Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

«ΔΙΕΡΕΥΝΗΣΗ ΚΑΙ ΜΕΛΕΤΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΓΙΑ ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ (physical layer security) ΣΕ ΑΣΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ (outdoor urban topology), ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΦΥΣΙΚΗΣ ΚΑΤΑΣΤΡΟΦΗΣ,΄Η ΑΝΘΡΩΠΟΓΕΝΟΥΣ ΠΑΡΕΜΒΑΣΗΣ»

ΠΙΤΣΟΥΛΗΣ ΒΑΣΙΛΕΙΟΣ
Α.Μ.: 2013084
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΧΡΥΣΙΚΟΣ ΘΕΟΦΙΛΟΣ

ΣΠΑΡΤΗ

ΝΟΕΜΒΡΙΟΣ 2018

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Αρχικά, στο πρώτο κεφάλαιο θα αναφερθούμε στα ηλεκτρονικά συστήματα επικοινωνίας, στις βασικές αρχές λειτουργίας τους και στο φυσικό επίπεδο των ηλεκτρονικών συστημάτων επικοινωνίας. Οι πληροφορίες που θα δοθούν στο πρώτο κεφάλαιο είναι απαραίτητες γνώσεις για τον αναγνώστη για τη συνέχεια της εργασίας.

Στο δεύτερο κεφάλαιο θα αναφερθούμε στα ζητήματα ασφαλείας για τα ασύρματα δίκτυα επικοινωνίας, και κυρίως στην περίπτωση υπολογιστικών συστημάτων. Θα παρουσιαστούν τα περισσότερα και σημαντικότερα ζητήματα ασφαλείας, ο τρόπος με τον οποίο συμβαίνουν, καθώς και οι πιθανές λύσεις τους.

Στο τρίτο κεφάλαιο, θα γίνει ακριβών η ίδια διαδικασία αλλά για την περίπτωση της κινητής τηλεφωνίας. Η σταθερή τηλεφωνία, στην οποία το κανάλι είναι το καλώδιο, είναι εξαιρετικά πιο απλό ζήτημα, και για αυτό το λόγο δεν θα γίνει εκτενής αναφορά.

Στο τέταρτο κεφάλαιο θα παρουσιαστεί ένα σύντομο πλάνο αύξησης της ασφάλειας φυσικού επιπέδου.

Τέλος, θα παρουσιαστούν τα συμπεράσματα και η βιβλιογραφία.

ABSTRACT

Initially, in the first chapter we will analyze the electronic communication systems, their basic principles of operation and the physical level of electronic communication systems. The information to be given in the first chapter is necessary for the reader to work continuously.

In the second chapter we will discuss the security issues for wireless communication networks, especially in the case of computing systems. The most important security issues, the way they happen, and their possible solutions will be presented.

In the third chapter, the exact same procedure will be done, but in the case of mobile telephony. Fixed telephony, is an extremely simple situation compared to the wireless systems, and that is why there will be no extensive reporting.

The fourth chapter will present a brief plan to increase physical-level security.

At the end, will be presented the conclusions and bibliography.

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ ΣΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

1.1 Ηλεκτρονικά συστήματα επικοινωνίας

Ως ορισμό μπορούμε να αναφέρουμε ότι ένα σύστημα ηλεκτρονικών επικοινωνιών που χρησιμοποιεί ηλεκτρονικά σήματα είναι μια συλλογή μεμονωμένων δικτύων επικοινωνιών, συστημάτων μετάδοσης, σταθμών αναμετάδοσης, παρακείμενων σταθμών και τερματικού εξοπλισμού δεδομένων (DTE), τα οποία είναι συνήθως ικανά για διασύνδεση και διαλειτουργικότητα για να σχηματίσουν ένα ολοκληρωμένο σύνολο. Τα στοιχεία ενός συστήματος επικοινωνιών εξυπηρετούν έναν κοινό σκοπό, είναι τεχνικά συμβατά, χρησιμοποιούν κοινές διαδικασίες, ανταποκρίνονται στους ελέγχους και λειτουργούν σε ένωση (Schwartz & Bennett & Stein, 1996). Οι τηλεπικοινωνίες είναι μια μέθοδος επικοινωνίας (π.χ. για τις αθλητικές μεταδόσεις, τα μέσα μαζικής ενημέρωσης, τη δημοσιογραφία κ.λπ.). Ένα υποσύστημα επικοινωνιών είναι μια λειτουργική μονάδα ή λειτουργική διάταξη που είναι μικρότερη από τη μεγαλύτερη συνολική μονάδα και αποτελεί μέρος της (Schwartz & Bennett & Stein, 1996).

1.2 Τύποι συστημάτων επικοινωνίας

1.2.1 Κατηγορίες με βάση το μέσο

Ένα οπτικό σύστημα επικοινωνίας είναι οποιαδήποτε μορφή τηλεπικοινωνιών που χρησιμοποιεί το φως ως μέσο μετάδοσης. Ο εξοπλισμός αποτελείται από έναν πομπό,

ο οποίος κωδικοποιεί ένα μήνυμα σε ένα οπτικό σήμα, ένα κανάλι που μεταφέρει το σήμα στον προορισμό του και έναν δέκτη, ο οποίος αναπαράγει το μήνυμα από το ληφθέν οπτικό σήμα. Τα συστήματα επικοινωνίας οπτικών ινών μεταδίδουν πληροφορίες από το ένα μέρος στο άλλο, αποστέλλοντας φως μέσω μιας οπτικής ίνας. Το φως σχηματίζει ένα φέρον σήμα που διαμορφώνεται για να μεταφέρει πληροφορίες (Πανέτσος, 2007).

Ένα σύστημα ραδιοεπικοινωνίας αποτελείται από πολλά υποσυστήματα επικοινωνιών που παρέχουν δυνατότητα εξωτερικής επικοινωνίας. Ένα σύστημα ραδιοεπικοινωνίας περιλαμβάνει έναν αγωγό μετάδοσης στον οποίο παράγονται ηλεκτρικές ταλαντώσεις ή ρεύμα και ο οποίος είναι διατεταγμένος ώστε να προκαλεί τέτοια ρεύματα ή ταλαντώσεις που να διαδίδονται μέσω του ελεύθερου μέσου από ένα σημείο έως ένα άλλο απομακρυσμένο σημείο, και να το δέχεται ένας αγωγός λήψεως σε τέτοιο απομακρυσμένο σημείο προσαρμοσμένο ώστε να διεγείρεται από τις ταλαντώσεις ή τα ρεύματα που διαδίδονται από τον πομπό.

Τα συστήματα επικοινωνίας γραμμής ισχύος λειτουργούν μέσω ενός διαμορφωμένου φορέα σήματος στα καλώδια τροφοδοσίας. Υπάρχουν διαφορετικοί τύποι επικοινωνιών μέσω γραμμών μεταφοράς ισχύος που χρησιμοποιούν διαφορετικές ζώνες συχνοτήτων, ανάλογα με τα χαρακτηριστικά μετάδοσης σήματος της καλωδίωσης ισχύος που χρησιμοποιείται. Δεδομένου ότι το σύστημα ηλεκτρικής καλωδίωσης προοριζόταν αρχικά για μετάδοση εναλλασσόμενου ρεύματος, τα κυκλώματα καλωδίων ισχύος έχουν περιορισμένη μόνο δυνατότητα μεταφοράς υψηλότερων συχνοτήτων. Υπάρχει όμως το πρόβλημα της διάδοσης, που είναι ένας περιοριστικός παράγοντας για κάθε τύπο επικοινωνιών γραμμής ισχύος (Πανέτσος, 2007).

1.2.2 Κατηγορίες με βάση την τεχνολογία

Ένα σύστημα αμφίδρομης επικοινωνίας είναι ένα σύστημα που αποτελείται από δύο συνδεδεμένα μέρη ή συσκευές που μπορούν να επικοινωνούν μεταξύ τους και προς τις δύο κατευθύνσεις. Ο όρος duplex χρησιμοποιείται όταν περιγράφεται η επικοινωνία μεταξύ δύο συμβαλλομένων ή δύο συσκευών. Τα δίκτυα διπλής ροής (full-duplex) χρησιμοποιούνται σχεδόν σε όλα τα δίκτυα επικοινωνιών, είτε για να επιτρέπουν την αμφίδρομη επικοινωνία μεταξύ δύο συνδεδεμένων μερών είτε για να παρέχουν μια αντίστροφη διαδρομή για την παρακολούθηση και ρύθμιση από απόσταση του εξοπλισμού στον κάθε τομέα.

Η κεραία είναι βασικά ένα αγώγιμο μέσο που χρησιμοποιείται για να ακτινοβολεί ή να δέχεται ηλεκτρομαγνητικά κύματα. Λειτουργεί ως συσκευή μετάδοσης και λήψης δεδομένων κατάλληλα διαμορφωμένων σε υψίσυχνο κωδικοποιημένο σήμα ως ηλεκτρομαγνητικά κύματα. Στο τέλος λήψης οι τηλεπικοινωνιακές διατάξεις του δέκτη μετατρέπουν τα ηλεκτρομαγνητικά κύματα σε ηλεκτρικά σήματα που βασικής ζώνης (Schwartz & Bennett & Stein, 1996).

Υπάρχουν πολλοί τύποι κεραιών που χρησιμοποιούνται στην επικοινωνία. Παραδείγματα συσκευών που χρησιμοποιούν αυτή την τεχνολογία επικοινωνιών είναι:

- Τηλέφωνο
- Κινητό τηλέφωνο
- Τηλέγραφος
- Το λειτουργικό Microsoft Windows
- Το καλώδιο τηλεόρασης

1.2.3 Κατηγοριοποίηση με βάση την περιοχή εφαρμογής

Ένα σύστημα στρατιωτικών επικοινωνιών είναι ένα σύστημα επικοινωνιών το οποίο (α) χρησιμοποιείται με άμεση στήριξη των στρατιωτικών δυνάμεων, (β) έχει σχεδιαστεί για να ικανοποιεί τις απαιτήσεις αλλαγής καταστάσεων και ποικίλων περιβαλλοντικών συνθηκών, (γ) παρέχει ασφαλή επικοινωνία, φωνής, δεδομένων και βίντεο μεταξύ χρηστών για τη διευκόλυνση της διοίκησης και του ελέγχου για την υποστήριξη των στρατιωτικών δυνάμεων και δ) συνήθως απαιτεί εξαιρετικά σύντομο χρόνο εγκατάστασης, συνήθως διάρκειας ωρών, προκειμένου να ικανοποιηθούν οι απαιτήσεις για συχνή μετεγκατάσταση.

Ένα σύστημα επικοινωνίας επείγουσας ανάγκης είναι οποιοδήποτε σύστημα (συνήθως βασισμένο σε υπολογιστή) το οποίο είναι οργανωμένο με πρωταρχικό σκοπό την υποστήριξης της αμφίδρομης επικοινωνίας μηνυμάτων έκτακτης ανάγκης μεταξύ ατόμων και ομάδων ατόμων. Αυτά τα συστήματα είναι συνήθως σχεδιασμένα για να μετατρέπουν τη διασταυρούμενη επικοινωνία των μηνυμάτων μεταξύ των διαφόρων τεχνολογιών επικοινωνίας.

Ένας αυτόματος διανομέας κλήσεων (ACD) είναι ένα σύστημα επικοινωνίας που αναστέλλει αυτόματα, αντιστοιχίζει και συνδέει τους καλούντες με τους χειριστές. Χρησιμοποιείται συχνά στην εξυπηρέτηση πελατών (όπως για παράπονα προϊόντων ή υπηρεσιών), στις παραγγελίες μέσω τηλεφώνου ή υπηρεσίες συντονισμού (όπως στον έλεγχο της εναέριας κυκλοφορίας).

Ένα Σύστημα Ελέγχου Φωνητικής Επικοινωνίας (VCCS) είναι ουσιαστικά ένα ACD με χαρακτηριστικά που το καθιστούν πιο προσαρμοσμένο για χρήση σε κρίσιμες καταστάσεις (χωρίς αναμονή) (Schwartz & Bennett & Stein, 1996).

1.3 Συστατικά μέρη

1.3.1 Πηγές

Οι πηγές μπορούν να ταξινομηθούν ως ηλεκτρικές ή μη ηλεκτρικές. Αποτελούν την προέλευση ενός μηνύματος ή ενός σήματος εισόδου. Παραδείγματα πηγών είναι τα εξής:

- Αρχεία ήχου (MP3, MKV, MP4, κλπ ...)
- Αρχεία κινούμενων εικόνων (GIF)
- Μηνύματα ηλεκτρονικού ταχυδρομείου
- Ανθρώπινη φωνή
- Εικόνα τηλεόρασης
- Ηλεκτρομαγνητική ακτινοβολία

1.3.2 Μετατροπείς εισόδου (αισθητήρες)

Οι αισθητήρες, όπως τα μικρόφωνα και οι κάμερες, συλλαμβάνουν μη ηλεκτρικές πηγές, όπως τον ήχο και το φως, και τις μετατρέπουν σε ηλεκτρικά σήματα. Αυτοί οι τύποι αισθητήρων ονομάζονται μετατροπείς εισόδου σε σύγχρονα αναλογικά και ψηφιακά συστήματα επικοινωνίας. Χωρίς μετατροπείς εισόδου δεν θα υπήρχε αποτελεσματικός τρόπος μεταφοράς μη ηλεκτρικών πηγών ή σημάτων σε μεγάλες αποστάσεις, δηλαδή οι άνθρωποι θα πρέπει να βασίζονται αποκλειστικά στα αισθητήρια όργανά τους για την μεταφορά σήματος και την επικοινωνία (Rappaport, 1996).

Παραδείγματα μετατροπέων εισόδου είναι:

- Μικρόφωνα
- Κάμερες
- Πληκτρολόγια
- Ποντίκι
- Αισθητήρες δύναμης
- Επιταχυνσιόμετρο

1.3.3 Πομπός

Μόλις το σήμα της πηγής μετατραπεί σε ηλεκτρικό σήμα, ο πομπός καλείται να τροποποιήσει αυτό το σήμα για να λάβει χώρα αποτελεσματική μετάδοση. Για να γίνει αυτό, το σήμα πρέπει να περάσει από ένα ηλεκτρονικό κύκλωμα που περιέχει τα ακόλουθα εξαρτήματα:

- Φίλτρο θορύβου
- Αναλογικός σε ψηφιακό μετατροπέα (μετατροπέας A / D)
- Κωδικοποιητής
- Ρυθμιστής
- Ενισχυτής σήματος

Αφού το σήμα ενισχυθεί, είναι έτοιμο για μετάδοση. Στο τέλος του κυκλώματος υπάρχει μια κεραία, όπου είναι το σημείο από το οποίο απελευθερώνεται το σήμα ως ηλεκτρομαγνητικά κύματα (ή ηλεκτρομαγνητική ακτινοβολία) στον χώρο (ασύρματο μέσο μετάδοσης) (Rappaport, 1996).

1.3.4 Κανάλια επικοινωνίας

Ένας δίαυλος επικοινωνίας είναι η έννοια που αναφέρεται στο φυσικό μέσο με το οποίο ταξιδεύει ένα σήμα. Υπάρχουν δύο τύποι μέσων με τα οποία ταξιδεύουν τα ηλεκτρικά σήματα, κατευθυνόμενα και μη κατευθυνόμενα. Τα κατευθυνόμενα μέσα αναφέρονται σε οποιοδήποτε μέσο που μπορεί να κατευθυνθεί από πομπό σε δέκτη μέσω καλωδίων σύνδεσης. Στην επικοινωνία οπτικών ινών, το μέσο είναι μια οπτική (γυάλινη) ίνα. Άλλα μέσα καθοδήγησης μπορεί να είναι τα ομοαξονικά καλώδια, το σύρμα τηλεφώνου, συνεστραμμένα ζεύγη (twisted pair cables) κλπ. Ο άλλος τύπος μέσων, τα μη κατευθυνόμενα μέσα, αναφέρεται σε οποιοδήποτε κανάλι επικοινωνίας που δημιουργεί χώρο μεταξύ του πομπού και του δέκτη. Για τη ραδιοφωνική επικοινωνία, το μέσο είναι ο αέρας. Ο αέρας είναι το μόνο μέσο μεταξύ του πομπού και του δέκτη για την επικοινωνία και μέσω RF, ενώ σε άλλες περιπτώσεις, όπως το σόναρ, το μέσο είναι συνήθως νερό, επειδή τα ηχητικά κύματα ταξιδεύουν αποτελεσματικά μέσω ορισμένων υγρών μέσων. Και οι δύο τύποι μέσων θεωρούνται μη κατευθυνόμενοι επειδή δεν υπάρχουν καλώδια σύνδεσης μεταξύ του πομπού και του δέκτη. Τα κανάλια επικοινωνίας περιλαμβάνουν σχεδόν τα πάντα, από το κενό του χώρου μέχρι τα στερεά κομμάτια του μετάλλου. Ωστόσο, ορισμένα μέσα προτιμώνται περισσότερο από άλλα. Αυτό συμβαίνει επειδή οι διαφορετικές πηγές ταξιδεύουν μέσω διαφορετικών μέσων με κυμαινόμενες αποδόσεις (Πανέτσος, 2007).

1.3.5 Δέκτης

Μόλις το σήμα περάσει από το κανάλι επικοινωνίας, πρέπει να ληφθεί αποτελεσματικά από ένα δέκτη. Ο στόχος του δέκτη είναι να καταγράψει και να ανακατασκευάσει το σήμα από τον πομπό (δηλαδή τον μετατροπέα A/D, τον

διαμορφωτή και τον κωδικοποιητή). Αυτό επιτυγχάνεται με τη διέλευση του ληφθέντος σήματος μέσω άλλου κυκλώματος που περιέχει τα ακόλουθα εξαρτήματα:

- Φίλτρο θορύβου
- Μετατροπέας ψηφιακού σε αναλογικό (μετατροπέας D/A)
- Αποκωδικοποιητής
- Αποδιαμορφωτής
- Ενισχυτής σήματος

Το σήμα υπόκειται σε σημαντική απώλεια ισχύος από τη στιγμή που θα περάσει από το κανάλι ή το μέσο επικοινωνίας. Το σήμα μπορεί να ενισχυθεί με τη διέλευσή του μέσω ενός ενισχυτή σήματος αφού απομακρυνθεί ο θόρυβος που θα έχει εισαχθεί από τα στοχαστικά φαινόμενα του ασύρματου καναλιού και από ανεπιθύμητες παρεμβολές, ομοκαναλικές ή γειτονικού καναλιού, και αφού επίσης αντιμετωπιστούν κατάλληλα τα προϊόντα θορύβου ενδοδιαμόρφωσης (Πανέτσος, 2007).

1.3.6 Μεταγωγέας εξόδου

Ο μετατροπέας εξόδου απλά μετατρέπει το ηλεκτρικό σήμα (που δημιουργείται από τον μετατροπέα εισόδου) πίσω στην αρχική του μορφή. Παραδείγματα μετατροπέων εξόδου είναι τα εξής:

- Ηχεία (Ήχος)
- Οθόνες
- Κινητήρες (Κίνηση)

- Φωτισμός (Οπτική)

Ορισμένα κοινά ζεύγη μεταγωγέων εισόδου και εξόδου είναι:

- Μικρόφωνα και ηχεία (σήματα ήχου)
- Πληκτρολόγια και οθόνες υπολογιστών
- Κάμερες και οθόνες υγρών κρυστάλλων (LCD)
- Αισθητήρες δύναμης (κουμπιά) και φώτα ή κινητήρες

Και πάλι, οι μετατροπείς εισόδου μετατρέπουν μη ηλεκτρικά σήματα όπως φωνή σε ηλεκτρικά σήματα που μπορούν να μεταδοθούν σε μεγάλες αποστάσεις πολύ γρήγορα. Οι μετατροπείς εξόδου μετατρέπουν το ηλεκτρικό σήμα σε ήχο ή εικόνα, κ.λπ. Υπάρχουν πολλοί διαφορετικοί τύποι μετατροπέων και οι συνδυασμοί είναι απεριόριστοι (Schwartz & Bennett & Stein, 1996).

1.4 Θεμελιώδεις έννοιες ασφαλείας

Η ασφάλεια πληροφοριακών συστημάτων και τηλεπικοινωνιών είναι κλάδος της επιστήμης που ασχολείται με την προστασία των υπολογιστών, των συστημάτων επικοινωνιών, των δικτύων και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή την παράνομη χρήση τους. Ανάμεσα στους συγγενικούς τομείς της ασφάλειας πληροφοριακών συστημάτων συμπεριλαμβάνονται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία (Scasfone & Mell, 2007). Στην παρούσα εργασία ωστόσο θα επεκταθούμε όχι μόνο

στην ασφάλεια από ανθρώπινη απειλή, αλλά και στην ασφάλεια των συστημάτων από την απειλή φυσικής καταστροφής.

1.4.1 Προϋποθέσεις ασφάλειας

Η ασφάλεια είναι πολύ σημαντική καθώς στηρίζεται σε τρεις βασικές ιδέες οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός συστήματος, και είναι οι εξής:

Ακεραιότητα (Integrity): Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και στην αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα (Πάγκαλος & Μαυρίδης, 2002).

Διαθεσιμότητα (Availability): Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Για παράδειγμα το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια

εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.

Εμπιστευτικότητα (Confidentiality):Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή. Για παράδειγμα: με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας.

1.5 Ανάλυση επικινδυνότητας

Η διαμόρφωση της πολιτικής ασφάλειας για τα συστήματα ενός οργανισμού έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να γίνει με διάφορους τρόπους, οι πιο συνηθισμένοι από αυτούς είναι η εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας (Risk Analysis) και η χρήση κάποιων από τα πρότυπα (standards) διαχείρισης ασφάλειας.

Για καλύτερη κατανόηση αρχικά δίνονται οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων:

Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών τυχαία ή με πρόθεση, μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Είναι η αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή, που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της

ακεραιότητας του συστήματος. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια.

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του συστήματος και για την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.

1.5.1 Οφέλη ανάλυσης επικινδυνότητας

Με την διαδικασία της ανάλυσης των κινδύνων, προκύπτουν τα εξής οφέλη:

- Γενική βελτίωση της ασφάλειας του συστήματος
- Στόχευση της ασφάλειας
- Βελτίωση της κατανόησης του συστήματος
- Κατανόηση της αναγκαιότητας της ασφάλειας
- Δικαιολόγηση των δαπανών για την ασφάλεια

1.5.2 Μέθοδοι ανάλυσης επικινδυνότητας

Για την αξιολόγηση, ή αλλιώς αποτίμηση, του επιπέδου ασφάλειας των πληροφοριακών και τηλεπικοινωνιακών συστημάτων μπορούν να εφαρμοστούν διάφορες τεχνικές ανάλυσης επικινδυνότητας. Οι πιο διαδεδομένες από τις οποίες

είναι οι SBA (Security By Analysis), η MARION και η CRAMM (CCTA Risk Analysis and Management Method). Σε αυτήν την περίπτωση, η διαμόρφωση της πολιτικής ασφάλειας γίνεται με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας.

Σημαντικά πλεονεκτήματα της πρακτικής αυτής είναι ότι η πολιτική ασφάλειας ανταποκρίνεται στις ιδιαίτερες ανάγκες του οργανισμού για τον οποίο έχει μελετηθεί η επικινδυνότητα, και ότι το επίπεδο της παρεχόμενης ασφάλειας με την κατάλληλη επιλογή των μέτρων προστασίας είναι αντίστοιχο των κινδύνων που αντιμετωπίζουν τα πληροφοριακά και τηλεπικοινωνιακά συστήματα ενός οργανισμού. Μειονέκτημα της προσέγγισης αυτής είναι το στοιχείο του υποκειμενισμού που εμπεριέχεται στις μεθόδους ανάλυσης επικινδυνότητας, τα αποτελέσματα των οποίων εξαρτώνται σε μεγάλο βαθμό από την εμπειρία και τις γνώσεις του αναλυτή (Scasfone & Mell, 2007).

1.5.3 Τύπος BPL

Καρδιά της ανάλυσης κινδύνων αποτελεί ο τύπος: $B > P * L$.

Τα τρία στοιχεία του τύπου BPL είναι:

B = Το κόστος για την πρόληψη μιας απώλειας

P = Η πιθανότητα να συμβεί μια απώλεια

L = Το συνολικό κόστος μιας απώλειας

Ο τύπος αυτός αποτελεί την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά και τηλεπικοινωνιακά συστήματα. Εμπεριέχει την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης. Ωστόσο αν και ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκουν σημαντικές δυσκολίες, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Η αντιστοίχηση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι πελάτες ή οι χρήστες του σε αυτόν (Siponen, 2000).

1.6 Μέτρα ασφαλείας

Η πολιτική ασφαλείας συμπληρώνεται από τα Μέτρα Ασφαλείας / Μέτρα Προστασίας (controls) ή Αντίμετρα (countermeasures), που αφορούν όλες τις διαδικασίες, τις τεχνικές, τις ενέργειες και τις συσκευές που περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού ή τηλεπικοινωνιακού συστήματος, καθώς και από το πλάνο υλοποίησης τους.

Τα αντίμετρα χωρίζονται σε 4 μεγάλες κατηγορίες:

- Πρόληψη: τα αντίμετρα αυτά προσπαθούν να μειώσουν τον κίνδυνο
- Διασφάλιση: εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των αντιμέτρων
- Ανίχνευση: προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών

- Επαναφορά: διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε

Για την επιτυχή εφαρμογή της πολιτικής ασφαλείας, το σχέδιο ασφαλείας πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης με επισκοπήσεις και επιθεωρήσεις της εφαρμογής του, ώστε με τις κατάλληλες αναθεωρήσεις να είναι πάντα up-to-date σε σχέση με τις τεχνολογικές εξελίξεις (Siponen, 2000).

Ολοκληρώνοντας το σχέδιο ασφαλείας, θα πρέπει να καταρτισθεί αναλυτικό σχέδιο έκτακτης ανάγκης, το οποίο θα περιλαμβάνει σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan), καθώς και σχέδιο αποκατάστασης λειτουργίας (contingency action plan). Η εισαγωγή (προσθήκη μηχανισμών) ασφαλείας σε ένα πληροφοριακό ή ένα τηλεπικοινωνιακό σύστημα είναι ένα δύσκολο και περίπλοκο έργο. Για την ελληνική πραγματικότητα ίσως η πλέον σημαντική δυσκολία οφείλεται στο σημαντικό κόστος της ασφάλειας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

K. Scasfone, P. Mell, (2007). Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology.

Radio Communications System (RCS) www.fas.org/man/dod-101/sys/ship/weaps/radio.htm

Rappaport, T. S. (1996). Wireless communications: principles and practice. Upper Saddle River, N.J.: Prentice Hall PTR.

S. Powell, J.P. Shim, (2009). Wireless Technology Application, Management and Security, Springer.

Schwartz, M., Bennett, W. R., & Stein, S. (1996). Communication systems and techniques. New York: IEEE Press.

Siponen, M., (2000).Policies for Construction of Information Systems Security Guidelines, Kluwer Academic Publishers.

Καρύδα Μαρία, (2005). Διοίκηση ασφάλειας πληροφοριακών συστημάτων, Αθήνα.

Πάγκαλος Γ., Μαυρίδης Ι.,(2002). Ασφάλεια πληροφοριακών συστημάτων και δικτύων. Θεσσαλονίκη.

Πανέτσος Σ., (2007), Επικοινωνίες & Δίκτυα Υπολογιστών, εκδόσεις Τζιόλα, Θεσσαλονίκη.

ΚΕΦΑΛΑΙΟ 2: ΑΣΦΑΛΕΙΑ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Εισαγωγή

Οι τεχνολογίες υπολογιστών και ασυρμάτων επικοινωνιών έχουν καταστεί ένα πολύ σημαντικό κομμάτι της ζωής των ανθρώπων τις τελευταίες δύο δεκαετίες. Ένα μεγάλο μέρος της αγοράς υπολογιστών σήμερα είναι η ασύρματη δικτύωση. Τα ασύρματα δίκτυα έχουν πολλά πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα.

Καθώς η τεχνολογία εξελίσσεται περαιτέρω, το hardware του υπολογιστή γίνεται όλο και μικρότερο. Ταυτόχρονα, η ασύρματη τεχνολογία προσφέρει στους ανθρώπους κινητικότητα, ταχύτητα και άλλες ανέσεις συγκριτικά με την ενσύρματη επικοινωνία.

Οι πρώτες συσκευές ασύρματης δικτύωσης χρησιμοποίησαν μήκη κύματος υπερύθρων για τη μετάδοση δεδομένων. Τα πιο πρόσφατα μοντέλα ασύρματων συσκευών αφορούν στις μικροκυματικές συχνότητες όπου λαμβάνει χώρα η πλειοψηφία τω επίγειων ασύρματων μεταδόσεων και λήψεων λόγω δυνατότητες για ευρυζωνικότητα και καλύτερη διεμβόλιση των υλικών μέσων και εμποδίων. Επίσης, στα μικροκύματα (300 MHz – 6 GHz) έχουμε κεραίες κατάλληλα μικρών και πεπερασμένων διαστάσεων λόγω χαμηλότερου μήκους κύματος (Chrysikos, 2009). Συνολικά, τα ραδιοκύματα προτιμώνται γιατί παρέχουν καλύτερη κάλυψη, η οποία είναι πολύ σημαντική για έναν χρήστη. Ταυτόχρονα γίνονται και περαιτέρω έρευνες για να ενισχυθεί η κάλυψη των ασύρματων δικτύων με τη χρήση τεχνικών διαμόρφωσης και επεξεργασίας ψηφιακού σήματος, αλλά και με μελέτη της δυνατότητας μετάδοσης και λήψης δεδομένων σε ζώνες μεγαλύτερων συχνοτήτων (εκατοστομετρική συχνότητα στο άνω άκρο της SHF ζώνης, χιλιοστομετρική μετάδοση στην EHF ζώνη).

Σε αναζήτηση καλύτερης ποιότητας, οι τεχνολογίες αλλάζουν συνεχώς. Μια από αυτές τις τεχνολογίες ήταν ο διαφορισμός κεραίας (antenna space diversity system). Σε αυτή την τεχνολογία υπάρχουν πολλοί πομποί που χρησιμοποιούνται για να

επιλεχθεί ποιος πομπός είναι πιο αποδοτικός για έναν συγκεκριμένο χρόνο και τοποθεσία. Σε αυτή τη διαμόρφωση, μόνο ένας πομπός και δέκτης πρέπει να χρησιμοποιούνται κάθε φορά.

Ένα πιο εξελιγμένο σύστημα που επήλθε ως εξέλιξη του προαναφερθέντος συστήματος είναι ένα σύστημα που μπορεί να χρησιμοποιεί πολλαπλές κεραίες ταυτόχρονα. Η χρήση πολλαπλών κεραιών ταυτόχρονα είναι το πρώτο βήμα των συστημάτων MIMO, Multiple Input Multiple Output. Με το MIMO (όταν ξεκινά η μετάδοση σήματος με πολλαπλές κεραίες) η απόδοση έχει βελτιωθεί εξαιρετικά από την απλή διαμόρφωση μιας κεραίας. Το MIMO βοήθησε επίσης στην επίλυση των προβλημάτων των πολλαπλών παρεμβολών. Για την ταυτόχρονη μετάδοση χρησιμοποιούνται διαφορετικές τεχνικές επεξεργασίας ψηφιακού σήματος. Η ποιότητα των δεδομένων βελτιώθηκε επίσης (Steyskal, 1987).

Τα συστήματα πολλαπλών κεραιών επιτρέπουν τη χρήση μορφοποίησης δέσμης. Η μέθοδος Beamforming είναι μια τεχνική επεξεργασίας ψηφιακού σήματος που επιτρέπει την τοποθέτηση του σήματος σε μια συγκεκριμένη διεύθυνση. Αυτό απαιτεί όλες οι κεραίες να χρησιμοποιούν την ίδια κωδικοποίηση. Σε ορισμένες περιπτώσεις, η σημασία της επεξεργασίας ψηφιακού σήματος είναι το σημαντικότερο βήμα, όπως όταν ο αριθμός των χωρικών ροών είναι μεγαλύτερος από τον αριθμό των κεραιών λήψης.

Το MIMO ως τεχνολογία οδήγησε στην ανάπτυξη της έννοιας της έξυπνης κεραίας λόγω της ικανότητάς του να προσαρμόζει ένα σήμα σε διαφορετικές καταστάσεις και απαιτήσεις. Στο πεδίο αυτό, οι άνθρωποι προσπαθούν να επωφεληθούν από τις έξυπνες κεραίες για υψηλότερες ταχύτητες, και για σκοπούς ασφαλείας. Οι έξυπνες κεραίες αποτελούν έναν ευρύ τομέα έρευνας, αλλά ταυτόχρονα αυξάνουν και τα απαιτούμενα μέτρα ασφαλείας από πιθανές παραβιάσεις(Liberty & Rappaport, 1999).

2.1 Βασικές αρχές ασφάλειας φυσικού επιπέδου

Στο μοντέλο ανοικτού συστήματος διασύνδεσης (OSI) 7 επιπέδων, το φυσικό επίπεδο ή το επίπεδο 1 είναι το η πρώτη (χαμηλότερη) βαθμίδα. Συνήθως αναφέρεται με τη συντόμευση PHY.

Το όνομα «φυσικό επίπεδο» μπορεί να είναι λίγο προβληματικό. Πολλοί άνθρωποι που μελετούν τη δικτύωση έχουν την εντύπωση ότι το φυσικό επίπεδο αφορά μόνο στις συσκευές και το υλικό, γεγονός που δεν ισχύει.

Το PHY περιέχει:

- Ορισμός προδιαγραφών υλικού
- Κωδικοποίηση και μετάδοση σήματος
- Μετάδοση δεδομένων και λήψη
- Σχεδίαση τοπολογίας και φυσικού δικτύου

Ορισμένες βασικές τεχνολογίες στο PHY είναι:

- CDMA
- OFDM
- MIMO

Σε όλα τα συστήματα επικοινωνίας, τα θέματα της εξακρίβωσης, της εμπιστευτικότητας και ιδιωτικότητας αναφέρονται συνήθως στα ανώτερα επίπεδα ασφάλειας, αλλά ένα μέρος αυτών των διαδικασιών βρίσκεται στο πρώτο επίπεδο.

Σήμερα, η επεξεργασία σήματος και η κρυπτογραφία δείχνουν ότι υπάρχει μεγάλη ανάγκη για ασφάλεια που πρέπει να αποκτηθεί από την κάλυψη των ατελειών του

φυσικού επιπέδου ασφαλείας. Για παράδειγμα, ενώ ο θόρυβος και η εξασθένιση σήματος αντιμετωπίζονται ως προβλήματα στις ασύρματες επικοινωνίες, αποτελέσματα ερευνών δείχνουν ότι μπορούν να αξιοποιηθούν για να κρύψουν μηνύματα από δυναμικές υποκλοπές ή συσκευές ελέγχου ταυτότητας, χωρίς να απαιτείται ένα επιπλέον μυστικό κλειδί (Chrysikos 2011).

Στο επόμενο υποκεφάλαιο, πριν εισαχθούμε στο κυρίως θέμα του κεφαλαίου, δηλαδή στην ασφάλεια φυσικού επιπέδου των ασύρματων δικτύων, θα αναλύσουμε το ευρέως χρησιμοποιούμενο πρωτόκολλο TCP.

2.2 Το πρωτόκολλο TCP

Το πρωτόκολλο TCP (transmission Control Protocol) είναι το πλέον διαδεδομένο και χρησιμοποιούμενο πρωτόκολλο στο διαδίκτυο. Χρησιμοποιείται κυρίως για την εγκαθίδρυση σύνδεσης και τον τερματισμό σύνδεσης. Επίσης, κάποια από τα θέματα που θα αναφέρουμε είναι η αξιόπιστη μεταφορά δεδομένων με επαναμεταφορά (Retransmission) και επαναταξινόμηση των εκτός σειράς πακέτων (packet re-ordering), ο έλεγχος ροής (Flow Control) και ο έλεγχος και η αποφυγή συμφόρησης (Congestion avoidance).

2.2.1 Header του TCP

Το κάθε πακέτο του πρωτοκόλλου TCP ονομάζεται τομέας ή segment, και έχει μια επικεφαλίδα ή header η οποία δίνει βασικές πληροφορίες για το πακέτο και για το πρωτόκολλο TCP. Κάθε επικεφαλίδα μπορεί να περιέχει από 5 ως 15 words (απουσία ή παρουσία όλων των επιλογών αντίστοιχα) (Gast, 2002).

2.2.2 Έναρξη σύνδεσης

Κάθε χρήστης πριν συνδεθεί με κάποιον αποστολέα θα πρέπει πρώτα να δεσμεύσει μια θύρα και να ανοίξει η θύρα, ώστε να γίνει εφικτό ο χρήστης να μπορεί να έχει σύνδεση. Το άνοιγμα αυτό καλείται παθητικό άνοιγμα. Μετά την δέσμευση της θύρας μπορεί να αρχίσει μια σύνδεση με τρίτο μέρος, διεργασία που καλείται ενεργό άνοιγμα, και ονομάζονται passive και active open αντίστοιχα. Η συμβολή και των τριών μερών ώστε να γίνει η σύνδεση καλείται τριπλή χειραψία ή 3-way handshake .

Έναρξη της σύνδεσης με τριμερή χειραψία (3-way handshake)

Φάση πρώτη:

Στην πρώτη φάση αποστέλλεται ένα πακέτο με το SYN bit ενεργοποιημένο. Ο πελάτης με τη σειρά του αποστέλλει το πεδίο αριθμού ακολουθίας στο header του TCP, στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number).

Φάση δεύτερη:

Ο αποστολέας στο άλλο άκρο απαντάει, είτε με συγχρονισμό αριθμών ακολουθίας SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1 του πελάτη) του πρώτου πακέτου του χρήστη για να αποδεχτεί τη σύνδεση ή συγχρονισμό αριθμών ακολουθίας/ επαναρύθμιση σύνδεσης (SYN/RST) για να ενημερώσει τον χρήστη ότι αρνείται τη σύνδεση και η διαδικασία σταματά.

Φάση τρίτη:

Όταν ο client πάρει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν πλέον να σταλούν τα δεδομένα. Κατά τη διάρκεια της τριμερούς χειραψίας, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κ.α. (Gast, 2002).

2.2.3 Τερματισμός σύνδεσης

Για τον τερματισμό της σύνδεσης απαιτείται μια συμβολή τεσσάρων μερών που καλείται τετραμερής χειραψία ή αλλιώς 4-way handshake. Στη διαδικασία αυτή το κάθε μέρος τερματίζει τη σύνδεση με ανεξάρτητο τρόπο.

Το πακέτο TCP το οποίο είναι υπεύθυνο για το τέλος της διεργασίας έχει header FIN, και όταν κάποιο μέλος θέλει να τερματίσει τη σύνδεση στέλνει το πακέτο με το FIN ενεργοποιημένο. Το πακέτο επιβεβαιώνεται από τις άλλες πλευρές με ACK, και αποστέλλει πακέτο FIN από την πλευρά της που επιβεβαιώνεται με ACK και από την άλλη πλευρά. Για να ολοκληρωθεί ένας τερματισμός χρειάζονται ουσιαστικά δύο αποστολές FIN και δύο ACK από κάθε πλευρά. Ο λόγος που θεωρούμε ότι είναι ανεξάρτητος ό τρόπος τερματισμού για κάθε πλευρά είναι ότι ο τερματισμός μπορεί να γίνει μόνο από τη μία πλευρά έστω και αν η άλλη δεν έχει τερματίσει.

Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει πλέον δεδομένα, ενώ η άλλη μπορεί. Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο υπολογιστές να στείλουν ταυτόχρονα ένα πακέτο FIN ο ένας στον άλλο. Στη συνέχεια ο καθένας επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση.

2.2.4 Μεταφορά δεδομένων

Αφού γίνει η σύνδεση και σταλούν τα ISN προς τις δύο πλευρές μπορεί να ξεκινήσει η ανταλλαγή δεδομένων. Για τη μεταφορά των δεδομένων θα πρέπει να εξεταστεί ο έλεγχος ροής ή flow control και οι τεχνικές ελέγχου συμφόρησης (congestion avoidance). Αν δεν υπάρξουν αυτοί οι έλεγχοι τότε απλά αποστέλλονται τα πακέτα στον παραλήπτη και εφόσον δεν υπάρχει υπέρβαση τα δεδομένα λαμβάνονται. Όταν ο παραλήπτης δέχεται πακέτα TCP στέλνει επιβεβαιώσεις (acknowledgement), δείχνοντας σε ποιο σημείο του ρεύματος από byte (byte stream) βρίσκεται. Αυτές οι επιβεβαιώσεις περιέχουν επίσης το επόμενο window (παράθυρο) που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

Εάν δεν υπάρχουν δεδομένα για να σταλούν, ο αποστολέας θα βρίσκεται σε αδράνεια αναμένοντας την εφαρμογή να βάλει δεδομένα στο byte stream ή να παραλάβει δεδομένα από το άλλο άκρο της σύνδεσης.

2.2.5 Έλεγχος ροής

Όπως αναφέραμε ο παραλήπτης μετά τη λήψη των πακέτων αποστέλλει acknowledgement, το οποίο επιβεβαιώνεται από τον host. Αφού επιβεβαιωθεί αποστέλλεται το επόμενο πακέτο. Υπάρχει η δυνατότητα αποστολής πολλών πακέτων ταυτόχρονα και όχι μέσω της διαδικασίας αποστολής acknowledgement, μέσω αλγορίθμων που ελέγχουν τη ροή πακέτων. Αυτός ο τρόπος βοηθάει στο να χρησιμοποιείται αποδοτικότερα το bandwidth (εύρος ζώνης) ενός δικτύου.

2.2.6 Έλεγχος συμφόρησης

Στην περίπτωση συμφόρησης στο δίκτυο, το πρωτόκολλο TCP θα πρέπει να μπορεί να ανταπεξέλθει, καθώς δεν έχει νόημα να λειτουργεί αν δεν υπάρχει ροή δεδομένων. Έπρεπε να δημιουργηθεί ένας τρόπος να μπορεί το πρωτόκολλο να αντιμετωπίσει και να αναγνωρίζει τη συμφόρηση στο δίκτυο, μέσω αλγορίθμων. Χρησιμοποιούνται διάφοροι μηχανισμοί για να επιτευχθεί υψηλή απόδοση και να μην υπερφορτωθεί το δίκτυο. Αυτοί οι μηχανισμοί περιλαμβάνουν τον αλγόριθμο αργής εκκίνησης (slow-start), τον αλγόριθμο αποφυγής συμφόρησης (congestion avoidance), τον αλγόριθμο γρήγορης επαναμεταφοράς (fast retransmit) και τον αλγόριθμο γρήγορης ανάκαμψης (fast recovery) (Perrig & Tygar, 2003).

Αλγόριθμος αργής εκκίνησης (Slow-start)

Αυτή η μέθοδος είναι ένας τρόπος ώστε να αποφευχθεί η συμφόρηση. Αν εξαρχής αποστέλλονταν πολλά πακέτα τότε θα ήταν σχεδόν βέβαιο ότι θα υπήρχε συμφόρηση στο δίκτυο. Η αρχή λειτουργίας αυτής της μεθόδου είναι η παρακάτω. Αρχικά υπάρχει άλλο ένα παράθυρο, το οποίο δέχεται ένα πακέτο κάθε φορά που λαμβάνεται πίσω ένα ACK μετά την αποστολή πακέτου. Τότε το παράθυρο συμφόρησης διπλασιάζει την τιμή του με τη λήψη κάθε επιπλέον πακέτου. Με τη μέθοδο αυτή μπορούν να αποστέλλονται συνεχώς πακέτα με εκθετική ροή, και ο ρυθμός ροής τους καθορίζεται από τον αριθμό ACK που λαμβάνονται πίσω (Perrig & Tygar, 2003).

Αποφυγή συμφόρησης (Congestion Avoidance)

Η συνεχής εκθετική ροή που είδαμε στην προηγούμενη μέθοδο ωστόσο, είναι βέβαιο ότι κάποια στιγμή οδηγεί στην υπερβολική αύξηση των πακέτων και πιθανών στην απώλειά τους. Αυτό θα συμβεί λόγω της συμφόρησης στους ενδιάμεσους δρομολογητές. Γι' αυτό το λόγο θα πρέπει να υπάρχει ένας έλεγχος ροής των πακέτων από μια τιμή αύξησης και άνω. Το σημείο αυτό ονομάζεται όριο αργού ξεκινήματος (slow start threshold- ssthresh) και η υπέρβασή του σηματοδοτεί τη μετάβαση από την εκθετική αύξηση της ροής των δεδομένων στην προσθετική. Αναλυτικά ο αλγόριθμος λειτουργεί ως εξής: Αρχικά τίθεται το cwnd σε 1 και το ssthresh σε 65535 και εφαρμόζεται η αργή εκκίνηση (slow start), δηλαδή ο ρυθμός αύξησης των δεδομένων είναι εκθετικός - για κάθε επιβεβαίωση που λαμβάνεται, το cwnd αυξάνεται κατά 1. Όταν συμβεί συμφόρηση που επισημαίνεται με τη λήξη του χρονικού περιθωρίου -RTO, τότε το όριο αργού ξεκινήματος τίθεται ίσο με το μισό του τρέχοντος μεγέθους του παραθύρου (ssthresh = cwnd 12) και το cwnd ίσο με 1. Στη συνέχεια για κάθε λαμβανόμενη επιβεβαίωση το cwnd αυξάνεται εκθετικά (slow start) για όσο διάστημα είναι μικρότερο ή ίσο με το sshthresh Όταν το cwnd γίνει μεγαλύτερο του ssthresh, τότε εφαρμόζεται προσθετική αύξηση, δηλαδή το παράθυρο συμφόρησης αυξάνεται κατά 1/cwnd για κάθε ACK που λαμβάνεται. Με αυτόν τον τρόπο τελικά το cwnd αυξάνεται κατά 1 σε κάθε Round-trip time σε αντίθεση με την αργή εκκίνηση όπου αυξάνεται σύμφωνα με των αριθμό των ACKs που λαμβάνονται σε κάθε RTT (Perrig & Tygar, 2003).

Γρήγορη επαναμεταφορά (fast retransmit)

Τα πακέτα εκτός σειράς (packet reordering) προέρχονται είτε από διαφορετική διαδρομή είτε επειδή χάθηκε κάποιο ενδιάμεσο πακέτο. Σε αυτή την περίπτωση το TCP στέλνει διπλά ACK που ονομάζονται duplicate ACK ή αλλιώς DACKs. Με την λήψη

ενός ή δύο DACKs ο παραλήπτης λαμβάνει το σήμα ότι πακέτα ελήφθησαν με διαφορετική σειρά, ενώ με τη λήψη τριών DACKs είναι σήμα ότι χάθηκε πακέτο λόγω συμφόρησης. Το TCP εφαρμόζει αργό ξεκίνημα, αποφυγή συμφόρησης, γρήγορη επαναμεταφορά (με την παραλαβή 3 DACK) και αμέσως μετά αργό ξεκίνημα (slow-start).

Γρήγορη Ανάκαμψη (Fast Recovery)

Η λήψη ενδιάμεσων επιβεβαιώσεων (Duplicate ACKs) είναι μια ένδειξη περιορισμένης συμφόρησης στο δίκτυο, εφόσον πακέτα εξακολουθούν να διακινούνται. Επομένως κρίνεται υπερβολική μια τόσο μεγάλη μείωση της ροής των δεδομένων όπως συμβαίνει στο μηχανισμό fast start, όπου τίθεται το cwnd = 1. Αντιθέτως κρίνεται αρκετό να μειωθεί το παράθυρο συμφόρησης στο μισό της προηγούμενης τιμής και να συνεχίσουν να στέλνονται πακέτα όσο λαμβάνονται DACKs .

2.3 Συστήματα ασφαλείας ασυρμάτων δικτύων

Σε αυτό το υποκεφάλαιο συζητούνται τα τρέχοντα συστήματα ασφάλειας ασυρμάτων δικτύων και οι προκλήσεις ασφαλείας τους. Η ασφάλεια ασύρματου δικτύου είναι πολύ σημαντική, ειδικά για ορισμένους τύπους υλικού και δεδομένων.

2.3.1 Κλασσικά συστήματα ασφαλείας ασυρμάτων δικτύων

Τα κλασσικά συστήματα ασφαλείας ασυρμάτων δικτύων μπορούν να κατηγοριοποιηθούν σε δύο μέρη: έλεγχος ταυτότητας και κρυπτογράφηση. Η

κρυπτογράφηση ελέγχεται από το WEP και είναι υπεύθυνη για την κωδικοποίηση των δεδομένων, οπότε δεν μπορεί να αποκωδικοποιηθεί από κάποιον άλλον που δεν είναι εξουσιοδοτημένος. Ο έλεγχος ταυτότητας είναι μια διαδικασία που ασκείται μεταξύ του δέκτη και του πομπού, οπότε οι δύο γνωρίζουν ο ένας τον άλλον και δεν επιτρέπουν σε άλλους ανθρώπους ή μέρη να μπουν στο δίκτυο. Ο έλεγχος ταυτότητας γίνεται μέσω του ελέγχου πρόσβασης, MAC layer (Proxim Wireless, 2003).

Έλεγχος ταυτότητας

Τα περισσότερα σημεία πρόσβασης παρέχουν τη δυνατότητα επαλήθευσης ταυτότητας. Τα επίπεδα MAC επαληθεύουν τη σύνδεση, επιτρέποντας έτσι τη σύνδεση μόνο σε καταχωρημένες διευθύνσεις MAC σε ένα δίκτυο. Ο έλεγχος ταυτότητας είναι μια διαδικασία που γίνεται με τον έλεγχο της διεύθυνσης MAC layer κατά την απόπειρα σύνδεσης. Αυτός ο μηχανισμός είναι ευάλωτος για δύο λόγους. Κατ 'αρχάς, οι διευθύνσεις MAC μπορούν να αλλάξουν, έτσι ώστε ένα επίπεδο MAC του πιστοποιημένου χρήστη να μπορεί να αντιγραφεί και να χρησιμοποιηθεί για την παροχή πρόσβασης. Δεύτερον, υπάρχει κίνδυνος να κλαπεί το λογισμικό και να δοθεί μη εγκεκριμένη πρόσβαση σε ένα δίκτυο. Σε ορισμένες περιπτώσεις, ο έλεγχος ταυτότητας μπορεί να είναι ένας τρόπος με τον οποίο το σημείο πρόσβασης μπορεί να επαληθεύσει έναν χρήστη, αλλά ένας χρήστης δεν επαληθεύει ένα σημείο πρόσβασης. Αυτό το είδος ελέγχου ταυτότητας είναι επικίνδυνο επειδή ένας χρήστης μπορεί να έχει πρόσβαση σε πληροφορίες σχετικά με άλλους χρήστες στο δίκτυο.

Κρυπτογράφηση

Στην ασύρματη επικοινωνία, μια μέθοδος κρυπτογράφησης είναι το WEP. Σήμερα, τα δίκτυα κρυπτογράφησης WEP δεν θεωρούνται ασφαλή δίκτυα, αλλά η τεχνολογία αυτή εξακολουθεί να είναι η πιο συνηθισμένη στην κρυπτογράφηση. Το σύστημα κρυπτογράφησης δεύτερης γενιάς ονομάζεται Virtual Private Networking, VPN.

Η κρυπτογράφηση WEP αποδεικνύεται ότι έχει κάποιες αδυναμίες. Ορισμένες περιπτώσεις δείχνουν ότι η κρυπτογράφηση WEP μπορεί να αποκωδικοποιηθεί εξαιτίας ενός ασθενούς φορέα εκκίνησης. Δεδομένου ότι οι χρήστες γνωρίζουν ότι το WEP δεν είναι ασφαλές, έχουν προσπαθήσει να επιλύσουν το πρόβλημα με βελτιωμένη κρυπτογράφηση WEP σε προϊόντα 802.11B. Μια εναλλακτική λύση στην κρυπτογράφηση WEP, είναι οι άνθρωποι να χρησιμοποιούν το λογισμικό VPN για την κρυπτογράφηση των δεδομένων τους, επειδή πιστεύεται ότι είναι πολύ πιο ασφαλές από την κρυπτογράφηση WEP. Το VPN προσφέρει πολύ καλύτερη κρυπτογράφηση, που είναι πιο δύσκολο να αποκωδικοποιηθεί από εισβολείς(Walker, 2000).

Σήμερα, υπάρχουν άλλες μέθοδοι κρυπτογράφησης που χρησιμοποιούνται στις εταιρίες και σε άλλους οργανισμούς για λόγους πιο ασφαλούς μετάδοσης δεδομένων. Επίσης, ακόμα και οι υπάρχουσες τεχνολογίες έχουν βελτιωθεί αρκετά μειώνοντας την πιθανότητας εισβολής σε ένα ασύρματο δίκτυο.

2.4 Ζητήματα ασφαλείας

Στη συμβατική επικοινωνία δεδομένων, τα δεδομένα μεταδίδονται μέσω καλωδίου. Ωστόσο, είναι πολύ προτιμότερο να δημιουργηθεί ένα σημείο πρόσβασης και να λειτουργήσει το δίκτυο χωρίς την ταλαιπωρία της καλωδίωσης. Με το ασύρματο δίκτυο, ένας χρήστης μπορεί να συνδεθεί στο δίκτυο και να εξακολουθήσει να χρησιμοποιεί το δίκτυο κάτω από την κάλυψη του σημείου πρόσβασης. Παρά αυτά

τα πλεονεκτήματα, η ασύρματη επικοινωνία έχει και αυξημένα προβλήματα ασφαλείας (Rysavy Research, 2007).

Μια ιδιότητα των ραδιοκυμάτων είναι η δυνατότητα διείσδυσης σε μεγάλες αποστάσεις. Είναι πολύ δύσκολο να προσδιοριστεί πόσο διαπερνούν και σε ποια κατεύθυνση. Πιθανοί χάκερ μπορούν να είναι μακριά με τους δέκτες τους και εξακολουθούν να καταγράφουν δεδομένα με τους πομπούς τους, για να αναλύσουν τον κώδικα ή να τα συλλέξουν δεδομένα και να τα αναλύσουν αργότερα. Μέσω αυτής της μεθόδου, οι χάκερ μπορούν να συγκεντρώσουν όλες τις πληροφορίες από τον στοχευμένο υπολογιστή όπως κωδικούς πρόσβασης, ηλεκτρονικά μηνύματα και ακόμη πιο προσωπικές πληροφορίες, όπως τραπεζικές πληροφορίες. Ένα πρόβλημα ασφαλείας είναι ότι οποιοσδήποτε υπολογιστής με τον ίδιο εξοπλισμό μπορεί να έχει πρόσβαση σε ένα μη ασφαλές ασύρματο δίκτυο. Χρησιμοποιώντας πιο ισχυρούς δέκτες ως εργαλείο ενίσχυσης, ένας υπολογιστής μπορεί να εντοπίσει διάφορα σήματα και να προσπαθήσει να μπει στο δίκτυο, ακόμα δηλαδή και αν το σήμα είναι πολύ αδύναμο για τον αρχικό εξοπλισμό (Rysavy Research, 2007).

2.4.1 Εύκολη πρόσβαση

Τα σημεία ασύρματης πρόσβασης πρέπει να είναι προσβάσιμα σε οποιονδήποτε χρήστη στο δίκτυο. Πριν ο χρήστης συνδεθεί στο δίκτυο, ο χρήστης πρέπει να μπορεί να δει το δίκτυο. Όταν ένας χρήστης επιχειρεί να συνδεθεί σε ένα δίκτυο, το σήμα χρήστη δεν είναι κρυπτογραφημένο. Επειδή δεν υπάρχει κρυπτογράφηση, κάποιος άλλος θα μπορούσε να ανιχνεύσει αυτό το σήμα χρήστη και να το χρησιμοποιήσει για πρόσβαση στο δίκτυο. Η προστασία του σήματος είναι μια λύση, αλλά δεν είναι πολύ πρακτική. Ένα δίκτυο πρέπει να έχει ισχυρό έλεγχο ταυτότητας και σύστημα ελέγχου

κρυπτογράφησης. Επίσης, θα πρέπει να χρησιμοποιείται VPN ως μέθοδος επαλήθευσης ταυτότητας(Proxim Wireless, 2003).

2.4.2 Πολλά σημεία πρόσβασης

Σε έναν μεγάλο αριθμό δικτύων, θα ήταν δύσκολο να παρακολουθήσει κάποιος την πρόσβαση όλων των χρηστών. Μια σχετική πρόκληση είναι η εκπαίδευση των χρηστών σχετικά με την ασφάλεια των δικτύων. Δυστυχώς, λόγω κυρίως αμέλειας των περισσότερων χρηστών, η πρόσβαση σε ένα οικιακό δίκτυο είναι εύκολη υπόθεση. Δεν υπάρχει εύκολη λύση για αυτό το είδος προβλήματος που σχετίζεται με χρήστες που κάνουν μη καλά ασφαλισμένα σημεία πρόσβασης. Για παράδειγμα, ένας διαχειριστής μπορεί να μεταβεί στα δωμάτια ενός κτιρίου για να βρει σημεία ασύρματης πρόσβασης. Ενδέχεται να εντοπιστούν κοντινά ασύρματα δίκτυα από άλλα σπίτια ή γραφεία και αυτό καθιστά δύσκολο να κατανοηθεί σε ποιο σημείο πρόσβασης είναι συνδεδεμένος κάποιος, και αν είναι νόμιμα συνδεδεμένος στο δίκτυο που κατέχει. Οι περιοδικοί έλεγχοι αποτελούν λύση για το πρόβλημα του μη ελεγχόμενου σημείου πρόσβασης, αλλά αυτό εξαρτάται από τους διαχειριστές δικτύων που ενδέχεται να μην έχουν χρόνο ή διάθεση να κάνουν τους ελέγχους.

2.4.3 Μη εξουσιοδοτημένη χρήση υπηρεσίας

Όταν οι άνθρωποι αγοράζουν ασύρματες συσκευές για να έχουν πρόσβαση στο διαδίκτυο στα σπίτια τους, η εγκατάσταση περιλαμβάνει προεπιλεγμένες ρυθμίσεις στη συσκευή. Οι ασύρματες συσκευές κατασκευάζονται έτσι ώστε να δίνουν κάποια ευκολία. Στην πιο απλή περίπτωση παραβίασης, η ασύρματη συσκευή δεν έχει

περιορισμούς ασφαλείας και είναι κοινό ότι πολλοί χρήστες δεν δημιουργούν κλειδί για ένα ασφαλές ασύρματο δίκτυο, επειδή απαιτεί χρόνο(Walker, 2000). Αυτό είναι ένα λάθος που προκαλεί δύο βασικά προβλήματα: προβλήματα πρόσβασης χωρίς έλεγχο ταυτότητας και προβλήματα εύρους ζώνης. Οι μη εξουσιοδοτημένες συνδέσεις μπορούν να χρησιμοποιούν τεράστιες ποσότητες δεδομένων, αν και υπάρχει ένα περιορισμένο συνολικό διαθέσιμο εύρος ζώνης. Η συνδυασμένη χρήση δεδομένων καθιστά τη χρήση του διαδικτύου αργή ή και άχρηστη για ορισμένες εφαρμογές που χρειάζονται μεγάλο εύρος ζώνης. Ειδικά σε περιοχές με πυκνό πληθυσμό , ενδέχεται να υπάρχουν πολλές μη εξουσιοδοτημένες συνδέσεις με πρόσβαση σε κάθε ασύρματο δίκτυο. Ωστόσο, οι πολλοί χρήστες ενδέχεται να μην αποτελούν πρόβλημα σε ορισμένες περιπτώσεις, όπου το ασύρματο δίκτυο εξυπηρετεί ακριβώς μεγάλο και ανώνυμο πλήθος χρηστών, που μεταβάλλεται κατά τη διάρκεια μίας εργάσιμης μέρας. Για παράδειγμα, ένας χώρος όπως μια δημόσια βιβλιοθήκη μπορεί να προσφέρει ασύρματη πρόσβαση στο Internet χωρίς να χρειάζεται να παρέχει κωδικούς πρόσβασης στους χρήστες. Αυτό είναι μια ευκολία για τη βιβλιοθήκη, επειδή έχει ακόμα στον έλεγχο του δικτύου. Επίσης, αυτός ο τύπος υπηρεσίας δεν θα προκαλούσε βλάβη στον πάροχο, όπως μια βιβλιοθήκη, όταν πολύτιμα δεδομένα δεν αποθηκεύονται στο ίδιο το δίκτυο. Αυτές είναι οι λεγόμενες περιπτώσεις εμπορικών τοπολογιών (Proxim Wireless, 2003), (Chrysikos, 2012). Στα ασύρματα δίκτυα, η κατοχύρωση της ασφάλειας σε υψηλά επίπεδα του OSI (άνω του επιπέδου 3) δεν είναι υποχρεωτική ή νομοτελειακή. Υπάρχουν ορισμένοι πάροχοι ασύρματου Internet που έχουν μη ασφαλείς ρυθμίσεις πρόσβασης στο Internet, πράγμα που σημαίνει ότι οι χρήστες δεν χρειάζονται καν κωδικό πρόσβασης και μπορούν να έχουν πρόσβαση στο δίκτυο με βασικά βήματα. Σε πολλούς δημόσιους χώρους, οι χρήστες έχουν πρόσβαση και χρησιμοποιούν το διαδίκτυο με δική τους ευθύνη. Ωστόσο, για τις επιχειρήσεις ή για κρατικούς οργανισμούς, τα ασύρματα δίκτυα πρέπει να εξασφαλίζονται με λύσεις ασφάλειας υψηλότερου επιπέδου,

συνήθως διαφορετικές από τους δημόσιους χώρους. Πολύτιμες ή ιδιωτικές πληροφορίες αποτελούν μέρος της κυκλοφορίας δεδομένων, επομένως οι εταιρείες και οι κρατικοί οργανισμοί θα πρέπει να έχουν διαφορετική ασφάλεια. Μεταξύ της σημερινής τεχνολογίας, το VPN διαθέτει μία από τις ισχυρότερες δυνατότητες πιστοποίησης. Το VPN παρέχει στον διαχειριστή του δικτύου μια επιλογή μεθόδων ελέγχου ταυτότητας, ανάλογα με τις δυνατότητες ασφάλειας του layer transport, TLS. Οι χρήστες μπορούν να συνδεθούν μόνο σε εξουσιοδοτημένα σημεία πρόσβασης(Proxim Wireless, 2003).

2.4.4 Περιορισμοί υπηρεσιών και επιδόσεων

Οι ασύρματες συνδέσεις έχουν χαμηλότερη χωρητικότητα από τις ενσύρματες συνδέσεις για μεταφορά δεδομένων. Για παράδειγμα, το 802.11B έχει χωρητικότητα 11 Mbps και τα νεότερα μοντέλα ασύρματων έχουν 54 Mbps. Η χωρητικότητα μοιράζεται μεταξύ όλων των χρηστών που είναι συνδεδεμένοι σε ένα ασύρματο δίκτυο. Λόγω της μικρότερης ταχύτητας ασύρματης σύνδεσης, οι συνδέσεις του δρομολογητή μπορούν να υπερφορτωθούν. Αξίζει πάντως να σημειωθεί πως η τάση στα ασύρματα δίκτυα είναι να προσεγγίσουν και εν τέλει να φτάσουν την ευρυζωνικότητα που παρέχουν τα ενσύρματα μέσα. Για παράδειγμα, το 802.11n μπορεί, υπό προϋποθέσεις, να παρέχει ευρυζωνικότητα της τάξης ενός VDSL (~50 Mbps), ενώ το υπό σχεδίαση 5G αναμένεται να πλησιάσει ρυθμούς της τάξης του 1 Gbps για κάλυψη ασύρματης σύνδεσης σε εσωτερικούς χώρους πολλών χρηστών (Chrysikos, 2018).

2.4.5 MAC Spoofing και Hacking

Η μετάδοση δεδομένων γίνεται με πλαίσια ή πακέτα δεδομένων. Κάθε πλαίσιο δεδομένων έχει μια κεφαλίδα και στην κεφαλίδα υπάρχει ένα μέρος της διεύθυνσης πηγής. Ένα πλαίσιο αποστέλλεται από την πηγή με τη διεύθυνση της πηγής στην κεφαλίδα (header). Δεν υπάρχει έλεγχος ταυτότητας για τα πλαίσια. Θα μπορούσε να υπάρχει ένας εισβολέας που μπορεί να στείλει το ίδιο πλαίσιο με τη σωστή διεύθυνση πηγής. Δεν υπάρχει ουσιαστική προστασία κατά της πλαστογράφησης.

Υπάρχουν όμως και ασύρματες συνδέσεις που υποστηρίζουν δύο τρόπους επίλυσης αυτού του προβλήματος. Ένας τρόπος είναι ένα ασύρματο σημείο πρόσβασης που απαιτεί την ταυτότητά του κατόχου πριν κληθεί να γίνει ο πρώτος έλεγχος ταυτότητας για σύνδεση. Το πρόβλημα δεν θα επιλυθεί μέχρι τα σημεία πρόσβασης να πιστοποιήσουν κάθε πλαίσιο. Κάποιες κρυπτογραφήσεις αποτελούν επίσης μια καλή άμυνα ενάντια σε αυτό το είδος επίθεσης (Walker, 2000).

2.4.6 Πιθανότητα υποκλοπής

Τα ασύρματα δίκτυα σήμερα δεν παρέχουν σχεδόν καμία προστασία από υποκλοπές. Οι κεφαλίδες πλαισίων είναι πάντα μη κρυπτογραφημένες, καθιστώντας εύκολο για έναν εισβολέα να αποθηκεύσει όλη την κίνηση μεταξύ ενός χρήστη και ενός σημείου πρόσβασης και να αναλύσει αργότερα τα δεδομένα.

Η κρυπτογράφηση δεδομένων υποτίθεται ότι είναι ο καλύτερος τρόπος για την προστασία των δεδομένων από αυτόν τον τύπο επίθεσης. Η κρυπτογράφηση WEP ήταν ευάλωτη επειδή προστατεύει μόνο το αρχικό σημείο ελέγχου μεταξύ του σημείου πρόσβασης και του χρήστη.

Τα τελευταία προϊόντα κρυπτογράφησης έχουν πολύ πιο πολύπλοκα συστήματα, και λειτουργούν αλλάζοντας το κλειδί ανά διαστήματα λεπτών. Για τον εισβολέα είναι πολύ δύσκολο να βρεθεί το σωστό κλειδί αλλά όχι αδύνατο.

Ακόμα νεότερα προϊόντα ασφάλειας ασύρματης επικοινωνίας υποτίθεται ότι προστατεύουν από τις εν λόγω ευπάθειες (Walker, 2000).

2.4.7 Επιθέσεις υψηλότερου επιπέδου

Στα συστήματα δικτύου υπάρχουν διάφοροι τρόποι επίθεσης, εάν η σύνδεση έχει ήδη καθοριστεί. Τα περισσότερα προϊόντα ασφαλείας σχεδιάζονται έτσι ώστε να μην υπάρχουν μη εξουσιοδοτημένες συνδέσεις.

Όλα τα δίκτυα μπορεί να είναι ευάλωτα εάν ένα μικρό μέρος του δικτύου είναι ευάλωτο. Αυτός είναι ο λόγος για τον οποίο τα δίκτυα πριν το υψηλότερο επίπεδο ασφάλειας, υποτίθεται ότι πρέπει να έχουν επίπεδα ασφαλείας στα χαμηλότερα επίπεδα. Μόλις αποκτηθεί η πρόσβαση, ανάλογα με την τοπολογία του δικτύου, θα μπορούσε να χρησιμοποιηθεί για να επιτεθεί ο εισβολέας σε άλλα δίκτυα. Συνεπώς, η ασφάλεια των δικτύων θα έπρεπε να προσανατολίζεται στην κάλυψη σε βασικό επίπεδο όλων των σημείων πρόσβασης (O'Neil Product Development Inc., 2009).

2.4.8 Απαιτήσεις ασφαλείας

Πρέπει, όπως ήδη αναφέρθηκε, να αναπτυχθούν ιδιαίτερες ρυθμίσεις ασφαλείας για τη διαχείριση των ασύρματων δικτύων. Αρχικά πρέπει να δημιουργηθεί κρυπτογράφηση για να αυξηθεί η ασφάλεια από απλές επιθέσεις. Οι παράνομες

συνδέσεις σημείου πρόσβασης θα πρέπει να εντοπίζονται, και θα πρέπει να υπάρχει και επαρκής ασφάλεια φυσικού επιπέδου.

Οι οργανισμοί και οι επιχειρήσεις διαθέτουν επιλογές λύσεων ασφάλειας, όπως ο περιορισμός της πρόσβασης των χρηστών και ο περιορισμός των ασύρματων δικτύων. Οι υπεύθυνοι ασφάλειας χρησιμοποιούν επίσης τυποποιημένα ρυθμιστικά συστήματα και κανόνες από κυβερνητικούς και ιδιωτικούς οργανισμούς, που έχουν δημοσιευτεί ως οδηγοί.

Μια συνήθης απαίτηση για την ασφάλεια ενός δικτύου είναι ότι τα δεδομένα δεν πρέπει να αποθηκεύονται ή να μεταδίδονται μέσω δημόσιων δικτύων. Τα δεδομένα θα πρέπει να κρυπτογραφούνται χρησιμοποιώντας πιστοποιημένους αλγόριθμους κρυπτογράφησης. Αυτοί οι πιστοποιημένοι αλγόριθμοι θα πρέπει να ενημερώνονται τακτικά για ασφαλείς επικοινωνίες, ώστε να παράγονται καλύτεροι και βελτιωμένοι αλγόριθμοι.

Ένας άλλος τρόπος για να εξασφαλιστούν οι συνδέσεις σε ένα δίκτυο είναι ο έλεγχος ταυτότητας, που έχει δύο επίπεδα. Μια απαίτηση θα ήταν ένα αντικείμενο ασφαλείας, όπως μια κάρτα ή ένα flash drive, το οποίο θα μεταφέρεται σε φυσική μορφή από έναν χρήστη που θα θέλει να συνδεθεί στο δίκτυο, αλλά κάτι τέτοιο θα μείωνε την ταχύτητα της συνολικής εμπειρίας που προσφέρει ένα ασύρματο δίκτυο. Ένα δεύτερο επίπεδο στον έλεγχο ταυτότητας θα μπορούσε να είναι ένας κωδικός πρόσβασης που πρέπει να παρέχει ο χρήστης για κάθε νέα σύνδεση ή βιομετρικά στοιχεία, όπως τα δακτυλικά αποτυπώματα.

Οι λύσεις ασφάλειας δικτύων είναι ευάλωτες έναντι των νέων τακτικών των επιτιθέμενων και οι κανονισμοί τείνουν να γίνονται αυστηρότεροι. Οι εταιρείες προσπαθούν να έχουν διαφορετικές, ισχυρότερες λύσεις ασύρματης ασφάλειας.

Ακόμη και όταν εφαρμόζονται διαφορετικοί μηχανισμοί ασύρματης ασφάλειας, οι περισσότεροι από αυτούς αποδεικνύονται ότι έχουν τρωτά σημεία. Αυτοί οι

μηχανισμοί ασφαλείας είναι η ταυτοποίηση των χρηστών, οι κρυπτογραφήσεις και τα τείχη προστασίας.

Και πάλι, ως γενικός ορισμός, ο έλεγχος ταυτότητας αποτελεί απαίτηση του δικτύου να επιβεβαιώσει νόμιμες συσκευές που έχουν πρόσβαση στο δίκτυο. Απαιτούνται πολιτικές ελέγχου ταυτότητας και συγχρονισμός με τις άλλες πολιτικές ή και συσκευές.

Όλα τα συστήματα ασφάλειας σχετίζονται με τις διαδικασίες διαχείρισης κινδύνου ενός οργανισμού. Με τη χρήση ισχυρότερων αλγορίθμων και νέων συστημάτων ασφαλείας, ο κίνδυνος μειώνεται κατά ένα μέρος, ή στο να επιτεθεί κάποιος στο δίκτυο ή στο να προσπεράσει τις ασφάλειες του δικτύου ο επιτιθέμενος.

Οι εταιρείες πρέπει να λαμβάνουν υπόψη όλα τα γεγονότα κινδύνου ή όταν συνδέουν δίκτυα με ασύρματα σημεία πρόσβασης ή άλλα δίκτυα.

Όπως αναφέρθηκε προηγουμένως, ο έλεγχος ταυτότητας δεν πρέπει να γίνεται μέσω κάποιας ταυτοποίησης της συσκευής ενός χρήστη. Θα πρέπει γίνεται άμεσα μεταξύ του χρήστη και του δικτύου. Τα διαπιστευτήρια ταυτότητας μπορούν να κλαπούν ή να αφαιρεθούν εύκολα από μια συσκευή η να βρεθεί ο τρόπος να αναπαραχθούν.

2.4.9 Επίπεδα ασφαλείας

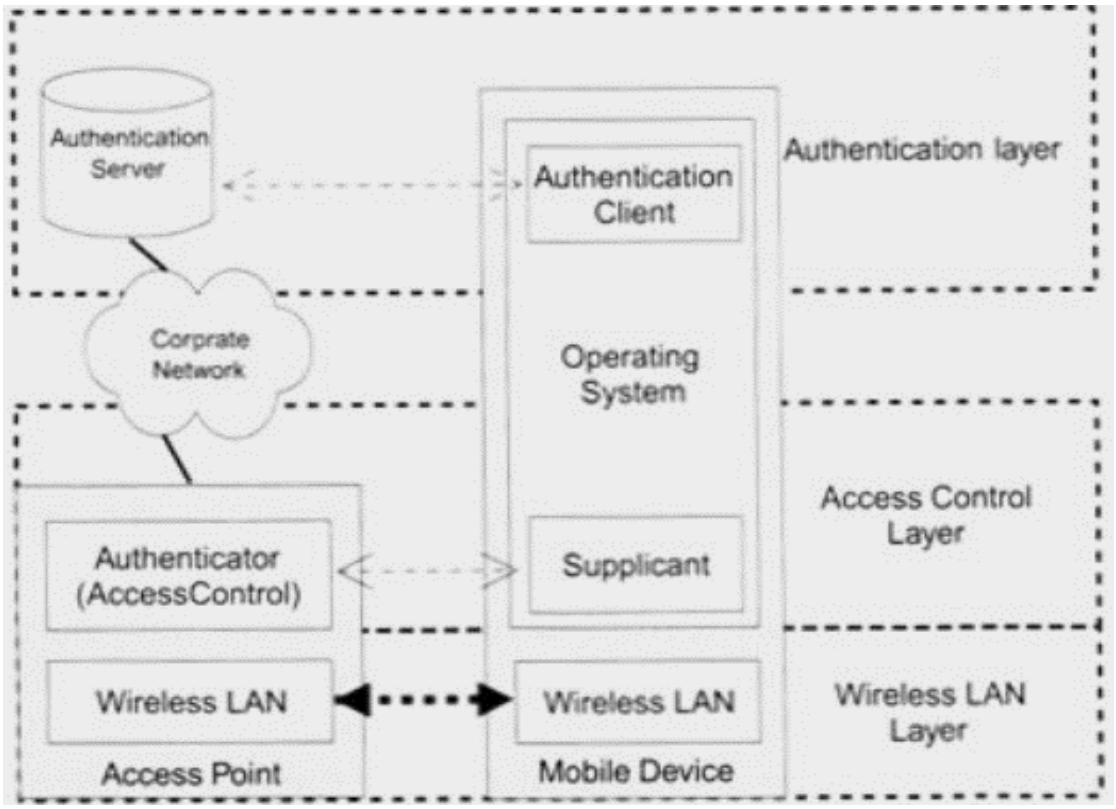
Τα δίκτυα έχουν επίπεδα ασφαλείας. Τα επίπεδα βοηθούν τους προγραμματιστές να εφαρμόζουν νέα συστήματα ασφαλείας που ταιριάζουν σε τρέχοντα και μελλοντικά συστήματα. Τα επίπεδα απαιτούνται για να καθοριστούν οι διαδικασίες στα δίκτυα διακριτές και διαχειρίσιμες. Τα ασύρματα δίκτυα έχουν επίσης τρία επίπεδα ασφαλείας που είναι αντίστοιχα με τα παραδοσιακά δίκτυα. Αυτά τα επίπεδα

ασφαλείας είναι το επίπεδο ασύρματου LAN, το επίπεδο ελέγχου πρόσβασης και το επίπεδο ελέγχου ταυτότητας.

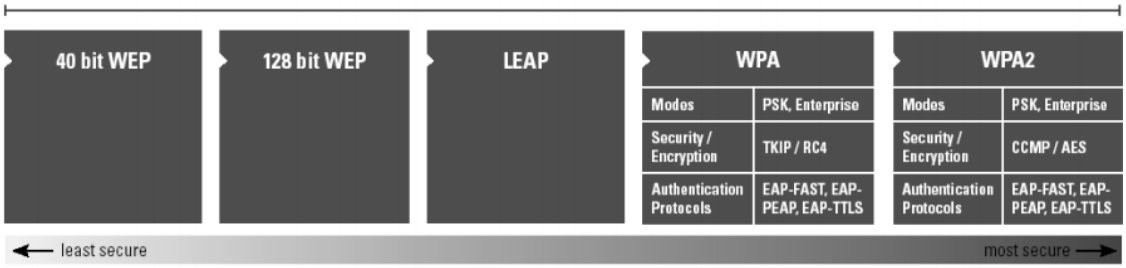
Το επίπεδο ασύρματου LAN είναι το χαμηλότερο επίπεδο που ασχολείται με δεδομένα. Αυτό το στρώμα στέλνει τα πακέτα δεδομένων και ελέγχει τις προσπάθειες πρόσβασης στο δίκτυο. Αυτό το επίπεδο είναι επίσης υπεύθυνο για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων μετά την εγκατάσταση της σύνδεσης.

Το επίπεδο ελέγχου πρόσβασης είναι υπεύθυνο για το περιεχόμενο κατά την κυκλοφορία δεδομένων. Αυτό το επίπεδο διασφαλίζει ότι όλα τα δεδομένα προέρχονται από τις επικυρωμένες συσκευές. Σε αυτό το επίπεδο λαμβάνονται νέες πληροφορίες σύνδεσης προς επαλήθευση πριν επιτραπεί η μετάβαση των δεδομένων μεταξύ των δύο συσκευών.

Το επίπεδο ελέγχου ταυτότητας επαληθεύει τις συνδέσεις. Επιβεβαιώνει την ταυτότητα των προσπαθειών σύνδεσης. Το επίπεδο ελέγχου ταυτότητας διατηρεί βάση δεδομένων για να προσδιορίσει τους χρήστες. Σε ένα μικρό δίκτυο, το επίπεδο ελέγχου ταυτότητας μπορεί να βρίσκεται στο σημείο πρόσβασης. Σε ασύρματα δίκτυα μεγάλης κλίμακας, τα δεδομένα αυτά αποθηκεύονται στον διακομιστή για να υπάρχει ένα πιο διαχειρίσιμο και αναβαθμίσιμο σύστημα ασφαλείας.



Σχήμα 2.1 Τα επίπεδα ασφαλείας ασύρματων δικτύων σχηματοποιημένα (Duruturk, 2010)



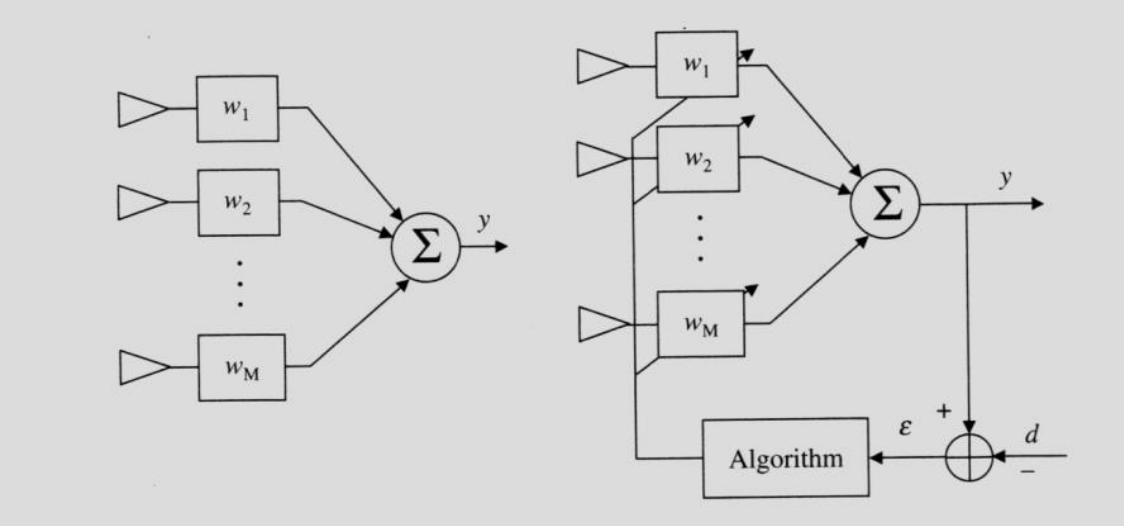
Σχήμα 2.2 Τα βασικά είδη ελέγχου εισόδου χρήστη, κρυπτογράφησης και γενικότερης ασφάλειας στα ασύρματα δίκτυα (Duruturk, 2010)

2.5 Κεραίες και ασφάλεια

Στις παραδοσιακές κεραίες συστοιχίας, οι μετατοπιστές φάσης κατευθύνουν τις ακτίνες προς την κατεύθυνση που θέλουμε. Οι φάσεις των σημάτων μεταβάλλονται απευθείας σε κάθε κεραία. Αυτό ονομάζεται ηλεκτρονική μετατόπιση φάσης, επειδή οι φάσεις μετατοπίζονται άμεσα στο ρεύμα του σήματος.

Τα σύγχρονα συστήματα διεύθυνσης δέσμης κατασκευάζονται με έξυπνες κεραίες, επειδή οι έξυπνες κεραίες είναι σε θέση να κατευθύνουν τη δέσμη με ορισμένα κριτήρια και με συγκεκριμένο τρόπο. Στις έξυπνες κεραίες έχει γίνει ήδη αναφορά στο πρώτο κεφάλαιο Ο τεχνολογικός αυτός εξοπλισμός ονομάζεται σχηματισμός ψηφιακής δέσμης ή έξυπνες συστοιχίες κεραίας. Ο όρος «έξυπνος» χρησιμοποιείται συνήθως για υπολογιστικά συστήματα. Στις έξυπνες κεραίες η δέσμη κατευθύνεται χρησιμοποιώντας προηγμένες τεχνικές επεξεργασίας ψηφιακού σήματος. Οι έξυπνες κεραίες είναι ανώτερες σε πολλούς τομείς έναντι των παραδοσιακών κεραιών. Επίσης, χρησιμοποιούνται σε συστήματα ραντάρ, κινητές ασύρματες συσκευές και ασύρματες επικοινωνίες πολλαπλής πρόσβασης.

Υπάρχουν αλγόριθμοι που ελέγχουν τις έξυπνες κεραίες ώστε να ανταποκρίνονται σε συγκεκριμένα κριτήρια. Αυτοί οι αλγόριθμοι ελέγχονται από αναλογικά κυκλώματα. Έχουν σχεδιαστεί για να μεγιστοποιούν την αναλογία σήματος - θορύβου και να ελαχιστοποιούν την πιθανότητα ρυθμού σφάλματος σήματος - σφάλματος. Οι αλγόριθμοι αυτοί, σχεδιάζονται επίσης ώστε να αναγνωρίζουν τα παρεμβαλλόμενα σήματα. Στις έξυπνες κεραίες απαιτείται η εφαρμογή αυτών των αλγορίθμων για να μετατραπεί ένα αναλογικό σήμα σε ψηφιακό σήμα, χρησιμοποιώντας μετατροπέα αναλογικού προς ψηφιακό. Δεδομένου ότι η κύρια διαδικασία γίνεται ψηφιακά, ονομάζεται επίσης ψηφιακή μορφοποίηση δέσμης. Το παρακάτω σχήμα δείχνει το ηλεκτρονικά παραγόμενο ψηφιακό σύστημα διεύθυνσης δέσμης.



Σχήμα 2.3 Ο τρόπος λειτουργίας μιας παραδοσιακής κεραίας αριστερά σε σχέση με μια έξυπνη κεραία στα δεξιά

Εκτός από τους αλγορίθμους σχηματισμού ψηφιακής δέσμης, υπάρχουν αλγόριθμοι που μπορούν επίσης να σχεδιαστούν έτσι ώστε να έχουν προσαρμοστικές ικανότητες σχηματισμού δέσμης. Ένα βασικό πλεονέκτημα της ψηφιακής διαμόρφωσης δέσμης είναι ότι εκτελείται από λογισμικό που μπορεί να βελτιωθεί και να τροποποιηθεί. Με πολύ παρόμοιο τρόπο στην πλευρά του δέκτη, η διαμόρφωση της δέσμης πραγματοποιείται ψηφιακά από τους αλγόριθμους.

Σε ένα απρόβλεπτο ηλεκτρομαγνητικό περιβάλλον, η προσαρμοστική διαμόρφωση δέσμης είναι η κυρίαρχη επιλογή για καλύτερη απόδοση από μια έξυπνη κεραία. Ο προσαρμοστής αλγορίθμων βελτιώνει την ποιότητα του σήματος.

Η μεγαλύτερη διαφορά μεταξύ των συμβατικών συστοιχιών και των προσαρμοστικών συστοιχιών είναι η δυνατότητα να ξεπερνούν προβλήματα στα δύσκολα

περιβάλλοντα όπως τα παρεμβαλλόμενα ηλεκτρομαγνητικά σήματα, οι επαναλαμβανόμενες επιστροφές ή οι παρεμβολές πολλαπλών διαδρομών.

2.6 Πολυπλεξία OFDM

Οι ψηφιακές εφαρμογές πολυμέσων με την ευρεία ανάπτυξή τους τα τελευταία χρόνια προκαλούν ακόμα μεγαλύτερες απαιτήσεις για τηλεπικοινωνιακά συστήματα ευρείας ζώνης. Οι απαιτήσεις σε τεχνικό εξοπλισμό για τις παραπάνω είναι πολύ υψηλές, ωστόσο το κόστος πρέπει να διατηρηθεί σε χαμηλά επίπεδα ώστε να είναι προσιτές στο ευρύ κοινό. Η απαίτηση για φθηνές λύσεις και συγχρόνως χρησιμοποίηση δικτύων ευρείας ζώνης οδηγεί στην πολυπλεξία, κατά την οποία όμως δεν επιλύονται κρίσιμα προβλήματα που παραμένουν προς αντιμετώπιση όπως η διασυμβολική παρεμβολή (ISI) ενώ παραμένουν υψηλές οι απαιτήσεις για την ποιότητα παρεχόμενων υπηρεσιών. Έπειτα από διάφορες τεχνικές μετάδοσης, από διαίρεση χώρου μέχρι και κώδικα, που έχουν προταθεί και χρησιμοποιηθεί στο παρελθόν, το OFDM φαίνεται να επικρατεί στα ασύρματα δίκτυα (HIPERLAN/2, IEEE 802.11a/g, MMAC) καθώς και στην εκπομπή ψηφιακού ήχου και εικόνας (DAB, DVB).

Η ιστορία έχει δείξει ότι κάθε δεκαετία υπάρχει μια τεράστια αλλαγή στον τρόπο υλοποίησης των κινητών τηλεπικοινωνιακών συστημάτων. Τα συστήματα πρώτης γενιάς (1G) που εμφανίστηκαν τη δεκαετία του 1980 ήταν βασισμένα σε αναλογική τεχνολογία, ενώ αυτά της δεύτερης γενιάς (2G) που εφαρμόζονταν από το 1990 σχεδόν, χρησιμοποιούσαν ψηφιακές τεχνολογίες. Χαρακτηριστικά παραδείγματα συστημάτων δεύτερης γενιάς είναι το ευρέως διαδεδομένο GSM αλλά και τα προσωπικά κυψελωτά δίκτυα (PCS, DCS-1800).

Ο στόχος για τα συστήματα τρίτης γενιάς (3G) ήταν η δυνατότητα μετάδοσης δεδομένων, ήχου και εικόνας σε εξωτερικά και εσωτερικά περιβάλλοντα με σχετικά υψηλές ταχύτητες. Με κεντρικό φορέα συχνότητας στα 2.1 GHz και χρησιμοποιώντας συστήματα πολλαπλής προσπέλασης διαίρεσης κώδικα (CDM/CDMA) επιτεύχθηκε τελικά η μετάδοση πληροφορίας με ταχύτητες πολύ υψηλές, όπως 144 Kbps για κινούμενους χρήστες, 384Kbps για εξωτερικό περιβάλλον και μέχρι τα 2Mbps για εσωτερικούς χώρους. Έτσι το πρότυπο 3G εισήγαγε την ευρυζωνικότητα στα δίκτυα κινητής τηλεφωνίας. Με το 3G, που υλοποιήθηκε στα πλαίσια του IMT-2000, δόθηκε η δυνατότητα να επιτευχθούν πολύ υψηλοί ρυθμοί δεδομένων και μεγάλες ταχύτητες στην κάτω ζεύξη. Το επόμενο βήμα στην εξέλιξη της τεχνολογίας ήταν η χρησιμοποίηση του OFDM. Οι εφαρμογές του περιλαμβάνουν τοπικά ασύρματα δίκτυα υψηλών ταχυτήτων, όπως IEEE802.11a, υψηλής ποιότητας τοπικά δίκτυα, όπως HIPERLAN/2, και κινητά τηλεπικοινωνιακά συστήματα με ευρείες εφαρμογές πολυμέσων (MMAC).

Η ιδέα μετάδοσης πληροφορίας χρησιμοποιώντας πολυπλεξία διαίρεσης συχνότητας (FDM) ξεκίνησε στα μέσα της δεκαετίας του 1960. Κάποια χρόνια νωρίτερα είχαν γίνει αρκετά βήματα προς αυτή τη κατεύθυνση. Τελικά η πρώτη υλοποίηση και χρησιμοποίηση της τεχνικής FDM έγινε το 1970 στις Η.Π.Α. Η αρχική ιδέα, που εφαρμόστηκε σε επικοινωνίες του στρατού, ήταν η δημιουργία παράλληλων συρμών δεδομένων και πολυπλεξία διαίρεσης συχνότητας με υποκανάλια που επικαλύπτονται μεταξύ τους. Ο στόχος ήταν η αποτελεσματική χρησιμοποίηση του διαθέσιμου εύρους ζώνης αλλά και η συγχώνευση του προστιθέμενου θορύβου του καναλιού με την παραμόρφωση που υφίσταται το σήμα λόγω του φαινομένου των πολλαπλών διοδεύσεων. Στο OFDM, κάθε φέρον είναι ορθογώνιο με τα υπόλοιπα ωστόσο αυτή η συνθήκη δε διατηρείται πάντα.

Για μεγάλο αριθμό υποκαναλιών, οι γεννήτορες ημιτονοειδών παλμών αλλά και οι σύμφωνοι αποδιαμορφωτές είναι πολύ ακριβοί και πολύπλοκοι στην υλοποίησή

τους. Ο παραλήπτης πρέπει να γνωρίζει απόλυτα τη φάση των φερόντων αλλά και τις χρονικές στιγμές δειγματοληψίας ώστε να διατηρήσει τη διασταύρωση συνομιλίας σε γειτονικά φέροντα κάτω από ένα επιτρεπτό όριο. Οι Weinstein και Ebert χρησιμοποίησαν το διακριτό μετασχηματισμό Fourier (DFT) σαν μέρος των διαδικασιών διαμόρφωσης και αποδιαμόρφωσης στον πομπό και το δέκτη αντίστοιχα. Επιπλέον για να εξαλειφθούν οι πολλοί ταλαντωτές σε κάθε υποφέρον καθώς και οι σύμφωνοι αποδιαμορφωτές που απαιτούνται σε ένα FDM σύστημα, χρησιμοποιήθηκε ένα απόλυτα ψηφιακό μέρος για την υλοποίηση του ταχύ μετασχηματισμού Fourier (FFT). Στο τελευταίο συνέβαλε και η εξέλιξη της VLSI τεχνολογίας με αποτέλεσμα την υλοποίηση του FFT με κυκλώματα πολύ υψηλής ολοκλήρωσης με μεγάλες ταχύτητες και χαμηλό κόστος.

Η πολυπλεξία ορθογωνικής διαίρεσης συχνότητας (OFDM) είναι μία μέθοδος μετάδοσης όπου χρησιμοποιούνται πολλά φέροντα για τη μετάδοση πληροφορίας. Διαιρείται το διαθέσιμο φάσμα σε πολλά κανάλια, κάθε ένα από τα οποία διαμορφώνεται από ένα χαμηλό ρυθμό δεδομένων. Η OFDM μέθοδος δεν είναι πολλαπλής προσπέλασης σε αντίθεση με την OFDMA, όπου μπορούν να μεταδώσουν ταυτόχρονα πολλοί χρήστες. Η ομοιότητα του OFDM με την πολλαπλή προσπέλαση διαίρεσης συχνότητας είναι ότι η πολλαπλή πρόσβαση χρηστών επιτυγχάνεται διαιρώντας το διαθέσιμο εύρος ζώνης σε πολλά κανάλια, τα οποία έπειτα κατανέμονται στους χρήστες.

2.7 Σύνοψη κεφαλαίου

Οι συμβατικοί τύποι ασφάλειας δικτύου βασίζονται σε κωδικούς πρόσβασης ή κλειδιά. Τα κύρια μειονεκτήματα των συμβατικών τύπων ασφάλειας ασύρματων δικτύων είναι η ευκολία υποκλοπών και η ευκολία παράνομης πρόσβασης στο δίκτυο.

Τα συστήματα ασφαλείας που βασίζονται σε κλειδιά αυξάνουν τα έξοδα για την ασφάλεια ενός δικτύου, ειδικά σε περιπτώσεις εταιριών. Όσο καλύτερη γίνεται και η ασφάλεια, αυξάνεται και η επιβάρυνση. Μπορεί επίσης να προκληθούν και προβλήματα διαχείρισης των κλειδιών από το δίκτυο, ειδικά σε δίκτυα υψηλού αριθμού κόμβων. Όλες αυτές οι ευπάθειες οδηγούν στην ανάγκη διερεύνησης λύσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Applebaum, S., (1966). Adaptive Arrays. Syracuse University Research Corporation.

Chrysikos, (2009). Theofilos Chrysikos, Giannis Georgopoulos and Stavros Kotsopoulos, “Empirical Calculation of Shadowing Deviation for Complex Indoor Propagation Topologies at 2.4 GHz”, International Conference on Ultra Modern Telecommunications (ICUMT 2009), October 12-14, 2009, St. Petersburg, Russia.

Chrysikos, (2011). Theofilos Chrysikos, Tasos Dagiuklas and Stavros Kotsopoulos, “Wireless Information-Theoretic Security in an Outdoor topology with Obstacles: Theoretical Analysis & Experimental Measurements”, EURASIP Journal on Wireless

Communications and Networking, Special Issue on Security and Resilience for Smart Devices and Applications.

Chrysikos, (2012). Theofilos Chrysikos and Stavros Kotsopoulos, “Characterization of Propagation Mechanisms for the 2.4 GHz Channel At Athens International Airport”, 6th European Conference on Antennas and Propagation (EuCAP 2012), Prague, Czech Republic, March 26-30.

Chrysikos, (2018). Theofilos Chrysikos, Panagiotis Georgakopoulos, Iliana Oikonomou, and Stavros Kotsopoulos, “Measurement-based characterization of the 3.5 GHz channel for 5G-enabled IoT at complex industrial and office topologies”, Wireless Telecommunications Symposium (WTS 2018), Phoenix, USA, April 18-20, 2018.

Duruturk, Mustafa, "Study of Physical Layer Security in Wireless Communications" (2010). Theses, Dissertations, & Student Research in Computer Electronics & Engineering. 4.

Edney, John and William A. Arbaugh. 2004. Real 802.11 Security Wi-Fi Protected Access and 802.11i. Boston: Addison Wesley Publishing.

Gast, Matthew. (2002). 802.11 Wireless Networks: The Definitive Guide: Creating and Administering Wireless Networks. Sebastopol, California: O’Reilly Media.

Gross, Frank. (2005). Smart Antennas for Wireless Communications: With MATLAB. New York: McGraw Hill.

Howels, P., “Intermediate Sidelobe Canceller,” U.S. Patent 3202990, Aug. 24, (1965).

Liberty, J., and T. Rappaport, (1999). Smart Antennas for Wireless Communications, New York: Prentice Hall.

O'Neil Product Development Inc. (2009). "The Importance of Enhanced Security and Encryption Protocols for Wireless Hardware," http://www.oneilprinters.com/Documents/RMS %20Product %20Announcement.pdf

Perrig, A and J.D. Tygar. (2003). Secure Broadcast Communication in Wired and Wireless Networks. Norwell, Massachusetts: Kluwer Academic Publishers.

Proxim Wireless. (2003). Wireless Network Security, ORiNOCO security white paper. http://www.sparcotech.com/Proxim%20Wireless%20Security.pdf.

Rysavy Research. (2007). "Security Requirements for Wireless Networking," http://www.rysavy.com/Articles/2007 12 rysavy research security white paper.pdf.

Steyskal, H. (1987). "Digital Beamforming Antennas - An Introduction" Microwave journal. Vol. 30.

Walker, Jesse, Intel Corp. whitepaper. (2000). "Unsafe at any Key Size: an analysis of the WEP encapsulation," http://md.hudora.de/archiv/wireless/unsafew.pdf.

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ ΔΙΚΤΥΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

3.1 Εισαγωγή

Τα δίκτυα κινητής τηλεφωνίας έχουν αυξηθεί ευρέως τα τελευταία χρόνια, με διευρυμένες δυνατότητες χρήσης από την προσωπική ζωή έως τις επιχειρηματικές ανάγκες. Αυτή η αυξημένη χρήση έχει φέρει περισσότερα προβλήματα ασφάλειας και συνεπώς έχει αυξήσει και τη σημασία της διατήρησης της ασφάλειας. Τα δίκτυα κινητής τηλεφωνίας αποτελούνται από δύο μέρη, το ενσύρματο backhaul (οπισθόζευξης) και το ασύρματο.

Το ενσύρματο backhaul είναι το τμήμα μεταξύ του σταθμού βάσης και της κεραίας του ασύρματου δικτύου. Πρόκειται για ένα εξαιρετικά αξιόπιστο δίκτυο με μεγάλη ικανότητα μεταφοράς δεδομένων. Η ασφάλεια σε αυτό το μέρος είναι πολύ σημαντική. Στο φυσικό επίπεδο που βασίζεται στο καλώδιο, το μέρος όπου μεταφέρονται τα φυσικά σήματα, τα δεδομένα είναι δύσκολο να αποκτηθούν, καθώς είναι δυνατή η φυσική προστασία καλωδίων και συσκευών. Το ασύρματο είναι το τελευταίο στάδιο, όπου εμπλέκεται και ο χρήστης. Αυτό το μέρος προφανώς πρέπει να είναι ασύρματο για την καλύτερη εξυπηρέτηση των χρηστών.

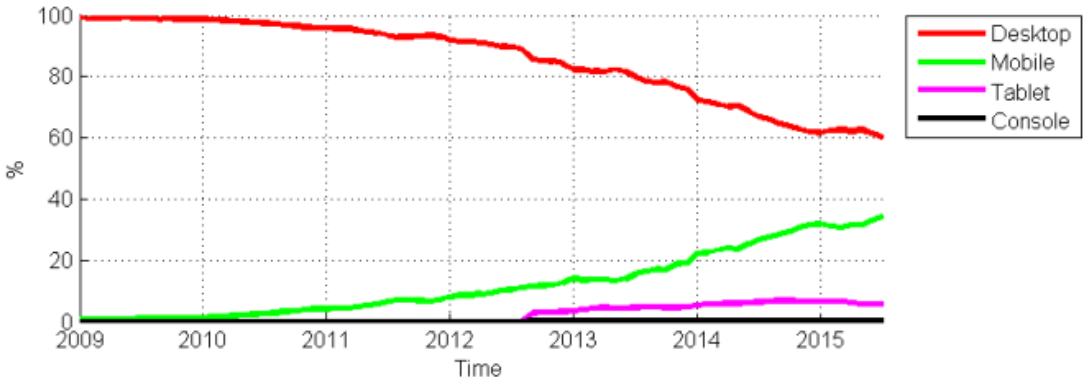
Το ασύρματο μέσο έχει ανοιχτό χαρακτήρα, επομένως οι ασύρματες συνδέσεις είναι πιο ευάλωτες σε επιθέσεις φυσικού επιπέδου σε σύγκριση με το ενσύρματο. Σε αυτό το κεφάλαιο, θα δοθεί μια γενική εικόνα για το γιατί στις ασύρματες τεχνολογίες η διατήρηση της ασφάλειας αποτελεί πρόκληση. Επιπλέον, θα εξηγηθούν οι τρέχουσες και μελλοντικές λύσεις για την προστασία του ασύρματου δικτύου κινητής τηλεφωνίας από επιθέσεις φυσικού επιπέδου.

Τα δίκτυα κινητής τηλεφωνίας αποτελούν ένα πολύ σημαντικό μέρος των σημερινών δικτύων επικοινωνίας. Με τα χρόνια, οι χρήστες έχουν αλλάξει την προτιμώμενη πλατφόρμα τους για πρόσβαση στο διαδίκτυο και σε άλλα δεδομένα χρησιμοποιώντας τεχνολογίες κινητής τηλεφωνίας αντί για συμβατικές συσκευές επιτραπέζιων υπολογιστών. Από τα στατιστικά στοιχεία των χρηστών, είναι εύκολο να διαπιστωθεί ότι το μερίδιο των χρηστών κινητών τηλεφώνων και tablet εμφανίζει

αυξανόμενη τάση ήδη εδώ και μια δεκαετία (FVC, 2008). Ως παράδειγμα, το Σχήμα 3.1 δείχνει το ποσοστό των χρηστών που έχουν πρόσβαση στις ιστοσελίδες που χρησιμοποιούν το StatCounter (FVC, 2008) χρησιμοποιώντας συσκευές όπως υπολογιστές, κινητά και tablet. Εδώ, μπορούμε εύκολα να δούμε ότι οι χρήστες προτιμούν να χρησιμοποιούν περισσότερο κινητά τηλέφωνα τον τελευταίο καιρό και η τάση δείχνει ότι η αύξηση χρήσης είναι πιθανό να συνεχιστεί στο εγγύς μέλλον.

Καθώς οι ασύρματες τεχνολογίες εξελίσσονται, οι χρήστες απαιτούν υψηλότερες ταχύτητες δεδομένων, αυξημένη αξιοπιστία και ασφάλεια για τις συνδέσεις κινητής τηλεφωνίας. Ωστόσο, η διατήρηση αυτών των απαιτήσεων δεν είναι εύκολη, καθώς τα κινητά δίκτυα είναι ιδιαίτερα ευάλωτα σε αποτυχίες, εισβολές και υποκλοπές. Επίσης, η δυνατότητα μετακίνησης των χρηστών, τα υποδίκτυα και η συνεχής αλλαγή σταθμών βάσης αυξάνουν την δυσκολία στην διατήρηση της ασφάλειας. Το ασύρματο μέσο, το οποίο χρησιμοποιείται για τη μεταφορά των σημάτων στον χρήστη κινητής τηλεφωνίας, είναι συνήθως λιγότερο αξιόπιστο, αλλάζει ταχέως και είναι ανοιχτό σε επιθέσεις. Εκτός από όλες αυτές τις προκλήσεις, το δίκτυο κινητής τηλεφωνίας θα πρέπει να επιβιώνει από εκ προθέσεως και από αθέλητες (φυσικές) απειλές.

Άρα αρχικά μπορούμε να πούμε ότι η συνεχής αύξηση χρήσης ασύρματων δικτύων σε σχέση με τα αντίστοιχα ενσύρματα είναι σχεδόν βέβαιη, παρά την αυξημένη ασφάλεια του ενσύρματου δικτύου. Το ασύρματο κανάλι, ωστόσο, εισάγει νέους τύπους απειλών που δεν αντιμετωπίζονται με κλασσικές λύσεις ασφάλειας που στοχεύουν κυρίως στην ασφάλεια του ενσύρματου δικτύου



Σχήμα 3.1 Παγκόσμια στατιστικά στοιχεία χρήσης πλατφόρμων που αποκτήθηκαν από το StatCounter Global Stats μεταξύ Δεκεμβρίου 2008 και Ιουνίου 2015 (FVC, 2008). Το μερίδιο των χρηστών κινητής τηλεφωνίας και tablet έχει συνεχώς αυξανόμενη τάση.

Για την αντιμετώπιση των απειλών ασφάλειας σε ασύρματα δίκτυα, θα πρέπει να χρησιμοποιούνται μέτρα ασφαλείας φυσικού επιπέδου (physical layer security) τα οποία να είναι σχεδιασμένα κατά παραγγελία ανάλογα με την κατάσταση του δικτύου.

Επίσης πρέπει να ληφθεί υπόψη ότι στα δίκτυα ασύρματης επικοινωνίας, υπάρχουν πολλές φυσικές προκλήσεις, όπως στοχαστικά φαινόμενα απωλειών και διαλείψεων του καναλιού και περιορισμένο εύρος ζώνης μετάδοσης. Επιπλέον, μπορεί να υπάρχουν άνθρωποι που προσπαθούν να εκτελέσουν διάφορες επιθέσεις για να καταγράψουν ή να αποτρέψουν την επικοινωνία μεταξύ των νόμιμων συμβαλλόμενων μερών. Η ασφάλεια φυσικού επιπέδου εντοπίζει και μετριάζει αυτές τις επιθέσεις με βάση τα χαρακτηριστικά του ασύρματου δικτύου.

Το βασικό σύστημα που μπορεί να οριστεί για την ασφάλεια φυσικού επιπέδου αποτελείται από τρεις κόμβους, έναν νόμιμο αναμεταδότη, έναν νόμιμο λήπτη και

έναν ακουστικό, που συχνά αναφέρονται ως Alice, Bob και Eve αντίστοιχα, στις περισσότερες έρευνες.

Χρησιμοποιώντας αυτό το βασικό σύστημα, μπορούν να αναλυθούν οι περισσότερες τεχνικές φυσικού επιπέδου. Σημειώστε ότι αυτό το βασικό μοντέλο μπορεί να αντιπροσωπεύει το ασύρματο τελικό μέρος ενός μεγαλύτερου δικτύου επικοινωνιών, για παράδειγμα ένα κινητό δίκτυο όπου ο σταθμός βάσης Alice είναι ο σταθμός βάσης και ο Bob είναι ο τελικός χρήστης. Σε ολόκληρο το κεφάλαιο, θα ακολουθήσει η ίδια προσέγγιση για την αντιμετώπιση των ζητημάτων ασφάλειας φυσικών επιπέδων των δικτύων κινητής τηλεφωνίας. Θα αναλύσουμε την τεχνολογία δικτύων κινητής τηλεφωνίας ως ξεχωριστό ασύρματο δίκτυο, ξεχωριστά από το υπόλοιπο δίκτυο που συχνά συνδέεται με καλώδια.

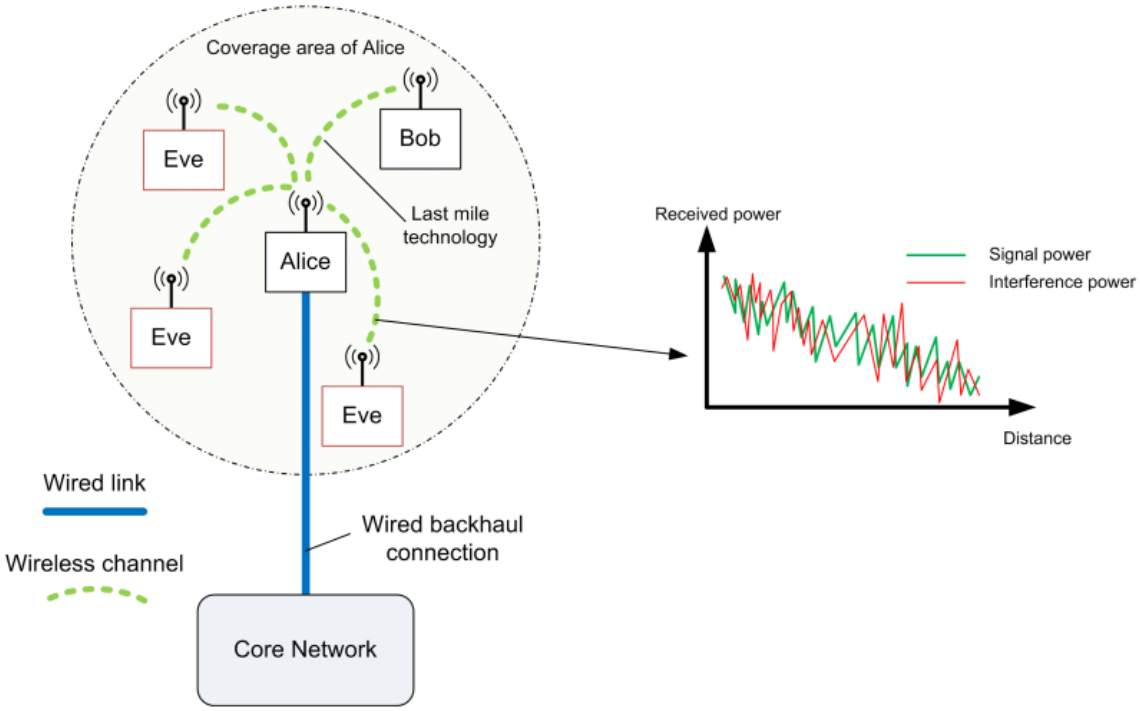
3.2 Τεχνολογίες ασύρματης κινητής τηλεφωνίας

Προκειμένου να παρέχεται ένα σύνολο υπηρεσιών, ένας σύνδεσμος επικοινωνίας αποτελείται από πολλά συστατικά που εκτελούν διαφορετικές λειτουργίες. Το εύρος και η ποιότητα αυτών των υπηρεσιών προκύπτουν από τις απαιτήσεις του τελικού χρήστη. Οι κύριες οντότητες που παρέχουν υπηρεσίες σε έναν τελικό χρήστη είναι πάροχοι υπηρεσιών δικτύου (NSP) και πάροχοι υπηρεσιών διαδικτύου (ISPs). Οι NSP κατασκευάζουν παγκόσμια δίκτυα και εκχωρούν εύρος ζώνης σε περιφερειακά NSP, τα οποία προσφέρουν το εύρος ζώνης σε τοπικούς ISP.

Οι ISP παρέχουν και διαχειρίζονται υπηρεσίες στους τελικούς χρήστες. Ως εκ τούτου, το συνολικό δίκτυο διατηρείται ως χωριστά μπλοκ και διάφορες τεχνολογίες μπορούν να χρησιμοποιηθούν σε κάθε μπλοκ. Σύμφωνα με τη δομή αυτή, το Internet

backbone, το δίκτυο ISP και το δίκτυο του τελικού χρήστη μπορούν να σχεδιαστούν και να λειτουργούν σχεδόν ξεχωριστά.

Το πρότυπο που χρησιμοποιείται για τον καθορισμό της τελικής σύνδεσης μεταξύ των παρόχων υπηρεσιών και του τελικού χρήστη αναφέρεται ως τεχνολογία τελευταίου μιλίου. Σε αντίθεση με την backhaul, η τεχνολογία τελευταίου μιλίου εξαρτάται επίσης από τις απαιτήσεις των τελικών χρηστών, όπου η κάλυψη και το κόστος μπορεί να καταστούν πιο σημαντικά από την αξιοπιστία και το ρυθμό μετάδοσης δεδομένων. Οι ασύρματες τεχνολογίες είναι οι κυριότεροι τρόποι εφαρμογής της τεχνολογίας του τελευταίου μιλίου. Η χρήση κινητών συσκευών και κινητών επικοινωνιών αυξάνεται ραγδαία στους χρήστες της τεχνολογίας (Bishop, 2006), (Blossom, http://www.gnu.org/software/gnuradio/). Το γεγονός ότι οι ασύρματες τεχνολογίες δεν μπορούν να επιτύχουν την αξιοπιστία και το ρυθμό μετάδοσης δεδομένων ενός ενσύρματου αντισυμβαλλόμενου καθίσταται δευτερεύουσα ανησυχία.



Σχήμα 3.2 Τα χαρακτηριστικά του ασύρματου καναλιού αυξάνουν τις απειλές ασφάλειας που οφείλονται στην ανοικτή φύση του καναλιού. Στο σχήμα υπάρχει ένας νόμιμος ασύρματος πομπός που ονομάζεται Alice ο οποίος είναι συνδεδεμένος στο κεντρικό δίκτυο με μια ενσύρματη σύνδεση και χρησιμοποιεί το ασύρματο μέσο για τη σύνδεση τελευταίου μιλίου για να επικοινωνήσει με το νόμιμο ακουστικό δέκτη Bob. Δεδομένου ότι το ασύρματο μέσο έχει ανοιχτό χαρακτήρα, οι παράνομοι δέκτες είναι επίσης σε θέση να συγκεντρώσουν τα σήματα από την Alice. Η ισχύς του λαμβανόμενου σήματος στην Eve εξαρτάται από την απόσταση και κυμαίνεται από συγκεκριμένα χαρακτηριστικά του καναλιού, όπως η εξασθένιση και η σκίαση. Οι παρεμβολές είναι ακόμα ένας σημαντικός παράγοντας. Σημειώστε ότι οι παρεμβολές έχουν μεγάλη επίδραση στην ποιότητα του σήματος.

3.3 Η ασύρματη τεχνολογία ως τεχνολογία τελευταίου μιλίου

Τα ασύρματα δίκτυα έχουν γίνει σήμερα ένα σημαντικό κομμάτι των δικτύων επικοινωνίας και επίσης φαίνεται να αποτελούν ισχυρό στοιχείο των μελλοντικών δικτύων επικοινωνίας. Πέρα από τα συστήματα 4ης γενιάς (4G) και τα συστήματα 5ης γενιάς (5G), τα πρότυπα IEEE 802.11 χρησιμοποιούνται από ένα μεγάλο μέρος των ευρυζωνικών συνδέσεων και επιλέγονται ώστε να συνδέσουν τις συσκευές τους στο διαδίκτυο για το τελευταίο στάδιο. Αυτό σημαίνει ότι οι ασύρματες τεχνολογίες θα επικρατήσουν έναντι των ενσυρμάτων ως τεχνολογία τελευταίου μιλίου στο μέλλον. Οι κύριοι λόγοι επιλογής ασύρματων τεχνολογιών είναι η κινητικότητα και η ευκολία χρήσης. Στην πραγματικότητα, σύμφωνα με την έκθεση KPCB 2015 Internet Trends της Mary Meeker (Bolle et al, 2003), το ποσοστό του χρόνου που αφιερώνεται στα κινητά ψηφιακά μέσα στις ΗΠΑ είναι ήδη υψηλότερο στο 51%, σε σύγκριση με τους ηλεκτρονικούς υπολογιστές με 42%.

Η χρήση των ασύρματων τεχνολογιών αυξάνει την κρίσιμη ευαισθησία ως προς το εύρος ζώνης και την ασφάλεια. Υπάρχει επίσης χαμηλότερο ποσοστό μετάδοσης δεδομένων, αλλά αυτό το μειονέκτημα παραβλέπεται εύκολα καθώς οι νεότερες ασύρματες τεχνολογίες έχουν υψηλότερα ποσοστά δεδομένων, ωστόσο τα ζητήματα ασφάλειας είναι κρίσιμα για τις ασύρματες τεχνολογίες λόγω της ανοικτής φύσης των ασύρματων ζεύξεων. Εκτός από τις απειλές ασφάλειας από τα ανώτερα επίπεδα, η χρήση ασύρματου μέσου έχει ιδιαίτερα τρωτά σημεία στο φυσικό επίπεδο. Αξίζει να επισημανθεί ότι εκτός από την προφανή χρήση ασύρματου μέσου σε δίκτυα κινητής τηλεφωνίας, ακόμη και για συνδέσεις ευρυζωνικού Internet, εξετάζονται οι ασύρματες τεχνολογίες γενικά (Brik et al, 2008), (Danev et al, 2009). Ως εκ τούτου, όταν αναφέρουμε ασύρματη ασφάλεια φυσικού επιπέδου, μιλάμε για τα περισσότερα από τα εμπορικά δίκτυα όπως τα κινητά δίκτυα και τα μελλοντικά ευρυζωνικά δίκτυα (Chrysikos, 2010).

3.4 Η σημασία του τελευταίου σταδίου για την ασφάλεια

Όπως προαναφέρθηκε, η κύρια πρόκληση ασφάλειας των ασύρματων τεχνολογιών ως τελευταίο στάδιο της σύνδεσης προκαλείται από την ανοικτή φύση του ασύρματου δικτύου. Στα συμβατικά ενσύρματα δίκτυα, το μέσο φυσικού επιπέδου αποτελείται από καλώδια και η μετάδοση σήματος μέσω καλωδίου μεταξύ δύο κόμβων θεωρείται ασφαλής. Αυτή είναι μια ακριβής παραδοχή, καθώς η ασφάλεια ενός καλωδίου θα μπορούσε εύκολα να επιτευχθεί φυσικά κάνοντας το καλώδιο απρόσιτο, για παράδειγμα με τη χρήση κλειδωμένων χώρων εξυπηρέτησης ή υπόγειων καλωδίων. Η επίθεση υποκλοπής, η οποία εκτελείται από παράνομη χρήση για την καταγραφή δεδομένων με την ακρόαση του συνδέσμου, γίνεται πολύ δύσκολο να είναι επιτυχής όταν τα καλώδια δεν είναι προσβάσιμα.

Ωστόσο, οι ασύρματες επικοινωνίες, αντί να χρησιμοποιούν καλώδια για τη μετάδοση των σημάτων, χρησιμοποιούνται κεραίες για τη μετάδοση και λήψη των σημάτων. Τα σήματα παρουσιάζουν παραμόρφωση στο μέτρο και στη φάση μετά την έξοδο από την κεραία του πομπού και πριν φτάσουν στην κεραία του δέκτη. Ωστόσο, όταν χρησιμοποιούνται τα ασύρματα κανάλια για τη μετάδοση σημάτων, το σήμα μπορεί να φτάσει οπουδήποτε εντός της εμβέλειας μετάδοσης, δηλαδή υπάρχει ένα τρέχον (στιγμιαίο) και ένα μέσο επίπεδο αποδεκτού σήματος προς παρεμβολή συν το θόρυβο (SINR).

Οι πάροχοι υπηρεσιών πρέπει να διατηρούν το SINR πάνω από ένα αποδεκτό επίπεδο για τους χρήστες τους, γεγονός που αποτελεί περιορισμό για την επιτυχή λήψη των σημάτων στην πλευρά του δέκτη. Για τα σήματα που μεταδίδονται από μια κεραία, υπάρχει ένα χωρικό μοτίβο που τα σήματα κατανέμονται και η ισχύς του σήματος μειώνεται μη-γραμμικά με την απόσταση. Στην πιο απλή περίπτωση που έχουμε μετάδοση σύμφωνα με το μοντέλο του ελεύθερου χώρου, η εξασθένηση της ισχύος

με την απόσταση ακολουθεί τον νόμο του αντιστρόφου τετραγώνου (inverse square law), ενώ σε πιο σύνθετα σενάρια ακολουθεί πιο ταχείες (severe) φθορές (Chrysikos, 2009). Η συνάρτηση του χώρου ως προς την ένταση του σήματος που βρίσκεται πάνω από κάποιο επίπεδο ονομάζεται περιοχή κεραίας. Αυτή η συνάρτηση ορίζει τις θέσεις στις οποίες μπορεί να ληφθεί επιτυχώς το σήμα.

Κάθε χρήστης εντός της εμβέλειας μετάδοσης, συμπεριλαμβανομένων των παράνομων δεκτών όπως οι υποκλοπείς, μπορεί να συλλάβει τα μεταδιδόμενα σήματα.

Ένα τυπικό δίκτυο κινητής τηλεφωνίας με ενσύρματο backhaul εμφανίζεται στο Σχήμα 3.2. Στο σχήμα, η κεραία ασύρματου πομπού στέλνει σήμα στην Alice και συνδέεται στο κεντρικό δίκτυο μέσω ενσύρματου συνδέσμου. Η Alice είναι ο νόμιμος πομπός, μεταδίδοντας σήματα στον νόμιμο δέκτη Bob, ενώ τα μηνύματα παραλαμβάνονται επίσης από παράνομους χρήστες, που αναφέρονται ως Eve. Η λαμβανόμενη ισχύς των σημάτων από την κεραία του πομπού σε σχέση με την απόσταση φαίνεται επίσης στο σχήμα, η οποία προκαλείται από τις εγγενείς ιδιότητες των ασύρματων καναλιών, όπως η απώλεια ισχύος και η σκίαση. Στη δεδομένη ρύθμιση, είναι σαφές ότι η ασφάλεια του συνολικού δικτύου επηρεάζεται από την ασφάλεια του τελευταίου σταδίου, που είναι ασύρματο.

3.5 Μοντέλα καναλιών για ασύρματα δίκτυα κινητής τηλεφωνίας

Σε ένα βασικό σενάριο ασύρματης επικοινωνίας, όπως αυτό που είδαμε στο προηγούμενο σχήμα, τα ηλεκτρικά σήματα μεταδίδονται στο κενό ως ηλεκτρομαγνητικά κύματα μέσω μιας κεραίας. Αυτά τα κύματα ανιχνεύονται και συλλαμβάνονται στη συνέχεια από μια κεραία λήψης και λαμβάνονται σήματα στην

πλευρά του δέκτη. Υπάρχουν διαφορετικά μοντέλα καναλιών τα οποία χρησιμοποιούνται συχνά στη βιβλιογραφία όπως τα μοντέλα καναλιών Rayleigh, Rician ή Nakagami (Danev et al, 2009), καθώς και μοντέλα Stanford University Interim (SUI) (Danev et al, 2009) ή 3GPP WIM2 (Edman et al, 2009). Τα φυσικά χαρακτηριστικά του καναλιού, όπως η απώλεια διαδρομής, η σκίαση, η εξασθένιση (μικρής κλίμακας και μεγάλης κλίμακας) και η μετατόπιση Doppler περιλαμβάνονται συνήθως σε αυτά τα μοντέλα. Η παρεμβολή, η οποία είναι το επιπρόσθετο ηλεκτρομαγνητικό σήμα που λαμβάνεται μαζί με το προβλεπόμενο σήμα, είναι μια άλλη σημαντική αιτία υποβάθμισης της ποιότητας του σήματος. Η παρεμβολή θεωρείται ξεχωριστό φαινόμενο από ό,τι ο θόρυβος παρόλο που αθροίζονται και από κοινού μειώνουν το SINR.

3.6 Προβλήματα των ασύρματων δικτύων κινητής τηλεφωνίας

1. Θερμικός θόρυβος: Και τα ενσύρματα και τα ασύρματα συστήματα επικοινωνίας υπόκεινται σε τυχαίες διακυμάνσεις στα επίπεδα λήψης σήματος, οι οποίες προκαλούνται από πολλές φυσικές πηγές. Αναφερόμενο ως θερμικός θόρυβος ή λευκός Gaussian θόρυβος, αυτό το φαινόμενο ακολουθεί Gaussian (κανονική) κατανομή ως προς το πλάτος του σήματος του θορύβου. Στα φαινόμενα θορύβου πρέπει να συμπεριλάβουμε και τον λεγόμενο ανθρωπογενή θόρυβο (man-made noise) που μπορεί να ακολουθεί επίσης την κανονική κατανομή και οφείλεται σε εκκίνηση μηχανών, φούρνων μικροκυμάτων και από άλλες διατάξεις που έχουν κατασκευασθεί από ανθρώπινο χέρι.

2. Απώλεια σήματος και εξασθένηση: Η απώλεια σήματος αναφέρεται στην αποδυνάμωση των σημάτων καθώς διαδίδονται μέσω του αέρα. Αυτή η αποδυνάμωση προκαλείται από την απόσταση μεταξύ πομπού και δέκτη (ντετερμινιστική απώλεια λόγω απόσταση, free-space distance-dependent attenuation). Εκτός από την απώλεια σήματος, η φάση των λαμβανόμενων σημάτων μέσω του ασύρματου διαύλου μπορεί να αλλάξει γρήγορα στο χρόνο, όπως επίσης και η συχνότητα κατά μία μικρή τιμή (frequency offset) (Ureten et al, 2007).

   Το φαινόμενο που ονομάζουμε εξασθένιση, συνήθως διαμορφώνεται ως τυχαία διαδικασία. Ως πλεονάζουσα απώλεια οδεύσεως νοούνται οι εξασθενήσεις μεγάλης κλίμακας, πέραν των ντετερμινιστικών απωλειών λόγω συχνότητας. Υπάρχουν δύο κύριες κατηγορίες εξασθένησης, η μεγάλης κλίμακας και η μικρής κλίμακας εξασθένηση. Μεγάλης κλίμακας εξασθένιση (large-scale fading) προκαλείται από απώλεια σήματος και σκίαση από μεγάλα αντικείμενα συγκρινόμενα με το μήκος κύματος της μεταδιδόμενης ηλεκτρομαγνητικής ακτινοβολίας (όπως κτίρια και λόφοι, αλλά και τοίχοι, πατώματα, οροφές). Η εξασθένηση μεγάλης κλίμακας είναι κατά κανόνα εξαρτώμενη από την συχνότητα (shadow fading).

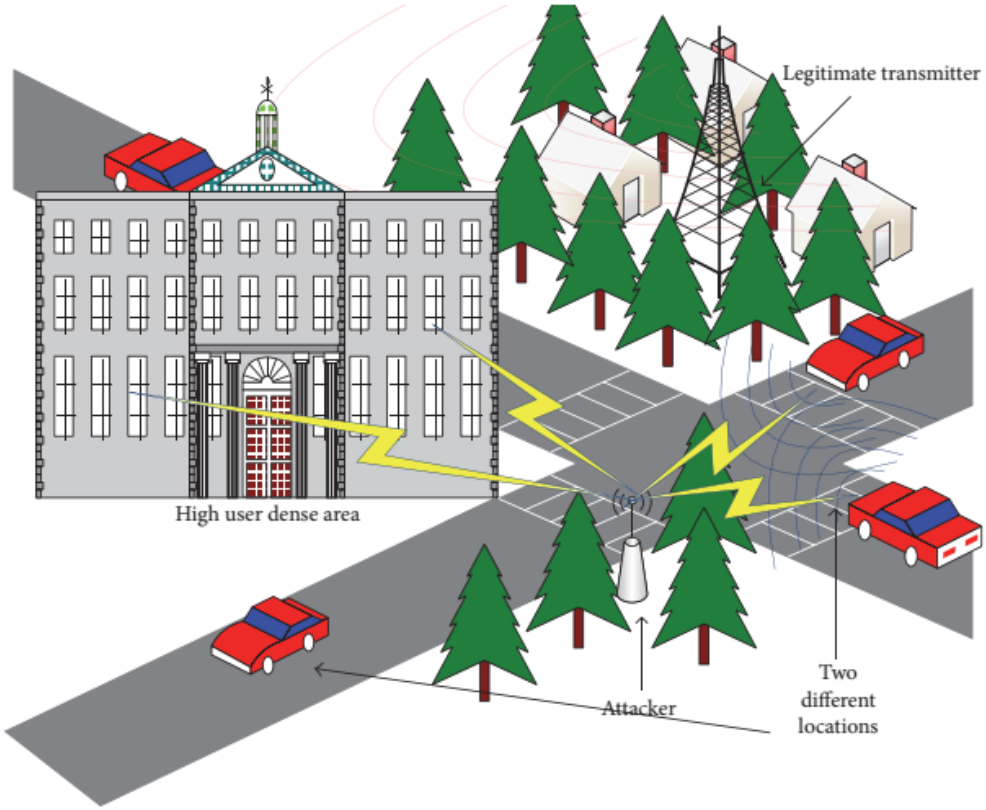
   Η εξασθένηση μικρής κλίμακας (small scale fading) προκαλείται γενικά από την παρεμβολή που προκαλείται από την ύπαρξη πολλαπλών διαδρομών μετάδοσης μεταξύ του πομπού και του δέκτη (φαινόμενα πολυόδευσης – multipath fading) και εξαρτάται επίσης από τη συχνότητα και οφείλεται σε αντικείμενα διαστάσεων της ίδιας τάξης με το μήκος κύματος της Η/Μ ακτινοβολίας. Τα πιο συχνά χρησιμοποιούμενα μοντέλα εξασθένισης μικρής κλίμακας είναι τα μοντέλα Rayleigh, Rician, Weibull, Nakagami.

3. Παρεμβολές πολλών χρηστών: Κατά τη μοντελοποίηση των αποτελεσμάτων του ασύρματου καναλιού, είναι σημαντικό να εξεταστεί η παρεμβολή πολλών χρηστών, δηλαδή τα σήματα των χρηστών που λαμβάνονται συνολικά από τον δέκτη. Βασικά, η κεραία του δέκτη δεν συλλαμβάνει μόνο τα σήματα του επιδιωκόμενου πομπού, αλλά και μια υπέρθεση σημάτων όλων των πομπών που χρησιμοποιούν την ίδια ζώνη συχνοτήτων που έχουν τον δέκτη στην εμβέλεια της κεραίας τους. Αυτά τα σήματα, τα οποία επίσης υπόκεινται σε εξασθένιση και απώλεια σήματος, λειτουργούν ως επιδείνωση της λήψης του σήματος. Συχνά είναι πολύ ισχυρά, περιορίζοντας σοβαρά τις τιμές SINR, και προκαλώντας πιθανώς διαταραχές της επικοινωνίας. Επιπρόσθετα, εκτός από τις φυσικές πηγές παρεμβολής που οφείλονται στο περιβάλλον, οι παρεμβολές μπορούν να δημιουργηθούν σκόπιμα από έναν αντίπαλο ή ανταγωνιστή. Στην περίπτωση αυτή, αναφερόμαστε σε επίθεση παρεμβολών κατά του δικτύου.

3.7 Επιθέσεις στο φυσικό επίπεδο σε ασύρματα δίκτυα

Στα δίκτυα ασύρματης επικοινωνίας, μπορεί να γίνει επίθεση σε μία ή περισσότερες από τις τέσσερις βασικές απαιτήσεις ασφαλείας του συστήματος που είναι η μυστικότητα, η αυθεντικότητα, η ακεραιότητα των δεδομένων και η ευρωστία. Η μυστικότητα περιγράφει την μη δημοσιοποίηση των δεδομένων μεταξύ της προέλευσης και του προορισμού. Ο έλεγχος ταυτότητας είναι η πράξη επιβεβαίωσης ότι ο προορισμός των δεδομένων έχει τα δικαιώματα πρόσβασης. Η ακεραιότητα των δεδομένων αναφέρεται στην πληρότητα και την πρωτοτυπία των δεδομένων κατά τη διάρκεια του κύκλου ζωής τους. Τέλος, είναι απαραίτητη η ευρωστία ώστε το σύστημα επικοινωνίας να παραμείνει λειτουργικό υπό δύσκολες συνθήκες. Οι κύριοι τύποι επίθεσης παρατίθενται στο Σχήμα 3.3 μαζί με τους στόχους τους. Αυτό το σχήμα

μπορεί να χρησιμεύσει ως ενδεικτικό παράδειγμα για επιθέσεις και όχι ως πλήρης κατάλογος όλων των επιθέσεων. Είναι πολύ δύσκολο να καλύψουμε τις επιθέσεις, καθώς ανακαλύπτονται καθημερινά νέοι τύποι. Μετά τις τελευταίες ανακαλύψεις, είναι ανάγκη να υπάρχουν συνεχώς ενημερωμένες πληροφορίες σχετικά με τις νεότερες πιθανές ευπάθειες ασφαλείας οποιουδήποτε συστήματος.



Σχήμα 3.3 Ενδεικτικοί στόχοι επίθεσης

Οι στοχευμένες επιθέσεις στο φυσικό επίπεδο μπορούν να ταξινομηθούν σε δύο ομάδες: παθητικές ή ενεργές επιθέσεις. Στις παθητικές επιθέσεις ο αντίπαλος δεν δίνει πληροφορίες στο σύστημα, καθιστώντας πολύ δύσκολο να εντοπιστούν αυτοί οι τύποι επιθέσεων. Από την άλλη πλευρά, κατά τη διάρκεια ενεργών επιθέσεων ο

αντίπαλος χρησιμοποιεί έναν πομπό, παρεμβαίνοντας ενεργά στο δίκτυο. Αυτές οι επιθέσεις είναι συνήθως ευκολότερο να εντοπιστούν, ωστόσο αυτό δεν σημαίνει ότι είναι εύκολο να αποφευχθούν. Οι στοχευμένες επιθέσεις στο φυσικό επίπεδο μπορούν επίσης να ομαδοποιηθούν με βάση τις στοχευμένες απαιτήσεις ασφαλείας τους, δηλαδή τη μυστικότητα, την αυθεντικότητα, την ακεραιότητα των δεδομένων και την ευρωστία(Κομνηνός και σύν.,2002).

Απαραίτητη προϋπόθεση για την ασφαλή λειτουργία των συστημάτων είναι ο έλεγχος. Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη μέσω του ελέγχου πρόσβασης, το σύστημα θα πρέπει να φροντίζει έτσι ώστε ο χρήστης αυτός να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό επιτυγχάνεται εφαρμόζοντας ελέγχους προσπέλασης.

Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες:

- Υποκείμενα. Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)

- Αντικείμενα. Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)

- Τρόπος προσπέλασης. Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών.

Ο έλεγχος προσπέλασης συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα. Η επιλογή της πολίτικης ελέγχου προσπέλασης εξαρτάται από τα επιμέρους χαρακτηριστικά του περιβάλλοντος που πρόκειται να προστατευτεί.

3.7.1 Επιθέσεις μυστικότητας

Οι κυριότεροι τύποι επίθεσης εναντίον του απορρήτου δεδομένων είναι η υποκλοπή και οι επιθέσεις κατά της μυστικότητας. Υποκλοπή είναι η πράξη της κρυφής ακρόασης της ιδιωτικής συνομιλίας των άλλων χωρίς τη συγκατάθεσή τους, η οποία προβλέπει τη συλλογή δεδομένων ασύρματης επικοινωνίας από μη νόμιμους χρήστες. Οι επιθέσεις υποκλοπής είναι συνήθως πολύ εύκολο να εκτελεστούν και πολύ δύσκολο να εντοπιστούν εξαιτίας της παθητικής τους φύσης.

Τέτοιες επιθέσεις μπορούν να εκτελεστούν με την κατάλληλη συντονισμένη λήψη και αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων, σε περίπτωση κρυπτογραφημένων δεδομένων. Η επίθεση υποκλοπής μπορεί να εφαρμοστεί είτε σε πραγματικό χρόνο είτε με χρονική καθυστέρηση και ηχογράφηση της συνομιλίας. Η παρακολούθηση σε πραγματικό χρόνο είναι πιο κρίσιμη, καθώς ο αντίπαλος μπορεί να χρησιμοποιήσει προσεγγίσεις βασισμένες σε brute-force με υψηλή υπολογιστική πολυπλοκότητα για να καταγράψει τα δεδομένα, που μπορεί να χρειάζεται περισσότερο χρόνο και προσπάθεια για εντοπιστεί η υποκλοπή.

Επίσης, σε μια παθητική επίθεση, η ανάλυση κυκλοφορίας είναι μια παρόμοια κατάσταση της υποκλοπής, όπου ο μη νόμιμος χρήστης δεν μπορεί να παρακολουθήσει τα δεδομένα επικοινωνίας αλλά συγκεντρώνει τις πληροφορίες κίνησης, όπως ταυτότητες μεταδότη / δέκτη ή ρυθμούς δεδομένων. Συνήθως η επίθεση ανάλυσης κυκλοφορίας εκτελείται όπου δεν είναι δυνατή η απόκτηση του μυστικού κλειδιού που χρησιμοποιείται για την κρυπτογράφηση (Πανέτσος, 2007).

Κύριο κλασσικό αντίμετρο για την υποκλοπή είναι η κρυπτογράφηση. Δεν υπάρχει ιδιαίτερο κλασικό μέτρο ασφάλειας για την ανάλυση της κυκλοφορίας. Οι προσφάτως προτεινόμενες προσεγγίσεις ασφάλειας σχήματος δέσμης και τεχνητού θορύβου

μπορούν να βοηθήσουν στην καταπολέμηση των παθητικών επιθέσεων, συμπεριλαμβανομένων των επιθέσεων ανάλυσης κυκλοφορίας και τις υποκλοπές.

3.7.2 Επιθέσεις ελέγχου ταυτότητας

Η πιστοποίηση ταυτότητας είναι η διαδικασία επιβεβαίωσης της νομιμότητας ενός πομπού. Οι συνηθέστεροι τύποι επίθεσης είναι οι brute-force, οι υποκλοπές, οι MIM και οι κλοπές ταυτότητας. Αυτές οι επιθέσεις είναι συνήθως ανιχνεύσιμες στο φυσικό επίπεδο.

Στις επιθέσεις MIM, ο αντίπαλος κάνει ανεξάρτητες συνδέσεις με τους κόμβους-στόχους (πραγματοποιώντας αμφίδρομη επικοινωνία) και μεταδίδει μηνύματα μεταξύ τους, γεγονός που τους κάνει να πιστεύουν ότι επικοινωνούν απευθείας ο ένας με τον άλλον. Οι επιθέσεις MIM περιλαμβάνουν επίσης επιθέσεις παρασίτων. Στην πραγματικότητα, κατά τη διάρκεια μιας επίθεσης MIM, ολόκληρη η συνομιλία ελέγχεται από τον εισβολέα. Πέρα από την παραβίαση του απορρήτου, είναι σαφές ότι οι επιθέσεις MIM μπορούν να είναι πολύ επικίνδυνες για τα συστήματα, καθώς ο εισβολέας είναι σε θέση να εισέλθει στο σύστημα ή να αλλάξει τα δεδομένα επικοινωνίας με επιβλαβή τρόπο. Σε μια επίθεση κλωνοποίησης ταυτότητας, ένας μη εξουσιοδοτημένος χρήστης προσποιείται ότι είναι νόμιμος χρήστης εξαπατώντας το σύστημα ελέγχου ταυτότητας. Μια επίθεση κλωνοποίησης ταυτότητας μπορεί να εφαρμοστεί με πολλούς τρόπους, συμπεριλαμβανομένης της λήψης των ακολουθιών επαλήθευσης ταυτότητας που βασίζονται σε χαρακτηριστικά φυσικού επιπέδου. Για παράδειγμα, ένας εισβολέας μπορεί να μιμηθεί τις πληροφορίες θέσης ή καναλιού του νόμιμου χρήστη και να πάρει πιστοποίηση για την πρόσβαση.

Οι κλοπές ταυτότητας (ID) πραγματοποιούνται συνήθως με τη λήψη και τον εντοπισμό δεδομένων κίνησης του δικτύου και τον προσδιορισμό κόμβου με τα δικαιώματα του δικτύου. Τα περισσότερα ασύρματα συστήματα επιτρέπουν κάποιο είδος φίλτρου ταυτότητας για να επιτρέπεται η πρόσβαση και η χρήση του δικτύου να γίνεται μόνο μέσα από εξουσιοδοτημένη συσκευή με συγκεκριμένα αναγνωριστικά. Οι απαραίτητες πληροφορίες ταυτότητας μπορούν επίσης να συγκεντρωθούν με την επίθεση brute-force, πράγμα που σημαίνει ότι δοκιμάζει ο επιτιθέμενος όλες τις πιθανές επιλογές κλειδιού ταυτότητας(Πανέτσος, 2007).

3.7.3 Επιθέσεις ακεραιότητας δεδομένων

Σε αυτή τη μορφή επίθεσης, γίνεται προσβολή των μεταδιδόμενων δεδομένων κατά τη διάρκεια του κύκλου ζωής της επικοινωνίας. Η συχνά παρατηρούμενη επίθεση στην ακεραιότητα των δεδομένων είναι οι τροποποιήσεις μηνυμάτων και οι επιθέσεις με παρεμβολές. Οι επιτιθέμενοι μπορούν να μεταδώσουν πλαστά στοιχεία ελέγχου, διαχείρισης ή δεδομένων μέσω ασύρματου καναλιού για να παραπλανήσουν τον δέκτη. Η τροποποίηση μηνύματος είναι η γενική κατηγορία τύπων επίθεσης που βασίζεται σε προσθήκες ή διαγραφές σε πραγματικά δεδομένα. Οι επιθέσεις παρεμπόδισης βασίζονται στη μετάδοση σημάτων που διακόπτουν τη σύνδεση επικοινωνίας, περιορίζοντας το SINR. Οι επιθέσεις με παρεμβολές μπορούν να οδηγήσουν σε διαταραχές στο δίκτυο. Οι επιθέσεις με βάση τον έλεγχο ταυτότητας μπορούν επίσης να οδηγήσουν σε προβλήματα ακεραιότητας δεδομένων, δεδομένου ότι τα δεδομένα είναι δυνατόν να κινούνται και να τροποποιούνται μετά την επαλήθευση του επιτιθέμενου.

Για την ανίχνευση επιθέσεων ακεραιότητας δεδομένων, μπορούν να πραγματοποιηθούν έλεγχοι ακεραιότητας, όπως τεχνικές βασισμένες σε κλειδιά ή προκαθορισμένες κεφαλίδες πακέτων. Σημειώστε ότι παρόλο που τέτοιες επιθέσεις μπορεί να μην εντοπίζονται πάντοτε, οι έλεγχοι ακεραιότητας εξακολουθούν να είναι ένας αποτελεσματικός τρόπος αντιμετώπισης των σφαλμάτων που σχετίζονται με το φυσικό επίπεδο κατά τη μετάδοση. Τέτοια σφάλματα μπορούν επίσης να καταπολεμηθούν χρησιμοποιώντας τεχνικές κωδικοποίησης και ελέγχου σφαλμάτων ή τεχνικές αυτόματης επανάληψης.

3.7.4 Επιθέσεις ευρωστίας

Αυτός ο τύπος επίθεσης στα ασύρματα δίκτυα συνεπάγεται κυρίως προσβολή της λειτουργικότητας του συστήματος επικοινωνίας. Οι μεγάλες επιθέσεις ευρωστίας είναι συνήθως επιθέσεις άρνησης εξυπηρέτησης (DoS). Μια επίθεση DoS στοχεύει στην εξάντληση των πόρων του δικτύου για τη διακοπή της επικοινωνίας μεταξύ των νόμιμων χρηστών. Η εμπλοκή είναι ο πιο συχνά παρατηρούμενος τύπος επίθεσης DoS. Οι επιθέσεις DoS μπορούν επίσης να εκτελεστούν από πολλούς κατανεμημένους αντιπάλους για να μειώσουν την πιθανότητα ανίχνευσής τους και ονομάζονται ως κατανεμημένες επιθέσεις DoS (DDoS) και θεωρούνται ως ένα από τα πιο δύσκολα ζητήματα ασφάλειας στα σημερινά συστήματα επικοινωνίας.

Τα αντίμετρα των επιθέσεων DoS ή DDoS δεν είναι ξεκάθαρα καθώς οι επιθέσεις αυτές μπορούν να εκτελεστούν με διάφορους τρόπους. Χρησιμοποιούνται συστήματα ανίχνευσης ανωμαλιών για να προσδιορίσουν εάν υπάρχει επίθεση σε οποιονδήποτε από τους πόρους του δικτύου. Προκειμένου να αποφευχθεί η ανίχνευση των DoS, χρησιμοποιείται συνήθως ένας εφεδρικός πόρος από τον

επιτιθέμενο. Εάν εντοπιστεί μια επίθεση DoS, ο κόμβος του ελεγκτή δικτύου συνήθως αποτρέπει τους αντιπάλους, εμποδίζοντας τη χρήση των πόρων τους. Μια άλλη προσέγγιση για την ενίσχυση της ευρωστίας ενός συστήματος είναι η διαφοροποίηση των πόρων του δικτύου με τη χρήση εφεδρικών πόρων. Αυτοί οι εφεδρικοί πόροι μπορούν να χρησιμοποιηθούν εάν ένας πόρος υποστεί επίθεση. Για παράδειγμα, αν ανιχνευτεί jammer, το ασύρματο δίκτυο μπορεί να αλλάξει σε διαφορετική συχνότητα για να αποφευχθούν χειρότερα αποτελέσματα (Πανέτσος, 2007).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Blossom, E. GNU software radio. http://www.gnu.org/software/gnuradio/.

Bolle, R., Connell, J., Pankanti, S., Ratha, N., AND SENIOR, a. Guide to Biometrics. Springer, 2003.

Chrysikos, (2009). Theofilos Chrysikos and Stavros Kotsopoulos, “Impact of channel-dependent variation of path loss exponent on Wireless Information-Theoretic Security”, Wireless Telecommunications Symposium 2009 (WTS ‘09), April 22-24, 2009, Prague, Czech Republic.

Chrysikos, (2010). Konstantinos Birkos, Theofilos Chrysikos, Stavros Kotsopoulos and Ioannis Maniatis, “Security and Quality of Service in Wireless Networks”, Book chapter in Handbook on Communication and Information Security, Springer, 2010.

Danev, B., Heydt-Benjamin, T. S., and Capkun, S. Physical-layer identification of RFID devices. In Proc. USENIX Security Symposium (2009).

Edman, M., AND Yener, B. Active attacks against modulation-based radiometric identification. TR 09-02, Rensselaer Institute of Technology, Aug. 2009.

Fingeprint verification competitions (FVC). http://bias.csr.uni-bo.it/fvc2006/.

O.Ureten, and N.Serinken. Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering 32, 1 (Winter 2007).

Κομνηνός, Θόδωρος Π. Σπυράκης , Παύλος Γ. , ‘Ασφάλεια δικτύων & υπολογιστικών συστημάτων : αναχαιτίστε τους εισβολείς’, 2002.

Πανέτσος Σ., ‘Επικοινωνίες & Δίκτυα Υπολογιστών’, εκδόσεις Τζιόλα, Θεσσαλονίκη 2007.

ΚΕΦΑΛΑΙΟ 4: ΠΛΑΝΟ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΙΝΔΥΝΩΝ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ

4.1 Ασφάλεια στο GSM (Παγκόσμιο Σύστημα Κινητών Επικοινωνιών)

Η κύρια πρόκληση για το GSM ήταν να εξασφαλίσει ότι το δίκτυο πρόσβασης καθώς το βασικό δίκτυο θα μπορούσε εύκολα να είναι προσβάσιμο. Ο ραδιοσύνδεσμος αποδείχθηκε πράγματι το πιο αδύναμο μέρος του δικτύου και υπήρχαν πολλοί τρόποι υποκλοπής μέσω συγκεκριμένου εξοπλισμού (Wyner, 1975).

Από την άλλη πλευρά, με το GSM ξεκίνησε η ψηφιακή εποχή στις τηλεπικοινωνίες. Αυτό σημαίνει ότι εισήχθησαν νέα χαρακτηριστικά, όπως η κωδικοποίηση ομιλίας, η ψηφιακή διαμόρφωση, η μετάβαση συχνότητας και η πολλαπλή πρόσβαση χρονικού διαχωρισμού (Time Division Multiple Access - TDMA). Υπό αυτές τις συνθήκες, η υποκλοπή έγινε πολύ πιο δύσκολη από ό, τι στην αναλογική περίπτωση και οι υπεύθυνοι εκμεταλλεύτηκαν τις δυνατότητες που προσφέρει η ψηφιακή τεχνολογία να κάνει το σύστημα εξαιρετικά ισχυρό σε πολλές περιπτώσεις επιθέσεων (Chrysikos et al, 2010).

Το GSM παρέχει τέσσερις βασικές υπηρεσίες ασφαλείας: (1) ανωνυμία, (2) επαλήθευση ταυτότητας, (3) σηματοδότηση δεδομένων και κρυπτογράφηση φωνής, και (4) ταυτοποίηση χρήστη και εξοπλισμού. Στο GSM, κάθε χρήστης αναγνωρίζεται από έναν μοναδικό αριθμό που περιέχεται στην κάρτα SIM (Subscriber identity module), που ονομάζεται διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI). Το IMSI είναι ένα σταθερό αναγνωριστικό που χρησιμοποιείται στις διαδικασίες διαχείρισης θέσης και στην αποτελεσματική δρομολόγηση κλήσεων και περιαγωγή. Η ανωνυμία στο GSM ασκείται με τη χρήση και ενός άλλου αναγνωριστικού εκτός από το IMSI. Αυτό το νέο αναγνωριστικό ονομάζεται προσωρινή ταυτότητα κινητού συνδρομητή (TMSI) και αποθηκεύεται επίσης στην κάρτα SIM. Ένα νέο TMSI εκδίδεται κάθε φορά που ένα κινητό τερματικό ενεργοποιείται σε μια νέα περιοχή Master Switching Center (MSC), ζητάει μια διαδικασία ενημέρωσης θέσης, προσπαθεί να πραγματοποιήσει μια κλήση ή επιχειρεί να ενεργοποιήσει μια υπηρεσία. Εφόσον έχει εκδοθεί αυτό το TMSI, αντικαθιστά το IMSI για τυχόν μελλοντικές επικοινωνίες εντός αυτού του συστήματος GSM. Από αυτό το σημείο, το IMSI δεν αποστέλλεται πλέον

μέσω του ραδιοφωνικού καναλιού και οι απαραίτητες πληροφορίες σηματοδότησης μεταξύ του MSC και του κινητού αποστέλλονται χρησιμοποιώντας το TMSI. Ως αποτέλεσμα, το IMSI προστατεύεται από τυχόν μη εξουσιοδοτημένη χρήση. Η τοποθεσία του χρήστη προστατεύεται επίσης, επειδή οι κακόβουλοι χρήστες δεν μπορούν να έχουν πρόσβαση στο IMSI και ταυτόχρονα δεν γνωρίζουν τη σχέση μεταξύ του IMSI και του TMSI.

Μετά τη διαδικασία αναγνώρισης, το επόμενο βήμα είναι η εξακρίβωση της ταυτότητας. Με τον έλεγχο ταυτότητας το κινητό αποδεικνύει ότι είναι πράγματι αυτό που αναμενόταν να είναι. Ο έλεγχος ταυτότητας προστατεύει το δίκτυο από μη εξουσιοδοτημένη χρήση. Η απλούστερη διαδικασία επαλήθευσης είναι ο κωδικός PIN τον οποίο καλείται να βάλει ο χρήστης κάθε φορά που ανοίγει το κινητό του. Το PIN που εισάγετε συγκρίνεται με το PIN που είναι αποθηκευμένο στην κάρτα SIM και αν είναι το ίδιο, επιτρέπεται η χρήση του κινητού τηλεφώνου.

Το GSM υιοθετεί ένα πολύ πιο εξελιγμένο μηχανισμό επαλήθευσης ταυτότητας. Όταν το κινητό τηλέφωνο βρίσκει ένα δίκτυο για να συνδεθεί, αποστέλλει ένα μήνυμα σύνδεσης βάσης που το εξυπηρετεί (BTS). Το BTS με τη σειρά του έρχεται σε επαφή με το MSC για να λάβει πληροφορίες σχετικά με την πρόσβαση του κινητού στο δίκτυο. Το MSC ζητά από το HLR δεδομένα για την παροχή πέντε τριπλών σειρών ασφαλείας. Κάθε τριάδα περιλαμβάνει τρεις αριθμούς: (1) έναν τυχαίο αριθμό (RAND), (2) μια υπογεγραμμένη απόκριση (SRES), και (3) ένα πλήκτρο συνόδου Kc. Εκτός από τα παραπάνω, υπάρχει ήδη κοινόχρηστο μυστικό κλειδί. Αυτό το κλειδί είναι ενσωματωμένο στην κάρτα SIM και είναι γνωστό και στο δίκτυο. Κατά συνέπεια, και η ασφάλεια της αρχιτεκτονικής βασίζεται στο γεγονός ότι μόνο οι νόμιμοι φορείς εκμετάλλευσης των δικτύων γνωρίζουν το κλειδί.

Η διαδικασία ελέγχου ταυτότητας που περιεγράφηκε προηγουμένως έχει επίσης ως αποτέλεσμα την καθιέρωση του κλειδιού συνόδου Kc , το οποίο συμβάλλει στη λειτουργία εμπιστευτικότητας της προσέγγισης ασφάλειας του GSM. Το Kc παράγεται από το Ki και το RAND χρησιμοποιώντας τον αλγόριθμο A8.

Η προστασία από μη εξουσιοδοτημένη ακρόαση ή πρόσβαση στα μεταδιδόμενα δεδομένα πραγματοποιείται μέσω κρυπτογράφησης (Maurer, 1997).

Παρά τις ιδιαίτερες λειτουργίες ασφαλείας στο GSM, υπάρχουν ορισμένα προβλήματα. Στο GSM, δεν υπάρχει πρόβλεψη για την προστασία της μεταδιδόμενης πληροφορίας. Ως αποτέλεσμα, υπάρχει πάντοτε ο κίνδυνος των επιθέσεων που αποσκοπούν στη διακοπή της επικοινωνίας. Δεύτερον, το πεδίο κρυπτογράφησης περιορίζεται μόνο στη διεπαφή ME-BTS και το κεντρικό τμήμα του δικτύου παραμένει κρυπτογραφικά ευπαθές. Μια άλλη πηγή ευπάθειας είναι το γεγονός ότι οι αλγόριθμοι κρυπτογράφησης δεν δημοσιεύονται στα πρότυπα και επομένως δεν είναι διαθέσιμοι για δημόσια εξέταση από την επιστημονική κοινότητα. Ο αλγόριθμος κρυπτογράφησης A5 που χρησιμοποιείται από το GSM θεωρείται ότι με την αυξανόμενη υπολογιστική ισχύ των σύγχρονων υπολογιστών μπορεί να γίνει μελλοντικά ευάλωτος. Ακόμα και με τη χρήση του πιο απλοϊκού τύπου επίθεσης, της επίθεσης brute force, το κλειδί κρυπτογράφησης μπορεί να βρεθεί μέσα σε μερικές ώρες. Η φάση επαλήθευσης ταυτότητας πάσχει επίσης επειδή είναι μονόδρομος ο έλεγχος ταυτότητας. Το δίκτυο μπορεί να είναι σε θέση να επαληθεύει την ταυτότητα του χρήστη, αλλά δεν υπάρχει επιλογή για τον χρήστη να επαληθεύει την ταυτότητα του δικτύου. Αυτό αφήνει ανοικτό το έδαφος για επιθέσεις στις οποίες ο επιτιθέμενος μπορεί να μεταμφιεστεί ως BTS. Τέλος, ένας άλλος τύπος επίθεσης στο GSM είναι η κλωνοποίηση SIM. Οι επιτιθέμενοι μπορούν να ανακτήσουν το κλειδί Ki από την κάρτα SIM του συνδρομητή και μπορούν να το χρησιμοποιήσουν είτε για να ακούσουν τη συνομιλία του χρήστη είτε για να κάνουν κλήσεις και να χρεώσουν τον νόμιμο χρήστη (Chrysikos et al, 2011).

4.2 Ασφάλεια στο UMTS (Τεχνολογία 3G)

Η ασφάλεια στο UMTS συνδέεται στενά με την ασφάλεια στο GSM, επειδή η τελευταία τεχνολογία είχε ήδη υιοθετήσει ορισμένα χαρακτηριστικά που ήταν γερά και δοκιμασμένα, και επίσης έπρεπε να υπάρξει κάποιο είδος διαλειτουργικότητας μεταξύ αυτών των δύο πλατφορμών, καθώς οι συνδρομητές GSM θα είναι στην πραγματικότητα οι νέοι χρήστες του 3G.

Όταν ένας κινούμενος συνδρομητής εισέρχεται σε μια περιοχή κάλυψης, του ανατίθεται ένα TMSI για να αντικαταστήσει το IMSI του για αναγνώριση και αποτελεσματική προώθηση κλήσεων. Όταν το κινητό εισέρχεται σε μια νέα περιοχή, συνεχίζει να αναγνωρίζει τον εαυτό του χρησιμοποιώντας το ίδιο TMSI. Τώρα, ο νέος κατάλογος χρηστών (VLR) δεν γνωρίζει σε ποιον απαντά αυτό το αναγνωριστικό και για το λόγο αυτό ζητάει τον παλιό VLR. Το βασικό σημείο είναι ότι ο νέος VLR δεν ανακτά το αντίστοιχο IMSI μέσω της διασύνδεσης. Αυτό συμβαίνει μόνο εάν δεν είναι δυνατή η ανάκτηση των πληροφοριών από το παλιό VLR. Στη συνέχεια ξεκινά η διαδικασία επαλήθευσης ταυτότητας και κλειδιού (AKA).

Εκτός από το IMSI και το TMSI, υπάρχει ένας άλλος αριθμός ταυτότητας που μπορεί να θέσει σε κίνδυνο τον εντοπισμό των χρηστών. Στο UMTS, έχει προστεθεί ένας αριθμός ακολουθίας (SQN) για να βοηθήσει το κινητό να επικυρώσει το δίκτυο, ένα χαρακτηριστικό που δεν υπάρχει στην περίπτωση του GSM. Το σύστημα χρησιμοποιεί ένα SQN ανά χρήστη και η ανιχνευσιμότητα του χρήστη εξαρτάται από τη δυνατότητα πρόσβασης ενός εισβολέα στο SQN.

Το νέο χαρακτηριστικό που αξίζει να παρατηρήσουμε σε σύγκριση με το GSM είναι η αμοιβαία φύση του ελέγχου ταυτότητας, καθώς τώρα και οι συνδρομητές

επαληθεύουν το δίκτυο. Η διαδικασία ελέγχου ταυτότητας ξεκινά όταν η SIM (USIM) στέλνει ένα μήνυμα σύνδεσης στο BTS από το οποίο θέλει να εξυπηρετηθεί. Το BTS ζητά από το υπεύθυνο MSC / VLR να επιτρέψει στο USIM να έχει πρόσβαση στο δίκτυο. Το MSC ζητά από την HLR να της αποστείλει ένα σύνολο δεδομένων ελέγχου ταυτότητας. Το διάνυσμα ελέγχου ταυτότητας UMTS είναι ένα σύνολο πέντε στοιχείων: (1) RAND, (2) Αναμενόμενη απόκριση (XRES), (3) ψηφιακό κλειδί (CK), (4) κλειδί ακεραιότητας (IK) και (5) Αυθεντικοποίηση (AUTN). Στην πρώτη HLR γενιά, το RAND παραγόταν μέσω μιας γεννήτριας τυχαίων αριθμών και ενός SQN. Στη συνέχεια, η HLR ζητά από το AuC να παράσχει το μυστικό κλειδί Ki που αντιστοιχεί στο συγκεκριμένο USIM. Αυτά τα τρία στοιχεία, το RAND, το SQN και το Ki μαζί με τον έλεγχο ταυτότητας (AMF) είναι τα κύρια στοιχεία ασφαλείας.

Όταν το MSC / VLR δέχεται το σύνολο των πακέτων δεδομένων, επιλέγει το πρώτο από αυτά και τα αποθηκεύει για μελλοντική χρήση. Στη συνέχεια στέλνει το RAND και το AUTN στο USIM. Όταν η USIM λάβει το RAND, αρχίζει να υπολογίζει το σωστό αποτέλεσμα για να το στείλει ως απάντηση στην προσπάθεια σύνδεσης. Το Ki είναι ήδη αποθηκευμένο στο USIM (Chrysikos et al, 2011).

Στην επόμενη φάση, το δίκτυο επικυρώνει το USIM. Το USIM στέλνει το User Authentication (RES) στο δίκτυο. Στο τέλος της διαδικασίας επαλήθευσης, έχουν δημιουργηθεί τρία κλειδιά: CK, IK και AK. Αυτά τα κλειδιά συμβάλλουν στην παροχή περαιτέρω χαρακτηριστικών που σχετίζονται με την ασφάλεια, όπως η εμπιστευτικότητα.

4.3 Ασφάλεια στο WiMAX

Δεδομένου του γεγονότος ότι το WiMAX προορίζεται για κάλυψη ευρείας περιοχής, υιοθετούνται αξιόπιστα χαρακτηριστικά ασφαλείας και πολλοί σύνθετοι μηχανισμοί ασφαλείας για την παρακολούθηση και τη μεταφορά εμπιστευτικών δεδομένων. Το πρότυπο 802.16 περιλαμβάνει ήδη ρυθμίσεις ασφαλείας.

Η αλλαγή κλειδιού κρυπτογράφησης και μεταφορά δεδομένων ζητούν τη χρήση ορισμένων συστημάτων κρυπτογράφησης. Οι αλγόριθμοι κρυπτογράφησης που υιοθετήθηκαν από το πρωτόκολλο 802.16 είναι οι: (α) RSA, (β) DES, (γ) AES, (δ) MAC (HMAC).

Το πρότυπο 802.16 χρησιμοποιεί πολλά κλειδιά κρυπτογράφησης και βασίζει το σύνολο πληροφοριών ασφαλείας σε έναν σταθμό βάσης και έναν ή περισσότερους σταθμούς συνδρομητών που υποστηρίζουν ασφαλή επικοινωνία. Οι κοινές πληροφορίες περιλαμβάνουν την κρυπτογραφική πλατφόρμα, ένα σύνολο μεθόδων για κρυπτογράφηση δεδομένων, έλεγχο ταυτότητας δεδομένων και ανταλλαγή κλειδιού κρυπτογράφησης (TEK). Υπάρχουν τρεις τύποι διαδικασιών ασφαλείας: (1) η συσχέτισης για τη μεταφορά δεδομένων unicast, (2) η ένωση ομάδων ασφάλειας (GSA) και (3) η ένωση ασφάλειας πολυμέσων για Broadcast Services (MBS) για την υπηρεσία MBS (MBSGSA).

Το κύριο πρωτόκολλο ελέγχου ταυτότητας που χρησιμοποιείται στο WiMAX είναι το πρωτόκολλο διαχείρισης πρωτεύοντος κλειδιού (PKM). Πρόκειται για πιστοποιημένο πρωτόκολλο πελάτη / διακομιστή. Ένας σταθμός βάσης επικυρώνει την έναρξη ανταλλαγής δεδομένων μέσω πιστοποίησης βάσει ψηφιακού πιστοποιητικού. Το πρωτόκολλο PKM βασίζεται στην κρυπτογραφία δημόσιου κλειδιού, η οποία εφαρμόζεται για να δημιουργηθεί ένα κοινό μυστικό μεταξύ του σταθμού βάσης και του συνδρομητή. Το PKM χρησιμοποιείται επίσης για περιοδική επανεγκατάσταση και ανανέωση κλειδιού (Baros et al, 2008).

4.4 Υλοποίηση πλάνου διαχείρισης

Η υλοποίηση ενός πλάνου διαχείρισης και αντιμετώπισης κινδύνων είναι μια σημαντική διαδικασία για κάθε οργανισμό. Σκοπός του πλάνου είναι η αποφυγή προβλέψιμων κινδύνων, η προστασία από λάθος αποφάσεις και η ελαχιστοποίηση των απωλειών και ζημιών από απρόβλεπτα γεγονότα.

Υπάρχουν πολλά διαθέσιμα συστήματα διαχείρισης και αντιμετώπισης κινδύνων που προτείνουν μια σειρά από μέτρα ασφάλειας τα οποία καλύπτουν ένα ευρύ σύνολο κινδύνων. Μεταξύ αυτών περιλαμβάνονται τόσο αυτόματοι μηχανισμοί όσο και διαδικασίες που πρέπει να ακολουθούνται από τα στελέχη του οργανισμού. Οι κατηγορίες που καλύπτονται είναι:

- Πολιτική Ασφαλείας
- Οργάνωση Ασφάλειας Πληροφοριών
- Διαχείριση Περιουσιακών Στοιχείων
- Διαχείριση Ανθρώπινων Πόρων
- Φυσική και Περιβαλλοντική Ασφάλεια
- Διαχείριση Επικοινωνιών και Λειτουργιών
- Έλεγχος Πρόσβασης
- Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
- Διαχείριση Συμβάντων Ασφάλειας Πληροφοριών
- Συμμόρφωση

Όσον αφορά την ασφάλεια των πληροφοριών στα ασύρματα υπολογιστικά συστήματα πρέπει χρησιμοποιείται ένα λειτουργικό και ενημερωμένο σύστημα Antivirus και πλήρες σύστημα Backup, καθώς και χρήση Firewall τόσο ως Hardware

όσο και ως Software. Αναπόσπαστο κομμάτι του συστήματος είναι οι έλεγχοι πρόσβασης στα δικαιώματα των χρηστών, οι έλεγχοι σε έγγραφα (Document Control) όπως ιστορικό αλλαγών ή αναθεωρήσεων, καταστροφή απαρχαιωμένου υλικού κ.α. και το σπουδαιότερο είναι να υπάρχει Πολιτική Αποκατάστασης (Disaster Recovery Policy) μετά από καταστροφή-φυσική ή μη.

Το πλάνο διαχείρισης ενός τέτοιου συστήματος εφαρμόζεται σε τέσσερις φάσεις, σε γενικές γραμμές οι φάσεις αυτές είναι οι εξής:

- Σχεδιασμός (Plan): Σε αυτήν την φάση σχεδιάζεται το όλο σύστημα, καταγράφονται όλα τα αγαθά και αναλύεται η επικινδυνότητα αυτών και επιλέγονται οι απαραίτητοι έλεγχοι.
- Εκτέλεση (Do): Εδώ συντελείται η εφαρμογή του συστήματος και των ελέγχων λειτουργίας.
- Έλεγχος (Check): Φάση στην οποία έχουμε την αντικειμενική αξιολόγηση του πλάνου αλλά και η αξιολόγηση των επιδόσεων αυτού (αποδοτικότητα και αποτελεσματικότητα).
- Ενεργοποίηση (Act): Σε αυτήν την φάση γίνονται αλλαγές όπου χρειάζονται, ώστε να βελτιστοποιηθεί το σύστημα.

Τα οφέλη που αποκομίζει ο οργανισμός με την εφαρμογή ενός τέτοιου συστήματος είναι ότι θα μειώσει τα συμβάντα σχετικά με την ασφάλεια του και επομένως θα αυξήσει και την αξιοπιστία του, εξασφαλίζοντας τα αγαθά και τα περιουσιακά στοιχεία από υποβάθμιση, απώλεια, ζημιά ή και κλοπή. Στην περίπτωση που ο οργανισμός είναι συγκεκριμένη εταιρία πρέπει να αναφέρουμε ότι συμμορφώνεται επίσης με την σχετική νομοθεσία αποκτώντας ανταγωνιστικό πλεονέκτημα, καθότι θα έχει πρόσβαση σε αγορές και πελάτες που απαιτούν υψηλά επίπεδα ασφάλειας από τους συνεργάτες τους. Και το σημαντικότερο όφελος θα είναι ότι θα έχει εξασφαλίσει την άμεση επαναφορά και λειτουργία των συστημάτων σε περίπτωση καταστροφής

μεγάλης κλίμακας, μιας και ένα μεγάλο μέρος επιθέσεων είναι δύσκολο ή ακόμα και αδύνατον να προβλεφθούν ή να αποφευχθούν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Bloch, M., Barros, J., Rodrigues, M. R. D., McLaughlin, S.W.: Wireless Information-Theoretic Security. IEEE Trans. Inf. Th. vol. 54, no. 6, 2515--2534 (2008)

Chrysikos, (2009). Theofilos Chrysikos, Giannis Georgopoulos and Stavros Kotsopoulos, “Empirical Calculation of Shadowing Deviation for Complex Indoor Propagation Topologies at 2.4 GHz”, International Conference on Ultra Modern Telecommunications (ICUMT 2009), October 12-14, 2009, St. Petersburg, Russia.

Chrysikos, (2011). Theofilos Chrysikos, Tasos Dagiuklas and Stavros Kotsopoulos, “Wireless Information-Theoretic Security in an Outdoor topology with Obstacles: Theoretical Analysis & Experimental Measurements”, EURASIP Journal on Wireless Communications and Networking, Special Issue on Security and Resilience for Smart Devices and Applications.

Maurer, U. M., Wolf S.: Information-theoretic key agreement: from weak to strong secrecy for free. In: Advances in Cryptology - EUROCRYPT 2000, LNCS, vol. 1807, pp. 351-368, Springer-Verlag, Heidelberg (2000)

Maurer, U. M.: Information-theoretically secure secret-key agreement by NOT authenticated public discussion. In: Advances in Cryptology - EUROCRYPT '97, LNCS, vol. 1233, pp. 209--225, Springer-Verlag, Heidelberg (1997)

Wyner, A. D.: The wire-tap channel. Bell Tech. J. 54, 1355-1387, (1975)

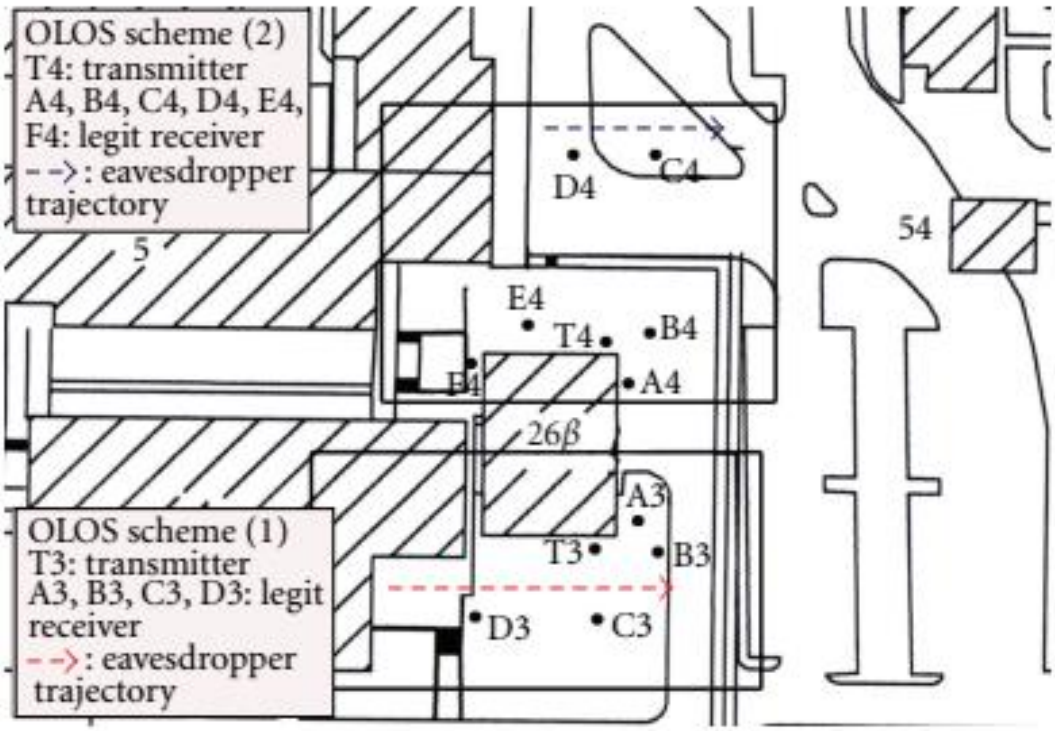
ΚΕΦΑΛΑΙΟ 5: ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ

5.1 Εισαγωγή

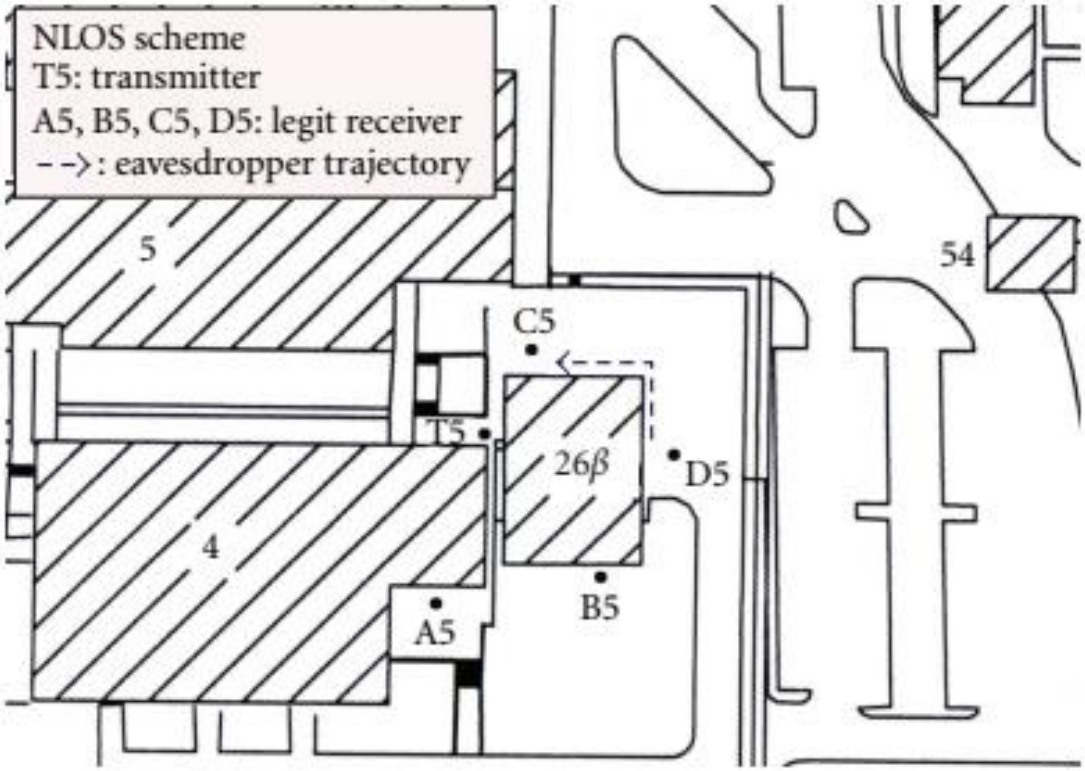
Η ασφάλεια έχει τις τελευταίες δεκαετίες βασικό ρόλο στις ασύρματες επικοινωνίες. Τα πρόσφατα δημοσιευθέντα έργα ανανέωσαν το ενδιαφέρον των ερευνητών για την ασφάλεια φυσικού επιπέδου, διαμορφώνοντας την έννοια Wireless Information-

Theoretic Security (WITS), ανοίγοντας το δρόμο για καρποφόρες προόδους τόσο στον ακαδημαϊκό χώρο όσο και στον τεχνολογικό κλάδο. Η θεωρητική ασφάλεια υποδηλώνει ότι η τέλεια μυστικότητα στην ασύρματη επικοινωνία μεταξύ ενός πομπού και ενός νόμιμου δέκτη παρουσία ενός υποκλοπέα (παθητικός εισβολέας) είναι εφικτή ακόμη και όταν ο μέσος λόγος σήματος προς θόρυβο (SNR) στο κύριο δίαυλο (που είναι εγκατεστημένος μεταξύ του πομπού και του νόμιμου δέκτη) είναι μικρότερος από το μέσο SNR του καναλιού που δημιουργείται μεταξύ του πομπού και του ηχογράφου, εάν αμφότερα τα κανάλια θεωρούνται ότι χαρακτηρίζονται από κατακρήμνιση Rayleigh. Έτσι, μπορούμε να παρακάμψουμε τον περιορισμό του μοντέλου καναλιού Gaussian wiretap, σύμφωνα με το οποίο το μέσο SNR του κύριου καναλιού πρέπει να είναι μεγαλύτερο από αυτό του καναλιού τηλεχειρισμού, προκειμένου να καθιερωθεί η τέλεια μυστικότητα.

Στην παρούσα εργασία, η WITS έχει προσδιοριστεί σε αυτόνομα δίκτυα εξετάζοντας το φαινόμενο Rayleigh στα κανάλια. Επιπλέον, έγινε μια σειρά από μετρήσεις θεωρητικής ασφάλειας, στην πιθανότητα μετακινούμενων χρηστών σε αυτόνομα δίκτυα. Δημιουργήθηκε ένα ad hoc δίκτυο, το οποίο αποτελείται από αυτόνομους χρήστες (φορητοί υπολογιστές που συνδέονται μέσω προσαρμογέων 802.11n) που μετακινούνται σε χαμηλής ταχύτητας τρόπο (απορρίπτοντας έτσι πιθανά φαινόμενα Doppler). Οι μέσοι SNRs τόσο του κύριου όσο και του δευτερεύοντος καναλιού υπολογίστηκαν μέσω κατάλληλου εξοπλισμού προκειμένου να αξιολογηθεί η θεωρητική ασφάλεια σε ένα πραγματικό υπαίθριο περιβάλλον με εμπόδια OLOS και Non-Line-of-Sight (NLOS). Τα αποτελέσματα κατέδειξαν σημαντική επίδραση της σχετικής θέσης του χρήστη στην αξιοπιστία WITS ως λύση φυσικής ασφάλειας.



Σχήμα 5.1 Διάταξη με εμπόδια της μορφής OLOS



Σχήμα 5.2 Διάταξη με εμπόδια της μορφής NLOS

Για τους απαραίτητους υπολογισμούς θα χρησιμοποιηθούν οι παρακάτω εξισώσεις:

$$P(C_s > 0) = \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}.$$

$$P(C_s > 0) = \frac{1}{1 + (d_M/d_W)^n}.$$

$$dR = \left(\frac{d'_M/d'_W}{d_M/d_W}\right) = \frac{d'_M d_W}{d_M d'_W} = \frac{d_W}{d'_W},$$

$$d'_W = d_W - u\Delta t.$$

$$\frac{1}{dR} = \frac{d'_W}{d_W} = \sqrt{\frac{(1 - P(C_s > 0))P(C_s > 0)'}{\left(1 - P(C_s > 0)'\right)P(C_s > 0)}},$$

$$C'_{\text{out}}(p) = \log_2\left(\frac{p + 1/\overline{\gamma}_M}{dR^2\left(\left(p + 1/\overline{\gamma}_M\right)/2^{Rs} - 1/\overline{\gamma}_M\right) + 1/\overline{\gamma}_M}\right)$$

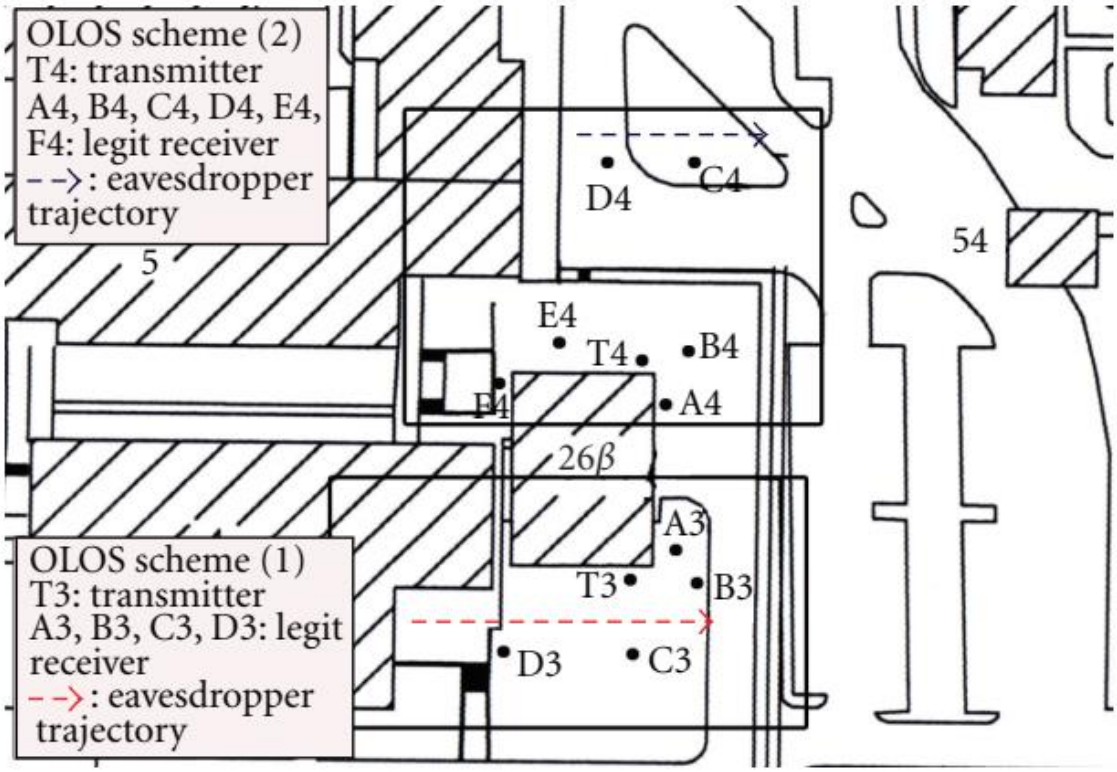
5.2 Μεθοδολογία

Μετακινούμενοι χρήστες σε αυτόνομο δίκτυο

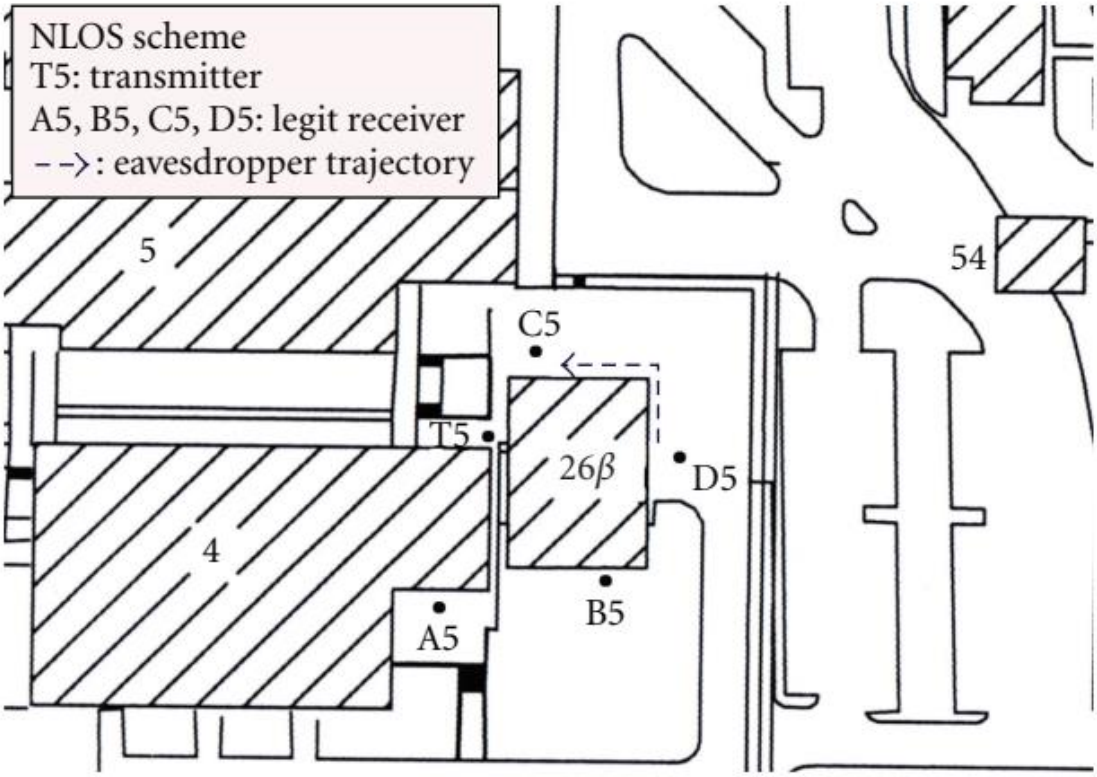
Οι ad hoc κόμβοι χρησιμοποιούν ένα μοντέλο κινητικότητας που προσομοιώνει τις κρίσιμες καταστάσεις αποστολής δεδομένων. Τα φυσικά εμπόδια αποτελούν αναπόσπαστο μέρος της υπό μελέτη περιοχής. Τα σημεία προορισμού επιλέγονται από τους κόμβους που βασίζονται τυχαία στην κανονική κατανομή. Κάθε κόμβος μπορεί να μετακινηθεί σε κάθε σημείο της περιοχής του δικτύου, εφόσον δεν βρίσκεται μέσα στα όρια ενός εμποδίου. Όταν επιλέγεται ένα σημείο προορισμού, ο κόμβος κινείται γύρω από τα εμπόδια ακολουθώντας μια διαδικασία αναδρομής. Εάν υπάρχει εμπόδιο στον κόμβο, ο κόμβος θέτει ως επόμενο ενδιάμεσο προορισμό του την κορυφή της άκρης του εμπόδιου που είναι άμεσα ορατή που είναι πλησιέστερα προς τον προορισμό και επαναλαμβάνει την ίδια διαδικασία ξανά με αρχικό σημείο την αρχική θέση και τον προορισμό του επιλεγμένου χρήστη. Διαφορετικά, ο κόμβος ακολουθεί αυτή την απευθείας γραμμή για να φτάσει στον επιθυμητό προορισμό.

Για τους σκοπούς των πειραματικών μετρήσεων δημιουργήθηκε ένα δίκτυο οχημάτων που αποτελείται από τρεις χρήστες. Τρεις φορητοί υπολογιστές εξοπλισμένοι με ενσωματωμένους ασύρματους προσαρμογείς 802.11n δημιούργησαν ένα ad hoc δίκτυο: ο πρώτος φορητός υπολογιστής λειτούργησε ως πομπός, ο δεύτερος φορητός υπολογιστής ήταν ο νόμιμος δέκτης και ο τρίτος φορητός υπολογιστής ήταν ο μη νόμιμος χρήστης που ηχογραφούσε τη συνομιλία.

5.3 Μετρήσεις



Σχήμα 5.1 Τοπολογία OLOS



Σχήμα 5.2 Τοπολογία NLOS

Σε αυτό το υποκεφάλαιο θα παρουσιάσουμε πειραματικές μετρήσεις από έρευνες των Chrysikos et al. (2011) για υποκλοπή ασύρματης επικοινωνίας σε εξωτερικό χώρο. Οι διατάξεις που χρησιμοποιήθηκαν στην ερευνα φαίνονται στα σύο παραπάνω σχήματα. Ο Πίνακας 5.1 απεικονίζει τα μέσα επίπεδα λαμβανόμενης ισχύος και το SNR για όλες τις νόμιμες θέσεις δέκτη (κύριο κανάλι), ενώ ο Πίνακας 2 παρουσιάζει τις υπολογισμένες τιμές για την πιθανότητα υποκλοπής. Οι μέσες τιμές λαμβανόμενης ισχύος ελήφθησαν μέσω του λογισμικού NetStumbler τόσο για το νόμιμο δέκτη όσο και για τον υποκλοπέα.

OLOS T3	Pr (nW)	Pr (dBm)	SNR (dB)
A3 (main)	1,26	-59	26
B3 (main)	0,32	-65	20
C3 (main)	0,03162	-75	10
D3 (main)	0,03162	-75	10
X31 (eaves)	0,00631	-82	3
X32 (eaves)	0,5	-63	22
X33 (eaves)	0,5	-63	22
X33 (eaves)	10	-65	20
X35 (eaves)	2,51	-56	29
X36 (eaves)	1,58	-58	27

Πίνακας 5.1 Μέση λήψη ισχύος και SNR για το σύστημα OLOS-1 (T3)

Pr legit. (nW)	Pr eaves. (nW)	SNR ratio	P(Cs > 0)
1,26	0,00631	0,005007937	0,995
1,26	0,5	0,396825397	0,716
1,26	0,5	0,396825397	0,716
1,26	10	7,936507937	0,112
1,26	2,51	1,992063492	0,334
1,26	1,58	1,253968254	0,444
0,32	0,00631	0,01971875	0,981
0,32	0,5	1,5625	0,390
0,32	0,5	1,5625	0,390
0,32	10	31,25	0,031
0,32	2,51	7,84375	0,113

0,32	1,58	4,9375	0,168
0,03162	0,00631	0,199557242	0,834
0,03162	0,5	15,81277672	0,059
0,03162	0,5	15,81277672	0,059
0,03162	10	316,2555345	0,003
0,03162	2,51	79,38013915	0,012
0,03162	1,58	49,96837445	0,020

Πίνακας 5.2 Οι υπολογισμένες τιμές για την πιθανότητα υποκλοπής

Η μέση τιμή SNR τόσο για το κύριο κανάλι όσο και για το δευτερεύον κανάλι υπολογίστηκε λαμβάνοντας υπόψη το επίπεδο παρεμβολών θορύβου -85 dBm (για όλα τα συστήματα), με βάση τα υπάρχοντα εμπορικά συστήματα (802.11g Wi-Fi) που λειτουργούν με την ίδια συχνότητα σε ad hoc δίκτυο 802.11n εντός εμβέλειας. Ο περιβαλλοντικός θόρυβος θεωρήθηκε -98 dBm (για όλα τα συστήματα).

Όπως φαίνεται από τα αποτελέσματα, τα μέσα επίπεδα λαμβανόμενης ισχύος είναι στην κλίμακα nW. Η μέση τιμή SNR τόσο για το κύριο κανάλι όσο και για το δευτερεύον κανάλι κυμαίνεται από λίγα dB πάνω από το μηδέν μέχρι σχεδόν τα 30 dB. Συνεπώς, οι υπολογισθείσες τιμές της πιθανότητας μη φυσιολογικής (αυστηρά θετικής) διακύμανσης κυμαίνονται από τη χειρότερη περίπτωση (τιμή 0,003), όπου το σύστημα WITS παραβιάζεται σε μεγάλο βαθμό (γM yW), μέχρι 0,995.

Όπως και στην περίπτωση του σχεδίου OLOS-1 (T3), τα μέσα επίπεδα λαμβανόμενης ισχύος παραμένουν στην κλίμακα nW, με ελαφρώς χαμηλότερες τιμές από την πρώτη περίπτωση. Αυτό είναι εμφανές στις νόμιμες θέσεις δέκτη B4, C4, D4 και E4. Όπως και

στο πρώτο σχέδιο OLOS για τη θέση A3, οι θέσεις A4 και F4 θεωρούνται ότι βρίσκονται πίσω από την επιφάνεια του κτιρίου σε σχέση με τον πομπό.

Εξετάστηκαν τρεις διαφορετικές περιπτωσιολογικές μελέτες σε σενάριο OLOS / NLOS για ένα αυτόνομο δίκτυο κινητών κόμβων χαμηλής ταχύτητας (φορητοί υπολογιστές συνδεδεμένοι μέσω δικτύου ad hoc 802.11n). Τα επίπεδα πρόσθετου θορύβου και παρεμβολής θεωρήθηκαν ότι είναι -85 dBm για όλα τα σενάρια, με βάση την παραδοχή περιβαλλοντικού θορύβου -98 dBm και καταγράφηκαν παρεμβολές από άλλα λειτουργικά δίκτυα 802.11g στην ίδια συχνότητα (2.4 GHz) εντός εύρους. Το λογισμικό NetStumbler χρησιμοποιήθηκε για την απόκτηση μέσων επιπέδων λαμβανόμενης ισχύος.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παροχή ασφάλειας στην ασύρματη επικοινωνία είναι μια δύσκολη εργασία. Σε αυτή την εργασία, εστιάσαμε στην ασφάλεια στο φυσικό επίπεδο. Για αυτό το λόγο θα γίνουν κάποιες τελικές παρατηρήσεις προτάσεις για την καλύτερη δυνατή ασφάλεια φυσικού επιπέδου.

Πώς γίνεται ανίχνευση ενός προβλήματος στο δίκτυο;

Για να αυξηθεί η ασφάλεια, η λήψη πληροφοριών είναι ίσως ο σημαντικότερος τομέας. Ενώ ορισμένες από τις πληροφορίες πλαισίου, όπως η πυκνότητα των χρηστών, είναι εύκολο να εντοπιστούν μέσω των διαθέσιμων τεχνικών ανίχνευσης, για ορισμένες από αυτές, είναι δύσκολο έργο. Όπως αναφέρθηκε προηγουμένως, σε ειδικές περιπτώσεις, όπως όταν η χώρα βρίσκεται σε μάχη και ο στρατός πρέπει να χρησιμοποιήσει τους σταθμούς και τις συχνότητες για την επικοινωνία, είναι εξαιρετικά κρίσιμο να ληφθούν άμεσα οι πληροφορίες στην περίπτωση υποκλοπής. Εάν υπάρχει ανάγκη απόκτησης ορισμένων παραμέτρων από τα ανώτερα επίπεδα για την ανίχνευση των πληροφοριών πλαισίου, θα έπρεπε να συνεργάζεται ο σταθμός εκπομπής με αυτά τα επίπεδα. Η συνεργασία μεταξύ των επιπέδων αποτελεί επίσης αντικείμενο αναπτυσσόμενων τεχνικών.

Πως μπορεί να επιτευχθεί προστασία των κινούμενων δεδομένων;

Όπως αναφέρθηκε, ενδέχεται να χρειαστούν λεπτομερείς αναφορές για την προσαρμογή του επιπέδου ασφάλειας. Για παράδειγμα, ο αριθμός των χρηστών σε σχέση με την χρήση πόρων μπορεί να είναι ένας λόγος που μπορεί να μην απαιτεί

υψηλό επίπεδο ανάλυσης, αλλά ως πληροφορία μπορεί να χρησιμοποιηθεί για την ανίχνευση επιτιθέμενων.

Πως πρέπει να γίνεται σωστά η κατανομή των πόρων;

Υπάρχουν πολλές μελέτες για την εξασφάλιση της επικοινωνίας στο φυσικό επίπεδο, οι περισσότερες από τις οποίες επικεντρώνονται σε συγκεκριμένες περιστάσεις. Πρέπει επίσης να ληφθεί υπόψη η ικανότητα προσαρμογής μιας συγκεκριμένης τεχνικής για την αλλαγή των αναγκών ασφαλείας. Για παράδειγμα, η ισχύς μετάδοσης μπορεί να είναι ένας περιοριστικός παράγοντας για ορισμένους χρήστες, οι οποίοι θα μπορούσαν να περιορίσουν την ευελιξία του επιπέδου ασφαλείας σε τεχνικές που βασίζονται σε τεχνητό θόρυβο. Επίσης, το συνολικό διαθέσιμο εύρος ζώνης πρέπει να λαμβάνεται υπόψη κατά την εφαρμογή μιας στρατηγικής ασφαλείας (http://www.itgovernance.co.uk).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Agilent. *Digital Signal Analyzer (DSA) 90804A,* 2008. http://www.home.agilent.com/.

Bishop, C. *Pattern Recognition and Machine Learning*. Springer, 2006.

Bloch, M., Barros, J., Rodrigues, M. R. D., McLaughlin, S.W.: *Wireless Information-Theoretic Security. IEEE Trans*. Inf. Th. vol. 54, no. 6, 2515--2534 (2008)

Blossom, E. GNU software radio. http://www.gnu.org/software/gnuradio/.

Bolle, R., Connell, J., Pankanti, S., Ratha, N., AND SENIOR, a. *Guide to Biometrics.* Springer, 2003.

Brik, V., Banerjee, S., Gruteser, M., and Oh, S. Wireless device identification with radiometric signatures. In *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)* (2008).

Chrysikos, T., Dagiuklas, T., Kotsopoulos, S.: *Wireless Information-Theoretic Security for Moving Users in Autonomic Networks*. In: IFIP Wireless Days 2010, pp. 1-5. IEEE Press, New York (2010)

Chrysikos, T., Dagiuklas, T., Kotsopoulos, S: *Wireless Information-Theoretic Security in an Outdoor Topology with Obstacles: Theoretical Analysis & Experimental Measurements. EURASIP Journal on Wireless Communications and Networking, Special Issue on Security and Resilience for Smart Devices and Applications*, doi: 10.1155/2011/628747 (2011)

Danev, B., AND Capkun, S. Transient-based identification of wireless sensor nodes. In *Proc. ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)* (2009).

Danev, B., Heydt-Benjamin, T. S., and Capkun, S. Physical-layer identification of RFID devices. In *Proc. USENIX Security Symposium* (2009).

Edman, M., AND Yener, B. Active attacks against modulation-based radiometric identification. TR 09-02, Rensselaer Institute of Technology, Aug. 2009.

Fingeprint verification competitions (FVC). http://bias.csr.uni-bo.it/fvc2006/.

ISO/IEC, 17799 Code of Practice for Information Security Management, Geneva, Switzerland, 2000.

Maurer, U. M., Wolf S.: *Information-theoretic key agreement: from weak to strong secrecy for free.* In: Advances in Cryptology - EUROCRYPT 2000, LNCS, vol. 1807, pp. 351-368, Springer-Verlag, Heidelberg (2000)

Maurer, U. M.: *Information-theoretically secure secret-key agreement by NOT authenticated public discussion*. In: Advances in Cryptology - EUROCRYPT '97, LNCS, vol. 1233, pp. 209--225, Springer-Verlag, Heidelberg (1997)

O.Ureten, and N.Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering 32,* 1 (Winter 2007).

Wyner, A. D.: *The wire-tap channel*. Bell Tech. J. 54, 1355-1387, (1975)

Κομνηνός, Θόδωρος Π. Σπυράκης , Παύλος Γ. , 'Ασφάλεια δικτύων & υπολογιστικών συστημάτων : αναχαιτίστε τους εισβολείς', 2002.

Πανέτσος Σ., 'Επικοινωνίες & Δίκτυα Υπολογιστών', εκδόσεις Τζιόλα, Θεσσαλονίκη 2007.