η τεχνολογία τελικά;

1.2 ΤΙ ΕΙΝΑΙ ΤΟ WI-FI

Με την ταχύτατη ανάπτυξη των προτύπων IEEE και την γιγάντωση της βιομηχανίας κατασκευαστών αντίστοιχων συσκευών, κρίθηκε αναγκαία η διασφάλιση της συμβατότητας μεταξύ των διάφορων συσκευών για την προστασία του αγοραστή.

Έτσι το 1999 ιδρύθηκε η WECA (Wireless Ethernet Compatibility Alliance), ένας μη κερδοσκοπικός οργανισμός που σκοπό έχει την πιστοποίηση ασύρματων συσκευών υλοποιημένα βάση του προτύπου 802.11.

Σε αυτόν τον οργανισμό συμμετέχουν εταιρείες παροχής υπηρεσιών WLAN, κατασκευαστές ολοκληρωμένων κυκλωμάτων, υπολογιστών, λογισμικού κ.α.

Η ένωση αυτή επινόησε μία σειρά από δοκιμές προκειμένου να πιστοποιεί τη συμβατότητα των IEEE προτύπων με τις νέες σε κυκλοφορία συσκευές. Οι συσκευές οι οποίες υποβάλλονται επιτυχώς στις δοκιμές αυτές, αποκτούν το λογότυπο Wi-Fi (Wireless Fidelity). Το λογότυπο αυτό αποτελεί κατά συνέπεια μία πιστοποίηση για τον υποψήφιο αγοραστή μιας συσκευής και μία εγγύηση για την επένδυσή του. Ο καταναλωτής αγοράζοντας μία πιστοποιημένη συσκευή, έχει την εγγύηση ότι η συσκευή θα συνεργαστεί με οποιαδήποτε άλλη συσκευή φέρει επίσης το λογότυπο (Εικόνα 1.1)

Εικόνα 1. 1 Λογότυπο Wi-Fi

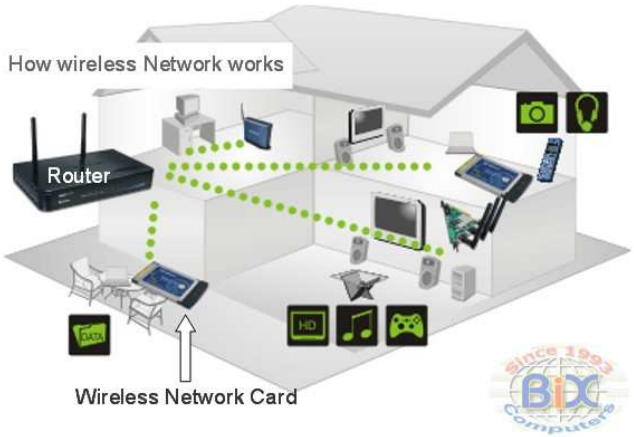
1.3 ΠΕΡΙΓΡΑΦΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ως ασύρματο τοπικό δίκτυο (WLAN) ορίζεται ένα σύστημα επικοινωνίας μέσω ηλεκτρομαγνητικών κυμάτων ανάμεσα σε σταθερούς ή κινητούς χρήστες επιτρέποντας την μεταξύ τους διασύνδεση και ανταλλαγή δεδομένων.

Η πρώτη γενιά συσκευών WLAN με τη χαμηλή ταχύτητα διάδοσης και την έλλειψη προτύπων δε ήταν ιδιαίτερα διαδεδομένη. Όμως τα σύγχρονα συστήματα είναι δυνατόν να μεταφέρουν δεδομένα σε αποδεκτές ταχύτητες.

Επίσης, νέες συσκευές και προϊόντα ασύρματης πρόσβασης βασιζόμενα σε τεχνολογίες spread-spectrum ραδιοφωνικά κύματα, υπέρυθρες ακτίνες, κυψελοειδείς και δορυφορικές επικοινωνίες, είναι πια πραγματικότητα.

Σήμερα υπάρχει στην αγορά ένας τεράστιος αριθμός από νέες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές, οι οποίοι ενσωματώνουν τεχνολογία ασύρματης πρόσβασης, είναι διαθέσιμοι για το ευρύ κοινό, αφού έχουν πλέον χαμηλό κόστος, ικανοποιητική υπολογιστική ισχύ και ποιότητα υπηρεσιών παρόμοια με τους σταθερούς υπολογιστές γραφείου.



Εικόνα 1. 2 Παράδειγμα εφαρμογής των ασύρματων τοπικών δικτύων

1.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Η χρήση των ασύρματων δικτύων έχουν όπως και όλες οι σύγχρονες τεχνολογίες τα υπέρ και τα κατά τους. Ονομαστικά μερικά από τα κυριότερα πλεονεκτήματα των ασύρματων τοπικών δικτύων είναι τα εξής:

- Ευκολία πρόσβασης
- Κινητικότητα
- Ταχύτητα και ευελιξία εγκατάστασης
- Μειωμένο κόστος χρήσης
- Συμβατότητα
- Νομαδική πρόσβαση
- Διασύνδεση

Όμως το κάθε πλεονέκτημα συνοδεύεται σχεδόν και από ένα μειονέκτημα. Αυτό οφείλεται στον ίδιο παράγοντα που μας επέτρεψε να υλοποιηθεί η ασύρματη τεχνολογία. Τα ηλεκτρομαγνητικά κύματα.

Η χρήση των ηλεκτρομαγνητικών κυμάτων για τη μεταφορά πληροφορίας κάνουν τα ασύρματα δίκτυα ευάλωτα και ευπρόσβλητα σε πολλά φυσικά αλλά και ανθρώπινα φαινόμενα παρεμβολής τα οποία αλλοιώνουν την επικοινωνία των χρηστών. Ονομαστικά τα κυριότερα προβλήματα που παρουσιάζονται στα ασύρματα τοπικά δίκτυα είναι τα εξής:

- Παρεμβολή λόγω πολλαπλών διαδρομών
- Path loss – Απώλεια οπτικής επαφής
- Παρεμβολές ραδιοσημάτων
- Διαχείριση ενέργειας
- Ασυμβατότητα συστημάτων
- Προστασία της υγείας των χρηστών
- Το φαινόμενο του κρυμμένου κόμβου
- Ασφάλεια δικτύου

Λόγω αυτών των προβλημάτων, έχουν δημιουργηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν δύσκολη, αλλά όχι αδύνατη, την υποκλοπή της πληροφορίας που μεταδίδεται.

Τέτοιες είναι οι τεχνικές εξάπλωσης φάσματος (spread spectrum) ενώ εάν απαιτείται περισσότερη ασφάλεια, καθορίζεται η χρήση κωδικοποίησης WEP (Wired Equivalent Privacy).

1.5 ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ

Για την δημιουργία ενός ασύρματου τοπικού δικτύου είναι απαραίτητη κάποια υλικοτεχνική υποδομή. Μιλάμε για διάφορα στοιχεία που συντονίζουν την μετάδοση, τη λήψη και την επεξεργασία του σήματος μεταξύ των χρηστών. Η δομή αυτή περιλαμβάνει τόσο το λογισμικό όσο και το ανάλογο υλικό εξοπλισμού. Οι κατηγορίες των στοιχείων αυτών αναφέρονται στη συνέχεια.

- **Συσκευές χρηστών**

  Η επικοινωνία των διαφόρων εφαρμογών και υπηρεσιών με τους χρήστες σε ένα ασύρματο δίκτυο γίνεται μέσω συγκεκριμένων συσκευών. Είτε το δίκτυο είναι ασύρματο ή ενσύρματο, οι συσκευές αποτελούν την πηγή επικοινωνίας μεταξύ του χρήστη και του δικτύου. Τέτοιες συσκευές είναι:

  - ✓ Σταθεροί Υπολογιστές γραφείου
  - ✓ Φορητοί Υπολογιστές
  - ✓ Υπολογιστές χειρός και παλάμης
  - ✓ IP Phones
  - ✓ IP Cameras
  - ✓ Εκτυπωτές
  - ✓ Projectors

- **Λογισμικό δικτύου**

  Ένα ασύρματο δίκτυο είναι δομημένο με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server, παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.α.

  Αυτά τα συστήματα στηρίζονται στην ύπαρξη ενός εξυπηρετητή, ο οποίος διαθέτει τις βάσεις δεδομένων στις οποίες μπορούν να έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι τελευταίες εκτελούν το δικό τους λογισμικό, το οποίο κατευθύνει τις εντολές του χρήστη στον εξυπηρετητή.

- **Ασύρματες κάρτες δικτύου (Wireless NIC's)**

  Η ασύρματη κάρτα δικτύου (Wireless Network Interface Card) χρησιμοποιείται για την μετάδοση του ψηφιακού σήματος ενός υπολογιστή μέσω του ασύρματου μέσου σε έναν άλλο υπολογιστή.

Στην διαδικασία αυτή συμπεριλαμβάνεται η διαμόρφωση και η ενίσχυση του σήματος.

Εικόνα 1. 3 Ασύρματη κάρτα δικτύου

- **Σημεία πρόσβασης (Access Points)**

  Το σημείο πρόσβασης είναι μια κεντρική συσκευή σε ένα ασύρματο τοπικό δίκτυο που παρέχει το εύρος για την ασύρματη επικοινωνία με τους άλλους σταθμούς σε ένα δίκτυο. Συνήθως συνδέεται σε ένα ενσύρματο δίκτυο και έτσι παρέχει μια γέφυρα ανάμεσα στο ενσύρματο δίκτυο και τις ασύρματες συσκευές.

Εικόνα 1. 4 Σημείο πρόσβασης - Router / Access Point

Τα σημεία πρόσβασης περιλαμβάνουν χαρακτηριστικά ασφάλειας όπως επικύρωση και κρυπτογράφηση, έλεγχο πρόσβασης που

βασίζεται σε λίστες ή φίλτρα καθώς και πολλά άλλα τα οποία συνήθως απαιτούν τη ρύθμισή τους από τον χρήστη - διαχειριστή σύμφωνα με τις προτιμήσεις ή ανάγκες του. Πολλά σημεία πρόσβασης περιλαμβάνουν επιπρόσθετα χαρακτηριστικά δικτύωσης, όπως πύλες διαδικτύου, κόμβους μεταγωγής, ασύρματες γέφυρες ή επαναλήπτες.

- **Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)**

  Οι ασύρματες τοπικές γέφυρες είναι πολύ σημαντικό κομμάτι της τοπολογίας ενός δικτύου καθώς συνδέουν πολλά τοπικά δίκτυα μεταξύ τους στο επίπεδο του υποστρώματος MAC για την δημιουργία ενός εκτενέστερου και πιο λειτουργικού δικτύου. Οι γέφυρες χωρίζονται σε δύο κατηγορίες.

  Οι τοπικές γέφυρες (Local Bridges) είναι η σύνδεση ανάμεσα σε κοντινά τοπικά δίκτυα.

  Οι απομακρυσμένες γέφυρες (Remote Bridges) είναι η σύνδεση ανάμεσα σε δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που υποστηρίζονται από τα πρωτόκολλα των τοπικών δικτύων.

Εικόνα 1. 5 Ασύρματη Γέφυρα

Οι γέφυρες ως συσκευές χρησιμεύουν στην διασύνδεση ασύρματου με ενσύρματου δικτύου. Επίσης υλοποιούν και διασυνδέσεις μεταξύ δύο ή περισσότερων ασύρματων τοπικών δικτύων. Σε αυτήν την περίπτωση οι γέφυρες συνήθως αναφέρονται και ως «Σημείο Πρόσβασης» (APs – Access Points).

- **Κεραίες**

  Οι κεραίες χρησιμεύουν στην εκπομπή του διαμορφωμένου σήματος μέσω του αέρα. Γενικά, οι κεραίες χωρίζονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από τα εξής πεδία:

  - ✓ Ισχύς μετάδοσης (Transmit power)

- ✓ Εύρος Ζώνης (Bandwidth)
- ✓ Μοντέλο Διάδοσης (Propagation pattern)
- ✓ Ευαισθησία (Gain)

Εικόνα 1. 6 Κεραίες

Ο τρόπος που μεταδίδει το σήμα μια κεραία καθορίζει επίσης και την περιοχή κάλυψης της. Για την μετάδοση του σήματος στα ασύρματα δίκτυα χρησιμοποιούνται κυρίως δύο είδη κεραιών. Οι πολυκατευθυντικές, που διοχετεύουν την ισχύ τους προς κάθε κατεύθυνση, και οι μονοκατευθυντικές, που συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.

1.6 ΤΟ ΠΡΟΤΥΠΟ 802.11

Το πρώτο πρότυπο ασύρματων τοπικών δικτύων το 802.11 και δημοσιεύτηκε το 1997. Το πρότυπο αυτό καθορίζει τον έλεγχο πρόσβασης στο μέσο (MAC) και τα φυσικά στρώματα για ένα τοπικό δίκτυο με ασύρματη σύνδεση. Σύμφωνα με αυτό το πρότυπο, εξετάζεται η τοπική ασύρματη δικτύωση συσκευών που βρίσκονται κοντά.

Από την αρχική του έκδοση το πρότυπο έχει επεκταθεί σε πολυάριθμες ομάδες, που καθορίζονται από το λατινικό αλφάβητο (a,b,c,…y,z).

1.6.1 Η οικογένεια

Στα τέλη του 1999 η IEEE κοινοποίησε δύο νέα συμπληρωματικά πρότυπα για WLANs, τα 802.11a, 802.11b. Στην δεκαετία που ακολούθησε κοινοποίησε και άλλα δύο πρότυπα 802.11g και 802.11n τα οποία και υλοποιήθηκαν σε εμπορικά προϊόντα και έγιναν τα πλέον επικρατέστερα. Αναλυτικά:

Το 802.11a έχει καθοριστεί έτσι ώστε να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps (ονομαστικός ρυθμός μετάδοσης), με συνήθη ρυθμό μετάδοσης 23 Mbits/s. Εμβέλεια εσωτερικού χώρου έως και 35 m και χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5 GHz.

Το 802.11b είναι ουσιαστικά ο αντικαταστάτης του αρχικού 802.11 καθώς υποστηρίζει ρυθμούς δεδομένων 11 Mbps, εμβέλεια εσωτερικού χώρου έως και 35 m και χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS (Direct-Sequence Spread Spectrum) στα 2.4 GHz.

Επίσης το 2003, η IEEE κοινοποίησε το πρότυπο 802.11g, το οποίο υποστηρίζει ρυθμούς μετάδοσης δεδομένων έως και 54 Mbps (ονομαστικός ρυθμός μετάδοσης), εμβέλεια εσωτερικού χώρου έως και 38m με την τεχνική OFDM και DSSS, στα 2.4 GHz.

Για το 2009, προτάθηκε από την IEEE το πρότυπο 802.11n, με συχνότητα 2.4 GHz και 5 GHz, μέγιστο ονομαστικό ρυθμό μετάδοσης 150 Mbits/s και εμβέλειες 70 m και 250 m (εσωτερικού χώρου και εξωτερικού χώρου αντίστοιχα).

v • d • e **802.11 network standards**

802.11 protocol	Release[5]	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)[6]	Allowable MIMO streams	Modulation	Approximate indoor range[citation needed]		Approximate outdoor range[citation needed]	
							(m)	(ft)	(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	38	125	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[B]	4	OFDM	70	230	250	820[7]
			40	15, 30, 45, 60, 90, 120, 135, 150[B]			70	230	250	820[7]

- A1 A2 IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- B1 B2 Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

Πίνακας 1. 1 802.11 πρότυπα

Εκτός των παραπάνω εκδόσεων έχουν προταθεί και κάποιες άλλες επεκτάσεις τους, οι οποίες όμως δεν έχουν υλοποιηθεί σε εμπορικά προϊόντα, έχουν περισσότερο ακαδημαϊκό ενδιαφέρον, και ονομαστικά είναι τα : 802.11f (ή IAPP), 802.11e.

1.6.2 Χαρακτηριστικά του 802.11

Η ζώνη συχνοτήτων των 2.4 GHz σήμερα είναι ιδιαίτερα δημοφιλής. Αυτό συμβαίνει διότι πρόκειται για ελεύθερη ζώνη που έχει συγκεκριμένα χαρακτηριστικά που χρησιμεύουν για μετάδοση σε μικρές αποστάσεις.

- **Εμβέλεια**

  Η εμβέλεια ενός τοπικού δικτύου σε εσωτερικούς χώρους κυμαίνεται από τα 20 – 38 μέτρα. Τα ραδιοκύματα όμως θα πρέπει να διαπεράσουν τοίχους και οροφές, οπότε έχουμε σημαντικές απώλειες. Επίσης το σήμα ανακλάται από τις προσπίπτουσες επιφάνειες. Σε περιβάλλον όμως με οπτική επαφή (Line on Sight), σε εξωτερικό χώρο, η εμβέλεια του ασύρματου δικτύου είναι μεγαλύτερη και εξαρτάται από διάφορους παράγοντες που σχετίζονται με τις συσκευές όπως την ευαισθησία του δέκτη, την ποιότητα των κεραιών και την ευθυγράμμισή τους, το επίπεδο παρεμβολών και θορύβου.

- **Ρυθμός μετάδοσης**

  Ο ρυθμός μετάδοσης του σήματος εξαρτάται από διάφορους παράγοντες όπως οι παράμετροι ραδιομετάδοσης (εμβέλεια, ανακλάσεις, απορρόφηση και ακτινοβολία), αλλά και ο αριθμός των χρηστών.

- **Ποιότητα επικοινωνίας**

  Μετά από εκατοντάδες εμπορικές και στρατιωτικές εφαρμογές, οι τεχνολογίες ασύρματης μετάδοσης έχουν γίνει πολύ αξιόπιστες. Αυτές μπορούν να παρέχουν στους χρήστες τους αξιόπιστες συνδέσεις και σε καλύτερο επίπεδο από ότι οι αντίστοιχες στην κινητή τηλεφωνία

- **Συμβατότητα με το υπάρχον δίκτυο**

  Τα πιο πολλά ασύρματα δίκτυα έχουν συγκεκριμένο τρόπο διασύνδεσης με τα ενσύρματα δίκτυα. Έτσι η προσάρτηση ασύρματης δικτύωσης, σε υπάρχουσες δομές δικτύων, μπορεί να γίνει με εύκολο τρόπο.

- **Παρεμβολές**

  Το ασύρματο τοπικό δίκτυο μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλες συσκευές που λειτουργούν στα 2.4 GHz όπως άλλα ασύρματα δίκτυα, ασύρματα τηλέφωνα, φούρνοι μικροκυμάτων και συσκευές Bluetooth. Σημαντικότερες όμως είναι οι παρεμβολές που προκύπτουν από την κακή σχεδίαση ενός ασύρματου δικτύου.

Για τον παραπάνω λόγο χρησιμοποιείται το 802.11a όπου είναι πιο καθαρή μπάντα.

- **Διαλειτουργικότητα**

  Οι περιπτώσεις κατά τις οποίες οι συσκευές δε συνεργάζονται μεταξύ τους είναι:

  - ✓ **Διαφορετικές τεχνολογίες**

    Μια μετάδοση βασισμένη σε τεχνολογία FHSS δεν μπορεί να συνεργαστεί με κάποια που βασίζεται σε τεχνολογία DSSS.

  - ✓ **Διαφορετικές συχνότητες**

    Συσκευές που λειτουργούν σε συχνότητα 5 (5,4 ή 5,7) GHz δεν μπορούν να δουλέψουν μαζί με συσκευές που εργάζονται στα 2,4 GHz.

  - ✓ **Διαφορετικές υλοποιήσεις**

    Συσκευές που προέρχονται από διαφορετικούς κατασκευαστές μπορεί να μην συνεργάζονται ή να συνεργάζονται μερικώς μεταξύ τους. Μια προσέγγιση στη λύση του προβλήματος είναι η δημιουργία του πιστοποιητικού Wi – Fi.

    Μία λύση που εξετάζεται είναι η πρόταση της IEEE για τη διαπομπή σε ετερογενή δίκτυα. Μία ομάδα της IEEE ασχολείται με την επίτευξη διαπομπής και συμβατότητας μεταξύ δικτύων με διαφορετικό τύπο τεχνολογίας, που μπορεί να ανήκει τόσο στο σύνολο των 802 προτύπων της IEEE όσο και σε άλλα πρότυπα (π.χ. κυψελωτά). Η κατεύθυνση στην οποία κινείται η ομάδα αυτή αναφέρεται ως MIH (Media Independent Handover), ενώ το σύνολο των σχετικών προτύπων είναι γνωστά ως 802.21.

Γενικότερα τα τελευταία χρόνια, ο στόχος διάφορων ερευνητικών σταθμών είναι οι έρευνες με στόχο την αύξηση της ευελιξίας των ασύρματων επικοινωνιών. Η τεχνολογία του Cognitive Radio ή Γνωστικά Συστήματα Ραδιοεπικοινωνιών αποβλέπει στην βελτίωση της επικοινωνίας, επιτρέποντας στα ασύρματα δίκτυα να διαθέτουν ευφυΐα – νοημοσύνη για να προσαρμόζονται κατάλληλα στις συνθήκες λειτουργίας.

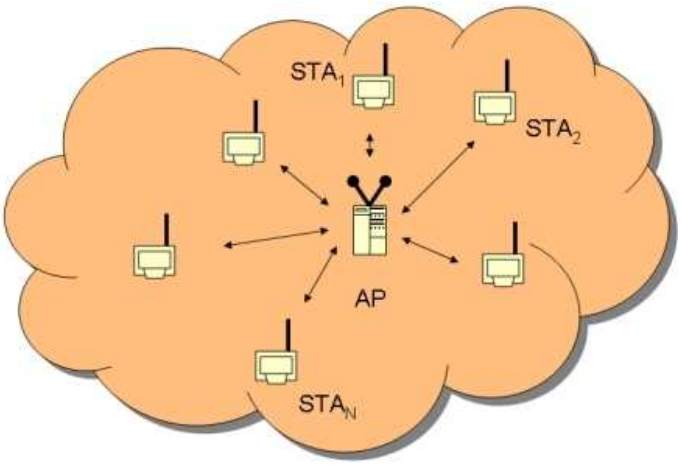
1.6.3 Η Τοπολογία του 802.11

Η τοπολογία του 802.11 αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο που να παρέχει την δυνατότητα μετακίνησης των σταθμών η οποία να μην γίνεται αντιληπτή από τα ανώτερα στρώματα, όπως το LLC (Logical Link Control). Ένας σταθμός (station) είναι κάθε συσκευή η οποία εμπεριέχει τις λειτουργίες του 802.11 (δηλαδή το επίπεδο MAC, το φυσικό στρώμα και μια διασύνδεση (Interface) με το ασύρματο μέσο.

Οι λειτουργίες του 802.11 προϋπάρχουν από τον κατασκευαστή σε μια ασύρματη κάρτα δικτύου (NIC), ενώ το λογισμικό διασύνδεσης οδηγεί την κάρτα (NIC) και τον σταθμό βάσης AP (Access Point).

- **BSS (Basic Service Set)**

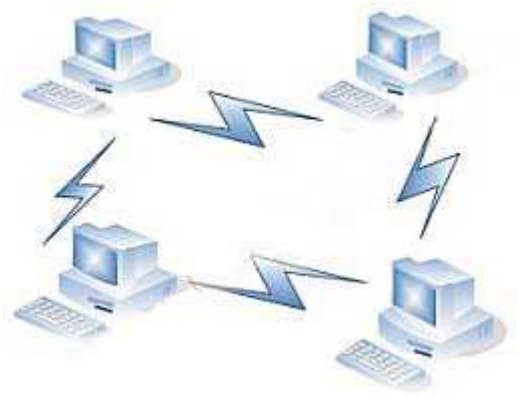
  Το βασικό δομικό στοιχείο ενός 802.11 LAN είναι το BSS (Basic Service Set). Στο παρακάτω σχήμα φαίνεται ένα BSS, το οποίο έχει N σταθμούς (STA_N), οι οποίοι είναι μέλη του BSS. Αν ένας σταθμός μετακινηθεί έξω από το BSS δεν μπορεί πλέον να επικοινωνεί άμεσα με τα άλλα μέλη του συγκεκριμένου BSS.



Εικόνα 1. 7 Σχηματική αναπαράσταση ενός BSS

- **IBSS (Independent Basic Service Set)**

  Το IBSS ή peer-to-peer ή Ad-Hoc είναι μια πολύ απλή τοπολογία για ασύρματα δίκτυα. Οι σταθμοί είναι ίσοι μεταξύ τους και επικοινωνούν ένας προς έναν χωρίς να υπάρχει κεντρικός σταθμός επικοινωνίας.



Εικόνα 1. 8 Σχηματική αναπαράσταση ενός IBSS

Ωστόσο απαραίτητη προϋπόθεση για την σωστή λειτουργία ενός τέτοιου συστήματος, είναι ο κάθε σταθμός να βρίσκεται εντός της εμβέλειας του άλλου. Το σύστημα IBSS είναι χρήσιμο σε περιπτώσεις που είτε δεν υπάρχει ασύρματη υποδομή είτε οι περιοχές που πρόκειται να καλυφθούν είναι περιορισμένες.

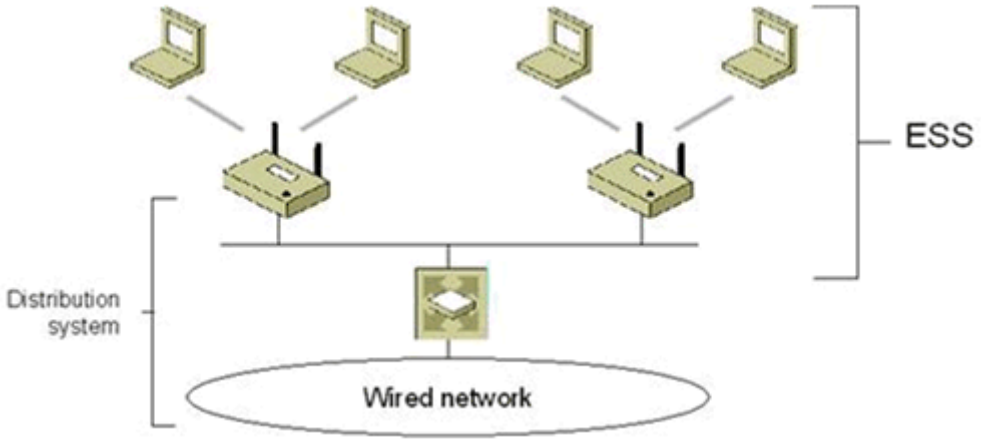
- **DS (Distribution System)**

  Με τον όρο DS εννοούμε ένα σύστημα διανομής. Πρόκειται για ένα δίκτυο το οποίο συνδέει τους σταθμούς βάσης τόσο μεταξύ τους όσο και με τα υπόλοιπα δίκτυα. Η πολύ μεγάλη ευελιξία στη σχεδίαση είναι ένα από τα βασικά πλεονεκτήματα της συγκεκριμένης τεχνολογίας.

- **ESS (Extended Service Set)**

  Όταν οι υπηρεσίες ενός συστήματος IBSS δεν είναι αρκετές, τότε στρεφόμαστε στην πιο σύνθετη δομή ενός τοπικού δικτύου, που ονομάζεται ESS. Με τη βοήθεια αυτού του συστήματος είναι δυνατή η διασύνδεση και η επικοινωνία πολλών BSS μεταξύ τους. Το στοιχείο που χρησιμοποιείται για την διασύνδεση των BSS είναι το σύστημα διανομής DS.

  Η πρόσβαση στο σύστημα διανομής γίνεται με την βοήθεια ενός σταθμού AP, ο οποίος παρέχει τη διασύνδεση των σταθμών που βρίσκονται σε διάφορα BSS στο σύστημα διανομής. Η διασύνδεση αυτή φαίνεται στην εικόνα 1.4.



Εικόνα 1. 9 Η σύνδεση των BSSs με το DS

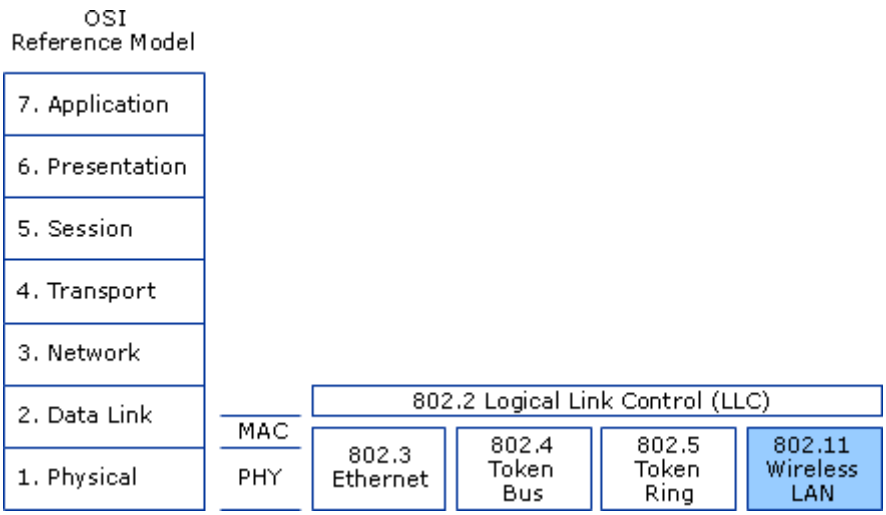
Η πληροφορία μετακινείται από BSS σε BSS μέσω των AP του συστήματος διανομής (DS), ενώ το σύστημα διανομής υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές να ελέγχουν την αντιστοίχηση της διεύθυνσης στον προορισμό για κάθε σταθμό που μετακινείται.

1.6.4 Η Αρχιτεκτονική του 802.11

Ενώ η τοπολογία καθορίζει τα αναγκαία μέσα για τη φυσική διασύνδεση του ασύρματου δικτύου, η αρχιτεκτονική καθορίζει τον τρόπο λειτουργίας του δικτύου. Η επιτροπή των 802.11 προτύπων ορίζει δύο ενδιάμεσα επίπεδα από το $2^{ο}$ επίπεδο (μετάδοση δεδομένων) του μοντέλου OSI. Αυτά τα επίπεδα είναι:

- ✓ LLC (802.2 Logical Link Control)
- ✓ MAC (Media Access Control)

Το ασύρματο πρότυπο 802.11 ορίζει τις προδιαγραφές για το φυσικό επίπεδο και το επίπεδο MAC που επικοινωνούν, μέχρι το επίπεδο LLC όπως φαίνεται στην εικόνα 1.5.



Εικόνα 1. 10 Σύγκριση OSI με 802.11

Τα πρωτόκολλα που χρησιμοποιούνται από όλες τις παραλλαγές του 802 (Ethernet, Token Bus, Token Ring, WLAN), όπως φαίνεται στην εικόνα 1.5, έχουν κοινά σημεία στη δομή τους.

- **Φυσικό Επίπεδο (Physical Layer)**

  Το πρότυπο 802.11 του 1997 καθορίζει πέντε επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο:

  - ✓ **Υπέρυθρες**
  - ✓ **FHSS (Frequency Hopping Spread Spectrum)**
  - ✓ **DHSS (Direct Sequence Spread Spectrum)**
  - ✓ **OFDM (Orthogonal Frequency-Division Multiplexing)**
  - ✓ **HR-DSSS(High Rate Direct Sequence Spread Spectrum)**

  Οι τρεις πρώτες τεχνικές λειτουργούν σε 1 ή 2 Mbps και με αρκετά μεγάλη ισχύ, έτσι ώστε να μην παρουσιάζουν πολλές διενέξεις. Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές οι δύο τελευταίες οι OFDM και HR-DSSS. Λειτουργούν στα 54 Mbps και 11 Mbps αντίστοιχα.

- **Το Επίπεδο σύνδεσης δεδομένων (Data Link Layer)**

  Το επίπεδο σύνδεσης δεδομένων εφαρμόζεται σε όλους τους 802.11 σταθμούς και επιτρέπει στο σταθμό να εγκαθιδρύει ένα δίκτυο ή να συμμετέχει σε ένα ήδη υπάρχον δίκτυο και να μεταφέρει δεδομένα που περνούν από το επίπεδο λογικής σύνδεσης ελέγχου (LLC).

  Αυτές οι λειτουργίες γίνονται χρησιμοποιώντας δύο μεθόδους υπηρεσιών. Τις υπηρεσίες σταθμών (Station Services) και τις υπηρεσίες των συστημάτων διανομής (Distribution System Service). Πριν όμως αρχίσουν να πραγματοποιούνται οι υπηρεσίες MAC επιπέδου, πρώτα πρέπει να πραγματοποιηθεί η πρόσβαση στο

ασύρματο μέσο. Το υπόστρωμα MAC παρέχει τις ακόλουθες βασικές λειτουργίες:

- ✓ Τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης.
- ✓ Τη λειτουργία της αναμετάδοσης του πακέτου.
- ✓ Τη λειτουργία της επιβεβαίωσης λήψης.
- ✓ Τη λειτουργία του κατακερματισμού και της επανασυναρμολόγησης του πακέτου.

- **Η πρόσβαση στο Ασύρματο Μέσο**

  Σε ένα ασύρματο δίκτυο είναι πιο περίπλοκο να μοιράζουμε την πρόσβαση μεταξύ των σταθμών διανομής από ότι σε ένα ενσύρματο. Αυτό συμβαίνει επειδή ένας ασύρματος σταθμός δεν είναι σε θέση να ανιχνεύσει μια σύγκρουση που μπορεί να συμβεί στη μετάδοσή του με την μετάδοση ενός άλλου σταθμού. Σε ένα ενσύρματο δίκτυο είναι εύκολο να ανιχνευτούν τυχόν συγκρούσεις με τον μηχανισμό Carrier Sense Multiple Access / Collision Detection (CSMA/CD).

  Το πρότυπο 802.11 καθορίζει έναν αριθμό από λειτουργίες συντονισμού του MAC επιπέδου για να συντονίσει την πρόσβαση μέσου μεταξύ πολλαπλών σταθμών. Η πρόσβαση στο μέσο μπορεί να γίνει είτε μέσω της λειτουργίας κατανεμημένου συντονισμού (Distributed Coordination Function – DCF), είτε μέσω της λειτουργίας σημείου συντονισμού (Point Coordination Function – PCF).

1.7 ΕΠΙΛΟΓΟΣ

Η χρήση των ασύρματων δικτύων είναι πλέον κοινός τόπος σε οικιακούς και εταιρικούς χώρους, ενώ έχει ήδη ξεκινήσει και επεκτείνεται η εξάπλωσή τους σε μητροπολιτική κλίμακα.

Στο κεφάλαιο αυτό μελετήθηκε το πρότυπο 802.11 που είναι πλέον ευρέως διαδεδομένο για τα ασύρματα δίκτυα. Αναφέρθηκαν γενικώς τα πλεονεκτήματα και τα μειονεκτήματα, υπογραμμίστηκαν τα δομικά στοιχεία των ασύρματων δικτύων και αναλύθηκε μία τεχνολογία ασύρματης δικτύωσης που στις μέρες μας έχει διευκολύνει την πρόσβαση στο διαδίκτυο και έχει απλοποιήσει τον τρόπο διασύνδεσης των χρηστών.

Δυστυχώς όμως το εύκολο και γρήγορο δεν είναι πάντα ασφαλές. Στο επόμενο κεφάλαιο θα μελετηθεί η ασφάλεια στα ασύρματα δίκτυα και οι κίνδυνοι που κρύβουν. Επίσης θα αναλυθεί πόσο ευάλωτες είναι οι δικλείδες ασφαλείας σε κακόβουλους «γνώστες» χρήστες, έτσι ώστε να προκαλέσουν την πρόσβασή τους στο δίκτυο.

Μεγάλη έμφαση θα δοθεί στο δημοφιλές στους κοινούς χρήστες “Wi–Fi” ή αλλιώς στο πρότυπο 802.11.

ΚΕΦΑΛΑΙΟ 2

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

2.1 ΕΙΣΑΓΩΓΗ

Οι χρήστες ενός ασύρματου δικτύου φυσικά μπορούν να επωφεληθούν από ένα σωρό πλεονεκτήματα, όμως σε αυτή την περίπτωση τίθεται ένα πολύ σημαντικό ερώτημα: Πόσο ασφαλής είναι η επικοινωνία σε ένα σύστημα όπου το μέσο μετάδοσης της πληροφορίας είναι ο αέρας;

Επιπλέον η ευρεία χρήση του διαδικτύου για την διακίνηση προσωπικών πληροφοριών αναδεικνύει ακόμα πιο πολύ το θέμα της ασφάλειας των δικτύων.

Η λύση έχει ήδη δοθεί (εν μέρει) με τις μεθόδους πιστοποίησης και κρυπτογράφησης των δεδομένων που χρησιμοποιούνται ευρέως σήμερα. Σε ένα ενσύρματο τοπικό δίκτυο οι απειλές αντιμετωπίζονται στο σημείο εξόδου προς το ISP (Internet Service Provider) με πολιτικές ασφάλειας στους δρομολογητές, με firewall κτλ.

Όμως σε ένα ασύρματο δίκτυο όλα τα παραπάνω δεν ισχύουν. Ιδιότητες της ασφαλούς επικοινωνίας αποτελούν τα ακόλουθα:

- Επικύρωση: Πριν από την μετάδοση δεδομένων, οι κόμβοι αναγνωρίζονται και ανταλλάσουν επικυρωμένα πιστοποιητικά.
- Κρυπτογράφηση: Πριν την αποστολή ενός ασύρματου πακέτου δεδομένων, ο κάθε υπολογιστής που το στέλνει θα πρέπει να το κρυπτογραφήσει.
- Ακεραιότητα: Διασφαλίζει ότι το στοιχείο που μεταδίδεται δεν έχει τροποποιηθεί.
- Μυστικότητα: Είναι ο όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα που προστατεύονται ενάντια στην ανάγνωση από αναρμόδια συμβαλλόμενα μέρη.

2.2 ΕΠΙΚΥΡΩΣΗ ΚΑΙ ΜΥΣΤΙΚΟΤΗΤΑ

Στην ουσία η έννοια της επικύρωσης αφορά τον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αποκτήσουμε πρώτα έλεγχο πρόσβασης στο μέσο και στη συγκεκριμένη περίπτωση στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και ακολούθως το δίκτυο επικυρώνει το σταθμό και ο σταθμός επικυρώνει το δίκτυο.

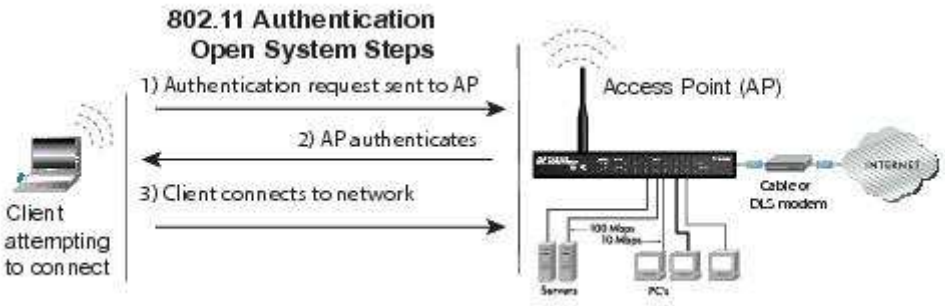
Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons – πλαίσια διαχείρισης (υπάρχει όμως και η περίπτωση να μην στέλνει beacons γιατί έχει κρυφό SSID όπου τότε περιμένει να λάβει αίτηση για να απαντήσει).

Τα beacons είναι αυτά τα οποία ανακοινώνουν την ύπαρξη ενός δικτύου. Το κάθε beacon περιλαμβάνει ένα Service Set Identifier (SSID) ή αλλιώς όνομα δικτύου. Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε ενεργητικά. Στην παθητική σάρωση ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης. Στην δεύτερη περίπτωση στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID, είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση.

Ακολούθως ο σταθμός διαλέγει το δίκτυο που θέλει να συνδεθεί. Την απόφαση μπορεί να λάβει ο ίδιος ο χρήστης ή ένα κατάλληλο λογισμικό που επιλέγει βασιζόμενο στην ισχύ του σήματος ή σε άλλα κριτήρια.

Στο 802.11 έχουμε δύο ειδών τρόπους επικύρωσης. Την επικύρωση ανοιχτού κλειδιού (Open System Authentication – OSA) και την επικύρωση μοιρασμένου κλειδιού (Shared Key Authentication – SKA). Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα της αίτησης επικύρωσης. Το δίκτυο μπορεί να δεχτεί ή αν απορρίψει αυτή την πρόταση ανάλογα με τις ρυθμίσεις ασφαλείας.

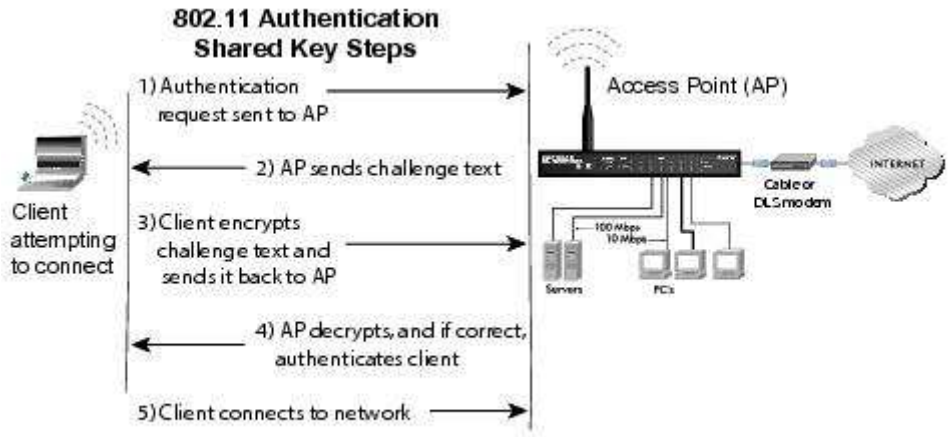
Χρησιμοποιώντας επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης όμως όχι και να επικοινωνήσει. Η συσκευή μπορεί να επικοινωνεί μόνο αν τα WEP κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης.



Εικόνα 2. 1 Επικύρωση Ανοιχτού Κλειδιού

Η επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόσκλησης – απάντησης. Για να χρησιμοποιήσουμε αυτή τη μέθοδο επικύρωσης, προϋποθέτει ότι το σημείο πρόσβασης και ο σταθμός είναι συμβατοί με τη λειτουργία WEP (Wired Equivalent Privacy) και ότι έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς

που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης.



Εικόνα 2. 2 Επικύρωση Μοιρασμένου Κλειδιού

(Σε όλες τις περιπτώσεις παρατηρείται η ομοιότητα στο Ethernet με το TCP/IP τη διαδικασία επικοινωνίας client-server το γνωστό 3-way-handshake. Ο όρος handshake χρησιμοποιείτε αρκετά και για την διαδικασία επικύρωσης στα ασύρματα δίκτυα.)

2.3 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Κρυπτογράφηση καλείται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή – μεταμφιέζονται προκειμένου να επιτευχθεί η ασφαλής μετάδοση πληροφοριών (encryption – E). Τα δεδομένα πριν από την κρυπτογράφηση ονομάζονται plaintext (P) ενώ τα δεδομένα μετά την κρυπτογράφηση αποτελούν το cipher text (C). Η αντίστροφη διαδικασία μετατροπής ονομάζεται αποκρυπτογράφηση (decryption).

Ο αλγόριθμος κρυπτογράφησης ή cipher είναι η μαθηματική ακολουθία που χρησιμοποιείται για την μεταμφίεση και αποκάλυψη των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης εμπεριέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενά τους.

2.3.1 WEP (Wired Equivalent Privacy)

Η πιο γνωστή επιλογή παροχής ασφάλειας για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11 είναι το Wired Equivalent Privacy (WEP). Με την επιλογή

του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα, μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν.

Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία αλλά και την ακεραιότητα των δεδομένων. Με τη βοήθεια ενός συμμετρικού αλγόριθμου κρυπτογράφησης, τον RC4, επιτυγχάνεται η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου.

Ο αλγόριθμος RC4 είναι ένας από τους σημαντικότερους παράγοντες της κρυπτογράφησης WEP, αφού μεταμορφώνει ένα σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτή η μέθοδος κάνει απλή τη διαδικασία διανομής κλειδιού, αφού το μόνο που θα πρέπει να μεταδοθεί μεταξύ των σταθμών είναι το μυστικό κλειδί.

Οι αδυναμίες του WEP ωστόσο είναι πολλές. Μέθοδοι για να ηττηθεί το WEP προκύπτουν από παντού.

2.3.2 TKIP (Temporal Key Integrity Protocol)

Μετά από τη συνειδητοποίηση της κρισιμότητας της κατάστασης και του κενού ασφαλείας που άφηνε το WEP, αναδύθηκε η λύση του TKIP.

Το TKIP προσφέρει μεγαλύτερη ασφάλεια καθώς παρέχει ανάμιξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό αναπαραγωγής κλειδιών, ο οποίος επιδιορθώνει τα ελαττώματα του WEP. Ενώ το μόνο που απαιτούσε στην αυγή της εμφάνισής του ήταν η αναβάθμιση του firmware και πιθανώς του λογισμικού-οδηγού της συσκευής.

Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο WEP για να ενισχύσει την ασφάλεια και να μειώσει τον αριθμό των επιθέσεων του WEP.

2.3.3 WPA (WI-FI PROTECTED ACCESS)

Το 2003, όταν άρχισε να γίνεται εμφανές το κενό ασφαλείας που άφηνε η κρυπτογράφηση WEP, η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA). Το WPA προέρχεται από το 802.11 πρότυπο και είναι σαν μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές.

Το WPA κάνει χρήση της μεθόδου TKIP, που προαναφέρθηκε και αυξάνει σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα

συστήματα LAN. Επίσης για τους οικιακούς χρήστες, το WPA παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key).

Το πρότυπο WPA ορίζει επίσης τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP. Η υποστήριξη προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο κατασκευαστής όσον αφορά τα προγράμματα οδήγησης.

2.3.4 AES (Advanced Encryption Standard)

Το WPA παρέχει τη δυνατότητα για κρυπτογράφηση με δυο αλγόριθμους, το RC4 και τον AES για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα.

Ο AES αποτελεί την νεότερη μέθοδος κρυπτογράφησης που έχει επιλεγεί από την κυβέρνηση των Η.Π.Α. για να αντικαταστήσει τον αλγόριθμο DES το 2001. Ο AES χρησιμοποιεί ένα αλγόριθμο γνωστό ως Rijndael.

Ο αλγόριθμος Rijndael πήρε το όνομα από τους δύο Ελβετούς εφευρέτες του Joan Daemen και Vincent Rijmen. Πρόκειται για έναν αλγόριθμο κρυπτογράφησης ομάδας (block), που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits, η οποία ονομάζεται μπλοκ.

Στις μέρες μας μπορούμε να βρούμε προϊόντα AES WRAP (Wireless Robust Authentication Protocol), αλλά η τελική προδιαγραφή καθορίζει τον αλγόριθμο AES CCMP (Counter Mode-Cipher Block Chaining Mac Protocol). Οι προδιαγραφές του 802.11i παρέχουν επίπεδο μετάδοσης δεδομένων βασισμένο στον AES. Η χρησιμοποίηση του πρότυπου AES μας προστατεύει από τις ενεργές ασύρματες επιθέσεις. Ωστόσο πρέπει να αναγνωριστεί ότι ένα ασύρματο πρωτόκολλο του επιπέδου μετάδοσης δεδομένων μπορεί να προστατεύσει μόνο το ασύρματο υποδίκτυο. Στα σημεία που η κίνηση διέρχεται από άλλα τμήματα του δικτύου, είτε σε δίκτυα τοπικής ή ευρείας περιοχής, απαιτείται προστασία υψηλού επιπέδου και κρυπτογράφηση από σημείο σε σημείο.

2.3.5 CCMP (Counter Mode With Cipher Block Chaining Message Authentication Code Protocol)

Η προσθήκη στο πρότυπο 802.11 που ορίζει την ασφάλεια της επόμενης γενιάς για τα ασύρματα δίκτυα ονομάζεται 802.11i. Το πρότυπο εκδόθηκε τελικά το 2004.

Το πρότυπο αυτό ορίζει μία νέα μέθοδο, για την ασφάλεια των δεδομένων στο MAC επίπεδο. Η μέθοδος αυτή (CCMP) λειτουργεί σύμφωνα με τον αλγόριθμο

κρυπτογράφησης AES. Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων.

2.3.6 WPA2 (Wi-Fi Protected Access Version 2)

Το WPA2 είναι ο διάδοχος του WPA και προορίζεται για να θέσει σε απευθείας σύνδεση το WPA με το 802.11i πρότυπο. Το WPA2 διαθέτει συμβατότητα προς τα πίσω με το WPA, όπως και με την κρυπτογράφηση TKIP και AES, την 802.1X / EAP επικύρωση και την τεχνολογία PSK, που είναι όλα μέρη του προτύπου. Τα ασύρματα δίκτυα που υποστηρίζουν την μικτή λειτουργία WPA και WPA2 κάνουν πιο εύκολη την μεταφορά των δεδομένων ανάμεσα στα πρότυπα.

Μια από τις πρώτες βελτιώσεις του WPA2 είναι ότι με την προσθήκη του AES CCMP, όπως στο 802.11i, παρέχει τη δυνατότητα ισχυρής κρυπτογράφησης. Μια άλλη βελτίωση που περιλαμβάνει το WPA2 είναι τη δυνατότητα για γρήγορη περιαγωγή. Αυτή η ικανότητα είναι σημαντική για τις εφαρμογές ήχου, όπου η μεταφορά τους είναι υψηλής ευαισθησίας. Η γρήγορη περιαγωγή επιτυγχάνεται με την επικύρωση των σταθμών και στα γειτονικά σημεία πρόσβασης αλλά και στο τελικό σημείο πρόσβασης όπου επιτυγχάνεται η επικοινωνία.

Υπάρχουν δύο εκδόσεις WPA2. Το WPA2-Personal και το WPA2-Enterprise. Το πρώτο προστατεύει την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες με τη χρήση της εγκατάστασης ενός κωδικού πρόσβασης. Το WPA2-Enterprise πιστοποιεί τους χρήστες του δικτύου μέσω ενός εξυπηρετητή.

2.3.7 Robust Secure Network (RSN)

Το πρότυπο 802.11i ορίζει έναν νέο τύπο ασύρματου δικτύου, το οποίο ονομάζεται Δίκτυο Ανθεκτικής Ασφάλειας (RSN).

Οπωσδήποτε οι ασύρματες συσκευές που θα υποστηρίζουν ένα τέτοιο δίκτυο θα πρέπει να έχουν νέες δυνατότητες. Αυτές είναι η επικύρωση, η διαχείριση κλειδιών σε υψηλό επίπεδο, η κρυπτογράφηση και την επικύρωση των δεδομένων που διακινούνται σε MAC επίπεδο.

Ένα δίκτυο RSN έχει πολύ αυστηρούς περιορισμούς όσον αφορά την προσβασιμότητα και επιβάλλονται αρκετοί περιορισμοί ασφάλειας. Ωστόσο, επειδή χρειάζεται χρόνος για να αναβαθμιστούν οι συσκευές και ο εξοπλισμός, το πρότυπο 802.11i ορίζει το Δίκτυο Μεταβατικής Ασφάλειας (Transitional Security Network – TSN).

Τα δίκτυα TSN υποστηρίζουν δίκτυα όπως το RSN αλλά και το WEP. Οι χρήστες που εισέρχονται σε ένα δίκτυο TSN μπορούν να λειτουργήσουν παράλληλα για όλα τα προηγούμενα συστήματα ασφάλειας.

2.4 ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Η γοητεία της πρόσβασης σε ένα ξένο μέσο και η εξερεύνηση δεδομένων που θεωρούνται μυστικά ή με άλλα λόγια ξένα για εμάς, αποτελούν ένα πολύ σημαντικό κίνητρο για πολλούς από τους επίδοξους επιτιθέμενους. Ωστόσο οι προθέσεις και οι στόχοι κάθε επίθεσης μπορεί να διαφέρουν. Μέσα σε γενικότερα πλαίσια, οι επιθέσεις σε ασύρματα δίκτυα μπορούν να χωριστούν σε παθητικές και ενεργητικές.

Ως παθητικές ορίζονται οι επιθέσεις που δε συμμετέχει ο επιτιθέμενος στο δίκτυο. Επίθεση τέτοιου τύπου αποτελεί το Sniffing ή Footprinting.

Οι ενεργητικές επιθέσεις προϋποθέτουν ότι ο επιτιθέμενος αναλαμβάνει ενεργή συμμετοχή στο δίκτυο. Οι ενεργητικές επιθέσεις χωρίζονται σύμφωνα με το σκοπό που έχουν οι επιτιθέμενοι σε τρεις βασικές κατηγορίες:

- Man in the Middle Attack (Τροποποίηση Δεδομένων)
- Spoofing (Μεταμφίεση)
- Denial Of Service – DoS Attack (Άρνηση Υπηρεσιών)

2.4.1 Παθητικές Επιθέσεις - Sniffers

Το Sniffing σχετίζεται με την ανάκτηση απόρρητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες και επαρκεί η φυσική πρόσβαση στο μέσο μεταφοράς για να επιτευχθεί. Έτσι ο επιτιθέμενος είναι σε θέση να διαβάσει όλες τις πληροφορίες που διακινούνται στο συγκεκριμένο δίκτυο, χωρίς να γίνει αισθητή η παρουσία του.

Ο επιτιθέμενος λοιπόν είναι σε θέση να γνωρίζει το SSID του ασύρματου δικτύου, μπορεί να προσδιορίσει τον κατασκευαστή του AP (Access Point) με την εξέταση της MAC διεύθυνσης και να εξακριβώσει πόσοι και ποιοί σταθμοί είναι συνδεδεμένοι με το συγκεκριμένο AP.

Εάν όμως χρησιμοποιείται κρυπτογράφηση στο δίκτυο, για παράδειγμα κρυπτογράφηση WEP, τότε ο επιτιθέμενος μπορεί να εξετάσει εάν χρησιμοποιείται ένα κλειδί ή εάν κάθε συσκευή έχει χωριστό κλειδί εντοπίζοντας τα αντίστοιχα bit στις 802.11 επιγραφές. Έτσι στη συνέχεια της εξέλιξης της επίθεσης αυτές οι

πληροφορίες θα φανούν χρήσιμες στον επιτιθέμενο και αυτό εξαρτάται από το στόχο ή το σκοπό του.

Μία άλλη μέθοδος είναι η τεχνική Footprinting (ανάλυση κυκλοφορίας). Το Footprinting είναι η μελέτη των εξωτερικών στοιχείων των μηνυμάτων (π.χ. η συχνότητα επικοινωνίας και το μέγεθος των πακέτων που διακινούνται). Με αυτό τον τρόπο είναι δυνατό να μαθευτούν πληροφορίες για τα δομικά στοιχεία και την πολιτική ασφάλειας που εφαρμόζεται στο δίκτυο.

2.4.2 Ενεργητικές Επιθέσεις: Man in the Middle Attack

Οι μέθοδοι τροποποίησης δεδομένων έχουν πολλούς διαφορετικούς στόχους, που κυμαίνονται από την τροποποίηση του ηλεκτρονικού ταχυδρομείου με κακόβουλο περιεχόμενο έως και την αλλαγή αριθμών σε μια ηλεκτρονική τραπεζική μεταφορά.

Ωστόσο παρότι τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν πραγματοποιηθεί στο παρελθόν, είναι αρκετά περιορισμένες στην πράξη λόγω του βαθμού δυσκολίας που έχουν.

Παράδειγμα αυτής της τεχνικής που είναι πιο κοντά στην πραγματικότητα είναι η αλλαγή της IP διεύθυνσης προορισμού ενός μηνύματος το οποίο διαβιβάζεται σε μια ασύρματη μετάδοση, το οποίο αντί να διαβιβαστεί στον αρχικό πραγματικό παραλήπτη, μεταφέρετε στον υποδυόμενο (και ορισμένο από τον επιτιθέμενο) παραλήπτη. Αυτή η τεχνική χρησιμοποιείται διότι το μήνυμα στην ασύρματη σύνδεση κρυπτογραφείται και δεν μπορεί να διαβαστεί το περιεχόμενο. Εάν ο επιτιθέμενος μπορεί να το πάρει διαβιβασμένο από το δίκτυο, θα λάβει την αποκρυπτογραφημένη έκδοση.

2.4.3 Ενεργητικές Επιθέσεις: Spoofing Attack

Κατά το Spoofing, ο επιτιθέμενος υποκρίνεται κάποιον νόμιμο χρήστη του δικτύου ώστε να αποκτήσει τα δικαιώματα σε δεδομένα ή πρόσβασης σε υπηρεσίες που επιθυμεί. Ουσιαστικά γίνεται χρήση της MAC διεύθυνσης, της IP διεύθυνσης ή των στοιχείων πρόσβασης (π.χ. όνομα χρήστη και κωδικός πρόσβασης) του νόμιμου χρήστη παραπλανώντας έτσι τις αντίστοιχες δικλείδες ασφαλείας στα αντίστοιχα επίπεδα δικτύου, από το φυσικό επίπεδο μέχρι το επίπεδο εφαρμογών.

Η μέθοδος αυτή είναι ιδανική εάν ο επιτιθέμενος θέλει να μην αποκαλυφθεί. Εάν η συσκευή του επιτιθέμενου «ξεγελάσει» το δίκτυο, τότε παίρνει

όλα τα δικαιώματα πρόσβασης που έχει η πραγματικά εξουσιοδοτημένη συσκευή. Επιπλέον δεν θα υπάρξει καμία προειδοποίηση ασφαλείας.

2.4.4 Ενεργητικές Επιθέσεις: Denial of Service – DoS Attack

Σε αυτή την περίπτωση τόσο ο σκοπός αλλά και η τεχνική της μεθόδου διαφέρουν. Σκοπός μιας τέτοιας επίθεσης είναι η ολική αχρήστευση του ασύρματου δικτύου για ένα χρονικό διάστημα. Ουσιαστικά αφαιρούνται τα δικαιώματα από όλους τους νόμιμους και μη νόμιμους χρήστες του δικτύου. Μια τέτοια επίθεση μπορεί να πραγματοποιηθεί με δυο τρόπους. Η πρώτη μέθοδος απλά κατακλύζει το στόχο υπολογιστή ή την NIC με πληροφορίες, ώστε να μπλοκάρει. Με τη δεύτερη μέθοδο στέλνονται καλά διατυπωμένες εντολές ή λάθος δεδομένα με στόχο να κολλήσει το σύστημα. Οι επιθέσεις DoS είναι οι πιο επικίνδυνες διότι υπάρχει μικρότερο περιθώριο προστασίας. Οι πέντε πιο γνωστοί μέθοδοι επιθέσεων DoS αναφέρονται ονομαστικά παρακάτω:

- **Flood Attack**
- **Ping of Death**
- **SYN**
- **Teardrop**
- **Smurf**

2.5 ΟΙ ΕΠΙΘΕΣΕΙΣ ΣΤΗΝ ΠΡΑΞΗ

Η ανάλυση και η περιγραφή μιας επίθεσης σε ένα ασύρματο δίκτυο που γίνεται παρακάτω θα είναι σύντομη και περιληπτική, δίχως λεπτομέρειες, και αναφέρεται ως παράδειγμα για εκπαιδευτικούς σκοπούς. Για περισσότερες λεπτομέρειες και πληροφορίες ο αναγνώστης μπορεί να ανατρέξει στο διαδίκτυο όπου υπάρχει πληθώρα από εγχειρίδια και βίντεο.

Οι μέθοδοι που χρησιμοποιούνται για την διείσδυση σε ένα ασύρματο δίκτυο δεν είναι δαπανηρές ούτε χρειάζονται την υποδομή κάποιου εξεζητημένου υλικού. Απαραίτητα εργαλεία αποτελούν ένας υπολογιστής, μια (συμβατή με τις μεθόδους που πρόκειται να χρησιμοποιηθούν) ασύρματη κάρτα δικτύου και το αντίστοιχο λογισμικό. Επίσης ο επιτιθέμενος θα πρέπει να βρίσκεται εντός εμβέλειας του στόχου του.

Ένα ευρέως διαδεδομένο πακέτο λογισμικών για άτομα που θέλουν να υποβάλουν το δίκτυό τους σε δοκιμασίες ασφάλειας είναι το BackTrack. Το Backtrack δεν είναι τίποτα άλλο από μια διανομή Linux που περιέχει μόνο μια

μεγάλη ποικιλία εργαλείων και εφαρμογών ανοικτού κώδικα για δοκιμές ασφάλειας δικτύων.

Εικόνα 2. 3 BackTrack 5 Επιφάνεια Εργασίας & Μενού

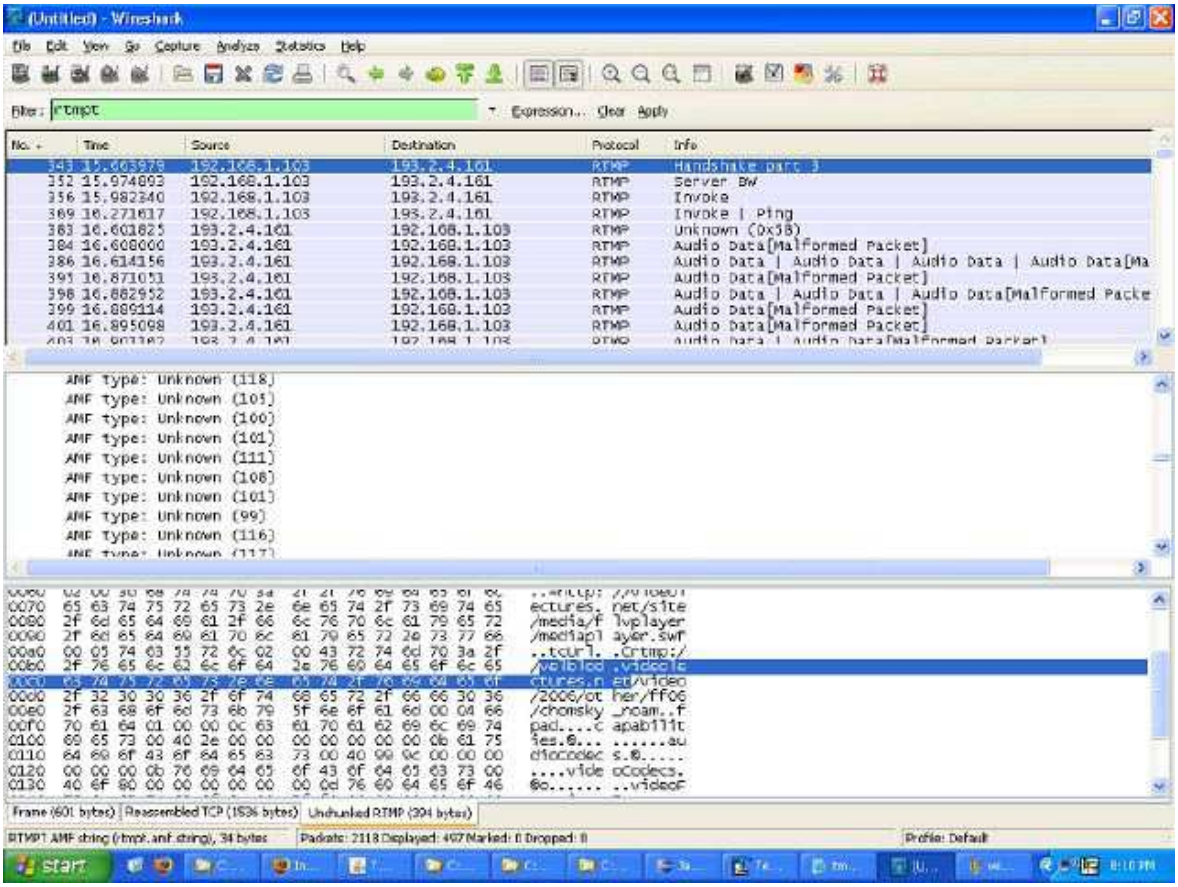
Οι κατηγορίες των εργαλείων του BackTrack που βοηθούν στην διείσδυση σε ένα ασύρματο δίκτυο είναι οι εξής:

- Συλλογή Πληροφοριών (Information Gathering)
- Χαρτογράφηση Δικτύων (Network Mapping)
- Ανάλυση Ράδιο-Δικτύων (Radio Network Analysis)

Υπάρχουν και άλλες κατηγορίες εργαλείων που αντικείμενο και στόχο έχουν την διείσδυση σε ιστοσελίδες, πληροφοριακά συστήματα ή λειτουργικά συστήματα.

2.5.1 Wireshark

Αποτελεσματικό εργαλείο και δημοφιλές για την παρακολούθηση όχι μόνο ενσύρματων, αλλά και ασύρματων τοπικών δικτύων είναι το Wireshark. Το Wireshark αυτό που κάνει είναι να μας παρουσιάζει τα περιεχόμενα των Ethernet πακέτων που κυκλοφορούν σε ένα δίκτυο σε ευανάγνωστη μορφή για τον χρήστη.



Εικόνα 2. 4 Γραφικό Περιβάλλον του Wireshark

Οι πληροφορίες που αποκτούνται με τη χρήση του Wireshark είναι οι MAC διευθύνσεις όλων των υπολογιστών που εκπέμπουν στο δίκτυο τη συγκεκριμένη χρονική στιγμή, τις IP διευθύνσεις, το πρωτόκολλο μετάδοσης και φυσικά τα δεδομένα. Τονίζεται ότι το Wireshark δεν απαιτεί από το υπολογιστικό σύστημα που φιλοξενείται να έχει πρόσβαση στο δίκτυο υπό παρακολούθηση. Η σύνδεση στο φυσικό μέσω επαρκεί, που στην περίπτωση των ασύρματων δικτύων, όπως έχει αναφερθεί, είναι ο αέρας.

2.5.2 Airmon-ng

Ένα ακόμη δημοφιλές πακέτο εργαλείων, επίσης αποτελεσματικό αποτελεί το airmon-ng. Δεν έχει γραφικό περιβάλλον και αυτό το κάνει να είναι λίγο πιο δύσκολο στη χρήση του. Το πακέτο airmon-ng περιέχει τα εξής εργαλεία που το καθένα με τη σειρά του μετά την εκτέλεσή του διαφωτίζει περισσότερο τον επιτιθέμενο:

- Airmon-ng
- Airodump-ng
- Aircrack-ng
- Aireplay-ng

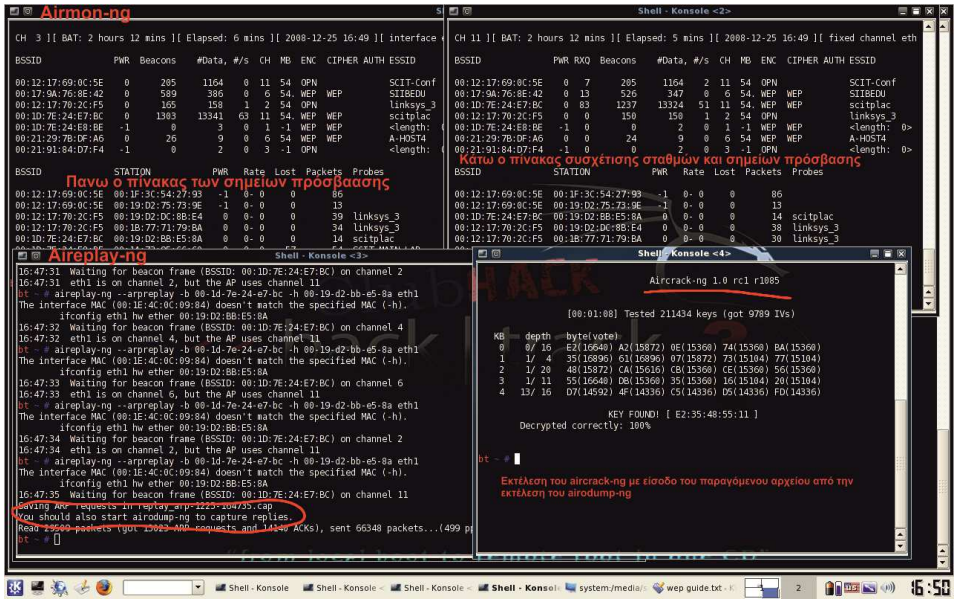
- Packetforge-ng

Το πακέτο airmon-ng, αντίθετα με το Wireshark, απαιτεί να τεθεί η κάρτα δικτύου σε κατάσταση παρακολούθησης. Εκτελώντας το airon-ng επιστρέφεται ένας πίνακας που περιέχει όλα τα σημεία πρόσβασης των ασύρματων δικτύων εντός εμβέλειας, ο οποίος και ανανεώνεται κάθε δευτερόλεπτο. Μερικά σημαντικά πεδία του πίνακα που επιστρέφεται είναι τα εξής:

- BSSID (MAC Address σημείου πρόσβασης)
- Beacons (ακέραιος αριθμός)
- Channel (1 – 11)
- Speed (Mbit/s)
- Encryption (WEP,WPA,WPA2)
- Cipher (WEP,CCMP)
- Authentication (PSK)
- ESSID (όνομα σημείου πρόσβασης)

Αφού επιλεχθεί το σημείο πρόσβασης για διείσδυση, εκτελείται παραμετροποιημένο το airmon-ng ξανά. Ο πίνακας πλέον που επιστρέφεται περιέχει και πληροφορίες για τους σταθμούς που έχουν συνδεθεί ήδη στο συγκεκριμένο ασύρματο δίκτυο.

Το μόνο πλέον που μένει να γίνει είναι μία ψεύτικη ταυτοποίηση για την συλλογή διανυσμάτων έναρξης (αφορά μόνο το WEP) αποθηκεύοντάς τα σε ένα τοπικό αρχείο. Εκτελούμε λοιπόν το airodump-ng το οποίο θα καταγράψει τα αιτήματα και τις επιβεβαιώσεις που θα διακινηθούν κατά την εκτέλεση του aireplay-ng παραμετροποιημένο για deauthentication του σταθμού-θύμα από το σημείο πρόσβασης. Ο σταθμός-θύμα θα προσπαθήσει να επανασυνδεθεί με το σημείο πρόσβασεις ανταλλάσοντας τα διανύσματα του κλειδιού. Έτσι το αρχείο που παρήγαγε το airodump-ng εισάγεται στο aircrack-ng και αποκρυπτογραφείται το WEP κλειδί.



Εικόνα 2. 5 Διαδοχικές οθόνες της υποκλοπής του WEP κλειδιού

Παρόμοια είναι και η διαδικασία και για τα WPA και WPA2. Οι διαφορές είναι η χρήση λεξικού για το σπάσιμο του κλειδιού και ο χρόνος επεξεργασίας για την αντιστοίχηση του 16δικού κλειδιού με αυτό στο ASCII.

2.5.3 Spoofing Software

Το Spoofing είναι η τεχνική της προσποίησης. Με τη βοήθεια της προσποίησης παρακάμπτονται διάφορες δικλείδες ασφαλείας που ελέγχουν τη φυσική (MAC) διεύθυνση και την IP διεύθυνση. Οι τεχνικές είναι γνωστές ως:

- IP Spoofing
- MAC Spoofing

Και οι δύο τεχνικές υλοποιούνται με την βοήθεια εργαλείων που κάνουν τις αντίστοιχες παραποιήσεις.

Με το IP Spoofing δημιουργούνται πακέτα με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.

Με το MAC Spoofing παραποιείται η εργοστασιακή MAC διεύθυνση της κάρτας δικτύου, έτσι ώστε να αποκρυφτεί η ύπαρξη του υπολογιστή και της κάρτας δικτύου ή για να του επιτραπεί η πρόσβαση σε ένα δίκτυο.

2.6 ΕΠΙΛΟΓΟΣ

Σε αυτό το κεφάλαιο μελετήθηκε η γηγενής ασφάλεια των ασύρματων τοπικών δικτύων που παρέχεται από την οικογένεια προτύπων 802.11. Επίσης αναφέρθηκε με ποιο τρόπο επιτυγχάνεται η επικύρωση, η μυστικότητα και οι διαθέσιμες τεχνικές κρυπτογράφησης που προσφέρεται από το 802.11.

Στη συνέχεια έγινε μία εγκυκλοπαιδική επισκόπηση σε τύπους επιθέσεων που αφορούν άμεσα τα ασύρματα δίκτυα και έχουν ως αδυναμία το μέσω μετάδοσής τους, που είναι ο αέρας. Παρ' όλα αυτά στην πράξη δεν είναι το ίδιο εύκολο με τη θεωρία. Αλλά δεν είναι και αδύνατον η διείσδυση σε ένα ασύρματο δίκτυο με τη βοήθεια και μόνο τριών απλών εργαλείων.

Το επόμενο κεφάλαιο εστιάζεται σε γνωστές τεχνικές ασφάλειας δικτύων, όπως είναι το firewall και γενικώς η διαχείριση του δικτύου. Θα αναφερθούν οι συνήθεις συμβουλές που δίνονται από τους ειδικούς για την θωράκιση ενός ασύρματου δικτύου και κατά πόσο τελικά αυτά μπορούν να αποτρέψουν μία εξωτερική επίθεση και διείσδυση σε ένα ασύρματο δίκτυο.

ΚΕΦΑΛΑΙΟ 3

ΤΕΧΝΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΠΑΡΑΚΑΜΨΗ ΤΟΥΣ ΣΕ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ

3.1 ΕΙΣΑΓΩΓΗ

Όπως φάνηκε στο προηγούμενο κεφάλαιο, ο επιτιθέμενος απέκτησε πρόσβαση στο δίκτυο και μετατρέπεται πλέον αυτομάτως σε εισβολέας. Οπότε δημιουργεί ανησυχία για την ασφάλειας των υπηρεσιών που προσφέρει το ασύρματο δίκτυο. Για αυτό η μη ικανοποιητική αποτελεσματικότητα των παλαιότερων μεθόδων κρυπτογράφησης και η μεγάλη εμβέλεια εκπομπής των ασύρματων δικτύων καθιστούν αναγκαία την ανεύρεση νέων περιοριστικών μεθόδων ασφάλειας που θα ενισχύσουν την προστασία των δεδομένων που μεταφέρονται με μέσο τον αέρα.

Οι έρευνες και οι μελέτες ανεύρεσης νέων μεθόδων κρυπτογράφησης είναι χρονοβόρες και στοιχίζουν αρκετά χρήματα μέχρι την υλοποίησή τους, έτσι οι προσπάθειες θωράκισης των ασύρματων δικτύων προσανατολίζονται προς την ανεύρεση λύσεων που θα προσφέρουν άμεσα αποτελέσματα με τη βοήθεια της υπάρχουσας τεχνογνωσίας των ενσύρματων δικτύων.

Ο αρχικός και βασικός στόχος κάποιου επιτιθέμενου σε ένα ασύρματο δίκτυο είναι το σημείο πρόσβασης (router/access-point). Αυτό επικρατεί διότι μετά την απόκτηση πρόσβασης στο τοπικό δίκτυο, ο επιτιθέμενος μπορεί να κινηθεί ανενόχλητος σε όποια κατεύθυνση επιθυμεί. Η παραμετροποίηση λοιπόν του δρομολογητή/σημείου πρόσβασης βοηθάει στην διαφύλαξη των δεδομένων. Στην καθημερινότητα αυτό σημαίνει, πως με τις εργοστασιακές ρυθμίσεις των δρομολογητών που υπάρχουν στην αγορά, υπάρχουν αποθηκευμένες και οι προκαθορισμένες ρυθμίσεις με τις οποίες το σημείο πρόσβασης θα λειτουργήσει με την πρώτη ενεργοποίηση της συσκευής.

Ένας επιτιθέμενος που έχει βάλει ως στόχο να επιτεθεί σε ένα σύστημα, οπωσδήποτε θα έχει κάποια επιτυχημένη προσπάθεια. Για αυτό το λόγο σε αυτό το κεφάλαιο παρουσιάζονται ορισμένα βασικά βήματα που μπορούν να βοηθήσουν στην ρύθμιση ενός ασφαλέστερου ασύρματου δικτύου. Θα μπορεί όμως με αυτές τις ρυθμίσεις ο εισβολέας να αποτραπεί ή απλά θα τον καθυστερήσουν;

Οι συμβουλές και οι προτεινόμενες ρυθμίσεις είναι παρόμοιες για όλα τα ασύρματα δίκτυα ανεξαρτήτως εξοπλισμού και υποδομής. Ωστόσο όμως θα υπάρξει περιορισμός στα τοπικά ασύρματα δίκτυα για λόγους απλοποίησης των μεθόδων διείσδυσης που θα αναφερθούν ως δείγμα του επιπέδου ασφαλείας.

3.2 ΣΤΡΑΤΗΓΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ

Όπως και στα ενσύρματα δίκτυα αποτελεί κανόνας η διασφάλιση των υπολογιστικών συστημάτων ενός ασύρματου δικτύου. Αυτό σημαίνει πως χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης σε λειτουργικά συστήματα, σε διαδικτυακές εφαρμογές, σε δρομολογητές κ.α.

Παρομοίως και ο δρομολογητής/σημείο πρόσβασης αποτελεί ένα υπολογιστικό σύστημα του ασύρματου τοπικού δικτύου το οποίο πρέπει να διαφυλαχτεί από παρείσακτους χρήστες.

3.2.1 Διαχείριση σημείου πρόσβασης

Οι περισσότεροι εμπορικοί δρομολογητές/σημεία πρόσβασης τρέχουν μια διαδικτυακή εφαρμογή για την διευκόλυνση του ιδιοκτήτη στην διαχείριση. Αυτή η διαδικτυακή εφαρμογή αποτελεί το διαχειριστικό περιβάλλον του δρομολογητή/σημείου πρόσβασης. Αυτές λοιπόν οι εφαρμογές έχουν εργοστασιακά προκαθορισμένο ζεύγος «όνομα χρήστη» και «κωδικό», όπου ο κωδικός συνήθως είναι απλός και πολύ αδύναμος. Παρ' αυτά, τα προκαθορισμένα στοιχεία αναγράφονται και στα εγχειρίδια χρήσης, οπότε κάποιος επιτιθέμενος μπορεί εύκολα να βρει τα συνθηματικά.

Άρα η αλλαγή των στοιχείων πρόσβασης στο διαχειριστικό περιβάλλον είναι ζωτικής σημασίας. Θέτοντας σε ισχύ νέο και ισχυρότερο κωδικό πρόσβασης στο διαχειριστικό περιβάλλον, μπορεί να αποτρέψει ή έστω να καθυστερήσει κάποιον εισβολέα του δικτύου να κάνει αλλαγές στις ρυθμίσεις του εξοπλισμού και τελικά να διαχειρίζεται αυτός το ασύρματο δίκτυο.

Η διαχείριση του δρομολογητή/σημείου πρόσβασης είναι απαγορευτικό να γίνεται είτε μέσω του ίδιου ασύρματου δικτύου ή με την απομακρυσμένη πρόσβαση μέσω Internet. Απενεργοποιώντας λοιπόν τις επιλογές «ασύρματη διαχείριση» και «απομακρυσμένη πρόσβαση» για το περιβάλλον διαχείρισης, επιτρέπεται πλέον μόνο η πρόσβαση από το ενσύρματο μέσο του τοπικού δικτύου. Έτσι ο εισβολέας και να αποκτήσει τα συνθηματικά δεν θα μπορέσει να γίνει ο διαχειριστής στη θέση του διαχειριστή.

3.2.2 Διευθυνσιοδότηση και Χρήστες

Από τα ενσύρματα δίκτυα Ethernet υπάρχει ήδη η τεχνογνωσία της στατικής και δυναμικής διευθυνσιοδότησης. Στα ασύρματα δίκτυα επικρατεί η δυναμική διευθυνσιοδότηση με έναν DHCP διακομιστή και αυτό διότι η πλειοψηφία

των χρηστών είναι εν κινήσει και περιστασιακοί. Συνήθως ο DHCP διακομιστής είναι ενσωματωμένος στο δρομολογητή/σημείο πρόσβασης. Αντίθετα σε περίπτωση που πρόκειται για ένα ασύρματο δίκτυο που χρησιμοποιείται μόνο από συγκεκριμένους χρήστες προτιμάτε η στατική διευθυνσιοδότηση.

Και στις δύο περιπτώσεις όμως μπορεί να περιοριστεί ο αριθμός των εν δυνάμει χρηστών θέτοντας σε εφαρμογή ένα υποδίκτυο στο ασύρματο τοπικό δίκτυο. Το πλήθος των διευθύνσεων του υποδικτύου καθορίζεται από τον διαχειριστή. Αν και υπάρχει η επιλογή στους δρομολογητές/σημεία πρόσβασης η δυνατότητα περιορισμού του αριθμού των συνδεδεμένων χρηστών, ωστόσο δίχως IP διεύθυνση ο χρήστης δεν μπορεί απολαμβάνει τις υπηρεσίες του ασύρματου δικτύου. Για αυτό μία καλή μέθοδος είναι να εφαρμόζεται η τεχνική των υποδικτύων.

Για να αυξηθεί το επίπεδο ασφαλείας του ασύρματου δικτύου, πολύ δυνατές και αποτελεσματικές μέθοδοι είναι το MAC filtering και στατικές δεσμεύσεις DHCP.

Το MAC filtering, αν και εφαρμόζεται στο φυσικό επίπεδο, ρυθμίζεται από το διαχειριστικό περιβάλλον του δρομολογητή/σημείου πρόσβασης. Είναι ένας πίνακας με καταχωρημένες τις μοναδικές φυσικές διευθύνσεις MAC των ασύρματων καρτών δικτύου που θα έχουν πρόσβαση στο ασύρματο τοπικό δίκτυο. Αυτό, όπως γίνεται αντιληπτό, μπορεί να εφαρμοστεί μόνο όταν οι χρήστες είναι προκαθορισμένοι.

Οι στατικές δεσμεύσεις DHCP εφαρμόζονται στον DHCP διακομιστή που εκτελείται στον δρομολογητή/σημείο πρόσβασης. Είναι ένας πίνακας αντιστοιχίας MAC διευθύνσεων και IP διευθύνσεων. Ο πίνακας μπορεί να ενημερώνεται χειροκίνητα, οπότε έχουμε πάλι την περίπτωση των προκαθορισμένων χρηστών, ή μπορεί να ενημερώνεται αυτόματα ώστε όταν ο ίδιος χρήστης προσπαθήσει να συνδεθεί μια άλλη φορά, να του αποδοθεί πάλι η ίδια διεύθυνση IP.

Ο συνδυασμός όλων των παραπάνω μεθόδων αυξάνει την πολυπλοκότητα του τρόπου διείσδυσης στο ασύρματο τοπικό δίκτυο. Ο εισβολέας θα πρέπει να ανακαλύψει έναν συνδυασμό από MAC διεύθυνση, IP διεύθυνση, μάσκα υποδικτύου και προεπιλεγμένης πύλης ώστε να αποκτήσει πρόσβαση στις υπηρεσίες του ασύρματου δικτύου.

3.2.3 Απόκρυψη του σημείου πρόσβασης

Υπάρχουν και κάποιες ρυθμίσεις στον δρομολογητή/σημείο πρόσβασης οι οποίες είναι δευτερεύουσες, αλλά εξίσου σημαντικές με τις προηγούμενες. Όπως ο επιτιθέμενος χρησιμοποιεί την προσποίηση για να διεισδύσει σε ένα δίκτυο, έτσι και ο διαχειριστής έχει την δυνατότητα να προσποιηθεί ότι το ασύρματο δίκτυο που

υφίσταται δεν υπάρχει. Αυτό επιτυγχάνεται με την απόκρυψη του SSID του σημείου πρόσβασης.

Το σημείο πρόσβασης προκαθορισμένα εκπέμπει κάθε 1/10 του δευτερολέπτου ένα σήμα επ' ονομαζόμενο beacon το οποίο περιλαμβάνει το SSID, το κανάλι που εκπέμπει, τις μεθόδους κρυπτογράφησης και αυθεντικοποίησης που χρησιμοποιεί και επίσης υπολογίζεται η απόστασή μεταξύ του σημείου πρόσβασης και του σταθμού με βάση την εξασθένηση του σήματος. Αυτές οι πληροφορίες όμως καθιστούν στο ασύρματο δίκτυο ευάλωτο προς τους κακόβουλους χρήστες. Η λύση είναι να απενεργοποιηθεί η εκπομπή του SSID και η ανίχνευση και η σύνδεση να γίνονται χειροκίνητα.

Με απενεργοποιημένη λοιπόν την εκπομπή του SSID στο σημείο πρόσβασης, ο επιτιθέμενος χάνει χρόνο περιμένοντας κάποιον εξουσιοδοτημένο χρήστη να επικοινωνήσει με το σημείο πρόσβασης, ώστε να υποκλέψει τις πληροφορίες που χρειάζεται για να εισβάλει στο ασύρματο δίκτυο. Και πάλι ο επιτιθέμενος γίνεται εισβολέας.

3.3 ΠΡΟΣΘΕΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Παρότι οι στρατηγικές που αναλύθηκαν παραπάνω μπορεί να προσφέρουν ένα ικανοποιητικό επίπεδο ασφαλείας, ωστόσο δεν αρκούν για να αποτρέψουν έναν επίμονο εισβολέα στο ασύρματο δίκτυο. Η λύση της χρήσης τείχους προστασίας και VPN έρχεται για να ενισχύσει ακόμη περισσότερο το επίπεδο ασφάλειας στα ασύρματα τοπικά δίκτυα.

3.3.1 Τείχος προστασίας

Το τείχος προστασίας είναι μία συσκευή ή ένα πρόγραμμα που επιτρέπει ή απορρίπτει πακέτα δεδομένων από ένα δίκτυο σε ένα άλλο. Στην περίπτωση που υλοποιείται με συσκευή έχει μεγάλο κόστος αγοράς και για αυτό το συναντάμε μόνο σε μεγάλα εταιρικά δίκτυα. Αντίθετα τα υλοποιημένα με λογισμικό τείχη προστασίας έχουν ελάχιστο κόστος απόκτησης και τα συναντάμε ακόμα και στα μικρότερα τοπικά δίκτυα.

Ανεξάρτητα της υλοποίησης, η κύρια λειτουργία ενός τείχους προστασίας είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό δίκτυο. Αν όμως το τοπικό δίκτυο χωρίζεται σε ένα ενσύρματο υποδίκτυο και ένα ασύρματο υποδίκτυο, τότε το τείχος προστασίας μπορεί να παρεμβάλλεται και ανάμεσα σε αυτά τα δύο

υποδίκτυα θέτοντας το επίπεδο εμπιστοσύνης στο μεν ασύρματο υποδίκτυο πιο χαμηλά από αυτό του ενσύρματου.

Πλέον η τεχνολογία των τειχών προστασίας με την ραγδαία ανάπτυξη της τεχνολογίας έχει φτάσει και αυτή σε μια γενιά ($4^{η}$ γενιά) που διαθέτει και γραφικό περιβάλλον μέσω του οποίου ο διαχειριστής και ο χρήστης μπορούν να κάνουν τις επιλογές τους όσον αφορά την ασφάλεια του δικτύου ή του υπολογιστή αντίστοιχα. Επίσης έχουν ενσωματωθεί στο λειτουργικό σύστημα και μπορούν να συνεργάζονται και με άλλα συστήματα ασφαλείας, όπως για παράδειγμα τα IPS's (Intrusion Prevention Systems) τα οποία θα αναφερθούν παρακάτω.

Αντίστοιχα ένα τείχος προστασίας μπορεί να παρακαμφθεί. Υπάρχουν πολλές μέθοδοι για να διαπεραστεί ένα τείχος προστασίας όπου ο πραγματικός εισβολέας δεν εντοπίζεται ή να παραμένει «αόρατος». Μερικές από αυτές αναφέρονται περιληπτικά παρακάτω, χρησιμοποιώντας το Nmap το οποίο επίσης υπάρχει στην διανομή BackTrack:

Fragment Packets: Κατακερματίζοντας τα πακέτα δεδομένων ενώ ταυτόχρονα σαρώνεται το δίκτυο, οπότε τα πακέτα του εισβολέα περνάνε από τον έλεγχο πακέτων δεδομένων του τείχους προστασίας

Specify MTU: Ορίζεται στο πακέτο ένα συγκεκριμένο MTU. Κατά την σάρωση δημιουργούνται πακέτα μεγέθους ίσο με αυτό που ορίζει ο εισβολέας. Παρόμοιο με τον κατακερματισμό πακέτων.

Decoy Addresses: Αποστέλλονται παραποιημένα πακέτα άλλων σταθμών του ίδιου υποδικτύου κατά τη σάρωση του δικτύου. Το τείχος προστασίας καταγράφει την IP διεύθυνση του εισβολέα και των σταθμών που χρησιμοποιήθηκαν. Έτσι δεν φαίνεται ποιος ξεκίνησε τη σάρωση.

Idle Zombie Scan: Χρησιμοποιείται ένας ανενεργός σταθμός να εκτελέσει την σάρωση σε έναν άλλον σταθμό στο ίδιο δίκτυο. Καταγράφεται η IP διεύθυνση του σταθμού «ζόμπι» και ο εισβολέας παραμένει απολύτως αόρατος.

Source Port Specification: Συνηθισμένο λάθος πολλών διαχειριστών είναι ο κανόνας που επιτρέπει εισερχόμενη κίνηση από μία συγκεκριμένη πόρτα. Ανεξάρτητα ποια είναι αυτή. Οπότε ο εισβολέας μπορεί να εκτελέσει την σάρωση του δικτύου ορίζοντας συγκεκριμένη πόρτα προέλευσης των πακέτων που στέλνει.

Append Random Data: Τα τείχη προστασίας μπορούν να ανιχνεύσουν πακέτα σάρωσης δικτύου δίνοντας βαρύτητα στο μέγεθος αυτών

των πακέτων. Τα πακέτα σάρωσης έχουν ένα συγκεκριμένο μέγεθος. Οπότε ο εισβολέας μπορεί να αυξομειώνει το μέγεθος των πακέτων για να επιτρέπεται η διέλευσή τους από τον έλεγχο.

MAC Address Spoofing: Τα τείχη προστασίας έχουν κανόνες φιλτραρίσματος MAC διευθύνσεων. Ο εισβολέας παραποιώντας τη MAC διεύθυνση του σταθμού του, με μία που έχει δικαιώματα, εκτελεί τη σάρωση χωρίς να γίνει αντιληπτός.

Η τοποθέτηση, λοιπόν, ενός τείχους προστασίας μεταξύ του ασύρματου και του ενσύρματου υποδικτύου, δυσκολεύει σε μεγάλο βαθμό τον εισβολέα. Οπότε αναλόγως το στόχο που έχει βάλει ο εισβολέας και το κέρδος που έχει να επωφεληθεί, μπορεί να επιμείνει ή να αποσυρθεί.

3.3.2 Virtual Private Network (VPN)

Τα VPN υπήρξαν και παραμένουν μια δεδομένη λύση ασφάλειας που παρέχει που παρέχει ασφαλή μετάδοση και ανταλλαγή δεδομένων μέσα ένα μη ασφαλές περιβάλλον. Με αυτή την έννοια τα VPN’s αποτελούν μια σημαντική μέθοδο ασφάλειας και για τα ασύρματα δίκτυα. Τα VPN’s ήταν αυτά αρχικά που θεωρήθηκαν ως λύση για τα κενά που παρουσίαζε το WEP.

Χωρίς πολλές τεχνικές λεπτομέρειες πρέπει να αναφερθεί ότι οι εξυπηρετητές που υλοποιούν τα VPN, αναλαμβάνουν να δρομολογούν όλη την κίνηση ενός σταθμού ανεξαρτήτως προορισμού. Λειτουργούν δηλαδή ως πύλες δικτύου του πελάτη, παρέχοντας παράλληλα μηχανισμούς πιστοποίησης και κρυπτογράφησης. Τα διασημότερα πρωτόκολλα είναι το PPTP και το IP SEC, ενώ ένας από τους πιο ισχυρούς αλγόριθμους κρυπτογράφησης που χρησιμοποιείται, είναι ο 3DES.

Να επισημανθεί ότι τα VPN’s λειτουργούν στο 3^{ο} επίπεδο του μοντέλου OSI. Δηλαδή λειτουργεί ως μία συμπληρωματική μέθοδος ασφάλειας για την πρόσβαση στο δίκτυο, αφού η πρόσβαση στο φυσικό μέσο που είναι ο αέρας δεν αποτρέπεται τελικά.

Πλεονέκτημα των VPN’s αποτελεί η επιπλέον κρυπτογράφηση που παρέχει στα δεδομένα και τις πληροφορίες που διακινούνται στο δίκτυο. Ωστόσο όμως, ο εισβολέας στο ασύρματο δίκτυο μπορεί να υποκλέψει τα διακινούμενα πακέτα με τα κρυπτογραφημένα δεδομένα και αφού αποσυνδεθεί να αποκρυπτογραφήσει να δεδομένα.

Το ίδιο πλεονέκτημα όμως αποτελεί και μειονέκτημα για την χρήση των VPN’s στα ασύρματα δίκτυα, διότι με την κρυπτογράφηση των VPN και την

κρυπτογράφηση του 802.11 αυξάνονται οι απαιτήσεις των δομικών στοιχείων του ασύρματου δικτύου σε επεξεργαστική ισχύ και ταχύτητες μετάδοσης και το τοπικό δίκτυο φορτώνεται με επιπλέον όγκο διακίνησης δεδομένων.

3.3.3 Intrusion Detection Systems (IDS)

Η ανίχνευση επιθέσεων έχει να κάνει με την παρακολούθηση γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και την ανάλυσή τους για υπογραφές επιθέσεων. Η εξέλιξη των IDSs είναι ραγδαία τα τελευταία χρόνια και συνεχώς γίνονται προσπάθειες για τη βελτίωσή τους κυρίως στο τομέα των συμπτωμάτων των λανθασμένων «συναγερμών» που παρουσιάζουν. Με την τρέχουσα μορφή τους τα IDSs παρέχουν σημαντική υποστήριξη στα ήδη υπάρχοντα μέτρα προστασίας ενός δικτύου και σε συνδυασμό με άλλους μηχανισμούς ασφάλειας αποτελούν σημαντικό εργαλείο για τους διαχειριστές.

Οι λανθασμένες επισημάνσεις είναι δύο κατηγοριών γνωστές ως «Θετικά Λάθη» και «Αρνητικά Λάθη». Θετικά λάθη ονομάζονται οι λανθασμένες επισημάνσεις που παράγει ένα IDS, όταν ανιχνεύει κάποιο γεγονός ως περίπτωση πιθανής επίθεσης, ενώ δεν είναι. Τα θετικά λάθη είναι δυνατόν να προκύψουν από κακή ρύθμιση του συστήματος. Επίσης μπορούν να προκύψουν και από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν από μία επίθεση, ως συμπεριφορά των συστημάτων που εμπλέκονται. Τα αρνητικά λάθη, αντιθέτως, είναι οι περιπτώσεις επιθέσεων τις οποίες το σύστημα δεν κατάφερε να επισημάνει μετά την εξέτασή τους. Αυτό συνήθως συμβαίνει κατά την εμφάνιση νέας στρατηγικής επίθεσης για την οποία δεν υπάρχει προηγούμενη περιγραφή.

Ο θόρυβος στο δίκτυο πολλές φορές μειώνει την αποτελεσματικότητα των IDSs. Τα IDSs παρουσιάζουν μεγάλη ευαισθησία στα πακέτα-σκουπίδια που ταξιδεύουν μέσα στο δίκτυο, και έτσι παρουσιάζουν μεγάλο ποσοστό λανθασμένης σήμανσης. Δεν είναι ασυνήθιστο ο αριθμός των πραγματικών επιθέσεων να είναι πολύ χαμηλότερος από τις λανθασμένες σημάνσεις, για αυτό και οι σημάνσεις για πραγματικές επιθέσεις συνήθως αγνοούνται ή χάνονται. Πολλές επιθέσεις προσαρμόζονται σε ξεπερασμένες εκδόσεις του λογισμικού. Η συχνή ενημέρωση της βιβλιοθήκης των υπογραφών των επιθέσεων είναι αυτή που μετριάζει τους κινδύνους για ένα σύστημα ή δίκτυο.

Ο εισβολέας δημιουργώντας διαφορετικές καταστάσεις στον IDS και στον στόχο του, παρακάμπτει την ανίχνευση της εισβολής. Αυτό το επιτυγχάνει με την χειραγώγηση της κίνησης του δικτύου ή ακόμα και με την ίδια της επίθεση.

3.4 ΕΠΙΛΟΓΟΣ

Συνοψίζοντας λοιπόν τις τεχνικές προστασίας και παράκαμψης αντίστοιχα, διαπιστώνει κανείς, πως ο εισβολέας στο μέσο του ασύρματου δικτύου, δεν αποτρέπεται τελικά να αποκτήσει πρόσβαση στις υπηρεσίες του δικτύου. Όμως, όσο δύσκολο είναι το έργο του διαχειριστή δικτύου να διατηρήσει τους χρήστες, τα δεδομένα και την πληροφορία ασφαλή, άλλο τόσο δύσκολο είναι και στον εισβολέα να παρακάμψει την ασφάλεια.

Έτσι λοιπόν δημιουργείτε η ανάγκη του εντοπισμού του κακόβουλου χρήστη σε ένα ασύρματο τοπικό δίκτυο. Όχι, όμως, η ανίχνευση της εισβολής, αφού αυτό καλύπτεται από τα IDSs, αλλά ο χωροταξικός εντοπισμός του ίδιου του εισβολέα σε πραγματικό χρόνο.

ΚΕΦΑΛΑΙΟ 4

ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΦΕΡΟΜΕΝΟΥ ΔΡΑΣΤΗ

4.1 ΕΙΣΑΓΩΓΗ

Στο προηγούμενο κεφάλαιο αναπτύχθηκαν οι μέθοδοι διείσδυσης αντίστοιχα με τα μέτρα ασφαλείας που μπορεί να πάρει ένας διαχειριστής για να προστατέψει το ασύρματο τοπικό δίκτυο της αρμοδιότητάς του.

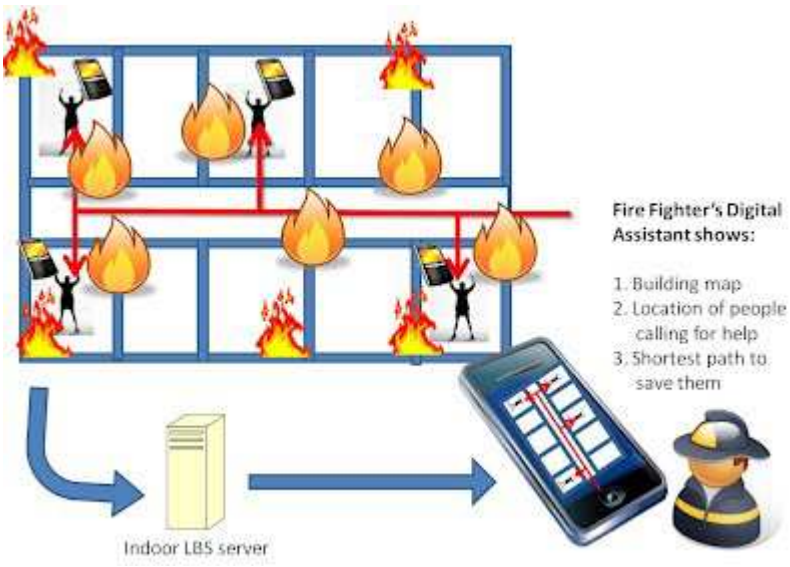
Αφού ο εισβολέας παρακάμψει τις δικλείδες ασφαλείας σε ένα ασύρματο δίκτυο και διαπράξει υποκλοπή ή παραποιήσει πληροφορίες και δεδομένα θα πρέπει να υπάρχει η δυνατότητα του χωροταξικού εντοπισμού. Ο διαχειριστής θα πρέπει να είναι σε θέση να πιάσει επ' αυτοφώρω τον εισβολέα αν είναι δυνατόν ώστε να μην διαρρεύσουν οι πληροφορίες.

Ο χρόνος, όμως, που θα μεσολαβήσει από την εύρεσης του στίγματος μέχρι να μεταβεί κάποιος στο σημείο, είναι αρκετός χρόνος για τον εισβολέα να συνεχίσει την επιζήμια πρακτική του και να παραποιήσει πολλές ακόμα πληροφορίες. Οπότε προτεραιότητα έχει ο «αφοπλισμός» του εισβολέα, που στην περίπτωσή μας είναι η ασύρματη κάρτα δικτύου της συσκευής του εισβολέα.

Σε αυτό το κεφάλαιο λοιπόν θα αναλυθεί με ποιον τρόπο θα μπορούσε ένας διαχειριστής να υλοποιήσει τον εντοπισμό τους εισβολέα χωρίς δραματικές αλλαγές στην υποδομή του τοπικού δικτύου και ειδικά στο ασύρματο υποδίκτυο. Επίσης θα δικαιολογηθεί και η χρήση των μεθόδων των κακόβουλων χρηστών από έναν διαχειριστή για να μπορεί να εξουδετερώσει τους εισβολείς.

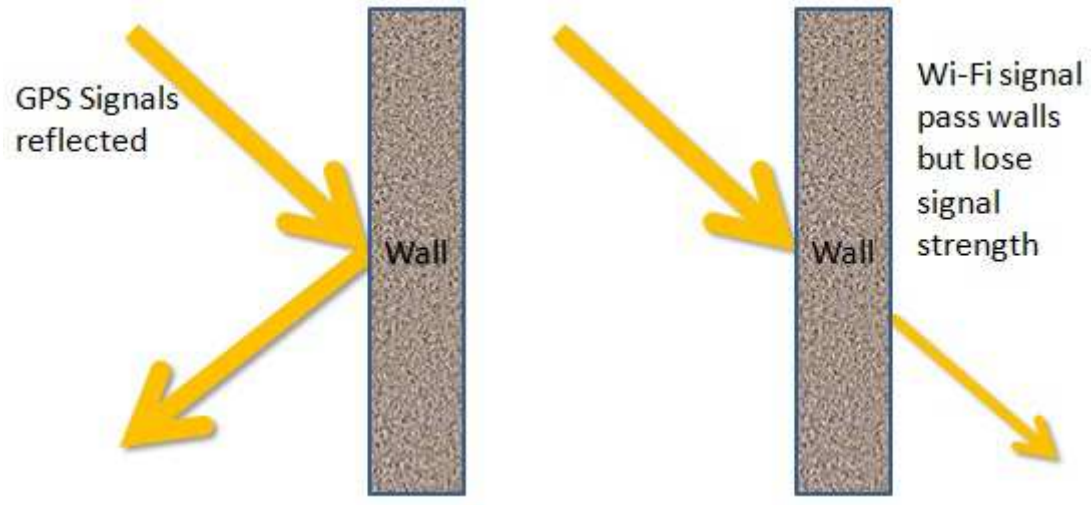
4.2 INDOOR LOCATION BASED SERVICES (INDOOR LBS)

Στο ερευνητικό εργαστήριο του πανεπιστημίου Maine στις Η.Π.Α., Virtual Environment & Multimodal Interaction (VEMI Lab) αναπτύχθηκε μία εφαρμογή για να καταστεί δυνατή η παροχή υπηρεσιών, βασισμένες στην τοποθεσία που βρίσκεται ο πελάτης. Παραδείγματα της εφαρμογής είναι η ξενάγηση σε ένα μουσείο ή σε περίπτωση έκτακτης ανάγκης σε ένα κτήριο, να μπορούν να σώματα ασφαλείας να εντοπίσουν τα θύματα. Έτσι ούτε ο επισκέπτης χάνει χρόνο και θα περιηγηθεί σε όλη την έκταση του μουσείου και τα σώματα ασφαλείας δεν θα χάσουν πολύτιμο χρόνο να εντοπίσουν και να σώσουν τα θύματα.



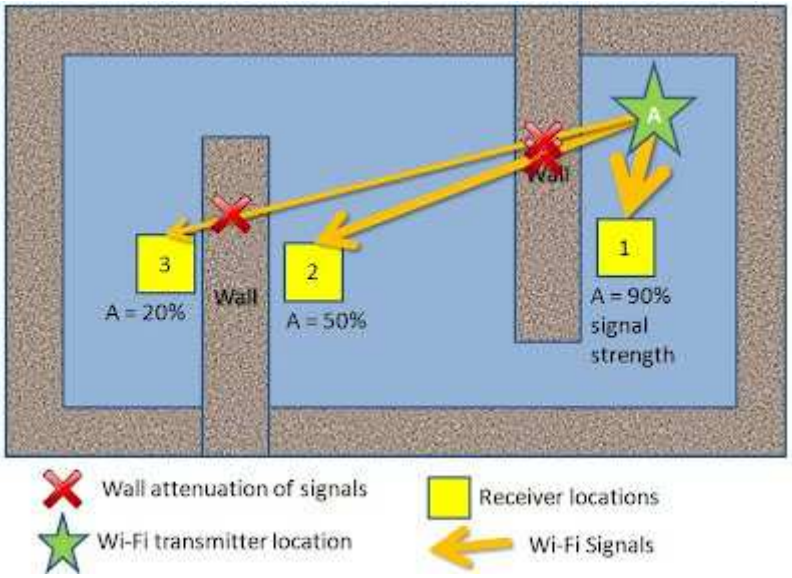
Εικόνα 4. 1 Παράδειγμα για Indoor Location Based Services

Όλα αυτά αποφάσισαν να τα υλοποιήσουν και να βασιστούν στα ήδη προεγκατεστημένα ασύρματα τοπικά δίκτυα (Wi-Fi) διότι το σήμα διαπερνά τους τοίχους, αλλά εξασθενίζει. Το GPS σήμα αντανακλάτε στους τοίχους και έτσι οι αντίστοιχες συσκευές δεν μπορούν να χρησιμοποιηθούν σε εσωτερικούς χώρους, οπότε και απορρίφθηκε. Όσο για τις τεχνολογίες των υπέρυθρων και Bluetooth απορρίφθηκαν γιατί προαπαιτούσαν νέα υποδομή, αντίθετα με τα Wi-Fi.



Εικόνα 4. 2 Συμπεριφορά σημάτων

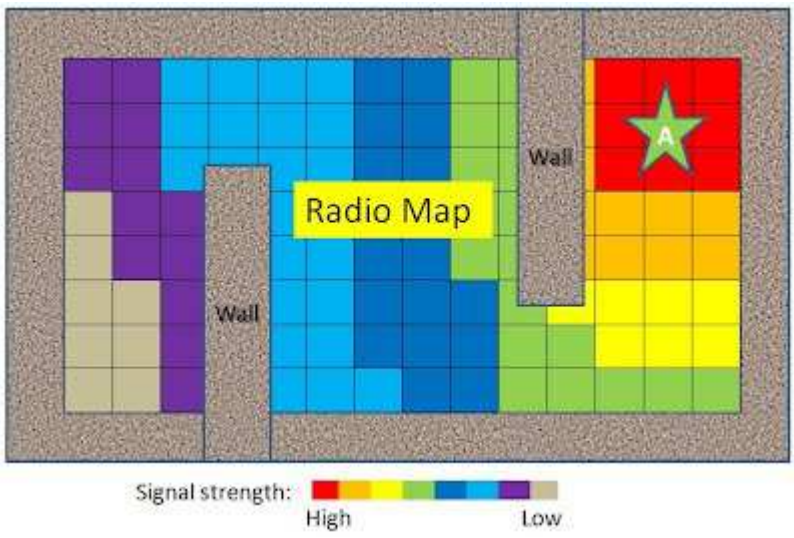
Η εφαρμογή αυτή εξαρτάται από δύο βασικά συστήματα. Το ένα είναι το Indoor Positioning System (IPS) το οποίο παρέχει το στίγμα του χρήστη μέσα στο κτήριο. Το δεύτερο είναι το Indoor Content Provider System, το οποίο παρέχει στον χρήστη τα περιεχόμενα, όπως χάρτες και λεπτομέρειες για την τοποθεσία. Το Wi-Fi σήμα είναι ελεύθερα διαθέσιμο μέσα στο κτήριο, μπορεί να διαπεράσει τους τοίχους και το σήμα αρκετά ισχυρό για την εύρεση τοποθεσίας. Η ισχύς του Wi-Fi σήματος εξαρτάται από την απόσταση και το πλήθος των τοίχων που υπάρχουν μεταξύ του πομπού και του δέκτη.



Εικόνα 4. 3 Παράδειγμα ισχύς σήματος σε εσωτερικούς χώρους

Προαπαιτούμενο αποτελεί η χαρτογράφηση της έντασης του σήματος. Αυτός ο χάρτης απεικονίζει την ένταση του σήματος που διαπερνά τον χώρο. Στο συγκεκριμένο εργαστήριο λοιπόν αποφάσισαν να χωρίσουν το κτήριο σε ίσα κελιά μεταξύ τους. Σε κάθε κελί κατέγραψαν την ισχύ του σήματος. Με αυτόν τον χάρτη λοιπόν επικαλύπτουν το πολεοδομικό σχέδιο του κτηρίου και δημιουργούν τους αντίστοιχους πίνακες ισχύς σήματος για το κάθε σημείο πρόσβασης ξεχωριστά.

Πρέπει να επισημανθεί όμως πως αυτό πρέπει να γίνεται κάθε φορά που αλλάζει το σημείο πρόσβασης. Κάθε σημείο πρόσβασης έχει διαφορετικά αποτελέσματα. Σίγουρα αν αλλάξει η διαρρύθμιση τους κτηρίου πρέπει να επαναληφτεί όλη η διαδικασία. Παρακάτω φαίνεται ο χάρτης ενός μόνο σημείου πρόσβασης.



Εικόνα 4. 4 Χάρτης ισχύς σήματος για ένα σημείο πρόσβασης

Η συγκεκριμένη ομάδα για να εντοπίσει κάποιον χρήστη μέσα στον χώρο χρησιμοποίησε τα διανύσματα ισχύς σήματος από διαφορετικά σημεία πρόσβασης. Εκτιμούνε πως εντοπίζουν τον χρήστη με ακρίβεια 2 μέτρων.

4.3 ΧΩΡΟΤΑΞΙΚΟΣ ΕΝΤΟΠΙΣΜΟΣ ΕΙΣΒΟΛΕΑ

Επιστρέφοντας στην ανάγκη που προέκυψε από το 3^{ο} κεφάλαιο, μια παρόμοια τεχνική μπορεί να χρησιμοποιηθεί για να υλοποιηθεί μια εφαρμογή χωροταξικού εντοπισμού του εισβολέα σε ένα ασύρματο τοπικό δίκτυο.

Υπάρχουν κάποιες εμπορικές λύσεις, αλλά δεν κυκλοφορούν δοκιμαστικές εκδόσεις για να διαπιστωθεί η αποτελεσματικότητα και να πειραματιστεί ο ενδιαφερόμενος. Η αγορά τους γίνεται κατόπιν επικοινωνίας με την εκάστοτε εταιρεία και το κόστος τους είναι υψηλό. Επίσης οι εταιρίες στοχεύουν περισσότερο σε λύσεις παρόμοιες με αυτή των συναδέλφων από το πανεπιστήμιο Maine, παρά σε λύσεις που αφορούν ειδικούς στην διαχείριση δικτύων.

Παρ’ όλα αυτά θα ακολουθήσει μία θεωρητική προσέγγιση με γνώμονα το χαμηλό κόστος εγκατάστασης και υλοποίησης και να μην χρειάζεται αλλαγή στην ήδη υπάρχουσα υποδομή του ασύρματου τοπικού δικτύου παρά μόνο κάποιες προσθήκες και σε υλικό και σε λογισμικό.

4.3.1 Χαρτογράφηση Ασύρματου Τοπικού Δικτύου

Για την χαρτογράφηση της ισχύς σήματος χρειάζεται ένας φορητός υπολογιστής γιατί είναι κατάλληλος για την ευκολία της κίνησης και το κατάλληλο λογισμικό που να μετατρέπει την ισχύ σήματος σε οπτική αναπαράσταση και να την χαρτογραφεί. Ένα τέτοιο λογισμικό αποτελεί η εμπορική εφαρμογή HeatMapper της Ekahau. Η Ekahau διαθέτει το HeatMapper δωρεάν για την υποστήριξη εφαρμογών και συσκευών της ίδιας εταιρείας. Ως δείγμα της λειτουργίας του HeatMapper υπάρχουν διαδοχικές εικόνες στο Παράρτημα Α’ με την χαρτογράφηση του 1^{ου} ορόφου του τμήματος Πληροφορικής του Α.Τ.Ε.Ι.Θ.

Το HeatMapper εγκαθίσταται σε έναν φορητό υπολογιστή εξοπλισμένο με μία ασύρματη κάρτα δικτύου. Αρχικά μπορούμε να φορτώσουμε μία εικόνα με την κάτοψη του κτηρίου ή έναν χάρτη για εξωτερικούς επίπεδους χώρους. Στη συνέχεια μόλις είναι έτοιμη η εφαρμογή προς χρήση, σαρώνει την περιοχή και εντοπίζει όλα τα σημεία πρόσβασης εντός εμβέλειας. Εν συνεχεία ο χρήστης ξεκινώντας χωροταξικά δίπλα από το σημείο πρόσβασης, περπατάει και ανάλογα με την κατεύθυνση που κινείται κουνάει το ποντίκι αντίστοιχα και διαδοχικά ανά τακτά διαστήματα πατάει το αριστερό κουμπί στο ποντίκι. Η εφαρμογή ανάλογα

την ισχύ του σήματος περιγράφει τις διακεκομμένες γραμμές (τα νοητά βήματα του χρήστη) με ένα αντίστοιχο χρώμα. Αφού τελειώσει ο χρήστης τον «περίπατο» πατάει μία φορά το δεξί κουμπί στο ποντίκι και ο χάρτης απεικονίζεται στην οθόνη.

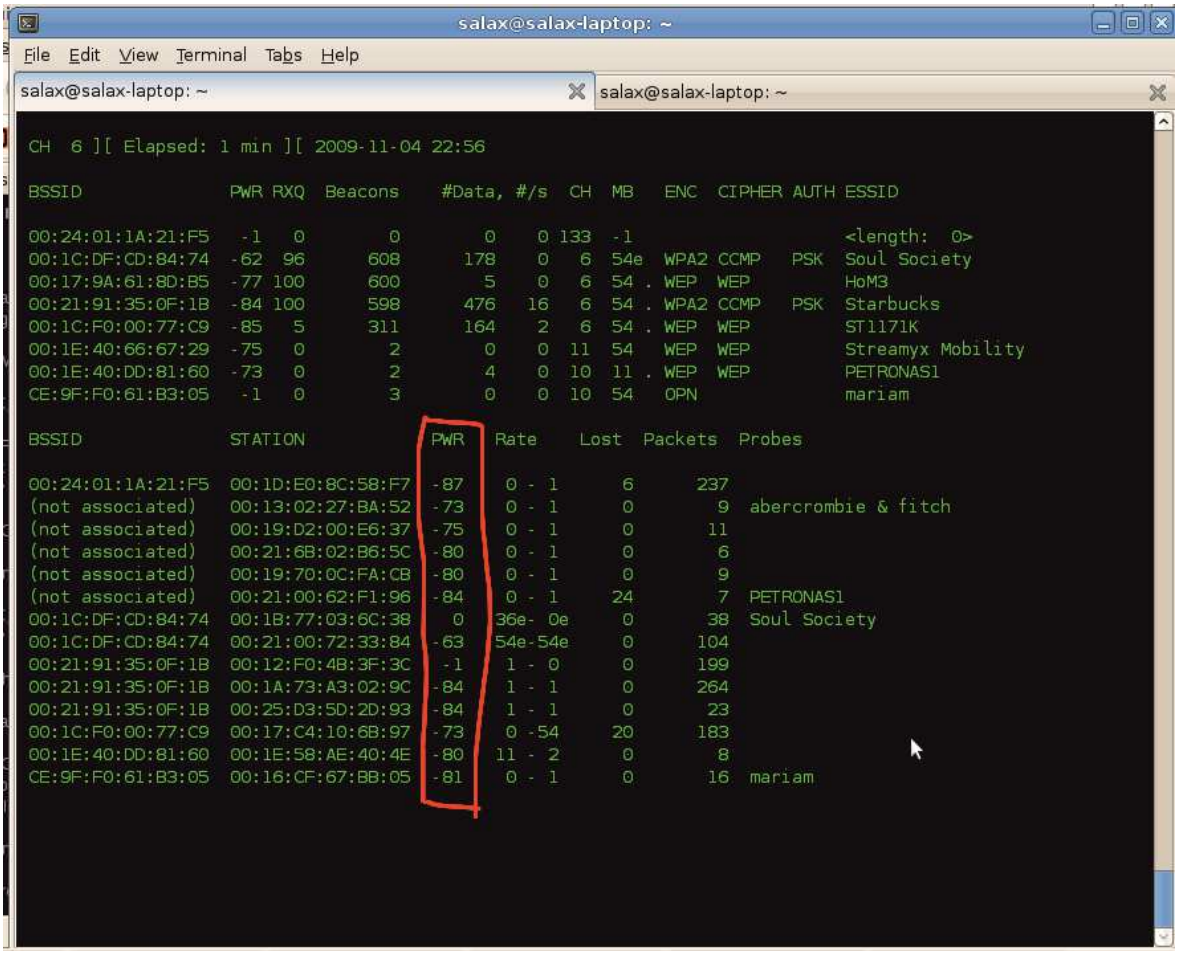
Η εφαρμογή αυτή χαρτογραφεί ουσιαστικά την επικαλυπτόμενη περιοχή από τα σημεία πρόσβασης του ασύρματου τοπικού δικτύου, δίνοντας πληροφορίες για το κάθε σημείο πρόσβασης και για την ισχύ του σήματος ξεχωριστά. Η ερμηνεία του χάρτη όμως είναι πιο διαφωτιστική όταν γίνεται η χρήση ενός πραγματικού σχεδίου του χώρου. Οι διαδρομές και τα κλικ μπορούν να γίνονται με κάποια σημεία αναφοράς στον πραγματικό χώρο και τα αντίστοιχα στο σχέδιο. Έτσι έχοντας την κλίμακα από τα σχέδια, την χαρτογράφηση της ισχύς του σήματος πάνω στα σχέδια πλέον είναι εφικτό να δημιουργηθεί ένας πίνακας ισχύς σήματος και απόστασης.

Σε αυτό το σημείο θα πρέπει να επισημανθεί πως αν αλλάξει κάτι στον συνδυασμό σημείο πρόσβασης και χώρου η μέτρηση θα πρέπει να επαναληφθεί.

4.3.2 Σταθμοί Κατάσκοποι

Κατά τη διάρκεια της μελέτης της εφαρμογής του πανεπιστημίου Maine, αλλά και άλλων παρόμοιων εμπορικών εφαρμογών, παρατηρήθηκε ότι χρησιμοποιούνται τα σημεία πρόσβασης για τον εντοπισμό των χρηστών. Με αυτόν τον τρόπο όμως αυξάνεται ο φόρτος εργασίας των σημείων πρόσβασης.

Στην παρούσα προσέγγιση για τον χωροταξικό εντοπισμό κακόβουλου χρήστη θα χρησιμοποιηθούν απλοί σταθμοί που θα έχουν το ρόλο του κατάσκοπου. Οι σταθμοί – κατάσκοποι είναι συνδεδεμένοι στο τοπικό δίκτυο ενσύρματα. Η ασύρματη διεπαφή λειτουργεί σε κατάσταση «Παρακολούθησης» μόνο, όπως και ο κακόβουλος χρήστης ρυθμίζει τον σταθμό του να λαμβάνει ό,τι κινείται στο δίκτυο. Από τη στιγμή που ο κακόβουλος χρήστης εισβάλει στο ασύρματο δίκτυο, οι σταθμοί – κατάσκοποι θα λαμβάνουν τα πακέτα του. Ο εισβολέας χρησιμοποιώντας το airmon-ng εντόπισε κάποιον χρήστη που συσχετίζεται με ένα συγκεκριμένο σημείο πρόσβασης και προσποιήθηκε την αποσύνδεση του θύματος για να αποκτήσει το WEP κλειδί. Το airmon-ng όμως μας παρέχει και άλλες πληροφορίες, συγκεκριμένα την ισχύ του σήματος του αποστολέα. Η ισχύς του σήματος οποιουδήποτε αποστολέα, μέσα στο ασύρματο τοπικό δίκτυο, για τον διαχειριστή, αποτελεί αξιοποιήσιμη πληροφορία.



Εικόνα 4. 5 Airmon-ng Ισχύς Σήματος χρηστών

Η ισχύς σήματος που αναγράφεται στον πίνακα των συσχετιζόμενων σταθμών είναι η ισχύς μεταξύ του σταθμού που συνδέεται με το συσχετιζόμενο σημείο πρόσβασης και του σταθμού που εκτελεί το airmon-ng.

Σε αυτό το σημείο είναι πλέον αναγκαία μια χαρτογράφηση που θα έχει ως επίκεντρο έναν σταθμό που θα μπορούσε να είναι οπουδήποτε. Η μέθοδος χαρτογράφησης που αναφέραμε παραπάνω στο ίδιο κεφάλαιο, θα πρέπει να αντιστραφεί για να έχουμε το επιθυμητό αποτέλεσμα. Χρησιμοποιώντας και πάλι το HeatMapper σε συνδυασμό με το πραγματικό σχέδιο του κτηρίου χαρτογραφούμε με κάθε σταθμό – κατάσκοπο για έναν σταθμό. Αυτό σημαίνει πως στην ίδια διαδικασία που περιγράφηκε για το HeatMapper το ρόλο του περιφερόμενου σταθμού θα πάρει ο σταθμός - κατάσκοπος (πλέον ακίνητος) και το ρόλο του σημείου πρόσβασης θα πάρει ένας περιφερόμενος σταθμός.

Στην πράξη δηλαδή θα δημιουργήσουμε μεταξύ του σταθμού – κατάσκοπου και του περιφερόμενου σταθμού ένα ad-hoc δίκτυο. Στο σταθμό κατάσκοπο θα εκτελείται το HeatMapper και η διαδρομή που χαράζεται ακολουθώντας πιστά στο σχέδιο του κτηρίου, θα είναι η διαδρομή που ακολουθεί ο περιφερόμενος σταθμός στο ρόλο του σημείου πρόσβασης. Έτσι θα πάρουμε μία χαρτογράφηση που θα μας δείχνει την ισχύ σήματος που θα λαμβάνει ο σταθμός – κατάσκοπος από οποιοδήποτε σταθμό και από οποιοδήποτε σημείο.

Από την «αντίστροφη χαρτογράφηση» λοιπόν βγαίνει ο πίνακας αντιστοίχησης ισχύς και απόστασης. Η αντίστροφη χαρτογράφηση επαναλαμβάνεται για όλους τους σταθμούς – κατασκόπους.

Ο σταθμός – κατάσκοπος πλέον είναι σε θέση να γνωρίζει σε πραγματικό χρόνο την απόσταση οποιουδήποτε αποστολέα από τον εαυτό του βασισμένη στην ισχύ του σήματος.

4.3.3 Δομικά Στοιχεία Υποδομής

Η υποδομή του ασύρματου δικτύου δεν αλλάζει ουσιαστικά. Στην υποδομή του ενσύρματου δικτύου όμως θα προστεθούν τουλάχιστον τρεις σταθμοί εξοπλισμένοι με Ethernet και 802.11 διεπαφές για κάθε σημείο πρόσβασης και ένας εξυπηρετητής για τη συλλογή, την επεξεργασία και την εμφάνιση της πληροφορίας.

Οι σταθμοί – κατάσκοποι δεν είναι απαραίτητο να αυξάνονται αναλογικά με τα σημεία πρόσβασης του ασύρματου δικτύου. Το πλήθος τους εξαρτάται περισσότερο από το ποσοστό αλληλοεπικάλυψης των σημείων πρόσβασης που θα έχουμε στο σύνολό του στο ασύρματο τοπικό δίκτυο. Σε αυτό το σημείο χρειάζεται η χαρτογράφηση του ασύρματου τοπικού δικτύου για την εξακρίβωση του πλήθους και της βέλτιστης θέσης των σταθμών – κατασκόπων.

Εκτός από τον εντοπισμό οποιουδήποτε χρήστη συμπεριλαμβανομένων και των κακόβουλων, ο εξυπηρετητής, με την ίδια υποδομή θα έχει την δυνατότητα να παρέχει στον διαχειριστή πληροφορίες για την κίνηση του ασύρματου τοπικού δικτύου αναλυτικά για κάθε χρήστη, όπως συμβαίνει και στα ενσύρματα δίκτυα.

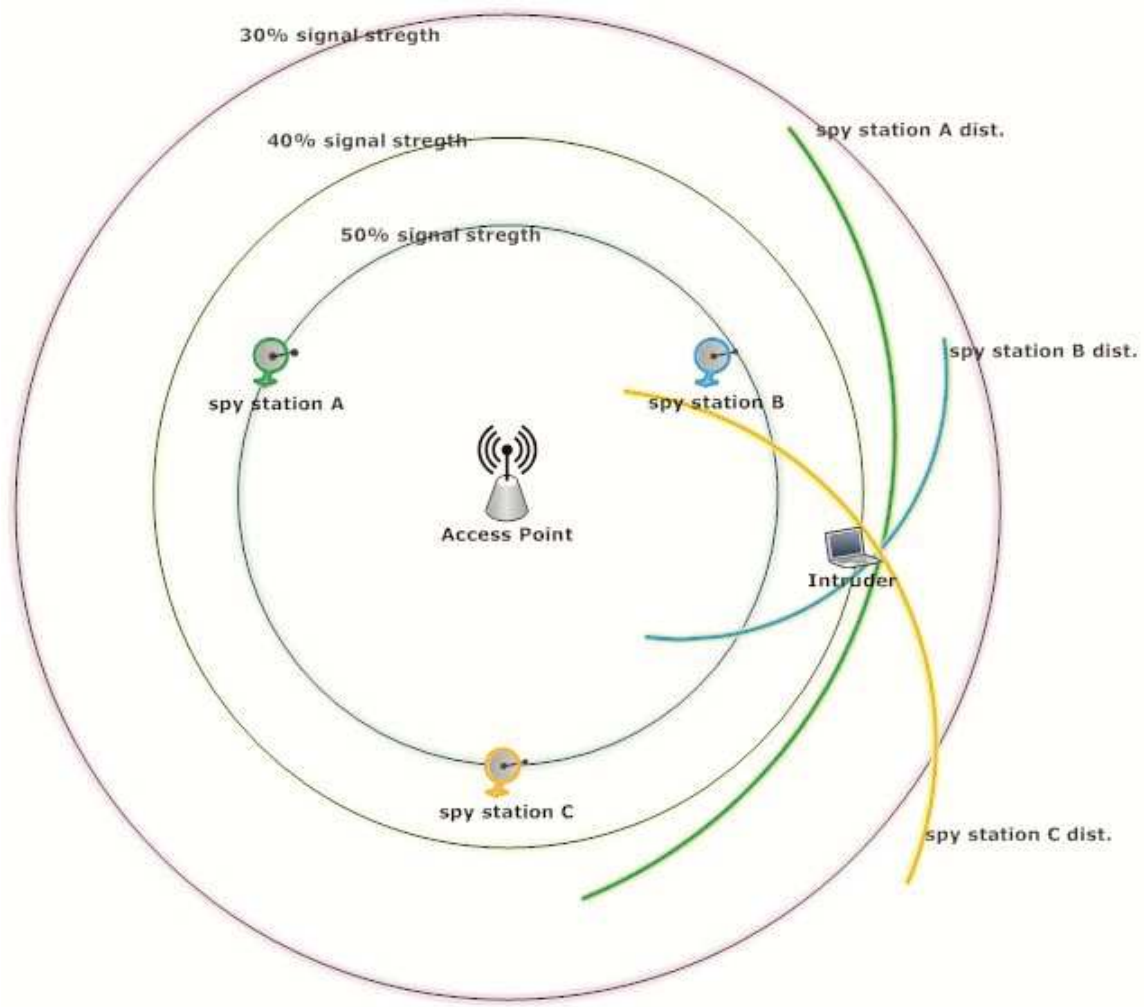
4.3.4 Εφαρμογή και Λογισμικό

Αφού συλλεχθούν οι απαραίτητες πληροφορίες από τους σταθμούς – κατάσκοπους και συγκεντρωθούν στον εξυπηρετητή, πλέον μπορεί να γίνει και η επεξεργασία.

Ο κάθε σταθμός - κατάσκοπος επιστρέφει μία τιμή για την ισχύ του σήματος ενός σταθμού. Από την αντίστροφη χαρτογράφηση του ασύρματου τοπικού δικτύου, ο πίνακας αντιστοίχησης μας επιστρέφει τις αποστάσεις.

Το στίγμα του συγκεκριμένου σταθμού μπορεί να υπολογιστεί πλέον ως μία ζεύξη συνόλων. Για κάθε σταθμό – κατάσκοπο έχουμε έναν νοητό κύκλο με ακτίνα ίση με την τιμή που μας επιστρέφει ο πίνακας αντιστοίχισης ισχύς-απόστασης, από την αντίστροφη χαρτογράφηση. Το σημείο που θα εφάπτονται

και οι τρεις νοητοί κύκλοι ή η περιοχή που καλύπτεται και από τους τρεις νοητούς κύκλους είναι και το στίγμα του σταθμού που ψάχνουμε.



Εικόνα 4. 6 Εντοπισμός πιθανού εισβολέα σε ασύρματο τοπικό δίκτυο

4.4 ΠΡΟΣΩΡΙΝΗ ΕΞΟΥΔΕΤΕΡΩΣΗ ΕΙΣΒΟΛΕΑ

Αφού ο διαχειριστής πλέον γνωρίζει το στίγμα του εισβολέα θα πρέπει να μεταβεί ο ίδιος μέχρι το σημείο. Ο χρόνος που μεσολαβεί από τη στιγμή του εντοπισμού μέχρι την άφιξη κάποιου στο σημείο μετριέται σε λεπτά. Ο χρόνος αυτός είναι πολύς. Βάση των μέγιστων ονομαστικών ταχυτήτων που έχουμε στα ασύρματα τοπικά δίκτυα 54 Mbps και 150 Mbps, μεταφράζεται σε 405 MB και 1125 MB όγκος δεδομένων που υποκλέπτονται κάθε λεπτό.

Μια επιλογή είναι ο διαχειριστής να απενεργοποιήσει την υπηρεσία που είναι υπό επίθεση, αλλά αυτό δεν αποτελεί λύση. Η άλλη επιλογή είναι να

εφαρμόσει και ο διαχειριστής παρόμοιες τακτικές με τους κακόβουλους χρήστες. Με το να εφαρμόσει ο διαχειριστής μία επίθεση Flood Attack στον εισβολέα η ασύρματη κάρτα δικτύου του σταθμού του δεν προλαβαίνει να επεξεργαστεί τα δεδομένα που της αποστέλλονται και προσπαθώντας να απαντήσει σε τεράστιο πλήθος δεδομένων, δεν μπορεί να ανταποκριθεί σε αιτήσεις ούτε του συστήματος ούτε του δικτύου. Έτσι ο χρόνος που μεσολαβεί για τη φυσική μετάβαση κάποιου προσώπου στον «τόπο του εγκλήματος», δεν θα είναι υπέρ του εισβολέα πλέον.

4.5 ΕΠΙΛΟΓΟΣ

Αναμφίβολα οι εμπορικές λύσεις για τον εντοπισμό χρηστών σε ένα ασύρματο τοπικό δίκτυο είναι αποτελεσματικές. Ο λόγος που χρησιμοποιούνται όμως στην πλειοψηφία τους είναι για να προσφέρουν υπηρεσίες προς τους χρήστες και όχι προς τους διαχειριστές των ασύρματων τοπικών δικτύων.

Η θεωρητική προσέγγιση για τη λύση που αναλύθηκε είχε ως στόχο την αποσυμφόρηση των σημείων πρόσβασης από την επιπλέον κίνηση για τον εντοπισμό χρηστών. Επίσης το σύστημα εντοπισμού με τους σταθμούς – κατάσκοπους αποτελεί μία πιο ανεξάρτητη λύση από το ασύρματο τοπικό δίκτυο, επιτρέποντας στον διαχειριστεί να προσθέσει μελλοντικά και άλλες εφαρμογές, όπως παρακολούθηση της κίνησης που πραγματοποιεί ο κάθε σταθμός ξεχωριστά.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Η ασφάλεια στα ασύρματα τοπικά δίκτυα προβληματίζει τους ειδικούς από όταν πρωτοεμφανίστηκαν. Έχει γίνει μεγάλη πρόοδος στον τομέα αυτό, που πλέον τα καθιστά κατά πολύ μεγάλο ποσοστό ασφαλή. Οι μέθοδοι παράκαμψης που αναφέρθηκαν στην παρούσα εργασία δεν είναι τόσο εύκολο να εφαρμοστούν, ακόμα και από επαγγελματίες. Ωστόσο όμως εξακολουθούν να αποτελούν απειλή για την ασφάλεια των ασύρματων τοπικών δικτύων.

Συμπεραίνεται λοιπόν πως στα ασύρματα τοπικά δίκτυα το μειονέκτημά τους που είναι ο αέρας, έχει συντελεστή με μεγάλη βαρύτητα. Ενσωματώνοντας όμως μία εφαρμογή χωροταξικού εντοπισμού εισβολέα σε ένα ασύρματο τοπικό δίκτυο, περιορίζονται οι τύποι επιθέσεων μόνο στους παθητικούς και μάλιστα μόνο στην παρακολούθηση. Η παρακολούθηση όμως παραπέμπει σε υποκλοπή. Τα κρυπτογραφημένα δεδομένα αποτελούν σκουπίδια για τον κακόβουλο χρήστη, αφού θα πρέπει να παρέμβει στο ασύρματο δίκτυο ενεργά για να μπορέσει να αποκτήσει το κλειδί αποκρυπτογράφησης. Σε αυτό το σημείο είναι ευάλωτος και μπορεί να εντοπιστεί χάρη σε μία εφαρμογή χωροταξικού εντοπισμού εισβολέα.

Πρόσθετη μελλοντική προσθήκη στην εφαρμογή χωροταξικού εντοπισμού εισβολέα, μπορεί να αποτελέσει η παρακολούθηση της κίνησης που δημιουργούν οι σταθμοί στο ασύρματο τοπικό δίκτυο. Οι σταθμοί – κατάσκοποι, αφού λαμβάνουν όλα τα πακέτα που διακινούνται στο ασύρματο δίκτυο, θα είναι εφικτός ο υπολογισμός της διακίνησης του όγκου δεδομένων από και για κάθε σταθμό στο ασύρματο τοπικό δίκτυο ξεχωριστά. Έτσι ο διαχειριστής μπορεί να παίρνει καλύτερες αποφάσεις, βασισμένος σε έγκαιρες και έγκυρες πληροφορίες. Το μεγαλύτερο πλεονέκτημα όμως είναι πως η εφαρμογή μίας τέτοιας λειτουργίας δεν επιβαρύνει το ασύρματο τοπικό δίκτυο και το σημείο πρόσβασης, αφού ο φόρτος εργασίας μεταφέρεται στους σταθμούς – κατάσκοπους.

Η θεωρητική προσέγγιση που έγινε μπορεί να αποτελέσει έναυσμα για την εφαρμογή της στην πράξη η οποία απαιτεί πολλές μετρήσεις, πολλά πειράματα, πολύ υπομονή και δυστυχώς χρηματικό κεφάλαιο. Ωστόσο όμως μέσα από τα πειράματα και τις μετρήσεις μπορούν να προκύψουν νέες ιδέες και βελτιωμένες λύσεις για να ελαχιστοποιηθεί κι άλλο ή και να μηδενιστεί το ποσοστό ανασφάλειας στα ασύρματα τοπικά δίκτυα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

BackTrack 5, Documentation, http://www.backtrack-linux.org (visited March 2012)

K. Connelly, Y. Liu, D. Bulwinkle, A. Miller, and I. Bobbitt, "A toolkit for automatically constructing outdoor radio maps," in Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), vol. 2, apr. 2005, pp. 248 – 253 Vol. 2.

J. Duntemann, Jeff Duntemann's Wi-Fi Guide, 2nd Edition, Paraglyph Press, 2004

Ekahau HeatMapper, http://www.ekahau.com, (visited March 2012)

M. Ergen, "802.11 Tutorial", Department of Electronic Engineering and Computer Science, University of California, 2002

M. S. Gast Matthew, Wireless Networks - The Definitive Guide, O'Reilly, 2003

IEEE Std 802.11 – 2007, "IEEE Standard for Information technology - elecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2007

J. & R. Larocca, Demystified, McGraw Hill – Telecom, 2002

S. S. Miller, "Wi-Fi Security", MacGraw Hill – Networking Professional, 2003

N. Reid, R. Seide, "Networking Handbook", MacGraw Hill – Osborne, 2003

VEMI Lab, http://www.vemilab.org, (visited March 2012)

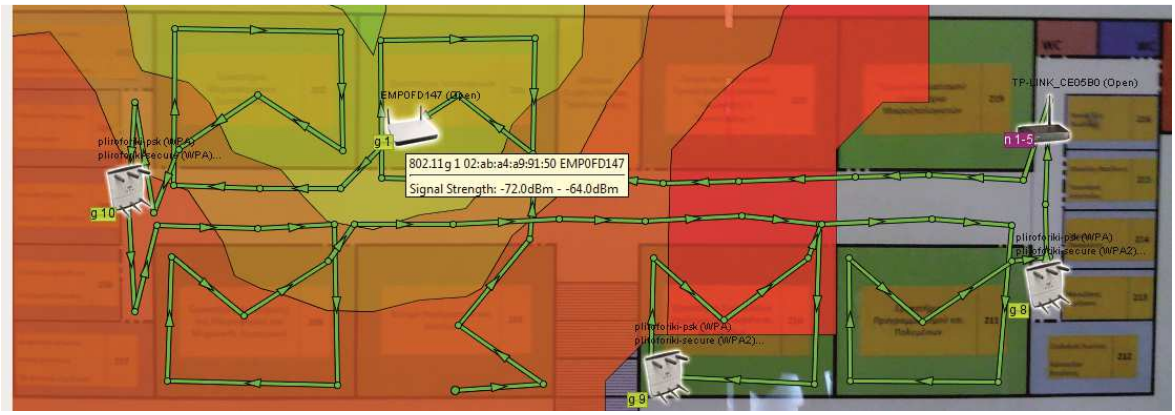
Β. Κώτσιας, «Μοντελοποίηση και Προσομοίωση Μηχανισμών Εντοπισμού Θέσης και Ad-Hoc Δρομολόγηση της Πληροφορίας σε Ασύρματα Δίκτυα», Διπλωματική Εργασία, Τομέας Ηλεκτρονικής και Υπολογιστών, Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2004

ΠΑΡΑΡΤΗΜΑΤΑ

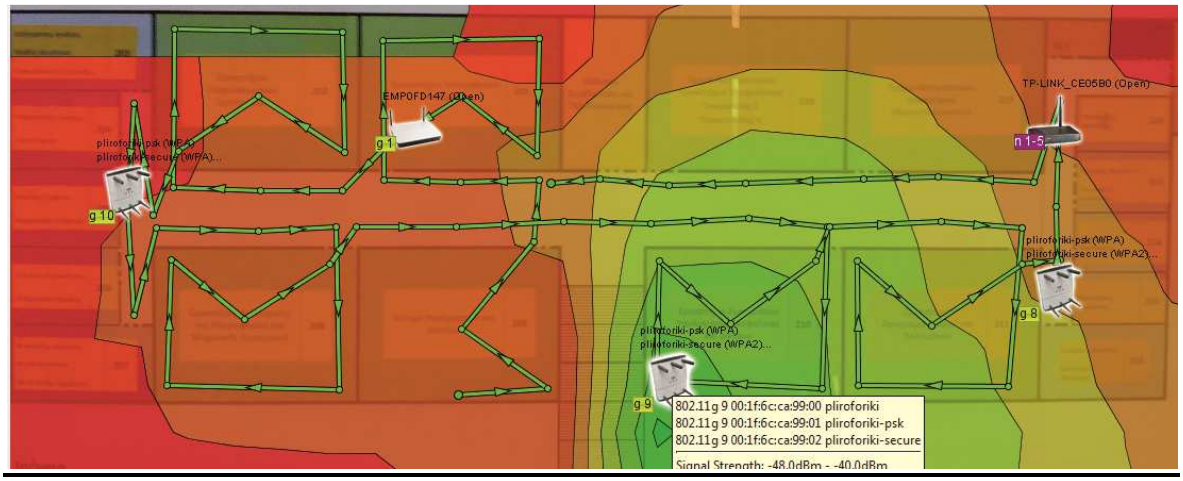
ΠΑΡΑΡΤΗΜΑ Α’

1ος ΟΡΟΦΟΣ

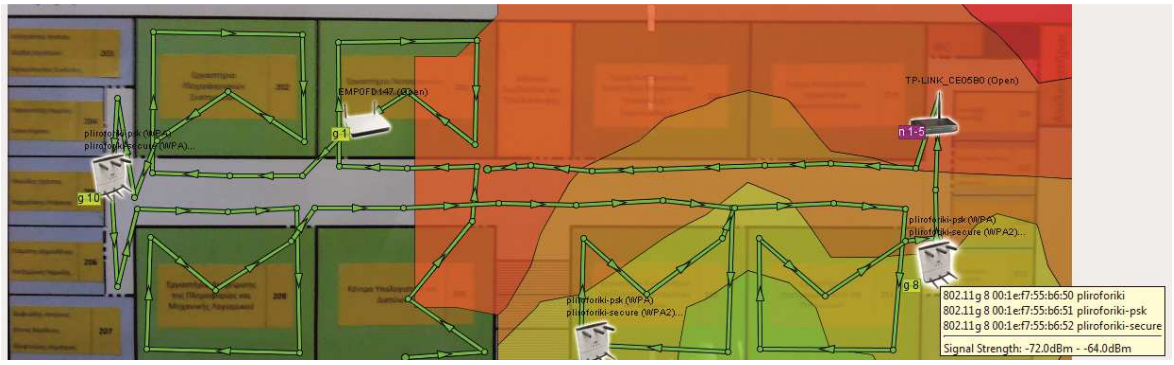
Αίθουσα 201



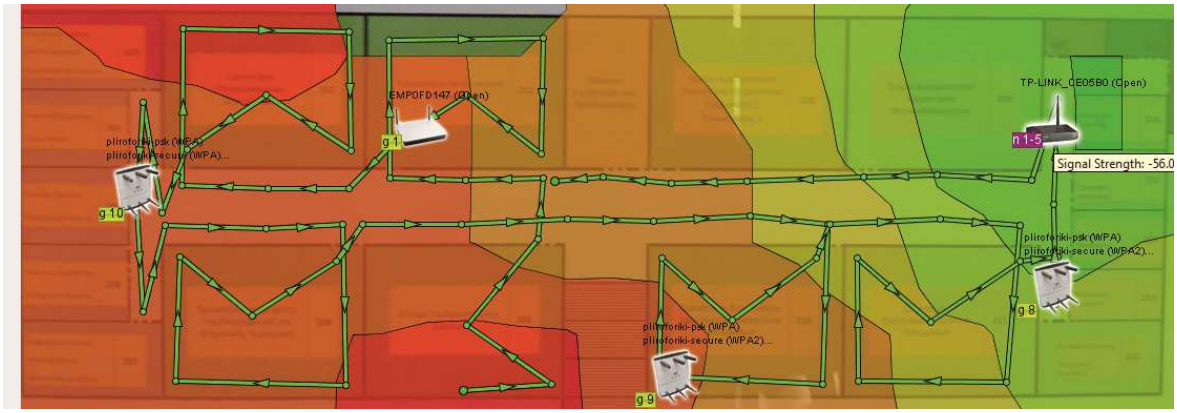
Αίθουσα 210



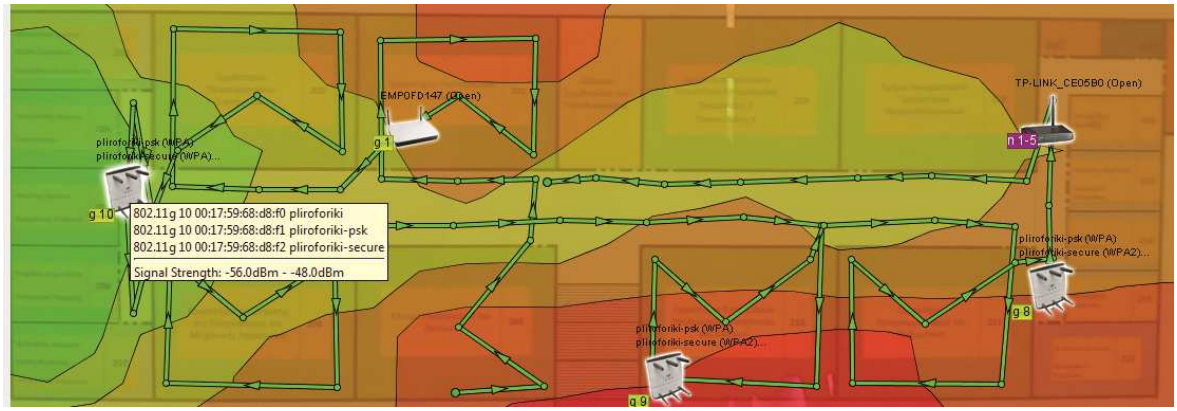
Αίθουσα 211



Αυτοματισμός



Γραφείο Καθηγητών



Συνολική κάλυψη