Μεταπτυχιακή Εργασία

Ασφάλεια σε Ασύρματα Τοπικά Δίκτυα

Φωτεινή Γραμουσένη

Επιβλέπων Καθηγητής:
Λέανδρος Τασιούλας

Μ.Ε. 2

Νοέμβριος 2001

Δίκτυα
Ασφάλεια σε Υπολογιστικά Δίκτυα

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Ακόμη και σε χώρους με την πιο εξελιγμένης τεχνολογίας εγκατάσταση καλωδίων οι δυνατότητες που προσφέρει ένα Ασύρματο Τοπικό Δίκτυο (Wireless Local Area Network – WLAN) είναι ασύγκριτες σε σχέση με ένα ενσύρματο LAN. Το κύριο πλεονέκτημά του είναι η κινητικότητα (mobility) που προσφέρει. Ο χρήστης μπορεί να έχει πρόσβαση στο δίκτυο όπου κι αν βρίσκεται, είτε πρόκειται για εσωτερικό είτε για εξωτερικό χώρο. Η διάρθρωση της παρούσας εργασίας είναι η εξής.

Στο Κεφάλαιο 1 περιγράφονται οι ομοιότητες και οι διαφορές που υπάρχουν μεταξύ των ενσύρματων LAN και των WLAN και αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα του καθενός. Στη συνέχεια, αναλύονται τα κριτήρια βάσει των οποίων πρέπει να επιλέγουμε ένα WLAN και παρουσιάζονται τα σημαντικότερα WLAN πρότυπα που έχουν αναπτυχθεί μέχρι σήμερα. Τέλος γίνεται μια σύγκριση μεταξύ των προτύπων αυτών και περιγράφονται τα πλεονεκτήματα και τα μειονεκτήματα του καθενός.

Το Κεφάλαιο 2 εστιάζει στο επικρατέστερο πρότυπο, το IEEE 802.11. Αναλύονται κάποιες βασικές έννοιες, απαραίτητες για την κατανόηση της λειτουργίας του, περιγράφεται η αρχιτεκτονική του και αναφέρονται οι βασικές υπηρεσίες του MAC επιπέδου.

Μία από αυτές τις υπηρεσίες, η ασφάλεια, θα απασχολήσει τα επόμενα κεφάλαια. Στο Κεφάλαιο 3 αναλύονται οι απαιτήσεις πού πρέπει να ικανοποιούνται για να θεωρείται ένα WLAN ασφαλές και παρουσιάζονται οι τρόποι με τους οποίους προσπαθεί το 802.11 να το πετύχει αυτό. Ο πρώτος τρόπος βασίζεται σε έναν μοναδικό αριθμό (SSID) που αντιστοιχεί σε κάθε υποδίκτυο, ο δεύτερος στηρίζεται στις MAC διευθύνσεις των κινούμενων χρηστών και ο τρίτος (και πιο ασφαλής) στον αλγόριθμο WEP. Η διαδικασία μάλιστα της πιστοποίησης με τη χρήση του WEP προσομοιώθηκε και μελετήθηκε στα πλαίσια αυτής της εργασίας.

Στο Κεφάλαιο 4 αναλύονται τα προβλήματα και οι αδυναμίες που έχει ο μηχανισμός της πιστοποίησης. Τα προβλήματα αυτά αφορούν την κατανομή και διαχείριση του κοινού κλειδιού, τον τρόπο ανταλλαγής των μηνυμάτων της πιστοποίησης (Πρόκληση-Απάντηση), την εμπιστευτικότητα και ακεραιότητα των δεδομένων και τον έλεγχο πρόσβασης. Το κατά πόσο είναι εφικτή η πραγματοποίηση επιθέσεων που βασίζονται στα παραπάνω προβλήματα μελετήθηκε πειραματικά και παρουσιάζονται τα αποτελέσματα αυτής της μελέτης.

Τέλος, στο Κεφάλαιο 5 προτείνονται κάποιες λύσεις στα παραπάνω προβλήματα και αναφέρονται οι προτάσεις κάποιων μελών της ομάδας εργασίας του IEEE 802.11.

ΚΕΦΑΛΑΙΟ 1

ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

1.1 Ασύρματα Τοπικά Δίκτυα (WLAN)

Η κατασκευή μικροεπεξεργαστών με χαμηλές απαιτήσεις ενέργειας, η βελτίωση της ποιότητας των οθονών και η τεχνολογία των μπαταριών έχουν ως αποτέλεσμα την κατασκευή πολύ ισχυρών φορητών προσωπικών υπολογιστών. Έχει μάλιστα αναπτυχθεί μια ακόμη μικρότερη κατηγορία προϊόντων οι Προσωπικοί Ψηφιακοί Βοηθοί (Personal Digital Assistants - PDAs). Έτσι, ολοένα και περισσότεροι εργαζόμενοι προτιμούν τη χρήση των φορητών υπολογιστών και νέες ανάγκες δημιουργούνται.

Οι χρήστες έχουν την ανάγκη να μετακινούνται στο χώρο εργασίας τους χωρίς να περιορίζονται από καλώδια δικτύου και ισχύος. Από την άλλη απαιτούν γρήγορη πρόσβαση στις πληροφορίες. Αυτά τα νέα δεδομένα έχουν εισάγει νέες απαιτήσεις για την ανάπτυξη των τοπικών δικτύων, μερικές από τις οποίες είναι οι υψηλότεροι ρυθμοί μετάδοσης, οι πιο αξιόπιστες υπηρεσίες κλπ.

Ένα ασύρματο τοπικό δίκτυο (Wireless LAN - WLAN) είναι ένα σύστημα μετάδοσης δεδομένων, το οποίο είναι σχεδιασμένο για να παρέχει πρόσβαση σε ένα δίκτυο ανεξάρτητα από τη θέση της υπολογιστικής συσκευής. Η μετάδοση των δεδομένων δε γίνεται μέσω κάποιας καλωδιακής εγκατάστασης, αλλά χρησιμοποιούνται τα ραδιοκύματα για το σκοπό αυτό. Σε μεγάλες εταιρείες τα WLAN χρησιμοποιούνται συνήθως ως ο σύνδεσμος ανάμεσα σε ένα υπάρχον ενσύρματο δίκτυο και σε ένα σύνολο από υπολογιστές-πελάτες, παρέχοντάς τους ασύρματη πρόσβαση στους πόρους και τις υπηρεσίες του δικτύου της εταιρείας.

Τα WLAN θα αποτελέσουν στο μέλλον τη βασική λύση για τη δικτύωση των περισσότερων επιχειρήσεων. Η ασύρματη αγορά επεκτείνεται ραγδαία, καθώς οι επιχειρήσεις ανακαλύπτουν τα πλεονεκτήματά της. Τα κέρδη της βιομηχανίας των ασύρματων LAN ξεπερνούσαν τα 300 εκατομμύρια δολάρια το 1998 και μέχρι το 2005 προβλέπεται να φτάσουν στο 1.6 δισεκατομμύριο δολάρια. Τα πρώτα WLAN αναπτύ-

χθηκαν σε βιομηχανικές εγκαταστάσεις, σε αποθήκες και σε μεγάλα καταστήματα. Σήμερα χρησιμοποιούνται εκτός από τα γραφεία εταιρειών και στα νοσοκομεία, όπου για το προσωπικό μπορεί να απαιτείται η πρόσβαση στα στοιχεία των ασθενών ενώ είναι σε κίνηση, σε αεροδρόμια, σε περιοχές κατασκευής έργων και σε πανεπιστήμια.

Έχουν αναπτυχθεί διάφορα πρωτόκολλα για να επιτευχθεί η επικοινωνία των ασύρματων τοπικών δικτύων. Για να γίνουν όμως γενικά αποδεκτά τα WLAN πρέπει να υπάρξει ένα κοινό πρότυπο για όλους τους κατασκευαστές, ώστε να εξασφαλιστεί η συμβατότητα και η αξιοπιστία των προϊόντων, ένα πρόβλημα για το οποίο προς το παρόν δεν έχει βρεθεί λύση.

1.2 Ομοιότητες και διαφορές με τα ενσύρματα LAN

Ομοιότητες

Ένα WLAN πρέπει να είναι παρόμοιο με ένα ενσύρματο τοπικό δίκτυο. Δηλαδή πρέπει να μπορεί να υποστηρίζει όλα τα πρωτόκολλα και εργαλεία διαχείρισης ενός ενσύρματου LAN.

Πρέπει να έχει σχεδιαστεί με κατάλληλη διεπαφή (interface) ώστε τα επίπεδα που υπάρχουν πάνω από το επίπεδο Ελέγχου Λογικής Ζεύξης (Logical Link Control – LLC) να μη μπορούν να καταλάβουν το είδος του δικτύου που μεταφέρει τα δεδομένα τους, δηλαδή αν πρόκειται για ενσύρματο ή ασύρματο δίκτυο.

Διαφορές

Δύο είναι οι σημαντικότερες διαφορές ανάμεσα στα ενσύρματα και τα ασύρματα LAN. Η πρώτη είναι φυσικά το γεγονός ότι δεν υπάρχουν καλώδια, εφόσον το μέσο μετάδοσης είναι ο αέρας, ενώ η δεύτερη αφορά την κινητικότητα (mobility), η οποία είναι πλέον εφικτή λόγω της έλλειψης καλωδίων. Σ' αυτές τις διαφορές οφείλονται τόσο τα πλεονεκτήματα, όσο και τα μειονεκτήματα των WLAN.

Το φυσικό επίπεδο που χρησιμοποιούν τα WLAN είναι διαφορετικό από αυτό των ενσύρματων δικτύων. Πιο συγκεκριμένα:

- Χρησιμοποιούν μέσο το οποίο δεν έχει ούτε απόλυτα, ούτε ορατά όρια, έξω από τα οποία οι σταθμοί με συμβατούς πομποδέκτες φυσικού επιπέδου δεν είναι ικανοί να λάβουν πλαίσια του δικτύου.
- Δεν προστατεύονται από εξωτερικά σήματα.
- Επικοινωνούν πάνω από ένα μέσο λιγότερο αξιόπιστο από τα καλώδια των ενσύρματων LAN.
- Έχουν δυναμική τοπολογία.
- Δεν έχουν πλήρη συνδεσιμότητα, επομένως η υπόθεση που γίνεται συνήθως ότι ο κάθε σταθμός μπορεί να ακούσει κάθε άλλο σταθμό δεν είναι σωστή (π.χ. κάποιοι σταθμοί μπορεί να «κρύβουν» ο ένας τον άλλο).

- Έχουν ιδιότητες διάδοσης που μεταβάλλονται με το χρόνο και δεν είναι συμμετρικές.

Εξαιτίας των περιορισμών στις ακτίνες του φυσικού επιπέδου, τα ασύρματα LAN που πρέπει να καλύψουν λογικές γεωγραφικές αποστάσεις μπορούν να δημιουργηθούν από βασικά στοιχεία που καλύπτουν μία συγκεκριμένη περιοχή το καθένα.

1.3 Πλεονεκτήματα και μειονεκτήματα των WLAN

1.3.1 Πλεονεκτήματα

Στα σύγχρονα περιβάλλοντα εργασίας οι εργαζόμενοι είναι εφοδιασμένοι με φορητούς υπολογιστές και αφιερώνουν τον περισσότερο χρόνο τους δουλεύοντας σε ομάδες οι οποίες ξεπερνούν τα λειτουργικά και γεωγραφικά όρια του γραφείου τους. Ένα μεγάλο μέρος του έργου τους παράγεται σε συναντήσεις και χρειάζονται πρόσβαση στο δίκτυο οπουδήποτε κι αν βρίσκονται. Τα WLAN παρέχουν στους χρήστες αυτή την ελευθερία που χρειάζονται στη σύνδεσή τους με το δίκτυο της εταιρείας τους. Ο χρήστης ενός WLAN δεν είναι περιορισμένος μόνο στην περιοχή γύρω από τη θύρα του δικτύου. Το τοπικό δίκτυο μπορεί να μεταφερθεί όπου βρίσκεται ο χρήστης, άμεσα και χωρίς να είναι απαραίτητη η αναζήτηση διαθέσιμης θύρας ή να χρειάζεται οποιαδήποτε συνεννόηση με τον διαχειριστή του συστήματος. Έτσι όλες οι πληροφορίες που διατίθενται από το δίκτυο στο γραφείο ενός εργαζομένου είναι επίσης διαθέσιμες σε οποιονδήποτε χώρο. Η κινητικότητα είναι ένα μεγάλο πλεονέκτημα των WLAN αλλά και η αιτία ύπαρξης της μεγάλης πολυπλοκότητας των ασύρματων τοπικών δικτύων.

Ένα άλλο σημαντικό πλεονέκτημα των WLAN είναι η ελευθερία αποφάσεων που παρέχεται στους διαχειριστές των δικτύων, εφόσον τους επιτρέπεται να σχεδιάσουν το δίκτυο χωρίς να λαμβάνουν υπόψη τους αν υπάρχει η απαιτούμενη καλωδίωση ή αν είναι εφικτή η τοποθέτηση των καλωδίων.

Οι επιχειρήσεις μπορούν να ωφεληθούν από την ανάπτυξη ενός WLAN συστήματος, γιατί παρέχει έναν πολύ καλό συνδυασμό της απόδοσης ενός ενσύρματου δικτύου, της κινητής πρόσβασης και της ευελιξίας στη διαχείριση του δικτύου. Η κινητικότητα βελτιώνει την παραγωγικότητα επειδή επιτρέπει πρόσβαση πραγματικού χρόνου στην πληροφορία ανεξάρτητα από τη θέση του εργαζομένου, για ταχύτερη και αποδοτικότερη λήψη αποφάσεων.

Επίσης η εγκατάσταση δικτύου έχει χαμηλό κόστος σε περιοχές με δυσκολίες στην καλωδίωση, όπως διατηρητέα κτίρια και χώροι κατασκευασμένοι από συμπαγείς τοίχους. Ένα άλλο σημαντικό όφελος για μια εταιρεία είναι το ελαχιστοποιημένο κόστος ιδιοκτησίας – ειδικά σε δυναμικά περιβάλλοντα που απαιτούν συχνές μεταβολές – λόγω της ελάχιστης καλωδίωσης και του μικρού κόστους εγκατάστασης ανά συσκευή και ανά χρήστη.

1.3.2 Μειονεκτήματα

Η σύνδεση ανάμεσα στους πομπούς και τους δέκτες γίνεται μέσω ραδιοκυμάτων ή υπέρυθρων ακτίνων. Επειδή οι μεταδόσεις ενός WLAN δεν είναι περιορισμένες μέσα σε ένα καλώδιο αλλά εκπέμπονται ευρέως, με αποτέλεσμα να μπορούν να τις ακούσουν όλοι, πρέπει να δοθεί ιδιαίτερη σημασία στην προστασία των δεδομένων. Είναι μια απαίτηση που δεν την ικανοποιούν αρκετά WLAN. Κάποια πρότυπα όμως έχουν προβλέψει πόσο σημαντική είναι η μυστικότητα των δεδομένων για τους χρήστες των WLAN και για το σκοπό αυτό έχουν ενσωματώσει ισχυρούς μηχανισμούς κρυπτογράφησης των δεδομένων, ώστε να παρέχεται ασφάλεια παρόμοια με τα ενσύρματα LAN.

Μία ακόμη συνέπεια της σύνδεσης μέσω του αέρα είναι η ιδιομορφία της διάδοσης μέσω των ηλεκτρομαγνητικών κυμάτων. Οποιοδήποτε αντικείμενο στο περιβάλλον είτε ανακλά το σήμα, είτε το απορροφά. Κάτι τέτοιο όμως μπορεί να προκαλέσει σημαντική εξασθένηση του σήματος που λαμβάνει ένας WLAN σταθμός και αρκετές φορές μπορεί να τον αποκόψει εντελώς από το υπόλοιπο δίκτυο. Στα μήκη κύματος ενός WLAN, μικρές αλλαγές στη θέση μπορούν να προκαλέσουν μεγάλες αλλαγές στην ισχύ του σήματος. Αυτό οφείλεται στο γεγονός ότι για να φτάσει το σήμα στον παραλήπτη ακολουθεί διαφορετικά μονοπάτια, ποικίλου μήκους και το κάθε επιμέρους σήμα που φτάνει έχει μια πολύ μικρή διαφορά φάσης από όλα τα υπόλοιπα. Προσθέτοντας αυτές τις διαφορετικές φάσεις προκύπτει το συνολικό σήμα που λαμβάνεται από τον χρήστη. Εφόσον αυτά τα επιμέρους σήματα άλλες φορές προσθέτουν στη φάση κι άλλες φορές είναι εκτός φάσης, μερικές φορές το σήμα είναι ισχυρό και μερικές ασθενές. Τα αντικείμενα που κινούνται στο περιβάλλον όπως άνθρωποι, πόρτες κ.α. μπορούν επίσης να επηρεάσουν το σήμα.

Υπάρχουν επίσης προβλήματα που προκύπτουν από την κινητικότητα που παρέχεται στους χρήστες των WLAN. Τα περισσότερα πρωτόκολλα και το μεγαλύτερο μέρος του εξοπλισμού που είναι σήμερα διαθέσιμα δεν είναι σχεδιασμένα ώστε να υποστηρίζουν την κινητικότητα. Είναι σχεδιασμένα με βάση την υπόθεση ότι οι διευθύνσεις που ανατίθενται στους κόμβους του δικτύου παραμένουν σε μία σταθερή τοποθεσία. Έτσι τα πρώτα WLAN απαιτούσαν ο σταθμός να κινείται μέσα σε μια περιοχή στην οποία το WLAN ήταν συνδεδεμένο με το LAN με γέφυρες επιπέδου-2. Αυτό ήταν απαραίτητο επειδή δεν υπήρχε κάποιος απλός τρόπος για να χειριστούμε την αλλαγή μιας διεύθυνσης επιπέδου-3 που χρειάζεται να γίνει ώστε ο σταθμός να μεταβεί από το ένα μέρος του δικτύου σε ένα άλλο που συνδέεται μέσω δρομολογητή με το πρώτο. Σήμερα υπάρχουν τρόποι αντιμετώπισης αυτού του προβλήματος, όπως το DHCP και το Mobile-IP.

Ένα άλλο πρόβλημα που εισάγεται λόγω της κινητικότητας είναι ότι οι υπηρεσίες που βασίζονται σε μια περιοχή χάνουν το σταθερό σημείο αναφοράς τους, που είναι η θέση ενός χρήστη, εφόσον οι διευθύνσεις δικτύου δεν αντιστοιχούν σε μια μοναδική φυσική διεύθυνση. Έτσι έννοιες όπως «ο κοντινότερος εκτυπωτής» πρέπει να οριστούν με διαφορετικό τρόπο, όταν η φυσική θέση ενός χρήστη του δικτύου αλλάζει συχνά. Αυτό μπορεί να αυξάνει την πολυπλοκότητα του παροχέα υπηρεσιών θέσης, αλλά ικανοποιεί τις ανάγκες του κινούμενου χρήστη.

1.4 Απαιτήσεις για την επιλογή ενός WLAN

Για την επιλογή του WLAN που ανταποκρίνεται στις ανάγκες μας πρέπει να ληφθούν υπόψη διάφοροι παράγοντες, οι σημαντικότεροι από τους οποίους είναι οι παρακάτω [7].

1.4.1 Ευκολία εγκατάστασης

Για την εγκατάσταση ενός WLAN χρειάζεται να εγκατασταθούν και να ρυθμιστούν τα σημεία πρόσβασης και οι κάρτες δικτύου των σταθμών. Το πιο σημαντικό στοιχείο αυτής της διαδικασίας είναι η σωστή τοποθέτηση των σημείων πρόσβασης. Η τοποθέτησή τους εγγυάται την κάλυψη και την επίδοση που απαιτείται από τον σχεδιασμό του δικτύου. Υπάρχουν αρκετά στοιχεία, τα οποία παρέχουν σημαντική βοήθεια στη διαδικασία της εγκατάστασης:

Έρευνα του χώρου. Για πλήρη WLAN που έχουν κυψελοειδή (cellular) αρχιτεκτονική, η σωστή τοποθέτηση των σημείων πρόσβασης καθορίζεται καλύτερα αν έχει γίνει μια έρευνα του χώρου, κατά τη διάρκεια της οποίας το άτομο που θα εγκαταστήσει το δίκτυο τοποθετεί τα σημεία πρόσβασης και καταγράφει την ισχύ του σήματος και την ποιότητα της πληροφορίας καθώς μετακινείται στην περιοχή κάλυψης. Οι περισσότεροι κατασκευαστές παρέχουν κάποια εργαλεία έρευνας, τα οποία διαφέρουν ως προς την ποσότητα και την ποιότητα των πληροφοριών που παρέχουν.

Δυνατότητα λειτουργίας πάνω από το Ethernet. Μερικοί κατασκευαστές διαθέτουν σημεία πρόσβασης τα οποία μπορούν να λειτουργήσουν πάνω από το Ethernet που συνδέει το σημείο πρόσβασης με το ενσύρματο δίκτυο. Αυτό συνήθως επιτυγχάνεται από μια μονάδα του εξοπλισμού, η οποία παίρνει από τον ενσύρματο διακόπτη AC ισχύ και τη σύνδεση των δεδομένων και σαν έξοδο δίνει DC ισχύ σε αχρησιμοποίητα ζεύγη αγωγών μέσα στο καλώδιο δικτύου που συνδέει τη μονάδα αυτή και το σημείο πρόσβασης. Αυτό το χαρακτηριστικό εξαλείφει την ανάγκη εγκατάστασης καλωδίου AC προς το σημείο πρόσβασης, καθιστώντας την εγκατάσταση πολύ πιο γρήγορη.

Εύκολη στη χρήση κάρτα δικτύου και εργαλεία ρύθμισης του σημείου πρόσβασης. Αφού εγκατασταθούν τα σημεία πρόσβασης πρέπει τόσο τα ίδια, όσο και οι κάρτες δικτύου (Network Interface Card – NIC) να ρυθμιστούν ώστε να μπορούν να χρησιμοποιηθούν. Όπως συμβαίνει με οποιοδήποτε τεχνικό προϊόν η ποιότητα της διεπαφής με τον χρήστη καθορίζει το χρόνο που θα απαιτηθεί για τη ρύθμιση του δικτύου ώστε να είναι σε θέση να τεθεί σε λειτουργία.

1.4.2 Ευκολία διαχείρισης

Εφόσον ένα ασύρματο LAN διαφέρει από τα ενσύρματα μόνο στα Επίπεδα 1 και 2 του OSI μοντέλου θα πρέπει να περιμένουμε τουλάχιστον το ίδιο επίπεδο δυσκολίας στη διαχείριση των συσκευών. Τα προϊόντα θα πρέπει να έχουν SNMP 2 υποστήριξη ώστε να μπορούν να εντοπίζονται και να διαχειρίζονται αυτόματα από τα ίδια εργαλεία που χρησιμοποιούνται και για τον εξοπλισμό των ενσύρματων LAN.

Εκτός από το SNMP θα ήταν χρήσιμο να μπορούν να ρυθμίζονται και να εξετάζονται τα σημεία πρόσβασης μέσω μιας εύκολης στη χρήση διεπαφής, όπως για παράδειγμα με έναν φυλλομετρητή (web browser). Μερικοί κατασκευαστές έχουν προσθέσει έναν εξυπηρετητή υπηρεσιών διαδικτύου (web server) στα σημεία πρόσβασής τους για να εξυπηρετήσουν αυτό το σκοπό. Τέλος η δυνατότητα διαχείρισης, ρύθμισης και αναβάθμισης των σημείων πρόσβασης ανά ομάδες απλοποιεί κατά πολύ τη διαχείριση του WLAN.

1.4.3 Εμβέλεια και απόδοση

Τα WLAN χρησιμοποιούν τα ραδιοκύματα για να επικοινωνούν επειδή αυτά τα κύματα έχουν την ικανότητα να διαπερνούν πολλές εσωτερικές κατασκευές και να ανακλώνται από τα εμπόδια. Η απόδοση των WLAN εξαρτάται από πολλούς παράγοντες. Μερικοί από αυτούς είναι ο αριθμός των χρηστών, η ακτίνα του μικροκελιού (microcell), οι παρεμβολές, η μετάδοση πολλαπλού μονοπατιού (multipath propagation), η υποστήριξη των προτύπων και το είδος του υλικού. Φυσικά οτιδήποτε επηρεάζει την κίνηση των δεδομένων στα ενσύρματα τμήματα του LAN, όπως η καθυστέρηση και η συμφόρηση, επηρεάζει και το ασύρματο τμήμα του LAN.

Από την άλλη, η μεγάλη εμβέλεια δεν είναι πάντα η καλύτερη λύση. Για παράδειγμα αν το δίκτυο απαιτεί υψηλή απόδοση και πλήρη κάλυψη η μεγάλη εμβέλεια μπορεί να δημιουργήσει δυσκολίες στην εφαρμογή κάποιου αλγορίθμου επαναχρησιμοποίησης καναλιών και τη διατήρηση παράλληλα της απαιτούμενης υψηλής απόδοσης.

1.4.4 Κινητικότητα

Η κινητικότητα (mobility) αφορά τον τρόπο με τον οποίο τα σημεία πρόσβασης παρακολουθούν τους χρήστες καθώς αυτοί μετακινούνται (roam) είτε μεταξύ δύο σημείων πρόσβασης του ίδιου υποδικτύου, είτε όταν οι χρήστες μετακινούνται μέσω ενός δρομολογητή ανάμεσα σε δύο υποδίκτυα.

Το πρώτο πρόβλημα το χειρίζονται πρωτόκολλα που είναι ορισμένα από τους κατασκευαστές και τα οποία μπορεί να διαφέρουν ως προς την απόδοσή τους. Αν το πρωτόκολλο δεν είναι αποδοτικό υπάρχει περίπτωση να χαθούν πακέτα καθώς ο χρήστης κινείται από το ένα σημείο πρόσβασης στο άλλο.

Το δεύτερο πρόβλημα το χειρίζονται μηχανισμοί περιαγωγής (roaming) του επιπέδου 3. Ο πιο δημοφιλής από αυτούς είναι το Mobile IP το οποίο είναι προς το παρόν γνωστό ως RFC 2002 από το Internet Engineering Task Force (IETF). Το Mobile IP λειτουργεί ορίζοντας για κάθε χρήστη έναν «home agent», το οποίο είναι κάποιο σημείο πρόσβασης. Μόλις ο ασύρματος σταθμός αφήσει την περιοχή στην οποία ανήκει και μπει σε μια νέα περιοχή το νέο σημείο πρόσβασης ρωτάει τον σταθμό ποιος είναι ο home agent του. Μόλις αυτός εντοπιστεί εγκαθίσταται αυτόματα μία προώθηση πακέτων ανάμεσα στα δύο σημεία πρόσβασης ώστε να εξασφαλιστεί η διατήρηση της IP διεύθυνσης του χρήστη και η διαφανής παραλαβή των δεδομένων από αυτόν. Εφόσον όμως το Mobile IP δεν έχει φτάσει στην τελική του μορφή οι κατασκευαστές μπορούν να παρέχουν τα δικά τους πρωτόκολλα χρησιμοποιώντας παρόμοιες τεχνικές

που εξασφαλίζουν ότι η IP κίνηση ακολουθεί έναν χρήστη καθώς κινείται μέσα σε δίκτυα που συνδέονται μέσω ενός δρομολογητή (π.χ. ανάμεσα σε δύο κτίρια).

Μία πολύ καλή εναλλακτική λύση για το πρόβλημα περιαγωγής του επιπέδου 3 είναι το Dynamic Host Configuration Protocol (DHCP), παρά το γεγονός ότι δεν έχει ολοκληρωθεί ακόμη. Το DHCP επιτρέπει στους χρήστες που κλείνουν ή θέτουν σε αναμονή τους φορητούς τους υπολογιστές πριν περάσουν σε ένα νέο δίκτυο να αποκτήσουν αυτόματα μια νέα IP διεύθυνση μόλις θέσουν ξανά σε λειτουργία τον υπολογιστή τους.

1.4.5 Διαχείριση Ισχύος

Τα ασύρματα προϊόντα των τελικών χρηστών είναι σχεδιασμένα να λειτουργούν με την ισχύ που τους παρέχει κάποια μπαταρία. Τα ασύρματα πρότυπα πρέπει να υποστηρίζουν κάποιο πρωτόκολλο το οποίο θα μεγιστοποιεί τη ζωή της μπαταρίας των ασύρματων συσκευών.

1.4.6 Ασφάλεια

Ένα σημαντικό μειονέκτημα των WLAN είναι όπως αναφέραμε τα προβλήματα ασφάλειας που προκύπτουν από το γεγονός ότι τα δεδομένα εκπέμπονται σε μια περιοχή, η οποία μπορεί να υπερβαίνει τα όρια της περιοχής που μπορεί να ελέγξει φυσικά ο οργανισμός. Έτσι μπορεί κάποιος να λάβει παθητικά τις ευαίσθητες πληροφορίες ενός οργανισμού, απλώς χρησιμοποιώντας την ίδια ασύρματη κάρτα δικτύου (NIC) από μία απόσταση την οποία δεν μπορεί να ελέγξει το προσωπικό ασφάλειας του δικτύου.

Αυτό το πρόβλημα μπορεί να υπάρξει και σε ένα ενσύρματο δίκτυο αλλά σε πολύ μικρότερο βαθμό. Η υπάρχουσα κυκλοφορία των ηλεκτρομαγνητικών κυμάτων μέσα από καλώδια επιτρέπει σε κάποιον να λάβει το σήμα χρησιμοποιώντας εξοπλισμό με ειδικούς αισθητήρες. Πρέπει όμως το άτομο αυτό να βρίσκεται πολύ κοντά στο καλώδιο για να λάβει το σήμα.

Πολλά από τα θέματα ασφάλειας που αφορούν τα WLAN είναι ίδια με αυτά των ενσύρματων LAN. Τα δεδομένα που μεταδίδονται σε ένα ενσύρματο LAN εσφαλμένα θεωρούνται προστατευμένα επειδή κάποιος πρέπει να βρίσκεται μέσα στο κτίριο για να έχει πρόσβαση στο δίκτυο. Αυτό είναι εντελώς αναληθές γιατί πρέπει να ληφθεί υπόψη και η πρόσβαση στο Διαδίκτυο. Πολύ συχνά οι χρήστες που βρίσκονται εντός του κτιρίου συνδέονται στο Διαδίκτυο, επιτρέποντας στους εισβολείς (που βρίσκονται έξω από το κτίριο) να μπουν στο δίκτυο αν δεν έχουν ληφθεί τα απαραίτητα μέτρα προστασίας. Υπάρχει επίσης και η απομακρυσμένη πρόσβαση του δικτύου από εργαζομένους που ταξιδεύουν ή δουλεύουν στο σπίτι τους (telnet), την οποία μπορεί να εκμεταλλευτεί κάποιος εισβολέας.

Τα παραπάνω παραδείγματα μας δείχνουν ότι τόσο τα ενσύρματα, όσο και τα ασύρματα δίκτυα εκτίθενται στους ίδιου κινδύνους ασφάλειας και έχουν τα ίδια προβλήματα. Αυτά είναι τα εξής:

- Επιθέσεις στη φυσική ασφάλεια του δικτύου (π.χ. άρνηση υπηρεσιών ή δηλιοφθορά).
- Μη εξουσιοδοτημένη πρόσβαση και υποκλοπή.
- Εσωτερικές επιθέσεις (εξουσιοδοτημένες) από χρήστες που είναι π.χ. δυσαρεστημένοι, απολυμένοι ή όχι και ξέρουν πώς να διαβάζουν, να διανέμουν και να μεταβάλλουν πολύτιμα δεδομένα της εταιρείας.

Επίσης τα μέτρα που λαμβάνονται για την ακεραιότητα και την ασφάλεια των δεδομένων σε ένα ενσύρματο LAN μπορούν να εφαρμοστούν και σε ένα WLAN. Μάλιστα, κάποια πρότυπα WLAN ενσωματώνουν μερικά επιπλέον στοιχεία ασφάλειας, τα οποία δεν είναι διαθέσιμα στα ενσύρματα δίκτυα. Για το λόγο αυτό μερικοί υποστηρίζουν ότι ένα σωστά εφαρμοσμένο και προστατευμένο WLAN είναι περισσότερο προστατευμένο από ένα ενσύρματο.

1.4.7 Κόστος

Το κόστος του υλικού περιλαμβάνει την προσθήκη νέων σημείων πρόσβασης στο δίκτυο και καρτών προσαρμογής του WLAN σε όλες τις ασύρματες συσκευές και υπολογιστές. Ο αριθμός των σημείων πρόσβασης εξαρτάται από την περιοχή που πρέπει να καλυφθεί, τον αριθμό των χρηστών και το είδος των απαιτούμενων υπηρεσιών. Η περιοχή κάλυψης των σημείων πρόσβασης εκτείνεται μέχρι μια συγκεκριμένη ακτίνα. Οι «ζώνες» των σημείων πρόσβασης επικαλύπτονται πολλές φορές για να εξασφαλίσουν την πλήρη κάλυψη της περιοχής. Το κόστος του υλικού εξαρτάται από παράγοντες όπως είναι οι απαιτήσεις επίδοσης και κάλυψης και η εμβέλεια των προϊόντων σε διαφορετικούς ρυθμούς μετάδοσης δεδομένων.

Εκτός από το κόστος του εξοπλισμού ένας πελάτης πρέπει να λάβει υπόψη του τα έξοδα εγκατάστασης λογαριασμού και συντήρησης καθώς και το κόστος που μπορεί να προκύψει λόγω κακής ποιότητας των προϊόντων. Αυτά τα έξοδα μπορούν να υπερβούν κατά πολύ το κόστος του αρχικού εξοπλισμού ενός WLAN. Τα προϊόντα που είναι εύκολα στην εγκατάσταση, χρήση και διαχείριση και τα οποία έχουν τις επιδόσεις που απαιτούνται μπορεί να κοστίζουν αρκετά. Τα χαρακτηριστικά που αναφέρθηκαν παραπάνω όπως η λειτουργία πάνω από το Ethernet, η μαζική ρύθμιση των σημείων πρόσβασης και ένα πλούσιο σύνολο από εργαλεία διαχείρισης, μπορούν να ελαττώσουν το συνολικό κόστος ενός ασύρματου τοπικού δικτύου.

1.5 Μερικά WLAN πρότυπα

1.5.1 Το Πρότυπο IEEE 802.11

Το 1997 η IEEE υιοθέτησε το πρώτο πρότυπο για WLAN, το 802.11 [1], [2], που αναθεωρήθηκε το 1999. Η ομάδα του IEEE 802.11 αποτελείται από εργαζομένους στις κορυφαίες εταιρείες παραγωγής εξοπλισμού για WLAN, παροχείς δικτύων, Πανεπιστημιακά εργαστήρια ερευνών, κατασκευαστές υπολογιστών και τελικούς χρήστες. Οι εταιρείες που εκπροσωπούν αυτό το γκρουπ είναι από την Ασία, την Αυστραλία, τον Καναδά, την Ευρώπη, το Ισραήλ και τις Ηνωμένες Πολιτείες.

Το πρωτόκολλο IEEE 802.11 περιγράφει ένα επίπεδο ελέγχου πρόσβασης του μέσου (Medium Access Control – MAC), υπηρεσίες και πρωτόκολλα διαχείρισης του MAC και τρία φυσικά (Physical - PHY) επίπεδα.

Τα τρία φυσικά επίπεδα έχουν είναι τα εξής: ένα baseband υπερύθρων (Infrared – IR), ένα ραδιοκυμάτων με Frequency Hopping Spread Spectrum (FHSS) και εύρος ζώνης 2.4 GHz και ένα ακόμη ραδιοκυμάτων με Direct Sequence Spread Spectrum (DSSS) με εύρος ζώνης 2.4 GHz. Και τα τρία φυσικά επίπεδα περιγράφουν τη λειτουργία του WLAN σε 1 και 2 Mbps.

Η τεχνική FHSS προσπαθεί να αποφύγει την παρεμβολή τρίτων μεταπηδώντας ταχύτατα από μια συχνότητα σε μια άλλη με ψευδοτυχαίο τρόπο. Ο παραλήπτης έχει τον ίδιο ψευδοτυχαίο αλγόριθμο με τον αποστολέα και μεταπηδάει με τον ίδιο τρόπο σε άλλη συχνότητα. Η τεχνική DSSS προσθέτει στα δεδομένα μια σειρά από ψευδοτυχαία bit. Ο παραλήπτης χρησιμοποιώντας τον ίδιο αλγόριθμο εξάγει αυτά τα επιπλέον bit και λαμβάνει τα πραγματικά δεδομένα.

Επίσης αναπτύχθηκαν δύο ακόμη φυσικά επίπεδα. Το πρώτο, το IEEE 802.11a, είναι ραδιοκυμάτων με Orthogonal Frequency Domain Multiplexing (OFDM) στις συχνότητες UNII (επομένως δε θα είναι διαθέσιμο στην Ευρώπη και την Ιαπωνία), με ρυθμό δεδομένων 6, 12 και 54 Mbps (και προαιρετικά 9, 18, 36 και 48 Mbps). Τυποποιήθηκε την άνοιξη του 1999 και χρησιμοποιεί 52 subcarriers σε ένα κανάλι των 20 MHz.

Το δεύτερο, το IEEE 802.11b, είναι μια επέκταση του DSSS φυσικού επιπέδου σε φάσμα συχνοτήτων 2.4 GHz και επιτυγχάνει ρυθμούς μετάδοσης των 5.5 και 11 Mbps.

1.5.2 Το πρότυπο HIPERLAN

Το πρότυπο HiperLan [17] έχει σχεδιαστεί από μια επιτροπή ερευνητών του ETSI. Λειτουργεί σε ένα εύρος ζώνης 5.1 – 5.3 GHz, οπότε δεν είναι απαραίτητη η spread spectrum. Ο ρυθμός μετάδοσης είναι 23.5 Mbps και έχει 5 κανάλια. Περιλαμβάνει προαιρετική κρυπτογράφηση (χωρίς να ορίζεται συγκεκριμένος αλγόριθμος) και εξοικονόμηση ενέργειας.

Η δρομολόγηση είναι ad hoc. Αυτό σημαίνει ότι αν ο προορισμός ενός πακέτου δεν είναι απευθείας συνδεδεμένος με τον αποστολέα, τότε οι ενδιάμεσοι σταθμοί θα το προωθήσουν με τον βέλτιστο τρόπο μέσα στο HiperLan δίκτυο. Επίσης η λειτουργία του είναι εντελώς ad hoc από την άποψη ότι δεν απαιτούνται κεντρικοποιημένοι έλεγχοι ή ρυθμίσεις.

Υπάρχει και μια δεύτερη έκδοση του προτύπου, η HiperLan II, η οποία σχεδιάστηκε για τη διαχείριση δικτύων υποδομής και ασύρματα συστήματα διανομής. Λειτουργεί στα 5 GHz (5.4 – 5.7 GHz).

Ήταν το πρώτο πρότυπο που βασιζόταν στη διαμόρφωση OFDM. Το κάθε sub-carrier μπορεί να χρησιμοποιήσει διαφορετική διαμόρφωση, γεγονός που επιτρέπει διαφορετικούς ρυθμούς δεδομένων (6, 9, 12, 18, 27 και 36 Mbps). Το πλάτος του καναλιού

είναι 20 MHz και περιλαμβάνει 48 OFDM κανάλια δεδομένων και άλλα 4 βοηθητικά κανάλια.

Το HiperLan II είναι ένα ασύρματο ATM σύστημα και το πρωτόκολλο MAC είναι ένα σχήμα TDMA που συντονίζεται κεντρικά με reservation slots.

Είναι σχεδιασμένο έτσι ώστε να μεταφέρει πακέτα ATM, αλλά και IP πακέτα και ψηφιακή φωνή (κινητών τηλεφώνων).

1.5.3 Το πρότυπο HomeRF

Το HomeRF [13], [14] σχεδιάστηκε από μια ομάδα η οποία συντονίζεται από την Proxim (ένα μέρος της ανήκει στην εταιρεία Intel) και είναι βασισμένη στο Shared Wireless Access Protocol (SWAP). Σχηματίστηκε με στόχο την προώθηση της χρήσης των WLAN στο σπίτι ή σε μικρά γραφεία. Το σπίτι αποτελεί μια πολύ καλή αγορά για τα WLAN, επειδή πολύ λίγα σπίτια έχουν στις μέρες μας καλωδίωση και το Ethernet ανάμεσα στα διάφορα δωμάτια κι επειδή η κινητικότητα είναι επιθυμητή μέσα σε έναν τέτοιο χώρο.

Το πρότυπο χρησιμοποιεί εύρος ζώνης 2.4 GHz και επιτυγχάνει ρυθμό μετάδοσης 10 Mbps. Είναι σχεδιασμένο με τέτοιο τρόπο, ώστε να αντιμετωπίζει το μεγαλύτερο εμπόδιο για την ανάπτυξη των WLAN: το κόστος. Οι περισσότεροι χρήστες δεν μπορούν να διαθέσουν τα χρήματα που χρειάζονται για την αγορά ασύρματων καρτών δικτύου που είναι απαραίτητες για τη διασύνδεση των υπολογιστών τους.

Το σημαντικότερο κόστος ενός WLAN είναι το μόντεμ, το οποίο έχει σχεδόν σταθερή τιμή, οπότε δεν υπάρχουν προοπτικές ελάττωσης της τιμής του. Τα μόντεμ με Frequency Hopping είναι λιγότερο ακριβά, το κόστος τους όμως αυξάνεται με την προσθήκη πολλών περιορισμών στη λειτουργία του. Το HomeRF ελαττώνοντας τους περιορισμούς αυτούς επιτρέπει μια πιο φθηνή εφαρμογή, διατηρώντας όμως καλή απόδοση. Το πρωτόκολλο MAC είναι υλοποιημένο σε λογισμικό, οπότε δεν προσθέτει στο τελικό κόστος του προϊόντος.

Ένα μεγάλο πλεονέκτημα του HomeRF είναι η ανάπτυξη της ασύρματης τηλεφωνίας, που επιτρέπει το PC να δρομολογεί τις τηλεφωνικές κλήσεις μέσα στο σπίτι ή να προσφέρει φωνητικές υπηρεσίες στους χρήστες.

1.5.4 Το πρότυπο Bluetooth

Το BlueTooth [8], [12], [14] αναπτύχθηκε από μια ομάδα η οποία ονομάζεται Bluetooth Special Interest Group (SIG) και η οποία σχηματίστηκε το 1998. Τα ιδρυτικά μέλη της είναι οι εταιρείες Ericsson, Nokia, Intel, IBM και Toshiba.

Είναι μια τεχνολογία *αντικατάστασης καλωδίων* και όχι ένα WLAN. Παρά το γεγονός ότι αυτές οι τεχνολογίες δεν παρέχουν τη δυνατότητα διαμοιραζόμενων αρχείων ή συσκευών όπως συμβαίνει σε ένα WLAN, παρέχουν τη δυνατότητα ταχύτατης αντιγραφής αρχείων και λειτουργίες συγχρονισμού των δεδομένων, επιτρέποντας στα δε-

δομένα των εφαρμογών να ανταλλάσσονται με ασύρματο τρόπο μεταξύ φορητών υπολογιστών, κινητών τηλεφώνων και άλλων φορητών συσκευών όπως τα PDA.

Το Bluetooth είναι ένα σύστημα χαμηλής ισχύος, χαμηλού κόστους και μικρής εμβέλειας ραδιοκυμάτων με frequency-hopping. Χρησιμοποιεί ραδιοκύματα με εύρος 2.45 GHz και ο θεωρητικός ρυθμός δεδομένων είναι το 1 Mbps. Η μεταπήδηση συχνοτήτων γίνεται με την τεχνική GFSK (Gaussian Frequency Shift Keying). Το Bluetooth υποστηρίζει είτε ένα ασύγχρονο κανάλι δεδομένων και μέχρι 3 ταυτόχρονα σύγχρονα κανάλια φωνής ή ένα κανάλι δεδομένων ταυτοχρόνως με ένα σύγχρονο κανάλι φωνής.

1.5.5 Σύγκριση των προτύπων

Τα πρότυπα 802.11 και Bluetooth είναι αναμφίβολα αυτά που έχουν τους περισσότερους υποστηρικτές και μάλιστα κυκλοφορούν ήδη στην αγορά τα προϊόντα τους

Ως προς την απόδοση, το IEEE 802.11 είναι αυτό που επιτυγχάνει τους υψηλότερους ρυθμούς μετάδοσης (11 Mbps), ενώ το άλλο σημαντικό του πλεονέκτημα είναι το υψηλό επίπεδο ασφάλειας που προσφέρει σε σχέση με τα άλλα WLAN πρότυπα.

Σε περιβάλλοντα όμως μεγάλης πυκνότητας (π.χ. διαμερίσματα) και όπου απαιτούνται τηλεφωνικές υπηρεσίες και υποστήριξη φωνής η επίδοση του HomeRF είναι πιο ικανοποιητική.

Ως προς το κόστος και την κατανάλωση ισχύος το HiperLan και το HomeRF δίνουν τα καλύτερα αποτελέσματα. Από την άλλη το HomeRF και το Hiperlan είναι δύο πρότυπα τα οποία παρέχουν μεγαλύτερη ευκολία εγκατάστασης και διαχείρισης του WLAN, εφόσον έχουν πιο απλό σχεδιασμό από το 802.11.

Τέλος το Bluetooth όπως έχουμε ήδη αναφέρει είναι μια τεχνολογία αντικατάστασης καλωδίων και όχι ένα πρότυπο για WLAN, οπότε πρέπει να χρησιμοποιείται σε συνδυασμό με κάποιο από τα παραπάνω πρότυπα. Έχει χαμηλή κατανάλωση ισχύος και χαμηλό κόστος, παρέχει ευκολία εγκατάστασης και διαχείρισης, αλλά δεν μπορεί να υποστηρίξει όλες τις υπηρεσίες ενός WLAN και έχει πολύ χαμηλή απόδοση.

Στα πλαίσια της παρούσας μεταπτυχιακής εργασίας υλοποιήθηκε ένα τμήμα του προτύπου IEEE 802.11, το οποίο αφορά την ασφάλεια που παρέχεται. Στη συνέχεια μελετήθηκε κατά πόσο επιτυγχάνονται οι στόχοι ασφάλειας που επιδιώκονται και αναλύθηκαν οι αδυναμίες του. Πάνω στις αδυναμίες αυτές στηρίχθηκε η υλοποίηση των δύο σημαντικότερων επιθέσεων κι έγιναν κάποιες προτάσεις που είναι δυνατό να λύσουν αυτά τα προβλήματα.

Στα επόμενα κεφάλαια θα περιγράψουμε το πρότυπο 802.11. Στο Κεφάλαιο 2 θα αναφερθούμε σε κάποιες βασικές έννοιες της αρχιτεκτονικής του και των υπηρεσιών που υποστηρίζονται. Στο Κεφάλαιο 3 περιγράφεται ο τρόπος με τον οποίο επιδιώκεται η ασφάλεια, ενώ στο Κεφάλαιο 4 αναλύονται τα προβλήματα που έχει αυτή και οι επιθέσεις που βασίζονται σε αυτά τα προβλήματα. Τέλος, στο Κεφάλαιο 5 αναφέρο-

νται τρόποι με τους οποίους θα μπορούσαν να αντιμετωπιστούν οι περισσότερες επιθέσεις.

ΚΕΦΑΛΑΙΟ 2

Το Πρότυπο IEEE 802.11

2.1 Σκοπός του 802.11

Ο σκοπός του προτύπου 802.11 είναι η παροχή ασύρματης σύνδεσης σε αυτόματα μηχανήματα, σε εξοπλισμό ή σε σταθμούς που η λειτουργία τους απαιτείται να είναι πολύ γρήγορη και οι οποίοι μπορεί να είναι φορητοί ή να βρίσκονται πάνω σε οχήματα που κινούνται σε μια μικρή περιοχή. Έχει σαν στόχο να περιγράψει ένα WLAN που παρέχει υπηρεσίες, οι οποίες μέχρι τώρα υπήρχαν μόνο στα ενσύρματα δίκτυα, όπως υψηλή απόδοση, αξιόπιστη μετάδοση των δεδομένων και συνεχή σύνδεση με το δίκτυο. Επίσης το IEEE 802.11 επιτρέπει κινητικότητα με διαφάνεια και έχει ενσωματωμένες λειτουργίες εξοικονόμησης ενέργειας για τον χρήστη του δικτύου.

Ειδικότερα, το πρότυπο 802.11:

- Περιγράφει τις λειτουργίες και τις υπηρεσίες που απαιτούνται, ώστε να μπορεί μία συμβατή με το IEEE 802.11 συσκευή να λειτουργεί μέσα σε ασύρματα τοπικά δίκτυα, καθώς και τα θέματα της κινητικότητας των σταθμών (μετάβαση – transition) μέσα στα δίκτυα αυτά.
- Ορίζει τις MAC διαδικασίες για την υποστήριξη των υπηρεσιών παράδοσης της ασύγχρονης μονάδας δεδομένων MAC υπηρεσιών (MAC service data unit – MSDU).
- Ορίζει μερικές τεχνικές και διαδικασίες διεπαφής για τα σήματα του φυσικού επιπέδου, τα οποία ελέγχονται από το IEEE 802.11 MAC.
- Επιτρέπει τη λειτουργία μιας συμβατής με το IEEE 802.11 συσκευής μέσα σε ένα ασύρματο τοπικό δίκτυο (local area network – LAN), το οποίο μπορεί να συνυπάρξει με άλλα επικαλυπτόμενα IEEE 802.11 LAN.

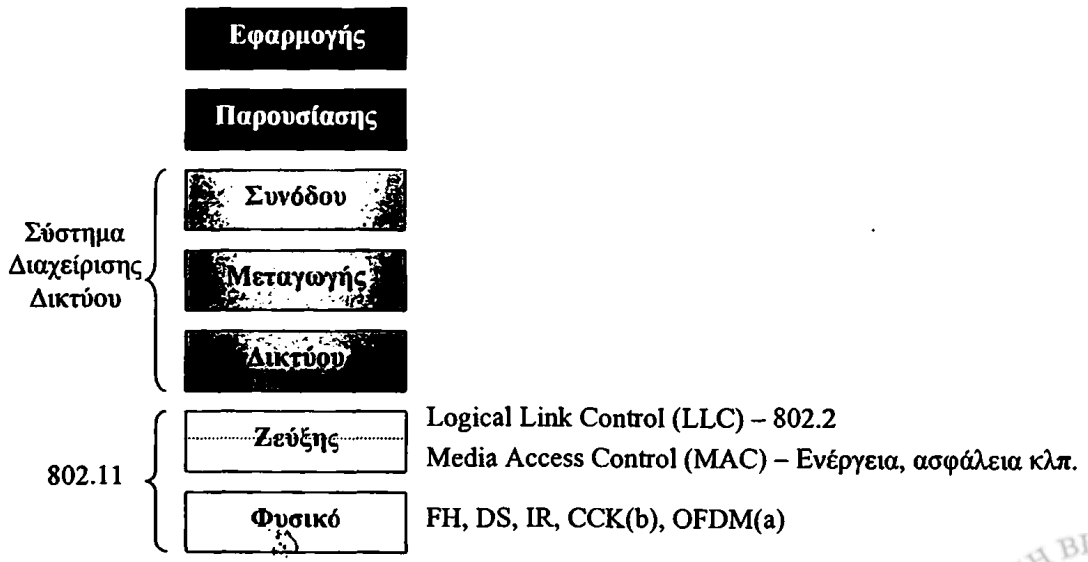
- Περιγράφει τις απαιτήσεις και τις λειτουργίες για την εξασφάλιση της μυστικότητας των πληροφοριών του χρήστη που μεταφέρονται στο ασύρματο μέσο (wireless medium – WM) και της πιστοποίησης των IEEE 802.11 συσκευών.

2.2 Το 802.11 και το μοντέλο OSI

Με τα 802.11 WLAN οι κινούμενοι χρήστες μπορούν να έχουν επίδοση, απόδοση και διαθεσιμότητα επιπέδου Ethernet. Η τεχνολογία του προτύπου επιτρέπει στους διαχειριστές να φτιάξουν ένα δίκτυο που συνδυάζει περισσότερες από μία τεχνολογίες LAN ώστε να ταιριάζει καλύτερα με τις ανάγκες των εταιρειών και των χρηστών.

Όπως όλα τα IEEE 802 πρότυπα έτσι και το 802.11 επικεντρώνεται στα δύο χαμηλότερα επίπεδα του μοντέλου ISO, το φυσικό επίπεδο και το επίπεδο ζεύξης (Εικόνα 2.1). Οποιαδήποτε εφαρμογή, σύστημα διαχείρισης δικτύου ή πρωτόκολλο μπορεί να εκτελεστεί σε ένα WLAN συμβατό με το 802.11 με την ίδια ευκολία με την οποία εκτελείται πάνω από το Ethernet.

Για να επιτευχθεί αυτή η ομοιότητα η διεπαφή του IEEE 802.11 είναι παρόμοια με αυτή του IEEE 802.3 και λειτουργεί κάτω από το IEEE 802.2 επίπεδο ελέγχου λογικής ζεύξης (LLC), παρέχοντας έτσι όλες τις υπηρεσίες που απαιτούνται για την υποστήριξη αυτού του επιπέδου. Αυτό έχει σαν αποτέλεσμα να μην μπορούν τα πρωτόκολλα που εκτελούνται πάνω από το IEEE 802.2 να το ξεχωρίσουν από το IEEE 802.3. Η χρήση λοιπόν της διεπαφής του IEEE 802.2 εγγυάται ότι τα επίπεδα πάνω από το LLC δε θα γνωρίζουν τι είδους είναι το δίκτυο που μεταφέρει τα δεδομένα τους (ενσύρματο ή ασύρματο).



Εικόνα 2.1. Το μοντέλο ISO και το 802.11

Η βασική αρχιτεκτονική, τα χαρακτηριστικά και οι υπηρεσίες των 802.11a και 802.11b ορίζονται από το 802.11 πρότυπο. Διαφορές υπάρχουν μόνο στο φυσικό επίπεδο, όπου έχουμε επιπλέον μεγαλύτερους ρυθμούς μετάδοσης και πιο σταθερή σύνδεση από το 802.11.

2.3 Η αρχιτεκτονική του IEEE 802.11

Η αρχιτεκτονική του IEEE 802.11 WLAN είναι σχεδιασμένη με τέτοιο τρόπο, ώστε να υποστηρίζει ένα δίκτυο στο οποίο οι περισσότερες αποφάσεις λαμβάνονται κατανεμημένα από τους κινούμενους σταθμούς. Αυτή η αρχιτεκτονική έχει αρκετά πλεονεκτήματα, συμπεριλαμβανομένου του γεγονότος ότι είναι ανεκτική σε σφάλματα όλου του εξοπλισμού του WLAN και εξαφανίζει οποιαδήποτε πιθανά σημεία συμφόρησης που θα μπορούσε να δημιουργήσει μία κεντρικοποιημένη αρχιτεκτονική. Είναι πολύ ευέλικτη, υποστηρίζει εύκολα μικρά, προσωρινά δίκτυα ή μεγάλα και μόνιμα ή σχεδόν μόνιμα δίκτυα. Επίσης έχουν προστεθεί στην αρχιτεκτονική και στα πρωτόκολλα τρόποι λειτουργίας εξοικονόμησης ενέργειας, ώστε να παρατείνεται η ζωή της μπαταρίας για τον κινούμενο εξοπλισμό χωρίς να χάνεται η σύνδεση.

Η αρχιτεκτονική του IEEE 802.11 περιλαμβάνει ένα σύνολο από στοιχεία: τον σταθμό, το σημείο, το ασύρματο μέσο, το βασικό σύνολο υπηρεσιών, το Σύστημα Διανομής (Distribution System - DS) και το επεκταμένο σύνολο υπηρεσιών. Περιλαμβάνει επίσης υπηρεσίες σταθμών και υπηρεσίες μετάδοσης. Τα στοιχεία αυτά θα περιγραφούν αναλυτικότερα παρακάτω.

Η αρχιτεκτονική του 802.11 μπορεί να φαίνεται υπερβολικά περίπλοκη. Όμως αυτή η πολυπλοκότητα είναι που παρέχει στα IEEE 802.11 WLAN ευρωστία και ευελιξία. Ενσωματώνει μάλιστα ένα επίπεδο εμμεσότητας (indirection) που δεν υπήρχε σε προηγούμενα LAN. Αυτό το επίπεδο εμμεσότητας, που το διαχειρίζεται εξολοκλήρου η αρχιτεκτονική του 802.11 και είναι διαφανές για τους χρήστες του πρωτοκόλλου των IEEE 802.11 WLAN, παρέχει στον κινούμενο σταθμό τη δυνατότητα να μετακινείται σε ένα WLAN, αλλά να φαίνεται ακίνητος για τα πρωτόκολλα πάνω από το MAC, τα οποία δεν περιλαμβάνουν την έννοια της κινητικότητας. Αυτό το τέχνασμα που εφαρμόζεται από το 802.11 επιτρέπει σε όλα τα υπάρχοντα πρωτόκολλα δικτύων να εκτελούνται πάνω από ένα WLAN χωρίς να χρειάζονται ειδικές ρυθμίσεις.

2.3.1 Σταθμοί και σημεία πρόσβασης

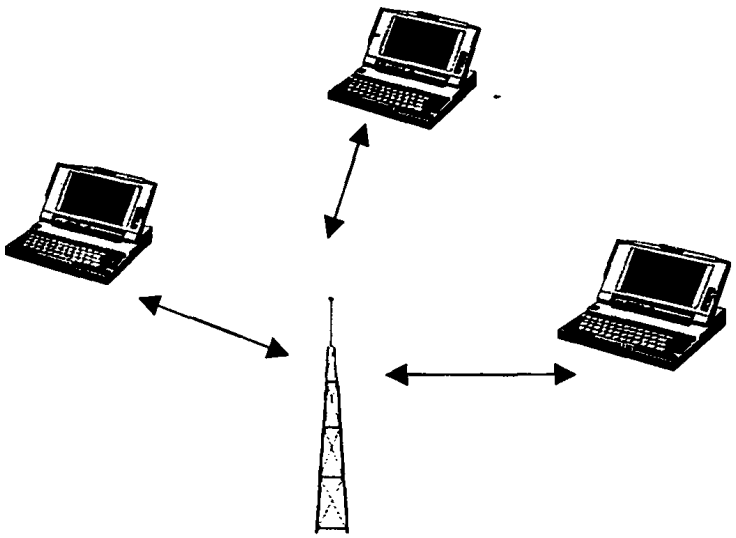
Το πρότυπο 802.11 ορίζει δύο συσκευές υλικού: έναν ασύρματο σταθμό (station - STA) και ένα σημείο πρόσβασης (access point – AP). Ο σταθμός είναι το στοιχείο που συνδέεται στο ασύρματο μέσο. Είναι μία συσκευή που έχει μία ασύρματη κάρτα δικτύου (Network Interface Card - NIC) και αποτελείται συνήθως από έναν ραδιοπομπό, μία ενσύρματη επικοινωνία δικτύου (π.χ. 802.3) και λογισμικό γέφυρας. Ο σταθμός μπορεί να είναι κινούμενος, φορητός ή ακίνητος. Ο κάθε σταθμός υποστηρίζει τις υπηρεσίες σταθμού (Distribution Service). Οι υπηρεσίες αυτές είναι η πιστοποίηση, η ακύρωση πιστοποίησης, η εμπιστευτικότητα και η μεταφορά των δεδομένων που αναφέρονται στο πρότυπο ως Μονάδες Δεδομένων Υπηρεσιών MAC (MAC Service Data Unit) ή MSDU.

Το AP είναι μια οντότητα, η οποία έχει την ίδια λειτουργικότητα με έναν σταθμό και αποτελεί έναν σταθμό βάσης για το ασύρματο δίκτυο. Λειτουργεί επίσης ως γέφυρα ανάμεσα στο ασύρματο κελί και σε ένα ενσύρματο δίκτυο, δηλαδή παρέχει στους ασύρματους σταθμούς πρόσβαση σε ένα ενσύρματο δίκτυο.

2.3.2 Μέθοδοι Λειτουργίας

Το πρότυπο 802.11 καθορίζει δύο μεθόδους λειτουργίας: infrastructure και ad hoc. Η πρώτη μέθοδος (Εικόνα 2.2) περιλαμβάνει το Μέσο του Συστήματος Διανομής (Distribution System Medium – DSM), ένα τουλάχιστον AP, το οποίο συνδέεται με το ενσύρματο δίκτυο και ένα σύνολο από φορητές οντότητες (Εικόνα 2.2). Αυτός ο σχηματισμός ονομάζεται Βασικό Σύνολο Υπηρεσιών (Basic Service Set – BSS). Όλοι οι σταθμοί επικοινωνούν με το AP.

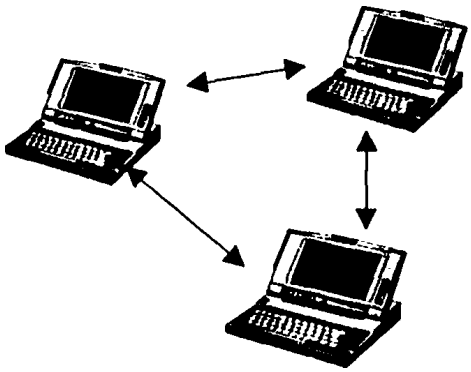
Όταν ένας κινούμενος σταθμός πρέπει να επικοινωνήσει με κάποιον άλλο, πρώτα επικοινωνεί με το AP και στη συνέχεια μέσω αυτού εγκαθίσταται η σύνδεση. Αυτό έχει σαν συνέπεια οι επικοινωνίες που αρχίζουν και καταλήγουν στο ίδιο BSS να χρειάζονται το διπλάσιο εύρος ζώνης από ότι θα χρειαζόταν μια επικοινωνία στην οποία οι σταθμοί θα επικοινωνούσαν απευθείας. Παρόλο που αυτό φαίνεται να είναι ένα σημαντικό κόστος, τα πλεονεκτήματα που παρέχονται από το AP ισοσταθμίζουν το κόστος αυτό. Ένα από αυτά τα πλεονεκτήματα είναι η προσωρινή αποθήκευση των μηνυμάτων προς έναν σταθμό ο οποίος λειτουργεί σε κατάσταση πολύ χαμηλής ισχύος.



Εικόνα 2.2. Η Μέθοδος Infrastructure

Στη μέθοδο ad hoc (που ονομάζεται επίσης μέθοδος απ' άκρο σ' άκρο (peer-to-peer) ή Ανεξάρτητο Βασικό Σύνολο Υπηρεσιών (Independent Basic Service Set-IBSS)) υπάρχει απλώς ένα σύνολο από 802.11 ασύρματους σταθμούς, οι οποίοι επικοινωνούν απευθείας ο ένας με τον άλλο, χωρίς τη χρήση σημείου πρόσβασης ή οποιασδή-

ποτε σύνδεσης με ενσύρματο δίκτυο (Εικόνα 2.3). Δεν είναι απαραίτητο να μπορούν όλοι οι σταθμοί να επικοινωνήσουν με όλους, αλλά ανήκουν όλοι στο ίδιο IBSS. Επίσης δεν υπάρχει η λειτουργία της μεταβίβασης της πληροφορίας. Έτσι αν ένας σταθμός πρέπει να επικοινωνήσει με κάποιον άλλο πρέπει αυτοί οι δύο να έρθουν σε απευθείας επικοινωνία.



Εικόνα 2.3. Η Μέθοδος Ad Hoc

Το βασικό χαρακτηριστικό αυτών των δικτύων είναι η περιορισμένη χρονική και χωρική επεκτασιμότητά τους. Ένα IBSS έχει μικρό αριθμό σταθμών και δημιουργείται για ένα συγκεκριμένο σκοπό π.χ. για τη συμμετοχή σε κάποια παρουσίαση συνεδρίου. Αυτή η μέθοδος είναι χρήσιμη για γρήγορη και εύκολη εγκατάσταση ασύρματων δικτύων, όπου δεν υπάρχουν χρήστες με ειδικές γνώσεις και οπουδήποτε δεν υπάρχει ή δεν απαιτείται ασύρματη υποδομή (π.χ. για ένα σύνολο από φορητούς υπολογιστές).

2.3.3 Το Επεκταμένο Σύνολο Υπηρεσιών και το Σύστημα Διανομής

Ένα από το πιο επιθυμητά πλεονεκτήματα ενός WLAN είναι η κινητικότητα που προσφέρει στους χρήστες του. Αυτή η κινητικότητα δε θα ήταν χρήσιμη αν ίσχυε μόνο για την περιοχή ενός BSS. Το IEEE 802.11 επεκτείνει την ακτίνα της κινητικότητας σε οποιαδήποτε απόσταση μέσω του Επεκταμένου Συνόλου Υπηρεσιών (Extended Service Set – ESS). Το ESS είναι ένα σύνολο από ένα ή περισσότερα BSS, τα οποία σχηματίζουν ένα δίκτυο. Εφόσον τα περισσότερα WLAN απαιτούν πρόσβαση σε ένα ενσύρματο LAN για διάφορες υπηρεσίες (εκτυπώσεις, αρχεία) θα πρέπει αυτά να λειτουργούν με τη μέθοδο infrastructure.

Τα AP επικοινωνούν μεταξύ τους, ώστε να προωθείται η κίνηση από το ένα BSS στο άλλο και να επιτρέπεται έτσι η μετακίνηση των κινούμενων σταθμών από ένα BSS σε ένα άλλο. Τα AP επιτυγχάνουν αυτή την επικοινωνία μέσω ενός αφηρημένου μέσου που ονομάζεται Σύστημα Διανομής (Distribution System – DS). Το DS είναι η ραχοκοκαλιά του WLAN και μπορεί να κατασκευαστεί από ενσύρματα ή ασύρματα δίκτυα. Το DS είναι ένας μηχανισμός με τον οποίο κάθε AP επικοινωνεί με κάποιο άλλο για να ανταλλάξει πλαίσια για σταθμούς στο ίδιο BSS, ή να προωθήσουν πλαίσια για σταθμούς από το ένα BSS στο άλλο, ή να ανταλλάξουν πλαίσια με ενσύρματα

δίκτυα. Όπως περιγράφεται από το πρότυπο 802.11 το DS δεν είναι απαραίτητα κάποιο δίκτυο. Το πρότυπο δε θέτει περιορισμούς στον τρόπο με τον οποίο το DS θα υλοποιηθεί, ορίζει μόνο τις υπηρεσίες που πρέπει να παρέχει. Έτσι το DS μπορεί να είναι ένα ενσύρματο δίκτυο όπως το 802.3 ή ένα ειδικού σκοπού κουτί που συνδέει τα AP και παρέχει τις απαιτούμενες υπηρεσίες μετάδοσης.

Οι επικοινωνίες που λαμβάνει ένα AP από το DS μεταδίδονται στο BSS ώστε να ληφθούν από τον παραλήπτη κινούμενο σταθμό. Για να υποστηριχθεί από το δίκτυο εξοπλισμός που δεν ανήκει στο ESS, το ESS και όλοι οι κινούμενοι σταθμοί του φαίνονται σαν ένα απλό δίκτυο MAC επιπέδου όπου όλοι οι σταθμοί είναι φυσικά ακίνητοι. Έτσι το ESS κρύβει την κινητικότητα των σταθμών από οτιδήποτε εκτός του ESS. Έτσι επιτυγχάνεται η εμμεσότητα που προσφέρει η αρχιτεκτονική του 802.11, επιτρέποντας σε υπάρχοντα πρωτόκολλα δικτύου που δεν εμπεριέχουν την έννοια της κινητικότητας να λειτουργούν σωστά με ένα WLAN, όπου υπάρχει πολλή κινητικότητα.

Μια περιοχή έρευνας αποτελεί η επικοινωνία μεταξύ των AP που χρησιμοποιούν διαφορετικά πρότυπα. Υπάρχει μια έρευνα στην οποία έχουν συνεργαστεί αρκετές βιομηχανίες για την ανάπτυξη του Πρωτοκόλλου Σημείων Πολλαπλής-Πρόσβασης (Inter-Access Point Protocol – IAPP). Εφόσον αυτή η εργασία δεν έχει περατωθεί, δεν είναι ακόμη δυνατό να επικοινωνήσουν μεταξύ τους AP διαφορετικών κατασκευαστών αρκετά καλά ώστε να επιτρέπεται η δημιουργία ESS από τα διαφορετικά αυτά AP.

2.4 Κινούμενοι και φορητοί χρήστες

Μία από τις απαιτήσεις του πρωτοκόλλου IEEE 802.11 είναι ο χειρισμός των κινούμενων (mobile), αλλά και των φορητών (portable) σταθμών. Φορητός σταθμός είναι ένας σταθμός, ο οποίος κινείται από τη μία περιοχή στην άλλη, αλλά δε χρησιμοποιείται κατά τη διάρκεια της μετακίνησης, παρά μόνο όταν βρίσκεται σε κάποιο σταθερό σημείο. Οι κινούμενοι σταθμοί έχουν πρόσβαση στο LAN και κατά τη διάρκεια της κίνησης.

Για τεχνικούς λόγους δεν αρκεί να χειριζόμαστε μόνο φορητούς σταθμούς. Οι συνέπειες των καθυστερήσεων στη διάδοσης κάνουν δύσκολη τη διάκριση ανάμεσα στους κινούμενους και τους φορητούς σταθμούς. Ακίνητοι σταθμοί φαίνονται πολύ συχνά σαν κινούμενοι λόγω των συνεπειών αυτών.

Ένα άλλο θέμα των κινούμενων σταθμών είναι ότι μπορεί συχνά να λειτουργούν με μπαταρία. Επομένως η διαχείριση της ισχύος είναι μία πολύ σημαντική μελέτη. Για παράδειγμα, δεν πρέπει να θεωρείται ότι ο δέκτης ενός σταθμού θα είναι πάντα σε λειτουργία.

2.5 Τύποι κινητικότητας (mobility)

Οι τρεις σημαντικότεροι τύποι μετακίνησης των σταθμών σε ένα δίκτυο είναι οι εξής:

1. ***Καμία μετακίνηση*** (No-transition): Σ' αυτόν τον τύπο ορίζονται δύο υποκατηγορίες, οι οποίες συνήθως δε διακρίνονται:
   α) Στατική – καμία κίνηση.
   β) Τοπική κίνηση – κίνηση των σταθμών που επικοινωνούν μέσα στην ακτίνα του φυσικού επιπέδου [π.χ. κίνηση μέσα σε μία περιοχή βασικών υπηρεσιών (Basic Service Area – BSA)].
2. ***BSS-μετακίνηση***: Αυτός ο τύπος ορίζεται ως μετακίνηση σταθμού από ένα BSS ενός ESS σε ένα άλλο BSS του ίδιου ESS.
3. ***ESS-μετακίνηση***: Αυτός ο τύπος ορίζεται ως μετακίνηση σταθμού από ένα BSS ενός ESS σε ένα BSS ενός άλλου ESS. Αυτή η περίπτωση υποστηρίζεται μόνο όταν ο σταθμός μπορεί να κινηθεί. Το 802.11 δεν μπορεί να εγγυηθεί τη διατήρηση των συνδέσεων στα ανώτερα επίπεδα. Μάλιστα είναι πολύ πιθανή η διακοπή των υπηρεσιών, γι' αυτό και έχει προταθεί η χρήση της πιστοποίησης του Mobile-IP γι' αυτή την περίπτωση [22].

Οι διαφορετικές υπηρεσίες σύνδεσης υποστηρίζουν τις διαφορετικές κατηγορίες μετακίνησης.

2.6 Υπηρεσίες του 802.11

2.6.1 Σύνδεση (Association)

Για την αποστολή ενός μηνύματος μέσα σε ένα DS, η υπηρεσία διανομής πρέπει να γνωρίζει με ποιο AP θα επικοινωνήσει για κάθε δεδομένο IEEE 802.11 σταθμό. Αυτή η πληροφορία παρέχεται στο DS μέσω μιας σύνδεσης (association). Η σύνδεση είναι αναγκαία, αλλά όχι ικανή, για την υποστήριξη BSS-μετακίνησης. Επίσης, είναι ικανή για την υποστήριξη καμίας-μετακίνησης. Η σύνδεση είναι μία Υπηρεσία Συστήματος Διανομής (Distribution Service System – DSS).

Προτού επιτραπεί σε έναν σταθμό η αποστολή μηνυμάτων μέσω ενός AP, πρέπει αυτός να συνδεθεί με το AP. Η πράξη με την οποία γίνεται η σύνδεση του σταθμού θέτει σε λειτουργία την υπηρεσία σύνδεσης (association service), η οποία παρέχει στον σταθμό AP μια αντιστοιχία στο DS. Το DS χρησιμοποιεί αυτή την πληροφορία για να πραγματοποιήσει την υπηρεσία διανομής των μηνυμάτων. Ο τρόπος με τον οποίο η πληροφορία που παρέχεται από την υπηρεσία σύνδεσης αποθηκεύεται και χρησιμοποιείται από το DS δεν καθορίζεται από το πρότυπο.

Σε οποιαδήποτε στιγμή, ένας σταθμός μπορεί να συνδεθεί με όχι περισσότερα από ένα AP. Αυτό εξασφαλίζει ότι το DS θα μπορεί να δίνει μία μοναδική απάντηση στην ερώτηση «Ποιο AP εξυπηρετεί τον σταθμό X;». Μόλις ολοκληρωθεί μία σύνδεση, ένας σταθμός μπορεί να κάνει πλήρη χρήση ενός DS (μέσω του AP) για να επικοινωνήσει. Η σύνδεση αρχικοποιείται πάντα από τον κινούμενο σταθμό και όχι από το AP. Ένα AP μπορεί να είναι συνδεδεμένο με πολλούς σταθμούς κάθε φορά.

Ένας σταθμός μαθαίνει πρώτα ποια AP υπάρχουν και στη συνέχεια κάνει αίτηση για την εγκατάσταση σύνδεσης, ενεργοποιώντας την υπηρεσία σύνδεσης.

2.6.2 Επανασύνδεση (Reassociation)

Η σύνδεση είναι ικανή για τη διανομή μηνυμάτων ανάμεσα σε IEEE 802.11 σταθμούς που δεν μετακινούνται. Για την υποστήριξη BSS-μετακίνησης απαιτούνται επιπλέον λειτουργίες. Αυτές οι επιπλέον λειτουργίες παρέχονται από την υπηρεσία επανασύνδεσης. Η επανασύνδεση είναι μία DSS.

Η υπηρεσία επανασύνδεσης ενεργοποιείται για να «μετακινήσει» μία υπάρχουσα σύνδεση από ένα AP σε ένα άλλο. Έτσι το DS εξακολουθεί να είναι ενημερωμένο για την τρέχουσα αντιστοιχία ανάμεσα στα AP και τους σταθμούς, καθώς οι σταθμοί μετακινούνται από ένα BSS σε ένα άλλο του ίδιου ESS. Η επανασύνδεση επιτρέπει επίσης την αλλαγή των χαρακτηριστικών μίας υπάρχουσας σύνδεσης ενώ ο σταθμός παραμένει συνδεδεμένος με το ίδιο AP. Η επανασύνδεση αρχικοποιείται πάντα από τον κινούμενο σταθμό.

2.6.3 Αποσύνδεση (Disassociation)

Η υπηρεσία αποσύνδεσης ενεργοποιείται όταν μία υπάρχουσα σύνδεση πρέπει να τερματιστεί. Η αποσύνδεση είναι μία DSS.

Μέσα σε ένα ESS αυτή η υπηρεσία λέει στο DS να ακυρώσει τις υπάρχουσες πληροφορίες σύνδεσης. Οι προσπάθειες αποστολής μηνυμάτων μέσω του DS σε έναν αποσυνδεδεμένο σταθμό θα είναι ανεπιτυχείς.

Η υπηρεσία αποσύνδεσης μπορεί να ενεργοποιηθεί από οποιαδήποτε πλευρά μιας σύνδεσης (AP ή μη AP- σταθμός). Η αποσύνδεση είναι ειδοποίηση και όχι αίτηση και δεν μπορεί να την αρνηθεί κανένα από τα δύο μέρη της σύνδεσης.

Τα AP μπορεί να χρειαστεί να αποσυνδεθούν από τους σταθμούς, ώστε να αφαιρεθούν για κάποιο λόγο από ένα δίκτυο. Οι σταθμοί θα προσπαθήσουν να αποσυνδεθούν όταν θα εγκαταλείψουν το δίκτυο. Πάντως, το πρωτόκολλο MAC δεν εξαρτάται από την ενεργοποίηση της υπηρεσίας αποσύνδεσης από τους σταθμούς. (η διαχείριση του MAC είναι σχεδιασμένη έτσι ώστε να διευθετεί την απώλεια ενός συνδεδεμένου σταθμού).

2.6.4 Υπηρεσίες ελέγχου πρόσβασης και εμπιστευτικότητας

Ο σχεδιασμός των ενσύρματων LAN προϋποθέτει την ύπαρξη των φυσικών χαρακτηριστικών των καλωδίων. Συγκεκριμένα, ο σχεδιασμός των ενσύρματων LAN προϋποθέτει την κλειστή και ελεγχόμενη φύση ενός ενσύρματου μέσου. Η ανοικτή φύση του μέσου ενός IEEE 802.11 LAN παραβιάζει αυτή την προϋπόθεση.

Παρέχονται λοιπόν δύο υπηρεσίες, ώστε να μπορέσει η λειτουργικότητα του IEEE 802.11 να κινείται στα ίδια επίπεδα με τις υποθέσεις των ενσύρματων LAN. Είναι η πιστοποίηση (authentication) και η μυστικότητα (privacy). Η πιστοποίηση χρησιμοποιείται στη θέση της φυσικής σύνδεσης των ενσύρματων μέσων. Η μυστικότητα χρησιμοποιείται, ώστε να παρέχεται η εμπιστευτικότητα που παρέχουν τα ενσύρματα μέσα.

2.6.5 Πιστοποίηση (Authentication)

Στα ενσύρματα LAN, μπορεί να χρησιμοποιηθεί φυσική ασφάλεια για να αποτραπεί η πρόσβαση χωρίς άδεια. Κάτι τέτοιο δεν μπορεί να συμβεί στα ασύρματα LAN, εφόσον χρησιμοποιούν ένα μέσο χωρίς ακριβή όρια.

Το IEEE 802.11 παρέχει τη δυνατότητα ελέγχου πρόσβασης στο LAN μέσω της υπηρεσίας πιστοποίησης. Αυτή η υπηρεσία χρησιμοποιείται από όλους τους σταθμούς για να δηλώσουν την ταυτότητά τους στους σταθμούς με τους οποίους θα επικοινωνήσουν. Αυτό ισχύει τόσο για τα ESS όσο και για τα IBSS δίκτυα. Αν ανάμεσα σε δύο σταθμούς δεν μπορέσει να εγκατασταθεί ένα επίπεδο πιστοποίησης αμοιβαία αποδεκτό, δεν θα μπορέσει να εγκατασταθεί κάποια σύνδεση. Η πιστοποίηση είναι μία Υπηρεσία Σταθμού (Station Service – SS).

Το IEEE 802.11 υποστηρίζει αρκετές διαδικασίες πιστοποίησης. Επίσης ο μηχανισμός που χρησιμοποιεί επιτρέπει την επέκταση των υποστηριζόμενων σχημάτων. Παρόλα αυτά στο IEEE 802.11 δεν είναι υποχρεωτική η χρήση κάποιου συγκεκριμένου σχήματος πιστοποίησης.

Το IEEE 802.11 παρέχει πιστοποίηση επιπέδου ζεύξης ανάμεσα σε δύο IEEE 802.11 σταθμούς. Δεν παρέχει όμως ούτε απ' άκρο σ' άκρο (end-to-end) (προέλευση μηνύματος προς προορισμό μηνύματος) ούτε από χρήστη σε χρήστη (user–to–user) πιστοποίηση. Χρησιμοποιείται απλώς για να φέρει την ασύρματη ζεύξη στο επίπεδο αυτών που θεωρούνται δεδομένα από τα φυσικά πρότυπα ενός ενσύρματου δικτύου. (Αυτή η χρήση της πιστοποίησης είναι ανεξάρτητη από οποιαδήποτε διαδικασία πιστοποίησης, η οποία μπορεί να χρησιμοποιείται στα υψηλότερα επίπεδα της στοίβας των πρωτοκόλλων ενός δικτύου.)

Το IEEE 802.11 υποστηρίζει την πιστοποίηση Κοινού Κλειδιού (Shared Key) και την πιστοποίηση Ανοιχτού Συστήματος (Open System). Η χρήση του πρώτου μηχανισμού πιστοποίησης απαιτεί την εφαρμογή του πρωτοκόλλου Ισοδύναμης με Ενσύρματη Μυστικότητας (Wired Equivalent Privacy – WEP). Σε ένα σύστημα πιστοποίησης Κοινού Κλειδιού η κάθε οντότητα αναγνωρίζεται από τη χρήση ενός κοινού, μυστικού κλειδιού κρυπτογράφησης WEP.

Αν είναι επιθυμητό, μπορεί να χρησιμοποιηθεί η πιστοποίηση Ανοιχτού Συστήματος, στην οποία μπορεί να πιστοποιηθεί οποιοσδήποτε σταθμός. Κάτι τέτοιο όμως μπορεί να παραβιάζει τις υποθέσεις των υψηλότερων επιπέδων του δικτύου.

Παρέχονται επίσης κάποιες λειτουργίες Βάσης Διαχείρισης Πληροφοριών (Management Information Base – MIB) για την υποστήριξη των συστημάτων πιστοποίησης του προτύπου.

Το IEEE 802.11 απαιτεί την αμοιβαία αποδεκτή και επιτυχή πιστοποίηση. Ένας σταθμός μπορεί να πιστοποιηθεί με πολλούς άλλους σταθμούς σε οποιαδήποτε δεδομένη χρονική στιγμή.

2.6.6 Προ-πιστοποίηση (Preauthentication)

Επειδή η διαδικασία της πιστοποίησης καταναλώνει πολύ χρόνο (εξαρτάται από το πρωτόκολλο πιστοποίησης που χρησιμοποιείται), η υπηρεσία πιστοποίησης μπορεί να ενεργοποιηθεί ανεξάρτητα από την υπηρεσία σύνδεσης.

Αν αφεθεί η πιστοποίηση μέχρι τη στιγμή της επανασύνδεσης, η ταχύτητα με την οποία μπορεί ένας σταθμός να επανασυνδεθεί μπορεί να ελαττωθεί, περιορίζοντας την απόδοση την κινητικότητας για την BSS-μετακίνηση. Η προ-πιστοποίηση γίνεται από έναν σταθμό ενώ αυτός είναι ήδη συνδεδεμένος με ένα άλλο AP (με το οποίο πιστοποιήθηκε προηγουμένως). Η χρήση της προ-πιστοποίησης αφαιρεί τον επιπλέον χρόνο που χρειάζεται η πιστοποίηση από τη διαδικασία επανασύνδεσης, στην οποία ο χρόνος είναι πολύ σημαντικός.

Το IEEE 802.11 δεν απαιτεί την προ-πιστοποίηση των σταθμών με τα AP, η πιστοποίηση όμως είναι απαιτούμενη πριν εγκατασταθεί οποιαδήποτε σύνδεση.

2.6.8 Από-πιστοποίηση (Deauthentication)

Η υπηρεσία της από-πιστοποίησης ενεργοποιείται όταν μία υπάρχουσα πιστοποίηση πρέπει να τερματιστεί και είναι μία SS.

Σε ένα ESS, εφόσον η πιστοποίηση είναι προαπαιτούμενη της σύνδεσης, η από-πιστοποίηση θα προκαλέσει την αποσύνδεση του σταθμού. Η από-πιστοποίηση μπορεί να ενεργοποιηθεί από οποιαδήποτε πιστοποιημένη πλευρά (το AP ή τον σταθμό). Δεν είναι αίτηση, αλλά ειδοποίηση και δεν μπορεί να την αρνηθεί καμία από τις δύο πλευρές.

2.6.9 Μυστικότητα (Privacy)

Για να μπορέσει η λειτουργικότητα των ασύρματων LAN να φτάσει το επίπεδο μυστικότητας των ενσύρματων το IEEE 802.11 παρέχει τη δυνατότητα της κρυπτογράφησης των δεδομένων. Αυτή η λειτουργία παρέχεται από τη μυστικότητα. Η μυστικότητα είναι μία SS.

Το IEEE 802.11 χρησιμοποιεί τον αλγόριθμο WEP για να παρέχει μυστικότητα ισοδύναμη με τα ενσύρματα LAN. Με τον αλγόριθμο WEP τα μηνύματα κρυπτογραφούνται ενώ χρησιμοποιούνται οι MIB λειτουργίες για την υποστήριξη του WEP. Ο αλγόριθμος αυτός θα περιγραφεί αναλυτικότερα στο επόμενο κεφάλαιο.

Βέβαια η μυστικότητα μπορεί να εφαρμοστεί μόνο για τα πλαίσια δεδομένων και για μερικά πλαίσια Διαχείρισης της Πιστοποίησης. Όλοι οι σταθμοί ξεκινούν «ανοιχτά» (in the clear) την εγκατάσταση των υπηρεσιών πιστοποίησης και μυστικότητας.

Η προκαθορισμένη κατάσταση μυστικότητας για όλους τους σταθμούς είναι «ανοιχτή». Αν δεν ενεργοποιηθεί η υπηρεσία μυστικότητας όλα τα μηνύματα θα αποστέλλονται μη κρυπτογραφημένα. Αν αυτό δε γίνει δεκτό από μία από τις δύο πλευρές, τα πλαίσια δεδομένων δε θα μεταδίδονται σωστά μεταξύ των LLC οντοτήτων. Τα μη

κρυπτογραφημένα πλαίσια που φτάνουν σ' έναν σταθμό στον οποίο η μυστικότητα είναι υποχρεωτική, καθώς και κρυπτογραφημένα πλαίσια δεδομένων που χρησιμοποιούν κάποιο άγνωστο για τον σταθμό κλειδί, απορρίπτονται χωρίς ειδοποίηση στο LLC.

ΚΕΦΑΛΑΙΟ 3

ΑΣΦΑΛΕΙΑ

3.1 Απαιτήσεις Ασφάλειας

Εξαιτίας του γεγονότος ότι τα ασύρματα δίκτυα χρησιμοποιούν ένα διαμοιραζόμενο μέσο, οτιδήποτε μεταδίδεται σ' αυτό μπορεί να υποκλαπεί και να παραποιηθεί. Η κρυπτογράφηση και η πιστοποίηση είναι πάντα απαραίτητες για την ανάπτυξη ενός ασύρματου συστήματος. Ο στόχος της προσθήκης αυτών των χαρακτηριστικών ασφάλειας είναι να γίνει το ασύρματο δίκτυο το ίδιο ασφαλές με ένα ενσύρματο.

Όταν εφαρμόζονται η κρυπτογράφηση και η πιστοποίηση πρέπει να ληφθούν υπόψη τρεις παράγοντες:

- *Η ανάγκη των πελατών για μυστικότητα.* Πόσο ισχυρά πρέπει να είναι τα πρωτόκολλα και πόσο θα κοστίζουν (σε χρήματα και χρόνο).
- *Η ευκολία χρήσης του.* Αν η εφαρμογή της ασφάλειας είναι δύσχρηστη δεν πρόκειται να χρησιμοποιηθεί.
- *Κυβερνητικοί κανόνες.* Η κρυπτογράφηση θεωρείται από πολλές κυβερνήσεις (συμπεριλαμβανομένων και των HIIA) ως πολεμικός εξοπλισμός, οπότε όλα τα προϊόντα κρυπτογράφησης ελέγχονται πριν γίνει η εξαγωγή τους.

Υπάρχουν τρεις βασικές μέθοδοι για την εξασφάλιση ασφαλούς πρόσβασης σε ένα AP που ανήκει σε κάποιο 802.11 δίκτυο:

- Ο Προσδιοριστής Συνόλου Υπηρεσιών (Service Set IDentifier – SSID).
- Το φιλτράρισμα των MAC διευθύνσεων (MAC address filtering).
- Η κρυπτογράφηση με τη χρήση του πρωτοκόλλου WEP.

Μπορεί να εφαρμοστεί ακόμη και μία μόνο από τις παραπάνω μεθόδους, αλλά ο συνδυασμός και των τριών είναι η πιο ασφαλής λύση.

3.2 Ο SSID

Ο έλεγχος πρόσβασης του δικτύου μπορεί να πραγματοποιηθεί χρησιμοποιώντας έναν SSID, ο οποίος αντιστοιχεί σε ένα AP ή σε ένα σύνολο από AP. Το κάθε AP χαρακτηρίζεται από ένα συγκεκριμένο SSID, το οποίο πρέπει να γνωρίζουν όλοι οι σταθμοί που επιθυμούν να συνδεθούν με το συγκεκριμένο AP. Αν ένας υπολογιστής θέλει να έχει πρόσβαση σε πολλά AP, πρέπει να έχει το σωστό SSID για κάθε AP.

Επειδή ο κάθε σταθμός πρέπει να δώσει τον σωστό SSID για να αποκτήσει πρόσβαση στο AP, ο SSID λειτουργεί σαν ένα απλό password και συνεπώς αποτελεί μέτρο ασφάλειας. Αυτή όμως η στοιχειώδης ασφάλεια παύει να υφίσταται όταν το AP είναι ρυθμισμένο να εκπέμπει καθολικά τον SSID του. Όταν συμβαίνει αυτό τότε επιτρέπεται σε οποιονδήποτε σταθμό ο οποίος μπορεί να μη γνωρίζει τον SSID να τον λάβει και να αποκτήσει πρόσβαση στο AP. Επιπλέον επειδή οι χρήστες ρυθμίζουν οι ίδιοι τα συστήματα-πελάτες τους με τους αντίστοιχους SSID, αυτοί είναι ευρέως γνωστοί και μπορούν εύκολα να χρησιμοποιηθούν από χρήστες στους οποίους κανονικά δεν επιτρέπεται η πρόσβαση.

3.3 Το Φιλτράρισμα των MAC Διευθύνσεων

Όπως ένα AP ή ένα σύνολο από AP αναγνωρίζονται από τον SSID τους, έτσι κι ένας σταθμός μπορεί να αναγνωριστεί από τη μοναδική MAC διεύθυνση της 802.11 κάρτας δικτύου του. Για μεγαλύτερη ασφάλεια σε ένα 802.11 δίκτυο, το κάθε AP μπορεί να προγραμματιστεί ώστε να κρατάει μια λίστα από MAC διευθύνσεις που αντιστοιχούν στους σταθμούς οι οποίοι επιτρέπεται να έχουν πρόσβαση στο AP. Αν η MAC διεύθυνση κάποιου σταθμού δεν ανήκει στη λίστα, τότε δεν του επιτρέπεται να συνδεθεί με το AP.

Το φιλτράρισμα των MAC διευθύνσεων παρέχει ικανοποιητική ασφάλεια, αλλά ταιριάζει περισσότερο σε μικρά δίκτυα. Το κάθε AP πρέπει να ρυθμιστεί από κάποιον (π.χ. από τον διαχειριστή του δικτύου) με ένα σύνολο από MAC διευθύνσεις και η λίστα αυτή πρέπει να διατηρείται πάντα ενημερωμένη. Αυτός ο επιπλέον φόρτος στη διαχείριση περιορίζει την επεκτασιμότητα αυτής της προσέγγισης.

Μια πιλοτική εφαρμογή που χρησιμοποιεί αυτή την τεχνική υλοποιήθηκε στο Πανεπιστήμιο UC Irvine [11]. Όσοι φοιτητές του Πανεπιστημίου επιθυμούν να έχουν πρόσβαση στο δίκτυο πρέπει να εγγραφούν, δίνοντας τη MAC διεύθυνσή τους. Στη συνέχεια τους παρέχεται ένα μοναδικό μυστικό κλειδί, το οποίο χρησιμοποιείται από τον παροχέα υπηρεσιών δικτύου για τον έλεγχο της πρόσβασης.

3.4 Ο Αλγόριθμος WEP

Τα WLAN στην απλή τους μορφή είναι ευάλωτα σε παθητική υποκλοπή και πολύ πιθανό σε ακόμη περισσότερα. Η καλύτερος τρόπος άμυνας είναι η κρυπτογράφηση. Αναγνωρίζοντας αυτή την ανάγκη, η IEEE 802.11 ορίζει ένα προαιρετικό σχήμα κρυπτογράφησης, το οποίο ονομάζεται Μυστικότητα Ισοδύναμη με την Ενσύρματη (Wired Equivalent Privacy - WEP) ώστε να προστατευθεί η επικοινωνία του επιπέδου ζεύξης από υποκλοπή καθώς κι από άλλες επιθέσεις. Όπως δηλώνει και το όνομά του, ο αλγόριθμος WEP έχει ως στόχο να δώσει στα WLAN επίπεδο μυστικότητας ισοδύναμο με αυτό των ενσύρματων LAN, κρυπτογραφώντας το RF σήμα. Ο αλγόριθμος WEP αποτελεί μέρος ενός διεθνούς προτύπου, το οποίο εφαρμόστηκε από διάφορους κατασκευαστές στο 802.11 υλικό τους και είναι προς το παρόν κοινόχρηστος. Τα περισσότερα προϊόντα της αγοράς που είναι συμβατά με το IEEE 802.11 υποστηρίζουν τον αλγόριθμο WEP. Είναι σχεδιασμένος έτσι ώστε να είναι αρκετά ισχυρός και να ικανοποιεί τις ανάγκες των περισσότερων ανθρώπων. Ενεργοποιώντας τον WEP, επιτρέπεται επίσης και η πιστοποίηση των σταθμών, επομένως με τον τρόπο αυτό παρέχεται καλύτερος έλεγχος πρόσβασης στο WLAN.

Η εμπιστευτικότητα των δεδομένων εξαρτάται από μία εξωτερική υπηρεσία διαχείρισης κλειδιού για την κατανομή των κλειδιών που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Πρόκειται για ένα θέμα ανοιχτό προς το παρόν, εφόσον δεν υπάρχει ακόμη κάποιος αλγόριθμος που να δίνει ικανοποιητικά αποτελέσματα στον τομέα αυτό.

Υπάρχει επίσης η δυνατότητα να ορίσουμε ότι ένα WLAN υποστηρίζει μυστικότητα, αλλά όχι πιστοποίηση. Κάτι τέτοιο όμως δεν ενδείκνυται, εφόσον αυτός ο συνδυασμός αφήνει το σύστημα ανοιχτό σε πολύ σοβαρές απειλές για την ασφάλεια του δικτύου.

Πρέπει να σημειωθεί πως αν το WEP δεν ικανοποιεί κάποιο χρήστη, μπορεί αυτός να χρησιμοποιήσει την IPSEC (Ασφάλεια IP – IP Security) για να παρέχει ασφάλεια στην κίνηση των IP δεδομένων μέσα στο WLAN. Μια τέτοια τακτική μπορεί να πετύχει το ίδιο αποτέλεσμα με το WEP, αλλά δίνει περισσότερες εναλλακτικές λύσεις όσον αφορά στη μέθοδο κρυπτογράφησης που θα χρησιμοποιηθεί.

3.4.1 Τα πλεονεκτήματα του WEP

Ο αλγόριθμος WEP έχει επιλεγεί επειδή έχει τις εξής ιδιότητες:

- *Είναι αρκετά ισχυρός*: Η ασφάλεια που παρέχει ο αλγόριθμος βασίζεται στη δυσκολία αποκάλυψης του κλειδιού με την τεχνική της εξαντλητικής αναζήτησης. Αυτό με τη σειρά του σχετίζεται με το μέγεθος του μυστικού κλειδιού και τη συχνότητα αλλαγής του. Ο WEP επιτρέπει την αλλαγή του κλειδιού.
- *Είναι αυτο-συγχρονιζόμενος για κάθε μήνυμα*: Αυτή η ιδιότητα είναι πολύ σημαντική για έναν αλγόριθμο κρυπτογράφησης επιπέδου ζεύξης δεδομένων, όπου η αποστολή «καλύτερης προσπάθειας» (best effort) θεωρείται δεδομένη και οι ρυθμοί απώλειας των δεδομένων μπορεί να είναι υψηλοί.

- *Είναι αποδοτικός*: Ο αλγόριθμος WEP είναι αποδοτικός και μπορεί να υλοποιηθεί είτε στο υλικό είτε στο λογισμικό.
- *Μπορεί να γίνει η εξαγωγή του*: Έχει γίνει κάθε προσπάθεια ώστε ο σχεδιασμός της λειτουργίας του WEP να μεγιστοποιεί τις πιθανότητες έγκρισης εξαγωγής του από τις ΗΠΑ. Βέβαια λόγω του πολιτικού και νομικού κλίματος που επικρατεί σε ότι αφορά την κρυπτογράφηση δεν μπορεί να υπάρξει καμία εγγύηση ότι οποιαδήποτε εφαρμογή χρησιμοποιεί τον WEP θα μπορεί να εξάγεται από τις ΗΠΑ.
- *Είναι προαιρετικός*: Η εφαρμογή και χρήση του WEP είναι προαιρετική για το IEEE 802.11.

Δυστυχώς, ο WEP παρά τα πλεονεκτήματά του δεν είναι ικανός να πετύχει τους στόχους που αφορούν την ασφάλεια ενός WLAN. Εκτός από τη χρήση του γνωστού αλγορίθμου RC4, ο οποίος θεωρείται ασφαλής, ο WEP έχει ένα σύνολο από αδυναμίες, που αποτελούν αφορμή για ένα σύνολο από επιθέσεις, τόσο ενεργητικές όσο και παθητικές, οι οποίες επιτρέπουν την υποκλοπή και την επέμβαση στις ασύρματες επικοινωνίες. Θα αναφερθούμε διεξοδικότερα στις αδυναμίες αυτές στο Κεφάλαιο 4.

3.4.2 Η θεωρία λειτουργίας της Κρυπτογράφησης

Η διαδικασία μεταβολής (δυαδικών) δεδομένων με σκοπό την απόκρυψη του περιεχομένου της πληροφορίας τους ονομάζεται κρυπτογράφηση (encryption - E). Τα δεδομένα που δεν είναι κρυπτογραφημένα ονομάζονται απλό κείμενο (plaintext - P). Τα κρυπτογραφημένα δεδομένα ονομάζονται κρυπτογραφημένο κείμενο (ciphertext - C). Ένας αλγόριθμος κρυπτογράφησης (cipher) είναι μία μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Οι σύγχρονοι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν μία ακολουθία κλειδιού (keystream - k) για να μεταβάλλουν την έξοδό τους. Η συνάρτηση κρυπτογράφησης E εφαρμόζεται στο P για την παραγωγή του C:

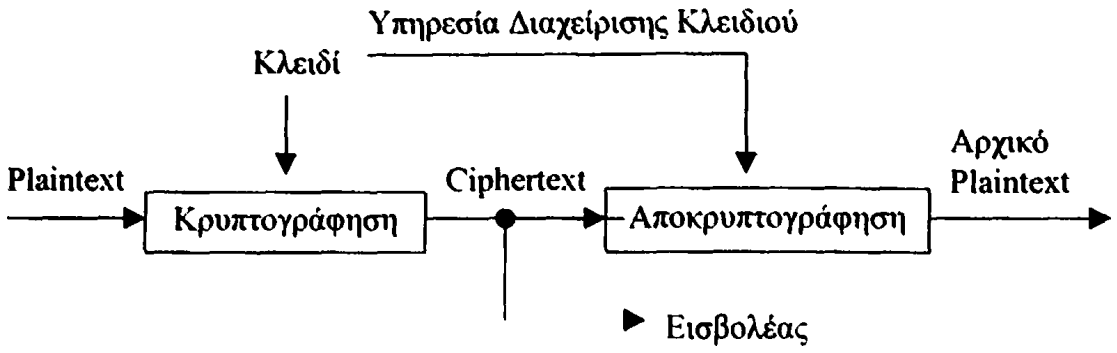
$$E_k(P) = C$$

Η διαδικασία μεταβολής του ciphertext σε plaintext ονομάζεται αποκρυπτογράφηση (decryption - D). Κατά τη διαδικασία αυτή η συνάρτηση αποκρυπτογράφησης D εφαρμόζεται στο C για την παραγωγή του P:

$$D_k(C) = P$$

Αν μπορεί να χρησιμοποιηθεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση τότε ισχύει το εξής (Εικόνα 3.1):

$$D_k(E_k(P)) = P$$



Εικόνα 3.1: Ένα εμπιστευτικό κανάλι δεδομένων

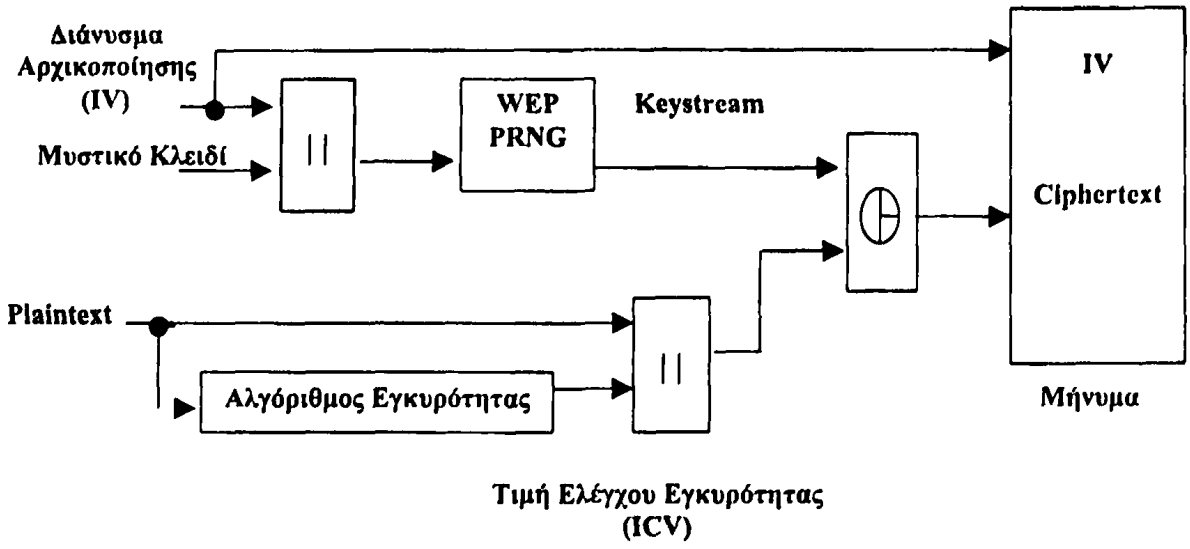
3.4.3 Ο Αλγόριθμος RC4

Ο αλγόριθμος RC4 αναπτύχθηκε το 1987 από τον Ron Rivest και τα πνευματικά δικαιώματα τα έχει η εταιρεία RSA Data Security. Ο RC4 είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης, ο οποίος παίρνει ως είσοδο ένα κλειδί και παράγει μια σειρά από ψευδοτυχαία bit, στα οποία εφαρμόζεται η πράξη του αποκλειστικού-ή με τα αρχικά δεδομένα (plaintext) και παράγεται το ciphertext και αντίστροφα. Το μήκος του plaintext δε χρειάζεται να είναι σταθερό. Το κλειδί πρέπει να το μοιράζονται όλοι οι σταθμοί που επιθυμούν να επικοινωνήσουν και σ' αυτό οφείλεται το γεγονός ότι μπορούν να χρησιμοποιούν τον ίδιο αλγόριθμο όλοι οι σταθμοί, αλλά μόνο αυτοί που γνωρίζουν το κοινό κλειδί έχουν τη δυνατότητα να αποκρυπτογραφήσουν σωστά τα κρυπτογραφημένα πλαίσια. Χρησιμοποιείται στο πρωτόκολλο SSL του Internet και σε πολλά άλλα προϊόντα κρυπτογράφησης. Τα πλεονεκτήματα της χρήσης του RC4 είναι τα εξής:

- Το κλειδί είναι ανεξάρτητο από το plaintext.
- Η κρυπτογράφηση και η αποκρυπτογράφηση είναι ταχύτατες, περίπου 10 φορές γρηγορότερη από τον DES.
- Είναι αρκετά απλός αλγόριθμος, οπότε μπορεί πολύ εύκολα να υλοποιηθεί από τους περισσότερους προγραμματιστές.
- Πιστεύεται πως δεν είναι ευάλωτος σε διαφορική και γραμμική κρυπτανάλυση.

3.4.4 Η θεωρία λειτουργίας του WEP

Ο WEP βασίζεται σε ένα μυστικό κλειδί k, το οποίο μοιράζονται οι σταθμοί που επικοινωνούν. Χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Είναι μία μορφή ηλεκτρονικού βιβλίου κωδικοποίησης στο οποίο εκτελούμε τη διαδικασία του αποκλειστικού-ή πάνω σε ένα βιβλίο από plaintext με ένα ψευδοτυχαίο κλειδί ίσου μήκους. Αυτή η ακολουθία κλειδί (keystream) δημιουργείται από τον αλγόριθμο WEP. Η διαδικασία που ακολουθείται περιγράφεται στην Εικόνα 3.2.



Εικόνα 3.2: Η κρυπτογράφηση WEP

Εφαρμόζονται δύο διαδικασίες στα δεδομένα του plaintext. Η μία το κρυπτογραφεί με τη χρήση του αλγορίθμου RC4 και η άλλη το προστατεύει από μη εξουσιοδοτημένη μεταβολή των δεδομένων.

Σύμφωνα με τα παραπάνω λοιπόν για την κρυπτογράφηση με τη χρήση του αλγορίθμου WEP αρχικά το μυστικό κλειδί (40 bit) συνενώνεται με ένα διάνυσμα αρχικοποίησης (Initialization Vector – IV, 24 bit) και προκύπτει ένα συνολικό κλειδί των 64 bit. Το κλειδί αυτό αποτελεί είσοδο σε μία Γεννήτρια Ψευδοτυχαίων Αριθμών (Pseudo Random Number Generator - PRNG). Η PRNG (λειτουργεί σύμφωνα με τον αλγόριθμο RC4) παράγει σαν έξοδο μία ψευδοτυχαία ακολουθία κλειδιού (keystream), η οποία εξαρτάται από το κλειδί που δίνεται σαν είσοδος. Στην ακολουθία που προκύπτει εφαρμόζεται το αποκλειστικό-ή με το plaintext. Το αποτέλεσμα αυτής της διαδικασίας είναι ένα ciphertext ίσου μεγέθους με τα δεδομένα που πρόκειται να μεταδοθούν (plaintext) συν 4 επιπλέον byte. Αυτό συμβαίνει επειδή το keystream χρησιμοποιείται και για την προστασία της τιμής ελέγχου εγκυρότητας (Integrity Check Value – ICV).

Για την προστασία από μη εξουσιοδοτημένη μεταβολή των δεδομένων, ένας αλγόριθμος εγκυρότητας (CRC-32) εφαρμόζεται στο plaintext για να παράγει την τιμή ICV.

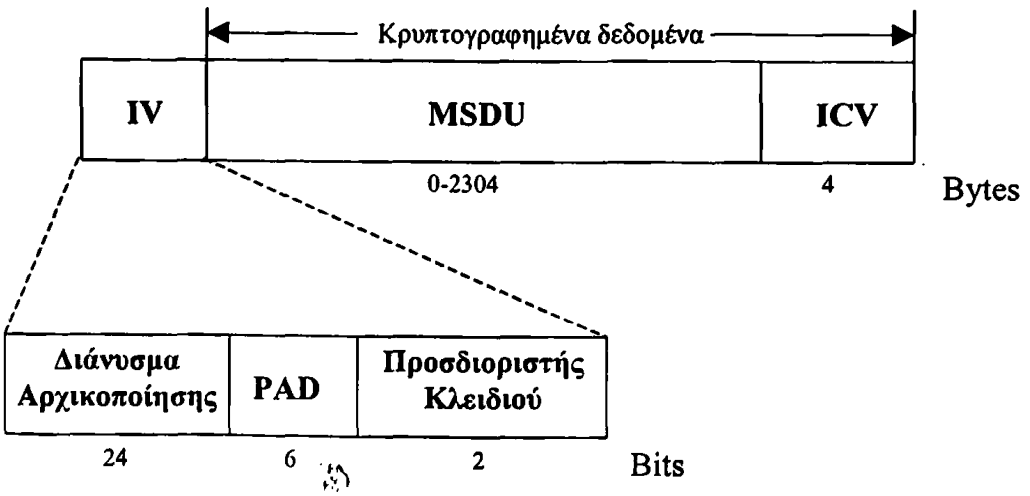
Το ciphertext δημιουργείται ως εξής. Αρχικά υπολογίζεται το ICV χρησιμοποιώντας τον αλγόριθμο CRC-32 στο plaintext κι έπειτα συνενώνεται το ICV με το plaintext. Στη συνέχεια επιλέγεται ένα τυχαίο IV και συνενώνεται με το μυστικό κλειδί. Με είσοδο αυτή τη συνένωση ο αλγόριθμος RC4 δίνει ως έξοδο μία ψευδοτυχαία ακολουθία κλειδί. Έπειτα κρυπτογραφείται η συνένωση του plaintext με το ICV εκτελώντας την πράξη XOR με την ψευδοτυχαία ακολουθία κλειδί. Τέλος αποστέλλεται μαζί με το ciphertext και το IV, το οποίο τοποθετείται στην αρχή του μηνύματος. Το IV, το

plaintext και το ICV συνθέτουν τα πραγματικά δεδομένα που αποστέλλονται στο πλαίσιο δεδομένων.

Κατά τη διαδικασία της αποκρυπτογράφησης το IV του εισερχόμενου μηνύματος χρησιμοποιείται για τη δημιουργία της ακολουθίας κλειδί που είναι απαραίτητη για την αποκρυπτογράφηση του μηνύματος. Συνθέτοντας το ciphertext με τη σωστή ακολουθία κλειδί εξάγεται το plaintext και το ICV. Στη συνέχεια εφαρμόζεται ο αλγόριθμος ελέγχου εγκυρότητας στο plaintext που αποκαλύφθηκε και συγκρίνεται το ICV που προκύπτει (ICV΄) με το ICV που μεταδόθηκε μαζί με το μήνυμα. Αν τα ICV και ICV΄ δεν είναι ίσα, το μήνυμα έχει σφάλματα και αποστέλλεται στη διαχείριση του MAC και στον αποστολέα σταθμό μία ειδοποίηση σφάλματος. Οι σταθμοί που αποστέλλουν λανθασμένα μηνύματα (επειδή δεν είναι δυνατή η αποκρυπτογράφηση) δεν πιστοποιούνται. Το ίδιο μυστικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση/αποκρυπτογράφηση των πλαισίων δεδομένων χρησιμοποιείται και για την πιστοποίηση των σταθμών.

Η WEP PRNG (RC4) είναι το κρίσιμο στοιχείο της WEP διαδικασίας, εφόσον είναι η πραγματική μηχανή κρυπτογράφησης. Το IV επεκτείνει τη ζωή του μυστικού κλειδιού και παρέχει την ιδιότητα του αυτό-συγχρονισμού στον αλγόριθμο. Το μυστικό κλειδί παραμένει σταθερό, ενώ το IV μεταβάλλεται περιοδικά. Κάθε νέο IV δημιουργεί ένα νέο keystream, επομένως υπάρχει ένα προς ένα αναλογία του IV και της εξόδου. Το IV μπορεί να αλλάζει για κάθε νέο μήνυμα και εφόσον τοποθετείται πάντα στο πλαίσιο του μηνύματος ο παραλήπτης θα είναι πάντα σε θέση να αποκρυπτογραφεί το μήνυμα.

Πρέπει να σημειωθεί ότι κρυπτογραφείται μόνο το κυρίως σώμα των πλαισίων δεδομένων. Έτσι ολόκληρο το MAC πρόθεμα (header) του πλαισίου δεδομένων παραμένει μη κρυπτογραφημένο και διαθέσιμο σε οποιονδήποτε εισβολέα. Επομένως το WEP παρέχει προστασία του περιεχομένου των πλαισίων δεδομένων, αλλά δεν προστατεύει το WLAN από άλλου είδους απειλές ασφάλειας όπως είναι η ανάλυση της κίνησης των δεδομένων (Εικόνα 3.3).



Εικόνα 3.3: Η WEP επέκταση του Σώματος του Πλαισίου

3.4.5 Η Διαχείριση των Κλειδιών

Το πρότυπο 802.11 παρέχει δύο μηχανισμούς για την επιλογή ενός κλειδιού κρυπτογράφησης ή αποκρυπτογράφησης. Ο πρώτος μηχανισμός χρησιμοποιεί ένα σύνολο από τέσσερα προκαθορισμένα κλειδιά. Τα κλειδιά αυτά τα μοιράζονται όλοι οι σταθμοί ενός BSS ή ενός ESS. Το πλεονέκτημα από τη χρήση των προκαθορισμένων κλειδιών είναι ότι εφόσον ο σταθμός αποκτήσει τα κλειδιά αυτά είναι σε θέση να επικοινωνήσει με ασφάλεια με όλους τους σταθμούς του BSS ή του ESS. Το μειονέκτημα είναι ότι αυτά τα κλειδιά κατανέμονται σε πολλούς σταθμούς κι έτσι είναι πολύ πιθανή η αποκάλυψή τους.

Ο δεύτερος μηχανισμός επιτρέπει σε κάποιον σταθμό να καθορίσει μια σχέση «αντιστοιχίας κλειδιού» (key mapping) με κάποιον άλλο σταθμό. Η αντιστοιχία κλειδιών επιτρέπει σε κάποιον σταθμό να δημιουργήσει ένα κλειδί, το οποίο θα χρησιμοποιείται για την επικοινωνία με έναν μόνο σταθμό. Παρόλο που δεν είναι απαιτούμενη από το πρότυπο αυτή η ένα προς ένα αντιστοιχία, είναι ο πιο ασφαλής τρόπος λειτουργίας ενός σταθμού, εφόσον το κάθε κλειδί θα το γνωρίζει μόνο ένας σταθμός. Όσο μικρότερος είναι ο αριθμός των σταθμών που χρησιμοποιούν το ίδιο κλειδί τόσο λιγότερο πιθανή θα είναι και η αποκάλυψη του κλειδιού.

Ένα χαρακτηριστικό του 802.11 ελέγχει τη χρήση του WEP σε έναν σταθμό. Αν πάρει την τιμή «ψευδής» τότε όλα τα πλαίσια αποστέλλονται στον σταθμό μη κρυπτογραφημένα. Αν είναι «αληθής», όλα τα πλαίσια θα αποστέλλονται κρυπτογραφημένα εκτός εάν για κάποιους παραλήπτες η χρήση του WEP είναι απενεργοποιημένη (θα πρέπει όμως να υπάρχει κάποια σχέση αντιστοιχίας κλειδιού με τον συγκεκριμένο παραλήπτη).

Για την κρυπτογράφηση ενός πλαισίου μπορεί να χρησιμοποιηθεί κάποιο από τα προκαθορισμένα κλειδιά μόνο στην περίπτωση που δεν υπάρχει κάποια αντιστοιχία κλειδιού ανάμεσα στον αποστολέα και τον παραλήπτη σταθμό. Υπάρχει περίπτωση να μην είναι διαθέσιμα και τα τέσσερα προκαθορισμένα κλειδιά. Στην περίπτωση όμως που είναι διαθέσιμα περισσότερα του ενός, ο σταθμός επιλέγει ένα από αυτά, σύμφωνα με κάποιον αλγόριθμο ο οποίος δεν ορίζεται από το πρότυπο και το χρησιμοποιεί για την κρυπτογράφηση του σώματος του πλαισίου (frame body) που πρέπει να σταλεί. Το WEP πρόθεμα και επίθεμα συνενώνονται με το κρυπτογραφημένο σώμα του πλαισίου. Το προκαθορισμένο κλειδί που χρησιμοποιείται δηλώνεται στο πεδίο του Προσδιοριστή Κλειδιού (KeyID) του προθέματος και η τιμή ελέγχου εγκυρότητας (ICV) στο επίθεμα (Εικόνα 3.3). Αν δεν υπάρχουν διαθέσιμα προκαθορισμένα κλειδιά το πλαίσιο απορρίπτεται.

Αν από την άλλη, υπάρχει κάποια αντιστοιχία κλειδιού ανάμεσα στον αποστολέα και τον παραλήπτη, τότε μόνο το κοινό αυτό κλειδί πρέπει να χρησιμοποιείται για την κρυπτογράφηση των πλαισίων που θα αποστέλλονται στον συγκεκριμένο παραλήπτη και το οποίο είναι αποθηκευμένο σε έναν πίνακα αντιστοίχησης κλειδιών (WEP Key Mappings Table). Υπάρχει κι ένας ακόμη πίνακας (WEP Key Mapping WEP On), ο οποίος καθορίζει για ποιους σταθμούς είναι ενεργοποιημένο το WEP και για ποιους όχι. Όταν πρόκειται να σταλεί ένα τέτοιο πλαίσιο, τότε το αντίστοιχο κλειδί επιλέγεται από τον πίνακα αντιστοιχίας κλειδιών κι εφόσον η αντίστοιχη τιμή στον πίνακα WEP Key Mapping WEP On είναι αληθής, το πλαίσιο αποστέλλεται κρυπτογραφη-

μένο. Στην περίπτωση αυτή η τιμή του Προσδιοριστή Κλειδιού είναι ίση με 0. Αν στον πίνακα Key Mapping WEP On η τιμή για τον συγκεκριμένο παραλήπτη είναι ψευδής τότε το πλαίσιο αποστέλλεται μη κρυπτογραφημένο.

Υπάρχει επίσης και η λειτουργία η οποία ελέγχει την αποστολή (Privacy Invoked) και αποδοχή των πλαισίων (Exclude Unencrypted). Όταν η δεύτερη είναι ψευδής, τότε όλα τα πλαίσια, κρυπτογραφημένα ή όχι, λαμβάνονται. Όταν όμως είναι αληθής, τότε ο σταθμός θα λάβει μόνο τα κρυπτογραφημένα πακέτα και τα υπόλοιπα απορρίπτονται. Σ' αυτή την περίπτωση δεν παρέχεται καμία ειδοποίηση στα πρωτόκολλα των υψηλότερων επιπέδων για τα πλαίσια που έχουν απορριφθεί.

Τέλος υπάρχουν δύο μετρητές που σχετίζονται με το WEP. Ο Μετρητής Μη Αποκρυπτογραφημένων (Undecryptable Count) που αντιπροσωπεύει τον αριθμό των κρυπτογραφημένων μηνυμάτων τα οποία ελήφθησαν αλλά δεν μπορούσαν να αποκρυπτογραφηθούν. Ο Μετρητής Λανθασμένων ICV (ICV Error Count) αντιπροσωπεύει τον αριθμό των πλαισίων για τα οποία υπήρχε κάποιο κλειδί που αποκρυπτογραφούσε σωστά το μήνυμα, αλλά η τιμή ICV ήταν λανθασμένη. Αυτοί οι δύο μετρητές θα πρέπει να παρακολουθούνται προσεκτικά γιατί μπορούν να δώσουν ενδείξεις για πιθανές επιθέσεις. Αν ο πρώτος μετρητής αυξάνει απότομα μπορεί κανείς να καταλάβει πότε το δίκτυο δέχεται επίθεση άρνησης υπηρεσιών (denial of service), ενώ αν αυξάνει απότομα ο δεύτερος μετρητής μια επίθεση αποκάλυψης του κλειδιού βρίσκεται κατά πάσα πιθανότητα σε εξέλιξη.

Πρέπει να σημειωθεί ότι υπάρχει μια ακόμη υλοποίηση του WEP, η οποία χρησιμοποιεί κλειδί μήκους 128 bit (μυστικό κλειδί των 104 bit), αλλά υπόκειται στην έγκριση του ελέγχου εξαγωγών των ΗΠΑ. Για αγορές εξαγωγών όπως η Σιγκαπούρη, αυτό σημαίνει 64-bit RC4 (με μυστικό κλειδί των 40-bit). Οι κάτοικοι των ΗΠΑ απολαμβάνουν την κρυπτογράφηση των 128-bit, η οποία φυσικά παρέχει πιο ικανοποιητικά επίπεδα ασφάλειας.

3.5 Η Πιστοποίηση

Η πιστοποίηση (authentication) είναι μια από τις υπηρεσίες του επιπέδου MAC και παρέχει έναν μηχανισμό με τον οποίο ένας σταθμός μπορεί να αποδείξει την ταυτότητά του σε κάποιον άλλο σταθμό του WLAN. Είναι μια διαδικασία κατά την οποία ανταλλάσσονται ερωτήσεις, ισχυρισμοί και αποτελέσματα. Για παράδειγμα θα μπορούσε ένας σταθμός να ισχυριστεί ότι είναι ο σταθμός 'Α' και να ρωτήσει τον σταθμό Β ποιος είναι. Στο σημείο αυτό η διαδικασία της πιστοποίησης διαφέρει ανάλογα με τον αλγόριθμο που χρησιμοποιείται. Μπορεί να συνεχίσει με τον σταθμό Β να λέει «Απόδειξέ μου ότι είσαι όντως ο σταθμός Α» και να ισχυρίζεται ότι ο ίδιος είναι ο σταθμός Β. Τότε ο σταθμός Α θα πρέπει να προσφέρει κάποια απόδειξη της ταυτότητάς του και θα απαιτήσει κάποια τέτοιου είδους απόδειξη από τον Β. Αν ήταν αποδεκτές οι αποδείξεις αυτές τότε ο κάθε σταθμός απαντά στον άλλο ότι ο ισχυρισμός του για την ταυτότητά του είναι πιστευτός.

Η πιστοποίηση μπορεί να χρησιμοποιηθεί μεταξύ δύο οποιωνδήποτε σταθμών. Είναι όμως προτιμότερο να γίνεται ανάμεσα σε έναν σταθμό κι ένα AP σε κάποιο LAN υποδομής. Στην περίπτωση αυτή το AP είναι το σημείο εισόδου του κάθε σταθμού στο ESS και πιθανώς στο ενσύρματο LAN πίσω από το ESS. Θα πρέπει να υπάρχει πλή-

ρης απόδειξη της ταυτότητας των σταθμών αν το δίκτυο πρέπει να προστατευθεί από μη εξουσιοδοτημένους χρήστες.

Υπάρχουν τα παρακάτω είδη πιστοποίησης στο 802.11, όπως περιγράφονται από το πρότυπο:

- **Πιστοποίηση Ανοιχτού Συστήματος.** Είναι η προκαθορισμένη υπηρεσία πιστοποίησης, η οποία δε χρησιμοποιεί πιστοποίηση.
- **Πιστοποίηση Κοινού Κλειδιού.** Αυτή περιλαμβάνει ένα κοινό μυστικό κλειδί που χρησιμοποιείται για την πιστοποίηση του σταθμού στο AP.

Στην Πιστοποίηση Ανοιχτού Συστήματος (Open System) ένας σταθμός μπορεί να συνδεθεί με οποιοδήποτε AP και να ακούσει όλα τα δεδομένα. Δεν πρόκειται για αλγόριθμο πιστοποίησης, εφόσον δεν υπάρχει η έννοια της επαλήθευσης της ταυτότητας των σταθμών. Εφαρμόζεται συνήθως στις περιπτώσεις όπου είναι πολύ σημαντική η ευκολία στη χρήση και ο διαχειριστής του δικτύου δεν επιθυμεί να ασχοληθεί καθόλου με την ασφάλεια του WLAN. Αν όμως απαιτείται ο έλεγχος πρόσβασης του δικτύου δε θα πρέπει να χρησιμοποιείται η Πιστοποίηση Ανοιχτού Συστήματος.

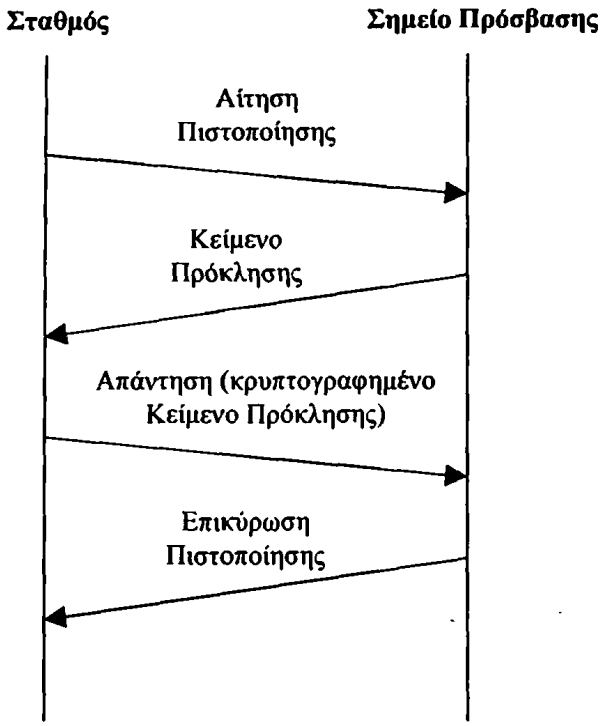
Η Πιστοποίηση Κοινού Κλειδιού (Shared Key) παρέχει μεγαλύτερη ασφάλεια από την προηγούμενη προσέγγιση. Για να χρησιμοποιηθεί η Πιστοποίηση Κοινού Κλειδιού από έναν σταθμό πρέπει αυτός να μπορεί να εκτελέσει τον αλγόριθμο WEP. Στην Εικόνα 3.4 περιγράφεται η λειτουργία της πιστοποίησης κοινού κλειδιού. Το κοινό μυστικό κλειδί βρίσκεται στο MIB του κάθε σταθμού και είναι σε μορφή μόνο εγγραφής (write-only). Έτσι είναι διαθέσιμο μόνο στον συντονιστή του MAC. Το 802.11 βέβαια δεν καθορίζει τον τρόπο με τον οποίο μπορούν να κατανεμηθούν τα κλειδιά σε κάθε σταθμό.

Τελευταία, εκτός από τους παραπάνω τρόπους πιστοποίησης υλοποιούνται και δύο άλλοι τρόποι [28]. Ο ένας χρησιμοποιεί το σύστημα Kerberos [21] και ο άλλος μία μη προκαθορισμένη πιστοποίηση.

Η διαδικασία που ακολουθείται είναι η εξής. Αρχικά ο σταθμός που ζητά πιστοποίηση στέλνει ένα πλαίσιο πιστοποίησης στο AP. Όταν το AP λαμβάνει το μήνυμα απαντά με ένα πλαίσιο πιστοποίησης που περιέχει 128 byte τυχαίου Κειμένου Πρόκλησης (Challenge Text), το οποίο έχει δημιουργηθεί από τη WEP μηχανή στην κανονική της μορφή. Στη συνέχεια ο σταθμός που έχει κάνει την αίτηση πιστοποίησης αντιγράφει το κείμενο πρόκλησης σε ένα πλαίσιο πιστοποίησης, το κρυπτογραφεί με το μυστικό κλειδί (λαμβάνοντας υπόψη τους κανόνες που ισχύουν για τα προκαθορισμένα κλειδιά ή τον πίνακα αντιστοιχίας των κλειδιών) και το στέλνει στο AP (απάντηση – response). Τέλος μόλις ληφθεί το πλαίσιο, το AP αποκρυπτογραφεί το Κείμενο Πρόκλησης χρησιμοποιώντας το σωστό κλειδί και το συγκρίνει με το κείμενο που είχε στείλει νωρίτερα. Αν είναι ίδια, θα απαντήσει ότι η πιστοποίηση είναι επιτυχής. Αν όχι, θα στείλει αρνητική απάντηση. Η διαδικασία αυτή ονομάζεται Πρόκληση-Απάντηση (Challenge-Response).

Ένας σταθμός μπορεί να εκτελέσει τη διαδικασία της πιστοποίησης με όσους σταθμούς επιθυμεί. Το πρότυπο δεν έχει θέσει κάποιο όριο όσον αφορά στον αριθμό των πιστοποιήσεων που μπορούν να γίνουν. Αυτό επιτρέπει σε έναν σταθμό να χρησιμο-

ποιήσει την υπηρεσία της προ-πιστοποίησης με άλλους σταθμούς, παρά το γεγονός ότι μπορεί να μην υπάρχει άμεση ανάγκη για κάτι τέτοιο.

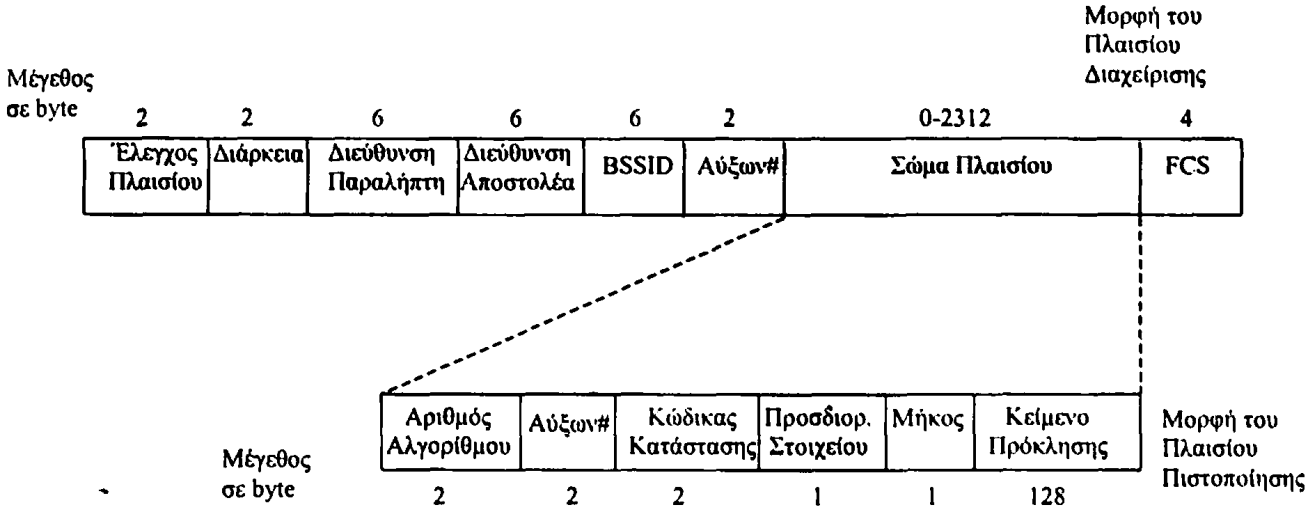


Εικόνα 3.4. Η πιστοποίηση κοινού κλειδιού

Πρέπει να σημειωθεί ότι αυτός ο αλγόριθμος πιστοποιεί μόνο την ταυτότητα του σταθμού Α στον Β. Έτσι το AP βρίσκεται πάντα σε πλεονεκτική θέση σε σχέση με τους κινούμενους σταθμούς σε ότι αφορά την πιστοποίηση, εφόσον ο σταθμός είναι αυτός που πρέπει να αρχίζει τη διαδικασία της πιστοποίησης. Για το λόγο αυτό, μόνο ο κινούμενος σταθμός εκτελεί τη διαδικασία της κρυπτογράφησης στο Κείμενο Πρόκλησης. Κάτι τέτοιο όμως αφήνει το WLAN ανοιχτό σε προβλήματα ασφάλειας. Υπάρχει η πιθανότητα κάποιος εισβολέας AP να μάθει το SSID του ESS και να ανακοινώσει την παρουσία του σύμφωνα με την αντίστοιχη διαδικασία του MAC επιπέδου. Έτσι κάποιοι κινούμενοι σταθμοί θα προσπαθήσουν να χρησιμοποιήσουν το συγκεκριμένο AP για την πρόσβασή τους στο WLAN. Ο εισβολέας τότε θα απαντήσει με επιτυχία στην πιστοποίηση και στη συνέχεια μπορεί να εκτελέσει την επίθεση της άρνησης υπηρεσιών ή να προσπαθήσει να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα των υψηλότερων επιπέδων όπως ονόματα χρηστών και password. Αν όμως τα δεδομένα είναι κρυπτογραφημένα με τη χρήση του WEP είναι πολύ δύσκολο να μπορέσει να αποκρυπτογραφήσει την πληροφορία.

Στην Εικόνα 3.5 περιγράφεται η μορφή του Πλαισίου Διαχείρισης της Πιστοποίησης (Authentication Management Frame). Εκτός από το Κείμενο Πρόκλησης υπάρχουν κάποια επιπλέον πεδία. Ο Κώδικας Κατάστασης (Status Code) είναι ίσος με 0 όταν έχουμε επιτυχία κι έχει μια τιμή σφάλματος όταν η πιστοποίηση έχει αποτύχει. Ο Προσδιοριστής Στοιχείου (Element Identifier) δηλώνει πότε περιλαμβάνεται το Κεί-

μενο Πρόκλησης. Το πεδίο του Μήκους (Length) δηλώνει το μήκος του Κειμένου Πρόκλησης και είναι ίσο με 128. Ο Αριθμός Αλγορίθμου (Algorithm Number) δηλώνει αν χρησιμοποιείται Πιστοποίηση Ανοιχτού Συστήματος ή Κοινού Κλειδιού. Στον Πίνακα 3.1 φαίνονται οι πιθανές τιμές των πεδίων αυτών.



Εικόνα 3.5: Το Πλαίσιο Διαχείρισης της Πιστοποίησης (Authentication Management Frame)

	Αύξων Αριθμός	Κώδικας Κατάστασης	Κείμενο Πρόκλησης	Χρήση WEP
Αίτηση Πιστοποίησης	1	Κράτηση	Όχι Παρόν	Όχι
Κείμενο Πρόκλησης	2	Κατάσταση	Παρόν	Όχι
Απάντηση	3	Κράτηση	Παρόν	Ναι
Επικύρωση Πιστοποίησης	4	Κατάσταση	Όχι Παρόν	Όχι

Πίνακας 3.1: Οι τιμές των πεδίων του Πλαισίου Διαχείρισης της Πιστοποίησης

Στα πλαίσια της παρούσας εργασίας προσομοιώθηκε το τμήμα της Πιστοποίησης του πρωτοκόλλου 802.11 με μια παραλλαγή που προσφέρει μεγαλύτερη ασφάλεια. Αφού αποδειχθεί η ταυτότητα του σταθμού, ο οποίος ξεκίνησε τη διαδικασία της πιστοποίησης, εκτελείται ξανά η διαδικασία της Πρόκλησης-Απάντησης (Challenge-Response). Γίνεται δηλαδή αμοιβαία πιστοποίηση AP-σταθμού, ώστε να μην υπάρχει η δυνατότητα σε κάποιον εισβολέα να προσποιηθεί ότι είναι κάποιο AP. Έτσι αποδείχθηκε ότι ελλείψει του μυστικού κλειδιού (είτε στο AP είτε στον σταθμό), η πιστοποίηση δεν είναι έγκυρη. Επίσης μελετήθηκαν κάποιες από τις αδυναμίες στην ασφάλεια του πρωτοκόλλου, όπως θα περιγραφούν στα επόμενα κεφάλαια.

ΚΕΦΑΛΑΙΟ 4

ΑΔΥΝΑΜΙΕΣ ΤΟΥ IEEE 802.11

4.1 Στόχοι ασφάλειας

Είναι πολύ σημαντικό για ένα πρωτόκολλο ασύρματων δικτύων να μπορεί να παρέχει ικανοποιητική ασφάλεια στους χρήστες. Το 802.11 χρησιμοποιεί το πρωτόκολλο WEP για να πετύχει τρεις στόχους ασφάλειας:

- **Εμπιστευτικότητα (confidentiality):** Ο βασικός του στόχος είναι να προφυλάξει το δίκτυο από υποκλοπές.
- **Έλεγχο πρόσβασης (access control):** Ένας δεύτερος στόχος είναι η προστασία πρόσβασης στην υποδομή του ασύρματου δικτύου. Το πρότυπο 802.11 περιλαμβάνει μία προαιρετική λειτουργία ώστε να απορρίπτει όλα τα πακέτα τα οποία δεν είναι σωστά κρυπτογραφημένα με το WEP.
- **Ακεραιότητα των δεδομένων (data integrity):** Ένας ακόμη στόχος είναι η προστασία από τη μεταβολή των μηνυμάτων και για το λόγο αυτό περιλαμβάνεται στη διαδικασία της πιστοποίησης ένα πεδίο ελέγχου ακεραιότητας (integrity checksum).

Όπως θα δούμε παρακάτω όμως υπάρχουν αρκετά προβλήματα στην ασφάλεια του 802.11, τα οποία αποτελούν αφορμή για ένα σύνολο από επιθέσεις.

4.2 Προβλήματα της ασφάλειας ενός WLAN

Τα σημαντικότερα προβλήματα ασφάλειας που αφορούν ένα WLAN χωρίζονται στις εξής κατηγορίες [26]:

- **Ανθρώπινα σφάλματα:** Προκύπτουν είτε από λανθασμένη ρύθμιση του δικτύου από τους διαχειριστές ή από λάθη στο λογισμικό.
- **Παραβίαση της εμπιστευτικότητας των δεδομένων:** Προκύπτει όταν κάποιος αποκτά παράνομα πρόσβαση στις πληροφορίες που διακινούνται στο WLAN. Για να συμβεί αυτό πρέπει να έχει στη διάθεσή του το κρυπτογαφημένο μήνυμα, τον αλγόριθμο αποκρυπτογράφησης και το κλειδί.
- **Πλαστογράφηση των δεδομένων:** Συμβαίνει όταν κάποιος εισάγει δεδομένα στο δίκτυο ως χρήστης του, ενώ στην πραγματικότητα δεν του επιτρέπεται η πρόσβαση σ' αυτό.
- **Άρνηση υπηρεσιών:** Συμβαίνει όταν κάποιος «φορτώνει» το δίκτυο με δεδομένα (έγκυρα ή όχι) και είτε εξαναγκάζει το δίκτυο να καταναλώσει την ενέργεια της μπαταρίας ή όταν δημιουργεί συμφόρηση στο AP.
- **Σφάλματα του υλικού:** Υπάρχει περίπτωση το υλικό να σταματήσει να λειτουργεί ή να προκαλέσει συμφόρηση αποστέλλοντας διαρκώς μηνύματα ή αποστέλλει τυχαία μηνύματα τα οποία να μοιάζουν με έγκυρα.

4.3 Οι αδυναμίες της Πρόκλησης-Απάντησης

4.3.1 Η επίθεση της εξαντλητικής αναζήτησης

Το πρώτο πρόβλημα έχει σχέση με τη διαδικασία της πρόκλησης-απάντησης. Μπορεί εύκολα κανείς να εκμεταλλευτεί το υπάρχον πρωτόκολλο πιστοποίησης, ώστε με την επίθεση της εξαντλητικής αναζήτησης (brute force attack) να αποκαλύψει το μυστικό κλειδί.

Όπως έχουμε δει στο προηγούμενο κεφάλαιο υπάρχουν δύο τρόποι υλοποίησης του WEP. Είναι το κλασικό WEP όπως περιγράφεται στο πρότυπο, με μήκος κλειδιού 64

bit και μία επεκταμένη έκδοση, η οποία έχει υλοποιηθεί από μερικούς κατασκευαστές και χρησιμοποιεί μεγαλύτερο πεδίο κλειδιού, ίσο με 128 bit. Αυτή η επέκταση του πρωτοκόλλου καθιστά αδύνατες τις επιθέσεις εξαντλητικής αναζήτησης, προς το παρόν τουλάχιστον, εξαιτίας της έλλειψης τεχνολογίας τέτοιων δυνατοτήτων. Όπως θα δούμε σε επόμενη παράγραφο όμως το κλειδί αυτό αποδεικνύεται αρκετά μικρό για άλλου είδους επιθέσεις.

Ας ξεκινήσουμε όμως με το κλασικό WEP, το οποίο ορίζει κλειδιά των 64 bit, επειδή την εποχή που δημιουργήθηκε το πρωτόκολλο αυτό υπήρχαν περιορισμοί από την κυβέρνηση των Ηνωμένων Πολιτειών όσον αφορά στην εξαγωγή τεχνολογίας που περιλαμβάνει αλγορίθμους κρυπτογράφησης. Όπως είδαμε το keystream προκύπτει από τη συνένωση ενός κοινού μυστικού κλειδιού και του IV, το οποίο αλλάζει για κάθε μήνυμα και έχει μήκος 24 bit. Επομένως το μυστικό κλειδί έχει μήκος ίσο με 40 bit.

Όταν αποστέλλεται ένα πακέτο, το IV τοποθετείται στην αρχή του πλαισίου και είναι μη κρυπτογραφημένο. Δεδομένου ότι αυτό το τμήμα του κλειδιού είναι γνωστό, όλα τα πιθανά keystream είναι ανάλογα με το μέγεθος του κοινού μυστικού κλειδιού, εφόσον αυτό είναι άγνωστο. Άρα στη χειρότερη περίπτωση πρέπει να εξεταστούν 2^{40} διαφορετικά keystream. Αυτό το μήκος κλειδιού όμως είναι αρκετά μικρό, ώστε να είναι δυνατές οι επιθέσεις εξαντλητικής αναζήτησης από μεμονωμένα άτομα ή από εταιρείες με υπολογιστικούς πόρους μετρίων δυνατοτήτων.

Για την έκδοση των 128-bit (WEP2) το μυστικό κλειδί έχει μήκος 104 bit κι έτσι προκύπτουν 2^{104} διαφορετικά κλειδιά. Ο χρόνος που χρειάζεται θεωρείται πολύ μεγάλος για τις σημερινές δυνατότητες των υπολογιστών. Όπως θα δούμε όμως σε επόμενες παραγράφους, υπάρχουν αδυναμίες του IEEE 802.11, οι οποίες δεν εξαρτώνται από το μήκος του κλειδιού κι επομένως δεν αντιμετωπίζονται ούτε με το WEP2.

Μελετήσαμε πειραματικά το χρόνο που χρειάζεται γι' αυτήν την επίθεση χρησιμοποιώντας την εξής αδυναμία της πρόκλησης-απάντησης. Ένας εισβολέας μπορεί να υποκλέψει το δεύτερο και το τρίτο μήνυμα διαχείρισης κατά τη διαδικασία της πρόκλησης-απάντησης. Το δεύτερο μήνυμα περιλαμβάνει την τυχαία πρόκληση μη κρυπτογραφημένη και το τρίτο την ίδια πρόκληση κρυπτογραφημένη με το κοινό κλειδί. Εφόσον κατέχει ένα plaintext (P) και το αντίστοιχο ciphertext (C) δε χρειάζεται καμία αλληλεπίδραση με το AP, ώστε να επαληθεύει το εκάστοτε keystream που προκύπτει. Απλώς εφαρμόζει τον αλγόριθμο WEP για τα 2^{40} διαφορετικά κλειδιά και συγκρίνει το νέο ciphertext C΄ με το C. Όταν το C΄ ταυτίζεται με το C το μυστικό κλειδί έχει αποκαλυφθεί.

Εφαρμόζοντας αυτή την επίθεση προέκυψε ότι ο χρόνος που χρειάζεται ένας υπολογιστής SUN SPARC με 512MB μνήμη είναι ίσος με 775421 sec ή 215 περίπου ώρες για μυστικό κλειδί μήκους 32 bit, επομένως για κλειδί μήκους 40 bit ο απαιτούμενος χρόνος είναι $215*2^8 = 55040$ ώρες περίπου ή 2293 ημέρες. Ο αριθμός αυτός μπορεί με μια πρώτη ματιά να φαίνεται υπερβολικά μεγάλος, αν όμως σκεφτεί

κανείς ότι μια τέτοια διαδικασία μπορεί πολύ εύκολα να εκτελεστεί παράλληλα από πολλούς υπολογιστές, με μεγαλύτερη ταχύτητα από αυτόν που χρησιμοποιήθηκε στο πείραμα, τότε ο απαιτούμενος χρόνος είναι υποπολλαπλάσιος του παραπάνω και η επίθεση είναι εφικτή σε αποδεκτό χρονικό διάστημα.

4.3.2 Η αποκάλυψη του keystream

Εκμεταλλευόμενος την ίδια αδυναμία της πρόκλησης-απάντησης, μπορεί ένας εισβολέας να εργαστεί ως εξής. Επειδή γνωρίζει το plaintext, το ciphertext και το δημόσιο IV έχει τη δυνατότητα να αποκαλύψει το keystream που δημιουργήθηκε χρησιμοποιώντας το πρωτόκολλο WEP [keystream(k, IV)] με το κοινό κλειδί k και το IV ως εξής:

$$\text{keystream}(k, IV) = C \oplus P$$

Το μέγεθος του keystream θα είναι ίσο με το μέγεθος του πλαισίου πιστοποίησης. Όλα τα υπόλοιπα πεδία του πλαισίου είναι γνωστά: ο αριθμός αλγορίθμου, ο αριθμός ακολουθίας, ο κώδικας κατάστασης, ο προσδιοριστής στοιχείου, το μήκος και το κείμενο πρόκλησης. Επίσης όλα τα στοιχεία εκτός του κειμένου πρόκλησης θα είναι τα ίδια σε όλες τις απαντήσεις πιστοποίησης.

Έτσι ο εισβολέας γνωρίζει όλα τα στοιχεία για μια επιτυχημένη πιστοποίηση χωρίς να γνωρίζει το κοινό μυστικό κλειδί. Ζητάει πιστοποίηση από το AP στο οποίο επιθυμεί να συνδεθεί και αυτό απαντάει με μία πρόκληση πιστοποίησης (μη κρυπτογραφημένη). Μόλις αυτός λάβει το κείμενο πρόκλησης R, υπολογίζει ένα σωστό πλαίσιο απάντησης ως εξής:

$$\text{keystream}(key, IV) \oplus R = C$$

Στη συνέχεια υπολογίζει την τιμή ελέγχου εγκυρότητας (ICV) και στέλνει το νέο πλαίσιο, το οποίο είναι σωστό και επιτυγχάνει τη σύνδεση με το AP.

Πρέπει βέβαια να σημειωθεί ότι μια τέτοια επίθεση είναι δυνατή μόνο στην περίπτωση που χρησιμοποιείται το ίδιο IV και κατ' επέκταση το ίδιο keystream. Αν το IV αλλάζει σε κάθε πακέτο (όπως ορίζεται στο πρότυπο) δεν μπορεί να πραγματοποιηθεί. Όπως όμως θα δούμε παρακάτω η επαναχρησιμοποίηση του IV δεν είναι καθόλου σπάνιο φαινόμενο.

4.4 Η διαχείριση και κατανομή του μυστικού κλειδιού

Όπως έχουμε ήδη αναφέρει, το πρότυπο 802.11 δεν ορίζει τον τρόπο με τον οποίο καθορίζονται και διαχειρίζονται τα μυστικά κλειδιά. Είναι ένα θέμα, για το οποίο πρέπει να ληφθούν αποφάσεις από τους κατασκευαστές, με αποτέλεσμα ελάχιστοι από αυτούς να έχουν υλοποιήσει κάποιου είδους διαχείριση ή συμφωνία κλειδιών στα προϊόντα τους. Δυστυχώς κανένας από τους κατασκευαστές δεν παρέχει αρκετές πληροφορίες, ώστε να μπορούμε να καταλάβουμε το επίπεδο ασφάλειας που παρέχεται με κάθε προϊόν. Μάλιστα, σε μερικές περιπτώσεις οι διαθέσιμες λεπτομέρειες υποδεικνύουν ότι χρησιμοποιούνται πρωτόκολλα με γνωστές αδυναμίες, όπως η συμφωνία κλειδιών Diffie – Helman χωρίς πιστοποίηση.

Το πρότυπο 802.11 ορίζει δύο μεθόδους με τις οποίες μπορούμε να χρησιμοποιήσουμε τα WEP κλειδιά. Η πρώτη μέθοδος παρέχει ένα παράθυρο από τέσσερα κλειδιά. Ένας σταθμός ή ένα AP μπορεί να αποκρυπτογραφήσει πακέτα που έχουν δημιουργηθεί με οποιοδήποτε από αυτά τα κλειδιά. Ωστόσο η μετάδοση των δεδομένων περιορίζεται μόνο σε ένα από αυτά τα τέσσερα κλειδιά που έχουν εισαχθεί από τον ίδιο τον διαχειριστή του δικτύου.

Η δεύτερη μέθοδος ονομάζεται πίνακας αντιστοιχίας κλειδιών. Σ' αυτή τη μέθοδο η κάθε MAC διεύθυνση μπορεί να έχει κι ένα διαφορετικό κλειδί. Το μέγεθος του πίνακα αντιστοιχίας κλειδιών πρέπει, σύμφωνα με το πρωτόκολλο 802.11, να είναι τουλάχιστον δέκα. Το μέγιστο μέγεθος όμως εξαρτάται από το υλικό. Η χρήση διαφορετικού κλειδιού για κάθε χρήστη μετριάζει τις επιθέσεις αποκρυπτογράφησης. Όμως τα κλειδιά μπορούν να μεταβληθούν και πάλι μόνο με την παρέμβαση του διαχειριστή του δικτύου, με αποτέλεσμα να μην είναι εφικτή η αλλαγή τους για μεγάλο χρονικό διάστημα. Έτσι προκύπτουν προβλήματα τα οποία επιτρέπουν επιθέσεις που βασίζονται στην επαναχρησιμοποίηση του keystream.

Το πρότυπο 802.11 από την άλλη, δεν καθορίζει τον τρόπο με τον οποίο μπορεί να επιτευχθεί η κατανομή των κλειδιών. Βασίζεται σε κάποιον εξωτερικό μηχανισμό ο οποίος περιλαμβάνει έναν πίνακα από 4 κοινά κλειδιά. Το κάθε μήνυμα περιλαμβάνει ένα πεδίο προσδιοριστή κλειδιού, το οποίο υποδεικνύει τη θέση στον πίνακα του κλειδιού που χρησιμοποιείται. Το πρότυπο υποστηρίζει επίσης έναν πίνακα, ο οποίος αντιστοιχίζει έναν προσδιοριστή για κάθε σταθμό, αλλά αυτή η επιλογή δεν υποστηρίζεται από πολλές εφαρμογές. Στην πράξη οι περισσότερες εφαρμογές χρησιμοποιούν ένα μόνο κλειδί για ένα ολόκληρο δίκτυο.

Αυτή η πρακτική έχει σοβαρές επιπτώσεις στην ασφάλεια του συστήματος, εφόσον ένα μυστικό το οποίο μοιράζονται πολλοί χρήστες δεν μπορεί να παραμείνει για πολύ καιρό κρυφό. Μερικοί διαχειριστές δικτύων προσπαθούν να βελτιώσουν την κατάσταση με το να μην αποκαλύπτουν το μυστικό κλειδί στους τελικούς χρήστες, αλλά να ρυθμίζουν οι ίδιοι τα μηχανήματά τους με το κλειδί. Βέβαια κάτι τέτοιο

λύνει ένα μέρος μόνο του προβλήματος, εφόσον τα κλειδιά αποθηκεύονται και πάλι στους υπολογιστές των χρηστών, όπου είναι δυνατή η υποκλοπή τους.

Η χρήση του ίδιου κλειδιού από πολλούς χρήστες αυξάνει και την πιθανότητα επαναχρησιμοποίησης του IV. Η πιθανότητα αυτή αυξάνει εκθετικά με τον αριθμό των χρηστών. Επίσης, το γεγονός ότι πολλοί χρήστες μοιράζονται το ίδιο κλειδί σημαίνει και πιο σπάνια αλλαγή του κλειδιού, εφόσον θα πρέπει να ρυθμιστούν οι οδηγοί δικτύου όλων των χρηστών.

4.5 Η επαναχρησιμοποίηση του keystream

Όπως έχουμε αναφέρει το WEP χρησιμοποιεί διαφορετικό IV για κάθε πακέτο, ώστε να διαφοροποιείται η ακολουθία-κλειδί για κάθε μεταδιδόμενο πλαίσιο μηνυμάτων. Το IV τοποθετείται στο μη κρυπτογραφημένο κομμάτι του πλαισίου, ώστε ο παραλήπτης να γνωρίζει με ποιον τρόπο θα το αποκρυπτογραφήσει. Έτσι το IV είναι διαθέσιμο και σε όσους επιθυμούν να επιτεθούν στο σύστημα. Εφόσον όμως το μυστικό κλειδί παραμένει άγνωστο γι' αυτούς, εξακολουθεί να διατηρείται η ασφάλεια του keystream.

Παρόλα αυτά, συμβαίνει συχνά να επαναχρησιμοποιούνται κάποια keystream και να τίθεται το σύστημα σε ένα σύνολο από κινδύνους. Αξίζει να σημειωθεί ότι εφόσον το κοινό μυστικό κλειδί k αλλάζει γενικά σπάνια, η επαναχρησιμοποίηση του IV σχεδόν πάντα προκαλεί την επαναχρησιμοποίηση του RC4 keystream. Επειδή τα IV είναι δημόσια, μπορεί πολύ εύκολα να ανιχνευθεί η επανάληψη του ίδιου IV. Επομένως οποιαδήποτε επαναχρησιμοποίηση των IV εκθέτει το σύστημα σε επιθέσεις επαναχρησιμοποίησης του keystream. Οι επαναχρησιμοποιήσεις των IV ονομάζονται «συγκρούσεις» (collisions). Ας δούμε αρχικά μερικά ρεαλιστικά σενάρια στα οποία μπορεί να συμβεί κάτι τέτοιο.

Το πρότυπο WEP προτείνει (αλλά δεν απαιτεί) την αλλαγή του IV μετά από κάθε πακέτο. Δεν αναφέρει όμως τίποτα άλλο σχετικά με τον τρόπο επιλογής των IV και μάλιστα οι περισσότερες υλοποιήσεις υστερούν σ' αυτό. Αρκετές PCMCIA κάρτες επαναφέρουν το IV στο 0 κάθε φορά που αρχικοποιούνται και στη συνέχεια το αυξάνουν κατά ένα κάθε φορά που μεταδίδεται ένα πακέτο. Οι κάρτες αυτές αρχικοποιούνται κάθε φορά που εισάγονται στον φορητό υπολογιστή, κάτι που συμβαίνει πολύ συχνά. Κατά συνέπεια τα IV με τις μικρές τιμές είναι πολύ πιθανό να χρησιμοποιούνται συχνά κατά τη διάρκεια ζωής ενός κλειδιού.

Από την άλλη, το WEP πρότυπο έχει ελαττώματα στην αρχιτεκτονική του, τα οποία εκθέτουν όλες τις WEP υλοποιήσεις σε σοβαρούς κινδύνους επαναχρησιμοποίησης του keystream, ανεξάρτητα από το πόσο προσεκτικά μπορεί να έχει σχεδιαστεί η υλοποίηση σε ότι αφορά τον IV. Το πεδίο IV που χρησιμοποιείται από το WEP έχει μέγεθος μόνο 24 bit και σχεδόν εγγυάται ότι το ίδιο IV θα χρησιμοποιηθεί για πολλά μηνύματα. Για παράδειγμα ένα AP που στέλνει πακέτα των 1500 byte στα 11Mbps θα εξαντλήσει τις διαθέσιμες τιμές του IV σε $1500*8/(11*10^6)*2^{24} \approx 1800$ δευτερόλεπτα, δηλαδή σε 5 περίπου ώρες. Εφόσον το IV έχει καθορισμένο από το πρότυπο μήκος 24

bits αυτή η ευπάθεια είναι πολύ σημαντική γιατί καμία συμβατή υλοποίηση δεν μπορεί να την αποφύγει.

Οι λεπτομέρειες των εφαρμογών μπορούν να κάνουν πολύ πιο συχνές τις IV συγκρούσεις της ακολουθίας κλειδιού. Σε μια εφαρμογή που χρησιμοποιείται ένα τυχαίο IV των 24 bit για κάθε πακέτο αναμένεται να εμφανιστούν συγκρούσεις αφού μεταδοθούν 5000 πακέτα, που σημαίνει μόνο μερικά λεπτά μετάδοσης. Ακόμη χειρότερα το πρότυπο 802.11 δεν απαιτεί το IV να αλλάζει με κάθε πακέτο, οπότε κάποια εφαρμογή θα μπορούσε να χρησιμοποιεί το ίδιο IV για όλα τα πακέτα χωρίς να υπάρχει κανένα πρόβλημα συμβατότητας.

4.6 Προβλήματα με την εμπιστευτικότητα των μηνυμάτων

4.6.1 Η αποκάλυψη του plaintext

Ένα γνωστό πρόβλημα των κρυπτογραφημένων ακολουθιών είναι ότι αν κρυπτογραφήσουμε δύο μηνύματα με το ίδιο IV και το ίδιο κλειδί, υπάρχει η πιθανότητα να αποκαλυφθεί κάποια πληροφορία για τα δύο μηνύματα. Αν για παράδειγμα έχουμε δύο ciphertext C_1 και C_2, που αποκρυπτογραφούνται αντίστοιχα στα plaintext P_1 και P_2, τότε ισχύει:

Αν	$C_1 = P_1 \oplus RC4(IV, k)$
και	$C_2 = P_2 \oplus RC4(IV, k)$
τότε	$C_1 \oplus C_2 = (P_1 \oplus RC4(IV, k)) \oplus (P_2 \oplus RC4(IV, k)) = P_1 \oplus P_2$

Δηλαδή αν εκτελεστεί η πράξη του αποκλειστικού-ή ανάμεσα στα δύο C_1 και C_2, τότε το keystream ακυρώνεται και το αποτέλεσμα είναι το αποκλειστικό-ή των δύο plaintext (P_1 και P_2).

Κάτι τέτοιο μπορεί να οδηγήσει σε ένα σύνολο από επιθέσεις. Το αποτέλεσμα που προκύπτει από την πράξη του αποκλειστικού-ή μπορεί να χρησιμοποιηθεί για την εξαγωγή συμπερασμάτων όσον αφορά στο περιεχόμενο των δύο μηνυμάτων.

Στην ειδική περίπτωση κατά την οποία είναι γνωστό το ένα από τα δύο plaintext, τότε είναι αυτομάτως γνωστό και το άλλο. Υπάρχουν γνωστές τεχνικές για την επίλυση ακολουθιών, οι οποίες αναζητούν αγγλικές λέξεις που μας δίνουν αποκλειστικό-ή στην τιμή $P_1 \oplus P_2$. Ακόμη και στην περίπτωση που είναι δύσκολη η εξαγωγή συμπεράσματος από τη στατιστική ανάλυση δύο μόνο plaintext, μπορεί να χρησιμοποιηθεί μεγαλύτερος αριθμός μηνυμάτων που κρυπτογραφήθηκαν με το ίδιο IV, με μικρή επιπλέον χρονική επιβάρυνση για την επεξεργασία τους.

Έτσι αν έχουμε στη διάθεσή μας n κρυπτογραφημένες ακολουθίες που επαναχρησιμοποιούν όλες το ίδιο keystream, έχουμε ένα πρόβλημα που είναι γνωστό

ως πρόβλημα βάθους n. Όσο το n αυξάνει η λύση είναι ευκολότερη, εφόσον μπορεί να υπολογιστεί το αποκλειστικό-ή κάθε ζεύγους κωδικοποιημένων κειμένων και είναι γνωστές πολλές κλασικές τεχνικές που επιλύουν τέτοια προβλήματα. Από τη στιγμή που αποκαλύπτεται το περιεχόμενο ενός από τα plaintext, είναι γνωστό το περιεχόμενο των n-1 plaintext με το ίδιο IV, αλλά και όλων των μελλοντικών μηνυμάτων που έχουν κρυπτογραφηθεί με το ίδιο keystream.

Πρέπει να σημειωθεί ότι απαιτούνται δύο συνθήκες για τις επιθέσεις αυτού του είδους:

- Η διαθεσιμότητα δύο ή περισσότερων plaintext των οποίων επαναχρησιμοποιείται ένα μέρος.
- Μερική γνώση κάποιων plaintext.

Μόλις ανακαλυφθούν δύο μηνύματα, τα οποία χρησιμοποιούν το ίδιο IV, μπορούν να εφαρμοστούν διάφορες μέθοδοι επίθεσης για την αποκάλυψη του plaintext. Αν το plaintext ενός από τα δύο μηνύματα είναι γνωστό είναι πολύ εύκολο να αποκαλυφθεί το περιεχόμενο του άλλου απευθείας.

Υπάρχουν αρκετοί τρόποι για την εξαγωγή καλών υποψηφίων για το plaintext. Πολλά πεδία των IP μηνυμάτων είναι προβλέψιμα [26]. Στον IP header για παράδειγμα από το σύνολο των πρώτων 128 bit μεταβάλλονται μόνο τα 56, ενώ τα υπόλοιπα παραμένουν σταθερά. Επίσης, οι ακολουθίες για το login είναι αρκετά ομοιόμορφες για πολλούς χρήστες και επομένως και τα περιεχόμενα τους – π.χ. η ακολουθία Password: ή το μήνυμα εισόδου (login) – μπορεί να είναι γνωστά στον εισβολέα και συνεπώς χρησιμοποιήσιμα για μια επίθεση επαναχρησιμοποίησης του keystream. Ένα άλλο παράδειγμα είναι η αναγνώριση κάποιας κοινής βιβλιοθήκης που μεταφέρεται από το σύστημα αρχείων του δικτύου. Κάτι τέτοιο μπορεί να επιτευχθεί με την ανάλυση της μορφής των πακέτων και του μήκους τους και θα μπορούσε να παρέχει μια μεγάλη ποσότητα γνωστών plaintext.

Υπάρχουν επίσης ακόμη πιο ύπουλοι τρόποι για την απόκτηση γνωστών plaintext. Είναι δυνατή η πρόκληση μετάδοσης γνωστού plaintext, στέλνοντας για παράδειγμα IP μηνύματα απευθείας σε κάποιον κινούμενο χρήστη (mobile host) από κάποιον κόμβο του Internet, ο οποίος ελέγχεται από τον εισβολέα. Επίσης ο εισβολέας μπορεί να στείλει e-mail σε κάποιους χρήστες και να περιμένει μέχρι αυτοί να το ελέγξουν με την ασύρματη σύνδεση. Με την αποστολή spam e-mail μπορούν να το πετύχουν αυτό χωρίς να κινήσουν υποψίες.

Μερικές φορές η απόκτηση γνωστού plaintext μπορεί να γίνει ακόμη πιο απλή. Αν κάποιο AP δεν έχει ενεργοποιημένη την επιλογή του ελέγχου πρόσβασης στο δίκτυο, τότε αυτό θα αποστέλλει τα μηνύματα εκπομπής (broadcast) και σε κρυπτογραφημένη, αλλά και σε μη κρυπτογραφημένη μορφή. Σε μια τέτοια περίπτωση ο εισβολέας μπορεί να στέλνει μηνύματα εκπομπής στο AP (θα είναι αποδεκτά εφόσον ο έλεγχος πρόσβασης είναι απενεργοποιημένος) και να παρατηρεί την κρυπτογραφημένη τους μορφή καθώς αυτά θα επαναμεταδίδονται. Πραγματικά κάτι τέτοιο είναι αναπόφευκτο σε ένα υποδίκτυο που περιλαμβάνει ένα μείγμα από πελάτες με και χωρίς την υποστήριξη κρυπτογράφησης. Εφόσον τα πακέτα εκπομπής

πρέπει να προωθηθούν σε όλους τους πελάτες δεν υπάρχει τρόπος να αποφευχθεί αυτή η τεχνική συγκέντρωσης γνωστών plaintext.

Τέλος όπως έχουμε αναφέρει παραπάνω ακόμη κι όταν δεν είναι διαθέσιμο γνωστό plaintext μπορεί να γίνει κάποια ανάλυση των δεδομένων αν είναι εφικτή κάποια βάσιμη υπόθεση για τη δομή των plaintext.

4.6.2 Λεξικά Αποκρυπτογράφησης

Μόλις γίνει γνωστό το plaintext για κάποιο μήνυμα που έχει υποκλαπεί, είτε μέσω της ανάλυσης λόγω σύγκρουσης των IV, είτε με άλλα μέσα ο εισβολέας μαθαίνει επίσης και την τιμή της ακολουθίας κλειδιού που χρησιμοποιείται για την κρυπτογράφηση του μηνύματος. Μπορεί στη συνέχεια να χρησιμοποιηθεί αυτή η ακολουθία κλειδί για την αποκρυπτογράφηση οποιουδήποτε άλλου μηνύματος το οποίο χρησιμοποιεί το ίδιο IV. Μετά από ένα χρονικό διάστημα ο εισβολέας είναι σε θέση να κατασκευάσει έναν πίνακα των keystream που αντιστοιχούν σε κάθε IV. Ένας πλήρης πίνακας έχει μέτριες απαιτήσεις σε χώρο – περίπου 1500 byte για καθένα από τα 2^{24} πιθανά IV ή κατά προσέγγιση 24 GB. Γίνεται λοιπόν αντιληπτό ότι κάποιος επίμονος εισβολέας μπορεί ύστερα από κάποια προσπάθεια να συγκεντρώσει αρκετή πληροφορία για την κατασκευή ενός πλήρους λεξικού αποκρυπτογράφησης, ειδικά αν σκεφτούμε τη χαμηλή συχνότητα αλλαγής των κλειδιών. Το κέρδος για τον εισβολέα είναι ότι μόλις γίνει διαθέσιμος ένας τέτοιος πίνακας είναι εφικτή η άμεση αποκρυπτογράφηση οποιουδήποτε ciphertext με πολύ μικρή προσπάθεια.

Βέβαια η δουλειά που απαιτείται για τη δημιουργία ενός τέτοιου λεξικού περιορίζει αυτή την επίθεση στους περισσότερο επίμονους εισβολείς, οι οποίοι είναι πρόθυμοι να επενδύσουν σε χρόνο και σε πόρους για να νικήσουν την ασφάλεια που παρέχει το πρωτόκολλο WEP. Μπορεί κάποιος να ισχυριστεί ότι το WEP δεν έχει σχεδιαστεί για την προστασία από τέτοιου είδους εισβολείς, εφόσον ένα κλειδί των 40 bit μπορεί να αποκαλυφθεί μέσω εξαντλητικής αναζήτησης σε σχετικά λίγο χρόνο με μέτρια μέσα. Η επίθεση του λεξικού όμως εξακολουθεί να ισχύει για οσοδήποτε μεγάλο κλειδί, εφόσον δεν εξαρτάται από το μέγεθος του κλειδιού, αλλά από το μέγεθος του IV, το οποίο είναι σταθερό και ορισμένο από το πρότυπο στα 24 bit.

Μπορεί επιπλέον η επίθεση του λεξικού να εφαρμοστεί ακόμη πιο εύκολα αν εκμεταλλευτεί κανείς τη συμπεριφορά των PCMCIA καρτών οι οποίες επαναφέρουν το IV στο 0 κάθε φορά που αρχικοποιούνται. Εφόσον η συνηθισμένη χρήση των PCMCIA καρτών περιλαμβάνει την αρχικοποίησή τους τουλάχιστον μία φορά την ημέρα, η δημιουργία ενός λεξικού μόνο για τις πρώτες χιλιάδες των IV θα επιτρέψει σε κάποιον εισβολέα να αποκρυπτογραφήσει το μεγαλύτερο μέρος της πληροφορίας που κατευθύνεται προς το AP. Σε μια εφαρμογή με πολλούς 802.11 πελάτες, οι συγκρούσεις των IV είναι άφθονες.

4.7 Προβλήματα με την ακεραιότητα των δεδομένων

Το πρωτόκολλο WEP χρησιμοποιεί όπως έχουμε πει ένα πεδίο ελέγχου εγκυρότητας για να εξασφαλίσει ότι τα πακέτα δε μεταβάλλονται κατά τη μετάδοσή τους.

Εφαρμόζεται στα δεδομένα ο αλγόριθμος CRC-32 και το αποτέλεσμα που προκύπτει αποτελεί μέρος των κρυπτογραφημένων δεδομένων του πακέτου. Όπως θα δούμε όμως παρακάτω το CRC checksum αδυνατεί να προστατεύσει το πακέτο από τις παρεμβάσεις των εισβολέων και είναι δυνατή η επίθεση που ονομάζεται Μεταβολή Μηνύματος (Message Modification).

Το CRC checksum έχει την ιδιότητα ότι αποτελεί γραμμική συνάρτηση του μηνύματος. Αυτό σημαίνει ότι για οποιαδήποτε x και y ισχύει:

$$c(x \oplus y) = c(x) \oplus c(y)$$

Αυτή είναι μια γενική ιδιότητα όλων των CRC checksum.

Μια συνέπεια της παραπάνω ιδιότητας είναι ότι μπορεί να γίνει ελεγχόμενη μεταβολή ενός ciphertext χωρίς να μεταβληθεί το checksum. Έστω για παράδειγμα κάποιο ciphertext C, το οποίο υποκλάπηκε πριν φτάσει στον προορισμό του.

$$(A) \rightarrow B: \langle IV, C \rangle$$

Έστω ότι το C αντιστοιχεί σε κάποιο άγνωστο μήνυμα M, έτσι ώστε:

$$C = RC4(IV, k) \oplus \langle M, c(M) \rangle \qquad (4.1)$$

Υπάρχει πιθανότητα να βρεθεί ένα νέο ciphertext C′ το οποίο αποκρυπτογραφείται σε ένα μήνυμα M′, όπου $M' = M \oplus \Delta$ και το Δ μπορεί να επιλεγεί τυχαία από τον εισβολέα. Τότε θα είμαστε σε θέση να αντικαταστήσουμε την αρχική μετάδοση με το νέο ciphertext, εξαπατώντας τον αποστολέα.

$$(A) \rightarrow B: \langle IV, C' \rangle$$

και κατά την αποκρυπτογράφηση ο παραλήπτης B θα λάβει το παραποιημένο μήνυμα M′ με το σωστό checksum.

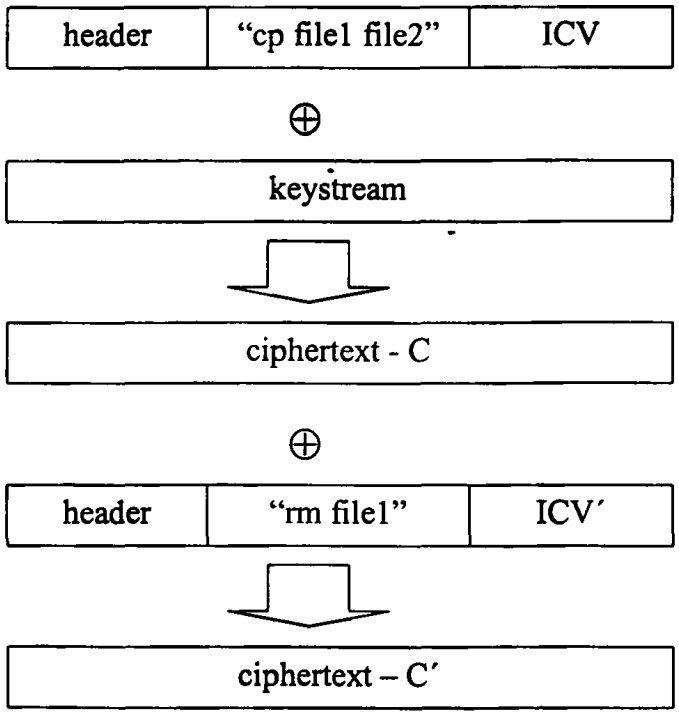
Ας δούμε όμως πώς από το C μπορούμε να υπολογίσουμε το C′ που αποκρυπτογραφείται στο M′ και όχι στο M. Αρκεί να παρατηρήσει κανείς ότι οι κρυπτογραφημένες ακολουθίες που προκύπτουν από τον αλγόριθμο RC4 είναι επίσης γραμμικές. Έστω τώρα ότι εκτελούμε το αποκλειστικό-ή της ποσότητας $\langle \Delta, c(\Delta) \rangle$ με τις δύο πλευρές της εξίσωσης (4.1) και πάρουμε ένα νέο ciphertext C′:

$$C' = C \oplus \langle \Delta, c(\Delta) \rangle = RC4(IV, k) \oplus \langle M, c(M) \rangle \oplus \langle \Delta, c(\Delta) \rangle$$

$$= RC4(IV, k) \oplus <M \oplus \Delta, c(M) \oplus c(\Delta)>$$
$$= RC4(IV, k) \oplus <M', c(M \oplus \Delta)>$$
$$= RC4(IV, k) \oplus <M', c(M')>$$

Στην παραπάνω ανάλυση χρησιμοποιήσαμε το γεγονός ότι το WEP checksum είναι γραμμικό, οπότε θα ισχύει ότι $c(M) \oplus c(\Delta) = c(M \oplus \Delta)$. Αυτό αποδεικνύει ότι μπορούμε να κάνουμε τυχαίες αλλαγές σε κάποιο μήνυμα χωρίς το φόβο ανίχνευσής τους. Έτσι λοιπόν το WEP checksum αδυνατεί να προστατεύσει την εγκυρότητα των δεδομένων, που είναι ένας από τους τρεις βασικούς στόχους του WEP.

Αξίζει να σημειωθεί ότι γι' αυτού του είδους τις επιθέσεις δεν είναι απαραίτητη η πλήρης γνώση του M. Ο εισβολέας χρειάζεται απλώς να γνωρίζει το αρχικό ciphertext C και την επιθυμητή μεταβολή Δ, ώστε να υπολογίσει το $C' = C \oplus <\Delta, c(\Delta)$. Για παράδειγμα αν θέλει κάποιος να αλλάξει το πρώτο bit του μηνύματος μπορεί να ορίσει ότι $\Delta = 1000...0$. Κάτι τέτοιο επιτρέπει στον εισβολέα να μεταβάλει το πακέτο έχοντας μερική μόνο γνώση του περιεχομένου του.



Εικόνα 4.1: Ένα παράδειγμα της μετατροπής μηνύματος

Για να γίνει κατανοητό πόσο σημαντική είναι αυτού του είδους η επίθεση υλοποιήθηκε το εξής παράδειγμα. Έστω ότι ένας σταθμός αποστέλλει το μήνυμα "cp file1 file2". Ο εισβολέας υποκλέπτει το ciphertext (C) του μηνύματος αυτού, εκτελεί την πράξη του αποκλειστικού-ή με το μήνυμα "rm file1", για το οποίο έχει υπολογίσει τη σωστή Τιμή Ελέγχου Εγκυρότητας (ICV') και προκύπτει ένα νέο

ciphertext (C΄), το οποίο γίνεται αποδεκτό από το άλλο άκρο. Αυτό συμβαίνει επειδή μόλις γίνει η αποκρυπτογράφηση και υπολογιστεί η Τιμή Ελέγχου Εγκυρότητας, ο παραλήπτης ελέγχει το ICV΄ και βλέπει ότι είναι σωστό. Η διαδικασία που ακολουθείται περιγράφεται στο σχήμα 4.1

4.8 Προβλήματα με τον έλεγχο πρόσβασης

Η δυνατότητα μεταβολής του περιεχομένου των κρυπτογραφημένων πακέτων μπορεί να αποτελέσει τη βάση και για την αποκρυπτογράφησή τους. Ένας εισβολέας συνήθως δεν προσπαθεί να επιτεθεί στον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται (ο RC4 στην περίπτωσή μας), εφόσον αυτός θεωρείται ασφαλής. Μπορεί ο ίδιος να μη γνωρίζει το κλειδί για να κάνει την αποκρυπτογράφηση, τα AP όμως έχουν αυτή τη δυνατότητα. Εξαπατώντας λοιπόν το AP μπορεί κάποιος να το χρησιμοποιήσει για να του αποκρυπτογραφεί τα πακέτα. Η δυνατότητα αλλαγής των μεταδιδόμενων πλαισίων παρέχει δύο πολύ εύκολους τρόπους για την εκμετάλλευση του AP με αυτόν τον τρόπο.

4.8.1 Αλλαγή της IP διεύθυνσης (IP redirection)

Αυτή η επίθεση μπορεί να εφαρμοστεί μόνο στην περίπτωση που το AP λειτουργεί ως δρομολογητής IP με μια σύνδεση Internet, κάτι που συμβαίνει πολύ συχνά, επειδή το WEP χρησιμοποιείται για να παρέχει πρόσβαση στο δίκτυο και σε κινούμενους χρήστες που μπορεί να βρίσκονται μακριά από το WLAN και χρειάζεται να συνδεθούν μέσω του Internet.

Η ιδέα στηρίζεται στην υποκλοπή ενός πακέτου και τη μεταβολή του με τη χρήση της τεχνικής που αναφέραμε. Αυτό που αλλάζει είναι η διεύθυνση του προορισμού σε μια νέα διεύθυνση, την οποία ο εισβολέας ελέγχει. Στη συνέχεια, το AP θα αποκρυπτογραφήσει το πακέτο και θα το στείλει στον (νέο) προορισμό του, όπου ο εισβολέας μπορεί πλέον να το διαβάσει. Το πακέτο που θα έχει υποστεί την αλλαγή θα κινείται από το ασύρματο δίκτυο προς το Internet, επομένως πολλά firewall θα το αφήσουν να περάσει χωρίς κανένα έλεγχο.

Ο ευκολότερος τρόπος για την αλλαγή της διεύθυνσης IP του προορισμού είναι να καταλάβει κανείς την αρχική διεύθυνση, κάτι που δεν είναι ιδιαίτερα δύσκολο. Για παράδειγμα όλη η εισερχόμενη πληροφορία θα προορίζεται σε κάποια συγκεκριμένη IP διεύθυνση του ασύρματου υποδικτύου, η οποία εύκολα μπορεί να εξακριβωθεί. Μόλις αποκρυπτογραφηθεί η εισερχόμενη πληροφορία, οι IP διευθύνσεις των άλλων άκρων θα αποκαλυφθούν και η εξερχόμενη πληροφορία θα αποκρυπτογραφηθεί με τον ίδιο τρόπο.

Για να μπορέσει να εφαρμοστεί αυτή η επίθεση χρειάζεται όχι μόνο να αλλάξουμε την IP διεύθυνση προορισμού, αλλά και να είμαστε σίγουροι ότι το checksum του τροποποιημένου πακέτου είναι σωστό, γιατί διαφορετικά το πακέτο θα απορριφθεί

από το AP. Εφόσον όμως το τροποποιημένο πακέτο διαφέρει μόνο στην IP διεύθυνση του προορισμού και είναι γνωστή και η παλιά τιμή της μπορούμε να υπολογίσουμε το νέο checksum.

4.8.2 Επιθέσεις αντίδρασης (Reaction Attacks)

Υπάρχει κι ένας ακόμη τρόπος για να εκμεταλλευτεί κανείς το AP, για τις περιπτώσεις στις οποίες ο αλγόριθμος WEP χρησιμοποιείται για την προστασία της TCP/IP πληροφορίας. Σε μια τέτοια επίθεση ο εισβολέας παρακολουθεί την αντίδραση του αποδέκτη ενός TCP πακέτου και χρησιμοποιεί τις παρατηρήσεις του για να εξάγει συμπεράσματα για το άγνωστο plaintext. Αυτή η επίθεση βασίζεται στο γεγονός ότι ένα TCP πακέτο είναι αποδεκτό μόνο όταν το TCP checksum είναι σωστό και τότε αποστέλλεται ένα πακέτο επιβεβαίωσης σαν απάντηση. Πρέπει να σημειωθεί ότι τα πακέτα επιβεβαίωσης μπορούν πολύ εύκολα να αναγνωριστούν από το μέγεθός τους, χωρίς να απαιτείται αποκρυπτογράφηση. Έτσι η αντίδραση του παραλήπτη θα αποκαλύπτει πότε το checksum είναι σωστό κατά την αποκρυπτογράφηση.

Η διαδικασία που ακολουθείται στη συνέχεια είναι η εξής. Αρχικά γίνεται υποκλοπή κάποιου ciphertext <IV, C> με άγνωστη αποκρυπτογράφηση P:

$$A \rightarrow (B) : <IV, C>$$

Στη συνέχεια αντιστρέφονται κάποια bit του C και προσαρμόζεται κατάλληλα το κρυπτογραφημένο CRC για τη δημιουργία ενός νέου ciphertext C΄ με σωστό CRC checksum και μεταδίδεται στο AP το C΄ μέσα σε ένα πλαστό πακέτο.

$$(A) \rightarrow B: <IV, C'>$$

Στο τέλος παρατηρούμε αν ο τελικός παραλήπτης απαντήσει με ένα TCP ACK πακέτο κι έτσι θα γνωρίζουμε αν το τροποποιημένο κείμενο είχε το σωστό TCP checksum και αν έγινε αποδεκτό από τον παραλήπτη.

Μπορούμε να επιλέξουμε ποια bit θα αλλάξουμε, χρησιμοποιώντας την τεχνική της μεταβολής του περιεχομένου του μηνύματος που περιγράψαμε παραπάνω. Μάλιστα, αν επιλέξουμε αυτά τα bit με έξυπνο τρόπο τότε το TCP checksum δε μεταβάλλεται.

Αξίζει να σημειωθεί ότι οι παραπάνω αδυναμίες (εκτός της εξαντλητικής αναζήτησης) αφορούν και τις δύο εκδόσεις του WEP, εφόσον δεν εξαρτώνται από το μήκος του κλειδιού [27].

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΡΟΤΑΣΕΙΣ

5.1 Προβλήματα συμβατότητας και σχεδιασμού

Το μεγαλύτερο πρόβλημα με τα δίκτυα ραδιοκυμάτων είναι ότι δεν υπάρχει ένα μοναδικό πρότυπο όπως το Ethernet, το οποίο να εγγυάται τη συμβατότητα ανάμεσα σε όλες τις συσκευές, αλλά πολλά πρότυπα ιδιόκτητα από διάφορους κατασκευαστές, που είναι φυσικά μη συμβατά μεταξύ τους. Βέβαια οι περισσότερες εταιρείες έχουν συνεργαστεί με την IEEE πάνω στο 802.11, αλλά εξαιτίας αυτού του γεγονότος έχουν δημιουργηθεί αρκετά προβλήματα.

Κατ' αρχήν ο κάθε κατασκευαστής προσπάθησε να προωθήσει τη δική του τεχνολογία και τις δικές του προδιαγραφές, ώστε το πρότυπο να πλησιάζει στο δικό του προϊόν. Το αποτέλεσμα είναι ένα πρότυπο που χρειάστηκε πολύ χρόνο για να ολοκληρωθεί, είναι εξαιρετικά πολύπλοκο και φορτωμένο με πάρα πολλά χαρακτηριστικά. Μάλιστα εξαιτίας της πολυπλοκότητας και των πολλών χαρακτηριστικών άργησαν να παράγουν προϊόντα για το 802.11, τα οποία για τον ίδιο λόγο ήταν αρχικά πολύ ακριβά.

Όπως έχουμε δει σε προηγούμενα κεφάλαια, το πρότυπο IEEE 802.11 χαρακτηρίζεται από μεγάλο βαθμό ευελιξίας. Αυτό το χαρακτηριστικό είναι πολύ χρήσιμο, επειδή έτσι παρέχεται μεγάλη ελευθερία στη διαχείριση του WLAN. Για δίκτυα που δημιουργούνται για να λειτουργήσουν για ένα μικρό χρονικό διάστημα (π.χ. για τις ανάγκες της συνεδρίασης μιας εταιρείας διάρκειας λίγων ωρών) ο διαχειριστής του δικτύου δε χρειάζεται να ορίσει ένα infrastructure δίκτυο, με όλα τα χαρακτηριστικά ασφαλείας ενός WLAN που χρησιμοποιείται σχεδόν μόνιμα.

Ο ευέλικτος όμως σχεδιασμός προσθέτει ένα μεγάλο αριθμό παραμέτρων, οι οποίες πρέπει να ρυθμιστούν από το διαχειριστή του δικτύου και καθιστούν τη διαδικασία

αυτή αρκετά δύσκολη. Αυτό έχει σαν αποτέλεσμα λίγοι διαχειριστές να εκμεταλλεύονται πλήρως τις δυνατότητες του προτύπου και κατά συνέπεια μειωμένη ασφάλεια στο WLAN.

Από την άλλη, το πρότυπο δεν εγγυάται πλήρη δια-λειτουργικότητα (interoperability). Τα προϊόντα πρέπει να χρησιμοποιήσουν τουλάχιστον το ίδιο φυσικό επίπεδο, τον ίδιο ρυθμό μετάδοσης και τον ίδιο τρόπο λειτουργίας.

Θα ήταν ίσως δυνατή κάποια αναθεώρηση με στόχο την ελάττωση των πολλών παραμέτρων που προέκυψαν λόγω των πιέσεων των κατασκευαστών. Επίσης θα ήταν καλό να αναπτυχθεί κάποιος εύκολος στη χρήση μηχανισμός για την αυτόματη ρύθμιση των χαρακτηριστικών διαχείρισης του ασύρματου τοπικού δικτύου, ώστε εκτός από ευέλικτο να είναι και εύχρηστο.

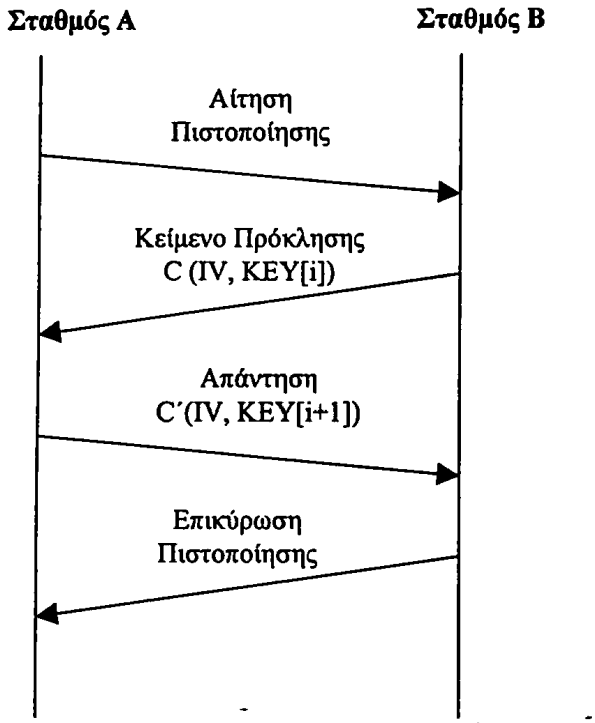
Παρόλα αυτά το 802.11 είναι ένα πρότυπο βασισμένο στην εμπειρία, ευέλικτο και πολύ καλά σχεδιασμένο, ενώ περιλαμβάνει πολλές βελτιστοποιήσεις και έξυπνες τεχνικές που έχουν αναπτυχθεί από τους διάφορους κατασκευαστές που συμμετείχαν στην ανάπτυξή του.

5.2 Η Πρόκληση-Απάντηση

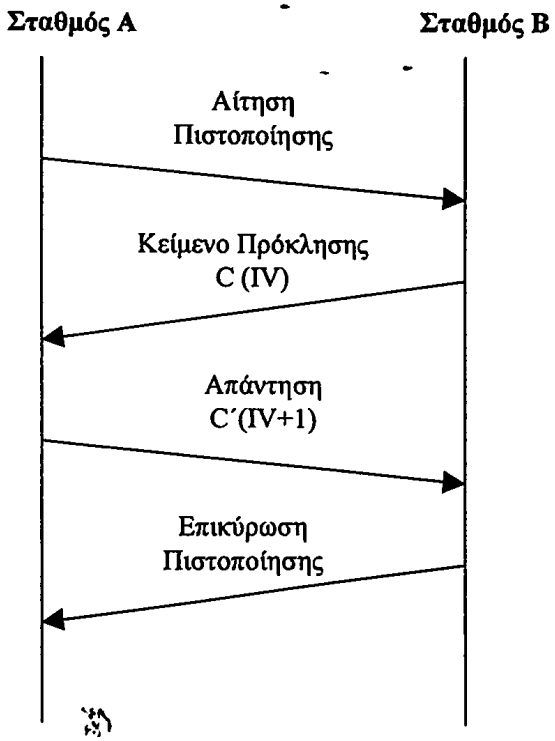
Όπως είδαμε στην Παράγραφο 4.2 η διαδικασία της Πρόκλησης-Απάντησης έχει ένα πολύ σημαντικό πρόβλημα. Μπορεί κάποιος να εκμεταλλευτεί τα δύο από τα τέσσερα βήματα της διαδικασίας για να αποκαλύψει το μυστικό κλειδί. Μια πιθανή λύση του προβλήματος θα μπορούσε να είναι η κρυπτογράφηση και των δύο μηνυμάτων. Το πρόβλημα βέβαια μ' αυτή την προσέγγιση είναι ότι δε θα έχουμε πλέον τρόπο να πιστοποιήσουμε έναν σταθμό, επειδή στην ουσία θα του αποστέλλουμε το ciphertext που πρέπει ο ίδιος να κρυπτογραφήσει για να αποδείξει ότι έχει το μυστικό κλειδί.

Υπάρχουν αρκετοί τρόποι αντιμετώπισης αυτού του προβλήματος. Στην περίπτωση που χρησιμοποιούνται περισσότερα από ένα μυστικά κλειδιά θα μπορούσε να ακολουθηθεί η εξής διαδικασία. Έστω ότι ο σταθμός Α ζητά πιστοποίηση από τον Β. Ο Β κρυπτογραφεί το μήνυμα χρησιμοποιώντας ένα από τα μυστικά κλειδιά και αποστέλλει στον Α το ciphertext C, το IV και τη θέση στον πίνακα αντιστοίχησης κλειδιών του συγκεκριμένου κλειδιού που χρησιμοποίησε. Ο Α λαμβάνει το μήνυμα, το αποκρυπτογραφεί και το κρυπτογραφεί εκ νέου χρησιμοποιώντας το ίδιο IV και το επόμενο σύμφωνα με τον πίνακα αντιστοιχίας μυστικό κλειδί. Ο Β λαμβάνει το νέο ciphertext C΄ και το αποκρυπτογραφεί γνωρίζοντας ποιο μυστικό κλειδί θα χρησιμοποιήσει. Στην Εικόνα 5.1 περιγράφεται αυτή η διαδικασία.

Στην περίπτωση που χρησιμοποιείται ένα μόνο μυστικό κλειδί μπορούμε να εκμεταλλευτούμε το IV. Στο παραπάνω σενάριο ο Α θα στείλει κρυπτογραφημένο το μήνυμα με ένα τυχαίο IV και ο Β αφού το αποκρυπτογραφήσει, το κρυπτογραφεί ξανά με ένα νέο IV (π.χ. IV+1). Ένα παράδειγμα φαίνεται στην Εικόνα 5.2.



Εικόνα 5.1: Χρήση διαφορετικών κλειδιών για την Πρόκληση-Απάντηση



Εικόνα 5.1: Παράδειγμα χρήσης διαφορετικών IV για την Πρόκληση-Απάντηση

5.3 Η διαχείριση του κλειδιού

Ένα από τα σημαντικότερα «τρωτά» σημεία του προτύπου IEEE 802.11 είναι η απουσία κάποιου μηχανισμού διανομής και διαχείρισης του μυστικού κλειδιού. Θα πρέπει αν είναι δυνατό ο κάθε σταθμός να έχει το δικό του μυστικό κλειδί. Το κλειδί αυτό θα αλλάζει συχνά με τη χρήση κάποιου μηχανισμού αυτόματης κατανομής κλειδιών. Επίσης πρέπει να αλλάζει οπωσδήποτε το μυστικό κλειδί σε κάθε IV σύγκρουση. Αρκετές προσπάθειες έχουν γίνει προς την κατεύθυνση αυτή [18], [20], [24].

Βέβαια επειδή το μήκος του IV είναι πολύ μικρό, οι IV συγκρούσεις είναι κι αυτές πολύ συχνό φαινόμενο. Μια καλή λύση θα ήταν ένα IV μήκους 128 bit, το οποίο χρειάζεται πολύ περισσότερο χρόνο μέχρι να εξαντληθεί.

5.4 Το CRC checksum

Είδαμε στο Κεφάλαιο 4 ότι το WEP αδυνατεί να παρέχει ασφαλή έλεγχο πρόσβασης. Το CRC checksum είναι μία συνάρτηση χωρίς κλειδί (unkeyed) του μηνύματος κι έτσι μπορεί να υπολογιστεί από οποιονδήποτε.

Αν κάποιος υποκλέψει ένα plaintext που αντιστοιχεί σε κάποιο μεταδιδόμενο πλαίσιο θα μπορέσει να εισάγει τυχαία κίνηση στο δίκτυο. Όπως έχουμε αναφέρει, η γνώση του plaintext και του ciphertext μπορούν να αποκαλύψουν την ακολουθία κλειδί. Στη συνέχεια, μπορεί αυτή η ακολουθία να χρησιμοποιηθεί για τη δημιουργία ενός νέου πακέτου με το ίδιο IV.

Επειδή ακριβώς το WEP έχει την ιδιότητα να μπορούν να επαναχρησιμοποιηθούν οι προηγούμενες τιμές των IV η επίθεση αυτή μπορεί να γίνει χωρίς ο παραλήπτης να αντιληφθεί οτιδήποτε.

Ένας τρόπος για την αποφυγή αυτού του προβλήματος είναι η απαγόρευση της χρήσης του ίδιου IV σε πολλά πακέτα. Το πρότυπο 802.11 όμως, ενώ συστήνει στους διαχειριστές των WLAN να μην επαναχρησιμοποιούν τα IV, δεν απαιτεί αυτό να αλλάζει σε κάθε πακέτο. Έτσι ο κάθε παραλήπτης θα πρέπει είτε να αποδέχεται επαναλαμβανόμενα IV, είτε να ρισκάρει το να μην είναι σε θέση να λειτουργήσει με κάποιες συμβατές συσκευές.

Αξίζει να σημειωθεί ότι για την επίθεση αυτή δεν ευθύνεται το CRC και οι ιδιότητές του. Οποιαδήποτε συνάρτηση που δε χρησιμοποιεί κλειδί δε θα είχε καμία επίδραση στην επίθεση. Μόνο ένας κώδικας πιστοποίησης μηνύματος με κλειδί (keyed message authentication code) όπως ο SHA1-HMAC θα μπορούσε να προστατεύσει τα μηνύματα από τέτοιου είδους επιθέσεις.

5.5 Άλλες προτάσεις

Όπως αναφέραμε στο προηγούμενο κεφάλαιο προβλήματα δημιουργούνται λόγω της σταθερής δομής του IP μηνύματος. Μία πιθανή λύση θα ήταν να προστίθενται στο plaintext κάποια τυχαία byte, είτε στην αρχή του, είτε σε κάποιο τυχαίο σημείο [26].

Έχει προταθεί επίσης η αντικατάσταση του Kerberos από ένα EAP-TLS handshake [25], για την προστασία του συστήματος από την επίθεση του λεξικού αποκρυπτογράφησης.

Μία άλλη προσέγγιση είναι η DHAKM (Diffie-Hellman Authentication and Key Management) [23]. Σύμφωνα μ' αυτήν σε κάθε πιστοποίηση χρησιμοποιούνται παράμετροι προηγούμενων συνδέσεων για την παραγωγή των νέων κλειδιών.

Επίσης μία πρόταση είναι η χρήση του ESP [19], ένα πρωτόκολλο που υποστηρίζει ένα σύνολο από διαφορετικούς αλγόριθμους κρυπτογράφησης (DES, 3DEC, RC5, CAST κλπ) και προσφέρει καλύτερη ασφάλεια.

5.6 Συμπεράσματα

Το IEEE 802.11 είναι ίσως το πιο διαδεδομένο πρότυπο που χρησιμοποιείται στα ασύρματα τοπικά δίκτυα. Είναι αποδεκτό από ένα πολύ μεγάλο σύνολο κατασκευαστών και συμβατό με πολλά προϊόντα. Έχει κάποια προβλήματα στην ασφάλεια που παρέχει, αλλά δεν παύει να αποτελεί μια πολύ ισχυρή βάση και με έναν πιο προσεγμένο σχεδιασμό μπορούν να επιτευχθούν οι στόχοι ασφάλειας που έχουν τεθεί.

ΠΑΡΑΡΤΗΜΑ

AP (Access Point): Ένας σταθμός ο οποίος παρέχει πρόσβαση στις υπηρεσίες διανομής μέσω του ασύρματου μέσου στους σταθμούς που είναι συνδεδεμένοι με αυτόν.

Ad hoc: Ένα ασύρματο τοπικό δίκτυο, το οποίο αποτελείται από σταθμούς που επικοινωνούν μεταξύ τους χωρίς την ύπαρξη κάποιου AP.

BSS (Basic Service Set): Ένα σύνολο από σταθμούς, οι οποίοι συντονίζονται από ένα AP.

DS (Distribution System): Το σύστημα που χρησιμοποιείται για τη διασύνδεση ενός συνόλου από BSS και LAN, δηλαδή τη δημιουργία ενός ESS.

DSS (Distribution System Service): Ένα σύνολο από υπηρεσίες που παρέχονται από το DS, ώστε να μπορεί το επίπεδο MAC να μεταδίδει δεδομένα ανάμεσα σε σταθμούς οι οποίοι δεν είναι απευθείας συνδεδεμένοι μεταξύ τους.

ESS (Extended Service Set): Ένα σύνολο από διασυνδεδεμένα BSS και LAN.

IV (Initialization Vector): Το διάνυσμα αρχικοποίησης για την παραγωγή του keystream.

Keystream: Η ακολουθία κλειδιού, δηλαδή μία ακολουθία από bit που προκύπτουν δίνοντας ως είσοδο στην γεννήτρια ψευδοτυχαίων αριθμών του αλγορίθμου WEP τη συνένωση του μυστικού κλειδιού κι ενός διανύσματος αρχικοποίησης (Initialization Vector – IV).

MIB (Management Information Base): Η βάση, στην οποία αποθηκεύονται όλες οι πληροφορίες που αφορούν τους σταθμούς του WLAN.

WEP (Wired Equivalent Privacy): Ο προαιρετικός αλγόριθμος κρυπτογράφησης που ορίζεται από το πρότυπο IEEE 802.11 και χρησιμοποιείται για να παρέχει εμπιστευτικότητα στα δεδομένα ενός WLAN ισοδύναμη με την εμπιστευτικότητα των δεδομένων ενός ενσύρματου LAN.

WLAN (Wireless Local Area Network): Ασύρματο τοπικό δίκτυο.

ΑΝΑΦΟΡΕΣ

[1] IEEE Std 802.11-1999, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

[2] B. O' Hara, A. Petrick, *The IEEE 802.11 Handbook,* Standards Information Network – IEEE Press.

[3] J. Walker, *Unsafe at any key size; An analysis of the WEP encaptulation,* Tech. Rep. 03628E, IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/documents/DocumentHolder/0-362.zi%p.

[4] W. Abaugh, N. Shankar, *Your 802.11 Wireless Network has No Clothes,* March, 2001.

[5] N. Borisov, I. Goldberg, D. Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11.* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[6] 3Com Wireless LANs, *How Wireless LANs Work,* 3Com Wireless LAN Scenarios. http://3com.com/mobile/wireless/wlan_works.html

[7] 3Com Wireless LANs, *What's New in Wireless LANs: The IEEE 802.11b Standard,* IEEE 802.11b Wireless LANs – Full Text. http://www.3com.com/technology/tech_net/white_papers/503072a.html

[8] T. H. Siang, *Security in Wireless LAN.*

[9] Linux Wireless LAN How to, *Wireless Overview – Some Wireless LAN Standards.*

[10] K. Kesarev, *Security level and solutions in wireless and mobile data transfer.*

[11] NACS - UCInet Mobile Access, http://www.nacs.uci.edu/ucinet/mobile

[12] M. Jakobsson, S. Wetzel, *Security Weaknesses in Bluetooth,* RSA Conference 2001, p. 176-191.

[13] HomeRF, *Home Networking Technologies Whitepaper,* HomeRF Working Group.

[14] Technology brief, *802.11 wireless security in business networks,* February 2001. www.dell.com.

[15] S. Weatherspoon, *Overview of IEEE 802.11b Security,* Network Communications Group, Intel Corporation.

[16] N. Borisov, I. Goldberg, D. Wagner, *Security of the WEP algorithm.* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[17] T. Rune, *Wireless Local Area Networks,* Netplan ApS.
http://www.netplan.dk/netplan/wireless.htm

[18] R. Housley, D. Whiting, J. Walker, *WEP2 Enhancements.*
http://grouper.ieee.org/groups/802/11/Documents/D1T551-600.html

[19] R. Moskowitz, *Using the Encapsulating Security Payload (ESP) for WLAN privacy and protection.*
http://grouper.ieee.org/groups/802/11/Documents/D1T551-600.html

[20] N. Cam-Winget, J. Walker, G. Chesson, *Authenticated Key Exchange at the MAC Layer.*
http://grouper.ieee.org/groups/802/11/Documents/D1T501-550.html

[21] B. Beach, *Security Requirements for Highly Mobile Devices.*
http://grouper.ieee.org/groups/802/11/Documents/D1T451-500.html

[22] L. Salgarelli, M. Buddhikot, S. Miller, *Adaptation of Existing Mobile IP Authentication for use in IEEE 802.11 Systems.*
http://grouper.ieee.org/groups/802/11/Documents/D1T451-500.html

[23] C. Rios, *Optional MAC-Level Authentication and Encryption Key Management.*
http://grouper.ieee.org/groups/802/11/Documents/D1T451-500.html

[24] A. Young, B. O' Hara, *A Re-key Proposal.*
http://grouper.ieee.org/groups/802/11/Documents/D1T501-550.html

[25] S. Blake-Wilson, *EAP-TLS Alternative for Security*, Certicom.
http://grouper.ieee.org/groups/802/11/Documents/D1T301-350.html

[26] A. Chickinsky, *Wireless LAN Security Threats.*
http://grouper.ieee.org/groups/802/11/Documents/D1T251-300.html

[27] B. Aboba, *WEP2 Security Analysis.*
http://grouper.ieee.org/groups/802/11/Documents/D1T251-300.html

[28] J.P. Edney, *EAPAuthentication Suite Advertising.*
http://grouper.ieee.org/groups/802/11/Documents/D1T300-350.html