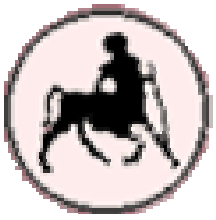
ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

Τμήμα Μηχανικών Η/Υ, Τηλεπικοινωνιών & Δικτύων



Διπλωματική Διατριβή

ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΕ ΑΣΥΡΜΑΤΑ ΑΔΟΜΗΤΑ ΔΙΚΤΥΑ

Γεώργιος Αθανασίου

Επιτροπή:

Λέανδρος Τασιούλας, *Καθηγητής Π.Θ., Επιβλέπων*

Ιορδάνης Κουτσόπουλος, *Λέκτορας Π.Θ.*

Γρηγόρης Γιοβανώφ, *Καθηγητής AIT*

Στους γονείς μου

Βλέπεις πράγματα
και αναρωτιέσαι «Γιατί;»
Αλλά εγώ ονειρεύομαι
πράγματα που
δεν υπήρξαν ποτέ
και λέω «Γιατί όχι;»

(George Bernhard Shaw)

Ευχαριστίες

Στην προσπάθειά μου αυτή συνέβαλαν πολλοί άνθρωποι τους οποίους νιώθω την ανάγκη να ευχαριστήσω. Ο επιβλέπων της διπλωματικής μου διατριβής καθηγητής κ. Λέανδρος Τασιούλας δεν σταμάτησε ποτέ να με κατευθύνει και να με διδάσκει. Σε όλη τη διάρκεια των σπουδών μου ήταν πάντα πρόθυμος να ακούσει και να υποστηρίξει κάθε ερευνητική μου ανησυχία. Τον ευχαριστώ από τα βάθη της καρδιάς μου για την εμπιστοσύνη που μου δείχνει και για την ευκαιρία που μου δίνει να συνεχίσω τις σπουδές μου.

Είμαι πολύ τυχερός να έχω δίπλα μου ανθρώπους όπως τον κ. Ιορδάνη Κουτσόπουλο που πάντα με φιλική διάθεση και με αμέριστο ενδιαφέρον μου προσφέρει απλόχερα τη βοήθειά του. Τον ευχαριστώ για τον πολύτιμο χρόνο που διέθεσε για όλη αυτή την προσπάθεια. Ευχαριστώ θερμά επίσης τον κ. Γρηγόρη Γιοβανώφ τον οποίο είχα την τύχη να γνωρίσω την περίοδο κατά την οποία αμφιταλαντευόμουν για το αντικείμενο της διπλωματικής μου διατριβής. Η διάθεσή αυτού του ανθρώπου να μου δείξει νέους δρόμους και η παρότρυνση του να τους ακολουθήσω με τιμά.

Νιώθω την ανάγκη να ευχαριστήσω τους ανθρώπους που μας έσμιξε η ζωή όλα τα χρόνια των σπουδών μου. Ευχαριστώ λοιπόν τους φίλους μου, που με τον δικό του τρόπο ο καθένας συνέβαλε και συνεχίζει να συμβάλει στην εκπλήρωση των στόχων μου. Δεν τους αναφέρω ονομαστικά αλλά ξέρουν πως κατέχουν σημαντική θέση στην καρδιά μου.

Τέλος κρατώ την τιμητική θέση για την οικογένειά μου. Είναι οι άνθρωποι που πάντα στηρίζουν τυφλά τις επιλογές μου. Η αγάπη και η εμπιστοσύνη που μου δείχνουν με συγκινεί πραγματικά. Τους ευχαριστώ από την καρδιά μου.

Ελπίζω να ανταποκρίθηκα και να συνεχίσω να ανταποκρίνομαι στις προσδοκίες όλων αυτών των ανθρώπων.

Γιώργος Αθανασίου

Βόλος, Ιούνιος 2005

Περίληψη

Τα ασύρματα δίκτυα σημείωσαν μεγάλη άνθιση τα τελευταία χρόνια και εισέβαλαν δυναμικά στην αγορά προσφέροντας ποιότητα υπηρεσιών που μπορεί να θεωρείται ανταγωνιστική με αυτή των ενσύρματων δικτύων. Η επανάσταση των ασύρματων δικτύων έχει μόλις αρχίσει. Κάθε νέο τεχνολογικό επίτευγμα πρέπει να περάσει από ένα στάδιο εντατικής ερευνητικής δραστηριότητας αποτέλεσμα της οποίας θα είναι αρχικά η λύση κάποιων βασικών προβλημάτων που ίσως υπάρχουν και έπειτα η βελτιστοποίηση της απόδοσης του. Αυτό τον καιρό παρατηρείται μια υπέρογκη ερευνητική προσπάθεια στον τομέα των ασύρματων δικτύων. Σαφώς υπάρχουν αρκετά σημεία της ασύρματης τεχνολογίας που δεν έχουν αναλυθεί επαρκώς.

Ένα από τα πιο σημαντικά προβλήματα είναι η ασφάλεια των δικτύων αυτών. Το γεγονός που καθιστά την προστασία των ασύρματων δικτύων από ποικίλες επιθέσεις πολύ δύσκολη υπόθεση, είναι ότι η λειτουργία τους διαφοροποιείται από αυτή των ενσύρματων. Το ασύρματο μέσο είναι πολύ πιο ευπαθές σε επιθέσεις από το ενσύρματο. Γίνεται αντιληπτό λοιπόν πως στον τομέα της ασφάλειας, σε αντίθεση ίσως με κάποιους άλλους τομείς, πρέπει να υπάρξει μια τελείως διαφορετική προσέγγιση από αυτή που υπάρχει στα ενσύρματα δίκτυα. Αυτό προϋποθέτει τη σωστή μελέτη των ευπαθειών και των ευαίσθητων χαρακτηριστικών αυτής της τεχνολογίας ώστε να προκύψουν κάποιες επαρκείς λύσεις. Στη συγκεκριμένη διπλωματική διατριβή θα γίνει αρχικά μία ανάλυση των τρωτών σημείων των ασύρματων δικτύων. Θα δοθεί έμφαση στα αδόμητα (ad hoc) ασύρματα δίκτυα τα οποία έχουν καθαρά κατανεμημένη αρχιτεκτονική, σε αντίθεση με τα δομημένα τα οποία έχουν πιο κεντρικοποιημένη αρχιτεκτονική. Στα αδόμητα δίκτυα δεν υπάρχει κάποια αρχική σχέση εμπιστοσύνης μεταξύ των κόμβων. Κάποιος κόμβος μπορεί να κερδίσει την εμπιστοσύνη των υπολοίπων μέσα από τη συνεργασία του στις βασικές λειτουργίες του δικτύου. Ένα σημαντικό θέμα στο οποίο θα εστιάσουμε κυρίως είναι ο τρόπος με τον οποίο γίνεται αντιληπτός ένας κόμβος που προσπαθεί να πλήξει την ασφάλεια του συστήματος αλλά και πόσο γρήγορα μπορεί να γίνει αυτό. Εξίσου σημαντικός είναι ο τρόπος με τον οποίο θα πρέπει να αντιδράσει το δίκτυο σε μια πιθανή επίθεση. Στόχος μας αρχικά είναι ο εντοπισμός και η ανάλυση κάποιων επιθέσεων και

στη συνέχεια ο σχεδιασμός μηχανισμών που προσδίδουν ανθεκτικότητα και επιτρέπουν τη σωστή λειτουργία του δικτύου. Συγκεκριμένα θα αναλυθούν οι ευπάθειες των μηχανισμών δρομολόγησης και ελέγχου πρόσβασης στο μέσο του δικτύου. Υπάρχει η αντίληψη πως η καλύτερη προσέγγιση θα ήταν η δημιουργία κάποιων ενοποιημένων (cross-layer) μηχανισμών που θα έχουν τη δυνατότητα να συνδυάσουν πληροφορίες από διαφορετικά στρώματα (layers) του δικτύου προσδίδοντας ταυτόχρονα ανθεκτικότητα σε πολλές λειτουργίες. Επίσης με αυτόν τον τρόπο διακόπτεται η επέκταση κάποιας επίθεσης. Μέσα από διαδικασίες προσομοίωσης θα δείξουμε πως ένα πρόβλημα ασφάλειας στο επίπεδο ελέγχου πρόσβασης στο μέσο του δικτύου μπορεί να προκαλέσει πολύ άσχημα αποτελέσματα στη διαδικασία της δρομολόγησης. Η ενοποίηση των επιπέδων ελέγχου πρόσβασης στο μέσο και δρομολόγησης μπορεί να αποτρέψει αυτές τις άσχημες επιπτώσεις. Ο ενοποιημένος μηχανισμός που προτείνεται αποτελεί μια καινοτόμα προσέγγιση στον τομέα της ασφάλειας και υπόσχεται πολύ καλά αποτελέσματα ακόμη κι όταν το ποσοστό των κακόβουλων χρηστών μέσα στο δίκτυο είναι μεγαλύτερο από 50%.

Περιεχόμενα

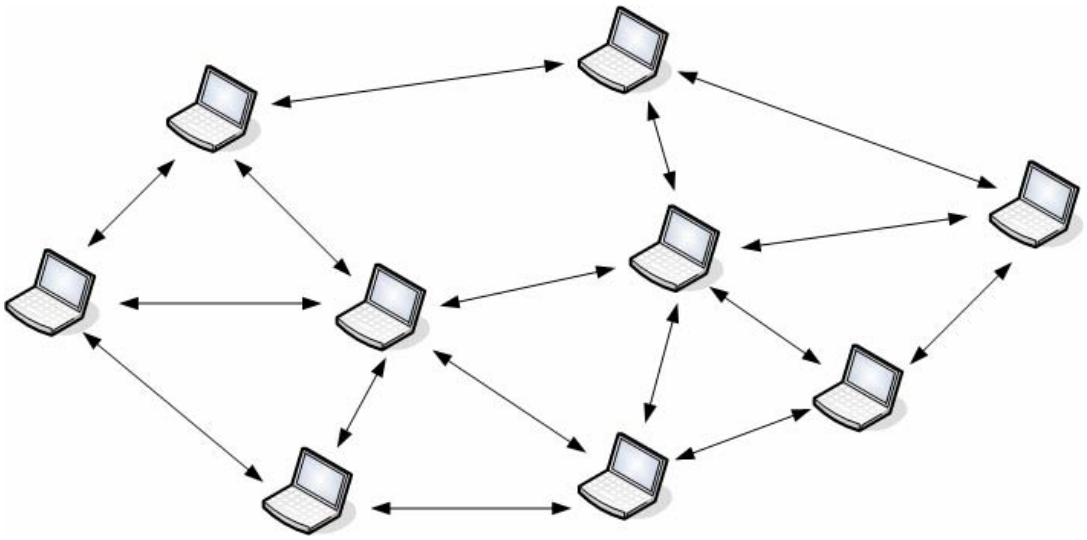
Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Τα ασύρματα αδόμητα (ad hoc) δίκτυα αποτελούνται από ένα σύνολο κόμβων που έχουν τη δυνατότητα να κινούνται. Οι κόμβοι αυτοί είναι ανεξάρτητοι μεταξύ τους και μπορούν να κινούνται αυθαίρετα σχηματίζοντας τυχαίες τοπολογίες. Στα συγκεκριμένα δίκτυα δεν υπάρχει η ανάγκη ύπαρξης κάποιας σταθερής υποδομής η οποία θα αναλάβει να φέρει εις πέρας βασικές λειτουργίες του δικτύου. Βασική προϋπόθεση για τη σωστή λειτουργία των δικτύων αυτών είναι η συνεργασία μεταξύ των κόμβων. Οι κόμβοι που βρίσκονται εντός της περιοχής εκπομπής τους επικοινωνούν μέσω των ασύρματων ζεύξεων. Όπως και σε οποιοδήποτε δίκτυο επικοινωνιών, έτσι και στα ασύρματα αδόμητα δίκτυα έχουμε τη μετάδοση πληροφορίας από κάποιο προορισμό σε κάποιο παραλήπτη. Τις περισσότερες φορές ο κόμβος που στέλνει την πληροφορία δεν συνδέεται απευθείας με τον παραλήπτη. Αυτό καθιστά σημαντική την ανάγκη εύρεσης μιας διαδρομής μεταξύ της πηγής της πληροφορίας και του προορισμού της. Προφανώς οι ενδιάμεσοι κόμβοι που αποτελούν μέρος της διαδρομής μετάδοσης της πληροφορίας είναι αναγκασμένοι να προωθήσουν την πληροφορία. Άρα βλέπουμε πως σε ένα αδόμητο δίκτυο οι κόμβοι λειτουργούν και ως δρομολογητές. Ένα παράδειγμα ενός αδόμητου δικτύου φαίνεται στο σχήμα 1.



Σχήμα 1: Παράδειγμα ασύρματου αδόμητου δικτύου.

1.1 Οι εφαρμογές των αδόμητων δικτύων

Τα τελευταία χρόνια οι ασύρματες τεχνολογίες έχουν εισέλθει δυναμικά στην αγορά. Το πιο γνωστό πρότυπο είναι το IEEE 802.11, [49], το οποίο έχει επικρατήσει λόγω της πολύ καλής λειτουργίας του αλλά και του χαμηλού κόστους των συσκευών που το υποστηρίζουν. Η απόδοση των ασύρματων τεχνολογιών έχει βελτιωθεί αρκετά και συνεχίζει να βελτιώνεται καθώς έχει προσελκύσει το ενδιαφέρον πολλών ερευνητικών προσπαθειών. Αποτέλεσμα της γρήγορης και χαμηλού κόστους ανάπτυξης των αδόμητων δικτύων είναι η εφαρμογή τους σε πολλούς τομείς. Τα αδόμητα δίκτυα χρησιμοποιήθηκαν αρχικά σε στρατιωτικές εφαρμογές καλύπτοντας μια ανάγκη για ασφαλή επικοινωνία σε δύσβατες περιοχές όπου δεν θα ήταν δυνατόν να εγκατασταθεί δικτυακή υποδομή. Προφανώς στις στρατιωτικές εφαρμογές υπάρχει η ανάγκη γρήγορης, αποδοτικής αλλά και αξιόπιστης επικοινωνίας. Τα αδόμητα δίκτυα είναι εξίσου σημαντικά σε καταστάσεις έκτακτης ανάγκης όπως επιχειρήσεις εύρεσης ή διάσωσης. Οι απαιτήσεις της συγκεκριμένης εφαρμογής είναι κοντά σε αυτές των στρατιωτικών εφαρμογών. Σε περιπτώσεις έκτακτης ανάγκης (π.χ. σεισμούς) όπου τα παραδοσιακά συστήματα επικοινωνιών είναι ανήμπορα να λειτουργήσουν, η τεχνολογία των αδόμητων δικτύων έχει να προσφέρει πολλά. Μία εφαρμογή των αδόμητων δικτύων η οποία είναι πιο προσιτή και καλύπτει πολλές φορές τις καθημερινές ανάγκες των πολιτών είναι τα

«αλληλοσυνδεόμενα» δίκτυα (mesh networks). Τα δίκτυα αυτά χαρακτηρίζονται από τον μεγάλο αριθμό των κόμβων που τα αποτελούν. Αυτό έχει σαν αποτέλεσμα η μετάδοση της πληροφορίας να πραγματοποιείται από πολλές διαδρομές χωρίς να επηρεάζεται από τα σφάλματα που ίσως υπάρχουν στις συνδέσεις ή από την κινητικότητα των κόμβων. Τα σενάρια ανάπτυξης των δικτύων αυτών είναι τα παρακάτω:

1. Κατοικημένες περιοχές όπου υπάρχει η ανάγκη ευρυζωνικής πρόσβασης στο internet.
2. Λεωφόροι, αστικοί ή εθνικοί δρόμοι όπου προσφέρεται η υπηρεσία της επικοινωνίας μεταξύ των κινούμενων οχημάτων.
3. Επαγγελματικές επικοινωνίες.
4. Πανεπιστημιουπόλεις όπου υπάρχει η ανάγκη φθηνής και άμεσης επικοινωνίας.

Μία από τις σημαντικότερες χρήσεις των αδόμητων δικτύων είναι σε υβριδικά δίκτυα. Με τον όρο υβριδικά εννοούμε τα διαφορετικής μορφής δίκτυα επικοινωνιών τα οποία επικοινωνούν μεταξύ τους (ενσύρματα δίκτυα, κυψελοειδή δίκτυα, οπτικά δίκτυα, ευρυζωνικά ασύρματα δίκτυα, τοπικά ασύρματα δίκτυα κλπ.). Οι απαιτήσεις για επικοινωνία στην εποχής μας καθιστούν έντονη την ανάγκη επίτευξης της συμβατότητας μεταξύ διαφορετικών δικτύων επικοινωνιών. Τα πλεονεκτήματα των υβριδικών δικτύων είναι η αυξημένη αξιοπιστία, η αυξημένη «ευκαμψία» τους, η πολύ καλή κάλυψη και ποιότητα επικοινωνίας και τέλος η βελτιωμένη χωρητικότητα για τη μεταφορά της πληροφορίας. Τέλος μια εξίσου σημαντική εφαρμογή των αδόμητων δικτύων είναι τα δίκτυα αισθητήρων (sensor networks). Τα δίκτυα αισθητήρων αποτελούνται από μικροσκοπικές συσκευές που έχουν τη δυνατότητα να ανιχνεύουν αυτομάτως παραμέτρους του περιβάλλοντος (π.χ. θερμοκρασία, υγρασία), να επεξεργάζονται τα δεδομένα που λαμβάνουν και να επικοινωνούν μεταξύ τους. Κι εδώ ο αριθμός των κόμβων που αποτελούν το κάθε δίκτυο είναι πολύ μεγάλος. Μία σημαντική απαίτηση των δικτύων αυτών είναι η όσο το δυνατόν χαμηλότερη κατανάλωση ενέργειας μιας και οι συσκευές τους έχουν μικρή τροφοδοσία με ισχύ.

1.2 Υπόβαθρο

Σε αυτή την ενότητα θα αναφερθούν κάποια βασικά στοιχεία του επηρεάζουν τον σχεδιασμό, την ανάπτυξη και τη λειτουργία των ασύρματων αδόμητων δικτύων. Λόγω

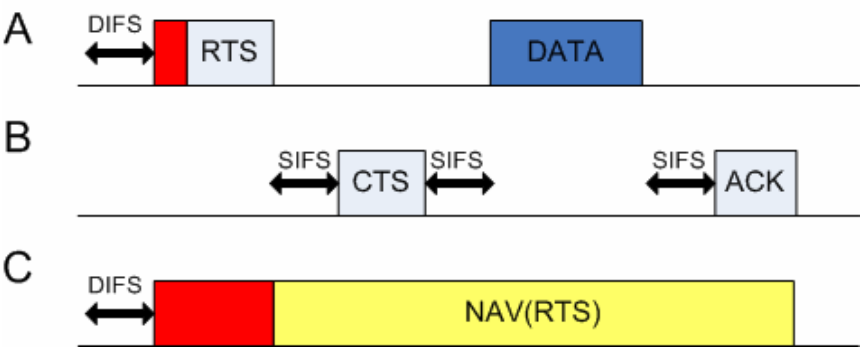
της περιορισμένης έκτασης θα γίνει λόγος μόνο για τις διαδικασίες ελέγχου πρόσβασης στο μέσο (Medium Access Control) και δρομολόγησης (Routing).

1.2.1 Έλεγχος πρόσβασης στο μέσο

Ο μηχανισμός ελέγχου πρόσβασης στο μέσο (MAC - Medium Access Control) του δικτύου είναι υπεύθυνος για τον σωστό διαμοιρασμό του καναλιού για τις μεταδώσεις των πακέτων. Ο έλεγχος πρόσβασης στα IEEE 802.11 ασύρματα δίκτυα βασίζεται στον μηχανισμό ο οποίος ονομάζεται CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Στα αδόμητα δίκτυα, των οποίων η αρχιτεκτονική είναι καθαρά κατανεμημένη, χρησιμοποιείται μια λειτουργία κατανεμημένου συντονισμού (DCF – Distributed Coordination Function) για τον διαμοιρασμό του καναλιού. Ουσιαστικά ο DCF είναι ο μηχανισμός που δίνει τη δυνατότητα στην τεχνολογία των δικτύων IEEE 802.11 να λειτουργούν με κατανεμημένο τρόπο. Στα IEEE 802.11 ασύρματα δίκτυα όπου υπάρχει κάποια υποδομή (infrastrcucture - WLANs) ο μηχανισμός που ελέγχει την πρόσβαση στο μέσο είναι ο PCF (Point Coordination function) και η λειτουργία του είναι πιο κεντρικοποιημένη από αυτή του DCF.

Ο DCF χρησιμοποιεί κάποια στοιχεία του CSMA/CA για να χειριστεί τον ανταγωνισμό των κόμβων που επιδιώκουν να αποκτήσουν πρόσβαση στο κανάλι. Κάθε κόμβος έχει μία μεταβλητή που χαρακτηρίζει το παράθυρο ανταγωνισμού (CW – Contention Window). Σε περίπτωση που κάποιος κόμβος θέλει να μεταδώσει κάποια πληροφορία επιλέγει μία τυχαία τιμή μεταξύ του 0 και του CW. Η τυχαία αυτή τιμή θα αποτελεί το backoff του συγκεκριμένου κόμβου. Η τιμή του backoff μειώνεται συνεχώς καθώς το κανάλι είναι ελεύθερο. Η μείωση αυτή «παγώνει» όταν το κανάλι είναι απασχολημένο. Όταν το backoff μηδενιστεί τότε ο συγκεκριμένος κόμβος έχει το δικαίωμα να μεταδώσει την πληροφορία του. Συγκεκριμένα, ο αποστολέα αρχικά στέλνει ένα RTS (Request To Send) πακέτο στον παραλήπτη της πληροφορίας. Ο παραλήπτης του στέλνει ένα CTS (Clear To Send) πακέτο και στη συνέχεια γίνεται η μετάδοση της πληροφορίας. Οι υπόλοιποι κόμβοι που θα ακούσουν τα RTS/CTS πακέτα αναγκάζονται να σιωπήσουν για το χρονικό διάστημα της μετάδοσης θέτοντας κατάλληλη τιμή στο NAV (Network Allocation Vector) τους. Τέλος εφόσον ο παραλήπτης λάβει την πληροφορία απαντάει με ένα πακέτο επιβεβαίωσης ACK (Acknowledgement) στον

αποστολέα. Αν η μετάδοση ολοκληρώθηκε με επιτυχία ο αρχικός κόμβος θέτει την τιμή του CW στην ελάχιστή του τιμή. Σε περίπτωση μη επιτυχούς μετάδοσης ο αποστολέας είναι αναγκασμένος να διπλασιάσει την τιμή του CW. Μεταξύ των μεταδόσεων των πακέτων διατηρούνται κάποια διαστήματα που καθορίζονται από τον μηχανισμό. Στο σχήμα 2 φαίνεται η διαδικασία που περιγράφηκε παραπάνω.



Σχήμα 2: Περιγραφή του μηχανισμού ελέγχου πρόσβασης στο μέσο.

Ο κόμβος Α ανταγωνίζεται τον κόμβο C ώστε να αποκτήσει πρόσβαση στο κανάλι και να μεταδώσει. Τελικά μεταδίδει ο Α, λόγω του ότι έχει επιλέξει μικρότερο backoff από αυτό του κόμβου C (Πλαίσιο με το κόκκινο χώμα).

1.2.2 Δρομολόγηση

Η διαδικασία της δρομολόγησης στα ασύρματα αδόμητα δίκτυα είναι αρκετά διαφορετική από τις παραδοσιακές τεχνικές δρομολόγησης στα ενσύρματα δίκτυα. Αυτό συμβαίνει αφενός γιατί δεν υπάρχει κάποια σταθερή υποδομή δικτύου, η τοπολογία αλλάζει συνεχώς λόγω της κινητικότητας των κόμβων και το ασύρματο μέσο έχει αρκετές ιδιαιτερότητες όσον αφορά το εύρος ζώνης και την αξιοπιστία της επικοινωνίας. Έχουν προταθεί αρκετά πρωτόκολλα δρομολόγησης για τα αδόμητα δίκτυα κατά καιρούς. Τα πρωτόκολλα αυτά μπορούν να κατηγοριοποιηθούν σε πολλές κατηγορίες με βάση τα χαρακτηριστικά τους και τον τρόπο λειτουργίας τους. Δεν θα προχωρήσουμε σε ανάλυση των κατηγοριών αυτών μιας και δεν είναι αυτοσκοπός της συγκεκριμένης διατριβής. Μετά από εμπειρία αρκετών χρόνων, εντατικής μελέτης και αξιολόγησης των πρωτοκόλλων αυτών θα λέγαμε ότι επικρατούν τα «κατά απαίτηση» πρωτόκολλα δρομολόγησης (On-demand routing protocols). Η αρχή λειτουργίας των πρωτοκόλλων

αυτών είναι η εξής: Εκτελούν μια διαδικασία εύρεσης διαδρομής δρομολόγησης μόνο όταν τους το ζητηθεί από κάποιο κόμβο, ο οποίος έχει κάποια πληροφορία να μεταδώσει.

Ένα από τα πιο γνωστά πρωτόκολλα δρομολόγησης που ακολουθούν την πιο πάνω αρχή είναι το DSR (Dynamic Source Routing Protocol), [50]. Στα πλαίσια της λειτουργίας του DSR, όταν κάποιος κόμβος έχει κάποια πληροφορία προς μετάδοση εγκαθίσταται μια διαδικασία αποστολής πακέτων αίτησης εύρεσης διαδρομής (routing requests). Τα πακέτα αυτά πλημμυρίζουν το δίκτυο. Κάθε κόμβος που λαμβάνει ένα τέτοιο πακέτο το επανεκπέμπει στους γειτονικούς του κόμβους, αν δεν είναι ο ίδιος ο προορισμός της πληροφορίας. Όταν ο προορισμός του route request λάβει κάποιο πακέτο (route request) χρησιμοποιεί την αντίστροφη διαδρομή για να απαντήσει στον αποστολέα με ένα πακέτο route reply το οποίο περιέχει όλη την πληροφορία της διαδρομής. Ο αποστολέας μόλις λάβει το route reply πακέτο διαβάζει την πληροφορία όσον αφορά την διαδρομή δρομολόγησης και χρησιμοποιεί τη διαδρομή αυτή για τη μετάδοση.

Ένα ακόμη πολύ γνωστό πρωτόκολλο δρομολόγησης το οποίο έχει αρκετές ομοιότητες με το DSR είναι το AODV (Ad Hoc On-Demand Distance Vector Routing Protocol), [51]. Στα πλαίσια λειτουργίας του AODV ο κόμβος που στέλνει κάποιο πακέτο και οι ενδιάμεσοι κόμβοι αποθηκεύουν πληροφορία σχετικά με το επόμενο κόμβο που θα συμπληρώσει τη διαδρομή προς τον προορισμό. Ακολουθείται η διαδικασία route request που περιγράψαμε πριν στο DSR. Η διαφορά που υπάρχει στο AODV είναι ότι το πρωτόκολλο χρησιμοποιεί σειριακούς αριθμούς προορισμού (DestSeqNum – Destination Sequence Numbers) για να καθοριστεί κατά πόσο ένα μονοπάτι προς τον προορισμό είναι πρόσφατο ή όχι. Ένας κόμβος ανανεώνει την πληροφορία που διαθέτει για ένα μονοπάτι μόνο αν ο σειριακός αριθμός του συγκεκριμένου πακέτου που έλαβε είναι μεγαλύτερος από τον σειριακό αριθμό που έχει ήδη αποθηκευμένο.

Κεφάλαιο 2

Ασφάλεια Ασύρματων Αδόμητων Δικτύων

Η Ασφάλεια των ασύρματων αδόμητων δικτύων είναι πολύ σημαντικό ζήτημα, ειδικά σε εφαρμογές όπου απαιτείται ένα ασφαλές δικτυακό περιβάλλον (π.χ. στρατιωτικές εφαρμογές). Δυστυχώς η παροχή ασφάλειας σε αδόμητα δίκτυα με καθαρά κατανεμημένη αρχιτεκτονική είναι πολύ δύσκολη. Επιθέσεις που προσπαθούν να πλήξουν την ασφάλεια του συστήματός μπορούν να αναπτυχθούν σε όλα τα επίπεδα της στοίβας των πρωτοκόλλων. Αυτή τη στιγμή υπάρχουν αρκετές ερευνητικές προσπάθειες που αποσκοπούν στην ενίσχυση της ασφάλειας των αδόμητων δικτύων σε όλο το εύρος των λειτουργιών τους. Στη βιβλιογραφία υπάρχουν αρκετές προσεγγίσεις που προσφέρουν όχι τόσο επαρκή προστασία από επιθέσεις. Η μελέτη που θα ακολουθήσει στην παρούσα διατριβή διέπεται από την αρχή ότι για την επίτευξη της αξιόπιστης προστασίας των αδόμητων δικτύων πρέπει να υιοθετηθούν νέες τεχνικές διαφορετικές από αυτές που εφαρμόζονται στα ενσύρματα δίκτυα. Οι τεχνικές αυτές ίσως προκύψουν βλέποντας το συγκεκριμένο πρόβλημα από μια άλλη οπτική γωνία και προτείνοντας νέες πρωτοποριακές λύσεις.

2.1 Ανασκόπηση των παραδοσιακών απαιτήσεων ασφάλειας

Ένα πρωτόκολλο που παρέχει ασφάλεια σε κάποιο σύστημα επικοινωνιών πρέπει «παραδοσιακά» να ικανοποιεί κάποιες βασικές απαιτήσεις:

1. **Αυθεντικοποίηση**: Η αυθεντικοποίηση είναι πάρα πολύ σημαντική σε ένα πληροφοριακό σύστημα. Πόσο μάλλον σε ένα δικτυακό σύστημα όπου υπάρχουν πολλές ξεχωριστές οντότητες των οποίων οι ταυτότητες δεν είναι γνωστές. Με τη διαδικασία της αυθεντικοποίησης ελέγχεται η ταυτότητα ενός χρήστη και εφόσον η ταυτότητα αυτή είναι αυθεντική. Στα αδόμητα δίκτυα δεν υπάρχει κάποια γενική αρχή που να χειρίζεται τις ταυτότητες των χρηστών. Για τον λόγο αυτό απαιτείται κάποια κατανεμημένη διαδικασία αυθεντικοποίησης.
2. **Εμπιστευτικότητα**: Αφορά κυρίως το περιεχόμενο των πακέτων που στέλνονται στο δίκτυο. Η πληροφορία που στέλνεται πρέπει να αποκαλύπτεται μόνο στον παραλήπτη της. Στον συγκεκριμένο τομέα ίσως έχουμε τις περισσότερες επιθέσεις. Κάποιος ενδιάμεσος κόμβος είτε κάποιος εισβολέας «κρατάει» τα πακέτα που λαμβάνει και αντί να τα προωθήσει διαβάζει την πληροφορία που περιέχουν. Ειδικά στα ασύρματα δίκτυα το πρόβλημα εντείνεται καθώς το ασύρματο μέσο δίνει πολύ εύκολα τη δυνατότητα σε κάποιο μη εξουσιοδοτημένο χρήστη, να κρυφακούσει. Επίσης η διαχείριση των κλειδιών των χρηστών είναι πολύ δύσκολη. Οι πιο γνωστές τεχνικές που προσπαθούν να υπερνικήσουν τέτοιες κακόβουλες συμπεριφορές είναι τεχνικές κρυπτογράφησης.
3. **Ακεραιότητα**: Αναφερόμαστε κι εδώ στην πληροφορία που μεταδίδεται στο δίκτυο. Φυσικά μας ενδιαφέρει απολύτως η ακεραιότητα της. Τα πακέτα που στέλνονται από κάποιο κόμβο θα πρέπει να φθάνουν στον προορισμό τους χωρίς να έχουν υποστεί παραποίηση της πληροφορίας που μεταφέρουν, σε κάποιο σημείο του δικτύου.
4. **Διαθεσιμότητα**: Όπως και σε κάθε πληροφορικό σύστημα όπου υπάρχουν πολλοί χρήστες οι οποίοι απολαμβάνουν μια πληθώρα υπηρεσιών, έτσι και στα αδόμητα δίκτυα η διαθεσιμότητα του δικτύου πρέπει να παραμένει σε υψηλά επίπεδα. Τα σφάλματα στις ασύρματες ζεύξεις αλλά και διάφορες μορφές επιθέσεων (DoS attacks) επιδεινώνουν την διαθεσιμότητα του δικτύου.
5. **Έλεγχος Πρόσβασης**: Οι χρήστες του δικτύου έχουν πρόσβαση στους πόρους του δικτύου, σε υπηρεσίες και σε δεδομένα σύμφωνα με τα δικαιώματα που τους έχουν παραχωρηθεί από το δίκτυο.

6. **Μη-Απάρνηση**: Με το συγκεκριμένο μηχανισμό ένας χρήστης δεν μπορεί να απαρνηθεί ότι δεν έχει στείλει ένα μήνυμα και ένας παραλήπτης δεν μπορεί να αρνηθεί ότι έλαβε ένα μήνυμα. Οι ψηφιακές υπογραφές βοηθάνε πολύ τον μηχανισμό της μη-απάρνησης.

2.2 Εδικά χαρακτηριστικά και ευπάθειες των αδόμητων δικτύων

Τα χαρακτηριστικά των αδόμητων δικτύων κάνουν την παροχή ασφάλειας πολύ δύσκολη υπόθεση. Όλα ξεκινούν από το ασύρματο μέσο και τις ιδιότητές του. Οι ασύρματες ζεύξεις είναι ευπαθείς σε παρεμβολές και διευκολύνουν τους κακόβουλους κόμβους στο να κρυφακούν τα δεδομένα που μεταδίδονται. Το ασύρματο κανάλι που χρησιμοποιείται διαμοιράζεται μεταξύ των κόμβων το δικτύου. Ένας κόμβος φθάνει να βρίσκεται εντός της περιοχής εκπομπής των άλλων κόμβων για να ακούσει την πληροφορία που μεταδίδουν. Στη λειτουργία των αδόμητων δικτύων υπάρχουν κάποιοι περιορισμοί όσον αφορά το εύρος ζώνης, την υπολογιστική ισχύ και την ισχύ εκπομπής. Ο πρώτος περιορισμός οφείλεται στη φύση του ασύρματου καναλιού, ο δεύτερος οφείλεται στις περιορισμένες υπολογιστικές δυνατότητες των ασύρματων συσκευών και ο τρίτος στην περιορισμένη τροφοδότηση του δικτύου με ισχύ. Οι τρεις πιο πάνω περιορισμοί πρέπει να ληφθούν σοβαρά υπόψη στον σχεδιασμό ενός συστήματος παροχής ασφάλειας. Στα αδόμητα δίκτυα δεν υπάρχει κάποια κεντρική αρχή (authority) που να ελέγχει τις λειτουργίες του δικτύου αλλά και τη συμπεριφορά των κόμβων που το αποτελούν (σε αντίθεση με τα ενσύρματα και τα δομημένα ασύρματα δίκτυα). Ωστόσο, μηχανισμοί που βασίζονται σε μία κεντρική αρχή (όπως μηχανισμοί διαμοιρασμού κλειδιών) δεν μπορούν να εφαρμοστούν στα αδόμητα δίκτυα. Επιπλέον στα αδόμητα δίκτυα δεν υπάρχει εξ αρχής, μια συσχέτιση μεταξύ των χρηστών. Επίσης δεν υπάρχει κάποια σχέση εμπιστοσύνης μεταξύ τους. Αυτό οφείλεται στην δυναμικότητα των δικτύων αυτών και στην αυξημένη κινητικότητα των κόμβων. Οι συσκευές που αποτελούν μέρος των αδόμητων δικτύων είναι τις περισσότερες φορές συμπαγείς και φορητές (Laptops, PDAs). Μπορούν έτσι πολύ εύκολα να διαρρηχθούν και κάποιος μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση στο δίκτυο (φυσική ασφάλεια).

2.3 Προβλήματα Ασφάλειας

Σε αυτή την υποενότητα θα μελετηθούν κάποιες επιθέσεις που εκμεταλλεύονται τις ευπάθειες των αδόμητων δικτύων και πλήττουν την ασφάλεια των συστημάτων. Θα κάνουμε λόγο για τις επιθέσεις που λαμβάνουν χώρα σε όλα τα επίπεδα του δικτύου αλλά θα δοθεί έμφαση σε επιθέσεις που δρουν στο επίπεδο ελέγχου πρόσβασης μέσου και στο επίπεδο δρομολόγησης. Επίσης κάποιες επιθέσεις μπορούν να λάβουν χώρα σε διαφορετικά επίπεδα είτε να επεκταθούν από το ένα επίπεδο στο άλλο. Η καταπολέμηση των επιθέσεων αυτών είναι πολύ δύσκολη. Αυτό γιατί αφενός χρειάζονται νέοι πιο πρωτοποριακοί μηχανισμοί που να λειτουργούν σε διαφορετικά επίπεδα και αφετέρου για την υλοποίηση των μηχανισμών αυτών πολλές φορές είναι απαραίτητη η τροποποίηση της λειτουργίας των διαφόρων επιπέδων. Κάνοντας μια προσπάθεια να κατηγοριοποιήσουμε τις επιθέσεις μπορούμε να πούμε πως διαχωρίζονται σε παθητικές και σε ενεργητικές επιθέσεις. Οι παθητικές (passive) επιθέσεις δεν επηρεάζουν τη λειτουργία του δικτύου αλλά αποσκοπούν στο να αποκτήσουν πρόσβαση στην πληροφορία που μεταδίδεται. Αντίθετα οι ενεργητικές (active) επιθέσεις δρουν ενάντια της σωστής λειτουργίας του δικτύου. Εκμεταλλεύονται όλα τα χαρακτηριστικά και τις λειτουργίες του δικτύου και με έξυπνες τακτικές δημιουργούν μία πτώση στην απόδοσή του. Παρακάτω θα περιγράψουμε κάποιες ενεργητικές επιθέσεις που συμβαίνουν σε όλα τα επίπεδα του δικτύου.

2.3.1 Προβλήματα ασφάλειας στο φυσικό επίπεδο (Physical Layer)

Στο φυσικό επίπεδο ένας κακόβουλος κόμβος μπορεί να αυξήσει την ισχύς εκπομπής του δημιουργώντας πολύ άσχημα αποτελέσματα στην ομαλή λειτουργία του δικτύου. Τα αποτελέσματα μιας τέτοιας συμπεριφοράς είναι τα παρακάτω:

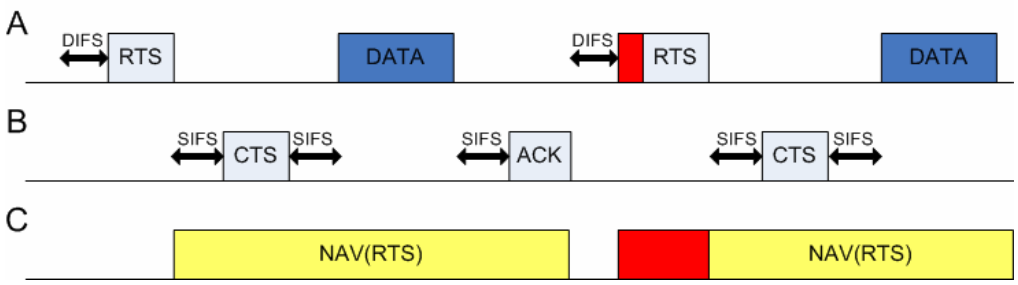
1. Υψηλός βαθμός παρεμβολών στην επικοινωνία των κόμβων.
2. Η συνολική ισχύς του συστήματος μειώνεται δραστικά καθώς ο χρόνος λειτουργίας περνά (για ειδικές εφαρμογές όπου παίζει σημαντικό ρόλο η συνολική ισχύς του συστήματος, π.χ. δίκτυα αισθητήρων).
3. Προβλήματα σωστού διαμοιρασμού του καναλιού και κατανομής των πόρων του δικτύου.

Επίσης κάποιοι κόμβοι θέλοντας να αποφύγουν την επικοινωνία με κάποιους άλλους κόμβους, να αποθηκεύσουν ενέργεια είτε να αποφύγουν να λειτουργήσουν προς όφελος των άλλων (π.χ. προώθηση πακέτων) μειώνουν κατά πολύ την ισχύ εκπομπής τους με αποτέλεσμα να μην μπορούν να επικοινωνήσουν με τους υπόλοιπους κόμβους και να αποφεύγουν την συνεργασία μαζί τους.

2.3.2 Προβλήματα ασφάλειας στο επίπεδο ελέγχου πρόσβασης στο μέσο (MAC Layer)

Στο επίπεδο έλεγχου πρόσβασης στο μέσο του δικτύου παρατηρούνται κάποιες τεχνικές που βοηθούν τους κακόβουλους χρήστες να αποκτήσουν γρηγορότερα πρόσβαση στο μέσο. Προφανώς αυτό έχει κάποιο άμεσο αντίκτυπο στο διαμοιρασμό του καναλιού για τους υπόλοιπους κόμβους. Έτσι λοιπόν, η «αμεροληψία» (fairness) όσον αφορά την πρόσβαση στο μέσο χάνεται. Παρακάτω θα δούμε κάποιες από αυτές τις τεχνικές οι οποίες εκμεταλλεύονται κυρίως τα τεχνικά χαρακτηριστικά του DCF.

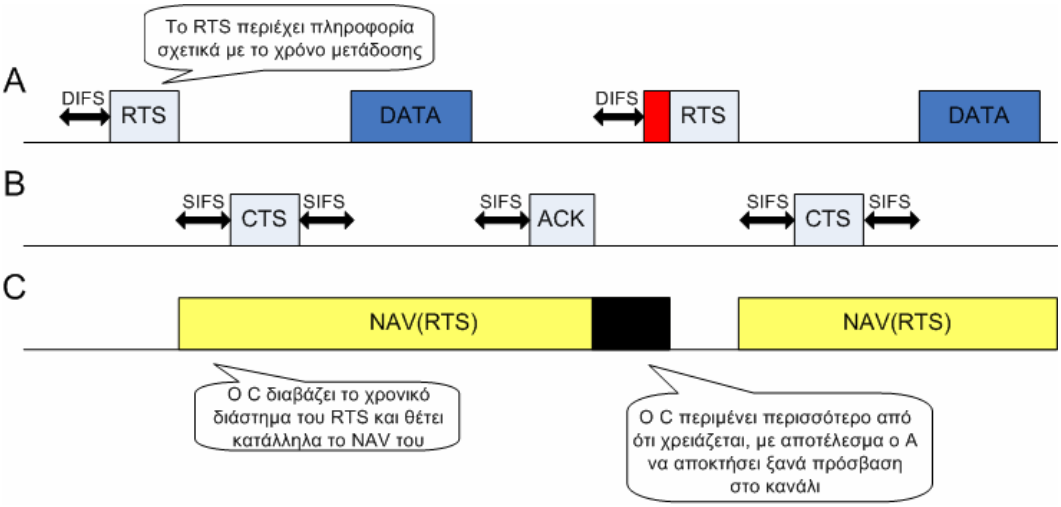
Ο DCF δεν έχει σχεδιαστεί ώστε να παρέχει κάποια ενσωματωμένη (embedded) προστασία ασφάλειας από επιθέσεις τέτοιου είδους. Αποτέλεσμα αυτής της σχεδιαστικής παράληψης είναι το γεγονός ότι η διαδικασία ελέγχου πρόσβασης στα αδόμητα δίκτυα πέφτει πολύ συχνά θύμα επιθέσεων, η τεχνική των οποίων είναι πάρα πολύ απλή. Μία κακόβουλη τεχνική που εκμεταλλεύεται τον μηχανισμό του backoff έχει πολύ καλά αποτελέσματα, μιας και όπως προβλέπει το πρότυπο το backoff επιλέγεται τυχαία από τον χρήστη που θέλει να μεταδώσει την πληροφορία. Ένας κακόβουλος χρήστης επιλέγει συνεχώς μικρότερα διαστήματα backoff (έξω από τα όρια που ορίζει ο DCF). Με αυτό τον τρόπο ο συγκεκριμένος χρήστης αποκτάει πρόσβαση στο μέσο πολύ γρήγορα καθιστώντας την πρόσβαση των άλλων χρηστών (που λειτουργούν σύμφωνα με τον DCF) αδύνατη. Στο σχήμα 3 φαίνεται ένα παράδειγμα της ευπάθειας του μηχανισμού του backoff. Ο χρήστης A ανταγωνίζεται με τον χρήστη C να μεταδώσουν στον B. Ο A παρουσιάζει μια άσχημη συμπεριφορά (misbehavior) και επιλέγοντας μικρά backoff αναγκάζει τον C να σιωπά συνεχώς.



Σχήμα 3: Ένα παράδειγμα κακόβουλης συμπεριφοράς στον μηχανισμό του backoff.

Μία άλλη, εξίσου επιτυχημένη τεχνική, εκμεταλλεύεται τη λειτουργία του NAV. Όπως γνωρίζουμε, όταν κάποιος κόμβος λάβει πρόσβαση στο κανάλι και έχει κάποια πληροφορία να μεταδώσει στέλνει αρχικά ένα πακέτο RTS στον παραλήπτη. Το πακέτο αυτό περιέχει πληροφορία σχετικά με το χρονικό διάστημα της μετάδοσης. Οι ανταγωνιστικοί κόμβοι διαβάζουν την πληροφορία αυτή και θέτουν κατάλληλα το NAV τους ώστε μετά την μετάδοση να έχουν τη δυνατότητα να μεταδώσουν κι εκείνοι. Εδώ εντοπίζεται άλλη μια αδυναμία του πρωτοκόλλου μιας και δεν ελέγχεται η εγκυρότητα της πληροφορίας που περιέχει το RTS. Για παράδειγμα ένας κακόβουλος χρήστης ενσωματώνει στο RTS που στέλνει μεγαλύτερη χρονική διάρκεια από αυτή που χρειάζεται πραγματικά για να μεταδώσει ένα πακέτο. Με αυτό τον τρόπο αναγκάζει τους υπόλοιπους ανταγωνιστικούς κόμβους να σιωπούν ακόμη και όταν η μετάδοση ολοκληρωθεί. Και φυσικά είναι ελεύθερος να ξαναμεταδόσει χωρίς την ύπαρξη ανταγωνισμού. Στο σχήμα 4 φαίνεται όλη η παραπάνω διαδικασία.

Μία τελευταία τεχνική διατάραξης της «αμεροληψίας» του DCF είναι η μη τήρηση των μεσοδιαστημάτων (SIFS/DIFS). Τα διαστήματα αυτά παρεμβάλλονται μεταξύ των μεταδόσεων των πακέτων για να αποφεύγονται οι πιθανές συγκρούσεις και να διασφαλίζεται ότι το κάθε πακέτο φθάνει στον προορισμό του. Ένας χρήστης λοιπόν που αποσκοπεί να παρακάμψει τον ανταγωνισμό των υπόλοιπων κόμβων στο να λάβουν πρόσβαση στο κανάλι μεταδίδει πριν συμπληρωθεί το χρονικό διάστημα DIFS. Με αυτόν τον μη νόμιμο τρόπο αποκτά πρόσβαση στο κανάλι πριν από τους υπόλοιπους κόμβους. Οι ανταγωνιστικοί κόμβοι το αντιλαμβάνονται αλλά στα πλαίσια της λειτουργία του DCF είναι ανήμποροι να αντιδράσουν.



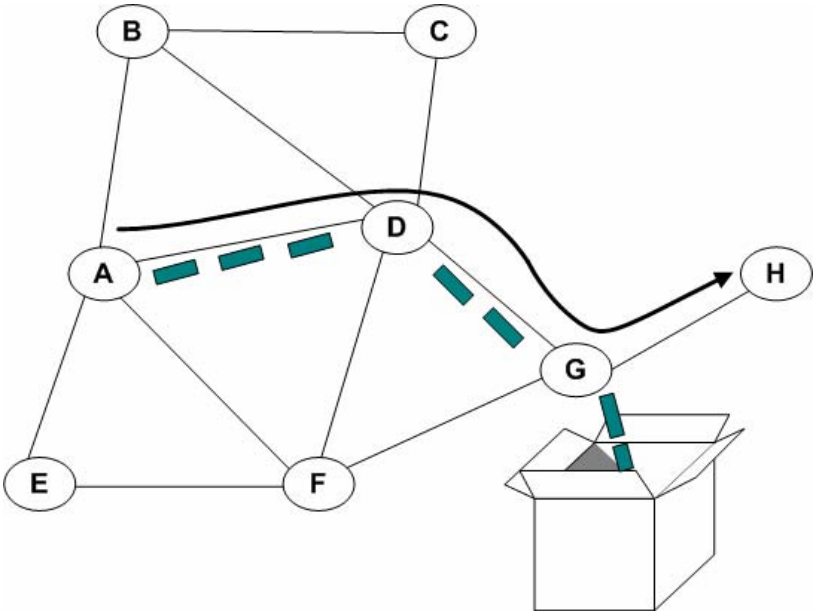
Σχήμα 4: Ένα παράδειγμα κακόβουλης συμπεριφοράς στον μηχανισμό του NAV.

2.3.3 Προβλήματα ασφάλειας στο επίπεδο δρομολόγησης (Routing Layer)

Στο επίπεδο δρομολόγησης έχει καταγραφεί μία πληθώρα επιθέσεων. Αρκετές από αυτές προσπαθούν να παρεμποδίσουν τη διαδικασία της δρομολόγησης πλήττοντας τη σωστή λειτουργία των πρωτοκόλλων δρομολόγησης. Παρακάτω αναλύονται οι πιο αντιπροσωπευτικές επιθέσεις σε αυτόν τον τομέα:

1. **Επιθέσεις άρνησης εξυπηρέτησης (DoS)**: Αυτό το είδος των επιθέσεων αποσκοπεί στην κατάρρευση της σωστής παροχής υπηρεσιών του δικτύου. Στο επίπεδο δρομολόγησης ένας εχθρικός κόμβος μπορεί να λάβει μέρος σε μία διαδικασία δρομολόγησης και αντί να συνεργαστεί, ώστε να επιτευχθεί η δρομολόγηση κάποιας πληροφορίας, με τη συμπεριφορά του καθιστά αδύνατη τη δρομολόγηση. Για παράδειγμα μπορεί να απορρίπτει τα πακέτα που λαμβάνει χωρίς να τα προωθεί, με αποτέλεσμα η ποιότητα παροχής υπηρεσιών (εδώ δρομολόγηση) να μειώνεται δραστικά. Στο παράδειγμα του σχήματος 5 ο κόμβος G δεν συνεργάζεται ώστε να ολοκληρωθεί η δρομολόγηση των πακέτων από τον A στον H. Δεν προωθεί τα πακέτα που λαμβάνει αλλά τα πετάει. Επίσης μπορεί να πλημμυρίσει το δίκτυο με άχρηστα πακέτα που δεν έχουν άλλο σκοπό από το να παρεμποδίσουν τη σωστή εκτέλεση των βασικών λειτουργιών του. Στόχος ενός κακόβουλου χρήστη μπορεί να είναι ένας συγκεκριμένος κόμβος. Στέλνοντάς του λοιπόν ένα μεγάλο αριθμό πακέτων σε τακτά χρονικά διαστήματα επηρεάζει τη

λειτουργία του. Πιο άσχημα αποτελέσματα προκαλούν οι κατανεμημένες επιθέσεις (Distributed Denial of Service Attacks) όπου πολλοί κόμβοι συνωμοτούν εναντίων κάποιων άλλων και ξεκινούν την επίθεση τους.



Σχήμα 5: Παράδειγμα κακόβουλης συμπεριφοράς στη διαδικασία της δρομολόγησης.

2. **Πλημμύρισμα των πινάκων δρομολόγησης**: Σε κάποια πρωτόκολλα δρομολόγησης οι κόμβοι διατηρούν πίνακες δρομολόγησης που περιέχουν πληροφορίες σχετικά με τα μονοπάτια και τους κόμβους που τα αποτελούν. Οι πίνακες αυτοί ανανεώνονται για κάθε νέα αίτηση έναρξης δρομολόγησης κάποιου πακέτου. Κάποιοι κόμβοι θέλοντας να γεμίσουν τους πίνακες δρομολόγησης των άλλων κόμβων στέλνουν συνεχώς αιτήματα δρομολόγησης (route requests). Πολλές φορές οι παραλήπτες της πληροφορίας, στους οποίους ισχυρίζονται πως θέλουν να στείλουν κάποια δεδομένα, δεν υπάρχουν καν.
3. **Ανταπαντήσεις για τη λήψη πακέτων**: Σύμφωνα με τα περισσότερα πρωτόκολλα δρομολόγησης όταν ένας κόμβος λάβει ένα πακέτο πρέπει να απαντήσει με μία επιβεβαίωση. Κάποιος κόμβος που αποσκοπεί στην υπερφόρτωση της επικοινωνίας του δικτύου και στην εξάλειψη της ενέργειας των άλλων κόμβων στέλνει συνεχώς τέτοιες απαντήσεις. Δημιουργείται έτσι μία σύγχυση στη δρομολόγηση των πακέτων.

Κάποιες γενικότερες επιθέσεις που αφορούν λιγότερο ή περισσότερο τη δρομολόγηση των πακέτων αλλά συμβαίνουν πάντα στο επίπεδο δρομολόγησης αναλύονται πιο κάτω:

1. **Επίθεση Wormhole**: Στα πλαίσια της συγκεκριμένης επίθεσης, ένας κόμβος λαμβάνει κάποια πακέτα και στη συνέχεια προσπαθεί να τα στείλει σε έναν άλλο κόμβο δημιουργώντας ένα «τούνελ». Αν ο αρχικός κόμβος που δημιουργεί το «τούνελ» κατέχει θέση καθοριστικής σημασίας για το δίκτυο (θέση από όπου περνάει αρκετή πληροφορία) τότε μπορούν να προκληθούν σοβαρά προβλήματα απώλειας πακέτων.
2. **Βυζαντινές επιθέσεις**: Κάποιοι ενδιάμεσοι κόμβοι δημιουργούν πακέτα που δρομολογούνται από μη αξιόπιστα μονοπάτια, βρόγχους δρομολόγησης και επιλεκτικά πετάνε κάποια πακέτα που λαμβάνουν. Οι κόμβοι αυτοί μπορούν να συνωμοτούν μεταξύ τους. Οι επιθέσεις αυτές είναι πολύ δύσκολο να ανιχνευθούν.
3. **Επιθέσεις Blackhole**: Κατά τη διαδικασία δρομολόγησης ενός πακέτου προς έναν προορισμό, κάποιος κακόβουλος κόμβος δημοσιοποιεί λανθασμένα μονοπάτια προς τον συγκεκριμένο προορισμό. Απώτερος σκοπός είναι η παρεμπόδιση της σωστής λειτουργίας εύρεσης βέλτιστου μονοπατιού και έτσι τα πακέτα δεν φθάνουν ποτέ στον προορισμό τους.
4. **Επίθεση κατανάλωσης πόρων του δικτύου**: Οι χρήστες που χρησιμοποιούν τη συγκεκριμένη τεχνική καταναλώνουν τους πόρους των άλλων χρηστών του δικτύου. Αυτοί οι πόροι μπορεί να είναι: εύρος φάσματος, ενέργεια, υπολογιστική ισχύς.

2.3.4 Προβλήματα ασφάλειας στο επίπεδο μεταφοράς (Transport Layer)

Στο επίπεδο μεταφοράς δεν έχουν παρατηρηθεί σοβαρές επιθέσεις και έτσι οι ερευνητικές προσπάθειες στον τομέα αυτόν έχουν κατευθυνθεί προς άλλες κατευθύνσεις (όπως τη βελτίωση της απόδοσης του TCP στα ασύρματα δίκτυα). Οι μόνες επιθέσεις που έχουν καταγραφεί αφορούν τα sessions που δημιουργούνται μεταξύ των κόμβων. Κάποιος κακόβουλος χρήστης μεταμφιέζεται σε έναν τελικό κόμβο ενός session. Με αυτόν τον τρόπο παίρνει στα χέρια του τον έλεγχο του session.

2.3.5 Προβλήματα ασφάλειας στο επίπεδο των εφαρμογών (Application Layer)

Στο επίπεδο των εφαρμογών δεν υπάρχει μεγάλο ενδιαφέρον για την ασφάλεια των εφαρμογών. Αυτό οφείλεται στο γεγονός ότι όλη η έρευνα κατευθύνεται προς την ανάπτυξη κάποιων εφαρμογών που θα λειτουργούν αποδοτικά επάνω στα αδόμητα δίκτυα. Ίσως θα μπορούσαμε να αναφερθούμε στη λογική της μη-απάρνησης που σχετίζεται με τις εφαρμογές. Όπως αναφέρθηκε και πιο πάνω, αν ένας χρήστης έχει συμμετάσχει σε κάποια επικοινωνία δεν μπορεί να το αρνηθεί.

2.4 Απαιτήσεις ασφάλειας των αδόμητων δικτύων

Έκτός από τις παραδοσιακές απαιτήσεις ασφάλειας, στα αδόμητα δίκτυα πρέπει να τονιστούν και κάποιες άλλες προκλήσεις που προκύπτουν λόγω των ιδιαίτερων χαρακτηριστικών τους:

1. Ένα πολύ σημαντικό ζήτημα είναι η ενίσχυση των μηχανισμών ελέγχου πρόσβασης στο μέσο του δικτύου. Όπως είδαμε ο DCF είναι ανήμπορος να αντιμετωπίσει διάφορες επιθέσεις. Η ενδυνάμωση του DCF πρέπει να γίνει υπό τις αρχές του δίκαιου διαμοιρασμού του καναλιού, της δίκαιης κατανομής των πόρων και τέλος του γρήγορου και αποδοτικού εντοπισμού των κακόβουλων κόμβων. Η κατανεμημένη φύση των αδόμητων δικτύων δυσχεραίνει τα πράγματα και ιδίως όταν υπάρχουν πολλοί κακόβουλοι κόμβοι που συνωμοτούν για ένα κοινό στόχο. Το IEEE 802.11 είναι ένα πρότυπο που έχει επικρατήσει και πολλές δικτυακές συσκευές το υποστηρίζουν. Οπότε τροποποιώντας τον MAC μηχανισμό του, δεν λύνουμε το πρόβλημα της ασφάλειας καθώς οι συσκευές (π.χ. δικτυακές κάρτες) που έχουν ήδη κατασκευαστεί δεν θα μπορέσουν να υποστούν τις κατάλληλες τροποποιήσεις. Αυτό που μπορεί να γίνει είναι η ανάπτυξη καινοτόμων μηχανισμών που θα μπορούν να ενισχύσουν την υπάρχουσα λειτουργία του MAC χωρίς να την τροποποιούν.
2. Όπως έγινε σαφές και πιο πάνω στα αδόμητα δίκτυα είναι απαραίτητοι κάποιοι μηχανισμοί που να προσδίδουν ασφάλεια στη διαδικασία της δρομολόγησης. Είδαμε την πληθώρα των επιθέσεων που προσπαθούν να πλήξουν τη δρομολόγηση των πακέτων μέσα στο δίκτυο. Οι μηχανισμοί αυτοί πρέπει να εγγυώνται πως η εύρεση ενός μονοπατιού για τη μετάδοση ενός πακέτου από την πηγή στον προορισμό του δεν θα παρενοχλείται από άλλες οντότητες. Οι

«πλαστές» αιτήσεις για δρομολόγηση, οι οποίες αρχικοποιούνται για διάφορους λόγους, δεν πρέπει να ενσωματώνονται στη λειτουργία της δρομολόγησης του δικτύου. Οι βρόγχοι δρομολόγησης πρέπει να εντοπίζονται και να αποφεύγονται. Η κατεύθυνση των διαδρομών που ακολουθούν τα πακέτα προς τον προορισμό τους δεν πρέπει να αλλάζει από ενδιάμεσους κακόβουλους κόμβους. Τα πακέτα δρομολόγησης πρέπει να διατηρούν την ακεραιότητα τους και δεν πρέπει να τροποποιούνται από τους εξουσιοδοτημένους κόμβους που συμμετέχουν στη δρομολόγηση.

3. Για την επίτευξη της ασφαλούς δρομολόγησης ένα απαραίτητο συστατικό είναι η σωστή διαχείριση των κλειδιών των χρηστών. Η διαχείριση των κλειδιών πρέπει να είναι κατανεμημένη και να υποστηρίζεται από υψηλή διαθεσιμότητα. Τα πράγματα είναι αρκετά δύσκολα μιας και στα αδόμητα δίκτυα δεν υπάρχει κάποια κεντρική αρχή που να αναλάβει τον διαμοιρασμό των κλειδιών στους χρήστες. Επίσης δεν υπάρχει κάποια υποδομή πάνω από την οποία η διαχείριση των κλειδιών θα γινόταν με ασφαλή τρόπο. Εφόσον η διαχείριση των κλειδιών επέλθει σε επιθυμητά επίπεδα λειτουργίας προχωράμε στην κρυπτογράφηση των πακέτων που μεταδίδονται στο δίκτυο. Πρέπει να ληφθεί υπόψη η χαμηλή υπολογιστική ισχύς των κόμβων, η χαμηλή ενέργεια που διαθέτουν για τις λειτουργίες τους αλλά και η αυξημένη κυκλοφορία που προκύπτει από το διαμοιρασμό των κλειδιών. Σύμφωνα με τους πιο πάνω περιορισμούς μπορούν να αναπτυχθούν αποδοτικές τεχνικές διαχείρισης κλειδιών αλλά και τεχνικές κρυπτογράφησης.
4. Βασική προϋπόθεση της σωστής λειτουργίας των αδόμητων δικτύων είναι η επίτευξη της συνεργασίας μεταξύ των κόμβων (Cooperation). Στη συνεργασία αυτή δεν πρέπει να συμμετέχουν κακόβουλοι κόμβοι. Επίσης, επειδή πολλές φορές οι κόμβοι είναι αναγκασμένοι για διατελέσουν κάποιες λειτουργίες (όπως προώθηση πακέτων) προς όφελος των άλλων κόμβων πρέπει να τους δίνονται τα κατάλληλα κίνητρα. Πρέπει να δημιουργηθούν κάποιοι μηχανισμοί που να ενισχύουν τη συνεργασία μεταξύ των κόμβων αλλά και να τιμωρούν τους κακόβουλους χρήστες. Ο σχεδιασμός τους πρέπει να είναι προσεκτικός ώστε να

μην επιβαρύνει τη λειτουργία του δικτύου (να μην σπαταλάει πολλούς πόρους του δικτύου).

Οι απαιτήσεις ασφάλειας που αναλύθηκαν πιο πάνω αποτελούν τη βάση δημιουργίας νέων-καινοτόμων μηχανισμών προστασίας. Στο επόμενο κεφάλαιο υπάρχει μία περιγραφή των πιο αντιπροσωπευτικών προσεγγίσεων που υπάρχουν αυτή τη στιγμή στη βιβλιογραφία. Οι μηχανισμοί που προτείνονται λύνουν μερικώς το πρόβλημα της ασφάλειας. Πεποίθηση της συγκεκριμένης διατριβής είναι ότι το πρόβλημα της ασφάλειας πρέπει να ερευνηθεί από μία νέα οπτική γωνία. Πρέπει να γίνει μια προσπάθεια να συνδυαστούν οι τεχνικές που προστατεύουν ξεχωριστά τις λειτουργίες κάθε επιπέδου και να προκύψουν κάποιες νέες προσεγγίσεις με μεγαλύτερο βαθμό προστασίας από επιθέσεις. Η ενοποίηση των διαφόρων επιπέδων (cross-layering) έχει δείξει πολύ καλά αποτελέσματα σε πολλούς ερευνητικούς τομείς των αδόμητων δικτύων. Στον τομέα της ασφάλειας δεν έχει γίνει αρκετή δουλειά αλλά η μελέτη που θα ακολουθήσει στη συγκεκριμένη διατριβή θα δείξει πως η ενοποίηση μπορεί να βοηθήσει στην βελτίωση της προστασίας ενός συστήματος και να παράσχει πλήρη ανθεκτικότητα σε όλα τα επίπεδα.

Κεφάλαιο 3

Βιβλιογραφική Έρευνα

Στον τομέα της ασφάλειας των ασύρματων αδόμητων δικτύων υπάρχει έντονο ερευνητικό ενδιαφέρον τα τελευταία χρόνια. Θα επικεντρωθούμε κυρίως σε μηχανισμούς που δουλεύουν στο επίπεδο ελέγχου πρόσβασης στο μέσο του δικτύου αλλά και στο επίπεδο δρομολόγησης. Για μηχανισμούς που προστατεύουν κάποιο από τα ανώτερα επίπεδα δεν θα γίνει λόγος μιας και δεν αφορούν άμεσα το αντικείμενο της συγκεκριμένης διατριβής.

3.1 Μηχανισμοί ασφάλειας στο επίπεδο ελέγχου πρόσβασης στο μέσο

Η δυσλειτουργία των κόμβων ενός δικτύου στο επίπεδο ελέγχου πρόσβασης στο μέσο, η οποία οφείλεται στη «μοχθηρία» ή την «εγωιστικότητα» τους, μπορεί να επιδράσει σημαντικά στην μείωση της απόδοσης του δικτύου. Πρόσφατες ερευνητικές προσπάθειες έχουν εξετάσει τις πιθανές δυσλειτουργίες που είναι πιθανόν να συμβούν στα ασύρματα IEEE 802.11 δίκτυα [1, 2, 3]. Στο παρόν εδάφιο θα παρουσιαστούν κάποια αντιπροσωπευτικά συστήματα που έχουν προταθεί πρόσφατα, σκοπός των οποίων είναι ο εντοπισμός και η καταπολέμηση προβλημάτων ασφάλειας στο επίπεδο ελέγχου πρόσβασης στο μέσο του δικτύου.

Είναι αντιληπτό πως ο μηχανισμός CSMA/CA, που χρησιμοποιείται στο IEEE 802.11, δεν είναι ανθεκτικός σε «εγωιστικές» συμπεριφορές των κόμβων αλλά και σε επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service attacks, DoS). Προτείνονται λοιπόν κάποιες τροποποιήσεις στο 802.11 CSMA/CA πρωτόκολλο, όσον αφορά τον

μηχανισμό backoff, για να την ισχυροποίησή του, [4]. Στη συγκεκριμένη προσέγγιση υπάρχει μια κατανεμημένη διαδικασία επιλογής της τυχαίας τιμής του backoff. Σε μία διαδικασία αποστολής και λήψης δεδομένων ο αποστολέας αλλά και ο παραλήπτης γνωρίζουν την τιμή του backoff, σε αντίθεση με τον αυθεντικό μηχανισμό του CSMA/CA. Με αυτό τον τρόπο ο παραλήπτης των δεδομένων μπορεί να παρατηρήσει τη συμπεριφορά του αποστολέα και μπορεί να εντοπίσει κάποια πιθανή δυσλειτουργία. Επίσης προτείνονται και κάποιοι αλγόριθμοι που λειτουργούν προς την κατεύθυνση του εντοπισμού κάποιας πιθανής παραπλάνησης στον μηχανισμό του backoff από ένα σύνολο από κόμβους που συνωμοτούν μεταξύ τους.

Οι P. Kyasanur και N. Vaidya στην προσέγγιση τους, [5], επισημαίνουν την αδυναμία των IEEE 802.11 δικτύων να αντιμετωπίσουν πιθανές επιθέσεις στο επίπεδο ελέγχου πρόσβασης στο μέσο. Γίνεται κι εδώ λόγος για τον μηχανισμό του backoff. Ο κόμβος που λαμβάνει τα δεδομένα καθορίζει την τιμή του bakoff που πρέπει να χρησιμοποιήσει ο αποστολέας. Με αυτό τον τρόπο ο παραλήπτης μπορεί να παρακολουθήσει αν όντως ο αποστολέας χρησιμοποίησε το backoff που του ανατέθηκε. Το κυρίως πρόβλημα στον συγκεκριμένο μηχανισμό είναι ότι ο παραλήπτης πρέπει να είναι έμπιστος. Το προτεινόμενο σχήμα αποτελείται από τρία βήματα:

1. Ο παραλήπτης ελέγχει, στο τέλος της μετάδοσης, αν ο αποστολέας αποκλίνει από τη σωστή λειτουργία του πρωτοκόλλου (μέσω τις τιμής του backoff που χρησιμοποιεί).
2. Αν ανιχνευθεί κάποια δυσλειτουργία, ο αποστολέας τιμωρείται. Ο βαθμός της τιμωρίας εξαρτάται από το είδος της απόκλισης που υπάρχει.
3. Αν η απόκλιση της συμπεριφοράς του αποστολέα, μετά από περισσότερες από μία μεταδόσεις, ξεπεράσει ένα προκαθορισμένο κατώφλι ο παραλήπτης μπορεί να ισχυριστεί πως υπάρχει σίγουρα πρόβλημα ασφάλειας με τον συγκεκριμένο κόμβο.

Τα αποτελέσματα των προσομοιώσεων δείχνουν πως ο συγκεκριμένος μηχανισμός επιτυγχάνει τον εντοπισμό και την αντιμετώπιση πιθανών προβλημάτων ασφάλειας στο επίπεδο ελέγχου πρόσβασης στο μέσο.

Μία άλλη ερευνητική προσπάθεια, [6], αναλύει τα πιθανά προβλήματα ασφάλειας που μπορούν να εμφανιστούν στην ανάπτυξη των IEEE 802.11 hotspots που παρέχουν

δημόσια ασύρματη πρόσβαση στο internet. Παρουσιάζεται ένα σύστημα (DOMINO), που έχει την ικανότητα να ανιχνεύει «άπληστες» (greedy) κομβικές συμπεριφορές στο επίπεδο ελέγχου πρόσβασης στο μέσο του δικτύου. Το DOMINO είναι ένα πακέτο λογισμικού που εγκαθίσταται στους κόμβους πρόσβασης (Access Points) και δεν επηρεάζει τη διαδικασία της αυθεντικοποίησης. Στις περισσότερες περιπτώσεις οι χρήστες ενός συστήματος παροχής ασύρματης πρόσβασης στο internet πρέπει να πληρώσουν ανάλογα με τις υπηρεσίες και την ποιότητα αυτών που απολαμβάνουν. Αυτό ίσως αποτελέσει κίνητρο για αρκετούς χρήστες ώστε να προσπαθήσουν να λάβουν όσο το δυνατόν καλύτερη ποιότητα υπηρεσιών με όσο το δυνατόν χαμηλότερο κόστος. Έτσι προσπαθούν, με διάφορες τεχνικές, να τροποποιήσουν τον διαμοιρασμό του μέσου προς όφελός τους φυσικά. Δυστυχώς αυτό μπορεί να έχει πολύ άσχημα αποτελέσματα στην ποιότητα υπηρεσιών που απολαμβάνουν οι υπόλοιποι χρήστες. Εδώ φαίνεται ο βαθμός απληστίας αυτών των κόμβων που αδιαφορώντας για τους υπόλοιπους χρήστες κάνουν τα πάντα για να επωφεληθούν οι ίδιοι. Μία χαρακτηριστική τεχνική που εφαρμόζεται από τους «άπληστους» χρήστες είναι η επιλογή μικρών τιμών των backoff ώστε να αποκτήσουν πιο γρήγορα πρόσβαση στο μέσο. Το DOMINO καταφέρνει να αντιμετωπίσει το πρόβλημα αυτό συγκρίνοντας τη μέση τιμή των backoff με ένα προκαθορισμένο κατώφλι. Η διαδικασία σύγκρισης χρησιμοποιεί τεχνικές ανάλυσης στατιστικών δεδομένων, οι οποίες είναι ενσωματωμένες στη λειτουργία των κόμβων πρόσβασης.

Κάποιες προσεγγίσεις που στηρίζονται στις αρχές της θεωρίας παιγνίων έχουν προταθεί πρόσφατα, [7, 8, 9]. Και εδώ έχουμε κάποιους μηχανισμούς διαχείρισης των τιμών του backoff. Επίσης αποδεικνύεται πως επιτυγχάνεται μία ισορροπία κατά Nash (Nash Equilibrium) ενάντια στους κόμβους που προσπαθούν «εγωιστικά» να αποκτήσουν πρόσβαση στο μέσο.

3.2 Μηχανισμοί ασφάλειας στο επίπεδο δρομολόγησης

Στο επίπεδο δρομολόγησης υπάρχουν αρκετές προσεγγίσεις που ασχολούνται με τα παρακάτω θέματα:

1. Ασφαλής Δρομολόγηση.
2. Διαχείριση κλειδιών και διαμοιρασμός αυτών.

3. Ενίσχυση της συνεργασίας μεταξύ των κόμβων.

Παρακάτω θα κάνουμε λόγο για κάποιους μηχανισμούς που λειτουργούν προς την κατεύθυνση της επίτευξης των παραπάνω στόχων. Κυρίως θα εστιάσουμε στην ενίσχυση της συνεργασίας μεταξύ των κόμβων.

Αρκετές ερευνητικές προσπάθειες που υπάρχουν στη βιβλιογραφία αναλύουν τα τρωτά σημεία των πιο δημοφιλή πρωτοκόλλων δρομολόγησης (πχ. DSR, AODV), και με διάφορες τροποποιήσεις προσπαθούν να τα ενισχύσουν. Οι περισσότερες προσεγγίσεις χρησιμοποιούν κατάλληλα διάφορες τεχνικές κρυπτογράφησης ώστε κατά τη διαδικασία της δρομολόγησης οι μη εξουσιοδοτημένοι κόμβοι να μην έχουν πρόσβαση σε πληροφορίες που δεν πρέπει να έχουν. Κάποιες πολύ αντιπροσωπευτικές προσεγγίσεις είναι:

1. SRP (Secure routing protocol), [10].
2. ARIADNE, [11].
3. SEAD, [12].
4. ARAN, [13].

Τα πρωτόκολλα που ασχολούνται με τη διαχείριση και το διαμοιρασμό των κλειδιών των χρηστών ενός δικτύου έρχονται να συμπληρώσουν τη δουλειά των πρωτοκόλλων ασφαλούς δρομολόγησης. Τα μυστικά κλειδιά που τα γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης αποτελούν τη βάση της κρυπτογράφησης της πληροφορίας που θα μεταδοθεί χωρίς να αποκαλυφθεί σε τρίτους. Επίσης ο συνδυασμός δημοσίου και προσωπικού κλειδιού δίνει τη δυνατότητα αυθεντικοποίησης των χρηστών. Εδώ έγκειται και η ανάγκη ύπαρξης ενός μηχανισμού που να διαμοιράζει αξιόπιστα τα δημόσια κλειδιά των χρηστών. Οι πιο αντιπροσωπευτικές προσεγγίσεις, [14, 15, 16, 17, 18, 19] προσπαθούν να επιτύχουν τους παραπάνω στόχους. Για τα πρωτόκολλα ασφαλούς δρομολόγησης και διαχείρισης κλειδιών δεν θα γίνει αναλυτική περιγραφή μιας και δεν αποτελούν αντικείμενο της συγκεκριμένης διατριβής.

Οι μηχανισμοί ενίσχυσης της συνεργασίας μεταξύ των κόμβων ενός αδόμητου δικτύου βασίζονται κυρίως στη διαχείρισης της φήμης (reputation) των κόμβων μέσα στο δίκτυο. Σε κάποιες προσεγγίσεις γίνεται χρήση της διαδικασίας της παρακολούθησης της συμπεριφοράς των κόμβων. Τέλος κάποιοι μηχανισμοί βασίζονται σε λογικές πληρωμής μεταξύ των κόμβων, χρησιμοποιώντας ηλεκτρονικές συναλλαγές.

Ο πρώτος μηχανισμός που προτάθηκε ώστε να επιτευχθεί η συνεργασία μεταξύ των κόμβων του δικτύου στηρίζεται στην παρακολούθησης της συμπεριφοράς των κόμβων, [20]. Καταφέρνει να αναγνωρίσει τους «ύποπτους» κόμβους και να τους αποτρέψει από το να πάρουν μέρος σε διάφορες λειτουργίες του δικτύου. Κάθε κόμβος διαθέτει ένα συστατικό παρακολούθησης (watchdog) ώστε να αντιλαμβάνεται τους «ύποπτους» κόμβους και ένα συστατικό αξιολόγησης (pathrater) το οποίο βοηθά τα πρωτόκολλα δρομολόγησης να αποφεύγουν τους κακόβουλους κόμβους. Πιο συγκεκριμένα το watchdog ανιχνεύει αν ένας κόμβος αρνείται να προωθήσει ένα πακέτο. Κατά τη διάρκεια της αποτίμησης της απόδοσης του συστήματος γίνεται λόγος για την άσχημη επίπτωση στην γενική απόδοση του δικτύου που μπορεί να προκαλέσουν κάποιοι κόμβοι που δεν συνεργάζονται και πως αυτό μπορεί να βελτιωθεί με το προτεινόμενο σύστημα.

Το OCEAN, [21] είναι ένας μηχανισμός που χρησιμοποιεί άμεση πληροφορία που αντλείται από τις παρατηρήσεις των κόμβων σχετικά με τη συμπεριφορά των υπολοίπων. Για κάθε κόμβο υπάρχει ένας βαθμός αξιοπιστίας. Ο βαθμός αυτός ανανεώνεται με βάση τη λειτουργία του συγκεκριμένου κόμβου. Αν ο βαθμός πέσει κάτω από ένα κατώφλι τότε ο κόμβος προστίθεται σε μία λίστα (faulty list). Η διαδικασία δρομολόγησης αποφεύγει τους κόμβους που βρίσκονται σε αυτή τη λίστα.

Οι P. Michiardi και R. Molva προτείνουν έναν γενικό μηχανισμό (CORE), [22], ο οποίος βασίζεται στη διαχείριση της φήμης (reputation) των κόμβων. Στόχος είναι η βελτίωση της συνεργασίας μεταξύ των κόμβων του δικτύου και η ανίχνευση των κόμβων που δρουν «εγωιστικά». Η φήμη του κάθε κόμβου βασίζεται στις πληροφορίες που προκύπτουν από την παρακολούθηση του.

Μία πρόσφατη προσέγγιση, [23, 24], εστιάζει κυρίως στη συνεργασία των κόμβων, στην σθεναρότητα του δικτύου (όσον αφορά θέματα ασφάλειας) και στην αμεροληψία στο διαμοιρασμό του μέσου που πρέπει να διατηρούνται σε ένα «υγιές» δίκτυο. Το πρωτόκολλο που προτείνεται είναι το CONFIDANT. Υπάρχει κι εδώ η έννοια της φήμης των κόμβων. Κάποιος κόμβος σχηματίζει κάποια άποψη για κάποιον άλλο μέσω της παρατήρησης είτε ρωτώντας κάποιους άλλους (friends) οι οποίοι ίσως έχουν κάποια εμπειρία επικοινωνίας μαζί του. Το κυρίως πρόβλημα του CONFIDANT είναι ότι τιμωρεί τους κόμβους αν αρνούνται να κάνουν προώθηση κάποιου πακέτου ανεξάρτητα της προηγούμενης συνεισφοράς τους στο δίκτυο. Αυτό έχει σαν αποτέλεσμα οι κόμβοι

που βρίσκονται στο κέντρο του δικτύου (όπου υπάρχει μεγάλη κυκλοφορία πληροφορίας) να αναγκάζονται να προωθούν οποιοδήποτε πακέτο λάβουν χωρίς να το ελέγξουν. Με αυτό τον τρόπο η απόδοση του δικτύου χειροτερεύει.

Ένα άλλο σύστημα, [25], χρησιμοποιεί έναν περιοδικό μηχανισμό εκπομπής. Κάθε κόμβος εκμεταλλευόμενος τον μηχανισμό αυτό στέλνει περιοδικά την άποψή του για τους γειτονικούς κόμβους του. Επίσης ένας κόμβος μπορεί να αρνηθεί να προωθήσει κάποιο πακέτο αλλά πρέπει να δικαιολογήσει τη συμπεριφορά του αυτή «δημοσιοποιώντας» τους λόγους που τον οδήγησαν σε αυτή τη συμπεριφορά. Προφανώς το πρόβλημα που δημιουργείται είναι ότι η επικοινωνία επιβαρύνεται καθώς έχουμε περισσότερη μετάδοση πληροφορίας (overhead).

Οι Krishna Paul και Dirk Westhoff στη δουλειά τους, [26], έχουν κάνει μια προσπάθεια να ανιχνεύσουν έναν μεγάλο αριθμό επιθέσεων στο πρωτόκολλο δρομολόγησης DSR (Dynamic Source Routing). Οι αναφορές κάποιων κόμβων του δικτύου για την άσχημη συμπεριφορά κάποιων άλλων, βοηθάει την ανίχνευση των «ύποπτων» κόμβων. Δεδομένου ότι υπάρχουν αρκετές αναφορές για έναν συγκεκριμένο κόμβο (υπάρχει δηλαδή ομοφωνία απόψεων για έναν κόμβο) είναι πολύ πιθανόν ο κόμβος αυτός να έχει πλήξει την ασφάλεια του δικτύου.

Έχει γίνει αρκετή δουλειά όσον αφορά τη διαχείριση της φήμης των κόμβων ενός δικτύου σε «ομότιμα» δίκτυα (peer-to-peer), [27-40]. Οι τεχνικές αυτές μπορούν να εφαρμοστούν στα ασύρματα αδόμητα δίκτυα με κάποιες τροποποιήσεις (λόγω του ασύρματου καναλιού).

Οι [41, 42] είναι δύο μηχανισμοί που ανιχνεύουν πιθανές ανωμαλίες στη λειτουργία των αδόμητων δικτύων. Αυτό επιτυγχάνεται είτε κατασκευάζοντας μοντέλα ανίχνευσης ανωμαλιών είτε χρησιμοποιώντας ειδικούς πράκτορες (agents) σε κάθε κόμβο, που επικοινωνούν μεταξύ τους.

Είναι αλήθεια ότι στα κατανεμημένα δίκτυα οι κόμβοι δεν έχουν κανένα ισχυρό κίνητρο ώστε να προωθούν τα πακέτα που λαμβάνουν προς όφελος κάποιων άλλων κόμβων. Υπάρχουν, στη βιβλιογραφία, κάποιες προσεγγίσεις που δίνουν κίνητρα στους κόμβους ενός δικτύου παρακινώντας τους να συνεργαστούν ώστε να επιτευχθεί η βέλτιστη απόδοσή του. Στις περισσότερες προσεγγίσεις υπάρχουν οικονομικά κίνητρα (virtual money).

Ένας από τους πρώτους μηχανισμούς που προτάθηκαν και λειτουργεί προς αυτή την κατεύθυνση, [43], θεωρεί τον κάθε κόμβο σαν ξεχωριστή οντότητα. Σε κάθε κόμβο υπάρχει μία υπομονάδα πιστωτικής μέτρησης. Ο πιστωτικός μετρητής μειώνεται όταν ο συγκεκριμένος κόμβος στέλνει ένα πακέτο και αυξάνεται όταν προωθεί ένα πακέτο (ο μετρητής πρέπει να είναι πάντα θετικός). Επίσης σε κάθε κόμβο υπάρχει ένας μηχανισμός που επιτρέπει τη πραγματοποίηση της παραπάνω διαδικασίας με ασφαλή τρόπο.

Οι Levente Buttyan και Jean-Piere Hubaux περιγράφουν το πρόβλημα της κατάρρευσης της διαθεσιμότητας του δικτύου για την παροχή υπηρεσιών όταν δεν υπάρχει η σωστή συνεργασία των κόμβων, [44]. Για την αντιμετώπιση του φαινομένου αυτού εισάγουν το ηλεκτρονικό χρήμα (money - nuggets). Οι κόμβοι του δικτύου προσπαθούν να συλλέξουν όσο το δυνατόν περισσότερα nuggets. Σε κάθε περίπτωση προώθησης ενός πακέτου ο συγκεκριμένος κόμβος πληρώνεται με ένα nugget. Επίσης για την αποστολή ενός πακέτου ο αποστολέας πρέπει να πληρώσει ένα nugget. Το κυρίως πρόβλημα στον μηχανισμό αυτόν είναι το γεγονός ότι το σύστημα πρέπει να υπολογίσει τον συνολικό αριθμό των nuggets που απαιτούνται για τη μετάδοση ενός πακέτου από τον προορισμό στον παραλήπτη του. Σε περίπτωση έλλειψης των nuggets το πακέτο θα εγκαταλειφθεί και σε περίπτωση πλεονασμού τα επιπλέον nuggets θα χαθούν. Αυτό μπορεί να αντιμετωπιστεί αν το σύστημα δίνει τη δυνατότητα στους χρήστες να αγοράζουν nuggets αν χρειαστούν.

Ένας ακόμη σύστημα που χρησιμοποιεί ένα πιστωτικό μηχανισμό προτάθηκε πρόσφατα (SPRITE), [45]. Εδώ κάθε κόμβος διατηρεί μία απόδειξη για κάθε πακέτο που λαμβάνει. Σε επόμενο βήμα ο κάθε κόμβος «φορτώνει» τις αποδείξεις που κατέχει στο σύστημα πιστωτικής εκκαθάρισης (CCS – Credit Clearance System). Με αυτό τον τρόπο αποδεικνύει ότι το πακέτο έφθασε ή προωθήθηκε. Στη συνέχεια ο CCS έχει το καθήκον να «πληρώσει» τον κόμβο του δημιούργησε το πακέτο (αρχικό κόμβο, αποστολέα) με βάση τις αποδείξεις που έχει για το συγκεκριμένο πακέτο. Σημαντικό θέμα είναι η διαθεσιμότητα του CCS. Αυτό έδωσε το κίνητρο στους συγγραφείς να εισάγουν τεχνικές ασφαλούς δρομολόγησης και διαμοιρασμού κλειδιών ώστε να επιτευχθεί η καλύτερη δυνατή διαθεσιμότητα.

Στο σύστημα των Raghavan και Snoeren, [46], ο μηχανισμός τιμολόγησης επιτρέπει κάθε κόμβο να θέτει αυθαίρετα τις δικές του οικονομικές απαιτήσεις για να προωθήσει κάποιο πακέτο. Κατά τη δρομολόγηση ενός πακέτου το σύστημα «πληρώνει» τους ενδιάμεσους κόμβους, ικανοποιώντας τις απαιτήσεις τους. Το πρόβλημα που δημιουργείται είναι το γεγονός ότι κάποιοι κόμβοι ίσως έχουν υπερβολικές οικονομικές απαιτήσεις. Αυτό μπορεί να αντιμετωπιστεί με κάποιο όριο που θα τεθεί στα «χρήματα» που μπορεί να ζητήσει ένας κόμβος.

Μία άλλη προσέγγιση, [47], δημιουργεί μία εικονική οικονομία. Προσπαθεί να μιμηθεί την οικονομία που υπάρχει στις ανθρώπινες κοινωνίες και έτσι προσαρμόζει την οικονομική ισορροπία στα κατανεμημένα δίκτυα και παρέχει αρκετά κίνητρα ώστε να διασφαλίσει τη σωστή λειτουργία της δρομολόγησης. Κάποιοι κόμβοι παίζουν το ρόλο της τράπεζας (banking nodes) και παρακολουθούν την όλη διαδικασία. Με την παρουσία των κόμβων αυτών διασφαλίζεται η τιμιότητα και η διαφάνεια της πληρωμής.

Τέλος, οι Anderreg και Eidenbenz προτείνουν ένα πρωτόκολλο, [48] το οποίο επιλέγει σε κάθε περίπτωση δρομολόγησης τη διαδρομή που συμφέρει οικονομικά.

Κεφάλαιο 4

Ανίχνευση και Αντιμετώπιση Κακόβουλης Συμπεριφοράς (Misbehavior Detection & Recovery)

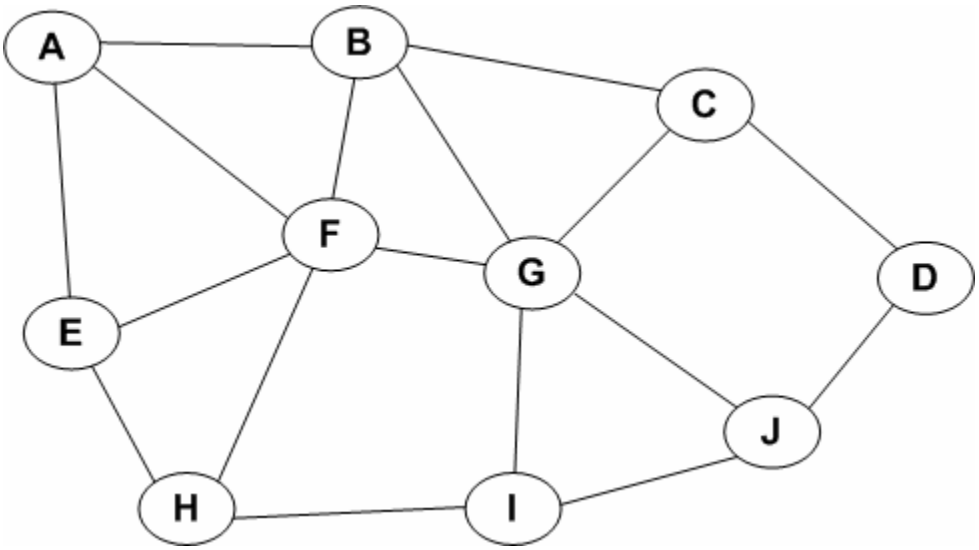
Στην ενότητα αυτή θα περιγράψουμε έναν μηχανισμό ανίχνευσης πιθανών κακόβουλων συμπεριφορών που λαμβάνουν χώρα στο επίπεδο ελέγχου πρόσβασης στο μέσο του δικτύου (MAC). Ο μηχανισμός αυτός βασίζεται στον ανταγωνισμό που υπάρχει μεταξύ των κόμβων (contention-based) για τη μετάδοση πληροφορίας. Είναι αρκετά γενικός ώστε να μπορεί να ανιχνεύει πολλών μορφών επιθέσεις (όπως επιθέσεις στον μηχανισμό του backoff, επιθέσεις στον μηχανισμό του NAV κλπ.). Οι κόμβοι που εφαρμόζουν τις επιθέσεις αυτές στο επίπεδο MAC έχουν σαν απώτερο σκοπό να λάβουν πρόσβαση στο μέσο και να μεταδώσουν γρηγορότερα από τους άλλους κόμβους. Δηλαδή, ο διαμοιρασμός του μέσου δεν είναι δίκαιος σε μία τέτοια κατάσταση (unfairness). Το MAC του IEEE 802.11 και ειδικότερα ο κατανεμημένος μηχανισμός DCF έχει κάποια προβλήματα δίκαιου διαμοιρασμού του καναλιού (unfairness) από μόνος του. Στη βιβλιογραφία υπάρχουν αρκετές αναφορές σε τέτοια προβλήματα (π.χ. hidden terminal) για τα οποία προτείνονται λύσεις. Όταν αυτά τα προβλήματα συνδυαστούν με επιθέσεις που έχουν τον ίδιο στόχο (να πλήξουν την «αμεροληψία» του MAC) τα πράγματα γίνονται πολύ άσχημα. Ο προτεινόμενος μηχανισμός λοιπόν, έρχεται να ενισχύσει τους μηχανισμούς αυτούς και να προσδώσει ανθεκτικότητα στο επίπεδο ελέγχου πρόσβασης.

4.1 Περιγραφή του μηχανισμού

Όπως αναφέρθηκε και πριν ο προτεινόμενος μηχανισμός βασίζεται στον ανταγωνισμό των κόμβων (contention-based). Στα πλαίσια της «υγιούς» λειτουργίας του

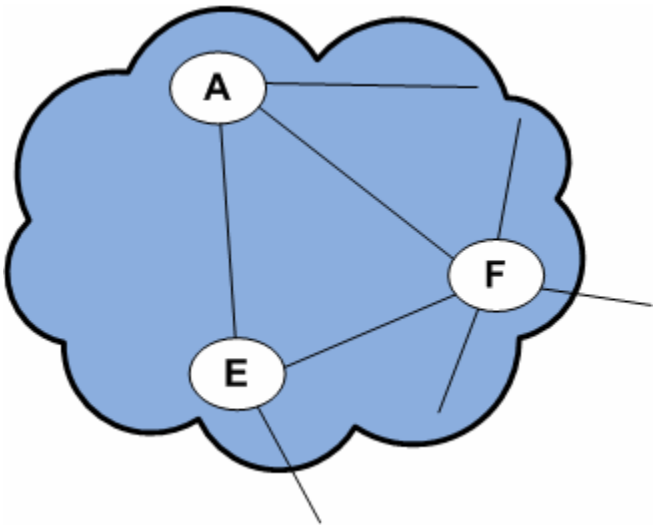
DCF ο κάθε κόμβος έχει ίδια πιθανότητα να αποκτήσει πρόσβαση στο κανάλι με τους υπόλοιπους. Δεδομένου βέβαια ότι η επιλογή του backoff είναι τυχαία και η τιμή του είναι μέσα στα επιτρεπτά όρια. Ο κόμβος με τη χαμηλότερη τιμή του backoff μεταδίδει πρώτος. Στη συνέχεια οι υπόλοιποι κόμβοι οι οποίοι θέλουν να μεταδώσουν και έχουν επιλέξει κάποιο backoff μεταδίδουν καθώς το backoff τους γίνει 0 (το backoff μειώνεται σε κάθε χρονική σχισμή – time slot που το κανάλι είναι ελεύθερο). Με αυτό τον τρόπο εγκαθίσταται μια «αμεροληψία» στον τρόπο λειτουργίας του DCF. Επίσης καθώς το πρωτόκολλο τεσσάρων φάσεων (RTS/CTS/DATA/ACK) λειτουργεί σωστά και ο μηχανισμός του NAV δεν έχει υποστεί κάποια παραβίαση, ο DCF εγγυάται τον δίκαιο διαμοιρασμό του καναλιού.

Η βάση του προτεινόμενου μηχανισμού είναι η δυνατότητα των κόμβων να παρακολουθούν (monitor) τη συμπεριφορά και τα πακέτα που στέλνουν οι γειτονικοί τους κόμβοι. Τα δεδομένα που προκύπτουν από την παρακολούθηση αυτή επεξεργάζονται και έτσι προκύπτει μία εκτίμηση (estimation) που κάνει ο κάθε κόμβος σχετικά με τα όρια της «νόμιμης» συμπεριφοράς των γειτονικών του κόμβων. Σε περίπτωση που τα όρια αυτά ξεπεραστούν ο συγκεκριμένος κόμβος θεωρείται ως κακόβουλος. Η λεπτομερής λειτουργία του μηχανισμού θα περιγραφεί μέσα από ένα παράδειγμα. Στο σχήμα 6 φαίνεται ένα ασύρματο αδόμητο δίκτυο, το οποίο αποτελείται από 10 κόμβους.



Σχήμα 6: Ένα ασύρματο αδόμητο δίκτυο.

Στο δίκτυο αυτό υπάρχουν πολλές περιοχές ανταγωνισμού. Μία περιοχή ανταγωνισμού αποτελείται από κόμβους που συνδέονται όλοι μεταξύ τους (βρίσκονται εντός της περιοχής εκπομπής τους). Η περιοχή ανταγωνισμού μπορεί να χαρακτηριστεί και ως «κλίκα» (clique). Μέσα στην περιοχή αυτή μόνο ένας κόμβος μπορεί να μεταδίδει σε κάθε χρονική σχισμή γιατί διαφορετικά θα έχουμε συγκρούσεις (collisions) στην επικοινωνία. Οι υπόλοιποι κόμβοι αναγκάζονται να σιωπούν. Για παράδειγμα, μία περιοχή ανταγωνισμού θεωρείται η περιοχή που περιλαμβάνει τους κόμβους {A, E, F}. Επίσης μέσα στην περιοχή αυτή όλοι οι κόμβοι θεωρούνται γειτονικοί και μπορούν να παρακολουθούν τα πακέτα που μεταδίδουν οι υπόλοιποι (που βρίσκονται μέσα στην περιοχή ανταγωνισμού). Ένας κόμβος μπορεί να συμμετάσχει σε περισσότερες από μία περιοχές ανταγωνισμού (π.χ. οι κόμβοι A, F συμμετέχουν σε δύο περιοχές ανταγωνισμού {A, E, F} και {A, B, F}). Σε μία τέτοια περίπτωση ο κάθε κόμβος παρακολουθεί τα πακέτα που μεταδίδονται σε όλες τις περιοχές ανταγωνισμού (στις οποίες συμμετέχει) και βγάζει κάποια συμπεράσματα για τους κόμβους της κάθε περιοχής ανταγωνισμού. Αυτό που έχει σημασία στον προτεινόμενο μηχανισμό είναι η παρακολούθηση των πακέτων δεδομένων (data packets) που στέλνουν οι κόμβοι. Σε χρονικό διάστημα μιας περιόδου ο κάθε κόμβος πρέπει να γνωρίζει τον ακριβή αριθμό των πακέτων δεδομένων που έστειλαν οι υπόλοιποι κόμβοι μέσα στην περιοχή ανταγωνισμού. Χωρίς βλάβη της γενικότητας θα περιγράψουμε τα βήματα του μηχανισμού για την περιοχή ανταγωνισμού {A, E, F} η οποία φαίνεται στο σχήμα 7.

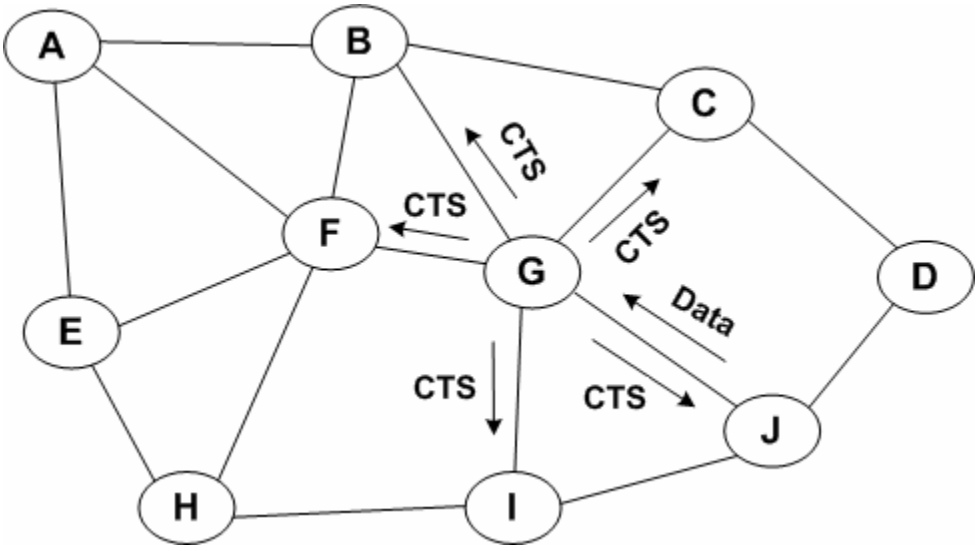


Σχήμα 7: Περιοχή ανταγωνισμού {A, E, F}.

Κατά το πρώτο βήμα του αλγορίθμου κάθε κόμβος της περιοχής ανταγωνισμού πρέπει να υπολογίσει τον μέσο ανταγωνισμό που βλέπει, με βάση βέβαια τη δραστηριότητα των υπολοίπων. Για τον υπολογισμό του μέσου ανταγωνισμού χρειαζόμαστε πληροφορία σχετικά με τα χρονικά διαστήματα που ο κάθε κόμβος μετέδωσε κάποιο πακέτο, αναγκάστηκε να σωπάσει από κάποιο κόμβο εντός της περιοχής ανταγωνισμού ή αναγκάστηκε να σωπάσει από κάποιο κόμβο εκτός της περιοχής ανταγωνισμού. Παρακάτω υπάρχουν κάποια σενάρια επικοινωνίας (για παράδειγμα μας ενδιαφέρει η αιτία για την οποία αναγκάζεται να σωπάσει ο κόμβος F και εφόσον αυτό το αντιλαμβάνονται οι υπόλοιποι κόμβοι της περιοχής ανταγωνισμού {A, E, F}):

1. Κάποιος κόμβος εντός της περιοχής ανταγωνισμού μεταδίδει σε κάποιο άλλο εντός ή εκτός της περιοχής ανταγωνισμού (π.χ. ο A μεταδίδει στον B). Οι E, F θα λάβουν το πακέτο RTS από τον A και θα αναγκαστούν να σωπάσουν και οι δύο κατά τη διάρκεια της μετάδοσης A→B.
2. Κάποιος κόμβος εκτός της περιοχής ανταγωνισμού μεταδίδει σε κάποιο κόμβο της περιοχής ανταγωνισμού (π.χ. ο B μεταδίδει στον A). Οι E, F θα λάβουν το CTS πακέτο από τον κόμβο A και έτσι θα σωπάσουν μέχρι το τέλος της μετάδοσης B→A.

3. Η τρίτη και πιο ενδιαφέρουσα περίπτωση είναι αυτή κατά την οποία ένας κόμβος της περιοχής ανταγωνισμού αναγκάζεται να σιωπά χωρίς να το γνωρίζουν οι υπόλοιποι (hidden terminal). Ένα παράδειγμα φαίνεται στο σχήμα 8.



Σχήμα 8: Σενάριο μετάδοσης J → G.

Ο κόμβος J μεταδίδει πληροφορία στον κόμβο G. Ο κόμβος G στέλνει ένα πακέτο CTS επιβεβαιώνοντας ότι το κανάλι είναι ελεύθερο και ότι ο J είναι ελεύθερος να μεταδώσει την πληροφορία του. Το CTS το λαμβάνει και ο F και έτσι αναγκάζεται να σιωπήσει για το χρονικό διάστημα της μετάδοσης. Αυτό όμως δεν το γνωρίζουν οι κόμβοι A, E μιας και δεν έχουν ακούσει το CTS. Δεδομένου λοιπόν πως ο κόμβος F σιωπά ο ανταγωνισμός στην περιοχή ανταγωνισμού {A, E, F} πέφτει στο 2 (σε όλες τις υπόλοιπες περιπτώσεις είναι 0 ή 3). Δηλαδή οι κόμβοι A και E μπορούν να μεταδώσουν με πιθανότητα 1/2 αντί του 1/3 (που ίσχυε πριν). Για τη σωστή λειτουργία του μηχανισμού οι κόμβοι A, E πρέπει να γίνουν γνώστες αυτού του γεγονότος γιατί σε αντίθετη περίπτωση θα προκύψουν εσφαλμένα συμπεράσματα. Οι κόμβοι λοιπόν είναι αναγκασμένοι, μέσω ενός καναλιού ελέγχου, να ενημερώνουν περιοδικά τους γειτονικούς τους για το χρονικό διάστημα που σιώπησαν (όταν εκείνοι δεν το γνωρίζουν και σε καταστάσεις όπως αυτή του σχήματος 8).

Επανερχόμαστε σε αυτό που είπαμε αρχικά, στον υπολογισμό του μέσου ανταγωνισμού σε διάστημα μιας περιόδου. Σαφώς, συνυπολογίζουμε την πληροφορία που στέλνεται μέσω του καναλιού ελέγχου. Χωρίζουμε το χρονικό διάστημα μιας περιόδου σε χρονικές σχισμές (time slots). Η πληροφορία που παίρνει ο κάθε κόμβος από το κανάλι ελέγχου καθορίζει το αν ένας κόμβος είναι ελεύθερος (free) ή έχει αναγκαστεί να σωπάσει (silenced). Δεν υπολογίζουμε τα σενάρια 1, 2 που αναφέρθηκαν πριν, μιας και δεν μας ενδιαφέρει η μεταβολή του ανταγωνισμού από 0→3 ή αντιστρόφως καθώς σε μία τέτοια περίπτωση κανένας κόμβος δεν απολαμβάνει κάποιο πλεονέκτημα απέναντι στους άλλους (είτε σιωπούν όλοι, είτε έχουν ίδιες πιθανότητες να μεταδώσουν εφόσον το κανάλι είναι ελεύθερο). Μας ενδιαφέρει κάθε ενδιάμεση κατάσταση όπου ο ανταγωνισμός μεταβάλλεται προς όφελος κάποιων κόμβων. Στο παράδειγμα του σχήματος 8 οι κόμβοι Α, Ε αυξάνουν την πιθανότητα να μεταδώσουν (από 1/3 σε 1/2) αφού η πιθανότητα μετάδοσης του F μηδενίζεται (επειδή αναγκάστηκε να σιωπήσει).

Έτσι λοιπόν, μετά από το χρονικό διάστημα μιας περιόδου κάθε κόμβος έχει πληροφορία σχετικά με τα χρονικά διαστήματα όπου οι υπόλοιποι κόμβοι της περιοχής ανταγωνισμού ήταν ελεύθεροι να ανταγωνιστούν για τη μετάδοση ή σιωπούσαν. Ο μέσος ανταγωνισμός θα υπολογιστεί από κάθε κόμβο της περιοχής ανταγωνισμού και το αποτέλεσμα που θα προκύψει πρέπει να είναι ίδιο σε κάθε κόμβο, καθώς έχουν όλοι τις ίδιες πληροφορίες. Ο μέσος ανταγωνισμός δίνεται από το πηλίκο του συνολικού αριθμού των χρονικών σχισμών κατά τις οποίες οι κόμβοι της περιοχής ανταγωνισμού ήταν ελεύθεροι να ανταγωνιστούν και του συνολικού αριθμού των χρονικών σχισμών μιας περιόδου.

$$\overline{Cont} = \frac{\sum_T free\ time\ slots}{period\ time\ slots}$$

Στη συνέχεια αφού υπολογίστηκε ο μέσος ανταγωνισμός ο κάθε κόμβος μπορεί να εκτιμήσει τον μέγιστο αριθμό των μεταδόσεων που θα μπορούσε να πραγματοποιήσει κάποιος γειτονικός κόμβος, με βάση τις συνθήκες που επικρατούσαν το χρονικό διάστημα της περιόδου. Η εκτίμηση αυτή δίνεται από τον παρακάτω τύπο:

$$Est_i = \left\lceil \frac{total\ \ data\ \ packets}{\overline{Cont}} \times \frac{free\ time\ slots\ of\ \ node\ i}{period\ time\ slots} \right\rceil$$

Ένας κόμβος i θεωρείται ότι είναι κακόβουλος και απολαμβάνει κάποιο μη νόμιμο πλεονέκτημα στο διαμοιρασμό του μέσου εφόσον ισχύει:

$$data\_packets(i) > Est_i \quad (1)$$

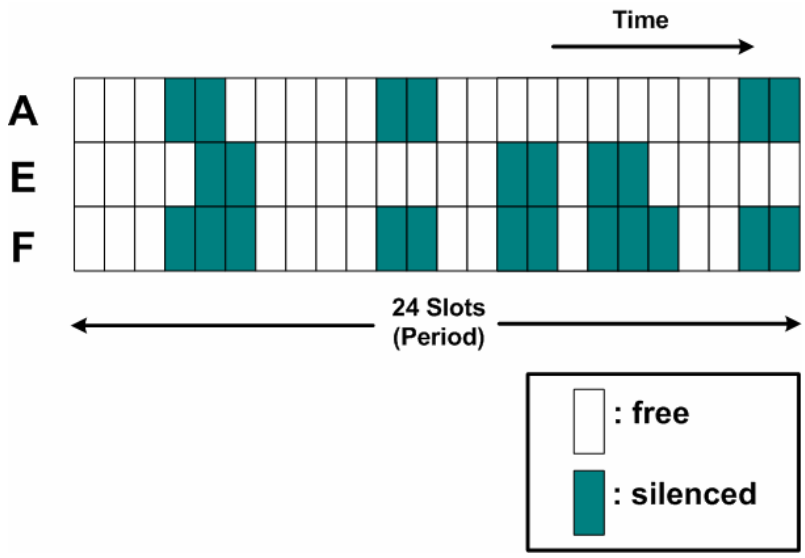
Αν θέλουμε να μετρήσουμε το μέγεθος της απόκλισης, αυτό είναι:

$$data\_packets(i) - Est_i$$

Παρακάτω θα δούμε ένα παράδειγμα εφαρμογής του μηχανισμού αυτού στη περιοχή ανταγωνισμού του σχήματος 7 ({A, E, F}). Θεωρούμε ότι η χρονική διάρκεια μιας περιόδου αποτελείται από 24 χρονικές σχισμές. Τα πακέτα δεδομένων που στάλθηκαν κατά τη διάρκεια μιας περιόδου (προέκυψαν από την παρακολούθηση – monitoring) φαίνονται στον πίνακα 1. Επίσης με βάση τις πληροφορίες που μεταδόθηκαν μέσω του καναλιού ελέγχου η κατάσταση που δημιουργήθηκε κατά τη διάρκεια της περιόδου (όσον αφορά τη διαμόρφωση του ανταγωνισμού), γνώστες της οποίας είναι όλοι οι κόμβοι της περιοχής ανταγωνισμού, φαίνεται στο σχήμα 9.

Contention range {A, E, F}	
Node	**Number of packets**
A	15
E	23
F	10

Πίνακας 1: Δεδομένα παρακολούθησης των κόμβων.



Σχήμα 9: Χρονικές σχισμές μιας περιόδου.

Αρχικά ο μέσος ανταγωνισμός που αντιλαμβάνονται οι κόμβοι είναι:

$$\overline{Cont} = \frac{48}{24} = 2$$

Η εκτίμηση για τον μέγιστο αριθμό εκπομπής πακέτων πληροφορίας για κάθε κόμβο είναι:

$$Est_F = \left\lceil \frac{10+23+15}{2} \times \frac{12}{24} \right\rceil = 12 \ \ packets$$

$$Est_E = \left\lceil \frac{10+23+15}{2} \times \frac{18}{24} \right\rceil = 18 \ \ packets$$

$$Est_A = \left\lceil \frac{10+23+15}{2} \times \frac{18}{24} \right\rceil = 18 \ \ packets$$

Συγκρίνουμε τις εκτιμήσεις με τα δεδομένα παρακολούθησης:

$$data\_packets(F) = 10 < Est_F = 12 \ \surd$$

$$data\_packets(E) = 23 > Est_E = 18 \ \times$$

$$data\_packets(A) = 15 < Est_A = 18 \ \surd$$

Παρατηρούμε λοιπόν πως υπάρχει πρόβλημα με τον κόμβο Ε και το μέγεθος της απόκλισης του από την εκτιμούμενη φυσιολογική συμπεριφορά είναι:

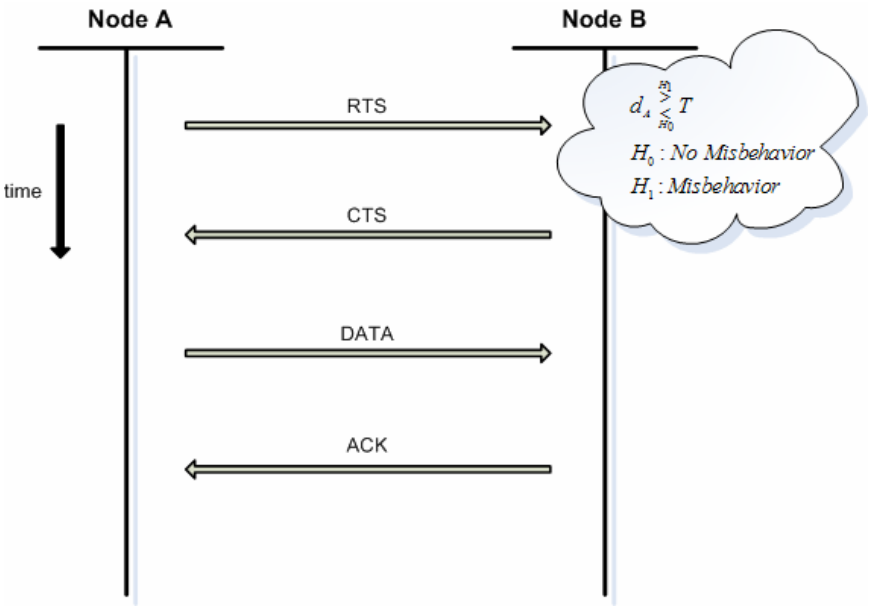
$$data\_packets(E) - Est_E = 23\text{-}18 = 5$$

Με τον τρόπο που περιγράφηκε πιο πάνω όλοι οι κόμβοι μπορούν να κάνουν κάποια εκτίμηση για τη συμπεριφορά των γειτονικών τους και να θέσουν κάποιο άνω όριο στη «νόμιμη» επιτρεπόμενη συμπεριφορά κάθε γειτονικού κόμβου. Η εκτίμηση που γίνεται αφορά τον μέγιστο επιτρεπόμενο αριθμό μεταδόσεων. Αν ο αριθμός αυτός ξεπεραστεί από κάποιο κόμβο τότε θεωρούμε ότι υπάρχει πρόβλημα ασφάλειας. Όλη αυτή η διαδικασία γίνεται περιοδικά. Ένα θέμα που προκύπτει είναι ο καθορισμός του χρόνου μιας περιόδου. Αν μία περίοδος αποτελείται από πολύ λίγες χρονικές σχισμές (time slots) τότε υπάρχει περίπτωση να μην εντοπιστεί κάποια δυσλειτουργία στη λειτουργία κάποιου κόμβου (αδυναμία ανίχνευσης). Αντίθετα αν η διάρκεια μιας περιόδου είναι πολύ μεγάλη τότε μπορεί να οδηγηθούμε σε λανθασμένα αποτελέσματα σχετικά με την ανίχνευση των κόμβων που έχουν πραγματικά πρόβλημα ασφάλειας (πρόβλημα λανθασμένης ανίχνευσης). Έτσι λοιπόν είναι θεμιτή η επιλογή μιας διάρκειας περιόδου η οποία να μην είναι πολύ μικρή αλλά ούτε και πολύ μεγάλη. Μία μέση κατάσταση είναι η πιο καλύτερη επιλογή. Η διάρκεια μιας περιόδου θα επηρεάσει πολύ τον καθορισμό του κατωφλίου (Threshold) που θα ορίσει τα όρια της «νόμιμης επιτρεπτής απόκλισης» ενός κόμβου. Κι εδώ υπάρχουν τα ίδια προβλήματα σχετικά με την τιμή που πρέπει να του αποδοθεί. Οι προσομοιώσεις που πραγματοποιήθηκαν, τα αποτελέσματα των οποίων θα παρατεθούν στην επόμενη υποενότητα, βοηθούν στον καθορισμό της βέλτιστης τιμής της χρονικής διάρκειας μιας περιόδου και σαν αποτέλεσμα στον καθορισμό της τιμής του κατωφλίου. Επίσης ένα σημαντικό θέμα στο οποίο βοήθησαν τα αποτελέσματα των προσομοιώσεων είναι ο συνολικός χρόνος εφαρμογής του μηχανισμού. Παρατηρήθηκε λοιπόν (όπως θα δούμε και στη συνέχεια) ότι αν ο χρόνος λειτουργίας του μηχανισμού είναι πολύ μεγάλος, οδηγούμαστε σε λανθασμένη ανίχνευση. Για αυτό το λόγο κρίνεται σκόπιμη η ανανέωση των δεδομένων σε τακτά χρονικά διαστήματα μέσα στα οποία θα είναι εγγυημένο πως όλοι οι κακόβουλοι κόμβοι θα έχουν ανιχνευθεί χωρίς να υπάρχει λανθασμένη ανίχνευση.

Τα όσα αναφέρθηκαν πιο πάνω αφορούν την ανίχνευση ενός πιθανού προβλήματος ασφάλειας. Αλλά ένας ολοκληρωμένος μηχανισμός ασφάλειας οφείλει να προβλέπει και την αντίδραση που πρέπει να υπάρχει εφόσον ανιχνευθούν κάποια κρούσματα κακόβουλης συμπεριφοράς. Σαφώς το πιο δύσκολο κομμάτι του μηχανισμού είναι η ανίχνευση γιατί εφόσον υπάρχει σοβαρή ένδειξη πως κάποιοι κόμβοι είναι κακόβουλοι

τότε η επιθυμητή αντίδραση είναι η απόρριψη των κόμβων αυτών από το δίκτυο. Συγκεκριμένα, εφόσον κάποιος κόμβος ανιχνεύσει κάποια δυσλειτουργία σε κάποιο άλλο γειτονικό του κόμβο τότε δεν τον θεωρεί ως μέρος του δικτύου. Αυτό το πετυχαίνει με το να μην του απαντάει σε κάποια πιθανή αίτηση για αποστολή δεδομένων (RTS). Με αυτό τον τρόπο είναι σίγουρο πως ένας κακόβουλος κόμβος θα βγει έξω από το δίκτυο. Στο σχήμα 10 φαίνεται ένα σενάριο κατά το οποίο ο κόμβος A θέλει να μεταδώσει πληροφορία στον B. Του στέλνει ένα RTS και ο B εφόσον το λάβει δεν απαντάει αμέσως με CTS, αλλά ελέγχει πρώτα αν ο A είναι κακόβουλος. Εξετάζει λοιπόν το ιστορικό της συμπεριφορά του A και συγκρίνει την πιθανή απόκλιση του (d_A) με κάποιο προκαθορισμένο κατώφλι. Αν αυτή είναι μεγαλύτερη από το κατώφλι δεν του απαντάει και τον αναγνωρίζει ως κακόβουλο. Σε αντίθετη περίπτωση, του απαντά κανονικά με ένα πακέτο CTS. Με άλλα λόγια μόλις ένας κόμβος λάβει μία αίτηση αποστολής δεδομένων από κάποιο γειτονικό του κόμβο i εφαρμόζει τον παρακάτω έλεγχο, το αποτέλεσμα του οποίου θα κρίνει αν θα συνεχιστεί η επικοινωνία μεταξύ τους:

```
if ( d_i < T) {
      reply with CTS while the channel is idle
}
else {
     identify i as a misbehaving node and avoid
     communicating with node i
}
```



Σχήμα 10: Έλεγχος ύπαρξης κακόβουλης συμπεριφοράς.

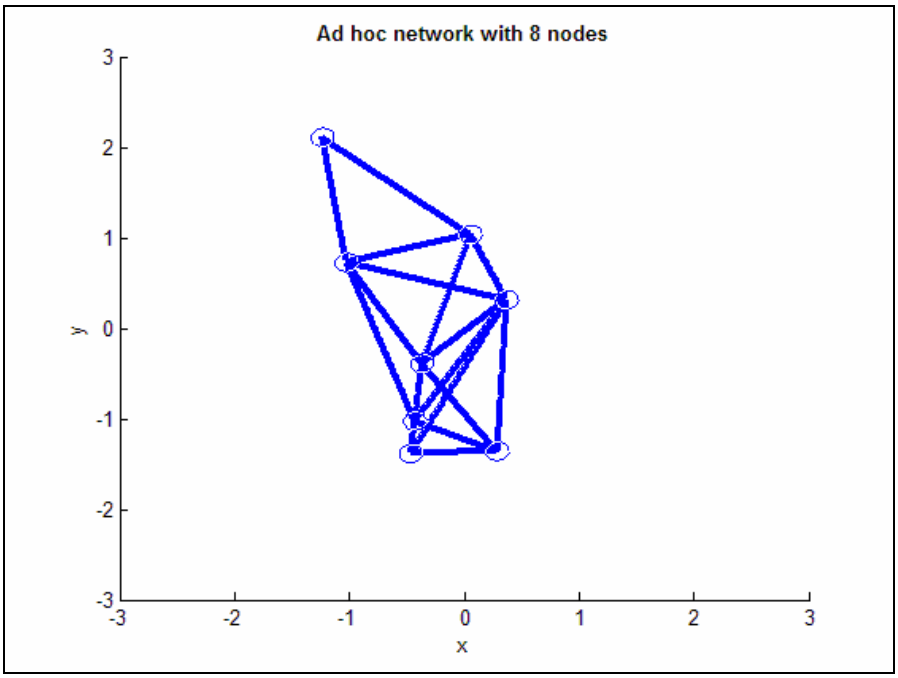
4.2 Αποτίμηση της απόδοσης του μηχανισμού

Για την αποτίμηση της απόδοσης του μηχανισμού που περιγράφηκε πιο πάνω υλοποιήθηκε ένας προσομοιωτής (simulator) σε MATLAB. Προσομοιώθηκε η λειτουργία του CSMA/CA (IEEE 802.11) και συγκεκριμένα του μηχανισμού DCF που υποστηρίζει τον κατανεμημένο διαμοιρασμό του μέσου σε ένα αδόμητο δίκτυο. Υποστηρίζεται το πρωτόκολλο τεσσάρων φάσεων για τη μετάδοση ενός σταθμού (RTS/CTS/DATA/ACK). Έτσι λοιπόν εφόσον ένας κόμβος επιθυμεί να μεταδώσει στέλνει ένα RTS πακέτο στον παραλήπτη και καθώς το κανάλι είναι ελεύθερο ο παραλήπτης του απαντάει με ένα πακέτο CTS. Ο αρχικός κόμβος στέλνει ένα πακέτο δεδομένων (DATA) και μόλις το πακέτο παραδοθεί ο παραλήπτης του απαντάει με ένα πακέτο επιβεβαίωσης (ACK).

Οι προσομοιώσεις εφαρμόστηκαν σε ασύρματα αδόμητα δίκτυα με τυχαίες τοπολογίες και αριθμό κόμβων. Πραγματοποιήθηκαν πολλά πειράματα όπου δοκιμάστηκαν διαφορετικές χρονικές διάρκειες περιόδων και διαφορετικές τιμές κατωφλίων. Τα όσα αναφέρθηκαν πιο πριν, όσον αφορά τη διάρκεια μιας περιόδου και την τιμή του κατωφλίου, επιβεβαιώθηκαν από τις προσομοιώσεις που πραγματοποιήσαμε. Σαφώς η τιμή του κατωφλίου επηρεάζεται από τη χρονική διάρκεια

μιας περιόδου και τις μεταδόσεις των πακέτων που πραγματοποιούνται κατά τη διάρκεια αυτή. Στα πειράματα που πραγματοποιήσαμε θεωρήσαμε πως η περίοδος αποτελείται από 300 χρονικές σχισμές (περίπου 0.3 sec). Επίσης με βάση αυτή τη χρονική διάρκεια μία πολύ καλή τιμή για το κατώφλι είναι 25.

Παρακάτω θα δούμε κάποια αποτελέσματα προσομοίωσης που υποδηλώνουν τη σωστή λειτουργία του μηχανισμού που προτείνεται. Το αδόμητο δίκτυο που προσομοιώθηκε αποτελείται από 8 κόμβους και η τοπολογία του προέκυψε τυχαία κατά τη διαδικασία της προσομοίωσης. Στο σχήμα 11 φαίνεται η τοπολογία του δικτύου καθώς και η επικοινωνία μεταξύ των κόμβων.

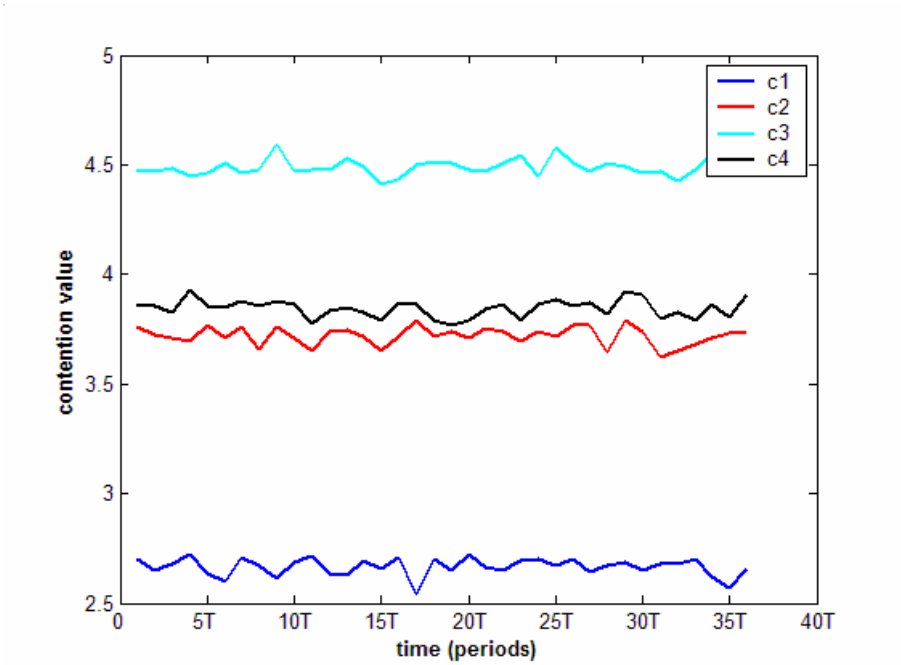


Σχήμα 11: Παράδειγμα δικτύου προσομοίωσης.

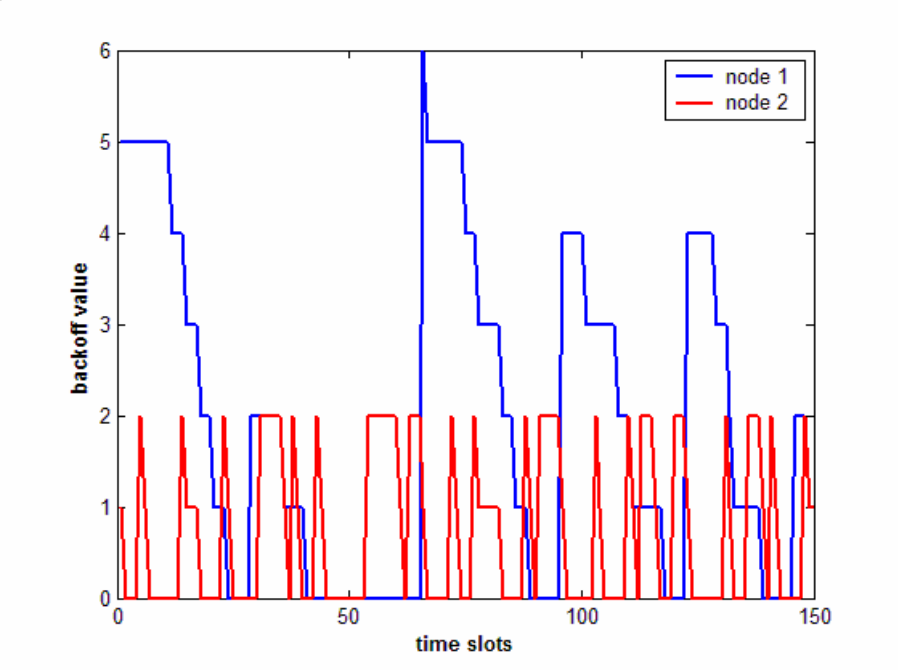
Οι περιοχές ανταγωνισμού που δημιουργούνται στο συγκεκριμένο αδόμητο δίκτυο είναι τέσσερις και περιγράφονται από τον παρακάτω πίνακα:

$$\underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}}_{nodes} \left\{ contention\ regions \right.$$

Ο μέσος ανταγωνισμός υπολογίζεται στο τέλος της κάθε περιόδου. Στο σχήμα 12 μπορούμε να δούμε την εξέλιξη του μέσου ανταγωνισμού σε διάστημα 35 περιόδων. Στο σχήμα 13 φαίνονται οι τιμές των backoff που επιλέγουν οι κόμβοι 1 και 2. Ο κόμβος 2 είναι ένας κακόβουλος κόμβος και όπως βλέπουμε επιλέγει μικρότερα backoff από τον 1 και γενικά από τους υπόλοιπους «υγιείς» κόμβους (η τιμη του backoff του είναι πάντα 2). Επίσης στο σχήμα 13 μπορούμε να δούμε πως ο κόμβος 2 με την τεχνική του αυτή καταφέρνει να μεταδίδει περισσότερες φορές από τον κόμβο 1. (ένας κόμβος μπορεί να μεταδώσει όταν η τιμή του backoff του πέσει στο 0). Στη συγκεκριμένη προσομοίωση θεωρούμε πως CW_{min}=4 και CW_{max}=12.

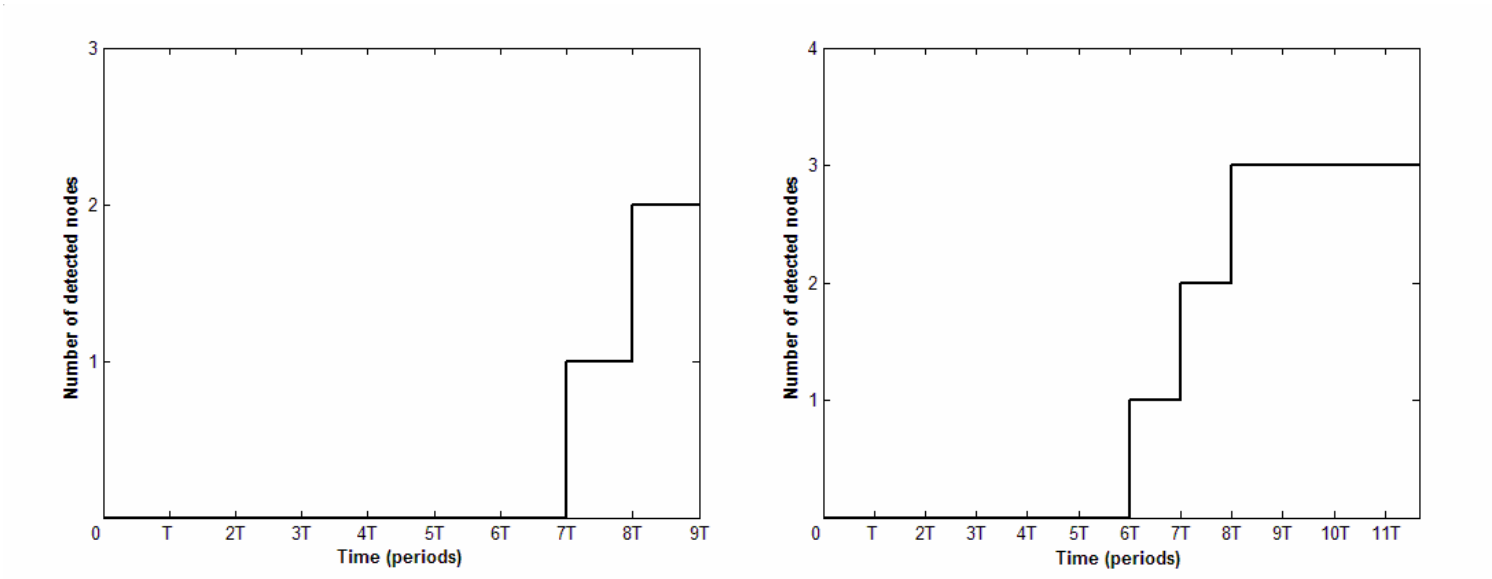


Σχήμα 12: Η εξέλιξη του μέσου ανταγωνισμού στις τέσσερις περιοχές ανταγωνισμού (c1, c2, c3, c4) κατά τη διάρκεια 35 περιόδων λειτουργίας του δικτύου.

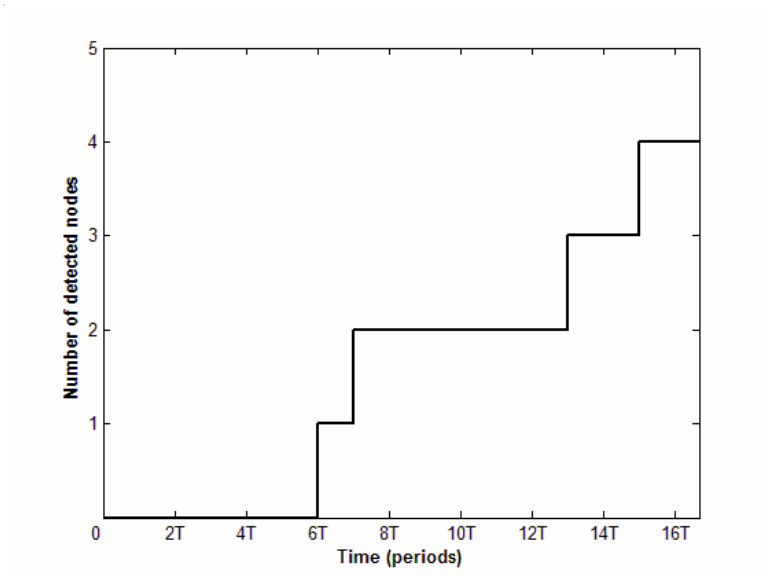


Σχήμα 13: Οι τιμές των backoff που επιλέγουν οι κόμβοι 1, 2.

Στα σχήματα 14, 15 απεικονίζονται κάποια αποτελέσματα της προσομοίωσης που χαρακτηρίζουν την απόδοση του συστήματος όσον αφορά το χρόνο ανίχνευσης των κακόβουλων κόμβων. Στα 14A και 14B παρατηρούμε ότι οι κακόβουλοι κόμβοι ανιχνεύονται σε πολύ μικρό χρονικό διάστημα (περίπου 8 περιόδων). Στο 14C, όπου το 50% των κόμβων του δικτύου είναι κακόβουλοι ο χρόνος ανίχνευσης αυξάνεται και είναι σχεδόν διπλάσιος από τις προηγούμενες περιπτώσεις. Ενδιαφέρον έχει να παρατηρήσουμε τι συμβαίνει όταν το ποσοστό των κακόβουλων κόμβων του δικτύου ξεπερνά το 50%. Για παράδειγμα στο σχήμα 15A (5 κακόβουλοι κόμβοι) ο χρόνος ανίχνευσης είναι πολύ μεγαλύτερος από πριν (σχεδόν διπλάσιος – 27T). Ένα ακραίο σενάριο εμφανίζεται στο σχήμα 15B όπου το 75% των κόμβων του δικτύου είναι κακόβουλοι. Προφανώς εδώ η ανίχνευση είναι πολύ δύσκολη υπόθεση καθώς υπάρχουν περιπτώσεις όπου οι κόμβοι κάποιας περιοχής ανταγωνισμού είναι όλοι κακόβουλοι και η «εγωιστική» συμπεριφορά του ενός, κατά κάποιο τρόπο, υπερκαλύπτει τη συμπεριφορά των άλλων. Παρατηρούμε λοιπόν πως από τη στιγμή που το ποσοστό των κακόβουλων κόμβων ξεπεράσει το 50% το πρόβλημα της ανίχνευσης δυσκολεύει αρκετά. Ο μηχανισμός αργεί αρκετά να ανιχνεύσει τα πιθανά προβλήματα ασφάλειας που υπάρχουν.

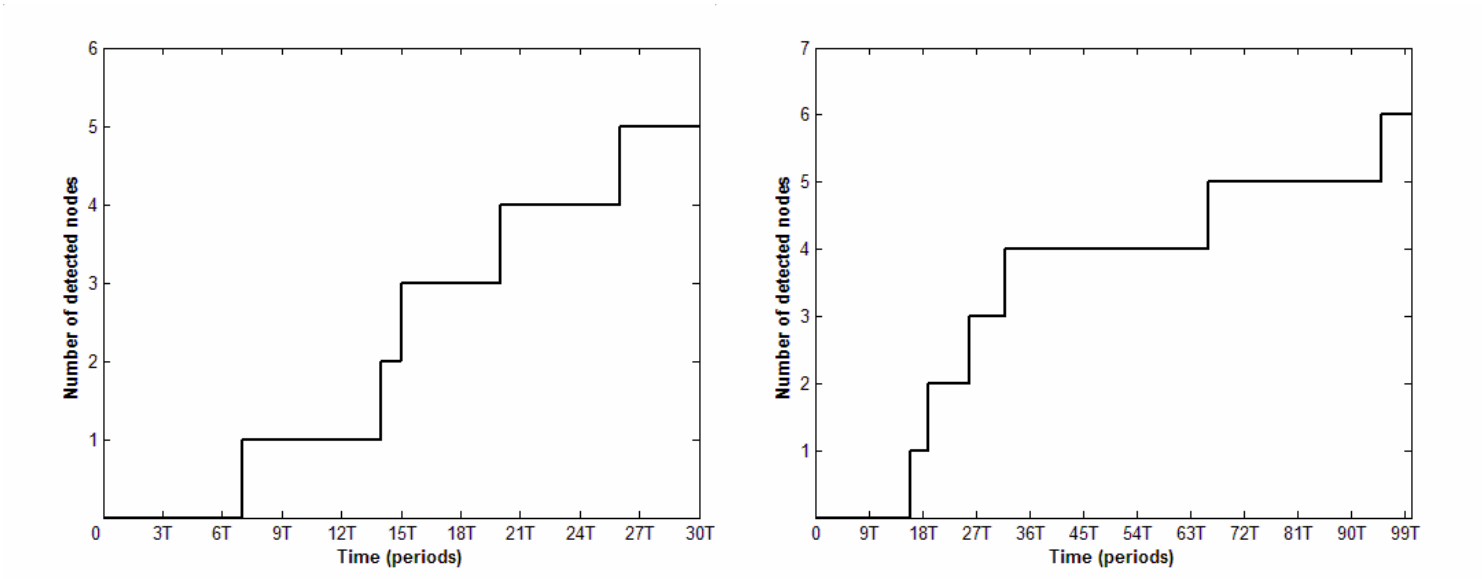


A) **B)**



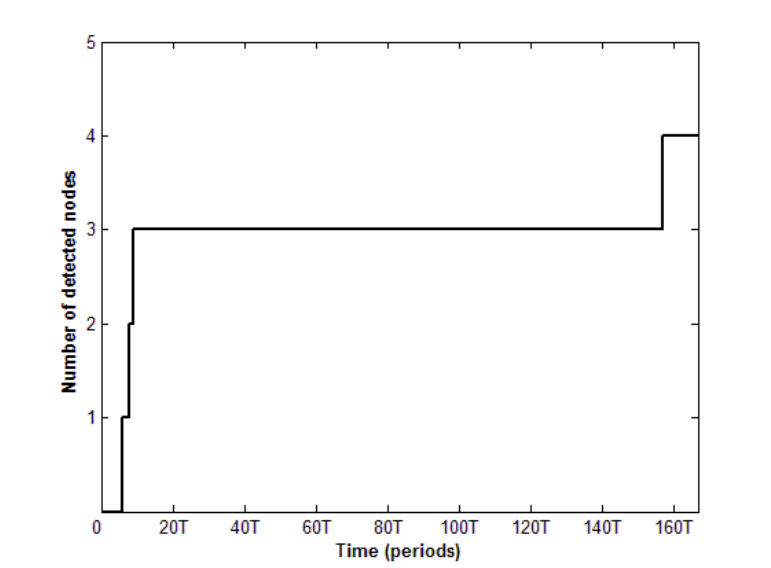
C)

Σχήμα 14: Αποτελέσματα προσομοίωσης: **A)** Ύπαρξη 2 κακόβουλων κόμβων, **B)** Ύπαρξη 3 κακόβουλων κόμβων, **C)** Ύπαρξη 4 κακόβουλων κόμβων (50% των συνολικών κόμβων).



A) **B)**

Σχήμα 15: Αποτελέσματα προσομοίωσης: **A)** Ύπαρξη 5 κακόβουλων κόμβων, **B)** Ύπαρξη 6 κακόβουλων κόμβων (75% των συνολικών κόμβων).



Σχήμα 16: Λανθασμένη ανίχνευση (false alarm).

Έχουμε δείξει πως όταν υπάρχουν κακόβουλοι κόμβοι μέσα σε ένα αδόμητο δίκτυο ο προτεινόμενος μηχανισμός καταφέρνει να ανιχνεύσει επιτυχώς όλους τους κόμβους που παρουσιάζουν πρόβλημα. Αυτό που μένει είναι να δείξουμε τι συμβαίνει με τη

λανθασμένη ανίχνευση (false alarm). Όπως φαίνεται από το σχήμα 16 υπάρχει περίπτωση λανθασμένης ανίχνευσης όταν η λειτουργία του μηχανισμού συνεχίζεται για μεγάλο χρονικό διάστημα χωρίς να ανανεώνονται τα δεδομένα που βοηθούν στην ανίχνευση. Συγκεκριμένα στο σχήμα 16 θεωρούμε πως έχουμε 3 κακόβουλους κόμβους στο δίκτυο, οι οποίοι ανιχνεύονται σε μικρό χρονικό διάστημα (<10T). Όμως καθώς η λειτουργία του μηχανισμού συνεχίζεται παρατηρούμε πως μετά από 155 περιόδους έχουμε λανθασμένη ανίχνευση. Η λανθασμένη ανίχνευση οφείλεται σε συγκρούσεις που τυχόν υπάρχουν στις μεταδώσεις των πακέτων δεδομένων καθώς επίσης και στην κατάσταση των συνδέσεων του δικτύου. Λόγω των συγκρούσεων ή των φτωχών σε απόδοση συνδέσεων πολλά πακέτα δεδομένων δεν φθάνουν σε όλους τους κόμβους. Αυτό επηρεάζει σε μικρό βαθμό την αποδοτική λειτουργία του μηχανισμού. Αλλά σε μεγάλα χρονικά διαστήματα λειτουργίας αυτό συσσωρεύεται, με αποτέλεσμα να έχουμε λανθασμένα συμπεράσματα. Για όλους τους λόγους αυτούς κρίνεται σκόπιμο να ανανεώνονται τα δεδομένα του συστήματος σε τακτά χρονικά διαστήματα. Οι πληροφορίες που προκύπτουν από την παρακολούθηση της συμπεριφοράς ενός κόμβου ή ακόμη και από το κανάλι ελέγχου, μόλις περάσει ένα συγκεκριμένο χρονικό διάστημα «πετιούνται». Με αυτό τον τρόπο ο μηχανισμός ξεκινάει ξανά από την αρχή τη λειτουργία του. Εδώ όμως πρέπει να δοθεί προσοχή γιατί η επιλογή του σημείου κατά το οποίο ο μηχανισμός θα ξεκινήσει ξανά πρέπει να γίνεται με τέτοιο τρόπο ώστε οι πραγματικά κακόβουλοι κόμβοι να έχουν ανιχνευθεί πριν από αυτό το σημείο. Σε αντίθετη περίπτωση θα έχουμε αστοχία στο να ανιχνευθούν όλοι οι κακόβουλοι κόμβοι. Προφανώς το σημείο επανέναρξης εξαρτάται από τη χρονική διάρκεια μιας περιόδου και από την τιμή του κατωφλίου. Με βάση τη χρονική διάρκεια της περιόδου και της τιμής του κατωφλίου που εφαρμόζονται στην διαδικασία της προσομοίωσης στα παραπάνω σενάρια ένα πολύ καλό σημείο επανέναρξης του μηχανισμού είναι το χρονικό σημείο 130T. Δηλαδή, κάθε χρονικό διάστημα 130 περιόδων ο μηχανισμός ξεκινάει ξανά με νέα δεδομένα. Η συγκεκριμένη τιμή προέκυψε από πειράματα που πραγματοποιήθηκα για ακραίες καταστάσεις (όπως πριν με 75% κακόβουλους κόμβους).

Κεφάλαιο 5

Ενοποίηση Επιπέδων (Cross-Layering)

Όπως αναφέρθηκε και σε προηγούμενη ενότητα η ενοποίηση των επιπέδων της στοίβας των πρωτοκόλλων (cross-layering) είναι ένα πολυδιάστατο θέμα και υπόσχεται πολύ καλά αποτελέσματα σε πολλούς τομείς εφαρμογής του. Παραδοσιακά η στοίβα των πρωτοκόλλων αποτελείται από επίπεδα τα οποία βρίσκονται το ένα πάνω από το άλλο. Αυτή η λογική υιοθετήθηκε λόγω της ευκολίας που παρέχει στον σχεδιασμό των δικτύων. Όμως η απόδοση και η συμπεριφορά των πρωτοκόλλων που λειτουργούν στα διάφορα επίπεδα ποικίλει ανάλογα με το πρωτόκολλο που έχει εγκατασταθεί στο επάνω ή κάτω επίπεδο. Για τον λόγο αυτό έχουν υλοποιηθεί πολλές αλληλεπιδράσεις μεταξύ των πρωτοκόλλων που δουλεύουν σε διαφορετικά επίπεδα. Αυτές οι αλληλεπιδράσεις που λαμβάνουν χώρα στα επίπεδα πρωτοκόλλων ενός κόμβου ή ακόμη και σε επίπεδα που ανήκουν σε διαφορετικούς κόμβους έχει αποδειχθεί ότι με σωστό σχεδιασμό μπορούν να επιφέρουν θετικά αποτελέσματα στην απόδοση των αδόμητων ασύρματων δικτύων. Τα αδόμητα δίκτυα είναι δυναμικά και μία αυστηρώς στρωματοποιημένη αρχιτεκτονική δεν είναι αρκετά ευέλικτη ώστε να μπορέσει να λειτουργήσει θετικά στη βελτίωση της απόδοσής τους.

Η ενοποίηση των επιπέδων δημιουργεί μία αλληλεξάρτηση μεταξύ τους με απώτερο στόχο τη βελτίωση της απόδοσης λειτουργίας των δικτύων. Σε μία ενοποιημένη αρχιτεκτονική (cross-layering architecture) οι πληροφορίες που χρειάζεται ένα πρωτόκολλο από κάποιο άλλο πρωτόκολλο που ίσως λειτουργεί σε άλλο επίπεδο είναι διαθέσιμες. Με αυτό τον τρόπο η συμπεριφορά των πρωτοκόλλων προσαρμόζεται

κατάλληλα. Για παράδειγμα με δεδομένα χαρακτηριστικά δικτύου και καναλιών εκπομπής το φυσικό επίπεδο (physical layer) μπορεί να θέσει κατάλληλα την ισχύ εκπομπής, την κωδικοποίηση και άλλες παραμέτρους ώστε να παρασχεθεί η απαιτούμενη ποιότητα υπηρεσίας. Σε μία στρωματοποιημένη αρχιτεκτονική τα πρωτόκολλα των επιπέδων λειτουργούν τις περισσότερες φορές ανεξάρτητα μεταξύ τους.

Παρόλα τα υποσχόμενα πλεονεκτήματα που μπορούν να αποκομίσουν τα αδόμητα δίκτυα από μία ενοποιημένη αρχιτεκτονική, από τη στιγμή που η αυτονομία του κάθε επιπέδου σπάει η κάθε σχεδιαστική λεπτομέρεια πρέπει να ερευνηθεί. Η ενοποίηση των επιπέδων μπορεί να προκαλέσει «βρόγχους» [52-53]. Επίσης μία οποιαδήποτε σχεδιαστική ατέλεια μπορεί να προκαλέσει σοβαρές διαταραχές στη σωστή λειτουργία του δικτύου. Οι διευκολύνσεις που μας παρέχει μια ενοποιημένη αρχιτεκτονική μπορεί να μας οδηγήσει στον ανεξέλεγκτο σχεδιασμό αλληλεπιδράσεων μεταξύ των επιπέδων. Αυτό θα έχει σαν αποτέλεσμα την κατασκευή μια αρχιτεκτονικής “spaghetti”. Κάθε αλλαγή που γίνεται, στα πλαίσια της ενοποίησης, πρέπει να λαμβάνει υπόψη τις επιπτώσεις που μπορεί να προκαλέσει.

Ο μόνος τρόπος για να πετύχει κανείς τα πλεονεκτήματα που απορρέουν από μία ενοποιημένη αρχιτεκτονική είναι να ξανασχεδιάσει τα πρωτόκολλα με τα νέα δεδομένα που υπάρχουν. Διαφορετικά λειτουργεί ένα πρωτόκολλο που είναι απομονωμένο από τα υπόλοιπα επίπεδα και διαφορετικά λειτουργεί όταν πρέπει να υπάρχει μια συνεργασία με τα πρωτόκολλα των άλλων επιπέδων. Στη βιβλιογραφία η ενσωμάτωση του φυσικού επιπέδου και του επιπέδου ελέγχου πρόσβασης στο μέσο επικρατεί. Πολλοί παράμετροι του φυσικού επιπέδου (ισχύς εκπομπής, κωδικοποίηση κλπ.) έχουν σημαντική επιρροή στην απόδοση του επιπέδου ελέγχου πρόσβασης στο μέσο. Η κατάλληλη προσαρμογή των παραμέτρων αυτών επηρεάζει θετικά την προσφερόμενη ποιότητα υπηρεσιών (QoS) του φυσικού επίπέδου αλλά και την παρατηρούμενη ποιότητα υπηρεσιών (QoS) των πιο πάνω επιπέδων. Σημαντική είναι και η συμβολή της ενοποίησης των επιπέδων στη διαδικασία της δρομολόγησης. Τα δεδομένα που προκύπτουν από τη λειτουργία ενός πρωτοκόλλου δρομολόγησης είναι πολλές φορές καθοριστικά για τη σωστή λειτουργία των πρωτοκόλλων των άλλων επιπέδων. Επίσης η ίδια η διαδικασία της δρομολόγησης χρειάζεται τη συμβολή των άλλων επιπέδων ώστε να ανακαλυφθούν τα τυχόν προβλήματα που υπάρχουν σε κάποιες συνδέσεις του δικτύου (links). Με αυτή τη γνώση

λοιπόν, το πρωτόκολλο δρομολόγησης θα μπορεί να επιλέξει διαδρομές που δεν θα περιέχουν τις ελαττωματικές συνδέσεις.

Οι διάφορες προσεγγίσεις που υπάρχουν αυτή τη στιγμή (όπως οι [54-58]) οι οποίες επωφελούνται των πλεονεκτημάτων της ενοποίησης των επιπέδων, για διαφορετικό σκοπό η κάθε μία, δεν ακολουθούν κάποιο πρότυπο (standard). Δηλαδή, δεν υπάρχει κάποιο πρότυπο που να καθορίζει τον τρόπο και γενικά τις διαδικασίες που πρέπει να ακολουθηθούν για τη μετάδοση της πληροφορίας από το ένα επίπεδο στο άλλο. Σαφώς υπάρχει η ανάγκη δημιουργίας ενός τέτοιου προτύπου. Η διαδικασία της ενοποίησης δεν επιτυγχάνεται χωρίς κόστος (στους πόρους του δικτύου). Στα πλαίσια δημιουργίας ενός στάνταρ πρέπει να γίνει έρευνα για το πως μεταδίδεται η πληροφορία μεταξύ των επίπέδων και ποιο κόστος επιφέρει κάθε τεχνική μετάδοσης της πληροφορίας. Παρακάτω συνοψίζονται κάποιες απαιτήσεις που υπάρχουν για την εκτέλεση της ενοποίησης των επιπέδων:

1. Επιπλέον φόρτο στην επικοινωνία (overhead).
2. Επιπλέον υπολογιστική δύναμη.
3. Καλύτερο signaling.
4. Ελαχιστοποίηση των σφαλμάτων των καναλιών μετάδοσης (channel errors).

Αυτή τη στιγμή γίνεται προσπάθεια για την κατασκευή τεχνικών μετάδοσης της πληροφορίας μεταξύ των επιπέδων. Υπάρχουν προτάσεις σύμφωνα με τις οποίες δεν απαιτείται η μετάδοση επιπλέον πληροφορίας μεταξύ των επίπεδων. Η ενοποιημένη πληροφορία μπορεί να προκύψει από τη σωστή επεξεργασία των headers των πακέτων που μεταδίδονται στο δίκτυο ή από κάποιες εκτιμήσεις κατά την επεξεργασίας της κυκλοφορίας. Μία τεχνική υποστηρίζει πως η πληροφορία θα μεταδίδεται μέσω των διεπαφών (interfaces) των πρωτοκόλλων. Προφανώς απαιτούνται συσκευές με πολλές διεπαφές. Τέλος, μία άλλη προσέγγιση λειτουργεί προς την κατεύθυνση της τροποποίησης των πρωτοκόλλων και των διεπαφών τους ώστε η πληροφορία να μεταφέρεται ως επιπλέον σήματα ελέγχου ή κωδικοποιημένη μέσα στα headers των πακέτων.

5.1 Η προσφορά της ενοποίησης στην ασφάλεια των αδόμητων δικτύων

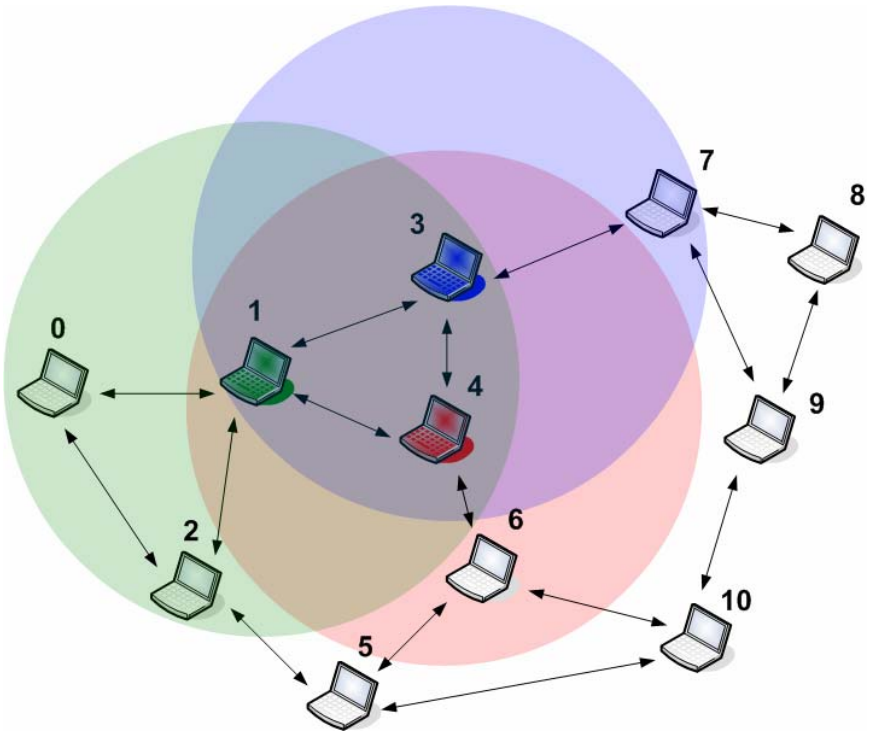
Σύμφωνα με όσα λέχθηκαν παραπάνω η προσφορά της ενοποίησης των επιπέδων είναι σημαντική εφόσον υπάρχει σωστός σχεδιασμός. Έχουν ήδη αρχίσει ερευνητικές προσπάθειες που χρησιμοποιούν τεχνικές ενοποίησης για την επίτευξη διάφορων στόχων (παροχή QoS, βελτιστοποίηση της ισχύος εκπομπής κλπ.). Μέχρι στιγμής δεν έχει γίνει κάποια σημαντική προσπάθεια ώστε να επιτευχθεί ένας ισχυρός μηχανισμός ασφάλειας μέσω της ενοποίησης των επιπέδων. Η συγκεκριμένη διατριβή αποσκοπεί στο να τονίσει πως είναι σημαντική μία προσέγγιση, που να επωφελείται των πλεονεκτημάτων της ενοποίησης, και στον τομέα της ασφάλειας των αδόμητων δικτύων.

Η διαχείριση της ασφάλειας των αδόμητων δικτύων είναι από τη φύση του ένα θέμα που απαιτεί τον συνδυασμό πληροφορίας από πολλά επίπεδα. Ένα πρόβλημα ασφάλειας μπορεί να συμβεί σε οποιοδήποτε επίπεδο του δικτύου και μπορεί να επηρεάσει τη σωστή λειτουργία των πρωτοκόλλων του συγκεκριμένου επιπέδου αλλά και των πρωτοκόλλων των άλλων επιπέδων. Οι ερευνητικές προσπάθειες που υπάρχουν μέχρι αυτή τη στιγμή συγκεντρώνονται στην αντιμετώπιση των προβλημάτων ασφάλειας που υπάρχουν σε κάποιο επίπεδο χωρίς να νοιάζονται τι συμβαίνει στα υπόλοιπα επίπεδα. Όμως υπάρχει σοβαρός κίνδυνος επέκτασης μιας δυσλειτουργίας από ένα επίπεδο και στα υπόλοιπα. Σε μία τέτοια κατάσταση η δημιουργία ενοποιημένων μηχανισμών ανίχνευσης προβλημάτων ασφάλειας και αντιμετώπισης αυτών, είναι μονόδρομος. Σίγουρα η επίτευξη ενός τέτοιου μηχανισμού είναι αρκετά δύσκολη υπόθεση, σύμφωνα με τα όσα λέχθηκαν πιο πάνω. Αρχικά τα πρωτόκολλα των διαφόρων επιπέδων πρέπει να τροποποιηθούν ώστε να συνεργάζονται και να ανταλλάσσουν πληροφορίες. Ο σχεδιασμός των τεχνικών ενοποίησης πρέπει να είναι προσεκτικός γιατί υπάρχει ο κίνδυνος να διευκολύνουμε την επέκταση μιας επίθεσης παρά να την περιορίζουμε και να την καταπολεμάμε. Η συχνή επικοινωνία μεταξύ των πρωτοκόλλων ίσως δημιουργεί επιπλέον ευπάθειες. Συνοψίζοντας θα λέγαμε πως το πεδίο της προστασίας των αδόμητων δικτύων μέσω της ενοποίησης των επιπέδων βρίσκεται σε πολύ αρχικά στάδια. Πρέπει να γίνει κάποια έρευνα στην κατεύθυνση του εντοπισμού του βαθμού επιρροής που υπάρχει μεταξύ των επιπέδων όταν συμβαίνει κάποιο πρόβλημα

ασφάλειας. Έπειτα μέσα από σωστό σχεδιασμό θα προκύψουν νέες καινοτόμες ενοποιημένες τεχνικές που να παρέχουν προστασία σε περισσότερα από ένα επίπεδα, χωρίς βέβαια να δημιουργούν νέες ευπάθειες. Παρακάτω θα περιγράψουμε ένα παράδειγμα όπου εμφανίζεται κάποια δυσλειτουργία στο επίπεδο ελέγχου πρόσβασης στο μέσο. Θα εστιάσουμε κυρίως στην επιρροή που έχει αυτή η δυσλειτουργία στη σωστή λειτουργία της δρομολόγησης.

5.2 Παράδειγμα δυσλειτουργίας στο επίπεδο ελέγχου πρόσβασης στο μέσο

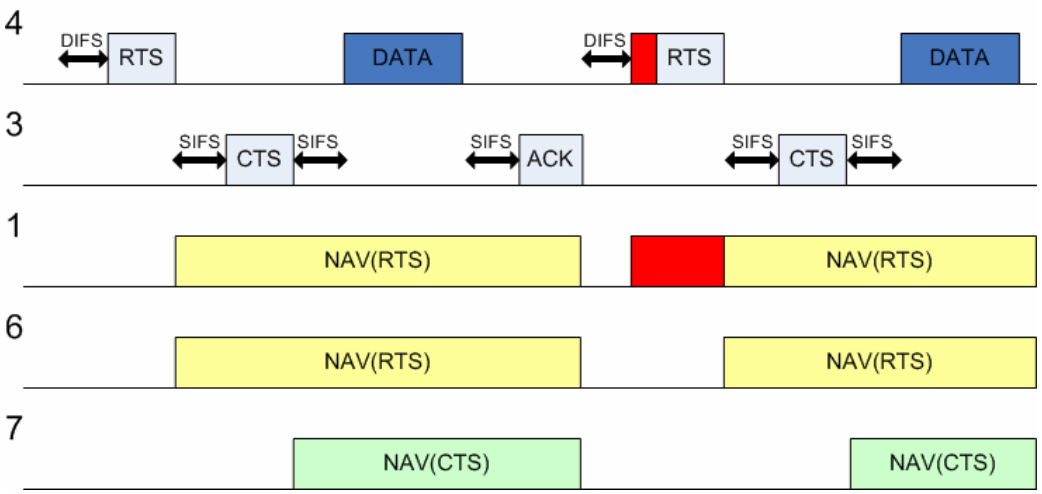
Στο ακόλουθο παράδειγμα περιγράφεται μια δυσλειτουργία που λαμβάνει χώρα στο επίπεδο ελέγχου πρόσβασης στο μέσο. Στην σχήμα 17 φαίνεται ένα ασύρματο αδόμητο δίκτυο. Ο έλεγχος πρόσβασης γίνεται με τη χρήση του μηχανισμού DCF του IEEE 802.11. Για τη δρομολόγηση των πακέτων χρησιμοποιούμε το DSR.



Σχήμα 17: Ένα ασύρματο αδόμητο δίκτυο.

Στο σχήμα 17 μπορούμε να δούμε τις περιοχές εκπομπής των κόμβων 1,3,4. Υποθέτουμε ότι ο κόμβος 4 είναι ένας κακόβουλος κόμβος και για τον λόγο αυτό χρωματίζεται με κόκκινο χρώμα. Υποθέτουμε επίσης ότι όλοι οι υπόλοιποι κόμβοι είναι «υγιείς» και δεν έχουμε προβλήματα κακόβουλης συμπεριφοράς. Η υπόθεσή αυτή μας βοηθάει να βγάλουμε καλύτερα συμπεράσματα όπως θα προκύψει παρακάτω. Χρωματίζουμε και τους κόμβους 1,3 καθώς επηρεάζονται άμεσα από τη συμπεριφορά του κόμβου 4. Ο κόμβος 4 προσπαθεί να αποκτήσει πρόσβαση στο μέσο χρησιμοποιώντας μικρότερα backoff από ότι καθορίζει ο μηχανισμός DCF. Αποτέλεσμα αυτού είναι ο μη δίκαιος διαμοιρασμός του μέσου. Ο κόμβος 4 μεταδίδει πολύ περισσότερες φορές από ότι οι ανταγωνιστικοί του κόμβοι. Οι κόμβοι που βρίσκονται στην περιοχή εκπομπής του 4 αναγκάζονται να σιωπούν για μεγάλα χρονικά διαστήματα. Ας δούμε την περίπτωση όπου οι κόμβοι 1,4 ανταγωνίζονται για να λάβουν πρόσβαση στο μέσο ώστε να μεταδώσουν πληροφορία στον κόμβο 3. Προφανώς ο 4 θα αποκτήσει πρόσβαση στο μέσο πρώτος. Θα συνεχίζει να μεταδίδει στον 3 αναγκάζοντας τον κόμβο 1 να σιωπά.

Στο επίπεδο δρομολόγησης υποθέτουμε ότι δεν υπάρχουν κρούσματα κακόβουλης συμπεριφοράς και όλοι οι κόμβοι συνεργάζονται για τη σωστή δρομολόγηση των πακέτων. Για παράδειγμα, όταν ο κόμβος 0 θέλει να στείλει ένα πακέτο στον κόμβο 8 το DSR πρωτόκολλο αρχικοποιεί ένα αίτημα δρομολόγησης (route request). Το πιο πιθανό μονοπάτι που θα προκύψει είναι το πιο σύντομο, δηλαδή το {0, 1, 3, 7, 8}. Η διαδρομή αυτή προκύπτει χωρίς να ληφθούν υπόψη οι συνθήκες που επικρατούν στο επίπεδο ελέγχου πρόσβασης στο μέσο. Οι ενδιάμεσοι κόμβοι (1, 3, 7) πρέπει να προωθήσουν τα πακέτα για τη σωστή ολοκλήρωση της διαδικασίας της δρομολόγησης. Αρχικά ο κόμβος 0 μεταδίδει ένα πακέτο στον κόμβο 1. Ο κόμβος 1 πρέπει να το προωθήσει στον κόμβο 3. Κατά τη διαδικασία της προώθησης ο κόμβος 1 πρέπει να αποκτήσει πρόσβαση στο μέσο. Δυστυχώς όμως, ο κακόβουλος κόμβος 4 μεταδίδει στον κόμβο 3 την ίδια χρονική στιγμή. Όπως περιγράψαμε πριν ο κόμβος 4 επιλέγει μικρά backoff και έτσι πετυχαίνει να μεταδίδει συνεχώς. Ο κόμβος 1 εξαναγκάζεται να σιωπά για ένα χρονικό διάστημα με αποτέλεσμα η διαδικασία της προώθησης να μην ολοκληρώνεται επιτυχώς. Στο σχήμα 18 φαίνονται κάποιες λεπτομέρειες που αφορούν τον έλεγχο πρόσβασης στο μέσο στην περιοχή του 4.



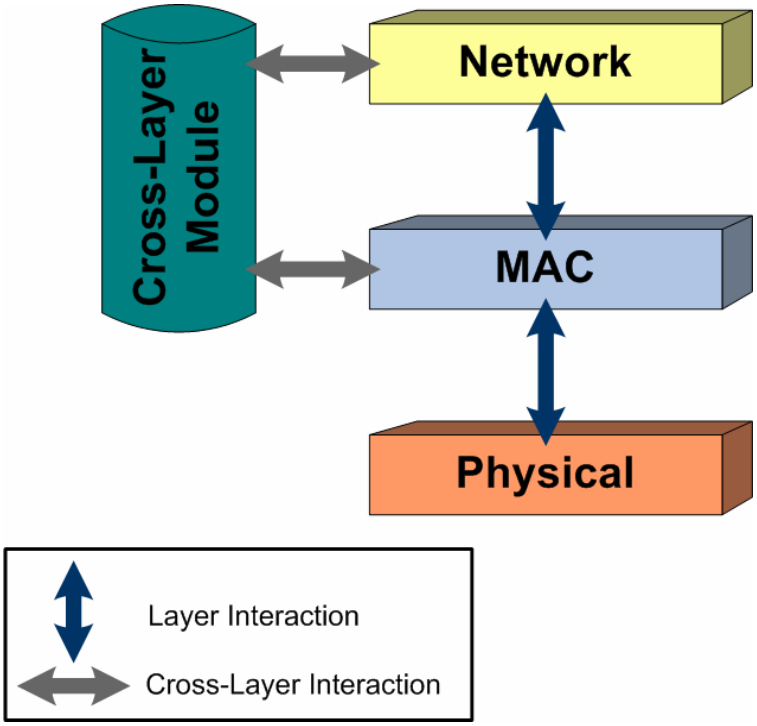
Σχήμα 18: Κακόβουλη συμπεριφορά στο επίπεδο ελέγχου πρόσβασης στο μέσο.

Όπως μπορούμε να δούμε και στο σχήμα οι κόμβοι 6 και 7 αναγκάζονται να σωπάσουν επίσης. Ο κόμβος 6 ακούει το πακέτο RTS από τον 4 και θέτει κατάλληλα το NAV του. Ο κόμβος 7 ακούει το πακέτο CTS που ο κόμβος 3 στέλνει στον 4. Το αποτέλεσμα της πιο πάνω διαδικασίας είναι: Ο κόμβος 1, που έχει αναλάβει να προωθήσει το πακέτο που του έχει στείλει ο 0, δεν στέλνει ACK στον 0 καθώς είναι ανήμπορος να προωθήσει το πακέτο. Πιο σωστά θα λέγαμε ότι ο κόμβος 1 δεν λαμβάνει καθόλου το πακέτο που του στέλνει ο κόμβος 0. Μετά από μικρό χρονικό διάστημα (timeout) ο κόμβος 0 ξαναπροσπαθεί να μεταδώσει το προηγούμενο πακέτο στον κόμβο 1, υποθέτοντας πως το πακέτο χάθηκε και δεν έφτασε ποτέ στον 1. Δυστυχώς, ο κόμβος 1 δεν μπορεί να λάβει πρόσβαση στο μέσο και έτσι βρίσκεται πάλι στην ίδια κατάσταση λόγω της κακόβουλης συμπεριφοράς του 4. Μετά από έναν αριθμό επαναμεταδώσεων (που προβλέπονται από το πρωτόκολλο) ο κόμβος 0 σταματά την προσπάθειά του να μεταδώσει στον 1. Επίσης αναγνωρίζει τον κόμβο 1 σαν κακόβουλο αφού βγάζει το συμπέρασμα πως δεν συνεργάζεται στη διαδικασία της δρομολόγησης. Στην πραγματικότητα όμως ο 1 είναι ένας «υγιής» κόμβος που αναγκάζεται να έχει αυτή τη συμπεριφορά λόγω της δυσλειτουργίας του 4 στο επίπεδο ελέγχου πρόσβασης στο μέσο. Ένα κοινός μηχανισμός που προσπαθεί να ανιχνεύσει κακόβουλες συμπεριφορές στο επίπεδο δρομολόγησης (π.χ. κάνοντας διαχείριση της φήμης των κόμβων , reputation management) καταλήγει στο ότι ο 1 είναι κακόβουλος. Αυτό το συμπέρασμα όμως προκύπτει χωρίς να γίνεται αντιληπτή η δυσλειτουργία στο επίπεδο ελέγχου πρόσβασης

στο μέσο. Εδώ είναι φανερή η προσφορά ενός ενοποιημένου μηχανισμού που θα επιτρέπει τη μετάδοση της πληροφορίας από το επίπεδο ελέγχου πρόσβασης στο επίπεδο δρομολόγησης. Σε περίπτωση που ο κόμβος 0 είχε γνώση για την κακόβουλη συμπεριφορά του 4, αφενός θα δικαιολογούσε τη συμπεριφορά του κόμβου 1 και αφετέρου θα αναγνώριζε τον κόμβο 4 ως κακόβουλο κόμβο. Παρακάτω θα περιγραφεί ένας μηχανισμός που βασίζεται στην ενοποιημένη πληροφορία που παρέχεται από το ένα στρώμα στο άλλο και καταφέρνει επιτυχώς να αντιμετωπίσει τέτοιες καταστάσεις.

5.3 Μηχανισμός προστασίας

Σε αυτή την υποενότητα γίνεται κάποια περιγραφή του προτεινόμενου μηχανισμού για την ανίχνευση κακόβουλων συμπεριφορών μέσω της ενοποίησης μεταξύ των επιπέδων ελέγχου πρόσβασης και δρομολόγησης. Στον συγκεκριμένο μηχανισμό υιοθετείται μία ενοποιημένη προσέγγιση καθώς θεωρούμε πως είναι ο πιο αποδοτικός τρόπος για τον εντοπισμό και την αντιμετώπιση παρόμοιων δυσλειτουργιών με το προηγούμενο παράδειγμα. Αρχικά πρέπει να γίνει κάποιος σχεδιασμός της αλληλεπίδρασης των δύο επιπέδων. Είναι σκόπιμο να διατηρηθεί ο διαχωρισμός των δύο επιπέδων μιας και δεν θα προχωρήσουμε σε μεγάλες τροποποιήσεις των πρωτοκόλλων που δουλεύουν στο κάθε επίπεδο. Αλλά, προφανώς τα πρωτόκολλα μπορούν να ανταλλάσσουν πληροφορίες. Οι πληροφορίες από κάθε επίπεδο διαμοιράζονται με τη χρήσης μιας υπομονάδας ενοποίησης (cross-layer module). Η υπομονάδα συλλέγει τις πληροφορίες από κάθε επίπεδο και τις αποθηκεύει. Οι πληροφορίες αυτές ανανεώνονται περιοδικά καθώς οι κατάσταση λειτουργίας κάθε επιπέδου αλλάζει. Το σχήμα 19 απεικονίζει την αρχιτεκτονική του συστήματος.

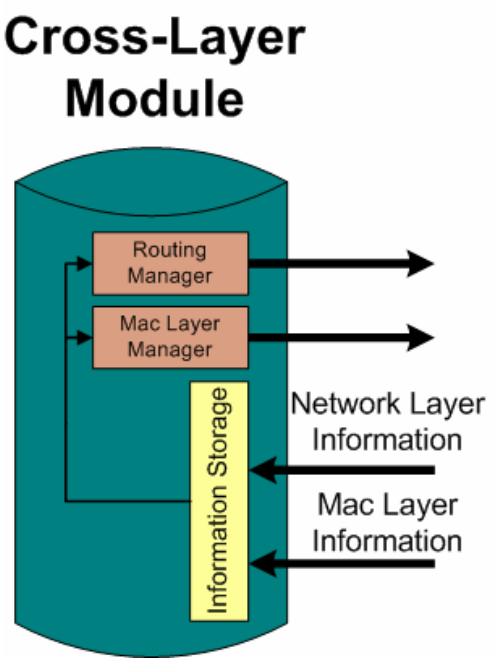


Σχήμα 19: Αρχιτεκτονική του συστήματος προστασίας.

Τα πλεονεκτήματα μιας τέτοιας αρχιτεκτονικής συνοψίζονται παρακάτω:

1. Η απόδοση των πρωτοκόλλων σε κάθε επίπεδο δεν επηρεάζεται αφού διατηρείται ο διαχωρισμός των δύο επιπέδων. Αντίθετα η απόδοσή τους βελτιώνεται καθώς χρησιμοποιούν πληροφορίες από άλλα επίπεδα.
2. Τα πλεονεκτήματα της παραδοσιακής στρωματοποιημένης αρχιτεκτονικής διατηρούνται (αναλύθηκαν πιο πριν).
3. Η επικοινωνία δεν επιβαρύνεται με επιπλέον φόρτο (overhead).
4. Δίνεται η δυνατότητα υλοποίησης πιο προσαρμόσιμων (adaptable) πρωτοκόλλων προς την κατεύθυνση της βελτίωσης της απόδοσης του δικτύου.

Στο σχήμα 20 φαίνεται η δομή της υπομονάδας ενοποίησης των επιπέδων στην οποία στηρίζεται όλη η διαδικασία της ενοποίησης.



Σχήμα 20: Συστατικά της υπομονάδας ενοποίησης των επιπέδων.

Τα απαραίτητα συστατικά της υπομονάδας αυτής είναι αρχικά μία αποθήκη πληροφοριών. Οι πληροφορίες από το επίπεδο ελέγχου πρόσβασης στο μέσο και από το επίπεδο δρομολόγησης αποθηκεύονται για να χρησιμοποιηθούν αργότερα (Information Storage). Οι πληροφορίες αυτές από μόνες τους δεν είναι χρήσιμες. Όμως ο συνδυασμός αυτών ίσως δώσει πολύ καλά αποτελέσματα. Οι διαχειριστές των δύο επιπέδων (MAC Layer Manager, Routing Manager) που είναι ενσωματωμένοι στην υπομονάδα έχουν κάποια υπολογιστική δυνατότητα ώστε να συνδυάσουν τις κατάλληλες πληροφορίες για τη σωστή αντίδραση ενός πρωτοκόλλου σε μία πιθανή επίθεση που μπορεί να λάβει χώρα στο ίδιο επίπεδο ή σε κάποιο άλλο.

Ας υποθέσουμε ότι βρισκόμαστε σε μία κατάσταση όπως αυτή που περιγράφηκε στο προηγούμενο παράδειγμα. Είδαμε πως η δυσλειτουργία του κόμβου 4 επηρεάζει τη διαδικασία της δρομολόγησης. Είναι ενδιαφέρον να αναλύσουμε την αντίδραση του προτεινόμενου συστήματος σε μία τέτοια κατάσταση. Αρχικά αυτό που πρέπει να γίνει είναι η ανίχνευση της κακόβουλης συμπεριφοράς του κόμβου 4 στο επίπεδο ελέγχου πρόσβασης στο μέσο. Η τεχνική της ανίχνευσης αναλύθηκε στην προηγούμενη ενότητα όπου και τεκμηριώθηκε η σωστή λειτουργία της. Υποθέτοντας λοιπόν πως η κακόβουλη συμπεριφορά του κόμβου 4 έχει ανιχνευθεί και έτσι οι κόμβοι που συνδέονται άμεσα με

τον κόμβο 4 (1, 3, 6) είναι γνώστες αυτού. Όπως έγινε αντιληπτό στο παράδειγμα το κυρίως πρόβλημα εντοπίζεται στο γεγονός ότι η διαδικασία της δρομολόγησης δεν έχει γνώση για την κακόβουλη συμπεριφορά του 4. Η άγνοια αυτή δημιουργεί προβλήματα εσφαλμένης ανίχνευσης κακόβουλης συμπεριφοράς (ο κόμβος 1 αναγνωρίζεται ως κακόβουλος κόμβος καθώς δεν προωθεί τα πακέτα που του στέλνονται). Η πληροφορία που καθορίζει πως ο κόμβος 4 είναι κακόβουλος αποθηκεύεται στην υπομονάδα ενοποίησης. Στη συνέχεια ο διαχειριστής του επιπέδου δρομολόγησης χρησιμοποιεί την πληροφορία για να βγάλει σωστά συμπεράσματα. Πιο συγκεκριμένα, ο κόμβος 1 ο οποίος γνωρίζει για το πρόβλημα ασφάλειας χρησιμοποιεί ένα κανάλι ελέγχου (control channel) και ενημερώνει τον κόμβο 0 για την κακόβουλη συμπεριφορά του κόμβου 4. Η πληροφορία που παρέχεται από τον κόμβο 1 αποθηκεύεται στην υπομονάδα ενοποίησης του κόμβου 0. Ο διαχειριστής δρομολόγησης του κόμβου 0 επωφελείται της πληροφορίας αυτής και αντιδρά κατάλληλα. Μία φυσική αντίδραση σε μία τέτοια κατάσταση είναι αφενός η αθώωση του κόμβου 1, ο οποίος είχε αναγνωριστεί πιο πριν ως κακόβουλος, και αφετέρου η έναρξη μιας νέας διαδικασίας δρομολόγησης η οποία θα καταλήξει σε μια νέα διαδρομή η οποία δεν θα επηρεάζεται από την κακόβουλη συμπεριφορά του κόμβου 4. Για παράδειγμα θα μπορούσε να χρησιμοποιηθεί ένα πρωτόκολλο πολλαπλής δρομολόγησης (multi-path) ώστε να υπάρχουν εναλλακτικές διαδρομές από τον κόμβο 0 στον κόμβο 8 και σε μία τέτοια περίπτωση να επιλεγεί η κατάλληλη διαδρομή (π.χ. η διαδρομή {0 ,2, 5,10, 9, 8}). Με αυτό τον τρόπο το σύστημα μας καταφέρνει κατά κάποιο τρόπο να παρακάμψει τη δυσλειτουργία που δημιουργείται και έτσι η διαδικασία της δρομολόγησης ολοκληρώνεται με επιτυχία. Επίσης οι κόμβοι που έχουν ενημερωθεί για την κακόβουλη συμπεριφορά του κόμβου 4 προσπαθούν στο μέλλον να αποφύγουν τη δρομολόγηση μέσω του κόμβου αυτού και τελικά ο κόμβος 4 απομονώνεται από το δίκτυο.

5.4 Αποτελέσματα προσομοίωσης

Στην υποενότητα αυτή υπάρχουν κάποια αποτελέσματα που προέκυψαν από την προσομοίωση του παραδείγματος που αναφέρθηκε πιο πριν. Η προσομοίωση έγινε στον προσομοιωτή δικτύων NS-2 [62] και τα χαρακτηριστικά της προσομοίωσης συνοψίζονται στον παρακάτω πίνακα.

NS2 Simulation Information

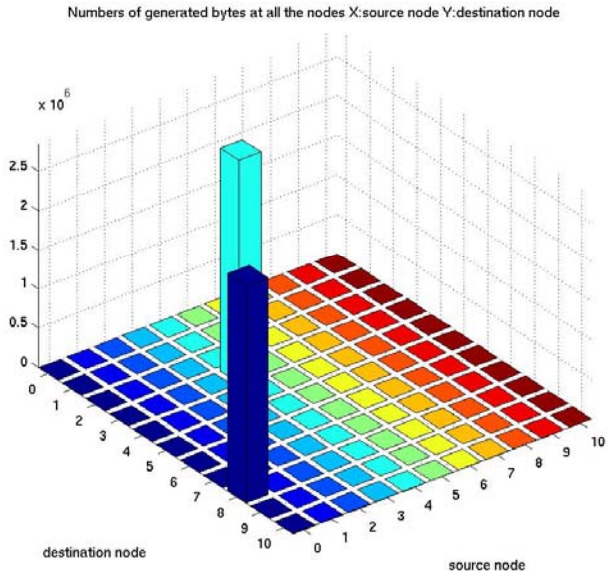
MAC	802.11
Routing	DSR
Traffic	CBR/UDP packets
Channel Capacity	2 Mbps
Packet Size	1000 bytes
Propagation	Free Space
Time Duration	50 sec

Πίνακας 2: Πληροφορίες προσομοίωσης.

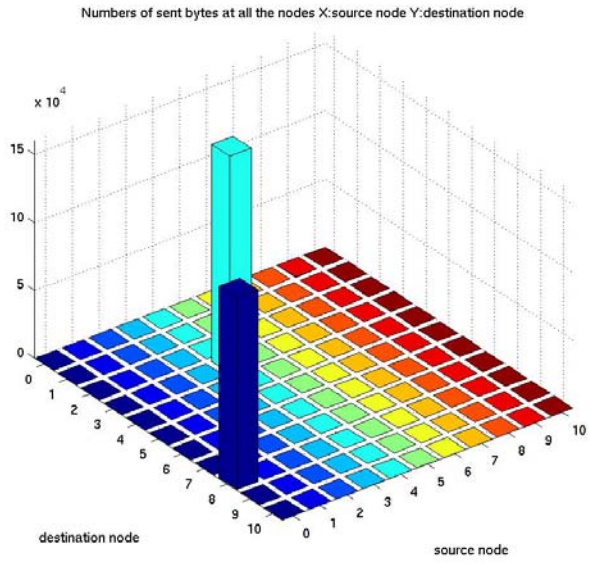
Η τοπολογία του αδόμητου δικτύου που προσομοιώθηκε είναι ίδια με την τοπολογία του δικτύου του παραδείγματος. Υποθέτουμε ότι τα ακόλουθα δύο γεγονότα συμβαίνουν ταυτόχρονα:

1. Ο κόμβος 0 δρομολογεί πακέτα προς τον κόμβο 8.
2. Ο κακόβουλος κόμβος 4 στέλνει συνεχώς πακέτα στον κόμβο 3.

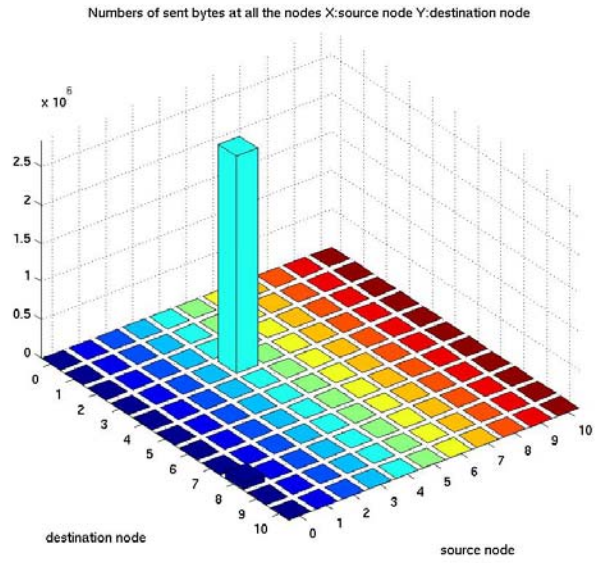
Ο κόμβος 4 χρησιμοποιεί μικρότερα backoff από ότι καθορίζει ο μηχανισμός DCF. Οι υπόλοιποι κόμβοι είναι «υγιείς». Αυτό σημαίνει πως συνεργάζονται για τη σωστή λειτουργία των πρωτοκόλλων. Στα πιο κάτω σχήματα φαίνονται τα δεδομένα που «γεννήθηκαν» σε όλους τους κόμβους καθώς και τα δεδομένα που στάλθηκαν στην περίπτωση «υγιούς» λειτουργίας και στην περίπτωση κακόβουλης συμπεριφοράς.



A)



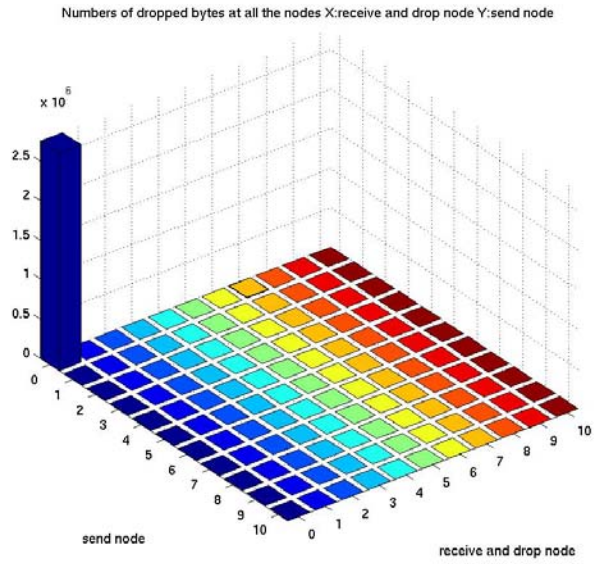
B)



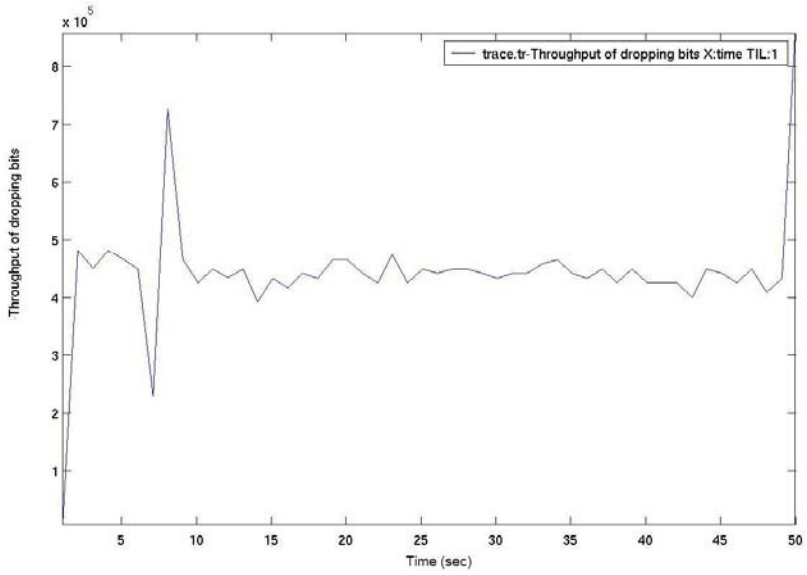
C)

Σχήμα 21: **A)** Δεδομένα που δημιουργήθηκαν σε όλους τους κόμβους, **B)** Δεδομένα που στάλθηκαν στην περίπτωση της κανονικής λειτουργίας των πρωτοκόλλων, **C)** Δεδομένα που στάλθηκαν σε περίπτωση κακόβουλης συμπεριφοράς.

Από τα σχήματα 21Β και 21C φαίνεται η επιρροή της κακόβουλης συμπεριφοράς του κόμβου 4 στη λειτουργία της δρομολόγησης. Όταν δεν υπάρχει κακόβουλη συμπεριφορά από κανένα κόμβο τα δεδομένα των κόμβων 0 και 4 φθάνουν στον προορισμό τους. Στην περίπτωση που ο κόμβος 4 συμπεριφέρεται «άπληστα» (επιλέγοντας μικρότερα backoff) είναι ελεύθερος να στείλει ένα μεγάλο αριθμό δεδομένων σε αντίθεση βέβαια με τον κόμβο 0. Ένας μικρός αριθμός των δεδομένων που στέλνει ο κόμβος 0 φθάνουν στον προορισμό τους λόγω της ανικανότητας του κόμβου 1 να προωθήσει τα πακέτα που λαμβάνει. Ο κόμβος 1, όπως ήδη έχουμε πει, αναγκάζεται να σωπάσει από τη συμπεριφορά του κόμβου 4. Στο σχήμα 22 φαίνονται τα δεδομένα που χάνονται στο δίκτυο όταν υπάρχει δυσλειτουργία. Παρατηρούμε λοιπόν πως ένας μεγάλος αριθμός δεδομένων πετιέται λόγω της άρνησης των ενδιάμεσων κόμβων, που έχουν αναγκαστεί να σιωπούν από τον 4, να τα δεχθούν και να τα προωθήσουν. Τα δεδομένα αυτά προφανώς αφορούν τη δρομολόγηση από τον κόμβο 0 στον κόμβο 8. Στη μετάδοση του κόμβου 4 προς τον κόμβο 3 δεν υπάρχει απώλεια δεδομένων. Αντιθέτως ο κόμβος 4 καταφέρνει να στείλει ένα μεγάλο όγκο δεδομένων στον 3. Στο σχήμα 23 φαίνονται τα δεδομένα που πετιούνται από τον κόμβο 0 (αφού ο 1 δεν μπορεί να τα λάβει) κατά τη διαδικασία της δρομολόγησης.

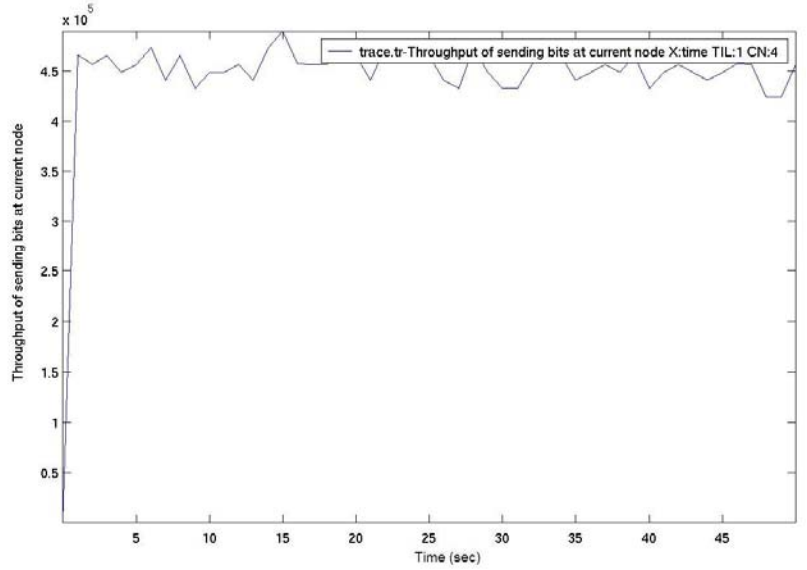


Σχήμα 22: Δεδομένα που πετιούνται κατά τη διαδικασία της δρομολόγησης.



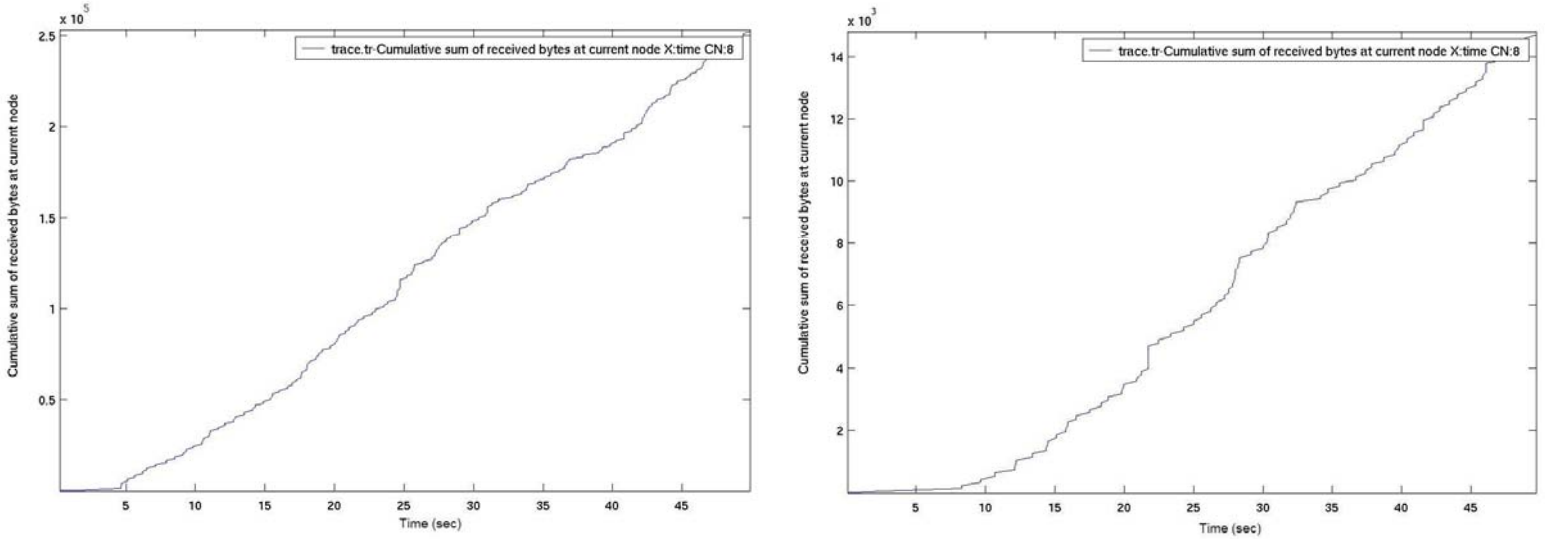
Σχήμα 23: Δεδομένα που πετιούνται από τον κόμβο 0 κατά τη διαδικασία της δρομολόγησης.

Το σχήμα 24 δείχνει τα δεδομένα που στέλνονται από τον κακόβουλο κόμβο 4. Προφανώς ο κόμβος 4 χρησιμοποιώντας μικρότερα backoff καταφέρνει να μεταδίδει συνεχώς. Έτσι καταφέρνει να μεταδώσει μία υπέρογκη ποσότητα δεδομένων σε αντίθεση βέβαια με τους ανταγωνιστικούς του κόμβους.



Σχήμα 24: Δεδομένα που στέλνονται από τον κόμβο 4.

Τέλος στο σχήμα 25 φαίνεται το συνολικό άθροισμα των δεδομένων που φθάνουν τελικά στον κόμβο 8. Στην περίπτωση όπου υπάρχει δυσλειτουργία 25Β η δρομολόγηση των πακέτων παρεμποδίζεται και φθάνουν λιγότερα δεδομένα σε σχέση με τη κανονική λειτουργία του πρωτοκόλλου.



A) **B)**

Σχήμα 25: **A)** Άθροισμα δεδομένων που στάλθηκαν στην περίπτωση της κανονικής λειτουργίας των πρωτοκόλλων (τάξης 10^5), **B)** Άθροισμα δεδομένων που στάλθηκαν σε περίπτωση κακόβουλης συμπεριφοράς. (τάξης 10^3).

Κεφάλαιο 6

Συμπεράσματα - Άξονες Μελλοντικής Έρευνας

Τα συστήματα επικοινωνιών που βασίζονται σε αυτό-οργανωμένες (self-organized) οντότητες που έχουν τη δυνατότητα να δημιουργούν δίκτυα επικοινωνιών χωρίς τη χρήση κάποιας προκαθορισμένης υποδομής αποτελούν ένα καινοτόμο σενάριο που έχει να προσφέρει πολλά στο μέλλον. Θα παίξει σημαντικό ρόλο στην επικοινωνία των ανθρώπων αλλά και στην οικονομία παρέχοντας νέες υπηρεσίες. Σημαντικός παράγοντας όμως για την επιτυχημένη παροχή των υπηρεσιών αυτών είναι να βασίζονται σε ένα δίκτυο που να είναι ανθεκτικό σε πιθανές ενέργειες που προσπαθούν να πλήξουν την ασφάλειά του. Όπως είδαμε η εγκατάσταση ενός ασφαλούς περιβάλλοντος σε καθαρά κατανεμημένα δίκτυα, όπως είναι τα αδόμητα δίκτυα, είναι πολύ δύσκολη υπόθεση. Η παροχή ασφάλειας δυσκολεύει όταν αναφερόμαστε σε «ανοιχτά δίκτυα» (open networks) για την παροχή υπηρεσιών, όπου ο καθένας μπορεί να έχει πρόσβαση (π.χ. πρόσβαση στο internet). Σε μία τέτοια κατάσταση η απουσία της κεντρικοποιημένης διαχείρισης σε συνδυασμό με το γεγονός ότι οι χρήστες είναι ξεχωριστές οντότητες και πολλές φορές δεν ανήκουν στην ίδια αρχή-οργανισμό, είναι επιτακτική η εγκατάσταση κάποιου μηχανισμού που να μπορεί να διαχειρίζεται τους χρήστες αλλά και να μπορεί να αμυνθεί σε επιθέσεις ασφάλειας που μπορεί να εμφανιστούν.

Στη συγκεκριμένη διατριβή έγινε αρχικά μια ανάλυση των ευπαθειών και των ειδικών χαρακτηριστικών των ασύρματων αδόμητων δικτύων που υποδηλώνει ότι η

προσέγγιση που πρέπει να υιοθετηθεί, προς την κατεύθυνση της ενίσχυσης της ανθεκτικότητας των δικτύων αυτών, πρέπει να βασίζεται σε νέες τεχνικές που δεν έχουν καμία σχέση με τις τεχνικές που εφαρμόζονται στα ενσύρματα δίκτυα ή στα δομημένα ασύρματα δίκτυα. Σημασία δόθηκε στις επιπτώσεις που μπορούν να προκαλέσουν κάποιες επιθέσεις που εκμεταλλεύονται τις ευπάθειες αυτές. Η ανάλυση μας εγκολπίζει τα προβλήματα ασφάλειας που λαμβάνουν χώρα σε όλα τα επίπεδα της στοίβας των πρωτοκόλλων του δικτύου, μιας και κρίνεται απαραίτητο πως πρέπει να υπάρχει συνεργασία μεταξύ των πρωτοκόλλων των διαφορετικών επιπέδων για την επιτυχή ανίχνευση και περιορισμό της εξάπλωσης των επιθέσεων. Πιο λεπτομερής ανάλυση πραγματοποιήθηκε για τις ευπάθειες και τις επιθέσεις στα επίπεδα δρομολόγησης (Routing) και ελέγχου πρόσβασης στο μέσο (MAC). Στη συνέχεια έγινε αναφορά στις προσεγγίσεις που υπάρχουν αυτή τη στιγμή στη βιβλιογραφία, οι οποίες αποτέλεσαν το έναυσμα και την κινητήριος δύναμη για τον σχεδιασμό ενός καινοτόμου μηχανισμού προστασίας.

Αρχικά προτάθηκε ένας γενικός μηχανισμός ανίχνευσης και αντιμετώπισης διαφόρων μορφών επιθέσεων που λαμβάνουν χώρα στο επίπεδο ελέγχου πρόσβασης στο μέσο (MAC). Οι επιθέσεις αυτές έχουν σαν απώτερο στόχο την απόλαυση ενός πλεονεκτήματος στο διαμοιρασμό του καναλιού στους χρήστες του δικτύου. Έτσι λοιπόν είναι πολύ συχνό το φαινόμενο κατά το οποίο ένας χρήστης προσπαθεί να επωφεληθεί των ευπαθειών του μηχανισμού διαμοιρασμού του μέσου (IEEE 802.11 – DCF) για να αποκτήσει πρόσβαση στο μέσο με «μη δίκαιο» τρόπο, εις βάρος βέβαια των άλλων χρηστών. Όπως έγινε αντιληπτό από την περιγραφή του DCF ο σχεδιασμός του δεν έγινε με τέτοιο τρόπο ώστε να υπάρχει κάποια ενσωματωμένη (embedded) ανθεκτικότητα σε τέτοιες επιθέσεις. Ο προτεινόμενος μηχανισμός βασίζεται στον ανταγωνισμό που υπάρχει μεταξύ των κόμβων που θέλουν να αποκτήσουν πρόσβαση στο μέσο του δικτύου και λειτουργεί με τέτοιο τρόπο ώστε να μην τροποποιείται το ήδη υπάρχον πρότυπο (IEEE 802.11). Αντιθέτως κάνει χρήση των ειδικών χαρακτηριστικών του IEEE 802.11 δημιουργώντας ένα περιβάλλον «αμεροληψίας» στο διαμοιρασμό του μέσου στους χρήστες. Τα αποτελέσματα των προσομοιώσεων που πραγματοποιήθηκαν δηλώνουν πως ο μηχανισμός καταφέρνει να εντοπίσει επιτυχώς τους κακόβουλους χρήστες και να τους απομονώσει από το δίκτυο.

Στη συνέχεια, έγινε μια μελέτη άξονας της οποίας ήταν η λειτουργία των επιπέδων δρομολόγησης και ελέγχου πρόσβασης στο μέσο. Συγκεκριμένα εστιάσαμε στις επιπτώσεις που μπορούν να προκληθούν σε ένα από τα δύο επίπεδα λόγω μιας δυσλειτουργίας του άλλου επιπέδου. Από τις προσομοιώσεις που πραγματοποιήθηκαν είδαμε πως μία πιθανή δυσλειτουργία στο επίπεδο ελέγχου πρόσβασης στο μέσο, έχει πολύ άσχημες επιπτώσεις στη λειτουργία των πρωτοκόλλων δρομολόγησης. Η ενοποιημένη (cross-layer) οπτική γωνία, με την οποία εξετάσαμε το συγκεκριμένο ζήτημα μας οδήγησε στο σχεδιασμό ενός ενοποιημένου μηχανισμού που κάνει χρήση του μηχανισμού ανίχνευσης επιθέσεων στο επίπεδο ελέγχου πρόσβασης στο μέσο. Βάση της αποδοτικής λειτουργίας του συγκεκριμένου ενοποιημένου μηχανισμού είναι η συνεργασία των πρωτοκόλλων δρομολόγησης και των πρωτοκόλλων ελέγχου πρόσβασης στο μέσο.

Όλες οι προσεγγίσεις που υπάρχουν αυτή τη στιγμή στη βιβλιογραφία ασχολούνται με την αντιμετώπιση συγκεκριμένων επιθέσεων που λαμβάνουν χώρα σε κάποιο επίπεδο της στοίβας των πρωτοκόλλων. Τα συστήματα αυτά δουλεύουν αρκετά καλά για τις επιθέσεις για τις οποίες έχουν σχεδιαστεί αλλά σε περιπτώσεις ύπαρξης άγνωστων επιθέσεων που ίσως λαμβάνουν χώρα σε κάποιο διαφορετικό επίπεδο αλλά επηρεάζουν τη λειτουργία των άλλων επιπέδων υπάρχει πρόβλημα. Σαφώς υπάρχει η ανάγκη υλοποίησης μηχανισμών που να λειτουργούν σε διαφορετικά επίπεδα, να συνδυάζουν τις κατάλληλες παραμέτρους από κάθε επίπεδο, να ανιχνεύουν γνωστές επιθέσεις αλλά και να μπορούν να αναγνωρίζουν νέες επιθέσεις. Ένας τέτοιος μηχανισμός που θα ικανοποιεί όλες αυτές τις απαιτήσεις θα πρέπει να είναι ενσωματωμένος σε κάθε συστατικό (component) του δικτύου. Κάποια επιθυμητά χαρακτηριστικά του μηχανισμού ασφάλειας είναι τα ακόλουθα:

1. Πρέπει να εμποδίζει επιτυχώς τις κακόβουλες επιθέσεις αλλά παράλληλα να έχει τη δυνατότητα να αντιμετωπίζει κάποιες άλλες «αστοχίες» (failures) του δικτύου όπως λανθασμένη διαμόρφωση των κόμβων (node misconfiguration), υπερβολική υπερφόρτωση του δικτύου ή «αστοχίες» στη λειτουργία του δικτύου.
2. Το σύστημα πρέπει να διατηρεί την ανθεκτικότητά του ακόμη κι αν ένα «τείχος αντίστασης» πέσει. Πρέπει δηλαδή, να υπάρχουν πολλά «τείχη αντίστασης» ώστε η απόδοση του συστήματος να μην εξαρτάται σε μεγάλο βαθμό από μια μορφή

αντίστασης σε πιθανές επιθέσεις. Αυτό πρακτικά σημαίνει πως σε περίπτωση που κάποιος κακόβουλος χρήστης εισέλθει στο δίκτυο και ξεπεράσει την αντίσταση κάποιου μηχανισμού ασφάλειας, πρέπει να υπάρχει ένας εναλλακτικός μηχανισμός που θα έχει την ικανότητα να τον ανιχνεύσει.

3. Πρέπει να υπάρχουν τεχνικές κρυπτογράφησης των μηνυμάτων ώστε να προστατεύεται η ακεραιότητα αλλά και να προσδίδεται κάποια αυθεντικοποίηση των χρηστών.
4. Ένα από τα πιο σημαντικά επιθυμητά χαρακτηριστικά του συστήματος είναι η ικανότητα που πρέπει να διαθέτει ώστε να ανιχνεύονται νέες επιθέσεις. Μία πιθανή προσέγγιση που λειτουργεί προς αυτή την κατεύθυνση είναι να οριστούν με ακρίβεια τα όρια μιας νόμιμης και μιας κακόβουλης συμπεριφοράς ενός χρήστη. Σε συνδυασμό με τη συνεργασία που υπάρχει μεταξύ των επιπέδων είναι εφικτή η δημιουργία ενός συστήματος που μπορεί να ανιχνεύει νέες επιθέσεις που προσπαθούν να πλήξουν την ασφάλεια του συστήματος.
5. Στα αδόμητα δίκτυα κανένας κόμβος δεν είναι εξ-αρχής έμπιστος από μόνος του. Αντιθέτως μέσα από τη συνεργασία μεταξύ των κόμβων δημιουργούνται ομάδες κόμβων που θεωρούνται έμπιστες συλλογικά. Στόχος είναι αυτές οι ομάδες να πληθύνουν αλλά και να συνενωθούν ώστε να δημιουργηθεί μια κατάσταση εμπιστοσύνης μέσα στο δίκτυο.
6. Τέλος οι επιθυμητές λειτουργίες του μηχανισμού πρέπει να είναι:
    - Πρόληψη.
    - Ανίχνευση επιθέσεων.
    - Εξακρίβωση κάποιας επίθεσης.
    - Αντίδραση.

Όλα όσα αναφέρθηκαν πιο πάνω αποτελούν αντικείμενο μελλοντικής έρευνας. Πρέπει να συμπληρώσουμε και κάποια ακόμη στοιχεία που πρέπει να ληφθούν υπόψη στον σχεδιασμό ενός μηχανισμού προστασίας τα οποία δεν έχουν ληφθεί υπόψη στις μέχρι τώρα προσεγγίσεις που υπάρχουν στη βιβλιογραφία. Η ετερογένεια που υπάρχει μεταξύ των συσκευών και των δικτύων είναι ένα σημαντικό θέμα που πρέπει να ληφθεί υπόψη στο σχεδιασμό συστημάτων ασφάλειας. Ανάλογα με τις δυνατότητες της κάθε

συσκευής ή του κάθε δικτύου μπορούμε να εφαρμόσουμε κατάλληλες στρατηγικές προστασίας. Τι γίνεται όμως όταν όλα αυτά τα ετερογενή δίκτυα / συσκευές επικοινωνούν μεταξύ τους; Τότε πρέπει να κάνουν την εμφάνισή τους νέοι προσαρμόσιμοι (adaptable) μηχανισμοί οι οποίοι να εκμεταλλεύονται όλες τις δυνατότητες της κάθε συσκευής / δικτύου.

Τα πρωτόκολλα που λειτουργούν σε όλα τα επίπεδα της στοίβας έχουν σχεδιαστεί σε ιδανικές συνθήκες όπου δεν υπάρχουν προβλήματα ασφάλειας. Η υπάρχουσα ερευνητική προσπάθεια προσπαθεί να ενισχύσει τη λειτουργία των πρωτοκόλλων αυτών και να προσδώσει, μέχρι κάποιο βαθμό, ανθεκτικότητα. Η ιστορία έχει δείξει πως τέτοιες τεχνικές δεν είναι τόσο αποδοτικές (κάτι ανάλογο συμβαίνει και στα προβλήματα ασφάλειας που υπάρχουν στα λειτουργικά συστήματα). Με άλλα λόγια δεν καταφέρνουμε πολλά, «μπαλώνοντας» τα ήδη υπάρχοντα πρωτόκολλα. Αντιθέτως, όσο περνούν τα χρόνια και οι προσφερόμενες υπηρεσίες πληθαίνουν, γίνεται συνεχώς όλο και πιο έντονη η ανάγκη σχεδιασμού νέων πρωτοκόλλων νέας γενιάς. Στον τομέα των αδόμητων δικτύων η αρχή έχει γίνει με την ενοποίηση των επιπέδων (cross-layering) όπου προβλέπεται πως θα υπάρχει μεγάλη ερευνητική προσπάθεια. Συνοψίζοντας λοιπόν απαιτούνται νέα πρωτόκολλα με ενσωματωμένες τεχνικές προστασίας που θα λειτουργούν σε συνεργασία μεταξύ τους. Η νέα γενιά των πρωτοκόλλων θα έχει σίγουρα περισσότερες δυνατότητες.

Σχετική Δημοσίευση

George Athanasiou, Leandros Tassiulas and Gregory S. Yovanof, **"Overcoming Misbehavior in Mobile Ad Hoc Networks: an Overview"**, accepted for publication in **ACM Crossroads**, July 2005

Βιβλιογραφία

[1] J. Hubaux, L. Buttyan, and S. Capkun, “The Quest for Security in Mobile Ad Hoc Networks”, in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc), Long Beach, CA, October 2001.

[2] L. Buttyan and J. H. (eds), “Report on a Working Session on Security in Wireless Ad Hoc Networks”, Mobile Computing and Communications Review, vol. 6, November 2002.

[3] S. Basagni et al., Mobile Ad Hoc Networking, IEEE Press and John Wiley & Sons, 2004.

[4] Alvaro A. Cardenas, Svetlana Radosavac, John S. Baras. “Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks”, Technical Report, 2004.

[5] P. Kyasanur and N. Vaidya, “Detection and handling of mac layer misbehavior in wireless networks”, in Proceedings of the International Conference on Dependable Systems and Networks, June 2003.

[6] J.-P. H. Maxim Raya and I. Aad, “Domino: A system to detect greedy behavior in ieee 802.11 hotspots”, in Proceedings of the Second International Conference on Mobile Systems, Applications and Services (MobiSys2004), Boston, Massachussets, June 2004.

[7] J. Konorski, “Multiple Access in Ad-Hoc Wireless LANs with Noncooperative Stations”, In *NETWORKING*, volume 2345 of *LNCS*. Springer, 2002.

[8] J. Konorski, “CSMA/CA Performance under Backoff Attacks: A Game-Theoretic Context”, Conference on Measuring and Evaluation of Computer and Communication Systems (MMB), 2004.

[9] M. Čagalj, S. Ganeriwal, I. Aad, J. P. Hubaux, “On Smart Cheating in CSMA/CA networks”, Proceedings of Infocom, 2005.

[10] P.Papadimitratos and Z.J. Haas. “Secure routing for mobile ad hoc networks.”, In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX. IEEE, January 27-31, 2002.

[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. “Ariadne: A secure ondemand routing protocol for adhoc networks.”, Technical Report Technical Report TR01-383, Department of Computer Science, Rice University, December 2001.

[12] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. “SEAD: secure efficient distance vector routing for mobile wireless adhoc networks.”, In Proceedings of the 4th IEEEWorkshop on Mobile Computing Systems&Applications (WMCSA 2002), IEEE, Calicoon, NY, to appear., June 2002.

[13] B. Dahill, B.N. Levine, E. Royer and C. Shields. “A Secure Routing Protocol for Ad Hoc Networks.”, In *10th International Conference on Network Protocols (ICNP'02)*, 2002.

[14] S. Capkun, L. Buttyan, and J. P. Hubaux. “Self-organized public-key management for mobile ad hoc networks.”, IEEE Transactions on Mobile Computing, page 17, 2003.

[15] H. Luo and S. Lu. “Ubiquitous and robust authentication services for ad hoc wireless networks”, 2000.

[16] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang. “Providing robust and ubiquitous security support for mobile ad-hoc networks.”, In Proceedings of Ninth Internation Conference on Network Protocols (ICNP’01),Riverside, CA, pages 251–260, November 11-14, 2001.

[17] A. Khalili, J. Katz, and W. Arbaugh. “Toward secure key distribution in truly ad-hoc networks.”, In Proceedings of the IEEE Workshop on Security and Assurance in Ad-Hoc Networks (SAINT), 2003.

[18] R.B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh. “Bootstrapping security associations for routing in mobile ad-hoc networks.”, ISR Technical Report 2002-44, Institute for Systems Research, May 2002.

[19] S. Zhu, S. Xu, S. Setia, and S. Jajodia. “Establishing pair-wise keys for secure communication in ad hoc networks: A probabilistic approach.”, Technical Report ISE-TR-03-01, George Mason University, March 2003.

[20] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. “Mitigating routing misbehavior in mobile ad hoc networks.”, In Proceedings of MOBICOM 2000, pages 255–265, 2000.

[21] Sorav Bansal and Mary Baker. “Observation-based cooperation enforcement in ad hoc networks.”, Technical Report, 2003.

[22] Pietro Michiardi and Refik Molva. “CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks.”, Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia., 2002.

[23] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol”, in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002, pp. 226–236.

[24] S. Buchegger and J. Y. Le Boudec, “Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks”, in Proceedings of Tenth Euromicro PDP (Parallel, Distributed and Network-based Processing), Gran Canaria, January 2002, pp. 403 – 410.

[25] H. Miranda and L. Rodrigues. “Preventing selfishness in open mobile ad hoc networks”, In Proceedings of the International Workshop on Mobile Distributed Computing (MDC), pages 440–445, Providence, Rhode Island USA, May 2003. IEEE. (Proceedings the 23nd International Conference on Distributed Computing Systems Workshops).

[26] Krishna Paul and Dirk Westhoff. “Context aware inferencing to rate a selfish node in dsr based ad-hoc networks.”, In Proceedings of the IEEE Globecom Conference, Taipeh, Taiwan, 2002. IEEE.

[27] P. Resnick, R. Zeckhauser, and E. Friedman, “Reputation systems”, in Communications of the ACM, December 2000, pp. 45–48.

[28] E. Friedman and P. Resnick, “The social cost of cheap pseudonyms”, Journal of Economics and Management Strategy, vol. 10, no. 2, pp. 173–199, 2001.

[29] L. Xiong and L. Liu, “Peertrust: Supporting reputation-based trust in peer-to-peer communities.”, in IEEE Transactions on Knowledge and Data Engineering (TKDE). IEEE, 2004.

[30] A. Abdul-Rahman and S. Hailes, “Supporting trust in virtual communities”, in Hawaii International Conference on System Sciences, Maui, Hawaii, January 2000.

[31] K. Aberer and Z. Despotovic, “Managing trust in a peer-2-peer information system”, in Tenth International Conferenceon Information and Knowledge Management CIKM01, Atlanta, GA, November 2001, pp. 310–317.

[32] C. Dellarocas, “Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior”, in ACM Conference on Electronic Commerce, Minneapolis, MN, October 2000, pp. 150–157.

[33] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, “Managing and sharing servents’ reputations in P2P systems”, Knowledge and Data Engineering, IEEE Transactions on, vol. 15, pp. 840–854, July 2003.

[34] B. C. Ooi, C. Y. Kiau, and K.-L. Tan, “Managing trust in peer-to-peer systems using reputation-based techniques”, in The 4th International Conference on Web Age Information Management. LNCS, August 2003, http://xena1.ddns.comp.nus.edu.sg/P2P/waim03.pdf.

[35] L. Liu, S. Zhang, K. D. Ryu, and P. Dasgupta, “R-chain: A self-maintained reputation management system in P2P networks”, in 17th ISCA International Conference on Parallel and Distributed Computing Systems (PDCS). ISCA, September 2004.

[36] S. Kirsner, “Catch me if you can”, 2003. [Online]. Available: http://www.fastcompany.com/magazine/73/kirsner.html

[37] G. David, N. David, O. M. Brian, and T. Douglas, “Using collaborative filtering to weave an information tapestry”, Communications of the ACM, vol. 35, no. 12, pp. 61–70, December 1992.

[38] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S., “Secure routing for structured peer-to-peer overlay networks”, in Fifth Symposium on Operating Systems Design and Implementation, Boston, MA., Winter 2002, pp. 299–314.

[39] J. Camenisch and E. V. Herreweghen, “Design and implementation of the idemix anonymous credential system”, IBM Research Division, Tech. Rep., 2002.

[40] M. Hauswirth, A. Datta, and K. Aberer, “Handling identity in peer-to-peer systems”, in 6th International Workshop on Mobility in Databases and Distributed Systems, in conjunction with the 14th International Conference on Database and Expert Systems Applications, September 2003.

[41] Y. Huang,W. Fan,W. Lee, and P. S. Yu. “Cross-feature analysis for detecting ad hoc routing anomalies.”, In Proceedings of the 23rd International Conference on Distributed Com- -puting Systems (ICDCS 2003), May 2003.

[42] Yongguang Zhang and Wenke Lee. “Intrusion detection in wireless ad-hoc networks.”, In Proceedings of MOBICOM 2000, pages 275–283, 2000.

[43] Levente Buttyan and Jean-Pierre Hubaux. “Stimulating cooperation in self-organizing mobile ad hoc networks.”, Technical Report DSC/2001/046, EPFLDI-ICA, August 2001.

[44] Levente Buttyan and Jean-Pierre Hubaux. “Enforcing service availability in mobile ad-hoc wans.”, In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000.

[45] S. Zhong, Y. Yang, and J. Chen. “Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks.”, Proceedings of Infocom, 2003.

[46] Barath Raghavan and Alex C. Snoeren. “Priority forwarding in ad hoc networks with self-interested parties.”, Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, June 2003.

[47] E. Fratkin, V. Vijayaraghavan, Y. Liu, D. Gutierrez, TM Li, and M. Baker. ”Participation Incentives for Ad Hoc Networks”, http://www.stanford.edu/yl314/ape/paper.ps

[48] Luzi Anderegg, Stephan Eidenbenz, “Ad hoc-VCG:A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks With Selfish Agents”, In Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom’03), San Diego, September 2003.

[49] L. M. S. C. of the IEEE Computer Society. “Wireless lan medium access control (mac) and physical layer (phy) specifications”, IEEE Standard 802.11, 1999 Edition, 1999

[50] Dave B. Johnson and David A. Maltz. “The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network”, (MANET) Working Group, IETF, Version 9, April 2003.

[51] Charles E. Perkins, Elizabeth M. Royer, and Santanu Das. “Ad hoc on demand distance vector (AODV) routing.”, Rfc 3561, IETF, July 2003.

[52] V. Kawadia and P.R. Kumar, “A Cautionary Perspective on Cross Layer Design”, submitted for publication in IEEE Wireless Comm., 2004.

[53] I. Chlamtac, M. Conti, and J. Liu, “Mobile Ad Hoc Networking: Imperatives and Challenges,”, Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 13-64.

[54] U. Kozat, J. Koutsopoulos, L. Tassiulas, “A Framework for Cross-layer Design of Energy-efficient Communication with QoS Provisioning in Multi-hop Wireless Networks”, Proceedings of IEEE INFOCOM04, Hong Kong 2004.

[55] S. Toumpis, A. J. Goldsmith, “Performance, optimization, and cross-layer design of mediaaccess protocols for wireless ad hoc networks”, IEEE International Conference on Communications ICC2003, Volume: 3 , 11-15 May 2003.

[56] A. Maharshi, L. Tong, A. Swami, “Cross-layer designs of multichannel reservation MAC under Rayleigh fading”, IEEE Transactions on Signal Processing, vol. 51, pp. 2054–2067, Aug. 2003.

[57] S, Shakkottai, T.S. Rappaport, P.C. Karlsson, “Cross Layer Design for Wireless Networks”, IEEE Comm. Mag., Vol. 41, No. 10,Oct. 2003.

[58] J. Lopez-Vicario, C. Anton-Haro, “A cross-layer approach to transmit antenna selection for High-Speed Downlink Packet Access”, submitted to IEEE Trans. On Wireless Communications, May 2004.

[59] C. Siva Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, 2004.

[60] Charles E. Perkins, Ad Hoc Networking, Addison-Wesley, 2001.

[61] Theodore S. Rappaport, Wireless Communications: Principles And Practice, Prentice Hall, 2002.

[62] K. Fall and K. Varadhan, “ns notes and documentation”, tech. rep., UC Berkley, LBL, USC/ISI, Xerox PARC, 2002.