ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΑΛΑΜΑΡΑ ΓΕΩΡΓΙΑ ΜΕ/0535

ΙΟΥΝΙΟΣ 2008

ΜΕΛΕΤΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΕΦΑΡΜΟΖΟΝΤΑΙ ΣΕ ΑΥΤΟΦΥΗ ΔΙΚΤΥΑ (AD HOC)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

Αφιερώνεται στους γονείς μου,
στην αδερφή μου και στο Γιώργο…

ΠΕΡΙΛΗΨΗ

Στην παρούσα διπλωματική εργασία γίνεται μια προσπάθεια παρουσίασης κι ανάλυσης των τεχνικών επίθεσης σε ένα ασύρματο δίκτυο ad hoc.

Για διευκόλυνση του αναγνώστη, γίνεται μια εισαγωγή γύρω από γενικότερα θέματα ασφάλειας που περιλαμβάνουν βασικούς τύπους απειλών, αρχιτεκτονική και βασικές αρχές ασφάλειας. Ακολουθεί μια σύντομη αναφορά στο τι είναι ένα ad hoc δίκτυο, ποια είναι τα βασικά του χαρακτηριστικά και πού βρίσκει εφαρμογή. Επίσης παρουσιάζεται και το Bluetooth δίκτυο όσον αφορά την ασφάλειά του καθώς επίσης και διάφοροι τύποι απειλών που δέχεται ένα τέτοιο δίκτυο.

Στη συνέχεια γίνεται μια εκτενής αναφορά στις βασικές αρχές ασφάλειας τόσο των ασύρματων δικτύων γενικά όσο και των δικτύων ad hoc ειδικότερα, περιλαμβάνοντας τις αδυναμίες των ad-hoc δικτύων και τα σημεία στα οποία είναι ιδιαίτερα τρωτά και έπειτα εισάγουμε τον αναγνώστη στην αποκαλούμενη διαχείριση κλειδιού, η οποία όπως παρουσιάζουμε, αποτελεί βασική αρχή για την ασφάλεια ενός ασύρματου δικτύου.

Ακολουθούν οι κατηγορίες τεχνικών επίθεσης external και internal, active και passive που δέχεται ένα δίκτυο ad hoc και αναλύονται τα διάφορα θέματα ασφάλειας των ad-hoc δικτύων με βάση τη δρομολόγηση των μηνυμάτων και των πρωτοκόλλων δρομολόγησης, την προώθηση των δεδομένων και του πρωτοκόλλου MAC. Παρατίθενται και οι διάφοροι τρόποι αντιμετώπισης των παραπάνω, για κάθε περίπτωση ξεχωριστά και παρουσιάζονται και διάφορες προληπτικές λύσεις αλλά και προτεινόμενες λύσεις προς εφαρμογή.

Στο τελευταίο κεφάλαιο, γίνεται αναφορά στα συστήματα ανίχνευσης εισβολών και στην αναγκαιότητα αλλά και χρησιμότητά τους στην ασφάλεια των ασύρματων δικτύων.

Στο τέλος της παρούσας διπλωματικής εργασίας παρατίθεται παράρτημα, στο οποίο ο αναγνώστης μπορεί να βρει τις επεξηγήσεις των διαφόρων εννοιών που θα συναντήσει κατά την ανάγνωση της εργασίας αυτής.

Στόχος της συγκεκριμένης διπλωματικής εργασίας είναι η προσέγγιση των επιθέσεων σε ένα ad-hoc δίκτυο και η αντιμετώπιση των επιθέσεων αυτών, με τέτοιο τρόπο ώστε να γίνουν κατανοητά από τον αναγνώστη.

Ιούνιος 2008

Αθήνα

ΕΥΧΑΡΙΣΤΙΕΣ

Θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή αυτής της διπλωματικής εργασίας κύριο Ξενάκη Χρήστο, για τη βοήθεια και καθοδήγηση που μου προσέφερε και κυρίως για την κατανόηση και την υπομονή του. Τέλος, θέλω να ευχαριστήσω τους γονείς μου για την αγάπη και την υποστήριξή τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

1 ΕΙΣΑΓΩΓΗ

1.1 ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΚΗ ΑΝΑΣΚΟΠΗΣΗ ΑΣΥΡΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η ασύρματη τεχνολογία έχει τις ρίζες της στα τέλη του 19^{ου} αιώνα (1896) με την εφεύρεση του ασύρματου τηλέγραφου από τον Ιταλό Marconi. Η εφεύρεση του Marconi επέτρεπε την αποστολή ραδιοκυμάτων με τη μορφή παύλας και τελείας σε μεγάλες αποστάσεις. Ο κώδικας αυτός έγινε γνωστός με το όνομα κώδικας του Morse (Morse code). Ακολουθώντας τα βήματα του πρωτοπόρου στις ασύρματες επικοινωνίες, ο Αμερικάνος εφευρέτης Reginald Fessenden έκανε πραγματικότητα την 1^{η} ραδιοφωνική μετάδοση δώδεκα χρόνια μετά το 1906.

Η ανάπτυξη και διάδοση του ραδιοφώνου (AM radio) ήταν τέτοια έτσι ώστε το 1902 για παράδειγμα 6 εκατομμύρια ραδιοφωνικές συσκευές είχαν αναπτυχθεί μόνο στις Η.Π.Α. Η ασύρματη τεχνολογία συνέχισε να αναπτύσσεται και να εξαπλώνεται ραγδαία (FM, τηλεόραση) στα χρόνια που ακολούθησαν, ενώ ο δεύτερος παγκόσμιος πόλεμος επιτάχυνε ακόμα περισσότερο τις εξελίξεις. Στα επόμενα χρόνια σταθμός στον τομέα των ασύρματων επικοινωνιών μπορεί να χαρακτηριστεί η εκτόξευση του δορυφόρου Sputnik από την πρώην Σοβιετική Ένωση το 1957.

Στις Η.Π.Α. τα πρώτα ασύρματα αναλογικά τηλέφωνα εμφανίστηκαν τη δεκαετία του ’70 και χαρακτηρίζονταν από πολλούς περιορισμούς συμπεριλαμβανομένου της αδυναμίας περιαγωγής κλήσεων. Η χρήση κελιών περιορισμένης ακτίνας επέτρεψε τελικά την περιαγωγή των κλήσεων και το πρώτο σύστημα αυτού του τύπου αναπτύχθηκε στο Σικάγο το 1979 (εμπορικά το 1984) με το όνομα Advanced Mobile Phone Service (AMPS). Παρόμοια συστήματα κινητής τηλεφωνίας έκαναν την εμφάνισή τους τόσο στην Ιαπωνία όσο και στην Ευρώπη στις αρχές της δεκαετίας του ’80, όπως το Total Access Communication System (TACS) που αποτελεί την Ευρωπαϊκή εκδοχή του AMPS.

Κατά τη διάρκεια της δεκαετίας του ’90, οι ασύρματες τεχνολογίες γνωρίζουν μεγάλη άνθηση. Το 1991, τα πρώτα εμπορικά GSM δίκτυα κάνουν την εμφάνισή τους από τις Σκανδιναβικές χώρες, ενώ ένα χρόνο αργότερα ακολουθεί η Αυστραλιανή ήπειρος. Χαρακτηριστικό επίσης είναι το γεγονός ότι το 1992 υπογράφηκε η πρώτη συμφωνία περιαγωγής πελατών μεταξύ δύο παρόχων που δραστηριοποιούνταν στον Ευρωπαϊκό χώρο: της Vodafone και της Telecom Φινλανδίας.

ΕΙΣΑΓΩΓΗ

Παράλληλα με την ανάπτυξη των ασύρματων υπηρεσιών φωνής, η δεκαετία του ’90 χαρακτηρίζεται από τη διάδοση διαφόρων υπηρεσιών δεδομένων όπως τα συστήματα τηλεειδοποίησης (paging systems). Η τηλεειδοποίηση ως μονόδρομη υπηρεσία, έκανε την εμφάνισή της ήδη από τη δεκαετία του ’60, αλλά η χρήση της περιοριζόταν μόνο στους τομείς της υγείας και της επιβολής του νόμου. Αντιθέτως, τη δεκαετία του ’90 οι πάροχοι ανάλογων υπηρεσιών εξέλιξαν τεχνολογικά τα αμφίδρομα πλέον συστήματά τους, προσθέτοντας διάφορα χαρακτηριστικά και υπηρεσίες, όπως η αποστολή αλφαριθμητικών δεδομένων. Στο χώρο των ασύρματων δικτύων δεδομένων εντάσσεται και το δίκτυο με την ονομασία Cellular Digital Packet Data (CDPD), το οποίο έκανε την εμφάνισή του το 1992 με ρυθμούς μετάδοσης 19,2 Kbps. Το συγκεκριμένο δίκτυο βασιζόταν στο πρωτόκολλο TCP/IP κι εκτός του ότι μπορούσε εύκολα να ολοκληρωθεί με το διαδίκτυο, ήταν δυνατό να χρησιμοποιηθεί κι από συσκευές του AMPS. Είναι χαρακτηριστικό ότι στα τέλη του 20^{ου} αιώνα, το δίκτυο CDPD διέθετε πάνω από 10 εκατομμύρια συνδρομητές στις Η.Π.Α.

Στο πλαίσιο αυτό, η ανάπτυξη και προτυποποίηση ασύρματων τοπικών δικτύων (Wireless Local Area Networks, WLAN) ξεκίνησε το 1990, όταν το γνωστό ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών μηχανικών (IEEE) δημιούργησε την επιτροπή 802.11.

Λίγα χρόνια αργότερα και παράλληλα με την ανάπτυξη ασύρματων δικτύων για επικοινωνία σε μεγάλες αποστάσεις, ξεκίνησε η προσπάθεια σχεδιασμού και υλοποίησης ασύρματων συστημάτων μικρής εμβέλειας. Το πρότυπο Bluetooth αποτέλεσε το πρώτο προϊόν ασύρματου συστήματος μικρής εμβέλειας το 2001.

Ταυτόχρονα με την εξέλιξη της ασύρματης τεχνολογίας και των σχετικών υπηρεσιών, ο Παγκόσμιος Ιστός αποτέλεσε μια πραγματικότητα, που γνώρισε πολύ γρήγορα σχεδόν καθολική αποδοχή. Ξεκινώντας από τις προσπάθειες της εταιρίας Netscape Communications και την ανάπτυξη του πρώτου φιλικού στο χρήστη φυλλομετρητή, οι διαδικασίες περιήγησης και αναζήτησης πληροφοριών στον παγκόσμιο ιστό έγιναν πολύ γρήγορα πραγματικότητα. Ως φυσικό επακόλουθο, η πρώτη προσπάθεια συνδυασμού της ασύρματης τεχνολογίας με το διαδίκτυο, έγινε το 1995 με τη δημιουργία του Wireless Application Protocol forum (WAP). Όμως αυτό το ασύρματο δίκτυο με τη μορφή του WAP ήταν πολύ αργό σε ταχύτητα για να καταφέρει να προσελκύσει μια μεγάλη μερίδα καταναλωτών.

Τελικά το 1999 οι πάροχοι υπηρεσιών άρχισαν να δοκιμάζουν νέες υπηρεσίες βασισμένες στο WAP, όμως παρόλα αυτά το WAP δε γνώρισε την αναμενόμενη

αποδοχή από τους καταναλωτές. Τα πράγματα δεν ήταν καλύτερα τα πρώτα χρόνια ούτε για τις τεχνολογίες Bluetooth και WLAN, αφού δε γνώρισαν τη γρήγορη κι ευρεία αποδοχή που αναμενόταν. Από τη μια μεριά, η γκάμα οι συσκευών Bluetooth ήταν πολύ περιορισμένη και η απόκτησή τους κόστιζε πάρα πολύ, ενώ ταυτόχρονα σημαντικές αδυναμίες στην ασφάλεια των δικτύων WLAN καθυστέρησαν την αποδοχή τους.

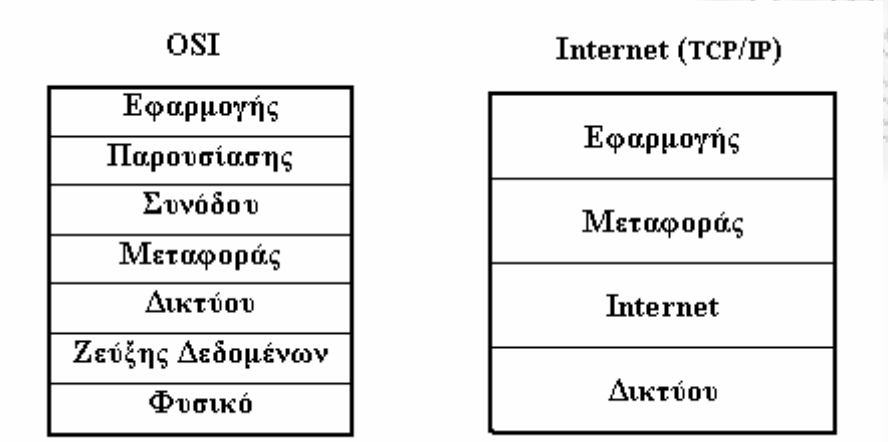
1.2 ΓΕΝΙΚΑ ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ

Είναι γενικά γνωστό πως τα ασύρματα και κινητά δίκτυα επικοινωνιών καλούνται να αντιμετωπίσουν περισσότερες απειλές σε σχέση με τα αντίστοιχα ενσύρματα. Έτσι, γίνεται σαφές ότι η ανάλυση των πιθανών αυτών απειλών αλλά και νέων που ενδέχεται να προκύψουν στο μέλλον πρέπει να αποτελεί σημαντική προτεραιότητα για κάθε ασύρματο σύστημα, δίκτυο ή τεχνολογία.

Η βασικότερη διαφορά μεταξύ ενσύρματων κι ασύρματων δικτύων στον τομέα της ασφάλειας είναι η απουσία οποιουδήποτε ελέγχου πρόσβασης στην περιοχή κάλυψης του ασύρματου δικτύου. Δηλαδή η δυνατότητα του επιτιθέμενου να κινείται μέσα στην περιοχή κάλυψης ανώνυμα επιχειρώντας κατά βούληση μια πλειάδα επιθέσεων, αρκετές από τις οποίες δεν συναντώνται στα ενσύρματα δίκτυα. Ειδικά στην περίπτωση των ασύρματων δικτύων ευρείας περιοχής (Wireless Wide Area Networks, WWAN) το μέσο πρόσβασης στο δίκτυο, δηλαδή το ποιος αποκτάει πρόσβαση στο δίκτυο ή στα δεδομένα που μεταδίδονται, είναι τις περισσότερες φορές αδύνατο να ελεγχθεί. Η μοναδική ίσως γνωστή χωροταξική παράμετρος για ένα ασύρματο δίκτυο είναι τα όρια ή η εμβέλεια του σήματος. Δρόμοι, πάρκα, γειτονικά κτίρια, αυτοκίνητα κ.λ.π. στην περιοχή αυτή μπορούν να προσφέρουν μια πιθανή πύλη εισόδου στον επιτιθέμενο. Είναι χαρακτηριστικό ότι το ασύρματο μέσο μπορεί, πολλές φορές, να εξασφαλίσει απόλυτη ανωνυμία στον επιτιθέμενο προκειμένου αυτός να επιτεθεί σε ενσύρματα δίκτυα π.χ. μέσω ενός ασύρματου σημείου πρόσβασης (Access Point, AP). Οι επιθέσεις αυτού του τύπου κατατάσσονται στην κατηγορία που είναι γνωστή ως illicit network use.

Αξίζει να σημειωθεί ότι το μοντέλο OSI (βλ. Εικόνα 1),στο οποίο βασίστηκε ο σχεδιασμός των ασύρματων δικτύων, δέχεται μια πλειάδα επιθέσεων στα διάφορα επίπεδά του, κυρίως όμως στα επίπεδα δικτύου, ζεύξης δεδομένων και στο φυσικό επίπεδο (physical layer). Οι απειλές στα επίπεδα εφαρμογής (application) και

μεταφοράς (transport) είναι κατά βάση όμοιες με αυτές που αντιμετωπίζουν τα ενσύρματα δίκτυα, με την παρατήρηση ότι στο ασύρματο περιβάλλον αυξάνονται σημαντικά οι πιθανότητες εκδήλωσής τους λόγω της σχέσης των επιπέδων αυτών με τα αμέσως κατώτερά τους.



Εικόνα 1. Τα επίπεδα του μοντέλου OSI και η σχέση τους με τα επίπεδα του απλουστευμένου) TCP/IP μοντέλου

1.2.1 Παθητικού Κι Ενεργού Τύπου Επιθέσεις

Όπως ήδη ειπώθηκε, η απουσία ελέγχων πρόσβασης στο (ραδιο)μέσο δίνει τη δυνατότητα στους επιτιθέμενους να παρακολουθούν (eavesdrop / snoop) οποιοδήποτε ασύρματο δίκτυο *παθητικά* (passively). Σκοπός τους για παράδειγμα μπορεί να είναι η καταγραφή των εκπεμπόμενων δεδομένων με στόχο την εκ των υστέρων αποκωδικοποίηση τους προκειμένου να αποκτήσουν πρόσβαση στις πληροφορίες που ανταλλάχθηκαν μεταξύ των νομίμων χρηστών και του δικτύου. Χαρακτηριστικό είναι το γεγονός πως ο επιτιθέμενος σε αυτή την περίπτωση δεν χρειάζεται τίποτα περισσότερο από μια απλή συσκευή πρόσβασης στο δίκτυο π.χ, μια ασύρματη κάρτα δικτύου, που μπορεί να προμηθευτεί από οποιοδήποτε κατάστημα εμπορίας υπολογιστών, δαπανώντας λίγες δεκάδες ευρώ. Εξάλλου μην ξεχνάμε πως όλες οι ασύρματες συσκευές έχουν τη δυνατότητα να εκπέμψουν και να λάβουν δεδομένα στο ραδιο-μέσο. Με μικρές δε τροποποιήσεις στο υλικό ή στο λογισμικό τους ορισμένες από αυτές είναι ικανές να λαμβάνουν οτιδήποτε εκπέμπεται μέσα στην εμβέλεια τους.

Επιπλέον, τέτοιου είδους συν-ακροάσεις είναι πολύ δύσκολο αν όχι αδύνατο να ανιχνευτούν ή να εμποδιστούν για οποιοδήποτε ασύρματο δίκτυο. Παραδείγματος χάριν, ακόμα και στην περίπτωση των ασύρματων δικτύων που ακολουθούν το πρότυπο IEEE 802.11 ο επιτιθέμενος με τη βοήθεια κατάλληλης κεραίας και πιθανώς

ενισχυτών μπορεί να βρίσκεται αρκετά μακρύτερα (ακόμα και 20 χιλιόμετρα) από το στόχο του π.χ. ένα σημείο ασύρματης πρόσβασης.

Πρέπει να σημειωθεί πως τα σημεία ασύρματης πρόσβασης σε ένα δίκτυο WLAN λειτουργούν όπως ακριβώς οι επαναλήπτες (repeater) και οι κατανεμητές καλωδίων (hub). Αυτό έχει ως αποτέλεσμα όλες οι συσκευές που είναι συνδεδεμένες στο δίκτυο να μπορούν υπό προϋποθέσεις (π,χ. όταν ο προσαρμογέας δικτύου τους τεθεί σε promiscuous λειτουργία) να ακούσουν την κίνηση δεδομένων από τις υπόλοιπες συσκευές.

Σημειώνεται ότι συνήθως η παρακολούθηση του δικτύου δεν αποσκοπεί, τουλάχιστον αρχικά, στην υποκλοπή των δεδομένων που μεταδίδονται, αλλά στη συλλογή διάφορων πληροφοριών, οι οποίες θα επιτρέψουν στον επιτιθέμενο αργότερα ύστερα από σχετική ανάλυση (traffic analysis) να εξαπολύσει την πραγματική (ενεργή, active) επίθεση εναντίον των αδύνατων σημείων που πιθανώς ανακάλυψε. Μερικές από τις πληροφορίας που είναι χρήσιμες σε κάθε επιτιθέμενο ενώ είναι παθητικός ωτακουστής μπορεί να είναι το ποιος χρησιμοποιεί το δίκτυο, η τοπολογία του δικτύου, οι δυνατότητες και τα χαρακτηριστικά των συσκευών, IP και Medium Access Control (MAC) διευθύνσεις, η εμβέλειά του, κλπ. Πολλά επίσης πρωτόκολλα δικτύου είναι πιθανό να μεταδίδουν υπό ορισμένες συνθήκες ή και συνεχώς, απροστάτευτα σε μορφή αρχικού κειμένου (cleartext) ευαίσθητα δεδομένα των χρηστών, όπως είναι το όνομα πρόσβασης (login name) και το συνθηματικό τους (password).

Ακόμα και στην περίπτωση που όλα τα δεδομένα μεταδίδονται μεταξύ των σταθμών του δικτύου κρυπτογραφημένα υπάρχει η δυνατότητα καταγραφής τους με σκοπό για παράδειγμα την εξαντλητική αναζήτηση του κλειδιού κρυπτογράφησης. Ακόμα χειρότερα, πολλοί αλγόριθμοι κρυπτογράφησης παρουσιάζουν εν γένει αδυναμίες.

Εκτός από την παθητική παρακολούθηση των δεδομένων του ασύρματου δικτύου, πολλές φορές οι επιτιθέμενοι εφαρμόζουν τακτικές ενεργού ωτακουστή (active eavesdropping). Παραδείγματος χάριν, ο εισβολέας εκμεταλλεύεται το πρωτόκολλο Address Resolution Protocol (ARP), το οποίο χρησιμοποιείται από τους σταθμούς του δικτύου για να ανακαλύψουν την MAC διεύθυνση άλλων σταθμών, γνωρίζοντας την IP διεύθυνσή τους. Πιο συγκεκριμένα, ο επιτιθέμενος απαντάει στις ARP αιτήσεις διάφορων σταθμών στέλνοντας τη δική του MAC, με αποτέλεσμα τελικώς να λαμβάνει πληροφορίες, οι οποίες απευθύνονταν στους σταθμούς «θύ-

ματα». Η επίθεση αυτή αναφέρεται συχνά ως ARP poisoning. Ο επιτιθέμενος μπορεί επίσης να επαναπροωθεί τα μηνύματα που λαμβάνει στα θύματα του δρώντας ως ενδιάμεσος (man-in-the-middle, MITM).

Οι περισσότερες ενεργού τύπου μέθοδοι επιθέσεων στα ασύρματα δίκτυα προσομοιάζουν με αυτές που αντιμετωπίζονται στα ενσύρματα δίκτυα. Αυτές περιλαμβάνουν μεταξύ άλλων: πρόσβαση στο δίκτυο χωρίς εξουσιοδότηση (unauthorized access), πλαστογράφηση των δεδομένων, της σηματοδοσίας ή ακόμα και υπόδηση ή προσποίηση) της ταυτότητας (πλαστοπροσωπία) άλλων κόμβων του δικτύου (spoofing / masquerading / impersonating), επιθέσεις άρνησης πρόσβασης στο δίκτυο ή παροχής υπηρεσιών (Denial of Service, DoS), επιθέσεις πλημμύρας (flooding), εισαγωγή κακόβουλου κώδικα (malware), κλπ. Είναι επίσης γεγονός πως με την εξέλιξη των ασύρματων δικτύων συνεχώς παρουσιάζονται και νέες παραλλαγές επιθέσεων. Μια από αυτές είναι η λεγόμενη *drive-by-spamming,* Σύμφωνα με αυτή, ο επιτιθέμενος που είναι εγκατεστημένος σε κινούμενο όχημα στέλνει εκατοντάδες χιλιάδες ενοχλητικά μηνύματα spam σε δίκτυα στα οποία έχει καταφέρει να αποκτήσει πρόσβαση.

Μια κοινή επίθεση τύπου spoofing / masquerading / impersonating λαμβάνει χώρα όταν ο επιτιθέμενος είναι σε θέση να χρησιμοποιήσει ένα πλαστό στοιχείο δικτύου που εισάγεται κατάλληλα από αυτόν και ταυτόχρονα να το παρουσιάζει στους υπολοίπους σταθμούς ως απολύτως νόμιμο. Παραδείγματος χάριν, στο σύστημα Global System for Mobile Communication (GSM) όπου μόνο ο συνδρομητής αυθεντικοποιείται στο δίκτυο και όχι το αντίθετο (one-way authentication), ο επιτιθέμενος θα μπορούσε έχοντας στη διάθεση του κατάλληλο εξοπλισμό να παριστάνει την κεραία και το σταθμό βάσης που συνδέονται οι συνδρομητές.

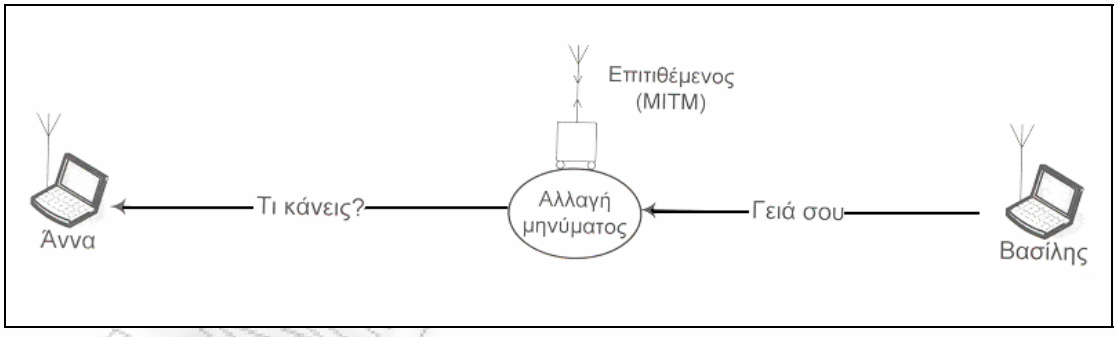
1.2.2 Επιθέσεις Ενδιάμεσου Και Επιθέσεις Μεταβολής Πληροφοριών Ή Λαθροχειρίας

Οι επιθέσεις τύπου Man-in-the-Middle (MITM) μπορούν να εκδηλωθούν με διαφόρους τρόπους σε ένα ασύρματο δίκτυο, έχοντας κύριο στόχο να υπονομεύσουν την ακεραιότητα ή και την εμπιστευτικότητα της συνόδου (session). Παραδείγματος χάριν, ο επιτιθέμενος μπορεί να υποδύεται ένα σταθμό βάσης σε ένα δίκτυο κινητών επικοινωνιών ή ένα σημείο πρόσβασης (AP) σε ένα τοπικό ασύρματο δίκτυο. Με αυτό τον τρόπο ενεργεί ως ενδιάμεσος μεταξύ του χρήστη και του νόμιμου δικτύου, υποκλέπτοντας και πιθανώς μεταβάλλοντας τις πληροφορίες που ανταλλάσσονται

μεταξύ των δύο άκρων και κατόπιν προωθώντας τις κατάλληλα στο νόμιμο αποδέκτη τους, όπως παρουσιάζεται στην Εικόνα 2.

Υπάρχουν τουλάχιστον δύο τρόποι για την μεταβολή ενός μηνύματος. Ο πρώτος θεωρεί την επιτόπου (on-the-fly) αλλαγή του, ενώ ο δεύτερος εφαρμόζει τακτικές καταγραφής του μηνύματος, αλλαγής του και τέλος επαναπροώθησής του σε ύστερο χρόνο (store and forward). Η πρώτη μέθοδος αν και θεωρητικά εφαρμόσιμη είναι στην πράξη πολύ δύσκολο να υλοποιηθεί.

Η μεταβολή των πληροφοριών (data spoofing / modification / tampering) μπορεί να περιλαμβάνει εισαγωγή (injection) παραπλανητικού ή κακόβουλου περιεχομένου και εντολών, αλλά και την τροποποίηση των δεδομένων σηματοδοσίας (control messages) του δικτύου έτσι ώστε να προκαλείται κατάσταση DoS. Για παράδειγμα, ο επιτιθέμενος μπορεί εισάγοντας κατάλληλες εντολές να επιτύχει τη βίαιη αποσύνδεση (disassociation) των χρηστών από το δίκτυο. Επίσης, ο εισβολέας είναι πιθανό να πλημμυρίσει (flood) το δίκτυο με μηνύματα σύνδεσης (connect messages) στα ασύρματα σημεία πρόσβασης, αποκλείοντας με αυτό τον τρόπο τους εξουσιοδοτημένους χρήστες να συνδεθούν. Ο αποτελεσματικότερος τρόπος άμυνας για επιθέσεις αυτού του τύπου είναι η προστασία της ακεραιότητας (integrity) των δεδομένων που μεταδίδονται.



Εικόνα 2. Το αλλοιωμένο μήνυμα εμφανίζεται να έχει σταλεί από το Βασίλη

Στην πράξη μια επίθεση MITM σε ασύρματο περιβάλλον ακολουθεί τα επόμενα βήματα:

1. Ο επιτιθέμενος κρυφακούει για μηνύματα που προέρχονται από τη συσκευή του χρήστη και κατευθύνονται στη κεραία του δικτύου (π.χ. σε κάποιο σημείο πρόσβασης)
2. Μόλις αντιληφθεί κάποιο μήνυμα το αποθηκεύει

3. Αλλοιώνει το άθροισμα ελέγχου (checksum) του πλαισίου δεδομένων του μηνύματος, το οποίο χρησιμοποιείται από τον δέκτη προκειμένου να αντιληφθεί σφάλματα στα δεδομένα. Αυτό θα αναγκάσει το σημείο πρόσβασης να αγνοήσει το μήνυμα ως λανθασμένο (αλλοιωμένο). Η αλλοίωση μπορεί να γίνει εκπέμποντας μια ξαφνική ριπή θορύβου.
4. Παραλλάσσει ένα μήνυμα επιβεβαίωσης (Acknowledgement, ACK.) λήψης τοποθετώντας τη διεύθυνση του AP και ακολούθως το αποστέλλει στον σταθμό του χρήστη. Έτσι ο τελευταίος πιστεύει ότι το μήνυμα που έστειλε παρελήφθη κανονικά από το AP.
5. Επανασυνθέτει το αρχικό μήνυμα - υπολογίζοντας το άθροισμα ελέγχου - και το προωθεί στο AP. Το τελευταίο πιστεύει πως το μήνυμα προέρχεται από το σταθμό του χρήστη.
6. Αναμένει για μήνυμα επιβεβαίωσης από το AP προς το σταθμό του χρήστη και μόλις το αντιληφθεί εκπέμπει ριπή θορύβου έτσι ώστε το μήνυμα να αγνοηθεί από το δέκτη. Με αυτόν τον τρόπο ο δέκτης δεν θα λάβει δύο επιβεβαιώσεις για το ίδιο μήνυμα.

Οι πληροφορίες που μπορεί να μεταδίδονται στο πλαστό σημείο πρόσβασης είναι δυνατό να περιλαμβάνουν αιτήσεις αυθεντικοποίησης, μυστικά κλειδιά, κλπ. αλλά και απλή κίνηση δεδομένων που καταγράφεται από τον επιτιθέμενο με σκοπό την αποκάλυψη π.χ. του WEP (Wired Equivalency Privacy) κλειδιού. Οι επιθέσεις αυτού του τύπου σχετίζονται με το επίπεδο συνδέσμου μεταφοράς δεδομένων (data link layer) του OSI μοντέλου. Επιπλέον, ο επιτιθέμενος μπορεί να διαθέτει ένα φορητό υπολογιστή με δύο προσαρμογείς δικτύου (Network Interfaces, NICs) έτσι ώστε ο ένας να χρησιμοποιείται μεταξύ του πλαστού AP και του υπολογιστή του, ενώ ο άλλος είναι επιφορτισμένος με το να προωθεί τα μηνύματα που λαμβάνονται από τον πρώτο στο νόμιμο AP (μεταβάλλοντας κατάλληλα τη MAC διεύθυνση πηγής). Εννοείται ότι η ίδια διαδικασία επαναλαμβάνεται και προς την αντίθετη κατεύθυνση. Σημειώστε επίσης ότι σε αυτή την περίπτωση ο επιτιθέμενος δεν χρειάζεται να γνωρίζει κανένα μυστικό κλειδί, γιατί οι διευθύνσεις MAC που χρειάζεται να μεταβάλλει δεν είναι κρυπτογραφημένες.

1.2.3 Επιθέσεις Παρεμβολών Ή Παρακώλυσης Επικοινωνιών

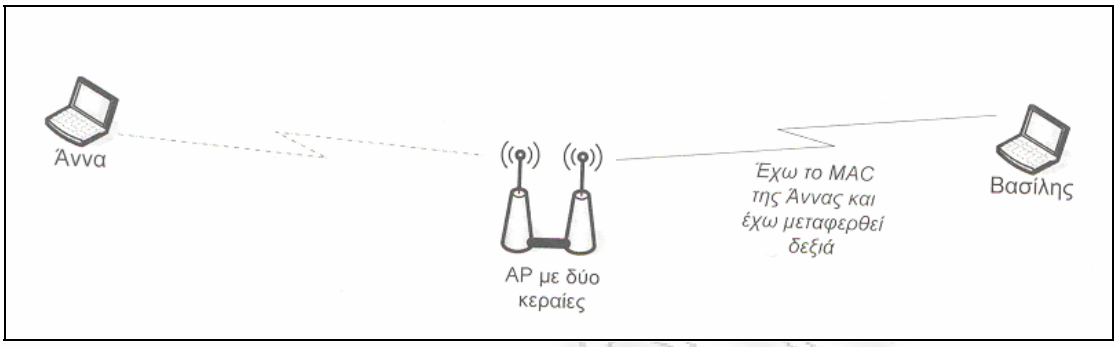
Παρακώλυση ή παρεμπόδιση των επικοινωνιών μέσω παρεμβολών (jamming) έχουμε στην περίπτωση που το σήμα του πομπού, του δέκτη ή του σημείου ασύρματης πρόσβασης (π.χ. κεραία) σε μια ασύρματη ζεύξη παρεμποδίζεται ή αλλοιώνεται εξαιτίας κάποιων παρεμβολών ή θορύβων (noise) που προκαλούνται ηθελημένα ή αθέλητα. Το αποτέλεσμα της επίθεσης jamming είναι να καταστεί το κανάλι επικοινωνίας ακατάλληλο. Γι' αυτό το λόγο θεωρείται κατά βάση επίθεση που εντάσσεται στη γενική κατηγορία DoS καν εκδηλώνεται συνήθως στο φυσικό επίπεδο (PHY layer) του OSI μοντέλου. Το εύρος (range) της περιοχής παρεμβολών εξαρτάται άμεσα από την ισχύ του πομπού που έχει στη διάθεση του ο επιτιθέμενος. Όπως είναι φανερό οι επιθέσεις αυτού του τύπου είναι ιδιαίτερα προσιτές στα ασύρματα δίκτυα σε αντίθεση με το σύνηθες περιβάλλον ενός ενσύρματου δικτύου.

Προκειμένου ο επιτιθέμενος να εξαπολύσει μια επίθεση παρεμβολής και παρακώλυσης επικοινωνιών σε ένα ασύρματο δίκτυο θα πρέπει πρώτα να αναλύσει το φάσμα συχνοτήτων που αυτό χρησιμοποιεί και κατόπιν να εκπέμψει με τη βοήθεια κάποιας σχετικής συσκευής ένα ισχυρό σήμα που συγκρούεται, παρεμποδίζει ή παρεμβαίνει (interfere) στις συχνότητες που το δίκτυο θύμα χρησιμοποιεί.

Η εισαγωγή θορύβου είναι ακόμα μια αποτελεσματική τεχνική. Ο εισαγόμενος στο δίκτυο θόρυβος πρέπει να είναι χαμηλής εντάσεως (amplitude) έτσι ώστε να προκαλέσει το φαινόμενο θανάτου από επανειλημμένη προσπάθεια (Death by Retry, DBR). Αυτό συμβαίνει όταν ο δέκτης ζητάει συνεχώς την επανάληψη αποστολής των μηνυμάτων, που σκοπίμως δεν εκπέμπονται όπως πρέπει, με αποτέλεσμα να εμπλακεί σε κατάσταση ατέρμονα βρόγχου. Από την άλλη πλευρά, ένας απλός τρόπος για την παρακώλυση των επικοινωνιών είναι η συνεχής πλημμύρα με άχρηστα δεδομένα των σημείων πρόσβασης έτσι ώστε αυτά να υπερφορτωθούν και να μην είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες. Παραδείγματος χάριν, μια επίθεση στο επίπεδο δικτύου (network layer) αυτή τη φορά, μπορεί να εκδηλωθεί πλημμυρίζοντας το δίκτυο με πλήθος αιτήσεων ping (ping flood atlack), αμέσως μόλις ο επιτιθέμενος αποκτήσει πρόσβαση σε ένα AP.

Επίσης, μια κοινή τεχνική για την εκδήλωση επίθεσης παρεμπόδισης επικοινωνιών που εκδηλώνεται όμως στο επίπεδο σύνδεσης δεδομένων (data link layer) του OSI μοντέλου είναι αυτή που εκμεταλλεύεται την ύπαρξη κεραιών πολλαπλής λήψης (diversity antennas) σε ένα AP (βλ. Εικόνα 3). Ας υποθέσουμε ότι ένα AP διαθέτει δύο κεραίες. Η πρώτη (1) καλύπτει την περιοχή αριστερά, ενώ η δεύτερη (2) την περιοχή δεξιά του AP. Ως αποτέλεσμα, οι χρήστες Α και Β

ευρισκόμενοι αριστερά και δεξιά του AP θα συνδεθούν στις κεραίες 1 και 2 αντίστοιχα. Ακολούθως, ο Β αλλάζει τη MAC διεύθυνση του σε αυτή του Α και μέσω ενός ενισχυτή ενισχύει το σήμα του έτσι ώστε να είναι τουλάχιστον ίσο ή καλύτερα δυνατότερο οπό αυτό του Α. Τότε ο Α αποκλείεται από την επικοινωνία με το AP και για όσο διάστημα ο Β εξακολουθεί να εκπέμπει στη συγκεκριμένη MAC.



Εικόνα 3. Επίθεση τύπου DoS στο επίπεδο σύνδεσης δεδομένων

Επιπλέον, οι περισσότεροι χρήστες δεν έχουν τρόπο να αντιληφθούν ότι μια επίθεση παρακώλυσης είναι σε εξέλιξη. Γι' αυτούς η συγκεκριμένη επίθεση εμφανίζεται σαν απουσία δικτύου και υπηρεσιών, όπως στην περίπτωση των κινητών τηλεφώνων όταν δεν υπάρχει δίκτυο. Οι διαχειριστές του ασύρματου δικτύου είναι τις περισσότερες φορές πολύ δύσκολο να ανακαλύψουν την πηγή των παρεμβολών γιατί κάτι τέτοιο απαιτεί φυσική επιτήρηση του χώρου. Τέλος, η απόκτηση μιας συσκευής παρεμβολών από το Διαδίκτυο για παράδειγμα δεν απαιτεί ιδιαίτερο κόστος.

1.3 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ ΚΙ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Παραδοσιακά, όπως παρουσιάζεται στην Εικόνα 4, μια αρχιτεκτονική ασφαλείας περιλαμβάνει δύο διακριτά τμήματα ή ζώνες: την έμπιστη (trusted) και τη μη έμπιστη (untrusted) ζώνη ασφαλείας. Η έμπιστη ζώνη ορίζει την περιοχή στην οποία υπάρχει πλήρης έλεγχος σχετικά με το ποιος έχει πρόσβαση, σε ποιες υποπεριοχές ακριβώς και υπό ποιο καθεστώς (π.χ. τι είδους ενέργειες είναι εξουσιοδοτημένος να κάνει). Με άλλα λόγια είναι μια πλήρως εποπτευόμενη και προστατευμένη ζώνη, όπως για παράδειγμα το σπίτι μας το βράδυ όπου έχει τεθεί σε λειτουργία ο συναγερμός ή το εσωτερικό τοπικό ενσύρματο δίκτυο της επιχείρησής μας. Κάποιος μπορεί με σχετική βεβαιότητα να υποθέσει ότι δεν υπάρχουν ή είναι πολύ δύσκολο να παρεισφρήσουν παρείσακτοι στη συγκεκριμένη περιοχή.

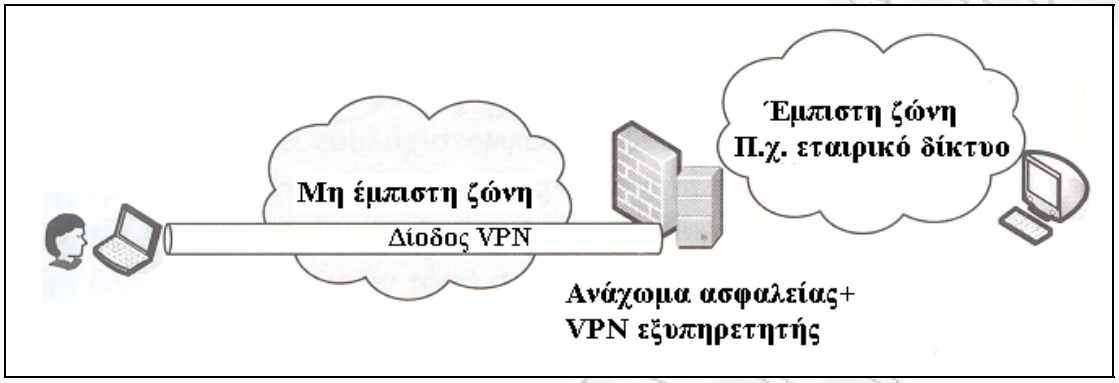
Από την άλλη μεριά, στη μη έμπιστη ζώνη, καραδοκούν κάθε είδους κακόβουλοι χρήστες που ενδέχεται να εξαπολύσουν μια πλειάδα επιθέσεων στα δεδομένα που μεταδίδονται μέσω αυτής. Κλασσικό παράδειγμα μη έμπιστης ζώνης, αποτελεί το διαδίκτυο. Για οποιοδήποτε δίκτυο, τα προβλήματα ανακύπτουν ακριβώς στο σημείο διεπαφής των δύο αυτών ζωνών. Δηλαδή στο σημείο που οι δυο παραπάνω ζώνες συναντώνται. Τυπικά στο σημείο αυτό, οι διαχειριστές του δικτύου τοποθετούν ένα ανάχωμα ασφαλείας (firewall) προκειμένου να προστατέψουν την έμπιστη ζώνη από αυτούς που βρίσκονται εκτός αυτής.

Εικόνα 4. Βασική αρχιτεκτονική ασφάλειας

Αλλά και πάλι, σημαντικά ζητήματα ασφαλείας προκύπτουν, όταν εξουσιοδοτημένοι χρήστες που βρίσκονται στη μη έμπιστη ζώνη, επιθυμούν να προσπελάσουν την έμπιστη. Παραδείγματος χάριν, οι αντιπρόσωποι μιας εταιρίας χρειάζεται να επικοινωνούν τακτικά με το εταιρικό (έμπιστο) δίκτυό τους ενώ βρίσκονται μακριά από αυτό. Μια λύση στο συγκεκριμένο πρόβλημα παρέχεται στο επίπεδο δικτύου του OSI μοντέλου με την ανάπτυξη εικονικών ιδιωτικών δικτύων (Virtual Private Network, VPN), όπως χαρακτηριστικά παρουσιάζεται στην Εικόνα 5. Είναι γνωστό πώς ένα VPN εκτείνει το έμπιστο τμήμα του δικτύου με τη δημιουργία έμπιστων, κρυπτογραφημένων διόδων (tunnels) μέσω των οποίων μπορούν να μεταφέρονται με ασφάλεια τα δεδομένα των χρηστών. Κάποιος θα μπορούσε να πει πως ένα VPN μοιάζει με τη μεταφορά πόσιμου νερού από ένα σημείο σε ένα άλλο μέσω ενός σωλήνα που εκτείνεται μέσα σε μια μολυσμένη περιοχή.

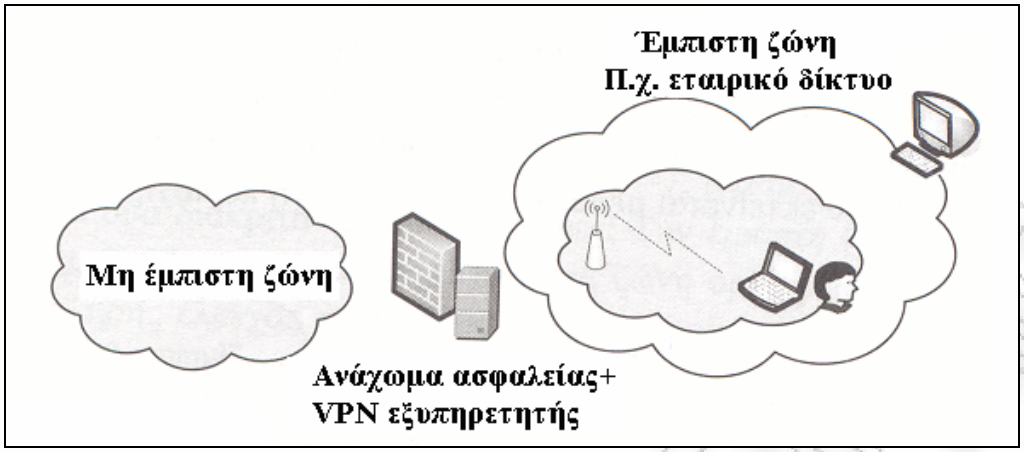
Όλα τα παραπάνω λειτουργούν σχετικά καλά σε ενσύρματο περιβάλλον. Ισχύει το ίδιο όμως και για τα ασύρματα και κινητά δίκτυα επικοινωνιών; Και βέβαια το κρίσιμο ερώτημα σε σχέση με την παραπάνω διττή αρχιτεκτονική έμπιστης και μη έμπιστης ζώνης είναι το που ακριβώς πρέπει να ενταχθούν τα ασύρματα δίκτυα. Θα

πρέπει να τα τοποθετήσουμε μέσα στην έμπιστη ζώνη ή στη μη έμπιστη, πίσω δηλ. από το ανάχωμα ασφαλείας; Η συγκεκριμένη ερώτηση μπορεί να απαντηθεί με δυο τρόπους και είναι βασικά θέμα των ιδιαίτερων συνθηκών που έχουμε να αντιμετωπίσουμε αλλά και διάφορων άλλων επιλογών.



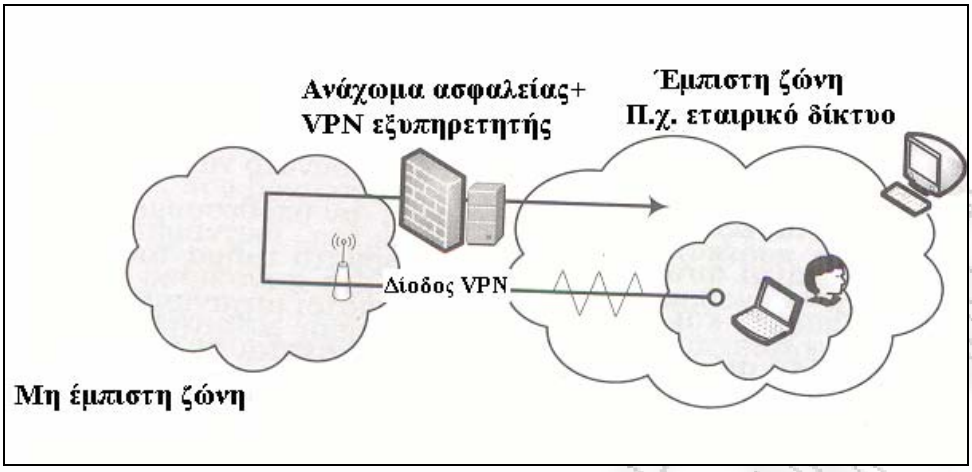
Εικόνα 5. Δημιουργία VPN διόδου για απομακρυσμένους χρήστες

Ορισμένες φορές είναι ξεκάθαρο ότι ένα ασύρματο δίκτυο πρέπει να θεωρείται ότι ανήκει στη μη έμπιστη ζώνη. Παραδείγματος χάριν, τα έμπιστα κινητά επικοινωνιών και τα WLAN που αναπτύσσονται σε δημόσιους χώρους, όπως ένα αεροδρόμιο ή ένας σιδηροδρομικός σταθμός ή ένα ξενοδοχείο ανήκουν σε αυτή την κατηγορία. Από την άλλη μεριά, ακόμη και το ασύρματο δίκτυο του σπιτιού ή της επιχείρησής μας, μπορεί να θεωρηθεί ότι βρίσκεται στη μη έμπιστη ζώνη, αφού το σήμα ταξιδεύει εκτός του κτιρίου κι εύκολα είναι δυνατό να παρακολουθηθεί από αυτούς που βρίσκονται έξω από αυτό. Επιπλέον, αν υποθέσουμε ότι τα ασύρματα σημεία πρόσβασης είναι συνδεδεμένα στο ενσύρματο τμήμα του δικτύου μας, όπως συνήθως συμβαίνει και δεν υπάρχουν αξιόπιστοι μηχανισμοί ασφαλείας μπορούμε να πούμε ότι το σύνολο του δικτύου μας βρίσκεται σε κίνδυνο. Η κατάσταση αυτή παρουσιάζεται στην Εικόνα 6.



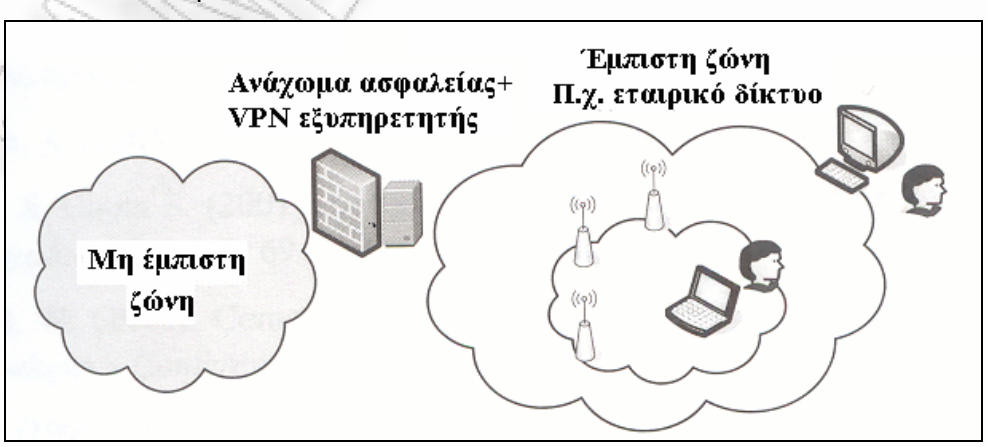
Εικόνα 6. Ασύρματη μη έμπιστη ζώνη στα πλαίσια προστατευμένου δικτυακού τομέα

Η προφανής απάντηση σε αυτές τις περιπτώσεις είναι η αντιμετώπιση όλων των χρηστών του ασύρματου τομέα δικτύου ως να ήταν απομακρυσμένοι χρήστες. Δηλ. να καταστήσουμε τη χρήση VPN γι' αυτούς υποχρεωτική παρά το ότι μπορεί να βρίσκονται στο γραφείο τους μέσα στο κτίριο της επιχείρησης μαζί με όλους τους υπολοίπους. Η επιλογή αυτή μεταφράζεται στα εξής: η κίνηση των δεδομένων των συγκεκριμένων χρηστών πρέπει να τυγχάνει επεξεργασίας από το VPN λογισμικό πριν ακόμα διοχετευτεί στο ασύρματο δίκτυο. Κατόπιν, μέσω των ασύρματων σημείων πρόσβασης, τα δεδομένα είναι απαραίτητο να περνούν πρώτα από το ανάχωμα ασφαλείας κι έπειτα μέσω του VPN εξυπηρετητή πριν τελικά να φτάσουν στον προορισμό τους. Προσοχή όμως! Όπως παρουσιάζεται στην Εικόνα 7, τα ασύρματα σημεία πρόσβασης πρέπει να συνδέονται στο ενσύρματο δίκτυο σε κατάλληλη διεπαφή εκτός της έμπιστης ζώνης, δηλ. πριν το ανάχωμα ασφαλείας. Η συγκεκριμένη λύση χαρακτηρίζεται από όλα τα γνωστά μειονεκτήματα των VPN, όπως για παράδειγμα αυξημένα διαχειριστικά κόστη π.χ. σε VPN λογισμικό, αυξημένη πολυπλοκότητα και μείωση της ταχύτητας του δικτύου, κ.λ.π.



Εικόνα 7. Ανάπτυξη VPN συνδέσεων για τους χρήστες του ασύρματου δικτυακού τομέα

Η δεύτερη επιλογή είναι να αντιμετωπίζουμε ένα ασύρματο δίκτυο ως αναπόσπαστο τμήμα της έμπιστης ζώνης. Βέβαια, αν και κάτι τέτοιο είναι αρκετά δύσκολο να πραγματωθεί στην περίπτωση των κινητών ασύρματων δικτύων επικοινωνιών και των ασυρμάτων δικτύων ευρείας περιοχής (W-WLAN) στα οποία το παρεχόμενο επίπεδο ασφάλειας έγκειται κυρίως στον πάροχο της υπηρεσίας, είναι αρκετά εφικτό για τα δίκτυα τύπου WLAN. Κινούμενοι προς την κατεύθυνση αυτή, πρέπει να καταστήσουμε τον ασύρματο τομέα του δικτύου μας πραγματικά ασφαλή, ώστε να παρέχει τουλάχιστον το ίδιο επίπεδο ασφαλείας με το ενσύρματο τμήμα της έμπιστης ζώνης. Βεβαίως, η προσέγγιση αυτή γεννά ένα ακόμη ερώτημα: είναι οι διάφοροι μηχανισμοί ασφαλείας που προσφέρονται για τα ασύρματα και κινητά δίκτυα επικοινωνιών τόσο αποτελεσματικοί ώστε να μπορούν να εγγυηθούν σε υψηλό βαθμό μια λύση αυτής της μορφής; Αν ναι, τότε ασφαλώς και έχουμε τη δυνατότητα να εντάξουμε τα ασύρματα δίκτυα στην έμπιστη ζώνη (βλ. Εικόνα 8), υποθέτοντας ότι όλοι οι υπόλοιποι παράγοντες (διαχειριστές, χρήστες, κ.λ.π) συνεργάζονται προς την ίδια κατεύθυνση.



Εικόνα 8. Οι ασύρματοι τομείς δικτύου θεωρούνται αναπόσπαστα τμήματα της έμπιστης ζώνης

1.4 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

Στην παρούσα ενότητα θα αναπτύξουμε εν συντομία και με απλά λόγια τις βασικές αρχές ασφαλείας, οι οποίες πρέπει να ακολουθούνται οπό όλους τους εμπλεκόμενους σε οποιοδήποτε δίκτυο και πολύ περισσότερο στα δίκτυα ασύρματων και κινητών επικοινωνιών. Από την πιστή τήρηση των παρακάτω αρχών εξαρτάται σε μεγάλο βαθμό εάν η πολιτική ασφαλείας μας και οι πρακτικές της θα έχουν την αναμενόμενη επιτυχία ή όχι.

Α. ***Μην επικοινωνείς με αγνώστους:*** Μιλώντας για ασφάλεια αυτή η φράση σημαίνει ότι πρέπει να είσαι απολύτως βέβαιος (ή τουλάχιστον σχεδόν βέβαιος) για την ταυτότητα μιας συσκευής ή / και ενός χρήστη πριν επικοινωνήσεις μαζί του. Στην πραγματικότητα, όλες οι παραδοσιακές μέθοδοι επικοινωνίας βασίζονται σε κάποιου είδους αναγνώριση της ταυτότητας του συνομιλητή. Παραδείγματος χάριν, όταν μιλάμε στο τηλέφωνο αναγνωρίζουμε το συνομιλητή από τη φωνή του αλλά και έμμεσα από το περιεχόμενο των πληροφοριών που μεταδίδει. Στην περίπτωση των ασύρματων ή κινητών δικτύων δεν αρκεί πάντοτε η επαλήθευση της ταυτότητας του συνομιλούντος στοιχείου δικτύου κάνοντας χρήση κάποιας διαδικασίας αυθεντικοποίησης (authentication). Είναι επίσης απαραίτητο να γνωρίζουμε ότι κάθε μήνυμα που λαμβάνουμε προέρχεται από συγκεκριμένο στοιχείο δικτύου. Η απλούστερη μέθοδος για να το επιτύχουμε αυτό είναι να ζητούμε από το συνομιλητή να αποδείξει ότι γνωρίζει ένα μυστικό κλειδί ή συνθηματικό (password). Αν αυτό ισχύει τότε η επικοινωνία μπορεί να ξεκινήσει. Η περαιτέρω ενσωμάτωση του μυστικού κλειδιού σε καθένα μήνυμα που λαμβάνεται ή αποστέλλεται μπορεί υπό προϋποθέσεις να εγγυηθεί την αυθεντικότητα των επιμέρους μηνυμάτων. Αυτό σημαίνει ότι αν οι επιτιθέμενοι δεν καταφέρουν με κάποιο τρόπο να αποκτήσουν το μυστικό κλειδί δεν θα είναι σε θέση να δημιουργήσουν αυθεντικά μηνύματα και να ξεγελάσουν τον πομπό ή το δέκτη. Στην ιδέα αυτή βασίζονται πολλά πρωτόκολλα ή μέθοδοι ασφαλείας των ασύρματων και κινητών επικοινωνιών, όπως ο μηχανισμός αυθεντικοποίησης του GSM.

Β. ***Μην αποδέχεσαι τίποτα χωρίς εγγυήσεις:*** Στο χώρο της ασφάλειας επικοινωνιών ο όρος εγγύηση σημαίνει εγγύηση αυθεντικότητας, δηλαδή απόδειξη ότι κάποιο μήνυμα δεν έχει αλλοιωθεί. Αν και ο συνομιλητής πρέπει να αυθεντικοποιηθεί πριν γίνουν αποδεκτά τα μηνύματα του, δεν είμαστε σε θέση να γνωρίζουμε αν τα μηνύματα που λαμβάνουμε αμέσως μετά τη διαδικασία

αυθεντικοποίησης είναι αυτά που αυτός έστειλε ή κατά κάποιο τρόπο αλλοιώθηκαν, καθυστέρησαν ή έχουν αντικατασταθεί εξ ολοκλήρου με κάποια άλλα. παραδείγματος χάριν, ο εισβολέας τοποθετείται μεταξύ του πομπού και του δέκτη, λαμβάνει τα μηνύματα του πομπού, τα αλλοιώνει κατά το δοκούν και αμέσως μετά τα προωθεί στο δέκτη. Ο δέκτης δεν είναι σε θέση να γνωρίζει ποιος (τελικά) του έστειλε το μήνυμα. Επιπλέον, δεν έχει άλλο τρόπο να αντιληφθεί την αλλοίωση ενός μηνύματος παρά μόνο κοιτάζοντας τα περιεχόμενά του. Γι' αυτό το λόγο είναι απαραίτητη η προστασία της ακεραιότητας των μηνυμάτων που μεταδίδονται μεταξύ των επικοινωνούντων στοιχείων δικτύου.

Γ. ***Όλοι πρέπει να αντιμετωπίζονται (ως εχθροί μέχρι αποδείξεως του εναντίον)****:* Στο ενσύρματο περιβάλλον του γραφείου μας είμαστε σε θέση με κάποιο βαθμό βεβαιότητας να γνωρίζουμε το που (π. χ. σε ποιο δίκτυο) συνδεόμαστε με την έννοια ότι τοποθετούμε το καλώδιο δικτύου στην πρίζα του τοίχου που ανήκει στην επιχείρηση στην οποία εργαζόμαστε. Αν ο συγκεκριμένος χώρος επιτηρείται σωστά και τα ερμάρια καλωδιώσεων είναι κλειδωμένα τότε μπορούμε να έχουμε ένα μεγάλο βαθμό εμπιστοσύνης στο δίκτυο μας. Αντίθετα, σε ένα ασύρματο περιβάλλον, οι σταθμοί των χρηστών είναι κατασκευασμένοι έτσι ώστε μόλις ενεργοποιούνται να αναζητούν τα δίκτυα με τα οποία μπορούν να συνδεθούν. Παραδείγματος χάριν, τα ασύρματα σημεία πρόσβασης (Access Points, APs) ενός WLAN δημοσιοποιούν την ταυτότητα τους, εκπέμποντας κατά διαστήματα σήματα ταυτότητας του δικτύου στο οποίο ανήκουν (beacon frames). Υπό αυτή την έννοια, δεν είναι καθόλου δύσκολο για οποιονδήποτε επιτιθέμενο να εγκαταστήσει ένα πλαστό AP στο απέναντι κτίριο ή στο φορτηγάκι του, το οποίο θα εκπέμπει την ταυτότητα του γνήσιου δικτύου, αναμένοντας ότι πολλές συσκευές χρηστών θα εξαπατηθούν και θα συνδεθούν τελικά σε αυτό.

Δ. ***Μην εμπιστεύεσαι κανέναν και τίποτα, για μεγάλο διάστημα****:* Όπως είδαμε στα παραπάνω η εγκαθίδρυση σχέσεων εμπιστοσύνης (trust) μεταξύ των επικοινωνούντων μερών είναι πολύ σημαντική. Στην περίπτωση όμως των ασύρματων και κινητών δικτύων επικοινωνιών η τακτική αναθεώρηση αυτών των σχέσεων εμπιστοσύνης είναι και απαραίτητη. Συνήθως, η συσκευή μας επικοινωνεί μόνο με συσκευές άλλων χρηστών *με* τις οποίες έχει προηγουμένως ανταλλάξει κάποιου είδους τεκμήριο ασφαλείας (security token). Παραδείγματος χάριν, ένα μυστικό κλειδί, ένα ψηφιακό πιστοποιητικό, κλπ. Παρόλα αυτά, όλα τα τεκμήρια

ασφαλείας έχουν συνήθως περιορισμένη διάρκεια ζωής και πρέπει να ανανεώνονται τακτικά.

Ε. ***Πάντα να χρησιμοποιείς καλά δοκιμασμένες και αποτελεσματικές λύσεις:*** Πάγια τακτική στο χώρο της ασφάλειας επικοινωνιών είναι η δυσπιστία για καθετί καινούργιο, όπως μια νέα πολιτική, ένα νέο πρωτόκολλο ή μηχανισμός ασφαλείας. Παραδείγματος χάριν, ένας νέος αλγόριθμος κρυπτογράφησης θα πρέπει να τεθεί στη δοκιμασία του χρόνου για αρκετά μεγάλο διάστημα προκειμένου να μπορούμε να πούμε με κάποιο ποσοστό βεβαιότητας ότι είναι ασφαλής με τα μέσα που προς το παρόν διαθέτουμε. Επιπλέον, στο χώρο των ασύρματων και κινητών επικοινωνιών οι αλγόριθμοι κρυπτογράφησης και γενικά τα πρωτόκολλα ασφαλείας είναι σχεδιασμένα έτσι ώστε να είναι αποδοτικά σε φορητές συσκευές περιορισμένων δυνατοτήτων σε επεξεργαστική ισχύ και μνήμη. Αυτό φυσικά σημαίνει ότι οι επιτιθέμενοι, έχοντας στη διάθεση τους ισχυρά συστήματα, μπορούν ευκολότερα να ανακαλύψουν εγγενείς αδυναμίες και να τις εκμεταλλευτούν προς όφελός τους.

ΣΤ. ***Πάντα να βρίσκεσαι σε ετοιμότητα:*** Όλα τα συστήματα, μη εξαιρουμένων του λογισμικού και του υλικού, κατασκευάζονται κάνοντας κάποιες υποθέσεις συνειδητές ή ασυνείδητες. Συμπεριλαμβανομένων και των αναπόφευκτων κατασκευαστικών λαθών, τις υποθέσεις αυτές προσπαθούν οι επιτιθέμενοι να εκμεταλλευτούν. Για παράδειγμα, οι υπεύθυνοι ανάπτυξης ενός αρθρώματος λογισμικού αναλυτή μηνυμάτων (parser module) για ένα εξυπηρετητή ή μια φορητή συσκευή μπορούν ασυνείδητα να υποθέσουν ότι ο εξυπηρετητής θα δέχεται πάντα σωστά μηνύματα κωδικοποιημένα σύμφωνα με τα ισχύοντα πρότυπα. Τι θα συμβεί όμως αν ένας επιτιθέμενος αρχίσει να αποστέλλει μηνύματα που ο αναλυτής του εξυπηρετητή δεν είναι δυνατό να επεξεργαστεί; Ένα διαφορετικό παράδειγμα αποτελεί η δημιουργία ενός νέου ή η παράλλαξη ενός υπάρχοντος ιομορφικού λογισμικού, το οποίο τα ήδη εγκατεστημένα αντίμετρα δεν μπορούν να ανιχνεύσουν. Τέτοιου είδους ζητήματα υποδεικνύουν ότι πρέπει πάντα να είμαστε σε επιφυλακή προκειμένου να είμαστε σε θέση να αντιμετωπίσουμε νέες απειλές και παραλλαγμένους τρόπους επιθέσεων, που δεν έχουν ακόμα εκδηλωθεί και λογικά οι κατασκευαστές των συστημάτων που χρησιμοποιούμε δεν τις έχουν λάβει υπόψη. Με άλλα λόγια, κανένα προϊόν, μέθοδος, πρωτόκολλο, μηχανισμός ή πολιτική ασφάλειας δεν μπορεί να θεωρηθεί 100% ασφαλής, ακόμα και αν έχει δοκιμαστεί στην πράξη για μεγάλο χρονικό διάστημα.

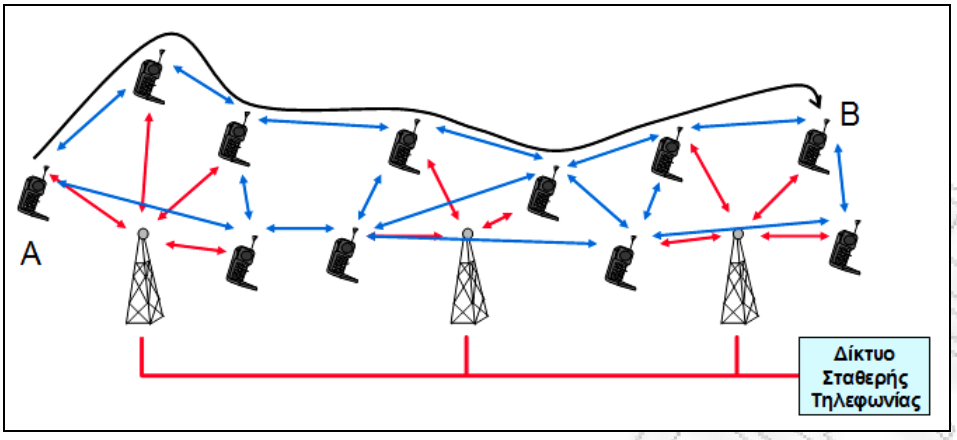
2 AD-HOC ΔΙΚΤΥΑ

Η έρευνα στα ασύρματα αδόμητα δίκτυα, άρχισε τη δεκαετία του 1970 με πρωτοβουλία της DARPA (Defense Advanced Research Projects Agency), φορέα του Αμερικάνικου στρατού. Η έρευνα συνεχίστηκε κατά τη δεκαετία του 1980 με μειωμένη ένταση. Έχει όμως ενταθεί τα τελευταία 10 χρόνια. Έχουν προταθεί πολλές μη στρατιωτικές εφαρμογές και η τεχνολογία των πομποδεκτών έχει βελτιωθεί δραματικά, υπάρχουν δε πολλά ενδιαφέροντα ερευνητικά προβλήματα.

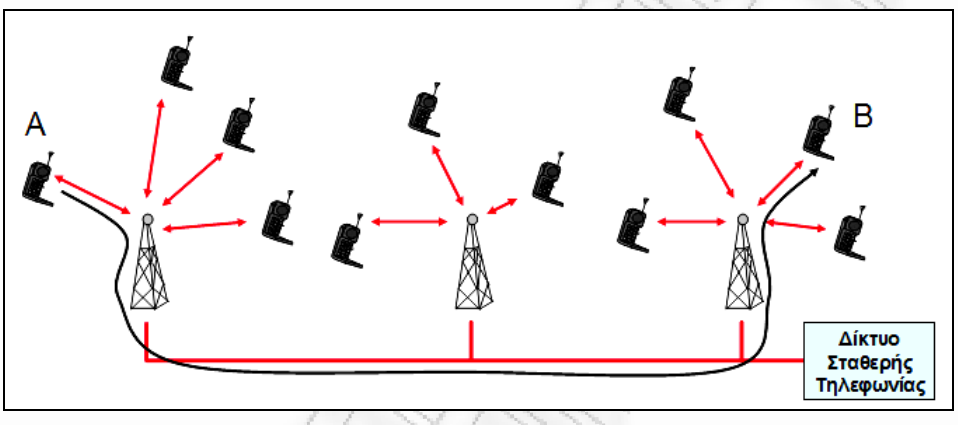
2.1 ΕΙΣΑΓΩΓΗ

Στα δίκτυα υπολογιστών ο όρος «ad-hoc» χρησιμοποιείται για να δηλώσει μια μέθοδο διασύνδεσης η οποία συνήθως σχετίζεται με ασύρματα δίκτυα. Δεν υπάρχει συγκεκριμένη ορολογία στα ελληνικά η οποία να δηλώνει ένα ad-hoc δίκτυο και ένα τέτοιο δίκτυο ονομάζεται είτε αδόμητο είτε κατ' απαίτηση δίκτυο, με τον δεύτερο όρο να επικρατεί στη βιβλιογραφία.

Τα δίκτυα ad-hoc εντάσσονται σε μια ευρύτερη κατηγορία δικτύων (Distributed Transient Network) η οποία ορίζεται σαν τα δίκτυα αυτά τα οποία είναι εν γένει αποκεντρωμένα και αποτελούνται κυρίως από κόμβους οι οποίοι δεν ανήκουν εξ ορισμού και διαρκώς στο δίκτυο αλλά έχουν την δυνατότητα να εισέρχονται ή να αποχωρούν από το δίκτυο οποιαδήποτε στιγμή και από οποιοδήποτε σημείο του. Η σύνδεση που πραγματοποιείται κατά μήκος ενός ad hoc δικτύου πραγματοποιείται καθ' όλη τη διάρκεια μιας σύζευξης και δεν απαιτεί την ύπαρξη σταθμού βάσης (Εικόνα 9) όπως το ασύρματο δίκτυο με υποδομή κυψέλης (Εικόνα 10), στο οποίο τα κινητά τερματικά ανταλλάσσουν δεδομένα αποκλειστικά με τους σταθμούς βάσης κι έχουν πολύ λίγες αρμοδιότητες. Αντίθετα, οι συσκευές ανακαλύπτουν την ύπαρξη άλλων συσκευών που βρίσκονται γύρω τους για να δημιουργήσουν ένα δίκτυο που αποτελείται από αυτές.

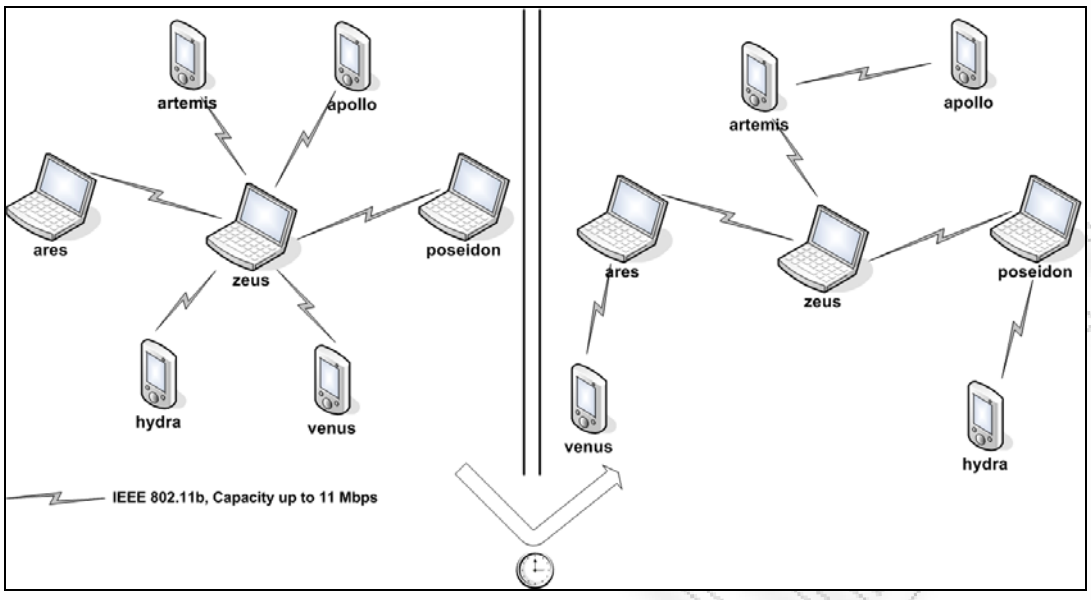


Εικόνα 9. Ασύρματο δίκτυο χωρίς υποδομή (ad hoc)

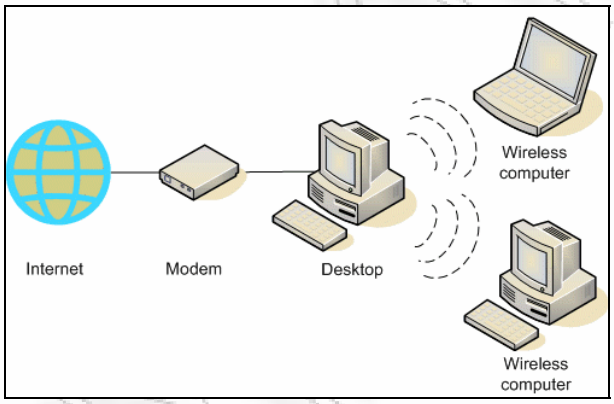


Εικόνα 10. Ασύρματο δίκτυο με υποδομή κυψέλης (κυψελωτό δίκτυο)

Οι συνδέσεις πραγματοποιούνται δια μέσου πολλών κόμβων (multihop ad-hoc network). Οι κόμβοι του δικτύου παίζουν ενεργό ρόλο κατά την δρομολόγηση των πακέτων, προωθώντας εκτός από τα δικά τους πακέτα και τα πακέτα γειτονικών κόμβων. Αυτό το χαρακτηριστικό είναι χρήσιμο σε περιπτώσεις που ο αποστολέας και ο παραλήπτης ενός πακέτου δεν βρίσκονται εντός της ακτίνας ο ένας του άλλου (ή πιθανόν μόνο ο ένας από τους δύο βρίσκεται εντός της ακτίνας του άλλου). Κάθε κόμβος έχει τη δυνατότητα να λάβει και να προωθήσει δεδομένα σε άλλους κόμβους. Αυτό έρχεται σε αντίθεση με παλαιότερες δικτυακές τεχνολογίες όπου υπάρχουν κόμβοι με αποκλειστική λειτουργία την προώθηση των δεδομένων σε άλλους κόμβους, όπως για παράδειγμα οι routers. Τα πρωτόκολλα δρομολόγησης στη συνέχεια αναλαμβάνουν την παροχή αξιόπιστων συνδέσεων ακόμα κι αν οι κόμβοι μετακινούνται. Έτσι η τοπολογία του δικτύου μπορεί να μεταβάλλεται ραγδαία και απρόβλεπτα. Ένα τέτοιο δίκτυο μπορεί να λειτουργεί αυτόνομα (Εικόνα 11) ή μπορεί να συνδέεται στο Internet (Εικόνα 12) και η ύπαρξή του συνήθως δεν είναι μόνιμη.



Εικόνα 11. Παράδειγμα ad-hoc δικτύου



Εικόνα 12. Ad-hoc συνδεδεμένο στο internet

Εξαιτίας της φορητής και μη δομημένης φύσης των δικτύων ad-hoc εγείρεται ένα σύνολο από νέες απαιτήσεις κατά το σχεδιασμό τους. Καταρχήν απαιτείται το δίκτυο να είναι αυτορυθμιζόμενο όσον αφορά στις διευθύνσεις και τη δρομολόγηση, ενώ σε επίπεδο εφαρμογής οι χρήστες του δικτύου συνήθως επικοινωνούν και συνεργάζονται ως ομάδες. Αυτό εγείρει ένα μεγάλο σύνολο προβλημάτων και προκλήσεων που θα πρέπει να αντιμετωπιστούν για την αποτελεσματική επικοινωνία.

2.2 ΟΡΙΣΜΟΣ AD-HOC ΔΙΚΤΥΟΥ

Πριν δώσουμε τον ορισμό των ad hoc δικτύων, πρέπει να απαντήσουμε στο ερώτημα: Γιατί ad hoc δίκτυα;

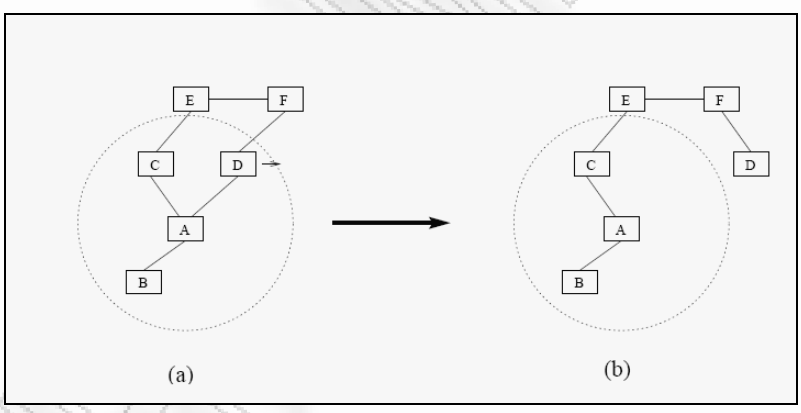
Η απάντηση συνοψίζεται στα ακόλουθα τρία χαρακτηριστικά τους:

1. Ευκολία ανάπτυξης

2. Ταχύτητα ανάπτυξης
3. Μειωμένη εξάρτηση από σταθερή υποδομή

Ένα ad-hoc δίκτυο είναι μία συλλογή από ασύρματους κινητούς κόμβους (nodes) που συνιστούν ένα προσωρινό δίκτυο χωρίς τη βοήθεια κάποιας υποδομής ή κάποιου κεντραρισμένου administrator. Σε ένα τέτοιο περιβάλλον, ίσως είναι απαραίτητο ένας κινητός host να θελήσει τη βοήθεια άλλων host προκειμένου να προωθήσει ένα πακέτο στον προορισμό του, εξαιτίας της περιορισμένης εμβέλειας του κάθε κινητού host στις ασύρματες μεταδόσεις. Με άλλα λόγια οι κόμβοι εξαρτώνται ο ένας από τον άλλο για να κρατήσουν συνδεδεμένο το δίκτυο.

Η κινητικότητα των κόμβων σε ένα ad-hoc δίκτυο δημιουργεί συχνές αλλαγές στην τοπολογία του δικτύου. Η Εικόνα 13 παρουσιάζει ένα τέτοιο παράδειγμα: αρχικά οι κόμβοι A και D συνδέονται σε απευθείας σύζευξη. Όταν ο D κινείται εκτός της εμβέλειας του A, η σύζευξη «σπάει». Εν τούτοις, το δίκτυο είναι ακόμη συνδεδεμένο γιατί ο κόμβος A μπορεί να φτάσει τον κόμβο D διαμέσου των κόμβων C, E και F.



Εικόνα 13. Οι κόμβοι A, B, C, D, E και F συνιστούν ένα ad-hoc δίκτυο. Ο κύκλος αντιπροσωπεύει την εμβέλεια του κόμβου A. Το δίκτυο αρχικά έχει την τοπολογία του (α). Όταν ο κόμβος D κινηθεί εκτός της εμβέλειας του κόμβου A, η τοπολογία του δικτύου αλλάζει σε αυτήν του (β).

2.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Κάθε δίκτυο περιγράφεται από ένα σύνολο χαρακτηριστικών. Τέτοια είναι το μέγεθος του δικτύου (αριθμός κόμβων), το είδος των κόμβων, ο χώρος που καταλαμβάνει, η τοπολογία του, το μέσο μετάδοσης και τα πρωτόκολλα επικοινωνίας.

Στον πίνακα 1 φαίνονται τα χαρακτηριστικά των ad hoc δικτύων όταν το μέσο μετάδοσης είναι ο αέρας.

Ad-hoc Networks
Δεν έχουν συμπεριφορά μετρητικής διάταξης και η επικοινωνία καθορίζεται από τις ανάγκες των εφαρμογών
Οι κόμβοι είναι πολλών και διαφόρων μεγεθών
Ανανεώσιμες και μεγαλύτερες πηγές ενέργειας
Δυνατότητα εύρεσης κι αποκατάστασης σφαλμάτων και αλλαγή μπαταρίας
Ο χρόνος ζωής των κόμβων δεν εξαρτάται από τη διάρκεια της μπαταρίας αφού αυτή αντικαθίσταται εύκολα
Μικρή πυκνότητα κόμβων
Περιοχή μετάδοσης που φτάνει τα 500 μέτρα
Ισχυρή υπολογιστική ισχύς και μεγάλη μνήμη
Οι κόμβοι επικοινωνούν με το δίκτυο σχεδόν σε όλη τη διάρκεια της σύνδεσης
Η επικοινωνία πραγματοποιείται μεταξύ συγκεκριμένων κόμβων όταν απαιτηθεί από τους χρήστες
Σχετικά ακριβοί κόμβοι
Μεγάλο εύρος ζώνης
Η λειτουργία του δικτύου είναι ίδια για όλες τις εφαρμογές
Συνεχόμενη ροή πληροφορίας

Πίνακας 1. Χαρακτηριστικά των ad-hoc δικτύων

Το κυριότερο χαρακτηριστικό των ad-hoc δικτύων είναι η φορητότητα. Οι κόμβοι μπορεί να μετακινούνται συνεχώς και αυτός είναι και ο λόγος ανάπτυξης των συγκεκριμένων δικτύων. Το δίκτυο συνήθως αποτελείται από μικρό αριθμό κόμβων κάθε φορά, γεγονός όχι απόλυτο, οι οποίοι μπορεί να εισέρχονται και να εξέρχονται από το δίκτυο με εντελώς τυχαία συχνότητα. Το δίκτυο είναι ετερογενές, δεν αποτελείται δηλαδή από έναν τύπο συσκευών. Μπορεί να αποτελείται από ένα σύνολο PDA, κινητών τηλεφώνων, φορητών υπολογιστών κτλ. τα οποία πρέπει να έχουν δυνατότητα επικοινωνίας μεταξύ τους.

Η κατανομή των κόμβων αυτών στο χώρο καθορίζει και την τοπολογία που θα χρησιμοποιηθεί. Αν για παράδειγμα όλες οι συσκευές βρίσκονται πολύ κοντά η μία

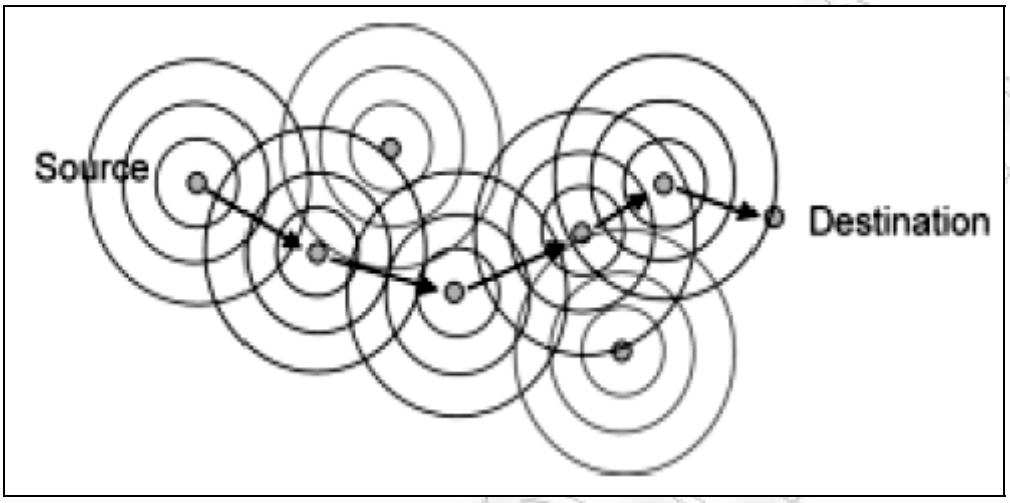
με την άλλη είναι εφικτή μία σύνδεση απλού hop από κόμβο σε κόμβο. Αντίθετα αν το δίκτυο εκτείνεται σε μεγάλη γεωγραφική έκταση απαιτείται multi-hop διασύνδεση μεταξύ των κόμβων. Η σημασία των ad-hoc δικτύων είναι πολύ μεγάλη, κυρίως χάρη στην μεγάλη ευκολία και ταχύτητα με την οποία μπορούν να εγκατασταθούν, αφού δεν απαιτούν την ύπαρξη σταθερής υποδομής. Ένα ακόμα πλεονέκτημα της δυναμικής τους φύσης είναι η εύκολη προσθήκη και απομάκρυνση νέων κόμβων, καθώς και το γεγονός ότι κάθε κόμβος εξαρτάται μόνο από τους γειτονικούς του, με αποτέλεσμα την αυξημένη αξιοπιστία των ad-hoc δικτύων.

Τα ad-hoc δίκτυα παρουσιάζουν σημαντική ανομοιογένεια, αφού κάθε κόμβος μπορεί να διαφέρει από τους υπόλοιπους σε πολλά χαρακτηριστικά, όπως την υπολογιστική ισχύ, την ακτίνα εκπομπής ή την διάρκεια ζωής των μπαταριών (αν π.χ. είναι ένας φορητός υπολογιστής ή ένας PDA). Επιπλέον, τα διάφορα ad-hoc δίκτυα μπορεί να διαφέρουν σε πολλά χαρακτηριστικά τους, όπως τους χρησιμοποιούμενους ρυθμούς επικοινωνίας, στο αν παρέχουν δυνατότητες broadcast ή multicast, στο αν συνυπάρχουν ή όχι με άλλα δίκτυα τα οποία έχουν κάποια σταθερή υποδομή ή τέλος, αν υποστηρίζουν την κινητικότητα των χρηστών και με τι ρυθμούς.

Ένα από τα κύρια χαρακτηριστικά των κινητών, ασύρματων κόμβων ενός ad-hoc δικτύου είναι η δυνατότητα να εκτελούν εργασίες ανεξάρτητα και ακολούθως να επικοινωνούν προκειμένου να συγχωνεύσουν τα αποτελέσματά τους, ώστε να επιτελέσουν λειτουργίες υψηλότερης πολυπλοκότητας. Κάτι τέτοιο καθιστά τα ad-hoc δίκτυα ιδανικά για την εκτέλεση κατανεμημένων λειτουργιών με έξυπνο και αποδοτικό τρόπο.

Σημαντικό ρόλο σε κάθε ad-hoc δίκτυο παίζει η ακτίνα μετάδοσης κάθε κόμβου. Συγκεκριμένα, όσο μεγαλύτερη είναι η ακτίνα μετάδοσης των κόμβων, τόσο μικρότερος θα είναι ο μέσος αριθμός μεταδόσεων που θα απαιτείται για την αποστολή ενός πακέτου από ένα κόμβο σε κάποιον άλλο. Από την άλλη μεριά η μικρή ακτίνα εκπομπής των κόμβων μειώνει την πιθανότητα συγκρούσεων, καθώς και τις παρεμβολές μεταξύ των κόμβων. Με άλλα λόγια, όσο μικρότερη είναι η ακτίνα εκπομπής, τόσο περισσότερες μεταδόσεις θα μπορούν να πραγματοποιούνται ταυτόχρονα. Επιπρόσθετα, η ακτίνα μετάδοσης παίζει καθοριστικό ρόλο και στην κατανάλωση ενέργειας κάθε κόμβου, η οποία είναι μια πολύ σημαντική παράμετρος στα περισσότερα ad-hoc δίκτυα και συχνά η σημαντικότερη στα MANET. Έτσι, η ακτίνα μετάδοσης θα πρέπει να επιλέγεται όσο το δυνατό μικρότερη, φροντίζοντας όμως ταυτόχρονα να μην είναι τόσο μικρή που το δίκτυο να παύει να είναι συνεκτικό.

Μια καλή επιλογή είναι, συνήθως, να επιλέγεται η ακτίνα μετάδοσης, έτσι ώστε κάθε μετάδοση να «ακούγεται» από περίπου 6 κόμβους (Εικόνα 14).



Εικόνα 14. Η μετάδοση «ακούγεται» από 6 κόμβους

Οι Micah Adler και Christian Scheideler, προτείνουν ένα μοντέλο τριών επιπέδων για την περιγραφή ενός δικτύου ad-hoc. Αρχικά, έχουμε το επίπεδο ελέγχου προσπέλασης μέσου (Medium Access Control layer), το οποίο είναι υπεύθυνο για την επικοινωνία από σημείο-σε-σημείο (node-to-node) στο φυσικό μέσο. Ακολούθως έχουμε το επίπεδο επιλογής διαδρομής (route selection layer), το οποίο είναι υπεύθυνο για την εύρεση κατάλληλων διαδρομών για τα πακέτα. Τέλος, έχουμε το επίπεδο χρονοπρογραμματισμού (scheduling layer), που είναι υπεύθυνο για τον καθορισμό της σειράς αποστολής των πακέτων.

2.4 ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Στα ασύρματα δίκτυα ad-hoc η επικοινωνία μεταξύ των κόμβων πραγματοποιείται μέσω καναλιών ραδιοσυχνοτήτων. Η τεχνολογία που χρησιμοποιείται μπορεί να είναι οποιαδήποτε από το ευρύ φάσμα τεχνολογιών για ασύρματες επικοινωνίες που υπάρχουν σήμερα. Κάποιες από αυτές αναλύονται στη συνέχεια.

Ανάλογα με την έκταση της περιοχής που καλείται να καλύψει το δίκτυο μπορεί να χρησιμοποιηθεί η τεχνολογία που χρησιμοποιείται στα Ασύρματα Προσωπικά Δίκτυα – Wireless Personal Area Networks (WPAN), στα Ασύρματα Τοπικά Δίκτυα – Wireless Local Area Networks ή στα Ασύρματα Μητροπολιτικά Δίκτυα – Wireless Metropolitan Area Networks (WMAN). Η ακτίνα κάλυψης ενός

WPAN είναι της τάξεως των μερικών μέτρων και μέχρι το πολύ 20 μέτρα. Η ακτίνα κάλυψης ενός WLAN περιορίζεται περίπου στα 100 μέτρα, ενώ η ακτίνα κάλυψης σε ένα WMAN είναι της τάξεως μερικών χιλιομέτρων. Για κάθε έναν από τους παραπάνω τύπους δικτύου έχουν προταθεί και διάφορες τεχνολογίες ασύρματης επικοινωνίας. Μερικά παραδείγματα δίνονται παρακάτω:

- ✓ WPAN: Bluetooth, UWB
- ✓ WLAN: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g
- ✓ WMAN: IEEE 802.16e

Τα βασικά χαρακτηριστικά των τεχνολογιών αυτών δίνονται στον πίνακα 1 μαζί με τα συστήματα GPRS και UMTS, τα οποία χρησιμοποιούνται στην κινητή τηλεφωνία, για ευκολότερη σύγκριση. Η μέγιστη ταχύτητα μεταφοράς δεδομένων (bit rate) και οι συχνότητες λειτουργίας είναι βασικά χαρακτηριστικά που καθορίζουν το κατά πόσο είναι κατάλληλη κάθε τεχνολογία για τις εφαρμογές που παρέχονται από ένα ad-hoc δίκτυο. Σε αντίθεση με τα συστήματα κινητής τηλεφωνίας, οι τεχνολογίες που χρησιμοποιούνται στα WPAN, WLAN και WMAN δεν είναι σχεδιασμένες για φορητή και κινητή επικοινωνία.

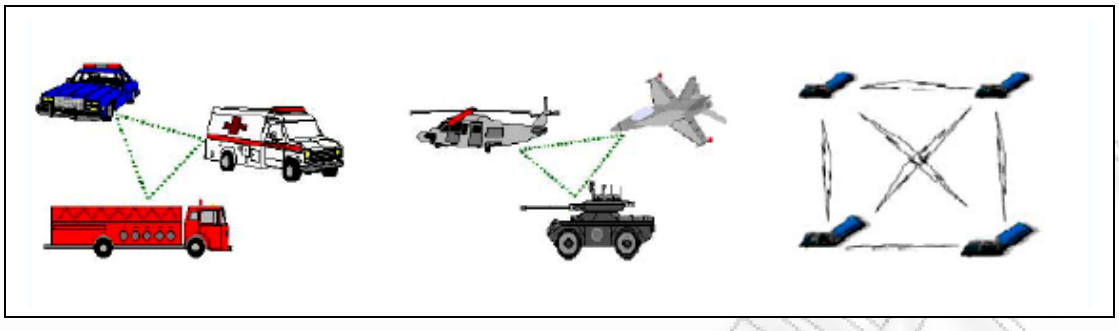
Παρόλα αυτά τα δίκτυα ad-hoc μπορεί να αποτελούνται από συχνά γρήγορα κινούμενους κόμβους. Στα συστήματα κινητής τηλεφωνίας αυτού του είδους η επικοινωνία είναι εφικτή με τη βοήθεια διαδικασιών handover και περιαγωγής. Το handover εφαρμόζεται όταν ο χρήστης μετακινείται από κυψέλη σε κυψέλη, ενώ η περιαγωγή απαιτεί ειδική δρομολόγηση από τους παρόχους των δικτύων μεταξύ των χωρών. Τα δίκτυα WLAN, WMAN και WPAN έχουν σχεδιασθεί για φορητά τερματικά και έχουν προδιαγραφές για το φυσικό επίπεδο και το επίπεδο σύνδεσης δεδομένων του μοντέλου OSI. Αυτά τα δίκτυα μπορούν να χειριστούν κινητούς κόμβους αλλά με σοβαρούς περιορισμούς. Ένας τρόπος για την αντιμετώπιση των περιορισμών αυτών είναι η χρήση φορητής IP διεύθυνσης για τους κόμβους (mobile IP) καθώς και η χρήση γρήγορων πρωτοκόλλων δρομολόγησης.

	Maximum data rate (17)	Frequency allocation	Channel bandwidth	Number of RF Channels	Multiple Access technology	Typical range	Mobility support
Bluetooth	1 Mbps	2.4 GHz (ISM)	1 MHz	79	FHSS	10 m	(1)
UWB	110 Mbps (at 10m)	3.1-10.6 GHz	Min. 500 MHz Max. 7.5 GHz	1-15	THSS OFDM (11)	10-15 m	(1)
IEEE 802.11b	11 Mbps	2.4-2.497 GHz (ISM)	25 MHz	3	DSSS	50-80 m (9)	(2)
IEEE 802.11g	54 Mbps	2.4-2.497 GHz (ISM)	(10)	(10)	(10)	50-80 m (9)	(2)
IEEE 802.11a	54 Mbps	various bands in 5 GHz region	20 MHz	US: 12 EU: 8 Japan: 4	OFDM	40-60 m (9)	(2)
IEEE 802.16e	75 Mbps	2-11 GHz 10-66 GHz (3)	1.5 – 20 MHz (3)	(3)	(15)	30 km (4) 4 km (5)	(6)
GPRS	171 kbps (12)	800, 900 and 1800 MHz bands (13)	200 kHz (13)	(13)	TDMA with FDD	1-5 km (14)	Handover possible also at high speeds
UMTS(W-CDMA) (8)	2 Mbps	1920-1980 MHz 2110-2170 MHz	5 MHz	(7)	DSSS	1-3 km (16)	Handover possible also at high speeds

Πίνακας 2. Βασικά χαρακτηριστικά διαφόρων ασύρματων τεχνολογιών

Notes:
(1) Technology by itself does not support handover.
(2) Movement within a cell is possible. Technology by itself does not support handover.
(3) IEEE 802.16 is designed for a wide range of licensed and license-exempt frequencies with flexile bandwidth allocation to accommodate easier cell planning throughout the world.
(4) With line of sight condition.
(5) Without line of sight condition.
(6) Mobility is only supported in the 2-6 GHz band. At walking speeds, handoff between adjacent cells is possible.
(7) Number of frequency bands depends on the operator's license.
(8) Of different variants of UMTS, here we only consider the European W-CDMA.
(9) Lower bound corresponds to 11 Mbps data rate, and upper bound corresponds to 2 Mbps data rate.
(10) For data rates 1, 2, 5.5 and 11 Mbps the same channel spacing, bandwidth and modulation is used as in IEEE 802.11b (for backwards compatibility). Other supported bit rates use OFDM.
11) UWB can be implemented using several spreading technologies. Most implementations use OFDM or THSS.
(12) This is the maximum data rate using 8 time slots and Coding Scheme 4 (CS-4).
(13) Same as in GSM.
(14) With Coding Scheme 1 (CS-1), the coverage radius of GSM voice and GPRS data is the same, with CS-2, CS-3 and CS-4 the coverage radius reduces. Typical range in this table is for urban areas. Theoretically the maximum range could be as much as 30 km.
(15) IEEE 802.16 physical layer supports three access technologies: 1. Single Carrier Modulation (CS), 2. OFDM in combination with TDMA and 3. OFDMA. OFDM and OFDMA are mainly proposed for no line of sight operation.
(16) Typical range in this table is for urban areas. Theoretically the maximum range could be as much as 20 km.
(17) Figures given here are for a single user. In the case of shared use of the radio channel, the capacity is divided amongst all users.

2.5 ΕΦΑΡΜΟΓΕΣ AD-HOC

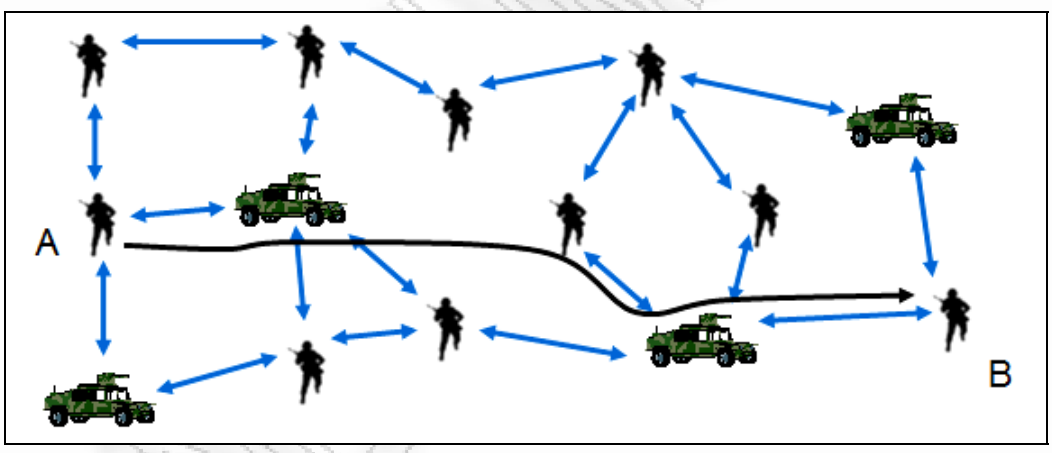


Εικόνα 15. Διάφορες εφαρμογές των ad-hoc δικτύων

- **Καταστάσεις έκτακτης ανάγκης:** Τα ad-hoc δίκτυα χρησιμοποιούνται συχνά σε εφαρμογές έρευνας και διάσωσης όπου πρέπει να υπάρχει γρήγορη ανάπτυξη επικοινωνιακού δικτύου με περιορισμένες ή μηδενικές υποδομές σε πιθανόν εχθρικό περιβάλλον (π.χ. σε εχθρική χώρα, σε δάση, στην θάλασσα, σε περιοχές που έχουν πληγεί από φυσικές καταστροφές κ.α.).
- **Δικτύωση σε εργασία:** Τα ad-hoc δίκτυα μπορούν να χρησιμοποιηθούν για διασύνδεση υπολογιστών σε περιπτώσεις που υπάρχει άμεση ανάγκη για την παροχή δικτυακών υπηρεσιών χωρίς την ύπαρξη των αναγκαίων υποδομών όπως παρακολούθηση συνεδρίων, συναντήσεις (meetings) για συνεργασία σε κάποιο κοινό έργο (project) κ.λ.π.
- **Δικτύωση σπιτιού:** Οι υπολογιστικές συσκευές που χρησιμοποιούμε (π.χ. φορητοί υπολογιστές, PDAs, κινητά τηλέφωνα κ.λ.π.) θα μπορούσαν να συνδέονται μέσω ενός αδόμητου δικτύου, έτσι ώστε να είναι πιο εύκολη η προσθήκη και αφαίρεση συσκευών από το δίκτυο.
- **Δίκτυα αισθητήρων (sensor networks or smart dust):** Για την παρακολούθηση και καταγραφή των περιβαλλοντολογικών συνθηκών σε μια περιοχή, μια λύση θα ήταν η ρίψη (π.χ. από αέρος) ενός μεγάλου αριθμού μικροσκοπικών αισθητήρων, οι οποίοι θα μπορούν να επικοινωνούν ασύρματα μεταξύ τους για να συγκεντρώνουν τα απαραίτητα δεδομένα. Για παράδειγμα θα μπορούσαν να χρησιμοποιηθούν σε ένα δάσος με στόχο τον εντοπισμό πυρκαγιάς.

Εικόνα 16. Δίκτυα αισθητήρων

- **Στρατιωτικές εφαρμογές:** Οι στρατιωτικές επιχειρήσεις αλλά και οι επιχειρήσεις ευαίσθητης ασφάλειας είναι οι κύριες εφαρμογές των ad-hoc δικτύων. Για παράδειγμα, οι στρατιωτικές μονάδες (π.χ. στρατιώτες, τανκ ή αεροπλάνα) που εξοπλίζονται με ασύρματες συσκευές, θα μπορούσαν να δημιουργήσουν ένα ad-hoc δίκτυο όταν βρίσκονται μέσα σε ένα πεδίο μάχης. Είναι προφανές, ότι σε ένα πεδίο μάχης δεν υπάρχει χρόνος για να στηθούν σταθμοί βάσης κι αν ακόμα υπήρχε χρόνος, το δίκτυο θα ήταν ευάλωτο σε επιθέσεις.



Εικόνα 17. Στρατιωτική εφαρμογή ad-hoc δικτύου

2.6 ΠΡΟΒΛΗΜΑΤΑ ΚΑΙ ΛΥΣΕΙΣ

Ένα από τα σημαντικότερα προβλήματα στα ad-hoc δίκτυα είναι η δρομολόγηση. Ο λόγος είναι ότι οι περισσότεροι από τους γνωστούς αλγορίθμους δρομολόγησης έχουν σχεδιαστεί ώστε να λειτουργούν κάτω από συνθήκες οι οποίες είναι πολύ πιο ευνοϊκές από αυτές που ισχύουν σε ασύρματα δίκτυα.

Μία από τις βασικότερες ιδιαιτερότητες που πρέπει να αντιμετωπίσουν οι αλγόριθμοι δρομολόγησης των ασύρματων δικτύων είναι η κινητικότητα των

χρηστών, η οποία αλλάζει πολύ συχνά την τοπολογία του δικτύου, με αποτέλεσμα να απαιτείται πολύ συχνά η κατασκευή νέων διαδρομών. Επιπρόσθετα, εξαιτίας του περιορισμένου διαθέσιμου εύρους ζώνης στα ασύρματα δίκτυα, απαιτείται ο αριθμός των σχετικών με την δρομολόγηση μηνυμάτων να είναι περιορισμένος. Επίσης, στα ασύρματα δίκτυα το ποσοστό των πακέτων που χάνονται είναι αρκετά υψηλό, τόσο εξαιτίας της αυξημένης πιθανότητας λαθών μετάδοσης, όσο και εξαιτίας της αυξημένης πιθανότητας καταστροφής συνδέσμων (π.χ. εξαιτίας της μετακίνησης ενός κόμβου). Όλα τα παραπάνω έχουν σαν αποτέλεσμα την διαφοροποίηση σε σχέση με τα ενσύρματα δίκτυα των ιδιοτήτων που επιθυμούμε να έχουν οι αλγόριθμοι δρομολόγησης στα ad-hoc δίκτυα.

Έτσι, καταρχήν, τα χρησιμοποιούμενα πρωτόκολλα θα πρέπει να είναι κατανεμημένα, με κάθε κόμβο να είναι αρκετά «έξυπνος» ώστε να μπορεί να παίρνει αποφάσεις δρομολόγησης. Αυτό είναι απαραίτητο, αφού ένα κεντρικοποιημένο πρωτόκολλο δρομολόγησης δεν θα ήταν αξιόπιστο σε περίπτωση κίνησης των κόμβων. Επιπρόσθετα, το πρωτόκολλο θα πρέπει να δημιουργεί γρήγορα δρομολογήσεις για να μπορούν να χρησιμοποιηθούν πριν αλλάξει η τοπολογία του δικτύου, διατηρώντας παράλληλα το επιπλέον φορτίο στο δίκτυο για τους σκοπούς της δρομολόγησης χαμηλό. Εκτός όλων αυτών, το πρωτόκολλο δρομολόγησης είναι επιθυμητό να μπορεί να παίρνει αποφάσεις δρομολόγησης βασιζόμενες και στην ενεργειακή κατάσταση κάθε κόμβου, καθώς και στην πιθανή επίδραση αυτών των αποφάσεων σε αυτήν. Τέλος, κάθε σύνδεσμος μεταξύ κόμβων θα πρέπει να θεωρείται από το πρωτόκολλο δρομολόγησης ως μίας κατεύθυνσης, αφού η επικοινωνία προς την μία κατεύθυνση μπορεί να περιορίζεται από φυσικούς παράγοντες ή και την μορφολογία του χώρου, την ακτίνα εκπομπής κάθε κόμβου και άλλα.

Τα πρωτόκολλα δρομολόγησης μπορούν να διακριθούν με βάση το εάν η δρομολόγηση γίνεται κατανεμημένα σε κάθε κόμβο ή κεντρικοποιημένα από τον κόμβο που στέλνει το πακέτο. Στην πρώτη περίπτωση κάθε κόμβος αποφασίζει για τον επόμενο κόμβο στον οποίο θα προωθήσει το πακέτο, ενώ στην δεύτερη περίπτωση, που πολλές φορές ονομάζεται δρομολόγηση πηγής (source routing) η διαδρομή που θα ακολουθήσει κάθε πακέτο καθορίζεται από τον κόμβο αποστολέα του πακέτου. Οι διαδρομές αυτές μπορεί να είναι είτε στατικές, είτε να προσαρμόζονται δυναμικά στην κατάσταση του δικτύου.

Ένας άλλος τρόπος διαχωρισμού των πρωτοκόλλων δρομολόγησης είναι σε πρωτόκολλα βασισμένα σε πίνακες (table driven protocols), όπου κάθε κόμβος

διατηρεί πληροφορίες για τους υπόλοιπους κόμβους του δικτύου και τα πρωτόκολλα βασιζόμενα στην κατ' απαίτηση αρχικοποίηση από την πηγή (source initiated on-demand driven protocols), τα οποία δημιουργούν μια διαδρομή όποτε αυτή ζητηθεί από κάποιον κόμβο αφετηρία. Χαρακτηριστικά παραδείγματα της πρώτης κατηγορίας είναι τα Dynamic Destination-Sequenced Distance-Vector Routing Protocol, Wireless Routing Protocol, Global State Routing, Fisheye State Routing, Hierarchical State Routing, Zone-based Hierarchical Link State Routing Protocol και Clusterhead Gateway Switch Routing Protocol. Στα on-demand routing protocols ανήκουν μεταξύ άλλων τα Cluster based Routing Protocol, Ad hoc On demand Distance Vector Routing, Dynamic Source Routing Protocol, Temporally Ordered Routing Algorithm, Associativity Based Routing και Signal Stability Routing.

Για την προσαρμογή των δρομολογίων στην κατάσταση του δικτύου χρησιμοποιούνται κυρίως δύο μεγάλες κατηγορίες αλγορίθμων. Η πρώτη κατηγορία είναι οι αλγόριθμοι βασιζόμενοι σε διανύσματα απόστασης (distance vectors). Σε αυτά τα πρωτόκολλα, κάθε κόμβος στέλνει σε όλους τους γειτονικούς του κόμβους τις αποστάσεις που γνωρίζει για όλους τους κόμβους του δικτύου. Κάθε κόμβος υπολογίζει με βάση τις πληροφορίες από τους γειτονικούς του κόμβους τα συντομότερα μονοπάτια προς κάθε πιθανό προορισμό (κλασικό παράδειγμα αυτού του είδους των αλγορίθμων είναι ο Distributed Bellman-Ford – DBF). Το σημαντικότερο μειονέκτημα αυτής της κατηγορίας αλγορίθμων είναι η αυξημένη πιθανότητα δημιουργίας «κυκλικών» βρόγχων στην δρομολόγηση ενός πακέτου εξαιτίας της παρουσίας σφαλμάτων σε κάποιον κόμβο. Αυτό θα έχει σαν αποτέλεσμα την πιθανότητα εγκλωβισμού πακέτων σε ένα τέτοιο βρόγχο, με αποτέλεσμα την καθυστέρηση παράδοσης ή και την απώλεια των πακέτων, η οποία σε περίπτωση σφαλμάτων στο ίδιο το πρωτόκολλο μπορεί να οδηγήσει σε οριστική κατάρρευση του δικτύου. Μια άλλη μεγάλη κατηγορία αλγορίθμων δρομολόγησης είναι οι αλγόριθμοι βασιζόμενοι στην κατάσταση των συνδέσμων (link state).

Στα πρωτόκολλα που χρησιμοποιούν τέτοιου είδους αλγορίθμους, κάθε κόμβος πληροφορεί τους γειτονικούς του για την κατάσταση των γειτονικών του συνδέσμων, με αποτέλεσμα κάθε κόμβος να έχει συνολική εικόνα του δικτύου. Με αυτόν τον τρόπο κάθε κόμβος μπορεί να επιλέξει το συντομότερο μονοπάτι προς οποιονδήποτε κόμβο χρησιμοποιώντας κάποιον κεντρικοποιημένο αλγόριθμο δρομολόγησης (π.χ. Dijkstra). Με την χρήση αυτών των αλγορίθμων η πιθανότητα δημιουργίας κύκλων εξαιτίας λανθασμένων, πιθανόν λόγω καθυστέρησης στην

διάδοση, πληροφοριών για την κατάσταση των συνδέσμων, μπορούν να επιλυθούν σύντομα.

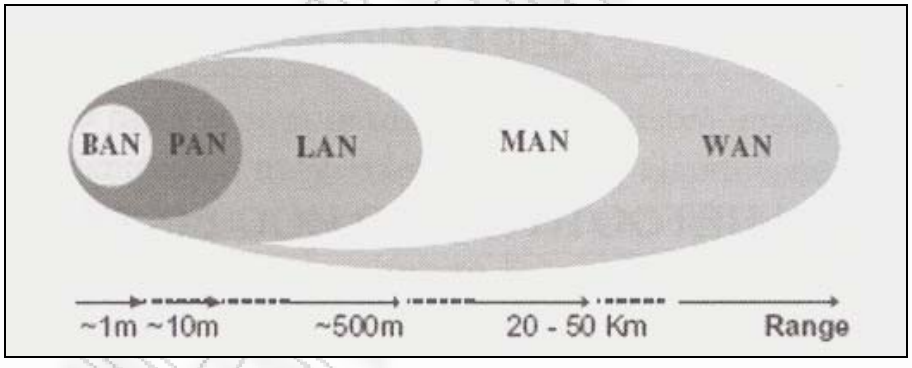
Από όσα αναφέρθηκαν παραπάνω η ύπαρξη πληθώρας διαθέσιμων πρωτοκόλλων δρομολόγησης θα πρέπει να είναι αναμενόμενη. Σε γενικές γραμμές μπορούμε να πούμε ότι δεν υπάρχει ένα πρωτόκολλο δρομολόγησης κατάλληλο για την πλειοψηφία των ad-hoc δικτύων, αλλά σε κάθε ad-hoc δίκτυο το πρωτόκολλο δρομολόγησης επιλέγεται με βάση τα ιδιαίτερα χαρακτηριστικά του.

3 BLUETOOTH ΚΑΙ AD HOC ΔΙΚΤΥΑ

3.1 ΕΙΣΑΓΩΓΗ

Η τεχνολογία ή καλύτερα η βιομηχανική προδιαγραφή ασύρματων δικτύων Bluetooth, που είναι γνωστή ως πρότυπο IEEE 802.15.1, γίνεται σταδιακά ένας πολύ δημοφιλής τρόπος αντικατάστασης των υπαρχουσών ενσύρματων συνδέσεων με ασύρματες συνδέσεις μικρής εμβέλειας. Είναι τεχνολογία που εισάγει νέα είδη εφαρμογών.

Ένα ad hoc δίκτυο έχει το βασικό πλεονέκτημα ότι δε χρειάζεται κάποιο σημείο πρόσβασης για να συνδεθούν οι υποψήφιοι κόμβοι. Όταν μία συσκευή βρεθεί στην περιοχή κάλυψης του δικτύου και διαθέτει το απαιτούμενο υλικό, μπορεί να συνδεθεί σε αυτό και να γίνει μέλος του. Συνήθως τα ad hoc δίκτυα χρησιμοποιούνται για την επέκταση των υπαρχόντων ενσύρματων ή ασύρματων δικτύων. Τα ad hoc δίκτυα μπορούν να ταξινομηθούν με βάση την περιοχή κάλυψης σε: Body (BAN), Personal (PAN), Local (LAN), Metropolitan (MAN), Wide (WAN).



Εικόνα 18. Τύποι δικτύων ανάλογα με την απόσταση

Τα MAN και WAN ad hoc δίκτυα, είναι ασύρματα δίκτυα που χρησιμοποιούν πολλές αναπηδήσεις (multi-hop), αλλά ακόμη αντιμετωπίζουν πολλά προβλήματα που αναζητούν λύση. Μερικά από αυτά τα προβλήματα είναι η διευθυνσιοδότηση και η ασφάλεια. Αντιθέτως, τα BAN, LAN και PAN ad hoc δίκτυα, τα οποία καλύπτουν μικρή περιοχή, είναι σε θέση να αξιοποιηθούν καλύτερα, γι' αυτό και πολλά κτιριακά συγκροτήματα τα χρησιμοποιηθούν για να δικτυωθούν.

Τα BAN δίκτυα συσχετίζονται άμεσα με τους φορετούς υπολογιστές (wearable computers). Ένας τέτοιος υπολογιστής διανέμει τα κομμάτια του στο ανθρώπινο σώμα που τον φέρει. Έτσι υπάρχουν οθόνες που προσαρμόζονται στα

μάτια του φορέα, ακουστικά, μικρόφωνα, κ.λ.π. Το δίκτυο αναλαμβάνει να ενώσει όλα αυτά τα κομμάτια, ώστε να δουλεύουν αρμονικά και χωρίς συγκρούσεις. Το εύρος επικοινωνίας ενός BAN είναι όσο περίπου είναι ένα ανθρώπινο σώμα, δηλ. 1,5-2 m.

Τα PAN δίκτυα ενώνουν φορητές συσκευές που μεταφέρουν οι χρήστες με άλλες φορητές ή σταθερές συσκευές. Ενώ τα δίκτυα BAN δικτυώνουν συσκευές σε μια περιοχή 1-2 μέτρων, τα PAN την επεκτείνουν στα 10 μέτρα.

Αν θέλουμε να δικτυώσουμε μια ευρύτερη περιοχή, η οποία θα φτάνει το ένα οικοδομικό τετράγωνο, δηλ. 100-500 μέτρα, τότε είναι προτιμότερο να αξιοποιήσουμε τη λύση του ασύρματου τοπικού δικτύου (WLAN). Ένα τέτοιο δίκτυο θα πρέπει να ικανοποιεί τις απαιτήσεις ενός απλού τοπικού δικτύου, δηλ. υψηλή χωρητικότητα, πλήρη συνδεσιμότητα μεταξύ των κόμβων, κ.λ.π. Όμως για να ικανοποιηθούν τα παραπάνω θα πρέπει να επιλυθούν κάποια θέματα ασύρματης φύσεως, όπως είναι η ασφάλεια δεδομένων που μεταδίδονται στον αέρα, η κατανάλωση ρεύματος και η φορητότητα των κόμβων.

Υπάρχουν δύο προσεγγίσεις για την υλοποίηση ενός τέτοιου δικτύου. Η πρώτη απαιτεί την ύπαρξη μιας σταθερής εγκατάστασης (infrastructure), η οποία θα συνδέει το ενσύρματο με το ασύρματο δίκτυο και θα παρέχει σε αυτό πρόσβαση στο διαδίκτυο. Η συσκευή αυτή ονομάζεται σημείο πρόσβασης (access point). Η δεύτερη προσέγγιση χρησιμοποιεί ad hoc δίκτυα, τα οποία είναι ομότιμα (peer-to-peer) δίκτυα αποτελούμενα από διάφορες συσκευές, οι οποίες βρίσκονται η μία εντός της ευρύτερης περιοχής της άλλης. Ένα τέτοιο δίκτυο δεν έχει σταθερή δομή, καθώς ανά πάσα στιγμή μπορεί να εισέλθει κάποια νέα συσκευή και να την τροποποιήσει.

3.2 ΑΣΦΑΛΕΙΑ ΣΤΑ AD HOC BLUETOOTH ΔΙΚΤΥΑ

Η σχεδίαση των ad-hoc δικτύων είναι αυτή που δημιουργεί κατά ένα σημαντικό ποσοστό, τα όποια προβλήματα ασφάλειας παρουσιάζονται σε αυτά τα δίκτυα. Όταν αναφερόμαστε στη σχεδίαση εστιάζουμε στο γεγονός ότι ένα ad-hoc δίκτυο δεν έχει σταθερή τοπολογία και οι συνδέσεις μεταξύ των κόμβων του είναι, κατά ένα μεγάλο ποσοστό, ασύρματες. Όλα αυτά τα χαρακτηριστικά των ad-hoc δικτύων τα καθιστούν περίπλοκα σε ζητήματα ασφάλειας κι ευπαθή σε διάφορες επιθέσεις.

➲ Διαθεσιμότητα

Στα ad-hoc δίκτυα η διαθεσιμότητα είναι πιο σημαντική σε σχέση με τα παραδοσιακά δίκτυα. Κι αυτό διότι όλες οι συσκευές εξαρτώνται η μία από την άλλη κι επιπλέον όλη η πληροφορία μεταφέρεται μέσω ραδιοκυμάτων με αποτέλεσμα η πτώση του δικτύου να είναι πολύ εύκολη. Για παράδειγμα, ένας κακόβουλος χρήστης θα μπορούσε να προσπαθήσει να εμποδίσει ή να παρέμβει στη ροή των πληροφοριών που μεταδίδονται. Επίσης, θα ήταν δυνατό να αλλοιωθούν οι πίνακες του πρωτοκόλλου δρομολόγησης που χρησιμοποιήθηκε στο δίκτυο αν αυτό λάβει (σκοπίμως) εσφαλμένες πληροφορίες.

Τα πρωτόκολλα δρομολόγησης είναι στην πραγματικότητα ένα από τα πιο τρωτά σημεία στα ad-hoc δίκτυα. Αυτά πρέπει να είναι σε θέση να χειριστούν δυναμικά τη μεταβαλλόμενη τοπολογία του δικτύου και τις τυχόν επιθέσεις από τους κακόβουλους χρήστες. Πάντως, υπάρχουν πρωτόκολλα δρομολόγησης, τα οποία μπορούν να προσαρμοστούν καλά στη μεταβαλλόμενη τοπολογία.

➲ Πιστοποίηση Ταυτότητας Και Διαχείριση Κλειδιών

Η πιστοποίηση ταυτότητας των κόμβων είναι ένα άλλο δύσκολο θέμα στα ad-hoc δίκτυα. Δεδομένου ότι υπάρχει ελάχιστη ή καμία υποδομή, η αναγνώριση των χρηστών, π.χ. οι συμμετέχοντες σε μία αίθουσα συνεδριάσεων, δεν είναι εύκολη. Από την άλλη, θα μπορούσε να χρησιμοποιηθεί ένα γενικό πρωτόκολλο για τη διαχείριση των κλειδιών. Αυτό όμως παρουσιάζει αρκετά μειονεκτήματα, αφού δεν ταιριάζει στα χαρακτηριστικά ενός ειδικού δικτύου με σημαντικά μικρότερους πόρους από τους κανονικούς υπολογιστές και μάλιστα με μη συγκεκριμένη και σταθερή τοπολογία.

➲ Εμπιστευτικότητα Και Ακεραιότητα

Η εμπιστευτικότητα είναι ένα πλέον τρωτό σημείο. Λόγω της ασύρματης ζεύξης, οποιοσδήποτε μπορεί να υποκλέψει το περιεχόμενο των μηνυμάτων. Ένας τρόπος να διασφαλιστεί η εμπιστευτικότητα της ροής των δεδομένων είναι η χρήση κλειδιού συνδυασμού για την κρυπτογράφησή τους. Η χρήση του συγκεκριμένου τύπου κλειδιού συνεπάγεται τη δημιουργία κλειδιών από την κύρια συσκευή με κάθε άλλη εξαρτημένη συσκευή, ανά ζεύγος. Έτσι, τα δεδομένα από έναν αποστολέα εξαρτημένο, πρώτα μεταφέρονται στον κύριο και μετά από αυτόν καταλήγουν στον παραλήπτη εξαρτημένο.

Εναλλακτικός τρόπος διασφάλισης της εμπιστευτικότητας της κίνησης των δεδομένων είναι η χρησιμοποίηση της θεώρησης του κύριου κλειδιού: κατά την κρυπτογράφηση των δεδομένων χρησιμοποιείται το ίδιο κλειδί από όλους τους κόμβους στα δίκτυα ad-hoc. Αν θέλουμε να χρησιμοποιήσουμε πιο πολύπλοκη δικτύωση ad hoc θα πρέπει να μεταφέρουμε την ασφάλεια ψηλότερα στο επίπεδο εφαρμογής.

Παράλληλα, χωρίς την απαραίτητη αυθεντικοποίηση δεν έχει νόημα να αναφερόμαστε στην εμπιστευτικότητα, αφού δε θα μπορούμε να καθορίσουμε ουσιαστικά σε ποιο συγκεκριμένο χρήστη θέλουμε να στείλουμε μία πληροφορία. Παρόμοια κατάσταση ισχύει και για την ακεραιότητα. Επειδή η σύνδεση είναι ασύρματη, τα δεδομένα είναι δυνατόν να τροποποιηθούν με διάφορες παρεμβάσεις στη συχνότητα των ραδιοκυμάτων.

3.3 ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ BLUETOOTH AD-HOC ΔΙΚΤΥΑ

Κύριος στόχος των επιθέσεων σε ένα Bluetooth ad hoc δίκτυο, είναι το πρωτόκολλο δρομολόγησης. Έτσι με την είσοδο ενός κακόβουλου κόμβου, μπορεί να διαταραχθεί η λειτουργία του μηχανισμού δρομολόγησης. Στόχος, λοιπόν, ενός πρωτοκόλλου ασφαλούς δρομολόγησης είναι να προστατεύει το δίκτυο από τις επεμβάσεις κακόβουλων κόμβων. Γενικά οι επιθέσεις μπορούν να κατηγοριοποιηθούν ως ακολούθως:

- ***Επιθέσεις διάσπασης της δρομολόγησης***: Σε αυτόν τον τύπο επίθεσης, ο κακόβουλος κόμβος ηθελημένα κι επανειλημμένα απορρίπτει πακέτα ελέγχου, δρομολογεί λανθασμένα τα πακέτα και διαδίδει λανθασμένα πληροφορίες που αφορούν τους γειτονικούς του κόμβους. Ο επιτιθέμενος θα προσπαθήσει να τροποποιήσει τις διευθύνσεις αποστολέα και παραλήπτη στα δρομολογούμενα μηνύματα, να μεταδώσει ψεύτικους συναγερμούς (false alarms) λανθασμένης δρομολόγησης ή να τροποποιήσει τυχόν μηνύματα σφαλμάτων, να πλαστογραφήσει μηνύματα τροποποιώντας τις διευθύνσεις του αποστολέα ή του παραλήπτη.
- ***Επιθέσεις κατανάλωσης των πόρων***: Σε αυτού του είδους την επίθεση ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους του συστήματος με τους ακόλουθους τρόπους: εκκινεί πολυάριθμες αιτήσεις δρομολόγησης, κάνει

επιλεκτική απόρριψη πακέτων, κάτι που έχει ως αποτέλεσμα τον αυξημένο αριθμό αιτήσεων δρομολόγησης από τους γειτονικούς κόμβους, που διαθέτουν περιορισμένες ικανότητες δρομολόγησης.

- ***Επιθέσεις στα διακινούμενα δεδομένα***: Σε αυτή την περίπτωση, ο επιτιθέμενος κόμβος τροποποιεί τα διακινούμενα δεδομένα έτσι ώστε να μην είναι πλέον αναγνώσιμα από το σύστημα. Αυτό συνεπάγεται την καταστροφή τους κι άρα την επιφόρτιση του δικτύου με την επαναποστολή τους.

3.3.1 Συνεργαζόμενοι Κακόβουλοι Κόμβοι

Οι επιθέσεις που θα αναφερθούν στα παρακάτω, πραγματοποιούνται από μία ομάδα κακόβουλων κόμβων, οι οποίοι συνεργάζονται για να επιφέρουν μεγαλύτερη ζημιά στο δίκτυο.

- ☑ ***Επίθεση wormhole***: Ένας κακόβουλος κόμβος ακούει ένα μήνυμα που μεταδίδεται σε μια περιοχή του δικτύου και το αναπαράγει σε μία άλλη περιοχή του δικτύου με τη βοήθεια ενός άλλου κόμβου.
- ☑ ***Επίθεση αόρατου κόμβου***: Αυτή η επίθεση μπορεί να πραγματοποιηθεί από οποιονδήποτε κόμβο βρίσκεται στο μονοπάτι δρομολόγησης. Μπορεί να θεωρηθεί ως μια επίθεση του τύπου ενδιάμεσου (man-in the middle attack). Η ζημιά που προκαλείται από αυτή την επίθεση, περιορίζεται στους κόμβους του συγκεκριμένου μονοπατιού.
- ☑ ***Rushing attack***: Αυτή η επίθεση μπορεί να εφαρμοστεί εναντίον οποιουδήποτε πρωτοκόλλου το οποίο χρησιμοποιεί συναρτήσεις εντοπισμού και διόρθωσης διπλών πακέτων. Ο επιτιθέμενος αποστέλλει ένα πακέτο στον προορισμό, συνήθως πρόκειται για τον ενδιάμεσο κόμβο στο μονοπάτι, το οποίο έχει διαμορφώσει έτσι ώστε να φαίνεται ως να είναι διπλό πακέτο. Κατά συνέπεια αυτό το πακέτο απορρίπτεται κι άρα η πληροφορία που μετέφερε, χάνεται.

4 ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ AD-HOC ΔΙΚΤΥΩΝ

4.1 ΕΙΣΑΓΩΓΗ

Τα ad-hoc δίκτυα μπορεί να διαφέρουν το ένα από το άλλο ανάλογα με το πεδίο εφαρμογής τους: Για παράδειγμα, μέσα σε μια επιστημονική σχολική αίθουσα με υπολογιστές, θα μπορούσε να δημιουργηθεί ad-hoc δίκτυο μεταξύ των PDAs των μαθητών και του σταθμού εργασίας του δασκάλου. Σε κάποιο άλλο σενάριο μια ομάδα στρατιωτών βρίσκεται σε εχθρικό περιβάλλον και προσπαθεί να κρατήσει μυστική τόσο την παρουσία της όσο και την αποστολή της από τον εχθρό. Οι στρατιώτες μεταφέρουν φορητές συσκευές επικοινωνίας και μπορούν να κρυφακούσουν την επικοινωνία μεταξύ των μονάδων του εχθρού, να κλείσουν εχθρικές συσκευές, να αλλάξουν αυθαίρετα την πορεία των εχθρών ή να υποδυθούν ότι είναι άτομα της εχθρικής ομάδας. Όπως είναι προφανές, αυτά τα δύο σενάρια δικτύωσης ad-hoc διαφέρουν μεταξύ τους σε πολλά σημεία: Στο πρώτο σενάριο για να δουλέψουν οι κινητές συσκευές χρειάζονται ένα ασφαλές και φιλικό περιβάλλον, όπου οι συνθήκες δικτύωσης είναι προβλέψιμες. Γι' αυτό δεν είναι απαραίτητες κάποιες ειδικές απαιτήσεις ασφαλείας.

Από την άλλη πλευρά, στο δεύτερο και μάλλον τραβηγμένο σενάριο, οι συσκευές δουλεύουν σε ένα άκρως εχθρικό και απαιτητικό περιβάλλον, στο οποίο η προστασία της επικοινωνίας και η διαθεσιμότητα και λειτουργία του δικτύου είναι αρκετά τρωτές και με μηδαμινή προστασία.

Καθώς η ad-hoc δικτύωση κατά κάποιο τρόπο ποικίλλει από τις περισσότερες παραδοσιακές προσεγγίσεις, τα θέματα ασφάλειας που ίσχυαν για τα δίκτυα του παρελθόντος, δεν είναι εντελώς εφαρμόσιμα στα ad-hoc δίκτυα.

Ενώ οι βασικές απαιτήσεις ασφάλειας παραμένουν (εμπιστευτικότητα-confidentiality και αυθεντικοποίηση-authenticity), η προσέγγιση ad-hoc δικτύωσης περιορίζει κάπως τη χρήση των εφικτών μηχανισμών ασφάλειας. Η παρουσίαση των κόμβων στα ad-hoc δίκτυα είναι κρίσιμη αφού το ποσό της διαθέσιμης ενέργειας για υπέρμετρο υπολογισμό και radio μετάδοση είναι υπό περιορισμό. Επιπρόσθετα, το διαθέσιμο εύρος ζώνης και οι ραδιοσυχνότητες μπορεί να είναι βαριά περιορισμένες και να αλλάζουν αρκετά γρήγορα. Τέλος, καθώς το ποσό της διαθέσιμης μνήμης και της ισχύος της CPU είναι τυπικά μικρό, η εφαρμογή δυνατής προστασίας σε ad-hoc δίκτυα είναι εξαιρετικά σημαντική.

Η ασφάλεια είναι σημαντικό ζήτημα για τα ad-hoc δίκτυα, ειδικά όταν πρόκειται για ευαίσθητες στην ασφάλεια εφαρμογές. Οι υπηρεσίες ασφάλειας των ad-hoc δικτύων δεν είναι όλες διαφορετικές από εκείνες που χρησιμοποιούνται σε άλλα δίκτυα. Ο σκοπός αυτών των υπηρεσιών είναι να προστατέψουν τις πληροφορίες και τους πόρους από επιθέσεις και από κακή συμπεριφορά (misbehaviour). Μιας κι αναφερόμαστε στην ασφάλεια, θα εξηγήσουμε τις ακόλουθες προδιαγραφές που πρέπει να εξασφαλίσει μια αποτελεσματική αρχιτεκτονική ασφαλείας:

- ⇨ διαθεσιμότητα
- ⇨ εμπιστευτικότητα
- ⇨ ακεραιότητα
- ⇨ αυθεντικοποίηση
- ⇨ απάρνηση ενέργειας ή πράξης (non-repudiation)

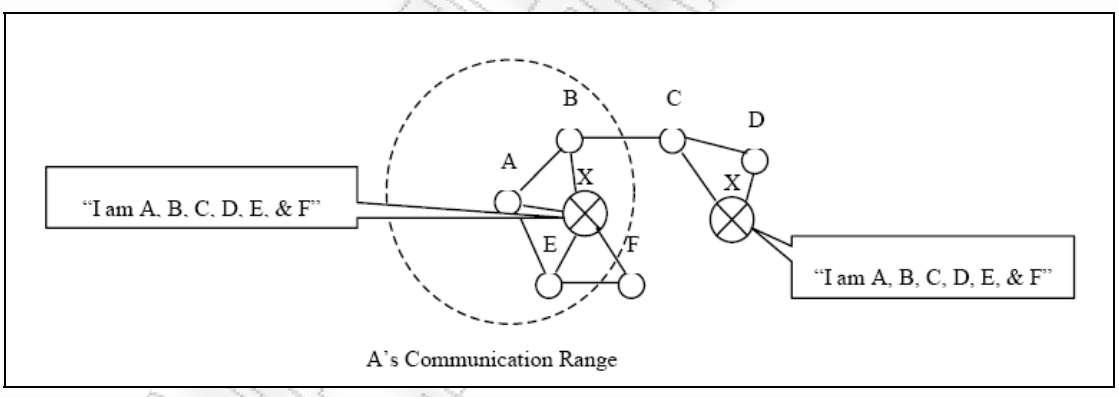
Η *Διαθεσιμότητα* εξασφαλίζει το ότι οι επιθυμητές υπηρεσίες δικτύου είναι διαθέσιμες όταν τις θέλουμε παρά την παρουσία των επιθέσεων. Τα συστήματα που εξασφαλίζουν διαθεσιμότητα στα MANET, ψάχνουν να πολεμήσουν τις επιθέσεις denial of service και energy starvation, όπως επίσης και την κακή συμπεριφορά των κόμβων (node misbehaviour) π.χ. selfishness κατά την προώθηση πακέτου. Η denial of service επίθεση μπορεί να πραγματοποιηθεί σε οποιοδήποτε επίπεδο ενός ad-hoc δικτύου. Στο φυσικό επίπεδο (Physical layer) και στο επίπεδο ελέγχου προσπέλασης μέσου (Medium Access Control layer), ο αντίπαλος μπορεί να χρησιμοποιήσει εμπλοκή (jamming) για να ανακατευτεί με την επικοινωνία στα φυσικά κανάλια. Στο επίπεδο δικτύου (network layer) ο αντίπαλος θα μπορεί να διασπάσει το πρωτόκολλο δρομολόγησης και να διακόψει-αποσυνδέσει το δίκτυο. Στα υψηλότερα επίπεδα ο αντίπαλος μπορεί να ρίξει τις υπηρεσίες υψηλού επιπέδου. Ένας τέτοιος στόχος είναι η υπηρεσία διαχείρισης κλειδιού (key management service), μια ουσιώδης υπηρεσία

για οποιαδήποτε ασφάλεια πλαισίου.

Η *εμπιστευτικότητα δεδομένων* εξασφαλίζει ότι βέβαιη πληροφορία δεν είναι ποτέ φανερή σε μη εξουσιοδοτημένες οντότητες. Η εμπιστευτικότητα των δεδομένων είναι τυπικά ενεργοποιημένη όταν εφαρμόζεται συμμετρική ή ασύμμετρη κρυπτογράφηση δεδομένων.

Η *ακεραιότητα* (ψηφιακή υπογραφή) εγγυάται ότι ένα μήνυμα που μεταφέρεται δε διαφθείρεται ποτέ. Αυτό συμβαίνει γιατί ένα μήνυμα που στέλνεται από τον κόμβο Α στον κόμβο Β δεν τροποποιήθηκε από κάποιον κακοήθη κόμβο C κατά τη διάρκεια της μετάδοσης. Ένα μήνυμα μπορεί να διαφθαρεί λόγω ήπιων αποτυχιών, όπως για παράδειγμα εξασθένηση της διάδοσης ραδιοσήματος ή λόγω κακοηθών επιθέσεων στο δίκτυο.

Η *αυθεντικοποίηση* (κωδικός πρόσβασης, πιστοποιητικό) εξασφαλίζει ότι η επικοινωνία από τον ένα κόμβο στον άλλο, είναι γνήσια. Χωρίς αυθεντικοποίηση ο αντίπαλος μπορεί να μασκαρευτεί ως κόμβος κι έτσι να κερδίσει μη εξουσιοδοτημένη πρόσβαση σε πόρους και ευαίσθητες πληροφορίες και να ανακατευτεί με τη λειτουργία των άλλων κόμβων.



Εικόνα 19. Αντίπαλοι κόμβοι οι οποίοι μεταδίδουν ψευδή δεδομένα δρομολόγησης. Όταν ένα μήνυμα στέλνεται σε έναν κόμβο που εσφαλμένα θεωρείται ότι είναι μέσα στην εμβέλεια μετάδοσης, χάνεται.

Η *απάρνηση ενέργειας ή πράξης* (non-repudiation) (αλυσίδα ψηφιακών υπογραφών) εξασφαλίζει ότι ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα και ότι ο παραλήπτης δεν μπορεί να αρνηθεί τη λήψη του. Η απάρνηση ενέργειας είναι χρήσιμη για ανίχνευση και απομόνωση των επικίνδυνων (compromised) κόμβων. Όταν ένας κόμβος Α παραλαμβάνει ένα λανθασμένο μήνυμα από ένα κόμβο Β, η απάρνηση ενέργειας επιτρέπει στον Α να κατηγορήσει τον Β χρησιμοποιώντας αυτό το μήνυμα και για να πείσει κι άλλους κόμβους ότι ο Β είναι επικίνδυνος (compromised).

4.2 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΟΥ (KEY MANAGEMENT)

Η ασφάλεια στη δικτύωση εξαρτάται σε πολλές περιπτώσεις από κατάλληλη διαχείριση κλειδιού. Η διαχείριση κλειδιού αποτελείται από ποικίλες υπηρεσίες εκ των οποίων η καθεμία είναι ζωτικής σημασίας για την ασφάλεια των συστημάτων δικτύωσης. Οι υπηρεσίες πρέπει να εξασφαλίζουν λύσεις για να είναι σε θέση να απαντούν στις ακόλουθες ερωτήσεις:

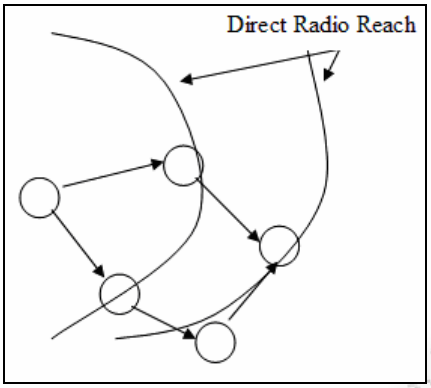
- ***Μοντέλο εμπιστοσύνης*** *(Trust model)*: πρέπει να έχουν καθοριστεί πόσα διαφορετικά στοιχεία στο δίκτυο μπορούν να εμπιστευτούν το ένα το άλλο. Το περιβάλλον και η περιοχή εφαρμογής του δικτύου επηρεάζουν ευρέως το απαιτούμενο μοντέλο εμπιστοσύνης. Συνεπώς, οι σχέσεις εμπιστοσύνης ανάμεσα στα στοιχεία του δικτύου, επηρεάζει τον τρόπο που το σύστημα διαχείρισης κλειδιού είναι κατασκευασμένο στο δίκτυο.
- ***Κρυπτοσυστήματα*** *(Cryptosystems)*: διαθέσιμα για τη διαχείριση του κλειδιού. Σε κάποιες περιπτώσεις μόνο οι δημόσιοι ή οι συμμετρικοί μηχανισμοί κλειδιού μπορούν να εφαρμοστούν, καθώς σε άλλα γενικά πλαίσια είναι διαθέσιμα κρυπτοσυστήματα ελλειπτικής καμπύλης (*Elliptic Curve Cryptosystems* (*ECC*)). Ενώ η κρυπτογράφηση δημόσιου κλειδιού προσφέρει περισσότερη σιγουριά (π.χ. γνωστές ψηφιακές υπογραφές-digital signature schemes),τα κρυπτοσυστήματα των δημόσιων κλειδιών είναι σημαντικά πιο αργά από τα αντίγραφα των μυστικών κλειδιών τους, όταν χρειάζεται παρόμοιο επίπεδο ασφαλείας. Αντιθέτως, τα συστήματα μυστικών κλειδιών προσφέρουν λιγότερη λειτουργικότητα και υποφέρουν πιο πολύ από προβλήματα, π.χ. διανομή κλειδιού (key distribution). Τα ECC κρυπτοσυστήματα είναι νεότερο πεδίο κρυπτογράφησης αλλά ήδη χρησιμοποιούνται ευρέως όπως για παράδειγμα στα συστήματα έξυπνων καρτών (smart card systems).
- ***Δημιουργία κλειδιού*** *(Key creation)*: πρέπει να καθοριστεί ποιες ομάδες χρηστών (parties) επιτρέπεται να παράγουν κλειδιά για τους εαυτούς τους ή για άλλες ομάδες και τι είδος κλειδιού.
- ***Αποθήκευση κλειδιού*** *(Key storage):* στα ad-hoc δίκτυα μπορεί να μην υπάρχει κεντραρισμένη αποθήκευση για τα κλειδιά. Ούτε να υπάρχει αποθηκευμένο αντίγραφο διαθέσιμο για ελάχιστη ανοχή (fault tolerance). Στα ad-hoc δίκτυα οποιοδήποτε στοιχείο δικτύου ενδεχομένως να πρέπει να

αποθηκεύσει το κλειδί του όπως επίσης και πιθανά κλειδιά άλλων στοιχείων. Επιπλέον τα κοινά μυστικά (shared secrets) εφαρμόζονται προκειμένου να διανέμουν τα τμήματα του κλειδιού σε διάφορους κόμβους. Σε τέτοιου είδους συστήματα η συμμόρφωση (compromising) ενός κόμβου δεν προβαίνει ακόμα σε συμβιβασμό με τα μυστικά κλειδιά.

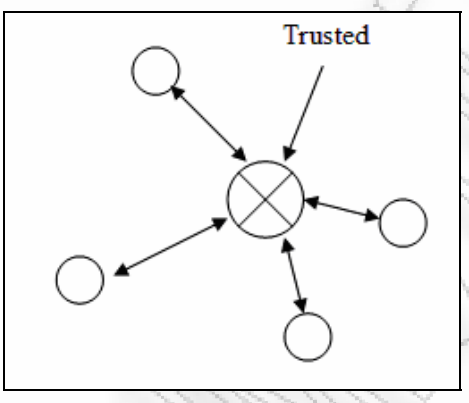
- ***Διανομή κλειδιού*** *(Key distribution)*: η υπηρεσία διαχείρισης κλειδιού πρέπει να σιγουρευτεί ότι τα παραγόμενα κλειδιά διανέμονται με ασφαλή τρόπο στους ιδιοκτήτες τους. Όποιο κλειδί πρέπει να κρατηθεί μυστικό, πρέπει να διανεμηθεί έτσι ώστε η εμπιστευτικότητα, η αυθεντικοποίηση και η ακεραιότητα δεν έχουν παραβιαστεί. Για παράδειγμα όταν εφαρμόζονται συμμετρικά κλειδιά και οι δύο ή όλη η παρέα (parties) που εμπλέκονται, πρέπει να παραλάβουν το κλειδί με ασφαλή τρόπο. Στην κρυπτογράφηση δημόσιου κλειδιού, ο μηχανισμός διανομής κλειδιού πρέπει να εγγυηθεί ότι τα ιδιωτικά κλειδιά παραδίδονται μόνο στους εξουσιοδοτημένους χρήστες. Η διανομή των δημόσιων κλειδιών δε χρειάζεται να προστατέψει την εμπιστευτικότητα, αλλά η ακεραιότητα και η αυθεντικοποίηση των κλειδιών πρέπει να έχουν εξασφαλιστεί.

4.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ MANETS ΠΟΥ ΤΑ ΚΑΝΕΙ ΤΡΩΤΑ ΣΕ ΕΠΙΘΕΣΕΙΣ

- **Χωρίς Υποδομή** (Infrastructureless): Οι κεντρικές υπηρεσίες, το εξειδικευμένο υλικό και οι σταθεροί δρομολογητές, είναι απαραιτήτως απόντες. Ένα ad-hoc δίκτυο είναι ένα δίκτυο χωρίς υποδομή. Αντίθετα από τα παραδοσιακά δίκτυα δεν υπάρχει καμία προαναπτυγμένη υποδομή όπως για παράδειγμα οι κεντρικοί δρομολογητές (administered routers) ή η ακριβής πολιτική για την υποστήριξη της end-to-end δρομολόγησης. Οι ίδιοι οι κόμβοι είναι αρμόδιοι για τη δρομολόγηση των πακέτων. Κάθε κόμβος στηρίζεται στους άλλους κόμβους για τη δρομολόγηση των πακέτων. Οι κινητοί κόμβοι που βρίσκονται στην άμεση ραδιοεμβέλεια ο ένας του άλλου, μπορεί να επικοινωνήσει άμεσα, αλλά οι κόμβοι που δεν μπορούν να επικοινωνήσουν άμεσα, πρέπει να εξαρτηθούν από τους ενδιάμεσους κόμβους για τη δρομολόγηση των μηνυμάτων.



Εικόνα 20. Δρομολόγηση στα ad-hoc δίκτυα



Εικόνα 21. Δρομολόγηση στα παραδοσιακά δίκτυα

- **Multi-hop**: Λόγω της έλλειψης κεντρικών δρομολογητών (routers) και πυλών (gateways), οι hosts είναι οι ίδιοι δρομολογητές. Κατά συνέπεια, τα πακέτα ακολουθούν τις διαδρομές multi-hop και περνούν μέσω των διαφορετικών κινητών κόμβων πριν φθάνουν στον τελικό προορισμό τους. Λόγω της πιθανής έλλειψης αξιοπιστίας τέτοιων κόμβων, αυτό το χαρακτηριστικό γνώρισμα παρουσιάζει μια σοβαρή ευπάθεια.
- **Συχνές αλλαγές στην τοπολογία δικτύων** (Frequent changes in network topology): Τα ad-hoc δίκτυα περιέχουν κόμβους που μπορούν συχνά να αλλάξουν τις θέσεις τους. Ως εκ τούτου η τοπολογία σε αυτά τα δίκτυα είναι ιδιαίτερα δυναμική. Αυτό οδηγεί σε συχνή αλλαγή γειτόνων στους οποίους ένας κόμβος στηρίζεται για τη δρομολόγηση. Κατά συνέπεια τα παραδοσιακά πρωτόκολλα δρομολόγησης δεν μπορούν πλέον να χρησιμοποιηθούν σε ένα τέτοιο περιβάλλον. Αυτό εξουσιοδοτεί νέα πρωτόκολλα δρομολόγησης που μπορούν να χειριστούν τη δυναμική τοπολογία με τη διευκόλυνση των φρέσκων ανακαλύψεων διαδρομών.

- **Ασύρματη χρήση συνδέσεων** (Wireless link use): Δεδομένου ότι η επικοινωνία είναι μέσω του ασύρματου μέσου, είναι δυνατό για οποιοδήποτε εισβολέα να τρυπήσει εύκολα την επικοινωνία. Τα ασύρματα κανάλια προσφέρουν φτωχή προστασία και τα μηνύματα ελέγχου που σχετίζονται με δρομολόγηση μπορούν να πειραχτούν. Το ασύρματο μέσο είναι ευαίσθητο στην παρεμβολή (interference), το μπλοκάρισμα (jamming), το κρυφάκουσμα (eavesdropping) και την παραμόρφωση σημάτων (distortion). Ένας εισβολέας μπορεί εύκολα να κρυφακούσει για να μάθει τις ευαίσθητες πληροφορίες δρομολόγησης ή να φράξει τα σήματα για να αποτρέψει τη διάδοση της δρομολόγησης των πληροφοριών ή χειρότερα να διακόψει τα μηνύματα και να τα παραμορφώσει για να χειριστεί τις διαδρομές. Τα πρωτόκολλα δρομολόγησης πρέπει να υιοθετηθούν καλά για να χειριστούν τέτοια προβλήματα. Αντίθετα από τα ενσύρματα δίκτυα, στα οποία ένας αντίπαλος πρέπει να κερδίσει τη φυσική πρόσβαση στα καλώδια του δικτύου ή να περάσει μέσω διάφορων γραμμών υπεράσπισης των firewalls και των πυλών (gateways), οι επιθέσεις σε ένα ασύρματο ad-hoc δίκτυο μπορούν να προέλθουν από όλες τις κατευθύνσεις και να στοχεύσουν οποιοδήποτε κόμβο. Ως εκ τούτου, τα ad-hoc δίκτυα δεν θα έχουν μια σαφή γραμμή υπεράσπισης και κάθε κόμβος πρέπει να προετοιμαστεί για να αμυνθεί ενάντια στις απειλές. Επιπλέον, τα πρωτόκολλα MAC που χρησιμοποιούνται στα ad-hoc δίκτυα, όπως το IEEE 802.11, στηρίζονται στην εμπιστευμένη συνεργασία σε μια γειτονιά για να εξασφαλίσουν πρόσβαση στο κανάλι, η οποία οδηγεί σε υψηλή ευπάθεια.
- **Αυτονομία μετακίνησης κόμβων** (Node movement autonomy): Οι κινητοί κόμβοι είναι γενικά αυτόνομες μονάδες που είναι σε θέση να κάνουν περιαγωγή (roaming) ανεξάρτητα. Αυτό σημαίνει ότι η ανακάλυψη ενός ιδιαίτερου κινητού κόμβου σε ένα μεγάλης κλίμακας ad-hoc δίκτυο, δεν μπορεί να γίνει εύκολα.
- **Άμορφο** (Amorphous): Η κινητικότητα των κόμβων και η ασύρματη συνδεσιμότητα επιτρέπουν στους κόμβους την αυθόρμητη είσοδο και έξοδο από το δίκτυο και την ακούσια δημιουργία και διακοπή συνδέσεων. Επομένως, η τοπολογία δικτύων δεν έχει καμία σταθερότητα σχετικά με

το μέγεθός της και τη μορφή της, οπότε αλλάζει συχνά. Οποιαδήποτε λύση ασφάλειας πρέπει να λάβει αυτό το χαρακτηριστικό γνώρισμα υπόψη.

- **Περιορισμός δύναμης** (Power limitation): Οι ad-hoc κινητοί hosts είναι μικροί και ελαφριοί και εφοδιάζονται συχνά με περιορισμένους πόρους δύναμης, όπως μικρές μπαταρίες. Αυτός ο περιορισμός προκαλεί μια ευπάθεια, δηλαδή, οι επιτιθέμενοι μπορεί να στοχεύσουν τις μπαταρίες μερικών κόμβων για να τους αποσυνδέσουν, οι οποίοι μπορούν να οδηγήσουν σε ένα χώρισμα (partition) του δικτύου. Αυτό καλείται επίθεση energy starvation attack ή sleep deprivation torture. Αυτό το χαρακτηριστικό γνώρισμα αντιπροσωπεύει επίσης έναν προκλητικό περιορισμό κατά το σχεδιασμό των λύσεων ασφάλειας για τα MANETs.
- **Περιορισμός δύναμης μνήμης και υπολογισμού** (Memory and computation power limitation): Οι ad-hoc ενεργοί κινητοί κόμβοι έχουν περιορίσει τις συσκευές αποθήκευσης και τις αδύναμες υπολογιστικές ικανότητες. Συνεπώς, οι υψηλές λύσεις ασφάλειας πολυπλοκότητας, όπως η συμμετρική ή ασύμμετρη κρυπτογράφηση στοιχείων, είναι δύσκολο να εφαρμοστούν.
- **Φυσική ευπάθεια κινητών συσκευών** (Mobile devices physical vulnerability): Οι κινητές συσκευές που χρησιμοποιούνται στα MANETs και στα κινητά δίκτυα γενικά, είναι ελαφριές και φορητές. Αυτό αντιπροσωπεύει την ευπάθεια, δεδομένου ότι οι συσκευές και οι πληροφορίες που αποθηκεύονται στις συσκευές μπορούν να κλαπούν εύκολα. Συνεπώς πρέπει να χρησιμοποιηθούν οι μηχανισμοί για την προστασία και των συσκευών αλλά και των πληροφοριών.

4.4 ΑΠΕΙΛΕΣ (THREATS)

Έχουμε χωρίσει τις απειλές που επηρεάζουν την ασφάλεια σε δυο κατηγορίες, επιθέσεις (attacks) και κακή συμπεριφορά (misbehaviour).

4.4.1 Επιθέσεις (Attacks)

Οι επιθέσεις περιλαμβάνουν οποιαδήποτε ενέργεια που στοχεύει ***σκόπιμα*** στο να προκαλέσει οποιαδήποτε ζημιά στο δίκτυο. Μπορούν να χωριστούν ανάλογα με την προέλευσή τους ή τη φύση τους. Η ταξινόμηση που βασίζεται στην προέλευση,

χωρίζει τις επιθέσεις σε δύο κατηγορίες, τις εξωτερικές (external) και τις εσωτερικές (internal), όπου μια ταξινόμηση βασισμένη στη φύση τους τις χωρίζει σε παθητικές (passive) και ενεργές επιθέσεις (active).

Εξωτερικές επιθέσεις (External attacks)

Περιλαμβάνει επιθέσεις που πραγματοποιούνται από έναν κόμβο ο οποίος δεν ανήκει στο λογικό δίκτυο ή δεν του επιτρέπεται η πρόσβαση σε αυτό. Οι εξωτερικές επιθέσεις, είναι τυπικά ενεργές επιθέσεις που έχουν στόχο π.χ. να προκαλέσουν συμφόρηση, να αναπαράγουν λανθασμένες πληροφορίες δρομολόγησης, να εμποδίσουν τις υπηρεσίες να εργαστούν σωστά ή να τις κλείσουν τελείως. Οι εξωτερικές επιθέσεις μπορούν τυπικά να εμποδιστούν χρησιμοποιώντας τυποποιημένους μηχανισμούς ασφαλείας όπως αναχώματα ασφαλείας (firewalls), κρυπτογραφία κ.λ.π.

Εσωτερικές επιθέσεις (Internal attacks)

Οι εσωτερικές επιθέσεις είναι τυπικά πιο σοβαρές επιθέσεις, αφού κακόβουλοι εσωτερικοί κόμβοι ανήκουν ήδη στο δίκτυο σαν εξουσιοδοτημένοι χρήστες και γι' αυτό προστατεύονται από τους μηχανισμούς ασφαλείας και τις υπηρεσίες που προσφέρει το δίκτυο. Γι' αυτό τέτοιοι κακόβουλοι εσωτερικοί κόμβοι που ίσως να λειτουργούν σε μια ομάδα, μπορούν να χρησιμοποιούν τα τυποποιημένα μέσα ασφάλειας για να προστατεύσουν τις επιθέσεις τους! Αυτό το είδος κακόβουλων χρηστών καλείται ***compromised node*** εφόσον οι ενέργειές τους εκθέτουν την ασφάλεια ολόκληρου του ad-hoc δικτύου.

Παθητικές επιθέσεις (Passive attacks)

Μία παθητική επίθεση είναι μία συνεχής συλλογή πληροφοριών η οποία μπορεί να χρησιμοποιηθεί αργότερα όταν πραγματοποιείται μία ενεργή επίθεση. Γι' αυτό, ο επιτιθέμενος κρυφακούει (eavesdrops) πακέτα και τα αναλύει προκειμένου να πάρει απαραίτητες πληροφορίες. Εξαιτίας της φύσης της ασύρματης ενδιάμεσης επικοινωνίας στην οποία υπάρχει μεγάλη δυνατότητα διαμοιρασμού, είναι πολύ πιο εύκολο για έναν επιτιθέμενο να πραγματοποιήσει μια τέτοια επίθεση σε αυτό το περιβάλλον παρά σε ένα παραδοσιακό ενσύρματο περιβάλλον. Η ασφάλεια που

πρέπει να αποδοθεί σε αυτή την περίπτωση, είναι η εμπιστευτικότητα της πληροφορίας.

Ενεργές επιθέσεις (Active attacks)

Περιλαμβάνει όλες τις επιθέσεις που πραγματοποιεί ο αντίπαλος όταν ενεργά αλληλεπιδρά με τα θύματα, όπως για παράδειγμα: ***sleep deprivation torture*** με στόχο τις μπαταρίες, ***hijacking*** στην οποία ο επιτιθέμενος παίρνει τον έλεγχο μιας επικοινωνίας μεταξύ δύο οντοτήτων και μασκαρεύεται σαν ένας από αυτούς, ***jamming*** η οποία προκαλεί μη διαθεσιμότητα καναλιού αφού το χρησιμοποιεί υπερβολικά, επιτίθεται ενάντια στα πρωτόκολλα δρομολόγησης, διαγράφει (deletion) τα δεδομένα ανταλλαγής κ.λ.π. Οι περισσότερες από αυτές τις επιθέσεις έχουν ως αποτέλεσμα denial of service (DoS), που είναι υποβιβασμός ή τέλος (halt) της επικοινωνίας μεταξύ των κόμβων.

4.4.2 Κακή Συμπεριφορά (Misbehaviour)

Ορίζουμε τις misbehaviour απειλές ως μη εξουσιοδοτημένη συμπεριφορά ενός εσωτερικού κόμβου που μπορεί αποτελεσματικά να προκαλέσει σκόπιμα ζημιά σε άλλους κόμβους. Σκοπός του κόμβου δεν είναι να πραγματοποιήσει μια επίθεση αλλά μπορεί να έχει άλλους σκοπούς όπως το να κερδίσει ένα άδικο πλεονέκτημα συγκριτικά με τους άλλους κόμβους. Για παράδειγμα, ένας μπορεί να μην εκτελέσει σωστά το MAC πρωτόκολλο με την πρόθεση να πάρει μεγαλύτερο εύρος ζώνης ή μπορεί να αρνηθεί να προωθήσει πακέτα σε άλλους για να εξοικονομήσει πόρους καθώς χρησιμοποιεί τους πόρους των άλλων και τους ρωτά για να προωθήσει τα δικά του πακέτα.

4.5 ΕΞΩΤΕΡΙΚΕΣ ΕΠΙΘΕΣΕΙΣ (EXTERNAL ATTACKS)

Οι εξωτερικές επιθέσεις κατευθύνονται στο φυσικό επίπεδο (physical layer) και στο επίπεδο ζεύξης δεδομένων (data link layer), εφόσον το αυθεντικοποιημένο πρωτόκολλο προστατεύει τα ανώτερα επίπεδα. Η ασφάλεια του φυσικού επιπέδου είναι δύσκολο να εξασφαλιστεί λόγω της πιθανής κινητής φύσης των κόμβων του ad-hoc δικτύου.

Χωρίζουμε τις εξωτερικές επιθέσεις σε δυο μεγάλες κατηγορίες: το παθητικό κρυφάκουσμα (passive eavesdropping), όπου ο αντίπαλος απλά ακούει τα σήματα

που μεταδίδονται και την ενεργή παρεμβολή (active interference) όπου ο αντίπαλος στέλνει σήματα ή δεδομένα που σχεδιάζονται για να διακόπτουν το δίκτυο με κάποιο τρόπο.

Μια ακόμα κατηγορία θα μπορούσε να είναι και η προσωποποίηση (Impersonation) που είναι ενεργή επίθεση (active attack) στην οποία ο αντίπαλος μπορεί να μασκαρευτεί ως ένας από τους φιλικούς κόμβους και να δώσει εσφαλμένες πληροφορίες στους άλλους κόμβους.

- **Passive Eavesdropping**

Αυτό μπορεί να επιτρέψει στους αναρμόδιους κόμβους να ακούσουν και να λάβουν μηνύματα συμπεριλαμβανομένης της ενημέρωσης (update) της δρομολόγησης. Ένας αναρμόδιος κόμβος θα είναι σε θέση να συγκεντρώσει τα δεδομένα που μπορούν να χρησιμοποιηθούν για να συμπεράνουν την τοπολογία του δικτύου και άλλες πληροφορίες όπως οι ταυτότητες των περισσότερο χρησιμοποιούμενων κόμβων που διαβιβάζουν ή λαμβάνουν τα δεδομένα. Ως εκ τούτου, μπορούν να απαιτηθούν τεχνικές για να κρύψουν τέτοιες πληροφορίες. Το κρυφάκουσμα είναι επίσης μια απειλή στην ιδιωτικότητα της θέσης. Σημειώστε ότι το παθητικό κρυφάκουσμα επίσης επιτρέπει στους αναρμόδιους κόμβους να ανακαλύψουν ότι ένα δίκτυο υπάρχει πραγματικά μέσα σε μια γεωγραφική θέση, ανιχνεύοντας ότι υπάρχει ένα παρόν σήμα. Έχουν αναπτυχθεί τεχνικές εφαρμοσμένης μηχανικής κυκλοφορίας για να καταπολεμήσουν αυτή την επίθεση.

- **Active Interference**

Η σημαντικότερη απειλή από την ενεργό παρέμβαση είναι το denial of service που προκαλείται με το φράξιμο του ασύρματου καναλιού επικοινωνίας ή την παραμόρφωση των επικοινωνιών. Τα αποτελέσματα τέτοιων επιθέσεων εξαρτώνται από τη διάρκειά τους και από τη χρήση του πρωτοκόλλου δρομολόγησης. Όσον αφορά τη δρομολόγηση των πακέτων δεδομένων, τα reactive πρωτόκολλα δρομολόγησης μπορούν να δουν τη denial of service επίθεση ως σπάσιμο συνδέσεων. Οι διαδικασίες συντήρησης διαδρομών θα αναγκάσουν τα περισσότερα πρωτόκολλα να αναφέρουν τη σύνδεση ως σπασμένη έτσι ώστε οι συμμετέχοντες κόμβοι να βρουν μια εναλλακτική διαδρομή. Τα proactive πρωτόκολλα δρομολόγησης δεν αντιδρούν

αμέσως στη μη παράδοση των πακέτων δεδομένων. Εάν η διαδρομή θεωρείται ότι έχει σπάσει, τελικά θα έχει διακοπεί προσωρινά (timed out) και θα είναι διαγραμμένη.

Πιθανώς ο σοβαρότερος τύπος επίθεσης denial of service, είναι μια επίθεση sleep deprivation torture, όπου η ενέργεια των κόμβων σπαταλιέται σκόπιμα. Με περιορισμένη δύναμη και πόρους, η πρόληψη τέτοιων επιθέσεων είναι εξαιρετικά σημαντική. Η ασφάλεια ενάντια σε τέτοιες επιθέσεις έχει ήδη μελετηθεί εκτενώς και έχει αναπτυχθεί από τους στρατιωτικούς για τα δίκτυα ραδιοπακέτων. Η τεχνολογία απλωμένου φάσματος έχει σχεδιαστεί να είναι ανθεκτική στο θόρυβο, την παρέμβαση, το μπλοκάρισμα (jamming) και την αναρμόδια εισβολή (intrusion).

Είναι συνετό να σημειωθεί ότι η προστασία ενάντια στη sleep deprivation torture επίθεση, δεν μπορεί να επιτευχθεί στο φυσικό στρώμα, ακόμα κι αν ο περιορισμός δύναμης είναι πράγματι μια φυσική ιδιότητα του στρώματος. Το γεγονός ότι τα επίπεδα δύναμης έχουν επιπτώσεις σε όλες τις λειτουργίες των ad-hoc δικτύων κάνει την ασφάλιση τέτοιων δικτύων ιδιαίτερα δύσκολη.

Υπάρχουν επίσης απειλές στην ακεραιότητα, π.χ. όπου ένας εξωτερικός επιτιθέμενος μπορεί να προσπαθήσει να επαναλάβει τα παλαιά μηνύματα ή να αλλάξει τη σειρά των μηνυμάτων. Τα παλαιά μηνύματα μπορούν να επαναληφθούν για να επανεισαγάγουν τις ξεπερασμένες (out-of-date) πληροφορίες. Οι πληροφορίες δρομολόγησης out-of-date, θα μπορούσαν να οδηγήσουν σε περαιτέρω denial of service δεδομένου ότι οι κόμβοι προσπαθούν να χρησιμοποιήσουν τις παλαιές αλλά άκυρες διαδρομές ή διαγράφουν τις τρέχουσες έγκυρες διαδρομές. Εάν το πρωτόκολλο δρομολόγησης αντιλαμβάνεται τους γείτονες με τη χρησιμοποίηση ελέγχων-παρακολούθησης των ληφθέντων πακέτων, η επανάληψη των παλαιών πακέτων μπορεί ψευδώς να οδηγήσει τους κόμβους στο να πιστεύουν ότι μια παλαιά σύνδεση με έναν γείτονα έχει γίνει και πάλι ενεργή και χρησιμοποιήσιμη.

Προσωποποίηση (Impersonation)

Οι επιθέσεις impersonation συνιστούν ένα σοβαρό ρίσκο ασφάλειας σε όλα τα επίπεδα μιας ad-hoc δικτύωσης. Αν δεν υποστηρίζεται κατάλληλη αυθεντικοποίηση των χρηστών, οι compromised nodes μπορούν π.χ. να εισχωρήσουν στο δίκτυο χωρίς να ανιχνευθούν ή να στείλουν εσφαλμένες πληροφορίες δρομολόγησης ενώ υποδύονται κάποιον άλλο έμπιστο κόμβο. Με την διαχείριση δικτύου ο επιτιθέμενος μπορεί να κερδίσει πρόσβαση στο σύστημα διαμόρφωσης σαν υπερ-χρήστης. Στο

επίπεδο υπηρεσίας, ένας κακόβουλος χρήστης μπορεί να έχει το πιστοποιημένο δημόσιο κλειδί του ακόμα και χωρίς τα κατάλληλα διαπιστευτήρια. Γι' αυτό οι επιθέσεις impersonation λαμβάνουν υπόψη όλες τις κρίσιμες λειτουργίες στα ad-hoc δίκτυα. Στο παράδειγμα της σχολικής αίθουσας, η impersonation επίθεση δεν είναι πιθανή ή ακόμα και εφικτή. Αν ένας κακόβουλος μαθητής προσωποποιηθεί τον εαυτό του σαν να είναι η συσκευή του δασκάλου, θα μπορούσε να έχει πρόσβαση ή να καταστρέψει δεδομένα που είναι αποθηκευμένα στη συσκευή του μαθητή ή του δασκάλου ή να τα ανταλλάξει μεταξύ τους. Το κέρδος της επίθεσης είναι μικρό. Πιθανότατα να γίνει αντιληπτή πολύ γρήγορα και οι πληροφορίες που μπορεί να μεταχειριστεί ή να έχει πρόσβαση, δεν είναι ιδιαίτερα κρίσιμες για να αξίζει τον κόπο η επίθεση. Στο άλλο παράδειγμα οι συνέπειες της επιτυχούς προσωποποίησης είναι πολύ πιο σοβαρές. Ένας εχθρικός κόμβος που ελέγχεται από τον εχθρό, μπορεί να εισχωρήσει στο ad-hoc δίκτυο χωρίς να τον ανιχνεύσουν και να προκαλέσει μόνιμη ζημιά στους άλλους κόμβους ή στις υπηρεσίες. Ένας κακόβουλος χρήστης είναι σε θέση να μασκαρευτεί ως ένας από τους φιλικούς κόμβους και να δώσει εσφαλμένες οδηγίες ή εσφαλμένη κατάσταση πληροφοριών στους άλλους κόμβους.

Οι απειλές προσωποποίησης μετριάζονται με την εφαρμογή δυνατών μηχανισμών αυθεντικοποίησης στα πλαίσια (contexts) όπου ένας χρήστης θα πρέπει να είναι σε θέση να εμπιστευτεί την προέλευση των δεδομένων που έλαβε ή αποθήκευσε. Πιο συχνά αυτό σημαίνει ότι σε κάθε επίπεδο η εφαρμογή των ψηφιακών υπογραφών ή τα ίχνη των κλειδιών (keyed fingerprints) πάνω από τα μηνύματα δρομολόγησης, η διαμόρφωση ή η κατάσταση των πληροφοριών ή η ανταλλαγή του φορτίου των δεδομένων της υπηρεσίας, είναι σε χρήση. Οι ψηφιακές υπογραφές που εφαρμόζονται με την κρυπτογράφηση δημόσιου κλειδιού, είναι ένα προβληματικό ζήτημα μέσα στα ad-hoc δίκτυα καθώς απαιτούν μία επαρκή και ασφαλή υπηρεσία διαχείρισης κλειδιού και σχετικά πολύ υπολογιστική ισχύ. Γι' αυτό σε αρκετές περιπτώσεις, είναι αναγκαίες λύσεις όπως η χρήση των συναρτήσεων keyed hash ή εκ των προτέρων πιστοποιημένα κλειδιά και ταυτοποιητές συνόδων (session identifiers). Εν τούτοις, δεν απομακρύνουν την απαίτηση για ασφαλή διαχείριση κλειδιού ή κατάλληλους μηχανισμούς προστασίας εμπιστευτικότητας.

4.6 ΕΣΩΤΕΡΙΚΕΣ ΕΠΙΘΕΣΕΙΣ (INTERNAL ATTACKS)

Οι απειλές που τίθενται από τους εσωτερικούς κόμβους είναι πολύ σοβαρές, δεδομένου ότι οι εσωτερικοί κόμβοι θα έχουν τις απαραίτητες πληροφορίες για να συμμετέχουν σε διανεμημένες διαδικασίες. Οι εσωτερικοί κόμβοι μπορούν να συμπεριφερθούν απρεπώς με ποικίλους διαφορετικούς τρόπους. Προσδιορίζουμε τέσσερις κατηγορίες απρεπούς συμπεριφοράς: αποτυχημένοι κόμβοι (failed nodes), άσχημα αποτυχημένοι κόμβοι (badly failed nodes), εγωιστικοί κόμβοι (selfish nodes) και κακόβουλοι κόμβοι (malicious nodes).

Σημειώστε ότι δύο κόμβοι απρεπούς συμπεριφοράς μέσα στην ίδια κατηγορία μπορούν να επιδείξουν διαφορετικούς βαθμούς ανακριβούς συμπεριφοράς κόμβων. Παραδείγματος χάριν, μερικοί κόμβοι θα είναι πιο εγωιστικοί από άλλους. Επίσης, ένας κόμβος μπορεί να καταδείξει τις συμπεριφορές περισσότερες από μια κατηγορίες - πράγματι, αυτό μπορεί ακόμη και να είναι η χαρακτηριστική περίπτωση.

💣 Failed Nodes

Οι αποτυχημένοι κόμβοι είναι απλά εκείνοι που είναι ανίκανοι να εκτελέσουν μια λειτουργία. Αυτό θα μπορούσε να είναι για πολλούς λόγους, συμπεριλαμβανομένης της διακοπής ισχύος και των περιβαλλοντικών γεγονότων. Τα κύρια ζητήματα για ad-hoc δρομολόγηση αποτυγχάνουν να ενημερώσουν τις δομές δεδομένων ή την αποτυχία να σταλούν ή να διαβιβαστούν τα πακέτα δεδομένων, συμπεριλαμβανομένων των μηνυμάτων δρομολόγησης. Αυτό είναι σημαντικό δεδομένου ότι εκείνα τα πακέτα δεδομένων μπορούν να περιέχουν σημαντικές πληροφορίες που αναφέρονται στην ασφάλεια, όπως τα δεδομένα αυθεντικοποίησης και οι πληροφορίες δρομολόγησης. Μια αποτυχία στην προώθηση μηνυμάτων λάθους θα σημαίνει ότι οι αρχικοί κόμβοι δεν θα μάθουν για τις σπασμένες συνδέσεις και θα συνεχίσουν να προσπαθούν να τις χρησιμοποιήσουν, προκαλώντας δυσχέρειες. Η απειλή του να υπάρχουν αποτυχημένοι κόμβοι είναι η σοβαρότερη, εάν οι αποτυχημένοι κόμβοι απαιτούνται ως τμήμα μιας διαδρομής έκτακτης ανάγκης ή της δημιουργίας μέρους μιας ασφαλούς διαδρομής.

💣 Badly Failed Nodes

Οι άσχημα αποτυχημένοι κόμβοι εκθέτουν τα χαρακτηριστικά γνωρίσματα των αποτυχημένων κόμβων όπως η μη αποστολή ή η προώθηση των πακέτων

δεδομένων ή των μηνυμάτων διαδρομών. Επιπλέον μπορούν επίσης να στείλουν τα ψεύτικα μηνύματα δρομολόγησης, τα οποία είναι ακόμα σωστά σχηματοποιημένα, αλλά περιέχουν ψεύτικες πληροφορίες και είναι μια απειλή για την ακεραιότητα του δικτύου. Παραδείγματος χάριν, τα ψεύτικα αιτήματα διαδρομών για έναν κόμβο που δεν υπάρχει, μπορούν να κυκλοφορήσουν στο ad-hoc δίκτυο καταναλώνοντας το πολύτιμο εύρος ζώνης, δεδομένου ότι κανένας κόμβος δεν μπορεί να παρέχει μια κατάλληλη απάντηση. Τα περιττά αιτήματα διαδρομών για τις διαδρομές που έχουν ήδη οι άσχημα αποτυχημένοι κόμβοι, επίσης στέλνονται. Οι ψεύτικες απαντήσεις διαδρομών σε απάντηση ενός αληθινού αιτήματος διαδρομών, μπορεί να οδηγήσουν σε ψεύτικες διαδρομές που ιδρύονται και διαδίδονται μέσω του δικτύου. Τα ψεύτικα μηνύματα λάθους διαδρομών θα αναγκάσουν τις εργαζόμενες ζεύξεις να χαρακτηριστούν ως σπασμένες, κινώντας ενδεχομένως μια διαδικασία συντήρησης διαδρομών.

Τα πρωτόκολλα που στηρίζονται στις λειτουργίες αντίληψης γειτόνων (neighbor sensing operations) είναι επίσης τρωτά, δεδομένου ότι τα ψεύτικα μηνύματα μπορούν να προκαλέσουν τους κόμβους να «αισθάνονται» παραπάνω γείτονες. Αυτό ισχύει ιδιαίτερα στα πρωτόκολλα όπως το LANMAR, το οποίο δε στηρίζεται σε ένα συγκεκριμένο μήνυμα αίσθησης γειτόνων, αλλά εάν ένα μήνυμα ελέγχου δρομολόγησης που περιέχει μια άγνωστη διεύθυνση προέλευσης παραλαμβάνεται άμεσα, κατόπιν αυτή η διεύθυνση χρησιμοποιείται ως νέος γείτονας.

Τα πρωτόκολλα όπως το AODV περιλαμβάνουν μέσα στα μηνύματα λάθους διαδρομών έναν κατάλογο επιρρεπών κόμβων στους οποίους τα λάθη διαδρομών πρέπει να είναι διπλής εκπομπής (unicast). Εάν αυτός ο κατάλογος είναι μεγάλος, τότε η απειλή όχι μόνο έχει επιπτώσεις στην ακεραιότητα του δικτύου, αλλά είναι επίσης μια denial of service επίθεση, δεδομένου ότι οι πόροι και το εύρος ζώνης καταναλώνονται από το μεγάλο όγκο των μηνυμάτων λάθους διαδρομών που στέλνονται και τα περιττά αιτήματα και οι απαντήσεις διαδρομών χρησιμοποιούνται για να βρουν τις εναλλακτικές διαδρομές.

Selfish Nodes

Οι εγωιστικοί κόμβοι εκμεταλλεύονται το πρωτόκολλο δρομολόγησης για δικό τους πλεονέκτημα π.χ. για να ενισχύσουν την απόδοση ή να σώσουν τους πόρους. Οι εγωιστικοί κόμβοι χαρακτηρίζονται από την απροθυμία τους να συνεργαστούν όταν το πρωτόκολλο το απαιτεί, οπότε υπάρχει ένα σχετικό προσωπικό

κόστος και θα εκθέσει τις ίδιες συμπεριφορές με τους αποτυχημένους κόμβους, ανάλογα με το ποιες διαδικασίες αποφασίζουν να μην αποδώσουν. Η μείωση πακέτων είναι η κύρια επίθεση των εγωιστικών κόμβων, όπου τα περισσότερα πρωτόκολλα δρομολόγησης δεν έχουν κανέναν μηχανισμό για να ανιχνεύσουν εάν τα πακέτα δεδομένων έχουν διαβιβαστεί, με το DSR να είναι η μόνη εξαίρεση. Κατά συνέπεια, ένα άλλο σχέδιο συμπεριφοράς που λαμβάνεται υπόψη είναι η μερική μείωση, η οποία θα μπορούσε δύσκολα να αποτραπεί και να ανιχνευθεί. Είναι σημαντικό να υπογραμμιστεί ότι, σε αυτό το πρότυπο, οι εγωιστικοί κόμβοι δεν εκτελούν οποιαδήποτε δράση για να συμβιβαστεί η ακεραιότητα το δικτύου με την ενεργή εισαγωγή ανακριβών πληροφοριών.

💣 Malicious Nodes

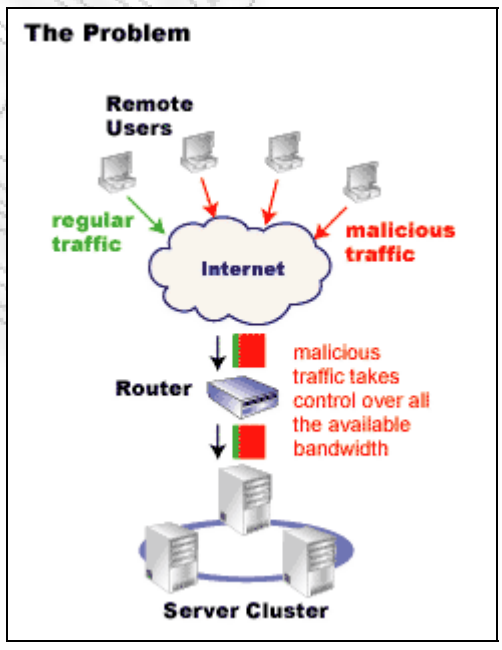
Οι κακόβουλοι κόμβοι στοχεύουν να διακόψουν σκόπιμα τη σωστή λειτουργία του πρωτοκόλλου δρομολόγησης, αρνούμενοι τις υπηρεσίες του δικτύου αν είναι δυνατόν. Ως εκ τούτου, μπορούν να επιδείξουν οποιαδήποτε από τις συμπεριφορές που παρουσιάζονται από τους άλλους τύπους αποτυχημένων κόμβων. Ο αντίκτυπος των ενεργειών ενός κακόβουλου κόμβου αυξάνεται πολύ εάν είναι η μόνη σύνδεση μεταξύ ομάδων των γειτονικών κόμβων.

i. Denial of Service

Η denial of service απειλή είτε παράγεται από μια μη σκόπιμη αποτυχία είτε από μια κακόβουλη ενέργεια, είναι ένα πολύ σοβαρό ρίσκο ασφάλειας σε οποιοδήποτε κατανεμημένο σύστημα. Οι συνέπειες αυτών των επιθέσεων, εν τούτοις βασίζονται στην περιοχή εφαρμογής του ad-hoc δικτύου. Στο παράδειγμα με την σχολική τάξη που αναφέρθηκε σε πιο πάνω παράγραφο, οποιοσδήποτε από τους κόμβους είτε η κεντραρισμένη συσκευή του δασκάλου είτε τα φορητά σύνεργα των μαθητών, μπορούν να καταρρεύσουν ή να κλείσουν τελείως χωρίς να καταστραφεί απολύτως τίποτα. Η τάξη μπορεί να συνεχίσει να εργάζεται κανονικά χρησιμοποιώντας άλλα εργαλεία. Αντιθέτως, στο σενάριο με το πεδίο μάχης, η επαρκής αποστολή των στρατιωτών εξαρτάται πλήρως από την κατάλληλη λειτουργία του ad-hoc δικτύου στο οποίο εργάζονται οι συσκευές τους. Αν ο εχθρός μπορεί να τερματίσει το δίκτυο, η ομάδα των στρατιωτών θα πρέπει να διαιρεθεί σε

τρωτές μονάδες που δεν μπορούν να επικοινωνήσουν ούτε μεταξύ τους ούτε με το αρχηγείο τους.

Η denial of service επίθεση έχει πολλές μορφές: ο κλασσικός τρόπος είναι να πλημμυρίσει οποιοδήποτε κεντραρισμένο πόρο έτσι ώστε να μη λειτουργεί σωστά ή να καταρρεύσει, αλλά σε ένα ad-hoc δίκτυο αυτό δεν είναι εφαρμόσιμη προσέγγιση εξαιτίας της κατανομής της υπευθυνότητας. Η κατανεμημένη denial of service επίθεση είναι πολύ πιο σοβαρή απειλή: εάν οι επιτιθέμενοι έχουν αρκετή υπολογιστική ισχύ (computing power) και εύρος ζώνης για να λειτουργήσουν, μικρότερα ad-hoc δίκτυα μπορεί να καταρρεύσουν ή να γίνουν υπερπλήρεις σχετικά εύκολα. Είναι ωστόσο πιο σοβαρές απειλές για τα ad-hoc δίκτυα. Οι compromised nodes μπορούν να είναι σε θέση να αναδιαμορφώσουν το πρωτόκολλο δρομολόγησης ή κάποιο τμήμα αυτού έτσι ώστε να στέλνουν πληροφορίες δρομολόγησης αρκετά συχνά ώστε να προκαλούν συμφόρηση και να εμποδίζουν τους κόμβους να κερδίζουν νέες πληροφορίες γύρω από την αλλαγμένη τοπολογία του δικτύου. Στη χειρότερη περίπτωση ο αντίπαλος μπορεί να αλλάξει το πρωτόκολλο δρομολόγησης για να λειτουργεί αυθαίρετα ή ακόμα και με τον μη έγκυρο τρόπο που θέλει ο επιτιθέμενος. Αν οι compromised nodes και οι αλλαγές στο πρωτόκολλο δρομολόγησης δεν ανιχνεύονται, οι συνέπειες είναι σοβαρές, αφού από την οπτική των κόμβων, το δίκτυο δείχνει να δουλεύει κανονικά. Αυτού του είδους η μη έγκυρη λειτουργία του δικτύου που αρχίζει από κακόβουλος κόμβους, καλείται **byzantine failure**.



Εικόνα 22. Μια επίθεση DoS

ii. Spoofing

Ο κακόβουλος κόμβος μπορεί να μασκαρευτεί ως άλλη οντότητα κατά τη διάρκεια εύρεσης υπηρεσίας. Μπορεί να παριστάνεται ως:

- Ένας κόμβος FW. Επάνω στη λήψη ενός νόμιμου μηνύματος υπηρεσιών, μπορεί να μη διαβιβάσει το μήνυμα σε άλλους κόμβους. Η ανακάλυψη υπηρεσιών δεν μπορεί να πραγματοποιηθεί εάν αυτός ο κόμβος FW είναι η μόνη σύνδεση μεταξύ δύο κόμβων. Ο στόχος απειλής θα ήταν οι προοριζόμενοι παραλήπτες των μηνυμάτων υπηρεσιών.
- Ένας κόμβος SU και να μεταδώσει ένα μήνυμα SrvReq μέσω του δικτύου. Ένας κόμβος SP ή SD που λαμβάνει το μήνυμα μπορεί να σκεφτεί ότι αλληλεπιδρούν με έναν νόμιμο κόμβο SU. Ο στόχος απειλής είναι εδώ η SP, SD ή ακόμα και ένας κόμβος FW.
- Ένας άλλος νόμιμος κόμβος SP που προσφέρει υπηρεσίες σε έναν άγνωστο κόμβο SU.
- Ένας κόμβος SD που αναγγέλλει την παρουσία του στο δίκτυο. Αυτός ο κακόβουλος κόμβος SD μπορεί να είναι κοντινότερος (λιγότερα hops μακριά) σε μερικοί από τους κόμβους SU ή SP. Μπορούν έπειτα να επιλέξουν να αλληλεπιδράσουν με αυτόν τον κακόβουλο κόμβο SD αντί ενός νόμιμου που είναι πιο πέρα.

Οι στόχοι απειλής είναι οι οντότητες στις οποίες ο κακόβουλος κόμβος θα μεταμφιέζεται. Το spoofing αποτελεί ενεργή (active) επίθεση.

iii. Λαθροχειρία (Tampering)

Ο κακόβουλος κόμβος ίσως να μπορεί να συλλάβει και να τροποποιήσει τα νόμιμα μηνύματα υπηρεσιών που περνούν από το δίκτυο με έναν από τους ακόλουθους τρόπους:

- ❖ Αλλαγή των νόμιμων μηνυμάτων υπηρεσιών με την αλλαγή του περιεχομένου τους. Κατά συνέπεια, οι προοριζόμενοι παραλήπτες των μηνυμάτων υπηρεσιών δεν θα παρουσιαστούν με τις εξακριβωμένες πληροφορίες υπηρεσιών. Αυτό δυσκολεύει (compromises) πολύ τη διαδικασία ανακαλύψεων υπηρεσιών. Οι άμεσοι στόχοι απειλής είναι τα μηνύματα υπηρεσιών, ενώ οι έμμεσοι στόχοι απειλής είναι οι προοριζόμενοι παραλήπτες των αλλαγμένων μηνυμάτων.

- ❖ Διαγραφή των νόμιμων μηνυμάτων υπηρεσιών. Οι προοριζόμενοι παραλήπτες των μηνυμάτων υπηρεσιών δεν θα είναι σε θέση να λάβουν τα μηνύματα. Η ανακάλυψη υπηρεσιών έπειτα δεν θα πραγματοποιηθεί δεδομένου ότι πρέπει. Αυτή η απειλή έχει την ίδια επίδραση με έναν εγωιστικό κόμβο που δεν θέλει να διαβιβάσει τα μηνύματα SrvReq και SrvAdv σε άλλους κόμβους. Σε αυτήν την περίπτωση, ο άμεσος στόχος απειλής είναι το διαγραμμένο μήνυμα υπηρεσιών, ενώ ο έμμεσος στόχος απειλής είναι ο προοριζόμενος παραλήπτης του αρχικού μηνύματος υπηρεσιών.
- ❖ Εισαγωγή ψευδών μηνυμάτων υπηρεσιών. Ένας κακόβουλος κόμβος μπορεί να μεταδώσει ψευδή (fraudulent) μηνύματα υπηρεσιών (π.χ., SrvReq, SrvAdv, ή DirAdv) στο δίκτυο. Αυτή η απειλή είναι παρόμοια με τη spoofing απειλή που συζητείται ανωτέρω. Οι στόχοι απειλής είναι εδώ οι προοριζόμενοι παραλήπτες των ψευδών μηνυμάτων.

Είναι φανερό πως το tampering είναι ενεργής απειλή.

iv. Repudiation

Ένας κακόβουλος κόμβος μπορεί αργότερα να αρνηθεί να εκτελέσει μια ορισμένη ενέργεια. Παραδείγματος χάριν, ένας κακόβουλος κόμβος SU (Service User), SP (Service Provider) ή SD (Service Directory) μπορεί να αρνηθεί ότι έχει στείλει ένα μήνυμα SrvReq, SrvAdv ή DirAdv, αντίστοιχα. Ομοίως, μπορεί να αρνηθεί ότι έχει λάβει ένα συγκεκριμένο μήνυμα υπηρεσιών. Ο στόχος απειλής θα ήταν η οντότητα με την οποία αλληλεπιδρούσε ο κακόβουλος κόμβος. Η repudation είναι μια ενεργός απειλή.

v. Information Disclosure

Το κρυφάκουσμα είναι ιδιαίτερα απλό σε μια εγκατάσταση όπως το ad-hoc δίκτυο, δεδομένου ότι ο αρχικός τρόπος επικοινωνίας μεταξύ των κόμβων είναι ένα ασύρματο κανάλι.

Κατά τη διάρκεια της διαδικασίας ανακαλύψεων υπηρεσιών, ένας κακόβουλος κόμβος είναι σε θέση να κρυφακούσει τα μηνύματα υπηρεσιών που ανταλλάσσονται μεταξύ των οντοτήτων υπηρεσιών, ή της μετάδοσης μέσω του δικτύου από τους κόμβους SU ή SP. Ένας κατάλογος των υπηρεσιών που

απαιτούνται και που διαφημίζονται μπορεί έτσι εύκολα να συνταχθεί και αυτό αποτελεί μια επίθεση απαρίθμησης (enumeration attack). Από τις συγκεντρωμένες πληροφορίες, ένας κακόβουλος κόμβος μπορεί να μάθει τα εξής: τον τύπο υπηρεσιών που καλούνται από τους κόμβους SU, τον τύπο των υπηρεσιών που προσφέρονται από τους κόμβους SP, ποιοι και που είναι οι κόμβοι SD και την τοπολογία των δικτύων. Τέτοιες πληροφορίες μπορούν να είναι εξαιρετικά χρήσιμες για τον κακόβουλο κόμβο και μπορούν να χρησιμοποιηθούν στη συνέχεια: για να συμπεράνουν ή να προβλέψουν τα μελλοντικά σχέδια ανακαλύψεων υπηρεσιών ή ως νοημοσύνη για την προώθηση των επόμενων επιθέσεων (π.χ. επαναλαμβάνοντας ορισμένα μηνύματα). Η κοινοποίηση των πληροφοριών υπηρεσιών μπορεί να θεωρηθεί παραβίαση της ιδιωτικότητας των μεμονωμένων οντοτήτων.

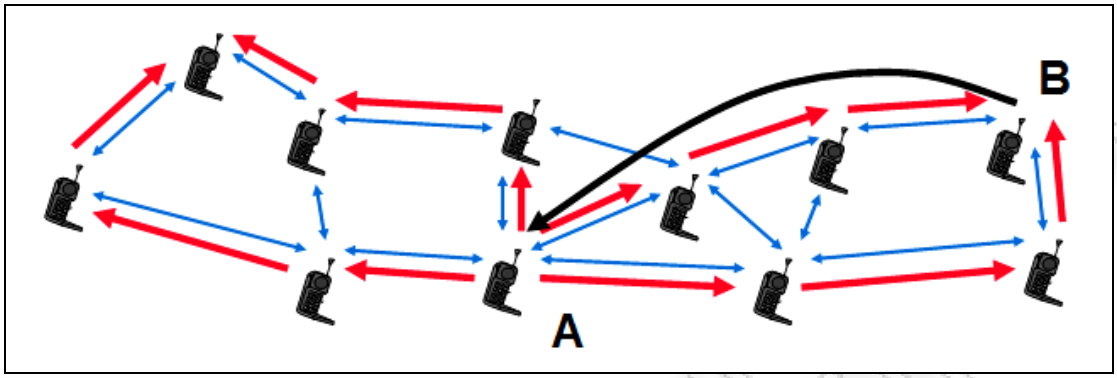
Οι άμεσοι στόχοι απειλής είναι επομένως τα μηνύματα υπηρεσιών και οι έμμεσοι στόχοι απειλής περιλαμβάνουν τη μυστικότητα ή ακόμα και τη διαθεσιμότητα των κόμβων SU, SP και SD. Μια απειλή κοινοποίησης πληροφοριών δεν αναστατώνει τη διαδικασία ανακαλύψεων υπηρεσιών. Πολύ συχνά, οι νόμιμες οντότητες υπηρεσιών μπορεί να μην καταλάβουν καν ότι πραγματοποιείται μια τέτοια επίθεση. Γι' αυτό αυτός ο τύπος απειλής είναι συνήθως γνωστός ως παθητική απειλή.

vi. Elevation Of Privileges

Αυτό συμβαίνει όταν ένας κακόβουλος κόμβος, με μερικά παράνομα μέσα, είναι σε θέση να κερδίσει περισσότερα προνόμια από όσα ήδη έχει. Αυτή η απειλή πραγματοποιείται σε σχέση με την απειλή spoofing. Όταν ένας κακόβουλος κόμβος είναι σε θέση να μεταμφιεστεί ως μια άλλη οντότητα (π.χ. ένας κόμβος SU, SP, SD ή FW), αυτό υποθέτει τα προνόμια και τις ικανότητες εκείνης της οντότητας.

Πρέπει να σημειωθεί ότι οι προαναφερθείσες απειλές εμφανίζονται σπάνια στην απομόνωση. Τις περισσότερες φορές, μια απειλή μπορεί να οδηγήσει σε άλλη, δεδομένου ότι είναι αλληλένδετες.

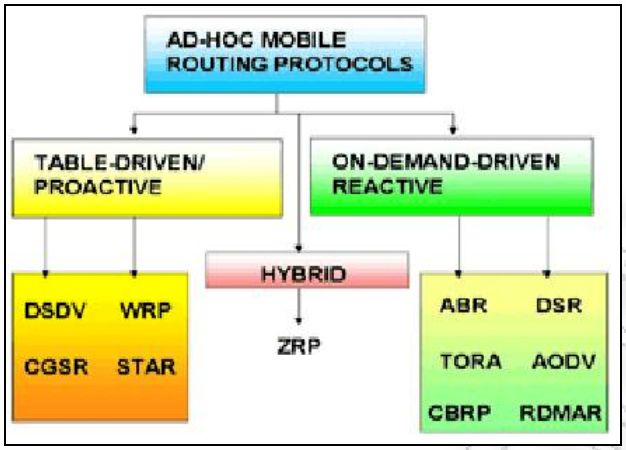
5 ΑΣΦΑΛΕΙΑ ΔΡΟΜΟΛΟΓΗΣΗΣ



Εικόνα 23. Δρομολόγηση στα ad-hoc δίκτυα

Ένα πρωτόκολλο δρομολόγησης ενός MANET βρίσκει διαδρομές ανάμεσα στους κόμβους στους οποίους προωθούνται τα πακέτα δεδομένων προς τον τελικό προορισμό. Σε αντίθεση με τα παραδοσιακά δίκτυα, τα πρωτόκολλα δρομολόγησης των MANETs πρέπει να είναι προσαρμόσιμα για να αντιμετωπίσουν τα χαρακτηριστικά που παρουσιάστηκαν παραπάνω και ιδιαίτερα τις συχνές αλλαγές στην τοπολογία του δικτύου. Το πρόβλημα-πρόκληση της δρομολόγησης των ad-hoc δικτύων έχει μελετηθεί εκτενώς, ιδιαίτερα από την ομάδα του MANET, την Internet Engineering Task Force (IETF). Αυτές οι μελέτες έχουν κατασταλάξει σε διάφορα πρωτόκολλα, τα οποία μπορούν να χωριστούν σε δύο κατηγορίες: proactive (table driven) και reactive (on-demand). Τα reactive πρωτόκολλα είναι πιο προσαρμόσιμα στα MANET περιβάλλοντα από ότι τα proactive. Η Εικόνα 24 δείχνει τις κατηγορίες των πρωτοκόλλων δρομολόγησης των ad-hoc δικτύων.

Εν τούτοις, το πρόβλημα με όλες αυτές τις λύσεις είναι ότι εμπιστεύονται όλους τους κόμβους και δε λογοδοτούν για την ασφάλεια, γι' αυτό είναι πολύ τρωτά σε επιθέσεις. Είναι πολύ σημαντικό να ασφαλίζουμε το πρωτόκολλο δρομολόγησης. Αν το πρωτόκολλο δρομολόγησης υπονομεύεται (subverted) και τα μηνύματα μπορούν να μεταβάλλονται στη μεταφορά, τότε καμία ασφάλεια στα πακέτα δεδομένων των ανώτερων επιπέδων μπορεί να μετριάσει τις απειλές.



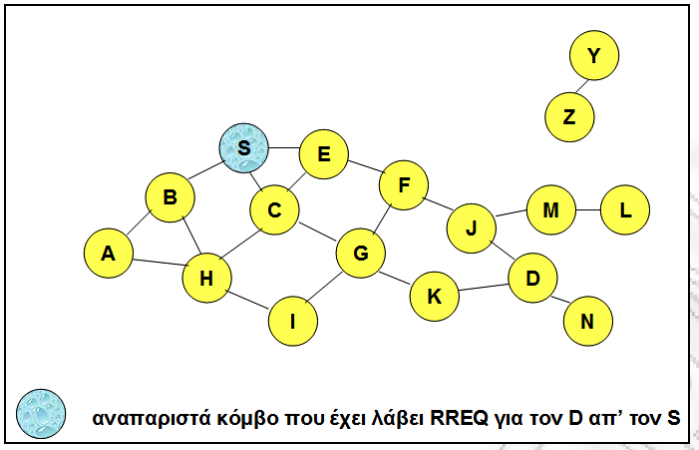
Εικόνα 24. Οι κατηγορίες των πρωτοκόλλων δρομολόγησης των ad-hoc δικτύων

5.1 DSR (DYNAMIC SOURCE ROUTING)

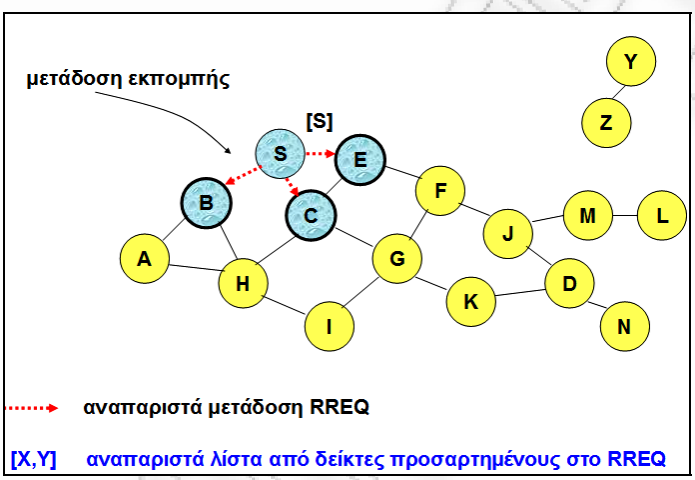
Το DSR είναι reactive πρωτόκολλο που βασίζεται στην προσέγγιση δρομολόγησης πηγής (source route). Η βασική αρχή αυτής της προσέγγισης είναι ότι επιλέγεται όλη η διαδρομή από την πηγή και τοποθετείται σε κάθε πακέτο που στέλνεται. Κάθε κόμβος κρατά στη μνήμη του τις δρομολογήσεις πηγής που έμαθε. Όταν πρέπει να στείλει ένα πακέτο, πρώτα ελέγχει μέσα στη μνήμη του για την ύπαρξη τέτοιας διαδρομής. Αν δεν είναι διαθέσιμος μέσα στη μνήμη ο κατάλληλος προορισμός, ο κόμβος πραγματοποιεί μία εύρεση διαδρομής εκπέμποντας πακέτο ερώτησης (RREQ) μέσω του δικτύου. Όταν λάβει το RREQ, ο κόμβος ψάχνει μια διαδρομή μέσα στη μνήμη του για τον προορισμό του RREQ. Όταν τη βρει, στέλνει πακέτο απάντησης (RREP) στην πηγή. Εν τούτοις, αν δεν υπάρχει κατάλληλη διαδρομή ο κόμβος προσθέτει τη διεύθυνσή του στο RREQ και συνεχίζει να εκπέμπει.

Όταν ένας κόμβος ανιχνεύσει μια αποτυχία διαδρομής, στέλνει πακέτο λάθους (RER) στην πηγή που χρησιμοποιεί την ίδια ζεύξη και μετά ξαναρχίζει τη διαδικασία εύρεσης διαδρομής.

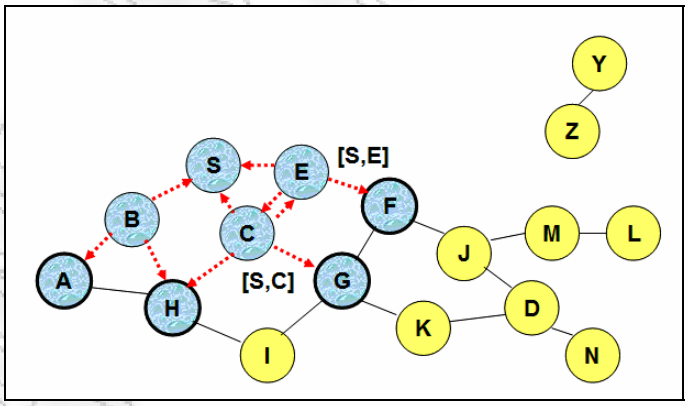
Η ανακάλυψη δρομολογίου φαίνεται στις Εικόνες 25, 26, 27, 28, 29 και 30:



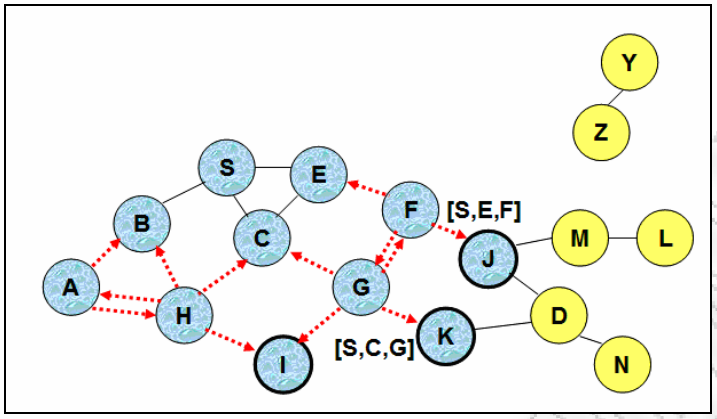
Εικόνα 25. Ο κόμβος αφετηρία S 'πλημμυρίζει' ένα πακέτο Αίτησης Δρομολογίου (Route Request - RREQ)



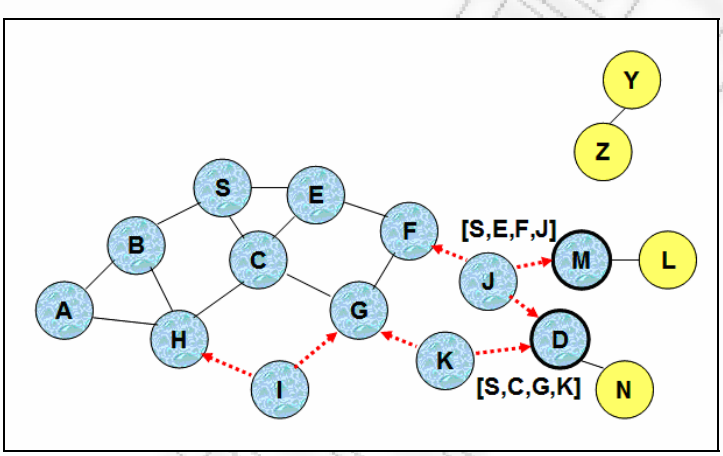
Εικόνα 26. Αρχίζει η μετάδοση εκπομπής του RREQ



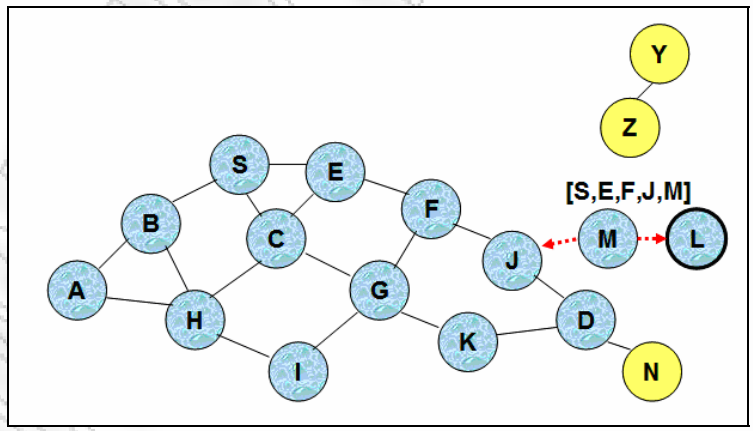
Εικόνα 27. Ο κόμβος H δέχεται πακέτο από δύο γείτονες: πιθανότητα σύγκρουσης



Εικόνα 28. Ο κόμβος C δέχεται RREQ από τον G και τον H αλλά δεν το προωθεί ξανά γιατί ο κόμβος C έχει ήδη προωθήσει RREQ μια φορά

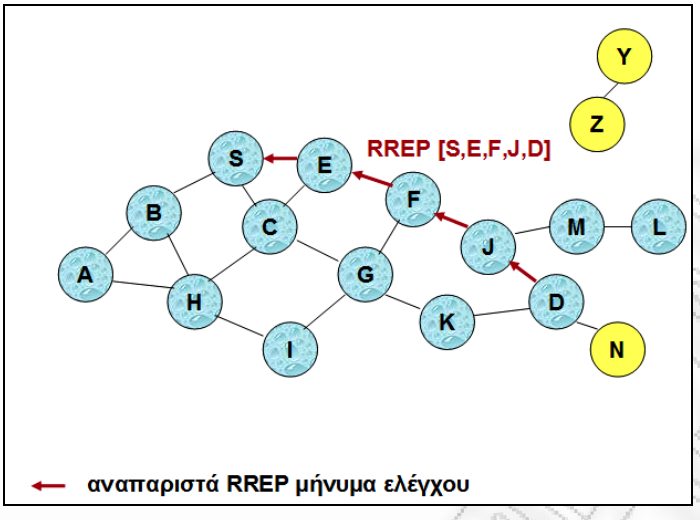


Εικόνα 29. Οι κόμβοι J και K μεταδίδουν και οι δύο RREQ στον κόμβο D. Εφόσον οι κόμβοι J και K κρύβονται ο ένας από τον άλλο, οι μεταδόσεις τους μπορεί να συγκρουστούν



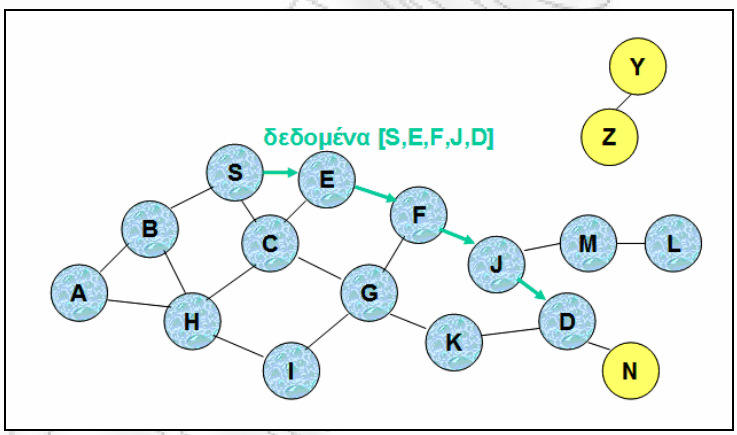
Εικόνα 30. Ο κόμβος D δεν προωθεί RREQ, γιατί είναι ο επιθυμητός στόχος της ανακάλυψης του δικτύου

Η απάντηση δρομολογίου φαίνεται στην Εικόνα 31:



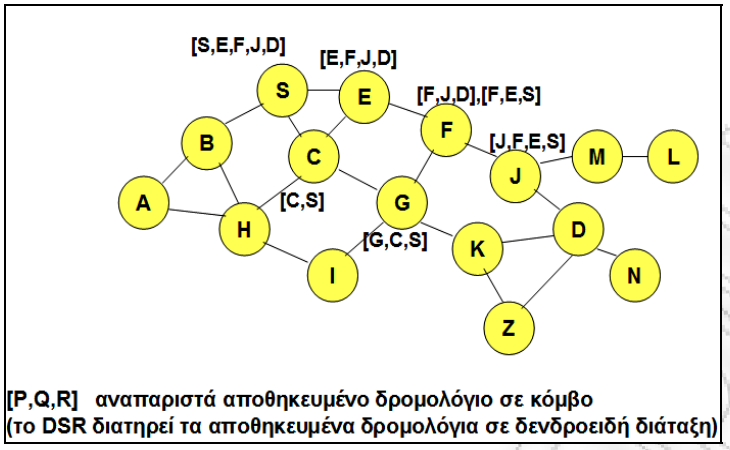
Εικόνα 31. Ο προορισμός D λαμβάνοντας το πρώτο RREQ, στέλνει ένα πακέτο Απάντησης Δρομολογίου (Route Reply - RREP) μέσω του αντίστροφου δρομολογίου. Το RREP περιλαμβάνει το δρομολόγιο από τον S στον D, μέσω του οποίου το RREQ έφτασε στον κόμβο D

Η παράδοση δεδομένων στο DSR φαίνεται στην ακόλουθη Εικόνα (Εικόνα 32):

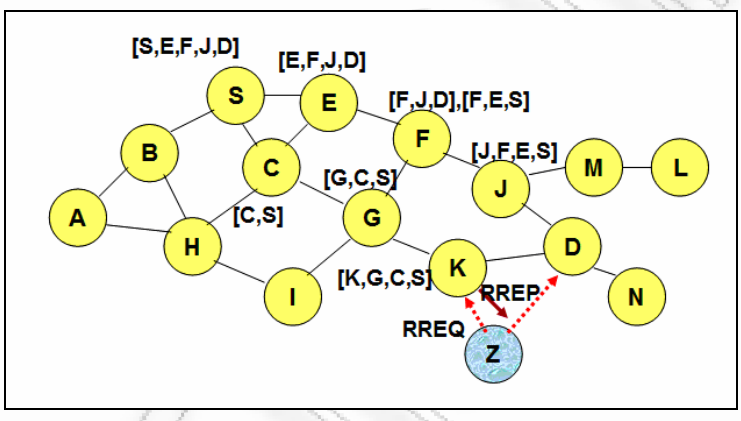


Εικόνα 32. Ο κόμβος S δεχόμενος το RREP, αποθηκεύει το δρομολόγιο που περιέχεται στο RREP. Όταν ο κόμβος S στέλνει ένα πακέτο δεδομένων στον D, ολόκληρο το δρομολόγιο περιέχεται στην επικεφαλίδα του πακέτου γι' αυτό και το όνομα δρομολόγηση πηγής. Οι ενδιάμεσοι κόμβοι χρησιμοποιούν το πηγαίο δρομολόγιο που περιέχεται σε ένα πακέτο, για να καθορίσουν σε ποιόν πρέπει να προωθηθεί το πακέτο

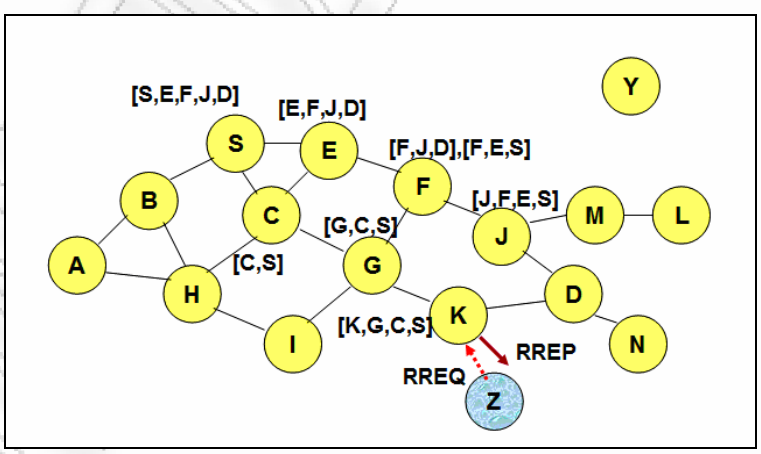
Στις Εικόνες 33, 34 και 35 που έπονται, παρουσιάζεται η χρήση της αποθήκευσης δρομολογίων:



Εικόνα 33. Όταν ο κόμβος S μαθαίνει πως ένα δρομολόγιο προς τον κόμβο D καταστρέφεται, χρησιμοποιεί ένα άλλο δρομολόγιο απ' την τοπική του μνήμη, αρκεί ένα τέτοιο δρομολόγιο προς τον D να υπάρχει εκεί - αλλιώς, ο κόμβος S αρχικοποιεί νέα ανακάλυψη μονοπατιού

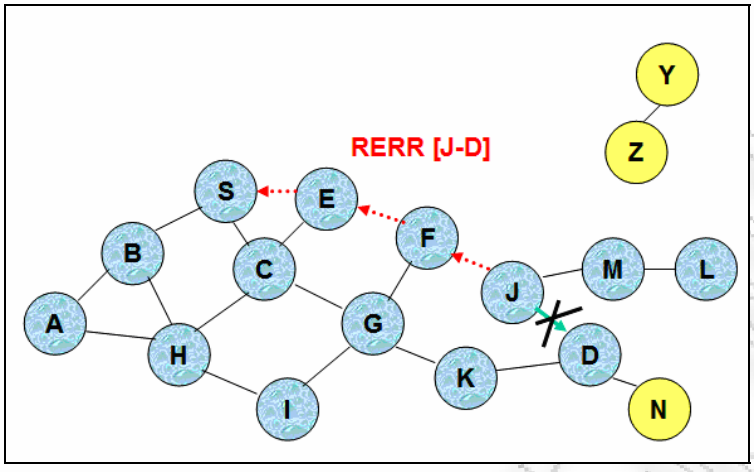


Εικόνα 34. Όταν ο κόμβος Z στέλνει μια αίτηση δρομολογίου για τον κόμβο C, ο κόμβος K επιστρέφει μια απάντηση δρομολογίου [Z,K,G,C] προς τον κόμβο Z, συνήθως χρησιμοποιώντας αποθηκευμένο δρομολόγιο



Εικόνα 35. Έστω ότι δεν υπάρχει σύνδεσμος ανάμεσα στον D και τον Z. Η Απάντηση Δρομολογίου (RREP) απ' τον K περιορίζει το 'πλημμύρισμα' των RREQ

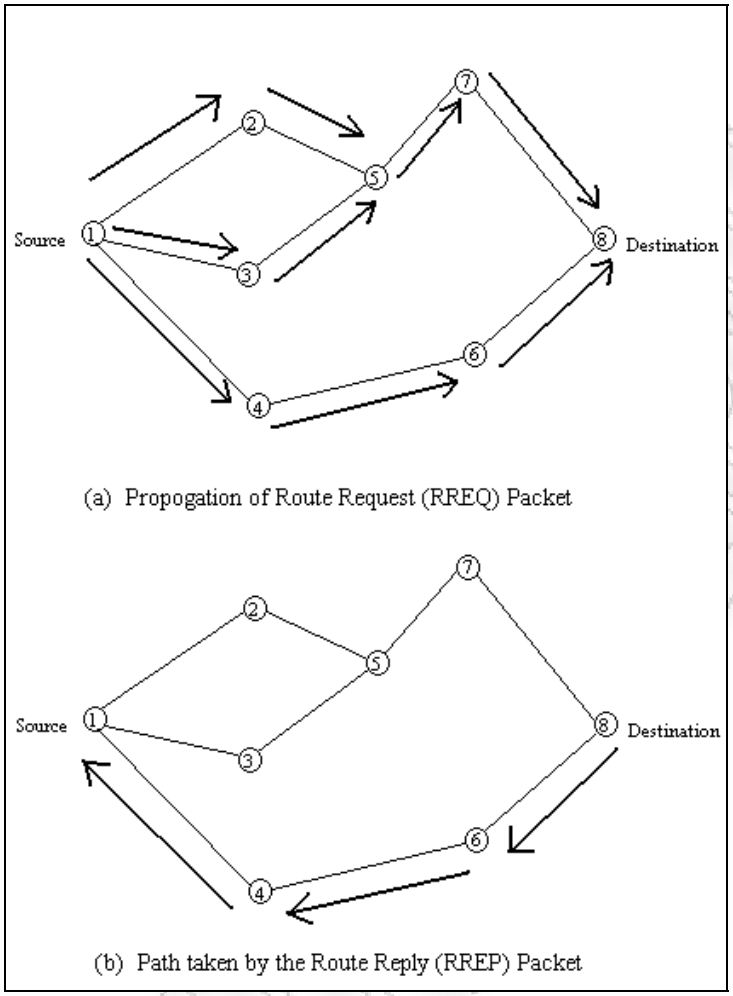
Τέλος, παρουσιάζεται σχηματικά (Εικόνα 36) το σφάλμα δρομολογίου (RER):



Εικόνα 36. Ο J στέλνει ένα Σφάλμα Δρομολογίου στον S κατά μήκος του δρομολογίου J-F-E-S, όταν η προσπάθειά του να προωθήσει ένα πακέτο δεδομένων του S (με δρομολόγιο SEFJD) μέσω του J-D αποτυγχάνει οι κόμβοι που 'ακούν' το RERR ανανεώνουν τα αποθηκευμένα δρομολόγιά τους, για να αφαιρέσουν το σύνδεσμο J-D

5.2 AODV (AD HOC ON-DEMAND DISTANCE VECTOR)

Το AODV είναι πρωτόκολλο δρομολόγησης hop-by-hop. Όταν ένας κόμβος πρέπει να στείλει ένα πακέτο δεδομένων σε έναν προορισμό στον οποίο δεν έχει διαδρομή, πρέπει να εκπέμψει ένα RREQ σε όλους του τους γείτονες. Κάθε γείτονας το κάνει αυτό μέχρι να φτάσει στον προορισμό του (ή ένας κόμβος με έγκυρη διαδρομή στον προορισμό). Αυτός ο κόμβος στέλνει ένα RREP πακέτο που ταξιδεύει το αντίστροφο μονοπάτι μέχρι να φτάσει την πηγή. Πάνω από τη λήψη της απάντησης κάθε μεσάζον αναβαθμίζει το δικό του routing table. Με αυτόν τον τρόπο «χτίζεται» μία διαδρομή ανάμεσα στην πηγή και στον προορισμό. Διαφορετικά από το DSR, η πηγή δε χρησιμοποιεί όλη τη διαδρομή μέσα στα εξερχόμενα πακέτα. Μάλλον, η απόφαση για το επόμενο hop παίρνεται ξεχωριστά μετά από κάθε hop. Εφόσον στηρίζεται στην αρχή του παράγοντα απόστασης (distance vector principle), οι AODV αναθέσεις αυξάνουν μονότονα τις ακολουθίες αριθμών στις διαδρομές, οι οποίες καθορίζουν την ανανέωση των διαδρομών, όπως και τη μέτρηση των hop (hop count) η οποία καθορίζει τη βέλτιστη διαδρομή.



Εικόνα 37. Λειτουργία του AODV

5.2.1 Ανεπιφύλακτη Έμπιστη Σχέση Μεταξύ Γειτόνων

Τα τρέχοντα ad-hoc πρωτόκολλα δρομολόγησης έμφυτα εμπιστεύονται όλους τους συμμετέχοντες. Τα περισσότερα ad-hoc πρωτόκολλα δρομολόγησης είναι συνεργάσιμα από φύση τους και εξαρτώνται από τους γειτονικούς κόμβους μέχρι τα πακέτα διαδρομής. Αυτό το αφελές μοντέλο εμπιστοσύνης επιτρέπει στους κακόβουλους κόμβους να παραλύουν ένα ad-hoc δίκτυο με την εισαγωγή εσφαλμένων αναβαθμίσεων δρομολόγησης, την επανάληψη παλιών μηνυμάτων, την αλλαγή των αναβαθμίσεων δρομολόγησης ή τη διαφήμιση λανθασμένων πληροφοριών δρομολόγησης. Καθώς αυτές οι επιθέσεις είναι πιθανές και σε δίκτυο με υποδομή (fixed network), το ad-hoc περιβάλλον τις μεγεθύνει και κάνει δύσκολη την ανίχνευσή τους.

5.2.2 Απόδοση (Throughput)

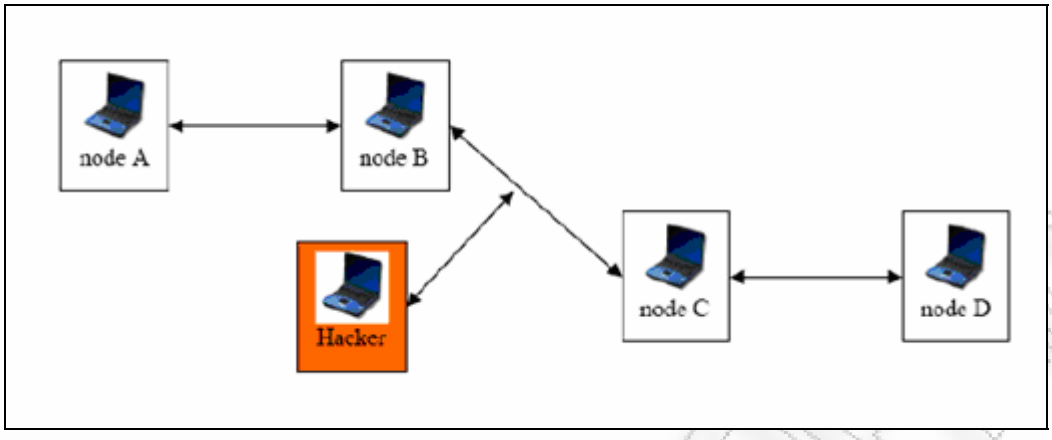
Τα ad-hoc δίκτυα μεγιστοποιούν την ολική απόδοση (throughput) του δικτύου χρησιμοποιώντας όλους τους διαθέσιμους κόμβους για δρομολόγηση και προώθηση. Εν τούτοις, ένας κόμβος μπορεί να έχει κακή συμπεριφορά με το να συμφωνεί στην προώθηση πακέτων και μετά αποτυγχάνει στο να το κάνει, επειδή είναι υπερφορτωμένος (overloaded), εγωιστής (selfish), κακόβουλος (malicious) ή καταστραμμένος (broken). Οι κόμβοι με κακή συμπεριφορά μπορεί να αποτελέσουν σημαντικό πρόβλημα. Αν και η μέση απώλεια στην απόδοση οφείλεται στην κακή συμπεριφορά των κόμβων και δεν είναι τόσο υψηλή, στη χειρότερη περίπτωση είναι πολύ υψηλή.

5.3 ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

Τα παραπάνω προτεινόμενα πρωτόκολλα δρομολόγησης των MANET είναι θέμα για πολλούς διαφορετικούς τύπους επιθέσεων. Ανάλογες υλοποιήσεις υπάρχουν στα ενσύρματα δίκτυα, αλλά μπορούν εύκολα να ξεπεραστούν από την υπάρχουσα ισχυρή υποδομή. Σε αυτή την παράγραφο παρουσιάζουμε και αναλύουμε διάφορες κατηγορίες επιθέσεων κατά των πρωτοκόλλων δρομολόγησης. Χωρίς απώλεια γενικότητας, αυτές οι επιθέσεις εξετάζονται σύμφωνα με τα πρωτόκολλα AODV και DSR, που χρησιμοποιούνται ως αντιπρόσωποι των on-demand πρωτοκόλλων του ad-hoc δικτύου. Εν τούτοις, σχεδόν όλα τα παραδοσιακά on demand πρωτόκολλα έχουν τις ίδιες αδυναμίες, συνεπώς δε θεωρούνται κατάλληλα για τα κινητά ad-hoc δίκτυα.

5.3.1 Επιθέσεις Χρησιμοποιώντας Τροποποίηση (Modification)

Η κίνηση του δικτύου μπορεί να ανακατευθυνθεί και να πραγματοποιηθούν DoS επιθέσεις, τροποποιώντας τις πληροφορίες δρομολόγησης, όπως την αλλαγή των πεδίων ελέγχου του μηνύματος των πακέτων δεδομένων ή την προώθηση των μηνυμάτων δρομολόγησης με εσφαλμένες τιμές (falsified values). Παραθέτουμε διάφορες επιθέσεις που χρησιμοποιούν τροποποίηση στις ακόλουθες παραγράφους.



Εικόνα 38. Ένας κακόβουλος κόμβος "Hacker" μπορεί να διατηρήσει την κίνηση ώστε να μη φτάσει στον κόμβο D επιμένοντας να διαφημίζει στον κόμβο B μια κοντινότερη διαδρομή για τον κόμβο D, παρά τη διαδρομή στον κόμβο D που διαφημίζει ο C

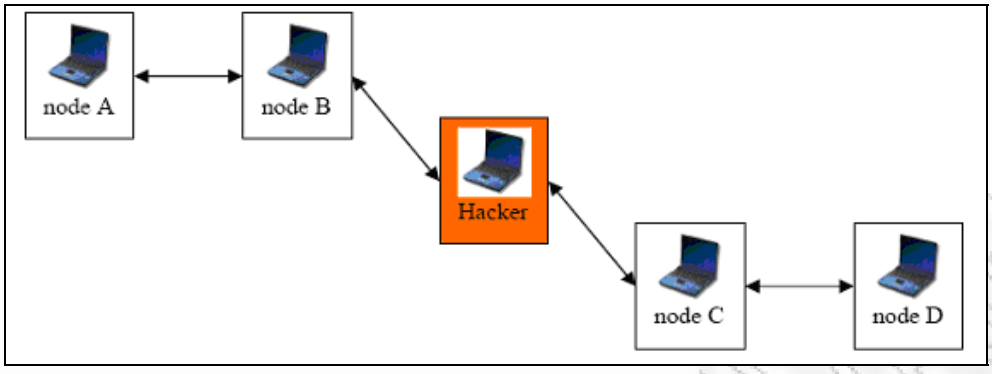
5.3.1.1 Επιθέσεις Χρησιμοποιώντας Τροποποιήσεις Πεδίων Πρωτοκόλλου Μηνυμάτων

Τα τρέχοντα πρωτόκολλα δρομολόγησης υποθέτουν ότι οι κόμβοι δεν αλλάζουν τα πεδία πρωτοκόλλου των μηνυμάτων που περνάνε από τους κόμβους αυτούς. Τα πακέτα δρομολόγησης μεταφέρουν σημαντική πληροφορία ελέγχου η οποία ελέγχει τη συμπεριφορά της μετάδοσης των δεδομένων στα ad-hoc δίκτυα. Εφόσον το επίπεδο εμπιστοσύνης σε ένα παραδοσιακό ad-hoc δίκτυο δεν μπορεί να μετρηθεί ή να ενδυναμωθεί, οι εχθρικοί ή οι compromised κόμβοι ενδεχομένως να συμμετέχουν κατευθείαν στην εύρεση διαδρομής και να σταματούν και να φιλτράρουν τα πρωτόκολλα δρομολόγησης πακέτου έτσι ώστε να διακόψουν την επικοινωνία. Οι κακόβουλοι κόμβοι μπορούν εύκολα να προκαλέσουν ανακατεύθυνση στην κίνηση του δικτύου και οι DoS επιθέσεις απλώς αλλάζοντας αυτά τα πεδία.

Για παράδειγμα στο δίκτυο που παρουσιάζεται στην Εικόνα 40, ένας κακόβουλος κόμβος M θα μπορούσε να κρατήσει την κίνηση μακριά από τον X επιμένοντας να γνωστοποιεί στον B μια κοντινότερη διαδρομή στον X από τη διαδρομή στον X που γνωστοποιείται από τον C.

Οι επιθέσεις μπορούν να κατηγοριοποιηθούν ως απομακρυσμένες (remote) επιθέσεις ανακατεύθυνσης και denial of service επιθέσεις.

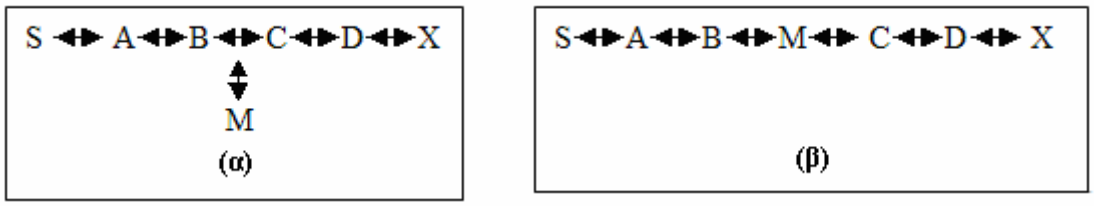
(a) Απομακρυσμένη Ανακατεύθυνση με τροποποιημένη διαδρομή ακολουθίας αριθμών (AODV)



Εικόνα 39. Όταν ο κόμβος Α θέλει να επικοινωνήσει με τον κόμβο D, μεταδίδει ένα μήνυμα ρωτώντας όλους τους κόμβους για την καλύτερη διαδρομή προς τον D. Ο Β θα λάβει το μήνυμα και θα το προωθήσει. Ο κόμβος C θα απαντήσει ότι έχει άμεση διαδρομή με τον D και στο μήνυμα απάντησης θα δώσει τιμή για το μετρικό. Εάν ο κακόβουλος κόμβος επίσης απαντήσει στον Β ότι έχει άμεση διαδρομή στον D με μικρότερη τιμή μετρικού από τον C, ο Β Θα θεωρήσει αυτή τη διαδρομή ως την καλύτερη και θα διαγράψει το μονοπάτι του κόμβου C.

Οι επιθέσεις απομακρυσμένης ανακατεύθυνσης καλούνται και επιθέσεις μαύρης τρύπας (black hole attacks). Στις επιθέσεις αυτές, ένας κακόβουλος κόμβος χρησιμοποιεί πρωτόκολλα δρομολόγησης για να διαφημίζει τον εαυτό του ως το κοντινότερο μονοπάτι στους κόμβους των οποίων τα πακέτα θέλει να σταματήσει-υποκλέψει (intercept). Πρωτόκολλα όπως το AODV επισπεύδουν και διατηρούν διαδρομές αναθέτοντας τη μονότονη αύξηση της ακολουθίας αριθμών στις διαδρομές προς μια συγκεκριμένη κατεύθυνση. Στο AODV κάθε κόμβος μπορεί να ανακατευθύνει την κίνηση διαμέσου του ιδίου, διαφημίζοντας μια διαδρομή σε έναν κόμβο με έναν προορισμό ακολουθίας αριθμών πιο μεγάλο από την αυθεντική τιμή.

Η Εικόνα 40 παρουσιάζει ένα παράδειγμα ad-hoc δικτύου. Ας υποθέσουμε έναν κακόβουλο κόμβο M ο οποίος παραλαμβάνει το RREQ που έχει προέλευση τον S και προορισμό τον X αφού έχει επανεκπεμφθεί από τον B κατά τη διάρκεια της εύρεσης διαδρομής. Ο M ανακατευθύνει την κίνηση προς τον εαυτό του και στέλνει στον ίδιο και στον B ένα RREP που περιέχει έναν σημαντικά υψηλότερο αριθμό ακολουθίας προορισμού για τον X από την αυθεντική τιμή που τελευταία γνωστοποιήθηκε από τον X.



Εικόνα 40. Παράδειγμα ad-hoc δικτύου όπου ο κακόβουλος κόμβος M ανακατευθύνει την κίνηση προς τον εαυτό του και στέλνει στον ίδιο και στον B ένα RREP που περιέχει έναν σημαντικά υψηλότερο αριθμό ακολουθίας προορισμού για τον X από την αυθεντική τιμή που τελευταία γνωστοποιήθηκε από τον X

(b) Ανακατεύθυνση με τροποποιημένο hop count (AODV)

Μια επίθεση ανακατεύθυνσης είναι επίσης πιθανή σε ορισμένα πρωτόκολλα όπως π.χ. το AODV τροποποιώντας το πεδίο μέτρησης hop (hop count field) στην εύρεση διαδρομής μηνύματος. Όταν οι αποφάσεις δρομολόγησης δεν μπορούν να παρθούν από άλλες μετρήσεις (metrics), το AODV χρησιμοποιεί το πεδίο μέτρησης των hop για να καθορίσει ένα κοντινότερο μονοπάτι. Στα AODV οι κακόβουλοι κόμβοι μπορούν να έλξουν διαδρομές προς τους ίδιους μηδενίζοντας το πεδίο μέτρησης hop του RREP. Ομοίως, θέτοντας στο άπειρο το πεδίο μέτρησης hop του RREP, οι διαδρομές θα τείνουν να δημιουργηθούν και δεν θα περιλαμβάνουν τους κακόβουλους κόμβους.

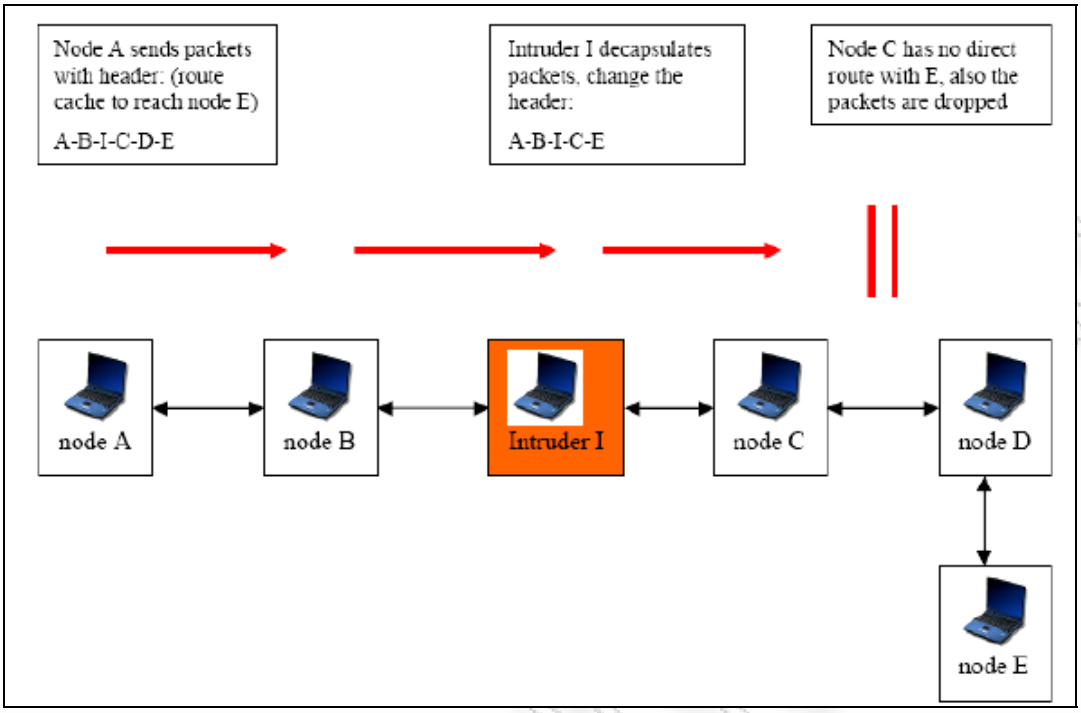
Εφόσον ο κακόβουλος κόμβος μπόρεσε να εισχωρήσει ανάμεσα σε δυο κόμβους που επικοινωνούν, μπορεί να κάνει οτιδήποτε με τα πακέτα που περνάνε μεταξύ τους. Μπορεί να διαλέξει να βάλει πακέτα για να επιτελέσει μια denial of service επίθεση ή εναλλακτικά να χρησιμοποιήσει τη θέση του στη διαδρομή ως πρώτο βήμα για την επίθεση man-in-the-middle.

Μια τέτοια επίθεση είναι πιο απειλητική όταν συνδυάζεται με το spoofing. Η επίθεση ανακατεύθυνσης είναι πιθανή ακόμη κι αν το πρωτόκολλο χρησιμοποιεί άλλες μετρήσεις (metrics) από τους αριθμούς των hop. Σε αυτή την περίπτωση αυτό που έχει να κάνει ο επιτιθέμενος είναι να τροποποιήσει το πεδίο που χρησιμοποιείται για να υπολογίσει το μετρικό αντί να μετρήσει τα hops.

(c) Denial of service με τροποποιημένες διαδρομές πηγής

Το DSR είναι ένα πρωτόκολλο δρομολόγησης το οποίο σαφώς δείχνει την κατάσταση των διαδρομών στα πακέτα των δεδομένων. Αυτές οι διαδρομές στερούνται ελέγχους ακεραιότητας και μια απλή denial of service επίθεση μπορεί να πραγματοποιηθεί στο DSR αλλάζοντας τις διαδρομές των πηγών στις επικεφαλίδες των πακέτων.

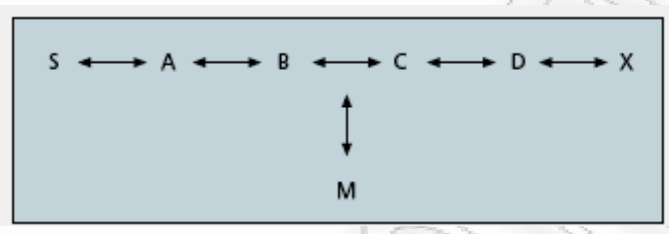
Η τροποποίηση στις διαδρομές των πηγών στα DSR ενδεχομένως να περιλαμβάνει την εισαγωγή των βρόχων σε ένα συγκεκριμένο μονοπάτι. Αν και το DSR εμποδίζει το looping κατά τη διάρκεια της διαδικασίας εύρεσης διαδρομής, υπάρχουν ανεπαρκείς φρουροί ασφάλειας (safeguards) για να εμποδίσουν την είσοδο των βρόχων μέσα σε μια διαδρομή πηγής, αφού η διαδρομή έχει διασωθεί (salvaged).



Εικόνα 41. Ο κακόβουλος κόμβος τοποθετείται μέσα στο δίκτυο. Εάν ο κόμβος Α θέλει να επικοινωνήσει με τον κόμβο Ε, του στέλνει πακέτα δεδομένων ακολουθώντας την πορεία μνήμης του (route cache) προς τον κόμβο Ε συμπεριλαμβάνοντας και τον κακόβουλο κόμβο. Επίσης, όταν ο κακόβουλος κόμβος παραλάβει τα πακέτα δεδομένων, μπορεί να αλλάξει την επικεφαλίδα των πακέτων αυτών για να αποβάλλει τις πληροφορίες των δεδομένων

Όπως έχουμε ήδη δει το DSR αξιοποιεί τη στρατηγική δρομολόγησης πηγής, γι' αυτό οι κόμβοι της πηγής δείχνουν κατηγορηματικά την κατάσταση των διαδρομών στα πακέτα δεδομένων. Αυτές οι διαδρομές στερούνται τον όποιο έλεγχο ακεραιότητας οπότε οι αλλαγές των διαδρομών πηγής στις επικεφαλίδες των πακέτων μπορούν εύκολα να γίνουν από τους κακόβουλους κόμβους, έχοντας ως αποτέλεσμα επιθέσεις τύπου denial-of-service. Υποθέτουμε ότι υπάρχει ένα μονοπάτι από τον S στον X, όπως δείχνει η Εικόνα 42. Επίσης υποθέτουμε ότι οι C και X είναι εκτός εμβέλειας ισχύος ο ένας με τον άλλο κι ότι ο M είναι ένας κακόβουλος κόμβος που επιχειρεί να επιτεθεί με denial-of-service. Υποθέτουμε ότι ο S επιθυμεί να επικοινωνήσει με τον X στον οποίο έχει μια ισχύουσα (unexpired) διαδρομή στη μνήμη διαδρομών του. Ο S μεταδίδει ένα πακέτο δεδομένων προς τον X με τη διαδρομή πηγής (S,A,B,M,C,D,X) προσαρμοσμένη στην επικεφαλίδα του πακέτου. Όταν ο M παραλάβει το πακέτο μπορεί να αλλάξει τη διαδρομή της πηγής στην επικεφαλίδα του πακέτου, π.χ. μπορεί να διαγράψει τον D από τη διαδρομή της πηγής. Συνεπώς, όταν ο C παραλάβει το αλλαγμένο πακέτο, προσπαθεί να το προωθήσει στον X. εφόσον ο X είναι εκτός της εμβέλειας ισχύος του C, το πακέτο δε θα φτάσει στον X. Ο C θα θεωρήσει ότι η ζεύξη με το X είναι διακεκομμένη, κι έτσι

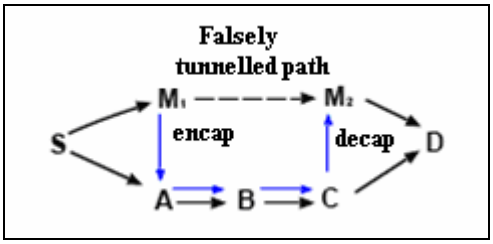
θα στείλει ένα πακέτο RER πίσω στον S μέσω του M. Όταν ο M παραλάβει το πακέτο, απλά θα το αφήσει. Γι' αυτό ο S ακόμη θα χρησιμοποιεί τη διαδρομή διαμέσου του M και αυτό θα συνεχιστεί να εκτελείται με τον τρόπο αυτό, έχοντας ως αποτέλεσμα μια denial of service επίθεση εναντίον στην υπηρεσία δρομολόγησης. Αυτή η επίθεση μπορεί επίσης να χρησιμοποιηθεί για να προκαλέσει sleep deprivation εφόσον τα πακέτα θα μεταδίδονται πάλι και πάλι διαμέσου των compromised διαδρομών.



Εικόνα 42. Επίθεση DoS

5.3.1.2 Tunnelling

Δυο απομακρυσμένοι κόμβοι μπορούν να συνεργαστούν για να ενθυλακώσουν (encapsulate) και να ανταλλάξουν μηνύματα μεταξύ τους διαμέσου υπαρχόντων διαδρομών δεδομένων και να δώσουν την εντύπωση ότι είναι γειτονικοί-συνεχόμενοι (adjacent). Γι' αυτό ενδεχομένως να συνεργαστούν για να παρουσιάσουν εσφαλμένα το μήκος των διαθέσιμων μονοπατιών με ενθυλάκωση και σήραγγα (tunnelling) ανάμεσά τους και να παράγουν νόμιμα (legitimate) μηνύματα δρομολόγησης από άλλους κόμβους, εμποδίζοντας τους ενδιάμεσους κόμβους από ορθή προσαύξηση του μετρικού που χρησιμοποιείται για να μετρά τα μήκη των μονοπατιών (όπως το hop count). Για παράδειγμα στην Εικόνα 43 οι M1 και M2 είναι κακόβουλοι κόμβοι που χρησιμοποιούν το μονοπάτι (M1, A, B, C, M2) σα σήραγγα. Όταν ο M1 παραλαμβάνει ένα πακέτο αίτησης διαδρομής (RREQ) από τον S, το ενθυλακώνει και το βάζει σε σήραγγα στον M2 όπου ο τελευταίος φυσικά προωθεί. Αφότου ο M2 λάβει το RREP από τον D, το βάζει σε σήραγγα και το στέλνει πίσω στον M1, όπου κάνει το ίδιο και στον S, με αποτέλεσμα να δημιουργεί μια λάθος διαδρομή (S, M1, M2, D) όπου μπορεί να θεωρηθεί ως η πιο βέλτιστη.



Εικόνα 43. Τα μήκη των μονοπατιών εξαπατούνται από tunneling

5.3.2 Επιθέσεις Εξαπάτησης (Spoofing Attacks)

Το Spoofing συμβαίνει όταν ένας κόμβος παραμορφώνει την ταυτότητά του στο δίκτυο, π.χ. αλλάζει την MAC ή την IP διεύθυνσή του στα εξερχόμενα πακέτα. Αυτή η επίθεση μπορεί αμέσως να συνδυαστεί με επιθέσεις τροποποίησης. Αυτές οι δύο επιθέσεις (spoofing και modification) όταν συνδυάζονται μεταξύ τους μπορεί να έχουν ως αποτέλεσμα σοβαρής κακής πληροφορίας (misinformation) όπως π.χ. τη δημιουργία βρόχων διαδρομής.

5.3.3 Επιθέσεις Με Χρήση Πλαστογραφίας (Fabrication)

Η παραγωγή εσφαλμένων μηνυμάτων δρομολόγησης ορίζεται ως πλαστογράφηση μηνυμάτων. Τέτοιες επιθέσεις δύσκολα ανιχνεύονται.

(a) Ψεύτικα μηνύματα λάθους διαδρομών στα AODV και DSR

Τα AODV και DSR εφαρμόζουν τα μέτρα συντήρησης μονοπατιών (path maintenance measures) για να ανακτηθούν τα κατεστραμμένα μονοπάτια όταν κινούνται οι κόμβοι. Εάν ο κόμβος προορισμού ή ένας ενδιάμεσος κόμβος κινηθεί κατά μήκος των ενεργών μονοπατιών, η σύνδεση προς τα πάνω (upstream) των κόμβων σπάει και μεταδίδεται ένα μήνυμα λάθους διαδρομών σε όλους τους ενεργούς upstream γείτονες. Ο κόμβος ακυρώνει επίσης τη διαδρομή για αυτόν τον προορισμό στον πίνακα δρομολόγησής του.

Η ευπάθεια είναι ότι οι επιθέσεις δρομολόγησης μπορούν να πραγματοποιηθούν με την αποστολή των ψεύτικων μηνυμάτων λάθους διαδρομών (route error messages). Υποθέστε ότι ο κόμβος S έχει μια διαδρομή προς τον κόμβο X μέσω των κόμβων A, B και C, όπως στην Εικόνα 42. Ένας κακόβουλος κόμβος μπορεί να πραγματοποιήσει μια denial of service επίθεση ενάντια στον X στέλνοντας συνεχώς μηνύματα λάθους διαδρομών στον B που εξαπατά τον κόμβο C, υποδεικνύοντας μια σπασμένη σύνδεση μεταξύ των κόμβων C και X. Ο B λαμβάνει

το spoofed μήνυμα λάθους διαδρομών σκεπτόμενος ότι προήλθε από τον C. Ο B διαγράφει τον πίνακα δρομολόγησής του για τον X και διαβιβάζει το μήνυμα λάθους διαδρομών προς τον A, ο οποίος έπειτα διαγράφει και τον δικό του πίνακα δρομολόγησης. Εάν ο M ακούει και μεταδίδει τα spoofed μηνύματα λάθους διαδρομών όποτε μια διαδρομή καθιερώνεται από τον S στον X, ο M μπορεί επιτυχώς να αποτρέψει τις επικοινωνίες μεταξύ του S και του X.

(b) Μετάδοση ψεύτικων διαδρομών

Στα DSR ένας κόμβος μπορεί να ενημερώσει τον πίνακα δρομολόγησής του (μνήμη διαδρομών-route cache) στηριζόμενος στις πληροφορίες των επικεφαλίδων που κατέχουν τα πακέτα που προωθεί. Οι διαδρομές μπορούν επίσης να μαθευτούν από τα αδιάκριτα-επιπόλαια (promiscuously) λαμβανόμενα πακέτα. Η ευπάθεια είναι ότι ένας επιτιθέμενος θα μπορούσε εύκολα να εκμεταλλευτεί αυτήν τη μέθοδο εκμάθησης διαδρομών και να δηλητηριάσει έπειτα τις μνήμες διαδρομών (route caches) των γειτόνων του, αναμεταδίδοντας πακέτα που περιέχουν πλαστογραφημένες διαδρομές.

(c) Cache Poisoning Διαδρομών Στα DSR

Αυτή είναι μια παθητική επίθεση που μπορεί να εμφανιστεί στα DSR λόγω του επιπόλαιου (promiscuous) τρόπου ενημέρωσης του πίνακα δρομολόγησης που χρησιμοποιείται από τα DSR. Αυτό εμφανίζεται όταν οι πληροφορίες που αποθηκεύονται στον πίνακα δρομολόγησης στους δρομολογητές διαγράφονται, αλλάζονται ή εγχέονται με ψεύτικες πληροφορίες.

Εκτός από την εκμάθηση των διαδρομών από τις επικεφαλίδες των πακέτων, που ένας κόμβος επεξεργάζεται κατά μήκος ενός μονοπατιού, οι διαδρομές στο DSR ενδεχομένως να μαθευτούν από τα επιπόλαια (promiscuously) λαμβανόμενα πακέτα. Ένας κόμβος που κρυφακούει οποιοδήποτε πακέτο μπορεί να προσθέσει τις πληροφορίες δρομολόγησης που περιλαμβάνονται στην επικεφαλίδα εκείνου του πακέτου στη μνήμη διαδρομών του, ακόμα κι αν εκείνος ο κόμβος δεν είναι στο μονοπάτι από την πηγή στον προορισμό.

Η ευπάθεια είναι ότι ένας επιτιθέμενος θα μπορούσε εύκολα να εκμεταλλευτεί αυτήν την μέθοδο εκμάθησης διαδρομών και δηλητηρίασης (poison) μνημών διαδρομών. Υποθέτουμε ότι ένας κακόβουλος κόμβος M θέλει να δηλητηριάσει τις

διαδρομές στον κόμβο Χ. Εάν ο Μ ήταν να μεταδώσει spoofed πακέτα με διαδρομές πηγής στον Χ μέσω του εαυτού του, οι γειτονικοί κόμβοι που κρυφακούνε τη μετάδοση πακέτων μπορούν να προσθέσουν τη διαδρομή στη μνήμη διαδρομών τους.

(d) Επίθεση υπερχείλισης Πίνακα Δρομολόγησης (Routing table)

Στην επίθεση υπερχείλισης πίνακα δρομολόγησης, ο επιτιθέμενος προσπαθεί να δημιουργήσει διαδρομή σε ανύπαρκτους κόμβους. Ο στόχος του επιτιθέμενου είναι να δημιουργήσει αρκετούς δρομολογητές για να αποτρέψουν τις νέες διαδρομές από τη δημιουργία τους ή να συντρίψει το πρωτόκολλο. Η εφαρμογή της επίθεσης νομιμοποιεί τις διαδρομές του πίνακα δρομολόγησης. Οι proactive αλγόριθμοι δρομολόγησης (Proactive routing algorithms) προσπαθούν να ανακαλύψουν τις πληροφορίες δρομολόγησης ακόμη και προτού να χρειαστούν, ενώ οι reactive αλγόριθμοι (reactive algorithms) τις δημιουργούν μόνο όταν απαιτούνται. Αυτό καθιστά τους proactive αλγορίθμους πιο τρωτούς στις επιθέσεις υπερχείλισης πίνακα.

5.3.4 Καμία Περίπτωση Ανίχνευσης Και Απομόνωσης Κόμβων Με Κακή Συμπεριφορά

Όπως παρατηρήσαμε νωρίτερα, οι κόμβοι απρεπούς συμπεριφοράς (misbehaving nodes) μπορούν να έχουν επιπτώσεις στην απόδοση δικτύων στα σενάρια των χειρότερων περιπτώσεων. Τα υπάρχοντα ad-hoc πρωτόκολλα δρομολόγησης δεν περιλαμβάνουν κάποιο μηχανισμό για να προσδιορίσουν τους κόμβους απρεπούς συμπεριφοράς. Είναι απαραίτητο σαφώς να καθοριστούν οι κόμβοι απρεπούς συμπεριφοράς προκειμένου να αποτραπούν τα ψευδώς θετικά (false positives). Μπορεί να είναι πιθανό ένας κόμβος να εμφανίζεται με απρεπή συμπεριφορά όταν πραγματικά αντιμετωπίζει προσωρινό πρόβλημα όπως η υπερφόρτωση ή η χαμηλή μπαταρία. Ένα πρωτόκολλο δρομολόγησης πρέπει να είναι σε θέση να προσδιορίσει τους κόμβους απρεπούς συμπεριφοράς και να τους απομονώσει κατά τη διάρκεια της λειτουργίας εύρεσης διαδρομών.

5.3.5 Εύκολη Διαρροή Πληροφοριών Γύρω Από Την Τοπολογία Του Δικτύου

Τα ad-hoc πρωτόκολλα δρομολόγησης όπως τα AODV και DSR μεταφέρουν πακέτα εύρεσης διαδρομών στο σαφές κείμενο (text). Αυτά τα πακέτα περιέχουν τις διαδρομές που ακολουθούνται από ένα πακέτο. Με την ανάλυση αυτών των πακέτων

οποιοσδήποτε εισβολέας μπορεί να ανακαλύψει τη δομή του δικτύου. Οι επιθέσεις μπορεί να χρησιμοποιήσουν πληροφορίες για να ξέρουν ποιοι άλλοι κόμβοι είναι δίπλα στο στόχο ή τη φυσική θέση ενός συγκεκριμένου κόμβου. Μια τέτοια επίθεση μπορεί να γίνει παθητικά. Μπορεί να αποκαλύψει τους ρόλους των κόμβων στο δίκτυο και τη θέση τους. Οι εισβολείς μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να επιτεθούν στους κόμβους ελέγχου εντολής (command control nodes).

5.3.6 Έλλειψη Αυτο-Σταθερότητας Ιδιοκτησίας (Lack Of Self-Stabilization Property)

Η δρομολόγηση των πρωτοκόλλων πρέπει να είναι σε θέση να αναρρώσει από μια επίθεση σε πεπερασμένο χρόνο. Ένας εισβολέας δεν πρέπει να είναι σε θέση να θέσει μόνιμα εκτός λειτουργίας ένα δίκτυο με την έγχυση ενός μικρότερου αριθμού κακώς ενημερωμένων (mal-informed) πακέτων δρομολόγησης. Π.χ. τα AODV, εν τούτοις είναι επιρρεπή σε προβλήματα αυτο-σταθεροποίησης δεδομένου ότι οι αριθμοί ακολουθίας χρησιμοποιούνται για να ελέγξουν τους χρόνους εγκυρότητας διαδρομών και η ανακριβής κατάσταση μπορεί να παραμείνει αποθηκευμένη στους πίνακες δρομολόγησης για μεγάλο χρονικό διάστημα.

5.3.7 Γρήγορες Επιθέσεις (Rushing Attacks)

Πρόσφατα έχει καθοριστεί μια νέα επίθεση αποκαλούμενη γρήγορη επίθεση (rushing attack). Σχεδόν σε όλα τα on-demand πρωτόκολλα δρομολόγησης, για να περιοριστεί το ανώτατο όριο εύρεσης διαδρομών (overhead), κάθε κόμβος προωθεί μόνο ένα RREQ προερχόμενο από οποιαδήποτε εύρεση διαδρομής, γενικά την πρώτη λαμβανόμενη. Αυτή η ιδιοκτησία μπορεί να χρησιμοποιηθεί με γρήγορη προώθηση των λαμβανόμενων RREQs.

Για μια εύρεση διαδρομών, εάν τα RREQs που διαβιβάζονται από τον επιτιθέμενο είναι τα πρώτα που φθάνουν σε κάθε γείτονα του στόχου, τότε οποιαδήποτε διαδρομή που λαμβάνεται από αυτήν την εύρεση διαδρομών θα περιλαμβάνει τον επιτιθέμενο. Δηλαδή όταν ένας γείτονας του στόχου λαμβάνει το βιαστικό RREQ από τον επιτιθέμενο, διαβιβάζει εκείνο το RREQ και δεν θα διαβιβάσει περαιτέρω RREQ από αυτήν την εύρεση διαδρομών. Κατά συνέπεια, ο αρχικοποιητής (initiator) θα είναι ανίκανος να ανακαλύψει οποιεσδήποτε χρησιμοποιήσιμες διαδρομές (δηλ., διαδρομές που δεν περιλαμβάνουν τον

επιτιθέμενο) που περιέχουν τουλάχιστον δύο hops (τρεις κόμβοι). Σε γενικά πλαίσια, ένας επιτιθέμενος που μπορεί να διαβιβάσει RREQs γρηγορότερα από τους νόμιμους κόμβους μπορεί να πραγματοποιήσει μια τέτοια επίθεση και να περιληφθεί σε όλες τις διαδρομές που ευρέθησαν. Η γρήγορη επίθεση μπορεί επίσης να χρησιμοποιηθεί ενάντια σε οποιοδήποτε πρωτόκολλο που προβλέψιμα προωθεί οποιοδήποτε ιδιαίτερο RREQ για κάθε εύρεση διαδρομών. Ο επιτιθέμενος κάνει το ίδιο πράγμα, εκτός από το ότι τα πακέτα που στέλνει πρέπει να ταιριάζουν με τα κατάλληλα χαρακτηριστικά. Εντούτοις, στην ακόλουθη συζήτηση υποθέτουμε ότι οι κόμβοι διαβιβάζουν το πρώτο λαμβανόμενο RREQ.

Πώς μπορεί ένας επιτιθέμενος να μεταφέρει επειγόντως τα πακέτα RREQ για να πραγματοποιήσει μια γρήγορη επίθεση; Ένας κακόβουλος κόμβος μπορεί να χρησιμοποιήσει μια ή περισσότερες από τις ακόλουθες τεχνικές:

- ✓ **Να αφαιρέσει τις καθυστερήσεις του MAC ή/και των δικτύων κατά την αποστολή των πακέτων**: Τα πρωτόκολλα επιπέδου MAC και επιπέδου δικτύου χρησιμοποιούν τις καθυστερήσεις στη μετάδοση πακέτων για να αποφύγουν τις συγκρούσεις. Κατά συνέπεια, ένας επιτιθέμενος μπορεί να αρνηθεί αυτές τις καθυστερήσεις για να μεταφέρει επειγόντως το αίτημα που προωθεί.
- ✓ **Να διαβιβάσει τα RREQs σε υψηλότερη δύναμη**: Ένας επιτιθέμενος που εφοδιάζεται με μια ισχυρή υποστήριξη επικοινωνίας μπορεί να χρησιμοποιήσει μια υψηλότερη δύναμη μετάδοσης για να διαβιβάσει RREQs, καλύπτοντας με αυτόν τον τρόπο μια υψηλότερη εμβέλεια δύναμης από άλλους κόμβους και οι περαιτέρω κόμβοι θα επιτευχθούν στα λιγότερα hops. Αντίθετα από τις άλλες τεχνικές, αυτή η τεχνική γενικά, δεν επιτρέπει στον επιτιθέμενο να περιληφθεί σε μια μοναδική ανακαλυμμένη διαδρομή, δεδομένου ότι δεν μπόρεσε να λάβει το RREP (εκτός από την περίπτωση όπου έχει έναν ιδιαίτερα ευαίσθητο δέκτη). Εν τούτοις, αποκλείει την ανακάλυψη των έγκυρων διαδρομών.
- ✓ **Η υιοθέτηση της τεχνικής wormhole**: Δύο επιτιθέμενοι μπορούν να χρησιμοποιήσουν μια υψηλής ποιότητας σήραγγα για να περάσουν ένα πακέτο RREQ μεταξύ τους, που του επιτρέπουν να φθάσει στον τελικό προορισμό του πριν από τα άλλα RREQs. Αυτό μπορεί να γίνει όταν ένας κόμβος είναι πιο κοντά στην πηγή και ο άλλος είναι πιο κοντά στον προορισμό και υπάρχει μεταξύ των δύο κόμβων ένα μονοπάτι με υψηλή ποιότητα (π.χ., μέσω ενός

ενσύρματου δικτύου). Σημειώστε ότι μια πρόσθετη υψηλής ποιότητας διαδρομή απαιτείται για αυτήν την επίθεση, η οποία είναι διαφορετική από την tunelling που παρουσιάστηκε πριν, η οποία χρησιμοποιεί ασύρματες διαδρομές multi-hop.

Ο πίνακας 3 παρέχει μια περίληψη των ευπαθειών των DSR και AODV στις επιθέσεις που παρουσιάζονται σε αυτή την παράγραφο. Όπως βλέπουμε, τα AODV είναι τρωτά στις επιθέσεις τροποποίησης αριθμού ακολουθίας και hop-count, δεδομένου ότι είναι βασισμένα στο διάνυσμα απόστασης (distance vector). Αφ' ενός, τα DSR, που είναι βασισμένα στη δρομολόγηση πηγής και χρησιμοποιούν την επιπόλαια (promiscuous) εκμάθηση διαδρομών, είναι ευαίσθητα στην τροποποίηση διαδρομών πηγής και στην πλαστογραφημένη μετάδοση διαδρομών. Και τα δύο πρωτόκολλα είναι τρωτά στο tunnelling, το spoofing, την πλαστογραφημένη επεξεργασία λάθους διαδρομών (falsified route error fabrication) και στις γρήγορες επιθέσεις (rushing attacks).

Attack	AODV	DSR
Attacks using modification		
Modifying route sequence numbers	Yes	No
Modifying hop counts	Yes	No
Modifying source route	No	Yes
Tunneling	Yes	Yes
Spoofing attacks	Yes	Yes
Attacks using fabrication		
Falsifying route errors	yes	Yes
Broadcast falsified routes	No	Yes
Rushing attacks	Yes	Yes

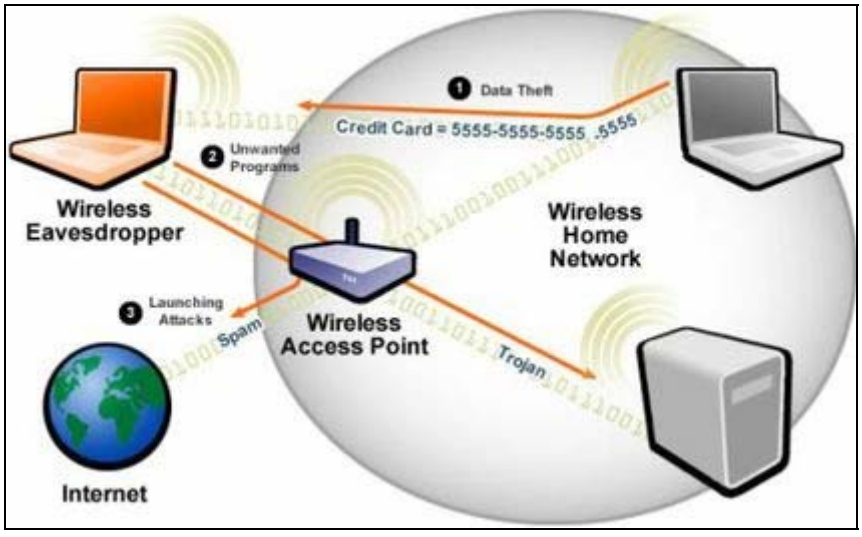
Πίνακας 3. Αδυναμίες AODV και DSR πρωτοκόλλων

6 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΠΡΟΩΘΗΣΗ ΔΕΔΟΜΕΝΩΝ

Η προστασία του επιπέδου δικτύων στα MANETs είναι ένα ιδιαίτερα σημαντικό ερευνητικό θέμα. Οι λειτουργίες πυρήνων που παρέχονται σε αυτό το στρώμα είναι η δρομολόγηση και η προώθηση πακέτου και είναι στενά συνδεδεμένες. Η υπηρεσία διαβίβασης δεδομένων αποτελείται από τη σωστή αναμετάδοση των λαμβανόμενων πακέτων από κόμβο σε κόμβο έως ότου φθάνουν στον τελικό προορισμό τους, ακολουθώντας τις διαδρομές που επιλέχθηκαν και που διατηρούνται από το πρωτόκολλο δρομολόγησης. Οι κακόβουλες επιθέσεις ή η εγωιστική απρεπής συμπεριφορά σε καθέναν από αυτούς, θα διασπάσουν τις κανονικές λειτουργίες των δικτύων.

6.1 ΑΠΕΙΛΕΣ ΣΤΗΝ ΠΡΟΩΘΗΣΗ ΔΕΔΟΜΕΝΩΝ

6.1.1 Κρυφάκουσμα (Eavesdropping)



Τα ασύρματα κανάλια που χρησιμοποιούνται στα MANETs είναι ελεύθερα και εύκολα υλοποιήσιμα. Επιπλέον, ο αυθαίρετος (promiscuous) τρόπος, που

σημαίνει τη σύλληψη των πακέτων από έναν κόμβο που δεν είναι ο κατάλληλος προορισμός, επιτρέπεται και υιοθετείται από τα πρωτόκολλα για να λειτουργήσει ή για να εξασφαλίσει περισσότερη αποδοτικότητα, π.χ. ένα πρωτόκολλο δρομολόγησης μπορεί να χρησιμοποιήσει αυτόν τον τρόπο για να μάθει τις διαδρομές. Αυτά τα χαρακτηριστικά γνωρίσματα μπορούν να χρησιμοποιηθούν από τους κακόβουλους κόμβους για να κρυφακούσουν τα πακέτα κατά τη μεταφορά, κατόπιν να τα αναλύσουν για να λάβουν τις εμπιστευτικές και ευαίσθητες πληροφορίες. Η προφανής προληπτική λύση για να προστατευθούν οι πληροφορίες, είναι να κρυπτογραφηθούν τα πακέτα, αλλά η κρυπτογράφηση των δεδομένων δεν αποτρέπει τους κακόβουλους κόμβους από το να κρυφακούσουν και να προσπαθήσουν να σπάσουν τα κλειδιά αποκρυπτογράφησης. Προς το παρόν καμία λύση ανίχνευσης δεν είναι διαθέσιμη και η ανίχνευση αυτής της επίθεσης είναι ένα ανοικτό ερευνητικό θέμα. Δεδομένου ότι το σπάσιμο των κλειδιών είναι πάντα δυνατό και η βασική ανάκληση στα MANETs είναι προβληματική, το κρυφάκουσμα παραμένει μια σοβαρή επίθεση ενάντια στην αποστολή δεδομένων.

6.1.2 Επίθεση Dropping Data Packets

Δεδομένου ότι τα πακέτα ακολουθούν τις διαδρομές multi-hop και περνούν μέσω των κινητών κόμβων, ένας κακόβουλος κόμβος μπορεί να συμμετέχει στη δρομολόγηση, να περιληφθεί στις διαδρομές και να ρίξει όλα τα πακέτα που παίρνει για να διαβιβάσει. Για να το κάνει αυτό, ο κακόβουλος κόμβος επιτίθεται πρώτος στο πρωτόκολλο δρομολόγησης για να κερδίσει τη συμμετοχή στη δρομολόγηση, χρησιμοποιώντας μια ή περισσότερες από τις επιθέσεις που παρουσιάστηκαν προηγουμένως. Αυτή η επίθεση έχει τα ίδια αποτελέσματα με την εγωιστική συμπεριφορά (selfish misbehaviour) που παρουσιάζεται παρακάτω.

6.1.3 Εγωιστική Συμπεριφορά Στην Προώθηση Των Πακέτων

Σε πολλές πολιτικές εφαρμογές, όπως τα δίκτυα των αυτοκινήτων και η παροχή εγκαταστάσεων επικοινωνίας στις απομακρυσμένες περιοχές, οι κόμβοι τυπικά δεν ανήκουν σε μια ενιαία αρχή και δεν ακολουθούν έναν κοινό στόχο. Σε τέτοια δίκτυα, η διαβίβαση των πακέτων στους άλλους δεν είναι προς το άμεσο συμφέρον των κόμβων, οπότε δεν υπάρχει κανένας καλός λόγος για να εμπιστευθούν οι κόμβοι και να υποτεθεί ότι συνεργάζονται πάντα. Πράγματι, ένας εγωιστικός

κόμβος μπορεί να προσπαθήσει να συντηρήσει τους πόρους του, ιδιαίτερα την ισχύ των μπαταριών που είναι ένας πολύτιμος πόρος, με τη ρίψη των πακέτων που καλείται να προωθήσει ενώ χρησιμοποιεί υπηρεσίες άλλων κόμβων και καταναλώνει τους πόρους τους για να διαβιβάσει τα πακέτα του προς τους μακρινούς κόμβους. Αυτό δεν είναι μια σκόπιμη επίθεση αλλά μία εγωιστική συμπεριφορά. Εντούτοις, αντιπροσωπεύει έναν πιθανό κίνδυνο που απειλεί την ποιότητα της υπηρεσίας στο δίκτυο καθώς επίσης και μια από τις σημαντικότερες απαιτήσεις ασφάλειας δικτύων, δηλ. τη διαθεσιμότητα.

7 ΑΣΦΑΛΕΙΑ ΠΡΩΤΟΚΟΛΛΟΥ MAC

Μετά τη συζήτηση των ζητημάτων ασφάλειας σχετικά με το επίπεδο δικτύων, συζητάμε τώρα τα πρωτόκολλα του MAC. Παρουσιάζουμε μια δραστηριότητα απρεπούς συμπεριφοράς που απειλεί έναν από τους σημαντικότερους σκοπούς των πρωτοκόλλων MAC, δηλαδή τη δικαιοσύνη (fairness) στην πρόσβαση καναλιών.

7.1 ΑΠΡΕΠΗΣ ΣΥΜΠΕΡΙΦΟΡΑ ΣΤΑ ΚΑΝΑΛΙΑ ΠΡΟΣΒΑΣΗΣ

Το πρόβλημα

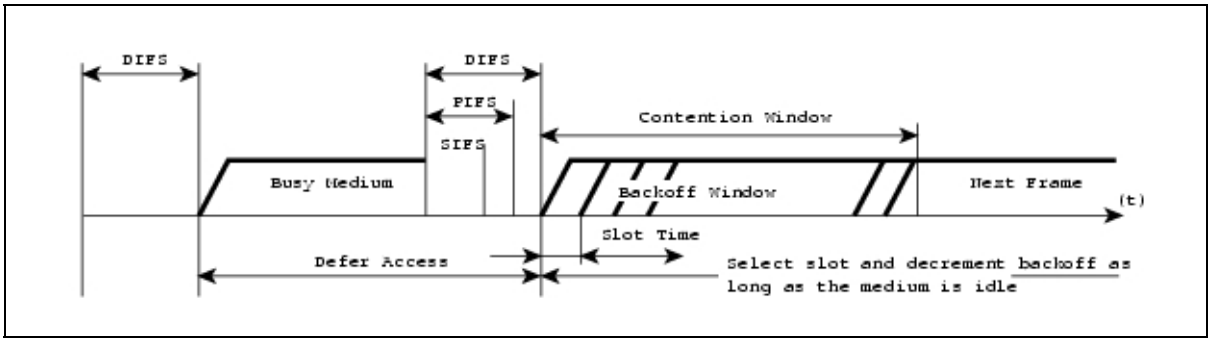
Δεδομένου ότι δεν υπάρχει καμία κεντρική αρχή στα MANETs, ασύρματα πρωτόκολλα ενδιάμεσου ελέγχου πρόσβασης (MAC), όπως το IEEE 802.11, χρησιμοποιούν μηχανισμούς contention resolution για το διαμοιρασμό του ασύρματου καναλιού. Το contention resolution είναι τυπικά βασισμένο σε συνεταιριστικούς μηχανισμούς που εξασφαλίζουν ένα λογικό μερίδιο του καναλιού για όλους τους συμμετέχοντες κόμβους. Σε αυτό το περιβάλλον, μερικοί εγωιστικοί hosts στο δίκτυο μπορούν να συμπεριφερθούν απρεπώς με το να αποτυγχάνουν να εμμείνουν στο πρωτόκολλο MAC, με την πρόθεση της λήψης ενός άδικου μεριδίου του καναλιού. Η παρουσία εγωιστικών κόμβων που παρεκκλίνουν από το πρωτόκολλο contention resolution μπορεί να μειώσει το μερίδιο απόδοσης που παραλαμβάνεται από τους προσαρμοσμένους κόμβους.

Το IEEE 802.11 πρωτόκολλο MAC, που είναι το τυποποιημένο πρωτόκολλο MAC για τα ασύρματα δίκτυα, έχει δύο μηχανισμούς για το contention resolution: ένας κεντραρισμένος μηχανισμός που καλείται PCF (Point Coordination Function: λειτουργία συντονισμού σημείου) και ένας πλήρως διανεμημένος μηχανισμός που καλείται DCF (Distributed Coordination Function: διανεμημένη λειτουργία συντονισμού). Η PCF χρειάζεται έναν κεντραρισμένο ελεγκτή (όπως ένα σταθμό βάσεων) και μπορεί μόνο να χρησιμοποιηθεί στα βασισμένα σε υποδομή δίκτυα, κατά συνέπεια δεν πρόκειται να ληφθεί υπόψη στον ad-hoc τρόπο. Αντίθετα, η DCF χρησιμοποιείται ευρέως στα βασισμένα σε υποδομή ασύρματα δίκτυα καθώς επίσης και στα ad hoc ασύρματα δίκτυα.

Η DCF χρησιμοποιείται από το δίκτυο 802.11 κι αποτελείται από δύο βασικά συστατικά: 1) Interframe space (IFS) και 2) random backoff (παράθυρο ανταγωνισμού-contention window). Το IFS επιτρέπει στο 802.11 να ελέγχει ποια

κίνηση (traffic) έχει πρώτη πρόσβαση στο κανάλι εφόσον ο φορέας Carrier Sense δηλώνει ότι το κανάλι είναι ελεύθερο.

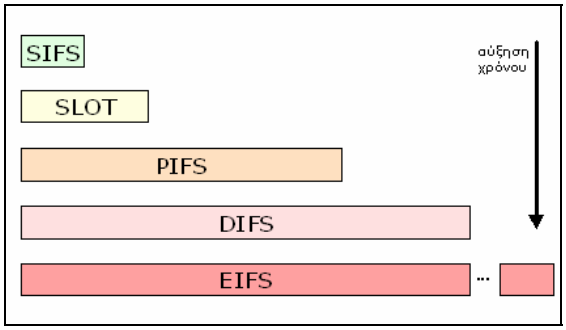
1) Interframe space (IFS)



Εικόνα 44. Interframe Spaces (IFSs)

Το πρότυπο 802.11 ορίζει τα ακόλουθα interframe spaces:

- Short Interframe Space (SIFS). Το μικρότερο χρονικά διάστημα. Χρησιμοποιείται μεταξύ μεταδόσεων πλαισίων μεγίστης προτεραιότητας, αλληλουχίας κατατετμημένων πλαισίων, RTS/CTS, ACK.
- Slot: Βασική μονάδα χρόνου στο 802.11 MAC.
- Point (coordination function) Interframe Space (PIFS): SIFS + 1 Slot. Χρησιμοποιείται στην μέθοδο προσπέλασης PCF.
- Distributed (coordination function) interframe space (DIFS): SIFS + 2 Slot. Το μεγαλύτερο σταθερού μεγέθους διάστημα. Χρησιμοποιείται από όλους τους σταθμούς.
- EIFS: Μεταβλητό μέγεθος.

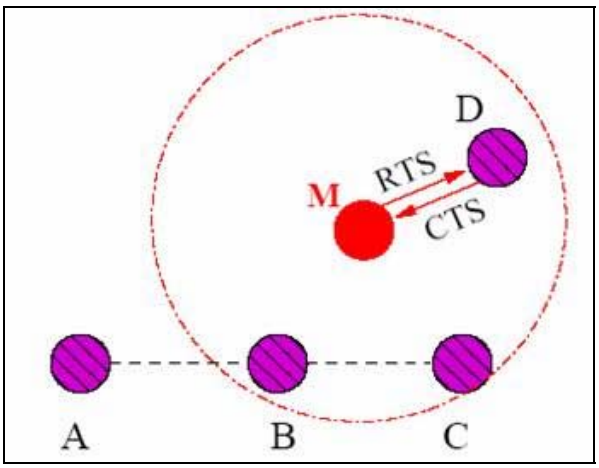


Εικόνα 45. Τα interframe spaces του προτύπου 802.11

2) Τυχαία Οπισθοχώρηση (Random Backoff)

Η DCF χρησιμοποιεί την επιλογή CSMA/CA (πολλαπλή πρόσβαση με ακρόαση φέροντος / αποφυγή σύγκρουσης Carrier Sense Multiple Access/Collision Avoidance) για το resolving contention μεταξύ των πολλαπλών κόμβων που έχουν πρόσβαση στο κανάλι. Ένας κόμβος (αποστολέας) με τα δεδομένα που διαβιβάζει στο κανάλι επιλέγει μια τυχαία backoff τιμή από τη σειρά [0;CW], όπου το CW (contention window-παράθυρο ανταγωνισμού) είναι μια μεταβλητή που διατηρείται από κάθε κόμβο. Ενώ το κανάλι είναι αδρανές, ο μετρητής backoff μειώνεται κατά ένα μετά από κάθε χρονοσχισμή (time slot) (ένα σταθερό διάστημα-interval του χρόνου) και ο μετρητής παγώνει όταν το κανάλι απασχολείται. Ο κόμβος μπορεί να έχει πρόσβαση στο κανάλι όταν ο μετρητής backoff μειώνεται στο μηδέν.

Αφότου ο μετρητής backoff είναι στο μηδέν, ο αποστολέας μπορεί να διατηρήσει το κανάλι για τη διάρκεια της μεταφοράς δεδομένων με το να ανταλλάσσει πακέτα ελέγχου στο κανάλι. Ο αποστολέας αρχικά στέλνει ένα πακέτο RTS (αίτημα προς αποστολή) στο δέκτη, κατόπιν ο δέκτης αποκρίνεται με ένα CTS πακέτο (καθαρίστε για να στείλετε). Αυτή η ανταλλαγή RTS-CTS είναι προαιρετική στο IEEE 802.11. Στοχεύει στην εξασφάλιση της κράτησης (reservation) καναλιών κατά τη διάρκεια της μετάδοσης δεδομένων. Και τα δύο πακέτα περιέχουν την προτεινόμενη διάρκεια της μετάδοσης δεδομένων. Άλλοι κόμβοι που κρυφακούνε είτε το RTS είτε το CTS (ή και τα δύο) απαιτούνται για να αναβάλουν τις μεταδόσεις στο κανάλι κατά τη διάρκεια που διευκρινίζεται στο RTS/CTS.



Εικόνα 46. Οι κόμβοι M και D συνεννοούνται και παρεμβάλλονται στην επικοινωνία του μονοπατιού των κόμβων B και C

Μετά από μια επιτυχή ανταλλαγή RTS/CTS, ο αποστολέας διαβιβάζει ένα πακέτο δεδομένων, το οποίο θα αναγνωριστεί από ένα ACK. Εάν η μετάδοση δεδομένων του κόμβου είναι επιτυχής, ο κόμβος μηδενίζει το CW του σε μια ελάχιστη αξία (CWmin), διαφορετικά εάν ο αποστολέας δεν λαμβάνει το CTS, τότε το CW διπλασιάζεται, αλλά δεν πρέπει να υπερβεί μια μέγιστη αξία CWmax. Ένας κόμβος απρεπούς συμπεριφοράς μπορεί να λάβει περισσότερο από το σημαντικό μέρος του εύρους ζώνης:

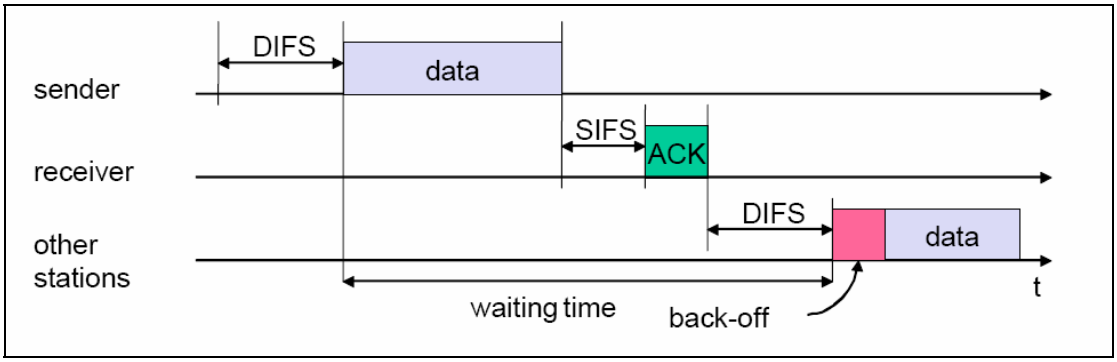
- ✓ Επιλέγοντας backoff τιμές από μια διαφορετική διανομή με τη μικρότερη μέση backoff τιμή από τη διανομή που διευκρινίζεται από το DCF (π.χ., με την επιλογή backoff των τιμών από τη σειρά [0, CW/4] αντί της σειράς [0, CW]).
- ✓ Χρησιμοποιώντας μια διαφορετική στρατηγική αναμετάδοσης που δεν διπλασιάζει την τιμή CW μετά από τις συγκρούσεις. Σημειώνουμε ότι δεν είναι ευεργετικό για έναν εγωιστικό κόμβο να μην καθυστερηθεί καθόλου ή να επιλέξει μια πολύ μικρή σταθερή περίοδο, δεδομένου ότι αυτό μπορεί να οδηγήσει σε ένα πολύ υψηλό ποσοστό σύγκρουσης και στην απώλεια των πακέτων που στέλνει.

Τέτοια εγωιστική συμπεριφορά μπορεί σοβαρά να υποβιβάσει την απόδοση των καλά-συμπεριφερόμενων κόμβων. Για παράδειγμα, τα αποτελέσματα προσομοίωσης που επιτυγχάνονται από τους Kyasanur και Vaidya δείχνουν ότι σε ένα δίκτυο που περιέχει οκτώ κόμβους που στέλνουν πακέτα σε έναν κοινό δέκτη με έναν από τους οκτώ κόμβους να συμπεριφέρεται απρεπώς με το να επιλέγει backoff τιμές από τη σειρά [0,CW/4], η απόδοση των άλλων επτά κόμβων υποβιβάζεται κατά τουλάχιστον 50 τοις εκατό. Μέχρι στιγμής δεν υπάρχει καμία δημοσιευμένη λύση που προτείνεται σε αυτό το σύνθετο πρόβλημα, εκτός από τη λύση που προτείνεται από τους Kyasanur και Vaidya.

Συνοψίζουμε τη λειτουργία του DCF:

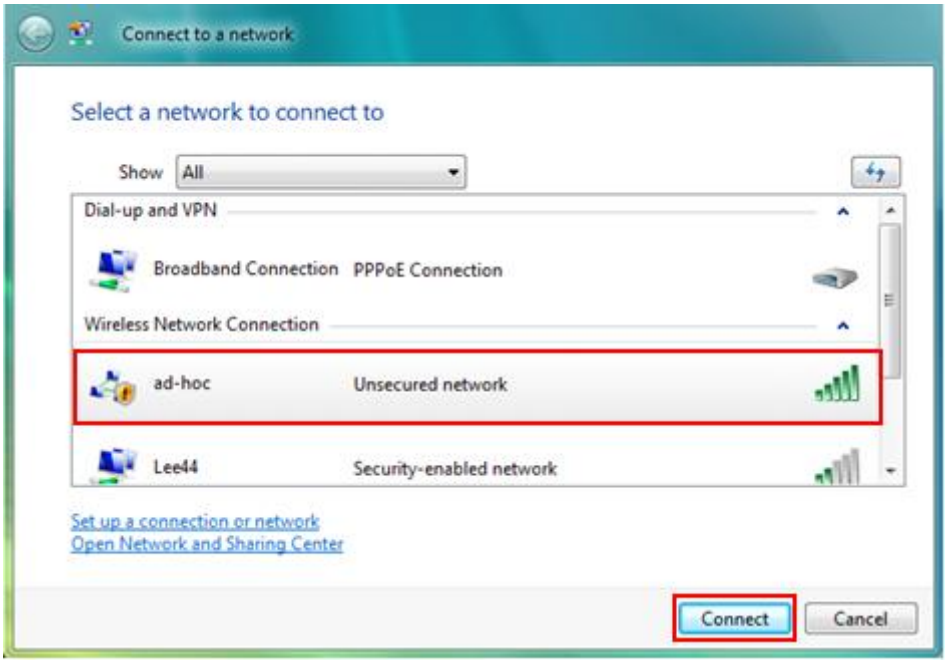
- ❖ Όταν μεταδίδεται ένα πακέτο, επιλέγεται ένα διάστημα οπισθοχώρησης μέσα στο εύρος τιμών [0, CW].
- ❖ Αντίστροφη μέτρηση όσο το κανάλι είναι αδρανές.
- ❖ Η αντίστροφη μέτρηση αναστέλλεται για τα διαστήματα που το κανάλι είναι ενεργό.
- ❖ Όταν φτάσει στο 0, μεταδίδεται RTS.

- Η επιλογή ενός μεγάλου CW οδηγεί σε μεγάλα διαστήματα οπισθοχώρησης, με αποτέλεσμα μεγαλύτερο overhead.
- Η επιλογή ενός μικρού CW οδηγεί σε μεγαλύτερο αριθμό συγκρούσεων (όταν δύο κόμβοι φτάσουν στο 0 συγχρόνως).
- Αφού ο αριθμός των κόμβων που προσπαθούν να μεταδώσουν την ίδια στιγμή μπορεί να αλλάζει με το χρόνο, απαιτείται κάποιος μηχανισμός για τη διαχείριση του ανταγωνισμού.
- IEEE 802.11 DCF: το παράθυρο ανταγωνισμού CW επιλέγεται δυναμικά, εξαρτώμενο από την συχνότητα εμφάνισης συγκρούσεων.
- Όταν ένας κόμβος δε λάβει CTS σε απάντηση κάποιου RTS που έστειλε, διπλασιάζει το cw (μέχρι κάποιο άνω όριο).
- Όταν ένας κόμβος ολοκληρώνει επιτυχημένα μια μεταφορά δεδομένων, επαναφέρει το CW σε CWmin.



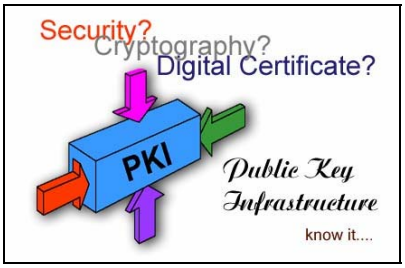
Εικόνα 47. Λειτουργία DCF

8 ΛΥΣΕΙΣ



8.1 ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ

8.1.1 Αυθεντικοποίηση Κατά Τη Διάρκεια Όλων Των Φάσεων Δρομολόγησης



Αυτή η λύση αποτελείται από τη χρησιμοποίηση των τεχνικών αυθεντικοποίησης κατά τη διάρκεια όλων των φάσεων δρομολόγησης, για να αποκλείσει τους επιτιθεμένους και τους αναρμόδιους κόμβους από τη συμμετοχή στη δρομολόγηση. Οι περισσότερες από τις προτεινόμενες λύσεις που ανήκουν σε αυτήν την κατηγορία, τροποποιούν τα υπάρχοντα πρωτόκολλα δρομολόγησης για να δημιουργήσουν λύσεις βασισμένες στην αυθεντικοποίηση. Δεδομένου ότι χρησιμοποιούν τις ψηφιακές υπογραφές, αυτές οι λύσεις στηρίζονται σε μια αρχή πιστοποιητικών (certificate authority (CA)), η οποία απαιτεί τη χρήση ενός εμπιστευμένου κεντρικού υπολογιστή πιστοποιητικών του οποίου το δημόσιο κλειδί είναι a priori γνωστό σε όλους τους έγκυρους κόμβους. Αυτή η εμπιστοσύνη σε έναν

σταθερό κεντρικό υπολογιστή αποδίδει τη λύση συγκεντρωμένα και είναι λιγότερο προσαρμόσιμη. Το σημαντικότερο πλεονέκτημα αυτής της προσέγγισης είναι ότι αποκλείει τους εξωτερικούς αναρμόδιους κόμβους από τη συμμετοχή στη δρομολόγηση, επομένως όλες οι επιθέσεις που παρουσιάστηκαν προηγουμένως αποτρέπονται όταν πραγματοποιούνται από έναν εξωτερικό κόμβο. Επιπλέον, μερικές από τις επιθέσεις που πραγματοποιούνται από έναν εξουσιοδοτημένο κόμβο μπορούν να αποτραπούν (beaten), όπως διευκρινίζει ο πίνακας 4.

Solutions	Attacks prevented	Drawbacks
Authentication during all phases	All external attacks, and the following internal attacks Spoofing Redirection by modifying route sequence number	Requires certificate authority or key sharing mechanism
Trust-level metric	All attacks prevented by authentication All attacks on higher trust-level nodes	Requires certificate authority or key sharing mechanism Difficulty to define trust level
Secure neighbor verification	All attacks prevented by authentication Rushing	Requires certificate authority or key sharing mechanism Important overhead when mobility increases
Randomize message forwarding	Rushing	Latency
Onion encryption	All external attacks, and the following internal attacks Spoofing DoS by modifying source route	Requires certificate authority or key sharing mechanism High computational cost

Πίνακας 4. Λύσεις για την ασφάλεια των πρωτοκόλλων δρομολόγησης

8.1.2 Μετρικό Επίπεδο Εμπιστοσύνης (Trust-Level Metric)

Ο Yi και οι λοιποί καθόρισαν μια νέα μετρική που καλείται τιμή εμπιστοσύνης η οποία κυβερνά τη συμπεριφορά του πρωτοκόλλου δρομολόγησης. Αυτή η μετρική πρόκειται να ενσωματωθεί στα πακέτα ελέγχου για να αντανακλάσει την ελάχιστη τιμή εμπιστοσύνης που απαιτείται από τον αποστολέα. Κατά συνέπεια, ένας κόμβος που λαμβάνει οποιοδήποτε πακέτο δεν μπορεί ούτε να το επεξεργαστεί ούτε να το διαβιβάσει εκτός αν παρέχει το απαραίτητο επίπεδο εμπιστοσύνης που παρουσιάζεται στο πακέτο. Κατά αυτόν τον τρόπο, οι συντάκτες σχεδίασαν το SAR (Security-Aware Routing), ένα πρωτόκολλο που προήλθε από τα AODV και βασίστηκαν στις ιεραρχικές τιμές εμπιστοσύνης μετρική και αυθεντικοποίηση. Στο SAR αυτή η μετρική χρησιμοποιείται επίσης ως κριτήριο για να επιλέξει τις διαδρομές όταν πολλές διαδρομές που ικανοποιούν την απαραίτητη τιμή εμπιστοσύνης, είναι διαθέσιμες. Για καθορισμό των τιμών εμπιστοσύνης των κόμβων, οι συντάκτες εξετάζουν το παράδειγμα ενός στρατιωτικού πλαισίου, στο οποίο το επίπεδο εμπιστοσύνης ταιριάζει με το βαθμό ιδιοκτησίας του κόμβου (node's owner rank). Εντούτοις, στο γενικό πλαίσιο, όπου δεν υπάρχει καμία ιεραρχία στο δίκτυο, ο

καθορισμός των τιμών εμπιστοσύνης των κόμβων είναι προβληματικός. Αυτή η τεχνική είναι βασισμένη στην αυθεντικοποίηση και απαιτεί ένα ιεραρχικό μερίδιο κλειδιού. Το πλεονέκτημα αυτής της λύσης συγκριτικά με την προηγούμενη είναι ότι αποτρέπει τις επιθέσεις από έναν εσωτερικό κόμβο σε ένα πιο υψηλό επίπεδο εμπιστοσύνης.

8.1.3 Επαλήθευση Ασφαλών Γειτόνων (Secure Neighbour Verification)

Αυτή η λύση αποτελείται από μία three-round αυθεντικοποιημένη ανταλλαγή μηνυμάτων μεταξύ δύο κόμβων προτού ο καθένας να απαιτήσει τον άλλο ως γείτονα. Εάν αυτή η ανταλλαγή αποτυγχάνει, ο καλά-συμπεριφερόμενος κόμβος αγνοεί τον άλλο και δε χειρίζεται τα πακέτα που στέλνονται από αυτόν. Αυτή η λύση κτυπά την παράνομη χρήση μιας υψηλής εμβέλειας δύναμης για να πραγματοποιήσει τις γρήγορες επιθέσεις (rushing attacks). Δεδομένου ότι ο αποστολέας που χρησιμοποιεί τις υψηλότερες δυνάμεις δεν μπορεί να λάβει το πακέτο από τους περαιτέρω κόμβους, δεν θα είναι σε θέση να εκτελέσει τη διαδικασία ανίχνευσης γειτόνων και θα αγνοηθεί. Το σημαντικότερο μειονέκτημα αυτής της λύσης είναι τα σημαντικά γενικά έξοδα όταν αυξάνεται η κινητικότητα.

8.1.4 Τυχαία Αποστολή Μηνυμάτων

Αυτή η τεχνική προτείνεται από τον Yi και τους άλλους για να ελαχιστοποιηθεί η πιθανότητα ότι ένας ορμώμενος αντίπαλος μπορεί να κυριαρχήσει σε όλες τις επιστρεφόμενες διαδρομές. Στην παραδοσιακή προώθηση RREQ, ο λαμβάνων κόμβος διαβιβάζει αμέσως το πρώτο RREQ και απορρίπτει όλα τα επόμενα RREQs. Χρησιμοποιώντας αυτό το σχέδιο, ένας κόμβος συλλέγει αρχικά διάφορα RREQs και επιλέγει τυχαία ένα RREQ για να το διαβιβάσει. Υπάρχουν έτσι δύο παράμετροι σχετικές με αυτήν την τεχνική: καταρχάς, ο αριθμός πακέτων RREQ που συλλέγονται και δεύτερον ο αλγόριθμος από τον οποίο επιλέγονται τα διαλείμματα (timeouts). Σκεφτόμαστε ότι το μειονέκτημα αυτής της λύσης είναι ότι αυξάνει την καθυστέρηση της εύρεσης διαδρομών, δεδομένου ότι κάθε κόμβος πρέπει να περιμένει ένα timeout ή να λάβει έναν δεδομένο αριθμό πακέτων πριν διαβιβάζει το RREQ. Επιπλέον, η τυχαία επιλογή αποτρέπει την ανακάλυψη των βέλτιστων διαδρομών. Η βελτίωση διαδρομών μπορεί να οριστεί ως ο αριθμός των hops, η

ενεργειακή αποδοτικότητα (energy efficiency), ή άλλη μετρική, αλλά δεν είναι τυχαία.

8.1.5 Δρομολόγηση Onion (Onion Routing)

Ο Awerbuch και οι λοιποί πρότειναν τη χρήση μιας αποδοτικής ασύμμετρης στρατηγικής κρυπτογράφησης για να προστατεύσουν και να εξασφαλίσουν την ανωνυμία για τις διαδρομές πηγής κατά τη χρησιμοποίηση ενός πρωτοκόλλου δρομολόγησης πηγής. Αυτή η στρατηγική αποτελείται από την κρυπτογράφηση μιας ανακαλυμμένης διαδρομής πηγής κατά τη διάρκεια της ανακάλυψης διαδρομών σε μια μορφή που μοιάζει με κρεμμύδι και τη διαβίβαση των πακέτων δεδομένων χρησιμοποιώντας αυτήν την κρυπτογραφημένη onion διαδρομή. Κατά τη διάρκεια της φάσης απάντησης διαδρομών (αντίστοιχα η μετάδοση αιτήματος), κάθε κόμβος προσθέτει τη διεύθυνσή του στην επόμενη (αντίστοιχα προηγούμενη) μερίδα της ανακαλυμμένης διαδρομής και κρυπτογραφεί την έκβαση χρησιμοποιώντας το δημόσιο κλειδί του προηγούμενου κόμβου (αντίστοιχα το δικό του δημόσιο κλειδί). Κατά αυτόν τον τρόπο κάθε κόμβος θα είναι σε θέση να διαβάσει μόνο το επόμενο hop όταν διαβιβάζονται τα πακέτα δεδομένων και όχι οποιοιδήποτε άλλοι. Η onion κρυπτογράφηση μιας ανακαλυμμένης διαδρομής πηγής ($n0$, $n1$, …, nk) εκτελείται κατά τη διάρκεια της φάσης απάντησης ως εξής:

Η n_k ταυτότητα κρυπτογραφείται με Pn_{k-1} (το δημόσιο κλειδί του κόμβου n_{k-1}), το αποτέλεσμα δείχνεται από τον $[n_k]_{Pnk-1}$; στο n_{k-1} αυτή η έκβαση συνδέεται στην ταυτότητα του n_{k-1} και κρυπτογραφείται με Pn_{k-2}: $[nk–1, [n_k]_{Pnk-1}]_{Pnk-2}$ και ούτω καθεξής μέχρι την επίτευξη του διαδόχου της πηγής (n_1). Η έκβαση όλων αυτών των διαδικασιών είναι η ακόλουθη onion κρυπτογραφημένη διαδρομή πηγής: $[n_1, \ldots, [n_{k-1}, [n_k]_{Pnk-1}]_{Pnk-2} \ldots]P_{n0}$.

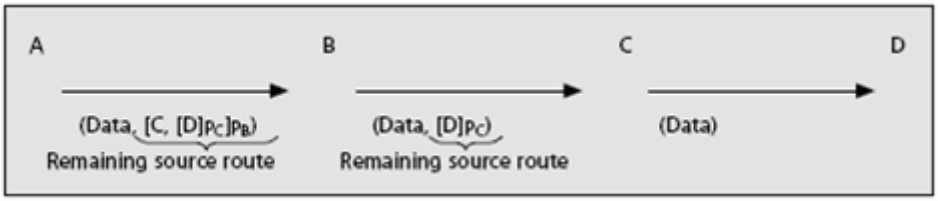
Αυτή η κρυπτογραφημένη διαδρομή θα χρησιμοποιηθεί για να καθοδηγήσει κάθε πακέτο δεδομένων. Ο n_0 κόμβος αποκρυπτογραφεί τη διαδρομή και παίρνει τη διεύθυνση του n_1, στην οποία διαβιβάζει το πακέτο, το υπόλοιπο μέρος κρυπτογραφείται με p_{n1} και δεν μπορεί να αποκρυπτογραφηθεί από τον n_0. Ο n_1 κάνει το ίδιο πράγμα και δρομολογεί το πακέτο και ούτω καθεξής μέχρι την επίτευξη του τελικού προορισμού.

Παράδειγμα

Υποθέτουμε ότι μια ανακαλυμμένη διαδρομή πηγής (B, C, D), που συνδέει τον A με τον D, είναι να χρησιμοποιηθεί από το A για να διαβιβάσει ένα πακέτο δεδομένων. Η onion-κρυπτογραφημένη ακολουθία αυτής της διαδρομής είναι: $[B, [C, [D]_{PC}]_{PB}]_{PA}$. Κατά την αποκρυπτογράφηση της διαδρομής με το ιδιωτικό κλειδί του, ο κόμβος A ανακτά τη διεύθυνση του B, στον οποίο διαβιβάζει το πακέτο. Οι άλλες διευθύνσεις (C, D) είναι κρυμμένες στον A και δεν μπορούν να αφαιρεθούν δεδομένου ότι κρυπτογραφούνται ασύμμετρα (υποθέτοντας ότι ο ασύμμετρος μηχανισμός κρυπτογράφησης είναι γερός). Όμοια, ο B (αντίστοιχα C) παίρνει τη διεύθυνση του C (αντίστοιχα D), χρησιμοποιώντας το ιδιωτικό κλειδί του, στο οποίο διαβιβάζει το πακέτο. Η Εικόνα 48 επεξηγεί αυτό το παράδειγμα.

Αυτός ο μηχανισμός εξασφαλίζει ότι κάθε κόμβος είναι μόνο ικανός να προσδιορίσει το διάδοχό του, όπου το υπόλοιπο της διαδρομής κρατιέται ανώνυμο. Συνεπώς, η επίθεση DoS με την τροποποίηση της διαδρομής πηγής αποτρέπεται. Όταν συνδυάζεται με την αυθεντικοποίηση, αυτός ο μηχανισμός είναι ισχυρός και αποδοτικός, αλλά πάσχει από υψηλό κόστος υπολογισμού.

Ο πίνακας 4 συνοψίζει τις αποτρέψιμες επιθέσεις και τις ανεπάρκειες κάθε λύσης που παρουσιάστηκε προηγουμένως, Όπως φαίνεται, όλες οι λύσεις υπερνικούν όλες τις εξωτερικές επιθέσεις και μερικές εσωτερικές επιθέσεις. Ακόμα, σχεδόν όλες οι λύσεις απαιτούν μια αρχή πιστοποιητικών ή έναν βασικό μηχανισμό διανομής, ο οποίος είναι προβληματικός στα MANETs. Η τυχαία αποστολή μηνυμάτων είναι η μόνη λύση που δεν είναι βασισμένη σε μια τέτοια απαίτηση, αλλά το πρόβλημα με αυτήν την προσέγγιση είναι η σημαντική λανθάνουσα κατάσταση που εισάγει. Κάθε λύση έχει και τα μειονεκτήματά της.



Εικόνα 48. Παράδειγμα προώθησης πακέτου με χρήση κρυπτογράφησης onion

8.1.6 Αποκρύπτοντας Την Τοπολογία Ή Τη Δομή Του Δικτύου

8.1.6.1 Χρήση Ανεξάρτητου Αντιπροσώπου Ασφαλείας (Security Agent-SA)

Αυτή η μέθοδος καλείται μέθοδος μη-κοινοποίησης (NDM) (Non-disclosure). Στην NDM διάφοροι ανεξάρτητοι αντιπρόσωποι ασφάλειας (SA) κατανέμονται στο δίκτυο. Κάθε ένας από αυτούς τους αντιπροσώπους SAi είναι κύριος ενός ζευγαριού ασυμμετρικών κρυπτογραφικών κλειδιών KSAi και KSAi-. Ο αποστολέας S επιθυμεί να διαβιβάσει ένα μήνυμα M στο δέκτη P χωρίς να αποκαλύψει τη θέση του. Ο S στέλνει το μήνυμα χρησιμοποιώντας διάφορους SAs: SA1 (SA2 (… (SAN (R. Το μήνυμα έχει ενθυλακωθεί N φορές χρησιμοποιώντας τα δημόσια κλειδιά KSA1… KSAn ως εξής.

$$M' = KSA1(SA2, (KSA2\ (SA3\ (\ldots(KSAN(R, M))\ldots))))$$

Για να παραδώσει το πακέτο, ο S το στέλνει στον πρώτο αντιπρόσωπο ασφάλειας SA1 που αποκρυπτογραφεί την εξωτερική ενθυλάκωση και διαβιβάζει το πακέτο στον επόμενο αντιπρόσωπο. Κάθε SA ξέρει μόνο τη διεύθυνση του προηγούμενου και επόμενου hop. Ο τελευταίος αντιπρόσωπος αποκρυπτογραφεί τελικά το μήνυμα και το διαβιβάζει στον P. Εισάγει ένα ανώτατο όριο (overhead) και ως εκ τούτου δεν προτιμάται για τη δρομολόγηση.

8.1.6.2 Πρωτόκολλο Δρομολόγησης Ζώνης (Zone Routing Protocol - ZRP)

Είναι ένα ιεραρχικό πρωτόκολλο όπου το δίκτυο διαιρείται σε ζώνες. Οι ζώνες λειτουργούν ανεξάρτητα μεταξύ τους. Το ZRP περιλαμβάνει δύο χωριστά πρωτόκολλα δρομολόγησης.

Μια τέτοια ιεραρχική δομή δρομολόγησης είναι ευνοϊκή όσον αφορά την ασφάλεια, δεδομένου ότι ένας καλά σχεδιασμένος αλγόριθμος πρέπει να είναι σε θέση να περιέχει ορισμένα προβλήματα σε μικρή μερίδα της ιεραρχίας αφήνοντας άλλες μερίδες απρόσβλητες.

Το ZRP έχει μερικά χαρακτηριστικά γνωρίσματα που φαίνεται να το καθιστούν κάπως λιγότερο ευαίσθητο στις επιθέσεις δρομολόγησης. Η ιεραρχική οργάνωσή του κρύβει μερικές από τις πληροφορίες δρομολόγησης μέσα στις ζώνες. Το ZRP παρέχει κάποια μορφή ασφάλειας ενάντια στην αποκάλυψη της τοπολογίας

δικτύων με τη διαίρεση της δρομολόγησης σε ζώνες, οι οποίες κρύβουν την εσωτερική οργάνωση.

8.2 ΛΥΣΕΙΣ ΑΝΙΧΝΕΥΣΗΣ ΕΝΑΝΤΙΑ ΣΤΟΝ ΕΓΩΙΣΜΟ (SELFISHNESS) ΤΗΣ ΠΡΟΩΘΗΣΗΣ ΔΕΔΟΜΕΝΩΝ

8.2.1 Ανατροφοδοτήσεις End To End (End To End Feedbacks)

Αυτός ο μηχανισμός αποτελείται από την αναγνώριση των πακέτων στο επίπεδο δικτύου κατά τρόπο end-to-end, για να καταστήσει αξιόπιστο το πρωτόκολλο δρομολόγησης (όπως το TCP). Δηλαδή ο κόμβος προορισμού αναγνωρίζει τα επιτυχώς λαμβανόμενα πακέτα με την αποστολή των ανατροφοδοτήσεων (ACKs) στην πηγή. Μια επιτυχής υποδοχή υπονοεί ότι η αντίστοιχη διαδρομή είναι λειτουργική, ενώ μια αποτυχία στην υποδοχή ACK μετά από ένα διάλειμμα μπορεί να θεωρηθεί ως ένδειξη ότι η διαδρομή είναι είτε σπασμένη, είτε compromised, είτε περιλαμβάνει τους εγωιστικούς κόμβους. Τα πρωτόκολλα δρομολόγησης που βασίζονται σε αυτήν την προσέγγιση, διατηρούν μια εκτίμηση για κάθε διαδρομή. Αυτή η εκτίμηση απεικονίζει την αξιοπιστία της διαδρομής και ενημερώνεται κάθε φορά που διαβιβάζεται ένα κομμάτι των δεδομένων (ένα σύνολο πακέτων δεδομένων) πέρα από τη διαδρομή. Αυξάνεται για κάθε επιτυχή υποδοχή (όταν λαμβάνει η πηγή το ACK εκείνου του κομματιού) και μειώνεται για κάθε αποτυχημένο κομμάτι (όταν λήγει ένα διάλειμμα χωρίς τη λήψη ενός ACK). Τα χαμένα πακέτα μπορούν να αναμεταδοθούν σε αυτήν την περίπτωση. Όταν η εκτίμηση πορειών μιας δεδομένης διαδρομής μειώνεται κάτω από ένα καθορισμένο κατώτατο όριο, το οποίο είναι αρκετά υψηλό για να υπερνικήσει τις απώλειες λόγω των συγκρούσεων, αυτή η διαδρομή δε θα χρησιμοποιηθεί άλλο. Επιπλέον, το πρωτόκολλο δρομολόγησης μπορεί να αλλάξει για να στηριχθεί σε αυτήν την εκτίμηση ως μετρικό και να επιλέξει τις πιο αξιόπιστες διαδρομές.

Το σημαντικότερο πρόβλημα με αυτήν την τεχνική είναι η έλλειψη ανίχνευσης κόμβων απρεπούς συμπεριφοράς. Αυτή η τεχνική μπορεί να ανιχνεύσει τους συμπεριφερόμενους απρεπώς ή κακόβουλους κόμβους κι αυτούς που είναι κατεστραμμένοι, αλλά χωρίς την παραγωγή οποιασδήποτε διάκρισης μεταξύ αυτών των δύο περιπτώσεων και χωρίς συμπληρωματικές πληροφορίες σχετικά με τον κόμβο που προκαλεί την απώλεια πακέτων. Εν τούτοις, αυτή η τεχνική βοηθά στην αποφυγή των άχρηστων μεταδόσεων πακέτων μέσω των αναξιόπιστων διαδρομών

και μπορεί να συνδυαστεί με άλλες περιπλοκότερες τεχνικές. Χρησιμοποιείται σε SMTP μαζί με μια άλλη τεχνική, αποκαλούμενη διασπορά στοιχείων (dispersal), η οποία θα παρουσιαστεί αργότερα. Χρησιμοποιείται επίσης συνδυασμένη με την εξέταση (probing), η οποία επίσης θα παρουσιαστεί αργότερα.

8.2.2 Εγκατάσταση Πρόσθετων Δυνατοτήτων Στο Δίκτυο Προκειμένου Να Μετριαστεί Η Απρεπής Συμπεριφορά Δρομολόγησης

Οι κόμβοι απρεπούς συμπεριφοράς μπορούν να μειώσουν την απόδοση δικτύων και να οδηγήσουν στη φτωχή ευρωστία. Ο Sergio Marti και οι άλλοι προτείνουν μια τεχνική για να προσδιορίσουν και να απομονώσουν τέτοιους κόμβους με την εγκατάσταση ενός φύλακα και ενός pathrater στο ad-hoc δίκτυο σε κάθε κόμβο.

Υποθέσεις

Υποτίθεται ότι οι ασύρματες συνδέσεις είναι αμφίδρομες. Τα περισσότερα πρωτόκολλα επιπέδων MAC το απαιτούν αυτό. Υποτίθεται επίσης η υποστήριξη για τον αυθαίρετο (promiscuous) τρόπο λειτουργίας των κόμβων. Αυτό βοηθά τους κόμβους να εποπτεύσουν ο ένας τη λειτουργία του άλλου. Η τρίτη υπόθεση είναι ότι το ελλοχεύον ad-hoc πρωτόκολλο δρομολόγησης είναι DSR. Είναι δυνατό να επεκταθεί ο μηχανισμός και σε άλλα πρωτόκολλα δρομολόγησης.

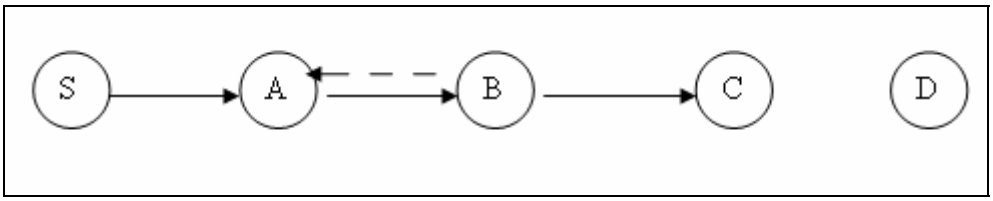
8.2.3 Έλεγχος Στον Promiscuous Τρόπο (Φυλακας-Watchdog)

Στο καλύτερο της γνώσης μας, ο Marti και οι άλλοι ήταν οι πρώτοι που εξέτασαν το πρόβλημα της απρεπούς συμπεριφοράς των κόμβων στη διαβίβαση δεδομένων στα MANETs. Καθόρισαν τη μέθοδο φυλάκων (watchdog), μια βασική τεχνική στην οποία στηρίζονται πολλές περαιτέρω λύσεις. Στοχεύει να ανιχνεύσει τους κόμβους απρεπούς συμπεριφοράς που δεν διαβιβάζουν τα πακέτα (ή τους κακόβουλους κόμβους που ρίχνουν σκόπιμα τα πακέτα) κατά τη χρησιμοποίηση ενός πρωτοκόλλου δρομολόγησης πηγής, με τον έλεγχο των γειτόνων στον αυθαίρετο (promiscuous) τρόπο.

Υποθέστε ότι ο κόμβος S στέλνει τα πακέτα στον D χρησιμοποιώντας μια διαδρομή συμπεριλαμβανομένων (μεταξύ των άλλων) τριών ενδιάμεσων κόμβων A, B και C. Όταν ο A διαβιβάζει ένα πακέτο στον B που διαβιβάζει στον C, ο A μπορεί

να ελέγξει εάν ο B διαβιβάζει κάθε πακέτο με το να αναλύει τα πακέτα που κρυφακούει κατά τη διάρκεια ενός δεδομένου διαλείμματος. Εάν ο A κρυφακούσει ένα πακέτο το ελέγχει κατά τη διάρκεια του σταθερού διαλείμματος, κατόπιν επικυρώνει την αποστολή του, διαφορετικά αυξάνει μια εκτίμηση σχετικά με τον B και θα κρίνει ότι ο B συμπεριφέρεται απρεπώς όταν το ποσοστό υπερβαίνει ένα δεδομένο κατώτατο όριο, κατόπιν δηλώνει τον S. Αυτός ο έλεγχος είναι γενικευμένος για κάθε ζευγάρι των hop στη διαδρομή πηγής.

Ο φύλακας (watchdog) είναι σε θέση να ανιχνεύσει τους κόμβους απρεπούς συμπεριφοράς σε πολλές περιπτώσεις και δεν απαιτεί overhead όταν κανένας κόμβος δεν συμπεριφέρεται απρεπώς. Εν τούτοις, αποτυγχάνει στην ανίχνευση της απρεπούς συμπεριφοράς σε μερικές περιπτώσεις. Για παράδειγμα, μετά από μια σύγκρουση στον C, ο B θα μπορούσε να παρακάμψει την αναμετάδοση του πακέτου χωρίς να ανιχνευτεί από τον A. Ο φύλακας (watchdog) επίσης αποτυγχάνει όταν συνεργούν δύο διαδοχικοί κόμβοι για να κρύψουν την απρεπή συμπεριφορά ο ένας του άλλου, που σημαίνει ότι ο B θα μπορούσε να συνεργήσει με τον C και να μην υποβάλει έκθεση στον A όταν συμπεριφέρεται απρεπώς ο C. Εν τούτοις, αυτή η συνεταιριστική απρεπής συμπεριφορά, είναι πολύ δύσκολο να ανιχνευθεί. Ένα άλλο μειονέκτημα με αυτήν την λύση είναι ότι μπορεί να προκαλέσει ψεύτικες ανιχνεύσεις, ειδικά όταν ο ελεγχόμενος κόμβος χρησιμοποιεί την τεχνική ελέγχου δύναμης για να συντηρηθεί η δύναμή του. Όταν ο C είναι πιο κοντά στον B από ότι στον A και όταν ο B διαβιβάζει τα πακέτα χρησιμοποιώντας την ελεγχόμενη δύναμη σύμφωνα με την απόσταση που τον χωρίζει από τον C, ο A δεν θα μπορούσε να κρυφακούσει την αποστολή του B και μπορεί να τον κατηγορήσει λανθασμένα. Η Εικόνα 49 δείχνει τη λειτουργία του watchdog.



Εικόνα 49. Η λειτουργία του watchdog

Πλεονεκτήματα

Ο watchdog μηχανισμός μπορεί να ανιχνεύσει κόμβους με απρεπή συμπεριφορά στο επίπεδο προώθησης κι όχι μόνο στο επίπεδο ζεύξης.

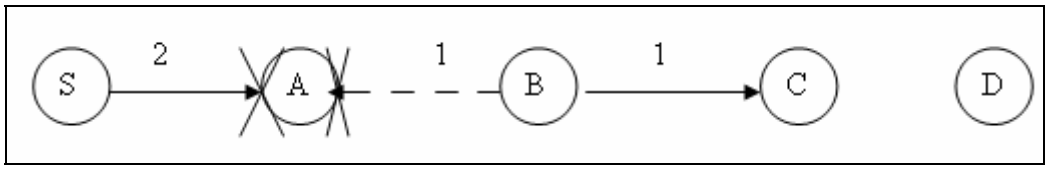
Αδυναμίες

Ίσως να μην ανιχνεύσει κόμβους με απρεπή συμπεριφορά παρουσία των 1) διφορούμενων συγκρούσεων (ambiguous collisions) 2) συγκρούσεων λήψης (receiver collisions) 3) περιορισμένης δύναμης μετάδοσης (limited transmission power) 4) ψεύτικης κακής συμπεριφοράς (false misbehavior) 5) σύγκρουσης (collision) 6) μερικής μείωσης (partial dropping).

8.2.3.1 Ανάλυση Των Αδυναμιών Του Watchdog

1) Διφορούμενη Σύγκρουση (Ambiguous collision)

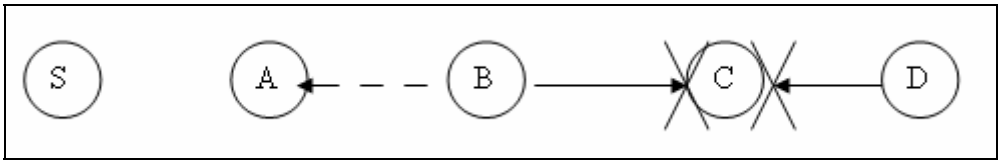
Το διφορούμενο πρόβλημα σύγκρουσης αποτρέπει τον Α από το να κρυφακούσει τις μεταδόσεις από τον Β. Όπως επεξηγεί η Εικόνα 50, μια σύγκρουση πακέτων εμφανίζεται στο Α ενώ αφουγκράζεται τον Β που διαβιβάζει ένα πακέτο. Ο Α δεν ξέρει εάν η σύγκρουση προκλήθηκε με την αποστολή σε ένα πακέτο όπως θα έπρεπε ή εάν ο Β δεν διαβίβασε ποτέ το πακέτο και η σύγκρουση προκλήθηκε από άλλους κόμβους στη γειτονιά του Α. Λόγω αυτής της αβεβαιότητας, ο Α πρέπει αντ' αυτού να συνεχίσει να προσέχει τον Β για μια χρονική περίοδο.



Εικόνα 50. Ambiguous collision

2) Σύγκρουση Λήψης (Receiver collision)

Στο πρόβλημα σύγκρουσης λήψης, ο κόμβος Α μπορεί μόνο να πει εάν ο Β στέλνει το πακέτο στον C, αλλά δεν μπορεί να πει εάν ο C το λαμβάνει. Εάν μια σύγκρουση εμφανίζεται στον C όταν πρώτα ο Β διαβιβάσει το πακέτο, ο Α βλέπει μόνο τον Β να προωθεί το πακέτο και υποθέτει ότι ο C το λαμβάνει επιτυχώς. Κατά συνέπεια, ο Β θα μπορούσε να προσπεράσει την αναμετάδοση του πακέτου και να αποφύγει την ανίχνευση (Εικόνα 51).



Εικόνα 51. Σύγκρουση λήψης (receiver collision)

3) Ψεύτικη Κακή Συμπεριφορά (False misbehavior)

Η ψεύτικη κακή συμπεριφορά μπορεί να εμφανιστεί όταν οι κόμβοι αναφέρουν ψευδώς άλλους κόμβους ότι συμπεριφέρονται απρεπώς. Ένας κακόβουλος κόμβος θα μπορούσε να προσπαθήσει να διαμοιράσει (partition) το δίκτυο με τον ισχυρισμό ότι μερικοί κόμβοι που τον ακολουθούν στο μονοπάτι, συμπεριφέρονται απρεπώς. Για παράδειγμα, ο κόμβος A θα μπορούσε να αναφέρει ότι ο κόμβος B δεν διαβιβάζει τα πακέτα όταν στην πραγματικότητα τα διαβιβάζει. Αυτό θα αναγκάσει τον S να χαρακτηρίσει τον B ως απρεπώς συμπεριφερόμενο όταν ο A είναι ο ένοχος. Αυτή η συμπεριφορά, εν τούτοις, θα ανιχνευθεί. Δεδομένου ότι ο A περνά τα μηνύματα επάνω στον B (όπως ελέγχεται από τον S), κατόπιν οποιεσδήποτε αναγνωρίσεις από τον D στον S θα περάσουν από τον A στον S και ο S θα αναρωτηθεί γιατί λαμβάνει τις απαντήσεις από τον D όταν υποθετικά ο B έριξε τα πακέτα στην μπροστινή κατεύθυνση. Επιπλέον, εάν ο A ρίξει τις αναγνωρίσεις για να τις κρύψει από τον S, ο κόμβος B θα ανιχνεύσει αυτή την απρεπή συμπεριφορά και θα την αναφέρει στον D.

4) Περιορισμένη Δύναμη Μετάδοσης (Limited transmission power)

Ένα άλλο πρόβλημα είναι ότι ένας κόμβος απρεπούς συμπεριφοράς που μπορεί να ελέγξει τη δύναμη μετάδοσής του, μπορεί να παρακάμψει το φύλακα (watchdog). Ένας κόμβος θα μπορούσε να περιορίσει τη δύναμη μετάδοσής του έτσι ώστε το σήμα να είναι αρκετά ισχυρό ώστε να κρυφακουστεί από τον προηγούμενο κόμβο αλλά πάρα πολύ αδύνατο για να παραληφθεί από τον αληθινό παραλήπτη.

5) Πολλαπλή Σύγκρουση Κόμβων (Multiple colliding nodes)

Οι πολλαπλοί κόμβοι στη συνεργία μπορούν να φτιάξουν μια περιπλοκότερη επίθεση. Παραδείγματος χάριν, ο B και ο C από το Εικόνα 43 θα μπορούσαν να συνεργήσουν για να προκαλέσουν αναστάτωση. Σε αυτήν την περίπτωση, ο B

διαβιβάζει ένα πακέτο στον C αλλά δεν υποβάλλει αναφορά στον A όταν ο C ρίχνει το πακέτο. Λόγω του περιορισμού του, μπορεί να είναι απαραίτητο να απαγορευθούν δύο διαδοχικοί ανέμπιστοι κόμβοι σε μια πορεία δρομολόγησης.

6) Partial dropping

Ένας κόμβος μπορεί να παρακάμψει το φύλακα (watchdog) με τη ρίψη των πακέτων σε ένα χαμηλότερο ποσοστό από το διαμορφωμένο ελάχιστο κατώτατο όριο κακής συμπεριφοράς του φύλακα (watchdog). Αν και ο φύλακας (watchdog) δε θα ανιχνεύσει αυτόν τον κόμβο ως απρεπώς συμπεριφερόμενος, αυτός ο κόμβος αναγκάζεται να διαβιβάσει στο εύρος ζώνης κατώτατων ορίων. Κατά αυτόν τον τρόπο ο φύλακας (watchdog) χρησιμεύει για να επιβάλει αυτό το ελάχιστο εύρος ζώνης. Για να εργαστεί κατάλληλα ο φύλακας (watchdog) πρέπει να ξέρει το που πρέπει να είναι ένα πακέτο σε δύο hops.

8.2.4 Pathrater

Ακριβώς όπως ο φύλακας (watchdog), το pathrater οργανώνεται από κάθε κόμβο. Συνδυάζει τη γνώση κόμβων απρεπούς συμπεριφοράς με τα δεδομένα αξιοπιστίας συνδέσεων στην επιλογή. Είναι η πιο αξιόπιστη διαδρομή. Κάθε κόμβος διατηρεί μια εκτίμηση για κάθε άλλο κόμβο που ξέρει στο δίκτυο. Υπολογίζει μια πορεία μετρική με τον υπολογισμό του μέσου όρου των εκτιμήσεων των κόμβων στην πορεία. Επιλέγουμε αυτό το μετρικό επειδή δίνει μια σύγκριση της γενικής αξιοπιστίας των διαφορετικών πορειών και επιτρέπει στο pathrater να μιμηθεί τον πιο σύντομο αλγόριθμο μήκους πορειών όταν δεν έχει συλλεχθεί καμία πληροφορία αξιοπιστίας, όπως εξηγείται κατωτέρω. Εάν υπάρχουν πολλαπλάσιες πορείες στον ίδιο προορισμό, επιλέγουμε την πορεία με το υψηλότερο μετρικό. Δεδομένου ότι το pathrater εξαρτάται από τη γνώση της ακριβούς πορείας που ένα πακέτο έχει διαβεί, πρέπει να εφαρμοστεί πάνω από ένα πρωτόκολλο δρομολόγησης πηγής.

Το pathrater ορίζει τις εκτιμήσεις στους κόμβους σύμφωνα με τον ακόλουθο αλγόριθμο. Όταν ένας κόμβος στο δίκτυο γίνεται γνωστός στο pathrater (μέσω της ανακάλυψης διαδρομών), το pathrater του ορίζει μια «ουδέτερη» εκτίμηση του 0.5. Ένας κόμβος πάντα εκτιμά τα ίδια ποσοστά με 1.0. Αυτό εξασφαλίζει ότι κατά τον υπολογισμό των ποσοστών πορειών, εάν όλοι οι άλλοι κόμβοι είναι ουδέτεροι κόμβοι (παρά πιθανοί κόμβοι απρεπούς συμπεριφοράς) το pathrater επιλέγει την κοντύτερη

πορεία μήκους. Το pathrater αυξάνει τις εκτιμήσεις των κόμβων σε όλες τις ενεργά χρησιμοποιημένες πορείες από 0.01 σε περιοδικά διαστήματα των 200 msec. Μια ενεργά χρησιμοποιημένη πορεία είναι εκείνη στην οποία ο κόμβος έχει στείλει ένα πακέτο μέσα στο προηγούμενο διάστημα αύξησης ποσοστού. Η μέγιστη τιμή που μπορεί να επιτύχει ένας ουδέτερος κόμβος είναι 0.8. Μειώνουμε την εκτίμηση ενός κόμβου στο 0.05 όταν ανιχνεύουμε ένα σπάσιμο συνδέσεων κατά τη διάρκεια διαβίβασης του πακέτου και ο κόμβος γίνεται απρόσιτος. Η χαμηλότερη συνδεδεμένη εκτίμηση ενός «ουδέτερου» κόμβου είναι 0.0. Το pathrater δεν τροποποιεί τις εκτιμήσεις-αξιολογήσεις (ratings) των κόμβων που δεν είναι εκείνη τη στιγμή σε ενεργή χρήση.

Ορίζουμε την ιδιαίτερα υψηλή αρνητική αξία, -100 στις προσομοιώσεις, στους κόμβους που υποψιάζονται ότι έχουν απρεπή συμπεριφορά, από το μηχανισμό watchdog. Όταν το pathrater υπολογίζει την μετρική πορεία, οι αρνητικές τιμές πορειών δείχνουν την ύπαρξη ενός ή περισσότερων πιθανών κόμβων απρεπούς συμπεριφοράς στην πορεία. Εάν ένας κόμβος είναι χαρακτηρισμένος ως συμπεριφερόμενος απρεπώς λόγω μιας προσωρινής δυσλειτουργίας ή μιας ανακριβούς κατηγορίας θα ήταν προτιμητέος εάν δεν αποκλείστηκε μόνιμα από τη δρομολόγηση. Επομένως οι κόμβοι που έχουν τις αρνητικές εκτιμήσεις θα πρέπει να αυξάνουν αργά τις εκτιμήσεις τους ή να γυρίσουν πίσω σε μια μη αρνητική αξία μετά από ένα μακροχρόνιο διάλειμμα.

8.2.5 Απόδοση (Performance)

Throughput and Overhead

Οι watchdog και pathrater μηχανισμοί μαζί με τον αλγόριθμο DSR βελτιώνουν την απόδοση κατά 27% αυξάνοντας το overhead από 12% σε 24%. Αλλά αυτό το overhead οφείλεται στον τρόπο που λειτουργεί το DSR για να διατηρήσει τις διαδρομές. Ο ίδιος ο φύλακας (watchdog) προσθέτει πολύ ελάχιστα το overhead. Αν και τα γενικά έξοδα είναι σημαντικά, αυτές οι επεκτάσεις βελτιώνουν ακόμα την καθαρή απόδοση. Στα δίκτυα με τη μέτρια κινητικότητα η απόδοση βελτιώνεται κατά 17% ενώ η υπερυψωμένη μετάδοση αυξάνεται από 9% σε 17%.

8.2.6 Κρυφάκουσμα Βασισμένο Στη Δραστηριότητα (Activity-Based Overhearing)

Ο Kargi και οι άλλοι προτείνουν την activity-based overhearing τεχνική, η οποία είναι μια γενίκευση της τεχνικής watchdog. Σε αυτήν την τεχνική, ένας κόμβος ελέγχει συνεχώς στον αυθαίρετο (promiscuous) τρόπο τη δραστηριότητα κυκλοφορίας όλων των γειτόνων του για τα κανονικά πακέτα δεδομένων και επιτηρεί την αποστολή κάθε πακέτου του οποίου ο επόμενος αποστολέας είναι επίσης στη γειτονιά του. Αυτό μπορεί να αυξήσει τον αριθμό παρατηρήσεων και να βελτιώσει την αποδοτικότητα του watchdog. Αυτή η γενική τεχνική υποφέρει επίσης από όλα τα προβλήματα που αναφέρονται ανωτέρω, ειδικά αυτά που αφορούσαν την τεχνική ελέγχου δύναμης, δεδομένου ότι στηρίζεται στον αυθαίρετο τρόπο ελέγχου.

8.2.7 Αμοιβαία Αποδοχή Σύμφωνη Με Τη Γειτονιά (Mutually According Admission In Neighbourhood)

Ο Yang και οι άλλοι έχουν περιγράψει μια ενοποιημένη λύση επιπέδου δικτύου βασισμένη στην προσέγγιση αμοιβαίας χορήγησης της αποδοχής στη γειτονιά. Αυτή η τεχνική στοχεύει στην προστασία και της δρομολόγησης και της αποστολής δεδομένων. Στον πυρήνα αυτής της λύσης είναι ένα κατώφλι (threshold) υπογραφής βασισμένο στην κρυπτογραφία και στην τεχνική watchdog. Στα ακόλουθα περιγράφουμε εν συντομία αυτήν την προσέγγιση:

Οι κόμβοι μιας γειτονιάς συμφωνούν αμοιβαία στις αποδοχές συμμετοχής και οι κόμβοι χωρίς ενημερωμένες αποδοχές αποκλείονται από οποιαδήποτε υπηρεσία δικτύων. Κάθε κόμβος έχει ένα κουπόνι (token) που εκδίδεται (issued) από τους τοπικούς γείτονές του, το οποίο του επιτρέπει να συμμετέχει στις διαδικασίες δικτύων. Το κουπόνι έχει μια περίοδο λήξης, της οποίας η τιμή εξαρτάται από το πόσο πολύ ο κόμβος κατόχων έχει συμπεριφερθεί καλά. Αυτό το τελευταίο ανανεώνει (αναπροσαρμογές) το κουπόνι πριν από τη λήξη του. Οι κόμβοι σε μια γειτονιά ελέγχουν σε συνεργασία ο ένας τον άλλον για να ανιχνεύσουν οποιοδήποτε κακή συμπεριφορά.

Υπάρχει ένα βασικό ζευγάρι SK/PK (μυστικό κλειδί και δημόσιο κλειδί), κάθε κουπόνι που μεταφέρεται από έναν κόμβο υπογράφεται με το σφαιρικό μυστικό κλειδί SK και μεταδίδεται περιοδικά στο hello μήνυμα που ρωτά για μια νέα επικύρωση. Η token επικύρωση μπορεί να ελεγχθεί χρησιμοποιώντας το PK σε οποιοδήποτε κόμβο. Σημειώστε ότι το hello μήνυμα ή το αναγνωριστικό σήμα είναι ένα πρόσθετο μήνυμα που μεταδίδεται περιοδικά από κάθε κόμβο για να ενημερώσει τους κόμβους σε μια γειτονιά για την παρουσία του εκπομπού. Κάθε κόμβος έχει ένα

μερικό κλειδί που είναι ένα μέρος του SK και συμμετέχει με την παροχή μιας μερικής υπογραφής της διαταγής K, κατά συνέπεια οι K διαφορετικές μερικές υπογραφές είναι επαρκείς για να παρέχουν τη σωστή υπογραφή. Με άλλα λόγια, το SK διαιρείται μεταξύ των κόμβων κατά τέτοιο τρόπο ώστε οι διαφορετικές υπογραφές K με τα διαφορετικά μερικά κλειδιά K να είναι απαραίτητες και επαρκείς για να καταστήσουν μια υπογραφή ισοδύναμη με αυτήν που γίνεται από το SK. Αυτή η τεχνική καλείται πολυωνυμική μυστική διανομή (polynomial secret sharing). Για να αποφασίσει εάν πρέπει να παρασχεθεί ένα μερικό υπογεγραμμένο σημείο για τον αιτούντα, η ιστορική συμπεριφορά του αιτούντος λαμβάνεται υπόψη. Για αυτόν το λόγο, το watchdog υιοθετείται για να ελέγξει τους γείτονες και να ανιχνεύσει οποιαδήποτε απρεπή συμπεριφορά και τα αιτήματα από τους κόμβους που θεωρούνται ότι συμπεριφέρονται απρεπώς, αρνούνται.

Ένας κόμβος πρέπει να έχει τουλάχιστον K γείτονες, διαφορετικά δεν μπορεί να πάρει ένα έγκυρο υπογεγραμμένο κουπόνι και συνεπώς θα αποκλειστεί άδικα. Επιπλέον, τα προβλήματα ανίχνευσης όλου του watchdog παραμένουν εκκρεμή με αυτήν την λύση, δεδομένου ότι ο watchdog χρησιμοποιείται για τον έλεγχο.

8.3 ΛΥΣΕΙΣ ΒΑΣΙΣΜΕΝΕΣ ΣΤΗ ΦΗΜΗ (REPUTATION-BASED SOLUTIONS)

Η φήμη είναι το ποσό εμπιστοσύνης που εμπνέεται από ένα ιδιαίτερο μέλος μιας κοινότητας σε μια συγκεκριμένη ρύθμιση ή μια περιοχή ενδιαφέροντος. Τα μέλη που συμβάλλουν πρόθυμα στην κοινοτική ζωή αναπτύσσουν μια καλή φήμη μεταξύ των κοινοτικών μελών, ενώ άλλα που αρνούνται να συνεργαστούν, φημίζονται άσχημα και βαθμιαία αποκλείονται από την κοινότητα. Τα συστήματα φήμης έχουν προταθεί για ποικίλες εφαρμογές, μεταξύ τους αναφέρουμε την επιλογή των καλών ομάδων (peers) σε ένα peer-to-peer δίκτυο, την επιλογή των συνεργατών συναλλαγής για on-line δημοπρασία και ιδιαίτερα την υπεράσπιση ενάντια στους συμπεριφερόμενους απρεπώς και κακόβουλους κόμβους στα κινητά ad-hoc δίκτυα.

Στο πλαίσιό μας (context), η φήμη ενός κόμβου είναι το ποσό εμπιστοσύνης που οι άλλοι κόμβοι χορηγούν σε αυτόν, σχετικά με τη συνεργασία και τη συμμετοχή του στην αποστολή των πακέτων. Ως εκ τούτου, κάθε κόμβος παρακολουθεί ο ένας τη φήμη του άλλου σύμφωνα με τη συμπεριφορά που παρατηρεί και οι πληροφορίες φήμης μπορούν να ανταλλαχθούν μεταξύ των κόμβων για να βοηθήσουν ο ένας τον άλλο να συμπεράνουν τις ακριβείς τιμές.

Υπάρχει μια ανταλλαγή μεταξύ της αποδοτικότητας στη χρησιμοποίηση των διαθέσιμων πληροφοριών και της ευρωστίας ενάντια στην παραπληροφόρηση. Εάν εξετάζονται οι εκτιμήσεις που γίνονται από άλλους, το σύστημα φήμης μπορεί να είναι τρωτό στις ψεύτικες κατηγορίες ή τον ψεύτικο έπαινο. Εντούτοις, εάν εξετάζεται μόνο η εμπειρία κάποιου, η δυνατότητα για την εκμάθηση από την εμπειρία των άλλων μένει αχρησιμοποίητη, γεγονός που μειώνει την αποδοτικότητα.

Έχουν προταθεί δύο λύσεις που ανήκουν στην κατηγορία βασισμένη στη φήμη, ο CORE και ο CONFIDANT. Στην πρώτη λύση, οι θετικές παρατηρήσεις (καλά-συμπεριφερόμενων κόμβων) διαδίδονται αλλά όχι οι αρνητικές παρατηρήσεις, οι οποίες μειώνουν τη δυνατότητα για την εκμάθηση από τις παρατηρήσεις που γίνονται από άλλους και μπορεί να μειώσει την αποδοτικότητα της ανίχνευσης απρεπούς συμπεριφοράς στο δίκτυο. Αφ' ενός, το σύστημα φήμης του CONFIDANT στηρίζεται στις αρνητικές εντυπώσεις εμπειρίας παρά στις θετικές. Ο Buchegger και οι λοιποί το δικαιολόγησαν από το γεγονός ότι η απρεπής συμπεριφορά είναι ιδανικά η εξαίρεση παρά ο κανόνας. Για να μετριάσει την ευπάθεια στις επιθέσεις DoS με τη διάδοση των ψεύτικων κατηγοριών, ο διευθυντής εμπιστοσύνης (trust manager) του CONFIDANT χρησιμοποιεί μια λειτουργία ποσοστού που ορίζει τα διαφορετικά βάρη στους τύπους ανιχνεύσεων συμπεριφοράς, για να δώσει με τέτοιο τρόπο περισσότερη σημασία στις τοπικές παρατηρήσεις κατά την υπολογισμό της εκτίμησης φήμης. Και η χρήση του CONFIDANT και η χρήση του CORE ελέγχουν τις ενώσεις που στηρίζονται πλήρως στον αυθαίρετο (promiscuous) τρόπου ελέγχου. Συνεπώς κληρονομούν όλες τα μειονεκτήματα ανίχνευσης του watchdog.

8.4 ΕΡΕΥΝΑ (PROBING)

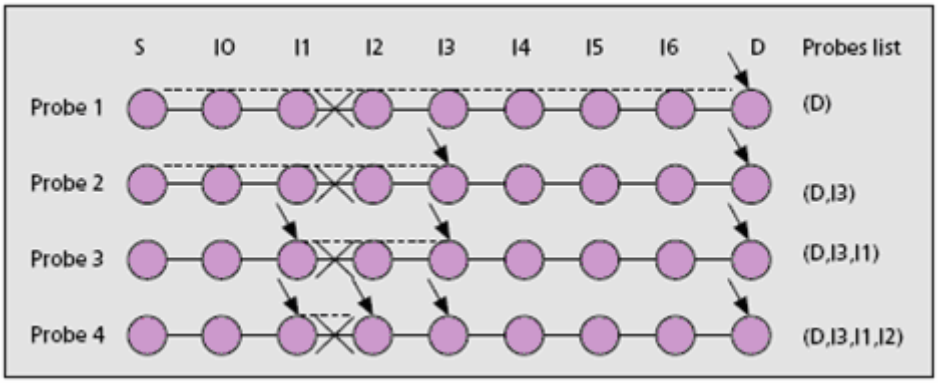
Αυτός ο μηχανισμός αποτελείται από απλή ενσωμάτωση εντολών στα πακέτα δεδομένων για να τα αναγνωρίσει. Αυτές οι εντολές καλούνται έλεγχοι (probes) και προορίζονται για τους επιλεγμένους κόμβους. Οι έλεγχοι γενικά πραγματοποιούνται όταν ανιχνεύεται μια διαδρομή που περιέχει έναν εγωιστικό ή κακόβουλο κόμβο (αλλά όχι η ταυτότητα εκείνου του κόμβου).

Ο Awerbuch και οι λοιποί είναι οι πρώτοι που χρησιμοποιούν αυτό τον μηχανισμό. Το πρωτόκολλο που έχουν προτείνει, είναι βασισμένο στις end-to-end ανατροφοδοτήσεις και απαιτεί τον προορισμό για να επιστρέψει ένα ACK στην πηγή για κάθε επιτυχώς λαμβανόμενο πακέτο δεδομένων. Η πηγή παρακολουθεί τον

αριθμό των πρόσφατων απωλειών (ACKs που δεν παραλαμβάνονται από ένα παράθυρο των πρόσφατων πακέτων).

Εάν ο αριθμός πρόσφατων απωλειών παραβιάζει το αποδεκτό κατώτατο όριο (threshold), το πρωτόκολλο καταχωρεί ένα σφάλμα (fault) μεταξύ της πηγής και του προορισμού και αρχίζει μια διχοτομική αναζήτηση στην πορεία, προκειμένου να προσδιοριστεί η ελαττωματική σύνδεση. Η πηγή ελέγχει την αναζήτηση με τη διευκρίνιση ενός καταλόγου ενδιάμεσων κόμβων στα μελλοντικά πακέτα δεδομένων. Τα προσδιοριστικά αυτών των κόμβων κρυπτογραφούνται με βάση την onion τεχνική. Κάθε κόμβος στον κατάλογο, εκτός από τον προορισμό, πρέπει να στείλει ένα ACK για το πακέτο. Αυτοί οι κόμβοι καλούνται probed κόμβοι. Ο κατάλογος ελέγχων καθορίζει ένα σύνολο μη-επικαλυπτόμενων διαστημάτων (non-overlapping intervals) που καλύπτουν ολόκληρη την πορεία, όπου κάθε διάστημα καλύπτει το subpath μεταξύ των δύο διαδοχικών ελέγχων που διαμορφώνουν τα σημεία τέλους του (endpoints).

Όταν ένα ελάττωμα ανιχνεύεται σε ένα διάστημα, το διάστημα διαιρείται σε δύο με την παρεμβολή ενός νέου ελέγχου. Αυτός ο νέος έλεγχος προστίθεται στον κατάλογο ελέγχων που επισυνάπτονται στα μελλοντικά πακέτα δεδομένων.



Εικόνα 52. Παράδειγμα βασικής έρευνας (probing)

Η διαδικασία της υποδιαίρεσης συνεχίζεται έως ότου ανιχνεύεται ένα ελάττωμα σε ένα διάστημα που αντιστοιχεί σε μια ενιαία σύνδεση, όπως φαίνεται στην Εικόνα 52. Σε αυτό το παράδειγμα, ο κόμβος I2 υποτίθεται ότι ήταν ένας εγωιστικός κόμβος που ρίχνει όλα τα πακέτα, συμπεριλαμβανομένων εκείνων που περιέχουν την εξέταση. Υποτίθεται επίσης ότι δεν υπάρχουν απαντήσεις (replies) στην εξέταση των εντολών. Όπως διευκρινίζεται, ο I2 θα ανιχνευθεί μετά από τέσσερις ελέγχους (όταν οι προηγούμενες υποθέσεις έχουν καταχωρηθεί). Το

σημαντικότερο μειονέκτημα αυτής της λύσης είναι ότι ένας κόμβος απρεπούς συμπεριφοράς, μπορεί εύκολα να πραγματοποιήσει μια εξέταση όταν προωθείται, πρέπει μόνο να αναλύσει τα πακέτα που λαμβάνει πριν τα ρίξει και επομένως μπορεί να παρακάμψει την εξέταση. Στα πλαίσια του προηγούμενου παραδείγματος, ο κόμβος I2 θα μπορούσε να διαβιβάσει τα πακέτα, συμπεριλαμβανομένων των πακέτων εξέτασης και απάντησης, στην εξέταση που εστάλη σε αυτόν. Με αυτόν τρόπο καμία αποτυχία έρευνας δε θα λάβει χώρα και γι' αυτό αυτή η έρευνα δε θα είναι σε θέση να ανιχνεύσει τον εγωιστικό κόμβο στην προκειμένη περίπτωση.

Μια πιο ενισχυμένη λύση έχει προταθεί από τον Kargl και άλλους. Αυτή η λύση χρησιμοποιεί την επαναληπτική εξέταση (iterative probing), η οποία διαφέρει από την προηγούμενη λύση στο γεγονός ότι κάθε εντολή απευθύνεται σε έναν κόμβο αντί ενός συνόλου κόμβων, επομένως η εντολή περιέχει μια κρυπτογραφημένη ταυτότητα κόμβων που προστίθεται σε έναν πρόσθετο τομέα στα πακέτα δεδομένων. Εάν ένα πακέτο δεδομένων δεν περιλαμβάνει καμία εντολή έρευνας, ο τομέας θα περιέχει έναν τυχαίο αριθμό, έτσι ώστε ένας παραλήπτης να μην μπορεί να διακρίνει τα πακέτα δεδομένων, συμπεριλαμβανομένης της εξέτασης από τα κανονικά πακέτα δεδομένων, εκτός αν είναι ο προορισμός της εντολής έρευνας. Αυτή η λύση είναι επίσης αναξιόπιστη, δεδομένου ότι καθιστά πιθανή την ανίχνευση της σύνδεσης που περιέχει τον εγωιστικό (ή κακόβουλο) κόμβο, αλλά δεν μπορεί να διακρίνει ποιος από τους δύο κόμβους που διαμορφώνουν τη σύνδεση είναι πραγματικά εκείνος με την κακή συμπεριφορά, δεδομένου ότι δεν υπάρχει καμία γνώση της εγωιστικής συμπεριφοράς κόμβων επάνω στην υποδοχή μιας έρευνας (είτε στέλνει το ACK είτε όχι). Στο προηγούμενο παράδειγμα, η επαναληπτική εξέταση ανιχνεύει τη σύνδεση (I1, I2) αλλά δεν μπορεί να ανιχνεύσει την κατάλληλη απρεπή συμπεριφορά.

Για να μετριάσουν αυτό το πρόβλημα ο Kargl και οι λοιποί πρότειναν τη σαφή εξέταση (unambiguous probing). Η αρχή αυτού του μηχανισμού είναι απλή και μπορεί να συνοψιστεί ως εξής. Μετά από μια επαναληπτική εξέταση, θα ανιχνευθεί μια σύνδεση (*Ii*, *Ii*+1). Για να καθορίσει ποιος από τους δύο ύποπτους κόμβους είναι ο ένοχος (αυτός με την απρεπή συμπεριφορά) κόμβος, ο κόμβος πηγής ζητά από τον κόμβο *Ii*–1 να ελέγξει εάν μπορεί αδιάκριτα (promiscuously) να κρυφακούσει την αποστολή του *Ii*. Σε αυτή την περίπτωση, ο *Ii*+1 είναι ο ένοχος κόμβος, διαφορετικά ο ένοχος κόμβος είναι ο *Ii*. Σκεφτόμαστε ότι αυτός ο μηχανισμός (unambiguous probing) υποφέρει από τα προβλήματα του φύλακα (watchdog), δεδομένου ότι

στηρίζεται στον αυθαίρετο (promiscuous) έλεγχο του προκάτοχου (predecessor) της ύποπτης σύνδεσης.

8.5 ΠΡΟΛΗΠΤΙΚΕΣ ΛΥΣΕΙΣ ΕΝΑΝΤΙΑ ΣΤΟΝ ΕΓΩΙΣΜΟ (SELFISHNESS) ΤΗΣ ΠΡΟΩΘΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Ως εδώ, έχουμε παρουσιάσει τις ανιχνεύσιμες λύσεις που στοχεύουν στην ανίχνευση του εγωιστικού misbehavior (ή της επίθεσης) στη διαβίβαση του πακέτου όταν εμφανίζεται στο δίκτυο. Μια άλλη προσέγγιση είναι να προσπαθήσει προενεργά (proactively) να αποφύγει αυτή την απρεπή συμπεριφορά, είτε με τη δραστηριοποίηση των κόμβων για συνεργασία είτε με τη λήψη των μέτρων για να αποτραπούν τα πακέτα από τη μείωση πριν σταλούν σε αυτούς. Στα εξής τμήματα συζητάμε δύο λύσεις που ταξινομούμε ως προληπτικές.

8.5.1 Nuglets

Στα πλαίσια του προγράμματος Terminodes, οι Buttyan και Hubaux έχουν προτείνει μια προσέγγιση βασισμένη στην οικονομία που υποκινεί τους κόμβους σε συνεργασία. Έχουν διαμορφώσει και έχουν αναλύσει αυτήν την προσέγγιση στην περαιτέρω εργασία τους. Οι συντάκτες έχουν εισαγάγει αυτό που καλούν εικονική συναλλαγή (virtual currency) ή nuglets, μαζί με τους μηχανισμούς για την πληρωμή/αμοιβή των υπηρεσιών χρήσης/παροχής. Η κύρια ιδέα αυτής της τεχνικής είναι ότι οι κόμβοι που χρησιμοποιούν μια υπηρεσία πρέπει να πληρώσουν για αυτήν (στα nuglets) στους κόμβους που παρέχουν την υπηρεσία. Αυτό καθιστά τα nuglets αναπόφευκτα για τη χρησιμοποίηση του δικτύου και παρακινεί κάθε κόμβο να αυξήσει το απόθεμα των nuglets του με την παροχή των υπηρεσιών σε άλλους κόμβους. Εκτός από την υποκίνηση για την παροχή υπηρεσιών, αυτός ο μηχανισμός μπορεί επίσης να αναγκάσει τους κόμβους να κάνουν μέτρια χρήση των υπηρεσιών δικτύου που χρεώνουν. Αυτή η προσέγγιση είναι μια γενική πρόταση που μπορεί να εφαρμοστεί σε οποιαδήποτε υπηρεσία. Οι συντάκτες το εφάρμοσαν στην υπηρεσία διαβίβασης.

Η πρώτη ερώτηση πίσω από αυτήν την πρόταση που πρέπει να απαντηθεί είναι το πώς να αντιπροσωπεύονται τα nuglets. Οι συντάκτες τους προτείνουν με την παρουσίασή τους από μετρητές στους κόμβους. Κάθε κόμβος έχει έναν μετρητή nuglet η αξία του οποίου αντιστοιχεί στον πλούτο του κόμβου. Εν τούτοις,

προκειμένου να αποτραπεί ο κόμβος από την παράνομη αύξηση του μετρητή του, ο μετρητής πρέπει να διατηρηθεί από μια εμπιστευμένη και ανθεκτική στην πλαστογράφηση ενότητα ασφάλειας υλικού σε κάθε κόμβο, στον οποίο στηρίζεται η ευρωστία αυτής της λύσης. Αυτό περιπλέκει την εφαρμογή και μπορεί να παρουσιάσει ένα μειονέκτημα.

Σε αυτήν την λύση, εάν ένας κόμβος συμπεριφερθεί εγωιστικά, δεν μπορεί να κερδίσει τα nuglets και θα είναι ανίκανο να στείλει τα πακέτα του. Επιπλέον, αυτή η λύση επιτρέπει την εξαγορά του κόμβου, δεδομένου ότι ένας κόμβος που είναι ανίκανος να στείλει το πακέτο του επειδή ξεμένει από nuglets, δεν αποκλείεται από το να κληθεί να συμμετέχει στην υπηρεσία προώθησης δεδομένων, ως εκ τούτου, μπορεί πάντα να διαβιβάσει τα πακέτα και να κερδίσει τα nuglets. Εντούτοις, ένα σημαντικό μειονέκτημα αυτής της προσέγγισης είναι ότι ένας καλά-συμπεριφερόμενος κόμβος που δεν καλείται να καθοδηγήσει αρκετά πακέτα, λόγω της θέσης του ή/και των επικοινωνιών των γειτόνων του, δεν θα μπορούσε να κερδίσει τα nuglets και θα είναι ανίκανος να στείλει τα πακέτα του.

8.5.2 Διασκορπισμός Δεδομένων (Data Dispersal)

Αυτή η προσέγγιση είναι βασισμένη στον αλγόριθμο Rabin, ο οποίος εκμεταλλεύεται την ύπαρξη των πολλαπλών διαδρομών από μια πηγή σε έναν προορισμό για να αυξήσει την αξιοπιστία κατά τη διαβίβαση των πακέτων.

Αποτελείται από την προσθήκη του πλεονασμού στο μήνυμα που στέλνει, κατόπιν το μήνυμα και ο πλεονασμός κωδικοποιούνται και διαιρούνται σε διάφορα κομμάτια και διασκορπίζονται στις διαθέσιμες διαδρομές, έτσι ώστε ακόμη και μια μερική υποδοχή να μπορεί να οδηγήσει στην επιτυχή αναδημιουργία του μηνύματος στο δέκτη. Σημειώστε ότι που κόμβος που χωρίζει (node-disjoint) διαδρομές, εξασφαλίζει περισσότερη αποδοτικότητα, δεδομένου ότι κάθε κόμβος που συμπεριφέρεται απρεπώς επηρεάζει μια μονή διαδρομή κατά τη χρησιμοποίηση αυτών των τύπων διαδρομών. Αυτή η τεχνική μπορεί να μετριάσει τη μερική απώλεια πακέτων που μπορεί να εμφανιστεί λόγω της απρεπούς συμπεριφοράς σε μερικές χρησιμοποιημένες διαδρομές, δεδομένου ότι η κωδικοποίηση και η διασπορά επιτρέπουν την αναδημιουργία του αρχικού μηνύματος με την επιτυχή υποδοχή οποιουδήποτε M διάφορου του N προωθούμενων κομματιών.

Η αναλογία N/M, ή παράγοντας πλεονασμού (redundancy factor), είναι μια κρίσιμη παράμετρος για αυτήν την λύση. Η αύξηση αυτής της αναλογίας εξασφαλίζει περισσότερη αξιοπιστία, δεδομένου ότι θα απαιτούνταν λιγότεροι αριθμοί κομματιών μεταξύ των γενικών σταλμένων κομματιών για να αναδημιουργήσουν το B, αλλά αυτή η επιλογή προκαλεί ένα σημαντικό πλεονασμό. Αφενός, η μείωση του παράγοντα πλεονασμού μειώνει τον πλεονασμό, αλλά παρέχει τη λιγότερη αξιοπιστία. Ως εκ τούτου, η επιλογή αυτής της παραμέτρου είναι ένα προκλητικό ζήτημα και πρέπει να βρεθεί μια μέση λύση μεταξύ της αξιοπιστίας και του πλεονασμού. Ακόμα κι αν αυτός ο μηχανισμός δεν αποτρέπει τους κόμβους από την απρεπή συμπεριφορά και δεν παρακινεί τους κόμβους για να συνεργαστεί, αντίθετα από την προηγούμενη προσέγγιση, σκεφτόμαστε ότι είναι χρήσιμος και μπορεί να μειώσει την εγωιστική απρεπή συμπεριφορά και τα αποτελέσματα των επιθέσεων στην αξιοπιστία επικοινωνίας και μπορεί να συνδυαστεί με μια αντιδραστική λύση.

Οι Papadimitratos και J. To Hass έχουν προτείνει το SMTP, μια λύση που χρησιμοποιεί αυτόν τον μηχανισμό. Αλλά αυτή η λύση έχει τα μειονεκτήματα της τεχνικής end-to-end ανατροφοδότησης που περιγράφηκε πιο πάνω, δεδομένου ότι στηρίζεται σε αυτήν. Ο πίνακας 5 συνοψίζει τα κύρια χαρακτηριστικά γνωρίσματα και τα μειονεκτήματα όλων των ανιχνεύσεων και των προληπτικών λύσεων που παρουσιάστηκαν σε αυτό το τμήμα.

Solutions	Class	Features	Drawbacks
End-to-end feedbacks	Detective	The destination sends back ACKs to the source Detects routes that include misbehaving	Does not detect the appropriate node Important overhead
Watchdog	Detective	Promiscuous mode usage Detects misbehaving in many cases No overhead when there is no misbehaving	Fails to detect the misbehaving in the following cases: • after a collusion • cooperated misbehavior • when the monitored control its transmission power Causes faults detection when using adaptable transmission powers
Activity-based overhearing	Detective	Generalization of the watchdog Provides more traffic to monitor More efficiency when the watchdog is operational	Watchdog's drawbacks
Mutually according admission	Detective	Nodes in neighborhood accord to each other participation admission Uses threshold cryptography	Unfairly excludes nodes with less than the predefined threshold (K) from the service Watchdog's drawbacks
CORE	Detective	Based on reputation Only positive impressions are propagated	No propagation of misbehaving detection Watchdog's drawbacks
CONFIDANT	Detective	Based on reputation Built on negative impression	Watchdog's drawbacks
Dichotomic probing	Detective	Incorporates commands into data packets Requires end-to-end feedback employment Uses onion encryption	Temperable
Iterative probing	Detective	Incorporates commands into data packets Requires end-to-end feedback employment Uses asymmetric encryption Detects the link containing the misbehaving node	Fails to detect the appropriate misbehavior
Unambiguous probing	Detective	Iterative probing + watchdog employment on the detected link upstream node	Watchdog's drawbacks
Nuglets	Preventive	Economic-based approach Nodes that use the service pay nodes that offer it Motivates nodes to cooperate Forces nodes to make moderate usage of the service Allows nodes' redemption	Unfairly prevent nodes not asked to forward packets from sending their own packets
Data dispersal	Preventive	Based on Rabin's algorithm Requires multi-path routing Reduces the misbehaving effects and increases the reliability	Does neither detect nor prevent nodes misbehavior

Πίνακας 5. Λύσεις για την ασφάλεια της προώθησης δεδομένων

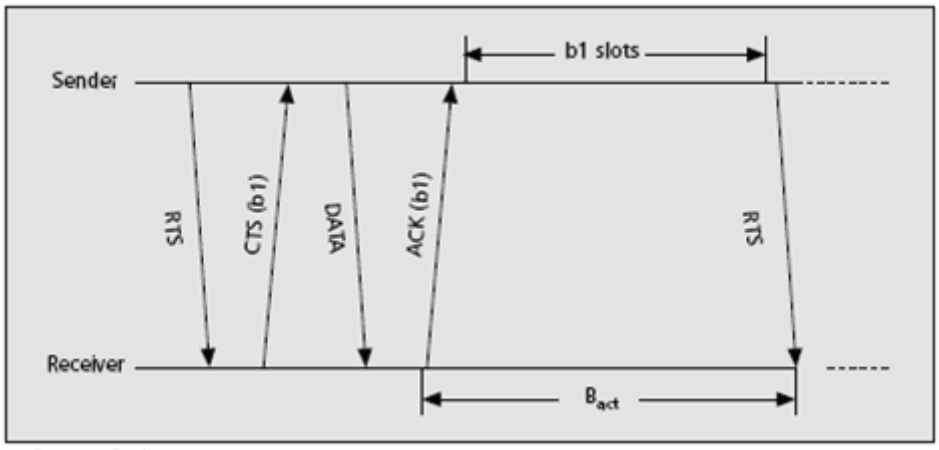
8.6 Η ΛΥΣΗ ΠΟΥ ΑΦΟΡΑ ΤΟ ΠΡΩΤΟΚΟΛΛΟ MAC

Λόγω της τυχαίας επιλογής του back off, είναι δύσκολο να γίνει διάκριση μεταξύ της νόμιμης επιλογής των μικρών τιμών back off και μιας απρεπούς συμπεριφοράς. Ως εκ τούτου, η ανίχνευση μιας απρεπούς συμπεριφοράς στρώματος του MAC είναι ένα περίπλοκο πρόβλημα. Οι Kyasanur και Vaidya έχουν προτείνει ένα σχέδιο για να επιλυθεί αυτό το πρόβλημα.

Το σχέδιο αποτελείται από τις τροποποιήσεις στο IEEE 802.11 πρωτόκολλο που επιτρέπει σε έναν δέκτη να προσδιορίσει την απρεπή συμπεριφορά αποστολέων μέσα σε ένα μικρό διάστημα παρατήρησης. Αντί του αποστολέα, ο δέκτης επιλέγει μια τυχαία back off τιμή b1 και την επισυνάπτει στο CTS και στα πακέτα ack που

διαβιβάζει στον αποστολέα. Ο αποστολέας χρησιμοποιεί αυτή την back off τιμή στην επόμενη μετάδοση στο δέκτη. Αυτή η ανταλλαγή συνοψίζεται στο Εικόνα 47.

Με αυτές τις τροποποιήσεις, ένας δέκτης μπορεί να προσδιορίσει τους αποστολείς που παρεκκλίνουν από το πρωτόκολλο με την παρατήρηση του αριθμού των ανενεργών σχισμών (idle slots) μεταξύ των διαδοχικών μεταδόσεων από τον αποστολέα (B_{act} στην Εικόνα 53). Εάν αυτός ο παρατηρηθείς αριθμός των idle slots είναι λιγότερος από ορισμένο back off, το όργανο ελέγχου συνειδητοποιεί ότι ο αποστολέας μπορεί να είχε παρεκκλίνει από το πρωτόκολλο. Το μέγεθος των παρατηρηθέντων αποκλίσεων πέρα από έναν μικρό αριθμό λαμβανόμενων πακέτων, χρησιμοποιείται για να εντοπίσει την απρεπή συμπεριφορά αποστολέων με υψηλή πιθανότητα. Το προτεινόμενο σχέδιο προσπαθεί επίσης να αρνηθεί οποιοδήποτε πλεονέκτημα απόδοσης που μπορούν να λάβουν οι κόμβοι απρεπούς συμπεριφοράς. Για να το επιτύχουν αυτό και να αποθαρρύνουν την απρεπή συμπεριφορά, οι παρεκκλίνοντες αποστολείς είναι τιμωρημένοι, δηλ., όταν αντιλαμβάνεται ο δέκτης ότι ένας αποστολέας έχει περιμένει λιγότερο από ορισμένο back off, προσθέτει μια ποινική ρήτρα στο επόμενο back off εκείνου του αποστολέα.



Εικόνα 53. Αλληλεπίδραση αποστολέα και παραλήπτη

9 ΠΡΟΤΑΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ AD-HOC ΔΙΚΤΥΩΣΗΣ

9.1 DDM

Το πρωτόκολλο δυναμικής πολλαπλής διανομής προορισμού (DDM Dynamic Destination Multicast) είναι ένα πρωτόκολλο πολλαπλής διανομής που είναι σχετικά διαφορετικό από πολλά άλλα ad-hoc πρωτόκολλα βασισμένα σε πολλαπλή διανομή. Στα DDM η ομάδα μέλους δεν είναι περιορισμένη με έναν διανεμημένο τρόπο, δεδομένου ότι μόνο στον αποστολέα των δεδομένων δίνεται η εξουσιοδότηση στον έλεγχο στον οποίο οι πληροφορίες πραγματικά παραδίδονται. Κατά αυτόν τον τρόπο οι κόμβοι DDM γνωρίζουν την ομάδα μέλους των κόμβων με την επιθεώρηση των επικεφαλίδων του πρωτοκόλλου.

Η DDM προσέγγιση αποτρέπει επίσης τους ξένους κόμβους από το να προσχωρήσουν αυθαίρετα στις ομάδες. Αυτό δεν υποστηρίζεται άμεσα σε πολλά άλλα πρωτόκολλα. Εάν η ομάδα μέλους και η διανομή των δεδομένων της πηγής πρέπει να περιοριστούν, πρέπει να εφαρμοστούν τα εξωτερικά μέσα όπως η διανομή των κλειδιών.

Το DDM έχει δύο τρόπους λειτουργίας: τον stateless mode και τον soft-state mode. Στον stateless mode η συντήρηση των πολλαπλών συνδέσεων και ο περιορισμός της ομάδας μέλους, αντιμετωπίζονται συνολικά με την κωδικοποίηση των πληροφοριών αποστολής σε μια πρόσθετη επικεφαλίδα των πακέτων δεδομένων. Οι κόμβοι δεν είναι απαραίτητο να αποθηκεύσουν τις πληροφορίες κατάστασης. Αυτό το είδος αντιδραστικής προσέγγισης εγγυάται ότι δεν υπάρχει καμία μάταιη ανταλλαγή των στοιχείων ελέγχου κατά τη διάρκεια των ανενεργών περιόδων. Κατά συνέπεια στα μικρά ad-hoc δίκτυα που δεν χρειάζονται ουσιαστική κλιμάκωση, αυτό το είδος της αρκετά αντιδραστικής προσέγγισης μπορεί να είναι εξαιρετικά χρήσιμο. Ο soft-state mode, αφενός, απαιτεί ότι οι κόμβοι θυμούνται τα επόμενα hops κάθε προορισμού και δεν χρειάζεται να γεμίζουν τις επικεφαλίδες του πρωτοκόλλου με κάθε προορισμό. Και στους δύο τρόπους, οι κόμβοι πρέπει πάντα να είναι σε θέση να παρακολουθήσουν την ομάδα των μελών. Σύμφωνα με τους συντάκτες, το DDM είναι καταλληλότερο για τα δυναμικά δίκτυα που έχουν μικρές πολλαπλές ομάδες. Εν τούτοις, αυτήν την περίοδο το σχέδιο DDM , δεν προτείνει οποιεσδήποτε λύσεις για την εξασφάλιση των δικτύων DDM υπό αυτήν τη μορφή. Επιπλέον, δεν παρέχει

κάποιες προτάσεις για ένα συγκεκριμένο πρωτόκολλο που χειρίζεται τον απαραίτητο έλεγχο πρόσβασης που απαιτείται στον περιορισμό της ομάδας μέλους.

9.2 OLSR

Το Βελτιστοποιημένο πρωτόκολλο κρατικής δρομολόγησης συνδέσεων (OLSR Optimized Link State Routing protocol), είναι ένα δυναμικό και table driven πρωτόκολλο που εφαρμόζει μια πολυ-τοποθετημένη στη σειρά (multi-tiered) προσέγγιση με τους MPR (multi-point relays). Οι MPRs επιτρέπουν στο δίκτυο να εφαρμόσουν πλημμύρα, αντί της πλήρους πλημμύρας node-to-node, με την οποία το ποσό των ανταλλαγμένων δεδομένων ελέγχου μπορεί ουσιαστικά να ελαχιστοποιηθεί. Αυτό επιτυγχάνεται με τη διάδοση των πληροφοριών κατάστασης συνδέσεων μόνο για τους επιλεγμένους MPR κόμβους.

Δεδομένου ότι η MPR προσέγγιση είναι η καταλληλότερη για τα μεγάλα και πυκνά ad-hoc δίκτυα, στα οποία η κυκλοφορία είναι τυχαία και σποραδική, επίσης το πρωτόκολλο OLSR λειτουργεί καλύτερα υπό αυτήν τη μορφή σε αυτό το είδος περιβαλλόντων. Τα MPRs επιλέγονται έτσι ώστε μόνο οι κόμβοι με τη συμμετρική (αμφίδρομη) σύνδεση one-hop με έναν άλλο κόμβο μπορούν να παρέχουν τις υπηρεσίες. Κατά συνέπεια στα πολύ δυναμικά δίκτυα όπου υπάρχει συνεχώς ένα ουσιαστικό ποσό ομοιοκατευθυνόμενων συνδέσεων, αυτή η προσέγγιση μπορεί να μην λειτουργήσει κατάλληλα. Το OLSR εργάζεται με έναν συνολικά διανεμημένο τρόπο, π.χ. η MPR προσέγγιση δεν απαιτεί τη χρήση των συγκεντρωμένων πόρων. Η προδιαγραφή πρωτοκόλλου OLSR δεν περιλαμβάνει οποιεσδήποτε πραγματικές προτάσεις για την προτιμημένη αρχιτεκτονική ασφάλειας για να εφαρμοστεί με το πρωτόκολλο. Το πρωτόκολλο είναι, εντούτοις, προσαρμόσιμο στα πρωτόκολλα όπως το πρωτόκολλο ενθυλάκωσης Διαδικτύου MANET (IMEP), δεδομένου ότι έχει ως σκοπό να λειτουργήσει ανεξάρτητα από άλλα πρωτόκολλα.

9.3 ODMRP

Το On-Demand Multicast Routing Protocol (ODMRP) είναι ένα mesh-based multicast πρωτόκολλο δρομολόγησης (ODMRP) για τα ad-hoc δίκτυα. Εφαρμόζει την προσέγγιση πλημμύρας (scoped flooding), στην οποία ένα υποσύνολο κόμβων – μιας ομάδα προώθησης- μπορεί να προωθήσει τα πακέτα. Τα μέλη στις ομάδες προώθησης, χτίζονται και διατηρούνται δυναμικά κατ' απαίτηση. Το πρωτόκολλο δεν

εφαρμόζει τη δρομολόγηση πηγής. Το ODMRP είναι καταλληλότερο για τα MANETs όπου η τοπολογία του δικτύου αλλάζει γρήγορα και οι πόροι περιορίζονται. Το ODMRP υποθέτει αμφίδρομες συνδέσεις, που περιορίζει κάπως την πιθανή περιοχή της εφαρμογής για αυτήν την πρόταση. Το ODMRP μπορεί να μην είναι κατάλληλο για χρήση σε δυναμικά δίκτυα στα οποία οι κόμβοι μπορούν να κινηθούν γρήγορα και απρόβλεπτα και να έχουν ποικίλη δύναμη ραδιομετάδοσης. Πρόσφατα το ODMRP δεν καθορίζει ή δεν εφαρμόζει οποιαδήποτε μέσα ασφάλειας υπό αυτήν τη μορφή, όπως στην υπό εξέλιξη εργασία. Η ομάδας αποστολής ελέγχεται από το ίδιο το πρωτόκολλο.

9.4 AODV AND MAODV

Το Ad Hoc On-Demand Distance-Vector πρωτόκολλο δρομολόγησης (AODV), είναι ένα unicast-based reactive πρωτόκολλο δρομολόγησης για τους κινητούς κόμβους στα ad-hoc δίκτυα. Επιτρέπει τη multi-hop δρομολόγηση και οι κόμβοι στο δίκτυο διατηρούν δυναμικά την τοπολογία μόνο όταν υπάρχει κυκλοφορία. Αυτήν την περίοδο το AODV δεν καθορίζει οποιουσδήποτε μηχανισμούς ασφάλειας.

Οι συντάκτες προσδιορίζουν την ανάγκη της κατοχής κατάλληλων υπηρεσιών εμπιστευτικότητας και ταυτοποίησης μέσα στη δρομολόγηση, αλλά δεν προτείνουν καμία λύση για αυτές. Εν τούτοις το IPSec, αναφέρεται ως μια πιθανή λύση. Το Multicast Ad Hoc On-Demand Distance-Vector πρωτόκολλο δρομολόγησης (MAODV), επεκτείνει το πρωτόκολλο AODV με multi-cast χαρακτηριστικά.

Οι πτυχές ασφάλειας που σημειώνονται αυτήν την περίοδο στο σχέδιο του MAODV είναι παρόμοιες με το AODV πρωτόκολλο.

9.5 TBRPF

Η τοπολογία μετάδοσης βασισμένη στην αντίστροφη πορεία προώθησης (Topology Broadcast based on Reverse-Path Forwarding-TBRPF), είναι ένα καθαρό προενεργές πρωτόκολλο δρομολόγησης κατάστασης-ζεύξης για τα ad-hoc δίκτυα που μπορούν επίσης να εφαρμοστούν ως προενεργές μέρος μιας υβριδικής λύσης. Κάθε ένας από τους κόμβους του δικτύου στο TBRPF μεταφέρει πληροφορίες κατάστασης σε κάθε σύνδεση του δικτύου, αλλά η διάδοση πληροφοριών βελτιστοποιείται με την

εφαρμογή της αντίστροφη πορεία προώθησης αντί των δαπανηρών τεχνικών πλημμύρας ή μετάδοσης.

Το TBRPF λειτουργεί στα IPv4 των ad-hoc δικτύων και μπορεί επίσης να εφαρμοστεί στην ιεραρχική δικτυακή αρχιτεκτονική. Οι συντάκτες της πρότασης αυτής, ωστόσο, δεν προτείνουν κάποιους συγκεκριμένους μηχανισμούς για την ασφάλεια του πρωτοκόλλου. Τέλος, το πρωτόκολλο, ακριβώς όπως σε κάθε άλλο ad-hoc πρωτόκολλο δρομολόγησης δικτύων, μπορεί να προστατευθεί με το IPSec, αλλά αυτή η προσέγγιση δεν είναι επίσημα σε λειτουργία αυτήν την περίοδο μέσα από το TBRPF.

10 ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ ΣΤΑ ΑΣΥΡΜΑΤΑ AD-HOC ΔΙΚΤΥΑ

10.1 ΑΝΑΓΚΗ ΓΙΑ ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ

Η χρήση των ασύρματων συνδέσεων καθιστά ένα ασύρματο ad-hoc δίκτυο τρωτό στις κακόβουλες επιθέσεις, που κυμαίνονται από το παθητικό κρυφάκουσμα (passive eavesdropping) στην ενεργό παρέμβαση (active interference). Ωστόσο στα ενσύρματα δίκτυα ο επιτιθέμενος πρέπει να αποκτήσει πρόσβαση στα φυσικά μέσα π.χ.: καλώδια δικτύων κ.λπ. ή να περάσει μέσω ενός μεγάλου αριθμού firewalls και gateways. Το σενάριο των ασύρματων δικτύων είναι πολύ διαφορετικό, δεν υπάρχουν firewall και gateways, άρα οι επιθέσεις πραγματοποιούνται από όλες τις κατευθύνσεις. Κάθε κόμβος στο ad-hoc δίκτυο πρέπει να προετοιμαστεί για τη σύγκρουση με τον αντίπαλο.

Κάθε κινητός κόμβος στο ad-hoc δίκτυο είναι μια αυτόνομη μονάδα ελεύθερη να κινείται ανεξάρτητα. Αυτό σημαίνει ότι ένας κόμβος με ανεπαρκή φυσική προστασία είναι πάρα πολύ ευαίσθητος στη σύλληψη, την πειρατεία ή στο συμβιβασμό (compromise). Είναι δύσκολο να ανιχνεύσει ένα μοναδικά συμβιβασμένο κόμβο ενός μεγάλου δικτύου, όπου οι επιθέσεις προέρχονται από τους συμβιβασμένους κόμβους είναι πολύ καταστρεπτικότερες και πολύ πιο δύσκολο να ανιχνευθούν. Ως εκ τούτου κάθε κόμβος σε ένα ασύρματο ad-hoc δίκτυο πρέπει να είναι σε θέση να λειτουργεί σε μια κατάσταση όπου να μην εμπιστεύεται καμία ομάδα.

Τα ad-hoc δίκτυα έχουν μια αποκεντρωμένη αρχιτεκτονική και πολλοί ad-hoc αλγόριθμοι δικτύων στηρίζονται στη συνεταιριστική συμμετοχή των μελών των κόμβων. Οι αντίπαλοι μπορούν να εκμεταλλευτούν αυτήν την έλλειψη συγκεντρωμένης απόφασης - κάνοντας την αρχιτεκτονική για να εισάγουν νέους τύπους επιθέσεων που στοχεύουν στο σπάσιμο των συνεταιριστικών αλγορίθμων.

Επιπλέον, η ad-hoc δρομολόγηση παρουσιάζει περισσότερες ευπάθειες από όσο μπορεί κάποιος να φανταστεί, δεδομένου ότι τα περισσότερα πρωτόκολλα δρομολόγησης για τα ad-hoc δίκτυα είναι συνεταιριστικά από τη φύση τους. Ο αντίπαλος που συμβιβάζει έναν ad-hoc κόμβο θα μπορούσε να πετύχει στο ρίξιμο ολόκληρου του δικτύου με τη διάδοση των ψεύτικων πληροφοριών δρομολόγησης και αυτό θα μπορούσε να καταλήξει σε όλους τους κόμβους δίνοντας τα δεδομένα στο συμβιβασμένο κόμβο.

Οι τεχνικές πρόληψης εισβολών όπως η κρυπτογράφηση και η αυθεντικοποίηση μπορούν να μειώσουν τους κινδύνους μιας εισβολής αλλά δεν μπορούν να τους αποβάλουν πλήρως π.χ.: η κρυπτογράφηση και η αυθεντικοποίηση δεν μπορούν να αμυνθούν ενάντια στους συμβιβασμένους κόμβους.

10.2 ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

Σε γενικούς τομείς η «εισβολή» ορίζεται ως «οποιαδήποτε ομάδα ενεργειών που προσπαθούν να συμβιβάσουν την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα των πόρων του δικτύου».

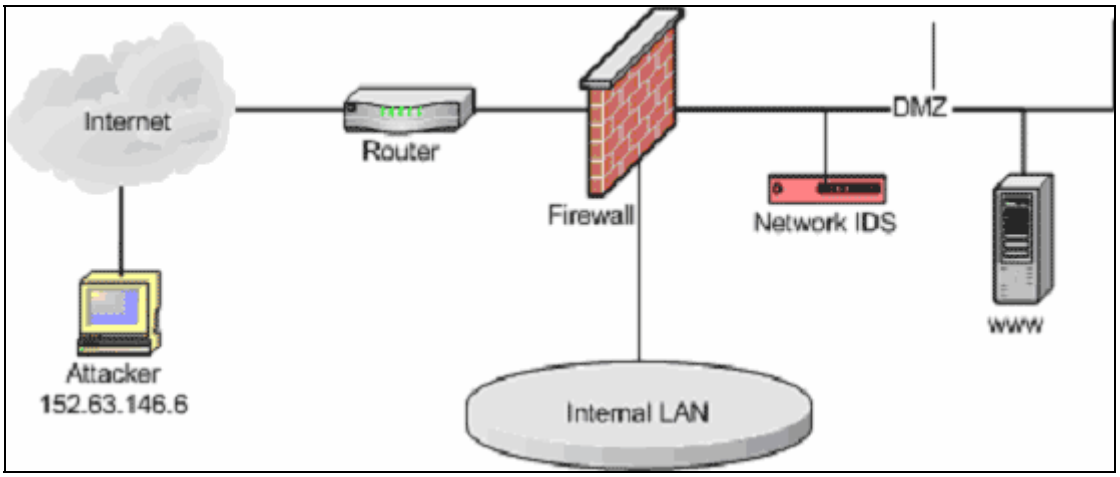
Τα πρωτόκολλα και τα συστήματα που προορίζονται να παρέχουν τις υπηρεσίες μπορούν να είναι ο στόχος των επιθέσεων όπως η διανεμημένη denial of service (DDOS). Η ανίχνευση εισβολής μπορεί να χρησιμοποιηθεί ως δεύτερη γραμμή υπεράσπισης για να προστατεύσει τα συστήματα δικτύων επειδή μόλις ανιχνευθεί μια εισβολή η απάντηση μπορεί να τεθεί σε ισχύ για να ελαχιστοποιήσει τη ζημιά ή να συγκεντρώσει τα στοιχεία για τη συνέχιση ή να προωθήσει τις αντίθετες επιθέσεις.

Η ανίχνευση εισβολής υποθέτει ότι οι «δραστηριότητες χρηστών και προγράμματος είναι αισθητές», που σημαίνει ότι οποιαδήποτε δραστηριότητα που αρχίζει ο χρήστης ή ένα πρόγραμμα εφαρμογής, συνδέεται κάπου με τους πίνακες συστημάτων ή κάποιο είδος συστήματος καταγραφής και τα συστήματα ανίχνευσης εισβολής (IDS) έχουν εύκολη πρόσβαση σε αυτά τα συστήματα καταγραφής. Αυτό το σύστημα καταγραφής σχετικό με τα δεδομένα του χρήστη καλείται δεδομένα ελέγχου (audit data). Κατά συνέπεια, η ανίχνευση εισβολής είναι η σύλληψη όλων των δεδομένων ελέγχου, βάσει του ότι τα δεδομένα ελέγχου καθορίζουν εάν μια σημαντική παρέκκλιση από την κανονική συμπεριφορά του συστήματος κι εάν ισχύει τότε το IDS αναφέρει ότι το σύστημα είναι κάτω από επίθεση. Με βάση τον τύπο των δεδομένων ελέγχου το IDS μπορεί να ταξινομηθεί σε 2 τύπους δηλαδή:

α) Βασισμένο στο δίκτυο (Network based): Το βασισμένο στο δίκτυο IDS κάθεται στην πύλη δικτύων και συλλαμβάνει και εξετάζει τα πακέτα δικτύων που περνούν από τη διεπαφή του υλικού δικτύων.

β) Βασισμένο στον υπολογιστή (Host based): Το βασισμένο στον υπολογιστή IDS στηρίζεται στο λειτουργικό σύστημα των δεδομένων ελέγχου που εξετάζει κι αναλύει τα γεγονότα που παράγονται από τους χρήστες ή τα προγράμματα στον υπολογιστή.

10.3 ΣΥΣΤΗΜΑΤΑ ΑΝΊΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ (IDS)



Εικόνα 54. Σύστημα ανίχνευσης εισβολών (IDS)

Τα συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems-IDS) είναι συστήματα λογισμικού, τα οποία ανιχνεύουν εισβολές σε ένα δίκτυο υπολογιστών με βάση ορισμένα σήματα. Τα ενεργά IDS προσπαθούν να μπλοκάρουν τις επιθέσεις, αποκρίνονται με αντίμετρα ή τουλάχιστον προειδοποιούν τους διαχειριστές, κατά την εξέλιξη της επίθεσης. Τα παθητικά IDS απλώς καταγράφουν την εισβολή ή δημιουργούν ίχνη παρακολούθησης, τα οποία γίνονται εμφανή αφού επιτύχει η επίθεση.

Ενώ τα παθητικά συστήματα μπορούν να θεωρηθούν κάπως άχρηστα στο να αποτρέπουν επιθέσεις, υπάρχουν αρκετές ενδείξεις επιθέσεων, οι οποίες γίνονται εμφανείς μόνο μετά την ολοκλήρωση μιας εισβολής. Για παράδειγμα, αν ένας δυσαρεστημένος διαχειριστής δικτύου του δικτύου υπολογιστών μιας επιχείρησης αποφασίσει να επιτεθεί στην επιχείρηση, θα έχει όλα τα κλειδιά και τους κωδικούς πρόσβασης που είναι αναγκαίοι για να συνδεθεί. Κανένα ενεργό σύστημα δεν θα προειδοποιήσει για αυτήν του την ενέργεια. Τα παθητικά IDS μπορούν όμως να ανιχνεύσουν τις αλλαγές που κάνει ένας διαχειριστής σε συστήματα αρχείων, τις διαγραφές ή όποια άλλη καταστροφή προκαλέσει.

Το σύστημα ανίχνευσης επιθέσεων μιας εταιρείας μεσαίου μεγέθους καταγράφει κατά μέσω όρο εκατοντάδες προσπάθειες αυτοματοποιημένων επιθέσεων κάθε μέρα.

Χρησιμότητα των IDSs

Καθώς οι δικτυακές επιθέσεις έχουν αυξηθεί κατά πολύ τα τελευταία χρόνια τόσο σε πλήθος όσο και σε βαθμό επικινδυνότητας, τα IDSs αποτελούν μία απαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε οργανισμού.

Η Ανίχνευση Επιθέσεων επιτρέπει στους οργανισμούς να προστατέψουν τα συστήματά τους και τις πληροφορίες που βρίσκονται σε αυτά, από κινδύνους που προκύπτουν από την αυξημένη δικτυακή διασύνδεση μεταξύ των συστημάτων τους.

Ισχυρά και Αδύναμα Σημεία των IDSs

Παρόλο που τα IDSs θεωρούνται μία πολύτιμη προσθήκη στην πολιτική ασφάλειας ενός δικτύου, υπάρχουν κάποιες λειτουργίες τις οποίες εκτελούν ικανοποιητικά και άλλες για τις οποίες δεν θεωρούνται επαρκή. Σε καμία περίπτωση δεν πρέπει να ανατίθεται σε ένα IDS να εκτελέσει λειτουργίες, τις οποίες εκτελούν άλλοι τύποι μηχανισμών ασφάλειας, πιο ολοκληρωμένα και πιο αποδοτικά.

Μερικές από τις λειτουργίες που επιτελούνται με επιτυχία από τα IDSs είναι :

- Η παρακολούθηση και η ανάλυση των δραστηριοτήτων σε ένα σύστημα και της συμπεριφοράς των χρηστών.
- Μοντελοποίηση της φυσιολογικής, συνήθους δραστηριότητας ενός συστήματος ή ενός δικτύου και στην συνέχεια παρακολούθηση για διακυμάνσεις και αλλαγές που μπορεί να προκύψουν στη δραστηριότητα αυτή.
- Αναγνώριση των συμβάντων που αντιστοιχούν σε μία γνωστή επίθεση.
- Ειδοποίηση των αρμόδιων υπευθύνων, με το κατάλληλο τρόπο, όταν εντοπιστεί μία επίθεση.
- Επιτρέπουν σε άτομα που δεν θεωρούνται ειδικοί σε θέματα ασφάλειας δικτύων, να εκτελούν σημαντικές λειτουργίες παρακολούθησης του δικτύου για πιθανές επιθέσεις.

Μερικές από τις λειτουργίες που τα IDSs δεν μπορούν να εκτελέσουν ικανοποιητικά είναι:

- Να αναπληρώσουν άλλους, ανύπαρκτους ή κακώς ρυθμισμένους μηχανισμούς ασφάλειας. Τέτοιοι μπορεί να είναι firewalls, μηχανισμοί αυθεντικοποίησης και ταυτοποίησης, μηχανισμοί ελέγχου πρόσβασης,

ανίχνευση και αντιμετώπιση ιών, κρυπτογραφημένη διασύνδεση μεταξύ συστημάτων.

- Άμεσα να ανιχνεύσουν, να ειδοποιήσουν και να αντιδράσουν σε μία επίθεση, σε μεγάλα δίκτυα με πολύ αυξημένο traffic ή σε συστήματα με λίγους ελεύθερους πόρους.
- Να ανιχνεύσουν νέα είδη επιθέσεων ή παραλλαγές παλαιοτέρων.
- Να δράσουν αποτελεσματικά σε επιθέσεις που υλοποιούνται από εξειδικευμένους και έμπειρους επιτιθέμενους και ειδικά στην περίπτωση που αυτοί έχουν αντιληφθεί την ύπαρξή τους και γνωρίζουν τρόπους να τα παρακάμψουν.
- Αυτοματοποιημένα να ερευνήσουν και να αναλύσουν μία επίθεση, χωρίς την ανθρώπινη συμμετοχή.
- Παρουσιάζουν πρόβλημα σε δίκτυα που διασυνδέονται με switches, καθώς αυτά δεν τους επιτρέπουν να έχουν παθητικά πρόσβαση σε όλο το traffic του δικτύου.
- Παρουσιάζουν συμπτώματα από False Positives και False Negatives, ιδιαίτερα στην περίπτωση που δεν έχουν ρυθμιστεί σωστά, και αυτό είναι κάτι που μειώνει την αξιοπιστία τους.

Πρακτική Χρήση των IDSs

Ο τρόπος με τον οποίο ένας οργανισμός θα σχεδιάσει την στρατηγική χρήσης και υλοποίησης IDSs, ώστε να προστατέψει αποτελεσματικά το δίκτυό του και κατ' επέκταση τα συστήματα που συνδέονται σε αυτό και τις πληροφορίες που περιέχουν, έχει άμεση σχέση με την τοπολογία του δικτύου και το είδος της πληροφορίας που πρέπει να διαφυλαχτεί.

Σε κάθε περίπτωση η εφαρμογή IDSs, για να καλύψει με επιτυχία τις ανάγκες για προστασία ενός δικτύου, απαιτεί μελέτη και σχεδιασμό, καθώς και εξειδικευμένο προσωπικό, ώστε να διαχειρίζεται και να επιβλέπει συνεχώς την λειτουργία τους και να δρα αποτελεσματικά και υπεύθυνα στην περίπτωση εμφάνισης μίας επίθεσης.

Στις περισσότερες περιπτώσεις η πιο αποδοτική και προτεινόμενη πρακτική για την πληρέστερη προστασία ενός μεγάλου δικτύου, είναι η χρήση NIDSs και HIDSs σε συνδυασμό μεταξύ τους,.

Σήμερα διατίθενται αρκετά και διάφορα IDSs, υλοποιημένα τόσο σε Hardware ή Software, όσο και με την μορφή εμπορικών ή Open Source εφαρμογών, ενώ η σωστή επιλογή ενός τέτοιου εργαλείου, εξαρτάται από τους στόχους και τις ανάγκες προστασίας κάθε δικτύου.

11 ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα ad-hoc δίκτυα είναι ιδιαίτερα χρήσιμα δίκτυα, εύκολα στην ανάπτυξη και το σχεδιασμό και άμεσα υλοποιήσιμα. Το γεγονός όμως ότι είναι ασύρματα και στερούνται βασικής και σταθερής υποδομής, παρουσιάζουν αρκετές αδυναμίες και είναι ιδιαίτερα τρωτά σε διαφόρων τύπων επιθέσεις.

Λαμβάνοντας υπόψη τις βασικές προδιαγραφές-προϋποθέσεις για την ασφάλεια ενός συστήματος, συμπεραίνουμε εύκολα πως δεν είναι άμεσα εφαρμόσιμες σε ένα δίκτυο τύπου ad-hoc. Επίσης, οι επιθέσεις που πραγματοποιούνται ενάντια σε ένα ad-hoc δίκτυο, εκμεταλλεύονται όλες τις δυνατότητες και υπηρεσίες που προσφέρει, οδηγώντας το δίκτυο σε κατάρρευση.

Μελετώντας την ασφάλεια των πρωτοκόλλων δρομολόγησης των ad-hoc δικτύων, βγάλαμε εύκολα το συμπέρασμα ότι τα on demand πρωτόκολλα δρομολόγησης είναι ακατάλληλα για τα ad-hoc δίκτυα παρόλο που είναι εύκολα προσαρμόσιμα σε τέτοια ασύρματα περιβάλλοντα. Αυτό οφείλεται στο γεγονός ότι τα περιορισμένης δυνατότητας DSR και AODV πρωτόκολλα που παρουσιάστηκαν στην παρούσα διπλωματική εργασία, βασίζονται στην ανεπιφύλακτη συνεργασία των συμμετεχόντων κόμβων του δικτύου συμβάλλοντας έτσι στη δημιουργία ενός αφελούς μοντέλου εμπιστοσύνης το οποίο χάνει σε απόδοση (throughput) και καταναλώνει αρκετή ενέργεια. Το δίκτυο εκτίθεται σε κίνδυνο, συνεπώς, είναι αναγκαία η ανάπτυξη νέων πρωτοκόλλων ή η αναβάθμιση των ήδη υπαρχόντων, που δε θα κοστίζουν σε απόδοση και θα παρέχουν επαρκώς μηχανισμούς άμυνας ενάντια στις κακόβουλες κι ανεπιθύμητες επιθέσεις (π.χ. νέοι αλγόριθμοι στα DSR, τα AODV-Spanning Tree να αντικαταστήσουν τα AODV αφού καλύπτουν τα μειονεκτήματά τους).

Η ακεραιότητα των μηνυμάτων δρομολόγησης είναι ιδιαίτερα σημαντική στα ad-hoc δίκτυα και σε όλους τους τύπους δικτύων γενικότερα. Οι επιθέσεις που περιλαμβάνουν αλλαγή του περιεχομένου των μηνυμάτων, πλαστογράφηση, διαρροή πληροφοριών κλπ. ανιχνεύονται δύσκολα και επιφέρουν σοβαρές συνέπειες στο δίκτυο όπως π.χ. το σπάσιμο μιας ζεύξης, τη μείωση της απόδοσης του συστήματος, την εξάντληση των πόρων ενέργειας του δικτύου, την ολική κατάρρευση κι απενεργοποίηση του δικτύου.

Οι κοινές ανησυχίες στα ad-hoc δίκτυα περιλαμβάνουν τον έλεγχο πρόσβασης. Δεν υπάρχει κατάλληλος μηχανισμός αυθεντικοποίησης ώστε να

απαγορεύεται η πρόσβαση των ξένων κόμβων στο δίκτυο. Επιπλέον, η επικοινωνία μεταξύ των εσωτερικών κόμβων στο δίκτυο δεν προστατεύεται από τις επιθέσεις που αφορούν την εμπιστευτικότητα. Άρα πρέπει να περιληφθεί στο επίπεδο δικτύων ένας μηχανισμός έγκυρης κρυπτογράφησης στην περίπτωση που το επίπεδο ζεύξης δεν υποστηρίζει κρυπτογράφηση.

Το θέμα της κρυπτογράφησης των δεδομένων είναι εξαιρετικά σημαντικό αφού πάνω σε αυτό βασίζεται η εγκυρότητα και η γνησιότητα των μηνυμάτων, ωστόσο δεν αποτρέπει τους κακόβουλους κόμβους από το να προσπαθήσουν να σπάσουν τα κλειδιά αποκρυπτογράφησης. Επειδή προς το παρόν δεν υπάρχει καμία λύση που να αφορά την ανίχνευση των επιθέσεων που στηρίζονται στην κρυπτογράφηση, η ανίχνευση αυτής της επίθεσης είναι ένα ανοικτό ερευνητικό θέμα.

Στα ad-hoc δίκτυα διακυβεύεται η σημαντικότερη απαίτηση ασφάλειας, δηλ. η διαθεσιμότητα του δικτύου. Αφού το δίκτυο στηρίζεται στη συνεργασία των κόμβων, συνεπάγεται ότι η οποιαδήποτε εγωιστική συμπεριφορά οποιουδήποτε κόμβου εκτός του ότι θα στοχεύσει τους πόρους του συστήματος και ιδιαίτερα την ισχύ των μπαταριών που αποτελούν πολύτιμη πηγή, θα σημάνει denial of service. Στα ad-hoc δίκτυα οι κακόβουλοι κόμβοι ενδεχομένως να προσφέρουν μια ανύπαρκτη υπηρεσία multi-hop για να ανακατευθύνουν ανακριβώς την κυκλοφορία και να προκαλέσουν συμφόρηση εάν ο κόμβος επιτρέπεται να έχει πρόσβαση στο δίκτυο. Η επίθεση denial of service βασικά απειλεί τη λειτουργία σε όλους τους τύπους των δικτύων και είναι τυπικά αδύνατον να την αποτρέψουν.

Όσον αφορά το MAC πρωτόκολλο και πάλι στόχος παραμένει η διαθεσιμότητα του δικτύου αφού οι κόμβοι συμπεριφέρονται απρεπώς κι αρνούνται να συνεργαστούν για τον επιτυχή διαμοιρασμό του ασύρματου καναλιού. Αυτό έχει συνέπειες στην απόδοση των κόμβων με καλή συμπεριφορά και γενικότερα σε ολόκληρο το δίκτυο. Η δε λύση που προτείνεται, αφορά τροποποιήσεις στο IEEE 802.11 πρωτόκολλο και από ότι φαίνεται μάλλον αποτελεί σχετικά καλή προσπάθεια αντιμετώπισης των προβλημάτων που αντιμετωπίζει αυτό το πρωτόκολλο.

Αφού ένα δίκτυο στηρίζει την ασφάλειά του στις απαιτήσεις διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση και απάρνηση ενέργειας, χρειάζεται να βρεθούν λύσεις που να στηρίζονται σε αυτές. Συνεπώς, σε θέματα αυθεντικοποίησης και ακεραιότητας, στρεφόμαστε σε λύσεις που αφορούν τροποποίηση των υπαρχόντων πρωτοκόλλων δρομολόγησης και χρησιμοποιούν ψηφιακά πιστοποιητικά των οποίων τα δημόσια κλειδιά είναι γνωστά σε όλους τους

έγκυρους κόμβους ή υψηλό υπολογιστικό κόστος. Αυτό σημαίνει καλή άμυνα απέναντι στις εξωτερικές επιθέσεις αλλά δυστυχώς μόνο σε κάποιες εσωτερικές επιθέσεις όπως spoofing, ανακατεύθυνση με τροποποίηση της ακολουθίας αριθμών της πηγής, rushing attacks και DoS. Εύκολα λοιπόν συμπεραίνουμε πως δεν υπάρχει κατάλληλος ή καλύτερα ιδανικός μηχανισμός ασφάλειας ενάντια σε όλους του τύπους επιθέσεων. Όλες οι προτεινόμενες κι εφαρμοζόμενες λύσεις, καλύπτουν μόνο ορισμένες ανάγκες του δικτύου κι αφήνουν πάντα ανοιχτά θέματα ασφαλούς δικτύωσης, επικοινωνίας και συνεργασίας.

Όλοι οι μηχανισμοί ασφάλειας που εφαρμόζονται στη δικτύωση απαιτούν λίγο πολύ τη χρήση του συστήματος κρυπτογραφίας, η οποία εμπλέκει μια ισχυρή απαίτηση για τον ασφαλή και αποδοτικό μηχανισμό διαχείρισης κλειδιού. Στα ad-hoc δίκτυα δίνεται έμφαση στο ρόλο μιας αξιόπιστης υπηρεσίας διαχείρισης κλειδιού, λαμβάνοντας υπόψη τους περιορισμένους πόρους και τις ενδεχομένως ποικίλες συνθήκες στις οποίες λειτουργούν οι κόμβοι. Οι παραδοσιακές και συγκεντρωμένες προσεγγίσεις δεν μπορούν συχνά να εφαρμοστούν στο περιβάλλον στο οποίο λειτουργούν τα ad-hoc δίκτυα, το οποίο αναγκάζει τη χρήση των διανεμημένων υπηρεσιών που δεν στηρίζονται στους ενιαίους πόρους όσον αφορά άλλους κόμβους ή πορείες επικοινωνίας.

Ωστόσο κάποιες άλλες λύσεις που παρουσιάστηκαν σε αυτή τη διπλωματική εργασία, όπως το ZRP πρωτόκολλο το οποίο αποκρύπτει την τοπολογία του δικτύου, φαίνονται να είναι ίσως οι λιγότερο ευαίσθητες στις επιθέσεις δρομολόγησης. Η αποκάλυψη της τοπολογίας του δικτύου σαφώς κι αποτελεί μειονέκτημα γιατί φανερώνεται η δρομολόγηση των μηνυμάτων και το δίκτυο εκτίθεται σε κίνδυνο από κακόβουλους χρήστες.

Όπως έχει ήδη αναφερθεί, βασικό στοιχείο επιτυχούς δικτύωσης είναι η συνεργασία των κόμβων μεταξύ τους. Αν κάποιος κόμβος παρουσιάσει απρεπή συμπεριφορά τότε οι συνδέσεις του δικτύου παύουν να είναι ασφαλείς και σε μερικές περιπτώσεις υπάρχει περίπτωση διακοπής ή καταστροφής τους. Η τοποθέτηση ενός φύλακα (watchdog) στο δίκτυο, ανιχνεύει τους κόμβους απρεπούς συμπεριφοράς σε πολλές περιπτώσεις και δεν απαιτεί overhead όταν κανένας κόμβος δεν συμπεριφέρεται απρεπώς. Εν τούτοις, παρουσιάζει αδυναμίες στην ανίχνευση των κόμβων με κακή συμπεριφορά σε κάποιες περιπτώσεις, γεγονός που ακόμη μια φορά μαρτυρά την έλλειψη ισχυρής κάλυψης του δικτύου και της εξασφάλισης της ασφαλούς λειτουργίας του.

Η φήμη είναι το ποσό εμπιστοσύνης που εμπνέεται από έναν ιδιαίτερο κόμβο ενός δικτύου σε μια συγκεκριμένη ρύθμιση ή μια περιοχή ενδιαφέροντος. Οι κόμβοι που συμβάλλουν πρόθυμα στην ομαλή λειτουργία του δικτύου, αναπτύσσουν μια καλή φήμη μεταξύ των κόμβων, ενώ άλλοι που αρνούνται να συνεργαστούν, φημίζονται άσχημα και βαθμιαία αποκλείονται από το δίκτυο. Πρόκειται δηλαδή για την εμπιστοσύνη που αναπτύσσουν οι κόμβοι μεταξύ τους. Οι προτεινόμενες λύσεις CORE και CONFIDANT δεν αποτελούν και την καλύτερη επιλογή προστασίας της δρομολόγησης των μηνυμάτων αφού έχουν τα ίδια μειονεκτήματα με την τεχνική του watchdog.

Αν και η λύση της έρευνας (probing) φαίνεται να είναι σχετικά καλός μηχανισμός προστασίας, εν τούτοις αποκαλύπτει ψεγάδια αφού στηρίζεται στον promiscuous τρόπο ελέγχου και συνεπώς υποφέρει από τα προβλήματα του watchdog.

Σε γενικές γραμμές όσες λύσεις στηρίχθηκαν στην εγωιστική συμπεριφορά και στη φήμη των κόμβων, παρουσίασαν κενά και ελλείψεις που καμία περαιτέρω λύση από όσες είδαμε, δεν κάλυψαν. Καταλαβαίνει λοιπόν κανείς, ότι το θέμα της ασφάλειας του ασύρματου ad-hoc δικτύου σε όλα σχεδόν τα επίπεδα του μοντέλου OSI, αποτελεί ανοικτό ερευνητικό θέμα και απαιτεί ιδιαίτερη κι επίμονη ανάλυση αφού το δίκτυο αυτό είναι εξαιρετικά ευέλικτο και ασταθές.

Τα συστήματα ανίχνευσης εισβολών που είδαμε εν τάχει, αποτελούν απαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε οργανισμού. Είναι ικανά να παρακολουθούν ολόκληρο το δίκτυο και να ανιχνεύουν οποιαδήποτε ύπουλη ή επικίνδυνη εισβολή και ενημερώνουν τους αρμόδιους χρήστες. Όμως και πάλι δεν είναι τόσο ικανά ώστε να καλύψουν όλες τις ανάγκες του δικτύου και παρουσιάζουν όπως είναι αναμενόμενο, ανεπάρκειες.

Όπως όλα τα δίκτυα, έτσι και το ασύρματο ad-hoc δίκτυο δέχεται διαφόρων ειδών απειλές με τη διαφορά ότι λόγω της φυσικής του υποδομής, ο αριθμός των επιθέσεων ξεπερνά κατά πολύ αυτόν των ενσύρματων δικτύων. Σαφώς και απαιτεί καλό σχεδιασμό και αρκετά δυνατό μηχανισμό προστασίας, όμως επειδή κάθε λύση προσανατολίζεται σε διαφορετικά χαρακτηριστικά κάθε φορά, δεν υπάρχει ακόμη ξεκάθαρος και σταθερός μηχανισμός ασφάλειας που να καλύπτει αν όχι όλα, τα περισσότερα ευάλωτα σημεία του ad-hoc δικτύου. Επισημαίνεται ακόμη μια φορά ότι το θέμα της ασφαλούς λειτουργίας ενός ad-hoc δικτύου, αποτελεί ανοιχτό ερευνητικό θέμα.

12 ΕΠΙΛΟΓΟΣ

Στην παρούσα διπλωματική εργασία παρουσιάσαμε θέματα ασφάλειας και δείξαμε ότι τα ιδιαίτερα χαρακτηριστικά αυτού του νέου περιβάλλοντος, το κάνουν πιο τρωτό στις επιθέσεις κι ότι οι λύσεις που αναπτύχθηκαν για standard δίκτυα είτε είναι ακατάλληλες είτε δεν είναι άμεσα εφαρμόσιμες γι' αυτό το περιβάλλον. Αντιμετωπίσαμε διάφορα προβλήματα σχετικά με τα διαφορετικά επίπεδα δικτύου.

Για το επίπεδο δικτύων παρουσιάσαμε τους διαφορετικούς τύπους επιθέσεων στη δρομολόγηση των πρωτοκόλλων και έπειτα ταξινομήσαμε και συζητήσαμε τις προτεινόμενες τεχνικές για να μετριάσουμε αυτές τις επιθέσεις. Σχεδόν όλες αυτές οι τεχνικές χρησιμοποιούν την κρυπτογράφηση δημόσιου κλειδιού και γι' αυτό απαιτούν την αρχή πιστοποιητικών (certificate authority) για τη διαχείριση κλειδιού, η οποία είναι μάλλον προβληματική. Έχουμε εξετάσει επίσης τα δεδομένα προώθησης και έχουμε παρουσιάσει τις επιθέσεις κρυφακούσματος, τις επιθέσεις μείωσης πακέτων (dropping) και την εγωιστική απρεπή συμπεριφορά, μαζί με τις ταξινομήσεις και τις συζητήσεις των προτεινόμενων λύσεων. Όπως παρουσιάζεται, οι προληπτικές λύσεις ενάντια στην εγωιστική κακή συμπεριφορά και τη μείωση πακέτων παρακινούν τους κόμβους μόνο να συνεργαστούν ή να αποφύγουν τα πακέτα. Σχεδόν όλες οι λύσεις ανίχνευσης, αφενός, στηρίζονται στην τεχνική φυλάκων (watchdog), η οποία αποτυγχάνει να ανιχνεύσει σωστά τον ένοχο (κακόβουλο ή εγωιστικό) κόμβο σε μερικές περιπτώσεις, ιδιαίτερα κατά την εφαρμογή της τεχνικής ελέγχου δύναμης που χρησιμοποιείται από μερικά πρωτόκολλα δρομολόγησης που προτείνονται στη συνέχεια στον τομέα της βελτιστοποίησης κατανάλωσης ισχύος. Απαιτείται σαφώς μια νέα λύση που στηρίζεται σε μια τεχνική διαφορετική από αυτή του φύλακα για να υπερνικήσει το πρόβλημα.

Όσον αφορά το κρυφάκουσμα, απαιτείται μια λύση ανίχνευσης. Η χρησιμοποίηση της κρυπτογράφησης θα μπορούσε να βοηθήσει στην προστασία της εμπιστευτικότητας των δεδομένων, αλλά είναι ανεπαρκής δεδομένου ότι το σπάσιμο των κλειδιών είναι πάντα δυνατό και η ανάκληση κλειδιού στα MANETs είναι προβληματική. Το κρυφάκουσμα παραμένει μια σοβαρή επίθεση ενάντια στην αποστολή δεδομένων και αντιπροσωπεύει ένα ανοικτό ερευνητικό θέμα για τα MANETs.

Σχετικά με το επίπεδο MAC, παρουσιάσαμε το selfishness στην κακή συμπεριφορά πρόσβασης καναλιών, το οποίο σπάζει τη δικαιοσύνη και έχει επιπτώσεις στην αποδοτικότητα των δικτύων. Η μόνη λύση που προτάθηκε, παρουσιάστηκε και συζητήθηκε. Στη συζήτησή μας επεξηγήσαμε πώς αυτή η λύση μπορεί λανθασμένα να κατηγορήσει τους καλώς συμπεριφερόμενους κόμβους και πώς είναι ανίκανη να ανιχνεύσει αυτό που αποκαλέσαμε συνεταιριστική κακή συμπεριφορά (cooperative misbehavior). Αυτό το πρόβλημα αντιπροσωπεύει επίσης έναν εύφορο τομέα έρευνας.

Όσον αφορά στο επίπεδο εφαρμογής, μελετήσαμε το πρόβλημα διαχείρισης κλειδιού, το οποίο μπορεί επίσης να θεωρηθεί ως ελλοχεύων μηχανισμός για τα χαμηλότερα πρωτόκολλα όπως η δρομολόγηση. Αναλύθηκαν διάφορες λύσεις για την διαχείριση ιδιωτικού και δημόσιου κλειδιού. Δείξαμε ότι είναι μια πρόκληση να παρέχεται μια αποδοτική λύση ιδιωτικού κλειδιού όπου όλοι οι κόμβοι συμμετέχουν στη βασική κατασκευή με ελάχιστο άνω όριο και υπολογισμό. Το πρόβλημα σε αυτόν τον τύπο υποδομής κλειδιού είναι ότι παρέχει την αυθεντική και αποδοτική διανομή κλειδιού. Με τον όρο αυθεντικό εννοούμε ότι όταν ο αιτών ζητά το δημόσιο κλειδί ενός άλλου κόμβου, το πρωτόκολλο πρέπει να εξασφαλίσει ότι παρέχεται το σωστό κλειδί και ότι κανένας αντίπαλος δεν μπορεί επιτυχώς να παρέχει στον αιτούντα ένα πλαστογραφημένο κλειδί.

Τα συστήματα ανίχνευσης εισβολών (IDSs), που είναι ουσιαστικά όταν αποτυγχάνουν τα προληπτικά μέτρα, είναι συστήματα λογισμικού, τα οποία ανιχνεύουν εισβολές σε ένα δίκτυο υπολογιστών με βάση ορισμένα σήματα. Παρόλο που τα IDSs θεωρούνται μία πολύτιμη προσθήκη στην πολιτική ασφάλειας ενός δικτύου, υπάρχουν κάποιες λειτουργίες τις οποίες εκτελούν ικανοποιητικά και άλλες για τις οποίες δεν θεωρούνται επαρκή όπως για παράδειγμα το ότι δεν μπορούν να ερευνήσουν και να αναλύσουν μία επίθεση, χωρίς την ανθρώπινη συμμετοχή ή να ανιχνεύσουν και να αντιδράσουν άμεσα σε μία επίθεση σε μεγάλα δίκτυα με πολύ αυξημένο traffic ή σε συστήματα με λίγους ελεύθερους πόρους.

ΑΝΑΦΟΡΕΣ

1. **A survey of security issues in mobile ad hoc and sensor networks (IEEE Communications-Fourth Quarter 2005, Volume 7, No 4).**
2. **Security in Ad Hoc Networks (Vesa Karpijoki-Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory).**
3. **Security in Ad Hoc Networks (Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla, Anil Garikapati-Computer Science Department, University of Kentucky).**
4. **Security in Ad-Hoc Routing Protocols (Prof. Deshpande Vivek S. Lecturer, Maharashtra Institute Of Technology Women Engineering. Pune, Maharashtra, India).**
5. **A service discovery threat model for ad hoc networks (Adrian Leung, Christian Mitchell-Royal Holloway, University of London).**
6. **Security vulnerabilities in ad hoc networks (Po-Wah Yau, Chris J. Mitchell-Mobile VCE Research group, Royal Holloway, University of London).**
7. **Securing Ad-hoc networks (Lidong Zhou-Department of Computer Science, Zygmunt J. Haas-School of Electrical Engineering- Cornell University).**
8. **Security in Ad Hoc Networks (Vesa Kärpijoki Helsinki University of Technology Telecommunications Software and Multimedia Laboratory).**
9. **A Secure Routing Protocol for Ad Hoc Networks (Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer-Dept. of Computer Science University of California, Santa Barbara, Dept. of Computer Science University of Massachusetts, Amherst, Dept. of Computer Science Georgetown University, Washington DC).**
10. **Tutorial on wireless ad-hoc networks (David Remondo-Dept. Telematics Eng. EPSC, Tech. University of Catalonia, Barcelona-Spain, July 2004).**
11. **A service discovery threat model for ad hoc networks (Adrian Leung and Chris Mitchell Information Security Group Royal Holloway, University of London Egham, Surrey, UK).**

12. **Routing Data Authentication in Wireless Ad Hoc Networks (Mark Torgerson, Cryptography and Information Systems Surety Department-Brian Van Leeuwen ,Networked Systems Survivability and Assurance).**
13. **Ασφάλεια Ασύρματων και κινητών δικτύων επικοινωνιών, ασφάλεια σε αυτόνομα και δευτερογενή περιβάλλοντα Bluetooth, IEEE 802.11, 802.16, UMTS (Γεωργίου Καμπουράκη, Στέφανου Γκρίτζαλη, Σωκράτη Κάτσικα-Εκδόσεις Παπασωτηρίου).**
14. **Ασφάλεια δικτύων (Φωτιαδάκη Παναγιώτα-Τμήμα Μηχανικών Η/Υ και Πληροφορικής Πολυτεχνική Σχόλη Πανεπιστήμιο Πάτρας).**
15. **Χειρισμοί ασφαλείας στα δίκτυα υπολογιστών-Τεχνική διάσταση.**
16. **Σημειώσεις μαθήματος «ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ» Κ. Βασιλάκης Ακαδημαϊκό έτος 2004-2005.**
17. **Μέθοδοι δρομολόγησης σε ασύρματα δίκτυα αυθαίρετης τοπολογίας (Κρομμύδας Ιωάννης-Πανεπιστήμιο Πατρών).**
18. **Ad-Hoc and Sensor Networks: Technology and Applications (Δήμητρα Καμπιτάκη-Πανεπιστήμιο Μακεδονίας)**
    http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2007/Ad-Hoc%20and%20Sensor%20Networks.pdf
19. **Ασύρματα αδόμητα (ad hoc) δίκτυα: Εφαρμογές και ερευνητικά θέματα**
    www.eng.ucy.ac.cy/toumpis/publications/volos.ppt
20. **Προσομοίωση λειτουργίας ασύρματου δικτύου (802.11)**
    www.teiser.gr/icd/ptixiakes_parousiaseis/Kollaras%20Antonis%20(WLAN%20Simulation).ppt
21. **wireless ad-hoc networks**
    xanthippi.ceid.upatras.gr/courses/mobile/Presentations/Lecture3.ppt

ΠΑΡΑΡΤΗΜΑ

☙ ΑΚΡΩΝΥΜΙΑ ❧

- **WLAN (Wireless Local Area Network):** Είναι ασύρματο τοπικό δίκτυο μεταξύ δύο ή περισσότερων computer χωρίς τη χρήση καλωδίων.
- **WPAN (Wireless Personal Area Network):** Είναι ασύρματο τοπικό δίκτυο μεταξύ υπολογιστών για επικοινωνία μεταξύ συσκευών όπως το τηλέφωνο και το PDA, κοντά σε ένα άτομο.
- **WMAN (Wireless Metropolitan Area Network):** Είναι ασύρματο δίκτυο για μία πόλη.
- **WWAN (Wireless Wide Area Network):** Είναι ασύρματο δίκτυο όπου οι υπολογιστές είναι πολύ μακριά ο ένας από τον άλλο.
- **GSM (Global System for Mobile communication):** Είναι ψηφιακό σύστημα κινητής τηλεφωνίας που χρησιμοποιείται ευρέως στην Ευρώπη και σε άλλα μέρη του κόσμου.
- **Symmetric encryption:** Είναι η μετάφραση των δεδομένων σε έναν μυστικό κωδικό. Πρόκειται για κρυπτογράφηση όπου χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος.
- **Assymetric encryption:** Πρόκειται για κρυπτογράφηση που χρησιμοποιεί διαφορετικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος.
- **OSI (Open Systems Interconnection):** Είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για σχεδίαση επικοινωνιών και δικτυακών πρωτοκόλλων για υπολογιστές. Είναι γνωστό και ως Μοντέλο των επτά επιπέδων.
- **MAC (Medium Access Control):** Υποεπίπεδο ελέγχου προσπέλασης μέσου του επιπέδου ζεύξης δεδομένων του OSI μοντέλου
- **IP address:** Είναι η ταυτότητα ενός υπολογιστή ή μιας συσκευής σε ένα TCP/IP δίκτυο.
- **BSS (Basic Service Set):** Είναι εργαλείο για την αρχιτεκτονική IEEE 802.11 WLAN.

- **AP (Access Point):** Είναι hardware συσκευή ή software υπολογιστή, το οποίο χρησιμοποιείται για επικοινωνία χρηστών ασύρματης συσκευής σε ενσύρματο τοπικό δίκτυο.
- **VPN (Virtual Private Network):** Εικονικό ιδιωτικό δίκτυο με χρήση μηχανισμών ασφαλείας.
- **SMTP (Simple Mail Transfer Protocol):** Είναι πρωτόκολλο για αποστολή e-mail μεταξύ των servers.
- **WAP (Wireless Application Protocol):** Πρωτόκολλο για εφαρμογές κινητής τηλεφωνίας
- **WEP (Wired Equivalency Privacy):** Πρωτόκολλο ασφαλείας για δίκτυα 802.11
- **NIC (Network Interface):** Προσαρμογέας ή κάρτα δικτύου
- **False Positive:** Ένα ψευδές θετικό σήμα (false positive) προκύπτει όταν ένα σύστημα εντοπισμού εισβολών αναφέρει μία επίθεση, ενώ στην πραγματικότητα δεν υπάρχει σχετική επίθεση σε εξέλιξη.
- **False Negative:** Τα ψευδώς αρνητικά σήματα (false negative) παράγονται όταν ένα σύστημα ανίχνευσης εισβολών αποτυγχάνει να αναφέρει μια πραγματική επίθεση που βρίσκεται σε εξέλιξη.