ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

&

ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΜΗΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΗΣ ΔΡΟΜΟΛΟΓΗΣΗ ΣΕ ΑΥΤΟΦΥΗ (AD-HOC) ΔΙΚΤΥΑ

ΦΟΙΤΗΤΗΣ

ΜΕΛΕΣΑΝΑΚΗΣ ΓΡΗΓΟΡΙΟΣ

ΕΠΙΒΛΕΠΩΝ

ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

Περιεχόμενα

Περίληψη

Τα τελευταία χρόνια παρατηρείται μία ραγδαία εξάπλωση των ασύρματων τηλεπικοινωνιακών τεχνολογιών. Ένα ad-hoc ασύρματο τηλεπικοινωνιακό δίκτυο κινητών κόμβων έχει την δυνατότητα για ασύρματη μεταφορά δεδομένων και δημιουργείται δυναμικά και αυτόνομα.

Η διαδικασία εύρεσης των διαδρομών που πρέπει να ακολουθήσουν τα δεδομένα για να μεταφερθούν από τον ένα κόμβο στον άλλο ονομάζεται δρομολόγηση και είναι μία από τις ουσιώδεις λειτουργίες που πρέπει να υποστηρίζει ένα δίκτυο. Η δρομολόγηση σε δίκτυα ad-hoc αποτελεί βασικό πεδίο έρευνας επειδή τα υπάρχοντα πρωτόκολλα δρομολόγησης δεν είναι αποδοτικά εξαιτίας των ιδιαίτερων χαρακτηριστικών των δικτύων αυτών. Η ομάδα εργασίας MANET του IETF έχει στόχο την προτυποποίηση ενός αποδοτικού πρωτοκόλλου δρομολόγησης για τα δίκτυα αυτά.

Στην παρούσα εργασία περιγράφουμε τα σημαντικότερα από τα πρωτόκολλα δρομολόγησης που έχουν προταθεί. Μελετούμε διεξοδικά το σημαντικότερο από αυτά, το πρωτόκολλο δυναμικής δρομολόγησης πηγής (Dynamic Source Routing). Ο αλγόριθμος δρομολόγησης αυτού του πρωτοκόλλου είναι απλός και αποδοτικός, σχεδιασμένος ειδικά για χρήση πάνω από ασύρματα δίκτυα ad-hoc πολλαπλών συνδέσεων με κινούμενους κόμβους. Ο αλγόριθμος του DSR επιτρέπει στο δίκτυο να είναι πλήρως αυτόνομο, τόσο στη διαδικασία οργάνωσης, όσο και στη διαδικασία δρομολόγησης, χωρίς να είναι απαραίτητη η παρουσία κάποιας προϋπάρχουσας υποδομής δικτύου ή διαχείρισης δικτύου. Η ανάλυση του συγκεκριμένου πρωτοκόλλου δημιουργεί ερωτηματικά σχετικά με την απόδοσή του. Αν και έχουν ήδη προταθεί πολλοί τρόποι βελτίωσης του πρωτοκόλλου.

Εστιάζουμε στο χρόνο ζωής των διαδρομών διαφορετικού μήκους σε ένα ασύρματο δίκτυο ad-hoc. Επεκτείνουμε τις λειτουργίες της Route Cache, ώστε να μη χρησιμοποιεί μία διαδρομή πέραν του προβλεπόμενου χρόνου ζωής της. Επίσης αναφερόμαστε στη χρήση της παραμέτρου Time-To-Live των αποθηκευμένων διαδρομών δρομολόγησης, που επιτυγχάνει σημαντικές βελτιώσεις.

Τέλος εξετάζουμε το σημαντικό πρόβλημα της αυθεντικοποίησης που αποτελεί τη βάση για την ασφαλή δρομολόγηση των δεδομένων.

1. Ασύρματα ad-hoc Δίκτυα

1. Ασύρματα Τηλεπικοινωνιακά Δίκτυα

Τα τελευταία χρόνια παρατηρείται μια τρομακτική αύξηση του πλήθους των φορητών υπολογιστών και υπολογιστών χειρός η οποία σε συνδυασμό με την σύγχρονη τάση για δημιουργία συστημάτων, μικρότερου μεγέθους, με όλο και μεγαλύτερη υπολογιστική ισχύ, έχει σαν αποτέλεσμα την ανάγκη για δημιουργία νέων εφαρμογών, πρωτοκόλλων, αλγορίθμων και δια-επικοινωνιακών συστημάτων, με σκοπό να καλύψουν τις αυξανόμενες ανάγκες των πολιτών, που χρησιμοποιούν αυτές τις τεχνολογίες. Ταυτόχρονα παρατηρείται μία μεγάλη εξάπλωση των ασύρματων τηλεπικοινωνιακών συστημάτων, τόσο με την ραγδαία εξάπλωση της κινητής τηλεφωνίας, όσο και των άλλων ασύρματων τηλεπικοινωνιακών συστημάτων δεδομένων. Σήμερα οι άνθρωποι χρησιμοποιούν διάφορες τηλεπικοινωνιακές συσκευές, τόσο για τις καθημερινές συνομιλίες και επαφές με άλλους ανθρώπους, όσο και για την ανταλλαγή δεδομένων και πληροφοριών από οποιοδήποτε σημείο και αν βρίσκονται. Στην νέα πραγματικότητα που διαφαίνεται ότι θα φέρουν, λόγω της γρήγορης εξάπλωσης τους, οι ασύρματες φορητές υπολογιστικές συσκευές, έρχεται η επιστήμη των υπολογιστών και συγκεκριμένα ο τομέας των ασύρματων δικτύων να αναπτύξει τα απαραίτητα πρωτόκολλα, συστήματα επικοινωνιών, για να μπορέσει να ικανοποιήσει τις ανάγκες των χρηστών, για εύκολη και άνετη πρόσβαση σε κάθε είδους υπηρεσίες και πληροφορίες μέσω αυτών των τεχνολογιών.

Στην νέα αυτή πραγματικότητα, στην οποία κατευθυνόμαστε, βασικό ρόλο θα έρθουν να παίξουν οι νέες υπηρεσίες για τις νέες κατηγορίες χρηστών που θα χρησιμοποιούν τους υπολογιστές και τις υπηρεσίες από οποιοδήποτε σημείο και αν βρίσκονται. Η βασική τους ανάγκη όμως θα παραμείνει η ίδια και αυτή δεν είναι άλλη από την καθολική και εύκολη πρόσβαση στον παγκόσμιο δικτυακό ιστό. Οι χρήστες απαιτούν, και δίκαια από κάθε άποψη, η έλευση των νέων τεχνολογιών να μπορέσει να τους εξασφαλίσει αυτό που σήμερα έχουν, καθολική πρόσβαση σε υπηρεσίες τόσο για προσωπική όσο και για επαγγελματική χρήση, διευκολύνοντας τον τρόπο που γίνεται αυτό, με την μικρότερη δυνατή καθυστέρηση και κόστος και την μεγαλύτερη δυνατή ευκολία και ευελιξία. Σήμερα αυτό είναι δυνατόν αφού υπάρχουν ασύρματες τεχνολογίες, που μπορούν να επιτρέψουν την γρήγορη, ικανοποιητική και χωρίς μεγάλο κόστος επικοινωνία, καθώς και συσκευές που έρχονται να ικανοποιήσουν τις ανάγκες των χρηστών. Στο μέλλον πιστεύεται ότι όλοι οι πολίτες θα έχουν αυτού του τύπου τις επικοινωνίες δεδομένες.

Σήμερα παρατηρούμε μία έξαρση στην ανάπτυξη και δημιουργία τεχνολογικών λύσεων για να μπορέσουν να υποστηρίξουν την ασύρματη επικοινωνία μεταξύ υπολογιστικών συστημάτων. Οι υπολογιστές αναπτύσσονται όλο και περισσότερο αποκτώντας όλο και περισσότερες δυνατότητες και παράλληλα το λογισμικό εξελίσσεται γοργά για να μπορέσει να υποστηρίξει τις νέες υπηρεσίες και τεχνολογίες. Στην παγκόσμια αγορά καθημερινά εμφανίζονται όλο και περισσότερα προϊόντα προς αυτή την κατεύθυνση από ότι στο παρελθόν. Σε αυτό έχει συμβάλει, τα τελευταία χρόνια, η αύξηση του εύρους των ασύρματων καναλιών, που είναι μεγαλύτερο από δέκα έως εκατό φορές, από αυτό που είχαμε

στη διάθεση μας μερικά χρόνια πριν. Τα παραπάνω, σε συνδυασμό με την εξέλιξη στην ευκολία με την οποία ο οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση στον παγκόσμιο δικτυακό ιστό, έχουν σαν αποτέλεσμα να θεωρούνται δεδομένες όλο και περισσότερες από τις βασικές λειτουργίες ενός δικτύου, πράγμα το οποίο δημιουργεί προκλήσεις σε μία ανερχόμενη τεχνολογία, αφού πέρα από τα προβλήματα που έχει να λύσει, πρέπει να φροντίσει να υποστηρίζει και το σύνολο των λειτουργιών που οι χρήστες σήμερα θεωρούν δεδομένες.

2. Πρωτόκολλα Επικοινωνίας

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, UWBWLAN: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g WMAN: IEEE 802.16e

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.

	Ταχύτητα (Mbps)	Εμβέλεια	Συχνότητα	Διασύνδεση	Κατάσταση	Υποστ.
Bluetooth	**1 Mbps**	**10 m**	**2.4 GHz**	**Καμία**	**Διαθέσιμο**	**Erricson IBM Intel Toshiba Nokia Motorola**
HomeRF	**2 Mbps**	**50 m**	**2.4 GHz**	**Ethernet**	**Διαθέσιμο**	**Promix Intel, HP 3COM Motorola**
HiperLAN Type 1	**24 Mbps**	**50m**	**5 GHz**	**Ethernet ATM, IP**	**Διαθέσιμο**	**ETSI Promix HP, IBM Xircom Nokia**
HiperLAN Type 2	**54 Mbps**	**<150 m**	**5 GHz**	**Ethernet ATM, IP UMTS Firewire PPP**		**ETSI Promix HP, IBM Xircom Nokia Erricson Dell, TI**
IEEE 802.11	**2 Mbps**	**100m-2Km**	**2.4 GHz**	**Ethernet**	**Διαθέσιμο**	**Cisco Lucent 3Com**
802.11b	**11 Mbps**	**-//-**	**2.4 GHz**	**Ethernet**	**Διαθέσιμο**	**Apple**
802.11a	**54 Mbps**	**-//-**	**5GHz**	**Ethernet**	**Διαθέσιμο**	**Nokia**
802.11g	**54 Mbps**	**-//-**	**2.4 GHz**		**Διαθέσιμο**	**Combaq**
Wi - Max	**70 Mbps**	**70 Km**	**2-11 GHz**		**Διαθέσιμο**	**RedLine**

Κύρια Χαρακτηριστικά Προτύπων

2.1. Πρότυπα Ασύρματων Τοπικών Δικτύων (WLAN)

Το Institute of Electrical and Electronic Engineers (IEEE) είναι ένας οργανισμός που, μεταξύ των άλλων, δημιουργεί και δημοσιεύει πρότυπα. Είναι ιδιαίτερα γνωστό για την οικογένεια προτύπων IEEE 802, που καλύπτουν τα τοπικά και μητροπολιτικά δίκτυα (LAN/MAN). Τα ασύρματα τοπικά δίκτυα ορίζονται από το πρότυπο 802.11 του οργανισμού IEEE.

Η Wi-Fi Alliance είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ειδικεύεται στα 802.11 ασύρματα τοπικά δίκτυα (WLAN). Ιδρύθηκε το 1999 με σκοπό την διασφάλιση της συμβατότητας μεταξύ των WLAN προϊόντων διαφόρων κατασκευαστών, μέσω μιας διαδικασίας πιστοποίησης. Όλοι σχεδόν οι κατασκευαστές εξοπλισμού ασύρματης δικτύωσης είναι μέλη του οργανισμού και συμμετέχουν στο πρόγραμμα πιστοποίησης. Το λογότυπο Wi-Fi που φέρουν τα προϊόντα που περνούν την διαδικασία πιστοποίησης, αποτελεί εγγύηση συμβατότητας.

2.1.1. Το πρότυπο IEEE 802.11

Το 1997 το IEEE δημοσίευσε το πρότυπο με τίτλο: **"Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications".** Πρόκειται για ένα λεπτομερές κείμενο 528 σελίδων, το οποίο σε γενικές γραμμές ορίζει τα παρακάτω:

Την αρχιτεκτονική των ασυρμάτων τοπικών δικτύων
- Διάφορες υπηρεσίες όπως συσχέτιση (association), αυθεντικοποίηση (authentication) και μυστικότητα (privacy)
- Την δομή των πλαισίων (frames)
  Τις λειτουργίες Frequency Hopping Spread Spectrum (FHSS) και Direct Sequence Spread Spectrum (DSSS)
- Τον αλγόριθμο Wired Equivalent Privacy (WEP)

Το πρότυπο ορίζει δύο τύπους φυσικού επιπέδου (PHY): την υπέρυθρη φασματική περιοχή (IR) και την ελεύθερη μπάντα ραδιοσυχνοτήτων στα 2,4 Ghz. Τελικά όμως, για το IR φυσικό επίπεδο δεν έγινε καμία υλοποίηση και έτσι επικράτησε η μπάντα των 2,4 Ghz.

Επίσης ορίζει ρυθμούς μετάδοσης 1 και 2 Mbps και την μέθοδο προσπέλασης μέσου **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance),** η οποία ερμηνεύεται ως **πολλαπλή προσπέλαση με ανίχνευση φορέα και αποφυγή συγκρούσεων.** Η χρήση της μεθόδου αυτής, λόγω των μηχανισμών αποφυγής συγκρούσεων, μειώνει τους πραγματικούς ρυθμούς μετάδοσης περίπου στο μισό των ονομαστικών.

2.1.2. Η τροποποίηση IEEE 802.11b

Το 1999 το IEEE δημοσίευσε μια τροποποίηση του αρχικού προτύπου με τίτλο: **"Higher-Speed Physical Layer Extension in the 2.4-Ghz Band",** η οποία επεκτείνει το αρχικό πρότυπο 802.11, προσθέτοντας τους ρυθμούς μετάδοσης των 5,5 και 11 Mbps στην μπάντα των 2.4 GHz. Η νέα προδιαγραφή υποστηρίζει μόνο την διαμόρφωση DSSS που χρησιμοποιεί τον τύπο διαμόρφωσης Complementary Code Keying (CCK). Επίσης προσθέτει και κάποια νέα χαρακτηριστικά, όπως:

- Δυνατότητα επιλογής μικρότερου προοιμίου (short preamble) των 72 bits στο επίπεδο 2 (OSI) σε αντίθεση με το μεγάλο προοίμιο (long preamble) των 144 bits του αρχικού 802.11. Η δυνατότητα αυτή αποσκοπεί στον ταχύτερο συγχρονισμό των συσκευών. Φυσικά για λόγους συμβατότητας με το αρχικό πρότυπο, ως προεπιλογή χρησιμοποιείται το μεγάλο προοίμιο.
- Δυνατότητα επιλογής καναλιών, σε αντίθεση με την στατική κατανομή καναλιού στο 802.11

2.1.3. Η τροποποίηση IEEE 802.11a

Επίσης το 1999, το IEEE δημοσίευσε μια τροποποίηση με τίτλο: **"Higher-Speed Physical Layer Extension in the 5 Ghz Band"** η οποία περιγράφει ένα ασύρματο τοπικό δίκτυο που λειτουργεί στην μπάντα των 5 GHz. Η προδιαγραφή 802.11a χρησιμοποιεί την διαμόρφωση Orthogonal Frequency Division Multiplexing (OFDM), η οποία παρέχει μεγαλύτερους ρυθμούς μετάδοσης έως 54 Mbps έχοντας όμως μικρότερη εμβέλεια. Ένα πλεονέκτημα της χρήσης της μπάντας των 5 GHz είναι η μείωση των προβλημάτων λόγω παρεμβολών, καθώς πρόκειται για μια πιο "καθαρή" μπάντα σε σχέση με τα 2.4 GHz. Ένας λόγος που το πρότυπο αυτό δεν επικράτησε σε σχέση με το 802.11b είναι ότι δεν είναι συμβατό με αυτό.

2.1.4. Η τροποποίηση IEEE 802.11g

Το 2003 δημοσιεύτηκε μια τροποποίηση με τίτλο: **"Amendment 4: Further Higher Data Rate Extension in the 2.4 Ghz Band"**. Είναι μια επέκταση η οποία προσθέτει ρυθμούς μετάδοσης έως 54 Mbps στην μπάντα των 2.4 GHz χρησιμοποιώντας διαμόρφωση OFDM-DSSS.

Το βασικό πλεονέκτημα του 802.11g είναι ότι είναι συμβατό με το 802.11b, οπότε συσκευές 802.11b και 802.11g μπορούν να συνυπάρχουν σε ένα δίκτυο.

2.1.5. Η τροποποίηση IEEE 802.11n

Στις αρχές του 2004, το IEEE ανακοίνωσε ότι σχημάτισε μια νέα ομάδα εργασίας, η οποία ονομάζεται Task Group n ή TGn. Η ομάδα αυτή ανέλαβε την δημιουργία μιας τροποποίησης του αρχικού προτύπου 802.11, με σκοπό την επίτευξη πραγματικού ρυθμού μεταφοράς τουλάχιστον 100 Mbps. Αυτό σημαίνει ότι ο θεωρητικός ρυθμός μεταφοράς θα πρέπει να είναι τουλάχιστον 200 Mbps. Για να επιτευχθούν τέτοιες ταχύτητες επιβάλλεται η μετάβαση σε νέες

τεχνολογίες ασύρματης μετάδοσης και στη συγκεκριμένη περίπτωση, θα χρησιμοποιηθεί η τεχνολογία MIMO (Multiple Input - Multiple Output). Η ονομασία προήλθε από το γεγονός ότι η τεχνολογία αυτή χρησιμοποιεί πολλαπλές κεραίες για την αποστολή και λήψη δεδομένων και οι οποίες λειτουργούν ταυτόχρονα και ανεξάρτητα η κάθε μία.

2.1.6. Η τροποποίηση IEEE 802.11i

Το 2004 η IEEE δημοσίευσε μια τροποποίηση με τίτλο: **"Amendment 6: Medium Access Control (MAC) Security Enhancements",** η οποία περιγράφει κάποιες επεκτάσεις στο υποεπίπεδο MAC που αποσκοπούν σε ισχυρότερη ασφάλεια. Περιλαμβάνει πρωτόκολλα όπως τα 802.1X, TKIP, CCMP και άλλα.

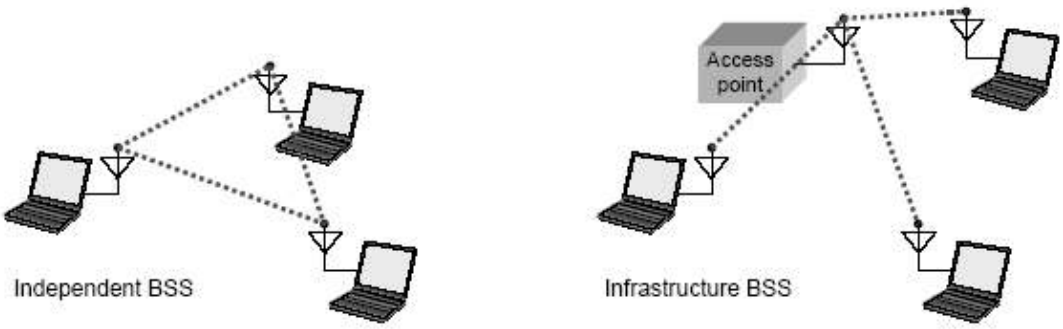
2.1.7. Η προδιαγραφή WPA της Wi-Fi Alliance

Το 2001, μια ομάδα του Πανεπιστημίου της Καλιφόρνια, ανακάλυψε και παρουσίασε κάποιες αδυναμίες του πρωτοκόλλου ασφαλείας WEP. Έτσι το IEEE σχημάτισε την ομάδα εργασίας i (802.11i) με σκοπό την δημιουργία μιας πιο άρτιας λύσης σχετικά με την ασφάλεια του προτύπου 802.11. Όμως, λόγω των χρονοβόρων διαδικασιών που απαιτούνται για την θέσπιση των προτύπων του IEEE, η Wi-Fi Alliance ανέλαβε την ανάπτυξη του προτύπου ασφαλείας Wi-Fi Protected Access (WPA), το οποίο βασίστηκε σε μια πρώιμη έκδοση (draft) του 802.11i. Ουσιαστικά αποτελεί ένα υποσύνολο των μηχανισμών του 802.11i (το οποίο πλέον ονομάζεται και WPA2)

3. Ασύρματα ad-hoc Δίκτυα

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. Ένα ad-hoc ασύρματο τηλεπικοινωνιακό δίκτυο αποτελείται από δύο ή περισσότερους κινητούς κόμβους, υπολογιστικές συσκευές (φορητούς υπολογιστές, υπολογιστές χειρός, κινητά τηλέφωνα κ.τ.λ.), οι οποίοι έχουν δυνατότητα για ασύρματη μετάδοση και λήψη δεδομένων. Οι συσκευές μέσα σε ένα τέτοιο δίκτυο έχουν την δυνατότητα επικοινωνίας με οποιαδήποτε άλλη συσκευή, η οποία βρίσκεται στην εμβέλεια τους ή στην εμβέλεια μιας γειτονικής τους συσκευής. Στην πρώτη περίπτωση η επικοινωνία γίνεται απευθείας μεταξύ των δύο κόμβων, ενώ στην δεύτερη περίπτωση η επικοινωνία γίνεται με τη χρήση ενός ή περισσότερων ενδιάμεσων κόμβων, οι οποίοι αναλαμβάνουν την μεταγωγή των δεδομένων από τον αποστολέα στον παραλήπτη.

Ένα ad-hoc ασύρματο τηλεπικοινωνιακό δίκτυο έχει την δυνατότητα να δημιουργείται δυναμικά και αυτόνομα χωρίς να χρειάζεται την παρουσία άλλων ενεργών και μη ενεργών δικτυακών συσκευών και μπορεί να προσαρμόζεται δυναμικά στις εκάστοτε συνθήκες.



Αυτό σημαίνει ότι έχει την ικανότητα να ξανά-προσαρμόζεται και να δημιουργείται από την αρχή και οι ίδιοι οι κόμβοι, που αποτελούν το δίκτυο, αναλαμβάνουν και την διαχείριση των πόρων και την επιτέλεση των λειτουργιών του. Ο όρος ad-hoc σημαίνει ότι το δίκτυο μπορεί να πάρει πολλές μορφές, να αποτελείται από κόμβους που κινούνται στο χώρο, να λειτουργεί αυτόνομα και να είναι διασυνδεόμενο με κάποιο άλλο δίκτυο. Οι συσκευές που μετέχουν σε ένα τέτοιο δίκτυο, πρέπει να μπορούν να αντιλαμβάνονται την παρουσία άλλων συσκευών, που θα μπορούσαν να συμμετέχουν στο ίδιο δίκτυο, καθώς και να μπορούν να ενεργοποιήσουν τις κατάλληλες διαδικασίες, πρωτόκολλα διασύνδεσης, ούτως ώστε να είναι αυτό εφικτό, με απώτερο σκοπό την επικοινωνία, την ανταλλαγή δεδομένων και την χρήση των υπηρεσιών του δικτύου.

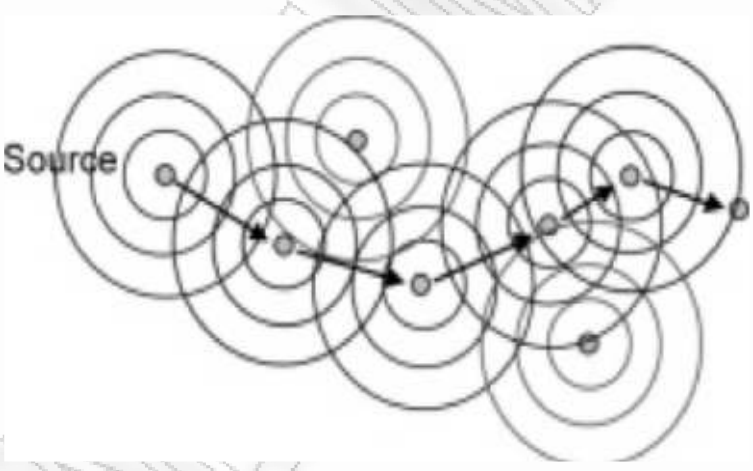
3.1. Δίκτυα κατ' Απαίτηση

Το κυριότερο χαρακτηριστικό των κατ' απαίτηση 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 ένα PDA). Επιπλέον, τα διάφορα ad-hoc δίκτυα μπορεί να διαφέρουν σε πολλά χαρακτηριστικά τους, όπως τους

χρησιμοποιούμενους ρυθμούς επικοινωνίας, 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.

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.



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.

4. Μοντέλα Λειτουργίας Ad-hoc Ασύρματων Δικτύων

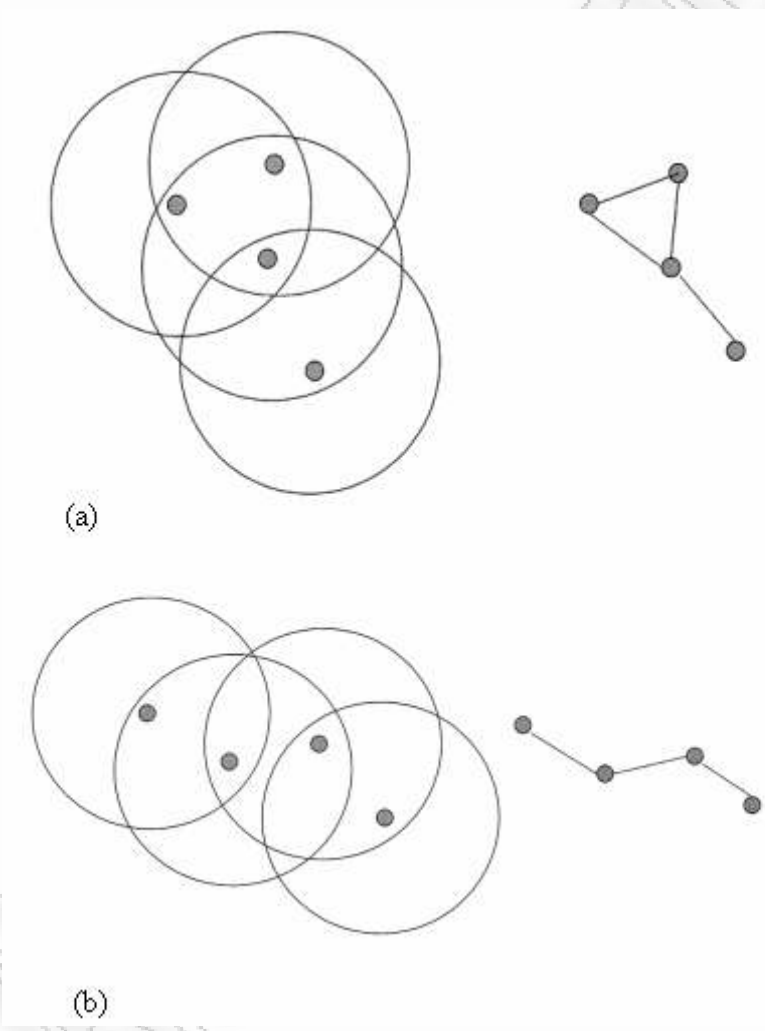
Τα ασύρματα δίκτυα ad-hoc αποτελούνται από κινητούς κόμβους οι οποίοι πρέπει να επιτελέσουν επιπλέον έργο για να μπορέσει το δίκτυο να λειτουργήσει. Στην περίπτωση που μας αφορά, οι κόμβοι των δικτύων αυτών πρέπει να φροντίσουν να εκτελούνται οι βασικές λειτουργίες ενός δικτύου για τη μεταγωγή δεδομένων μεταξύ των κόμβων του δικτύου, εργασία που στα κλασσικά δίκτυα την επιτελούν οι δρομολογητές και τα άλλα ενεργά μη τερματικά στοιχεία του δικτύου. Η καταγραφή των βέλτιστων διαδρομών, μέσω των ενεργών συνδέσεων ενός δικτύου για την μεταφορά δεδομένων, είναι από τις βασικότερες λειτουργίες που πρέπει να έχει ένα δίκτυο υπολογιστών, αφού πολύ απλά χωρίς αυτή δεν είναι δυνατό να υπάρξει.

Υπάρχουν πολλά διαφορετικά είδη πρωτοκόλλων διαθέσιμα σήμερα για την δρομολόγηση δεδομένων σε ένα δίκτυο υπολογιστών, τα οποία μπορούν να λειτουργήσουν αρκετά ικανοποιητικά. Τα πρωτόκολλα αυτά είναι σχεδιασμένα να μπορούν να λειτουργήσουν σε ένα ad-hoc δίκτυο, το οποίο δεν έχει την υποδομή που έχουν τα κλασσικά δίκτυα. Πολλά από τα πρωτόκολλα που έχουμε διαθέσιμα, στα κλασικά ενσύρματα δίκτυα, δεν μπορούν να λειτουργήσουν σε δίκτυα χωρίς υποδομή. Για να είναι δυνατή η λειτουργία τους, είναι απαραίτητες αλλαγές για να μπορέσουν να προσαρμοστούν στα χαρακτηριστικά των ad-hoc δικτύων. Από παρατηρήσεις, πειράματα και προσομοιώσεις που έχουν γίνει, τα πρωτόκολλα αυτά σε καμία περίπτωση δεν μπορούν να έχουν την αναμενόμενη απόδοση και σίγουρα δεν πετυχαίνουν την ίδια απόδοση με αυτή που έχουν, όταν εφαρμόζονται στα κλασσικά δίκτυα. Το γεγονός αυτό μας κάνει να πιστεύουμε ότι για να αντιμετωπίσουμε αποτελεσματικά το πρόβλημα της δρομολόγησης χρειαζόμαστε νέα πρωτόκολλα, τα οποία θα δημιουργηθούν για να λειτουργούν αποκλειστικά σε συνθήκες όπως αυτές που υπάρχουν στα ad-hoc δίκτυα.

Ένα ad-hoc δίκτυο ορίζεται σαν ένα δίκτυο, το οποίο μπορεί να υπάρχει και να λειτουργεί, χωρίς να είναι αναγκαία η διασύνδεση του με κάποια υπάρχουσα δικτυακή υποδομή ή διαχείριση, και επιτρέπει στους κόμβους που είναι συνδεμένοι σε αυτό να επιτελέσουν όποιες λειτουργίες επιθυμούν για την ανταλλαγή δεδομένων και πληροφοριών. Σαν παράδειγμα μπορούμε να πούμε ότι ένα ασύρματο ad-hoc δίκτυο, πολύ απλά, μπορεί να δημιουργηθεί όταν σε ένα χώρο, πχ ένα δωμάτιο, ανοίγουν κάποιοι φορητοί υπολογιστές, οι οποίοι διαθέτουν ασύρματες κάρτες δικτύου και μπορούν απλά ενεργοποιώντας τις να μπορέσουν να σχηματίσουν ένα ασύρματο δίκτυο μεταξύ τους, για να ανταλλάξουν δεδομένα.

5. Κινητικότητα Κόμβων

Όπως γνωρίζουμε στα ασύρματα ad-hoc δίκτυα οι κόμβοι μπορούν να κινούνται. Αυτό είναι ένα από τα βασικότερα χαρακτηριστικά των δικτύων αυτού του τύπου και αποτελεί ένα από τα σημαντικότερα κομμάτια κάθε ερευνητικής μελέτης πάνω στα ασύρματα ad-hoc δίκτυα. Για να μπορέσουμε να συμπεριλάβουμε το συγκεκριμένο χαρακτηριστικό των κόμβων στις διάφορες προσομοιώσεις, έχουν αναπτυχθεί διάφορα μοντέλα κίνησης των κόμβων, με τα οποία μπορούμε να προσομοιώσουμε, κατά το δυνατό, την κίνηση που θα είχαν οι κόμβοι, εάν λειτουργούσαν σε ένα πραγματικό δίκτυο. Τα διάφορα μοντέλα που υπάρχουν βασίζονται κυρίως σε στατιστικές μελέτες γύρω από την κίνηση των ad-hoc κόμβων.



(a) Αναπαράσταση ad-hoc δικτύου, (b) Μεταβολή της τοπολογίας εξαιτίας της κίνησης των κόμβων

Τα μοντέλα κινητικότητας των κόμβων των ad-hoc ασύρματων δικτύων είναι από τις σημαντικές δομικές μονάδες μιας προσομοίωσης, σύμφωνα με τις μελέτες που έχουν γίνει πάνω στα ασύρματα αυτά δίκτυα. Οι ερευνητές μπορούν να επιλέξουν από μία ποικιλία μοντέλων, που έχουν αναπτυχθεί για την περιοχή των ασύρματων τηλεπικοινωνιακών συστημάτων και κατ' επέκταση και των ασύρματων ad-hoc δικτύων.

6. Χωρητικότητα

Το ερώτημα που προκύπτει εδώ είναι πως μπορεί να μεταχειριστεί η αύξηση του αριθμού των χρηστών σε σχέση με το throughput που μπορεί να επιτευχθεί. Το γεγονός ότι κάθε κόμβος έχει και τον επιπλέον ρόλο να προωθεί ξένα προς αυτόν πακέτα δημιουργεί περαιτέρω παρεμβολή και περιορίζει την ικανότητα εξυπηρέτησης που έχουν ad-hoc δίκτυα μεγάλου αριθμού κόμβων.

Το μέγεθος ενός ad-hoc δικτύου σχετίζεται άμεσα με την ποιότητα των υπηρεσιών που μπορεί να προσφέρει αυτό το δίκτυο. Πρόσφατες έρευνες έδειξαν ότι όσο μεγαλώνει το μέγεθος ενός ad-hoc δικτύου τόσο μικρότερο γίνεται το throughput του δικτύου. Κάποιες άλλες μελέτες έδειξαν ότι υψηλή κινητικότητα των κόμβων μπορεί να οδηγήσει σε καλύτερα αποτελέσματα όσον αφορά το throughput σε κάποιες περιπτώσεις ενώ σε κάποιες άλλες μπορεί να μένει σταθερό το throughput ακόμα και αν ο αριθμός των ασύρματων κόμβων αυξάνει με το χρόνο.

Άλλες παράμετροι που επηρεάζουν τη χωρητικότητα (capacity) ενός δικτύου είναι τα πρότυπα κίνησης (traffic patterns) και οι τοπικές ράδιο-αλληλεπιδράσεις.

7. Η Ενέργεια στα ad-hoc Δίκτυα.

Στα ασύρματα δίκτυα το σύνολο των συσκευών που συνδέονται σε αυτά (notebooks, personal digital assistants (PDAs), κινητά τηλέφωνα, αισθητήρες) αναπόφευκτα λειτουργούν με παροχή ισχύος από μπαταρίες. Η ασύρματη φύση τους και η ανάγκη για κινητικότητα είναι οι λόγοι που επιβάλλουν κάτι τέτοιο. Είναι επομένως ξεκάθαρο ότι ο χρόνος ζωής της μπαταρίας είναι κρίσιμος παράγοντας για αυτού του είδους τα δίκτυα και γενικότερα στο τομέα του κινητού υπολογισμού (mobile computing).

Η τεχνολογία των μπαταριών υπολείπεται σε σχέση με την αντίστοιχη στο τομέα των τηλεπικοινωνιών την τελευταία δεκαετία. Το γεγονός αυτό οδηγεί στη προσπάθεια σχεδιασμού ενεργό-αποδοτικού υλικού και λογισμικού που θα επεκτείνει το χρόνο ζωής των δικτυακών συσκευών και κατά επέκταση και του δικτύου. Στο σημείο αυτό αναφέρουμε ότι σαν χρόνος ζωής ενός ασύρματου ad-hoc δικτύου θεωρούμε τον χρόνο μέχρι να εξαντληθεί η ενέργεια σε κάποιον (οποιονδήποτε) κόμβο.

Μία φορητή συσκευή αποτελείται από διάφορα τμήματα υλικού τα οποία καταναλώνουν ενέργεια. Ενδεικτικά αναφέρουμε τα εξής components: display monitor, δίσκος, CPU, μνήμες καθώς και η wireless network interface κάρτα. Η τελευταία μάλιστα μπορεί να καταναλώσει 10-50% των συνολικών αποθεμάτων ενέργειας του συστήματος. Είναι επομένως φανερό ότι υπάρχει η ανάγκη για υποστήριξη σχεδιασμού χαμηλής κατανάλωσης όλων των components που συμμετέχουν στη κατανάλωση ενέργειας.

Επίσης αναφέρουμε ότι κάθε κόμβος ενός ασύρματου δικτύου μπορεί να βρίσκεται σε 4 καταστάσεις λειτουργίας: στη κατάσταση μετάδοσης, στη κατάσταση παραλαβής, στη κατάσταση αναμονής και στη κατάσταση αναστολής. Και οι 4 καταστάσεις δαπανούν ενέργεια με τη τελευταία να δαπανά τη μικρότερη. Κατά τη κατάσταση της μετάδοσης η ενέργεια δαπανάται για τη δημιουργία, τη διαμόρφωση και την υπόλοιπη επεξεργασία του σήματος που πρόκειται να μεταδοθεί. Κατά τη κατάσταση

της παραλαβής, ενέργεια δαπανάται για την επεξεργασία του λαμβανόμενου σήματος ενώ στη κατάσταση αναμονής ενέργεια δαπανάται για τη παρακολούθηση του φυσικού μέσου μετάδοσης. Λόγω της χαμηλής κατανάλωσης που παρουσιάζει η $4^{η}$ κατηγορία, παρατηρείται προσπάθεια εύρεσης τεχνικών οι οποίες θα μπορούν να προβλέπουν τις χρονικές στιγμές στις οποίες θα μπορούν κάποιοι κόμβοι να μπουν σε κατάσταση αναστολής.

Από όλα τα παραπάνω γίνεται αντιληπτό ότι για να επιτευχθεί χαμηλή κατανάλωση ενέργειας θα πρέπει το πρόβλημα να αντιμετωπιστεί σε όλες τις πτυχές του. Μια και μόνο αποσπασματική αντιμετώπιση δεν μπορεί να δώσει ικανοποιητικά αποτελέσματα και κατά συνέπεια η προσπάθεια θα πρέπει να γίνει προς όλες τις κατευθύνσεις στις οποίες γίνεται αξιοποίηση των διαθέσιμων πόρων ενέργειας του δικτύου.

Τα πρωτόκολλα εξοικονόμησης ενέργειας χωρίζονται σε δύο κατηγορίες:

- Στα transmitter power control και στα
- Power managements.

Στη πρώτη κατηγορία κάθε κόμβος προσαρμόζει την ισχύ μετάδοσής του προς τους υπόλοιπους. Αυτό είχε ως συνέπεια, εκτός από τη μείωση της κατανάλωσης ενέργειας και τη μείωση της παρεμβολής, την αλλαγή με δυναμικό τρόπο της τοπολογίας του δικτύου. Ένα επιπλέον πλεονέκτημα είναι και η αύξηση της χρήσης του wireless bandwidth. Στη δεύτερη κατηγορία αναπτύσσονται αλγόριθμοι είτε στο MAC, είτε στο network, είτε σε υψηλότερα επίπεδα οι οποίοι έχουν ως στόχο την καλύτερη διαχείριση της ενέργειας.

8. Το Πρόβλημα της Ασφάλειας στα ad-hoc Δίκτυα

Όπως έχει αναφερθεί τα ad-hoc δίκτυα χαρακτηρίζονται από το ότι σε αυτά δεν υπάρχει μια κεντρική λειτουργία διαχείρισης του δικτύου και ότι υπάρχει συνεχής αλλαγή της τοπολογίας. Τα χαρακτηριστικά αυτά κάνουν τα ad-hoc δίκτυα ευπρόσβλητα σε ένα αριθμό επιθέσεων (attacks). Για να γίνουν αυτά τα δίκτυα ευρέως αποδεκτά στον εμπορικό κόσμο θα πρέπει να επιλυθεί το θέμα της ασφάλειας (security) που είναι υπέρτατης σημασίας και το οποίο είναι εξαιρετικά δύσκολο να επιτευχθεί. Οι λόγοι είναι η ευπάθεια των ασύρματων συνδέσμων, η περιορισμένη φυσική προστασία των κόμβων, η έλλειψη μιας κεντρικής παρακολούθησης καθώς επίσης και η δυνατότητα που υπάρχει να συνδεθεί στο δίκτυο εξωτερικός εχθρικός κόμβος ο οποίος θα επιχειρήσει να βλάψει το δίκτυο.

Ο όρος ασφάλεια υπονοεί την ικανοποίηση πληθώρα απαιτήσεων και αναγκών.
Ενδεικτικά αναφέρουμε μερικές από αυτές στη συνέχεια.

- Διαθεσιμότητα (availability). Ο όρος διαθεσιμότητα σημαίνει ότι οι υπηρεσίες που παρέχονται από όλους τους κόμβους του δικτύου θα πρέπει να συνεχίζουν να παρέχονται ανεξαρτήτως ύπαρξης επιθέσεων. Οι κόμβοι θα πρέπει να μπορούν να επικοινωνούν ανά πάσα στιγμή.

- Αυθεντικότητα (authenticity). Με τον όρο αυθεντικότητα εννοείται ότι όσοι κόμβοι συμμετέχουν στην επικοινωνία είναι γνήσιοι. Αυτό σημαίνει ότι θα πρέπει να υπάρξει κάποιος τρόπος ώστε οι κόμβοι να μπορούν να αποδείξουν την ταυτότητά τους.

- Εμπιστευτικότητα (confidentiality). Για να ικανοποιηθεί η εμπιστευτικότητα θα πρέπει να μην επιτρέπεται σε κάποιον εξωτερικό κόμβο να μπορεί να προσπελάσει τη πληροφορία που διασχίζει δύο κόμβους.

- Ακεραιότητα (Integrity). Το πακέτο ή το μήνυμα που παραδίδεται δε θα πρέπει να έχει τροποποιηθεί. Με άλλα λόγια παραλαμβάνεται ότι έχει αποσταλεί.

- Επικαιρότητα (timeliness). Με τον όρο επικαιρότητα εννοούμε ότι οι routing ενημερώσεις θα πρέπει να παραδίδονται εγκαίρως.

- Απομόνωση (isolation). Η απομόνωση απαιτεί το πρωτόκολλο που χρησιμοποιείται να είναι ικανό να απομονώνει όσους κόμβους επιδεικνύουν κακή συμπεριφορά.

- Εξουσιοδότηση (authorization). Έχει να κάνει με τα προνόμια και τις εξουσιοδοτήσεις που σχετίζονται με τον κάθε κόμβο του δικτύου.

Διάφορα μοντέλα έχουν προταθεί στη βιβλιογραφία για την επίλυση του προβλήματος της ασφάλειας.

9. Εφαρμογές Mobile Ασύρματων ad-hoc Δικτύων

Υπάρχουν πολλές εφαρμογές στα κινητά ad-hoc ασύρματα δίκτυα. Στην πραγματικότητα οποιαδήποτε καθημερινή εφαρμογή όπως το ηλεκτρονικό ταχυδρομείο και η μεταφορά αρχείων, μπορεί να θεωρηθεί εύκολα υλοποιήσιμη μέσα σε ένα περιβάλλον ad-hoc δικτύων. Οι υπηρεσίες του παγκόσμιου ιστού είναι επίσης δυνατόν να λειτουργήσουν σε περίπτωση που οποιοσδήποτε κόμβος στο ad-hoc δίκτυο μπορεί να χρησιμεύσει ως μια πύλη προς το διαδίκτυο.

Δεν χρειάζεται να υπογραμμίσουμε το ευρύ φάσμα των στρατιωτικών εφαρμογών που έχουν δημιουργηθεί για τα ειδικά δίκτυα. Η τεχνολογία δικτύων αυτού του τύπου αναπτύχθηκε αρχικά λαμβάνοντας υπόψη στρατιωτικές εφαρμογές, ειδικά στο πεδίο της μάχης όπου ένα κλασσικό δίκτυο με προϋπάρχουσα υποδομή είναι σχεδόν αδύνατο να υπάρξει. Τα ad-hoc δίκτυα έχουν την ικανότητα της αυτό-δημιουργίας και αυτονομίας και μπορούν να χρησιμοποιηθούν όπου άλλες τεχνολογίες είτε αποτυγχάνουν είτε δεν μπορούν να λειτουργήσουν αποτελεσματικά. Τα προηγμένα σύγχρονα χαρακτηριστικά γνωρίσματα των ασύρματων ad-hoc δικτύων, όπως το μεγάλο εύρος ζώνης του ασύρματου καναλιού, που τα κάνει συμβατά με τις εφαρμογές πολυμέσων, την ικανότητα μεταγωγής (roaming) και τέλος το συντονισμό και την ικανότητα συνεργασία με άλλες δομές δικτύων, δημιουργούν την ανάγκη σχεδιασμού και υλοποίησης νέων εφαρμογών.

Μερικές γνωστές εφαρμογές των ad-hoc δικτύων είναι:

- Συλλογική συνεργασία (Collaborative Work) — Με τον όρο αυτό περιγράφουμε όλες τις περιπτώσεις όπου οι άνθρωποι επιθυμούν να ανταλλάξουν δεδομένα, για να μπορέσουν να εργαστούν και να συνεργαστούν για την ολοκλήρωση συγκεκριμένων διεργασιών, είτε αυτές έχουν να κάνουν με την εργασία τους είτε με την διασκέδαση τους. Η ανάγκη για επικοινωνία και ανταλλαγή δεδομένων είναι κρισιμότερο να συμβεί σε εξωτερικό περιβάλλον και χώρο και όχι στα γραφεία, στα σπίτια ή όπου αλλού είναι δυνατή η χρησιμοποίηση κλασικών δικτύων. Τα ad-hoc δίκτυα έρχονται να ικανοποιήσουν ακριβώς αυτή την ανάγκη και να δώσουν λύση στο πρόβλημα της επικοινωνίας των υπολογιστικών συστημάτων, χωρίς αυτά να είναι απαραίτητα συνδεδεμένα σε κάποια δικτυακή υποδομή.

- Οι εφαρμογές διαχείρισης κρίσεων (Crisis Management Applications) — Οι εφαρμογές αυτές έρχονται να υποστηρίξουν τους μηχανισμούς αντιμετώπισης κρίσεων που καλούνται να αντιμετωπίσουν, παραδείγματος χάριν φυσικές καταστροφές, όπου η τηλεπικοινωνιακή υποδομή μπορεί να είναι εκτός λειτουργίας και η γρήγορη αποκατάσταση της είναι σημαντικά κρίσιμη. Με τη χρησιμοποίηση των ad-hoc δικτύων, μια προσωρινή υποδομή θα μπορούσε να οργανωθεί σε ώρες αντί για ημέρες ή εβδομάδες, που θα απαιτούνταν για τα κλασικά τηλεπικοινωνιακά συστήματα. Επίσης τα ad-hoc δίκτυα θα μπορούσαν να χρησιμοποιηθούν για την εύρεση και διάσωση πολιτών που βρίσκονται εγκλωβισμένοι, πχ σε ένα κτίριο ή μια υπόγεια σήραγγα, μετά από μια μεγάλη καταστροφή όπως ένα σεισμό.

- Δίκτυα μικρής εμβέλειας, προσωπικά ασύρματα δίκτυα, Bluetooth (Personal Area Networks (PAN), Bluetooth) — Ένα PAN είναι ένα ασύρματο τοπικό δίκτυο μικρής εμβέλειας, του οποίου οι κόμβοι βρίσκονται κοντά σε ένα άτομο, και συνήθως είναι εγκατεστημένοι στα ρούχα του ή σε προσωπικά του αντικείμενα.

2. Δρομολόγηση σε Ασύρματα Κινητά Δίκτυα

1. Ορισμός του Προβλήματος

Είναι σαφές ότι η δρομολόγηση σε ένα Mobile Ad-Hoc δίκτυο (MANET) είναι εγγενώς διαφορετική από την δρομολόγηση στα κλασικά ενσύρματα δίκτυα. Η δρομολόγηση σε ένα τέτοιο δίκτυο εξαρτάται από πολλούς παράγοντες συμπεριλαμβανομένης της τοπολογίας των κόμβων, της επιλογής των διαδρομών, της κινητικότητας των κόμβων του δικτύου, την πρωτοβουλίας έκδοσης ενός νέου

αιτήματος δρομολόγησης και άλλων χαρακτηριστικών που θα μπορούσαν να εξυπηρετήσουν στην εύρεσης των βέλτιστων διαδρομών γρήγορα και αποτελεσματικά. Η μικρή διαθεσιμότητα πόρων στα ad-hoc ασύρματα δίκτυα απαιτεί αποδοτική χρησιμοποίηση τους και ως εκ τούτου επιβάλει την βέλτιστη δρομολόγηση των δεδομένων. Επίσης, η ιδιαίτερα δυναμική φύση των ad-hoc δικτύων επιβάλλει την ύπαρξη αυστηρών περιορισμών στη δρομολόγηση των πρωτοκόλλων που σχεδιάζονται συγκεκριμένα για αυτά, επηρεάζοντας κατά συνέπεια τις κατευθύνσεις στην μελέτη και έρευνα που συντελείτε γύρω από αυτά τα πρωτόκολλα. Μια από τις σημαντικότερες προκλήσεις στο σχεδιασμό ενός πρωτοκόλλου δρομολόγησης για ένα ad-hoc δίκτυο είναι το γεγονός ότι, από τη μια πλευρά, κάθε κόμβος του δικτύου πρέπει να κατέχει πληροφορίες τουλάχιστον για τις ενεργές συνδέσεις με τους γείτονές του για τον καθορισμό μιας διαδρομής και αφ' ετέρου η τοπολογία των δικτύων αυτών μπορεί να αλλάξει αρκετά συχνά με αποτέλεσμα να αλλάζει και το σύνολο των γειτόνων του κάθε κόμβου. Επιπλέον, καθώς ο αριθμός των κόμβων του δικτύου μπορεί να είναι αρκετά μεγάλος, η εύρεση μιας διαδρομής προς κάποιο προορισμό απαιτεί επίσης τη συχνή ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των κόμβων. Κατά συνέπεια, ο όγκος των νέων πληροφοριών δρομολόγησης είναι αρκετά μεγάλος και αυξάνεται όταν στο δίκτυο υπάρχουν κόμβοι υψηλής κινητικότητας. Οι κόμβοι αυτοί μπορούν να προκαλέσουν μεγάλες καθυστερήσεις και συμφόρηση στο ασύρματο κανάλι κάνοντας αδύνατη ή πολύ δύσκολη την μετάδοση πραγματικών δεδομένων.

2. Το πρόβλημα της Δρομολόγησης στα Ασύρματα ad-hoc Δίκτυα

Το πρόβλημα της δρομολόγησης σε ένα ασύρματο ad-hoc τηλεπικοινωνιακό δίκτυο, το οποίο αποτελείται από κινητούς κόμβους, ορίζεται ως η διαδικασία εύρεσης μιας διαδρομής από έναν κόμβο του δικτύου προς ένα άλλο κόμβο του ίδιου δικτύου με σκοπό την μεταφορά δεδομένων. Ως διαδρομή σε ένα ασύρματο ad-hoc δίκτυο ορίζουμε την ακολουθία των κόμβων μέσω των οποίων θα διαβιβαστούν τα πακέτα δεδομένων στον προορισμό τους. Υποθέτουμε ότι οι κόμβοι, στο δίκτυο αυτό, δεν μπορούν να μεταβιβάσουν απευθείας τα δεδομένα ο ένας στον άλλο, λόγω της περιορισμένης εμβέλειας του ασύρματου πομπού και γι' αυτό χρησιμοποιούνται ενδιάμεσοι κόμβοι για να μπορέσουν να μεταδοθούν τα δεδομένα στον προορισμό τους. Οι κόμβοι σε ένα ασύρματο ad-hoc δίκτυο στις περισσότερες περιπτώσεις μπορούν και κινούνται, με αποτέλεσμα η θέση τους στο δίκτυο να αλλάζει συνεχώς. Καθώς αλλάζει η θέση τους, αλλάζει και η κατάσταση του δικτύου, άλλες συνδέσεις γίνονται ενεργές, άλλες ανενεργές, νέοι κόμβοι εισέρχονται και προσθέτονται στο δίκτυο, ενώ άλλοι απομακρύνονται και αποβάλλονται. Το γεγονός αυτό επιβάλει οι κόμβοι του δικτύου άλλες φορές να παίζουν το ρόλο τερματικών κόμβων, που είναι είτε οι κόμβοι προέλευσης είτε οι κόμβοι του προορισμού των πακέτων, που ταξιδεύουν στο δίκτυο και άλλες το ρόλο των δρομολογητών ή των μεταγωγέων, που φροντίζουν να προωθήσουν πακέτα, που δεν προορίζονται γι' αυτούς στους κόμβους προορισμού. Για το λόγο αυτό, σε ένα ασύρματο ad-hoc δίκτυο είναι απαραίτητο ένα πρωτόκολλο δρομολόγησης, για να διατηρηθούν οι βασικές λειτουργίες του δικτύου, τις οποίες τώρα έχουν επιφορτιστεί οι κόμβοι.

3. Δρομολόγηση στο Επίπεδο των Συνδέσεων

Στη δρομολόγηση στο επίπεδο συνδέσεων κάθε κόμβος διατηρεί μια άποψη της τοπολογίας του δικτύου με ένα βάρος για κάθε σύνδεση. Κάθε κόμβος μεταδίδει σε

όλους του υπόλοιπους κόμβους περιοδικά τις πληροφορίες δρομολόγησης που κατέχει, τις οποίες λαμβάνουν οι υπόλοιποι κόμβοι του δικτύου και ενημερώνουν του πίνακες με τις δικές τους πληροφορίες δρομολόγησης. Στη συνέχεια εφαρμόζοντας έναν αλγόριθμό εύρεσης της συντομότερης διαδρομής επιλέγουν τον επόμενο κόμβο για κάθε ξεχωριστό προορισμό. Ασυνεπείς απόψεις της τοπολογίας του δικτύου μπορούν να οδηγήσουν στο σχηματισμό βρόχων στις διαδρομές, πράγμα που επηρεάζει την απόδοση του αλγόριθμου δρομολόγησης και σκοπός είναι ο εντοπισμός και η απαλοιφή αυτών.

4. Δρομολόγηση με την Χρήση του Διανύσματος της Απόστασης

Κάθε κόμβος κοιτάει μόνο το κόστος των εξερχόμενων συνδέσεών του και αντί της μετάδοσης αυτών των πληροφοριών σε όλους τους κόμβους, μεταδίδει περιοδικά σε κάθε ένα από τους γείτονές του την δικιά του εκτίμηση της πιο σύντομης διαδρομής προς κάθε άλλο κόμβο στο δίκτυο. Οι κόμβοι που λαμβάνουν την πληροφορία αυτή την χρησιμοποιούν για να υπολογίσουν εκ νέου τις διαδρομές προς όλους τους κόμβους του δικτύου, χρησιμοποιώντας ενός αλγορίθμου εύρεσης των συντομότερων μονοπατιών.

5. Δρομολόγηση Πηγής

Η δρομολόγηση πηγής περιγράφει ότι κάθε πακέτο έχει ενσωματωμένο το πλήρες μονοπάτι προς τον κόμβο προορισμού. Ο ενδιαφερόμενος κόμβος συλλέγει όλες τις δυνατές επιλογές διαδρομών και επιλέγει την καλύτερη, σύμφωνα με ένα μέτρο σύγκρισης. Το πλεονέκτημα της μεθόδου αυτής είναι ότι είναι πολύ εύκολο να αποφευχθούν οι κυκλικοί βρόχοι στις διαδρομές δρομολόγησης, αφού ο κόμβος που επιλέγει μια διαδρομή μπορεί να εξασφαλίσει ότι δεν περιέχει βρόγχους. Το μειονέκτημα είναι ότι για κάθε πακέτο απαιτείται μία μικρή αρχική καθυστέρηση για την εύρεση μιας διαδρομής.

6. Τεχνική Πλημμύρας

Πολλά πρωτοκόλλα δρομολόγησης για να μεταδώσουν πληροφορίες δρομολόγησης, τις εκπέμπουν από τον κόμβο προέλευσης προς όλους τους άλλους κόμβους του δικτύου με την τεχνική της πλημμύρας. Η τεχνική αυτή είναι μια ευρέως χρησιμοποιημένη μορφή ασύρματης μετάδοσης και λειτουργεί ως εξής. Ο κόμβος προέλευσης στέλνει τις πληροφορίες του στους γείτονές του (στην ασύρματη περίπτωση, αυτό σημαίνει, σε όλους τους κόμβους που είναι μέσα στη εμβέλεια του πομπού). Οι γείτονες αναμεταδίδουν στους γείτονές τους τις πληροφορίες που λαμβάνουν. Η διαδικασία αυτή συνεχίζεται έως ότου οι πληροφορίες δρομολόγησης παραληφθούν από όλους τους κόμβους του δικτύου. Ένας κόμβος αναμεταδίδει κάθε πακέτο μόνο μια φορά. Αν λάβει ξανά πακέτο που έχει ήδη προωθήσει απλά το αγνοεί και για να το εξασφαλίσει αυτό χρησιμοποιεί έναν αριθμό ο οποίος αυξάνεται για κάθε νέο πακέτο που ο κόμβος στέλνει.

7. Proactive versus Reactive Πρωτόκολλα Δρομολόγησης

Στα πρωτόκολλα δρομολόγησης βασική λειτουργία είναι η διαδικασία εύρεσης των διαδρομών ανάμεσα στους κόμβους του δικτύου. Ένα από τα πιο ενδιαφέροντα ερευνητικά θέματα, ιδιαίτερα τα τελευταία χρόνια, είναι το εάν οι κόμβοι σε ένα ad-

hoc δίκτυο θα πρέπει να κρατούν στοιχεία για κάθε δυνατή διαδρομή ανάμεσα σε δύο οποιοδήποτε κόμβους του δικτύου ή θα πρέπει να κρατούν στοιχεία μόνο για τις διαδρομές εκείνες που είναι άμεσου ή μεγάλου ενδιαφέροντος. Στην πράξη αυτό που συμβαίνει είναι ότι οι κόμβοι του δικτύου δεν χρειάζονται κάποια διαδρομή προς ένα άλλο κόμβο παρά μόνο στην περίπτωση που χρειαστούν να στείλουν δεδομένα προς αυτόν, είτε αυτός είναι ο κόμβος προορισμού των δεδομένων, είτε είναι ένας ενδιάμεσος κόμβος που πρέπει να περάσουν τα δεδομένα για να φτάσουν στον τελικό προορισμό τους. Η έρευνα και η ανάλυση που γίνεται, πάνω σε διάφορα σενάρια και πρωτόκολλα έχει ως στόχο να αποδείξει ποια από τις δύο απόψεις είναι η πιο αποδοτική και γιατί.

Τα πρωτόκολλα τα οποία κρατούν στοιχεία για όλες τις πιθανές διαδρομές που μπορεί να χρειαστούν οι κόμβοι σε ένα δίκτυο έχουν το πλεονέκτημα ότι όταν ζητηθεί μία συγκεκριμένη διαδρομή, από οποιοδήποτε σημείο του δικτύου σε οποιοδήποτε άλλο, αυτή θα υπάρχει και θα προωθηθεί προς χρήση χωρίς καθυστέρηση. Με άλλα λόγια όποια διαδρομή και αν επιθυμούμε να ζητήσουμε προς χρήση, αν υπάρχει, θα μπορούμε να την έχουμε στη διάθεση μας χωρίς να περιμένουμε, επειδή η διαδικασία αναζήτησης έχει ήδη ολοκληρωθεί και τα αποτελέσματα βρίσκονται έτοιμα προς χρήση. Τέτοια πρωτόκολλα ονομάζονται proactive και το βασικό χαρακτηριστικό είναι ότι περιοδικά αναζητούν όλες τις πιθανές διαδρομές προς κάθε κόμβο του δικτύου, για να μπορούν να τις χρησιμοποιήσουν όποια στιγμή τις χρειαστούν.

Από την άλλη μεριά έχουμε τα πρωτόκολλα τα οποία ενεργοποιούν την διαδικασία εύρεσης ενός μονοπατιού (διαδρομής) από ένα κόμβο σε ένα άλλο, μόνο όταν εκδοθεί από τον ενδιαφερόμενο κόμβο ανάλογο αίτημα. Τα πρωτόκολλα αυτά είναι φυσικό να κάνουν σαφώς μικρότερη χρήση του εύρους καναλιού σε σχέση με τα προηγούμενα πρωτόκολλα για την εύρεση των ζητούμενων διαδρομών. Έχουν όμως το σημαντικό μειονέκτημα της αρχικής καθυστέρησης κάθε φορά που ζητείται μία διαδρομή, αφού πριν προωθηθεί στον αιτούντα κόμβο πρέπει να ενεργοποιηθεί η διαδικασία εύρεσης και μετά να τον εξυπηρετήσουν.

8. Ομάδα Εργασίας MANET

Ο σκοπός αυτής της ομάδας εργασίας είναι η τυποποίηση πρωτοκόλλων δρομολόγησης IP, κατάλληλα για την εφαρμογή τους σε ασύρματα στατικά και δυναμικά τηλεπικοινωνιακά δίκτυα επικοινωνιών. Η θεμελιώδης σχεδιαστική αρχή των πρωτοκόλλων αυτών είναι τα ιδιαίτερα χαρακτηριστικά που έχουν οι ασύρματες συνδέσεις σε ένα δίκτυο και το πώς αυτά μπορούν να επηρεάσουν ένα πρωτόκολλο δρομολόγησης. Η δρομολόγηση σε ένα δυναμικό ασύρματο δίκτυο επηρεάζεται σε πολύ μεγάλο βαθμό από παράγοντες όπως, οι σχετικές θέσεις των κόμβων στο δίκτυο, η κίνηση των κόμβων, η εμβέλεια των ασύρματων πομποδεκτών, τα φυσικά εμπόδια ή άλλες πηγές παρεμβολής που μπορεί να επηρεάζουν την μετάδοση. Τα χαρακτηριστικά αυτά και άλλα τα οποία δεν αναφέρουμε, έχουν σαν αποτέλεσμα η δρομολόγηση να πρέπει να εκτελείται δυναμικά κάτω από διαφορετικές συνθήκες κάθε φορά. Το ζητούμενο λοιπόν και ο στόχος της συγκεκριμένης ομάδας εργασίας είναι η έρευνα και η μελέτη υποψήφιων πρωτοκόλλων δρομολόγησης, τα οποία θα μπορούν να ικανοποιούν τις ιδιαίτερες ανάγκες που παρουσιάζουν τα ασύρματα δίκτυα.

Στο παρελθόν αυτή η ομάδα εργασίας έχει εστιάσει την έρευνα της σε μια ευρεία σειρά από προβλήματα και ζητήματα απόδοσης των σχετικών υποψηφίων πρωτοκόλλων. Πλέον όμως ο σκοπός της είναι η συγκέντρωση και η προώθησης των προδιαγραφών διάφορων πρωτοκόλλων δρομολόγησης σε μορφή RFC (Request For Comments). Μερικά από τα πρωτόκολλα αυτά είναι ο AODV, ο DSR, ο OLSR και το TBRPF. Τα πρωτόκολλα που αναφέραμε είναι αυτά τα οποία παρέμειναν υποψήφια για την έκδοση του τελικού προτύπου, μέσα από μια πλειάδα προτάσεων και υποψηφιοτήτων. Μπορούμε να πούμε ότι είναι τα περισσότερο ώριμα πρωτόκολλα, όσο αφορά την κατανόηση και εφαρμογή των ιδιαίτερων χαρακτηριστικών των MANETs, κάτι που βρίσκουμε σε κάθε ένα από αυτά τα πρωτόκολλα. Αν και αυτά παρέχουν ένα βασικό σύνολο πρωτοκόλλων που καλύπτουν τις απαιτήσεις των MANETs, απαιτείται περισσότερη εμπειρία και πειραματισμός για την απόκτηση μιας καλύτερης άποψης για την συνολική τους απόδοση. Τελικός σκοπός της ομάδας εργασίας αυτής είναι λοιπόν να συντονίσει όλη αυτή την συζήτηση και έρευνα και να βοηθήσει στην καλύτερη και γρηγορότερη αξιοποίηση των γνώσεων και των συμπερασμάτων που εξάγονται από την έρευνα που γίνεται από πολλές ομάδες πάνω στην δρομολόγηση στα Mobile Ad-hoc Networks.

Πάνω σε αυτή τη βάση η ομάδα εργασίας μετά την ολοκλήρωση της έρευνας και της εξαγωγής των συμπερασμάτων και των αποτελεσμάτων θα προσπαθήσει να σχεδιάσει, να αναπτύξει και να καθιερώσει ένα σύνολο κοινών χαρακτηριστικών δρομολόγησης, που πρέπει να έχει κάθε αλγόριθμος δρομολόγησης σε ένα ad-hoc mobile δίκτυο και θα το καταθέσει στον διεθνή οργανισμό Internet Standards. Οι γνώσεις που θα αποκτηθούν από την έρευνα στα υπάρχοντα πρωτόκολλα θα χρησιμοποιηθούν σαν βάση για την δημιουργία των σχεδιαστικών αρχών, για να προκύψει ένα νέο πρωτόκολλο δρομολόγησης, που θα είναι καθολικά αποδεκτό και αποδοτικό σε κάθε περίπτωση.

Ως τμήμα αυτής της προσπάθειας η ομάδα εργασίας θα εξετάσει τις πτυχές της ασφάλειας και του ελέγχου συμφόρησης στα πρωτόκολλα δρομολόγησης.

9. Περιγραφή Πρωτοκόλλων Δρομολόγησης των MANET's.

9.1. Proactive και Reactive Πρωτόκολλα Δρομολόγησης

Τα ad-hoc πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν ως Proactive και Reactive. Τα πρώτα εξουσιοδοτούν τους κόμβους σε ένα ad-hoc κινητό δίκτυο να ανακαλύπτουν και να γνωρίζουν τις διαδρομές προς όλους τους πιθανούς προορισμούς του δικτύου έτσι ώστε, όταν πρέπει να διαβιβαστεί ένα πακέτο, να είναι ήδη γνωστή η διαδρομή που αυτό πρέπει να ακολουθήσει. Τα πρωτόκολλα της δεύτερης κατηγορίας υιοθετούν μια διαφορετική προσέγγιση με την οποία οι κόμβοι ανακαλύπτουν μόνο τις διαδρομές προς αυτούς τους προορισμούς, για τους οποίους γίνεται σχετική αίτηση εύρεσης μιας διαδρομής. Ένας κόμβος δεν χρειάζεται να γνωρίζει μια διαδρομή προς ένα προορισμό, παρά μόνο όταν πακέτα δεδομένων τα οποία πρέπει να προωθήσει, έχουν σαν τελικό προορισμό τους τον κόμβο αυτό. Τα proactive πρωτόκολλα έχουν το πλεονέκτημα ότι ένας κόμβος υπόκειται στην ελάχιστη καθυστέρηση για την απόκτηση μιας διαδρομής, αφού αυτή αν υπάρχει θα είναι διαθέσιμη στους πίνακες δρομολόγησης του συγκεκριμένου κόμβου. Εντούτοις τα πρωτόκολλα αυτά δεν είναι αποδοτικά σε όλες τις περιπτώσεις και σενάρια

χρήσης, δεδομένου ότι χρησιμοποιούν ένα ουσιαστικό μέρος των πόρων του δικτύου για την διατήρηση και ανανέωση των πληροφοριών δρομολόγησης που γνωρίζουν οι κόμβοι. Για να αντιμετωπίσουν ακριβώς αυτό το μειονέκτημα, τα re-active πρωτόκολλα υιοθετούν την προσέγγιση της εύρεσης μιας διαδρομής για έναν προορισμό μόνο όταν αυτό απαιτείται. Τα re-active πρωτόκολλα καταναλώνουν πολύ λιγότερους πόρους σε σχέση με τα προηγούμενα, αλλά η αρχική καθυστέρηση εύρεσης μιας διαδρομής μπορεί να είναι σημαντικά μεγάλη και μπορεί να είναι, αν όχι μεγαλύτερη, συγκρίσιμη με τον χρόνο που απαιτείται για την μεταφορά των πραγματικών δεδομένων ανάμεσα σε δύο κόμβους. Εν συντομία, μπορούμε να καταλήξουμε στο συμπέρασμα ότι κανένα πρωτόκολλο δεν είναι υλοποιημένο να λειτουργεί το ίδιο αποδοτικά και αποτελεσματικά σε όλα τα πιθανά δικτυακά περιβάλλοντα και γι' αυτό έχουν γίνει προτάσεις που χρησιμοποιούν υβριδικές προσεγγίσεις για την αντιμετώπιση αυτού του προβλήματος.

9.2. Proactive Πρωτόκολλα Δρομολόγησης (Table Driven)

Σε αυτό το τμήμα εξετάζουμε μερικά από τα σημαντικότερα proactive πρωτόκολλα δρομολόγησης.

9.2.1. Destination Sequenced Distance Vector Routing Protocol

Το (DSDV) είναι ένα δυναμικό πρωτόκολλο, που χρησιμοποιεί διανυσματικές αποστάσεις, βάση των συνδέσεων από τις οποίες αποτελείται κάθε διαδρομή, για την δρομολόγηση των δεδομένων σε ένα ad-hoc δίκτυο. Απαιτεί από κάθε κόμβο να μεταδίδει περιοδικά αναπροσαρμοσμένες πληροφορίες δρομολόγησης στους άλλους κόμβους του δικτύου. Κάθε κινητός κόμβος στο δίκτυο, διατηρεί έναν πίνακα δρομολόγησης για όλους τους πιθανούς προορισμούς μέσα στο δίκτυο και τον αριθμό των απαιτούμενων συνδέσεων (hops) προς κάθε προορισμό. Κάθε καταχώρηση στον πίνακα αυτόν είναι μαρκαρισμένη με έναν αριθμό ακολουθίας, που ορίζεται από τον κόμβο προορισμού. Οι αριθμοί ακολουθίας επιτρέπουν στους κόμβους να διακρίνουν τις διαδρομές που είναι αποθηκευμένες και διατηρημένες στους πίνακες δρομολόγησης για μεγάλο χρονικό διάστημα, από τις καινούριες διαδρομές, αποφεύγοντας, παράλληλα, με τον τρόπο αυτόν την δημιουργία βρόχων στα μονοπάτια δρομολόγησης. Περιοδικά, σε όλους τους κόμβους του δικτύου, μεταδίδονται ανανεωμένες πληροφορίες δρομολόγησης με σκοπό την διατήρηση της συνέπειας των δεδομένων που βρίσκονται αποθηκευμένα στους πίνακες δρομολόγησης στους κόμβους του ad-hoc δικτύου.

Για να αποτρέψουν την κυκλοφορία στο δίκτυο μεγάλου όγκου πληροφοριών δρομολόγησης, οι αναπροσαρμογές των διαδρομών μπορούν να χρησιμοποιήσουν δύο τύπους πακέτων για να προωθήσουν στους κόμβους του δικτύου τις νέες πληροφορίες, «πλήρεις μεταδόσεις όλων των καταχωρήσεων ενός πίνακα ή επιλεκτικές μεταδόσεις των νέων καταχωρήσεων των πινάκων δρομολόγησης». Στην πρώτη περίπτωση δημιουργούνται μηνύματα πακέτων που μεταφέρουν όλες τις διαθέσιμες πληροφορίες δρομολόγησης, χρησιμοποιώντας πολλαπλές μονάδες δεδομένων (network protocol data units, NPDUs) για την μετάδοση των πληροφοριών. Τα πακέτα αυτά μεταδίδονται σπάνια και συνήθως κατά την περίοδο μετακίνησης των κόμβων του δικτύου. Στην δεύτερη περίπτωση μεταδίδονται μηνύματα, που περιέχουν μόνο εκείνες τις πληροφορίες δρομολόγησης που έχουν αλλάξει από την τελευταία μετάδοση όλων των καταχωρήσεων των πινάκων

δρομολόγησης. Κάθε μια από αυτές τις μεταδόσεις πρέπει να μπορεί να χρησιμοποιήσει ένα συγκεκριμένο μέγεθος πακέτων NPDU, ούτως ώστε με τον τρόπο αυτό να μειωθεί ο όγκος της κυκλοφορίας που παράγεται. Οι κινητοί κόμβοι διατηρούν έναν πρόσθετο πίνακα όπου αποθηκεύουν τα δεδομένα δρομολόγησης που περιέχονται στα μηνύματα των καινούριων μεταδιδόμενων πληροφοριών δρομολόγησης. Οι μεταδόσεις διαδρομών δρομολόγησης περιέχουν τη διεύθυνση του προορισμού, τον αριθμό των συνδέσεων που απαιτούνται για να φθάσουν στον προορισμό τους, καθώς επίσης και έναν νέο αριθμό μοναδικό για τη κάθε μετάδοση. Η διαδρομή που επιλέγεται να χρησιμοποιηθεί είναι αυτή που περιέχει τον πιο πρόσφατο αριθμό ακολουθίας. Σε περίπτωση που υπάρχουν διαδρομές με τον ίδιο αριθμό ακολουθίας, η διαδρομή με μικρότερο μήκος χρησιμοποιείται ως βέλτιστη.

Οι κόμβοι επίσης παρακολουθούν το χρόνο εγκαθίδρυσης των διαδρομών ή το μέσο σταθμισμένο χρόνο αναμονής των διαδρομών που παραλαμβάνονται για έναν προορισμό, προτού παραληφθεί η καλύτερη διαδρομή. Με τον τρόπο αυτό καθυστερούν την μετάδοσης πληροφοριών δρομολόγησης, μειώνοντας την κυκλοφορία του δικτύου, περιμένοντας να μεταδώσουν διαδρομές που θα μπορούσαν να είναι υποψήφιες για να επιλέγουν, δηλαδή οι κόμβοι αποφεύγουν να μεταδώσουν μια διαδρομή αν πιστεύουν ότι στο άμεσο μέλλον από ένα άλλο κόμβο υπάρχει πολύ μεγαλύτερη πιθανότητα να μεταδοθεί μια καλύτερη διαδρομή.

9.2.2. The Wireless Routing Protocol

Το ασύρματο πρωτόκολλο δρομολόγησης (WRP) είναι ένα πρωτόκολλο που βασίζεται σε πίνακες δρομολόγησης με στόχο την εύρεση και διατήρηση πληροφοριών δρομολόγησης μεταξύ όλων των κόμβων του δικτύου. Κάθε κόμβος στο δίκτυο είναι αρμόδιος για τη διατήρηση τεσσάρων πινάκων: του πίνακα απόστασης, του πίνακας δρομολόγησης, του πίνακα κόστους των συνδέσεων των κόμβων και τέλος ενός πίνακα που περιέχει ένα κατάλογο μηνυμάτων αναμετάδοσης (Message Retransmission List MRL). Κάθε καταχώρηση του MRL περιέχει τον αριθμό ακολουθίας του μηνύματος ενημέρωσης ενός μετρητή αναμετάδοσης, ενός διανύσματος καταχωρήσεων απαιτήσεων επιβεβαιώσεων, μίας για κάθε γειτονικό κόμβο, και ενός καταλόγου ενημερώσεων διαδρομών που περιέχονται στα μηνύματα ενημέρωσης. Για την μετάδοση από ένα κόμβο των αρχείων του MRL στους γείτονες του, μέσω ενός μηνύματος ενημέρωσης, είναι απαραίτητο να λάβει από κάθε κόμβο επιβεβαίωση της ορθής τους μετάδοσης.

Οι κόμβοι ενημερώνουν ο ένας τον άλλο για τις αλλαγές των συνδέσεων μεταξύ τους, λόγω της κινητικότητας, μέσω της χρήσης των μηνυμάτων ενημέρωσης. Ένα μήνυμα ενημέρωσης στέλνεται μόνο μεταξύ γειτονικών κόμβων και περιέχει έναν κατάλογο αναπροσαρμογών (με τον προορισμό, την απόσταση από τον προορισμό, και τον προκάτοχο του προορισμού), καθώς επίσης και έναν κατάλογο με τους κόμβους που πρέπει να απαντήσουν με μια επιβεβαίωση παραλαβής των δεδομένων αυτών (Acks). Μετά την επεξεργασία των νέων πληροφοριών δρομολόγησης από τους γείτονες ή την ανίχνευση μιας αλλαγής σε μια σύνδεση, στέλνονται μηνύματα αναπροσαρμογών στους γείτονες κόμβους, περιέχοντας τις αλλαγές που έχουν ανακαλυφθεί. Σε περίπτωση απώλειας μιας σύνδεσης μεταξύ δύο κόμβων, οι κόμβοι στέλνουν μηνύματα ενημέρωσης στους γείτονές τους. Οι γείτονες τροποποιούν έπειτα τις καταχωρήσεις τους και ελέγχουν για νέες πιθανές διαδρομές μέσω άλλων κόμβων, για κάθε πιθανό προορισμό. Οποιεσδήποτε νέες πορείες ανακαλυφθούν, μεταδίδονται

και αυτές, έτσι ώστε να μπορούν να ενημερώσουν τους πίνακές τους και οι υπόλοιποι κόμβοι του δικτύου, αναλόγως.

Οι κόμβοι μαθαίνουν για την ύπαρξη των γειτόνων τους από την παραλαβή των μηνυμάτων επιβεβαιώσεων ή άλλων μηνυμάτων. Εάν ένας κόμβος δεν μεταδίδει τέτοια μηνύματα, πρέπει να στείλει ένα (HELLO) μήνυμα εντός ενός καθορισμένου χρονικού διαστήματος, για να εξασφαλίσει την διασύνδεση με τους γείτονες του. Διαφορετικά, η έλλειψη μηνυμάτων οποιοδήποτε τύπου από κάποιο κόμβο, δείχνει αποτυχία για εκείνη τη σύνδεση, γεγονός που μπορεί να προκαλέσει ένα λάθος συναγερμό. Όταν ένας κόμβος λαμβάνει ένα (HELLO) μήνυμα από έναν νέο κόμβο του δικτύου, ο νέος κόμβος προστίθεται στον πίνακα δρομολόγησης και λαμβάνει ένα αντίγραφο των πινάκων δρομολόγησής του κόμβου στον οποίο έστειλε αρχικά το (HELLO) μήνυμα.

Μία σημαντική καινοτομία του WRP είναι ο τρόπος με τον οποίο επιτυγχάνει την απομάκρυνση των κυκλικών βρόχων στις διαδρομές δρομολόγησης. Οι κόμβοι που συμμετέχουν στη διαδικασία δρομολόγησης επιβάλλεται να εκτελούν ελέγχους συνέπειας με τις παλιότερες πληροφορίες δρομολόγησης για κάθε διαδρομή, που αναφέρονται από όλους τους γείτονές τους, με αποτέλεσμα να εξαλείφουν οποιουσδήποτε κυκλικές διαδρομές. Ταυτόχρονα παρέχουν την δυνατότητα διόρθωσης μιας διαδρομής μετά από την αποτυχία μίας σύνδεσης πάνω σε αυτή.

9.3. Reactive Πρωτόκολλα Δρομολόγησης (On – Demand)

Σε αυτό το τμήμα περιγράφουμε τα σημαντικότερα reactive πρωτόκολλα δρομολόγησης.

9.3.1. Δυναμική Δρομολόγηση Πηγής (Dynamic Source Routing)

Ο δυναμικός αλγόριθμος δρομολόγησης πηγής (DSR) είναι μια καινοτόμα προσέγγιση στη δρομολόγηση ενός MANET, στην οποία οι κόμβοι επικοινωνούν χρησιμοποιώντας διαδρομές πηγής, που συμπεριλαμβάνονται στα πακέτα δεδομένων και τις οποίες χρησιμοποιούν οι ενδιάμεσοι κόμβοι για να τα προωθήσουν από τον κόμβο προέλευσης στον κόμβο προορισμού. Αναφέρεται ως ένα από τα καλά παραδείγματα reactive πρωτοκόλλου δρομολόγησης. Στον DSR, οι κινητοί κόμβοι διατηρούν Route Caches που περιέχουν καταχωρημένες τις διαδρομές πηγής τις οποίες ο κάθε κόμβος γνωρίζει. Οι καταχωρήσεις στην Route Cache ενημερώνονται συνεχώς καθώς νέες διαδρομές ανακαλύπτονται. Το πρωτόκολλο αποτελείται από δύο μηχανισμούς: τον μηχανισμό εύρεσης διαδρομών και τον μηχανισμό συντήρησης διαδρομών.

Όταν ένας κόμβος επιθυμεί να αποστείλει κάποια δεδομένα, αρχικά προσπαθεί να χρησιμοποιήσει μια διαδρομή που πιθανόν υπάρχει ήδη στην Route Cache του. Εάν μια ισχύουσα διαδρομή για τον συγκεκριμένο προορισμό υπάρχει, θα χρησιμοποιήσει αυτήν την διαδρομή για να μεταδώσει τα δεδομένα. Εάν όμως μια τέτοια διαδρομή δεν υπάρχει στην Route Cache, ενεργοποιείται η διαδικασία εύρεσης διαδρομών με τη μετάδοση ενός μηνύματος αιτήματος μιας νέας διαδρομής. Το μήνυμα αυτό περιέχει τη διεύθυνση προορισμού, μαζί με τη διεύθυνση του κόμβου προέλευσης και έναν μοναδικό αριθμό αναγνώρισης. Κάθε κόμβος που λαμβάνει το πακέτο ελέγχει

εάν έχει αποθηκευμένη μια ισχύουσα διαδρομή για τον συγκεκριμένο προορισμό. Εάν όχι, προσθέτει τη διεύθυνσή του στο πεδίο διευθύνσεων των κόμβων διέλευσης του πακέτου και προωθεί το μήνυμα στους γειτονικούς του κόμβους. Για να περιοριστεί ο αριθμός των μηνυμάτων που διαδίδονται από κάθε κόμβο, ένας κόμβος μεταδίδει ένα τέτοιο μήνυμα μόνο εάν το λάβει για πρώτη φορά και δεν υπάρχει ήδη η διεύθυνση του στο πεδίο διευθύνσεων των κόμβων που έχει επισκεφτεί το μήνυμα. Μια απάντηση σε ένα αίτημα εύρεσης μιας διαδρομής παράγεται, είτε όταν παραληφθεί το εν λόγω μήνυμα από τον κόμβο προορισμού, είτε όταν ένας ενδιάμεσος κόμβος περιέχει στην Route Cache του μια ισχύουσα διαδρομή προς τον προορισμό. Στο πακέτο αποθηκεύεται όλη η αλληλουχία κόμβων από την οποία έχει περάσει το πακέτο, έως ότου φτάσει στον κόμβο προορισμού ή σε έναν ενδιάμεσο κόμβο και δημιουργηθεί μια απάντηση διαδρομής (Route Reply).

Η συντήρηση διαδρομών πραγματοποιείται μέσω της χρήσης πακέτων λαθών (Route Error) σε διαδρομές και των πακέτων επιβεβαιώσεων. Τα πακέτα (Route Error) παράγονται σε έναν κόμβο όταν παρουσιαστεί πρόβλημα στην μετάδοση των δεδομένων στο επίπεδο συνδέσεων του δικτύου. Όταν ένα τέτοιο πακέτο παραληφθεί, η καταχωρημένη διαδρομή στην οποία παρουσιάστηκε το λάθος, καθώς και όλες οι άλλες, που περιέχουν το σύνδεσμο στον οποίο παρουσιάστηκε το πρόβλημα, αφαιρούνται από την Route Cache του κόμβου. Τα πακέτα επιβεβαιώσεων, εν αντιθέσει, καθώς και τα πακέτα παθητικών επιβεβαιώσεων χρησιμοποιούνται για να ελέγξουν τη σωστή λειτουργία των συνδέσεων του δικτύου.

9.3.2. The Ad Hoc On-Demand Distance Vector Routing Protocol

Το πρωτόκολλο δρομολόγησης (AODV) είναι ένας συνδυασμός του πρωτοκόλλου DSDV και του DSR. Δανείζεται το βασικό μηχανισμό ανακάλυψης διαδρομών και συντήρησης διαδρομών από τον DSR και τη χρήση της δρομολόγησης μέσω των συνδέσεων (hop-by-hop), τους αριθμούς ακολουθίας και τα περιοδικά αναγνωριστικά μηνύματα από τον DSDV. Ο AODV ελαχιστοποιεί τον αριθμό των αναγκαίων μεταδόσεων με την εύρεση διαδρομών μόνο κατόπιν παραγγελίας, σε αντιδιαστολή με τη διατήρηση ενός πλήρους καταλόγου διαδρομών προς κάθε πιθανό προορισμό του δικτύου όπως συμβαίνει στον αλγόριθμο DSDV. Ο AODV ταξινομείται ως ένας αλγόριθμος δρομολόγησης που λειτουργεί εξ' ολοκλήρου on-demand, δεδομένου ότι οι κόμβοι, που δεν ανήκουν σε μια συγκεκριμένη διαδρομή, δεν διατηρούν πληροφορίες δρομολόγησης γι' αυτή και δεν συμμετέχουν στη ανταλλαγή πληροφοριών από πίνακες δρομολόγησης. Ο AODV υποστηρίζει μόνο συμμετρικές συνδέσεις και αποτελείται από δύο διαφορετικές φάσεις:

- Ανακάλυψη διαδρομών, συντήρηση διαδρομών, και

- Αποστολή δεδομένων.

Όταν ένας κόμβος επιθυμεί να στείλει ένα μήνυμα και δεν έχει ήδη μια έγκυρη διαδρομή προς τον προορισμό, ενεργοποιεί την διαδικασία εύρεσης διαδρομών για να εντοπίσει τον αντίστοιχο κόμβο προορισμού. Μεταδίδει ένα μήνυμα αιτήματος διαδρομών (RREQ) στους γείτονές του, οι οποίοι το διαβιβάζουν στους δικούς τους γείτονές και ούτως καθ' εξής, μέχρι το αίτημα να προσεγγίσει είτε τον κόμβο προορισμού, είτε έναν ενδιάμεσο κόμβο με μια ισχύουσα διαδρομή προς τον

προορισμό. Ο AODV χρησιμοποιεί αριθμούς ακολουθίας για κάθε προορισμό για να εξασφαλίσει ότι όλες οι διαδρομές δεν περιέχουν βρόχους και περιγράφουν τις πιο πρόσφατες πληροφορίες δρομολόγησης. Κάθε κόμβος διατηρεί τον αριθμό ακολουθίας του, καθώς επίσης και ένα μοναδικό αριθμό ταυτότητας για κάθε μετάδοση, ο οποίος αυξάνεται για κάθε (RREQ) που ο κόμβος στέλνει και μαζί με τη διεύθυνση IP του κόμβου προσδιορίζει μοναδικά κάθε ξεχωριστή μετάδοση δεδομένων προς έναν προορισμό. Μαζί με τον αριθμό ακολουθίας του κόμβου και του μοναδικού αριθμού μετάδοσης για τον συγκεκριμένο προορισμό, το RREQ περιλαμβάνει τον πιο πρόσφατο αριθμό ακολουθίας για τον προορισμό. Οι ενδιάμεσοι κόμβοι μπορούν να απαντήσουν στο RREQ μόνο εάν έχουν μια διαδρομή προς τον προορισμό της οποίας ο αντίστοιχος αριθμός ακολουθίας είναι μεγαλύτερος ή ίσος με αυτόν που υπάρχει στο μήνυμα αιτήματος. Κατά τη διάρκεια της διαδικασίας της εύρεσης μιας διαδρομής, οι ενδιάμεσοι κόμβοι στη διαδρομή καταγράφουν στους πίνακες δρομολόγησης τους τις διευθύνσεις του γείτονα από τον οποίο το πρώτο μήνυμα παραλήφθηκε. Με τον τρόπο αυτόν καθιερώνουν μια αντίστροφη διαδρομή προς τον κόμβο προορισμού του μηνύματος. Τα αντίγραφα του ίδιου RREQ, που πιθανώς να παραληφθούν αργότερα, απορρίπτονται. Μόλις το RREQ φθάσει στον προορισμό ή σε έναν ενδιάμεσο κόμβο με μια ισχύουσα διαδρομή, ο κόμβος αυτός δημιουργεί ένα πακέτο απάντησης (RREP), το οποίο μεταδίδει πίσω στον κόμβο από τον οποίο έλαβε αρχικά το RREQ. Δεδομένου ότι το RREP καθοδηγείται πίσω κατά μήκος της αντίστροφης διαδρομής που έχει δημιουργηθεί από τους ενδιάμεσους κόμβους, οι κόμβοι κατά μήκος της πορείας αυτής, καθώς προωθούν, το πακέτο οργανώνουν τις προς τα εμπρός καταχωρήσεις μονοπατιών στους πίνακες δρομολόγησης τους, που δείχνουν τον κόμβο από τον οποίο το RREP προήλθε. Αυτές οι καταχωρήσεις διαδρομών περιγράφουν την ενεργό διαδρομή δρομολόγησης του συγκεκριμένου RREP. Σε κάθε καταχώρηση μιας διαδρομής στους πίνακες δρομολόγησης αντιστοιχεί ένας χρόνος ζωής διαδρομών, που προκαλεί τη διαγραφή τους από τους πίνακες, εάν αυτές δεν χρησιμοποιηθούν μέσα στο συγκεκριμένο χρονικό διάστημα. Ο λόγος για τον οποίο ο AODV υποστηρίζει μόνο συμμετρικές συνδέσεις είναι ότι το RREP διαβιβάζεται κατά μήκος της πορείας που δημιουργείται από το RREQ.

Οι διαδρομές στον AODV διατηρούνται ως εξής, στις περιπτώσεις που κάποιος κόμβος κατά μήκος της διαδρομής κινείται με αποτέλεσμα η διαδρομή αυτή να μην ισχύει πλέον. Όταν ένας κόμβος προέλευσης μιας διαδρομής κινείται, είναι σε θέση να ενεργοποιήσει ξανά τον μηχανισμό εύρεσης διαδρομών για να ανακαλύψει μια νέα διαδρομή προς τον προορισμό. Εάν ένας κόμβος κατά μήκος της διαδρομής κινείται, ο προς τα πάνω (upstream) γείτονάς του παρατηρεί την κίνηση του και διαδίδει ένα μήνυμα ανακοίνωσης αποτυχίας της σύνδεσης (RREP with infinite metric) σε κάθε ένας από τους ενεργούς προς τα πάνω (upstream) γείτονές του, για να τους ενημερώσει για τη κατάρρευση του συγκεκριμένου μέρους της διαδρομής. Οι κόμβοι αυτοί διαδίδουν στη συνέχεια το μήνυμα κατάρρευσης των συνδέσεων στους προς τα πάνω γείτονές τους και η διαδικασία αυτή συνεχίζεται έως ότου το μήνυμα το λάβει ο κόμβος πηγή της συγκεκριμένης διαδρομής. Ο κόμβος αυτός έπειτα ενεργοποιεί, αν το κρίνει απαραίτητο και αναγκαίο να διατηρήσει μια διαδρομή για τον συγκεκριμένο προορισμό, τον μηχανισμό εύρεσης διαδρομών του πρωτοκόλλου. Ένα ακόμα χαρακτηριστικό του πρωτοκόλλου είναι η χρήση μηνυμάτων (HELLO), με περιοδικές τοπικές μεταδόσεις από έναν κόμβο για να ενημερώσει κάθε άλλο κινούμενο κόμβο για την παρουσία άλλων κόμβων στην περιοχή εμβέλειας του. Τα μηνύματα αυτά μπορούν να χρησιμοποιηθούν για να διατηρήσουν την τοπική συνδεσιμότητα ενός

κόμβου με τους γείτονες του. Εντούτοις, η χρήση αυτών των μηνυμάτων δεν είναι απαραίτητη σε όλες τις περιπτώσεις, αφού οι κόμβοι «ακούγοντας» τις αναμεταδώσεις των πακέτων δεδομένων μπορούν να εξασφαλίσουν την διασύνδεση τους με τους γειτονικούς τους κόμβους. Γενικά τόσο από τα πακέτα δεδομένων που προωθούνται από έναν κόμβο ή μπορούν να ληφθούν χωρίς να προορίζονται γι' αυτόν, όσο και ειδικά μηνύματα, όπως τα (HELLO) μηνύματα, χρησιμοποιούνται για να μπορούν οι κόμβοι ενός ad-hoc δικτύου να αποκτούν μια όσο το δυνατόν καλύτερη εικόνα για το ίδιο το δίκτυο, τους γείτονες τους και τις ενεργές συνδέσεις τους.

9.3.3. Associativity Based Routing

Το πρωτόκολλο ABR, είναι μια διαφορετική προσέγγιση στην δρομολόγηση ad-hoc ασύρματων δικτύων. Στις διαδρομές που ανακαλύπτει είναι απαλλαγμένο από βρόχους, αδιέξοδα (deadlocks), παραλαβή διπλών πακέτων και καθορίζει μια νέα τεχνική δρομολόγησης για τα ad-hoc ασύρματα δίκτυα. Στο ABR, μια διαδρομή επιλέγεται βασιζόμενη σε ένα παράγοντα που είναι γνωστός ως βαθμός συσχέτισης της ευστάθειας (degree of association stability). Κάθε κόμβος παράγει περιοδικά ένα αναγνωριστικό μήνυμα για να δηλώσει την ύπαρξή του στους υπόλοιπους κόμβους του δικτύου. Όταν το μήνυμα αυτό παραλαμβάνεται από τους γειτονικούς κόμβους, αναγκάζει τους πίνακες συσχέτισης να ενημερωθούν. Η συσχέτιση της ευστάθειας καθορίζεται από τη σταθερότητα σύνδεσης ενός κόμβου όσον αφορά έναν άλλο κόμβο στο χρόνο και στο χώρο. Ένας υψηλός (χαμηλός) βαθμός συσχέτισης της ευστάθειας μπορεί να δείξει μια χαμηλή (υψηλή) κατάσταση κινητικότητας των κόμβων. Οι δείκτες καταγραφής ρυθμίζονται ξανά όταν κινούνται οι γείτονες ενός κόμβου ή ο ίδιος ο κόμβος απομακρύνεται. Ένας θεμελιώδης στόχος είναι να παραχθούν διαδρομές που έχουν μεγάλο χρόνο ζωής για τα ειδικά δίκτυα. Οι τρεις φάσεις του ABR είναι: Ανακάλυψη διαδρομών, Αναδημιουργία διαδρομών (RRC) και Διαγραφή διαδρομών.

Η φάση ανακάλυψης διαδρομών υλοποιείται από μια συνεχή διαδικασία μετάδοσης μιας ερώτησης και αναμονή μιας απάντησης (Broadcast Query Reply, BQ-REPLY). Ένας κόμβος που επιθυμεί μια διαδρομή μεταδίδει ένα μήνυμα BQ σε αναζήτηση των κόμβων που έχουν μια διαδρομή προς τον προορισμό. Όλοι οι κόμβοι που λαμβάνουν την ερώτηση (χωρίς να είναι ο τελικός προορισμός του μηνύματος) επισυνάπτουν τις διευθύνσεις τους και τους δείκτες συσχέτισης τους, σε σχέση με τους γείτονές τους, μαζί με πληροφορίες ποιότητας των συνδέσεων QoS στο πακέτο ερώτησης. Ο κόμβος στον οποίο προωθείται το μήνυμα σβήνει τις καταχωρήσεις των δεικτών συσχέτισης των προς τα πάνω γειτόνων κόμβων του και διατηρεί μόνο αυτές τις καταχωρίσεις που συσχετίζονται με αυτόν και τους κόμβους που είναι αντίθετα με την κατεύθυνση προώθησης του μηνύματος. Κατ' αυτό τον τρόπο, κάθε πακέτο που φθάνει στον προορισμό περιέχει τους δείκτες συσχέτισης των κόμβων κατά μήκος της διαδρομής. Ο κόμβος προορισμού έπειτα είναι ικανός να επιλέξει την καλύτερη διαδρομή με την εξέταση των δεικτών συσχέτισης κατά μήκος κάθε μίας από τις διαδρομές. Όταν οι πολλαπλές διαδρομές έχουν τον ίδιο γενικό βαθμό συσχέτισης ευστάθειας, η διαδρομή με τον ελάχιστο αριθμό συνδέσμων επιλέγεται. Ο προορισμός στέλνει έπειτα ένα πακέτο απάντησης πίσω στον κόμβο προέλευσης. Οι κόμβοι που προωθούν το μήνυμα αυτό χαρακτηρίζουν τις διαδρομές τους ως έγκυρες. Όλες οι άλλες διαδρομές παραμένουν ανενεργές, με αποτέλεσμα να αποφεύγεται η αποστολή διπλών πακέτων να φθάνουν στον προορισμό.

9.4. Flow Oriented Routing

9.4.1. Relative Distance Micro Discovery Ad-Hoc Routing

Το πρωτόκολλο δρομολόγησης RDMAR είναι ένα ιδιαίτερα προσαρμοστικό και αποδοτικό πρωτόκολλο. Μπορεί να λειτουργήσει αρκετά ικανοποιητικά σε μεγάλα ασύρματα ad-hoc δίκτυα στα οποία παρατηρείται μέτρια κινητικότητα. Βασική σχεδιαστική αρχή του πρωτοκόλλου είναι η αντίδραση του στην διακοπή της ενεργής λειτουργίας αποτυχημένων συνδέσεων, σε μια πολύ μικρή περιοχή του δικτύου κοντά στο σημείο της αλλαγής των συνδέσεων του δικτύου. Η συμπεριφορά αυτή επιτυγχάνεται μέσω της χρήσης ενός νέου μηχανισμού για την ανακάλυψη διαδρομών, αποκαλούμενου Relative Distance Micro-Discovery (RDM), ο οποίος έχει σαν βασικής έννοια την δημιουργία μηνυμάτων, ως αντίδρασης του πρωτοκόλλου σε ένα γεγονός και την διάδοση τους με την μορφή πλημμύρας, η οποία μπορεί να περιοριστεί χρησιμοποιώντας την σχετική απόσταση (RD) μεταξύ δύο τερματικών. Κάθε φορά που προκαλείται μια αναζήτηση διαδρομών μεταξύ των δύο τερματικών, ένας επαναληπτικός αλγόριθμος υπολογίζει μια εκτίμηση της σχετικής τους απόστασης, λαμβάνοντας υπόψη ένα μέσο ρυθμό κινητικότητας, πληροφορίες για την περίοδο που έχει παρέλθει από την πιο πρόσφατη επικοινωνίας τους και τις προηγούμενες τιμές της. Το μήνυμα ερώτησης (query) το οποίο δημιουργείται βασισμένο στο υπολογισμένο αυτό RD, προωθείται με την τεχνική της πλημμύρας σε όλους του κόμβους του δικτύου σε μια περιοχή η οποία κεντροθετείται στον κόμβο πηγής του αιτήματος ευρέσεως διαδρομών και με μέγιστη ακτίνα διάδοσης ίση με την κατ' εκτίμηση σχετική απόσταση RD. Η παραπάνω διαδικασία χρησιμεύει για να ελαχιστοποιηθεί η συμφόρηση του δικτύου και η συνολική καθυστέρηση που προκαλείται από το πρωτόκολλο δρομολόγησης.

Στο RDMAR, τα δεδομένα δρομολογούνται μεταξύ των κόμβων του δικτύου με τη χρησιμοποίηση πινάκων δρομολόγησης αποθηκευμένων σε κάθε κόμβο. Κάθε κόμβος έχει το ρόλο τόσο του τερματικού όσο και του δρομολογητή. Κάθε πίνακας δρομολόγησης περιέχει πληροφορίες για όλους ξεχωριστά τους πιθανούς προορισμούς στο δίκτυο. Κάθε καταχώρηση στον πίνακα αυτόν περιέχει τον επόμενο κόμβο, στον οποίο πρέπει να μεταδοθούν τα δεδομένα για να μπορέσουν να προωθηθούν στον τελικό προορισμό τους. Η σχετική απόσταση (Relative Distance RD) περιέχει μια προσέγγιση της απόστασης, εκφρασμένη σε πλήθος συνδέσεων (hops), ανάμεσα στον κόμβο αυτό και τον κόμβο προορισμού και τον χρόνο (Time Last Update TLU) από την τελευταία φορά που ο κόμβος είχε λάβει πληροφορίες δρομολόγησης για τον συγκεκριμένο προορισμό. Μία μεταβλητή που ονομάζεται (RT_Timeout) περιέχει το χρονικό διάστημα που απομένει προτού θεωρηθεί η συγκεκριμένη διαδρομή άκυρη και τέλος έναν αναγνωριστικό αριθμό που (Route Flag), που δηλώνει εάν η διαδρομή είναι ενεργή. Ο RDMAR περιλαμβάνει δύο κύριους μηχανισμούς:

- Εύρεση διαδρομών — Όταν φθάνει μια αίτηση σε έναν κόμβο για μια διαδρομή προς ένα άλλο κόμβο και δεν υπάρχει διαθέσιμη κάποια διαδρομή, ενεργοποιείται ο μηχανισμός εύρεσης διαδρομών του πρωτοκόλλου. Το μήνυμα αίτησης για την νέα διαδρομή μπορεί, είτε να διαδοθεί με την τεχνική της πλημμύρας σε όλους του κόμβους του δικτύου, είτε να περιοριστεί η μετάδοση του μηνύματος σε μια συγκεκριμένη περιοχή, βάση μιας πρόβλεψης

της θέσης του κόμβου προορισμού, που γίνεται με τον υπολογισμό μιας πρόβλεψης, για την απόσταση του κόμβου προορισμού από τις πληροφορίες που υπάρχουν στους πίνακες δρομολόγησης.

- Συντήρηση διαδρομών — Ένας ενδιάμεσος κόμβος, κατά την υποδοχή ενός πακέτου δεδομένων, επεξεργάζεται αρχικά τις πληροφορίες δρομολόγησης και τις διαβιβάζει έπειτα στον επόμενο κόμβο. Στη συνέχεια μεταδίδει ένα μήνυμα με σκοπό να εξετάζει εάν μια αμφίδρομη σύνδεση, με ένα προηγούμενο κόμβο, είναι εφικτή. Ο RDMAR επομένως, δεν υποθέτει την ύπαρξη αμφίδρομων συνδέσεων αλλά παρόλα αυτά εξετάζει τη δυνατότητα αυτή. Κατά τον τρόπο αυτό, οι κόμβοι που προωθούν ένα πακέτο δεδομένων έχουν πάντα αρκετές πληροφορίες δρομολόγησης για να στείλουν ένα μελλοντικό πακέτο επιβεβαίωσης πίσω στην πηγή. Εάν η προώθηση του πακέτου δεδομένων, είτε λόγω κάποιου λάθους που υπάρχει στις συνδέσεις της διαδρομής, είτε λόγω του ότι δεν υπάρχει καμία διαθέσιμη διαδρομή, αποτύχει, η διαδικασία επαναλαμβάνεται μέχρι έναν μέγιστο αριθμό και στη συνέχεια εάν η αποτυχία εμμένει, ενεργοποιείται η διαδικασία εύρεσης διαδρομών.

9.4.2. Signal Stability Routing (SSR)

Είναι ένα on-demand πρωτόκολλο δρομολόγησης. Αντίθετα από τους αλγορίθμους που περιγράφηκαν μέχρι τώρα, το SSR επιλέγει διαδρομές βασισμένες στην ισχύ των σημάτων των ασύρματων πομποδεκτών μεταξύ των κόμβων και στην σταθερότητα διατήρησης της θέσης από τους κόμβους του δικτύου. Οι εντάσεις των σημάτων των γειτονικών κόμβων λαμβάνονται από περιοδικά αναγνωριστικά μηνύματα από το επίπεδο συνδέσεων κάθε κόμβου. Αυτό το κριτήριο επιλογής διαδρομών SSR έχει την επίδραση της επιλογής διαδρομών που αποτελούνται από συνδέσεις που έχουν «stronger connectivity).

9.5. Πρωτόκολλα Adaptive Routing (Situation-Aware) - Δρομολόγηση Αναστροφής Συνδέσεων

Στην παράγραφο αυτή θα περιγράψουμε το σημαντικότερο πρωτόκολλο αυτής της οικογένειας το οποίο ονομάζεται TORA (Temporally Ordered Routing Algorithm).

Ο αλγόριθμος δρομολόγησης (TORA) είναι ένας ιδιαίτερα προσαρμοστικός, κατανεμημένος αλγόριθμος βασισμένος στην έννοια της αντιστροφής συνδέσεων, ο οποίος διαθέτει ειδικό μηχανισμό εξάλειψης βρόγχων μέσα στις διαδρομές, έχοντας ως σκοπό την ελαχιστοποίηση των αντιδράσεων στις τοπολογικές αλλαγές του δικτύου.

Μια βασική σχεδιαστική αρχή του αλγορίθμου είναι ότι προσπαθεί να αντιμετωπίσει την κινητικότητα και την αλλαγή της τοπολογία των κόμβων, απομονώνοντας τους κόμβους του δικτύου που δεν αφορά ούτε και επηρεάζει αυτή η αλλαγή. Αυτό έχει σαν αποτέλεσμα οι τυχών αλλαγές στην τοπολογία του δικτύου που συμβαίνουν σε μια συγκεκριμένη περιοχή να επηρεάζουν μια μικρή ομάδα κοντινών κόμβων και όχι τους απομακρυσμένους. Η ανταλλαγή μηνυμάτων ελέγχου δρομολόγησης λοιπόν σε μια περιορισμένη ομάδα κόμβων, που βρίσκονται κοντά στην αλλαγή, έχει ως αποτέλεσμα την καλύτερη απόδοση του πρωτοκόλλου και την αποφυγή χρήσης

ιεραρχικών αλγορίθμων δρομολόγησης που θα προσέθεταν έξτρα πολυπλοκότητα. Η εύρεση των καλύτερων διαδρομών θεωρείται δευτερεύουσας σημασίας και πολύ συχνά δεν χρησιμοποιούνται οι βέλτιστες διαδρομές, εάν η διαδικασία εύρεσης νέων διαδρομών είναι δυνατόν να αποφευχθεί. Τέλος το πρωτόκολλο αυτό χαρακτηρίζεται και από την ικανότητα δρομολόγησης μέσω πολλαπλών διαδρομών.

Το TORA είναι ικανό να λειτουργήσει σε ένα ιδιαίτερα δυναμικό περιβάλλον όπως συνήθως είναι ένα ασύρματο ad-hoc δίκτυο με κινούμενους κόμβους. Η διαδικασία δρομολόγησης ξεκινά σε όλες τις περιπτώσεις από έναν κόμβο (source node). Οι κόμβοι πρέπει να διατηρούν τις πληροφορίες δρομολόγησης για τους παρακείμενους κόμβους (γειτονικούς κόμβους). Το πρωτόκολλο εκτελεί τρεις βασικές λειτουργίες:

- Δημιουργία διαδρομών,
- Συντήρηση διαδρομών, και
- Εξάλειψη διαδρομών.

Για κάθε κόμβο στο δίκτυο, ένας ξεχωριστός κατευθυνόμενος μη-κυκλικός γράφος (Directed Acyclic Graph DAG) διατηρείται για κάθε προορισμό. Όταν ένας κόμβος αποφασίσει ότι χρειάζεται μια διαδρομή για κάποιον προορισμό, διαδίδει προς όλους τους κόμβους του δικτύου ένα μήνυμα αναζήτησης (Query), που περιέχει τη διεύθυνση του προορισμού για τον οποίο απαιτεί μια διαδρομή. Αυτό το πακέτο προωθείται από κόμβο σε κόμβο, έως ότου φθάσει είτε στον κόμβο προορισμού, είτε σε έναν ενδιάμεσο κόμβο που έχει αποθηκευμένη μια διαδρομή προς τον προορισμό. Ο παραλήπτης του μηνύματος αυτού μεταδίδει ένα μήνυμα ενημέρωσης (Update), που απαριθμεί το ύψος που γνωρίζει σε σχέση με τον κόμβο προορισμού. Καθώς το μήνυμα αυτό προωθείται στο δίκτυο, κάθε κόμβος που το λαμβάνει ρυθμίζει το δικό του ύψος προς το συγκεκριμένο προορισμό κατά μία μονάδα μεγαλύτερο από το ύψος του γειτονικού του κόμβου από τον οποίο το έλαβε. Η διαδικασία αυτή έχει σαν αποτέλεσμα την δημιουργία μιας σειράς κατευθυνόμενων συνδέσεων από τον αρχικό αποστολέα της αναζήτησης της διαδρομής, προς τον κόμβο που παρήγαγε το μήνυμα ενημέρωσης (Update). Όταν ένας κόμβος αντιληφθεί ότι μια διαδρομή προς ένα συγκεκριμένο προορισμό δεν ισχύει πλέον, αναπροσαρμόζει το ύψος που έχει αποθηκεύσει γι' αυτή την διαδρομή στο μέγιστο που μπορεί να υπολογίσει από τις πληροφορίες που έχει συλλέξει από τους γείτονες του και διαδίδει στη συνέχει ένα μήνυμα (Update). Εάν ο κόμβος δεν έχει κάποιον γείτονα που μπορεί να τον πληροφορήσει για το ύψος προς τον συγκεκριμένο προορισμό, ενεργοποιεί την διαδικασία εύρεσης μιας νέας διαδρομής, όπως περιγράφεται ανωτέρω. Όταν ένας κόμβος ανιχνεύσει την κατάτμηση του δικτύου, δημιουργεί ένα μήνυμα καθαρίσματος (Clear) που ρυθμίζει εκ νέου την κατάσταση των διαδρομών και διαγράφει διαδρομές που πλέον δεν είναι ενεργές.

Το TORA είναι υλοποιημένο πάνω από το επίπεδο του IMEP το πρωτόκολλο ενθυλάκωσης των MANET, το οποίο εγγυάται τη με σειρά αξιόπιστη παράδοση όλων των μηνυμάτων ελέγχου της διαδικασίας της δρομολόγησης από έναν κόμβο σε κάθε ένα από τους γείτονές του και την ειδοποίηση για την δημιουργία μιας νέας ή την κατάργηση μιας παλιάς σύνδεσης με ένα γειτονικό κόμβο, στο επίπεδο του πρωτοκόλλου δρομολόγησης. Για να μειώσει την καθυστέρηση, το IMEP προσπαθεί να ομαδοποιήσει πολλά μηνύματα ελέγχου του TORA και του ίδιου του IMEP (τα

οποία αναφέρονται ως αντικείμενα) σε ένα ενιαίο πακέτο πριν από κάθε μετάδοση. Κάθε τέτοιο πακέτο φέρνει έναν αριθμό ακολουθίας και έναν κατάλογο άλλων κόμβων από τους οποίους απαιτείται μία λήψη επιβεβαίωσης. Το IMEP μεταδίδει κάθε ίδιο τέτοιο πακέτο περιοδικά και συνεχίζει να το μεταδίδει, εάν είναι απαραίτητο, για κάποια περίοδο, μετά το πέρας της οποίας το TORA ενημερώνεται για όλες τις συνδέσεις που δεν ισχύουν πλέον, λόγω του ότι δεν έχει ληφθεί κάποια επιβεβαίωση.

Όπως αναφέραμε νωρίτερα, κατά τη διάρκεια της δημιουργίας και συντήρησης διαδρομών, οι κόμβοι χρησιμοποιούν το «ύψος» σαν μέτρο εγκαθίδρυσης ενός κατευθυντικού μη κυκλικού γράφου διαδρομών, (DAG) προς τον προορισμό. Στις συνδέσεις, μετά από αυτή τη διαδικασία, ορίζεται μια κατεύθυνση (προς τα πάνω ή προς τα κάτω) βασισμένη με το σχετικό ύψος των γειτονικών κόμβων. Σε περιόδους κινητικότητας των κόμβων ο γράφος διαδρομών DAG περιέχει μη συνεπείς πληροφορίες και η διαδικασία συντήρησης διαδρομών είναι απαραίτητη για να εγκαθιδρύσει ξανά ένα γράφο διαδρομών, ο οποίος περιέχει τις νέες πληροφορίες δρομολόγησης.

Ο συγχρονισμός είναι ένας σημαντικός παράγοντας στο πρωτόκολλο TORA, επειδή το «ύψος» εξαρτάται από το χρόνο αποτυχίας των συνδέσεων. Το TORA υποθέτει ότι όλοι οι κόμβοι έχουν συγχρονίσει τα ρολόγια τους, χρησιμοποιώντας μια αρκετά αξιόπιστη υπηρεσία συγχρονισμού, όπως είναι το GPS (Global Positioning System). Οι παράγοντες που χρησιμοποιούνται από το TORA σαν μέτρο για τις διαδικασίες δρομολόγησης και διατήρησης των διαδρομών είναι οι εξής πέντε:

1. Λογικός χρόνος αποτυχίας μιας σύνδεσης,
2. Η μοναδική ταυτότητα του κόμβου που καθόρισε το νέο επίπεδο αναφοράς,
3. Ένα bit που περιγράφει ένα δείκτη αντανάκλασης,
4. Μια παράμετρος διάδοσης,
5. Η μοναδική ταυτότητα του κόμβου.

Το TORA είναι ένα πρωτόκολλο μερικώς reactive και μερικώς proactive. Είναι reactive υπό την έννοια ότι η διαδικασία εύρεσης διαδρομών αρχίζει μετά από σχετική αίτηση κάποιου κόμβου. Εντούτοις, η συντήρηση των διαδρομών γίνεται proactive έτσι ώστε οι πολλαπλάσιες επιλογές δρομολόγησης να είναι διαθέσιμες και έγκυρες σε περίπτωση ύπαρξης αποτυχημένων συνδέσεων.

9.6. Υβριδικά Πρωτόκολλα Δρομολόγησης

9.6.1. Πρωτόκολλο Δρομολόγησης Ζώνης (Zone Routing Protocol)

Το πρωτόκολλο δρομολόγησης ζώνης (ZRP) είναι ένα υβριδικό παράδειγμα reactive και proactive δρομολόγησης. Περιορίζει το πεδίο της proactive διαδικασίας μόνο στην περιοχή όπου βρίσκονται οι γείτονες ενός κόμβου, ενώ η αναζήτηση σε όλο το δίκτυο μπορεί να εκτελεστεί αποτελεσματικά με τη αναζήτηση συγκεκριμένων κόμβων μετά από σχετικό αίτημα, όπως σε ένα reactive πρωτόκολλο.

Στο ZRP, ένας κόμβος διατηρεί proactively διαδρομές προς τους κόμβους προορισμούς μέσα σε μια περιοχή, η οποία αναφέρεται ως ζώνη δρομολόγησης και ορίζεται ως μια συλλογή των κόμβων, των οποίων η ελάχιστη απόσταση συνδέσεων από τον εν λόγω κόμβο δεν είναι μεγαλύτερη από μια παράμετρο, καλούμενη ακτίνα

ζώνης. Κάθε κόμβος διατηρεί την ακτίνα ζώνης του. Από το πρωτόκολλο επιτρέπεται και επιβάλλετε να υπάρχει μια επικάλυψη γειτονικών ζωνών.

Η κατασκευή μιας ζώνης δρομολόγησης απαιτεί ένας κόμβος να γνωρίζει ποιοι είναι οι γείτονές του. Ένας γείτονας ορίζεται ως ένας κόμβος που μπορεί να επικοινωνήσει άμεσα με τον εν λόγω κόμβο και ανακαλύπτεται μέσω ενός πρωτοκόλλου ανακαλύψεως γειτόνων του επιπέδου MAC (Neighbor Discovery Protocol NDP). Το ZRP διατηρεί τις ζώνες δρομολόγησης μέσω ενός proactive πρωτοκόλλου καλούμενου (Intrazone Routing Protocol IARP), που υλοποιείται ως ένα τροποποιημένο διανυσματικό σχήμα απόστασης. Το πρωτόκολλο αυτό είναι αρμόδιο για την εύρεση των διαδρομών για τους προορισμούς που βρίσκονται έξω από τη ζώνη δρομολόγησης. Το IERP χρησιμοποιεί έναν μηχανισμό ερώτησης και απάντησης (query-response) για να ανακαλύψει τις διαδρομές μετά από σχετική αίτηση κάποιου κόμβου. Το IERP διακρίνεται από τον κλασικό αλγόριθμο πλημμύρας λόγω της χρησιμοποίηση διαδικασίας προώθησης μηνυμάτων γνωστής ως border casting. Το ZRP παρέχει αυτήν την υπηρεσία μέσω μιας διεργασίας αποκαλούμενης, (Border Resolution Protocol BRP).

Το στρώμα δικτύου προκαλεί μία IERP ανακάλυψη διαδρομών όταν ένα πακέτο στοιχείων πρόκειται να σταλεί σε έναν προορισμό που δεν βρίσκεται μέσα στη ζώνη δρομολόγησής του. Η πηγή παράγει ένα μήνυμα αναζήτησης διαδρομών, το οποίο προσδιορίζεται μεμονωμένα από έναν αριθμό ταυτότητας και έναν αριθμό αιτήματος του κόμβου πηγής. Η ερώτηση έπειτα μεταδίδεται στους απομακρυσμένους κόμβους από την ζώνη δρομολόγησης. Κατά την παραλαβή ενός τέτοιου πακέτου, ένας κόμβος προσθέτει τον δικό του αριθμό ταυτότητας. Η ακολουθία των καταγραμμένων αριθμών αυτών διευκρινίζει μια διαδρομή από την πηγή στην τρέχουσα ζώνη δρομολόγησης. Εάν ο προορισμός δεν εμφανίζεται στη τρέχουσα ζώνη δρομολόγησης, το μήνυμα αυτό προωθείται στους απομακρυσμένους κόμβους της ζώνης δρομολόγησης. Εάν ο κόμβος προορισμού είναι μέλος της τρέχουσας ζώνης δρομολόγησης, αποστέλλεται πίσω στην πηγή μια απάντηση που περιέχει την συγκεκριμένη διαδρομή, ακολουθώντας απλά την αντίστροφη διαδρομή από αυτή που περιέχει. Ένας κόμβος θα απορρίψει οποιοδήποτε μήνυμα αναζήτησης διαδρομών, το οποίο έχει επεξεργαστεί ξανά. Ένα σημαντικό χαρακτηριστικό αυτής της διαδικασίας είναι ότι μια μοναδική αναζήτηση διαδρομών μπορεί να επιστρέψει πολλαπλές απαντήσεις με διαδρομές για τον προορισμό, δίνοντας την δυνατότητα επιλογής της καλύτερης από αυτές στους κόμβους, βάση κάποιων χαρακτηριστικών της ποιότητας τους.

9.6.2. Landmark Routing (LANMAR) for MANET with Group Mobility

Το πρωτόκολλο δρομολόγησης (LANMAR) συνδυάζει τα χαρακτηριστικά γνωρίσματα του FSR και της διαδικασίας δρομολόγησης Landmark. Η βασική καινοτομία είναι η χρήση ορόσημων για κάθε σύνολο κόμβων που κινούνται ως ομάδα (όπως, μια ομάδα στρατιωτών στο πεδίο της μάχης) προκειμένου να μειωθεί η συνολική καθυστέρηση δρομολόγησης. Όπως και στον FSR, οι κόμβοι ανταλλάσσουν πληροφορίες μόνο με τους γειτονικούς τους κόμβους. Οι διαδρομές στο πλαίσιο του Fisheye είναι ακριβείς, ενώ οι διαδρομές στις μακρινές ομάδες κόμβων «συνοψίζονται» (summarized) από τα αντίστοιχα ορόσημα. Ένα πακέτο που κατευθύνεται σε έναν μακρινό προορισμό στοχεύει αρχικά προς το αντίστοιχο

ορόσημο της απομακρυσμένης ομάδας κόμβων και καθώς πλησιάζει πιο κοντά στον προορισμό χρησιμοποιεί τελικά μια πιο συγκεκριμένη διαδρομή που παρέχεται από το Fisheye. Στο αρχικό σχήμα ενσύρματων δικτύων με ορόσημα, η προκαθορισμένη διεύθυνση κάθε κόμβου απεικονίζει τη θέση του μέσα στην ιεραρχία και βοηθά την εύρεση μιας διαδρομής σε αυτόν. Κάθε κόμβος γνωρίζει τις διαδρομές προς όλους τους άλλους κόμβους μέσα στο ιεραρχικό σχήμα. Επιπλέον, κάθε κόμβος γνωρίζει τις διαδρομές προς τα διάφορα "ορόσημα" σε διαφορετικά ιεραρχικά επίπεδα. Η αποστολή πακέτων είναι σύμφωνη με την ιεραρχία ορόσημων και η πορεία καθορίζεται από την ιεραρχία υψηλότερου επιπέδου στα χαμηλότερα επίπεδα καθώς ένα πακέτο πλησιάζει προς τον προορισμό.

Το LANMAR δανείζεται την έννοια των ορόσημων για να παρακολουθήσει τα λογικά υποδίκτυα. Ένα υποδίκτυο αποτελείται από μέλη που έχουν κοινά ενδιαφέροντα και είναι πιθανόν να κινηθούν ως "ομάδα" (όπως, στρατιώτες στο πεδίο μάχης, ή μια ομάδα σπουδαστών). Ένας κόμβος "ορόσημων" εκλέγεται σε κάθε υποδίκτυο. Το ίδιο το σχέδιο δρομολόγησης είναι τροποποιημένη έκδοση του FSR. Η κύρια διαφορά όμως είναι ότι ο πίνακας δρομολόγησης του FSR περιέχει όλους τους κόμβους στο δίκτυο, ενώ ο πίνακας δρομολόγησης στο LANMAR περιλαμβάνει μόνο τους κόμβους άμεσου ενδιαφέροντος και τους κόμβους ορόσημων (landmark nodes). Αυτό το χαρακτηριστικό γνώρισμα βελτιώνει πολύ την κλιμάκωση του πρωτοκόλλου με τη μείωση του μεγέθους των πινάκων δρομολόγησης και την συνολικής κυκλοφορίας των δεδομένων στο δίκτυο. Όταν ένας κόμβος πρέπει να αναμεταδώσει ένα πακέτο, εάν ο προορισμός είναι ένας από τους γείτονες του, η διεύθυνση βρίσκεται στον πίνακα δρομολόγησης και το πακέτο διαβιβάζεται άμεσα. Διαφορετικά, το υποδίκτυο που πιθανά βρίσκεται ο προορισμός αναζητάτε και το πακέτο καθοδηγείται προς το αντίστοιχο ορόσημο εκείνου του υποδικτύου. Το πακέτο εντούτοις δεν είναι αναγκαίο να περάσει μέσω του κόμβου ορόσημου αλλά μπορεί να προωθηθεί άμεσα στον προορισμό, μόλις φτάσει κοντά στο συγκεκριμένο υποδίκτυο.

Η ανταλλαγή ανανεωμένων πληροφοριών δρομολόγησης στο LANMAR είναι παρόμοια με του FSR. Κάθε κόμβος ανταλλάσσει περιοδικά πληροφορίες τοπολογίας με τους γείτονές του. Σε κάθε αναπροσαρμογή, ο κόμβος στέλνει τις νέες καταχωρήσεις στο πεδίο Fisheye του, συμπεριλαμβάνοντας επίσης στο μήνυμα αυτό ένα διάνυσμα απόστασης με μέγεθος ίσο με τον αριθμό των λογικών υποδικτύων (δηλ, των κόμβων ορόσημων). Μέσω αυτής της διαδικασίας ανταλλαγής, οι καταχωρήσεις στους πίνακες δρομολόγησης με τους μεγαλύτερους αριθμούς ακολουθίας αντικαθιστούν αυτούς με τους μικρότερους.

9.7. Ιεραρχικά Πρωτόκολλα Δρομολόγησης

9.7.1. Fisheye State Routing (FSR)

Το πρωτόκολλο (FSR) εισάγει την έννοια ενός πολύ-επίπεδου fisheye σχήματος για να μειώσει την συνολική καθυστέρηση της διαδικασίας της δρομολόγησης σε μεγάλα ασύρματα ad-hoc δίκτυα. Οι κόμβοι ανταλλάσσουν τις καταχωρήσεις κατάστασης συνδέσεων με τους γείτονές τους με μια συχνότητα που εξαρτάται από την απόσταση στον προορισμό. Από τις καταχωρήσεις της κατάστασης των συνδέσεων, οι κόμβοι κατασκευάζουν το χάρτη τοπολογίας ολόκληρου του δικτύου και υπολογίζουν τις βέλτιστες διαδρομές. Ο FSR προσπαθεί να βελτιώσει την κλιμάκωση ενός

πρωτοκόλλου δρομολόγησης με την προσπάθεια για συγκέντρωση των πληροφοριών της τοπολογίας των κόμβων του δικτύου, που είναι οι πλέον πιθανές να απαιτηθούν για την δρομολόγηση δεδομένων προς αυτούς. Υποθέτει ότι αλλαγές, που στην τοπολογία του τμήματος του δικτύου βρίσκονται κοντύτερα σε έναν κόμβο, είναι πιθανότερο να πρέπει να επεξεργαστούν για την ανανέωση των πληροφοριών δρομολόγησης που κατέχει ο κόμβος αυτός, από ότι οι αλλαγές που συμβαίνουν μακριά από αυτόν. Το πρωτόκολλο φροντίζει να ενημερώνονται συχνότερα, για τις αλλαγές του δικτύου, οι κόμβοι που βρίσκονται κοντύτερα σε αυτές.

9.8. Γεωγραφικά Πρωτόκολλα Δρομολόγησης

9.8.1. Location Aided Routing (LAR)

Το πρωτόκολλο δρομολόγησης LAR εκμεταλλεύεται τις πληροφορίες θέσεως των κόμβων στο δίκτυο, τις οποίες χρησιμοποιεί για να περιορίσει το πεδίο της πλημμύρας του μηνύματος αναζήτησης μίας νέας διαδρομής, το οποίο υλοποιείται όπως και στα πρωτόκολλα AODV και DSR. Οι πληροφορίες θέσης των κόμβων ενός ad-hoc ασύρματου δικτύου μπορούν να ληφθούν μέσω του GPS (Global Positioning System). Το πρωτόκολλο LAR περιορίζει την αναζήτηση μιας διαδρομής στην αποκαλούμενη ζώνη αιτήματος, που καθορίζεται βασιζόμενη στην αναμενόμενη θέση του κόμβου προορισμού κατά την διάρκεια της διαδικασίας εύρεσης διαδρομών. Δύο είναι οι σημαντικές σχεδιαστικές αρχές της λειτουργίας του LAR, η αναμενόμενη ζώνη (Expected Zone) και η ζώνη αιτήματος (Request Zone).

Αρχικά θα περιγράψουμε την Αναμενόμενη ζώνη (Expected Zone). Θεωρήστε ότι ένας κόμβος S πρέπει να ανακαλύψει μια διαδρομή προς τον κόμβο D, γνωρίζοντας ότι ο κόμβος D βρισκόταν στη θέση L στο χρόνο t_0, και ότι ο τρέχων χρόνος είναι t_1. Η αναμενόμενη ζώνη (Expected Zone) του κόμβου D, από την αντίληψη του κόμβου S στο χρονικό t_1 είναι η περιοχή που αναμένεται να βρίσκεται ο κόμβος D, την οποία ο κόμβος S μπορεί να καθορίσει γνωρίζοντας την αρχική θέση του κόμβου D, την χρονική στιγμή t_0. Παραδείγματος χάριν, εάν ο κόμβος S γνωρίζει ότι ο κόμβος D ταξιδεύει με μέση ταχύτητα v, μπορεί να υποθέσει ότι η αναμενόμενη ζώνη είναι η κυκλική περιοχή ακτίνας v(t1 - t0), με κέντρο τη θέση L. Εάν η πραγματική ταχύτητα του κόμβου D συμβαίνει να είναι μεγαλύτερη από την μέση, ο κόμβος προορισμού τότε μπορεί να βρίσκεται εκτός από την αναμενόμενη ζώνη την χρονικής στιγμή t_1. Κατά συνέπεια, η αναμενόμενη ζώνη είναι μόνο μια εκτίμηση που γίνεται από τον κόμβο S για να καθορίσει μια περιοχή που ενδεχομένως θα βρίσκεται ο D το χρονικό διάστημα t_1.

Εάν ο κόμβος S δεν γνωρίζει μια προηγούμενη θέση του κόμβου D, δεν μπορεί εύλογα να καθορίσει την αναμενόμενη ζώνη και σε αυτή την περίπτωση ο κόμβος είναι υποχρεωμένος να υποθέσει ότι η ολόκληρη περιοχή που καλύπτεται από το ασύρματο ad-hoc δίκτυο είναι η αναμενόμενη ζώνη). Σε αυτήν την περίπτωση, ο LAR λειτουργεί σαν ένας κλασσικός αλγόριθμος πλημμύρας για την διάδοση των μηνυμάτων αναζήτησης διαδρομών. Γενικά, η γνώση περισσότερων πληροφοριών σχετικά με την κινητικότητα ενός κόμβου οδηγεί στην εύρεση μιας μικρότερης αναμενόμενης ζώνης. Η ζώνη αιτήματος καθορίζεται βάση της αναμενόμενης ζώνης. Θεωρούμε τον κόμβο S που πρέπει να καθορίσει μια διαδρομή προς τον κόμβο D. Ο κόμβος S καθορίζει δυναμικά ή στατικά (implicitly or explicitly) μια ζώνη αιτήματος για την συγκεκριμένη διαδικασία εύρεσης μιας διαδρομής. Ένας κόμβος, που

παραλαμβάνει το μήνυμα αυτό, το προωθεί μόνο εάν ανήκει στη ζώνη αιτήματος (σε αντίθεση από τον αλγόριθμό πλημμύρας των AODV και DSR). Για να αυξηθεί η πιθανότητα να φθάσει το αίτημα διαδρομών στον κόμβο D, η ζώνη αιτήματος πρέπει να περιλαμβάνει την αναμενόμενη ζώνη (που περιγράφεται ανωτέρω). Επιπλέον, η ζώνη αιτήματος μπορεί επίσης να περιλάβει και άλλες περιοχές γύρω από τη ζώνη αιτήματος.

Με βάση αυτές τις πληροφορίες ο κόμβος πηγή μπορεί να καθορίσει τις τέσσερις γωνίες της αναμενόμενης ζώνης, τις οποίες συμπεριλαμβάνει στο μήνυμα αιτήματος διαδρομών που μεταδίδει όταν ενεργοποιείται η διαδικασία εύρεσης διαδρομών. Όταν ένας κόμβος λαμβάνει ένα τέτοιο μήνυμα, το απορρίπτει εάν η τωρινή θέση του δεν είναι μέσα στο τμήμα που περιγράφεται από τις συντεταγμένες που περιέχονται στο αίτημα δρομολόγησης.

9.8.2. Distance Routing Effect Algorithm for Mobility (DREAM)

Ο DREAM είναι ένα πρωτόκολλο δρομολόγησης για τα ad-hoc ασύρματα δίκτυα και βασίζεται σε δύο πρωτότυπες παρατηρήσεις. Η πρώτη, αποκαλούμενη επίδραση στην απόσταση (distance effect), εκμεταλλεύεται το γεγονός ότι όσο μεγαλύτερη η απόσταση που χωρίζει δύο κόμβους, τόσο πιο αργά εμφανίζονται να κινούνται ο ένας σε σχέση με τον άλλο. Συνεπώς οι πληροφορίες θέσης στους πίνακες δρομολόγησης μπορούν να ενημερωθούν συναρτήσει της απόστασης που χωρίζει τους κόμβους χωρίς να γίνεται συμβιβασμός στην ακρίβεια της διαδικασίας της δρομολόγησης. Η δεύτερη ιδέα είναι αυτή που προκαλεί την αυτόνομη αποστολή πληροφοριών αναπροσαρμογών θέσεως, κινούμενων κόμβων, βασισμένη μόνο στο ποσοστό κινητικότητας κάθε κόμβου. Διαισθητικά είναι σαφές ότι σε έναν κατευθυνόμενο αλγόριθμο δρομολόγησης, για τους πιο αργά κινούμενους κόμβους, πρέπει να ενημερώνουμε λιγότερο συχνά τους πίνακες δρομολόγησης σε σχέση με τους γρηγορότερα κινούμενους κόμβους. Κατ' αυτό τον τρόπο, κάθε κόμβος μπορεί να βελτιστοποιήσει τη συχνότητα με την οποία στέλνει μηνύματα αλλαγών του δικτύου και να μειώνει αντίστοιχα το εύρος ζώνης και την ενέργεια που χρησιμοποιεί, οδηγώντας σε ένα πλήρως κατανεμημένο, αυτόνομο και αποδοτικό σύστημα δρομολόγησης. Με βάση αυτούς τους πίνακες δρομολόγησης, ο προτεινόμενος κατευθυνόμενος αλγόριθμος στέλνει μηνύματα στη "καταγεγραμμένη κατεύθυνση" του κόμβου προορισμού και εγγυάται την παράδοση των δεδομένων προς της κατεύθυνση αυτή με μια δεδομένη πιθανότητα.

9.9. Power Aware Routing Protocol

Σε αυτό το πρωτόκολλο χρησιμοποιούνται μετρήσεις βασισμένες στην ισχύ κατανάλωσης κάθε κόμβου, για την επιλογή των διαδρομών στο ασύρματο ad-hoc δίκτυο. Έχει αποδειχθεί ότι η χρησιμοποίηση τέτοιων χαρακτηριστικών σε έναν αλγόριθμο δρομολόγησης, μειώνει το κόστος ανά πακέτο στην διαδικασία δρομολόγησης κατά 5 - 30 τοις εκατό σε σχέση με τη δρομολόγηση της συντομότερης διαδρομής. Η χρησιμοποίηση τέτοιων μεθόδων εξασφαλίζει ότι ο μέσος χρόνος ζωής των κόμβων αυξάνεται σημαντικά και κατά συνέπειας ο χρόνος που μπορεί το δίκτυο να διατηρηθεί ενεργό αυξάνεται, χωρίς τελικά η καθυστέρηση

παράδοσης των δεδομένων να αυξάνεται. Τέτοια πρωτόκολλα έχουν μεγάλη χρήση στην περίπτωση που το ασύρματο ad-hoc δίκτυο αποτελείται από σένσορες, οι οποίοι είναι συσκευές που έχουν περιορισμένη ενέργεια και είναι κρίσιμο να διατηρηθεί το δίκτυο ενεργό όσο το δυνατό περισσότερο.

9.10. Multicast Routing

Το Multicasting είναι η διαδικασία κατά την οποία τα πακέτα δεδομένων από μια συσκευή αποστέλλονται ταυτόχρονα μέσω πολλαπλών μονοπατιών στον προορισμό τους. Όπως και με τα κλασσικά ενσύρματα δίκτυα το multicasting σε ένα MANET είναι επίσης δύσκολο να επιτευχθεί και είναι ακόμα δυσκολότερο στην περίπτωση της κίνησης των κόμβων που δημιουργούν αλλαγή στην τοπολογία του δικτύου αρκετά συχνά. Επομένως, τα πρωτόκολλα δρομολόγησης αυτά, πρέπει να λαμβάνουν υπόψη και τις αλλαγές θέσεως των κόμβων. Αν και δεν είναι τμήμα της συγκεκριμένης εργασίας, θεωρούμε σκόπιμο για λόγους πληρότητας να αναφερθούμε απλά στα δύο σημαντικότερα πρωτόκολλα δρομολόγησης με χρήση πολλαπλών μονοπατιών, το AODV και το ODMRP, που προτείνονται από ομάδα εργασίας MANET της IETF.

9.10.1. Multicasting AODV (MAODV)

Στον αλγόριθμο δρομολόγησης AODV οι κόμβοι προσχωρούν σε μια ομάδα πολλαπλής προώθησης δεδομένων κατόπιν σχετικής αιτήσεως (on-demand), δημιουργώντας ένα δέντρο πολλαπλής διανομής (multicast-tree) μεταξύ τους. Το δέντρο αυτό αποτελείται από τα μέλη της ομάδας και κόμβους συνδεδεμένους με τα μέλη της ομάδας, επιτρέπει σε έναν άλλο κόμβο να μπορεί να προσχωρήσει σε μια πολλαπλής διανομής ομάδα ακόμα κι αν απαιτούνται περισσότεροι από ένα σύνδεσμοι για να προσεγγίσει ένα άλλο μέλος της ομάδας.

9.10.2. On-Demand Multicast Routing Protocol (ODMRP)

Το πρωτόκολλο ODMRP βασίζεται στην δημιουργία ενός πλέγματος μεταξύ των κόμβων (mess-based) αντί δέντρου που χρησιμοποιεί το προηγούμενο, που επιτρέπει την δρομολόγηση δεδομένων μέσω πολλαπλών διαδρομών, παρέχοντας καλύτερη συνδεσιμότητα μεταξύ των κόμβων. Με την δημιουργίας ενός πλέγματος παρέχονται πολλαπλές διαδρομές και τα πακέτα μπορούν να παραδοθούν στους προορισμούς τους καθώς οι κόμβοι μετακινούνται και αλλάζουν θέσεις στο δίκτυο. Επιπλέον, τα μειονεκτήματα των multicast δέντρων στα ασύρματα κινητά ad-hoc δίκτυα (π.χ., διαλείπουσα συνδεσιμότητα, συχνός επανα-σχηματισμός του δέντρου, συγκέντρωση κυκλοφορίας, και άλλων) αποφεύγονται. Για να δημιουργηθεί ένα πλέγμα για κάθε ομάδα πολλαπλής διανομής δεδομένων, ο ODMRP χρησιμοποιεί την έννοια της προώθησης ανά ομάδα. Η έννοια αυτή περιγράφει ότι η ομάδα προώθησης (forwarding group) είναι ένα σύνολο αρμόδιων κόμβων για την μετάδοση των multicast δεδομένων. Ο ODMRP ενεργοποιεί τις διαδικασίες δρομολόγησης κατόπιν παραγγελία (on-demand), για να αποφευχθεί η συνολική καθυστέρηση, με στόχο τη βέλτιστη απόδοσης του πρωτοκόλλου σε μεγαλύτερα δίκτυα. Κανένα μήνυμα ελέγχου δεν απαιτείται για να αφήσει ένας κόμβος μια ομάδα.

3. Δρομολόγηση και Caching

Τα ιδιαίτερα χαρακτηριστικά των ad-hoc ασύρματων δικτύων έχουν συζητηθεί σε προηγούμενες παραγράφους. Οι κόμβοι ενός τέτοιου δικτύου συνήθως κινούνται και έχουν το ρόλο τόσο του δρομολογητή όσο και του τερματικού κόμβου, έχουν ασύρματους πομποδέκτες περιορισμένης εμβέλειας, περιορισμένο εύρος καναλιού και παρόμοια χαρακτηριστικά όσο αφορά την επεξεργαστική ισχύ, την διαθέσιμη μνήμη και άλλα. Η άμεση επικοινωνία μεταξύ δυο οποιωνδήποτε κόμβων σε ένα ad-hoc δίκτυο επιτρέπονται μόνο όταν υπάρχει η δυνατότητα της απευθείας διασύνδεση τους. Σε όλες τις άλλες περιπτώσεις για να είναι δυνατή η επικοινωνία των κόμβων απαιτείται η προώθηση των πακέτων δεδομένων μέσω ενδιάμεσων κόμβων του δικτύου. Η έλλειψη σταθερής και προϋπάρχουσας υποδομής στα δίκτυα αυτά επιτάσσει την διατήρηση λειτουργιών, που σε άλλη περίπτωση, όπως στα κλασσικά δίκτυα, εκτελεί το backbone κομμάτι του δικτύου και συγκεκριμένα το κομμάτι αυτό που αποτελείται από συσκευές ειδικού τύπου, όπως δρομολογητές, hubs, switches, από τους ίδιους του κόμβους του δικτύου, για να είναι δυνατή η λειτουργία ενός τέτοιου δικτύου και η μεταφορά δεδομένων μεταξύ των κόμβων αυτού.

Τα πρωτόκολλα τα οποία έχουν αναπτυχθεί για τα ενσύρματα δίκτυα, δεν μπορούν να λειτουργήσουν αποδοτικά στα ασύρματα ad-hoc δίκτυα λόγω των ιδιαίτερων χαρακτηριστικών, όπως αναφέραμε και παραπάνω. Οι λόγοι είναι πολλοί και οι σημαντικότεροι από αυτούς είναι, η περιορισμένη εμβέλεια των ασύρματων πομποδεκτών, η κινητικότητα των κόμβων, η περιορισμένη επεξεργαστική ισχύ και ενέργεια των κόμβων του δικτύου και άλλοι.

Τα πρωτόκολλα δρομολόγησης των ad-hoc δικτύων μπορούν να κατηγοριοποιηθούν σε τρεις βασικές κατηγορίες: reactive, proactive, και υβριδικά. Ένα δυναμικό πρωτόκολλο δρομολόγησης proactive, που ονομάζεται επίσης table-driven πρωτόκολλο, απαιτεί από κάθε κόμβο να διατηρεί έναν ενημερωμένο πίνακα δρομολόγησης, έτσι ώστε μια διαδρομή είναι εύκολα διαθέσιμη όταν ζητηθεί για την αποστολή πακέτων δρομολόγησης.

Στα reactive πρωτόκολλα δρομολόγησης, που ονομάζονται επίσης on-demand πρωτόκολλα, οι κόμβοι δεν απαιτείται να διατηρούν πίνακες δρομολόγησης, αποθηκεύουν τις διαδρομές σε ειδικούς πίνακες που ονομάζονται Caches και άντ' αυτού ενεργοποιούν μια διαδικασία εύρεσης διαδρομών, όποτε απαιτείται ένα συγκεκριμένο μονοπάτι ανάμεσα σε δύο κόμβους. Ένα reactive πρωτόκολλο προκαλεί μικρότερη συμφόρηση στο δίκτυο όσο αφορά τα μηνύματα ελέγχου που απαιτούνται για την δημιουργία των πινάκων δρομολόγησης, στους οποίους δεν είναι απαραίτητο να διατηρούνται πληροφορίες για όλους τους πιθανούς προορισμούς του δικτύου. Οι διαδρομές που βρίσκονται αποθηκευμένες στις Caches, μπορεί όταν ζητηθούν για να χρησιμοποιηθούν να είναι άκυρες, εξαιτίας της αλλαγής της τοπολογίας των κόμβων στο δίκτυο λόγω της κινητικότητας τους. Τα πρωτόκολλα αυτά εισάγουν μία σημαντική καθυστέρηση κατά την αναμονή εύρεσης μιας διαδρομής μετά την ενεργοποίηση του μηχανισμού αναζήτησης διαδρομών, όπου οι κόμβοι πρέπει να στείλουν σχετικά μηνύματα εύρεσης της διαδρομής σε ένα μεγάλο μέρος του δικτύου.

Για την χρησιμοποίηση μόνο των θετικών στοιχείων και των δύο παραπάνω κατηγοριών πρωτοκόλλων δρομολόγησης έχουν προταθεί υβριδικά πρωτόκολλα, τα

οποία συνδυάζουν στοιχεία και των δύο προσεγγίσεων. Στα πρωτόκολλα αυτά, ένας κόμβος διατηρεί μόνο πληροφορίες συνδέσεων για τους κόμβους, που βρίσκονται μέσα σε μια ζώνη, εντός της οποίας χρησιμοποιείται μια proactive προσέγγιση για την δρομολόγηση, ενώ εκτός αυτής χρησιμοποιεί ένα reactive πρωτόκολλο εύρεσης και διατήρησης διαδρομών προς τους μακρινούς προορισμούς.

1. Τρόποι βελτίωσης της απόδοσης των πρωτοκόλλων Δρομολόγησης

Υπάρχουν πάρα πολλοί και διαφορετικοί τρόπο βελτίωσης της απόδοσης συγκεκριμένων πρωτοκόλλων. Σε όλα τα πρωτόκολλα που έχουν προταθεί, υπάρχουν στοιχεία στη διεθνή βιβλιογραφία που περιγράφουν τρόπους βελτίωσης της απόδοσης τους, διαφορετικοί για κάθε ένα πρωτόκολλο. Σε αυτή την εργασία, πέρα από την αναλυτική περιγραφή του μεγαλύτερου συνόλου, αλλά και των κατά την γνώμη μας σημαντικότερων πρωτοκόλλων, ασχοληθήκαμε ιδιαίτερα με την περιγραφή του πρωτοκόλλου δυναμικής δρομολόγησης πηγής (Dynamic Source Routing - DSR). Η μελέτη του συγκεκριμένου πρωτοκόλλου ανέγειρε πολλά ερωτήματα σχετικά με τους τρόπους βελτίωσης της απόδοσης του. Το πρωτόκολλο αυτό είναι το χαρακτηριστικότερο πρωτόκολλο δρομολόγησης πηγής, το οποίο μπορεί εύκολα να προσαρμοστεί και να λειτουργήσει κάτω από οποιεσδήποτε συνθήκες του δικτύου. Παρακάτω θα αναλύσουμε την έρευνα που έγινε στην βελτίωση της απόδοσης του πρωτοκόλλου DSR, με την χρησιμοποίηση τεχνικών αποθήκευσης διαδρομών, σε ειδικούς πίνακες δρομολόγησης στους κόμβους προέλευσης των διαδρομών.

2. Το πρόβλημα του Caching στους αλγόριθμους δρομολόγησης πηγής.

Στα on-demand πρωτόκολλα δρομολόγησης μια διαδρομή που έχει πρόσφατα ανακαλυφθεί αποθηκεύεται σε ειδικούς πίνακες, για να μπορεί να χρησιμοποιηθεί ξανά την επόμενη φορά που θα ζητηθεί. Δύο περιπτώσεις μπορούμε να ξεχωρίσουμε στην διαδικασία αποθήκευσης διαδρομών (route caching).Στη πρώτη περίπτωση, ένας κόμβος αποθηκεύει διαδρομές πηγής σε ειδικούς πίνακες, ώστε να είναι διαθέσιμες στο μέλλον όταν αυτό ζητηθεί και ονομάζεται αποθήκευση διαδρομών πηγής (source route caching). Οι αποθηκευμένες διαδρομές μπορούν να ζητηθούν από τον ίδιο τον κόμβο που τις έχει αποθηκεύσει ή από κάποιον άλλο με ένα μήνυμα αναζήτησης διαδρομών το οποίο έστειλε στο κόμβο που έχει αποθηκευμένη την διαδρομή και μπορεί να εξυπηρετήσει το αίτημα αυτό. Σαν επέκταση των ανωτέρω, πολλά on-demand πρωτόκολλα δρομολόγησης, όπως ο AODV και ο DSR, επιτρέπουν και σε ενδιάμεσους κόμβους (κόμβους μη-προορισμού που έχουν λάβει αντίγραφα του μηνύματος αναζήτησης διαδρομών από τον κόμβο προέλευσης) που έχουν μια αποθηκευμένη διαδρομή, να απαντήσου στο αίτημα του κόμβου προορισμού αποστέλλοντας την διαδρομή πηγής που έχουν διαθέσιμη σε αυτόν. Η δεύτερη αυτή περίπτωση ονομάζεται ενδιάμεση εναποθήκευση διαδρομών (intermediate route caching).

2.1. Λόγοι και οφέλη της αποθήκευσης διαδρομών σε ένα on-demand πρωτόκολλο δρομολόγησης

Δυο είναι οι βασικοί λόγοι και τα οφέλη αποθήκευσης των διαδρομών σε ένα on-demand πρωτόκολλο δρομολόγησης ενός ad-hoc δικτύου. Ο πρώτος και ποιο

σημαντικός αναφέρεται στην μείωση της καθυστέρησης εύρεσης μιας νέας διαδρομής. Όπως έχουμε αναφέρει ήδη, κατά την διαδικασίας αναζήτησης διαδρομών, ένας κόμβος, όταν λάβει ένα μήνυμα αναζήτησης μιας διαδρομής, ελέγχει εάν μπορεί να εξυπηρετήσει το αίτημα αυτό με μία διαδρομή από αυτές που έχει αποθηκευμένες στους πίνακες δρομολόγηση. Στην περίπτωση αυτή επιστρέφει αμέσως μια απάντηση στον κόμβο προέλευσης του αιτήματος, με αποτέλεσμα να είναι σημαντικά μικρότερη η καθυστέρηση εύρεσης μιας διαδρομής. Ο λόγος είναι προφανής, αφού το μήνυμα αναζήτησης δεν είναι αναγκαίο να ταξιδέψει έως τον κόμβο προορισμού, αλλά πολύ γρηγορότερα μια έγκυρη αποθηκευμένη διαδρομή μεταδίδεται ως απάντηση στον κόμβο προέλευσης. Αυτό είναι ιδιαίτερα σημαντικό στην μετάδοση δεδομένων πραγματικού χρόνου, όπως ήχου και εικόνας, όπου η επιτυχής αναπαραγωγή των δεδομένων στον παραλήπτη είναι ευαίσθητη στην καθυστέρηση μετάδοσης των δεδομένων.

Ο δεύτερος λόγος αφορά την μείωση της κυκλοφορίας των μηνυμάτων ελέγχου που απαιτούνται στην αναζήτηση μίας νέας διαδρομής. Κάθε φορά που ενεργοποιείται ο μηχανισμός αναζήτησης διαδρομών, οι κόμβοι ελέγχουν εάν μια διαδρομή προς τον συγκεκριμένο προορισμό είναι διαθέσιμη και έγκυρη στην Cache και στην περίπτωση που δεν υπάρχει μεταδίδουν ένα μήνυμα αναζήτησης στους υπόλοιπους κόμβους του δικτύου.

2.2. Μειονεκτήματα της αποθήκευσης διαδρομών σε ένα on-demand πρωτόκολλο δρομολόγησης

Η αποθήκευση μιας διαδρομής σε μιας Cache όμως μπορεί να έχει και αρνητικά αποτελέσματα. Η περίπτωση στην οποία αναφερόμαστε έχει να κάνει με την χρησιμοποίηση αποθηκευμένων διαδρομών οι οποίες δεν είναι έγκυρες. Αυτό μπορεί να συμβεί είτε λόγω της κινητικότητας, είτε λόγω της απενεργοποίησης κάποιων κόμβων, με αποτέλεσμα να μην είναι δυνατή η μετάδοση των δεδομένων πάνω από το συγκεκριμένο μονοπάτι προς τον προορισμό. Όταν χρησιμοποιείται μια διαδρομή από την Cache ενός κόμβου η οποία δεν είναι έγκυρη, προσθέτει παραπάνω κυκλοφορία και καθυστέρηση στη δρομολόγηση των δεδομένων, αφού θα απαιτηθεί χρόνος για να ανακαλυφθούν οι σπασμένες συνδέσεις και να σταλεί μήνυμα λάθους στον κόμβο προορισμού των δεδομένων, ο οποίος στη συνέχεια θα ενεργοποιήσει την διαδικασία εύρεσης μιας νέας διαδρομής. Ανάλογα με την υλοποίηση του κάθε πρωτοκόλλου δρομολόγησης, καθ' όλη αυτή την διαδικασία, δεδομένα αλλά και μηνύματα ελέγχου θα έχουν ήδη μεταδοθεί κατά μήκος της διαδρομής, που είναι έγκυρη, έως τη σύνδεση που είναι σπασμένη, αναγκάζοντας τον κόμβο πηγής των δεδομένων να πρέπει να στείλει ξανά τα δεδομένα προς τον προορισμό μέσω της νέας διαδρομής.

3. Έρευνα στη διεθνή βιβλιογραφία για την αποθήκευση διαδρομών

Στη σχετική βιβλιογραφία περιγράφονται διάφορες μέθοδοι αντιμετώπισης του συγκεκριμένου προβλήματος, με σκοπό την αποδοτική χρήση των τεχνικών αποθήκευσης διαδρομών στους κόμβους ενός ad-hoc ασύρματου τηλεπικοινωνιακού δικτύου, σε ένα reactive πρωτόκολλο δρομολόγησης. Οι μέθοδοι αυτοί, μερικές από τις οποίες θα αναφέρουμε παρακάτω, προσπαθούν να εντοπίσουν τρόπους ακύρωσης διαδρομών που δεν είναι έγκυρες και περιγράφουν μονοπάτια πάνω από τα οποία

υπάρχουν διακομμένες συνδέσεις για να εμποδίσουν τους κόμβους από την χρήση αυτών των διαδρομών.

3.1. Βελτιστοποίηση της απόδοσης με τη χρήση της παραμέτρου Time-To-Live (TTL)

Η on-demand δρομολόγηση μειώνει την συνολική κίνηση του δικτύου και την καθυστέρηση των δεδομένων που διακινούνται στα ασύρματα ad-hoc δίκτυα των οποίων οι κόμβοι κινούνται αλλά έχει και το σημαντικό μειονέκτημα της αρχικής καθυστέρηση ανάμεσα σε ένα αίτημα μιας διαδρομής και την λήψης μιας απάντησης με μια έγκυρη διαδρομή. Στην παρούσα εργασία περιγράφεται μία μέθοδος ελαχιστοποίησης της καθυστέρησης, σε on-demand πρωτόκολλα δρομολόγησης πηγής, μέσω της βελτιστοποίησης της παραμέτρου Time-To-Live (TTL), στις διαδρομές των πινάκων αποθήκευσης διαδρομών (Route Cache Tables).

Στην εργασία [Liang 2003] παρουσιάζεται ένα αναλυτικό πλαίσιο για τον προσδιορισμό της αναμενόμενης καθυστέρησης δρομολόγησης, όταν ένας κόμβος πηγής ή ένας ενδιάμεσος κόμβος έχει μια αποθηκευμένη διαδρομή προς οποιοσδήποτε προορισμό, λαμβάνοντας υπόψη την μεταβλητή TTL. Επιπλέον, προτείνονται οι αριθμητικές μέθοδοι που καθορίζουν την βέλτιστη τιμή του TTL, για μία πρόσφατα αποθηκευμένη διαδρομή. Χρησιμοποιώντας ένα αναλυτικό πλαίσιο οι συγγραφείς μελετάνε τον τρόπο με τον οποίο η καθυστέρηση δρομολόγησης επηρεάζεται από το μήκος των διαδρομών, τη συχνότητα έκδοσης νέων αιτημάτων διαδρομών και τη συχνότητα αλλαγής της τοπολογίας των κόμβων του δικτύου. Καταλήγουν στο συμπέρασμα ότι η προτεινόμενη τεχνική μπορεί να μειώσει σημαντικά την καθυστέρηση δρομολόγησης σε συστήματα, που είτε δεν χρησιμοποιούν Route Cache, είτε χρησιμοποιούν υποθέτοντας ότι ο χρόνος ζωής των διαδρομών είναι άπειρος. Τέλος παρουσιάζουν αποτελέσματα προσομοίωσης για να υποστηρίξουν τα θεωρητικά συμπεράσματα τους.

Η προσέγγιση αυτή περιγράφει ότι για την ελαχιστοποίηση του φαινομένου ύπαρξης άκυρων διαδρομών σε μια Cache, ορίζουμε μια παράμετρο που αντιστοιχεί σε κάθε ξεχωριστή διαδρομή και συνεπώς καταχώρηση στον πίνακα δρομολόγησης προς ένα προορισμό, που περιγράφει το χρόνο ζωής μιας διαδρομής. Μετά την πάροδο της χρονικής αυτής διάρκειας η εν λόγω διαδρομή θεωρείται άκυρη και επιτρέπεται η διαγραφή της από τους πίνακες δρομολόγησης, αφού έχει «λήξει» ο χρόνος ζωής της και δεν πρέπει να χρησιμοποιηθεί πλέον από τους κόμβους του δικτύου.

Ως χρόνο ζωής μιας διαδρομής ορίζουμε τον χρόνο στον οποίο η διαδρομή είναι έγκυρη και μπορεί να χρησιμοποιηθεί με επιτυχία από έναν κόμβο για την αποστολή δεδομένων. Τον ορίζουμε χρησιμοποιώντας μια μεταβλητή που ονομάζουμε «Time-To-Live (TTL)» και εννοούμε τον χρόνο ζωής και παραμονής μιας διαδρομής στην Route Cache ενός κόμβου. Από εδώ και πέρα θα χρησιμοποιούμε το ακρωνύμιο TTL και θα αναφερόμαστε στον χρόνο αυτό. Όταν ο χρόνος αυτός παρέλθει μια διαδρομή πρέπει να μην χρησιμοποιείται, να ακυρώνεται και να διαγράφεται από την Cache των κόμβων. Η μεταβλητή αυτή είναι δύσκολο να οριστεί στα ασύρματα ad-hoc δίκτυα, λόγω των δυναμικών χαρακτηριστικών του δικτύου, που αλλάζουν με την πάροδο του χρόνου. Η συγκεκριμένη εργασία προσπαθεί να δώσει ένα γενικό αναλυτικό πλαίσιο για τον προσδιορισμό της με όσο το δυνατό μικρότερο σφάλμα.

Μια παρόμοια προσέγγιση, έξω από του σκοπούς αυτής της εργασίας, είναι να χρησιμοποιηθεί μια διαδικασία ακύρωσης διαδρομών. Ο μηχανισμός αυτός στηρίζεται στην μετάδοση μηνυμάτων που περιγράφουν μια σπασμένη σύνδεση και αναγκάζουν τους κόμβους που έχουν διαδρομές με την συγκεκριμένη σύνδεση να ακυρώσουν τις συγκεκριμένες εγγραφές στους πίνακες αποθήκευσης τους. Αυτή είναι μια proactive διαδικασία, η οποία μπορεί να οδηγήσει στην δημιουργία μεγάλου όγκου μηνυμάτων ελέγχου, που ταξιδεύουν στο ad-hoc δίκτυο. Τα μηνύματα αυτά, τα οποία πρέπει να μεταδοθούν στους κόμβους του δικτύου, χρησιμοποιούν τεχνικές πλημμύρας για την μετάδοση τους και υπάρχει περίπτωση να μην καταφέρουν να προσεγγίσουν όλους του κόμβους του δικτύου, λόγω της κινητικότητας των κόμβων και της συνεχής αλλαγής των γεωγραφικών θέσεων τους.

3.1.1. Χαρακτηριστικά της παραμέτρου TTL

Η μεταβλητή TTL περιγράφει τον χρόνο στον οποίο μια αποθηκευμένη διαδρομή θεωρούμε ότι μπορεί να χρησιμοποιηθεί έχοντας μεγάλη πιθανότητα να είναι έγκυρη διαδρομή. Στην πραγματικότητα είναι πολύ δύσκολο να περιγράψουμε, με μαθηματικές εκφράσεις, την τιμή της TTL με μεγάλη ακρίβεια. Αυτό που μπορούμε να κάνουμε είναι να προσπαθήσουμε να προβλέψουμε μια τιμή, για το TTL κάθε διαδρομής, με όσο το δυνατό μικρότερο σφάλμα. Εάν στο TTL τεθεί μία πάρα πολύ μικρή τιμή, είναι πολύ πιθανό να απορρίπτονται έγκυρες διαδρομές από τους πίνακες δρομολόγησης και να παρατηρείται μεγάλη καθυστέρηση λόγω της ενεργοποίησης της διαδικασίας εύρεσης διαδρομών. Από την άλλη, εάν στο TTL τίθενται μεγάλες τιμές, είναι πολύ πιθανό να χρησιμοποιούνται άκυρες διαδρομές, με αποτέλεσμα και πάλι να έχουμε επιπλέον καθυστέρηση στη δρομολόγηση των δεδομένων πριν ανακαλυφθεί ο σπασμένος σύνδεσμος για να ενεργοποιηθεί η διαδικασία εύρεσης μιας νέας διαδρομής.

Κατά συνέπεια, είναι απαραίτητος ένας αλγόριθμος που να μπορεί να προβλέπει με ακρίβεια τις βέλτιστες τιμές που πρέπει να έχει η μεταβλητή αυτή για τη βέλτιστη απόδοση του πρωτοκόλλου δρομολόγησης. Στην εργασία αυτή παρουσιάστηκε ένα μαθηματικό μοντέλο ανάλυσης, που μπορεί με μερικές υποθέσεις να μας βοηθήσει, με μικρό σφάλμα, να κάνουμε σωστές υποθέσεις για την τιμή της παραμέτρους αυτής.

3.1.2. Μέθοδος υπολογισμού της βέλτιστης τιμής TTL

Προφανώς, η βέλτιστη TTL μιας διαδρομή-κρύπτης εξαρτάται από το πόσο σταθερή είναι η τοπολογία διαδρομών στο ασύρματο ad-hoc δίκτυο. Υποθετικά, εάν η κατάσταση όλων των συνδέσεων για το μέλλον ήταν γνωστή, η TTL θα έπρεπε να πάρει τιμή ίση με την χρονική περίοδο όπου για πρώτη φορά οποιαδήποτε σύνδεση, μέρος μίας διαδρομής, θα αποτύγχανε και θα διακοπτόταν. Στην πραγματικότητα όμως μπορούμε μόνο να υπολογίσουμε τη διάρκεια ζωής των διαδρομών από στατιστικά δεδομένα και να βελτιστοποιήσουμε τη TTL με σκοπό να ελαχιστοποιήσουμε την αναμενόμενη καθυστέρηση δρομολόγησης.

3.2. Ensuring Cache Freshness in On-Demand Ad Hoc Network Routing Protocols

Σε αυτή την εργασία παρουσιάζεται ένας νέος μηχανισμός, που εγγυάται την μείωση του ποσοστού των πολυδιατηρημένων και μη έγκυρων αποθηκευμένων πληροφοριών δρομολόγησης στις Route Caches. Σύμφωνα με την συγκεκριμένη προσέγγιση επιτυγχάνουμε την καλύτερη διαχείριση των πληροφοριών μιας Cache με την παρεμπόδιση ανταλλαγής μη-έγκυρων πληροφοριών ανάμεσα στους κόμβου του δικτύου. Συγκεκριμένα οι κόμβους αποτρέπονται από το να συγκρατούν πληροφορίες για διαδρομές δρομολόγησης, οι οποίες περιέχουν συνδέσεις για τις οποίες έχει ήδη αναφερθεί κάποιο λάθος. Το συγκεκριμένο πρωτόκολλο δεν στηρίζεται σε κάποιους μηχανισμούς δρομολόγησης των ad-hoc δικτύων όπως η αποθήκευση αρνητικών πληροφοριών δρομολόγησης. Επιτρέπει σε έναν κόμβο, που έχει λάβει ένα μήνυμα για μια σύνδεση που έχει διακοπεί, να λάβει και ένα μήνυμα εύρεσης μιας διαδρομής που περιέχει την σύνδεση αυτή, να τοποθετήσει τα δύο αυτά γεγονότα διαδοχικά και να καθορίσει ποιο από τα δύο εμφανίστηκε πρώτο, για να μπορέσει να συμπεράνει ποιο από τα δύο ισχύει, προσπαθώντας να διατηρεί πληροφορίες που είναι όσο το δυνατό εγκυρότερες.

3.2.1. Περιγραφή της μεθόδου

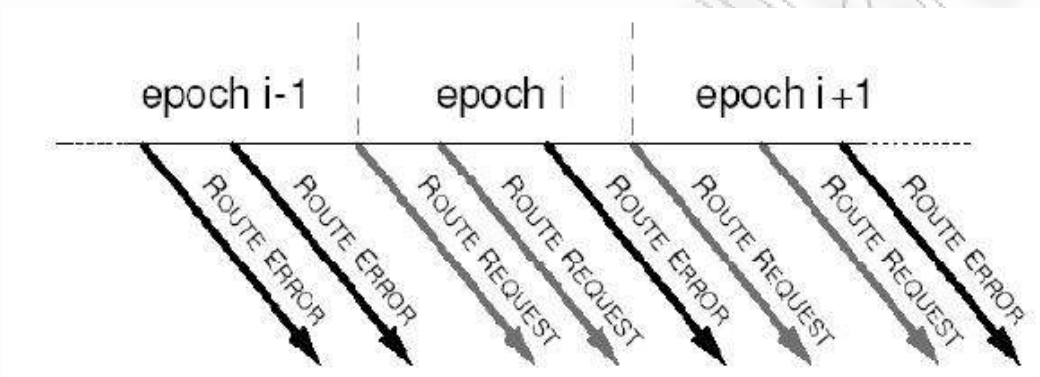
Η προσέγγισή στην παρούσα εργασία αφορά τη μείωση του πλήθους των άκυρων αποθηκευμένων πληροφοριών δρομολόγησης με την συλλογή αρκετών πληροφοριών δρομολόγησης, ώστε να είναι δυνατή η αποκατάσταση διαδρομών για τις οποίες έχει αναφερθεί λάθος σε κάποιες συνδέσεις.

Όταν είναι δυνατή η διαδοχική χρονική τοποθέτηση πληροφοριών δρομολόγησης για νέες έγκυρες διαδρομές αλλά και μηνυμάτων λαθών, για διαδρομές οι οποίες περιέχουν συνδέσεις που έχουν διακοπεί, πολυδιατηρημένες άκυρες πληροφορίες δεν μπορούν να αποθηκευτούν ξανά στην «Route Cache» ενός κόμβου μετά από την διαγραφή τους. Κάτι τέτοιο μπορεί να συμβεί όταν ένας κόμβος ακυρώσει μια αποθηκευμένη διαδρομή, η οποία περιέχει μια άκυρη σύνδεση και λάβει μία απάντηση στο μέλλον, που περιέχει την εν λόγω άκυρη σύνδεση, με σκοπό να την αποθηκεύσει ξανά στην «Route Cache».

Στην παρούσα εργασία οι συγγραφείς χρησιμοποιούν μια τεχνική που ονομάζεται «epoch numbers» με σκοπό να περιγράψουν μια ακολουθία από γεγονότα. Η τεχνική αυτή επιτρέπει σε ένα κόμβο του δικτύου να γνωρίζει την αλληλουχία διαφόρων γεγονότων, ώστε να μπορέσει να πάρει όταν είναι απαραίτητο την σωστότερη απόφαση στην δρομολόγηση των δεδομένων. Στην λύση που παρουσιάζεται δεν είναι απαραίτητη η χρήση συγχρονισμένων ρολογιών ή η χρήση timestamps πληροφοριών. Στην εργασία αυτή παρουσιάζεται μια λύση wraparound των ακέραιων αριθμών, που χρησιμοποιούμε για να αναπαραστήσουμε τους «epoch numbers», που ονομάζεται «generation numbers» και εκφράζει το χρόνο παραμονής των πληροφοριών στους πίνακες αποθήκευσης.

Στην παρουσία συγκρουόμενων πληροφοριών δρομολόγησης οι κόμβοι πρέπει να δημιουργήσουν μια αλληλουχία από διακριτά γεγονότα. Για να το πετύχουν σε κάθε κόμβο διατηρείται ένας «epoch number», που ανήκει σε αυτόν, ο όποιος αντιστοιχείται με κάθε σύνδεση κάθε πρόσφατου γείτονα και με κάθε νέο μήνυμα διακοπής συνδέσεων, που ο ίδιος ο κόμβος στέλνει. Παραδείγματος χάριν, εάν κατά

τη διάρκεια του «epoch number» i του κόμβου A, εάν ο κόμβος A ανακαλύψει ότι ο B είναι ένα νέος γείτονας του, συνδέει τη σύνδεση από τον A στον B με τον «epoch number» i (ανεξάρτητος από τον «epoch number» του κόμβου B). Κάθε «Route Cache» περιλαμβάνει τόσο θετικές όσο και αρνητικές πληροφορίες για τις συνδέσεις κάθε κόμβου, μαζί με τον αντίστοιχο «epoch number» για κάθε μία από αυτές, Κάθε πακέτο που περιέχει πληροφορίες δρομολόγησης περιλαμβάνει επίσης τον «epoch number» για κάθε ξεχωριστή σύνδεση στη διαδρομή για τον αντίστοιχο κόμβο.



Εικόνα 8: Οι «epoch numbers» σε ένα κόμβο

Η αλληλουχία των συνδέσεων γίνεται, χρησιμοποιώντας «epoch numbers», στους κόμβους αποστολής των δεδομένων. Κάθε φορά που μία αποθηκευμένη σύνδεση ενός κόμβου έρχεται σε σύγκρουση με πληροφορίες δρομολόγησης που πρόσφατα έλαβε, ο κόμβος επιλέγει τις πληροφορίες με τον μεγαλύτερο «epoch number». Όταν η ανίχνευση μίας σύνδεσης και η θραύση μίας σύνδεσης έχουν τον ίδιο «epoch number», οι πληροφορίες θραύσης της σύνδεσης παίρνουν προτεραιότητα. Οι «epoch numbers» αυξάνονται ανάλογα με τις ανάγκες για να διατηρήσουν την κατάλληλη αλληλουχία των πληροφοριών δρομολόγησης, όπως διευκρινίζεται στο παραπάνω σχήμα. Ειδικότερα, όποτε ένας κόμβος δημιουργεί ή διαβιβάζει ένα πακέτο «Route Request» αφότου έχει δημιουργηθεί ήδη ένα «Route Error», αυξάνει τον «epoch number» του.

Σαν παράδειγμα της χρήσης των «epoch numbers», υποθέστε ότι ο κόμβος A αποθηκεύει μια σύνδεση από τον κόμβο B στον κόμβο C με «epoch number» 1 και χρησιμοποιεί αυτήν τη σύνδεση ως τμήμα μιας διαδρομής. Κατόπιν ο κόμβος A θα δεχόταν ένα «Route Error» για αυτήν την σύνδεση μόνο με «epoch number» μεγαλύτερο ή ίσο 1. Σε μία τέτοια περίπτωση ο κόμβος A θα αγνοήσει οποιαδήποτε σύνδεση από το B στον C με «epoch number» μικρότερο ή ίσο με αυτόν στο μήνυμα «Route Error» και δεν θα προσθέσει τις συγκεκριμένες πληροφορίες στην «Route Cache» του. Αυτό αποτρέπει τον κόμβο A να διατηρεί πληροφορίες, οι οποίες περιέχουν λάθη και είναι πολυδιατηρημένες από αυτές που είναι νεότερες και έχουν μεγαλύτερη πιθανότητα να είναι έγκυρες.

Οι «epoch numbers» υλοποιούνται, με την χρήση ακεραίων, οι οποίοι σε ένα υπολογιστικό σύστημα περιγράφονται με ένα περιορισμένο πλήθος δυαδικών ψηφίων και έχουν συγκεκριμένο μη-άπειρο πλήθος. Καθώς οι «epoch numbers» αυξάνονται συνεχώς, με την πάροδο του χρόνου υπάρχει ο φόβος υπερχείλισης του ακέραιου αριθμού που χρησιμοποιείται στην υλοποίηση. Για τον λόγο αυτό έχει αναπτυχθεί ένας μηχανισμός για την αποφυγή της υπερχείλισης των ακεραίων που αποθηκεύονται οι «epoch numbers». Για να το πετύχουμε αυτό αρχικά περιορίζουμε τον ρυθμό με τον οποίο οι «epoch numbers» χρησιμοποιούνται. Δεδομένου ότι ο στόχος μας είναι να περιορίσουμε τον αριθμό των «epoch numbers» που μπορούν να χρησιμοποιηθούν σε ένα διάστημα, πριν ξεκινήσει πάλι η αρίθμηση τους από την αρχή. Κατά κάποιο τρόπο χωρίζουμε σε διάφορα μέρη το χώρο στο οποίο μπορούν να κυμαίνονται οι «epoch numbers» στην πάροδο του χρόνου λειτουργίας του δικτύου.

Όποτε ένα πακέτο στέλνεται, με μια διαδρομή πηγής από κάποιον κόμβο, περιέχει έναν «epoch number» και έναν «generation number» για κάθε σύνδεση που περιέχεται στην διαδρομή δρομολόγησης. Ο «epoch number» επιλέγεται να είναι αυτός που αντιστοιχεί στη συγκεκριμένη σύνδεση και περιέχεται στην «Route Cache» του κόμβου. Για να επιλεγεί ο «generation number», ο κόμβος υπολογίζει το χρόνος άφιξης του πακέτου αυτού στον τελευταίο κόμβο που έλαβε το πακέτο από όπου παίρνει το «generation number» και το αυξάνει κατά ένα και τον χρησιμοποιεί. Όποτε ο «generation number» αυξάνεται, ο κόμβος ελέγχει εάν ο αριθμός έχει περάσει ένα συγκεκριμένο πάνω όριο. Σε αυτή την περίπτωση, στον «epoch number» τίθεται μια ειδική τιμή (όπως το 0) και οι κόμβοι μπορούν να υποθηκεύσουν συγκεκριμένη σύνδεση μόνο εάν δεν γνωρίζουν προηγουμένως ότι δεν είναι έγκυρη.

3.2.2. Ανάλυση του πρωτοκόλλου

3.2.2.1. Network Overhead

Για να χρησιμοποιήσουν τους «epoch» και «generation number» για όλες τις καταχωρήσεις μίας «Route Cache» τους περιλαμβάνουμε σε κάθε διεύθυνση για κάθε διαδρομή πηγής, σε όλα τα μηνύματα ελέγχου του πρωτοκόλλου δρομολόγησης. Κατά συνέπεια, είναι δυσανάλογο, το μεγέθους των πληροφοριών για τους αριθμούς αυτούς και το μέγεθος της διεύθυνσης του κάθε κόμβου στο δίκτυο. Αυτό προσθέτει ένα σημαντικό «overheard» στο δίκτυο.

3.2.2.2. Storage Overhead

Το σχήμα των «epoch numbers» προσθέτει έναν σταθερό παράγοντα «overhead» στην αποθήκευσης της κατάστασης των συνδέσεων, δεδομένου ότι κάθε σύνδεση πρέπει να περιέχει τις πληροφορίες αυτές. Αυτό το επιπλέον μέγεθος των πληροφοριών που πρέπει να αποθηκεύονται ανά σύνδεση, συμπεριλαμβανομένων και των πληροφοριών του συγκεκριμένου πρωτοκόλλου, είναι σταθερό και αυξάνουν τις πληροφορίες που αποθηκεύονται για την κατάσταση των συνδέσεων σε μια Cache, κατά ένα σταθερό παράγοντα.

3.2.2.3. Αποτελέσματα

Τα αποτελέσματα της συγκεκριμένης προσέγγισης είναι αρκετά ικανοποιητικά. Η συγκεκριμένη λύση λειτουργεί αρκετά αποδοτικά και αποτρέπει τους κόμβους από την χρησιμοποίηση παλαιότερων άκυρων πληροφοριών δρομολόγησης από νέες πληροφορίες, για τις οποίες δεν υπάρχει αναφορά για κάποιο λάθος κάποιας σύνδεσης. Η τεχνική αυτή προσφέρει στους κόμβους την δυνατότητα να γνωρίζουν την χρονολογική σειρά γεγονότων που μπορούν να επηρεάσουν την διαδικασία δρομολόγησης, όπως η ανακάλυψη ύπαρξης νέων συνδέσεων με νέους κόμβους και η αναφορά λαθών σε συγκεκριμένες συνδέσεις, προσφέροντας τους τις απαραίτητες γνώσεις για να μπορέσουν να χρησιμοποιούν αποδοτικά τις πληροφορίες αυτές.

4. Ο Αλγόριθμος Δρομολόγησης Dynamic Source Routing (DSR)

Ο δυναμικός αλγόριθμος δρομολόγησης για ασύρματα ad-hoc δίκτυα είναι ένα απλό και αποδοτικό πρωτόκολλο δρομολόγησης σχεδιασμένο ειδικά για χρήση πάνω από ασύρματα δίκτυα πολλαπλών συνδέσεων (hops) στα οποία οι κόμβοι δεν παραμένουν στάσιμοι αλλά κινούνται. Ο DSR επιτρέπει στο δίκτυο στο οποίο χρησιμοποιείται να είναι πλήρως αυτόνομο, τόσο στην διαδικασία οργάνωσης όσο και στη διαδικασία προσδιορισμού των διαφόρων παραμέτρων του δικτύου, χωρίς να είναι απαραίτητη η παρουσία κάποιας προϋπάρχουσας δικτυακής υποδομής ή διαχείρισης του δικτύου. Το πρωτόκολλο αποτελείται από δύο ξεχωριστούς και αυτόνομους μηχανισμούς, την «Εύρεσης των Διαδρομών» (Route Discovery) και τη «Διατήρησης Διαδρομών» (Route Maintenance), οι οποίες συνεργάζονται και λειτουργούν παράλληλα επιτρέποντας στους κόμβους του δικτύου να ανακαλύπτουν διαδρομές πηγής (source routes) προς κάθε δυνατό προορισμό που επιθυμούν και να τις διατηρούν στην πάροδο του χρόνου λειτουργίας. Η επιλογή της χρήσης διαδρομών πηγής, επιτρέπει την μεταγωγή πακέτων δεδομένων με την χρήση μονοπατιών που δεν περιέχουν βρόγχους. Οι ενδιάμεσοι κόμβοι χωρίς να χρειάζονται επιπλέον πληροφορίες για την κατάσταση των συνδέσεων στο δίκτυο, προωθούν τα πακέτα, σύμφωνα με την διαδρομή που πρέπει να ακολουθήσουν στον επόμενο κόμβο, έως ότου αυτά φτάσουν στον προορισμό του. Παράλληλα οι ενδιάμεσοι κόμβοι αποθηκεύουν σε ειδικούς πίνακες τις πληροφορίες δρομολόγησης, που μεταφέρουν τα πακέτα, για μελλοντική χρήση. Όλες οι λειτουργίες του πρωτοκόλλου λειτουργούν κατόπιν σχετικού αιτήματος από τους ενδιαφερόμενους κόμβους, επιτρέποντας την κλιμάκωση αυτού ανάλογα με τις απαιτήσεις και τις συνθήκες στο δίκτυο.

1. Εισαγωγή

Το δυναμικό πρωτόκολλο δρομολόγησης πηγής (DSR) είναι ένα απλό και αποδοτικό πρωτόκολλο δρομολόγησης που σχεδιάστηκε ειδικά για χρήση σε ασύρματα ad-hoc δίκτυα πολλαπλών συνδέσεων (hop) κινητών κόμβων. Χρησιμοποιώντας τον DSR, το δίκτυο είναι εντελώς αυτόνομο και δεν απαιτείται η ύπαρξη κάποιας υποδομής ή κεντρικής διαχείρισης αυτού. Οι κόμβοι του δικτύου μπορούν και πρέπει να συνεργάζονται για την μεταφορά των πακέτων από τον ένα στον άλλον, ούτως ώστε να είναι δυνατή η μεταφορά δεδομένων μεταξύ των κόμβων αυτών, που η απευθείας επικοινωνία δεν είναι δυνατή. Καθώς οι κόμβοι στο δίκτυο κινούνται, συνδέονται ή αποσυνδέονται από αυτό, οι συνθήκες του δικτύου, όπως παρεμβολές στο ασύρματο

μέσο, εμπόδια στην ασύρματη μετάδοση των δεδομένων και τα δεδομένα δρομολόγησης, καθορίζονται αυτόματα από το πρωτόκολλο δρομολόγησης DSR, δεδομένου ότι ο αριθμός ή η ακολουθία ενδιάμεσων συνδέσεων (hop), που πρέπει να διανύσουν τα πακέτα για να φθάσουν σε οποιοδήποτε πιθανό προορισμό, μπορεί να αλλάξει οποιαδήποτε στιγμή και η προκύπτουσα τοπολογία του δικτύου κάθε στιγμή μπορεί να είναι αρκετά διαφορετική. Το πρωτόκολλο DSR επιτρέπει στους κόμβους να ανακαλύπτουν δυναμικά νέες διαδρομές προς οποιοδήποτε προορισμό του δικτύου. Κάθε πακέτο δεδομένων που αποστέλλεται, μεταφέρει στην επικεφαλίδα (header) του την πλήρη διαδρομή που πρέπει να διανύσει για να φτάσει στον προορισμό του, επιτρέποντας στο πρωτόκολλο δρομολόγησης να είναι λειτουργικό και απλό για τους ενδιάμεσου κόμβους, αποφεύγοντας παράλληλα την ενδεχόμενη ύπαρξη κυκλικών βρόχων μέσα στη διαδρομή. Ταυτόχρονα με την μεταγωγή των πακέτων οι ενδιάμεσοι κόμβοι αποκτούν νέες πληροφορίες δρομολόγησης, τις οποίες τις συλλέγουν και τις αποθηκεύουν σε ειδικούς πίνακες για μελλοντική χρήση.

2. Υποθέσεις στην λειτουργίας του πρωτοκόλλου

Παρακάτω παραθέτουμε μερικές από τις βασικές λειτουργικές υποθέσεις πάνω στις οποίες βασίστηκε η σχεδίαση και η υλοποίηση του πρωτοκόλλου δρομολόγησης DSR.

2.1. Διαθεσιμότητα των κόμβων και συμμετοχή στις λειτουργίες του πρωτοκόλλου.

Υποθέτουμε ότι όλοι οι κόμβοι του δικτύου, που επιθυμούν να επικοινωνήσουν με άλλους κόμβους μέσα σε ένα ad-hoc δίκτυο, είναι πρόθυμοι να συμμετέχουν πλήρως στην διαδικασία δρομολόγησης των πακέτων του δικτύου. Συγκεκριμένα, κάθε κόμβος που συμμετέχει στο δίκτυο, πρέπει να είναι πρόθυμος να μεταγάγει πακέτα για τους άλλους κόμβους του δικτύου.

2.2. Διάμετρος του δικτύου

Αναφερόμαστε στον ελάχιστο αριθμό μονοπατιών που απαιτούνται, για να μεταδοθεί ένα πακέτο, από οποιοδήποτε κόμβο που βρίσκεται σε μία ακριανή θέση του ad-hoc δικτύου, σε έναν άλλο κόμβο που βρίσκεται στο αντίθετο άκρο, σαν «διάμετρο» του δικτύου. Υποθέτουμε ότι η διάμετρος ενός τέτοιου δικτύου θα είναι συχνά μικρή (π.χ. με τιμές από 5 έως 10 μονοπάτια).

2.3. Αλλοιωμένα πακέτα

Τα πακέτα που μεταδίδονται σε ένα ασύρματο δίκτυο μπορεί να χαθούν ή να αλλοιωθούν. Ένας κόμβος που λαμβάνει ένα αλλοιωμένο πακέτο έχει την ικανότητα να το ανιχνεύσει και να το απορρίψει.

2.4. Μοντέλο κίνησης των κόμβων

Οι κόμβοι μέσα στο ειδικό δίκτυο μπορούν να κινηθούν οποιαδήποτε στιγμή χωρίς προειδοποίηση και να συνεχίσουν να κινούνται συνεχώς και προς τυχαία κατεύθυνση. Υποθέτουμε ότι η ταχύτητα με την οποία οι κόμβοι κινούνται είναι συγκρίσιμη

(moderate) σε σχέση με την καθυστέρηση στην ασύρματη μετάδοση των πακέτων από τα χαμηλότερα επίπεδα του δικτύου. Συγκεκριμένα ο DSR μπορεί να υποστηρίξει δίκτυα στα οποία οι κόμβοι τους κινούνται με οποιαδήποτε ταχύτητα, αργά ή γρήγορα, και προς οποιαδήποτε τυχαία κατεύθυνση. Υποθέτουμε όμως ότι οι κόμβοι δεν κινούνται συνεχώς τόσο γρήγορα ώστε να αναγκάζουν το πρωτόκολλο να ενεργοποιεί για κάθε πακέτο την διαδικασία εύρεσης μίας νέας διαδρομής, με αποτέλεσμα η καθυστέρηση στη μετάδοση να είναι πολύ μεγαλύτερη από την περίπτωση χρήσης της τεχνικής της πλημμύρα κάθε μεμονωμένου πακέτου στο δίκτυο, ελπίζοντας κάποιο από αυτά να φτάσει στον προορισμό του.

2.5. Λειτουργία promiscuous mode

Υποθέτουμε ότι οι κόμβοι μπορούν να ενεργοποιήσουν την λειτουργία promiscuous mode στο υλικό της ασύρματης διεπαφής του δικτύου τους, αναγκάζοντας το να παραδίδει κάθε λαμβανόμενο πακέτο στα ανώτερα στρώματα του δικτύου, χωρίς να φιλτράρει τη διεύθυνση προορισμού των πακέτων, απορρίπτοντας όλα αυτά που δεν προορίζονται για τον συγκεκριμένο κόμβο. Με αυτόν τον τρόπο οι κόμβοι λαμβάνουν όλα τα πακέτα που μπορούν να «ακούσουν» στο ασύρματο κανάλι. Αν και δεν απαιτείται, η δυνατότητα αυτή είναι κοινή στο υλικό που χρησιμοποιείται στις δικτυακές ασύρματες κάρτες σήμερα και μερικές από τις βελτιστοποιήσεις του πρωτοκόλλου DSR μπορούν να εκμεταλλευθούν τη δυνατότητα αυτή. Η χρήση του promiscuous τρόπου μπορεί επίσης να αυξάνει την κατανάλωση ισχύς του υλικού του δικτύου, αφού πρέπει ο ασύρματος πομποδέκτης να μένει ενεργός πολύ περισσότερο χρόνο. Αν και έχει παρατηρηθεί ότι οι βελτιστοποιήσεις που έχουν γίνει κάνουν τον DSR περισσότερο αποδοτικό, το πρωτόκολλο μπορεί εύκολα να χρησιμοποιηθεί και χωρίς αυτές ή να προγραμματιστεί, ώστε να τις ενεργοποιεί περιοδικά.

2.6. Αμφίδρομη και μη-αμφίδρομη επικοινωνία

Η δυνατότητα ασύρματης επικοινωνίας μεταξύ οποιωνδήποτε κόμβων μπορεί κατά περιόδους να μην λειτουργεί εξίσου καλά και προς στις δύο κατευθύνσεις, οφειλόμενη παραδείγματος χάριν, στην χρήση διαφορετικών κεραιών σε κάθε κόμβο, παν-κατευθυντικών ή κατευθυντικών, διάδοσης των ηλεκτρομαγνητικών κυμάτων ή των πηγών παρεμβολών γύρω από τους κόμβους. Αυτό έχει σαν αποτέλεσμα η επικοινωνία μεταξύ δυο κόμβων σε πολλές περιπτώσεις να λειτουργεί και προς τις δύο κατευθύνσεις, αλλά σε άλλες να λειτουργεί μόνο προς τη μία κατεύθυνση, κάθε χρονική στιγμή, επιτρέποντας την επικοινωνία προς την μία φορά. Αν και πολλά πρωτόκολλα δρομολόγησης λειτουργούν σωστά μόνο στην πρώτη περίπτωση ο DSR μπορεί επιτυχώς να ανακαλύψει τις διαδρομές σε ένα δίκτυο και να δρομολογήσει τα πακέτα τόσο στην πρώτη όσο και στην δεύτερη περίπτωση. Αν και μερικά πρωτόκολλα περιορίζονται να χρησιμοποιούνται στην περίπτωση που χρησιμοποιείται ο ένας ή ο άλλος τύπος από συνδέσεις, ο DSR μπορεί να λειτουργήσει εξίσου καλά και αποδοτικά και με τα δύο, εκμεταλλευόμενος πρόσθετες βελτιστοποιήσεις.

2.7. Ανάθεση διευθύνσεων IP στους κόμβους του δικτύου

Κάθε κόμβος επιλέγει μια μοναδική διεύθυνση IP από την οποία αναγνωρίζεται στο δίκτυο. Αν και ένας κόμβος μπορεί να έχει πολλές διαφορετικές διεπαφές δικτύων και

όπως σε ένα κλασικό δίκτυο IP, σε κάθε μια από αυτές θα αντιστοιχούσε μια διαφορετική διεύθυνση IP, απαιτούμε από τους κόμβους, κατά την συμμετοχή στο πρωτόκολλο DSR, να επιλέξουν και να χρησιμοποιούν μόνο μία από τις διευθύνσεις αυτές. Με τον τρόπο αυτό κάθε κόμβος μπορεί να αναγνωριστεί από όλους τους υπόλοιπους στο δίκτυο, ανεξάρτητα από το ποια συγκεκριμένη διεπαφή χρησιμοποιείται. Σύμφωνα με την ορολογία που χρησιμοποιείται από το Mobile IP, αναφερόμαστε στη διεύθυνση την οποία χρησιμοποιεί κάθε κινητός κόμβος σε ένα ad-hoc δίκτυο ως «home address». Η διεύθυνση αυτή μπορεί να οριστεί από οποιοδήποτε μηχανισμό (στατική ή δυναμική ανάθεση, με χρήση DHCP). Η επιλογή της μεθόδου ανάθεσης διευθύνσεων IP είναι έξω από το πεδίο και το σκοπό του πρωτοκόλλου δρομολόγησης DSR και δεν επηρεάζει την απόδοση του.

3. Περιγραφή του πρωτοκόλλου DSR

3.1. Επισκόπηση και Σημαντικές Ιδιότητες του πρωτοκόλλου

Το πρωτόκολλο δρομολόγησης DSR αποτελείται από δύο μηχανισμούς που λειτουργούν (συνεργάζονται) ταυτόχρονα για την ανακάλυψη διαδρομών και τη διατήρηση τους σε ένα ασύρματο ad-hoc τηλεπικοινωνιακό δίκτυο.

Η εύρεση διαδρομών είναι ο μηχανισμός κατά τον οποίο ένας κόμβος S που επιθυμεί να στείλει ένα πακέτο σε έναν κόμβο προορισμού D ζητάει και λαμβάνει μια διαδρομή για τον κόμβο αυτό. Ο μηχανισμός αυτός χρησιμοποιείται μόνο όταν επιχειρεί ο κόμβος S να στείλει ένα πακέτο στον D και δεν γνωρίζει ήδη μια διαδρομή προς αυτόν.

Η συντήρηση διαδρομών είναι ο μηχανισμός κατά τον οποίο ένας κόμβος S ανιχνεύει, αν μια ήδη υπάρχουσα και χρησιμοποιούμενη διαδρομή για έναν κόμβο προορισμού D είναι σωστή ή όχι επιτρέποντας την επικοινωνία ανάμεσα τους, στην περίπτωση που η τοπολογία του δικτύου έχει αλλάξει και δεν είναι δυνατόν να χρησιμοποιηθεί η διαδρομή αυτή, επειδή κατά μήκος της διαδρομής ένα μονοπάτι δεν λειτουργεί. Όταν η διαδικασία αυτή υποδείξει μια διαδρομή η οποία σε κάποιο σημείο είναι «διακομμένη», δηλαδή μία συγκεκριμένη σύνδεση μεταξύ δύο κόμβων της διαδρομής έχει διακοπεί, ο κόμβος S μπορεί να προσπαθήσει να χρησιμοποιήσει οποιαδήποτε άλλη διαδρομή συμβαίνει να γνωρίζει για τον D ή να ενεργοποιήσει την διαδικασία εύρεσης διαδρομών για τον D. Η συντήρηση διαδρομών χρησιμοποιείται μόνο κατά την διάρκεια αποστολής δεδομένων από τον S στον D. Η εύρεση και η συντήρηση διαδρομών λειτουργούν εξ ολοκλήρου αυτόνομα και μόνο μετά από αντίστοιχη αίτηση ενός κόμβου. Ειδικότερα και αντίθετα από άλλα πρωτόκολλα, ο DSR δεν απαιτεί την ύπαρξη περιοδικά λαμβανόμενων μηνυμάτων ελέγχου, με πληροφορίες για τις αλλαγές στις διαδρομές του δικτύου, λόγω της αλλαγής της φυσικής θέσης των κόμβων, για την συντήρηση των διαδρομών που έχουν ήδη ανακαλυφθεί. Και οι δυο βασικοί μηχανισμοί λειτουργίας του πρωτοκόλλου ενεργοποιούνται μόνο μετά από σχετική απαίτηση των κόμβων του δικτύου, επιτρέποντας έτσι την κλιμάκωση της κίνησης που δημιουργούν τα πακέτα ελέγχου του DSR, για την εύρεση και συντήρηση των διαδρόμων προς το μηδέν, όταν όλοι οι κόμβοι είναι περίπου στάσιμοι και όλες οι διαδρομές που απαιτούνται για την τρέχουσα επικοινωνία έχουν ήδη ανακαλυφθεί. Αυτό σημαίνει ότι η κίνηση που δημιουργείται λόγω των πακέτων των διαδικασιών εύρεσης και συντήρησης

διαδρομών κλιμακώνεται ανάλογα και προσαρμόζεται σύμφωνα με τις ανάγκες του πρωτοκόλλου για την επιτυχή δρομολόγηση των πακέτων δεδομένων, ανάλογα με την κινητικότητα και σχετική θέση των κόμβων στο δίκτυο, (δηλ. αυξάνεται όταν παρατηρείται μεγάλη κινητικότητα και μειώνεται όταν η κινητικότητα είναι μικρή).
Οι κόμβοι συνήθως αποθηκεύουν μόνο μία διαδρομή για κάθε προορισμό μέσα σε ένα ad-hoc δίκτυο, είτε αυτή προκύπτει από την διαδικασία εύρεσης διαδρομών, είτε από τις πληροφορίες δρομολόγησης, που συλλέγουν κατά την μεταγωγή πακέτων δεδομένων. Ένας κόμβος όμως μπορεί να αποθηκεύσει πολλαπλές διαδρομές για οποιοδήποτε προορισμό. Αυτό επιτρέπει την γρήγορη αντίδραση των πρωτοκόλλων δρομολόγησης, εξαιτίας των αλλαγών των τοπολογικών χαρακτηριστικών του δικτύου, οι οποίες έχουν σαν άμεσο αποτέλεσμα την ανάγκη εύρεσης νέων διαδρομών προς τους προορισμούς. Σε μία τέτοια περίπτωση ο κόμβος μπορεί να χρησιμοποιήσει μία από τις αποθηκευμένες διαδρομές προς τον προορισμό, όταν αυτή που ήδη χρησιμοποιεί αποτύχει στην αποστολή των δεδομένων. Ο μηχανισμός αυτός δημιουργεί μικρότερη καθυστέρηση στην εύρεση μιας νέας διαδρομής, μετά από την ανακάλυψη μιας «διακομμένης» διαδρομής, από την καθυστέρηση που θα παρατηρούσαμε από την ενεργοποίηση ξανά της διαδικασίας εύρεσης διαδρομών.

Η λειτουργία της εύρεσης και της συντήρηση διαδρομών υποστηρίζονται, τόσο από ασύρματα κανάλια που λειτουργούν είτε προς την μία ή την άλλη κατεύθυνση, όσο και από κανάλια που υποστηρίζουν την μετάδοση δεδομένων ταυτόχρονα και προς τις δύο κατευθύνσεις. Ο DSR επιτρέπει σε ένα ασύρματο ad-hoc δίκτυο την ύπαρξη και των δύο τύπων ασύρματων καναλιών αφού μπορεί να λειτουργήσει εξίσου αποδοτικά και στις δύο περιπτώσεις.

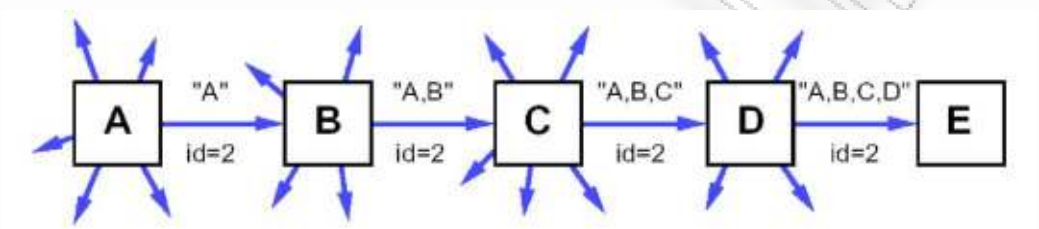
Τελειώνοντας την επισκόπηση των σημαντικότερων χαρακτηριστικών του DSR αναφέρουμε ότι υποστηρίζει επίσης και τη δια-σύνδεση ενός ασύρματου ad-hoc δικτύου με ένα οποιοδήποτε άλλο δίκτυο, διαφορετικού τύπου, επιτρέποντας σε μια διαδρομή από την πηγή προς τον κόμβο προορισμού, να μπορεί να αποτελείται από μονοπάτια κόμβων που ανήκουν είτε στο ένα είτε στο άλλο δίκτυο. Υποστηρίζει την εύρεση διαδρομών για κόμβους που βρίσκονται έξω από ένα ad-hoc δίκτυο και ανήκουν στον παγκόσμιο δικτυακό ιστό, αρκεί ο κόμβος του ad-hoc δικτύου που χρησιμοποιείται ως «πύλη» (gateway) να μπορεί να συμπληρώσει την αίτηση για το εν λόγω μονοπάτι και να επιστρέψει την πλήρη διαδρομή στην πηγή, με το κομμάτι που ανήκει στο άλλο δίκτυο. Στην περίπτωση αυτή ο κόμβος που ανήκει και στα δύο δίκτυα ονομάζεται «κόμβος πύλη» (gateway) και μπορεί να χρησιμοποιεί αλγόριθμους δρομολόγησης διαφορετικούς από τον DSR.

4. Μηχανισμός εύρεσης διαδρομών

Όταν κάποιος κόμβος S δημιουργεί ένα νέο πακέτο που προορίζεται για κάποιον άλλο κόμβο D, τοποθετεί στην επικεφαλίδα του πακέτου αυτού μια διαδρομή πηγής που δίνει την ακολουθία των κόμβων και συνδέσεων (hops), που το πακέτο πρέπει να ακολουθήσει για να φτάσει στον προορισμό του. Σύμφωνα με το πρωτόκολλο DSR, ο κόμβος S θα αποκτήσει μια κατάλληλη διαδρομή δρομολόγησης από την cache, μια ειδική μνήμη που έχει αποθηκευμένες τις διαδρομές προς τους διάφορους κόμβους του ad-hoc δικτύου, που έχει ανακαλύψει μέχρι την παρούσα χρονική στιγμή. Εάν όμως κάποια διαδρομή δεν βρίσκεται στην cache, το πρωτόκολλο θα ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών για να βρει μια νέα διαδρομή προς τον S. Σε

αυτήν την περίπτωση καλούμε τον S κόμβο προέλευσης και τον D κόμβο προορισμού του μηχανισμού εύρεσης διαδρομών.

Στην παρακάτω εικόνα περιγράφεται ένα παράδειγμα εύρεσης μιας διαδρομής, στο οποίο ένας κόμβος A προσπαθεί να ανακαλύψει μια διαδρομή προς τον κόμβο E. Για να ξεκινήσει η διαδικασία, ο κόμβος A μεταδίδει ένα μήνυμα «Route Request» προς όλους τους κόμβους οι οποίοι βρίσκονται στην εμβέλεια του. Κάθε τέτοιο μήνυμα προσδιορίζει τους κόμβους προέλευσης και προορισμού και περιέχει ένα αριθμό μοναδικό και καθορισμένο από τον κόμβο προέλευσης του κάθε αιτήματος εύρεσης μιας διαδρομής. Κάθε τέτοιο μήνυμα επίσης περιέχει ένα πεδίο στο οποίο υπάρχουν οι διευθύνσεις κάθε ενδιάμεσου κόμβου μέσω του οποίου τα αντίγραφο του αρχικού αιτήματος έχουν διαβιβαστεί και καταλήξει στον κόμβο αυτό. Αυτό το πεδίο αρχικοποιείται με έναν κενό κατάλογο όταν ενεργοποιείται η διαδικασία εύρεσης διαδρομών.



Μηχανισμός Εύρεσης Διαδρομών

Όταν ένας κόμβος λαμβάνει ένα «Route Request», εάν είναι ο κόμβος προορισμού της συγκεκριμένης διαδικασία εύρεσης διαδρομής, επιστρέφει ένα μήνυμα «Route Reply» στον κόμβο προέλευσης του αιτήματος, δίνοντας και ένα αντίγραφο του πεδίου των διαδρομών από το πακέτο του «Route Request». Όταν ο κόμβος προέλευσης λάβει το «Route Reply», αποθηκεύει στην «Route Cache» του την διαδρομή, για τη χρήση της στην μετέπειτα αποστολή των δεδομένων. Εάν ο κόμβος που λαμβάνει το «Route Request» έχει δει πρόσφατα και άλλο μήνυμα «Route Request» από τον ίδιο προορισμό με τον ίδιο αριθμό ταυτότητας στο αίτημα ή εάν διαπιστώνει ότι η διεύθυνσή του κόμβου αυτού παρατίθεται ήδη στο πεδίο διαδρομών του μηνύματος, αγνοεί το συγκεκριμένο μήνυμα και καταστρέφει το σχετικό πακέτο. Διαφορετικά, αυτός ο κόμβος επισυνάπτει τη διεύθυνσή του στο πεδίο διαδρομών στο μήνυμα «Route Request» και το προωθεί σε όλους τους κόμβους που βρίσκονται στην εμβέλεια του, με τον ίδιο αριθμό ταυτότητας του συγκεκριμένου αιτήματος, για να συνεχιστεί η διαδικασία.

Στην επιστροφή του μηνύματος «Route Reply» από τον κόμβος E, στον κόμβο A που ενεργοποίησε την διαδικασία, βλέπε στο παραπάνω σχήμα, θα προσπαθήσει να εντοπίσει και ο E μία διαδρομή προς τον A, χρησιμοποιώντας αρχικά την «Route Cache» για να εντοπίσει την διαδρομή αυτή. Εάν βρίσκεται εκεί μια διαδρομή θα τη χρησιμοποιήσει, ενώ σε διαφορετική περίπτωση θα ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών. Για να αποφύγουν πιθανές άπειρες επαναλήψεις της διαδικασίας αυτής, δηλαδή των επαναλαμβανόμενων διαδικασιών εύρεσης διαδρομών, ο κόμβος E πρέπει να μεταφέρει στο μήνυμα της αίτησης για την διαδρομή προς τον A «Route Request» και την απάντηση του, «Route Reply», στην πρότερη αίτηση από τον A. Ο κόμβος E θα μπορούσε απλά να αντιστρέψει την ακολουθία των μονοπατιών, που

υπάρχει στο πεδίο διαδρομών, της αίτησης για εύρεση της διαδρομής που έλαβε και να χρησιμοποιήσει αυτή την διαδρομή για να αποστείλει την απάντηση του στον κόμβο προέλευσης του αιτήματος, μόνο αν το πρωτόκολλο MAC, όπως αυτό του IEEE 802.11, υποστηρίζει κανάλια που επιτρέπουν την ταυτόχρονη αποστολή δεδομένων και προς τις δύο κατευθύνσεις, (δηλ μία ενεργή σύνδεση από ένα κόμβο Α στον Β, προϋποθέτει, εξαιτίας του πρωτοκόλλου MAC, ότι και η σύνδεση από τον Β στον Α είναι ενεργή). Εντούτοις στον DSR υποστηρίζονται συνδέσεις που επιτρέπουν την μεταφορά δεδομένων είτε προς την μία είτε προς την άλλη κατεύθυνση είτε και προς τις δύο, οπότε ο μηχανισμός εύρεσης των διαδρομών είναι σχεδιασμένος για να υποστηρίζει και τους δύο τύπους καναλιών επικοινωνίας.

Κατά την έναρξη του μηχανισμού ανακάλυψης διαδρομών, ο κόμβος προέλευσης του αιτήματος αποθηκεύει ένα αντίγραφο του αρχικού μηνύματος σε έναν τοπικό προσωρινό πίνακα που ονομάζεται «Send Buffer» . Ο πίνακας αυτός περιέχει ένα αντίγραφο κάθε πακέτου, που δεν μπορεί να διαβιβαστεί από τον συγκεκριμένο κόμβο, επειδή δεν υπάρχει διαθέσιμη ακόμα μια διαδρομή πηγής προς τον προορισμό του πακέτου. Κάθε τέτοιο πακέτο είναι μαρκαρισμένο με την χρονική στιγμή που τοποθετήθηκε στον «Send Buffer». Κάθε πακέτο είναι προβλεπόμενο να διαγραφεί από τον πίνακα αυτό μετά από κάποια προϋπολογισμένη περίοδο. Εάν είναι απαραίτητο να αντικαταστήσουμε κάποια εγγραφή λόγω υπέρ-πληρότητας, χρησιμοποιούμε κάποιο αλγόριθμο αντικατάστασης δεδομένων, όπως ο (First In First Out, FIFO) ή οποιοδήποτε άλλο.

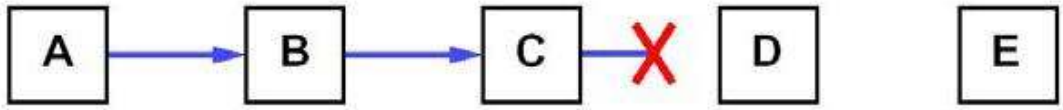
Όσο ένα πακέτο παραμένει στον «Send Buffer», ο κόμβος πρέπει περιστασιακά να φροντίσει να ενεργοποιεί ξανά τον μηχανισμό εύρεσης διαδρομών για τον προορισμό του πακέτου και ανάλογα με την πάροδο του χρόνου πρέπει να φροντίζει να μειώνει την συχνότητα ενεργοποίησης αυτής της διαδικασίας. Όταν για ένα προορισμό δεν καταφέρνουμε, για ένα μεγάλο χρονικό διάστημα, να βρούμε μία διαδρομή είναι πιθανό ο κόμβος αυτός να είναι εκτός του δικτύου και να μην είναι δυνατό να βρούμε τελικά μια τέτοια διαδρομή. Συγκεκριμένα, λόγω της περιορισμένης ασύρματης εμβέλειας των κόμβων και της κίνησης τους μέσα στο δίκτυο, κατά περιόδους το δίκτυο μπορεί να κατατμηθεί σε δύο ή περισσότερα τμήματα με αποτέλεσμα να μην υπάρχει την δεδομένη χρονική περίοδο καμία ακολουθία μονοπατιών μεταξύ των κόμβων, μέσω των οποίων ένα πακέτο θα μπορούσε να διαβιβαστεί για να φθάσει στον προορισμό του. Ανάλογα με το μοντέλο μετακίνησης των κόμβων και την πυκνότητα των κόμβων στο δίκτυο, τέτοιες κατατμήσεις στα ad-hoc δικτύων μπορούν να είναι σπάνιες ή μπορεί να συμβαίνουν συχνά.

Εάν για κάθε μια τέτοια κατάσταση ενεργοποιείται ο μηχανισμός εύρεσης διαδρομών για κάθε πακέτο, ένας πολύ μεγάλος αριθμός από μη παραγωγικά «Route requests» θα προωθούνταν σε άλλους κόμβους του δικτύου. Για την μείωση του φαινομένου αυτού χρησιμοποιούμε μια τεχνική που ονομάζεται «exponential back-off», για να περιοριστεί ο ρυθμός με τον οποίο ενεργοποιούνται οι νέες ανακαλύψεις διαδρομών από οποιοδήποτε κόμβο του δικτύου, πάντα προς τον ίδιο κόμβο προορισμού. Εάν ένας κόμβος προσπαθεί να αποστείλει πακέτα δεδομένων προς τον ίδιο κόμβο συχνότερα από ότι το σχετικό όριο επιτρέπει, τα πακέτα που δεν μπορούν να μεταδοθούν πρέπει να αποθηκευτούν στον «Send Buffer», έως ότου παραλάβει ο κόμβος αυτός ένα «Route Reply», αλλά και πάλι ο κόμβος πρέπει να μην ενεργοποιεί την αναζήτηση διαδρομών μέχρι το ελάχιστο επιτρεπόμενο όριο για τον συγκεκριμένο προορισμό επιτευχθεί.

5. Μηχανισμός συντήρησης διαδρομών στον DSR

Ο κόμβος που δημιουργεί ή προωθεί ένα πακέτο χρησιμοποιώντας μια διαδρομή πηγής, είναι αρμόδιος για την λήψη της επιβεβαίωσης, ότι το πακέτο έχει παραληφθεί επιτυχώς από τον επόμενο στη διαδρομή δρομολόγησης κόμβο. Το πακέτο αυτό μπορεί να μεταδοθεί ξανά μέχρι έναν μέγιστο αριθμό προσπαθειών έως ότου η επιβεβαίωση για την επιτυχή μετάδοση του παραληφθεί.

Στο παράδειγμα που περιγράφεται στο παρακάτω σχήμα, ο κόμβος Α έχει δημιουργήσει ένα πακέτο για να το μεταδώσει στον κόμβο Ε, χρησιμοποιώντας μια διαδρομή πηγής, μέσω των ενδιάμεσων κόμβων Β, C, και D. Σε αυτήν την περίπτωση, ο κόμβος Α είναι αρμόδιος για την λήψη του πακέτου από τον Β, ο κόμβος Β είναι αρμόδιος για την λήψη από τον C, ο κόμβος C είναι αρμόδιος για την λήψη από τον D, και ο κόμβος D είναι αρμόδιος για την παραλαβή του πακέτου τελικά από τον προορισμό Ε. Οι επιβεβαιώσεις παραλαβής των πακέτων από τον ένα κόμβο στον άλλο πάνω στο μονοπάτι της διαδρομής, σε πολλές περιπτώσεις, προσφέρονται στο πρωτόκολλο DSR χωρίς κόστος, είτε λόγω του υπάρχοντος πρωτοκόλλου MAC που χρησιμοποιείται (όπως οι επιβεβαιώσεις που υποστηρίζονται, στο επίπεδο συνδέσεων του δικτύου, από το πρότυπο της IEEE 802.11), είτε από τις λεγόμενες παθητικές επιβεβαιώσεις (passive acknowledgements), στις οποίες ένας κόμβος επιβεβαιώνει μια επιτυχημένη παραλαβή από έναν άλλο κόμβο, προσπαθώντας να ακούσει τον άλλο κόμβο να μεταδίδει το πακέτο που έλαβε επιτυχώς, με τη σειρά του, στον επόμενο κόμβο. Εάν κανένας από αυτούς τους μηχανισμούς επιβεβαίωσης δεν είναι διαθέσιμος, ο κόμβος που διαβιβάζει το πακέτο μπορεί να θέσει ένα ειδικό πεδίο, στην επικεφαλίδα του πακέτου (header), για να ζητήσει την αποστολή μιας επιβεβαίωσης από το πρωτόκολλο δρομολόγησης. Το πρόβλημα σε αυτή την περίπτωση είναι ότι εφόσον θα αναλάβει ο DSR να στείλει το μήνυμα επιβεβαίωσης, θα το κάνει χρησιμοποιώντας τις μεθόδους της μετάδοσης πακέτων δεδομένων, δηλαδή είτε θα χρησιμοποιήσει την σύνδεση ανάμεσα στους δύο κόμβους, εάν αυτή υποστηρίζει την μετάδοση δεδομένων και προς τις δύο κατευθύνσεις, ή στην περίπτωση που αυτό δεν συμβαίνει θα προσπαθήσει να εντοπίσει μια διαδρομή προς τον κόμβο αυτό, το οποίο μπορεί να έχει σαν αποτέλεσμα το μήνυμα επιβεβαίωσης να ταξιδέψει από διαφορετικό μονοπάτι.



Περίπτωση ενεργοποίησης μηχανισμού συντήρησης διαδρομών

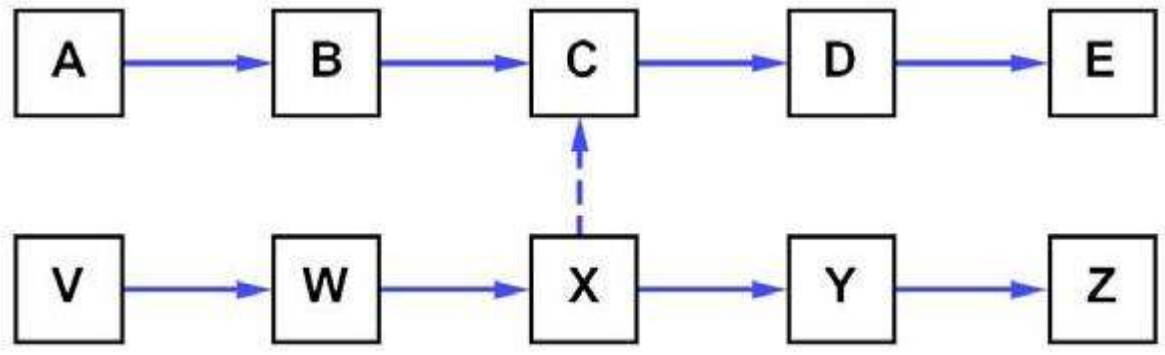
Εάν ένας κόμβος έχει να προωθήσει ένα πακέτο το οποίο έχει ξεπεράσει το μέγιστο αριθμό αναμεταδόσεων, χωρίς να έχει λάβει επιβεβαίωση για την παραλαβή του, αυτός ο κόμβος δημιουργεί ένα μήνυμα «Route Error» και το στέλνει στον κόμβο που είχε αρχικά δημιουργήσει το πακέτο αυτό. Μέσα σε αυτό το μήνυμα περιέχονται όλες οι πληροφορίες για την σύνδεση πέρα από την οποία το πακέτο δεν μπορούσε να μεταδοθεί. Στην παραπάνω εικόνα, εάν ο κόμβος C δεν καταφέρει να παραδώσει το

πακέτο που θέλει να προωθήσει στον επόμενο κόμβο D, επιστρέφει ένα μήνυμα «Route Error» στον κόμβο A, δηλώνοντας ότι η σύνδεση από τον C στον D είναι «διακομμένη». Ο κόμβος A αφαιρεί στη συνέχεια αυτήν την διαδρομή από την «Route Cache», θεωρώντας την άκυρη και οποιαδήποτε αναμετάδοση του αρχικού πακέτου στον προορισμό του είναι μια λειτουργία που θα εκτελέσουν τα ανώτερα στρώματα του δικτύου όπως το TCP, όταν το αντιληφθούν. Ο κόμβος A στην συνέχεια μπορεί να χρειαστεί μία νέα διαδρομή προς τον κόμβο E και για το λόγο αυτό πρέπει να μπορέσει να αντικαταστήσει την συγκεκριμένη διαδρομή με μία καινούρια ενεργή. Οι επιλογές που έχει είναι να χρησιμοποιήσει μία διαδρομή που βρίσκεται στην «Route Cache» του ή να ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών για τον συγκεκριμένο κόμβο, για να ανακαλύψει μια νέα διαδρομή, για να στείλει τελικά τα πακέτα δεδομένων.

6. Επιπρόσθετες λειτουργίες εύρεσης διαδρομών

6.1. Παρακολούθηση και αποθήκευση επιπρόσθετων πληροφοριών δρομολόγησης

Ένας κόμβος που προωθεί ή που παρακολουθεί οποιοδήποτε πακέτο φτάνει στον ασύρματο δέκτη του, μπορεί να προσθέσει τις πληροφορίες δρομολόγησης που περιέχονται σε εκείνο το πακέτο στην «Route Cache» του. Συγκεκριμένα, η διαδρομή πηγής που χρησιμοποιείται σε ένα πακέτο δεδομένων, η ήδη υπολογισμένη διαδρομή που υπάρχει στο πεδίο ενός μηνύματος «Route Request» και η διαδρομή που υπάρχει σε ένα μήνυμα «Route Reply», είναι οι πληροφορίες που μπορεί ένας κόμβος να αποθηκεύσει στην «Route Cache». Αυτές οι πληροφορίες μπορούν να αποθηκεύονται από οποιαδήποτε κόμβο που, είτε το πακέτο απευθύνεται σε αυτόν είτε όχι.



Περιορισμοί στην Εναποθήκευση των πληροφοριών Δρομολόγησης

Ένας περιορισμός, εντούτοις, στην αποθήκευση τέτοιων πληροφοριών δρομολόγησης είναι η ύπαρξη κατευθυνόμενων συνδέσεων στο ad-hoc δίκτυο. Παραδείγματος χάριν, το σχήμα επεξηγεί μια κατάσταση στην οποία ο κόμβος A χρησιμοποιεί μια διαδρομή πηγής για να επικοινωνήσει με τον κόμβο E. Καθώς ο κόμβος C διαβιβάζει ένα πακέτο δεδομένων, κατά μήκος της διαδρομής από τον A στον E, μπορεί να προσθέσει στην «Route Cache» του τις «προς τα εμπρός» διαδρομές που μαθαίνει προς τους κόμβους D και E. Παρόλα αυτά, οι προς τα πίσω διαδρομές που θα μπορούσε κάποιος να εξάγει από το μονοπάτι που ακολουθεί το πακέτο, από τον C προς τον B και από τον B στον A, μπορούν να μην λειτουργήσουν, επειδή οι συνδέσεις αυτές μπορεί να είναι κατευθυνόμενες προς την αντίθετη κατεύθυνση. Εάν

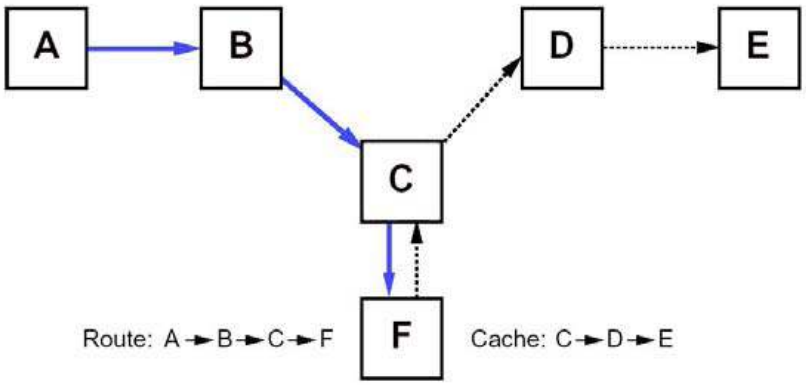
ο κόμβος C γνωρίζει ότι οι συνδέσεις είναι αμφίδρομες, παραδείγματος χάριν λόγω του πρωτόκολλου MAC που χρησιμοποιείται από τα χαμηλότερα στρώματα του δικτύου, θα μπορούσε να τις αποθηκεύσει, ενώ αν γνώριζε το αντίθετο δεν θα έπρεπε να τις κρατήσει στην «Route Cache».

Επιπλέον, ο κόμβος V στην παραπάνω εικόνα χρησιμοποιεί μια διαφορετική διαδρομή πηγής για να επικοινωνήσει με τον κόμβο Z. Εάν ο κόμβος C παρακολουθεί τα πακέτα που προέρχονται από τον κόμβο X, για να τα διαβιβάσει στον Y (από τον V), ο κόμβος C πρέπει να εξετάσει εάν οι σχετικές συνδέσεις είναι αμφίδρομες ή όχι πριν τις αποθηκεύσει. Εάν η σύνδεση από τον X στον C (σύνδεση από την οποία το πακέτο παραλήφθηκε) είναι αμφίδρομη, ο C μπορεί να αποθηκεύσει τη σύνδεση από τον ίδιο στο X, τη σύνδεση από τον X στον Y, καθώς και τη σύνδεση από τον Y στον Z. Εάν μπορούμε να υποθέσουμε ότι όλες οι συνδέσεις είναι αμφίδρομες, ο C θα μπορούσε επίσης να αποθηκεύσει τις συνδέσεις από τον X στον W και από τον W στον B.

6.2. Απαντώντας στο μήνυμα «Route Request» χρησιμοποιώντας πληροφορίες από την «Route Cache».

Ένας κόμβος που λαμβάνει ένα «Route Request» για το οποίο δεν είναι ο προορισμός, ψάχνει στην «Route Cache» του για μια διαδρομή προς τον κόμβο προορισμού. Εάν μία κατάλληλη διαδρομή εντοπιστεί, ο κόμβος επιστρέφει στον κόμβο προέλευσης ένα μήνυμα «Route Reply» αντί να προωθήσει το αίτημα που έλαβε στους γειτονικούς του κόμβους. Στο «Route Reply», θέτει το πεδίο που περιγράφει το μονοπάτι δρομολόγησης το οποίο είχε ακολουθήσει το μήνυμα «Route Request» για να φτάσει σε αυτόν τον κόμβο μαζί με το υπόλοιπο μονοπάτι που γνωρίζει και έχει αποθηκευμένο στην «Route Cache».

Εντούτοις, πριν διαβιβάζει ένα πακέτο «Route Reply», που παρήχθη χρησιμοποιώντας τις πληροφορίες που περιέχονται στην «Route Cache», πρέπει να εξασφαλιστεί ότι η προκύπτουσα διαδρομή που έχει επιλεγεί, δεν περιέχει κανέναν κόμβο παραπάνω από μία φορά, δηλαδή δεν περιέχονται κυκλικοί κλειστοί βρόγχοι στην διαδρομή. Παραδείγματος χάριν, στο παρακάτω σχήμα επεξηγείται μια περίπτωση στην οποία ένα «Route Request» για τον κόμβο E έχει παραληφθεί από τον κόμβο F, ο οποίος ήδη έχει αποθηκευμένη στην «Route Cache» του μια διαδρομή προς τον E. Εάν ο κόμβος F απαντήσει στο αίτημα, η προκύπτουσα διαδρομή σίγουρα θα περιέχει ένα βρόγχο αφού θα πρέπει τα πακέτα να περάσουν δύο φορές από τον ίδιο κόμβο.

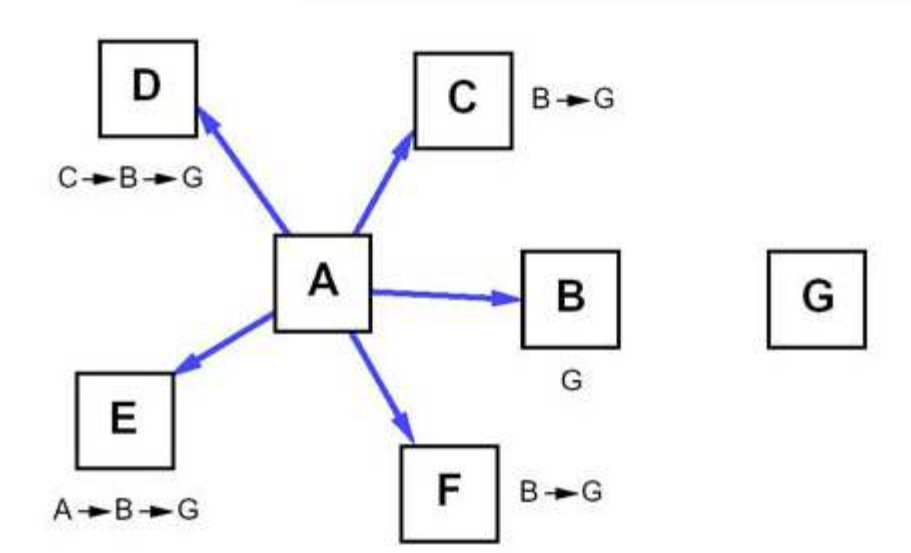


Αποφυγή Απάντησης σε Αίτημα Δρομολόγησης λόγω ύπαρξης
Διπλότυπων συνδέσεων στη Διαδρομή

Ο κόμβος F θα μπορούσε, σε αυτήν την περίπτωση, να προσπαθήσει να επεξεργαστεί τη διαδρομή και να αποβάλει τυχών βρόγχους, με συνέπεια να προκύψει μια διαδρομή από τον A στον B στον C στο D και προς το E, αλλά σε αυτήν την περίπτωση ο κόμβος F δεν θα ήταν μέρος αυτής της διαδρομής. Ο μηχανισμός εύρεσης διαδρομών στο πρωτόκολλο DSR απαγορεύει στον κόμβο F την επιστροφή μιας τέτοιας διαδρομής από την «Route Cache» του για δύο λόγους. Κατ' αρχάς, ο περιορισμός αυτός αυξάνει την πιθανότητα η προκύπτουσα διαδρομή να ισχύει, αφού ο F σε αυτήν την περίπτωση θα είχε λάβει ένα «Route Error», εάν η διαδρομή είχε σταματήσει να ισχύει. Δεύτερον, αυτός ο περιορισμός σημαίνει ότι ένα «Route Error», που διατρέχει τη διαδρομή, είναι πολύ πιθανό να περάσει μέσω οποιουδήποτε κόμβου που έστειλε το «Route Reply» για τη διαδρομή (συμπεριλαμβανομένου και του F), κάτι το οποίο βοηθάει να εξασφαλιστεί ότι, όλα τα δεδομένα δρομολόγησης, τα οποία πλέον δεν ισχύουν στις «Route Caches» των κόμβων απ' όπου περνά το μήνυμα λάθους, αφαιρούνται από αυτές (όπως στον F) κατά τρόπο έγκυρο και σωστό. Σε διαφορετική περίπτωση, η επόμενη ανακάλυψη διαδρομών που θα αρχίσει από τον A μπορεί επίσης να μολυνθεί από ένα «Route Reply» από τον F που περιέχει μία διαδρομή που δεν ισχύει. Εάν το «Route Request» δεν ικανοποιεί αυτούς τους περιορισμούς ο κόμβος το απορρίπτει και δεν το εξυπηρετεί ούτε το προωθεί σε επόμενο κόμβο (ο κόμβος F σε αυτό το παράδειγμα πρέπει να απορρίψει το «Route Request»).

6.3. Παρεμπόδιση των πολλαπλών Route Reply (Route Reply Storms)

Η δυνατότητα για τους κόμβους να απαντήσουν σε ένα «Route Request» βασισμένοι στις πληροφορίες που υπάρχουν στις «Route Caches» τους, θα μπορούσε να οδηγήσει σε πολλές περιπτώσεις σε ένα πιθανό καταιγισμό από απαντήσεις σε αιτήματα εύρεσης μιας διαδρομής «Route Reply Storms». Ειδικότερα, εάν ένας κόμβος εκπέμψει προς όλους τους κόμβους του δικτύου ένα «Route Request», για έναν κόμβο προορισμού, για τον οποίο οι γείτονες του έχουν μια διαδρομή αποθηκευμένη στην «Route Cache» τους, κάθε ένας θα προσπαθήσει να στείλει ένα «Route Reply» και με αυτόν τον τρόπο να καταναλώσει μέρος του εύρους ζώνης του ασύρματου καναλιού και έτσι να αυξήσει τον αριθμό των πιθανών συγκρούσεων στο κανάλι.



Πολλαπλά μηνύματα απάντησης διαδρομών (Route Reply Storm)

Παραδείγματος χάριν, στην κατάσταση που παρουσιάζεται στην παραπάνω εικόνα, οι κόμβοι B, C, D, E, και F λαμβάνουν το «Route Request» από τον A, για την εύρεση μιας διαδρομής προς τον G, και κάθε ένας από αυτούς έχει μια τέτοια διαδρομή προς τον G για να επιστρέψει πίσω στον A. Κάτω από κανονικές συνθήκες όλοι θα προσπαθούσαν να απαντήσουν στον A με τις διαδρομές που έχουν στις «Route Caches» τους και θα έστελναν τα «Route Reply» την ίδια περίπου χρονική στιγμή, αφού όλοι έλαβαν τα «Route Request» περίπου την ίδια στιγμή. Οι ταυτόχρονες αυτές απαντήσεις από διαφορετικούς κόμβους μπορούν να δημιουργήσουν συγκρούσεις μεταξύ μερικών ή όλων των πακέτων με τις απαντήσεις και επίσης μπορούν να προκαλέσουν συμφόρηση στο ασύρματο κανάλι. Επιπλέον, είναι πολύ πιθανό οι διαφορετικές απαντήσεις να περιγράφουν διαδρομές με διαφορετικά μήκη.

Εάν ένας κόμβος μπορεί να ενεργοποιήσει, στο υλικό της διεπαφής του δικτύου του, το promiscuous mode, λαμβάνοντας όλα τα πακέτα που μπορεί να φτάσουν σε αυτόν είτε προορίζονται για αυτόν είτε όχι, πρέπει να καθυστερήσει την μετάδοση του δικού του μηνύματος «Route Reply» για μια μικρή χρονική περίοδο, προσπαθώντας να εντοπίσει εάν ο κόμβος προέλευσης του αιτήματος έχει αρχίζει να στέλνει ήδη δεδομένα στον προορισμό χρησιμοποιώντας μια συντομότερη διαδρομή από αυτήν που έχει αυτός.

Η αποστολή του «Route Reply» πρέπει να καθυστερήσει για μια τυχαία περίοδο. Κατά την διάρκεια της καθυστέρησης ο κόμβος λαμβάνει όλα τα πακέτα τα οποία είναι στην εμβέλεια του, προσπαθώντας να εντοπίσει αυτά που έχουν κόμβους προέλευσης και προορισμού αυτούς που έχει και η διαδρομή για την οποία πρέπει να σταλεί η σχετική απάντηση. Εάν ένα τέτοιο πακέτο δεδομένων εμφανιστεί και χρησιμοποιεί διαδρομή συντομότερη από αυτή που έχει διαθέσιμη, ο κόμβος υποθέτει ότι έχει ήδη βρεθεί μια διαδρομή καλύτερη ή εξίσου καλή με αυτή που έχει επιλέξει. Σε αυτήν την περίπτωση ακυρώνεται η συγκεκριμένη διαδικασία.

6.4. Όριο προώθησης ενός «Route Request»

Κάθε μήνυμα «Route Request» περιέχει ένα αριθμό, ο οποίος αυξάνεται κάθε φορά που προωθείται αυτό από ένα κόμβο σε ένα άλλο. Ο αριθμός αυτός αυξάνεται και στην περίπτωση που ξεπεράσει ή εξισωθεί με ένα πάνω όριο οι κόμβοι σταματούν να το προωθούν και το καταστρέφουν πριν φτάσει το αίτημα στον προορισμό του. Εκμεταλλευόμενοι αυτή την ιδιότητα του πρωτοκόλλου μπορούμε να στείλουμε «Route Request» με όριο ίσο με το μηδέν. Τα αιτήματα αυτά έχουν σαν σκοπό να ανακαλύψουν εάν ο κόμβος προορισμού είναι γειτονικός με τον κόμβο προέλευσης ή αν υπάρχει στις «Route Cache» των γειτονικών κόμβων μια διαθέσιμη διαδρομή. Εάν ο κόμβος που δημιούργησε αυτή την ειδική αίτηση δεν πάρει απάντηση μέσα σε κάποιο χρονικό διάστημα ένα κανονικό μήνυμα «Route Request» στέλνεται.

7. Πρόσθετα χαρακτηριστικά γνωρίσματα συντήρησης διαδρομών

7.1. Αυτόματος περιορισμός του μήκους των διαδρομών

Οι διαδρομές που χρησιμοποιούνται από το πρωτόκολλο δρομολόγησης DSR μπορούν να γίνονται συντομότερες αυτόματα, εάν μία ή περισσότερες ενδιάμεσες συνδέσεις πάνω στη διαδρομή κριθεί ότι δεν είναι απαραίτητες. Αυτός ο μηχανισμός αυτόματης μείωσης του μήκους των διαδρομών, με την αφαίρεση μη απαραίτητων συνδέσεων που είναι σε χρήση, είναι παρόμοιος με τη χρήση των παθητικών επιβεβαιώσεων. Συγκεκριμένα, εάν ένας κόμβος παραλάβει ένα πακέτο και επεξεργαστεί την διαδρομή που περιέχει, ανακαλύπτοντας ότι ο κόμβος αυτός, στο τμήμα της διαδρομής που ακόμα δεν έχει χρησιμοποιηθεί, είναι ένας από τους προορισμούς του πακέτου, μπορεί να διαγράψει όλους τους ενδιάμεσους κόμβους και συνδέσεις, θεωρώντας ότι αυτές δεν χρειάζονται, αφού αυτός έχει ήδη λάβει το πακέτο και μπορεί να το προωθήσει στον επόμενο προορισμό του, βάση της διαδρομής πηγής που περιέχει.

7.2. Αποθηκεύοντας αρνητικές πληροφορίες

Σε μερικές περιπτώσεις, ο DSR θα μπορούσε ενδεχομένως να επωφεληθεί από τους κόμβους που αποθηκεύουν αρνητικές πληροφορίες στις «Route Caches». Παραδείγματος χάριν, εάν ένας κόμβος αποθηκεύει το γεγονός ότι μια σύνδεση είναι διακομμένη (παρά απλά να αφαιρέσει αυτή τη σύνδεση από την «Route Cache» του), μπορεί να εγγυηθεί ότι κανένα «Route Reply», που λαμβάνεται σε απάντηση για ένα αίτημα μιας διαδρομή, δεν θα γίνει αποδεκτό εάν περιέχει αυτήν την διακομμένη σύνδεση. Μια μικρή περίοδος λήξης πρέπει να εισαχθεί στις πληροφορίες αυτές, για να δώσουμε την ευκαιρία στον κόμβο να εισάγει στην «Route Cache» του ξανά μια διαδρομή που περιέχει τον εν λόγω σύνδεσμο όταν αυτός ξαναγίνει ενεργός. Επίσης είναι χρήσιμο να αποθηκεύονται αρνητικές πληροφορίες δρομολόγησης όταν μια σύνδεση, λόγω ιδιαίτερων χαρακτηριστικών, κάποιες φορές λειτουργεί σωστά και κάποιες όχι. Σε μια τέτοια περίπτωση οι κόμβοι θα μπορούσαν να χρησιμοποιούν την συγκεκριμένη σύνδεση όταν περιέχεται σε μία διαδρομή, μόνο στην περίπτωση που δεν υπάρχουν αρνητικές πληροφορίες.

8. Υποστήριξη για ετερογενή δίκτυα και το mobile IP

Στο σχηματισμό και την ανάπτυξη ενός ad-hoc δικτύου, σε πολλές περιπτώσεις, οι κόμβοι έχουν τον ίδιο τύπο ασύρματων διεπαφών δικτύου, που επιτρέπει την απλή δρομολόγηση μεταξύ των κόμβων του δικτύου, μέσω οποιοδήποτε ακολουθιών συνδέσεων μεταξύ των κόμβων.

Εντούτοις, υπάρχει και η περίπτωση το δίκτυο να αποτελείται από κόμβους που έχουν διαφορετικού τύπου διεπαφών δικτύου, με διαφορετικά χαρακτηριστικά για την κάθε μία, όπως παραδείγματος χάριν την εμβέλεια του ασύρματου πομπού, (η μια μπορεί να έχει μεγαλύτερη εμβέλεια από την άλλη). Ένα τέτοιο χαρακτηριστικό παράδειγμα έχουμε στην περίπτωση ενός ad-hoc στρατιωτικού δικτύου στο οποίο οι στρατιώτες χρησιμοποιούν περιορισμένης εμβέλειας πομπούς για να επικοινωνούν μεταξύ τους, ενώ χρησιμοποιούν πομπούς μεγαλύτερης εμβέλειας για την επικοινωνία με άλλες ομάδες.

Αυτός ο γενικός τύπος δικτύων είναι αντίστοιχος με τα δίκτυα ασύρματης επικάλυψης (wireless overlay networks). Λόγω του υψηλού βαθμού τοπικότητας που παρατηρείται μεταξύ των κόμβων που επικοινωνούν άμεσα ο ένας με τον άλλον, μια τέτοια δικτυακή σύνθεση επιτρέπει την γρήγορη επικοινωνία μεταξύ τέτοιων κόμβων, επιτρέποντας συγχρόνως την επικοινωνία και με άλλους μακρινούς κόμβους του δικτύου, χωρίς την απαίτηση για εύρεση πολύ μεγάλων διαδρομών από τον ένα κόμβο στον άλλο. Οι κόμβοι που διαθέτουν ραδιοπομπούς μεγαλύτερης εμβέλειας, επιτρέπουν την διασπορά των διαφόρων διάκενων μεταξύ των κόμβων του δικτύου μειώνοντας την πιθανότητα κατάτμηση του δικτύου εξαιτίας τους.

8.1. Χρήση δεικτών διεπαφών στον DSR

Ο DSR υποστηρίζει την αυτόματη δρομολόγηση σε ετερογενείς συνθέσεις δικτύων, μέσω του λογικού πρότυπου μοντέλου ανάθεσης διευθύνσεων του. Χρησιμοποιώντας συμβατική ανάθεση IP διευθύνσεων, κάθε κόμβος επιλέγει μια διαφορετική διεύθυνση IP για κάθε μια από τις ενδεχομένως πολλές διεπαφές δικτύων του, αλλά και κάθε κόμβος πρέπει να επιλέξει να χρησιμοποιεί σαν διεύθυνση του για την λειτουργία του πρωτοκόλλου μια από αυτές για όλη την επικοινωνία και την ανταλλαγή των μηνυμάτων του στο δίκτυο. Η χρήση μιας διεύθυνσης IP ανά κόμβο δίνει στον DSR τη δυνατότητα να μεταχειρίζεται το δίκτυο ως μια ενιαία περιοχή δρομολόγησης. Για να είναι δυνατή η διάκριση των διεπαφών δικτύων, ο κάθε κόμβος ορίζει ανεξάρτητα έναν μοναδικό δείκτη διεπαφών σε κάθε μια από αυτές. Ο δείκτης αυτός των διεπαφών είναι μια τιμή που καθορίζεται από τον ίδιο τον κόμβο και πρέπει να επιλέγεται με τέτοιο τρόπο ώστε να είναι μοναδική μόνο μεταξύ των διεπαφών του. Σε πολλά λειτουργικά συστήματα υποστηρίζεται ούτως η άλλως η λειτουργία αυτή και μπορεί να χρησιμοποιηθεί ως έχει, για να εξυπηρετήσουμε το σκοπό μας.

8.2. Διασύνδεση με το Διαδίκτυο και mobile IP

Ο DSR υποστηρίζει την δια-επικοινωνία μεταξύ ενός ad-hoc δικτύου και του διαδικτύου, επιτρέποντας στα πακέτα να δρομολογούνται με διαφανή τρόπο από το ad-hoc δίκτυο σε κόμβους του διαδικτύου και το ανάποδο. Για να είναι δυνατή αυτή η λειτουργικότητα, ένας ή περισσότεροι κόμβοι του ad-hoc δικτύου πρέπει να

συνδέονται με το διαδίκτυο, έτσι ώστε να μπορούν να συμμετέχουν στο ad-hoc δίκτυο μέσω του DSR και επίσης να συμμετέχουν στο διαδίκτυο μέσω κλασικής δρομολόγησης IP. Έναν τέτοιο κόμβο τον ονομάζουμε «πύλη» μεταξύ του ad-hoc δικτύου και του διαδικτύου. Κατ' αυτό τον τρόπο ο DSR επιτρέπει, παραδείγματος χάριν, την εξάπλωση της κάλυψης γύρω από έναν ασύρματο σταθμό βάσεων, που παίζει το ρόλο της πύλης για το διαδίκτυο, μέσω πολλαπλών συνδέσεων μεταξύ των κόμβων ενός ad-hoc δικτύου. Είναι επίσης δυνατό ένας τέτοιος κόμβος να λειτουργήσει ως «Mobile IP home agent», επιτρέποντας στους κόμβους να επισκέπτονται το ad-hoc δίκτυο, που παίζει το ρόλο ενός «Mobile IP foreign network», καθώς και στους κόμβους που αποτελούν το ad-hoc δίκτυο να επισκέπτονται άλλα δίκτυα, επίσης χρησιμοποιώντας το «Mobile IP».

5. Ο Αλγόριθμος Δρομολόγησης Ad – hoc On Demand Distance Vector (AODV)

1. Εισαγωγή

Λόγω του γεγονότος της απουσίας συσκευών δρομολόγησης σε ένα ad – hoc δίκτυο, κάθε κόμβος θα πρέπει να συνεισφέρει στην δρομολόγηση, στην ασφάλεια και γενικότερα στη ομαλή λειτουργία του δικτύου. Λόγω της απουσίας «κεντρικού ελέγχου» γίνεται πολύ ευκολότερη η διείσδυση μη εξουσιοδοτημένων μονάδων στο δίκτυο. Με άλλα λόγια οι κίνδυνοι ασφαλείας είναι πολύ μεγαλύτεροι. Επίσης η συνεχής κίνηση των κόμβων αλλά και το γεγονός χρήσης ασύρματου και όχι ενσύρματου διαύλου, συμβάλουν με τον τρόπο τους στην ανάγκη για έμφαση στην ασφάλεια αυτού του είδους των δικτύων. Αυτό αλλά και άλλα χαρακτηριστικά των ad – hoc δικτύων, κάνουν τη δρομολόγηση ένα αρκετά ενδιαφέρον πεδίο για τους ερευνητές. Ο ad – hoc On – Demand Distance Vector είναι ένας από τους ευρύτερα χρησιμοποιούμενους αλγορίθμους, αλλά και ένας αλγόριθμος που συνεχώς εξελίσσετε και συμπληρώνετε με το πέρασμα του χρόνου, κυρίως στο κομμάτι της ασφάλειας.

2. Ασφάλεια Επικοινωνίας

Σε γενικές γραμμές, δύο είναι οι πιθανές επιθέσεις σε ένα ad – hoc δίκτυο:

- Παθητικές (passive) και
- Ενεργητικές (active)

Στην πρώτη κατηγορία, ο επιτιθέμενος δεν παρεμβαίνει στο πρωτόκολλο δρομολόγησης. Αυτό που κάνει είναι να παρακολουθεί και να καταγράφει της κίνηση προσπαθώντας με τον τρόπο αυτό να εξάγει χρήσιμες γι’ αυτόν πληροφορίες σχετικά με την ιεραρχία των κόμβων, την τοπολογία του δικτύου κ.τ.λ.

Στην δεύτερη κατηγορία (active attacks), οι «επιτιθέμενοι» κόμβοι, παρεμβαίνουν στην ομαλή λειτουργία του πρωτοκόλλου, μεταβάλλοντας τις πληροφορίες δρομολόγησης, παρέχοντας εσφαλμένες πληροφορίες αλλά και προσποιούμενοι άλλους «πιστοποιημένους» κόμβους.

Σε γενικές γραμμές, κρυπτογραφικοί μηχανισμοί χρησιμοποιούνται για την προστασία των πρωτοκόλλων δρομολόγησης, με την εφαρμογή αμοιβαίων σχέσεων εμπιστοσύνης μεταξύ των κόμβων. Το πρόβλημα της ασφάλειας είναι και το βασικό πρόβλημα στα ad – hoc δίκτυα και μπορεί να χωριστεί σε δύο κατηγορίες.

- Η πρώτη κατηγορία έχει να κάνει με την ασφάλεια τις επικοινωνίας των κόμβων μεταξύ τους και
- Η δεύτερη με την ασφάλεια των δεδομένων που μεταφέρονται στο ασύρματο μέσο.

Στο κεφάλαιο αυτό θα εξετάσουμε το κλασικό πρωτόκολλο δρομολόγησης AODV αλλά και τα μειονεκτήματα ασφαλείας που αυτό περιέχει. Στη συνέχεια θα μελετήσουμε τις προτάσεις που έγιναν από διάφορους ερευνητές προς την κατεύθυνση της αύξησης του επιπέδου ασφαλείας για το πρωτόκολλο αυτό.

3. Περιγραφή του Πρωτοκόλλου AODV

Το πρωτόκολλο AODV δεν έχει ανάγκη κανενός κεντρικού συστήματος διαχείρισης για τον έλεγχο της διαδικασίας δρομολόγησης. Τα reactive πρωτόκολλα όπως το AODV τείνουν αν ελαττώνουν το φόρτο λόγω των μηνυμάτων ελέγχου κίνησης (control traffic messages) πληρώνοντας το κόστος του χρόνου που απαιτείται για την εύρεση νέων διαδρομών. Το AODV αντιδρά γρήγορα στις αλλαγές τοπολογίας του δικτύου και ενημερώνει μόνο τους κόμβους που επηρεάζονται από τις αλλαγές αυτές. Τα “Hello Messages” που χρησιμοποιεί για τον έλεγχο των συνδέσεων είναι σχετικά περιορισμένα με αποτέλεσμα να μην αυξάνουν σημαντικά την κίνηση στο δίκτυο. Ένα ακόμα σημαντικό χαρακτηριστικό του AODV είναι και ο περιορισμός κατανάλωσης ενέργειας που επιτυγχάνει, αφού ο κόμβος προορισμού απαντά μια φορά μόνο, στην πρώτη αίτηση και αγνοεί τις υπόλοιπες. Ο πίνακας δρομολόγησης διατηρεί το πολύ μία διαδρομή ανά προορισμό. Αν μία εγγραφή στον πίνακα δεν χρησιμοποιηθεί για συγκεκριμένο χρονικό διάστημα τότε παύει να ισχύει και διαγράφεται, όπως και μια μη έγκυρη διαδρομή.

Στα On – Demand πρωτόκολλα, εφαρμόζεται η τακτική κατά την οποία οι κόμβοι παρακολουθούν τη λειτουργία της δρομολόγησης και ενημερώνουν τον αποστολέα για πιθανά λάθη στην διαδρομή. Στην περίπτωση που υπάρχει διακοπή σε κάποια από τις συνδέσεις, ο κόμβος που θα το αντιληφθεί, στέλνει ένα “route error” πακέτο στον αποστολέα, ο οποίος με το που θα το παραλάβει, αφαιρεί από την cash όλες τις διαδρομές που περιέχουν την προβληματική σύνδεση και αμέσως ενεργοποιεί μια «διαδικασία εύρεσης διαδρομής». Ο αλγόριθμος AODV ελαχιστοποιεί τον αριθμό των μεταδόσεων με το να δημιουργεί της διαδρομές on – demand, όταν δηλαδή αυτές χρειάζονται, σε αντίθεση με άλλους αλγόριθμους που κάνουν το ακριβός αντίθετο.

Μπορούμε να χωρίσουμε το πρωτόκολλο AODV σε δύο φάσεις:

- Στη φάση της ανακάλυψης διαδρομών και
- Στη φάση της συντήρησης ή διαχείρισης αυτών.

Οι κόμβοι δεν εκτελούν τις διαδικασίες εύρεσης διαδρομής ή «συντήρησης» αυτών, εκτός και πρέπει να επικοινωνήσουν με κάποιον άλλο κόμβο ή χρησιμοποιούνται ως ενδιάμεσοι κατά τη διάρκεια μιας διαδρομής πακέτου.

Τοπικά μηνύματα (Hello messages) χρησιμοποιούνται για τον έλεγχο της επικοινωνίας μεταξύ γειτονικών κόμβων, γεγονός που ελαττώνει το χρόνο απόκρισης σε αιτήσεις δρομολόγησης, αλλά και ενεργοποιεί τη διαδικασία ενημέρωσης όταν αυτό κρίνεται απαραίτητο.

Οι κόμβοι καθώς και οι εγγραφές στους πίνακες δρομολόγησης εμπεριέχουν ένα αύξοντα αριθμό ο οποίος χρησιμοποιείτε για τον εντοπισμό λανθασμένων εγγραφών. Κάθε κόμβος διαχειρίζεται δύο μετρητές, τον αύξοντα αριθμό του κόμβου (node sequence number) και το μετρητή μετάδοσης (broadcast ID). Όταν ένας κόμβος θελήσει να επικοινωνήσει με κάποιον άλλο για τον οποίο δεν έχει καταχωρημένη κάποια διαδρομή, μεταδίδει ένα πακέτο - αίτηση εύρεσης διαδρομής (route request packet) στους γειτονικούς κόμβους. Το πακέτο αυτό έχει την παρακάτω μορφή:

Type	Flag	Resvd	hopcnt
Broadcast_id			
Dest_addr			
Dest_sequence_#			
Source_addr			
Source_Sequence_#			

Πακέτο εύρεσης διαδρομής (AODV)

Όπου το Source _Sequence_# δηλώνει το πόσο πρόσφατη είναι η αντίστροφη διαδρομή προς την πηγή, ενώ το Dest_sequence_# δηλώνει αντίστοιχα το πόσο πρόσφατη είναι η διαδρομή για τον προορισμό. Τα Source_addr και Dest_addr, ορίζουν τη μοναδικότητα του αιτήματος εύρεσης διαδρομής.

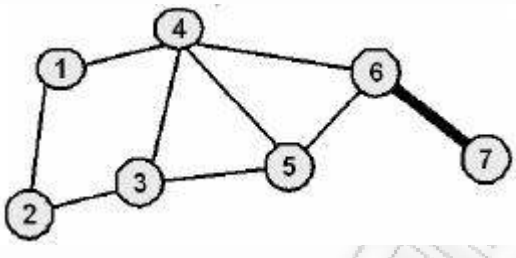
Κάθε γειτονικός κόμβος που θα παραλάβει το πακέτο:

- Επιστρέφει ένα απαντητικό πακέτο δρομολόγησης (route reply packet) αν η πληροφορία για τη διαδρομή προς τον προορισμό υπάρχει στην cache του, ή
- Προωθεί το πακέτο του αιτήματος στους δικούς του γειτονικούς κόμβους.

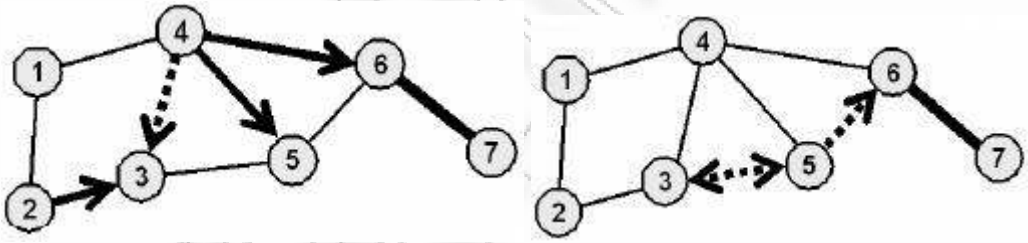
Όταν ένας κόμβος δεν μπορεί να απαντήσει στην αίτηση εύρεσης διαδρομής, τότε αυξάνει το μετρητή που αναφέρετε στον αριθμό των ενδιάμεσων κόμβων (hops) και αποθηκεύει τις πληροφορίες που έχουν να κάνουν με τη διαδρομή που θα ακολουθήσει το απαντητικό πακέτο (reverse path). Οι πληροφορίες που αποθηκεύονται είναι: Ο γειτονικός κόμβος που στέλνει το πακέτο – αίτησης εύρεσης διαδρομής, η IP διεύθυνση του κόμβου προορισμού, η IP διεύθυνση του κόμβου πηγής, ο αύξον αριθμός εκπομπής (broadcast ID), ο αριθμός του κόμβου πηγής

(source node's sequence number) και ο χρόνος πέραν του οποίου παύει να ισχύει το αντίστροφο μονοπάτι (reverse path) για την αποφυγή συγκέντρωσης άχρηστων πληροφοριών.

Για παράδειγμα, ας υποθέσουμε ότι στο παρακάτω σχήμα, ο κόμβος 1 θέλει να στείλει δεδομένα στον κόμβο 7 και ο κόμβος 6 είναι ο μόνος που γνωρίζει πληροφορίες δρομολόγησης για τον συγκεκριμένο κόμβο.



Ο κόμβος 1 λοιπόν, στέλνει ένα αίτημα εύρεσης διαδρομής στους γειτονικούς κόμβους. Με τα εξής χαρακτηριστικά: Source_addr = 1, dest_addr = 7, broadcast_id = broadcast_id + 1, source_sequence_# = source_sequence_# + 1, dest_sequence_# = last dest_sequence_# για τον κόμβο 7. Οι κόμβοι 2 και 4 με τη σειρά τους αφού βεβαιωθούν ότι πρόκειται για νέα αίτηση εύρεσης διαδρομής, προωθούν το αίτημα αφού πρώτα ενημερώσουν το source_sequence_# για τον κόμβο 1 και αυξήσουν την τιμή στο hop_cnt του πακέτου. Έτσι το πακέτο φτάνει στον κόμβο 6 (από τον κόμβο 4), ο οποίος έχει πληροφορίες δρομολόγησης για τον κόμβο 7. Ο κόμβος 6 θα πρέπει να επιβεβαιώσει ότι το dest_sequence_# είναι μικρότερο ή ίσο από αυτό που ο ίδιος γνωρίζει για τον κόμβο 7. Οι κόμβοι 3 και 5 θα προωθήσουν το αίτημα στον κόμβο 6 ο οποίος και θα αναγνωρίσει ότι πρόκειται για το ίδιο αίτημα που έλαβε από τον κόμβο 4 (duplicate packets).

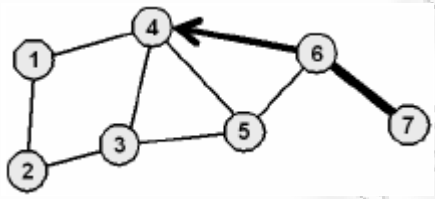


Έτσι αν κάποιος κόμβος παραλάβει ένα πακέτο – αίτηση εύρεσης νέας διαδρομής, η οποία περιέχει τη διαδρομή που μόλις ανακαλύφθηκε, τότε στέλνει ένα απαντητικό μήνυμα (route reply packet) στον γειτονικό κόμβο από τον οποίο παρέλαβε το αίτημα. Το απαντητικό μήνυμα έχει την παρακάτω μορφή:

Type	Flag	prsz	hopcnt
Dest_addr			
Dest_sequence_#			
Source_addr			
lifetime			

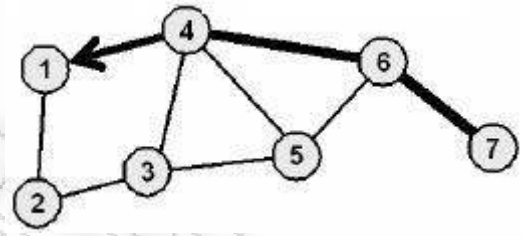
Η μορφή του Route Reply Packet στον AODV

Οι ενδιάμεσοι κόμβοι μεταδίδουν την απάντηση έως την πηγή, χρησιμοποιώντας τις ανάστροφες διαδρομές δρομολόγησης που έχουν κρατήσει στην cache (cached reverse route entries). Άλλες αιτήσεις εύρεσης διαδρομής αγνοούνται, εκτός και το dest_sequence_# είναι μεγαλύτερο από το προηγούμενο ή το dest_sequence_# είναι το ίδιο αλλά το hop_cnt μικρότερο (σε αυτή την περίπτωση σημαίνει ότι υπάρχει συντομότερη διαδρομή). Τελικά η απάντηση στο ερώτημα εύρεσης διαδρομής φτάνει στον κόμβο ο οποίος και τη ζήτησε, που με τη σειρά του χρησιμοποιεί τους γείτονες που του απάντησαν ως επόμενους κόμβους για να στείλει το μήνυμά του στον κόμβο προορισμού. Έτσι για παράδειγμα ο κόμβος 6 που γνωρίζει μια διαδρομή για τον κόμβο 7 στέλνει απάντηση στον κόμβο 4 (route reply).



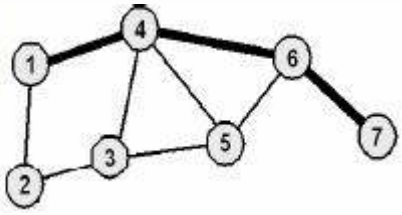
AODV Route Reply

Στην περίπτωση αυτή θα έχουμε: Source_addr = 1, dest_addr = 7, dest_sequence_# = maximum (own sequence number, dest_sequence_# στο rout request), hop_cnt = 1. Ο κόμβος 4 πιστοποιεί ότι αυτή είναι μια νέα απάντηση στο ερώτημα εύρεσης διαδρομής (στη δική μας περίπτωση) ή μια απάντηση που έχει μικρότερο hop count και μεταδίδει το πακέτο στον κόμβο 1.



Επίσης αυξάνει το hop_cnt του πακέτου. Ο κόμβος 1 έχει πλέον μια έγκυρη διαδρομή για τον κόμβο 7 με 3 ενδιάμεσους κόμβους και μπορεί να τη χρησιμοποιήσει για να στείλει data.

Dest	Next	Hops
7	4	3



Όπως είναι φυσικό η πιθανότητα να υπάρξουν αλλαγές δρομολόγησης είναι πάντα υπαρκτή και κάτι τέτοιο εντοπίζετε στην περίπτωση που υπάρχει αποτυχία κάποιου από τα περιοδικά “Hello Packets” που στέλνονται από κόμβο σε κόμβο ή αποτυχία στη μετάδοση πακέτου στον επόμενο κόμβο. Σε αυτήν την περίπτωση στέλνεται πίσω

στον κόμβο πηγής ένα πακέτο λάθους δρομολόγησης (route error packet). Ο κόμβος πηγής ή οποιοσδήποτε άλλος κόμβος της διαδρομής μπορεί να δημιουργήσει ένα νέο μονοπάτι και να διορθώσει το λάθος στέλνοντας ένα νέο πακέτο – αίτημα εύρεσης διαδρομής.

Το πρωτόκολλο AODV είναι κατάλληλο για δυναμικά δίκτυα αλλά η αλήθεια είναι ότι υπάρχει καθυστέρηση στην δημιουργία των διαδρομών δρομολόγησης αφού π.χ. μια αποτυχία μετάδοσης, μπορεί να οδηγήσει σε μια προσπάθεια δημιουργίας νέας διαδρομής.

4. Οι Διάφορες Εκδόσεις του Πρωτοκόλλου AODV

Υπάρχουν αρκετές διαφορετικές εκδόσεις του πρωτοκόλλου AODV (MAD – HOC, AODV – UCSB, AODV - UU, Kernel – AODV, AODV - UIUC). Κάθε μία από αυτές τις διαφορετικές εκδόσεις, σχεδιάστηκε και αναπτύχθηκε ανεξάρτητα από τις υπόλοιπες, όλες όμως εκτελούν τις ίδιες διεργασίες. Η πρώτη διαθέσιμη στο ευρύ κοινό έκδοση του πρωτοκόλλου, ήταν η Mad – Hoc. Δυστυχώς όμως είχε αρκετά bug με αποτέλεσμα να μην λειτουργεί σωστά και ουσιαστικά σήμερα να υπάρχει μόνο ως ιστορική αναφορά. Η πρώτη έκδοση του AODV – UCSB (University of California, Santa – Barbara), χρησιμοποιούσε τη στρατηγική της μετατροπής πυρήνα (kernel modification strategy). Το AODV – UU είχε τον ίδιο σχεδιασμό με το AODV – UCSB. Η βασική λογική της έκδοσης αυτής στηρίζεται σε έναν user – space daemon, ενώ η έκδοση AODV – UU (Uppsala University) περιέχει υποστήριξη Internet Gatewaying.

Η έκδοση AODV – UIUC είναι παρόμοια με τις AODV – UCSB και AODV – UU, εκτός από το γεγονός ότι διαχωρίζει εντελώς τις διαδικασίες routing και forwarding. Η διαδικασία του routing protocol λαμβάνει χώρα στο user – space daemon, ενώ το packet forwarding στον πυρήνα (kernel).

Όλες οι παραπάνω εκδόσεις χρησιμοποιούν τα λεγόμενα “Hello Messages” για να επιβεβαιώσουν την σύνδεση μεταξύ των κόμβων και να εντοπίσουν συνδέσεις που δεν ισχύουν πια (link breaks).

5. Μειονεκτήματα του Πρωτοκόλλου AODV

Είναι πιθανό για μια ενεργή διαδρομή να λήξη η περίοδος χρήσης της. Ο προσδιορισμός ενός λογικού χρονικού περιθωρίου, μετά το οποίο μια διαδρομή δεν θα πρέπει να χρησιμοποιείτε, είναι δύσκολη μιας και οι κόμβοι είναι κινητοί και το ποιος στέλνει που, δεν είναι δυνατόν να προβλεφθεί.

Το πρωτόκολλο AODV συγκεντρώνει ένα μικρό μόνο ποσοστό πληροφοριών δρομολόγησης. Αυτό με τη σειρά του προκαλεί πολλές φορές ένα κύμα από αιτήσεις εύρεσης διαδρομών που αρκετές φορές προκαλεί πρόβλημα στο δίκτυο (network overhead). Ένα τέτοιο κύμα που ξεφεύγει από τον έλεγχο δημιουργεί πολλές περιττές μεταδώσεις, με αποτέλεσμα το πρόβλημα να επιτείνεται.

Ένα άλλο σοβαρό μειονέκτημα του συγκεκριμένου πρωτοκόλλου (είναι κάτι που συναντούμε και σε πολλά άλλα πρωτόκολλα Ad – Hoc δικτύων) είναι και το γεγονός ότι η απόδοσή του δεν είναι και τόσο ικανοποιητική όσο μεγαλύτερο γίνεται το δίκτυο. Η βασική διαφορά ενός μεγάλου από ένα μικρό δίκτυο είναι το μήκος του

μέσου μονοπατιού (average path length). Είναι λογικό ότι ένα μεγάλο μονοπάτι είναι περισσότερο ευάλωτο στο πρόβλημα των «κομμένων συνδέσεων» (link breakages). Επίσης όσο το μέγεθος ενός δικτύου μεγαλώνει, η απόδοση του πέφτει, μιας και αυξάνονται οι διεργασίες διαχείρισης (administrative load).

Το πρωτόκολλο AODV είναι ευάλωτο σε πολλών ειδών επιθέσεις ασφαλείας, μιας και βασίζεται στην εικασία ότι όλοι οι κόμβοι είναι σε θέση να συνεργαστούν μεταξύ τους. Χωρίς τη συνεργασία αυτή καμιά δρομολόγηση δεν μπορεί να υλοποιηθεί και κανένα πακέτο να αποσταλεί. Υπάρχουν δύο ειδών κόμβοι που αρνούντε τη συνεργασία με τους υπόλοιπους: οι κακόβουλοι (malicious) και αυτοί που επιδεικνύουν ιδιοτελή συμπεριφορά (selfish). Οι κακόβουλοι, είτε δεν μπορούν να ακολουθήσουν το πρωτόκολλο επικοινωνίας, είτε προσπαθούν με διάφορους τρόπους να επιτεθούν στο δίκτυο και τις λειτουργίες του. Οι κόμβοι με την ιδιοτελή συμπεριφορά δεν συμμετέχουν σε ορισμένες λειτουργίες του δικτύου (π.χ. απορρίπτουν πακέτα για να εξοικονομήσουν ενέργεια τα οποία θα μπορούσαν να αυξήσουν την αποτελεσματικότητα του δικτύου).

6. Ασφαλής Δρομολόγηση μέσο του AODV Πρωτοκόλλου

Για να προφυλάξει το δίκτυο από διάφορες κακόβουλες επιθέσεις, το πρωτόκολλο θα πρέπει να εκπληρώνει ένα σύνολο από προϋποθέσεις και να μπορεί να βεβαιώσει ότι το μονοπάτι που οδηγεί από την πηγή στον προορισμό θα λειτουργεί χωρίς πρόβλημα, ακόμα και στην περίπτωση παρουσίας κακόβουλων κόμβων. Ορισμένες από αυτές τις προϋποθέσεις είναι και οι εξής:

- Εξουσιοδοτημένοι κόμβοι θα πρέπει να εκτελούν τη διεργασία εύρεσης διαδρομής.
- Η αποκάλυψη της τοπολογίας του δικτύου θα πρέπει να είναι από μηδενική έως ελάχιστη.
- Το πρωτόκολλο θα πρέπει να είναι σε θέση να εντοπίζει σκοπίμως αλλοιωμένα μηνύματα δρομολόγησης.
- Θα πρέπει να υπάρχει μηχανισμός αποφυγής του φαινόμενου των άσκοπων κύκλων κατά τη δρομολόγηση των πακέτων (routing loops).

Ορισμένα από τα τρωτά σημεία του πρωτοκόλλου AODV είναι τα εξής:

- Η λανθασμένη αύξηση των μετρητών (sequence numbers): Οι μετρητές προορισμού (destination sequence numbers) φανερώνουν το πόσο «φρέσκια» είναι μια διαδρομή. Οι μετρητές αυτοί μεταβάλλονται, μόνο όταν ένα νεότερο πακέτο ελέγχου παραληφθεί, ο μετρητής του οποίου είναι μεγαλύτερος. Αυτό μπορεί να έχει ως αποτέλεσμα, ένας κακόβουλος κόμβος να αυξάνει το μετρητή αυτό, με σκοπό να επιβάλλει μια νέα διαδρομή για κάποιον προορισμό.

- Η δόλια μείωση του μετρητή ενδιάμεσων σταθμών (Hop Count): Το πρωτόκολλο AODV έχει ως ισχυρότερο κριτήριο για την επιλογή, το πόσο «φρέσκια» είναι μια διαδρομή, σε αντίθεση με το μήκος αυτής. Με άλλα

λόγια ένας κόμβος θα προτιμούσε ένα πακέτο ελέγχου με μεγάλο αύξοντα αριθμό προορισμού και μετρητή ενδιάμεσων σταθμών, από ένα πακέτο με μικρότερο αύξοντα αριθμό προορισμού και μετρητή ενδιάμεσων σταθμών. Στην περίπτωση όμως που οι αύξοντες αριθμοί προορισμού είναι ίδιοι για δύο πακέτα ελέγχου, τότε η διαδρομή με το μικρότερο μετρητή ενδιάμεσων σταθμών επιλέγετε. Έτσι, ένας κακόβουλος κόμβος, θα μπορούσε να εκμεταλλευθεί το χαρακτηριστικό αυτό, μειώνοντας το μετρητή ενδιάμεσων σταθμών.

Η προσπάθεια να γίνει το πρωτόκολλο AODV περισσότερο ασφαλές χωρίστηκε σε τρεις κατηγορίες:

- Ανταλλαγή κλειδιού
- Ασφαλής Δρομολόγηση
- Προστασία Δεδομένων

Στις περισσότερες περιπτώσεις που έχουμε ανταλλαγή κλειδιού, έχουμε μια έμπιστη αρχή για την αρχική αυθεντικοποίηση. Μια παραλλαγή της κεντρικής αρχής είναι και το μοντέλο του Δημόσιου κλειδιού (Distributed Public – Key Model). Γενικά, η χρήση μιας κεντρικής έμπιστης οντότητας σε ένα τέτοιο δυναμικό περιβάλλον, μπορεί να θεωρηθεί από μη πρακτική έως και μη ασφαλής. Και αυτό γιατί μια οντότητα δεν μπορεί σε ένα τέτοιο περιβάλλον να είναι διαρκώς διαθέσιμη (π.χ. λόγω διακοπής στην επικοινωνία με κάποιο γειτονικό κόμβο). Ορισμένοι ερευνητές προτείνουν πριν την είσοδο του οποιουδήποτε κόμβου στο δίκτυο να πρέπει αυτός να παραλάβει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού από την κεντρική οντότητα, όπως και να παραλάβει και το δημόσιο κλειδί της οντότητας αυτής. Μετά από αυτό, οι κόμβοι είναι σε θέση να ανταλλάσουν κλειδιά μεταξύ τους για την πραγματοποίηση της οποιασδήποτε επικοινωνίας, χωρίς την παρέμβαση της κεντρικής οντότητας, χρησιμοποιώντας οποιοδήποτε πρωτόκολλο ανταλλαγής κλειδιών κατάλληλο για Ad – Hoc δίκτυα. Αυτού του είδους τα κλειδιά είναι χρήσιμα για την ασφάλεια της διαδικασίας που έχει να κάνει με τη δρομολόγηση και φυσικά για την ασφαλή ροή των δεδομένων. Για να αποφευχθούν πολλαπλές peer to peer κρυπτογραφήσεις κατά τη διάρκεια μαζικών μεταδόσεων, χρησιμοποιείτε ένα «ομαδικό κλειδί» χρησιμοποιώντας το κατάλληλο πρωτόκολλο για την περίπτωση των ομαδικών κλειδιών. Στην περίπτωση αυτή έχει προταθεί η ιδέα να συμμετέχουν οι γειτονικοί κόμβοι σε μια διαμοιραζόμενη διαδικασία δημιουργίας ενός ζευγαριού RSA κλειδιού.

Το βασικό πρόβλημα ασφαλείας στα Ad – Hoc δίκτυα, είναι το γεγονός ότι οι ενδιάμεσοι κόμβοι συμμετέχουν στον καθορισμό των διαδρομών. Έτσι λοιπόν κρίνετε απαραίτητο μόνο εξουσιοδοτημένοι κόμβοι να έχουν τη δυνατότητα να μεταβάλλουν τα πακέτα που καθορίζουν τη διαδικασία δρομολόγησης, έτσι ώστε να αποφευχθεί η παρέμβαση από κακόβουλους κόμβους. Η συμμετρική peer to peer κρυπτογράφηση προτάθηκε από κάποιους ερευνητές, έτσι ώστε να απαγορεύσει την αλλαγή των πακέτων που έχουν να κάνουν με την δρομολόγηση από τους ενδιάμεσους κόμβους. Όλα λοιπόν τα πακέτα που έχουν να κάνουν με την δρομολόγηση, πρώτα κρυπτογραφούνται και μετά μεταδίδονται.

7. Βελτιώσεις Ασφαλείας για το Πρωτόκολλο AODV

Υπάρχουν δύο βασικοί τύποι επιθέσεων σε ένα Ad – Hoc δίκτυο που ακολουθεί το πρωτόκολλο AODV.

- Εσωτερικές Επιθέσεις
- Εξωτερικές Επιθέσεις

Οι εσωτερικές επιθέσεις πραγματοποιούνται από κακόβουλους ή ιδιοτελής (selfish) κόμβους. Κακόβουλοι είναι οι κόμβοι που μπορούν να αυθεντικοποιηθούν από τα δίκτυο ως νόμιμοι, με αποτέλεσμα να τους εμπιστεύονται οι υπόλοιποι, αλλά την ίδια στιγμή συμπεριφέροντε με τρόπο που δημιουργεί πρόβλημα. Ιδιοτελής είναι οι κόμβοι αυτοί που έχουν την τάση να αρνούνται την παροχή υπηρεσιών που έχουν να κάνουν με τη σωστή λειτουργία του δικτύου και των πρωτοκόλλων αυτού, με σκοπό να διατηρήσουν τους ίδιους πόρους.

Οι εξωτερικές επιθέσεις πραγματοποιούνται από κακόβουλους κόμβους. Οι κόμβοι αυτοί δεν μπορούν να αυθεντικοποιήσουν τους εαυτούς τους στο δίκτυο, λόγω του γεγονότος ότι δεν διαθέτουν τις σωστές κρυπτογραφικές πληροφορίες.

Διάφορα μοντέλα έχουν προταθεί τα οποία διαχειρίζονται τις επιθέσεις ασφαλείας. Ένα από τα γνωστότερα αποτελείτε από:

- Το μοντέλο εντοπισμού της επίθεσης
- Το μοντέλο άμυνας απέναντι στις επιθέσεις

Στο μοντέλο εντοπισμού επίθεσης κάθε κόμβος ενεργοποιεί ένα μοντέλο το οποίο παρακολουθώντας τις κινήσεις των διπλανών του, προσπαθεί να εντοπίσει πιθανή ύποπτη συμπεριφορά. Όταν το όριο της μη πρέπουσας συμπεριφοράς ξεπεραστεί για κάποιον από τους κόμβους, τότε η πληροφορία για το συγκεκριμένο κόμβο αποστέλλετε και στους υπόλοιπους. Το πρωτόκολλο εντοπισμού, εφαρμόζεται σε όλους τους κόμβους του δικτύου.

Στο μοντέλο άμυνας απέναντι στις επιθέσεις, όταν κάποιος κόμβος χαρακτηριστεί ως κακόβουλος, η πληροφορία αυτή μεταδίδετε σε ολόκληρο το δίκτυο μέσο ενός Mal πακέτου. Αν οποιοσδήποτε άλλος κόμβος υποπτεύεται τον ίδιο κόμβο ως κακόβουλο, τότε μεταδίδει στο δίκτυο ένα ReMal πακέτο. Αν αυτό συμβεί δύο ή περισσότερες φορές για ένα συγκεκριμένο κόμβο, τότε ο κόμβος απομονώνεται από το δίκτυο ως κακόβουλος, με τη μετάδοση ενός Purge πακέτου.

6. Επιθέσεις σε ad – hoc Δίκτυα

1. Εισαγωγή

Όσο περισσότερο μεγαλώνει ένα ad – hoc δίκτυο, η απουσία κεντρικού ελέγχου κάνει τα προβλήματα ασφαλείας να γίνονται ολοένα και μεγαλύτερα, με αποτέλεσμα η χρησιμότητα ενός τέτοιου δικτύου να τίθεται υπό αμφισβήτηση. Στο κεφάλαιο αυτό μελετάμε τις υπάρχουσες επιθέσεις στην ασφάλεια ενός τέτοιου δικτύου, ταξινομώντας τες ταυτόχρονα στο αντίστοιχο επίπεδο δικτύου. Ένας όσο το δυνατόν ασφαλέστερος αλγόριθμος δρομολόγησης για αυτό τον τύπο δικτύων, παραμένει ακόμα και σήμερα μια περιοχή έρευνας με τεράστιο ενδιαφέρον. Δεν υπάρχει μοναδικός αλγόριθμος, που να αντιμετωπίζει με επιτυχία όλες τις γνωστές επιθέσεις όπως wormhole, rushing attack κ.τ.λ. Ένας τέτοιος αλγόριθμος θα πρέπει να περιλαμβάνει την αποτροπή, τον εντοπισμό και την ενδεδειγμένη αντίδραση ενάντια σε μια τέτοια επίθεση.

- Μηχανισμός Αποτροπής: με ένα τέτοιο μηχανισμό, οι γνωστές τακτικές όπως η αυθεντικοποίηση, ο έλεγχος πρόσβασης και η ψηφιακή υπογραφή, χρησιμοποιούνται για να παρέχουν την πρώτη γραμμή άμυνας. Άλλες τακτικές όπως έξυπνες κάρτες (με την παράλληλη χρήση PIN) ή βιομετρική επαλήθευση ταυτότητας μπορούν επίσης να χρησιμοποιηθούν.

- Μηχανισμός Αντίδρασης: ο μηχανισμός αυτός χρησιμοποιεί μεθόδους όπως IDS (Intrusion Detection System). Τέτοια συστήματα ανιχνεύουν «μη φυσιολογικές» συμπεριφορές.

2. Τύποι Επίθεσης σε ένα Ad – Hoc Δίκτυο

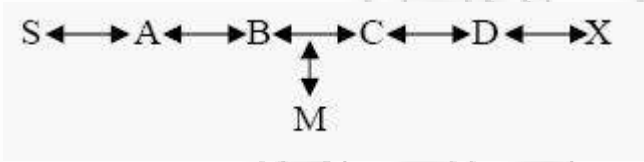
Τα Ad – Hoc Δίκτυα είναι ευάλωτα σε διαφόρων ειδών επιθέσεις. Ανάλογου τύπου επιθέσεις υπάρχουν και στα ενσύρματα δίκτυα, όμως η αντιμετώπισή τους είναι πολύ πιο εύκολη. Δύο είναι οι τύποι των επιθέσεων αυτών: δυναμικές (active) και παθητικές (passive) επιθέσεις. Δυναμική είναι η επίθεση, στην οποία ο κακόβουλος κόμβος (malicious), θα πρέπει να καταναλώσει ένα ποσό ενέργειας παραπάνω από αυτό που καταναλώνει ένας κανονικός κόμβος, για πραγματοποιήσει την επίθεση. Στις παθητικές επιθέσεις, οι κόμβοι (selfish), π.χ. δεν εκτελούν κάποιες από τις διεργασίες που είναι απαραίτητες για την ορθή λειτουργία του δικτύου, προσπαθώντας έτσι να εξοικονομήσουν ενέργεια. Οι επιθέσεις σε ένα ad – hoc δίκτυο θα μπορούσαν επίσης να χωριστούν στις παρακάτω κατηγορίες:

- Επιθέσεις Μετατροπής (Modification)
- Επιθέσεις Πλαστών Στοιχείων (Impersonation)
- Fabrication Attack

- WormHole
- Απουσία Συνεργασίας (Lack of Cooperation)

2.1 Επιθέσεις Μετατροπής

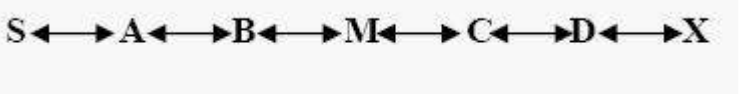
Παράδειγμα μιας επίθεσης αυτού του είδους, έχουμε π.χ. όταν ένας κακόβουλος κόμβος προωθεί την δικτυακή κίνηση, με τρόπο ώστε να πραγματοποιεί επίθεση Denial of Service (DoS), τροποποιώντας τα πεδία των μηνυμάτων. Στο παρακάτω σχήμα, ο κακόβουλος κόμβος M, αλλάζει την πορεία των πακέτων που αντί να πηγαίνουν στον κόμβο X μέσο του κόμβου C, αλλάζουν πορεία αφού ο M προτείνει συνεχώς μια «ψεύτικη» συντομότερη διαδρομή.



Ad – Hoc Δίκτυο και κακόβουλος κόμβος.

Με τον τρόπο αυτό επιτυγχάνετε υπονόμευση της δικτυακής κυκλοφορίας με αποτέλεσμα το γνωστό DoS, απλά αλλάζοντας τα πεδία του πρωτοκόλλου. Μέσο της μεθόδου αυτής, ο επιτιθέμενος μπορεί να προκαλέσει την απόρριψη πακέτων στο δίκτυο ή το να ακολουθήσουν τα πακέτα κατά πολλή μεγαλύτερες διαδρομές, με αποτέλεσμα φυσικά την άνευ λόγου καθυστέρηση στην επικοινωνία.

Στο παρακάτω σχήμα ας υποθέσουμε ότι ο κόμβος S επιθυμεί να επικοινωνήσει με τον X και ότι ο M είναι κακόβουλος κόμβος.



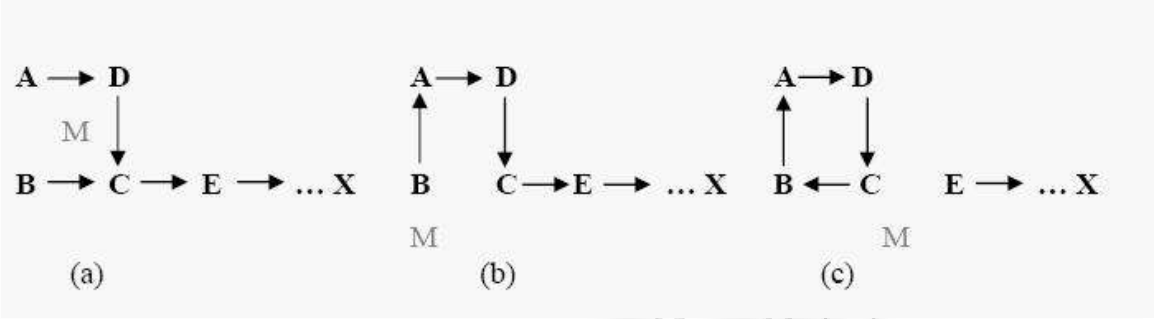
DoS σε Ad – Hoc Δίκτυο

Έστω λοιπόν ότι ο S έχει στην route cache του μια έγκυρη διαδρομή προς τον κόμβο X την S→A→B→M→C→D→X. Η διαδρομή αυτή περνάει στο header του πακέτου και μεταδίδετε από τον S. Όταν ο M παραλάβει το πακέτο μπορεί να μεταβάλλει τα περιεχόμενα του header σβήνοντας για παράδειγμα τον κόμβο D. Όταν λοιπόν το πακέτο φτάσει στον C αυτός προσπαθεί να το μεταδώσει απευθείας στον X, πράγμα αδύνατο αφού δεν υπάρχει απευθείας επικοινωνία μεταξύ των δύο κόμβων. Έτσι η επικοινωνία καταλήγει ανεπιτυχής.

2.2. Επιθέσεις Πλαστών Στοιχείων

Από τη στιγμή που δεν υπάρχει καμιά διαδικασία αυθεντικοποίησης στα Ad – Hoc δίκτυα, ένας κακόβουλος κόμβος θα μπορούσε να πραγματοποιήσει επιθέσεις παριστάνοντας έναν άλλο κόμβο του δικτύου π.χ. Spoofing. Spoofing έχουμε όταν ένας κακόβουλος κόμβος, αλλάζει την MAC ή την IP διεύθυνσή του

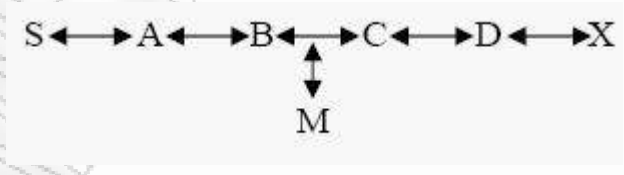
στα πακέτα που στέλνει, δημιουργώντας έτσι πρόβλημα στην κίνηση των δεδομένων στο δίκτυο. Αποτέλεσμα μιας τέτοιας επίθεσης θα μπορούσε για παράδειγμα να αποτελεί, τα πακέτα να κινούνται σε συνεχείς κύκλους, το οποίο με τη σειρά του οδηγεί στον χωρισμό του δικτύου σε μικρότερα. Παρακάτω παραθέτουμε ένα αναλυτικό παράδειγμα αυτής της περίπτωσης.



Στο παραπάνω σχήμα, ο κόμβος A μπορεί να επικοινωνήσει με τον B και τον D, ο B με τον A και τον C, ο D με τον A και τον C και ο C μπορεί να επικοινωνήσει με τους B, D και E. Ο κόμβος M μπορεί να επικοινωνήσει με τους A, B, C και D ενώ ο κόμβος E με τον C και με τον επόμενο ακριβώς κόμβο με αυτόν, προς τη μεριά του X. Ο κακόβουλος κόμβος M, μπορεί να ανακαλύψει την τοπολογία του δικτύου αναλύοντας τα discovery packets και να σχηματίσει μια αλυσίδα, τέτοια ώστε κανένας κόμβος να μην μπορεί τελικά να επικοινωνήσει με τον X.

2.3. Fabrication Attack

Ως fabrication χαρακτηρίζεται η επίθεση κατά την οποία, μια μη εξουσιοδοτημένη μονάδα, όχι μόνο αποκτά πρόσβαση αλλά και εισάγει παραχαραγμένα πακέτα στο σύστημα. Στα Ad – Hoc δίκτυα, τέτοια παραχαραγμένα πακέτα είναι για παράδειγμα οι λανθασμένες πληροφορίες δρομολόγησης. Τέτοιου είδους επιθέσεις είναι δύσκολο να αναγνωριστούν, μιας και οι κακόβουλοι κόμβοι εμφανίζονται ως εξουσιοδοτημένα μέλη του δικτύου, ειδικότερα στην περίπτωση αλλοιωμένων μηνυμάτων που υποστηρίζουν ότι δεν είναι δυνατή η επικοινωνία, με κάποιον από τους γειτονικούς κόμβους.



Έστω στο παραπάνω σχήμα ότι ο κόμβος S έχει μια διαδρομή για τον κόμβο X μέσο των A, B, C και D. Ο κακόβουλος κόμβος M μπορεί να προκαλέσει μια Denial of Service επίθεση εναντίον του X στέλνοντας route error μηνύματα στον B, παριστάνοντας τον κόμβο C, ισχυριζόμενος ότι έχει διακοπεί η επικοινωνία μεταξύ των κόμβων C και X. Ο B λαμβάνει το χαλκευμένο route error μήνυμα, νομίζοντας ότι προέρχεται από τον C και διαγράφει την εγγραφή στον πίνακα δρομολόγησής του για τον X, ενώ παράλληλα προωθεί το μήνυμα για τον δήθεν κομμένο σύνδεσμο στον A, ο οποίος με τη σειρά του σβήνει την ανάλογη εγγραφή και από τον δικό του πίνακα δρομολόγησης. Αν ο M συνεχίσει την

τακτική αυτή, κάθε φορά που επικοινωνούν ο S με τον X, τότε μπορεί να διακόψει οριστικά την επικοινωνία τους.

2.4. Απουσία Συνεργασίας

Τα Ad – Hoc δίκτυα βασίζουν τη λειτουργία τους στη συνεργασία όλων των κόμβων που τα απαρτίζουν. Όσο περισσότεροι κόμβοι συνεργάζονται για τη μεταφορά δικτυακής κίνησης τόσο περισσότερο ισχυρό είναι το δίκτυο. Μια δυσλειτουργία (εσκεμμένα) που μπορεί να παρουσιάσει ένας κόμβος είναι η «ιδιοτελής» συμπεριφορά. Ένας «ιδιοτελής» κόμβος, προσπαθεί να διατηρήσει όσο γίνετε υψηλότερα τα δικά του επίπεδα ενέργειας, ενώ ταυτόχρονα χρησιμοποιεί τις υπηρεσίες που προσφέρουν οι υπόλοιποι κόμβοι, καταναλώνοντας αρκετή από τη δική τους πολύτιμη ενέργεια. Μια τέτοια συμπεριφορά, θέτει σε κίνδυνο τη σωστή λειτουργία του δικτύου, όταν για παράδειγμα δεν εκτελείτε από κάποιον κόμβο οι προώθηση πακέτων στους γειτονικούς σε αυτόν κόμβους. Η επίθεση αυτή συναντάτε στη βιβλιογραφία και με το όνομα “Black Hole” Attack.

3. Επιθέσεις στο “Physical Layer” του Δικτύου

Η ασφάλεια στο φυσικό επίπεδο είναι πολύ σημαντική για τα Ad – Hoc δίκτυα μιας και πολλές επιθέσεις πραγματοποιούνται στο επίπεδο αυτό. Οι ποιο γνωστές από τις επιθέσεις αυτές είναι:

- Eavesdropping
- Παρεμβολή (Interference)
- Denial of Service (Άρνηση Εξυπηρέτησης)
- Jammin

Το σήμα σε ένα Ad – Hoc δίκτυο μπορεί εύκολα να αλλοιωθεί. Ένας επιτιθέμενος με επαρκή ένταση εκπομπής και γνώση του συστήματος, μπορεί να αποκτήσει πρόσβαση στο ασύρματο μέσο. Στις παραγράφους που ακολουθούν, θα περιγράψουμε τις επιθέσεις Eavesdropping, παρεμβολής και Jammin.

3.1. Eavesdropping

Eavesdropping είναι η διαδικασία κατά την οποία κάποιος δέκτης, διαβάζει μηνύματα και συνομιλίες άθελά του. Οι κόμβοι σε ένα Ad – Hoc δίκτυο μοιράζονται το ασύρματο μέσο, όπου μέσο του RF φάσματος (spectrum), γίνονται οι μεταδόσεις. Αυτές με τη σειρά τους, μπορούν να υποκλεφτούν από δέκτες συντονισμένους στην κατάλληλη συχνότητα. Εκτός όμως από αυτό, μπορεί να γίνει και το αντίστροφο. Δηλαδή “fake” μηνύματα μπορούν να μεταδοθούν στο δίκτυο.

3.2. Παρεμβολή και Jammin

Το Jammin και η παρεμβολή σε ένα σήμα μπορεί να οδηγήσει στο χαμό ή την καταστροφή ενός μηνύματος. Ένας ισχυρός πομπός μπορεί να εκπέμψει με τέτοια ισχύ ώστε να προκαλέσει πρόβλημα στην επικοινωνία μεταξύ των κόμβων σε ένα Ad – Hoc δίκτυο. Ο παλμός (pulse) και ο τυχαίος θόρυβος (random noise) είναι οι πιο κοινοί τύποι signal jamming.

4. Επιθέσεις στο Επίπεδο Σύνδεσης Δεδομένων (Link Layer)

Τα Ad – Hoc δίκτυα ακολουθούν μια peer – to – peer αρχιτεκτονική κατά την οποία, στο επίπεδο σύνδεσης δεδομένων, δημιουργείτε μια σύνδεση «1 hop» μεταξύ των γειτόνων. Πολλές επιθέσεις μπορούν να πραγματοποιηθούν στο Επίπεδο Σύνδεσης Δεδομένων διαταράσσοντας την ομαλή λειτουργία των πρωτοκόλλων του επιπέδου. Τα MAC πρωτόκολλα θα πρέπει να συντονίσουν τις εκπομπές των κόμβων στο κοινό μέσο. Το IEEE 802.11 MAC πρωτόκολλο χρησιμοποιεί μηχανισμούς κατανομής που βασίζονται σε δύο διαφορετικές λειτουργίες. Η μία είναι η Distributed Coordination Function (DCF) η οποία είναι ένα πλήρως κατανεμημένο πρωτόκολλο πρόσβασης και η δεύτερη που είναι ένα συγκεντρωτικό πρωτόκολλο και ονομάζεται Point Coordination Function (PCF).

4.1. Απειλές στο IEEE 802.11 MAC

Το 802.11 MAC είναι ευάλωτο σε επιθέσεις DoS (Denial of Service). Μια τέτοια επίθεση που θα μπορούσε να πραγματοποιηθεί προσθέτοντας bit στα πακέτα. Θα μπορούσε επίσης να πραγματοποιηθεί μέσο του πεδίου NAV (Network Allocation Vector) που υπάρχει στα πακέτα RTS/CTS (Ready to Send/ Clear to Send). Κατά τη διάρκεια της διαδικασίας RTS/CTS (Hand Shake) , ένα πακέτο που περιέχει το χρόνο που απαιτείτε για την ολοκλήρωση της CTS, δεδομένα και ACK στέλνονται από τον αποστολέα. Όλοι οι γειτονικοί κόμβοι του αποστολέα αλλά και του παραλήπτη, διορθώνουν τα NAV πεδία τους σύμφωνα με την ώρα που παρέλαβαν την διάρκεια της εκπομπής. Ένας επιτιθέμενος που βρίσκετε κοντά στην περιοχή, ενημερώνετε κι αυτός με τη σειρά του για την διάρκεια της επικοινωνίας και μπορεί να μεταδώσει ορισμένα bit μέσα στην περίοδο αυτή, για να προκαλέσει bit errors στο θύμα.

4.2. Απειλές στο IEEE 802.11 WEP

Η πρώτη ασπίδα ενάντιων των επιθέσεων που δημιουργήθηκε για το IEEE 802.11, είναι η Wired Equivalent Privacy (WEP). Αρχικά σχεδιάστηκε για να παρέχει ασφάλεια για τα WLAN. Έχει όμως αρκετά σχεδιαστικά προβλήματα και αρκετές αδυναμίες στο πως ο αλγόριθμος κρυπτογραφικής RC4 χρησιμοποιείτε στον WEP. Είναι γνωστό ότι ο WEP παρουσιάζει αδυναμίες όταν χρησιμοποιούνται τεχνικές εύρεσης του κλειδιού κρυπτογραφικής (cipher key recovery attacks). Ο WEP αντικαταστάθηκε από τον AES στο 802.11i. Κάποιες από τις αδυναμίες του WEP περιγράφονται παρακάτω:

- Δεν υπάρχει διαχείριση κλειδιού στο WEP πρωτόκολλο. Η έλλειψη αυτή είναι μεγάλο μειονέκτημα ασφαλείας, ακόμα περισσότερο όταν μιλάμε για μυστικά κλειδιά που μοιράζονται σε μεγάλους πληθυσμούς.

- Το IV (Initialization Vector) που χρησιμοποιείτε στο WEP, είναι ένα πεδίο 24bit και αποτελεί μέρος του RC4. Έτσι δίνετε η δυνατότητα στον επιτιθέμενο να χρησιμοποιήσει μεθόδους ευρέσεως κλειδιού (key recovery attack) γνωστές και ως αναλυτικές μέθοδοι.

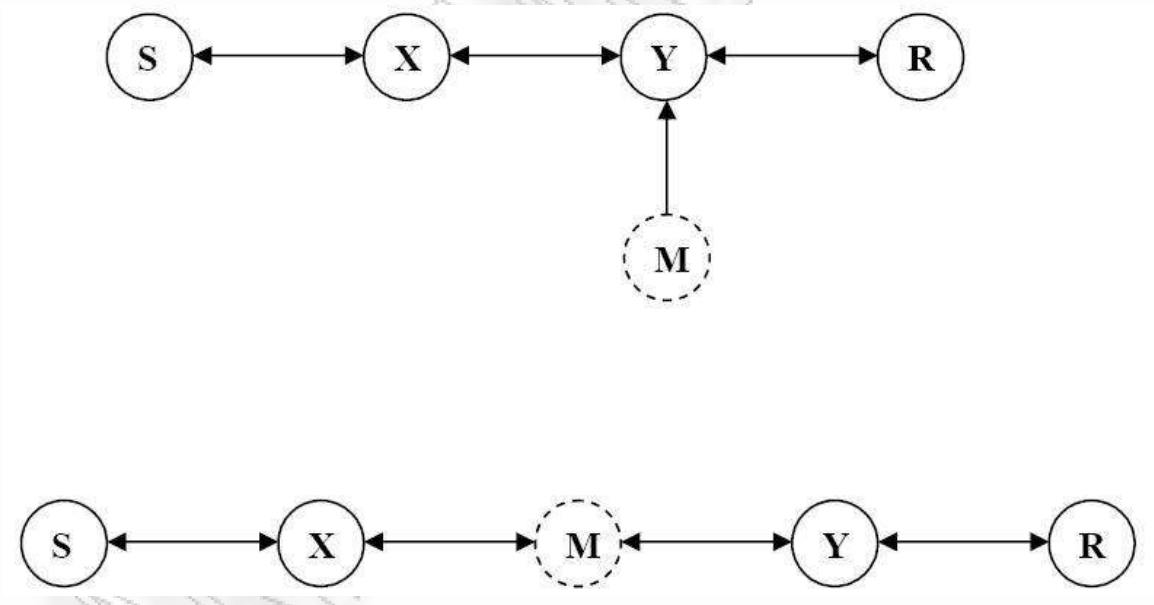
- Η συνδυασμένη χρήση ενός μη κρυπτογραφικού αλγορίθμου, CRC 32 με ένα stream chipper, είναι επίσης ένα πρόβλημα ασφαλείας.

5. Επιθέσεις Ασφαλείας στο Επίπεδο Δικτύου

Στα Ad – Hoc δίκτυα, οι κόμβοι λειτουργούν ταυτόχρονα και ως δρομολογητές που ανακαλύπτουν και διαχειρίζονται τις διαδρομές για τους κόμβους του δικτύου. Η εγκατάσταση ενός αξιόπιστου συνδέσμου μεταξύ των κόμβων που θέλουν να επικοινωνήσουν, είναι η κύρια ευθύνη του πρωτοκόλλου δρομολόγησης ενός Ad – Hoc δικτύου. Οποιαδήποτε παρεμβολή στη διαδικασία δρομολόγησης, μπορεί να επηρεάσει τη σωστή επικοινωνία και να παραλύσει ολόκληρο το δίκτυο. Άρα λοιπόν η ασφάλεια στο επίπεδο του δικτύου, παίζει σημαντικό ρόλο στην ασφάλεια ολόκληρου του δικτύου.

5.1. Επιθέσεις

Πολλές είναι οι επιθέσεις στο επίπεδο δικτύου που έχουν αναγνωριστεί και μελετηθεί στην προσπάθεια για ασφαλέστερα δίκτυα. Ένας επιτιθέμενος μπορεί να μπει ανάμεσα στον αποστολέα και τον παραλήπτη «απορροφώντας» τη δικτυακή κίνηση και να ελέγξει με τον τρόπο αυτό τη ροή των δεδομένων. Για παράδειγμα, στο παρακάτω σχήμα, ο κακόβουλος κόμβος M παρεμβάλλεται μεταξύ του αποστολέα S και του παραλήπτη R.



Routing Attack

Τα τρωτά σημεία του επιπέδου δικτύου χωρίζονται σε δύο κατηγορίες:

- Routing Attacks
- Packet Forwarding Attacks

Ως Routing Attack, αναφέρεται κάθε δραστηριότητα που προωθεί ενημερώσεις δρομολόγησης (routing updates), οι οποίες δεν καλύπτουν τις προδιαγραφές των πρωτοκόλλων δρομολόγησης.

5.1.1. Η επίθεση Routing Table Overflow

Η επίθεση αυτή λαμβάνει χώρα στους proactive αλγορίθμους, οι οποίοι όπως έχουμε αναφέρει, ανανεώνουν τις πληροφορίες δρομολόγησης περιοδικά. Για την πραγματοποίηση μιας τέτοιας επίθεσης ο επιτιθέμενος προσπαθεί να δημιουργήσει διαδρομές για μη υπαρκτούς κόμβους στο δίκτυο. Έτσι στέλνει μεγάλο αριθμό αιτήσεων και προκαλεί υπερχείλιση του πίνακα δρομολόγησης. Ο στόχος είναι να υπάρχουν τόσα δρομολόγια, ώστε η δημιουργία νέων να αποτρέπετε.

5.1.2. Routing Cache Poisoning Attack

Η επίθεση αυτή κάνει χρήση του γεγονότος ότι οι πίνακες δρομολόγησης ανανεώνονται με ανομοιογενή τρόπο. Αυτό συμβαίνει όταν οι πληροφορίες που φυλάσσονται στους πίνακες αυτούς σβήνονται, μεταβάλλονται ή «εμπλουτίζονται» με λανθασμένες πληροφορίες. Ας υποθέσουμε για παράδειγμα ότι ο κακόβουλος κόμβος Μ, θέλει να επηρεάσει τις διαδρομές προς τον κόμβο Χ. Ο Μ μπορεί να μεταδώσει πακέτα με αλλοιωμένες πληροφορίες με κόμβο πηγής τον Χ, οπότε οι γειτονικοί του κόμβοι θα προσθέσουν την διαδρομή που προτείνει ο Μ στις route caches τους.

5.2. Άλλες προηγμένες επιθέσεις

Στις πρόσφατες μελέτες, επιθέσεις προηγμένες και δυσδιάκριτες εντοπίστηκαν στα Ad – Hoc δίκτυα. Κάποια από τα πρωτόκολλα εμπλούτισαν τις υπηρεσίες τους, ενώ κάποια άλλα προτάθηκαν για να αντιμετωπίσουν τις επιθέσεις. Ο τομέας όμως αυτός εξακολουθεί να αποτελεί πεδίο ισχυρού ερευνητικού ενδιαφέροντος. Παρόλα αυτά οι επιθέσεις Blackhole, Byzantine, Wormhole και Rushing αποτελούν τυπικά παραδείγματα και περιγράφονται στις επόμενες παραγράφους.

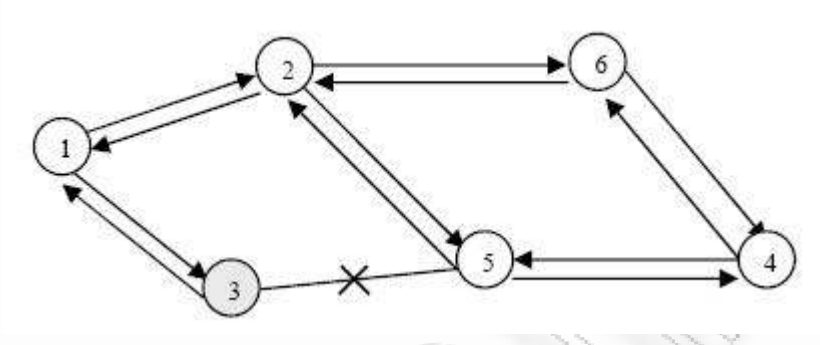
5.2.1. Η Επίθεση Wormhole

Η επίθεση Wormhole είναι επίσης γνωστή και ως επίθεση Tunneling. Ο επιτιθέμενος δημιουργεί ένα τούνελ και χρησιμοποιεί encapsulation και decapsulation για να δημιουργήσει μια ψεύτικη διαδρομή μεταξύ δύο κακόβουλων κόμβων.

5.2.2. Η Επίθεση Blackhole

Η επίθεση Blackhole πραγματοποιείτε σε δύο βήματα. Σε πρώτη φάση, ο κακόβουλος κόμβος εκμεταλλεύεται το ασύρματο Ad – Hoc πρωτόκολλο δρομολόγησης, όπως π.χ. το AODV, ισχυριζόμενος ότι κατέχει μια έγκυρη διαδρομή για τον κόμβο προορισμού. Φυσικά η διαδρομή είναι λανθασμένη και έχει ως σκοπό να ανακόψει τη σωστή κυκλοφορία των πακέτων. Σε δεύτερη φάση ο επιτιθέμενος αφού έχει δεχθεί τα πακέτα, δεν τα μεταδίδει ποτέ. Σε μια πιο προηγμένη μορφή της επίθεσης αυτής, ο επιτιθέμενος μεταβάλλει το

περιεχόμενο πακέτων που προέρχονται από ορισμένους κόμβους, ενώ κάποια άλλα τα αφήνει ως έχουν. Με τον τρόπο αυτό ο επιτιθέμενος ξεγελά τους γειτονικούς κόμβους οι οποίοι και παρακολουθούν τα εισερχόμενα μηνύματα. Στο παρακάτω σχήμα ο κόμβος 1 θέλει να στείλει πακέτα δεδομένων στον κόμβο 4 και ξεκινά την διαδικασία εύρεσης διαδρομής.



Το πρόβλημα Blackhole

Ας υποθέσουμε ότι ο κόμβος 3 είναι ένας κακόβουλος κόμβος και ισχυρίζεται ότι έχει μια έγκυρη διαδρομή για τον κόμβο προορισμού. Έτσι μόλις λάβει τα RREQ πακέτα στέλνει άμεσος απάντηση στον κόμβο 1. Αν η απάντηση από τον κόμβο 3 φτάσει πρώτη στον κόμβο 1, τότε αυτός πιστεύει ότι η διαδικασία εύρεσης διαδρομής ολοκληρώθηκε, αγνοεί όλες τις άλλες απαντήσεις που του έρχονται από τους υπόλοιπους κόμβους και στέλνει τα πακέτα στον κόμβο 3. Αυτό φυσικά έχει σαν αποτέλεσμα, όλα τα πακέτα να χάνονται στον κακόβουλο κόμβο 3.

5.2.3. Η Επίθεση Byzantine

Αυτού του είδους η επίθεση μπορεί να πραγματοποιηθεί από έναν μόνο κακόβουλο κόμβο ή από ομάδα κόμβων που συνεργάζονται για το λόγο αυτό. Μια ομάδα από κόμβους που έχουν σκοπό να παρεμποδίσουν τη σωστή λειτουργία του δικτύου, μπορούν για παράδειγμα να δημιουργούν αλυσίδες στη διαδρομή των πακέτων, να προωθούν τα πακέτα σε μακρινές διαδρομές αντί να επιλέγουν τις σωστές, ακόμα και να απορρίπτουν τα πακέτα. Η επίθεση αυτή μειώνει την απόδοση του δικτύου, και επίσης διαταράσσει τις υπηρεσίες δρομολόγησης.

5.2.4. Η Επίθεση Rushing

Στην επίθεση Wormhole, δύο επιτιθέμενοι κόμβοι σχηματίζουν μεταξύ τους τούνελ για να αλλοιώσουν την πραγματική διαδρομή. Αν για παράδειγμα η μετάδοση στο τούνελ είναι αρκετά γρήγορη, τότε τα πακέτα σε αυτό μεταδίδονται γρηγορότερα σε σύγκριση με αυτά που μεταδίδονται μέσα από μια multi – hop διαδρομή και η επίθεση καταλήγει σε Rushing. Βασικά, είναι μια άλλη μορφή της DoS (Denial of Service) επίθεσης, η οποία μπορεί να τεθεί σε

λειτουργία εναντίον όλων των ως τώρα γνωστών πρωτοκόλλων δρομολόγησης, όπως τα ARAN και Ariadne.

5.2.5. Η Επίθεση Resource Consumption

Η ενέργεια είναι ίσως η σημαντικότερη παράμετρος σε ένα Ad – Hoc δίκτυο. Οι συσκευές που έχουν σαν μόνη πηγή ενέργειας τις μπαταρίες, προσπαθούν να μην την καταναλώνουν άσκοπα, μεταδίδοντας δεδομένα μόνο όταν αυτό είναι απολύτως απαραίτητο. Ο στόχος της επίθεσης Resource Consumption είναι να αναγκάσει το θύμα με διάφορες μεθόδους να μεταδίδει – λαμβάνει πακέτα συνεχώς, έτσι ώστε να εξαντληθούν οι ενεργειακοί του πόροι.

5.2.6. Η Επίθεση Location Disclosure

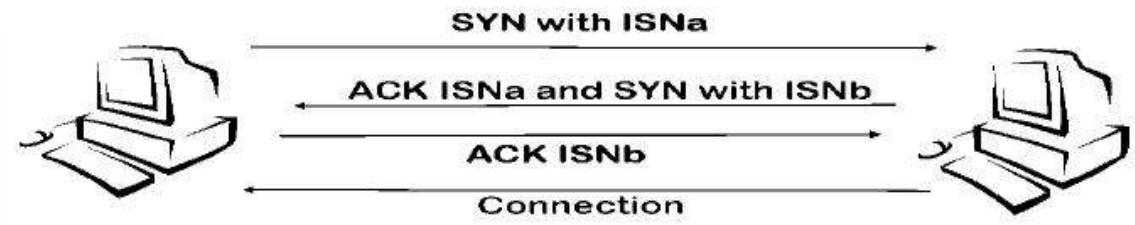
Το είδος αυτό της επίθεσης είναι μέρος της επίθεσης Information Disclosure. Ο κακόβουλος κόμβος διαβάζει πληροφορίες που αφορούν τη δομή του δικτύου και χρησιμοποιεί τις πληροφορίες αυτές για την επίθεση. Συγκεντρώνει πληροφορίες που έχουν να κάνουν με τη θέση των κόμβων και γνωρίζει ποιοι κόμβοι εμπεριέχονται σε κάθε διαδρομή. Η ανάλυση της δικτυακής κίνησης (traffic analysis) είναι μια από τις επιθέσεις που δεν έχουν ακόμα αντιμετωπιστεί στα Ad – Hoc δίκτυα.

6. Επιθέσεις Ασφαλείας στο Επίπεδο Μεταφοράς

Τα θέματα ασφαλείας που έχουν να κάνουν με το επίπεδο αναφοράς είναι η αυθεντικοποίηση, η ασφάλεια της επικοινωνίας (data encryption), ο χειρισμός των καθυστερήσεων, η απώλειες πακέτων κ.τ.λ. Το επίπεδο μεταφοράς στα Ad – Hoc δίκτυα προσφέρει μια end – to – end επικοινωνία, αξιόπιστη μεταφορά πακέτων, έλεγχο δικτυακής κίνησης, έλεγχο συμφόρησης κ.τ.λ. Όπως και στο TCP πρωτόκολλο στο Ιντερνέτ, οι κόμβοι σε ένα Ad – Hoc δίκτυο είναι ευάλωτοι στις επιθέσεις SYN Flooding και Session Hijacking. Στις επόμενες παραγράφους θα εξετάσουμε διεξοδικότερα τις απειλές – επιθέσεις στο επίπεδο μεταφοράς.

6.1. Η Επίθεση SYN Flooding

Η επίθεση SYN Flooding, είναι ένα είδος DoS επίθεσης, η οποία πραγματοποιείτε με τη δημιουργία μεγάλου αριθμού TCP συνδέσεων με τον κόμβο – στόχο. Μια TCP σύνδεση μεταξύ των δύο μερών που επικοινωνούν μεταξύ τους πραγματοποιείτε με την ολοκλήρωση μιας «χειραψίας» τριών μερών όπως φαίνετε στο παρακάτω σχήμα.



Η TCP χειραψία τριών μερών

Ο αποστολέας στέλνει ένα SYN μήνυμα στον δέκτη με ένα τυχαίο αριθμό ISN (Initial Sequence Number). Ο παραλήπτης με τη σειρά του δημιουργεί ένα ISN και στέλνει ένα άλλο SYN μήνυμα το οποίο περιέχει το ISN σαν απόδειξη της σωστής παραλαβής του μηνύματος SYN. Ο αποστολέας στη συνέχεια στέλνει ack (acknowledgement) μήνυμα στον παραλήπτη. Με τον τρόπο αυτό πραγματοποιείτε η επικοινωνία μέσο TCP.

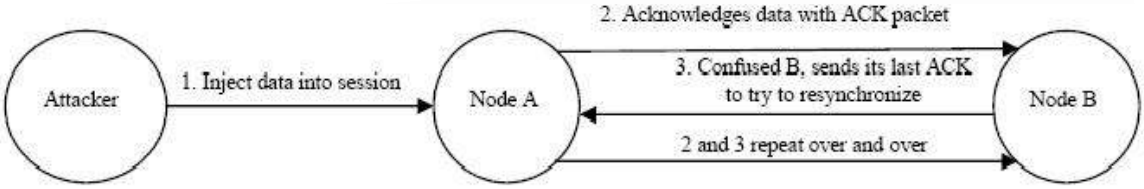
Στην επίθεση SYN Flooding, ο κακόβουλος κόμβος στέλνει μεγάλο αριθμό από πακέτα SYN στον στόχο, παραλλάσσοντας την διεύθυνση επιστροφής τον πακέτων. Όταν ο κόμβος προορισμού λάβει τα πακέτα, στέλνει SYN – ACK πακέτα στον αποστολέα και περιμένει απάντηση. Το θύμα αποθηκεύει όλα τα πακέτα σε έναν πεπερασμένου μεγέθους πίνακα καθώς περιμένει τις απαντήσεις. Αυτές οι συνδέσεις που περιμένουν απάντηση μπορούν να δημιουργήσουν πρόβλημα (overflow the buffer) και να κάνουν το σύστημα μη διαθέσιμο για αρκετή ώρα.

6.2. Η Επίθεση Session Hijacking

Η επίθεση αυτή είναι μια «τρύπα» στην ασφάλεια του συστήματος που δίνει τη δυνατότητα σε ένα κακόβουλο κόμβο να συμπεριφερθεί ως μέλος του συστήματος. Όλες οι επικοινωνίες αυθεντικοποιούντε μόνο στην αρχή τους. Ο επιτιθέμενος μπορεί να το εκμεταλλευτεί αυτό και να πραγματοποιήσει την επίθεση Session Hijack. Στην αρχή αλλοιώνει την IP διεύθυνση του στόχου και διαπιστώνει το σωστό sequence number. Στη συνέχεια πραγματοποιεί DoS επίθεση με αποτέλεσμα ο στόχος να παραμένει μη διαθέσιμος για ώρα. Έτσι ο επιτιθέμενος μπορεί να συνεχίσει να επικοινωνεί με το υπόλοιπο δίκτυο ως νόμιμος κόμβος.

6.3. TCP ACK Storm

Το είδος αυτό της επίθεσης είναι πολύ απλό. Για να πραγματοποιηθεί όμως, ο επιτιθέμενος ξεκινάει μια Session Hijacking επίθεση στην αρχή. Όπως φαίνετε στην παρακάτω εικόνα,



Η επίθεση TCP ACK Storm

ο επιτιθέμενος στέλνει δεδομένα και ο κόμβος Α επιβεβαιώνει ότι τα έλαβε με ένα ACK πακέτο στον κόμβο Β. Ο κόμβος Β μπερδεύετε, μιας και το πακέτο περιέχει μη αναμενόμενο σειριακό αριθμό και προσπαθεί να επανασυγχρονιστεί με τον Α, στέλνοντας ένα ACK πακέτο το οποίο και περιέχει τον επιδιωκόμενο αριθμό. Η διαδικασία όμως αυτή επαναλαμβάνεται επ' άπειρον και αποτελεί την TCP ACK Storm.

7. Επιθέσεις Ασφαλείας στο Επίπεδο Εφαρμογών

Οι εφαρμογές θα πρέπει να σχεδιαστούν ώστε να διαχειρίζονται με επιτυχία προβλήματα όπως συχνές διακοπές στη σύνδεση, καθυστερήσεις στη μεταφορά των δεδομένων, αλλά και απώλειες πακέτων. Όπως και άλλα επίπεδα, έτσι και το επίπεδο εφαρμογών, αποτελεί πειρασμό για τους εχθρούς ενός δικτύου. Λόγο του γεγονότος ότι το επίπεδο αυτό περιέχει δεδομένα χρηστών που υποστηρίζουν πολλά πρωτόκολλα όπως SMTP, HTTP, TELNET και FTP, τα οποία έχουν πολλές αδυναμίες, αποτελεί τρωτό σημείο ενός δικτύου. Οι γνωστότερες επιθέσεις στο επίπεδο αυτό είναι η επίθεση κακόβουλου κώδικα (malicious code attack) και η επίθεση άρνησης συμμόρφωσης (repudiation attack).

7.1. Η Επίθεση Κακόβουλου Κώδικα

Υπάρχουν πολλές μορφές κακόβουλου κώδικα όπως virus, worm, spy – wares και Trojan Horse που μπορούν να προκαλέσουν την σημαντική μείωση της απόδοσης ή ακόμα και την κατάρρευση ενός υπολογιστικού συστήματος ή ενός δικτύου. Ένας επιτιθέμενος λοιπόν, μπορεί να εξαπολύσει μια τέτοιου είδους επίθεση σε ένα Ad – Hoc δίκτυο.

7.2. Repudiation Attack

Η λύση που προτάθηκε για την επίλυση του προβλήματος αυθεντικοποίησης στο επίπεδο δικτύου και στο επίπεδο μεταφοράς δεν ήταν αρκετή. Αυτό οφείλετε στο ότι η επίθεση Repudiation, έχει να κάνει με την άρνηση συμμετοχής στην επικοινωνία. Παράδειγμα τέτοιας συμπεριφοράς σε θέματα εμπορείου, θα μπορούσε για παράδειγμα να αποτελεί ένα άτομο, που αρνείται μια αγορά μέσο πιστωτικής κάρτας ή που αρνείται τις ηλεκτρονικές συναλλαγές του.

7. Αντιμετώπιση Επιθέσεων

Η ασφαλής δρομολόγηση (routing) είναι απαραίτητη για την αποδοχή και χρήση των Ad – Hoc δικτύων για πολλές εφαρμογές, αλλά τα τωρινά προτεινόμενα πρωτόκολλα δρομολόγησης ,για αυτά τα δίκτυα, είναι ανασφαλή. Ο σχεδιασμός ενός πρωτόκολλου δρομολόγησης το οποίο να ικανοποιεί τους προτεινόμενους στόχους ασφαλείας είναι ένα ανοιχτό πρόβλημα. Η κωδικοποίηση ζεύξης στρώματος και οι μηχανισμοί αυθεντικότητας μπορεί να είναι μια πρώτη λογική προσέγγιση για άμυνα από mote-class insiders, άλλα η κρυπτογράφηση, από μόνη της, δεν είναι αρκετή. Η πιθανή παρουσία εχθρών με lap-top, insiders και η περιορισμένη συσχέτιση μηχανισμών ασφαλείας end-to-end απαιτούν προσεκτικό σχεδιασμό πρωτοκόλλων.

1. Συστήματα Ανίχνευσης Επιθέσεων (IDS)

Τα συστήματα ανίχνευσης επιθέσεων (Intrusion Detection Systems), αν και δεν είναι καινούργια, τα τελευταία χρόνια άρχισαν να εφαρμόζονται στα Ad – Hoc δίκτυα. Τα συστήματα ανίχνευσης απειλών είναι προϊόντα με μορφή λογισμικού ή και υλικού, τα οποία αυτοματοποιούν τη διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε παράνομες δραστηριότητες. Τα συστήματα αυτά συλλέγουν πληροφορίες και στη συνέχεια τις αναλύουν για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης. Όταν το σύστημα ανίχνευσης εισβολών συλλέγει πληροφορίες για το δίκτυο και προσπαθεί να αποφανθεί για το αν δέχεται επίθεση ή όχι, τότε έχουμε «δικτυακό σύστημα ανίχνευσης εισβολής» (Network Based IDS). Ενώ όταν συλλέγονται και επεξεργάζονται πληροφορίες σε επίπεδο υπολογιστή - διακομιστή για να αποφασίσει αν το σύστημα δέχεται επίθεση, τότε έχουμε «σύστημα ανίχνευσης εισβολής εγκατεστημένο σε υπολογιστή» (Host Based IDS).

1.1 Πλαίσιο Λειτουργίας IDS Συστημάτων

Η ομαλή λειτουργία ενός δικτύου θέτει τα πλαίσια δραστηριοτήτων των Σ.Α.Ε.. Απαραίτητη προϋπόθεση για την σωστή λειτουργία ενός Σ.Α.Ε. είναι η τήρηση συγκεκριμένων χαρακτηριστικών από το δίκτυο.
Γενικά χαρακτηριστικά:

- Οι ενέργειες των κόμβων και οι διεργασίες που εκτελούνται από δίκτυο θα πρέπει να ακολουθούν έναν στατιστικά προβλέψιμο πρότυπο.

- Οι ενέργειες των κόμβων δεν θα πρέπει σε καμία περίπτωση να υπονομεύουν την πολιτική ασφαλείας του δικτύου.

- Κάθε ομάδα κόμβων χρησιμοποιεί συγκεκριμένο σύνολο εντολών εντός των επιτρεπτών ορίων. Ένα παράδειγμα από την καθημερινή ζωή για την συγκεκριμένη περίπτωση, θα μπορούσε π.χ. να αποτελεί το γεγονός, ένας πελάτης να εισάγει εντολές συντήρησης ενός συστήματος.

Αν το δίκτυο δέχεται επίθεση, τότε κάποιο από τα παραπάνω χαρακτηριστικά δεν τηρείται. Τα Σ.Α.Ε. στηρίζουν την επιτήρηση τους στη πληρότητα των χαρακτηριστικών αυτών. Συνεπώς τα παραπάνω, γενικά χαρακτηριστικά, είναι προαπαιτούμενα για την ομαλή λειτουργία ενός Σ.Α.Ε..

1.2. Γενικά Χαρακτηριστικά IDS

Κάθε τύπος συστήματος ανίχνευσης εισβολών έχει ένα συγκεκριμένο τρόπο λειτουργίας. Το σύστημα αποτελείται από διαφορετικά αλληλοσυνδεόμενα μέρη. Κάθε ένα από αυτό έχει επωμιστεί με τη διεκπεραίωση κάποιας υπηρεσίας. Ένα τυπικό IDS περιλαμβάνει τα ακόλουθα:

- Μηχανισμό συλλογής πρωτογενούς πληροφορίας. Στόχος του είναι η σύλληψη των συμβάντων και η συλλογή των πληροφοριών σχετικά με αυτά. Σε ένα δίκτυο η αποστολή δεδομένων από ένα κόμβο, αποτελεί ένα συμβάν και τα δεδομένα την πληροφορία του συμβάντος.

- Μηχανισμό επεξεργασίας των πληροφοριών. Η επεξεργασία των πληροφοριών είναι το πιο νευραλγικό τμήμα διότι αναλύει διεξοδικά τα στοιχεία που συλλέχθηκαν από το προηγούμενο τμήμα και λαμβάνει την απόφαση για την λήψη δράσης ή όχι.

- Μηχανισμό αντίμετρων. Ο μηχανισμός αυτός αναπτύσσεται σε περίπτωση αναγνώρισης εισβολής. Ειδοποιεί το αρμόδιο προσωπικό ή αυτοματοποιημένα λαμβάνει δράση έναντι του επιτιθέμενου.

- Μηχανισμό αποθήκευσης και ανάκλησης των πληροφοριών. Η αποθήκευση των πληροφοριών και των αντίμετρων που πιθανώς αναπτύχθηκαν εξυπηρετεί σκοπούς διατήρησης αρχείου. Αποθηκεύονται σε βάσεις δεδομένων ή σε αρχεία τύπου ημερολογίου για περαιτέρω χρήση ή ανάλυση. Ουσιαστικά αποτελούν το ιστορικό του συστήματος.

Το ιδανικό σύστημα ανίχνευσης επίθεσης θα πρέπει να καλύπτει συγκεκριμένα κριτήρια. Για να επιτευχθεί ο μέγιστος βαθμός προστασίας και ευελιξίας ενός IDS απαιτείται, κατά τη φάση της ανάπτυξης του, να λαμβάνονται υπόψη τα παρακάτω χαρακτηριστικά στοιχεία:

- Το IDS θα πρέπει να έχει μεγάλο εύρος ανίχνευσης απειλών. Αν αυτό δεν είναι εφικτό κατά τα πρώτα στάδια ανάπτυξης του, μπορεί να ενσωματωθεί μηχανισμός εκμάθησης. Είναι σπουδαίο πλεονέκτημα το IDS να έχει τη δυνατότητα προσαρμογής σε νέες απειλές ή αλλαγές της συμπεριφοράς των κόμβων

- Επίσης, θα πρέπει να ανιχνεύει έγκαιρα τις επιθέσεις. Διακρίνονται δύο κατηγορίες IDS. Η πρώτη λειτουργεί off - line και συνεπώς μπορεί να ενημερώσει για επίθεση μόνο αφού έχει ήδη γίνει. Η δεύτερη λειτουργεί runtime έχοντας την δυνατότητα προειδοποίησης ακόμη και πριν εκδηλωθεί μία επίθεση. Περισσότερες λεπτομέρειες θα δοθούν παρακάτω.

- Πρέπει να έχει όσο το δυνατό λιγότερους εσφαλμένους συναγερμούς (false positive / negative alarm), δηλαδή ότι το δίκτυο δέχεται επίθεση, ενώ κάτι τέτοιο δεν συμβαίνει. Χαμηλός ρυθμός εσφαλμένων συναγερμών συνιστά ένα ακριβές σύστημα. Πρέπει να σημειωθεί ότι η ακρίβεια ενός IDS είναι πολλές φορές παραμετροποιήσιμη.

- Το IDS θα πρέπει να έχει τη δυνατότητα να διαχειρίζεται αυτόνομα τα σφάλματα του. Όπως κάθε λογισμικό έτσι και σε αυτή τη περίπτωση επιβάλλεται η ορθή αντιμετώπιση των σφαλμάτων. Τη στιγμή που θα παρουσιάσει σφάλμα το σύστημα θα πρέπει να διακοπεί οποιαδήποτε συναλλαγή στο δίκτυο και στη συνέχεια να επανέρχεται χωρίς ανθρώπινη παρέμβαση στη κατάσταση που ήταν πριν αυτό.

- Όσο είναι δυνατό θα πρέπει να είναι ανεξάρτητο πλατφόρμας (cross compatibility).

- Τέλος, το IDS θα πρέπει να εκτελείται καταναλώνοντας όσο το δυνατό λιγότερους πόρους συστήματος. Ιδιαίτερα σοβαρό θέμα, καθώς η συνεχής λειτουργία του παράλληλα με του δικτύου, χωρίς σωστή διαχείριση πόρων, μπορεί να προκαλέσει κατάρρευση του ίδιου του δικτύου.

Η αξιολόγηση ενός IDS μπορεί να βασιστεί στα προαναφερθέντα χαρακτηριστικά.

1.3. Ταξηνόμηση IDS

Τα συστήματα ανίχνευσης επίθεσης δύναται να ταξινομηθούν με βάση το μοντέλο συμπεριφοράς που ακολουθούν.

Ως μοντέλο συμπεριφοράς ορίζεται το πρότυπο του τυπικού κόμβου του δικτύου που προστατεύουν. Τα IDS χρησιμοποιούν μοντέλα συμπεριφοράς για την «μέτρηση» της απόκλισης της παρατηρούμενης συμπεριφοράς με την καταχωρημένη. Αυτά τα συστήματα καλούνται μοντέλα ανίχνευσης διαταραχών (anomaly detection).

Το άλλο είδος IDS χρησιμοποιεί μοντέλα συμπεριφοράς για τη σύγκριση των καταγραφόμενων ενεργειών ενός κόμβου με καταχωρημένες υπογραφές γνωστών απειλών. Αυτά ονομάζονται μοντέλα κακής συμπεριφοράς (misuse detection /

signature detection). Στην πράξη τα προαναφερθέντα μοντέλα συνδυάζονται συχνά μεταξύ τους.

1.4. Μοντέλα ανίχνευσης Διαταραχών

Τα μοντέλα ανίχνευσης διαταραχών θεωρούν ότι η απροσδόκητη συμπεριφορά αποτελεί τεκμήριο επίθεσης. Η λήψη απόφασης γίνεται με στατιστική επεξεργασία των ενεργειών των κόμβων.

Μία υποκατηγορία αυτών των μοντέλων, είναι τα μοντέλα κατωφλίου (threshold detection). Αυτού του είδους τα μοντέλα λαμβάνουν απόφαση για τη λήψη μέτρων με βάση κάποιες προκαθορισμένες τιμές κατωφλίου. Στην εμφάνιση ενός αναμενόμενου γεγονότος αποδίδεται ένα όριο τιμών, αν το γεγονός συμβεί με τιμή εκτός ορίων τότε σημάνει συναγερμός. Αυτό βοηθά στην εύκολη παραμετροποίηση, ενώ αυξάνει την πολυπλοκότητα του μοντέλου.

Μία ακόμα υποκατηγορία είναι τα μοντέλα στατιστικών ροπών. Το μοντέλο αυτό χρησιμοποιεί στατιστικές ροπές. Ο αναλυτής γνωρίζει τον μέσο και την τυπική απόκλιση (οι δύο πρώτες ροπές) και πιθανότατα άλλα μέτρα συσχέτισης (ροπές υψηλότερης τάξης). Αν οι τιμές βρίσκονται εκτός του αναμενόμενου διαστήματος γι' αυτή τη ροπή, η συμπεριφορά που αντιπροσωπεύουν οι τιμές θεωρείται διαταραγμένη. Επειδή η κατανομή της περιγραφής του συστήματος μπορεί να εμπεριέχει καθυστερήσεις, τα μοντέλα ανίχνευσης διαταραχών συνυπολογίζουν αυτές τις αλλαγές τροποποιώντας τους στατιστικούς κανόνες με βάση τους οποίους λαμβάνονται οι αποφάσεις. Επιπλέον η περιγραφή της κατανομής κάθε συστήματος ενημερώνεται σε τακτά χρονικά διαστήματα (π.χ. κάθε μέρα), με βάση τη συμπεριφορά που έχει παρατηρηθεί. Τα μοντέλα στατιστικών ροπών παρέχουν μεγαλύτερη ευελιξία από τα μοντέλα τιμών κατωφλίου. Με την ευελιξία, όμως, εμφανίζονται και προβλήματα πολυπλοκότητας.

Η τρίτη υποκατηγορία είναι τα μοντέλα πρόβλεψης προτύπων. Αυτό το μοντέλο ανίχνευσης σκοπό έχει την πρόβλεψη μελλοντικών συμβάντων χρησιμοποιώντας τη γνώση συμβάντων που έχουν ήδη πραγματοποιηθεί. Κάθε συμβάν που έχει ήδη πραγματοποιηθεί, θέτει το σύστημα σε μία κατάσταση το αμέσως επόμενο συμβάν το θέτει σε μία άλλη κατάσταση, έτσι κατασκευάζεται ένα σύνολο πιθανοτήτων μετάβασης. Ένα συμβάν με χαμηλό ποσοστό εμφάνισης αποτελεί πιθανή απειλή. Το ακόλουθο παράδειγμα αποδεικνύει τον τρόπο λειτουργίας του συστήματος. Έστω ότι ισχύει ο κανόνας:

$$E1\text{-}E2 \rightarrow (E3 = 86\%, E4 = 14\%)$$

Αυτό σημαίνει ότι με γνωστή χρονική σειρά των καταστάσεων E1 και E2, η πιθανότητα να ακολουθήσει το E3 είναι 86% και το E4 14%. Συνεπώς αν μετά τα E1 και E2 ακολουθήσει το E5 θα σημάνει συναγερμός (δεν αναμένονταν η εμφάνιση του). Το πρόβλημα προκύπτει όταν το E5 είναι εντελώς άγνωστο, τότε μπορεί απλά να χαρακτηρισθεί ως ύποπτο, όμως κάτι τέτοιο αυξάνει τους εσφαλμένους συναγερμούς. Γενικά, τα μοντέλα πρόβλεψης προτύπων ανιχνεύουν ανώμαλες συμπεριφορές ευκολότερα από τα άλλα μοντέλα, είναι πιο προσαρμόσιμα σε αλλαγές και απαιτούν μικρό χρόνο εκτέλεσης.

1.5. Μοντέλα Ανίχνευσης Κακής Συμπεριφοράς

Η ανίχνευση κακής συμπεριφοράς (misuse detection) βασίζεται στην αναζήτηση καταστάσεων του συστήματος που είναι γνωστό ότι είναι βλαβερές. Ο τρόπος λειτουργίας των μοντέλων μοιάζει με την λειτουργία των αντιβιοτικών λογισμικών. Μπορούν να ανιχνεύσουν όλες τις γνωστές επιθέσεις αλλά το κύριο μειονέκτημα τους είναι η αδυναμία να αντιμετωπίσουν άγνωστες απειλές. Είναι αρκετά σοβαρό πρόβλημα διότι η ταυτοποίησης μίας απειλής προϋποθέτει την επιτυχή εκτέλεση της τουλάχιστον μία φορά. Παράλληλα, οι διαχειριστές καλούνται συνεχώς να ενημερώνουν τους κανόνες κακής συμπεριφοράς. Από την άλλη, το πλεονέκτημα τους είναι ότι όταν αντιληφθούν μία συγκεκριμένη απειλή έχουν την δυνατότητα να παρέχουν πολλές πληροφορίες σχετικά με αυτή.

1.6. Αντιμετώπιση Απειλών

Τα συστήματα ανίχνευσης απειλών ενσωματώνουν μηχανισμούς ανάπτυξης αντίμετρων έναντι των επιθέσεων. Στόχος είναι να αντιμετωπισθεί η απειλή και να προστατευθεί το δίκτυο. Ορισμένα συστήματα αποτρέπουν την επίθεση, ενώ κάποια άλλα αποκρίνονται στην επίθεση και καταβάλλουν προσπάθεια να αποκαταστήσουν την εφαρμογή.

Το βέλτιστο θα ήταν η ανίχνευση και διακοπή της απόπειρας εισβολής προτού καταστεί επιβλαβής. Αυτό απαιτεί την συνεχή λειτουργία του συστήματος και την τοποθέτηση του στην πρώτη γραμμή άμυνας. Αναλυτικότερα, είναι προτιμότερο κάθε είσοδος πριν εισαχθεί στο δίκτυο, πρώτα να ελέγχεται από το IDS, προλαμβάνοντας κατά αυτό τον τρόπο την επίθεση. Ακόμη καλύτερα αν το IDS λειτουργεί ως μηχανισμός του ίδιου του πρωτοκόλλου δρομολόγησης και όχι ανεξάρτητα, δίνεται η εντύπωση στους επιτιθέμενους ότι η επίθεση πέτυχε.

Συνεπώς τα IDS εφαρμόζουν διαφορετικά αντίμετρα κατά περίπτωση. Οι δυνατές ανταποκρίσεις ενός συστήματος είναι οι ακόλουθες:

- Καταστολή της επίθεσης με ταυτόχρονη απομάκρυνση του επιτιθέμενου από το δίκτυο. Πλήρης απόρριψη του κακόβουλου κόμβου και περιορισμός του σε ελεγχόμενη περιοχή.

- Ταυτοποίηση μίας επίθεσης και κατάταξης της ως προς το είδος και την επικινδυνότητα της.

- Περιορισμός της ζημιάς περιορίζοντας τον κακόβουλο κόμβο.

- Αποκατάσταση του δικτύου.

- Παρακολούθηση της επίθεσης συλλέγοντας πληροφορίες για το προφίλ του επιτιθέμενου.

- Η αντεπίθεση δεν θα πρέπει να βασίζεται σε έναν αυτοματοποιημένο μηχανισμό.

2. Μέτρα Αντιμετώπισης Εναντίον Επιθέσεων Ανάλυσης Ισχύος

2.1. Ισορροπία Κατανάλωσης Ισχύος

Οι τεχνικές αυτές θα είναι εφαρμόσιμες όπου είναι δυνατόν. Όποτε μια λειτουργία εκτελείται στο hardware, μια συμπληρωματική λειτουργία θα πρέπει να εκτελείται για να διαβεβαιώσει ότι η συνολική κατανάλωση ισχύος της μονάδας διατηρεί ισορροπία σχετικά με τις ψηλές τιμές.

Τέτοια σχετική λειτουργία με την οποία η κατανάλωση ισχύος είναι σταθερή και ανεξάρτητη από τις εισόδους και τα bits κλειδιών, εμποδίζει όλα τα είδη των επιθέσεων κατανάλωσης ισχύος

.

2.2. Μείωση του Μεγέθους του Σήματος

Μια προσέγγιση για την αποτροπή επιθέσεων DPA (Differential Power Analysis) είναι η μείωση των μεγεθών σημάτων, όπως η χρησιμοποίηση ενός σταθερού μονοπατιού εκτέλεσης κώδικα, και ισορροπώντας βάρη Hanging και να αναφέρουν μεταβάσεις ή να προασπίζουν φυσικώς την συσκευή. Δυστυχώς, τέτοια μείωση μεγέθους σήματος γενικά, δεν μειώνει το μέγεθος του σήματος στο μηδέν, όπως ένας εισβολέας με έναν άπειρο αριθμό δειγμάτων, που είναι ικανός να εκτελέσει DPA στο (υψηλά διαβαθμισμένο) σήμα.

2.3. Πρόσθεση Θορύβου

Άλλη μια προσέγγιση εναντίον του DPA είναι η εισαγωγή θορύβου μέσα στα μέτρα για την κατανάλωση ισχύος.

Όπως οι μειώσεις μεγέθους σήματος, έτσι και η πρόσθεση θορύβου αυξάνει τον αριθμό των απαιτούμενων δειγμάτων για την επίθεση, πιθανώς σε ένα μεγάλο αριθμό. Εξάλλου, η εκτέλεση χρονισμού και η τάξη μπορεί να υποτίθεται ότι παράγει ένα παρόμοιο αποτέλεσμα. Ξανά, μόνος του ο χρόνος αυξάνει τον αριθμό των δειγμάτων που απαιτούνται, παρόλα αυτά εάν αυτός αυξάνεται, είναι αρκετά μεγάλος για να κάνει την δειγματοληψία ακατόρθωτη, εξαιτίας του απαιτούμενου αριθμού δειγμάτων, οπότε το μέτρο αντιμετώπισης λειτουργεί κανονικά

Μια επίλυση του προβλήματος για να αποφευχθούν επιθέσεις DPA χρησιμοποιώντας τον θόρυβο, είναι η πρόσθεση τυχαίων υπολογισμών που αυξάνουν το επίπεδο θορύβου αρκετά, για να κάνει τα σημεία κλίσης DPA (DPA bias spikes) μη ανιχνεύσιμα. Ο κύριος στόχος είναι να προστεθεί αρκετός τυχαίος θόρυβος για να σταματήσει μια επίθεση, και όχι μόνο να προσθέσει μια minimal επικεφαλίδα.

2.4. Τροποποίηση του Σχεδιασμού Αλγορίθμου

Μια τελευταία προσέγγιση εναντίον των επιθέσεων του DPA είναι ο σχεδιασμός κρυπτοσυστημάτων με ρεαλιστικές υποθέσεις για το επικείμενο (underlying) hardware. Σαν απλό παράδειγμα, hashing ένα 160 bito κλειδί με το SHA πριν την χρησιμοποίηση του σαν κλειδί θα μπορούσε αποτελεσματικά να καταστρέψει μερικές πληροφορίες που πιθανόν ένας εισβολέας να έχει μαζέψει για το

κλειδί. Ομοίως, η χρήση του δείκτη και της τροποποίησης του προτύπου (modulus) των επεξεργαστών σε κοινό κλειδί σχεδίων μπορεί να χρησιμοποιηθεί για να εμποδίσει τους εισβολείς από μια συσσώρευση πληροφοριών μέσα από έναν μεγάλο αριθμό λειτουργιών.

Αυτό μπορεί να λύσει το πρόβλημα, αλλά απαιτεί αλλαγές σχεδιασμού στους αλγόριθμους και στα ίδια τα πρωτόκολλα τα οποία είναι δυνατόν να κάνουν το αποτελεσματικό προϊόν να μη ενδίδει με τα στάνταρ και τις λεπτομέρειες.

3. Ανίχνευση Επιθέσεων

Η ανίχνευση μιας εξελισσόμενης επίθεσης άρνησης υπηρεσίας βασίζεται σε τεχνικές διάγνωσης ανωμαλίας. Πέρα από την καθ' αυτή ανακάλυψη μιας επίθεση DDoS η πρόκληση για έναν διαχειριστή ή ένα αυτόματο σύστημα IDS είναι να καταφέρουν να διαχωρίσουν περιστατικά φυσιολογικής αύξησης της κίνησης από πραγματικές κακόβουλες επιθέσεις. Μέρος της διαδικασίας ανίχνευσης είναι και ο προσδιορισμός των χαρακτηριστικών της κίνησης επίθεσης. Τα χαρακτηριστικά αυτά θα επιτρέψουν να διαχωριστεί από νόμιμες επικοινωνίες ή άλλες (ταυτόχρονες) επιθέσεις, και θα προσδιορίσουν τυχόν μέτρα αντιμετώπισης της. Η δυσκολία που παρουσιάζει το πρόβλημα της ανίχνευσης έγκειται, αφενός στην εξασφάλιση της απαραίτητης υπολογιστικής ισχύος ώστε να γίνει με επαρκή ταχύτητα η ανάλυση στοιχείων (ειδικά στα Ad – Hoc δίκτυα), αφετέρου στην εγκυρότητα και απόδοση των αλγορίθμων που θα χρησιμοποιηθούν για την ανάλυση.

Απ' ευθείας ανίχνευση γίνεται στο δίκτυο-θύμα με την παρατήρηση αυξημένης κίνησης ή και συμφόρησης. Για την ανακάλυψη ανωμαλιών στην κίνηση αυτή πρέπει να καταγραφεί, κατά τον ίδιο τρόπο που αυτό γίνεται στα συστήματα Network IDS (NIDS), και στη συνέχεια να αναλυθούν διάφορα χαρακτηριστικά της.
Η μετρούμενη αύξηση της χρησιμοποίησης μιας σύνδεσης μεταξύ κόμβων, μπορεί να οφείλεται σε φυσιολογικά αίτια και επομένως απαιτείται ανάλυση του είδους και του προορισμού της.
Οι μέθοδοι που επιτρέπουν την καλύτερη διάκριση των αιτιών της συμφόρησης του δικτύου και, εφόσον ανιχνευτεί μια εξελισσόμενη επίδεση, εντοπίζουν τα χαρακτηριστικά της, βασίζονται στη λεπτομερή ανάλυση της εισερχόμενης κίνησης. Με βάση αυτές τις μετρήσεις ροών μπορούν να υλοποιηθούν συστήματα IDS διάγνωσης ανωμαλιών για περιστατικά DDoS. Αναλογικά μεγάλη αύξηση πακέτων σε σχέση με τις ροές κίνησης αποτελεί ένδειξη για την ύπαρξη μιας συνεχούς αποστολής δεδομένων από τις ίδιες πηγές προς τις ίδιες κατευθύνσεις. Δυσανάλογα πολλές ροές και αύξηση του λόγου ροών προς πακέτα, δείχνουν την αποστολή μικρού αριθμού πακέτων από μεγάλο αριθμό πολλών διαφορετικών διευθύνσεων. Οι παράμετροι αυτοί μπορούν να συνδυαστούν και με άλλα δεδομένα όπως το εύρος των διευθύνσεων παραλήπτη, τα συγκεκριμένα είδη των πακέτων κ.λπ. Τα στοιχεία αυτά μπορούν να διαγνώσουν κάποια περιστατικά DDoS ακόμα και αν η κίνηση δεν παρουσιάζει συνολικά σημαντικές διαφορές.

4. Ανακάλυψη της Διαδρομής

Η ανακάλυψη της διαδρομής που ακολουθεί μια επίδεση για να καταλήξει στο θύμα επιτρέπει, αν γίνει κατά τη διάρκεια ενός περιστατικού, την ανάσχεση της. Στην περίπτωση αυτή ο εντοπισμός του μονοπατιού θα πρέπει να γίνει πολύ σύντομα και με μεγάλη ακρίβεια. Ακόμα όμως και μετά από το τέλος του περιστατικού, η

ανακάλυψη της πλήρους διαδρομής μπορεί να οδηγήσει στην πηγή της επίθεσης και να αποτρέψει την περαιτέρω δράση της. Αυτοματοποιημένες διαδικασίες ανακάλυψης της διαδρομής απαιτούν συνήθως να προϋπάρχουν κατάλληλες υποδομές ανίχνευσης και παρακολούθησης.

5. Αντίδραση στην Επίθεση

Διαδικασίες μη ορισμένες με σαφήνεια και μη αυτοματοποιημένες δεν παρέχουν την ταχύτητα που απαιτείται για το χειρισμό τέτοιων περιστατικών. Επιπλέον δεν υπάρχει τυποποίηση στα δεδομένα που θα ανταλλαγούν.

Ένας πρόσθετος παράγοντας δυσκολίας είναι η συνήθης έλλειψη συγκεκριμένης πολιτικής αντιμετώπισης των επιθέσεων..

Οι δυνατές λύσεις αντιμετώπισης των επιδέσεων DDoS μπορούν να κατηγοριοποιηδούν ως προληπτικές (proactive) ή κατασταλτικές (reactive).

- Μια πολύ τυπική προληπτική αντίδραση είναι η παρεμπόδιση πακέτων με διευθύνσεις προέλευσης που δεν αντιστοιχούν στις εφαρμοζόμενες πολιτικές δρομολόγησης. Προφανώς όσο μεγαλύτερος αριθμός κόμβων συμμετέχει, τόσο πιο αποδοτικό θα είναι το αποτέλεσμα κατά των επιδέσεων DDoS. Εντούτοις η μέθοδος έχει αδυναμίες: χρειάζεται αποδοτική υλοποίηση των αλγορίθμων φιλτραρίσματος, με δεδομένο ότι πρόκειται για κόμβους που χειρίζονται μεγάλους όγκους κίνησης. Επιπλέον υπάρχουν περιπτώσεις που η ακριβής δρομολόγηση δεν είναι γνωστή και έτσι η μέθοδος μπορεί να οδηγήσει σε παρεμπόδιση νόμιμων επικοινωνιών.

- Όταν η επίθεση έχει σα στόχο μόνον ένα συγκεκριμένο κόμβο, μια πρακτική που χρησιμοποιείται είναι η πλήρης διακοπή της κίνησης προς αυτόν στον ακριβώς προηγούμενο κόμβο. Η μέθοδος ονομάζεται «διοχέτευση σε μαύρη τρύπα» (blackholing) και μπορεί να υλοποιηθεί πολύ εύκολα. Επιπλέον δεν έχει ιδιαίτερο υπολογιστικό κόστος επειδή χρησιμοποιείται ο μηχανισμός δρομολόγησης αντί αυτού του φιλτραρίσματος. Αν και ολοκληρώνει την άρνηση δικτυακής σύνδεσης προς το θύμα, ουσιαστικά αποκόπτοντάς το, το δίκτυο ανακουφίζεται από την κακόβουλη κίνηση.

- Μια άλλη πρόταση συνδυάζει την επιλογή νέας δρομολόγησης για την κίνηση του θύματος μέσα από σήραγγες με μια παραλλαγή της μεθόδου αποκοπής της επιθετικής κίνησης προς το τελικό θύμα. Στο δίκτυο δημιουργούνται σήραγγες. Στη συνέχεια όλη η κίνηση προς το θύμα οδηγείται από αυτό το δρόμο. Στη συνέχεια μέσα από άλλες σήραγγες η νόμιμη κίνηση καταλήγει στον παραλήπτη. Η λύση αυτή, απαιτεί τη γρήγορη ανίχνευση των επιθέσεων, την αλλαγή στη δρομολόγηση προς και από συγκεκριμένους κόμβους και, κυρίως, την ικανότητα για ακριβή εντοπισμό της κακόβουλης κίνησης προς και από το θύμα.

8. Αυθεντικοποίηση

1. Εισαγωγή

Οι μηχανισμοί πιστοποίησης ταυτότητας προσπαθούν να επαληθεύσουν τη γνησιότητα των διαπιστευτηρίων (credentials) που δηλώνουν οι εμπλεκόμενοι. Κατά τις διαδικασίες αυθεντικοποίησης, μια συσκευή που επιθυμεί να γίνει μέρος ενός ασύρματου δικτύου θα πρέπει να αποδείξει στο δίκτυο ότι είναι *γνήσια.* Με τον όρο γνήσια εννοείται ότι αυτή δεν είναι πλαστή ή ότι δεν έχει υποστεί τροποποιήσεις τόσο στο λογισμικό όσο και στο υλικό της.

Τα περισσότερα αντικείμενα αξίας στον σημερινό κόσμο διαθέτουν κάποιο τρόπο για να αποδείξουν τη γνησιότητα τους. Χαρακτηριστικά, μπορούν να αναφερθούν τα χαρτονομίσματα. Αυτά διαθέτουν τη δυνατότητα να αποδείξουν ότι είναι γνήσια στο σύνολο τους, αλλά συγχρόνως και ότι διαφέρουν μεταξύ τους βάσει ενός κωδικού αριθμού που διαθέτει το καθένα. Η αλλοίωση κάποιων στοιχείων ή χαρακτηριστικών τους (σκισίματα, φθορές, κλπ), δημιουργεί συνήθως υποψίες στον κάτοχό τους για τη γνησιότητα αυτών, οπότε καταφεύγει στις ανάλογες λύσεις.

Δυστυχώς, μέχρι στιγμής υπάρχουν πολύ λίγοι τρόποι μέσω των οποίων μπορεί να αποδειχθεί ότι ένα υπολογιστικό σύστημα είναι γνήσιο. Στην προσπάθεια να δοθεί απάντηση στη συγκεκριμένη ερώτηση, δηλαδή για το αν ένα υπολογιστικό σύστημα είναι γνήσιο μπορεί κάποιος να αποκριθεί ότι «δείχνει να είναι γνήσιο» και «συμπεριφέρεται με τον ενδεδειγμένο τρόπο» αλλά πάλι δεν είναι σε θέση να είναι σίγουρος. Πράγματι, στα υπολογιστικά συστήματα αυτή η απάντηση είναι και η σωστή αφού η δυναμική φύση του λογισμικού που διαθέτουν δεν επιτρέπει να προσδιορίσουμε εύκολα τυχόν τροποποιήσεις που έχουν υποστεί.

Προκειμένου να αποδειχθεί η γνησιότητα ενός υπολογιστικού συστήματος και η ικανότητα αυτού να αυθεντικοποιηθεί θα πρέπει να επαληθευθούν δύο πράγματα:

- Πρώτον, η συσκευή θα πρέπει να είναι ένα πραγματικό υπολογιστικό σύστημα με γνήσιες ιδιότητες και όχι ένας κακόβουλος χρήστης που μιμείται την συσκευή. Αν η συσκευή δεν είναι γνήσια, αλλά απομίμηση, το περιβάλλον διαχείρισης θα πρέπει να αποτρέψει την αυθεντικοποίηση.

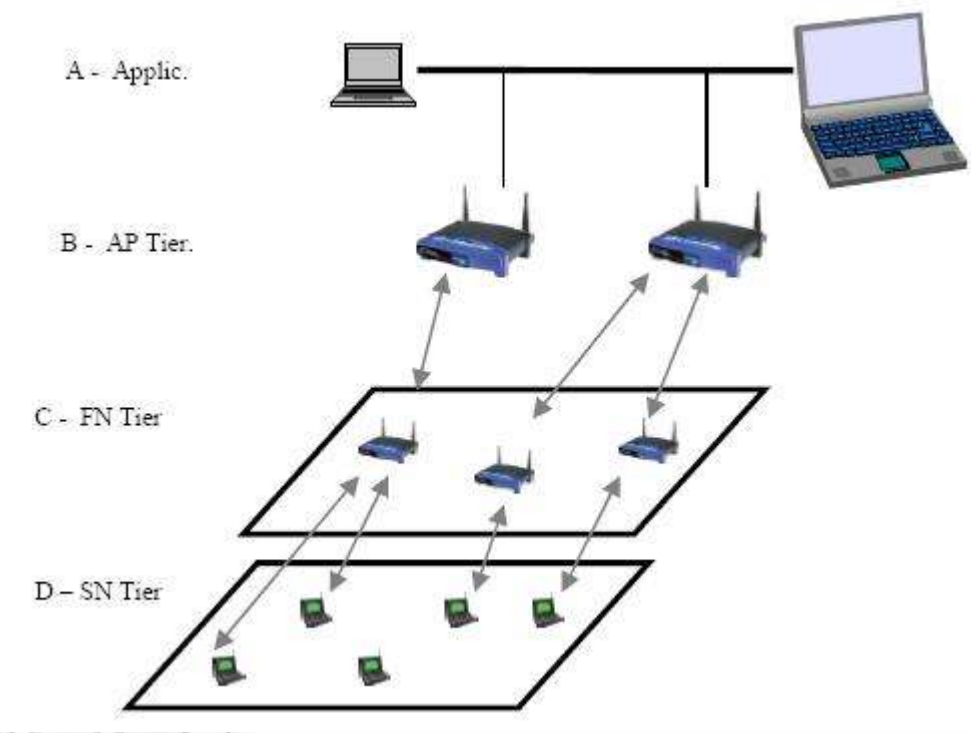
- Δεύτερον, το υπολογιστικό σύστημα θα πρέπει να διαθέτει το ενδεδειγμένο λογισμικό (software) και σύστημα υλικού (hardware) ή και επιπλέον ιδιότητες που έχουν καθοριστεί και αναμένει ο διαχειριστής αυθεντικοποίησης. Αν όλα τα παραπάνω είναι πλήρως καθορισμένα τότε η συμπεριφορά του συστήματος είναι η αναμενόμενη. Κάθε πιθανή διαφοροποίηση δημιουργεί υπόνοιες και ενεργοποιεί μηχανισμούς άρνησης πρόσβασης

Παρακάτω αναλύονται οι υπάρχουσες προσεγγίσεις που έχουν γίνει στο χώρο των ασύρματων δικτύων για την αυθεντικοποίηση των συσκευών. Στο σύνολο τους είναι περιορισμένες και οι περισσότερες από αυτές καλύπτουν το θέμα επιφανειακά. Οι λύσεις που προτείνονται, απευθύνονται σε ορισμένα είδη δικτύων και δεν προτείνεται κάτι που να μπορεί να καλύψει όλο το εύρος των ασύρματων δικτύων.

2. Ad-Hoc Δίκτυα

Τα Ad-Hoc δίκτυα αποτελούν μια άλλη κατηγορία δικτύων με πολλές ιδιαιτερότητες. Η αυθεντικοποίηση στηρίζεται επί το πλείστον στην ιεράρχηση των ad-hoc δικτύων. Ιεραρχημένα ad-hoc δίκτυα θεωρούν αυτά που είναι χωρισμένα σε επίπεδα, με κάθε επίπεδο να περιλαμβάνει συσκευές που εκτελούν παρόμοιες εργασίες και έχουν ως σκοπό να υποστηρίξουν την λειτουργία των συσκευών των χρηστών.

Η αυθεντικοποίηση στην προκειμένη περίπτωση στηρίζεται σε ένα μοντέλο όπου οι κόμβοι του δικτύου ζητάνε από τους γειτονικούς σε αυτούς κόμβους να δημιουργήσουν σχέσεις εμπιστοσύνης. Ακολούθως οι σχέσεις αυτές χρησιμοποιούνται ως βάση για να πραγματοποιηθεί η αυθεντικοποίηση.



Κάθε οντότητα διατηρεί μια λίστα με τις έμπιστες οντότητες. Χρησιμοποιεί, δε, αυτήν την λίστα κάθε φορά που επιθυμεί να δημιουργήσει ένα κανάλι επικοινωνίας μεταξύ δύο ή περισσοτέρων συσκευών. Η αυθεντικοποίηση των εισερχομένων συσκευών στο δίκτυο στηρίζεται στην ανταλλαγή ενός μυστικού που ελέγχεται μέσω κάποιον εφαρμογών. Το μυστικό αυτό δεν είναι τίποτα άλλο από ένα σύνολο δεδομένων που αποτελεί το συνθηματικό των συσκευών, το οποίο υπολογίζεται μέσω των εφαρμογών λογισμικού.

Όπως συμβαίνει σε οποιαδήποτε διαδικασία αυθεντικοποίησης, κάθε εισερχόμενη συσκευή θα πρέπει να αποδείξει ότι έχει το δικαίωμα εισόδου. Τα δεδομένα δεν θεωρούνται έμπιστα μέχρι αποδείξεως του αντιθέτου. Για αυτό το λόγο κάθε συσκευή είναι εφοδιασμένη με ένα πιστοποιητικό (iCert) το οποίο και εκδίδεται από μια τρίτη

έμπιστη οντότητα (TTP), η οποία αποτελεί μέλος του δικτύου. Η οντότητα αυτή δεν είναι τίποτα περισσότερο από μια συσκευή που είναι ικανή να δημιουργεί υπογραφές RSA, των οποίων το δημόσιο κλειδί είναι γνωστό σε όλες τις συσκευές που έχουν την δυνατότητα να επαληθεύσουν τις RSA υπογραφές.

Όταν το σημείο πρόσβασης Β ή μια συσκευή χρήστη Δ θέλει να γίνει μέλος του δικτύου, θα πρέπει να παρουσιάσει το πιστοποιητικό (iCert). Αυτό θα ελεγχθεί από μια εφαρμογή Α για την γνησιότητα του.

Αν το πιστοποιητικό (iCert) είναι το γνήσιο, η εφαρμογή Α θα ιδρύσει ένα κοινό μυστικό $K_{A, B}$ ή $K_{A, Δ}$, με το οποίο θα δίνεται η δυνατότητα στην συσκευή να επικοινωνήσει με την εφαρμογή. Σε περίπτωση που η συσκευή είναι μέλος του δικτύου το πιστοποιητικό (iCert) γίνεται λιγότερο σημαντικό. Για το διάστημα που οι συσκευές Β, Δ δεν διακόπτουν την σύνδεση, η σχέση εμπιστοσύνης που έχει δημιουργηθεί διατηρείται. Επιπλέον όμως κάθε συσκευή θα πρέπει να αυθεντικοποιηθεί και με τα υπόλοιπα μέλη του δικτύου αφού η τοπολογίες των ad-hoc δικτύων αλλάζουν συνεχώς, με πολλές εξόδους και εισόδους διαφορετικών οντοτήτων. Η εφαρμογή Α δίνει την δυνατότητα αυτή εκδίδοντας περιοδικά νέα πιστοποιητικά για κάθε σημείο πρόσβασης ή απλής συσκευής.

Έχοντας ένα δίκτυο με πιστοποιημένες συσκευές που έχουν δημιουργήσει σχέσεις εμπιστοσύνης μπορούμε να δημιουργήσουμε μια υπηρεσία αυθεντικοποίησης δεδομένων. Η αυθεντικοποίηση αυτή θα διασφαλίσει τόσο την ακεραιότητα των δεδομένων αλλά συγχρόνως θα έχει ως αποτέλεσμα επιπλέον αποτελέσματα αυθεντικοποίησης αφού για την ανταλλαγή των δεδομένων θα χρησιμοποιηθούν και πάλι τα ήδη παραχθέντα πιστοποιητικά.

Τα πιστοποιητικά που εκδίδονται βασίζονται πάνω στο πρωτόκολλο TESLA, το οποίο και χρησιμοποιεί τεχνικές ασύμμετρης κρυπτογραφίας που είναι κατάλληλες για συσκευές που χρησιμοποιούν περιορισμένης διάρκειας πηγές ενέργειας. Τονίζεται ότι μόνο για το σημείο πρόσβασης απαιτούνται ισχυρές υπολογιστικές δυνατότητες μιας και αυτό θα δημιουργεί τα πιστοποιητικά και τις RSA υπογραφές.

Η αυθεντικοποίηση των συσκευών στην παραπάνω περιγραφή επιτυγχάνεται αφού τα πιστοποιητικά που δημιουργούνται αφορούν την συσκευή και όχι τον χρήστη. Αυτά αποθηκεύονται εντός της συσκευής και ο χρήστης δεν μπορεί να παρέμβει ούτε για να τα τροποποιήσει ούτε και να τα χρησιμοποιήσει σε άλλη συσκευή.

Μια ενδιαφέρουσα λύση η οποία αφορά αποκλειστικά τα ad-hoc δίκτυα, παρουσιάζεται από τους Michael Jarrett και Paul Ward. Η πιστοποίηση των συσκευών στηρίζεται στο ήδη υπάρχον πρωτόκολλο, το οποίο και χρησιμοποιείται για την δρομολόγηση των δεδομένων. Το πρωτόκολλο αυτό είναι το γνωστό Ad-Hoc On Demand Distance Vector (AODV). Η πιστοποίηση των συσκευών σε αυτήν περίπτωση είναι έμμεση. Τα πιστοποιητικά που δημιουργούν οι ασύρματες συσκευές δεν χρησιμοποιούνται για την αυθεντικοποίηση τους αλλά για την προστασία της δρομολόγησης. Μέσω όμως αυτής της διαδικασίας υλοποιείται ταυτόχρονα και η επαλήθευση των πιστοποιητικών.

Τα πιστοποιητικά που χρησιμοποιούνται προέρχονται από την ήδη γνωστή μέθοδο έμπιστων υπολογισμών. Οι υπολογισμοί στηρίζονται στο λειτουργικό σύστημα και στο λογισμικό που είναι διαθέσιμο και πρέπει να θεωρείται ήδη έμπιστο διότι σε διαφορετική περίπτωση η όλη διαδικασία δεν θα ήταν αξιόπιστη. Η διαδικασία δρομολόγησης και αυθεντικοποίησης έχει τα παρακάτω καθήκοντα.

- Πρέπει να υπακούει στους ήδη υπάρχοντες κανόνες δρομολόγησης που απορρέουν από το πρωτόκολλο που έχει επιλεχθεί. Σε καμιά περίπτωση δεν θα πρέπει να υποδύεται άλλη συσκευή τροφοδοτώντας το δίκτυο με λανθασμένες μετρήσεις, αγνοώντας προκλήσεις από γειτονικούς σταθμούς ή ακόμα και καθυστερώντας σε αποκρίσεις μηνυμάτων.
- Πρέπει να απαιτεί την πιστοποίηση των αιτούντων που θέλουν να εισέλθουν στο ασύρματο δίκτυο και
- Πρέπει να παρακολουθεί τις αναφορές που διακινούνται στο δίκτυο.

Επιπλέον υπάρχουν τρεις δεσμευτικές συμφωνίες - κλειδιά προκειμένου να γίνει η πιστοποίηση. Η πρώτη συμφωνία αφορά στο φιλτράρισμα της κίνησης, που χωρίζεται σε επίπεδα. Σε κάθε ένα από αυτά υπάρχει συγκεκριμένος έλεγχος από συγκεκριμένες εφαρμογές. Η δεύτερη συμφωνία επιβάλει την επικοινωνία μέσω ασφαλών εισόδων-εξόδων (input-output) προκειμένου να ελέγχεται η αυθεντικότητα της συσκευής, ενώ τέλος θα πρέπει να καταγράφονται όλες οι ενέργειες της συσκευής σε αρχεία.

Το νέο αυτό πρωτόκολλο ονομάζεται Trusted Computing Ad-Hoc On Demand Distance Vector (TCAODV), ενώ η όλη φιλοσοφία μπορεί να εφαρμοστεί και σε άλλα πρωτόκολλα της σειράς των ad-hoc δικτύων. Κάθε συσκευή χρησιμοποιεί ένα δημόσιο κλειδί, το οποίο αποθηκεύεται σε αυτήν για τις ανάγκες της δρομολόγησης και λαμβάνεται κατά την διαδικασία αρχικοποίησης. Όταν μια συσκευή Α επιθυμεί να εγκαταστήσει μια σύνδεση δρομολόγησης με την Β, θα αποστείλει μια αίτηση. Αυτό εκτελείται αυτόματα από το πρωτόκολλο AODV, το οποίο επιπλέον στην περίπτωση αυτή θα περιέχει και ένα πακέτο υπογεγραμμένο με το δημόσιο κλειδί. Αυτό το πακέτο θα περιέχει δεδομένα από υπολογισμούς που επικυρώνουν την πιστοποίηση της συσκευής, πληρώντας συγχρόνως προϋποθέσεις και προδιαγραφές που αναφέρθηκαν προηγουμένως

Αφού η συσκευή δεχτεί την αίτηση δρομολόγησης και πιστοποιήσει το δημόσιο κλειδί θα ελέγξει επίσης την ορθότητα των υπολογισμών που επικυρώνουν την πιστοποίηση. Αν από τη διαδικασία επαλήθευσης προκύψουν τα επιθυμητά αποτελέσματα το πακέτο γίνεται δεκτό. Από την άλλη μεριά αν η επαλήθευση αποτύχει το πακέτο θα δρομολογηθεί σε άλλη συσκευή για περαιτέρω χρήση, προσθέτοντας όμως και αυτή την υπογραφή της.

Επίσης, αναφέρεται ότι επειδή δεν επαρκεί το δημόσιο κλειδί προκειμένου να ελεγχθεί η σωστή συμπεριφορά της κάθε συσκευής χρησιμοποιείται και ένα συμμετρικό κλειδί. Με αυτόν τον τρόπο, όποτε διακόπτεται η σύνδεση, ένα νέο συμμετρικό κλειδί μεταδίδεται κρυπτογραφημένο με το δημόσιο κλειδί, ενώ όλα τα δεδομένα που διακινούνται κρυπτογραφούνται με το συμμετρικό.

1. **Routing Participation:** Όλες οι οντότητες θα πρέπει να συμμετάσχουν στις διαδικασίες δρομολόγησης.

2. **Routing Honesty:** Οι οντότητες θα πρέπει να δίνουν ακριβείς μετρήσεις και σωστές αναφορές για σφάλματα σύνδεσης.

3. **Traffic Forwarding:** Οι οντότητες θα πρέπει να προωθούν τα δεδομένα όπως αυτά ορίζονται από το πρωτόκολλο.

4. **Bandwidth Allocation:** Οι οντότητες δεν θα πρέπει να δρομολογούν δεδομένα υπερβαίνοντας τις δυνατότητες του καναλιού μετάδοσης.

5. **Confidentiality:** Οι οντότητες θα πρέπει να προστατεύουν τα περιεχόμενα των πακέτων που στέλνουν, καθώς και των επικεφαλίδων κατά την επικοινωνία από ωτακουστές.

6. **Authentication:** Οι οντότητες θα πρέπει να πιστοποιούν τις συσκευές στις οποίες δρομολογούν τα πακέτα

	Routing Participation	**Routing Honesty**	**Traffic Forwarding**	**Bandwidth Allocation**	**Confidentiality**	**Authentication**
TCAODV	X	X	X	X	X	X
ARAN		X				X
SAR					X	
Watchdog		X	X	X		
CONFIDENT		X	X	X		
AD-MIX	X		X		X	
Nuglets	X		X			
Cell	X		X		X	X

Πίνακας 2. Βασικές Υπηρεσίες Πρωτοκόλλων Ad Hoc Δικτύων

3. Άλλες Λύσεις

Πολλοί οργανισμοί προσπαθώντας να αυξήσουν τα επίπεδα ασφαλείας των ασύρματων δικτύων προτείνουν διάφορες λύσεις. Οι περισσότερες από αυτές στηρίζονται στην αυθεντικοποίηση των ασύρματων συσκευών, χρησιμοποιώντας φορητές μνήμες τύπου Flash ή έξυπνες κάρτες (smart cards). Στην συγκεκριμένη περίπτωση οι απόψεις διίστανται για το κατά πόσο η χρήση τέτοιων μεθόδων γίνεται προκειμένου να αυθεντικοποιηθεί ο χρήστης ή η συσκευή.

Οι έξυπνες κάρτες και οι φορητές μνήμες διαθέτουν πιστοποιητικά που έχουν εκδοθεί βάση της ταυτότητας του χρήστη. Η ενσωμάτωση όμως του εξοπλισμού που αναγνωρίζει τόσο τις κάρτες, όσο και τις φορητές μνήμες πάνω στις ασύρματες συσκευές διαφοροποιεί αυτήν την κατάσταση. Έτσι, πολλοί επικαλούνται ότι τα πιστοποιητικά μπορεί να εκδίδονται για τον χρήστη, αλλά χωρίς αυτά ούτε ο ίδιος, αλλά ούτε και η συσκευή μπορεί να αυθεντικοποιηθεί στον δίκτυο. Ουσιαστικά η προαναφερθείσα περιγραφή αποτελεί μια υβριδική μέθοδο αυθεντικοποίησης.

Έξυπνες Κάρτες

Η έξυπνη κάρτα διαθέτει όλες εκείνες τις πληροφορίες που χρειάζονται προκειμένου ο χρήστης να αυθεντικοποιηθεί στην ασύρματη συσκευή. Η τελευταία διαθέτει ενσωματωμένο υλικό (hardware) μέσω του οποίου τοποθετείται και γίνεται η ανάγνωση της κάρτας.

Το συγκεκριμένο υλικό συνοδεύεται και από κατάλληλο λογισμικό προκειμένου να γίνουν οι διαδικασίες αυθεντικοποίησης. Το σημαντικότερο είδος λογισμικού είναι η εκάστοτε εφαρμογή που κάνει την πιστοποίηση. Στην αρχή ο χρήστης θα δώσει τον μυστικό κωδικό προκειμένου να γίνει δεκτός από την συσκευή. Αμέσως μετά, ξεκινάει ένας διάλογος μεταξύ της συσκευής και της κάρτας. Ο διάλογος αυτός έχει ως σκοπό να διαπιστώσει την αυθεντικότητα της κάρτας του χρήστη.

Μετά το πέρας αυτής τις διαδικασίας τα πιστοποιητικά που διαθέτει η κάρτα χρησιμοποιούνται προκειμένου να αναπαραχθεί ουσιαστικά ένας άλλος κωδικός, ο οποίος και θα χρησιμοποιηθεί όταν η συσκευή θελήσει να εισέλθει σε ένα δίκτυο. Το πρωτόκολλο που χρησιμοποιείται είναι το πρωτόκολλο πρόκλησης-απάντησης, ενώ οι ενέργειες που λαμβάνουν χώρα δεν διαφέρουν κατά πολύ αυτών του GSM.

Η παραπάνω φιλοσοφία, αποτελεί μια καλή λύση αυθεντικοποίησης, η οποία όμως είναι απαγορευτική για πολλούς, λόγω υψηλού κόστους. Επιπλέον, μπορεί να εφαρμοστεί μόνο σε ορισμένου τύπου δίκτυα .

Flash Μνήμες

Πολλοί κατασκευαστές στηριζόμενοι στην φιλοσοφία λειτουργίας των έξυπνων καρτών προσπάθησαν να επινοήσουν πρακτικότερες μεθόδους. Μια από αυτές ήταν να χρησιμοποιήσουν φορητές μνήμες (flash memory). Σε αυτήν την περίπτωση το πιστοποιητικό χωρίζεται σε δύο ίσα μέρη. Το ένα μέρος αποθηκεύεται στην φορητή μνήμη και το άλλο στην ασύρματη συσκευή.

Επιπλέον αξίζει να αναφερθεί ότι πολλές φορές εκδίδονται επιπλέον τρία πιστοποιητικά, εκ των οποίων το ένα το γνωρίζει ο χρήστης, το άλλο η συσκευή και το τελευταίο είναι αποθηκευμένο στην φορητή μνήμη. Αυτά χρησιμοποιούνται για να πιστοποιήσουν τον χρήστη και την φορητή μνήμη ως προς την συσκευή.

Κάθε φορά που ο χρήστης επιθυμεί να αυθεντικοποιηθεί στην συσκευή θα πρέπει να συνδέσει την φορητή μνήμη και να δώσει τα κατάλληλα συνθηματικά. Στην συνέχεια και όταν η συσκευή χρειαστεί να αυθεντικοποιηθεί σε κάποιο δίκτυο και ενώ γνωρίζει το ένα μέρος από τα συνθηματικά θα πρέπει να αναζητήσει στην φορητή μνήμη το άλλο μέρος. Αυτό βρίσκεται σε σημείο που είναι προκαθορισμένο και γνωρίζει η συσκευή.

Εκτελώντας στην συνέχεια κατάλληλες πράξεις μέσω του λογισμικού που διαθέτει κάνει την επανασύνδεση αυτών. Με τον τρόπο αυτό θα καταλήξει στο πιστοποιητικό μέσω του οποίου θα αυθεντικοποιηθεί στο δίκτυο. Θα πρέπει να επισημανθεί ότι τα πιστοποιητικά αυτά μπορεί να προέρχονται από κάποια αρχή πιστοποίησης που τα εκδίδει βάσει των ιδιοτήτων του χρήστη και τα φυσικά χαρακτηριστικά της συσκευής ή σπανιότερα προέρχονται αποκλειστικά από την αρχιτεκτονική του συστήματος ή άλλες παραμέτρους.

Παραλλαγές

Μια άλλη προσέγγιση σε ότι αφορά την αυθεντικοποίηση συσκευής έχει υποστηριχθεί από διάφορα επιστημονικά ιδρύματα τα οποία έχουν καταλήξει, στο ότι ο απλός τρόπος εμφύτευσης ενός κωδικού αριθμού στο λογισμικού του συστήματος αποτελεί την καλύτερη και οικονομικότερη μέθοδο αυθεντικοποίησης συσκευής.

Στην προκειμένη περίπτωση η συσκευή Α που έχει αναλάβει την αυθεντικοποίηση υπολογίζει έναν τυχαίο αριθμό των 24 δυαδικών ψηφίων και το αποστέλλει στην προς αυθεντικοποίηση συσκευή Β. Στην συνέχεια η Β και αφού διαθέτει ένα μυστικό αριθμό υπολογίζει ένα κρυπτογραφημένο αλφαριθμητικό που αποτελείται από τον μυστικό αριθμό, τα δεδομένα που έστειλε ο Α και έναν σειριακό αριθμό μέσω της οποίας αναγνωρίζεται η συσκευή. Ο Β αποστέλλει το κρυπτογραφημένο αλφαριθμητικό στον Α, ο οποίος υπολογίζει με τις ίδιες παραμέτρους την ίδια τιμή και συγκρίνει τα αποτελέσματα που αν είναι τα ίδια πιστοποιεί τελικά τον Β.

Τέτοιας φύσεως μέθοδοι αυθεντικοποίησης είναι εύκολο να υλοποιηθούν με μοναδικό πρόβλημα ότι δεν παρέχουν σε καμιά περίπτωση τα επίπεδα ασφαλείας που υπόσχονται, αφού οι ωτακουστές εύκολα μπορούν να υποκλέψουν τα πιστοποιητικά που μεταδίδονται.

Σε παραπλήσια επίπεδα κινείται και η πρόταση που γίνεται από τον οργανισμό Trusted Computing Group (TCG). Αυτό που προτείνεται ως λύση είναι η χρήση ενός ειδικού ενσωματωμένου κυκλώματος εγκατεστημένου στην συσκευή που προσφέρει ισχυρή αυθεντικοποίηση και πιστοποίηση της συσκευής, ενώ συγχρόνως επιτρέπει την προστασία ευαίσθητων πληροφοριών και την μη εξουσιοδοτημένη πρόσβαση κακόβουλων δικτύων.

Το συγκεκριμένο κύκλωμα τοποθετείται στα είδη υπάρχοντα κυκλώματα της μητρικής πλακέτας. Όλα τα κλειδιά κρυπτογράφησης καθώς και άλλες πληροφορίες ασφαλείας αποθηκεύονται σε αυτήν.

Το ειδικό κύκλωμα ονομάζεται Trusted Platform Modules (TPM) και η βασική του λειτουργία είναι η δημιουργία ασφαλών κλειδιών (safe keys) καθώς και η αποθήκευσή τους. Για την δημιουργία αυτών των κλειδιών χρησιμοποιείται μια γεννήτρια ψευδοτυχαίων αριθμών, οι οποίοι αποτελούν τη φύτρα για την διαδικασία κρυπτογράφησης και την έναρξη λειτουργίας των συναρτήσεων δημιουργίας των πιστοποιητικών.

Σε διαφορετικά επίπεδα κινείται η πρόταση των Naveen Sastry et al. Αυτοί προτείνουν έναν τρόπο επαλήθευσης των συσκευών ενός ασύρματου δικτύου, ο οποίος βασίζεται σε μηχανισμούς που έχουν να κάνουν με την φυσική τοποθεσία που βρίσκονται οι συσκευές. Το συγκεκριμένο πρωτόκολλο δεν έχει πολλές απαιτήσεις αφού δεν απαιτεί μηχανισμούς συγχρονισμού, κρυπτογραφίας ή ωρολόγια ακριβείας. Είναι δε καταλληλότερο για μικρές συσκευές με περιορισμένες επεξεργαστικές δυνατότητες.

Τα φυσικά χαρακτηριστικά που εμφανίζονται στον περιβάλλοντα χώρο μιας ασύρματης συσκευής είναι πολλά. Ένα από αυτά είναι και η περιοχή που είναι τοποθετημένη. Το μειονέκτημα που προκύπτει από αυτού του είδους την αυθεντικοποίηση είναι ότι οι συσκευές ή θα πρέπει να είναι σταθερά εγκατεστημένες σε κάποιο σημείο ή να κινούνται σε ένα περιορισμένο χώρο. Ο χώρος αυτός θα πρέπει να είναι κατάλληλα μελετημένος ιδιαίτερα σε ότι αφορά τις αποστάσεις που βρίσκονται οι υπόλοιπες ασύρματες συσκευές. Θα πρέπει να είναι γνωστό δηλαδή, σε

τι απόσταση βρίσκεται η συσκευή S1 ως προς την συσκευή S2, αυτή ως προς την S3 και όλες μαζί μεταξύ τους. Επιπλέον, θα πρέπει η κάθε συσκευή να γνωρίζει για τις άλλες αν μπορούν να μετακινηθούν και σε τι αποστάσεις.

Λαμβάνοντας υπόψη αυτές τις παραμέτρους κάθε μία συσκευή έχει αποθηκευμένα όλα αυτά τα δεδομένα για τους γείτονές της. Ο λόγος είναι ότι η αυθεντικοποίηση προέρχεται από το πόσο χρονικό διάστημα απαιτείται να φτάσει ένα ραδιοκύμα (RF) από την μια συσκευή στην άλλη. Γνωρίζοντας την ταχύτητα των ραδιοκυμάτων, καθώς και την τοποθεσία που έχει δηλώσει κάθε μια από τις συσκευές, προβαίνει στους κατάλληλους υπολογισμούς για να διαπιστώσει αν το σήμα που ελήφθη ανταποκρίνεται στον χρόνο που χρειάστηκε για να παραληφθεί.

Συνεπώς, γνωρίζοντας η S1 ότι η S2 βρίσκεται στην περιοχή R2 και το αντίστροφο, γνωρίζει τον χρόνο που θα χρειαστεί το σήμα να φτάσει από την μια συσκευή στην άλλη. Με αυτόν τον τρόπο αποδεικνύει η μια στην άλλη ότι είναι η πραγματική συσκευή αφού μόνο αυτή μπορεί να γνωρίζει τον χρόνο που απαιτείται για το σήμα να φτάσει από την τοποθεσία A2 στην τοποθεσία A1.

Φυσικά, αν και δεν αναφέρεται κάτι τέτοιο, θα πρέπει να χρησιμοποιείται κάποιους είδους συμμετρικής ή ασύμμετρης κρυπτογραφίας, ειδάλλως οι επιθέσεις που μπορεί να δεχτεί ένα πρωτόκολλο με αυτά τα χαρακτηριστικά είναι πολλές. Μία από αυτές μπορεί να είναι η εύκολη καταγραφή από ωτακουστές των δεδομένων που μεταφέρονται εφόσον δεν θα υπάρξει κρυπτογράφηση.

Τέλος, η χρήση ηλεκτρομαγνητικών υπογραφών αποτελεί μια πρωτοποριακή μέθοδο αναγνώρισης των συσκευών και προτάθηκε από τους Remley et al. Η όλη τους φιλοσοφία στηρίχτηκε πάνω στην λογική ότι τα ηλεκτρομαγνητικά κύματα τα οποία μεταδίδονται από συσκευή σε συσκευή έχουν μικρές διαφοροποιήσεις. Οι διαφοροποιήσεις αυτές οφείλονται στις ανομοιότητες που παρουσιάζουν τα ηλεκτρικά κυκλώματα και στις διαφορετικές τοπολογίες των κεραιών από κατασκευαστή σε κατασκευαστή. Τα ιδιαίτερα χαρακτηριστικά του κάθε ηλεκτρομαγνητικού κύματος μπορούν να προσδιοριστούν και να αποτελέσουν το πιστοποιητικό γνησιότητας μιας συσκευής.

Τα χαρακτηριστικά αυτά προσδιορίστηκαν μέσα από μετρήσεις που έγιναν χρησιμοποιώντας υπερευαίσθητους δέκτες. Οι διαφορές που παρουσιάστηκαν αν και μικρές, μπορούσαν να καταγραφούν και να προκύψουν ασφαλή συμπεράσματα. Επιπλέον, διαπίστωσαν ότι μπορούν να καταγράψουν με αρκετά μεγάλη ακρίβεια τον προσανατολισμό και τη θέση της κεραίας που εκπέμπει το σήμα. Ακόμα, οι μετρήσεις διέφεραν ανάλογα με την πόλωση της κεραίας.

Όλα αυτά τα γνωρίσματα πράγματι μπορεί να αποτελέσουν ένα είδος ψηφιακής υπογραφής, που ονόμασαν ηλεκτρομαγνητική υπογραφή. Η μέθοδος αυτή παρουσιάζει αρκετά πλεονεκτήματα, αλλά παρ' όλα αυτά δεν γίνονται αναφορές για τον τρόπο διαφοροποίησης των συσκευών και των τύπων που ανήκουν στον ίδιο κατασκευαστή και κατά συνέπεια τα κυκλώματα και οι κεραίες θα είναι πανομοιότυπα.

9. Μελλοντική Δουλειά

Ο σκοπός της συγκεκριμένης εργασίας ήταν η περιγραφή των σημαντικότερων πρωτοκόλλων δρομολόγησης στα ασύρματα ad-hoc δίκτυα, που αποτελούνται από κινητούς κόμβους και η μελέτη των προβλημάτων ασφάλειας αυτών. Στο παρόν

κεφάλαιο, στο πρώτο μέρος, θα μιλήσουμε για τα σημαντικότερα θέματα που θα απασχολήσουν στο μέλλον την έρευνα και την ανάπτυξη των ασύρματων ad-hoc δικτύων, ενώ στο δεύτερο θα αναφερθούμε στην μελλοντική δουλειά που πιστεύουμε ότι πρέπει να γίνει πάνω στην βελτιστοποίηση του χρόνου ζωής των αποθηκευμένων διαδρομών και κατά συνέπεια στην βελτίωσης της απόδοσης του πρωτοκόλλου.

Όπως έχουμε αναφέρει ήδη, η έρευνα των ασύρματων ad-hoc δικτύων δεν μπορεί να χαρακτηριστεί ακόμα εξαντλητική και πλήρης. Ένα μεγάλο μέρος της προσπάθειας μέχρι τώρα ήταν στην επινόηση των πρωτοκόλλων δρομολόγησης για την αποτελεσματική υποστηρίξει και αποδοτική επικοινωνία των κόμβων του δικτύου. Εντούτοις, υπάρχουν ακόμα πολλά προβλήματα και θέματα που αξίζουν περαιτέρω έρευνα, όπως:

- Scalability — Μέχρι ποιο σημείο μπορεί το μέγεθος, ενός ad-hoc ασύρματου δικτύου, να αυξάνεται.

- Address auto-configuration — Ποιος πρέπει να είναι ο αυτόματος τρόπος ανάθεσης διευθύνσεων στους κόμβους ενός ασύρματου ad-hoc δικτύου. Είναι απαραίτητη η σχεδίαση και ανάπτυξη ενός νέου πρωτοκόλλου ανάθεσης διευθύνσεων στα MANET.
- Interoperation with the Internet — Ο αποτελεσματικός και αποδοτικός τρόπος διασύνδεσης ενός ad-hoc δικτύου με το διαδίκτυο και τις υπηρεσίες που αυτό προσφέρει.

- Improvement of interaction between layers — Υλοποίηση νέων μηχανισμών επικοινωνίας των στρωμάτων της στοίβας του δικτύου, η διαεπικοινωνία τους πολλές φορές κρίνεται απαραίτητη για την βελτίωση της απόδοσης.

- Quality of service (QoS) — Πόσο καλά εφαρμογές, με συγκεκριμένους περιορισμούς, μπορούν να λειτουργήσουν σε ένα MANET.

- Applications for MANET — Ποιες θα είναι οι εφαρμογές που θα κάνουν χρήση της τηλεπικοινωνιακής τεχνολογίας των Mobile Ad-hoc Networks. (Killer applications for MANETs)

- Security — Η ασφάλεια αποτελεί αναπόσπαστο κομμάτι των τηλεπικοινωνιακών δικτυακών συστημάτων και συνεπώς είναι ένα από τα σημαντικότερα θέματα και στα ασύρματα ad-hoc δίκτυα. Το ερώτημα είναι πώς σε δίκτυα δίχως δομή, προϋπάρχουσα υποδομή και διαχείριση, μπορούμε να προσφέρουμε υπηρεσίες ασφάλειας όπως, αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα.

- Power control — Ο τρόπος μεγιστοποίησης της ζωής και της λειτουργίας του δικτύου, με τον αποδοτικότερο τρόπο χρήσης των πηγών ενέργειας των κόμβων (συνήθως μπαταριών).

Μερικά από τα παραπάνω θέματα θα συζητηθούν παρακάτω.

1. Ερευνητικά θέματα και προβλήματα στα ασύρματα ad-hoc δίκτυα

1.1. Scalability

Λόγω πολλών αντιφατικών παραγόντων και χαρακτηριστικών των ασύρματων ad-hoc δικτύων, κανένας δεν μπορεί να ορίσει το μέγεθος ή το όριο του μεγέθους ενός τέτοιου δικτύου. Αυτό που με ασφάλεια μπορούμε να πούμε είναι ότι ένα τέτοιο δίκτυο δεν μπορεί να έχει μέγεθος αντίστοιχο ή ίσο με αυτό που έχει σήμερα το Ιντερνετ, το οποίο αριθμεί δεκάδες εκατομμύρια τερματικών. Στην πραγματικότητα σήμερα, δεν υπάρχουν αναφορές για κανένα ad-hoc ασύρματο δίκτυο που να έχει υλοποιηθεί, παρά μόνο αυτά που έχουν δημιουργηθεί για στρατιωτικούς σκοπούς από τον στρατό των Ηνωμένων Πολιτειών, για τα οποία δεν έχουμε στοιχεία και χαρακτηριστικά.

Οι περισσότερες προσομοιώσεις στα ασύρματα ad-hoc δίκτυα έχουν γίνει με τα μεγέθη των δικτύων να φτάνουν ακόμα και τους 10000 (δέκα χιλιάδες) κόμβους. Τα εργαλεία προσομοίωσης σε περιπτώσεις τέτοιες απαιτούν πολύ μεγάλα μεγέθη μνήμης, σκληρών δίσκων και υπολογιστικής ισχύς για να μπορέσουν να λειτουργήσουν. Γενικά πειράματα που ξεπερνούν τις λίγες χιλιάδες κόμβους απαιτούν πολύ μεγάλο χρόνο εκτέλεσης των πειραμάτων και της συλλογής των αποτελεσμάτων. Γενικά ο χρόνος εκτέλεσης ενός πειράματος εξαρτάται άμεσα από τον αριθμό των κόμβων του δικτύου και από τις παραμέτρους τις οποίες θέλουμε κάθε φορά να μετράμε και να συλλέγουμε. Αυτό δημιουργεί πρόβλημα στην μελέτη της συμπεριφοράς των πρωτοκόλλων τέτοιων δικτύων που αποτελούνται από πολλές εκατοντάδες ή και χιλιάδες κόμβους.

Στην εργασία αυτή περιγράψαμε διάφορα πρωτόκολλα δρομολόγησης. Για όλα τα πρωτόκολλα που περιγράψαμε, αλλά και για τον DSR, έχουν γίνει πειράματα τα οποία περιορίζονταν σε μεγέθη δικτύων της τάξης των μερικών εκατοντάδων κόμβων, στην καλύτερη περίπτωση. Τα εργαλεία μοντελοποίησης και προσομοίωσης δεν επιτρέπουν την εκτέλεση πειραμάτων σε μεγαλύτερα δίκτυα και μας περιορίζουν. Αυτό έχει σαν αποτέλεσμα να μην μπορούμε να γνωρίζουμε σήμερα την συμπεριφορά των διαφόρων πρωτοκόλλων των ασύρματων ad-hoc δικτύων, συμπεριλαμβανομένων και των πρωτοκόλλων δρομολόγησης, σε συνθήκες όπου το μέγεθος του δικτύου αυξάνεται υπερβολικά από λίγες εκατοντάδες σε πολλές δεκάδες χιλιάδες κόμβους.

1.2. Ποιότητα υπηρεσιών σε ad-hoc ασύρματα δίκτυα

Τα περισσότερα από τα πρωτόκολλα δρομολόγησης, στα οποία αναφερθήκαμε στην εργασία αυτή, έχουν σαν σκοπό την εύρεση μονοπατιών ανάμεσα σε δύο κόμβους του δικτύου απλά χωρίς να εξετάζουν την ποιότητα των δικτυακών υπηρεσιών που μπορούν να προσφερθούν πάνω από αυτή την διαδρομή.

Σήμερα υπάρχουν προτάσεις για την υλοποίηση πρωτοκόλλων δρομολόγησης τα οποία εξετάζουν την ποιότητα της σύνδεσης για την εύρεση μιας διαδρομής. Τα πρωτόκολλα αυτά δεν έχουν την απόδοση που έχουν αυτά που προτείνονται ως υποψήφια πρότυπα από την ομάδα εργασίας MANET της IETF, αλλά ανακαλύπτουν διαδρομές οι οποίες περιέχουν συνδέσεις υψηλής ποιότητας.

Η παροχή όμως ποιότητας στις προσφερόμενες υπηρεσίες των ασύρματων δικτύων και συγκεκριμένα των πρωτοκόλλων δρομολόγησης, αφορά την εύρεση διαδρομών ικανών να υποστηρίξουν την εφαρμογή η οποία θα χρησιμοποιήσει το συγκεκριμένο μονοπάτι για την μετάδοση δεδομένων σε ένα άλλο κόμβο του δικτύου. Το ερώτημα στην περίπτωση αυτή είναι εάν το πρωτόκολλο δρομολόγησης είναι ικανό να βρίσκει διαδρομές ικανές να εξυπηρετήσουν τις ανάγκες των εφαρμογών για να λειτουργήσουν. Συγκεκριμένα το πρωτόκολλο πρέπει να μπορεί να βρίσκει διαδρομές για τις οποίες μπορεί να εγγυηθεί για το απαιτούμενο bandwidth και την ελάχιστη καθυστέρηση μετάδοσης των δεδομένων. Τα χαρακτηριστικά αυτά είναι κρίσιμα για τις εφαρμογές πραγματικού χρόνου μετάδοσης ήχου και εικόνας, εφαρμογές μετάδοσης ιατρικών ή άλλων ευαίσθητων δεδομένων, στρατιωτικών εφαρμογών και άλλων.

1.3. Client-Server vs. Pear to Pear application model

Σήμερα γίνεται λόγος για το είδος των εφαρμογών που θα μπορούσαν να λειτουργήσουν αποδοτικά πάνω από τα ad-hoc ασύρματα τηλεπικοινωνιακά δίκτυα.

Γενικά οι δικτυακές εφαρμογές μέχρι σήμερα ακολουθούσαν το μοντέλο του εξυπηρέτη και του εξηπηρετητή (client — server model). Το μοντέλο αυτό υπαγορεύει ότι στο δίκτυο υπάρχουν κόμβοι που επιτελούν συγκεκριμένες εργασίες και προσφέρουν τις υπηρεσίες του σε άλλους κόμβους του δικτύου, οι οποίοι χρησιμοποιούν τις υπηρεσίες αυτές. Οι υπηρεσίες αυτές έχουν να κάνουν με την επεξεργασία, μετάδοση και ανταλλαγή πληροφοριών και για να λειτουργήσουν απαιτούν την παρουσία ενός ή περισσότερων server, που έχουν την ευθύνη εκτέλεσης τους και ενός ή περισσότερων clients, που χρησιμοποιούν τις υπηρεσίες αυτές μέσω του server. Το μοντέλο αυτό δουλεύει πολύ καλά, και σήμερα είναι πολύ διαδεδομένο. Ολόκληρος ο παγκόσμιος δικτυακός ιστός (World Wide Web, www) ή όπως έχουμε συνηθίσει να λέμε κοινά, Ιντερνετ, είναι βασισμένος στο μοντέλο αυτό. Εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, το ηλεκτρονικό εμπόριο, οι ηλεκτρονικές τραπεζικές συναλλαγές, λειτουργούν σύμφωνα με το μοντέλο αυτό.

Στα ασύρματα ad-hoc τηλεπικοινωνιακά δίκτυα όμως το μοντέλο αυτό δεν μπορεί να λειτουργήσει. Τα χαρακτηριστικά των δικτύων αυτών τα έχουμε συζητήσει σε προηγούμενα κεφάλαια. Επίσης έχουμε επισημάνει και τις διαφορές που έχουν με τα δίκτυα, ενσύρματα ή ασύρματα, τύπου Ethernet. Η βασικότερη από αυτές είναι η δυνατότητα της αυτοδημιουργίας και της δυναμικής αλλαγής των χαρακτηριστικών τους στην πάροδο του χρόνου. Αυτό το χαρακτηριστικό κάνει αδύνατη τη λειτουργία του μοντέλου client-server, που περιγράψαμε παραπάνω. Η βασική αρχή του μοντέλου αυτού είναι η ύπαρξη ενός κόμβου, ο οποίος μπορεί να προσφέρει με μεγάλη αξιοπιστία μια υπηρεσία (server). Στην περίπτωση των ad-hoc δικτύων το χαρακτηριστικό αυτό δεν μπορεί να υπάρξει.

Για να μπορέσει λοιπόν το μοντέλο αυτό να λειτουργήσει σε ένα δίκτυο τέτοιου τύπου πρέπει να απαντηθούν τα παρακάτω ερωτήματα. Σε ποιόν κόμβο σε ένα ασύρματο ad-hoc δίκτυο θα υπάρχει η υπηρεσία; Πώς οι άλλοι κόμβοι θα μπορούν να ανακαλύπτουν την υπηρεσία αυτή, εφόσον δεν θα μπορούν να γνωρίζουν εκ των προτέρων την ύπαρξη της; Οι προσφερόμενες υπηρεσίες θα είναι συγκεκριμένες, θα

περιγράφονται με κάποιο πρότυπο και καθολικό τρόπο κατανοητό για όλους τους κόμβους του δικτύου και πώς αυτοί θα γνωρίζουν ποια υπηρεσία να χρησιμοποιήσουν; Θα μπορούν όλοι οι κόμβοι στο δίκτυο να χρησιμοποιήσουν την υπηρεσία αυτή; Ποιος θα είναι υπεύθυνος και θα ορίζει ποιος έχει δικαίωμα να την χρησιμοποιεί, authentication, authorization; Τι θα γίνει στην περίπτωση που δεν θα είναι πλέον δυνατό να δίδεται στους κόμβους η υπηρεσία αυτή;

Οι απαντήσεις στις ερωτήσεις αυτές δεν είναι προφανείς αλλά σήμερα φαίνεται ότι υπάρχουν οι απαραίτητες τεχνολογίες που θα μπορούσαν να δώσουν λύση στο συγκεκριμένο πρόβλημα. Στο σημείο αυτό θα τις αναφέρουμε, χωρίς να είναι θέμα της συγκεκριμένης εργασίας. Οι τεχνολογίες αυτές δεν είναι άλλες από τα Peer-To-Peer συστήματα και η τεχνολογία των grids. Τα πρώτα αναφέρονται σε συστήματα τα οποία δεν ακολουθούν το μοντέλο του client-server, αλλά όλοι οι κόμβοι καλούνται να επιτελέσουν και τους δύο ρόλους. Υπάρχουν διαφορές όσο και οι ομοιότητες των ad-hoc ασύρματων δικτύων (MANETs) και των Peer-To-Peer (p2p) συστημάτων καθώς και δυνατότητες συνεργασίας των δύο αυτών δικτυακών συστημάτων, παρά τις πολλές και σημαντικές διαφορές τους. Η τεχνολογία των grids αναφέρεται σε συστήματα που αποτελούνται από κόμβους οι οποίοι μπορούν να εκτελούν με κατανεμημένο τρόπο, με κοινό σκοπό, την λειτουργία μίας διεργασίας ή μίας υπηρεσίας. Τα χαρακτηριστικά αυτής της τεχνολογίας ταιριάζουν επίσης με ένα ad-hoc δικτυακό περιβάλλον και μπορούν να χρησιμοποιηθούν για την δημιουργία λογισμικού για τα δίκτυα αυτά.

1.4. Security

Η ασφάλεια στα δίκτυα υπολογιστών αποτελεί ένα από τα σημαντικότερα σύγχρονα θέματα και προβλήματα. Σήμερα είναι πολύ σημαντικό ένα τηλεπικοινωνιακό σύστημα και οι προσφερόμενες υπηρεσίες αυτού να είναι ασφαλείς. Η ασφάλεια ενός συστήματος ορίζεται ως οι διαδικασίες εκείνες που εγγυώνται την ακεραιτότητα και εμπιστευτικότητα των δεδομένων και την αυθεντικοποίηση των χρηστών. Σήμερα τα θέματα ασφάλειας στα ασύρματα ad-hoc δίκτυα δεν έχουν ερευνηθεί αρκετά και ο λόγος είναι ότι η έρευνα στα θέματα ασφάλειας σε αυτού του τύπου τα δίκτυα είναι πολύ δύσκολη λόγω των ιδιαίτερων χαρακτηριστικών τους. Η υλοποίηση υπηρεσιών και μηχανισμών ασφάλειας στα ασύρματα ad-hoc δίκτυα παρόμοιων με αυτές που υπάρχουν στα άλλα τηλεπικοινωνιακά συστήματα δεν μπορεί να γίνει. Υπάρχουν πολλά προβλήματα τα οποία δύσκολα μπορούν να υπερπηδηθούν. Το βασικότερο από όλα έχει να κάνει με την απουσία κάποιας κεντρικής διαχείρισης του δικτύου, η οποία θα μπορούσε να αναλάβει κεντρικό ρόλο στις υπηρεσίες ασφαλείας. Ο ρόλος μιας τέτοιας οντότητας σε ένα δίκτυο είναι χωρίς άλλο η διανομή των απαραίτητων πληροφοριών, παραδείγματος χάριν, κλειδιών στους κόμβους του δικτύου για να μπορέσουν να χρησιμοποιήσουν τους μηχανισμούς ασφαλείας

Τα ασύρματα ειδικά δίκτυα έχουν προταθεί για να υποστηρίξουν σενάρια όπου δεν υπάρχει καμία δικτυακή υποδομή. Τα ασύρματα ad-hoc δίκτυα εισάγουν δύο κύρια προβλήματα που συνήθως δεν αντιμετωπίζονται από τα παραδοσιακά πρωτόκολλα δρομολόγησης, την έλλειψη υποστήριξης προϋπάρχουσας υποδομής και τις συχνές αλλαγές στην τοπολογία των κόμβων του δικτύου. Στο φυσικό επίπεδο το ασύρματο κανάλι προσφέρει μικρή προστασία στα πακέτα του πρωτοκόλλου, τα οποία είναι ευαίσθητα σε εξωτερικές παρεμβολές του ασύρματου σήματος, στην παρουσία jamming κόμβων, στην αλλοίωση των δεδομένων που μεταφέρουν και στην μη

εξουσιοδοτημένη παραλαβή τους (eavesdropping) από κόμβους του δικτύου. Η προσθήκη επιπρόσθετων μηχανισμών, που θα εξασφαλίζουν την ασφαλή μετάδοση των πακέτων πληροφοριών, κώδικες διόρθωσης λαθών, frequency hopping σχήματα, κ.λπ, στα φυσικό και MAC επίπεδο, μπορεί να αντιμετωπίσει αυτά τα προβλήματα. Τα πρωτόκολλα δρομολόγησης από την φύση τους στηρίζονται στην συνεργασία των κόμβων του δικτύου και στην αμοιβαία εμπιστοσύνη αυτών για την μεταγωγή των πακέτων δεδομένων. Το γεγονός αυτό επιτρέπει σε κακόβουλους κόμβους να μπορούν να παραλύσουν ένα τέτοιο δίκτυο με την παρεμβολή λανθασμένων πληροφοριών δρομολόγησης, επανάληψη παλαιών πληροφοριών δρομολόγησης, αλλαγή αναπροσαρμοσμένων νέων πληροφοριών δρομολόγησης ή μετάδοση λανθασμένων πληροφοριών δρομολόγησης. Οι επιθέσεις αυτές είναι δυνατές και στα κλασικά ενσύρματα δίκτυα επίσης, αλλά η φύση του περιβάλλοντος των ad-hoc δικτύων ενισχύει τις επιθέσεις αυτές και κάνει δυσκολότερο τον εντοπισμό τους.

2. Μελλοντική δουλειά στο πρόβλημα του caching

2.1. Χαρακτηρισμός διαδρομών δρομολόγησης

Κριτήρια που μπορούν να βελτιώσουν σημαντικά την απόδοση ενός αλγορίθμου, εκτός από τη βελτιωμένη λειτουργία της Route Cache υπάρχουν πολλά. Η χρησιμοποίηση και άλλων χαρακτηριστικών όπως η ενέργεια που απαιτείται για την χρήση του συγκεκριμένου μονοπατιού, μπορούν να συνδυαστούν και να χρησιμοποιηθούν για τον χαρακτηρισμό εγκυρότητας διαδρομών δρομολόγησης. Η υλοποίηση μας επιτρέπει την εισαγωγή και άλλων παραμέτρων για τον χαρακτηρισμό των διαδρομών δρομολόγησης.

2.2. Εφαρμογή του TTL και σε άλλους αλγόριθμους δρομολόγησης

Στα πειράματα που εκτελέστηκαν, χρησιμοποιήθηκε σαν αλγόριθμος δρομολόγησης ο DSR, αφού είναι ένα από τα σημαντικότερα πρωτόκολλο της κλάσης του στον χώρο των δικτύων ad-hoc. Για να μπορέσουμε να γενικεύσουμε τα συμπεράσματα μας είναι απαραίτητο να εφαρμόσουμε την συγκεκριμένη τεχνική και σε άλλα πρωτόκολλα δρομολόγησης που χρησιμοποιούν αποθηκευμένες πληροφορίες δρομολόγησης.

Χαρακτηριστικά αναφέρουμε την εφαρμογή της τεχνικής αυτής στον AODV. Η διαφορά είναι ότι στην περίπτωση αυτή οι πίνακες δρομολόγησης αφορούν τους ενδιάμεσους κόμβους, και η επιλογή των αντίστοιχων τιμών του TTL πρέπει να υπακούει διαφορετικούς κανόνες.

3. Βελτίωση παραμέτρων προσομοίωσης

Στο τέλος αφήσαμε, όπως πιστεύουμε ένα από τα σημαντικότερα θέματα, το πρόβλημα της δημιουργία μοντέλων και σεναρίων προσομοίωσης που να μπορούν να προσεγγίζουν όσο είναι το δυνατό τα πραγματικά ασύρματα ad-hoc δίκτυα.

Μια από τις σημαντικότερες μεθόδους για την αξιολόγηση των χαρακτηριστικών των ad-hoc τηλεπικοινωνιακών δικτύων είναι η χρήσης της μεθόδου της προσομοίωσης.

Η προσομοίωση παρέχει στους ερευνητές την δυνατότητα μελέτης της συμπεριφοράς των πρωτοκόλλων κάτω από ελεγχόμενες συνθήκες όπως, τα επαναλαμβανόμενα σενάρια, η απομόνωση συγκεκριμένων παραμέτρων και η εξερεύνηση ποικίλων παραμέτρων και αποτελεσμάτων. Η τοπολογία και η κίνηση των κόμβων του δικτύου είναι βασικοί παράγοντες για την μελέτη του δικτυακού συστήματος, κατά την διάρκεια της προσομοίωσης. Οι κόμβοι αφού τοποθετηθούν σε μία αρχική θέση, αρχίζουν να κινούνται μέσα στα γεωγραφικά όρια του δικτύου, σύμφωνα με αυτά που υπαγορεύει το μοντέλο της κίνησης τους. Η κινητικότητα των κόμβων επηρεάζει άμεσα την απόδοση των πρωτοκόλλων δρομολόγησης Τα αποτελέσματα προσομοίωσης που επιτυγχάνονται με τα μη ρεαλιστικά σενάρια κίνησης μπορούν να μην απεικονίσουν σωστά την απόδοση τους. Η πλειοψηφία των υπαρχόντων προτύπων κινητικότητας για ασύρματα ad-hoc δίκτυα δεν παρέχει ρεαλιστικά σενάρια μετακίνησης. Τα περισσότερα περιορίζονται στην δημιουργία τυχαίων μονοπατιών που ακολουθούν οι κόμβοι κατά την διάρκεια της προσομοίωσης.

Στο μέλλον είναι απαραίτητο να δημιουργηθούν μοντέλα κίνησης, τα οποία θα επιτρέπουν στους ερευνητές να ορίσουν ένα ασύρματο δίκτυο, το οποίο θα αποτελείται από κόμβους που θα μπορούν να κινούνται σε ένα περιβάλλον που θα προσεγγίζει την πραγματικότητα. Με άλλα λόγια πρέπει να δημιουργηθούν ρεαλιστικά μοντέλα κίνησης, τα οποία δεν θα περιγράφουν απλά ένα χώρο μέσα στον οποίο θα μπορούν να κινούνται οι κόμβοι του δικτύου, αλλά θα περιέχουν και εμπόδια τα οποία περιορίζουν την κίνηση τους, καθώς επίσης και την εμβέλεια των ασύρματων μεταδόσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. M.S. Corson, J. Macker, and S. Batsell, "Architectural Considerations for Mobile Mesh Networking," In Proceedings of the IEEE MILCOM, October 1996.

2. IETF MANET Working Group,
http://www.ietf.org/html.charters/manet-charter.html

3. C.E. Perkins and P. Bhagwat,"Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," In Computer Comm. Review, October 1994.

4. S. Murthy and J.J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," In ACM Mobile Networks and Applications Journal, October 1996.

5. David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. 1996.

6. C.E. Perkins and E. Royer, "Ad hoc on-demand distance vector routing," IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

7. V.D. Park and M.S. Corson, "A highly adaptive distributed routing algorithm for mobile and wireless networks," In Proceeding of IEEE INFOCOM, April 1997.

8. G. Aggelou and R. Tafazolli, "RDMAR: A bandwidth-efficient routing protocol for mobile ad hoc networks," in ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), August 1999.

9. Z. Haas et al, "The performance of query control schemes for the zone routing protocol," in ACM SIGCOMM, 1998.

10. A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," IEEE Journal on Selected Areas of Communications, August 1999.

11. G. Pei, M. Gerla, and X. Hong, "Lanmar: Landmark routing for large scale wireless ad hoc networks with group mobility," In ACM MobiHoc, August 2000.

12. P.F. Tsuchiya, "The Landmark Hierarchy: a new hierarchy for routing in very large networks," In Computer Communication Review, Aug. 1988.

13. Jiejun Kong, Xiaoyan Hong, Yunjung Yi, JoonSang Park, Jun Liu, Mario Gerla, "A Secure Adhoc Routing Approach using Localized Selfhealing Communities".

14. Patroklos G. Argyroudis, Donal O'Mahony, "Secure Routing for Mobile Ad hoc Networks"

15. Panagiotis Papadimitratos and Zygmunt J. Haas, “Secure Routing for Mobile Ad hoc Networks”, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002

16. Dr. Mustapha GUEZOURI and Abdelaziz OUAMRI, “Optimizing Routes Quality and Scattering in the AODV Routing Protocol”, Signal Image Lab, Department of Electronics, University of Science and Technology, Oran, Algeria

17. Zeyad M, Alfawaer, GuiWei Hua and Nidal Abu Hamdeh, “Utilization of AODV in Wireless Ad – Hoc Networks”, School of Science and Engineering, Bei hang University, Beijing 100083, China

18. Juan-Carlos Ruiz, Jesus Friginal, David de-Andres, Pedro Gil, “Black Hole Attack Injection in Ad-Hoc Networks”, Fault Tolerance Systems Group, Universidad Politecnica de Valencia, Spain

19. Pin Nie, “Security in Ad Hoc Network”, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology

20. Panagiotis Papadimitratos, Zygmunt J. Haas, “Secure Message Transmission in Mobile Ad-Hoc Networks”, Electrical and Computer Engineering Department, Cornell University, USA