ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗΣ ΔΙΚΥΤΩΝ

ΠΡΟΤΥΠΟ IEEE 802.11

ΓΚΙΟΚΑΣ ΟΡΕΣΤΗΣ ΑΝΑΣΤΑΣΙΟΣ

Α.Μ. 1047061

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

OSI: Open Systems Interconnection model

(V)LAN: (Vitrual) Local Area Network

IEEE: Institute of Electrical and Electrinics Engineers

MAC: Medium Access Control

PHY: Physical

CSMA: Carrier Sense Multiple Access

LLC: Logical Link Control

FHSS: Frequency Hopping Spread Spectrum

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

PLCP: Physical Layer Convergence Procedure

PMD: Physical Medium Dependent

PAN: Personal Area Networks

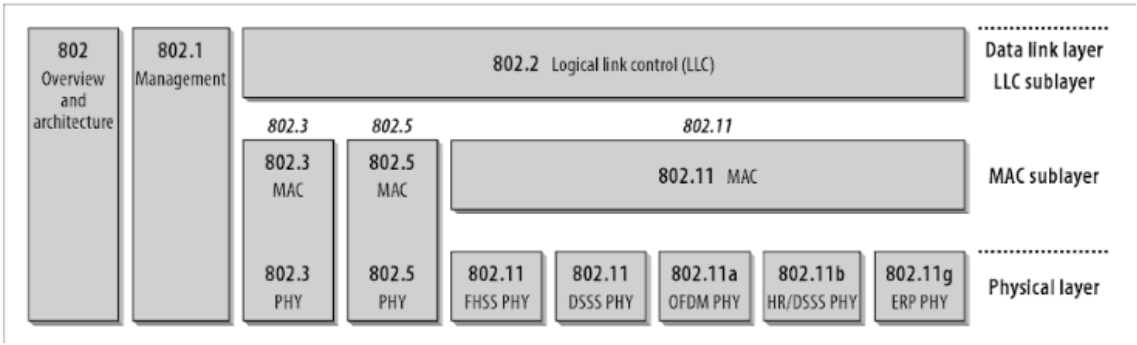
MIMO: Multiple Input-Multiple Output

WEP: Wired Equivalent Privacy

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Σύνοψη των δικτύων 802.11

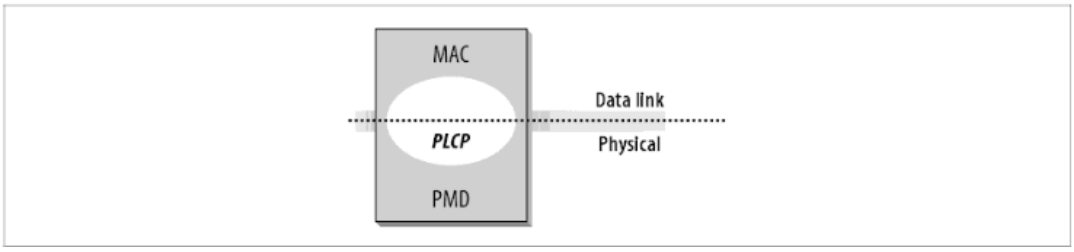
Το 802.11 είναι μέλος της οικογένειας IEEE 802, μιας σειράς προδιαγραφών για τεχνολογίες τοπικού δικτύου LAN. Το σχήμα 1-1 δείχνει τη σχέση μεταξύ των διάφορων συνιστωσών της οικογένειας 802 και τη θέση τους στο μοντέλο OSI.



Σχήμα 1-1: Η οικογένεια IEEE 802 και η σχέση της με το μοντέλο OSI

Οι προδιαγραφές του IEEE 802 επικεντρώνονται στα δύο χαμηλότερα επίπεδα του μοντέλου OSI επειδή ενσωματώνουν τόσο στοιχεία φυσικής όσο και στοιχεία σύνδεσης δεδομένων. Όλα τα 802 δίκτυα διαθέτουν ένα στοιχείο MAC και ένα στοιχείο Physical (PHY). Το MAC address είναι ένα σύνολο κανόνων που καθορίζουν τον τρόπο πρόσβασης στο μέσο και την αποστολή δεδομένων, αλλά οι λεπτομέρειες της μετάδοσης και της λήψης παραμένουν στη PHY. Οι ιδιαίτερες προδιαγραφές της σειράς 802 αναγνωρίζονται από έναν δεύτερο αριθμό. Για παράδειγμα, 802.3 είναι η προδιαγραφή για ένα Carrier Sense Multiple Access δίκτυο με ανίχνευση σύγκρουσης (CSMA/CD), το οποίο σχετίζεται (και συχνά αποκαλείται εσφαλμένα) Ethernet . Άλλες προδιαγραφές περιγράφουν άλλα τμήματα του πρωτοκόλλου 802. Το 802.2 καθορίζει έναν κοινό σύνδεσμο, το Logical Link Control (LLC), ο οποίος μπορεί να χρησιμοποιηθεί από οποιαδήποτε τεχνολογία LAN χαμηλότερου επιπέδου. Τα χαρακτηριστικά διαχείρισης για 802 δίκτυα καθορίζονται στο 802.1. Μεταξύ των πολλών αρμοδιοτήτων της 802.1 είναι η γεφύρωση (bridging)(802.11D) και τα

εικονικά LAN, ή VLANS (802.1Q). Το 802.11 είναι απλά ένα άλλο επίπεδο σύνδεσης που μπορεί να χρησιμοποιήσει την ενσωμάτωση 802.2 / LLC. Η βασική προδιαγραφή 802.11 περιλαμβάνει το 802.11 MAC και δύο φυσικά επίπεδα: ένα φυσικό επίπεδο φάσματος διασποράς συχνότητας (FHSS) και ένα επίπεδο διασύνδεσης ευρείας ζώνης άμεσης ακολουθίας (DSSS) [1]. Οι μεταγενέστερες αναθεωρήσεις του 802.11 πρόσθεσαν επιπλέον φυσικά επίπεδα. Το 802.11b καθορίζει ένα επίπεδο άμεσης ακολουθίας υψηλής ταχύτητας (HR/DSSS), τα προϊόντα που βασίζονται στο 802.11b βγήκαν στην αγορά το 1999 και ήταν τα πρώτα συστήματα PHY μαζικής αγοράς, το 802.11a περιγράφει ένα φυσικό επίπεδο που βασίζεται σε ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM). Το 802.11g είναι το νεότερο φυσικό επίπεδο. Προσφέρει υψηλότερη ταχύτητα μέσω της χρήσης OFDM, αλλά με συμβατότητα προς τα πίσω με το 802.11b. Η συμβατότητα προς τα πίσω όμως έχει τα μειονεκτήματά της. Όταν οι χρήστες 802.11b και 802.11g συνυπάρχουν στο ίδιο σημείο πρόσβασης, απαιτείται πρόσθετο γενικό πρωτόκολλο, μειώνοντας τη μέγιστη ταχύτητα για χρήστες 802.11g. Το 802.11 επιτρέπει πρόσβαση σε κινητό δίκτυο, για να εκπληρωθεί αυτός ο στόχος, ενσωματώθηκαν στην MAC πρόσθετα χαρακτηριστικά. Ως αποτέλεσμα, το MAC 802.11 μπορεί να φαίνεται πολύπλοκο σε σύγκριση με άλλες προδιαγραφές MAC IEEE 802. Η χρήση ραδιοκυμάτων απαιτεί επίσης σχετικά σύνθετο PHY. Το 802.11 χωρίζει το PHY σε δύο γενικά μέρη: τη Διαδικασία Σύγκλισης Φυσικής Στρώσης (PLCP), για τη χαρτογράφηση των πλαισίων MAC στο μέσο και ένα σύστημα Φυσικών Ενδιάμεσων Εξαρτήσεων (PMD) για τη μετάδοση αυτών των πλαισίων. Το PLCP περιβάλλει το όριο των MAC και των φυσικών στρωμάτων, όπως φαίνεται στο Σχήμα 1-2. Στο 802.11, το PLCP προσθέτει ένα αριθμό πεδίων στο πλαίσιο καθώς μεταδίδεται στον αέρα.



Σχήμα 1- 2: Ανάλυση του επιπέδου PHY

Τα πρωτόκολλα 802.11 έχουν πολλές λεπτομέρειες που μπορούν να τροποποιηθούν, αλλά οι περισσότερες εφαρμογές του 802.11 αποκρύπτουν αυτήν την πολυπλοκότητα. Πολλά από τα χαρακτηριστικά του προτύπου ενεργοποιούνται μόνο όταν το δίκτυο έχει

συμφόρηση, είτε με πολλή κίνηση είτε με μεγάλο αριθμό ασύρματων σταθμών. Τα δίκτυα πιέζουν όλο και περισσότερο τα όρια και από τις δύο πλευρές.

ΚΕΦΑΛΑΙΟ 2: MULTI-HOP ΔΙΚΤΥΑ

2.1 Εισαγωγή στα Multi-hop δίκτυα

Στα κυψελοειδή και ασύρματα τοπικά δίκτυα, η ασύρματη επικοινωνία εμφανίζεται μόνο στον τελευταίο σύνδεσμο μεταξύ ενός σταθμού βάσης και του ασύρματου τελικού συστήματος. Στα ασύρματα multi-hop δίκτυα υπάρχει ένας ή περισσότεροι ενδιάμεσοι κόμβοι κατά μήκος της διαδρομής που λαμβάνουν και προωθούν τα πακέτα μέσω ασύρματων συνδέσεων. Τα ασύρματα δίκτυα multi-hop έχουν πολλά πλεονεκτήματα: Σε σύγκριση με τα δίκτυα με άμεσες ασύρματες συνδέσεις, τα ασύρματα δίκτυα πολλαπλών συνδέσεων μπορούν να επεκτείνουν την κάλυψη ενός δικτύου και να βελτιώσουν τη συνδεσιμότητα. Επιπλέον, η μετάδοση μέσω πολλαπλών "σύντομων" συνδέσεων ενδέχεται να απαιτεί λιγότερη ισχύ μετάδοσης και ενέργεια από τους "μεγάλους" συνδέσμους. Επιπλέον, επιτρέπουν υψηλότερους ρυθμούς μετάδοσης δεδομένων που οδηγούν σε υψηλότερη απόδοση και πιο αποδοτική χρήση του ασύρματου μέσου. Τα ασύρματα δίκτυα Multi-hop αποφεύγουν την εκτεταμένη εγκατάσταση καλωδίων και μπορούν να χρησιμοποιηθούν με οικονομικά αποδοτικό τρόπο. Σε περίπτωση πυκνών δικτύων πολλαπλών συνδέσεων, ενδέχεται να διατίθενται αρκετές διαδρομές που μπορούν να χρησιμοποιηθούν για την αύξηση της ευρωστίας του δικτύου. Δυστυχώς, τα πρωτόκολλα που αναπτύσσονται για σταθερά ή κυψελοειδή δίκτυα καθώς και για το διαδίκτυο δεν είναι βέλτιστα για ασύρματα δίκτυα πολλαπλών συνδέσεων. Αυτό ισχύει ιδιαίτερα για τα πρωτόκολλα δρομολόγησης, γι' αυτό το λόγο έχουν αναπτυχθεί τα εντελώς νέα πρωτόκολλα δρομολόγησης unicast, multicast και broadcast για ad-hoc και δίκτυα αισθητήρων.

2.2 Μεταφορά Πακέτων σε Δίκτυα Multi-hop

Στα ασύρματα δίκτυα πολλαπλών συνδέσεων, οι κόμβοι επικοινωνούν μεταξύ τους χρησιμοποιώντας λιγότερα κανάλια και δεν χρειάζονται κοινή υποδομή ή κεντρικό έλεγχο. Οι κόμβοι μπορούν να συνεργάζονται μεταξύ τους προωθώντας ή αναμεταδίδοντας πακέτα, ενδεχομένως με τη συμμετοχή πολλών κόμβων αναμετάδοσης. Αυτό επιτρέπει στους κόμβους που δεν συνδέονται άμεσα να επικοινωνούν μέσω ενδιάμεσων επαναλήψεων χωρίς να αυξάνουν την ισχύ μετάδοσης. Αυτή η αναμετάδοση πολλαπλών χορδών είναι μια πολύ ελπιδοφόρα λύση για την αύξηση της απόδοσης και την κάλυψη για μια μεγάλη φυσική περιοχή. Χρησιμοποιώντας πολλούς ενδιάμεσους κόμβους, ο αποστολέας μπορεί να μειώσει τη δύναμη μετάδοσης περιορίζοντας έτσι τα φαινόμενα παρεμβολής και επιτρέποντας τη χωρική επαναχρησιμοποίηση των ζωνών συχνοτήτων. Σε δίκτυα ad-hoc, το μέσο μοιράζεται και οι κόμβοι ρυθμίζουν την πρόσβαση στο μέσο με κατανεμημένο τρόπο, ανεξάρτητα από την τρέχουσα κυκλοφορία. Συγκεκριμένα δίδονται τυπικά πρωτόκολλα δρομολόγησης ad-hoc που προσπαθούν να ελαχιστοποιήσουν τους κόμβους αναμετάδοσης στη διαδρομή. Οι κόμβοι πιο κοντά στο κέντρο του δικτύου είναι πιο πιθανό να γίνουν ένας κόμβος αναμετάδοσης. Αυτό έχει το μειονέκτημα ότι ένας κόμβος που χρησιμεύει ως κόμβος αναμετάδοσης για μεταφορές πολλαπλών γειτονικών κόμβων είναι επιρρεπής σε προβλήματα απόδοσης. Όταν υπάρχουν πολλαπλές επαναμεταδόσεις σε μια διαδρομή από άκρο σε άκρο, είναι σημαντικό να ελέγχεται η επιβάρυνση για κάθε μετάδοση ενός πακέτου. Δυστυχώς, τα τρέχοντα συστήματα ελέγχου πρόσβασης μεσαίου επιπέδου (MAC) και τα φυσικά επίπεδα για δίκτυα πολλαπλών συνδέσεων δικτύων τοπικού ασύρματου τοπικού δικτύου (WLAN) επιβάλλουν υψηλά έξοδα για τη μετάδοση μικρών πακέτων δεδομένων τα οποία χρησιμοποιούνται για κλήσεις Voice over Internet Protocol (VoIP). Με το συνδυασμό

πολλών μικρών πακέτων σε μεγαλύτερες, η μετάδοση πακέτων πάνω μπορεί να μειωθεί σημαντικά. [2]

2.3 Ad-hoc Δίκτυα

Τα δίκτυα ad hoc αποτελούν βασικό παράγοντα στην εξέλιξη των ασύρματων επικοινωνιών. Αυτοοργανωμένα ad hoc δίκτυα PDAs ή φορητοί υπολογιστές χρησιμοποιούνται στην αντιμετώπιση προβλημάτων. Αυτά τα δίκτυα κληρονομούν τα παραδοσιακά προβλήματα των ασύρματων και κινητών επικοινωνιών, όπως η βελτιστοποίηση του εύρους ζώνης, ο έλεγχος ισχύος και η βελτίωση της ποιότητας μετάδοσης. Επιπλέον, η πολυεπίπεδη φύση τους και η πιθανή έλλειψη μίας σταθερής υποδομής εισάγουν νέα ερευνητικά προβλήματα όπως η διαμόρφωση του δικτύου, η ανακάλυψη συσκευών και η συντήρηση τοπολογίας, καθώς και διευθυνσιοδότηση και αυτοδιάθεση ad-hoc. Διάφορες προσεγγίσεις και πρωτόκολλα έχουν προταθεί για την αντιμετώπιση ad-hoc προβλημάτων δικτύωσης και πολλές προσπάθειες τυποποίησης βρίσκονται σε εξέλιξη για την τεχνολογία του Διαδικτύου, καθώς και σε ακαδημαϊκά και βιομηχανικά ερευνητικά έργα. Στα ad hoc δίκτυα, οι ασύρματοι κεντρικοί υπολογιστές μπορούν να επικοινωνούν μεταξύ τους ελλείψει σταθερής υποδομής. Αυτά τα δίκτυα αποτελούνται συνήθως από ίσους κόμβους που επικοινωνούν μέσω ασύρματων ζεύξεων χωρίς κεντρικό έλεγχο. Τα δίκτυα αισθητήρων, που ονομάζονται επίσης υβριδικά ad hoc δίκτυα, συνδέονται με κέντρα παρακολούθησης που συλλέγουν δεδομένα όπως θερμοκρασία, ανίχνευση χημικών ή κίνηση. Τα τελευταία χρόνια, κρατικές υπηρεσίες σε αρκετές χώρες έχουν υποστηρίξει την έρευνα στα δίκτυα αισθητήρων. Για παράδειγμα, το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ εγκαινίασε ένα διεπιστημονικό πρόγραμμα για την έρευνα αισθητήρων και αισθητήρων δικτύων το 2003 [3]. Ορισμένα δίκτυα ad hoc συνδέονται με σταθερή υποδομή μέσω σημείων πρόσβασης. Για παράδειγμα, το πλέγμα ή τα δίκτυα στέγης [4] αποτελούνται από κεραίες τοποθετημένες πάνω από κτίρια για την παροχή ασύρματης πρόσβασης στο διαδίκτυο. Τα οχήματα σε αυτοκινητόδρομο μπορούν να δημιουργήσουν ένα ad hoc

δίκτυο για χρήση στη διάδοση των πληροφοριών κυκλοφορίας. Μπορούν να λειτουργούν ως ένα καθαρό ad hoc δίκτυο στο οποίο ένα μεμονωμένο όχημα ανιχνεύει συμβάντα κυκλοφορίας και εκκινεί μια εκπομπή σε άλλα οχήματα. Εναλλακτικά, τα κυψελοειδή σημεία πρόσβασης ή τα σημεία πρόσβασης στο Internet που βρίσκονται κοντά στο δρόμο μπορούν να μεταδώσουν τις πληροφορίες. Τα πολυπολιτισμικά κυψελοειδή δίκτυα εμφανίστηκαν πρόσφατα ως εναλλακτική επικοινωνία σε εκδηλώσεις όπου συγκεντρώνεται ένας τεράστιος αριθμός χρηστών σε μια μικρή περιοχή όπως ένα στάδιο. Τα δίκτυα "peer-to-peer" είναι ad hoc δίκτυα στα οποία είναι ενσωματωμένο ένα δίκτυο επικάλυψης στο Internet. Σε ένα δίκτυο P2P, δύο ή περισσότεροι hosts μπορούν να χρησιμοποιούν κατάλληλα συστήματα πληροφοριών και επικοινωνίας για να συνεργάζονται αυθόρμητα χωρίς κεντρικό συντονισμό.

2.3.1 Επικοινωνία δικτύου ad hoc

Η επικοινωνία μεταξύ δύο οικοδεσποτών σε ένα δίκτυο ad hoc δεν είναι πάντα άμεση, αλλά μπορεί να προχωρήσει σε ένα multihop έτσι ώστε κάθε οικοδεσπότης να είναι επίσης δρομολογητής. Οι κεντρικοί υπολογιστές δικτύου ad hoc μπορούν να χρησιμοποιήσουν πρωτόκολλα όπως το πρότυπο ελέγχου πρόσβασης πολυμέσων IEEE 802.11 για επικοινωνία μέσω της ίδιας συχνότητας ή μπορούν να εφαρμόσουν τεχνολογία Bluetooth ή άλλη τεχνολογία αναβάθμισης συχνότητας. Επειδή η κατανάλωση ρεύματος είναι ευθέως ανάλογη με την απόσταση μεταξύ των κεντρικών υπολογιστών, οι άμεσες μεταδόσεις ενός καναλιού μεταξύ δύο κεντρικών υπολογιστών μπορούν να απαιτήσουν σημαντική ισχύ, προκαλώντας παρεμβολές σε άλλες παρόμοιες μεταδόσεις. Για να αποφύγετε αυτό το πρόβλημα δρομολόγησης, δύο κεντρικοί υπολογιστές μπορούν να χρησιμοποιήσουν τη μετάδοση πολλαπλών σταθμών για να επικοινωνούν μέσω άλλων κεντρικών υπολογιστών στο δίκτυο. Με την τεχνολογία IEEE 802.11 [5], η αποφυγή των παρεμβολών συγκρούσεων - μετάδοσης είναι δύσκολη λόγω του προβλήματος των κρυφών σταθμών: Δύο κεντρικοί υπολογιστές που δεν επικοινωνούν απευθείας μπορούν ταυτόχρονα να μεταδίδουν μηνύματα σε έναν κοινό γείτονα με την ίδια συχνότητα. Τέλος, εκτός από τη διατήρηση

μιας τρέχουσας εργασίας δρομολόγησης ή τη διευκόλυνση της διαδρομής εγκατάσταση, τα δίκτυα κινητής τηλεφωνίας πρέπει επίσης να υποστηρίζουν τη διαχείριση θέσης παρακολουθώντας την τοποθεσία του χρήστη.

2.3.2 Προβλήματα με το Network Layering

Τα προβλήματα που παρουσιάζονται στο επίπεδο δικτύου των ad hoc δικτύων περιλαμβάνουν τον έλεγχο της τοπολογίας, την κυκλοφορία των δεδομένων και την πρόσβαση στις υπηρεσίες. Τα προβλήματα ελέγχου τοπολογίας περιλαμβάνουν την ανακάλυψη των γειτονικών κόμβων, την αναγνώριση της θέσης, τον προσδιορισμό της ακτίνας μετάδοσης, την καθιέρωση συνδέσεων με τους γείτονες, τον προγραμματισμό του χρόνου αδράνειας του κόμβου και τις ενεργές περιόδους, τη σύμπλεξη, την κατασκευή του κυρίαρχου συνόλου (κάθε κόμβος ανήκει ή έχει έναν γείτονα από το δεσπόζον σύνολο) διατηρώντας την επιλεγμένη δομή. Τα προβλήματα επικοινωνίας δεδομένων περιλαμβάνουν:

• *δρομολόγηση:* στέλνοντας ένα μήνυμα από μια πηγή σε έναν κόμβο προορισμού,

• *εκπομπή:* στέλνοντας ένα μήνυμα από μια πηγή σε όλους τους άλλους κόμβους του δικτύου,

• *διαμεσολάβηση:* στέλνοντας ένα μήνυμα από μια πηγή

σε ένα σύνολο επιθυμητών προορισμών,

• *geocasting:* στέλνοντας ένα μήνυμα από μια πηγή

σε όλους τους κόμβους σε μια γεωγραφική περιοχή και

• *ενημέρωση τοποθεσίας:* διατηρώντας εύλογα ακριβείς πληροφορίες σχετικά με την τοποθεσία των άλλων κόμβων.

Τα προβλήματα πρόσβασης σε υπηρεσίες περιλαμβάνουν πρόσβαση στο Internet, την πρόσβαση σε κυψελοειδή δίκτυα, την αναπαραγωγή δεδομένων ή υπηρεσιών κατά την ανίχνευσή τους και τη μοναδική διεύθυνση IP σε συγχώνευση ή περιπτώσεων διασπασμένου δικτύου. [6]

2.4 Αναλύοντας το πρόβλημα

Στο “Cooperative Cache-Based Data Access in Ad Hoc Networks” , οι Guohong Cao, Liangzhong Yin και Chita Das προτείνουν αποτελεσματικές λύσεις στο πρόβλημα αποθήκευσης δεδομένων. [7] Σε συνεταιριστική κρυφή μνήμη ορισμένοι κόμβοι σε ένα ad hoc δίκτυο αναπαράγουν δεδομένα από διακομιστές χρησιμοποιώντας αρχεία που έχουν αναπαραχθεί ήδη για να ικανοποιήσουν τις απαιτήσεις άλλων κόμβων πρόσβασης. Αυτό θα πρέπει να μειώσει την κυκλοφορία στο δίκτυο ή ακόμα και να παράσχει την υπηρεσία, εάν ο διακομιστής αποσυνδεθεί εν συνεχεία. Οι προτεινόμενες λύσεις περιλαμβάνουν caching δεδομένων, δημιουργώντας ένα άλλο αντίγραφο των δεδομένων στο κόμβο και χρησιμοποιώντας μερικές νέες υβριδικές μεθόδους Μια αναδυόμενη περιοχή έρευνας σε δίκτυα αισθητήρων είναι η κάλυψη και η παρακολούθηση της περιοχής. Στην "Παρακολούθηση της ενεργειακής απόδοσης για τα δίκτυα αισθητήρων", οι Jean Carle και David Simplot-Ryl, κατατάσσουν την αναφορά δεδομένων αισθητήρων σε δύο κατηγορίες: οδηγούμενες και κατ’ απαίτηση. Προτείνουν τη διαίρεση του προβλήματος παρακολούθησης της περιοχής σε τρία υποπρογράμματα, καθένα από τα οποία απαιτεί μια ενεργειακά αποδοτική λύση. Αυτά τα δευτερεύοντα προβλήματα λύνονται με την κατασκευή ενός δένδρου DFS, την επιλογή αισθητήρων για κάλυψη περιοχής και την αναφορά δεδομένων αισθητήρα με συνάθροιση δεδομένων. Τα πρωτόκολλα εφαρμόζουν πολύ μικρές αλλαγές στους ρόλους των αισθητήρων για να επεκτείνουν τη διάρκεια ζωής του δικτύου. Οι προτεινόμενες λύσεις χρησιμοποιούν κυρίαρχα σύνολα και κατ’ εξαίρεση ελάχιστα δέντρα. Στο Cross Layering στο Mobile Ad-hoc Network Design, ο Marco Conti και οι συνεργάτες του περιγράφουν ένα ευρωπαϊκό έργο που ξεπερνά τα υπάρχοντα

προβλήματα επιδόσεων επιτρέποντας στα πρωτόκολλα που ανήκουν σε διαφορετικά επίπεδα να συνεργάζονται, μοιράζοντας πληροφορίες σχετικά με την κατάσταση του δικτύου διατηρώντας ταυτόχρονα ξεχωριστά επίπεδα. Οι συγγραφείς προτείνουν την ενεργοποίηση των αισθητήρων στην κατάσταση δικτύου, ώστε να μπορούν να στέλνονται σήματα μεταξύ των επιπέδων. Αυτό επιτρέπει σε κάθε επίπεδο να διατηρεί το υπάρχον δίκτυο και να προσαρμόζει ανάλογα την απόδοσή του. Αυτή η καινοτόμος προσέγγιση πολλαπλών στρωμάτων αφορά κυρίως την ασφάλεια και τη συνεργασία, την ενεργειακή διατήρηση και τα ζητήματα ποιότητας των υπηρεσιών. Πολλές πιθανές εφαρμογές δικτύου ad hoc για κινητά περιλαμβάνουν τη συνεργασία μεταξύ μιας ομάδας κόμβων. Ο Chao Gui και ο Jian Li περιγράφουν διάφορες τεχνικές για ομαδικές επικοινωνίες σε ad hoc δίκτυα, συμπεριλαμβανομένου του multicasting, broadcasting, και geocasting, και προτείνουν αντιπροσωπευτικά πρωτόκολλα για καθεμιά από αυτές τις κατηγορίες. Παρέχουν επίσης μια επισκόπηση σχετικών ζητημάτων όπως το σχεδιασμό πρωτοκόλλου, τη συντήρηση του κράτους και την απόδοση. Εξετάζουν ζητήματα όπως η αξιοπιστία, η εξοικονόμηση ενέργειας, η ποιότητα των υπηρεσιών και η ασφάλεια. και σχολιάζει τις μελλοντικές κατευθύνσεις έρευνας για ομαδικές επικοινωνίες σε ad hoc δίκτυα. Στην ενότητα "Δρομολόγηση και ασφάλεια σε δίκτυα ad hoc για κινητά", ο Nikola Milanovic και οι συνάδελφοι προτείνουν μια έρευνα σχετικά με τη δρομολόγηση, τις υπερφορτώσεις του δικτύου και τα θέματα ασφάλειας, με βάση τα τρέχοντα σχέδια του IETF. Οι συγγραφείς περιγράφουν τέσσερεις αλγορίθμους δρομολόγησης που δεν βασίζονται σε υποθέσεις: δρομολόγηση δυναμικής πηγής κατόπιν ζήτησης, διανυσματικής ad hoc διεύθυνσης εξ αποστάσεως, προωθημένη βελτιστοποιημένη δρομολόγηση γραμμής σύνδεσης και μετάδοση τοπολογίας βασιζόμενη στην προώθηση αντίστροφης κατεύθυνσης. Συζητείται επίσης μια πρόσφατα προτεινόμενη υβριδική προσέγγιση που συνδυάζει τα πλεονεκτήματα της κατ' απαίτηση και της βελτιστοποιημένης δρομολόγησης σύνδεσης-συνδέσεων για ασύρματα δίκτυα αισθητήρων. Αντί να χρησιμοποιήσει το παραδοσιακό επίπεδο δικτύου που βασίζεται στο IP για την υλοποίηση πρωτόκολλων δρομολόγησης πολλαπλών μεταδόσεων, στο "Προσανατολισμένο πολυλειτουργικό δίκτυο με επικάλυψη σε κινητά ad hoc περιβάλλοντα", ο Li Xiao και οι συνάδελφοι προτείνουν ένα μοντέλο που βελτιώνει την αποδοτικότητα και την ευρωστία του multicast overlay, με τη βοήθεια των πληροφοριών εντοπισμού για τους κόμβους μέλη. Όπως τα δίκτυα P2P, το POM σχηματίζει ένα εικονικό δίκτυο, το οποίο αποτελείται μόνο από κόμβους μελών, πάνω από τη φυσική υποδομή. Ο κόμβος των μελών μπορεί να σχηματίσει μια

ομάδα βραχυπρόθεσμων πολυεκπομπών για να εκτελέσει ορισμένα σημαντικά καθήκοντα Τα δέντρα επικάλυψης μπορούν να έχουν διαφορετικά επίπεδα προτεραιότητας ανάλογα με τη σημασία της υπηρεσίας που εκτελούν. Αυτή η προσέγγιση αποφεύγει την ανάγκη αλλαγής του δέντρου επιπέδων εφαρμογής στις υποκείμενες αλλαγές δικτύου.

ΚΕΦΑΛΑΙΟ 3: IEEE 802.11 AC

3.1 Εισαγωγή στα δίκτυα Wi-Fi 5ης γενιάς

Η κίνηση δεδομένων κινητής τηλεφωνίας αυξήθηκε 18x μεταξύ 2011 και 2016 λόγω της αύξησης των συνδρομητών κινητής τηλεφωνίας και των απαιτήσεων σχετικά με το εύρος ζώνης για την υποστήριξη εφαρμογών που έχουν μεγάλες απαιτήσεις σε δεδομένα [8]. Συνεπώς, υπάρχει ανάγκη για συσκευές και πρότυπα ικανά να ανταπεξέλθουν στα δίκτυα κινητής τηλεφωνίας νέας γενιάς, τα οποία απαιτούν πολύ υψηλές ροές δεδομένων για τη διατήρηση των εφαρμογών βίντεο, φωνής, ζωντανών τυχερών παιχνιδιών και επαυξημένης πραγματικότητας, μεταξύ άλλων. Για το σκοπό αυτό, η Ομάδα Εργασίας IEEE 802.11ac (TGac) επεξεργάζεται μια τροπολογία με στόχο την επίτευξη μέγιστης αθροιστικής δυναμικότητας δικτύου τουλάχιστον 1 Gbps σε ζώνες κάτω των 6 GHz, εξαιρουμένης της ζώνης 2,4 GHz. Συγκεκριμένα, το πρότυπο προβλέπει μέγιστη ταχύτητα μετάδοσης πρόσβασης (MAC) τουλάχιστον 500 Mb/s για έναν μόνο χρήστη και τουλάχιστον 1 Gb/s στην περίπτωση πολλαπλών χρηστών. Το 802.11n [9], σε αντίθεση με όλες τις προηγούμενες τροποποιήσεις του προτύπου 802.11, στοχεύει στη βελτίωση της συνολικής διακίνησης του δικτύου καθώς και του κάθε χρήστη ξεχωριστά [10]. Λόγω της σημαντικής αύξησης του ρυθμού που επιτυγχάνεται με το 802.11ac, ο όρος πολύ υψηλός βαθμός παραγωγής (VHT) χρησιμοποιείται επίσης σε σχέση με αυτή τη νέα τροποποίηση. Στον Πίνακα 1 παρουσιάζεται μια περίληψη της εξέλιξης του προτύπου 802.11 συγκρίνοντας μερικά από τα κύρια χαρακτηριστικά κάθε γενιάς. Ο πίνακας παρουσιάζει διαφορές μεταξύ των 802.11b, a, g, n, και ac. Έχουν προταθεί αρκετές τροποποιήσεις προκειμένου να επιτευχθούν τα ποσοστά παραγωγικότητας της τάξης των gigabit.

Feature/IEEE standard	802.11b	802.11g/a	802.11n	802.11ac
Maximum data rate per stream (Mb/s)	11	54	>100	>500 (Assuming 80 MHz channels)
Frequency band	2.4 GHz	2.4 GHz/5 GHz	2.4 GHz and 5 GHz	5 GHz
Channel width (MHz)	20	20/20	20 and 40 (40 is optional)	20,40,80, 160, and 80+80 (last two are optional)
Antenna technology	Single-input single-output (SISO)	SISO	Multiple-Input Multiple-Output (MIMO)	MIMO/MU-MIMO
Transmission technique	Direct sequence spread spectrum (DSSS)	DSSS and orthogonal frequency-division multiplexing (OFDM)	OFDM	OFDM
Maximum number of spatial streams	1	1	4	8
Beamforming-capable	No	No	Yes	Yes
Date ratified by IEEE	1999	2003/1999	2009	Expected 2014

Πίνακας 1: Σύγκριση των προτύπων IEEE 802.11

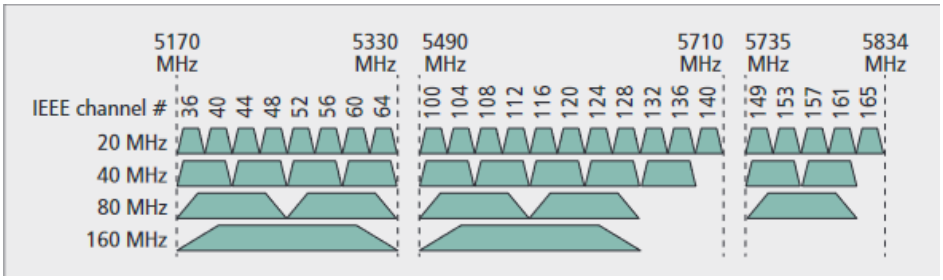
Εδώ θα εξετάσουμε τα διάφορα χαρακτηριστικά και βελτιώσεις που διαφοροποιούν το 802.11ac από τα προηγούμενα πρότυπα. Πιο συγκεκριμένα, θα περιγράψουμε τις βασικές τροποποιήσεις τόσο σε φυσικό επίπεδο όσο και σε MAC. Ενώ πολλές από τις προδιαγραφές του 802.11n έχουν διατηρηθεί για το 802.11ac (π.χ. στατική και δυναμική σύνδεση καναλιών και ταυτόχρονες ροές δεδομένων), αυτές έχουν ενισχυθεί για να επιτρέπουν την υποστήριξη ευρύτερων καναλιών καθώς και περισσότερων ροών δεδομένων, δύο βασικά χαρακτηριστικά που επιτρέπουν στο 802.11ac να επιτύχει τα ποσοστά μετάδοσης gigabit είναι: Η στατική και δυναμική σύνδεση καναλιών και η πολλαπλή έξοδος πολλαπλών εισόδων (MU-MIMO). Για να ενεργοποιηθούν αυτές οι δύο λειτουργίες, απαιτούνται ουσιαστικές τροποποιήσεις στο PHY. Ως επί το πλείστον, σε επίπεδο MAC, οι προτεινόμενες αλλαγές απαιτούνται για να διασφαλιστεί η συμβατότητα με το τροποποιημένο PHY. Συγκεκριμένα, βασικά χαρακτηριστικά που προτείνονται στην τροπολογία 802.11ac περιλαμβάνουν τα ακόλουθα: Υποχρεωτική υποστήριξη για κανάλια 20, 40 και 80 MHz και προαιρετική υποστήριξη για 160 MHz και 80 + 80 MHz πλάτους καναλιών (συνεχόμενα και μη συνεχόμενα, αντίστοιχα). Επιπλέον, προτείνεται ένα αίτημα για αποστολή / εκκαθάριση για αποστολή (RTS / CTS) μηχανισμού τόσο για τη στατική όσο και για την δυναμική κράτηση εύρους ζώνης. Το 802.11ac εισάγει το MU-MIMO προτείνοντας ένα μοναδικό πρωτόκολλο ρητής ανατροφοδότησης που επιτρέπει τη

μετάδοση ακτινοβολίας. Αυτό έρχεται σε αντίθεση με τα προηγούμενα πρότυπα, όπου εισήχθησαν διαφορετικές μέθοδοι μορφοποίησης νημάτων για ένα χρήστη, αλλά καμία από αυτές δεν είχε εντολή πιστοποίησης. Αυτό οδήγησε στην έλλειψη συμβατικότητας μεταξύ των διαφόρων κατασκευαστών. Επιπλέον, ο αριθμός των χωρικών ροών αυξάνεται από τέσσερα σε 802.11n σε οκτώ σε 802.11ac. Όσον αφορά τα συστήματα διαφοροποίησης και κωδικοποίησης. Το 802.11ac δίνει εντολή μονής διαμόρφωσης χωρικής ροής έως 64-τετραγωνικής διαμόρφωσης εύρους (OAM) με ταχύτητα κωδικοποίησης 5/6 και δυαδική κωδικοποίηση συνελικτών. Επιτρέπει επίσης υψηλότερη πυκνότητα κωδικοποίησης (256-0AM με ρυθμό κωδικοποίησης 3/4 και 5/6) και τη χρήση κωδικοποίησης μπλοκ διαστήματος χρόνου (STBC) και κώδικα ελέγχου ισοτιμίας χαμηλής πυκνότητας (LDPC) ως επιλογές. Επιπλέον, το πρότυπο καθορίζει τη χρήση διαφορετικών σχημάτων συσσωμάτωσης πλαισίων. Συγκεκριμένα, προτείνει την υποχρεωτική χρήση της συσσωμάτωσης πλαισίων για την αύξηση της χρήσης του καναλιού και της αποτελεσματικότητας της MAC. Η τροπολογία 802.11ac αναπτύσσεται για την αντιμετώπιση διαφορετικών τύπων μοντέλων χρήσης. Οι κύριες κατηγορίες είναι η ασύρματη απεικόνιση, η διανομή High Definition περιεχομένου στο σπίτι της και άλλου περιεχομένου, ταχεία μεταφόρτωση και λήψη μεγάλων αρχείων από και προς τους διακομιστές, κυκλοφορία backhaul, χρήση σε πανεπιστήμια και αίθουσες συνεδριάσεων και κατασκευή αυτοματισμού δαπέδων. Παρατηρήστε ότι οι σταθμοί 802.11ac είναι συμβατοί με τις συσκευές παλαιού τύπου. Δηλαδή, η νέα τροποποίηση καθορίζει χαρακτηριστικά επιπλέον του 802.11n, πράγμα που σημαίνει ότι ένας σταθμός συμμόρφωσης 802.11ac μπορεί επίσης να υποστηρίζει όλα τα υποχρεωτικά χαρακτηριστικά που ορίζονται στο 802.11n.

3.2 Καναλοποίηση

3.2.1 Υποστηριζόμενο εύρος συχνοτήτων

Η τροπολογία ορίζει ότι όλες οι συσκευές υποστηρίζουν κανάλια 20, 40 και 80 MHz. Επιπλέον, παρέχει προαιρετική υποστήριξη για λειτουργία σε κανάλια 160 MHz. 80 και 160 MHz κανάλια μπορούν να σχηματιστούν με συνδυασμό δύο γειτονικών μη επικαλυπτόμενων καναλιών 40 και 80 MHz, αντίστοιχα. Η τροπολογία διευκρινίζει επίσης ότι δύο μη γειτονικά κανάλια 80 MHz μπορούν να χρησιμοποιηθούν για τη διαμόρφωση ενός σήματος 160 MHz. Σημαντικότερα, μια συσκευή που λειτουργεί σε μη συνεχόμενα 80 + 80 MHz θα πρέπει να είναι σε θέση να επικοινωνεί με συσκευές που λειτουργούν σε συνεχόμενα 160 MHz εάν τα πρώτα τμήματα τοποθετούνται σε συχνότητα ώστε να ταιριάζουν με την κατανομή του ήχου της τελευταίας περίπτωσης. Στο Σχήμα 3-1 παρουσιάζεται η κατανομή του καναλιού για την περιοχή των Η.Π.Α.

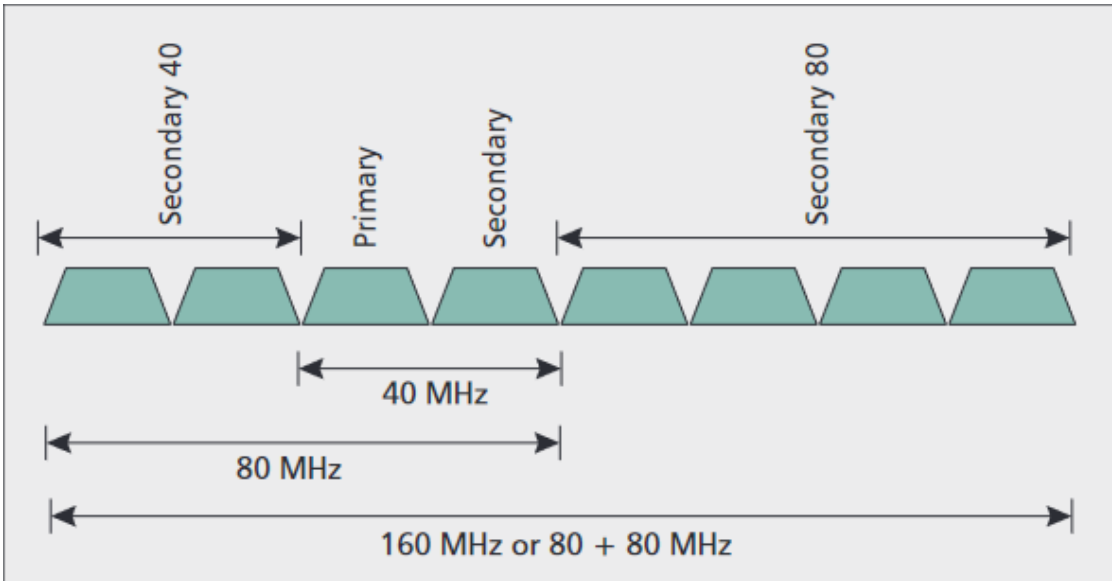


Σχήμα 3- 1: Διαμερισμός συχνοτήτων στις Ηνωμένες Πολιτείες

3.2.1

3.2.1 Κύρια και δευτερεύοντα υποκανάλια

Παρόμοια με το 802.11n, κανάλια αποτελούμενα από 40 MHz ή περισσότερα, απαιτούν πάντα ένα πρωτεύον υποκανάλι εύρους 20 MHz. Επιπλέον, κανάλια 80 MHz έχουν πρωτεύον 40 MHz subchannel και δευτερεύον 40 MHz. Το ίδιο ισχύει για κανάλια 160 MHz και 80 + 80 MHz, τα οποία αποτελούνται από δευτερεύοντα και πρωτεύοντα κανάλια των 80 MHz. Στο σχήμα 3-2 απεικονίζεται αυτή τη σχέση μεταξύ του πρωτογενούς και του δευτερεύοντος υποκαναλιού βάσει των διαφορετικών επιλογών εύρους ζώνης. Σε όλες τις περιπτώσεις, το πρωτεύον τέτοιο κανάλι χρησιμοποιείται για την ανίχνευση φορέα προκειμένου να διασφαλιστεί ότι καμία άλλη συσκευή δεν μεταδίδει. Η παρουσία του δευτερεύοντος καναλιού 20 MHz είναι επίσης απαραίτητη για την εγγύηση της συνύπαρξης και της συμβατότητας με τις παλαιότερες συσκευές 802.11. Μόνο ο κύριος υποδίαυλος εκτελεί πλήρη εκτίμηση καναλιών (CCA), η οποία περιλαμβάνει την ανίχνευση πακέτων ξεκινώντας από το πρώτο. Αντίθετα, ο δευτερεύων υποδίαυλος δεν απαιτείται να εκτελεί πλήρη CCA. Η ευαισθησία CCA του κύριου υποκαναλιού είναι 82 dBm για ένα έγκυρο σήμα 202 MHz 802,11, 79 dBm για ένα έγκυρο σήμα 802,11 40 MHz, 76 dBm για ένα έγκυρο σήμα 80 MHz και 73 dBm για ένα έγκυρο 160 MHz. Από την άλλη πλευρά, για τον δευτερεύοντα υποδίαυλο η ευαισθησία βελτιώθηκε από -62 dBm σε -72 dBm και για τα κανάλια των 20 και 40 MHz, σε σύγκριση με τα 802.11n (και -69 dBm για τα κανάλια των 80 MHz). Σύμφωνα με μια συσκευή 802.11ac θα πρέπει να ανιχνεύσει εάν ο πρωτεύων υποδίαυλος είναι απασχολημένος μέσα σε 4 μs με πιθανότητα μεγαλύτερη από 90 τοις εκατό. Το δευτερεύον κανάλι της συσκευής έχει μέχρι 25μs για να ανιχνεύσει εάν είναι απασχολημένο με την ίδια πιθανότητα.



Σχήμα 3- 2: Πρωτεύουσα και δευτερεύουσα επιλογή καναλιού

3.3 Στατική και δυναμική πρόσβαση σε κανάλια

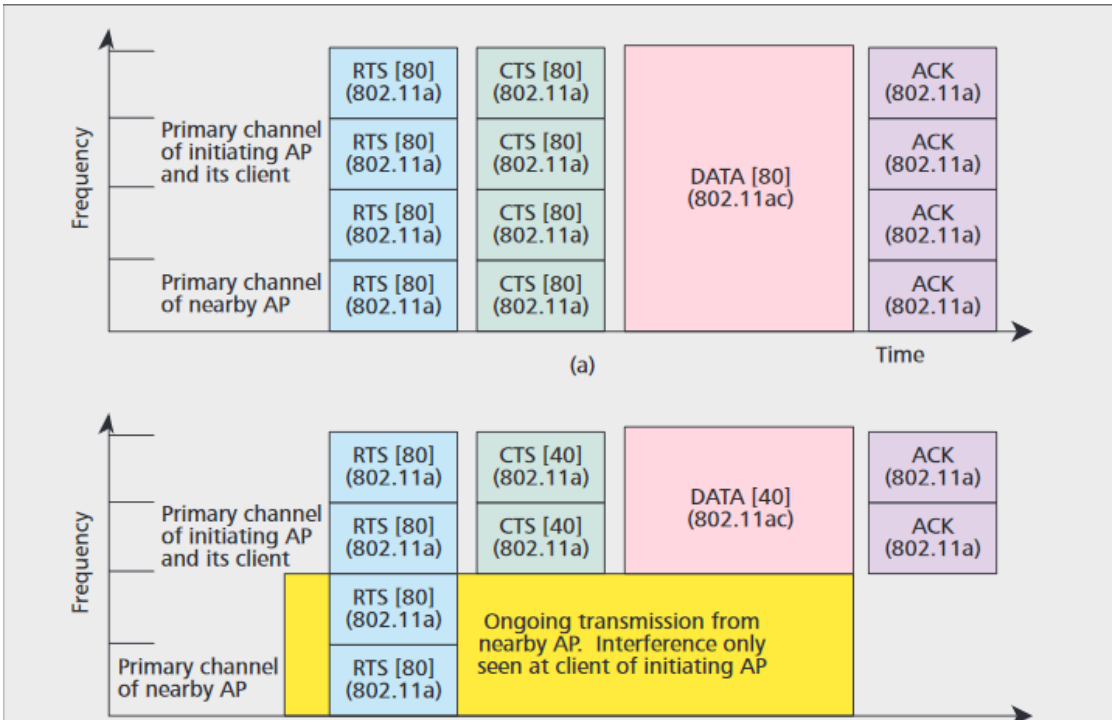
Το IEEE 802.11ac επεκτείνει τις πολιτικές πρόσβασης καναλιών που προτείνονται στο 802.11n στην περίπτωση καναλιών 80 και 160 MHz. Προκειμένου μια μονάδα 802.11ac να μπορεί να μεταδίδει δεδομένα πρωτοκόλλου (PDU) διαδικασίας σύγκλισης 80 MHz, πρέπει να ισχύουν δύο προϋποθέσεις: Το πρωτεύον κανάλι ακολουθεί κανόνες ενισχυμένου προσπελάσιμου καναλιού (EDCA), οπότε χρειάζεται (DIFS) συν τη διάρκεια του μετρητή αναμονής (backoff). Και οι τρεις δευτερεύοντες υποδίαυλοι πρέπει να ήταν αδρανείς για μια χρονική περίοδο μεταξύ των διαστημάτων πλαισίου συντονισμού (PIFS) αμέσως πριν από την εκπνοή του μετρητή backoff οποιοσδήποτε από τους δευτερεύοντες υποσταθμούς είναι απασχολημένος, ο σταθμός μπορεί να ακολουθήσει είτε κανόνες στατικής είτε δυναμικής πρόσβασης καναλιού όπως υπαγορεύεται από το 802.11n: Στατική

πρόσβαση καναλιού: Ας θεωρήσουμε έναν σταθμό 802.11ac που προσπαθεί να μεταδώσει σε 80 MHz. Εάν ο δευτερεύων υποσταθμός του καναλιού είναι απασχολημένος, ο σταθμός θα επιλέξει μια τυχαία περίοδο αποκοπής εντός του τρέχοντος μεγέθους του παραθύρου σύγκρουσης για να ξεκινήσει ξανά η διαδικασία αμφισβήτησης και να συνεχίσει να επιχειρεί μόνο μέχρι να μην υπάρχει καμία παρέμβαση σε κανένα από τα δευτερεύοντα κανάλια. Παρατηρήστε ότι με έναν μεγάλο αριθμό παλαιών σταθμών θα μειωθεί η πιθανότητα πρόσβασης στο μέσο με ένα τέτοιο ευρύ κανάλι. Δυναμική πρόσβαση καναλιών: Ο σταθμός 802.11ac μπορεί να επιχειρήσει να μεταδώσει μέσω ενός καναλιού χρησιμοποιώντας 20 ή 40 MHz αντ' αυτού Αυτό θα εξαρτηθεί από κάθε CCA υποδίκτυο. Αυτό είναι σαφώς πιο ευέλικτη προσέγγιση, η οποία επιτρέπει πιο αποτελεσματική κατανομή πόρων, επειδή ο σταθμός μπορεί να μεταδίδει πάνω από ένα κλάσμα του αρχικού εύρους ζώνης. Όλες οι εκπομπές θα πρέπει πάντα να περιλαμβάνουν το πρωτεύον κανάλι για να ενημερώσουν τον δέκτη σχετικά με τα κανάλια που θα χρησιμοποιήσει ο πομπός [11].

3.4 Μηχανισμοί RTS/CTS

Εάν ένα σημείο πρόσβασης 802.11ac (AP) βρίσκεται κοντά σε άλλα παλαιότερα AP, είναι πιθανό ότι το πρωτεύον κανάλι THC 20 MHz οποιασδήποτε από τις τελευταίες είναι οποιοδήποτε εντός 80 ή 160 MHz από το προηγούμενο κανάλι. Αυτό σημαίνει ότι τα διαφορετικά AP και οι πελάτες τους μπορούν να μεταδίδουν σε αλληλεπικαλυμμένους χρόνους σε διαφορετικά υποκανάλια, οδηγώντας έτσι σε συγκρούσεις ή αναβολές [9]. Για να ξεπεραστεί αυτό το πρόβλημα, το 802.11ac ορίζει μια χειραψία για να χειριστεί σωστά τόσο τη στατική όσο και τη δυναμική κατανομή καναλιών. Αυτή η χειραψία αποτελείται από έναν τροποποιημένο μηχανισμό RTS / CTS που παρέχει πληροφορίες σχετικά με το τρέχον διαθέσιμο εύρος ζώνης. Παρουσιάζεται ακολούθως πώς λειτουργεί το βελτιωμένο πρωτόκολλο RTS / CTS με το ακόλουθο παράδειγμα [απεικονίζεται στο σχήμα 3] [9]: Εξετάζουμε ένα σενάριο στο οποίο ένα αρχικό AP θέλει να μεταδώσει δεδομένα σε έναν συνδεδεμένο πελάτη

μέσω ενός καναλιού 80 MHz. Το AP πρώτα ελέγχει εάν το κανάλι είναι αδρανές. Εάν είναι, μεταδίδει πολλαπλά RTS στην επίσημη μορφή του 802.11a PPDU (ένα RTS για κάθε υποκανάλι 20 MHz). Επομένως, αναμένεται ότι κάθε κοντινή συσκευή (κληρονομιά ή 802.11ac) μπορεί να λάβει ένα RTS στο πρωτεύον κανάλι της. Κάθε μία από αυτές τις συσκευές ορίζει το NAV. Πριν από ένα αντιγράψει το δεδομένο στον δέκτη με CTS, ελέγχει εάν είναι κατειλημμένο κάποιο από τα δευτερεύοντα κανάλια στη ζώνη των 80 MHz. Ο πελάτης απαντά μόνο με ένα CTS σε αυτούς τους δευτερεύοντες αγωγούς που είναι αδρανείς και αναφέρει το συνολικό εύρος ζώνης του αναπαραγόμενου CTS. Όπως συμβαίνει και με το RTS, το CTS αποστέλλεται σε μορφή PPDU 802.11a και αναπαράγεται σε διαφορετικούς αναμεταδότες 20 MHz που είναι αδρανείς. Σημειώστε στο Σχήμα 3 τις δύο διαφορετικές περιπτώσεις. Στο Σχήμα 3-3 δεν υπάρχει παρεμβολή ούτε από το αρχικό AP ούτε από τον πελάτη του. Από την άλλη πλευρά, στο Σχήμα 3b ένα ήδη κοντινό AP μεταδίδει ήδη πριν αρχίσει το AP εκκίνησης. Ωστόσο, είναι μόνο παρεμβαίνει στον πελάτη. Επομένως, ο πελάτης πρέπει να ενημερώσει το AP απαντώντας με ένα μόνο CTS στους δευτερεύοντες αγωγούς.



Σχήμα 3- 3: Ενισχυμένοι μηχανισμοί RTS/CTS χωρίς παρεμβολές (α) και με παρεμβολές (β)

3.5 Single-User MIMO

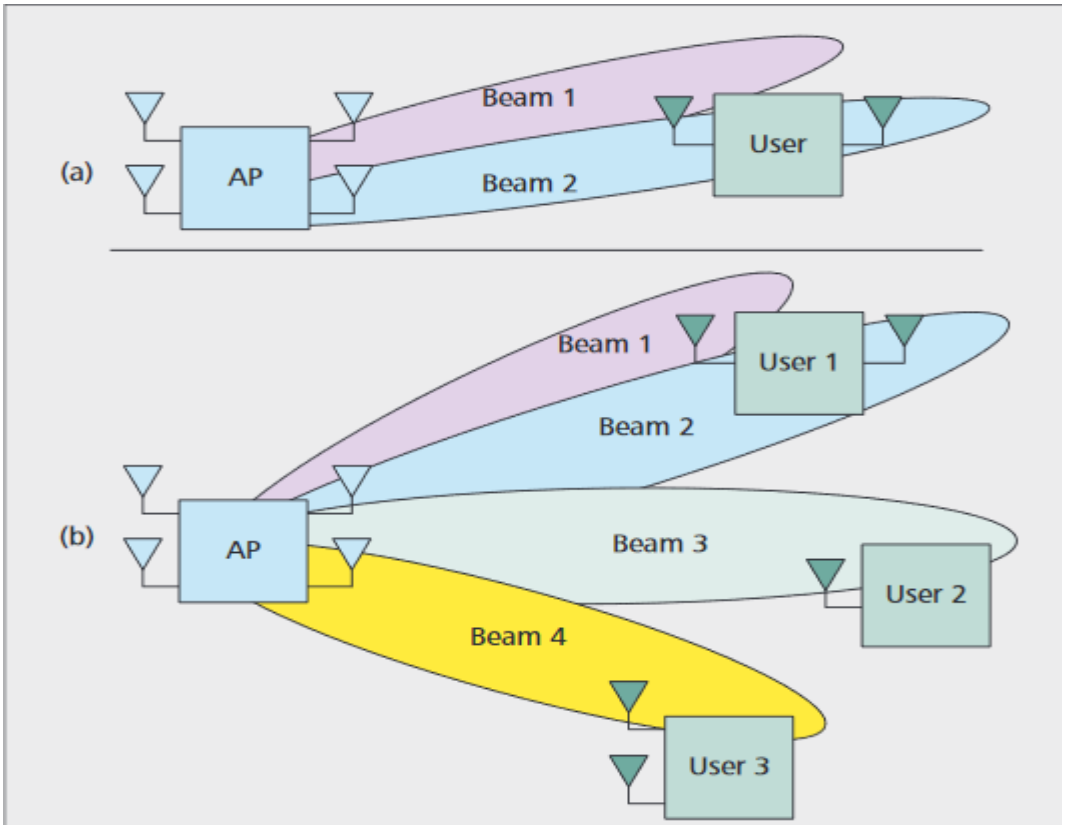
Το SU-MIMO εκμεταλλεύεται την ικανότητα πολλαπλών κεραιών να μεταδίδουν και να δέχονται δεδομένα για να βελτιώσουν την ικανότητα και την αξιοπιστία μιας μετάδοσης. Χρησιμοποιώντας κώδικες διαστήματος-χρόνου, ένα σύστημα SU-MIMO αυξάνει την ποικιλομορφία, αυξάνοντας έτσι την αξιοπιστία. Από την άλλη πλευρά, μεταδίδοντας διαφορετικές πληροφορίες για διαφορετικές ροές, μπορεί να παρέχει σημαντικά πολλαπλασιαστικά κέρδη, αυξάνοντας έτσι την ικανότητα σύνδεσης. Αυτό το σχήμα απεικονίζεται στο Σχ. 4α. Παρατηρήστε ότι ένας σταθμός πολλαπλών κεραιών έχει έναν μόνο χρήστη τη φορά.

3.6 Multi-User MIMO

Το MU-MIMO ορίζεται από το πρότυπο ως "τεχνική όπου πολλαπλοί σταθμοί, cache με δυνητικά πολλαπλές κεραίες, ανεξάρτητες ροές δεδομένων εκπομπής και/ή λήψης ταυτόχρονα". Δηλαδή, το MU-MIMO επιτρέπει στους σταθμούς που διαθέτουν πολλαπλές κεραίες να μεταδίδουν ταυτόχρονα πολλές ροές δεδομένων σε πολλαπλούς χρήστες μέσω του ίδιου καναλιού συχνότητας. Για παράδειγμα, εάν ένα AP έχει τέσσερις κεραίες, μπορεί να εξυπηρετήσει τέσσερις χρήστες μιας κεραίας κάθε φορά ή δύο χρήστες που έχουν δύο κεραίες, στέλνοντας μέχρι ένα ρεύμα ανά κεραία λήψης (με την ίδια συχνότητα). Στο σχήμα 4b απεικονίζεται η βασική ιδέα πίσω από το MU-MIMO. Παρατηρήστε ότι το AP μπορεί να εξυπηρετήσει ταυτόχρονα μεμονωμένους

χρήστες πολλαπλών κεραιών. Ιδανικά, ο αριθμός των ταυτόχρονων ροών δεδομένων που επιτρέπονται από τις τεχνικές MU-MIMO περιορίζεται μόνο από τον ελάχιστο αριθμό κεραιών είτε από το AP είτε από την πλευρά του δέκτη (π.χ. στο Σχήμα 4β φαίνεται ότι αν και υπάρχουν πέντε πιθανές κεραίες λήψης που κατανέμονται μεταξύ τριών διαφορετικών χρηστών, το AP έχει μόνο τέσσερις κεραίες για μετάδοση). Σε λειτουργία πολλαπλών χρηστών, η τροπολογία 802.11ac υποστηρίζει μέχρι τέσσερα ρεύματα που εξυπηρετούν τέσσερις διαφορετικούς χρήστες ταυτόχρονα ή έως και

τέσσερις ροές ανά χρήστη. Επιπλέον, η τροπολογία καθορίζει την υποστήριξη για διαφορετική διαμόρφωση και ρυθμό κωδικοποίησης για κάθε σταθμό που εξυπηρετείται σε μετάδοση MU-MIMO καθοδικής ζεύξης. Ένας σταθμός μετάδοσης MU-MIMO απαιτεί γνώση των πληροφοριών κατάστασης καναλιών (CSI) από όλους τους χρήστες προκειμένου να μειωθεί η ποσότητα παρεμβολών μεταξύ χρηστών που παράγονται από τις πολλαπλές ταυτόχρονες ροές. Για να επιτευχθεί αυτό, οι



Σχήμα 3- 4: α) SU-MIMO σύνδεση β) MU-MIMO σύνδεση

περισσότερες υπάρχουσες προσεγγίσεις χρησιμοποιούν συνδυασμό στρατηγικών όπως η ανατροφοδότηση, όπου ο σταθμός διαβίβασης λαμβάνει ένα μέτρο του CSI και

κωδικοποίηση δεδομένων, και οι πληροφορίες αυτές χρησιμοποιούνται για την εκτέλεση ακύρωσης παρεμβολών μεταξύ χρηστών στην πλευρά του πομπού. Το 802.11ac καθορίζει μία μέθοδο συμπιεσμένης μορφοποίησης δέσμης που βασίζεται στη χρήση ρητής ανατροφοδότησης για την υλοποίηση του MU-MIMO (τεχνική γνωστή ως μορφοποίηση δέσμης MU).

ΚΕΦΑΛΑΙΟ 4: ΑΣΦΑΛΕΙΑ WLAN ΔΙΚΤΥΩΝ

4.1 Τρωτά σημεία του WEP προτύπου

Επί του παρόντος, το WEP είναι το πρότυπο ασφαλείας που περιγράφεται για όλα τα πρότυπα 802.11 (βλέπε σχήμα 1). ο στόχος είναι για να διασφαλιστεί η ασφάλεια του WLAN στο ίδιο επίπεδο με τα ενσύρματα δίκτυα. Το WEP βασίζεται στο συμμετρικό σύστημα αλγορίθμων RC4. Οι διαχειριστές αναπτύσσουν ένα μυστικό κλειδί και στα δύο σημεία πρόσβασης και τις ασύρματες συσκευές οι οποίες χρησιμοποιούν το κλειδί για την κρυπτογράφηση δεδομένων και την εξακρίβωση της ακεραιότητας των δεδομένων. Επιπλέον, το AP μπορεί να χρησιμοποιήσει το κλειδί για την αυθεντικότητα των πελατών του. Αν και η συνολική κρυπτογραφία αλγορίθμων RCA είναι αρκετά ισχυρή, το πρότυπο WEP υιοθετεί μια προσέγγιση για τη χρήση του. Ένα από τα μεγαλύτερα downfalls του WEP είναι ότι τα μυστικά του κλειδιά (τα οποία οι ασύρματες συσκευές και τα σημεία πρόσβασης τους μοιράζονται) είναι σχετικά βραχύτερα από άλλα κλειδιά πρωτοκόλλων ασφάλειας τυπικά, 40 bits σε WEP, αν και το πρότυπο επιτρέπει έως 104. Το WEP συγκαλύπτει ένα κοινό μυστικό κλειδί με ένα σύντομο διάνυσμα αρχικοποίησης 24 bit (IV) για να δημιουργήσει το κύριο ρεύμα RC4. Για παράδειγμα, το WEP συγκαλύπτει ένα μυστικό κλειδί 40 bit με 24 bit IV, δημιουργεί ένα κύριο ρεύμα κλειδιών RC4 64 bit. Το V αποστέλλεται στον δέκτη με απλό κείμενο έτσι ώστε ο δέκτης να μπορεί να παράγει το ίδιο ρεύμα κλειδιού, πράγμα που σημαίνει ότι οι εισβολείς μπορούν να δουν τη λίστα 24 bits κάθε πλήκτρου που αποστέλλεται με WEP. Επιπλέον, το γεγονός ότι το IV είναι τόσο μικρό σχεδόν εγγυάται θα χρησιμοποιηθεί για πολλαπλά μηνύματα. Στην πραγματικότητα, το ίδιο IV μπορεί να επαναχρησιμοποιηθεί σε λιγότερο από μισή μέρα εάν υπάρχει σημαντική δραστηριότητα. Ένας τρίτος, μπορεί να συλλέξει εύκολα ένα IV και να το χρησιμοποιήσει για να ανακτήσει το κλειδί που χρησιμοποιεί το AP και τις ασύρματες συσκευές. Το τρέχον πρότυπο 802.11 έχει οδηγίες για το πώς, ή ακόμα και αν το V

πρέπει να αλλάξει. Ορισμένοι προμηθευτές εξοπλισμού χρησιμοποιούν στην πραγματικότητα το ίδιο IV για κάθε κύριο ρεύμα, πράγμα που σημαίνει ότι ένας αποκωδικοποιητής είναι εγγυημένο ότι θα αποκαλύψει την IV σε εύλογο χρονικό διάστημα. Άλλα συστήματα παράγουν τα IVs διαδοχικά, τα οποία αυξάνονται με τη μετάδοση του κάθε πακέτου WEP ασφάλειας μια επίσης κακή λύση για τη διαχείριση κλειδιών, η οποία μπορεί να αφήσει τα κλειδιά σε μια συσκευή αμετάβλητη για μεγάλες χρονικές περιόδους. Εάν η συσκευή χαθεί ή κλαπεί, ένας εισβολέας θα μπορούσε να χρησιμοποιήσει το κλειδί για να θέσει σε κίνδυνο όχι μόνο αυτή τη συσκευή, αλλά οποιαδήποτε άλλη συσκευή που μοιράζεται το ίδιο κλειδί. Οι λύσεις δυναμικής διαχείρισης κλειδιών θα μπορούσαν να συμβάλουν στην άμβλυνση της απειλής των κλειδιών WEP που πέφτουν σε λάθος χέρια καθώς και στην αύξηση της πολυπλοκότητας Επιπλέον, η προσθήκη στις ελλείψεις των πρωτοκόλλων είναι η εφαρμογή του αλγόριθμου Cyclic Redundan cy (CRC) -32. Ο οποίος υπολογίζει ένα άθροισμα ελέγχου 32-bit για να ελέγξει την ακεραιότητα των πακέτων που αποστέλλονται μέσω του WLAN. Επειδή το άθροισμα ελέγχου που δημιουργεί το CRC-32 είναι μια μη ερυθρογραφική τιμή, γνωστές επιθέσεις, όπως επίθεση side channel, μπορούν να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων.

4.2 Ανησυχίες για τα WLAN δίκτυα δημόσιας χρήσης

Ένα άτομο που επιχειρεί να συνδεθεί σε ένα εταιρικό δίκτυο μέσω δημόσιου δικτύου μπορεί να αποτελέσει μια άλλη απειλή για ένα ιδιωτικό δίκτυο. Για παράδειγμα, οι χρήστες που έχουν πρόσβαση σε ένα δημόσιο hotspot WLAN σε καφετέρια ή αεροδρόμιο ανοίγουν ένα κανάλι στο εταιρικό τους δίκτυο. Συνήθως, τα δημόσια δίκτυα δεν προσφέρουν ασφάλεια. αυτό επιτρέπει στους επιτιθέμενους στην περιοχή να παρακολουθούν το δίκτυο και να βλέπουν όλα τα πακέτα που μεταφέρονται με απλό κείμενο στο WLAN. Αυτός ο τύπος επίθεσης έχει αυξηθεί τα τελευταία χρόνια, καθώς τα δημόσια δίκτυα έχουν γίνει πιο δημοφιλή και θα συνεχίσουν να αυξάνονται καθώς όλο και περισσότερα pop-ups εμφανίζονται σε όλο τον κόσμο. Οι χρήστες δεν έχουν ιδέα ότι μόλις άνοιξαν μια πίσω πόρτα στο δίκτυο της εταιρείας τους. Οι επιτιθέμενοι σε απόσταση χιλιόμετρα μακριά από τη φυσική τοποθεσία του δικτύου

μπορούν έτσι να αποκτήσουν πλήρη πρόσβαση. Αντί να διασχίζουν ένα τείχος προστασίας και άλλα μέτρα ασφαλείας για να αποκτήσουν πρόσβαση, μπορούν απλώς να παρακολουθούν τη χρήση τους σε δημόσια δίκτυα WLAN. Οι διαχειριστές μπορούν να διαμορφώσουν τα συστήματά τους ώστε να αποκλείσουν την πρόσβαση στο δίκτυο από τα δημόσια δίκτυα WLANS, αλλά αυτό περιορίζει τη διαθεσιμότητα της κινητικότητας και των υπηρεσιών των χρηστών.

4.3 Βελτιώσεις ασφαλείας των WLAN δικτύων

Οι διαχειριστές δικτύων πρέπει να διασφαλίζουν ότι τα προϊόντα τους διαθέτουν τις τελευταίες αναβαθμίσεις του υλικολογισμικού, οι οποίες διαδραματίζουν βασικό ρόλο στην ικανότητα απόδοσης, ασφάλειας και διαχείρισης ενός προϊόντος. Οι διαχειριστές μπορούν να χρησιμοποιήσουν το EWG για να πιστοποιήσουν τους χρήστες WLAN και να φιλτράρουν μη εξουσιοδοτημένους χρήστες. Εάν οι διαχειριστές χρησιμοποιούν κεντρικούς διακομιστές διανομής κλειδιών, μπορούν εύκολα και αποτελεσματικά να διαχειριστούν τα κλειδιά WEP. Ωστόσο, αυτό αυξάνει την πιθανότητα αποτυχίας ενός σημείου που είναι ένα γενικό πρόβλημα σε μια κεντρική αρχιτεκτονική καθαρού έργου. Ένα σύστημα ανίχνευσης εισβολών (IDS) μπορεί να βοηθήσει τους διαχειριστές δικτύου να παρακολουθήσουν προσεκτικά το WLAN. Ορισμένοι τύποι IDS επιτρέπουν στους διαχειριστές δικτύου να καθορίζουν πολιτικές και κανόνες WLAN, ενώ άλλοι τύποι λογισμικού βοηθούν στον έλεγχο και την αξιολόγηση WLAN. Επιπλέον, το εικονικό ιδιωτικό δίκτυο (VPN) προσφέρει ασφαλή σύνδεση μέσω δημόσιου δικτύου WLAN δημιουργώντας μια σήραγγα ή ασφαλή κρυπτογραφημένη σύνδεση μεταξύ της συσκευής του χρήστη και του προορισμού. Αυτό προσθέτει την απαραίτητη ασφάλεια στις δημόσιες συνδέσεις WLAN και επιτρέπει σε όσους ταξιδεύουν για επαγγελματικούς σκοπούς να χρησιμοποιούν τις συσκευές τους σε δημόσιους χώρους χωρίς να ανησυχούν για τους εισβολείς που εισάγουν τα πακέτα που σχετίζονται με τη σύνδεσή τους. Ένα προσωπικό τείχος προστασίας που φορτώνεται στον εξοπλισμό του χρήστη μπορεί να προσθέσει ένα επιπλέον επίπεδο ασφάλειας σε τέτοια σενάρια. Τέλος, οι διαχειριστές μπορούν να εφαρμόσουν μια υποδομή δημόσιου κλειδιού (PKI) σε ένα WLAN για να

παρέχουν αξιόπιστες υπηρεσίες ασφαλείας. Όπως συμβαίνει με τα παραδοσιακά ενσύρματα δίκτυα, οι πολιτικές είναι σημαντικές στον κόσμο των WLAN. Δεν υπάρχει τέλεια πολιτική που θα πρέπει να τηρεί κάθε εταιρεία, αλλά όλοι πρέπει να έχουν και να εφαρμόζουν ένα σύνολο πολιτικών ασφαλείας προσαρμοσμένες στις ανάγκες του περιβάλλοντος WLAN. Για παράδειγμα, οι πολιτικές WLAN πρέπει να απαγορεύουν στους υπαλλήλους να προσθέτουν μόνοι τους AP στο δίκτυο.

4.4 Το μέλλον της ασφάλειας των WLAN δικτύων

Όπως συζητήσαμε προηγουμένως, υπάρχουν πολλά νέα πρότυπα υπό ανάπτυξη για μελλοντική ασφάλεια WLAN. Επί του παρόντος, το AES φαίνεται να είναι η βάση της επόμενης γενιάς του WEP κάτω από το 802.11i. Το AES επιτρέπει στους διαχειριστές να καθορίζουν το μέγεθος του κλειδιού σε 128, 192 ή 256 bits. Το αναθεωρημένο πρότυπο WEP θα χρησιμοποιήσει πιθανώς ένα πραγματικό μέγεθος κλειδιού 128 bit, αν και αυτό μπορεί να συμβεί μόνο όταν επικυρωθεί το AES ως μέρος της επόμενης γενιάς WEP. Η χρήση του AES θα εξαλείψει επίσης τη χρήση του 24-bit IV, το οποίο είναι ένα από τα μεγαλύτερα μειονεκτήματα της τρέχουσας έκδοσης του WEP AES, ωστόσο, έχει μερικά μειονεκτήματα. Επειδή η επόμενη γενιά WEP χρησιμοποιεί AES, θα είναι τεράστια ανάληψη υποχρέωσης μιας εταιρείας να αντικαταστήσει υπάρχοντα AP και άλλα εξαρτήματα WLAN προκειμένου να είναι συμβατά με το νέο πρότυπο. Η χρήση ενός μεγάλου μεγέθους κλειδιού (τουλάχιστον 128 bits) σημαίνει επίσης ότι οι συσκευές πελάτη θα χρειαστούν επιπλέον επεξεργαστική ισχύ για την κρυπτογράφηση και αποκρυπτογράφηση τους. Αυτό θα μπορούσε να επιβραδύνει τις συσκευές και τελικά να διαταράξει πολλούς χρήστες, αλλά το αποτέλεσμα παραμένει να το δούμε. Το AES θα απαιτήσει επίσης πολύ περισσότερη κατανάλωση ενέργειας από ό,τι οι περισσότερες υπάρχουσες κάρτες WLAN παρέχουν στους χρήστες και γεννούν φόβους για πρόσθετη αποστράγγιση στις φορητές συσκευές τους, (φορητούς υπολογιστές, φορητές συσκευές κ.λπ.). Γι' αυτό το λόγο δεν είναι λίγοι εκείνοι που απέρριπταν συνεχώς την ιδέα της αύξησης της κατανάλωσης ενέργειας των καρτών WLAN. Το TKIP θα μπορούσε να αποτελέσει βραχυπρόθεσμη λύση για την αντιμετώπιση των αδυναμιών του WEP έως ότου η IEEE επίσημα συμφωνήσει με το πρότυπο 802.11i. Το TKIP θα χρησιμοποιεί ένα χρονικό κλειδί 128 bit, αλλά όλοι οι χρήστες σε ένα

συγκεκριμένο AP θα μοιράζονται το ίδιο κλειδί: εάν ένας χρήστης δεχθεί επίθεση, τότε όλοι οι χρήστες αυτού του AP γίνονται ευάλωτοι στις επιθέσεις. Η μεγάλη διαφορά μεταξύ του WEP και του TKIP είναι ότι ένα χρονικό κλειδί αλλάζει κάθε 10.000 πακέτα στο TKIP, ενώ τα κλειδιά WEP είναι στατικά. Άλλοι τύποι φυσικών στοιχείων διερευνούνται για την προώθηση της ασφάλειας WLAN. Όπως αναφέρθηκε, οι EWG αποδεικνύονται σημαντικό μέρος των δικτύων WLAN και η δημοτικότητά τους θα συνεχίσει να αυξάνεται καθώς βελτιώνεται η ασφάλεια που παρέχουν. Ορισμένοι προμηθευτές επίσης αποκαλύπτουν νέα προϊόντα που υιοθετούν μια πιο συγκεντρωτική προσέγγιση για την εφαρμογή του WLAN με "χαζά φυσικά APs που συνδέονται με κεντρικά μεταλλαγμένους εγκεφάλους." Αυτή η προσέγγιση θα μπορούσε να συμβάλει στην απλοποίηση της εμφύτευσης και της διαχείρισης του WLAN. η τεχνολογία της κεραίας είναι ακόμα σε μικρή ηλικία, αλλά αυτή η περιοχή της ασύρματης τεχνολογίας μπορεί να ενισχύσει την ασφάλεια WLAN στο εγγύς μέλλον.

4.5 Συμπεράσματα

Τα δίκτυα WLAN προσφέρουν νέες υπηρεσίες που δεν μπορούν να παράσχουν τα παραδοσιακά ενσύρματα δίκτυα LAN, αλλά εισάγουν επίσης νέες ανησυχίες σχετικά με την ασφάλεια. Αν και οι ανησυχίες σχετικά με την ασφάλεια των υπηρεσιών WLAN δεν μπορούν να εξαλειφθούν πλήρως, μπορούμε να τις μετριάσουμε με την κατάλληλη ενσωμάτωση προτύπων, τεχνολογιών, διαχείρισης, πολιτικών και υπηρεσιών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αναφορές

[1] M. Gast, 802.11 wireless networks: the definitive guide, " O'Reilly Media, Inc.", 2005.

[2] T. Braun, MULTI-HOP WIRELESS NETWORKS, Bern, Switzerland, 2010.

[3] «US National Science Foundation,» 2003. [Ηλεκτρονικό]. Available: www.nsf.gov/pubs/2003/nsf03512/nsf03512.htm.

[4] Sonic, «sonic.com,» [Ηλεκτρονικό]. Available: www.sonic.net/sales/rooftop/faq.shtml) .

[5] I. Akyildiz, «A Survey on Sensor Networks,» *IEEE Comm.,* pp. 102-114, August 2002.

[6] S. Basagni, «Mobile Ad Hoc Networking,» *IEEE Press,* 2003.

[7] Y.-D. L. &. Y.-C. Hsu, «Multihop Cellular: A New Architecture for Wireless Communications,» *IEEE Infocom 2000,* pp. 1273-1282, 2000.

[8] Cisco Inc., «Cisco Visual Networking iIndex: Global,» 2011. [Ηλεκτρονικό]. Available: http://cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

[9] IEEE 802.11n-2009,, «IEEE Standard for Local and Metropolitan Area Networks — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements,» αρ. 11, 2009.

[10] R. V. Nee, «Breaking the Gigabit-Per-Second Barrier With 802.11ac,» *IEEE Wireless Communications,* p. 4, April 2011.

[11] M. Park, «IEEE 802.11ac: Dynamic Bandwidth Access,» *Proc. IEEE ICC,* 2011.