ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Αδυναμίες Ασφάλειας και Επιθέσεις σε Manet Δίκτυα

Γρηγόριος Μητρόπουλος

Η εργασία υποβάλλεται για την μερική κάλυψη των απαιτήσεων
με στόχο την απόκτηση του Μεταπτυχιακού Διπλώματος
Σπουδών στα Ψηφιακά Συστήματα

Επιβλέπων Καθηγητής : Χρήστος Ξενάκης

Ιούνιος 2011

Αφιερώνεται στους πραγματικούς μου φίλους

Θέμα

Αδυναμίες Ασφάλειας και Επιθέσεις σε Manet Δίκτυα

«*Τα adhoc δίκτυα και κατ επέκταση τα manet είναι δίκτυα τυχαία διαμορφωμένα, χωρίς σταθερή υποδομή δικτύου και βασίζονται σε ασύρματες συνδέσεις ώστε να μπορούν να επικοινωνούν μεταξύ τους οι συσκευές. Λόγω της έλλειψης σταθερής υποδομής δικτύου, τα εν λόγω δίκτυα είναι τρωτά σε διάφορες επιθέσεις. Στην πτυχιακή αυτή εργασία, θα γίνει μια εκτενής μελέτη των επιθέσεων σε ad hoc δίκτυα, με σκοπό την ταξινόμηση και κατηγοριοποίηση τους με βασικό κριτήριο το επίπεδο διαστρωμάτωσης (application, presentation, session, transport, network, data-link, και physical layer) στο οποίο πραγματοποιούνται οι εν λόγω επιθέσεις.* »

Keys Words: AdHoc, Manet, OSI Model, Attacks, IDS

Περίληψη

Τα Ad hoc δίκτυα μπορούν να διαμορφώνονται, να συγχωνεύονται ή να διαχωρίζονται σε διαφορετικά δίκτυα ακαριαία χωρίς κατ 'ανάγκη να στηρίζονται σε μια σταθερή υποδομή για τη διαχείριση της ενέργειας. Οι κόμβοι των AdHoc δικτύων είναι συχνά κινητοί το οποίο υποδηλώνει ότι εφαρμόζουν την ασύρματη επικοινωνία για τη διατήρηση της σύνδεσης και η συγκεκριμένη κατηγορία αυτών των δικτύων ονομάζεται κινητά adhoc δίκτυα ή αλλιώς Mobile AdHoc Networks (MANET).

Όσον αφορά τις επιθέσεις στα Manets στο φυσικό επίπεδο του προτύπου OSI είναι αυξημένες εξαιτίας της ασύρματης ιδιότητας των παραπάνω δικτύων τα οποία έχουν σαν μέσο μετάδοσης τον αέρα. Τα MANET βασίζονται στην ανοικτή "peer to peer" αρχιτεκτονική πολλαπλών βημάτων (multihops) ώστε να γίνει η επικοινωνία σε επίπεδο δικτύου. Οι επιθέσεις μπορούν επίσης να πραγματοποιηθούν στο επίπεδο ζεύξης δεδομένων διακόπτοντας τη συνεργασία των πρωτοκόλλων του συγκεκριμένου επιπέδου. Η βασική ιδέα πίσω από τις επιθέσεις στο επίπεδο του δικτύου είναι να απορροφηθεί η κυκλοφορία του δικτύου και να προκληθεί η εκτροπή και ως εκ τούτου ο έλεγχος της ροής της κυκλοφορίας του δικτύου. Οι στόχοι του πρωτοκόλλου TCP (πρωτόκολλο επιπέδου μεταφοράς) στα Manet περιλαμβάνουν τη συγκρότηση μιας «end-to-end» σύνδεσης, μιας «end-to-end» αξιόπιστης παράδοσης των πακέτων, έλεγχο ροής, έλεγχο συμφόρησης και συμψηφισμό της «end-to-end» σύνδεσης στο τέλος. Οι επιθέσεις στο επίπεδο εφαρμογών είναι ελκυστικές για τους επιτιθέμενους επειδή οι πληροφορίες που αναζητούν υπάρχουν μέσα στις εφαρμογές και το γεγονός αυτό έχει ένα αντίκτυπο στην επίτευξη των στόχων τους. Ορισμένες από τις επιθέσεις στα Manet μπορεί να ξεκινήσουν και να εκτελεστούν σε περισσότερα από ένα επίπεδα του προτύπου OSI.

Η επιτυχία των δικτύων Manet εξαρτάται σε μεγάλο βαθμό από το αν οι κανόνες ασφαλείας είναι έμπιστοι. Ωστόσο τα χαρακτηριστικά των Manets δημιουργούν προκλήσεις αλλά και ευκαιρίες για την επίτευξη των στόχων ασφάλειας όπως η εμπιστευτικότητα (confidentiality), η ταυτοποίηση (authentication), η ακεραιότητα (integrity), η διαθεσιμότητα (availability), ο έλεγχος πρόσβασης (access control) και η μη άρνηση αναγνώρισης ή η μη αποποίησης ευθυνών (non-repudation)

Οι μεγάλες προκλήσεις που αντιμετωπίζουν τα δίκτυα Manet από την αρχιτεκτονική του διαδικτύου μπορούν να ταξινομηθούν ως εξής: 1) Στην ενσωμάτωση των αναδυόμενων ασυρμάτων στοιχείων του δικτύου όπως οι φορητές συσκευές, οι ad-hoc δρομολογητές και οι ενσωματωμένοι αισθητήρες στο υφιστάμενο πλαίσιο του πρωτοκόλλου και 2) Στην παροχή «end-to-end» υπηρεσιών η οποία διευκολύνει την ανάπτυξη εφαρμογών.

Abstract

The Ad hoc networks can be developed, merged or separated into different networks instantaneously without necessarily relying on a solid infrastructure for energy management. The nodes of AdHoc mobile networks are often indicating that applying wireless communication to maintain the connection and the specific type of these networks is called Mobile AdHoc Networks (MANET).

Regarding attacks on Manets physical layer of OSI model is increased because of the status of these wireless networks which have the means of transmission in the air. The MANET based on open "peer to peer" architecture multihops to make contact at the network level. The attacks may also be made at the data link disrupting cooperation protocols at that level. The basic idea behind the attacks at the network layer is to absorb network traffic and cause a diversion and thereby control the flow of network traffic. The objectives of the protocol TCP (transport layer protocol) to Manet include the establishment of a «end-to-end» link, association of «end-to-end» reliable delivery of packets, flow control, congestion control and offset the «end-to-end» link at the end. The attacks on application level is attractive to attackers because information seekers are in their applications and this has an impact on achieving their goals. Some of the attacks on Manet can start and run more than one level of the OSI model.

The success of Manet networks depends largely on whether safety standards are trusted. However, the characteristics of Manets create challenges and opportunities for the achievement of security such as confidentiality, authentication, integrity, availability, access control and non-repudiation.

The major challenges faced by Manet networks architecture of the Internet could be classified as follows: 1) The integration of emerging wireless network elements such as mobile devices, ad-hoc routers and sensors embedded in the existing framework of the protocol, and 2) Providing «end-to-end» services that facilitates the development of applications.

Ευχαριστίες

Ολοκληρώνοντας την διπλωματική μου εργασία θα ήθελα πρωτίστως να ευχαριστήσω τον καθηγητή μου, Χρήστο Ξενάκη, επίκουρο καθηγητή του τμήματος Ψηφιακών Συστημάτων του Πανεπιστήμιου Πειραιά ό οποίος μου επιστέφτηκε την συγκεκριμένη θεματική ενότητα την οποία ήθελα να μελετήσω. Πολύτιμη ήταν επίσης η συνεισφορά του βοηθού του καθηγητή μου, Χριστόφορου Πάνου ο οποίος με μεγάλη προθυμία με βοήθησε καθ' όλη την διάρκεια εκπόνησης αυτής της εργασίας.

Θα ήθελα επίσης να ευχαριστήσω τους γονείς μου οι οποίοι με στήριξαν πραγματικά καθ' όλη την διάρκεια των σπουδών μου, δίνοντας μου εμμέσως πραγματικά εφόδια για την μετέπειτα ζωή μου που δεν είναι άλλα από την μορφή μου.

Τέλος θα ήθελα να ευχαριστήσω όλους τους συναδέλφους-συμφοιτητές μου με τους όποιους συνεργάστηκα και μοιράστηκα πολλές ανησυχίες κατά την διάρκεια εκπόνησης του μεταπτυχιακού μου κύκλου σπουδών όπως επίσης και τους πραγματικούς μου φίλους οι οποίοι με ανέχτηκαν.

Αθήνα , Ιούνιος 2011

Μητρόπουλος Γρηγόρης

Περιεχόμενα

Περιεχόμενα Εικόνων

Κεφάλαιο 1

Εισαγωγή

1.1 Εισαγωγή

Ένα ad hoc δίκτυο είναι μια συλλογή από κόμβους που δεν χρειάζεται να βασίζονται σε μια προκαθορισμένη υποδομή ώστε να κρατήσουν συνδεδεμένο το δίκτυο. Τα Ad hoc δίκτυα μπορούν να διαμορφώνονται, να συγχωνεύονται ή να διαχωρίζονται σε διαφορετικά δίκτυα ακαριαία χωρίς κατ 'ανάγκη να στηρίζονται σε μια σταθερή υποδομή για τη διαχείριση της ενέργειας.[24] Έτσι ένα δίκτυο ad hoc ορίζεται ως *"ένα αυτόνομο σύστημα των δρομολογητών που συνδέονται με ασύρματες συνδέσεις, την ένωση των οποίων υποστηρίζει ένας αυθαίρετος γράφος. Οι δρομολογητές είναι ελεύθεροι να κινούνται και να οργώνονται τυχαία και αυθαίρετα. Επομένως η ασύρματη τοπολογία του δικτύου μπορεί να αλλάξει γρήγορα και απρόβλεπτα. Ένα τέτοιο δίκτυο μπορεί να λειτουργεί με ένα αυτόνομο τρόπο ή μπορεί να συνδεθεί με την ευρύτερη λειτουργία του διαδικτύου ως ένα υβριδικό-σταθερό δίκτυο ad hoc. "[25]*

Οι κόμβοι των AdHoc δικτύων είναι συχνά κινητοί το οποίο υποδηλώνει ότι εφαρμόζουν την ασύρματη επικοινωνία για τη διατήρηση της σύνδεσης και η συγκεκριμένη κατηγορία αυτών των δικτύων ονομάζεται κινητά ad hoc δίκτυα ή αλλιώς **Mobile AdHoc Networks** (MANET). Η κινητικότητα δεν είναι ωστόσο η απαίτηση για τους κόμβους σε adhoc δίκτυα και έτσι ενδέχεται να υπάρχουν στατικοί και ενσύρματοι κόμβοι οι οποίοι μπορούν να κάνουν χρήση των υπηρεσιών που προσφέρονται από σταθερές δικτυακές υποδομές. Τα MANETs αποτελούν ένα νέο πρότυπο του ασύρματου δικτύου προσφέροντας απεριόριστη κινητικότητα χωρίς καμία σχετική υποδομή, όπως σταθμό βάσης ή κινητά κέντρα μεταγωγής.

Η παρούσα διπλωματική αναφέρεται στις αδυναμίες ασφάλειας και επιθέσεις σε Manet δίκτυα και ένας **ορισμός** τους παρατίθενται παρακάτω:

Mobile Ad-hoc Network (MANET) *είναι ένα αυτο-οργανώσιμο αυτο-σχηματιζόμενο ασύρματο δίκτυο με διαδρομές πολλαπλών τμημάτων (multi-hop), όπου η δομή του δικτύου αλλάζει δυναμικά λόγω της κινητικότητας των κόμβων ή αλλαγών στην τοπολογία.*

1.2 Ιστορική Αναδρομή

Η πρώτη γενεά Ad-hoc δικτύων στις αρχές της δεκαετίας του 1970 λεγόταν "**packet radio networks"** (ραδιοφωνικά δίκτυα πακέτου - **PRNET**) και βρίσκονταν υπό την αιγίδα του Defense Advanced Research Projects Agency (DARPA). Τα PRNET παρείχαν μέσω ενός κοινού ραδιοφωνικό καναλιού την ανταλλαγή δεδομένων μεταξύ γεωγραφικά χωρισμένων υπολογιστών. Ένα από τα πλεονεκτήματα τους ήταν η κινητικότητα. Ένα πακέτο (PR) θα μπορούσε να λειτουργεί εν κινήσει. Δεύτερον, δεδομένου ότι δεν υπάρχουν καλώδια για να τρέξει το δίκτυο θα μπορούσε να εγκατασταθεί ή να αναπτυχθεί γρήγορα. Ένα τρίτο

πλεονέκτημα είναι η ευκολία στην σχετική ρύθμιση και στην αναδιάταξη. Τα πρωτόκολλα PRNET εκμεταλλεύτηκαν τις ραδιοτηλεοπτικές εκπομπές και τις ιδιότητες των κοινών καναλιών για να επιτρέψουν την επέκταση και την αναπροσαρμογή των δικτύων αυτόματα και δυναμικά. Όταν μια ομάδα πακέτων (PR) εξέρχονταν από την αρχική περιοχή αυτό δεν είχε δυσμενείς επιπτώσεις για το υπόλοιπο δίκτυο. Τα πακέτα αυτά εγκατέλειπαν το δίκτυο και είχαν την ευελιξία να λειτουργήσουν ως αυτόνομη ομάδα και να επανέλθουν στο αρχικό δίκτυο ή να συμμετάσχουν σε κάποια άλλη ομάδα. Η γενιά των PRNET δικτύων χαρακτηρίστηκε από την πλήρως αυτοματοποιημένη διαχείριση του δικτύου. Ένα PRNET δίκτυο αποτελείται από τα ακόλουθα μέρη :

- Το *υποδίκτυο (subnet) PRNET* με τα ραδιοφωνικά του πακέτα (PR). Το υποδίκτυο PRNET παρείχε τα μέσα της διασύνδεσης της κοινότητας των χρηστών.

- *Μια συλλογή συσκευών (υπολογιστές και τερματικά)* καθένα από τα οποία συνδεόταν με ένα πακέτο PR μέσω ενός υψηλού επιπέδου Data Link Control (HDLC) πρωτοκόλλου για την ανταλλαγή δεδομένων σε πραγματικό χρόνο[1].

Στη δεκαετία του 1980 τα PRNET δίκτυα εξελίχθηκαν στην **δεύτερη γενιά των ad hoc δικτύων** η οποία είναι γνωστή ως **Survivable Adaptive Radio Network** (SURAN). Τα SURAN παρείχαν ένα δίκτυο μεταγωγής πακέτου (packet-switched network) της κινητής τηλεφωνίας στο πεδίο της μάχης, σε ένα περιβάλλον δηλαδή χωρίς καμία υπάρχουσα υποδομή. Το SURAN αναπτύχθηκε από την έρευνα για την εξεύρεση λύσεων για την κατασκευή μικρότερων, λιγότερο ακριβών και λιγότερο ευάλωτων σε ηλεκτρονικές επιθέσεις, πακέτων. Τέλος το SURAN εκμεταλλεύτηκε τα πλεονεκτήματα της δικτύωσης των PRNET για το περιβάλλον μάχης ώστε να επιδείξει και έπειτα να αξιολογηθεί ένα ολοκληρωμένο δίκτυο που βασίζεται στην τεχνολογία του[1].

Η τρίτη γενιά Ad Hoc δικτύων η οποία προέκυψε στην δεκαετία του 1990 την οποία συνεχίζουμε να την χρησιμοποιούμε και σήμερα είναι τα **MANETs.** Οι πιο σημαντικές τεχνολογίες που προέκυψαν εξαιτίας της τεχνολογίας των MANET είναι η δικτύωση *Bluetooth* και τα *AdHoc δίκτυα αισθητήρων*. Το Bluetooth εμφανίστηκε στο προσκήνιο το 1998 περίπου και μας έδωσε τη δυνατότητα υποστήριξης πολλών χρηστών σε οποιοδήποτε περιβάλλον μέσω ενός μικρού δικτύου που είναι γνωστό ως *piconet*. Σε κάθε δεδομένη στιγμή έως και δέκα piconets μπορεί να υπάρχουν στην ίδια περιοχή κάλυψης. Μια συσκευή Bluetooth μπορεί να λειτουργήσει τόσο ως πελάτης (client) όσο και εξυπηρετητής (server) αλλά η ιδιότητα του κάθε εμπλεκόμενου στην σύνδεση θα πρέπει να καθοριστεί πριν τα δεδομένα αρχίσουν να ανταλλάσσονται. Η σύνδεση αυτή ονομάζεται σύζευξη και πρέπει να ζητηθεί πριν την καθιέρωσή της[1].

Ένα ασύρματο δίκτυο AdHoc αισθητήρων αποτελείται από έναν αριθμό αισθητήρων οι οποίοι κατανέμονται σε μία γεωγραφική περιοχή. Κάθε αισθητήρας έχει δυνατότητα ασύρματης επικοινωνίας και κάποιο επίπεδο νοημοσύνης για την επεξεργασία του σήματος και τη δικτύωση των δεδομένων.

Η παρούσα διπλωματική εργασία ασχολείται με τις επιθέσεις στα δίκτυα Manet όποτε στο παρόν κεφάλαιο γίνεται πλήρης περιγραφής των Manet δικτύων και στα επόμενα κεφάλαια των επιθέσεων σε αυτά, κατανεμημένων στο πρότυπο OSI[1].

Ημερομηνία	**Γενιά**	**Εξέλιξη**
1972	*1η*	• PRNET (Packet Radio Networks) • ALOHA (Arial Locations of Hazardous Atmospheres) • CSMA (Carrier Sense Medium Access)
1980	*2η*	• SURAN (Survivable Adaptive Radio Networks)
Νωρίτερα από το 1990	*3η*	• GloMo (Global Mobile Information Systems) • NTDR (Near-term Digital Radio) • Σύσταση Ομάδας Εργασίας για τα Manet,1991.
Μέσα και Αργότερα από το 1990		• JTRS (Joint Tactical Radio System), 1996. • IETF δημοσίευση διάφορων σχεδίων σχετικά με τα πρωτόκολλα δρομολόγησης στα MANET,2000. • IEEE Ίδρυση Εργαστηρίου για τα Manet και την Πληροφορική, 2000.
Μέλλον	*4η*	• Χρήση κινητών adhoc δρομολογητών για την παροχή στους χρήστες σύνδεσης στο Διαδίκτυο . • Κατανεμημένα δίκτυα αισθητήρων. • Δίκτυα αποκατάστασης καταστροφών.

Εικόνα 1 Ιστορική Ανάπτυξη των Manet [2].

1.3 Χαρακτηριστικά των δικτύων Manets

Η αρχή πίσω από την AdHoc δικτύωση είναι η αναμετάδοση με την τεχνική των πολλαπλών αλμάτων (multihops) το οποίο σημαίνει ότι τα μηνύματα διαβιβάζονται από τους άλλους κόμβους εάν ο κόμβος-στόχος δεν είναι άμεσα προσπελάσιμος.

Ένα δίκτυο MANET αποτελείται από κινητές μονάδες (π.χ. ένα δρομολογητή με πολλούς hosts και ασύρματες συσκευές που θα αποκαλούνται κόμβοι) οι οποίες είναι ελεύθερες να μετακινηθούν σε όποια κατεύθυνση επιθυμούν. Αυτοί οι κόμβοι χρησιμοποιώντας τις ασύρματες τεχνολογίες μετάδοσης δεδομένων όπως το *Bluetooth* και το πρωτόκολλο *802.11* μπορούν να βρίσκονται σε αεροπλάνα, πλοία, φορτηγά, αυτοκίνητα, ακόμα και σε ανθρώπους. Ένα δίκτυο MANET λοιπόν, είναι ένα αυτόνομο σύστημα αποτελούμενο από κινητούς κόμβους. Το σύστημα αυτό μπορεί να λειτουργεί απομονωμένο, στο οποίο η απουσία οποιουδήποτε κεντρικού σταθμού βάσεως καθιστά δύσκολη τη διαχείριση του δικτύου και την επικοινωνία με

ένα σταθερό δίκτυο. Στον δεύτερο τρόπο λειτουργίας το σύστημα θα λειτουργεί σαν ένα «αποκομμένο δίκτυο» (stub network) που συνδέεται με ένα σταθερό δίκτυο. Τα «αποκομμένα δίκτυα» μεταφέρουν δικτυακή κίνηση που προέρχεται ή κατευθύνεται προς τους εσωτερικούς κόμβους αλλά δεν επιτρέπει η εξωτερική κίνηση να μεταφερθεί μέσω του «αποκομμένου δικτύου».

Οι κόμβοι του δικτύου MANET είναι εξοπλισμένοι με ασύρματους πομπούς και δέκτες χρησιμοποιώντας κεραίες που μπορεί να είναι μη κατευθυντικές (omnidirectional), πολύ-κατευθυντικές (point-to-point), πιθανώς μεταβλητές, ή κάποιος συνδυασμός των παραπάνω. Σε κάποιο χρονικό σημείο ανάλογα με τη θέση των κόμβων, την εμβέλεια των πομποδεκτών τους, τη μεταδιδόμενη ισχύ τους και τα επίπεδα παρεμβολών, μια ασύρματη σύνδεση στη μορφή ενός τυχαίου AdHoc δικτύου δημιουργείται ανάμεσά τους. Αυτή η AdHoc τοπολογία μπορεί να αλλάξει με την πάροδο του χρόνου καθώς οι κόμβοι μετακινούνται ή αλλάζουν την ισχύ μετάδοσής τους.

Τα βασικά χαρακτηρίστηκα των Manets είναι τα εξής:

- *Μη ύπαρξη καλωδίωσης:* Όπως είναι φυσικό αφού πρόκειται για κινητό – ασύρματο δίκτυο, δεν υπάρχει κάποια μορφή καλωδίωσης όσον αφορά την δικτύωση των κόμβων γεγονός που κάνει πολύ φτηνή και εύκολη την εγκατάστασή του.

- *Δυναμική Τοπολογία:* Η τοπολογία δικτύου σε ένα Manet ασύρματο δίκτυο είναι ιδιαίτερα δυναμική λόγω της κινητικότητας των κόμβων. Μπορεί ο κάθε κόμβος να κινείται μέσα και έξω από την εμβέλεια του άλλου. Η τοπολογία αλλάζει εάν ένα από αυτά τα γεγονότα συμβεί ενώ ο πίνακας δρομολόγησης και ο πίνακας πολύ-εκπομπής πρέπει να αλλάξουν αναλόγως. Αυτό αυξάνει τη δυσκολία στη διαχείριση του δικτύου.

- *Κόμβοι με περιορισμένη κατανάλωση ενέργειας*: Πολλοί, αν όχι όλοι οι κόμβοι σε ένα δίκτυο MANET στηρίζονται σε μπαταρίες. Για το λόγο αυτό η ενέργεια που είναι δυνατόν να καταναλωθεί είναι περιορισμένη, γεγονός που έχει ως αποτέλεσμα η διαχείρισή της να αποτελεί μείζων θέμα για τη βελτιστοποίηση του όλου συστήματος.

  Προκειμένου να εξοικονομηθεί ενέργεια μερικές συσκευές μπορούν να λειτουργούν με έναν αντίστοιχο τρόπο. Κατά τη διάρκεια αυτής της περιόδου δεν είναι ενδεχομένως προσπελάσιμοι ή δεν επεξεργάζονται την κίνηση που περνά από αυτούς ή μεταπίπτουν στον κανονικό τρόπο λειτουργίας με καθυστέρηση. Από τη μια μεριά, οι περισσότερες ασύρματες συσκευές χρησιμοποιούν τις επικοινωνίες εξάπλωσης φάσματος οι οποίες χρειάζονται τη λήψη και την αποκωδικοποίηση του σήματος. Αυτές είναι ακριβές διαδικασίες που καταναλώνουν πολλή ενέργεια. Αφ' ετέρου, μερικοί σύνθετοι υπολογισμοί είναι επίσης πολύ ακριβοί και καθιστούν δύσκολη την εφαρμογή των συστημάτων δημόσιων κλειδιών στα AdHoc δίκτυα.

- *Περιορισμένη ασφάλεια σε φυσικό επίπεδο:* Παρόλο που σήμερα χρησιμοποιούνται σε μεγάλο ποσοστό στα κινητά δίκτυα σχεδόν όλες οι μέθοδοι ασφαλείας που υπάρχουν, αυτά παραμένουν ευάλωτα σε φυσικές

απειλές, κάτι που δεν παρατηρείται τόσο πολύ στα κλασικά ενσύρματα δίκτυα.

- *Περιορισμένο εύρος ζώνης:* Εκτός από την περιορισμένη ηλεκτρική ενέργεια που διατίθεται σε ένα δίκτυο MANET περιορισμοί υπάρχουν και όσον αφορά το εύρος ζώνης του, κάτι που μαζί με την χαμηλή του χωρητικότητα δημιουργούν στις περισσότερες περιπτώσεις προβλήματα συμφόρησης στο δίκτυο[30].

- *Φθηνοί επεξεργαστές:* Οι περισσότερες κινητές συσκευές έχουν τους φτηνούς και αργούς επεξεργαστές επειδή οι γρήγοροι επεξεργαστές κοστίζουν πολύ περισσότερο. Ως εκ τούτου παίρνει πολύ χρόνο να εκτελεστούν μερικοί σύνθετοι υπολογισμοί.

- *Περιορισμένη ικανότητα αποθήκευσης και άλλων πόρων:* Λόγω των περιορισμών μεγέθους και δαπανών οι περισσότερες κινητές συσκευές είναι εξοπλισμένες με περιορισμένη ικανότητα αποθήκευσης.

- *Κλιμάκωση (Scalability).* Σε κάποια πιθανά δίκτυα MANET όπως στρατιωτικά δίκτυα ή δίκτυα σε αυτοκινητόδρομους ο αριθμός των κόμβων ενδέχεται να είναι σχετικά μεγάλος, μερικές δεκάδες ή ακόμα και εκατοντάδες κόμβοι ανά περιοχή δρομολόγησης (routing area), επομένως απαιτείται η υποστήριξη κλιμάκωσης σε αυτά τα δίκτυα. Μπορεί η ανάγκη για κλιμάκωση να μην είναι μοναδική για τα MANET αλλά οι μηχανισμοί για την επίτευξή της είναι [31].

1.4 Εφαρμογές των δικτύων MANET

Τα MANET έχουν πρακτική εφαρμογή σε περιπτώσεις όπου δεν υπάρχει κάποια σταθερή ενσύρματη δικτυακή υποδομή (fixed wired infrastructure). Τέτοιες περιπτώσεις έχουμε όταν δεν είναι οικονομικά, πρακτικά ή γεωγραφικά εφικτό να δημιουργηθεί η απαραίτητη υποδομή ή επειδή οι καταστάσεις δεν επιτρέπουν την εγκατάστασή της, όπως :

- Σε μια συνεδριακή αίθουσα κατά τη διάρκεια συναντήσεων, όταν οι συμμετέχοντες θέλουν να ανταλλάξουν πληροφορίες.
- Σε μια αίθουσα διδασκαλίας κατά τη διάρκεια συζητήσεων με τον καθηγητή ή και κατά τη διάρκεια της διδασκαλίας.
- Σε ένα αεροδρόμιο όπου οι εργαζόμενοι θέλουν να ανταλλάξουν αρχεία.
- Σε μια επείγουσα επιχείρηση διάσωσης, όταν τα μέλη του σωστικού συνεργείου θέλουν να συντονίσουν την προσπάθειά τους. Για παράδειγμα σε περίπτωση όταν κάποιος σεισμός ή πλημμύρα καταστρέψει την ενσύρματη υποδομή των σταθερών δικτύων.
- Σε μάχες κατά τη διάρκεια πολέμου, για τον συντονισμό των στρατιωτών στην άμυνα και την επίθεση.
- Σε δίκτυα που αναφέρονται στη διαμοιρασμένη πρόσβαση στο Internet σε αστικές τοποθεσίες υψηλής πυκνότητας (Neighborhood Area Networks).

Στην παρακάτω εικόνα φαίνονται κατηγοριοποιημένες οι εφαρμογές στα Manet.

Εφαρμογές	**Περιγραφή**
Τακτικά Δίκτυα	Στρατιωτικές επικοινωνίες στο πεδίο της μάχης.
Δίκτυα Αισθητήρων	Συγκέντρωση ενσωματωμένων συσκευών αισθητήρων που χρησιμοποιούνται για τη συλλογή δεδομένων σε πραγματικό χρόνο και την αυτοματοποίηση των καθημερινών λειτουργιών. Τα δεδομένα συνδέονται άμεσα στο χρόνο και στο χώρο, π.χ. απομακρυσμένοι αισθητήρες για τον καιρό, αισθητήρες για τον εξοπλισμό παραγωγής. Μπορεί να έχουν μεταξύ 1000-100000 κόμβους και κάθε κόμβος να συλλέγει στοιχεία του δείγματος, στη συνέχεια να διαβιβάζει τα δεδομένα στην κεντρική υποδοχή για επεξεργασία χρησιμοποιώντας μικρές ομοιογενείς τιμές.
Υπηρεσίες Έκτακτης Ανάγκης	Εφαρμογές έρευνας και διάσωσης καθώς και αποκατάσταση καταστροφών π.χ. έγκαιρη ανάκτηση και διαβίβαση των δεδομένων των ασθενών (εγγραφές, κατάσταση, διάγνωση) από και προς το νοσοκομείο, αντικατάσταση μιας σταθερής υποδομής σε περίπτωση σεισμών, τυφώνων, πυρκαγιών, κλπ.
Εμπόριο	Ηλεκτρονικό Εμπόριο π.χ. ηλεκτρονικές πληρωμές από οπουδήποτε (δηλαδή απο ένα ταξί), Δυναμικό Επιχειρηματικό Περιβάλλον - πρόσβαση σε αρχεία πελατών που είναι αποθηκευμένα σε μια κεντρική τοποθεσία για την παροχή μιας σταθερής βάσης δεδομένων για όλους σε ένα κινητό γραφείο, μετάδοση ειδήσεων - οδικών συνθηκών - καιρικών συνθηκών.
Σπίτι & Επιχείρηση	Ασύρματη δικτύωση σπιτιού γραφείου (WLAN) π.χ. χρήση PDA για την εκτύπωση σε οποιοδήποτε σημείο, Personal Area Network (PAN), Body Area Network (BAN).
Εκπαίδευση	Δημιουργία εικονικών τάξεων ή αιθουσών συνεδριών.
Διασκέδαση	Πολυχρηστικά παιχνίδια, ρομποτικά κατοικίδια ζώα, εξωτερική πρόσβαση στο Internet.

Εικόνα 2 Εφαρμογές των Manets

1.5 Παράγοντες μιας Επίθεσης

Οι ακόλουθοι είναι οι κύριοι παράγοντες που επηρεάζουν την απόδοση μιας επίθεσης[5]:

- *Υπολογιστική δύναμη* (Computational Power): Αυτό επηρεάζει σαφώς την ικανότητα ενός εισβολέα να υποβιβάσει την ασφάλεια ενός δικτύου. Η εν λόγω δύναμη δεν χρειάζεται για να εντοπιστεί το δίκτυο αλλά για να αναλύσει με μεγάλη ταχύτητα την υποκλέπτουσα (eavesdropped) κυκλοφορία.

- *Ανάπτυξη ικανοτήτων* (Deployment Capability): Ο αριθμός των επιτιθέμενων μπορεί να κυμαίνεται από ένα μόνο κόμβο έως πολλούς «έξυπνους» κόμβους οι οποίοι με συνακόλουθη μεταβολή των δυνατοτήτων τους μπορούν να πραγματοποιήσουν πολύ σοβαρές επιθέσεις.

- *Περιοχή ελέγχου* (Location Control): Η θέση των κόμβων μπορεί να έχει σαφείς επιπτώσεις σε ότι ο αντίπαλος μπορεί να πράξει. Ο αντίπαλος μπορεί να περιορίζεται σε κόμβους στο γεωγραφικό σύνορο ενός δικτύου ή μπορεί να έχει την ικανότητα εκ των υστέρων να δημιουργήσει μια ομάδα «έξυπνων» κακόβουλων κόμβων όπου αυθαίρετα ο βαθμός διεισδυτικότητας στο δίκτυο μπορεί να επιτευχθεί.

- *Κινητικότητα* (Mobility): Η κινητικότητα φέρνει γενικά αύξηση της ισχύος. Επίσης ένας κινητός κόμβος μπορεί οποιαδήποτε στιγμή να παραμείνει σε στάση. Από την άλλη πλευρά, η κινητικότητα μπορεί να εμποδίσει έναν εισβολέα από το να έχει ως στόχο ένα συγκεκριμένο θύμα. Για παράδειγμα, ένας κόμβος που κινείται ενδέχεται να μην λαμβάνει όλα τα παραποιημένα πακέτα δρομολόγησης που ξεκίνησαν από τον εισβολέα. Συμπερασματικά, ο αντίκτυπος της κινητικότητας για την ανίχνευση, την αποφυγή ή την καταπολέμηση μια επίθεσης είναι ένα σύνθετο θέμα.

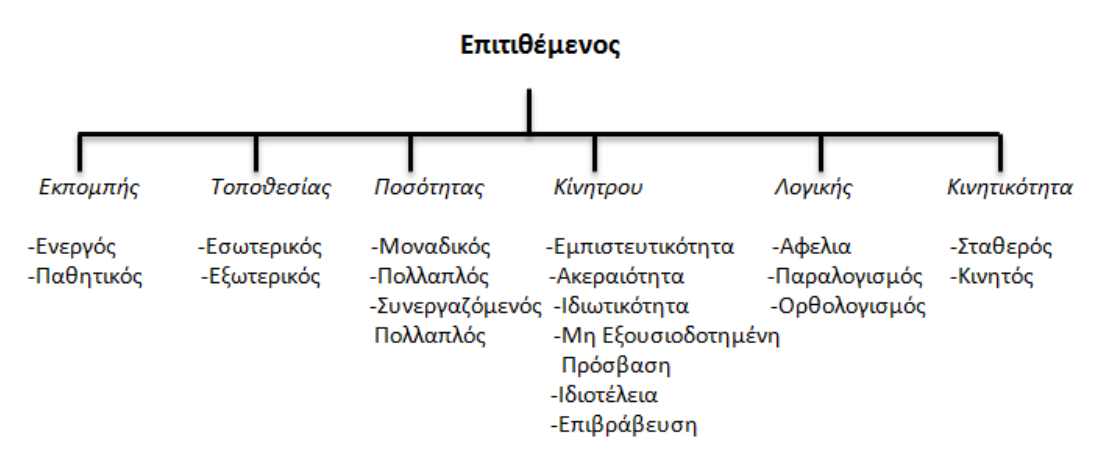
- *Ο βαθμός φυσικής πρόσβασης* (Degree of physical access) συμπεριλαμβανομένης της ικανότητας δέσμευσης των κόμβων και της δυνατότητας να προβαίνουν σε φυσική αποδόμηση [5].

1.6 Είδη επιθέσεων σε δίκτυα Manets.

Μια ποικιλία επιθέσεων είναι δυνατόν να συμβούν σε δίκτυα Manets. Ορισμένες επιθέσεις που ισχύουν για τα ενσύρματα δίκτυα ισχύουν και για ασύρματα δίκτυα και ορισμένες είναι ειδικά για τα MANETs. Αυτές οι επιθέσεις ασφάλειας μπορούν να ταξινομηθούν σύμφωνα με διαφορετικά κριτήρια όπως τον τομέα (domain) των επιτιθέμενων ή τις τεχνικές που χρησιμοποιούνται σε επιθέσεις. Αυτές οι επιθέσεις ασφάλειας στα Manet και σε όλα τα άλλα δίκτυα μπορεί σε γενικές γραμμές να

χαρακτηρίζονται από τα εξής κριτήρια: παθητική ή ενεργητική, εσωτερική ή εξωτερική, με βάση το διαφορετικό επίπεδο του προτύπου OSI στο οποίο συμβαίνουν δηλαδή με το πρωτόκολλο επικοινωνίας, με το αν ο επιτιθέμενος είναι ορατός ή κρυφός (stealthy or non-stealthy) και αν συναφείς με την κρυπτογραφία ή όχι.

Οι επιτιθέμενοι μπορούν επίσης να ταξινομηθούν ανάλογα με πολλά κριτήρια όπως της εκπομπής(emission), της τοποθεσίας (location), της ποσότητας (quantity), του κινήτρου (motivation), του ορθολογισμού (rationality) και της κινητικότητας (mobility) τα οποία φαίνονται στην παρακάτω εικόνα[4].



Εικόνα 3 Ταξινόμηση των επιτιθέμενων στα Manets

Μπορεί επίσης να υπάρχει ένας ή περισσότεροι εισβολείς . Όταν υπάρχουν πολλοί επιτιθέμενοι θα μπορούν να συνεργάζονται μεταξύ τους και έτσι η αντιμετώπιση τους είναι μια δύσκολη περίπτωση. Στο Hu et al. του 2005 δραστηριοποιούνται επιτιθέμενοι οι οποίοι συμβολίζονται ως *Active-nm*, όπου n είναι ο αριθμός των κόμβων που περιέχουν εμπιστευτικές πληροφορίες και m είναι ο συνολικός αριθμός των εμπιστευτικών πληροφοριών από τους εσωτερικούς και ξένους κόμβους. Προτείνουν, τότε μια ιεραρχία εισβολέα με την αύξηση της δύναμης ως εξής:

- Active-0-1: ο επιτιθέμενος διαθέτει μόνο ένα ξένο κόμβο.
- Active-0-x: ο εισβολέας είναι ιδιοκτήτης x ξένων κόμβων.
- Active-1-x: ο επιτιθέμενος κατέχει x κόμβους και μόνο ένας από αυτούς είναι εσωτερικός.
- Active-y-x: ο επιτιθέμενος διαθέτει x κόμβους και y από αυτούς είναι εσωτερικοί δηλαδή κατέχουν εμπιστευτικές πληροφορίες. [4]

Σημειώνουμε ότι σε αυτή την ιεραρχία όλοι οι κόμβοι αποτελούν ένα απλό εισβολέα. Ως εκ τούτου, υποτίθεται ότι συνεργάζονται μεταξύ τους.

Ένας αντίπαλος εκτελεί *επιθέσεις με κάποια κίνητρα (motivation),* όπως την διάσπαση της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και της ιδιωτικότητας (privacy). Αυτό μπορεί επίσης να γίνει για να αποκτήσει πρόσβαση σε

πόρους με "ευαίσθητες πληροφορίες". Ένας εισβολέας μπορεί επίσης να επιτεθεί για να εμποδίσει τις εργασίες μιας άλλης πλευράς[4].

Η μη χρησιμοποίηση, η δυσλειτουργία των κόμβων και οι αφελείς (naive) χρήστες μπορούν να γίνουν επίσης απειλές για ένα δίκτυο. Ωστόσο, η μη χρησιμοποίηση των κόμβων δεν είναι ο μόνος λόγος για «παράλογες» επιθέσεις. Ένας εισβολέας μπορεί να επιτεθεί μόνο και μόνο για να επιτεθεί και να «σπάσει» ένα σύστημα ασφαλείας αντιλαμβανόμενος σαν πρόκληση για τον εαυτό του[4].

Ακόμα οι *ορθολογικοι (rational) εισβολείς* πραγματοποιούν τις επιθέσεις τους για την απόκτηση των κόμβων κάτι που αξίζει περισσότερο από το κόστος της επίθεσης. Επίσης *οι επιτιθέμενοι μπορούν να είναι σταθεροί (fixed) ή κινητοί(mobile).* Η ανίχνευση κινητών επιτιθέμενων όπως και η υπεράσπιση εναντίον τους είναι γενικά πιο δύσκολη από ό, τι απέναντι σε ένα σταθερό αντίπαλο[4].

Ενεργές & Παθητικές Επιθέσεις: Οι επιθέσεις στα Manets μπορούν «χονδρικά» να ταξινομηθούν σε δύο μεγάλες κατηγορίες, δηλαδή στις παθητικές επιθέσεις και στις ενεργές επιθέσεις. Μια παθητική επίθεση λαμβάνει δεδομένα που ανταλλάσσονται στο δίκτυο χωρίς την διακοπή της λειτουργίας των επικοινωνιών τα οποία μπορούν αργότερα να χρησιμοποιηθούν σε μια ενεργή επίθεση ενώ η ενεργή επίθεση συνεπάγεται διακοπή ενημέρωσης, τροποποίηση ή κατασκευή της πληροφορίας που μεταδίδετε διαταράσσοντας έτσι τη φυσιολογική λειτουργία του δικτύου Manet. Παραδείγματα παθητικών επιθέσεων είναι οι υποκλοπές (eavesdropping), η ανάλυση της κίνησης των δεδομένων (traffic analysis) καθώς η και παρακολούθηση της κυκλοφορίας (monitoring). Παραδείγματα των ενεργών επιθέσεων αποτελούν οι παρεμβολές (jamming), η πλαστοπροσωπία (impersonating), η τροποποίηση (modification), η άρνηση παροχής υπηρεσιών (Denial of Service) και η επανάληψη του μηνύματος (message replay)[32].

Ενεργές Επιθέσεις

* *<u>Ανακριβής Προώθηση</u>*

- *Μη Προώθηση*
- *Αργή Προώθηση*
- *Επανειλημμένη Προώθηση*
- *Προώθηση των Μηνυμάτων στους Επιτιθέμενους για Ανάλυση*

* *<u>Άρνηση των Υπηρεσιών</u>*

- *Ψευδής Πληροφορίες Δρομολόγησης*
- *Νόθευση των Πληροφοριών Δρομολόγησης*
- *Υπερφόρτωση Δικτύου*
- *Έλλειψη μηνυμάτων λάθους, παρόλο που ένα λάθος έχει παρατηρηθεί*
- *Συγκέντρωση Πληροφοριών*

Παθητικές Επιθέσεις

* *<u>Συγκέντρωση Πληροφοριών (Υποκλοπή)</u>*

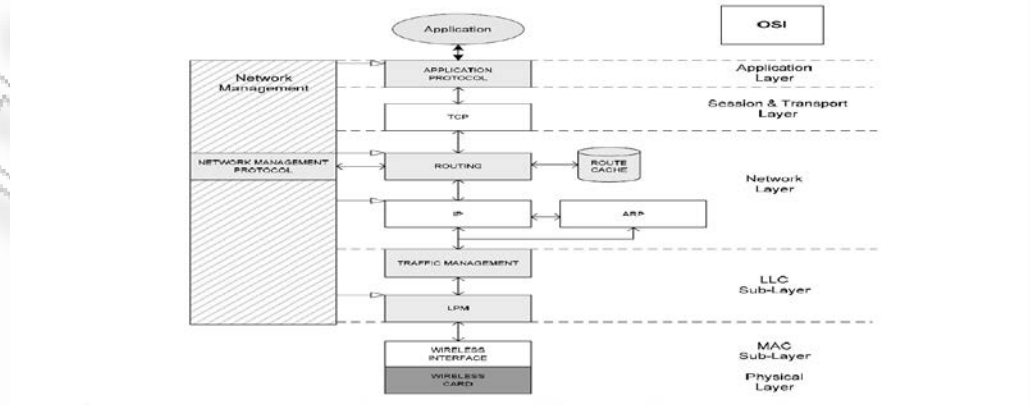
Εικόνα 4 Αναλυτική Ταξινόμηση Επιθέσεων (ενεργές-παθητικές) στα Manets

Εσωτερικές & Εξωτερικές Επιθέσεις: Οι επιθέσεις μπορούν επίσης να ταξινομηθούν στις εξωτερικές επιθέσεις και τις εσωτερικές επιθέσεις ανάλογα με τον

τομέα των επιθέσεων. Οι εξωτερικές επιθέσεις πραγματοποιούνται από τους κόμβους που δεν ανήκουν στην περιοχή του δικτύου και έχουν ως στόχο να προκαλέσουν συμφόρηση, να αναπαράγουν λανθασμένες πληροφορίες δρομολόγησης, να εμποδίσουν τις υπηρεσίες να λειτουργήσουν σωστά ή να τις απενεργοποιήσουν κτλ . Οι εσωτερικές επιθέσεις πραγματοποιούνται από κόμβους που στην πραγματικότητα είναι μέρος του δικτύου. Οι εσωτερικές επιθέσεις είναι πιο σοβαρές σε σύγκριση με τις εξωτερικές από την άποψη ότι οι εσωτερικοί – κακόβουλοι κόμβοι γνωρίζουν εμπιστευτικές και απόρρητες πληροφορίες και κατέχουν προνομιακά δικαιώματα πρόσβασης[32].

Πιο συγκεκριμένα ένας εισβολέας μπορεί να είναι εκ των έσω ή ξένος. Εκ των έσω είναι ένας κόμβος που έχει παραβιαστεί ή παραποιηθεί και αποτελεί μέρος του δικτύου. Ο επιτιθέμενος τότε γνωρίζει όλες τις κρυπτογραφικές πληροφορίες. Ως εκ τούτου, οι Αόρατες (Stealthy) Ενεργές Επιθέσεις μπορούν να οργανωθούν από επιτιθέμενους που κατέχουν εμπιστευτικές πληροφορίες. Εξωτερικές-Ξένες (Outside) επιθέσεις μπορεί να είναι είτε παθητικές ή ενεργές. Με άλλα λόγια ένας εσωτερικός επιτιθέμενος μπορεί να θεωρηθεί ως νομική οντότητα εντός του δικτύου, όπως ένας κόμβος που έχει καταχωρηθεί ή ένας κόμβος που επιτρέπεται να έχει πρόσβαση στο δίκτυο. Ξένος είναι συνήθως ένα κόμβος που δεν είναι ευπρόσδεκτος στο δίκτυο[4].

Επιθέσεις σε διάφορα επίπεδα του προτύπου OSI: Οι επιθέσεις είναι δυνατόν να ταξινομούνται περαιτέρω ανάλογα με το είδος τους και την τεχνικής τους σε πέντε (5) επίπεδα του προτύπου OSI. Το πρότυπο OSI σχεδιάστηκε από τον ISO (International Standard Organization) σύμφωνα με τον όποιο σχεδιάζονται όλα τα δίκτυα μιας και ο OSI είναι ο βασικός οργανισμός τυποποίησης με αναγνώριση σε πολλές χώρες. Η βασική ιδέα του προτύπου είναι ότι τα δεδομένα που διέρχονται από ένα δίκτυο περνάνε από τα επτά (7) διαφορετικά επίπεδα του προτύπου. Τα επίπεδα του προτύπου είναι ιεραρχικά τα εξής: το επίπεδο εφαρμογής, το επίπεδο παρουσίασης, το επίπεδο συνοδού, το επίπεδο μεταφοράς, το επίπεδο δικτύου, το επίπεδο ζεύξης δεδομένων και το φυσικό επίπεδο. Σε κάθε επίπεδο γίνονται ξεχωριστές εργασίες πάνω στα δεδομένα που τα προετοιμάζουν για το επόμενο κατά σειρά επίπεδο. Κάθε επίπεδο δέχεται τις υπηρεσίες του κατώτερου επιπέδου και προσφέρει με την σειρά του τις υπηρεσίες του στο ανώτερο επίπεδο. Η παρακάτω εικόνα παρουσιάζει μια ταξινόμηση των διαφόρων επιθέσεων ασφαλείας σε κάθε επίπεδο του προτύπου OSI[32]. Επίσης ορισμένες επιθέσεις μπορούν να δρομολογηθούν σε πολλά επίπεδα του προτύπου OSI. Για όλες αυτές τις επιθέσεις θα γίνει εκτενή ταξινόμηση και περιγραφή τους στα επίπεδα του OSI μιας και αυτό είναι το κύριο αντικείμενο της παρούσας εργασίας.



Εικόνα 5 Επικοινωνιακή διαστρωμάτωση των Manet δικτύων στο πρότυπο OSI

Επίπεδο	Επίθεση	Σκοπός
Εφαρμογής	Κακόβουλου Κώδικα	Μόλυνση των εφαρμογών & και των λειτουργικών συστημάτων
	DoS	Άρνηση παροχής υπηρεσιών
	Snooping	Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα ενός ατόμου
	Άρνησης Συμμόρφωσης	Άρνηση συμμετοχής σε όλη ή μέρος της επικοινωνίας
Μεταφοράς	Άρνησης Υπηρεσιών (DoS)	Άρνηση πρόσβασης σε νόμιμες υπηρεσίες
	Θύελλας ACK μηνυμάτων	Αποσυντονισμός της TCP διαδικασίας
	Session Hijacking (TCP)	Κλοπής ευαίσθητων πληροφοριών
Δικτύου	Επιθέσεις κατά τη φάση ανακάλυψης της διαδρομής (RREQ Attack).	Στοχεύουν στη ανακάλυψη ή στη φάση συντήρησης της δρομολόγησης μη ακολουθώντας τις προδιαγραφές των πρωτοκόλλων δρομολόγησης.
	Rushing	Γρήγορες επιθέσεις εναντίον των on-demand πρωτόκολλων δρομολόγησης
	Αποκάλυψης της Τοποθεσίας	Συγκέντρωση πληροφοριών τοπολογίας
	Καταβόθρας	Συγκέντρωση όλης της κίνησης μιας συγκεκριμένης περιοχής του δικτύου μέσω ενός εκτεθειμένου κόμβου
	Αναπαραγωγής Κόμβου	Προσθήκη ενός κόμβου στο υπάρχον δίκτυο αντιγράφοντας (αναπαράγοντας) το ID ενός υπάρχοντος κόμβου.
	Κατανάλωσης Πόρων	Ανούσια χρήση των Πόρων
	Μαύρης Τρύπας	Πτώση των μηνυμάτων
	Σκουληκότρυπας	Διατάραξη της Δρομολόγησης
Ζεύξης Δεδομένων	Αδυναμία του πεδίου NAV	Αλλοίωση στη συνεχιζόμενη μετάδοση του πλαισίου του επίπεδου ζεύξης δεδομένων μέσω ασύρματων παρεμβολών
	Διαταραχή στο MAC-DCF (Back Off)	Διατάραξη της MAC διαδικασίας
	Διαταραχή στο WEP	Διατάραξη του WEP πρωτοκόλλου
Φυσικό	Υποκλοπή	Απόκτηση ευαίσθητων πληροφοριών
	Φυσική Επίθεση	Φυσική προσέγγιση της κλοπής
	Παρεμβολή	Παρεμπόδιση της επικοινωνίας

Εικόνα 6 Επιθέσεις στα Manets στο πρότυπο OSI

Αόρατες (Stealthy) Επιθέσεις: Ορισμένες επιθέσεις ασφαλείας κάνουν χρήση της μυστικότητας σύμφωνα με την οποία οι επιτιθέμενοι προσπαθούν να κρύψουν τις ενέργειές τους είτε από έναν άνθρωπο ο οποίος κάνει παρακολούθηση του συστήματος είτε από ένα σύστημα ανίχνευσης εισβολής (Institution Detection System). Αλλά και άλλες επιθέσεις όπως DoS μπορούν να γίνουν με τον παραπάνω τρόπο[32].

Επιθέσεις που σχετίζονται με την Κρυπτογραφία ή την μη Κρυπτογραφία: Μερικές επιθέσεις σχετίζονται με την μη κρυπτογραφία και άλλες είναι κρυπτογραφικές επιθέσεις. Η παρακάτω εικόνα δείχνει κρυπτογραφικές επιθέσεις και παραδείγματα[32].

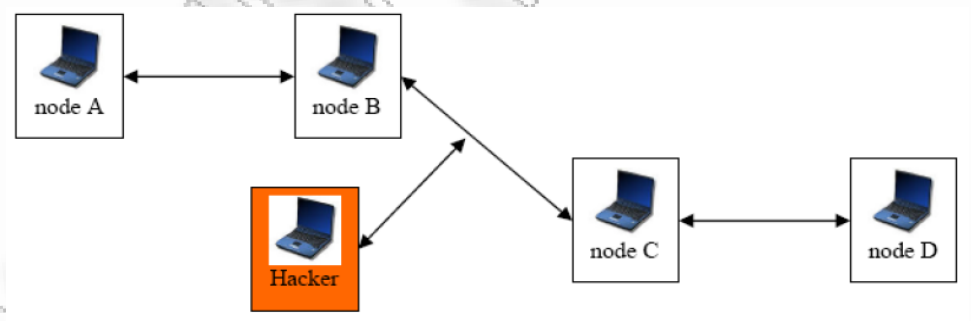
Κρυπτογραφικές Επιθέσεις	Παραδείγματα
Ψευδοτυχαίος αριθμός επιθέσεων	Nonce, Timestamp, Initialization Vector (IV)
Επίθεση Ψηφιακών Υπογραφών	Υπογραφές RSA,EIGamal,DSS
Επίθεση συγκρούσεων Hash	SHA-0,MD4,MD5,HAVAL-128,RIPEMD

Εικόνα 7 Επιθέσεις που σχετίζονται με την κρυπτογραφία

1.7 Πιθανές επιθέσεις στα Manet Πρωτόκολλα δρομολόγησης

Τα πρωτόκολλα δρομολόγησης στα Manet είναι αρκετά ανασφαλή επειδή οι εισβολείς μπορούν εύκολα να λαμβάνουν πληροφορίες σχετικά με την τοπολογία του δικτύου. Πράγματι στα πρωτόκολλα AODV και DSR τα πακέτα εντοπισμού της διαδρομής βρίσκονται σε απλό κείμενο. Έτσι ένας κακόβουλος κόμβος μπορεί να ανακαλύψει τη δομή του δικτύου μόνο με την ανάλυση αυτού του είδους των πακέτων και μπορεί να είναι σε θέση να καθορίσει τον ρόλο του κάθε κόμβου στο δίκτυο. Με όλες αυτές τις πληροφορίες μπορεί να πραγματοποιούνται σοβαρές επιθέσεις με σκοπό να διαταράξουν τη λειτουργία του δικτύου όπως με την απομόνωση σημαντικών κόμβων κλπ. Ας δούμε τις διάφορες δυνατές επιθέσεις με τη χρήση πρώτα της τροποποίησης (modification) στη συνέχεια με τη χρήση της πλαστοπροσωπίας (impersonation) και τέλος τις επιθέσεις οι οποίες χρησιμοποιούν πλαστογραφία (fabrication) [3].

1) Επιθέσεις χρησιμοποιώντας την τροποποίηση (modification): Ένας από τους πιο απλούς τρόπους για ένα κακόβουλο κόμβο να διαταράξει την καλή λειτουργία των Manet δικτύων είναι να εξαγγείλει καλύτερες διαδρομές τους άλλους κόμβους. Αυτό το είδος της επίθεσης βασίζεται στην τροποποίηση της αξίας της καταλληλότητας μιας διαδρομής ή στην αλλοίωση των πεδίων των μηνυμάτων ελέγχου (Denial of Service attacks)[3].

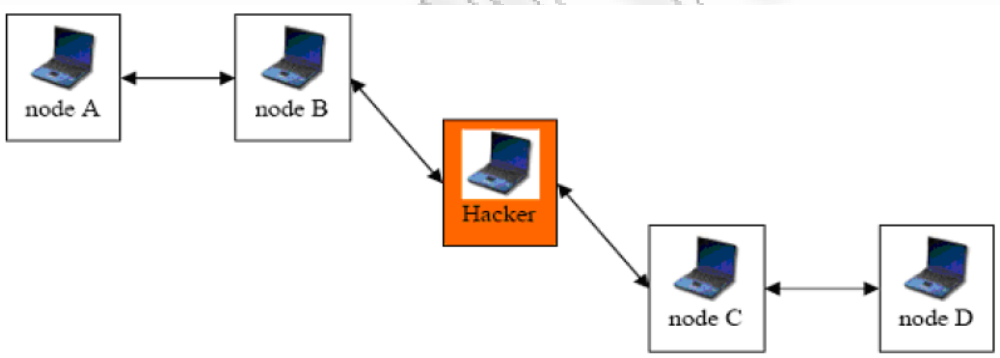


Εικόνα 8 Επιθέσεις χρησιμοποιώντας την τροποποίηση (modification)

Για παράδειγμα, στο δίκτυο που φαίνεται στην παραπάνω εικόνα ένας κακόβουλος κόμβος (node) «Hacker» θα μπορούσε να κρατήσει την κίνηση για την πρόσβαση στον κόμβο D μέσω της συνεχούς διαφήμισης στον κόμβο B για μια συντομότερη διαδρομή προς τον κόμβο D από την διαδρομή μέσω του κόμβου C.Οι τρόποι που μπορεί να γίνει αυτό είναι οι εξής:

- *α) Ανακατεύθυνση με την αλλαγή της ακολουθίας του αριθμού της διαδρομής.* Στα Manet δίκτυα όπως και στα ενσύρματα δίκτυα το καλύτερο μονοπάτι για την πρόσβαση σε έναν κόμβο προορισμού καθορίζεται από μια συγκεκριμένη τιμή. Όπως είναι εύκολα αντιληπτό όσο μικρότερη είναι αυτή η τιμή τόσο καλύτερη είναι η διαδρομή. Γι 'αυτό, ένας απλός τρόπος για να επιτεθεί ένας σε ένα δίκτυο είναι να αλλάξει αυτήν την τιμή με έναν μικρότερο αριθμό από το τελευταίο και έτσι θα έχει την "καλύτερη" τιμή.

  Στην παρακάνω εικόνα παρατηρούμε επίσης ότι όταν ο κόμβος A θέλει να επικοινωνήσει με τον κόμβο D μεταδίδει ένα μήνυμα ζητώντας από όλους τους κόμβους την καλύτερη διαδρομή για να φτάσει στον κόμβο D. Πιο συγκεκριμένα ο κόμβος B θα λάβει το μήνυμα και προς τα εμπρός. Ο κόμβος C θα απαντήσει ότι έχει μια άμεση διαδρομή προς τον κόμβο D και σε αυτό το μήνυμα απάντησης θα δώσει μια “τιμή” της διαδρομής. Τώρα, αν ο κακόβουλος κόμβος απαντήσει και αυτός στον κόμβο B ότι έχει άμεση διαδρομή προς τον κόμβο D με μικρότερο τιμή από ό, τι ο κόμβος C, ο κόμβος B θα εξετάσει αυτή τη διαδρομή ως την καλύτερη και θα διαγράψει τη διαδρομή με τον κόμβο C [3].

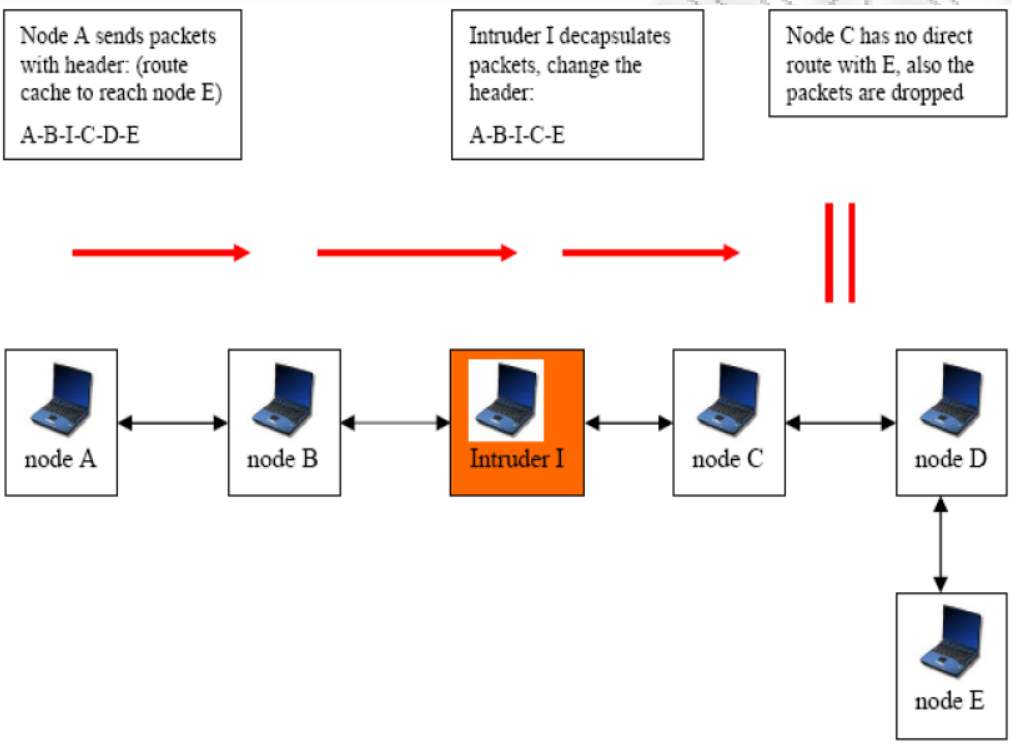


Εικόνα 9 Επίθεση ανακατεύθυνσης με την αλλαγή της ακολουθίας του αριθμού της διαδρομής

- *β) Επίθεση αναπροσανατολισμού με τροποποιημένα άλματα (ειδικά με το πρωτόκολλο AODV).* Όταν ένας κόμβος δεν μπορεί να αποφασίσει ποια είναι η καλύτερη διαδρομή μπορεί να χρησιμοποιήσει το μέσο αριθμό βημάτων για να αποφασίσει σε ποιο δρόμο βρίσκεται η καλύτερη διαδρομή για να φτάσει σε ένα συγκεκριμένο κόμβο. Αυτή είναι μια περίπτωση του πρωτόκολλου AODV. Στην περίπτωση αυτή, το πρωτόκολλο χρησιμοποιεί την “αξία” των αλμάτων για τον προσδιορισμό της βέλτιστης διαδρομής. Επίσης ένας κακόβουλος κόμβος μπορεί να διαταράξει το δίκτυο πάρα πολύ ανακοινώνοντας μια μικρότερη τιμή αλμάτων για την πρόσβαση ενός κόμβου. Σε γενικές γραμμές, οι κακόβουλοι κόμβοι χρησιμοποιούν την τιμή μηδέν για να είστε σίγουροι ότι έχουν τη μικρότερη τιμή αλμάτων[3].

- *γ)Denial of Service (DoS) επιθέσεις με τροποποιημένα δρομολόγια από την πηγή.* Η επίθεση DoS είναι γνωστή στην ασφάλεια των υπολογιστών και μπορεί να είναι αποτελεσματική σε AdHoc και κατ επέκταση σε Manet δίκτυα χωρίς ασφαλή πρωτόκολλα δρομολόγησης. Ένας απλός τρόπος για να κατανοήσει κανείς την λειτουργία των DoS επιθέσεων είναι να παρατηρήσει

την παρακάτω εικόνα. Στην εικόνα αυτή ένας κακόβουλος κόμβος βρίσκεται στο δίκτυο. Αν ο κόμβος Α θέλει να επικοινωνήσει με τον κόμβο Ε, στέλνει πακέτα δεδομένων σύμφωνα με τα δρομολόγια που υπάρχουν στην μνήμη cache του προς τον κόμβο Ε συμπεριλαμβανομένου και του κακόβουλου κόμβου. Επίσης, όταν ο κακόβουλος κόμβος θα λάβει τα πακέτα δεδομένων, μπορεί να αλλάξει την κεφαλίδα αυτών των πακέτων ώστε να ματαιωθεί η διαβίβαση των δεδομένων. Περισσότερα για το συγκριμένο τύπο επιθέσεων θα αναφέρουμε στο αντίστοιχο κεφάλαιο[3].



Εικόνα 10 Παράδειγμα DoS Επίθεσης

2)Επιθέσεις που χρησιμοποιούν πλαστοπροσωπία (impersonation). Οι επιθέσεις αυτές ονομάζονται "spoofing" δεδομένου ότι ο κακόβουλος κόμβος "κρύβει" την IP ή την MAC διεύθυνση του και χρησιμοποιεί μία άλλη. Στα σημερινά Manet πρωτόκολλα δρομολόγησης όπως το AODV και DSR δεν γίνεται έλεγχος ταυτότητας της διεύθυνση IP προέλευσης και έτσι ένας κακόβουλος κόμβος μπορεί να δρομολογήσει πολλές επιθέσεις με τη χρήση της πλαστοπροσωπίας. Για παράδειγμα, ένας κακόβουλος κόμβος μπορεί να δημιουργήσει βρόχους στο δίκτυο και να απομονώσει έναν κόμβο από το υπόλοιπο δίκτυο. Για να γίνει αυτό ο κακόβουλος κόμβος υιοθετεί μια διεύθυνση IP από άλλο κόμβο στο δίκτυο και την χρησιμοποιήσει για να ανακοινώσει μια νέα με μικρότερη τιμή διαδρομή στους άλλους κόμβους. Με αυτόν τον τρόπο μπορεί να τροποποιήσει εύκολα την τοπολογία του δικτύου[3].

3) Επιθέσεις πλαστογραφίας. Μπορούμε να διακρίνουμε τρία είδη επιθέσεων με τη χρήση της πλαστογραφίας .

- *α) Παραποίηση μηνυμάτων λάθους της διαδρομής*. Η πρώτη επίθεση είναι σύνηθες φαινόμενο στα πρωτόκολλα AODV και DSR επειδή αυτά τα δύο πρωτόκολλα χρησιμοποιούν τη συντήρηση των δρομολογίων για να

ανακτήσουν την καλή πορεία όταν πρέπει να κινηθούν σε κάποιες κόμβους. Η αδυναμία αυτής της αρχιτεκτονικής είναι ότι όταν κινείται ένας κόμβος, ο πλησιέστερος κόμβος του στέλνει μήνυμα λάθους στους άλλους για να τους ενημερώσει ότι η διαδρομή δεν είναι πλέον διαθέσιμη. Αν ένας κακόβουλος κόμβος υποκλέψει την ταυτότητα ενός άλλου κόμβου χρησιμοποιώντας πλαστογράφηση θα αποστείλει μηνύματα λάθους στους άλλους κόμβους και έτσι οι άλλοι κόμβοι θα ενημερώσουν τους πίνακες δρομολόγησης τους με αυτές τις πληροφορίες. Επίσης, ο κακόβουλος κόμβος μπορεί να απομονώσει κάθε κόμβο αρκετά εύκολα.

- *β) Επιθέσεις μόλυνσης-δηλητηρίασης της κρυφής (cache) μνήμης.* Αυτή είναι μια παθητική επίθεση που μπορεί να προκύψει στο DSR πρωτόκολλο κυρίως λόγω της ετερόκλητης λειτουργία του πίνακα δρομολόγησης του εν λόγο πρωτοκόλλου. Αυτό συμβαίνει όταν οι πληροφορίες που είναι αποθηκευμένες στον πίνακα δρομολόγησης σε δρομολογητές διαγράφονται ή αλλοιώνονται με ψευδή στοιχεία. Πράγματι, εκτός από την εκμάθηση δρομολόγιων από τις επικεφαλίδες των πακέτων τις οποίες ένας κόμβος επεξεργάζεται κατά μήκος μιας διαδρομής, στο πρωτόκολλο DSR οι διαδρομές μπορούν επίσης να γνωστοποιηθούν από ετερόκλητα πακέτα που λήφθηκαν από τους κόμβους. Ένας κόμβος ακούει κάθε πακέτο και μπορεί να προσθέσει πληροφορίες δρομολόγησης που περιέχονται στο πακέτο της επικεφαλίδας από την κρυφή μνήμη του, έστω και αν ο κόμβος δεν βρίσκεται στο μονοπάτι από την πηγή προς τον προορισμό.

  Η ευπάθεια του συστήματος αυτού είναι ότι ένας εισβολέας θα μπορούσε να εκμεταλλευτεί εύκολα αυτή τη μέθοδο εκμάθησης των διαδρομών και να τις αλλοιώσει. Για παράδειγμα ο κακόβουλος κόμβος έχει μόλις μεταδώσει ένα μήνυμα με πλαστή διεύθυνση IP στους άλλους κόμβους. Όταν οι κόμβοι λάβουν αυτό το μήνυμα θα προσθέσουν τη νέα διαδρομή στην κρυφή μνήμη τους και επίσης θα επικοινωνήσουν τώρα με αυτή τη διαδρομή για να καταλήξουν στον κακόβουλο κόμβο στην πραγματικότητα και όχι με τον κόμβο που είχε την ορθή διεύθυνση IP[3] .

Άλλες επιθέσεις με τη χρήση της πλαστογραφίας (fabrication) είναι οι ακόλουθες:

- *Επίθεση Επαναλήψης (Replay Attack):* ένας εισβολέας στέλνει παλιές διαφημίσεις σε έναν κόμβο με αποτέλεσμα να ενημερώσει τον πίνακα δρομολόγησης με ψευδής πλέον πληροφορίες.

- *Επίθεση Μαύρης Τρύπας (Black Hole):* ένας εισβολέας διαφημίζει μια διαδρομή προς όλους τους προορισμούς ώστε να προκαλέσει όλους τους κόμβους να δρομολογήσουν όλα τα πακέτα τους προς αυτή την κατεύθυνση[3].

4)Επιθέσεις δρομολόγησης υπερχείλισης πίνακα. Αν ένα ad-hoc δίκτυο χρησιμοποιεί ένα προληπτικό (proactive) πρωτόκολλο, αυτό σημαίνει όπως έχουμε προηγούμενα πει ότι ο αλγόριθμος του πρωτοκόλλου θα προσπαθήσει να αναζητήσει πληροφορίες δρομολόγησης ακόμη και όταν αυτό δεν είναι απαραίτητο. Πρόκειται για μια ευπάθεια που χρησιμοποιείται από αυτήν την επίθεση διότι ο εισβολέας

προσπαθεί να δημιουργήσει διαδρομή η οποία δεν υφίστανται. Αν δημιουργηθούν τώρα αρκετά δρομολόγια, αυτά δεν θα μπορούν να εκτελεστούν λόγου της ανικανότητας διαχείρισης του πρωτοκόλλου εξαιτίας της υπερχείλισης του πίνακα δρομολόγησης τους (cache memory)[3].

Στο παρόν κεφάλαιο έγινε μια απλή γενική αναφορά των επιθέσεων τις οποίες θα δούμε αναλυτικά στα επόμενα κεφάλαια.

Κεφάλαιο 2

Επιθέσεις στο Φυσικό Επίπεδο

2.1 Εισαγωγή

Όσον αφορά τις επιθέσεις στα Manets στο φυσικό επίπεδο του προτύπου OSI είναι αυξημένες εξαιτίας της ασύρματης ιδιότητας των παραπάνω δικτύων τα οποία έχουν σαν μέσο μετάδοσης τον αέρα. Ένα κοινό ραδιοφωνικό σήμα είναι πολύ εύκολο να παρεμποδιστεί και να διακοπεί. Έτσι ο εισβολέας ή αλλιώς κακόβουλος κόμβος μπορεί να «κρυφακούσει» ή να διακόψει την υπηρεσία των ασύρματων δικτύων όπως είναι τα Manets.

Οι πιο διαδεδομένες επιθέσεις που συμβαίνουν σε αυτό το επίπεδο είναι οι :

- Υποκλοπές (Eavesdropping)
- Παρεμβολές (Interference-Jamming)
- Φυσικές Επιθέσεις

2.2 Υποκλοπή

Υποκλοπή (Eavesdropping) είναι η παρακολούθηση και η ανάγνωση μηνυμάτων και συνομιλιών από μη εξουσιοδοτημένους κόμβους. Κάθε κινητός κόμβος στα κινητά adhoc δίκτυα μοιράζονται ένα ασύρματο μέσο. Η πλειοψηφία των ασύρματων επικοινωνιών χρησιμοποιούν το ραδιοφάσμα RF το οποίο μεταδίδεται από τη φύση. Σήματα που εκπέμπουν σε ραδιοκύματα μπορούν εύκολα να υποκλαπούν με δέκτες συντονισμένους στη σωστή συχνότητα. Έτσι τα μηνύματα που διαβιβάζονται μπορούν να υποκλαπούν καθώς και πλαστά μηνύματα μπορούν να διοχετευθούν στο δίκτυο [3].

Οι επιθέσεις αυτές της υποκλοπής στοχεύουν :

- να ακούσουν και να λάβουν μηνύματα δρομολόγησης (συμπεριλαμβανομένου της ενημέρωσης)

- να συγκεντρώσουν δεδομένα ώστε να συμπεράνουν την τοπολογία του δικτύου όπως και πληροφορίες για την ταυτότητα των περισσότερων χρησιμοποιουμένων κόμβων.

- να ανακαλύψουν ότι ένα δίκτυο υπάρχει σε μια γεωγραφική θέση ανιχνεύοντας το σήμα του απειλώντας έτσι την ιδιωτικότητα του δικτύου αλλά και των κόμβων του.

Στην πραγματικότητα τα AdHoc δίκτυα είναι λίγο πιο ασφαλή από τις υποκλοπές σε σύγκριση με άλλες πιο μακροχρόνιες σειρές ασύρματων τεχνολογιών επειδή τα

σήματα αποστέλλονται σε μικρές αποστάσεις. Ο αντίπαλος πρέπει να πάει αρκετά κοντά στον κόμβο που επιτέθηκε ώστε να είναι σε θέση να αξιοποιήσει την επίθεση[4].

2.3 Παρεμβολή

Τα ράδιοσήματα μπορούν να «μπλοκαριστούν» ή να δεχθούν παρεμβολές και έτσι προκαλείται απώλεια και ολική ή μερική καταστροφή των μηνυμάτων. Εάν ο εισβολέας (κακόβουλος κόμβος) έχει ένα ισχυρό πομπό μπορεί να δημιουργήσει ένα σήμα με αρκετή ισχύ ώστε να παρεμποδίσει τα σήματα του ad hoc δικτύου και να διακόψει την επικοινωνία. Οι συνηθέστεροι τύποι παρεμβολών αυτής της μορφής του σήματος είναι ένας τυχαίος θόρυβος και ένας παλμός. Ο εξοπλισμός για αυτού τους είδους τις παρεμβολές είναι εύκολα διαθέσιμος[3].

Όλες οι επιθέσεις του φυσικού επιπέδου μπορούν επίσης να εκγλυφθούν και ως DoS επιθέσεις διότι εμποδίζουν ένα δίκτυο από την εκτέλεση των αναμενόμενων λειτουργιών του. Σε αυτό το τμήμα, το φυσικό επίπεδο δηλώνει στο πρότυπο OSI ότι είναι υπεύθυνο για την εκπροσώπηση των bits 1 και 0 στο ασύρματο μέσο και μια επίθεση DoS στο φυσικό επίπεδο η οποία ονομάζεται παρεμβολή (Interference-Jamming) σημαίνει απειλή για την ασφάλεια κατά αυτής της εκπροσώπησης[4].

Ένας κακόβουλος κόμβος μπορεί να παρεμβάλει (jam) ένα ασύρματο μεταφορέα (wireless carrier) με τη διαβίβαση ένα σήματος σε αυτή τη συχνότητα. Το σήμα παρεμβολής συμβάλλει στην δημιουργία θορύβου και η δύναμή του είναι αρκετή για να μειώσει το λόγο σήματος προς θόρυβο (SNR) κάτω από το επίπεδο το οποίο χρησιμοποιούν οι κόμβοι για να λαμβάνουν σωστά τα στοιχεία πάνω στο κανάλι. Οι επιθέσεις των παρεμβολών (jamming) μπορούν να διεξάγονται *συνεχώς* σε μια περιοχή η οποία αποτρέπει όλους τους κόμβους της περιοχής από την «ορθή» επικοινωνία. Εναλλακτικά, παρεμβολές μπορούν να γίνουν προσωρινά σε τυχαία χρονικά διαστήματα τα οποία μπορεί να εξακολουθούν να είναι πολύ αποτελεσματικά και να παρεμποδίζουν τις μεταδόσεις[4].

Πιο συγκριμένα ο θόρυβος συνήθως προκαλείται από ανεπιθύμητα σήματα παρεμβολής του μεταφορέα (carrier). Υπάρχουν διάφορες μορφές θορύβου:

- *Λευκός Θόρυβος (White Noise):* ονομάζεται συχνά και θερμικός θόρυβος διότι είναι η συνάρτηση της θερμοκρασίας λόγω της θερμικής διέγερσης των ηλεκτρονίων. Δεν μπορεί να εξαλειφθεί. Ο θερμικός θόρυβος είναι ανεξάρτητος από τη συχνότητα και ως εκ τούτου καλείται και λευκός θόρυβος.

- *Θόρυβος Ενδοδιαμόρφωσης (Intermodulation noise*:): τα σήματα σε δύο διαφορετικές συχνότητες F_1 και F_2 μπορούν να παραγάγουν ένα σήμα σε μια συχνότητα που είναι το άθροισμα δηλαδή $F_1 + F_2$, η διαφορά δηλαδή $F_1 – F_2$ ή πολλαπλάσια δηλαδή $F_k \times n$, των αρχικών συχνοτήτων.

- *Θόρυβος Διαφωνίας (Crosstalk):* Όταν υπάρχει χρόνος επικάλυψης άνω των δύο ασύρματών μεταδόσεων οι οποίες παραλαμβάνονται από την ίδια κεραία τότε αυτές αλληλεπιδρούν μεταξύ τους. Αυτό είναι συνώνυμο με το

φαινόμενο έμπειρης στιχομυθίας (crosstalk phenomenon experienced) όταν οι δύο τηλεφωνικές γραμμές είναι ακουσίως συνδεμένες και επικοινωνούν μεταξύ τους.

- *Παλμικός (Impulse) θόρυβος:* Ακανόνιστες, απρόβλεπτες και πολύ μικρές αιχμές του θορύβου μπορεί να παρατηρηθούν σε ασύρματα κανάλια. Αυτές οφείλονται σε διάφορους παράγοντες και είναι ιδιαίτερα αποτελεσματικές στις ψηφιακές επικοινωνίες[4].

2.4 Φυσικές Επιθέσεις

Τα δίκτυα Manet συχνά λειτουργούν σε εχθρικά περιβάλλοντα. Σε τέτοια περιβάλλοντα το μικρό μέγεθος των κόμβων μαζί με την έλλειψη επιτήρησης και την κατανεμημένη ανάπτυξη του δικτύου τα κάνουν ευάλωτα σε φυσικές επιθέσεις. Ως φυσικές επιθέσεις θεωρούνται απειλές που επιφέρουν την φυσική καταστροφή των κόμβων. Σε αντίθεση με τις επιθέσεις που αναφέρθηκαν παραπάνω, οι φυσικές επιθέσεις καταστρέφουν τον κόμβο μόνιμα και οι απώλειες είναι μη αναστρέψιμες. Για παράδειγμα, οι επιτιθέμενοι μπορούν να εξάγουν κρυπτογραφικά μυστικά, να αλλάξουν τη διάταξη των κυκλωμάτων των κόμβων, να τροποποιήσουν τον προγραμματισμό των κόμβων ή να αντικαταστήσουν κόμβους με άλλους κακόβουλους υπό την επίβλεψη του επιτιθέμενου[31].

Συγκεκριμένα όταν οι κόμβοι είναι "αφύλακτοι" και ο αντίπαλος μπορεί να φτάσει φυσικά σε αυτούς μπορούν να δεχθούν επίθεση με τεχνικές αλλοίωσης (tampering techniques), όπως επιθέσεις microprobing, επιθέσεις κοπής με λέιζερ (lazer cutting), επιθέσεις επικεντρωμένες στην χειραγώγησης των ιόντων πορείας (ion-beam manipulation),επιθέσεις glitch και επιθέσεις ανάλυσης δύναμης (power analysis). Έτσι ο κόμβος παραποίησης (node tampering) μπορεί να βοηθήσει στη μεταμφίεση (masquerading). Ως εκ τούτου, η ανθεκτικότητα κατά της αλλοίωσης (tampering) είναι ένα θέμα που πρέπει να εξεταστεί προσεκτικά[4] .

Μπορούμε να ομαδοποιήσουμε τα συστήματα αλλοίωσης των κόμβων σε δύο κατηγορίες: στην επεμβατική αλλοίωση (invasive tampering) και στην μη επεμβατική αλλοίωση (non invasive tampering).Οι επεμβατικές τεχνικές στοχεύουν να αποκτήσουν απεριόριστη πρόσβαση σε έναν κόμβο. Στις μη επεμβατικές επιθέσεις η απεριόριστη πρόσβαση στον κόμβο δεν είναι αυτό που επιζητάτε . Αντί αυτού, από την ανάλυση της συμπεριφοράς ενός κόμβου προκύπτουν η κατανάλωση ενέργειας (power consumption), οι χρόνοι εκτέλεσης των αλγορίθμων για διάφορες εισόδους, τα απόρρητα στοιχεία σχετικά με τις διαδικασίες και τα κλειδιά που χρησιμοποιούνται από τα συστήματα κρυπτογράφησης[4].

Οι ηλεκτρομαγνητικοί παλμοί (EMP) είναι επίσης μεταξύ των απειλών που μπορούν να παρατίθενται σε φυσικές επιθέσεις ασφαλείας. Οι EMP είναι μια έκρηξη μικρής διάρκειας και υψηλής έντασης ηλεκτρομαγνητική ενέργεια που μπορεί να παράγει κύματα τάσης η οποία μπορεί να βλάψει τις ηλεκτρονικές συσκευές εντός εμβέλειας. Ο EMP είναι ένα φυσικό αποτέλεσμα των πυρηνικών εκρήξεων. Σήμερα, οι φορητές συσκευές που μπορούν να δημιουργήσουν EMP είναι ευρέως διαθέσιμες. Αν και υπάρχουν ακόμα πολλά άλυτα ζητήματα που σχετίζονται με την πρακτική εφαρμογή

των EMP τεχνολογιών, οι EMP είναι μια απειλή για όλα τα είδη των ηλεκτρικών συσκευών στο τακτικό πεδίο. Είναι όμως δυνατόν να κατασκευαστούν ηλεκτρονικές συσκευές που είναι περισσότερο ανθεκτικές στις EMP. Ως εκ τούτου, παραθέτουμε τις EMP επιθέσεις ως ένα είδος φυσικών επιθέσεων ασφάλειας[4].

Κεφάλαιο 3

Επιθέσεις στο Επίπεδο Ζεύξης Δεδομένων.

3.1 Εισαγωγή

Τα MANET όπως προηγούμενα έχουμε αναφέρει βασίζονται στην ανοικτή «peer to peer» αρχιτεκτονική πολλαπλών βημάτων (multihops) ώστε να γίνει η επικοινωνία σε επίπεδο δικτύου. Συγκεκριμένα, το ένα βήμα (hop) μεταξύ των γειτόνων συντηρείται από τα πρωτόκολλα επιπέδου ζεύξης δεδομένων και η δυνατότητα σύνδεσης με άλλους κόμβους στο δίκτυο μπορεί να επεκταθεί με τα πρωτόκολλα του επίπεδου δικτύου. Έτσι οι επιθέσεις μπορούν να πραγματοποιηθούν στο επίπεδο ζεύξης δεδομένων διακόπτοντας τη συνεργασία των πρωτοκόλλων του συγκεκριμένου επιπέδου[32].

Τα ασύρματου ελέγχου πρόσβασης στο μέσο (MAC) πρωτόκολλα είναι υπεύθυνα για το συντονισμό της μετάδοσης των κόμβων στο κοινό μέσο μετάδοσης. Επειδή το MAC πρωτόκολλο δεν είναι κατάλληλο για τον έλεγχο πρόσβασης ενός ραδιοσήματος το πρωτόκολλο 802.11 είναι ειδικά αφιερωμένο για αυτή την δουλεία στα ασύρματα τοπικά δίκτυα. Το πρωτόκολλο 802.11 MAC χρησιμοποιεί ειδικούς μηχανισμούς επίλυσης της διανομής του ασύρματου καναλιού. Η ομάδα εργασίας του *IEEE 802.11* πρότεινε δύο αλγόριθμους για την επίλυση της διανομής του καναλιού. Το ένα είναι ένα πλήρως κατανεμημένο πρωτόκολλο πρόσβασης και καλείται **Distributed Coordination Function (DCF).** Το άλλο είναι ένα κεντρικό πρωτόκολλο πρόσβασης που ονομάζεται **Point Coordination Function (PCF)**. Το PCF απαιτεί έναν σταθμό βάσης για την κεντρική λήψη των αποφάσεων. Το DCF χρησιμοποιεί το πρωτόκολλο αποφυγής συγκρούσεων (CSMA / CA) για την επίλυση του διαμοιρασμού του καναλιού μεταξύ των κόμβων που φιλοξενεί[32].

Πρακτικά ορίζονται τρεις τιμές για τα χρονικά διαστήματα (interframe space, **IFS**) τα οποία καθορίζουν την παροχή προτεραιότητας για την πρόσβαση στο κανάλι.

- Το **SIFS** που είναι το συντομότερο διάστημα και χρησιμοποιείται για μηνύματα ACK, CTS και τα πλαίσια ανταπόκρισης της δημοσκόπησης (poll response frames). Το SIFS μπορεί να χρησιμοποιηθεί όταν οι σταθμοί έχουν καταλάβει το μέσο και χρειάζονται να το κρατήσουν τόσο ώστε να εκτελεστεί η διαδικασία ανταλλαγής πακέτων. Χρησιμοποιώντας το μικρότερο κενό μεταξύ των μεταδόσεων κατά τη διάρκεια της διαδικασίας ανταλλαγής πακέτων, αποτρέπει τους άλλους σταθμούς που είναι υποχρεωμένοι να περιμένουν να γίνει αδρανές το μέσο για μεγαλύτερο διάστημα, από το να προσπαθήσουν να χρησιμοποιήσουν το μέσο, δίνοντας συνεπώς προτεραιότητα στην ολοκλήρωση της διαδικασίας ανταλλαγής πακέτων που είναι σε εξέλιξη.

- Το **DIFS** είναι το μακρύτερο IFS διάστημα και χρησιμοποιείται ως την ελάχιστη δυνατή και ασύγχρονη καθυστέρηση που υποστηρίζουν τα πλαίσια για την πρόσβαση. Γενικά ένας σταθμός που χρησιμοποιεί DCF θα μπορεί να

μεταδίδει αν ο μηχανισμός του ανίχνευσης φέροντος καθορίσει ότι το μέσο είναι αδρανές για διάστημα ακέραιο πολλαπλάσιο ενός DIFS μετά τη σωστή λήψη πακέτου και αν ο χρόνος οπισθοχώρησης έχει λήξει.

- Το **PIFS** είναι η μεσαία IFS και χρησιμοποιείται για την έκδοση δημοσκοπήσεων από τον κεντρικό ελεγκτή στο σύστημα PCF. Έτσι τα PIFS χρησιμοποιούνται μόνο από σταθμούς που λειτουργούν υπό την PCF για να κερδίσουν προτεραιότητα στην πρόσβαση στο μέσο με την έναρξη της περιόδου χωρίς ανταγωνισμό

Σε περίπτωση που υπάρξει μια σύγκρουση, αν το μέσο είναι ελεύθερο τότε ο σταθμός μεταδίδει το πλαίσιο που θέλει. Αν το μέσο είναι δεσμευμένο ο σταθμός περιμένει μέχρι το μέσο να μείνει ελεύθερο για κάποιο IFS. Τότε ξεκινάει τη διαδικασία της δυαδικής εκθετικής υποχώρησης (binary exponential backoff) για να καθορίσει πόσο θα είναι το επιπλέον χρονικό διάστημα αναμονής. Αυτό γίνεται επιλέγοντας τυχαία μια σχισμή του παραθύρου ανταγωνισμού (contention window). Αφού περάσει και αυτό το τελευταίο χρονικό διάστημα, ο σταθμός μεταδίδει το πλαίσιο που θέλει.

Το **CSMA/CA** είναι ένα κατανεμημένο (distributed) σύστημα πρόσβασης, δηλαδή δεν υπάρχει ένα συγκεκριμένο τερματικό που να ελέγχει την πρόσβαση στο κοινό ασύρματο μέσο κάτι το οποίο είναι απαραίτητο στα δίκτυα Manet

Η πολλαπλή πρόσβαση με ανίχνευση φέροντος και με αποφυγή συγκρούσεων είναι έτσι σχεδιασμένη ώστε να μειώνεται η πιθανότητα σύγκρουσης ανάμεσα σε δύο τερματικά κατά την προσπάθειά τους να καταλάβουν το κοινό μέσο. Αυτό ακριβώς είναι και το σημείο στο οποίο συμβαίνουν οι περισσότερες συγκρούσεις αφού αμέσως μετά την ολοκλήρωση της τελευταίας εκπομπής και την ελευθέρωση του μέσου όλοι οι σταθμοί επιχειρούν ταυτόχρονα την κατάληψή του. Η εισαγωγή λοιπόν, του επιπλέον τυχαίου χρόνου αναβολής (backoff time) αναγκάζει τα τερματικά να επιχειρήσουν σε τυχαίους και διαφορετικούς χρόνους την κατάληψη του μέσου. Επίσης, όταν το μέσο καταληφθεί από το πρώτο τερματικό, προλαβαίνει να γίνει αντιληπτό το γεγονός αυτό και από τα υπόλοιπα τερματικά τα οποία και σταματούν την δική τους προσπάθεια κατάληψης του μέσου. Τέλος, η διαδικασία backoff εισάγει και έναν πιο δίκαιο τρόπο κατάληψης του μέσου

Μετά από μία σύγκρουση και αφού έχει ολοκληρωθεί η μετάδοση του σήματος θορύβου, το τερματικό επιχειρεί την επανεκπομπή του πλαισίου του μετά από ένα συγκεκριμένο τυχαίο χρονικό διάστημα που καθορίζεται από την διαδικασία δυαδικής εκθετικής υποχώρησης. Η διαδικασία εύρεσης αυτού του χρονικού διαστήματος, που είναι πάντα ένα ακέραιο πολλαπλάσιο της χρονοθυρίδας (time slot) είναι η εξής: Για την ν-ιοστή επανεκπομπή, επιλέγεται ένας τυχαίος ακέραιος r από μία ομοιόμορφη κατανομή στο διάστημα $[0, 2^k)$, όπου το k είναι ο ελάχιστος αριθμός ανάμεσα στο ν και στο 10

Ας δούμε αναλυτικά την **διαδικασία κατάληψης του μέσου από ένα τερματικό.** Ένα τερματικό που θέλει να μεταδώσει ένα πλαίσιο «ακούει» το κανάλι και προσδιορίζει αν αυτό είναι απασχολημένο ή ελεύθερο. Αυτή η διαδικασία ονομάζεται

φυσική ανίχνευση φέροντος (Physical Carrier-Sense). Αν το κανάλι είναι απασχολημένο, το τερματικό περιμένει μέχρι αυτό να ελευθερωθεί. Όταν το κανάλι ελευθερωθεί, το τερματικό περιμένει αρχικά για χρόνο DIFS ενώ συνεχίζει να «ακούει» το κανάλι. Αφού παρέλθει αυτός ο χρόνος και το κανάλι συνεχίζει να είναι ελεύθερο, το τερματικό περιμένει για έναν επιπλέον τυχαίο αριθμό χρονοθυρίδων ο οποίος καθορίζεται από την διαδικασία backoff. Το τερματικό συνεχίζει να «ακούει» το κανάλι κατά την διάρκεια κάθε χρονοθυρίδας. Αν το κανάλι στην διάρκεια μιας χρονοθυρίδας είναι ελεύθερο ο επιπλέον χρόνος αναβολής μειώνεται κατά μία χρονοθυρίδα. Έτσι, όταν περάσει όλος ο χρόνος αναβολής και το κανάλι συνεχίζει να είναι ελεύθερο, το τερματικό αρχίζει την εκπομπή του πλαισίου του. Αν όμως το κανάλι «ακουστεί» απασχολημένο κατά την διάρκεια μιας χρονοθυρίδας, δηλαδή κάποιο άλλο τερματικό έχει προλάβει και έχει καταλάβει το μέσο, σταματά η διαδικασία κατάληψης του μέσου από τα υπόλοιπα τερματικά και δεν μειώνεται ο αριθμός χρονοθυρίδων του χρόνου αναβολής για αυτή την χρονοθυρίδα. Έτσι, όταν το κανάλι ελευθερωθεί ξανά για χρόνο μεγαλύτερο από DIFS, ο χρόνος αναβολής κάθε τερματικού θα συνεχίσει να μειώνεται από την τιμή στην οποία είχε προηγουμένως διακοπεί.

Στο επίπεδο ζεύξης δεδομένων στο στρώμα MAC οι επιθέσεις μπορεί να επιχειρούνται με τους εξής τρόπους :

- Εφόσον θεωρούμε δεδομένο ότι υπάρχει ένα μόνο κανάλι που επαναχρησιμοποιείται, κρατώντας το κανάλι απασχολημένο πλησίον του κόμβου οδηγεί σε μια επίθεση άρνησης παροχής υπηρεσιών (DoS) σε αυτό το κόμβο.

- Χρησιμοποιώντας ένα συγκεκριμένο κόμβο ο οποίος αναμεταδίδει συνεχώς ψευδή στοιχεία η διάρκεια ζωής της μπαταρίας του κόμβου ενδέχεται να εξαντληθεί.

Ο «end-to-end» έλεγχος της ταυτότητας μπορεί να αποτρέψει τις επιθέσεις αυτές από το να ξεκινήσουν. Αν ο κόμβος δεν περιλαμβάνει πιστοποιητικό γνησιότητας μπορεί να αποκλείεται από την πρόσβαση στο κανάλι. Ωστόσο, εάν οι κόμβοι συνωμοτούν και ο ένας από τους κόμβους είναι ο κόμβος της αποστολής και ο άλλος του προορισμού τότε οι επιθέσεις σε αυτό το στρώμα είναι πολύ εφικτές.

Οι πρόσφατες ερευνητικές προσπάθειες έχουν επισημάνει τα τρωτά σημεία των πρωτοκόλλων του επιπέδου ζεύξης δεδομένων και ιδιαίτερα για το απαραίτητο πρότυπο IEEE 802.11 MAC πρωτόκολλο που συναντάμε και στα δίκτυα MANETs. Είναι γνωστό ότι το 802.11 WEP είναι ευπαθές σε πολλούς τύπους επιθέσεων κρυπτογραφίας λόγω της κακής χρήσης της κρυπτογραφίας. Το πρωτόκολλο 802.11 είναι επίσης ευάλωτο σε επιθέσεις Denial of Service (DoS) οι οποίες στοχεύουν στο κανάλι επικοινωνίας και στα συστήματα κράτησης θέσεων. Ο εισβολέας μπορεί να εκμεταλλευτεί την εκθετική υποχώρηση του δυαδικού συστήματος (expotential backoff scheme) και να αρνηθεί την πρόσβαση στο ασύρματο κανάλι από τους γείτονές του. Επειδή ο τελευταίος νικητής (εισβολέας) είναι πάντα ευνοημένος

μεταξύ των τοπικών κόμβων υποστηρίζοντας έτσι μια συνεχείς μετάδοση μπορεί να συλλάβει για πάντα το κανάλι και να προκαλέσει άλλους κόμβους να υποχωρήσουν.

Επιπλέον τα backoffs στο επίπεδο ζεύξης δεδομένων μπορούν να φέρει αλυσιδωτές αντιδράσεις σε ανώτερα πρωτόκολλα τους στρώματος που χρησιμοποιούν τα συστήματα backoff (π.χ.TCP window managment). Ένα άλλο θέμα ευπάθειας των 802.11 προέρχεται από το πεδίο NAV (Network Allocation Vector) που απαιτούνται στα αιτήματα send/clear για την αποστολή (RTS / CTS) τα οποία δείχνουν τη διάρκεια της κράτησης του καναλιού. Έτσι ένας κακόβουλος γείτονας είτε αποστολέας είτε δέκτης μπορεί να ακούσει τυχαία τις πληροφορίες NAV και στη συνέχεια μέσω της ασύρματης παρεμβολής να εισάγει ένα 1-bit σφάλματος στο στρώμα πλαίσιο (Link Layer) του θύματος.

3.2 Διαταραχή στο MAC-DCF και στον μηχανισμό υποχώρησης (back off)

Τα ασύρματα πρωτόκολλα MAC αναλαμβάνουν να δημιουργήσουν όπως είπαμε συμπεριφορές συνεργασίας μεταξύ των κόμβων. Προφανώς ένας κακόβουλος κόμβος δεν ακολουθεί την κανονική λειτουργία των πρωτοκόλλων. Στο επίπεδο ζεύξης δεδομένων ένας κακόβουλος κόμβος μπορεί να διακόψει είτε τον ισχυρισμό χρησιμοποίησης ή κράτησης του καναλιού πάνω στον οποίο βασίζονται τα MAC πρωτοκόλλα[32].

Ένας κακόβουλος γείτονας είτε του αποστολέα είτε του παραλήπτη δεν μπορεί να ακολουθήσει εκ προθέσεως τις προδιαγραφές του πρωτοκόλλου. Για παράδειγμα, ο εισβολέας μπορεί να αλλοιώσει τα πλαίσια εύκολα εισάγοντας ορισμένα bits ή αγνοώντας τη συνεχιζόμενη μετάδοση. Θα μπορούσε επίσης να περιμένει λίγο SIFS ή να εκμεταλλευτεί την εκθετική υποχώρηση του δυαδικού συστήματος (binary exponential backoff scheme) για να εξαπολύσει επιθέσεις DoS στο IEEE 802.11 MAC. Το καθεστώς αυτό ευνοεί τον τελευταίο νικητή μεταξύ των υπόλοιπων κόμβων. Οι κόμβοι που έχουν μεγάλο φόρτο τείνουν να συλλάβουν το κανάλι μέσα από την συνεχή διαβίβαση δεδομένων προκαλώντας έτσι ελαφρύ φορτίο στους γείτονες με ατέλειωτα backoffs. Οι κακόβουλοι κόμβοι θα μπορούσαν να επωφεληθούν από αυτήν την ευπάθεια. Επιπλέον η υποχώρηση αυτή στο επίπεδο ζεύξης δεδομένων μπορεί να προκαλέσει μια αλυσιδωτή αντίδραση στα πρωτόκολλα των ανωτέρων επιπέδων που χρησιμοποιούν ένα σύστημα υποχώρησης, όπως η διαχείριση παράθυρου στο TCP πρωτόκολλο[32].

3.3 Αδυναμία του πεδίου NAV

Το πεδίο του φορέα χορήγησης δικτύου (Network Allocation Vector) που υπάρχει στα πλαίσια RTS / CTS εκθέτει μια άλλη αδυναμία και κατ' επέκταση μια DoS επίθεση στο στρώμα ζεύξης δεδομένων. Αρχικά το πεδίο NAV προτάθηκε για την άμβλυνση του προβλήματος του κρυμμένου τερματικού στον μηχανισμό του ενιαίου μεταφορέα (carrier sense mechanism). Κατά τη διάρκεια της RTS / CTS χειραψίας ο αποστολέας στέλνει πρώτα ένα μικρό πλαίσιο RTS που περιέχει τον χρόνο που απαιτείται για την ολοκλήρωση της CTS, της μεταφοράς δεδομένων και των πλαισίων ACK. Κάθε γείτονας του αποστολέα και του δέκτη θα ενημερώσει το πεδίο

NAV και θα αναβάλει τη διαβίβασή κατά τη διάρκεια της μελλοντικής συναλλαγής σύμφωνα με τον χρόνο που «άκουσε» τυχαία. Ένας εισβολέας μπορεί να ακούσει τις πληροφορίες του NAV και στη συνέχεια εκ προθέσεως να αλλοιώσει το πλαίσιο του επίπεδου ζεύξης δεδομένων μέσω ασύρματων παρεμβολών στη συνεχιζόμενη μετάδοση.

3.4 Αδυναμία του πρωτοκόλλου 802,11 WEP

Το πρωτόκολλο IEEE 802.11 WEP ενσωματώνει την τεχνολογία Wired Equivalent Privacy (WEP) για την παροχή στα WLAN συστήματα ενός μέτριου επίπεδου ιδιωτικότητας χρησιμοποιώντας την κρυπτογράφηση των ραδιοσημάτων. Το πρότυπο 802.11 WEP υποστηρίζει WEP κλειδιά κρυπτογραφίας των 40 bit, αν και ορισμένοι έχουν εφαρμόσει 104 bits αλλά ακόμη και 128 bits. Είναι γνωστό ότι το WEP έχει πλέον αποκρυπτογραφηθεί και το WEP αντικαθίσταται από το AES στο 802.11i. Ορισμένες από τις αδυναμίες 802,11 WEP είναι οι παρακάτω:

- Το WEP πρωτόκολλο δεν προσδιορίζει διαχείριση κλειδιών.
- Το διάνυσμα αρχικοποίησης (IV) το οποίο επαναχρησιμοποιείται είναι ένα 24-bit πεδίο που αποστέλλονται αυτούσιο και αποτελεί μέρος του κλειδιού κρυπτογράφησης RC4. Μια ποικιλία των διαθέσιμων κρυπτογραφικών μεθόδων μπορεί να αποκρυπτογραφήσει τα δεδομένα χωρίς να γνωρίζει το κλειδί κρυπτογράφησης.
- Η συνδυασμένη χρήση του μη κρυπτογραφικού αλγορίθμου ακεραιότητας CRC32 με την κρυπτογράφηση ροής είναι και αυτός ένας κίνδυνος ασφάλειας[27].
- Το WEP δεν εμποδίζει την παραχάραξη των πακέτων.
- Το WEP δεν εμποδίζει τις επιθέσεις αναπαραγωγής. Ένας εισβολέας μπορεί απλά να καταγράφει και να αναπαράγει πακέτα όπως επιθυμεί και αυτά να γίνονται αποδεκτά από τους νόμιμους κόμβους.
- Το WEP χρησιμοποιεί το RC4 αντικανονικά. Τα κλειδιά που χρησιμοποιούνται είναι πολύ αδύναμα και μπορεί να ανακαλύπτονται από συνήθης υπολογιστές (PCs) σε ώρες ή ακόμα σε λεπτά χρησιμοποιώντας ελεύθερα διαθέσιμο λογισμικό.
- Το WEP επιτρέπει σε έναν επιτιθέμενο χωρίς να ανιχνευθεί να τροποποιήσει ένα μήνυμα χωρίς να γνωρίζει το κλειδί κρυπτογράφησης.
- Η διαχείριση των κλειδών του WEP είναι ελλιπείς όπως και η ενημέρωση τους.

- Τέλος είναι εύκολη η τροποποίηση των μηνυμάτων ελέγχου ταυτότητας[29].

Είναι γνωστό ότι το πρωτόκολλο *IEEE 802.11WEP* είναι ευάλωτο σε επιθέσεις δύο κατηγοριών :

- **Επιθέσεις της ιδιωτικής ζωής και της ακεραιότητας μηνύματος.** Αυτές οι επιθέσεις βασίζονται σε διάφορους μηχανισμούς, όπως στο μικρό διάνυσμα αρχικοποίησης (IV), στον γραμμικό κυκλικό έλεγχο πλεονασμού (CRC -32 checksum) και στην ανάκτηση του κλειδιού από τις γνωστές plaintext επιθέσεις.

- **Πιθανολογικές επιθέσεις ανάκτησης των κλειδιών κρυπτογράφησης** όπως η επίθεση Fluhrer-Mantin-Shamir . Αυτές οι επιθέσεις βασίζονται στο γεγονός ότι η αρχική παραγωγή του RC4 κλειδιού είναι δυσανάλογα επηρεασμένη από έναν μικρό αριθμό βασικών bits, ιδιαίτερα από το πρόθεμα (prefix) και το «postfix» τμήμα του κλειδιού [28].

Κεφάλαιο 4

Επιθέσεις στο Επίπεδο Δικτύου

4.1 Εισαγωγή

Τα πρωτόκολλα του επιπέδου δικτύου διευκολύνουν την συνδεσιμότητα των γειτονικών κόμβων και όχι μόνο σε ένα δίκτυο Manet. Η συνδεσιμότητα μεταξύ κινητών κόμβων πραγματοποιείται χάρη στον σύνδεσμο των πολλαπλών αλμάτων και στηρίζεται σε μεγάλο βαθμό στις συνεταιριστικές αντιδράσεις μεταξύ των κόμβων του δικτύου. Σε μια ιδανική κατάσταση, όλοι οι κόμβοι υποτίθεται ότι είναι έμπιστοι στην εκτέλεση των εργασιών τους σύμφωνα με το πρωτόκολλο. Αλλά αυτό είναι μια ακραία υπόθεση για το ασταθές περιβάλλον των δικτύων Manet. Επειδή κάθε κόμβος είναι υπεύθυνος για τη λήψη αποφάσεων όσον αφορά την δρομολόγηση των πακέτων που φθάνουν σε αυτόν, γίνεται σχετικά εύκολα αντιληπτό ότι με μια εσφαλμένη συμπεριφορά κάποιου κόμβου μπορεί να πραγματοποιηθεί μια επίθεση σε ένα δίκτυο Manet [5] .

Μια μεγάλη ποικιλία επιθέσεων με στόχο το επίπεδο του δικτύου έχει εντοπιστεί και σε μεγάλο βαθμό μελετηθεί. Η βασική ιδέα πίσω από τις επιθέσεις στο επίπεδο του δικτύου είναι να απορροφηθεί η κυκλοφορία του δικτύου και να προκληθεί η εκτροπή και ως εκ τούτου ο έλεγχος ροής της κυκλοφορίας του δικτύου. *«Χτυπώντας»* τα πρωτόκολλα δρομολόγησης οι επιτιθέμενοι μπορούν να επιτύχουν αυτούς τους στόχους[5].

Πολλές μέθοδοι χρησιμοποιούνται από τους δράστες για να επιτευχθεί ο απώτερος στόχος της διακοπής της κυκλοφορίας στο δίκτυο. Τα πακέτα της κυκλοφορίας έτσι διαβιβάζονται σε μη βέλτιστα μονοπάτια γεγονός το οποίο εισαγάγει μια σημαντική καθυστέρηση. Επιπλέον, τα πακέτα θα μπορούσε να διαβιβαστούν σε ένα ανύπαρκτο μονοπάτι και να χαθούν. Οι επιτιθέμενοι μπορούν να δημιουργήσουν βρόχους δρομολόγησης και να εισαγάγουν έτσι σοβαρή συμφόρηση στο δίκτυο υποστηρίζοντας έτσι το κανάλι σε ορισμένους τομείς. Οι επιτιθέμενοι μπορούν ακόμη και να αποτρέψουν έναν κόμβο-πηγή από την εξεύρεση μιας διαδρομής για τον προορισμό προκαλώντας έτσι τον διαχωρισμό του δικτύου γεγονός το οποίο εντείνει την συμφόρηση του δικτύου και την υποβάθμιση των επιδόσεων[5].

Οι επιτιθέμενοι εναντίον ενός δικτύου μπορούν να ταξινομηθούν όπως έχουμε αναφέρει σε δύο ομάδες, στους εσωτερικούς και στους εξωτερικούς. Ενώ ένας εξωτερικός εισβολέας δεν είναι νόμιμος χρήστης του δικτύου, ένας εσωτερικός εισβολέας περιέχει εμπιστευτικές πληροφορίες και είναι εξουσιοδοτημένος κόμβος λαμβάνοντας έτσι μέρος στον μηχανισμό δρομολόγησης των δικτύων MANETs. Οι αλγόριθμοι δρομολόγησης έχουν χαρακτήρα συνεργασίας και έτσι μπορούν να επηρεάσουν ολόκληρο το σύστημα[5].

Ένας κόμβος Manet περιέχει εμπιστευτικές πληροφορίες και μπορεί έτσι να διαταράξει το δίκτυο επικοινωνιών εκ προθέσεως όπως επίσης και ενδέχεται να υπάρχουν και άλλοι λόγοι για την δυσλειτουργία του δικτύου. Η απειλή της

αποτυχημένης λειτουργίας των κόμβων είναι σοβαρή ιδιαίτερα στο πλαίσιο της έκτακτης ανάγκης για μια ασφαλή διαδρομή. Η αποτυχία τους έτσι μπορεί να οδηγήσει ακόμη και στην κατάτμηση του δικτύου, την αποκοπή της επικοινωνίας με άλλους κόμβους κτλ. Ένα κακόβουλος κόμβος μπορεί επίσης να συμπεριφέρεται σωστά ώστε να διαφυλάξει τους πόρους του. Ακόμα οι κακόβουλοι κόμβοι κάνουν χρήση των υπηρεσιών άλλων κόμβων αλλά δεν πρόκειται να ανταποδώσουν[5].

Θα πρέπει επίσης να εξεταστούν οι στόχοι των επιτιθεμένων. Στη δρομολόγηση επιθέσεων οι εισβολείς δεν ακολουθούν τις προδιαγραφές των πρωτοκόλλων δρομολόγησης και αποσκοπούν στη διατάραξη της επικοινωνίας του δικτύου με τους ακόλουθους τρόπους:

- *Διαταραχή της διαδρομής (Route Disruption)* δηλαδή τροποποίηση των υφισταμένων οδών δημιουργώντας βρόχους δρομολόγησης και προκαλώντας τα πακέτα να διαβιβάζονται κατά μήκος μιας διαδρομής που δεν είναι βέλτιστη ή ανύπαρκτη ή άλλως εσφαλμένη.

- *Κόμβος απομόνωσης (Node Isolation)* δηλαδή απομόνωση ενός κόμβου ή κάποιων κόμβων από την επικοινωνία με άλλους κόμβους στο δίκτυο προκαλώντας έτσι «στεγανοποίηση» του δικτύου και ούτω καθεξής.

- *Κατανάλωση Πόρων (Resource Consumptions)* δηλαδή μείωση της απόδοσης του δικτύου καταναλώνοντας το εύρος ζώνης του δικτύου ή τους πόρους των κόμβων[5].

Ένα πρωτόκολλο δρομολόγησης είναι ο μηχανισμός με τον οποίο ελέγχεται η κυκλοφορία των χρηστών μέσω του δικτύου από τον κόμβο πηγής στον κόμβο προορισμού. Οι σχετικοί στόχοι περιλαμβάνουν τη μεγιστοποίηση της απόδοσης του δικτύου από την χρήση του πρωτοκόλλου με την εφαρμογή των απαιτήσεων ενώ ελαχιστοποιείται το κόστος του ίδιου του δικτύου. Οι τέσσερις βασικές λειτουργίες δρομολόγησης σε ασύρματα adhoc δίκτυα είναι οι εξής:

- Η λειτουργία **Παραγωγής της Διαδρομής** (Path Generation) η οποία παράγει διαδρομές σύμφωνα με τις συγκεντρωμένες πληροφορίες κατάστασης του δικτύου οι οποίες προέρχονται από τους ίδιους τους κόμβους.

- Η λειτουργία **Επιλογής της Διαδρομής** (Path Selection) η οποία επιλέγει τα κατάλληλα μονοπάτια του δικτύου εφαρμόζοντας τις πληροφορίες για την κατάσταση του δικτύου.

- Η λειτουργία **Προώθησης των Δεδομένων** η οποία μεταδίδει τα δεδομένα του χρήστη κατά μήκος της επιλεγμένης διαδρομής.

- Τέλος η λειτουργία της **Συντήρησης του Μονοπατιού** η οποία εξασφαλίζει την διατήρηση της επιλεγμένης διαδρομής[2].

•

Γενικά οι επιθέσεις στο επίπεδο δικτύου πραγματοποιούνται με τους παρακάτω τρόπους :

1. Ο κακόβουλος κόμβος συμμετέχει σε μια πορεία δρομολόγησης πακέτων αλλά ο σκοπός του είναι η απώλεια ορισμένων πακέτων. Αυτό επιδεινώνει την ποιότητα των συνδέσεων και τις περαιτέρω προεκτάσεις για τις επιδόσεις της δρομολόγησης αν το TCP είναι το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιείται.

2. Ο κακόβουλος κόμβος μεταδίδει λανθασμένες ή ψευδής ενημερώσεις για τις διαθέσιμες πορείες δρομολόγησης. Οι ενέργειες αυτές θα μπορούσαν να οδηγήσουν σε συχνές αστοχίες στην εύρεση της διαδρομής και έτσι τα αποτελέσματα της δρομολόγησης δεν θα έχουν τα επιθυμητά αποτελέσματα.

3. Ο κακόβουλος κόμβος θα μπορούσε να αποστέλλει τις ίδιες ενημερώσεις για μεγάλο χρονικό διάστημα παρόλο που αυτές δεν ισχύουν. Αυτό θα μπορούσε να οδηγήσει σε εσφαλμένες διαδρομές και στην υποβάθμιση των επιδόσεων.

4. Ο κακόβουλος κόμβος επιδιώκει μείωση της παραμέτρου TTL (time-to-live) του πεδίου στο IP header έτσι ώστε το πακέτο να μην φτάνει ποτέ στον προορισμό[33].

Όλα τα παραπάνω θα μπορούσαν να οδηγήσουν σε κυκλοφοριακή συμφόρηση που προκαλείται είτε από αναμετάδοση πακέτων ή τη μετάδοση εσφαλμένων διαδρομών έτσι ώστε η επικοινωνία να διακοπεί σε ελάχιστο χρονικό διάστημα. Μια επίθεση του τύπου (1) μπορεί να αντιμετωπιστεί με την απόδοση των επιπέδων εμπιστοσύνης προς τους κόμβους και με διαδρομές που προσφέρουν το υψηλότερο επίπεδο της εμπιστοσύνης. Φυσικά, πολλές διαδρομές θα πρέπει να διατηρηθούν. Μια επίθεση του τύπου (4) μπορεί να εξουδετερώνεται απλά καθιστώντας υποχρεωτικά σε ένα κόμβο του δικτύου να εξασφαλίζει ότι η τιμή TTL θα είναι μεγαλύτερη από την τιμή των αλμάτων που χρειάζονται για τον επιθυμητό προορισμό[33].

Η οικογένεια των επιθέσεων που αφορούν την δρομολόγηση αναφέρεται σε κάθε πράξη της διαφήμισης των ενημερώσεων που δεν ακολουθούν τις προδιαγραφές του πρωτοκόλλου δρομολόγησης. Για παράδειγμα στο πλαίσιο του πρωτοκόλλου DSR (Dynamic Source Routing protocol), ο εισβολέας μπορεί να τροποποιήσει την διαδρομή που απαριθμούνται στα RREQ (Route Request) ή RREP (Route Reply) πακέτα διαγράφοντας έναν κόμβο από τη λίστα αλλάζοντας έτσι την σειρά των κόμβων στη λίστα ή προσαρτώντας έναν νέο κόμβο στη λίστα. Στα *distance vector* πρωτόκολλα δρομολόγησης όπως το AODV (Ad-hoc On-demand Distance Vector), ο εισβολέας μπορεί να διαφημίζει μια διαδρομή με μια μικρότερη απόσταση από την πραγματική απόσταση προς τον προορισμό ή να διαφημίσει ενημερώσεις δρομολόγησης με ένα μεγάλο αριθμό σειράς και να ακυρώσει όλες τις άλλες ενημερώσεις δρομολόγησης από άλλους κόμβους. Οι επιτιθέμενοι «*χτυπώντας*» τα πρωτόκολλα δρομολόγησης μπορούν να προσελκύσουν την κυκλοφορία προς ορισμένους προορισμούς οι οποίοι είναι υπό τον έλεγχό τους και να προωθήσουν τα πακέτα κατά μήκος μιας διαδρομής που δεν είναι η βέλτιστη ή ακόμη και ανύπαρκτη. Οι επιτιθέμενοι μπορούν να δημιουργήσουν δρομολόγηση που ακολουθεί την λογική

του βρόχου και έτσι να θεσπιστεί σοβαρή συμφόρηση στο δίκτυο. Πολλαπλοί συνεργοί επιτιθέμενοι μπορούν ακόμη να εμποδίσουν ένα κόμβο-πηγής από την εύρεση οποιασδήποτε διαδρομής προς κάποιον προορισμό[28].

Υπάρχουν ακόμη ενεργές ερευνητικές προσπάθειες για τον εντοπισμό και την εξουδετέρωση πιο εξελιγμένων και λεπτών επιθέσεων δρομολόγησης. Για παράδειγμα, ο εισβολέας ενδέχεται να υπονομεύσει περαιτέρω τους υπάρχοντες κόμβους στο δίκτυο ή να κατασκευάσει την ταυτότητά του και να μιμηθεί έναν άλλο νόμιμο κόμβο. Ένα ζευγάρι εισβολέων μπορεί να δημιουργήσει μια σκουληκότρυπα και μια συντόμευση της κανονικής ροής μεταξύ τους. Στα On-demand Adhoc πρωτόκολλα δρομολόγησης οι επιτιθέμενοι μπορούν να καθορίζουν την διαδικασία συντήρησης της διαδρομής και διαφημίζουν ότι μια ενεργή διαδρομή δεν υφίσταται[28].

4.2 Προληπτικά και Αντιδραστικά Πρωτόκολλα Δρομολόγησης

Τα Ad Hoc πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν ως Προληπτικά (**Proactive**, Table-Driven) ή Αντιδραστικά (**Reactive**, On- Demand).

Σε ένα *προληπτικό* πρωτόκολλο δρομολόγησης όλα τα δρομολόγια προς κάθε προορισμό διατηρούνται σε έναν ενημερωμένο (up-to-date) πίνακα. Έτσι οι αλλαγές στην τοπολογία του δικτύου ανανεώνονται συνεχώς καθώς εμφανίζονται.

Στο *αντιδραστικό* πρωτόκολλο δρομολόγησης μια σύνδεση μεταξύ δύο κόμβων δημιουργείται μόνο όταν ζητηθεί από μια πηγή. Όταν μια διαδρομή εντοπίζεται, διατηρείται με μια διαδικασία συντήρησης έως ότου ο προορισμός θα υφίστανται. Ο παρακάτω πίνακας παρουσιάζει μια σύγκριση μεταξύ των proactive και reactive πρωτόκολλων δρομολόγησης[15].

Πρωτόκολλα	Προληπτικά (Proactive)	Αντιδραστικά (Reactive)
Πλεονεκτήματα	➢ Μια διαδρομή μπορεί να επιλεγεί αμέσως χωρίς καμία καθυστέρηση.	➢ Ελάχιστο εύρος ζώνης χρησιμοποιείται για την συντήρηση των πινάκων δρομολόγησης. ➢ Περισσότερο αποτελεσματικά από ενεργειακής άποψης. ➢ Αποτελεσματική συντήρηση των δρομολογίων.
Μειονεκτήματα	▪ Περισσότερη κυκλοφορία. ▪ Περισσότερο εύρος ζώνης. ▪ Συμφόρηση δικτύου	▪ Καθυστέρηση στην εύρεση του δρομολογίου

Εικόνα 11 Πλεονεκτήματα και Μειονεκτήματα των Πρωτοκόλλων Δρομολόγησης

4.3 Επιθέσεις

4.3.1 Επιθέσεις κατά τη φάση ανακάλυψης της διαδρομής (RREQ Επίθεση).

Υπάρχουν κακόβουλες επιθέσεις που στοχεύουν στη ανακάλυψη ή στη φάση συντήρησης της δρομολόγησης μη ακολουθώντας τις προδιαγραφές των πρωτοκόλλων δρομολόγησης. Επιθέσεις που προκαλούνται από πλημμύρα μηνυμάτων δρομολόγησης, όπως μηνύματα πλημμύρας (flooding) «hello», μηνύματα πλημμύρας RREQ, μηνύματα πλημμύρας αναγνώρισης (acknowledgement), μηνύματα υπερχείλισης του πίνακα δρομολόγησης και μηνύματα δρομολόγησης βρόχων είναι απλά παραδείγματα επιθέσεων δρομολόγησης που στοχεύουν στην φάση της ανακάλυψης διαδρομής. Οι προληπτικοί (proactive) αλγόριθμοι δρομολόγησης όπως ο DSDV και ο OLSR προσπαθούν να ανακαλύψουν τις πληροφορίες δρομολόγησης πριν αυτό είναι αναγκαίο, ενώ οι on-demand αλγόριθμοι όπως ο DSR και ο AODV δημιουργούν διαδρομές μόνο όταν αυτό είναι απαραίτητο. Έτσι οι προληπτικοί αλγόριθμοι απαιτούν πολλές δαπανηρές μεταδόσεις και είναι χειρότεροι σε απόδοση από τους on-demand επειδή δεν ενσωματώνουν τη δυναμική των MANETs. Οι προληπτικοί αλγόριθμοι είναι πιο ευάλωτοι σε επιθέσεις υπερχείλισης του πίνακα δρομολόγησης. Ορισμένες από αυτές τις επιθέσεις είναι οι παρακάτω[32]:

Επίθεση υπερχείλισης (overflow) του πίνακα δρομολόγησης: Ένας κακόβουλος κόμβος διαφημίζει στους εξουσιοδοτημένους κόμβους που υπάρχουν στο δίκτυο, δρομολόγια που πηγαίνουν σε μη υπάρχοντες κόμβους. Αυτού του είδους η επίθεση συμβαίνει συνήθως σε προληπτικούς (proactive) αλγορίθμους δρομολόγησης που στοχεύουν στην περιοδική επαλήθευση των πληροφοριών δρομολόγησης. Ο εισβολέας προσπαθεί να δημιουργήσει αρκετά δρομολόγια ώστε να αποτρέψει να δημιουργηθούν νέα δρομολόγια. Οι προληπτικοί αλγόριθμοι δρομολόγησης είναι πιο ευάλωτοι σε επιθέσεις υπερχείλισης πίνακα δεδομένου ότι προσπαθήσουν να ανακαλύψουν πληροφορίες δρομολόγησης πριν να υπάρξει πραγματική ανάγκη. Έτσι ένας εισβολέας μπορεί να στείλει απλά υπερβολικές διαφημίσεις κάποιων διαδρομών ώστε να υπερχειλίσει τον πίνακα δρομολόγησης του θύματος[32].

Επίθεση "δηλητηρίασης" της κρυφής μνήμης (cache) δρομολόγησης: Σε επιθέσεις "δηλητηρίασης" της cache δρομολόγησης, οι εισβολείς επωφελούνται από την ετερόκλητη λειτουργία ενημέρωσης του πίνακα δρομολόγησης με το γεγονός ότι όταν ένας κόμβος που «κρυφακούει» κάθε πακέτο μπορεί να προσθέσει πληροφορίες από την προσωρινή του μνήμη στην κεφαλίδα του πακέτου έστω και αν ο κόμβος δεν βρίσκεται στην διαδρομή. Ας υποθέσουμε ότι ένας κακόβουλος κόμβος Μ θέλει να δηλητηριάσει το δρομολόγιο για τον κόμβο Χ. Ο κόμβος Μ μεταδίδει πλαστογραφημένα πακέτα στην διαδρομή προς τον Χ μέσω του ίδιου. Έτσι οι γειτονικοί κόμβοι που ακούν τυχαία το πακέτο μπορεί να προσθέσουν αυτή την διαδρομή στην δική τους κρυφή μνήμη(cache)[32].

Επίθεση κατά τη φάση συντήρησης της δρομολόγησης. Υπάρχουν επιθέσεις που στοχεύουν τη φάση της συντήρησης της διαδρομής με τη μετάδοση ψευδών μηνυμάτων ελέγχου όπως ψευδή μηνύματα αποκομμένης σύνδεσης τα οποία προκαλούν την δαπανηρή συντήρηση της διαδρομής και την επίκληση της λειτουργίας επισκευής. Για παράδειγμα, τα πρωτόκολλα AODV και DSR εφαρμόζουν διαδικασίες συντήρησης της διαδρομής για να ανακτήσουν σπασμένα μονοπάτια όταν οι κόμβοι κινούνται. Εάν ο κόμβος προορισμού ή ο ενδιάμεσος κόμβος κατά μήκος μιας ενεργής διαδρομής παρουσιάσει κάποιο πρόβλημα τότε ο γειτονικός κόμβος του σπασμένου συνδέσμου μεταδίδει ένα μήνυμα λάθους της διαδρομής προς όλους τους ενεργούς γείτονες του. Ο κόμβος αυτός επίσης διαψεύδει τον προορισμό αυτό στον πίνακα δρομολόγησης. Οι επιτιθέμενοι θα μπορούσαν να επωφεληθούν του μηχανισμού αυτού για να εξαπολύσουν επιθέσεις στέλνοντας εσφαλμένα μηνύματα λάθους της διαδρομής[32].

Επίθεση κατά τη φάση της διαβίβασης δεδομένων (Data Flooding Attack). Ορισμένες επιθέσεις έχουν ως στόχο την διαβίβαση των πακέτων δεδομένων. Σε αυτό το σενάριο ο κακόβουλος κόμβος συμμετέχει συνεταιριστικά στο πρωτόκολλο δρομολόγησης στην ανακάλυψη, στη φάση συντήρησης της διαδρομής αλλά και στη φάση διαβίβασης των δεδομένων και δεν διαβιβάζει τα πακέτα δεδομένων σύμφωνα με τον πίνακα δρομολόγησης. Οι κακόβουλοι κόμβοι απλά δεν μεταβιβάζουν τα πακέτα δεδομένων αλλά τροποποιούν τα δεδομένα του περιεχομένου και επαναλαμβάνουν ή στέλνουν ανεξέλεγκτα (flooding) πακέτα δεδομένων. Μπορούν επίσης επιλεκτικά να καθυστερήσουν τη διαβίβαση ευαίσθητων στον χρόνο πακέτων δεδομένων[32].

4.3.2 Επιθέσεις σε συγκεκριμένα πρωτόκολλα δρομολόγησης.

Υπάρχουν επιθέσεις που στοχεύουν κάποια συγκεκριμένα πρωτόκολλα δρομολόγησης. Αρχικά παρατίθενται μια εικόνα με τα συνήθη πρωτόκολλα δρομολόγησης στα Manet και στην συνέχεια θα γίνουν περιγραφές των επιθέσεων στα σημαντικότερα από αυτά.

Πρωτόκολλα		
Προληπτικά	*Διαδραστικά*	*Ασφάλειας*
CGSR,DRF,DSDV,DTDV, HSLS,HSR,LCA,MMRP,OLSR,STAR,TBRPF,WRP	ABR,AODY,AOMDY,ARA,BSR,CHAMP,DSR,DSRFLOW,FORP,LBR,LMR,LUNAR,PLBR,RDMR,SSR,SMR,TORA	ARAN,LHAP,SAODV, SAR,SEAD,SLSP,SMT, SPAAR,SRP,TESLA

Εικόνα 12 Πρωτόκολλα Δρομολόγησης στα Manet [15]

Στο **DSR** ο εισβολέας μπορεί να τροποποιήσει την πηγή της διαδρομής που απαριθμείται στα RREQ ή RREP πακέτα. Μπορεί να διαγράψει έναν κόμβο από τη λίστα, να αλλάξει τη σειρά ή να προσθέσει ένα νέο κόμβο στον κατάλογο.

Γενικά το DSR λειτουργεί ως εξής[11]: Οι κόμβοι στέλνουν ένα Route Request (RREQ) μήνυμα και όλοι οι κόμβοι που λαμβάνουν αυτό το μήνυμα εισάγουν τον εαυτό τους στην διαδρομή (source route) του μηνύματος και το διαβιβάζουν στους γείτονές τους εφόσον δεν έχουν λάβει κάποιο ίδιο αίτημα πριν. Αν ένας κόμβος που λαμβάνει το μήνυμα είναι ο προορισμός ή έχει μια διαδρομή προς τον προορισμό δεν προωθεί το αίτημα αλλά στέλνει μια απάντηση στην πηγή (RREP μήνυμα) που περιέχει την πλήρη διαδρομή προς τον προορισμό. Μπορεί να στείλει την απάντηση κατά μήκος της διαδρομής με την αντίστροφη σειρά προς την πηγή ή να εκδώσει μια αίτηση-μήνυμα (Route Request) συμπεριλαμβανομένης της οδού (source route) ώστε να επικοινωνήσει με την πηγή μόνο εάν η πρώτη διαδρομή (αντίστροφη σειρά προς την πηγή) δεν είναι δυνατή λόγω ασύμμετρης σύνδεσης. Μετά την παραλαβή ενός ή περισσότερων δρομολόγιων η πηγή επιλέγει την καλύτερη (από προεπιλογή τη συντομότερη) διαδρομή, την αποθηκεύει και στέλνει τα μηνύματα σε αυτή την πορεία.

Υπάρχουν μια σειρά πιθανών επιθέσεων στο DSR πρωτόκολλο επειδή δεν υπάρχει μέτρο ασφαλείας και επίσης επειδή έχει υιοθετηθεί ότι υπάρχει ειλικρινής συντονισμός των κόμβων μεταξύ τους αλλά και με το πρωτόκολλο. Μερικές από αυτές υπάρχουν παρακάτω

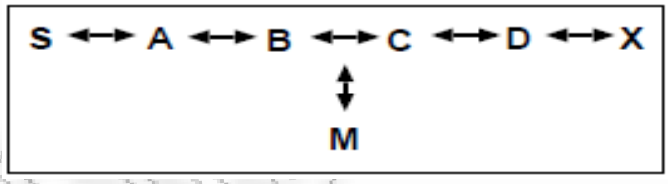
- *Απόρριψη πακέτων από έναν κόμβο λαμβάνοντας υπόψη τα ακόλουθα σενάρια:*
    - *Απόρριψη όλων των πακέτων* που δεν προορίζονται για να εκτελεστούν ή μερική πτώση αυτών.
    - *Μερική πτώση των πακέτων* που μπορεί να περιορίζεται σε συγκεκριμένα είδη όπως είναι μόνο πακέτα δεδομένων ή πακέτα ελέγχου διαδρομής που περιέχουν ένα ή περισσότερα πακέτα που προορίζονται για συγκεκριμένες κόμβους.

- *Αποφυγή αποστολής ενός σφάλματος διαδρομής (Route Error) όταν έχει ανιχνευθεί ένα λάθος* ώστε να αποτρέψει τους άλλους κόμβους από την αναζήτηση εναλλακτικών διαδρομών.

- Με την αποστολή πλαστών πακέτων δρομολόγησης ένας εισβολέας μπορεί να δημιουργήσει την λεγόμενη *μαύρη τρύπα (Black Hole)* δηλαδή έναν κόμβο όπου όλα τα πακέτα απορρίπτονται ή χάνονται.

- Η προσπάθεια *για την δημιουργία διαδρομών που περνούν από ένα κόμβο εμφανίζονται πλέον με την προσθήκη ορισμένων εικονικών κόμβων στην διαδρομή* και αποτελεί ένα άλλο είδος επίθεσης.

- Επίσης *η τροποποίηση της λίστας των κόμβων στην επικεφαλίδα (header) μιας αίτησης διαδρομής (Route Request) ή απάντησης για μια διαδρομή προκαλεί λανθασμένα πακέτα διαδρομής και προσθήκη εσφαλμένων διαδρομών στη μνήμη cache των άλλων κόμβων*. Πιο συγκεκριμένα στην παρακάτω εικόνα υπάρχει μια διαδρομή από τον κόμβο S στον κόμβο X αποτελούμενη από τους κόμβους A,B,C,D. Αν τώρα ένα πακέτο «ταξιδέψει» από τον κόμβο S στον κόμβο X θα περάσει από πολλούς κόμβους οι οποίοι θα προσθέσουν στην μνήμη cache τους το δρομολόγιο (S,A,B,C,X). Έτσι ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την ευπάθεια της διαδικασίας ανεύρεσης της διαδρομής του πρωτοκόλλου DSR και να "μολύνει" την μνήμη cache των κόμβων. Υποθέτουμε τώρα ότι ο κακόβουλος κόμβος M θέλει να μολύνει τα δρομολόγια προς τον κόμβο X και για αυτό στέλνει «*spoofed*» πακέτα στα δρομολόγια προς τον κόμβο X και έτσι μολύνει την cache των γειτόνων του κόμβου X[12].



Εικόνα 13 Επίθεση τροποποίησης της λίστας των κόμβων στην επικεφαλίδα (header) μιας αίτησης διαδρομής

- *Μείωση του ορίου αλμάτων (TTL) όταν λαμβάνετε ένα πακέτο* έτσι ώστε το πακέτο να μην γίνει ποτέ δεκτό από τον κόμβο προορισμού.

- *Εκκίνηση μιας περιόδου πολύ συχνών αιτημάτων διαδρομής (Route Request)* ώστε να καταναλωθεί το εύρος ζώνης και η (ηλεκτρική) ενέργεια των κόμβων και να προκληθεί συμφόρηση.

- *Αποστολή απαντήσεων διαδρομής (Route Reply) με χρόνο όχι ανάλογο με το μήκος της διαδρομής*. Αυτό μπορεί να δώσει μεγαλύτερη προτεραιότητα σε μεγάλες διαδρομές προσελκύοντας έτσι διαδρομές προς τον επιτιθέμενο είτε με μικρότερη προτεραιότητα σε σύντομες διαδρομές αποφεύγοντας έτσι τους εισβολείς.[11]

Στο **AODV (**Ad-hoc On Demand Distance Vector) γενικά ο εισβολέας μπορεί να διαφημίζει μια διαδρομή με μια μικρότερη απόσταση από την πραγματική ή να διαφημίσει μια ενημέρωση δρομολόγησης με ένα μεγάλο αριθμό σειράς και να ακυρώσει όλες τις ενημερώσεις δρομολόγησης από άλλους κόμβους[17].

Συγκριμένα το AODV είναι ένα αντιδραστικό (reactive) πρωτόκολλο δρομολόγησης. Είναι ίσως το πιο γνωστό πρωτόκολλο στα Manet. Πρόκειται για μια τροποποίηση του **DSDV** (Destination-Sequenced Distance Vector). Το DSDV είναι ένα παραδοσιακό "table-driven" πρωτόκολλο που επινοήθηκε για να λυθεί το πρόβλημα δρομολόγησης των βρόχων(rooting loop problem). Οι διαδρομές που είναι εγκατεστημένες βασίζονται σε συνεχή έλεγχο της κυκλοφορίας και είναι πάντοτε διαθέσιμες. Κάθε κόμβος διατηρεί έναν ή περισσότερους πίνακες που περιέχουν πληροφορίες για την τοπολογία όλων των κόμβων στο δίκτυο. Οι κόμβοι ενημερώνουν συνεχώς τους πινάκες ώστε να παρέχουν πάντοτε την τελευταία άποψη της τοπολογίας του δικτύου. Οι ανανεώσεις αυτές είναι τόσο συχνές που τα διαφημιστικά μηνύματα πρέπει να αποστέλλονται τακτικά ώστε να είναι βέβαιο ότι κάθε κόμβος μπορεί σχεδόν πάντα να βρει κάθε άλλο κόμβο στο δίκτυο. Τα δεδομένα που μεταδίδονται από τον κινητό κόμβο περιέχουν τον αύξων αριθμό, τη διεύθυνση προορισμού, το μέσο αριθμό βημάτων που απαιτούνται για τον προορισμό και την ακολουθία των πληροφοριών που έλαβε για τον προορισμό [17]. Εν ολίγοις το AODV είναι η «reactive» έκδοση του DSDV πρωτοκόλλου.

Η ζήτηση τώρα στο AODV για διαθέσιμο εύρος ζώνης είναι σημαντικά μικρότερη σε σχέση με τα proactive πρωτόκολλα μιας και το AODV δεν απαιτεί καθολικές περιοδικές διαφημίσεις. Παρέχει επίσης τη δυνατότητα για πολλαπλά βήματα (multi-hops), αυτόματη εκκίνηση (self-starting) και δυναμική δρομολόγηση (dynamic routing). Σε δίκτυα με μεγάλο αριθμό κινητών κόμβων το AODV είναι πολύ αποτελεσματικό δεδομένου ότι βασίζεται σε δυναμικές καταχωρήσεις των πινάκων των δρομολογίων στους ενδιάμεσους κόμβους. Το AODV επίσης ποτέ δεν παράγει βρόχους όπως δηλαδή δεν μπορεί να υπάρξει βρόχος στον πίνακα δρομολόγησης του κάθε κόμβου λόγω της έννοιας του αύξων αριθμού της ακολουθίας που έχει δανειστεί από το DSDV. Η ακολουθία αυτή των αριθμών χρησιμοποιείται ως «*γραμματόσημο χρόνου*» και επιτρέπει στους κόμβους να συγκρίνουν τις νέες πληροφορίες που έχουν για τους άλλους κόμβους στο δίκτυο. Το κύριο πλεονέκτημα του AODV είναι ότι χρησιμοποιείται η κορεσμένη διαδρομή αντί της συντομότερης[17].

Υιοθετώντας ένα συστηματικό τρόπο αναλύουμε τις επιθέσεις στις εμπιστευτικές πληροφορίες του πρωτόκολλου AODV. Εντοπίζοντας κατ 'αρχάς τους στόχους "κατάχρησης" (misuse goals) μιας εσωτερικής επίθεσης από έναν εισβολέα στη συνέχεια παραθέτουμε πώς αυτοί οι στόχοι μπορούν να επιτευχθούν με κακή χρήση της δρομολόγησης των μηνυμάτων. Οι στόχοι αυτοί της κατάχρησης παρατίθενται παρακάτω :

- *Διακοπή της διαδρομής (RD).* Η διακοπή της διαδρομής είτε διασπά μια υπάρχουσα διαδρομή ή αποτρέπει ένα νέο δρομολόγιο από την καθιέρωσή του.

- *Εισβολή της διαδρομής (RI).* Η εισβολή της διαδρομής σημαίνει ότι ένας εισβολέας προσθέτει ο ίδιος μια διαδρομή μεταξύ των δύο άκρων του καναλιού επικοινωνίας.

- *Κόμβος Απομόνωσης (NI).* Ο κόμβος απομόνωσης αναφέρεται στην παρεμπόδιση ενός δεδομένου κόμβου από την επικοινωνία με οποιονδήποτε άλλο κόμβο στο δίκτυο. Διαφέρει από τη διαδρομή διακοπής (RD) στο γεγονός ότι η διαδρομή διακοπής στοχεύει σε μια διαδρομή με δύο συγκεκριμένες παραμέτρους ενώ ο κόμβος απομόνωσης στοχεύει σε όλες τις πιθανές διαδρομές.

- *Κατανάλωση Πόρων (RC).* Η κατανάλωση πόρων αναφέρεται στην κατανάλωση του εύρους ζώνης επικοινωνίας ή στο χώρο αποθήκευσης του δικτύου σε μεμονωμένους κόμβους. Για παράδειγμα, ένας εισβολέας μπορεί να καταναλώσει το εύρος ζώνης του δικτύου, είτε να σχηματίσει μια κυκλική διαδρομή στο δίκτυο[10].

Για να διευκολυνθεί η ανάλυση ταξινομήθηκε περαιτέρω η κακή χρήση του πρωτοκόλλου AODV σε δύο κατηγορίες: στην **ατομική κατάχρηση** (atomic misuses) και στην **σύνθετη κατάχρηση** (compound misuses).Αρχικά η ατομική κατάχρηση εκτελείται από το χειρισμό ενός μηνύματος δρομολόγησης το οποίο δεν μπορεί να διαιρεθεί περαιτέρω. Αντίθετα, οι σύνθετες καταχρήσεις αποτελούνται από πολλαπλές ατομικές καταχρήσεις. Είναι εύκολο λοιπόν να αντιληφθούμε ότι η ατομική κατάχρηση μπορεί να χρησιμοποιηθεί ως δομικό στοιχείο των σύνθετων καταχρήσεων.

Όπως είπαμε η ατομική κατάχρηση είναι η «χειραγώγηση» ενός αδιαίρετου μηνύματος δρομολόγησης. Συγκεκριμένα διαιρούμε τις δράσεις της ατομικής κατάχρησης του πρωτοκόλλου AODV σε τέσσερις κατηγορίες:

- *Αποβολή (DR).* Ο επιτιθέμενος απλά καταστρέφει το μήνυμα δρομολόγησης.

- *Τροποποίηση και Εμπρός (MF).* Μετά την παραλαβή του μηνύματος δρομολόγησης ο εισβολέας τροποποιεί ένα ή περισσότερα πεδία στο μήνυμα και κατόπιν διαβιβάζει το μήνυμα στο γείτονά του (unicast) ή στους γείτονες του (broadcast).

- *Forge Απάντηση (FR).* Ο επιτιθέμενος στέλνει ένα μήνυμα σφυρηλάτησης (forge) σε απάντηση στο μήνυμα δρομολόγησης που έλαβε. Η forge απάντηση σχετίζεται κυρίως με την κακή χρήση των RREP μηνυμάτων τα οποία είναι σε απάντηση των RREQ μηνυμάτων.

- *Ενεργός Forge (AF).* Ο επιτιθέμενος στέλνει ένα μήνυμα δρομολόγησης forge χωρίς να λάβει καμία απάντηση που να σχετίζεται με το μήνυμα που έστειλε[10].

Εκ πρώτης όψεως οι σύνθετες καταχρήσεις φαίνεται να είναι απλές συνθέσεις ατομικών καταχρήσεων. Ωστόσο από κάποιες συνθέσεις των ατομικών καταχρήσεων γίνονται πιο ισχυρές επιθέσεις λόγω των αλλαγών στον αριθμό των μηνυμάτων. Για παράδειγμα, εάν ένας εισβολέας μεταδίδει τακτικά μηνύματα RREQ με ψευδείς

πληροφορίες στη γειτονιά ενός κόμβου θύματος, ο εισβολέας μπορεί να αποτρέψει επιτυχώς τον κόμβο του θύματος από τη λήψη μηνυμάτων[10].

Ατομική Κατάχρηση (Atomic Misuses): Στην παρακάτω ανάλυσή χρησιμοποιούμε ένα απλό σχήμα ονοματολογίας για τον εντοπισμό της ατομικής κατάχρησης το οποίο συνδυάζει το τύπο τους μηνύματος δρομολόγησης και την δράση της ατομικής κατάχρησης. Συγκεκριμένα, κάθε ατομική κατάχρηση ονομάζεται με τη μορφή «*MessageType*» δράσης, πράγμα που σημαίνει ότι ένας εισβολέας εφαρμόζει τη «δράση» σε ένα μήνυμα δρομολόγησης του τύπου «MessageType». Για συντομία, χρησιμοποιούμε τις συντομογραφίες που αναλύσαμε προηγουμένως οι οποίες εκπροσωπούν τις δράσεις της ατομικής κατάχρησης. Για παράδειγμα η δράση «RREP DR» αντιπροσωπεύει το γεγονός ότι ένας εισβολέας καταστρέφει (DR) ένα μήνυμα RREP. Χρησιμοποιούμε επίσης τα ονόματα με τη μορφή «*MessageType Action Goal*» η οποία εκπροσωπεί την προσπάθεια του εισβολέα να επιτευχθεί ο «*στόχος*» από την εφαρμογή της δράσης σε ένα μήνυμα δρομολόγησης του τύπου «MessageType». Για παράδειγμα, «RREP DR RD» αντιπροσωπεύει το γεγονός ότι ένας εισβολέας επιχειρεί να διαταράξει (RD) μια διαδρομή με τη ρίψη (DR) ένα μηνύματος RREP[10].

Ατομική Κατάχρηση RREQ Μηνυμάτων

Ο παρακάτω πίνακας συνοψίζει την ατομική κατάχρηση ενός μηνύματος RREQ. Η ατομική κατάχρηση δράσης μιας Forge απάντησης δεν ισχύει για RREQ μηνύματα δεδομένου ότι τα μηνύματα RREQ δεν χρησιμοποιούνται για να απαντήσουν σε οποιαδήποτε άλλη δρομολόγηση μηνυμάτων.

Ατομική Κατάχρηση	Τροποποίηση της διαδρομής	Εισβολή στην διαδρομή	Απομόνωση Κόμβου	Κατανάλωση πόρων
RREQ_DR	Ναι	Όχι	Όχι	Όχι
RREQ_MF	Ναι	Ναι	Εν μέρει	Όχι
RREQ_AF	Ναι	Ναι	Εν μέρει	Όχι

Εικόνα 14 Πίνακας Ατομικής κατάχρησης & Στόχων RREQ μηνυμάτων

Η ατομική κατάχρηση «*RREQ DR*» αναφέρεται στην πτώση του ληφθέντος μηνύματος RREQ. Εάν ένας εισβολέας πραγματοποιεί τέτοιες επιθέσεις στο σύνολο των μηνυμάτων RREQ που δέχεται, αυτό το είδος της καταστρατήγησης είναι ισοδύναμο στο να μην υπάρχει ο επιτιθέμενος κόμβος στο δίκτυο. Ο εσωτερικός εισβολέας μπορεί επίσης να καταστρέφει (drop) επιλεκτικά RREQ μηνύματα. Οι επιτιθέμενοι που ξεκινούν μια τέτοια κατάχρηση έχουν χαρακτήρα παρόμοιο με το εγωιστικούς κόμβους.

Η ατομική κατάχρηση «*RREQ MF*» αναφέρεται στην ατομική κατάχρηση με την οποία ένας εσωτερικός εισβολέας τροποποιεί ένα ή περισσότερα πεδία σε ένα μήνυμα RREQ που λαμβάνει και στη συνέχεια εκπέμπει το τροποποιημένο μήνυμα RREQ. Ο παρακάτω πίνακας παραθέτει τα πεδία των RREQ μηνυμάτων τα οποία ένας εισβολέας μπορεί να τροποποιήσει, καθώς και τις πιθανές τροποποιήσεις[10].

Πεδίο Μηνύματος RREQ	Τροποποιήσεις
Τύπος	Αλλαγή του τύπου μηνύματος
RREQ ID	Αύξηση του ώστε το ψευδές RREQ μήνυμα να γίνει αποδεκτό ή μείωση του ώστε το RREQ μήνυμα να μην γίνει δεκτό.
Μετρητής Νημάτων	Μείωση του ώστε να αναβαθμιστούν οι αντίστροφοι πίνακες δρομολόγησης των άλλων κόμβων ή αύξηση του ώστε να καταστεί άκυρη η αναβάθμιση.
IP Προορισμού	Αλλαγή με άλλη IP.
Αριθμός Ακολουθίας Προορισμού	Αύξηση του ώστε να αναβαθμιστούν οι (forward) πίνακες δρομολόγησης των άλλων κόμβων ή μείωση του ώστε να κατασταλεί η αναβάθμιση.
IP Πηγής	Αλλαγή με άλλη IP.
Αριθμός Ακολουθίας Πηγής	Αύξηση του ώστε να αναβαθμιστούν οι αντίστροφοι πίνακες δρομολόγησης των άλλων κόμβων ή μείωση του ώστε να καταστεί άκυρη η αναβάθμιση.
Flag	Αναστροφή

Εικόνα 15 Ενδεχόμενες τροποποιήσεις των πεδίων σε ένα RREQ μήνυμα.

Αρκετά πεδία έχουν άμεσες συνέπειες για την ασφάλεια κάθε φορά που τροποποιούνται. Το πεδίο «RREQ ID» μαζί με τη διεύθυνση IP προέλευσης προσδιορίζει με μοναδικό τρόπο την νεότητα ενός RREQ μηνύματος. Δεδομένου ότι ένας κόμβος δέχεται μόνο το πρώτο αντίγραφο ενός μηνύματος RREQ αυξημένο με το πεδίο RREQ ID μαζί με τη διεύθυνση IP προέλευσης αυτό μπορεί να εγγυηθεί ότι το ψεύτικο μήνυμα RREQ θα γίνει αποδεκτό από τους άλλους κόμβους.

Για να διασφαλιστεί η ελευθερία του βρόχου στο πρωτόκολλο AODV μετά τη λήψη ενός μηνύματος RREQ ο κόμβος ενημερώνει αντίστροφα τον πίνακα δρομολόγησης μόνο εάν η πηγή ακολουθίας του αριθμού του πεδίου στο μήνυμα RREQ είναι μεγαλύτερη από ότι στον πίνακα της δρομολόγησης ή οι αριθμοί ακολουθίας της πηγής είναι ίσοι αλλά το άλμα (hop) του τομέα στο μήνυμα RREQ είναι μικρότερο από ότι στον πίνακα δρομολόγησης. Ο εσωτερικός εισβολέας μπορεί επίσης να αλλάξει αυτούς τους τομείς ώστε να επηρεάσει τους πίνακες δρομολόγησης άλλων κόμβων[10].

Ένας ενδιάμεσος κόμβος ή ένας κόμβος "πηγής" ενημερώνει προς τα εμπρός του τον πίνακα δρομολόγησης αν ο αριθμός ακολουθίας προορισμού στο μήνυμα RREP είναι μεγαλύτερος από εκείνο του πίνακα δρομολόγησης ή οι αριθμοί ακολουθίας προορισμού είναι ίδιοι αλλά ο αριθμός των αλμάτων στο μήνυμα RREP αυξημένος κατά 1 είναι μικρότερος από εκείνο του πίνακα δρομολόγησης. Ο εσωτερικός εισβολέας μπορεί να αυξήσει τον αριθμό ακολουθίας ή να μειώσει τον αριθμό των αλμάτων σε forge μήνυμα RREQ ώστε να ενημερώσει τους πίνακες δρομολόγησης άλλων κόμβων ή να μειώσει τους αριθμούς ακολουθίας ή να αυξήσει το όριο αλμάτων για να αναιρέσει ένα μήνυμα RREQ.

Όταν ένας κόμβος ενημερώνει τον πίνακα δρομολόγησης του, το επόμενο άλμα στην είσοδο της διαδρομής αποδίδεται στον κόμβο από τον οποίο λαμβάνει το μήνυμα

RREQ. Ο εσωτερικός εισβολέας μπορεί να χειριστεί τη διεύθυνση IP προέλευσης στην κεφαλίδα IP για να αλλάξει την αντίστροφη διαδρομή.

Και οι δύο δράσεις «RREQ DR» και «RREQ MF» πρέπει να ενεργοποιούνται από ένα εισερχόμενο μήνυμα RREQ. Αντίθετα, ένας εσωτερικός εισβολέας μπορεί να εκτελέσει μια κατάχρηση RREQ AF για να σφυρηλατήσει (forge) ένα μήνυμα RREQ χωρίς να λαμβάνει ένα μήνυμα RREQ. Ο εσωτερικός εισβολέας μπορεί να χρειαστεί να συλλέξει κάποιες απαραίτητες πληροφορίες για να σφυρηλατήσει τα RREQ μηνύματα (π.χ. μέσω της ακρόασης της κυκλοφορίας). Θεωρητικά, ο εισβολέας μπορεί να σφυρηλατήσει οποιοδήποτε πεδίο σε ένα μήνυμα RREQ[10].

Τώρα θα εξετάσουμε **την ατομική κατάχρηση ενός μηνύματος RREQ, RREQ_MF_NI** με την οποία ένας εσωτερικός επιτιθέμενος εμποδίζει έναν κόμβο-θύμα από τη λήψη πακέτων δεδομένων από άλλους κόμβους για ένα μικρό χρονικό διάστημα. Ο εισβολέας μπορεί να κάνει τις ακόλουθες τροποποιήσεις όταν λάβει ένα μήνυμα RREQ από τον κόμβο θύμα:

- Αύξηση του RREQ ID με ένα μικρό αριθμό.
- Αντικατάσταση της διεύθυνσης IP προορισμού με μια μη πραγματική διεύθυνση IP.
- Αύξηση του αριθμού της πηγής τουλάχιστον κατά ένα.
- Ρύθμιση της διεύθυνσης IP προέλευσης στην κεφαλίδα IP με μια μη πραγματική διεύθυνση IP.

Ο επιτιθέμενος στη συνέχεια εκπέμπει το πλαστό μήνυμα. Όταν οι γείτονες του εισβολέα λαμβάνουν το forge μήνυμα RREQ ενημερώνουν τον επόμενο κόμβο προς τον κόμβο-πηγή για το μη υπάρχον κόμβο δεδομένου ότι το ψεύτικο μήνυμα RREQ έχει μεγαλύτερο αριθμό ακολουθίας πηγής. Λόγω της μη-υπαρκτής IP διεύθυνσης προορισμού το ψεύτικο μήνυμα μπορεί να μεταδοθεί στον «απώτατο» κόμβο στο ad-hoc δίκτυο. Όταν οι άλλοι κόμβοι θέλουν να στείλουν πακέτα δεδομένων προς τον κόμβο-πηγή θα χρησιμοποιήσουν τις διαδρομές που καθορίζονται από τα εικονικά μηνύματα RREQ και τα πακέτα δεδομένων θα μειωθούν λόγω των μη-υπαρκτών κόμβων.

Αυτή η ατομική κατάχρηση μπορεί να αποτρέψει έναν κόμβο-θύμα από τη λήψη πακέτων δεδομένων για ένα μικρό χρονικό διάστημα. Ωστόσο, δεν μπορεί να απομονώσει πλήρως τον κόμβο θύμα λόγω του τοπικού μηχανισμού επιδιόρθωσης στο πρωτόκολλο AODV. Οι άλλοι κόμβοι θα ξεκινήσουν ένα νέο γύρο ανακάλυψης της διαδρομής εφόσον διαπιστωθεί ότι τα πακέτα δεδομένων δεν μπορούν να παραδοθούν με επιτυχία. Επιπλέον, ο κόμβος-θύμα μπορεί ακόμη να είναι σε θέση να στείλει τα πακέτα δεδομένων σε άλλους κόμβους.

Πολλές από τις κακές χρήσεις της ατομικής κατάχρησης των RREQ μηνυμάτων χρησιμοποιούν RREQ μηνύματα για να προσθέσουν καταχωρήσεις στους πίνακες δρομολόγησης των άλλων κόμβων. Οι ενδείξεις αυτές είναι διαφορετικές από εκείνες που θεσπίζονται μέσω της κανονικής ανταλλαγής των RREQ και RREP μηνυμάτων. Ειδικότερα, αν η διάρκεια ζωής αυτών των καταχωρήσεων τεθεί σε προκαθορισμένη τιμή οι εισβολείς για να κάνουν τέτοιες αποτελεσματικές καταχωρήσεις θα πρέπει να ξεκινήσουν την ατομική κατάχρηση περιοδικά[10].

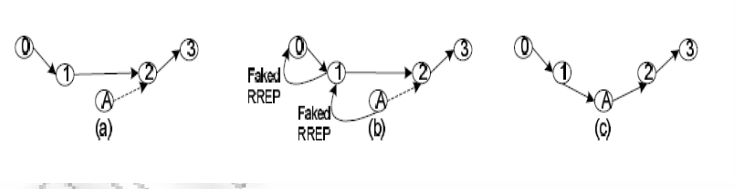
Ατομικές καταχρήσεις Route Reply (RREP) Μηνυμάτων

Η παρακάτω εικόνα συνοψίζει την ατομική κατάχρηση ενός μηνύματος RREP και εάν μπορούν να επιτευχθούν οι στόχοι της κατάχρησης. Η παραδοχή της ατομικής κατάχρησης των RREP μηνυμάτων είναι ότι ο εσωτερικός επιτιθέμενος πρέπει να είναι ήδη σε αντίστροφη διαδρομή η οποία να περιλαμβάνει έναν κόμβο-θύμα, έτσι ώστε να μπορεί να λάβει ένα μήνυμα RREP ή RREQ ή να στείλει ένα πλαστό RREP μέσω μερικών άλλων κόμβων. Λόγω αυτού του περιορισμού οι περισσότερες ατομικές καταχρήσεις των RREP μηνυμάτων συμπεριλαμβανομένων των RREP_DR και RREP _MF έχουν περιορισμένο αντίκτυπο.

Ατομική Κατάχρηση	**Τροποποίηση της διαδρομής**	**Εισβολή στην διαδρομή**	**Απομόνωση Κόμβου**	**Κατανάλωση πόρων**
RREQ_DR	Ναι	Όχι	Όχι	Όχι
RREQ_MF	Ναι	Ναι	Όχι	Όχι
RREQ_FR	Ναι	Ναι	Όχι	Όχι
RREQ_AF	Ναι	Ναι	Όχι	Ναι

Εικόνα 16 Πίνακας Ατομικής κατάχρησης & Στόχων RREP μηνυμάτων

Η ατομική κατάχρηση RREP_FR είναι ειδική για RREP μηνύματα. Αναφέρεται στην κατάχρηση στην οποία ο εισβολέας δημιουργεί ένα μήνυμα RREP σε απάντηση σε ένα μήνυμα RREQ. Για παράδειγμα, μετά την παραλαβή ενός μηνύματος RREQ, ένας εσωτερικός εισβολέας μπορεί να σφυρηλατήσει (forge) ένα μήνυμα RREP σαν να είχε μια αρκετά νέα διαδρομή προς τον κόμβο προορισμού. Για να καταστείλει τα άλλα νόμιμα μηνύματα RREP τα οποία ο κόμβος-πηγή μπορεί να λάβει από άλλους κόμβους, ο εισβολέας μπορεί να σφυρηλατήσει (forge) ένα ψεύτικο μήνυμα RREP αυξάνοντας τον αριθμό ακολουθίας προορισμού. Επομένως ένας εισβολέας μπορεί να διαταράξει τη διαδρομή μεταξύ του κόμβου-θύμα με ένα συγκεκριμένο προορισμό ή να εισβάλει στην διαδρομή μεταξύ άλλων με την κατάργηση των εναλλακτικών διαδρομών[10].



Εικόνα 17 Ένας εισβολέας εισβάλλει σε μια διαδρομή με την αποστολή ενός ενεργού faked RREP μηνύματος.

Μια ενδιαφέρουσα ατομική κατάχρηση είναι η «RREP_AF_RI». Εάν ένας εσωτερικός επιτιθέμενος έχει δρομολόγια τόσο για την πηγή όσο και για τον προορισμό μιας υπάρχουσας οδού (όπως φαίνεται στην παραπάνω εικόνα (α)), μπορεί να εισβάλει στη διαδρομή με την αποστολή ενός faked RREP μηνύματος στον κόμβο πηγή. Στην παραπάνω εικόνα υποθέτουμε ότι ο κόμβος Α είναι ο επιτιθέμενος κόμβος ο οποίος έχει ήδη ένα δρομολόγιο προς τους κόμβους 0 και 3 αντίστοιχα. Ο κόμβος Α μπορεί να σφυρηλατήσει (forge) ένα μήνυμα RREP ως εξής:

1. Ρυθμίζει την IP πηγής στον κόμβο 0.
2. Ρυθμίζει την IP προορισμού προς τον κόμβο 3.
3. Ρυθμίζει τον αύξοντα αριθμό της ακολουθίας προορισμού στον κόμβο 3 τουλάχιστον κατά μια μονάδα
4. Ορίζει την επικεφαλίδα της IP πηγής προς τον κόμβο 2.

5. Ρυθμίζει την IP προορισμού στην επικεφαλίδα στον κόμβο 1.

Ο κόμβος Α στέλνει πλαστά μήνυμα RREP στον κόμβο 1 ο οποίος με την σειρά του διαβιβάζει το faked RREP μήνυμα στον κόμβο 0 (εικόνα (b)). Όταν οι κόμβοι 0 και 1 λαμβάνουν τα εικονικά RREP μηνύματα ενημερώνουν τον αύξοντα αριθμό του κόμβου 3 στους πίνακες δρομολόγησης τους για τον αύξοντα αριθμό προορισμού στο faked RREP μήνυμα. Ο κόμβος 0 θα εξακολουθήσει να χρησιμοποιεί τον κόμβο 1 ως το επόμενο άλμα (hop) στον κόμβο 3 αλλά ο κόμβος 1 θα ενημερώνει τον κόμβο Α ως το επόμενο άλμα στον κόμβο 3. Εδώ πρέπει να σημειωθεί ότι ο κόμβος Α έχει ήδη ένα δρομολόγιο προς τον κόμβο 3. Ως αποτέλεσμα, ο κόμβος Α γίνεται με επιτυχία κομμάτι της διαδρομής από τον κόμβο 0 έως κόμβο 3 (εικόνα (c)).

Ατομικές Καταχρήσεις Route Error (RERR) Μηνυμάτων

Η παρακάτω εικόνα συνοψίζει τα τρία είδη της ατομικής κακής χρήσης των RERR μηνυμάτων και τους στόχους της κατάχρησης τα οποία μπορούν να επιτύχουν. Η δράση της κατάχρησης των forge απαντήσεων δεν ισχύει για τα μηνύματα RERR δεδομένου ότι τα μηνύματα RERR χρησιμοποιούνται για να απαντήσουν σε οποιαδήποτε δρομολόγηση μηνυμάτων.

Ατομική Κατάχρηση	**Τροποποίηση της διαδρομής**	**Εισβολή στην διαδρομή**	**Απομόνωση Κόμβου**	**Κατανάλωση πόρων**
RREQ_DR	Ναι	Όχι	Όχι	Όχι
RREQ_MF	Ναι	Όχι	Όχι	Ναι
RREQ_AF	Ναι	Όχι	Όχι	Ναι

Εικόνα 18 Πίνακας Ατομικής κατάχρησης & Στόχων RERR μηνυμάτων

Η ατομική κατάχρηση "RERR DR" έχει περιορισμένο αντίκτυπο στο δίκτυο που οφείλετε στις καθυστερήσεις για τον εντοπισμό των σφαλμάτων της διαδρομής δεδομένου ότι οι κόμβοι θα ανακαλύψουν τελικά τα προβληματικά δρομολόγια και θα δημιουργήσουν νέες διαδρομές[10].

Για να διαπιστωθεί ποιοι γείτονες θα πρέπει να λάβουν ένα μήνυμα RERR κάθε κόμβος διατηρεί μια "λίστα πρόδρομο (precursor list)" των γειτόνων του για κάθε διαδρομή. Όταν ανιχνευθεί μια προβληματική σύνδεση (broken link) ο κόμβος στέλνει ένα μήνυμα RERR σε όλους τους κόμβους που έχει στην «λίστα πρόδρομο». Για την έναρξη της κατάχρησης RERR_MF ένας εισβολέας μπορεί να τροποποιήσει το RERR μήνυμα αφού λάβει ένα μήνυμα RERR και στείλει το πλαστό μήνυμα RERR στους γείτονες του από την «λίστα πρόδρομο». Στον παρακάτω πίνακα παρατίθενται τα πεδία των RERR μηνυμάτων τα οποία ο εισβολέας μπορεί να χειριστεί. Μερικές φορές επίσης, ο εισβολέας μπορεί να τροποποιήσει τις διευθύνσεις IP στην επικεφαλίδα IP.

Πεδίο Μηνύματος RERR	**Τροποποιήσεις**
Τύπος	Αλλαγή της τιμής του τύπου
Dest Count	Τροποποίηση του σύμφωνα με τον αριθμό των μη προσιτών προορισμών που περιέχονται στο RERR μήνυμα.
Μη προσιτή IP προορισμού	Αλλαγή με άλλη IP.
Μη Προσιτός Αριθμός Ακολουθίας Προορισμού	Αύξηση του ώστε να αναβαθμιστεί ο πίνακας δρομολόγησης των άλλων κόμβων ή μείωση του ώστε να κατασταλεί η εισαγωγή.
Επιπρόσθετη Μη προσιτή IP προορισμού (αν χρειαστεί)	Προσθήκη νέας IP προορισμού η οποία να είναι ακόμα προσιτή.
Επιπρόσθετος Μη Προσιτός Αριθμός Ακολουθίας Προορισμού (αν χρειαστεί)	Αύξηση του για την αναβάθμιση του πίνακα δρομολόγησης των άλλων κόμβων ή μείωση του για να κατασταλεί η εισαγωγή.

Εικόνα 19 Πιθανές τροποποιήσεις των πεδίων των RERR μηνυμάτων

Σύνθετες Καταχρήσεις (Compound Misuses)

Ένας ή περισσότεροι επιτιθέμενοι μπορούν να συνδυάζουν μια σειρά από ατομικές καταχρήσεις και ενδεχομένως η κανονική χρήση των μηνυμάτων δρομολόγησης με οποιαδήποτε σειρά να ξεκινήσει σύνθετες καταχρήσεις. Για παράδειγμα, ένας εισβολέας μπορεί να εκκινήσει επανειλημμένα το ίδιο είδος της ατομικής κατάχρησης ώστε να καταστήσει έτσι την επίμονη του. Ως άλλο παράδειγμα ένας εισβολέας μπορεί να ξεκινήσει κάποιες πρώιμες ατομικές ή σύνθετες καταχρήσεις ώστε να προετοιμαστεί για κάποιες αργότερα. Ένα σημαντικό ζήτημα εδώ είναι να κατανοηθεί ότι οι σύνθετες καταχρήσεις μπορούν να χρησιμοποιηθούν ως “δομικές μονάδες” όλο και πιο σύνθετων επιθέσεων.

Για λόγους ευκολίας, θα επεκτείνουμε το σχήμα ονομασίας της ατομικής κατάχρησης η οποία χαρακτηρίζει την κακή χρήση των σύνθετων και ιδίου τύπου ατομικών καταχρήσεων. Συγκεκριμένα προστέθηκε στην αντίστοιχη ατομική κατάχρηση ένα «s» μετά από το είδος της δρομολόγησης στο μήνυμα που γίνεται η κατάχρηση. Για παράδειγμα ένα μήνυμα RREQs AF δηλώνει ότι ένας εισβολέας σφυρηλατεί (forge) ενεργά πολλαπλά μηνύματα RREQ.

Παρατηρούμε ότι το μεγαλύτερο μέρος των ατομικών καταχρήσεων που απευθύνονται σε διακοπή των υπηρεσιών μπορεί να δημιουργήσει μόνο προσωρινές επιπτώσεις που οφείλονται στον τοπικό μηχανισμό επιδιόρθωσης που παρατηρείται συχνά στα κινητά ad hoc πρωτόκολλα δρομολόγησης. Έτσι για να καταστεί ο αντίκτυπος αυτών των ανθεκτικών καταχρήσεων ένας εισβολέας θα πρέπει να επαναλάβει την ατομική κατάχρηση τακτικά[10].

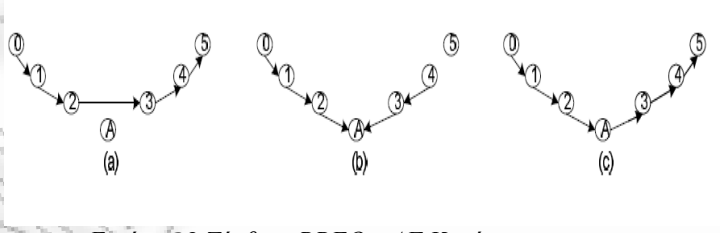
Μια άλλη κατηγορία σύνθετων καταχρήσεων είναι όταν ένας εισβολέας μπορεί να επιτύχει ορισμένους στόχους του μέσω της σύνθετης κατάχρησης και με προγραμματιζόμενό συνδυασμό κάποιων ατομικών καταχρήσεων.

Ένα παράδειγμα έχει ως εξής: Ένας εσωτερικός εισβολέας μπορεί να εισβάλει σε μια διαδρομή μέσα μια σύνθετη RREQs_AF κατάχρηση. Παρατηρώντας την παρακάτω εικόνα (a) υποθέτουμε ότι οι κόμβοι 0 έως 5 είναι φυσιολογικοί κόμβοι και ο κόμβος Α είναι ο κόμβος "εισβολέας". Περαιτέρω υποθέσουμε ότι υπάρχει μια διαδρομή από τον κόμβο 0 έως τον κόμβο 5. Ο επιτιθέμενος στον κόμβο Α μπορεί να σφυρηλατήσει (forge) ένα μήνυμα RREQ ως εξής:

1. Ρύθμιση της διεύθυνσης IP προέλευσης προς τον κόμβου 5.
2. Ρύθμιση της διεύθυνσης IP προορισμού προς τον κόμβος 0 .
3. Ρύθμιση του αύξοντα αριθμού πηγής με έναν αριθμό μεγαλύτερο από αυτόν της ακολουθίας του κόμβου 5.
4. Ρύθμιση της διεύθυνσης IP της πηγής στην κεφαλίδα IP για τον κόμβο Α. Ο κόμβος Α έπειτα μεταδίδει το ψεύτικό μήνυμα RREQ. Μετά την παραλαβή αυτού του μηνύματος οι κόμβοι 2 και 3 καθορίζουν τον κόμβο Α ως το επόμενο βήμα (hop) στον κόμβο 5 όπως φαίνεται στην παρακάτω εικόνα (b).

Για την περαιτέρω καθιέρωση της διαδρομής από τον κόμβο Α στον κόμβο 5 ο εισβολέας μπορεί να δημιουργήσει το δεύτερο μήνυμα RREQ ως εξής:

1. Ρύθμιση της διεύθυνσης IP προέλευσης προς τον κόμβο Α.
2. Ρύθμιση της διεύθυνσης IP προορισμού προς τον κόμβο 5.
3. Ορισμός του αριθμού της ακολουθίας προορισμού με έναν αριθμό μεγαλύτερο από την τρέχουσα ακολουθία του αριθμού του κόμβου 5 .
4. Ρύθμιση της διεύθυνσης IP προέλευσης στην επικεφαλίδα IP προς τον κόμβο Α. Ο κόμβος Α μπορεί να μεταδίδει στη συνέχεια αυτό το μήνυμα RREQ. Το μήνυμα αυτό θα βοηθήσει τον κόμβο Α να καθιερώσει ένα δρομολόγιο προς τον κόμβο 5, όπως φαίνεται στο παρακάτω σχήμα (c).



Εικόνα 20 Σύνθετη RREQs_AF Κατάχρηση

Όπως αναφέρθηκε παραπάνω, ένας ή περισσότεροι επιτιθέμενοι μπορούν να συνθέσουν τις επιθέσεις από αυθαίρετο συνδυασμό ατομικών ή και σύνθετων καταχρήσεων. Ειδικότερα οι επιτιθέμενοι μπορούν να χρησιμοποιούν διαφορετικές καταχρήσεις για να αλληλοσυμπληρώνονται. Για παράδειγμα το μήνυμα RREQs_AF είναι αποτελεσματικό στο να προλαμβάνει τον κόμβο-θύμα και να λαμβάνει μηνύματα από άλλους κόμβους και το μήνυμα RREP_AF είναι αποτελεσματικό ώστε να προλαμβάνει άλλους κόμβους από την παραλαβή μηνυμάτων από τον κόμβο-θύμα. Με το συνδυασμό τους από κοινού ο επιτιθέμενος ή οι επιτιθέμενοι μπορούν να απομονώσουν με επιτυχία έναν κόμβο. Επιπλέον ένας ή περισσότεροι επιτιθέμενοι μπορούν να χρησιμοποιούν ορισμένες καταχρήσεις ή κανονικά

μηνύματα δρομολόγησης ώστε να προετοιμαστούν τις μετέπειτα καταχρήσεις. Για παράδειγμα, όλες οι σχετικές RREP καταχρήσεις απαιτούν μια διαδρομή με συμμετοχή τόσο του εισβολέα όσο και του κόμβου-θύμα. Για να προετοιμαστεί για μια τέτοια κατάχρηση ένας εισβολέας μπορεί να χρησιμοποιήσει ένα κανονικό μήνυμα RREQ ή μια ατομική κατάχρηση (π.χ., RREQ AF) για τη δημιουργία των απαιτούμενων διαδρομών[10].

Στο **ARAN** (Authenticated Routing for Ad-hoc Networks) το οποίο είναι ένα on-demand πρωτόκολλο δρομολόγησης που ανιχνεύει και προστατεύει από κακόβουλες ενέργειες που πραγματοποιούνται από τρίτους. Αυτό το πρωτόκολλο εισάγει την ταυτοποίηση (authentication), την ακεραιότητα (integrity) του μηνύματος και τη μη αποποίηση ευθυνών (non-repudation) ως μέρος μιας ελάχιστης πολιτικής ασφάλειας. Αν και το ARAN έχει σχεδιαστεί για την ενίσχυση της adhoc ασφάλειας εξακολουθεί να είναι το *"ανοσοποιητικό σύστημα"* ώστε να προβεί στην καταστολή της επίθεσης[26].

Συγκεκριμένα το ARAN απαιτεί τη χρήση ενός αξιόπιστου πιστοποιητικού από κάποιο διακομιστή T (server). Πριν την είσοδο στο ad hoc δίκτυο, κάθε κόμβος πρέπει να ζητήσει ένα πιστοποιητικό υπογεγραμμένο από τον διακομιστή T. Η βεβαίωση περιέχει την IP διεύθυνση του κόμβου, το δημόσιο κλειδί του, μια χρονική σήμανση (timestamp) για την χρονική στιγμή που το πιστοποιητικό δημιουργήθηκε και μια χρονική διάρκεια μετά την οποία το πιστοποιητικό λήγει μαζί με την υπογραφή του διακομιστή T. Όλοι οι κόμβοι υποτίθεται ότι θα διατηρούν έγκυρα πιστοποιητικά με τον αξιόπιστο διακομιστή και πρέπει να γνωρίζουν το δημόσιο κλειδί του διακομιστή T[2].

Ο πρωταρχικός στόχος του πρωτοκόλλου ARAN είναι να βεβαιωθεί στην πηγή ότι το πακέτο έφτασε στον προορισμό. Όπως και με οποιοδήποτε ασφαλές σύστημα που βασίζεται στα κρυπτογραφικά πιστοποιητικά, το βασικό ζήτημα ανάκλησης (key revocation) θα πρέπει να αντιμετωπιστεί προκειμένου να βεβαιωθεί ότι όταν θα λήξει ή θα ανακληθεί το πιστοποιητικό δεν θα επιτρέπετε στον κάτοχο του να έχει πρόσβαση στο δίκτυο. Στο Aran όταν ένα πιστοποιητικό πρέπει να ανακληθεί ο έμπιστος διακομιστής στέλνει ένα μήνυμα προς την adhoc ομάδα που ανακοινώνει την ανάκληση του πιστοποιητικού. Κάθε κόμβος που λαμβάνει αυτό το μήνυμα, το μεταδίδει στους γείτονές του. Τα μηνύματα αυτά της ανάκλησης πρέπει να αποθηκευτούν μέχρι το πιστοποιητικό να ήξει κανονικά. Κάθε γείτονας του κόμβου με την ανάκληση πιστοποιητικού πρέπει να αλλάξει την δρομολόγηση του όπου είναι απαραίτητο ώστε να αποφευχθεί η μετάδοση μέσω μη εμπίστων κόμβων. Η μέθοδος αυτή δεν είναι και πολύ ασφαλής.[2]

Σε ορισμένες περιπτώσεις ένας μη-έμπιστος κόμβος του οποίου το πιστοποιητικό ανακαλείται μπορεί να είναι η μόνη σύνδεση μεταξύ των δύο τμημάτων σε ένα ad hoc δίκτυο. Στην περίπτωση αυτή ο κόμβος αυτός ενδέχεται να μην διαβιβάσει την ανακοίνωση της ανάκλησης για το πιστοποιητικό του με αποτέλεσμα την κατάτμηση του δικτύου και οι κόμβοι που έχουν λάβει την ειδοποίηση ακύρωσης δεν θα προωθούν τα μηνύματα τους μέσω του μη έμπιστου κόμβου ενώ όλοι οι άλλοι κόμβοι θα εξαρτώνται από αυτόν για να επικοινωνήσουν με το υπόλοιπο δίκτυο. Αυτό διαρκεί μόνο για όσο διάστημα το πιστοποιητικό του μη έμπιστου κόμβου θα ισχύει ή μέχρι ο κόμβος αυτός να μην είναι πλέον η μόνη σύνδεση μεταξύ των δύο διαχωρισμών του δικτύου. Από την στιγμή που η ανάκληση του πιστοποιητικού έχει

λήξει, ο μη έμπιστος κόμβος δεν είναι σε θέση να ανανεώσει το πιστοποιητικό του και δρομολόγηση σε αυτόν τον κόμβο παύει να υφίσταται. [2]

Το **ARIANDE** είναι και αυτό ένα on-demand ασφαλές adhoc πρωτόκολλο δρομολόγησης που βασίζεται στο DSR το οποίο υλοποιεί υψηλής απόδοσης συμμετρική κρυπτογραφία. Παρέχει από σημείο σε σημείο επικύρωση μιας διαδρομής χρησιμοποιώντας μηνύματα του πρωτοκόλλου MAC και ένα κοινό κλειδί μεταξύ των δύο επικοινωνούντων μερών[26].

Το πρωτόκολλο ARIANDE χρειάζεται κάποιο μηχανισμό για το bootstrap (παρουσιάστηκε από τον Efron το 1979 ως μια μη παραμετρική μέθοδο εκτίμησης της τυπικής απόκλισης εκτιμητών) των αυθεντικών κλειδιών που απαιτούνται από το πρωτόκολλο. Ειδικότερα, κάθε κόμβος χρειάζεται ένα κοινό μυστικό κλειδί ((K_s, D) το οποίο είναι το κλειδί μεταξύ μιας πηγής S και ενός προορισμού D) με κάθε κόμβο επικοινωνίας υψηλότερου επίπεδου, ένα αυθεντικό κλειδί TESLA για κάθε κόμβο του δικτύου και ένα αυθεντικό «Route Discovery Chain» δηλαδή ένα στοιχείο για κάθε κόμβο για τον οποίο αυτός ο κόμβος θα διαβιβάσει τα RREQ μηνύματα[2].

Το πρωτόκολλο είναι ευάλωτο σε έναν ενεργό εισβολέα (1-1) που πραγματοποιεί επιθέσεις κατά μήκος της διαδρομής που έχει ανακαλυφθεί. Επίσης ένας ενεργός εισβολέας μπορεί να επιχειρήσει να υποβαθμίσει τα on-demand πρωτόκολλα δρομολόγησης με την κατ επανάληψη κίνηση της «Ανακάλυψης της Διαδρομής» (Route Discovery). Σε ένα αίτημα ανακάλυψης μιας διαδρομής ο κάθε κόμβος θέλει τον έλεγχο της ταυτότητας κάθε κόμβου στην λίστα των κόμβων ώστε να εκτελέσει την λειτουργία «Route Reply». Σε αυτή την επίθεση, ένας εισβολέας στέλνει πακέτα αναζήτησης της διαδρομής (Route Request) τα οποία "πλημμυρίζουν" όλο το δίκτυο. Στο πρωτόκολλο Ariadne το αιτήματα Route Request δεν επικυρώνονται μέχρι να φθάσουν στο στόχο τους, επιτρέποντας έτσι σε έναν ενεργό εισβολέα να πλημμυρίσει ολόκληρο το δίκτυο με τέτοια αιτήματα[6].

Το ARIANDE αντιμετωπίζει τις επιθέσεις που πραγματοποιούνται από κακόβουλους κόμβους οι οποίοι τροποποιούν και κατασκευάζουν πληροφορίες δρομολόγησης και τις επιθέσεις που χρησιμοποιούν πλαστοπροσωπία. Προστατεύεται επίσης από επιθέσεις πλημμύρας των RREQ πακέτων που θα μπορούσαν να οδηγήσουν σε επιθέσεις δηλητηρίασης της Cache. Τέλος το ARIANDE είναι άτρωτο από την επίθεση σκουληκότρυπας μόνο στην προηγμένη έκδοση του. Χρησιμοποιώντας μια επέκταση που ονομάζεται TIK (TESLA με γνωστοποίηση Instant Key), που απαιτεί ένα ρολόι συγχρονισμού μεταξύ των κόμβων είναι δυνατόν να ανιχνευθούν ανωμαλίες που προκαλούνται από μια επίθεση σκουληκότρυπας βασιζόμενοι στο χρονοδιάγραμμα των αποκλίσεων[2].

Στο πρωτόκολλο TESLA (Timed Efficient Stream Loss-tolerant Authentication) σε κάθε πακέτο που εκπέμπεται από τον αποστολέα είναι προσαρτημένο μια παράμετρο MAC που παράγεται χρησιμοποιώντας ένα μυστικό κλειδί k, γνωστό αρχικά μόνο στον αποστολέα. Ο αποστολέας θα αποκαλύψει το κλειδί k στον παραλήπτη μετά από μια ορισμένη χρονική καθυστέρηση d. Ο δέκτης που θα λάβει το πακέτο θα το αποθηκεύσει χωρίς να είναι σε θέση να προβεί στον έλεγχο της ταυτότητας του μέχρι την παραλαβή του κλειδιού k. Μετά την καθορισμένη χρονική καθυστέρηση d, ο αποστολέας αποκαλύπτει το κλειδί k και ο δέκτης είναι τότε σε θέση να ταυτοποιήσει

τον αποστολέα. Η παράμετρος MAC ανά πακέτο είναι επαρκής για να παρέχει έλεγχο ταυτότητας και μια απαίτηση του πρωτοκόλλου είναι ο συγχρονισμός μεταξύ του αποστολέα και του παραλήπτη. Στο TESLA μια μονόδρομη βασική αλυσίδα (one-way key chain) χρησιμοποιείται για να παρέχει έλεγχο ταυτότητας και παράγεται επανειλημμένα χρησιμοποιώντας την ίδια λειτουργία (one-way hash) για το αρχικό κλειδί[4].

Το **SEAD** (Secure Efficient Distance Vector) βασίζεται στην εκδοχή-SQ του DSDV (Destination Sequenced Distance Vector) πρωτόκολλου. Σε μια προληπτική (ή περιοδική) δρομολόγηση των κόμβων το πρωτόκολλο πραγματοποιεί περιοδική ανταλλαγή πληροφοριών δρομολόγησης με τους άλλους κόμβους διευκολύνοντας την προσπάθεια του κάθε κόμβου να γνωρίζει πάντα μια τρέχουσα διαδρομή προς όλους τους προορισμούς του δικτύου[2]. Ασχολείται με επιτιθέμενους που τροποποιούν πληροφορίες δρομολόγησης καθώς και με τις επιθέσεις αναπαραγωγής και κάνει χρήση των μονόδρομων «hash» αλυσίδων και όχι της ασύμμετρης κρυπτογραφίας. Υπάρχουν δυο διαφορετικές προσεγγίσεις για την καταπολέμηση των επιθέσεων που χρησιμοποιούνται για τον έλεγχο ταυτότητας μηνυμάτων. Το πρωτόκολλο SEAD δεν μπορεί να αντιμετωπίσει επιθέσεις σκουληκότρυπας[26].

Το SEAD δεν χρησιμοποιεί καθυστέρηση ως προς την ανανέωση του πίνακα προκειμένου να αποτρέψει επιθέσεις από κόμβους που θα μπορούσαν να μην χρησιμοποιούν κακόβουλα την καθυστέρηση. Δεδομένου ότι ένας κόμβος επιλέγει την πρώτη διαδρομή που δέχεται με μεγαλύτερο αύξων αριθμό σειράς και το χαμηλότερο μετρικό, ένας εισβολέας θα μπορούσε διαφορετικά να επιχειρήσει να προκαλέσει μεγαλύτερη επισκεψιμότητα στον εαυτό του αποφεύγοντας την καθυστέρηση προκαλώντας έτσι ανανέωση των ενημερώσεων του. Μια τέτοια επίθεση θα μπορούσε να θέσει τον επιτιθέμενο σε θέση να διαβάζει, να τροποποιεί ή να απορρίψει πακέτα από άλλους κόμβους[7].

Ένας εισβολέας θα μπορούσε να στείλει ένα μεγάλο αριθμό αυθαίρετων πλαστών ενημερώσεων δρομολόγησης σε κάποιο κόμβο-θύμα και έτσι το θύμα θα είναι αναγκασμένο να δαπανήσει το σύνολο των πόρων του επεξεργαστή του προσπαθώντας να ελέγξει αυτές τις ενημερώσεις. Πρόκειται δηλαδή για την δημιουργία μιας αποτελεσματικής επίθεσης Άρνησης Υπηρεσιών (Denial-of-Service). Επίσης, ένας εισβολέας που έχει παραβιάσει έναν κόμβο μπορεί να στείλει ενημερώσεις υποστηρίζοντας ότι κάθε άλλος κόμβος είναι ένας γείτονας (μετρικό 1), προκαλώντας εσφαλμένα τους άλλους κόμβους να κατευθύνουν τα πακέτα για αυτό τον κόμβο προορισμού προς τον εισβολέα[7].

Μπορεί ακόμα ένας εισβολέας να τροποποιήσει τα μηνύματα ενημέρωσης της δρομολόγησης υπό διαμετακόμιση (transit) και όπως επίσης ένας εισβολέας θα μπορούσε να εμποδίσει την διαφήμιση ορισμένων διαδρομών. Ωστόσο, ένας εισβολέας θα μπορούσε επίσης να είναι σε θέση να αλλοιώσει το σύνολο των ενημερώσεων δρομολόγησης η οποία ισοδυναμεί με μια επίθεση παρεμβολών[7].

Τέλος το SEAD ασχολείται με επιτιθέμενους που τροποποιούν τις πληροφορίες δρομολόγησης που μεταδίδονται κατά τη φάση ενημέρωσης του πρωτοκόλλου DSDV-SQ. Ειδικότερα, η δρομολόγηση μπορεί να διακοπεί εάν ο εισβολέας τροποποιεί τον αύξων αριθμό και το μέτρο των μηνυμάτων ανανέωσης της δρομολόγησης στον πίνακα[2].

Το **SRP** (Secure Routing Protocol) σχεδιάστηκε ως μια επέκταση συμβατή με μια ποικιλία υφιστάμενων “reactive” πρωτόκολλων δρομολόγησης. Το SRP καταπολεμά τις επιθέσεις που διαταράσσουν τη διαδικασία ανακάλυψης διαδρομής και εγγυάται την απόκτηση ακριβών πληροφοριών τοπολογίας του δικτύου[2].

Συγκεκριμένα το SRP επιτρέπει την πρωτοβουλία για την ανακάλυψη μιας διαδρομής και απορρίπτει ψευδείς απαντήσεις. Βασίζεται στη διαθεσιμότητα μιας ένωσης ασφάλειας (SA-Secure Association) μεταξύ του κόμβου πηγής (S) και του κόμβου προορισμού (T). Η «SA» θα μπορούσε να δημιουργηθεί με τη χρήση υβριδικών κλειδιών κατανομής με βάση τα δημόσια κλειδιά των επικοινωνούντων μερών. Ο κόμβος πηγής S και ο κόμβος προορισμού T μπορούν να ανταλλάσσουν ένα μυστικό συμμετρικό κλειδί (KS, T) χρησιμοποιώντας τα δημόσια κλειδιά τους για τη δημιουργία ενός ασφαλούς καναλιού. Έτσι μπορούν στη συνέχεια να προχωρήσουν σε περαιτέρω μεταξύ τους αμοιβαίο έλεγχο ταυτότητας τους και στην αυθεντικότητά της δρομολόγησης των μηνυμάτων τους[2].

Αναλυτικότερα το SRP βασίζεται σε δημόσιο κλειδί μεταξύ του κόμβου πηγής και του κόμβου προορισμού. Στο SRP ένας κόμβος πηγής παράγει RREQ μηνύματα και τα εκπέμπει στους γείτονές του. Όταν ο κόμβος προορισμού παραλάβει τα RREQ μηνύματα ,επαληθεύει έτσι τον κόμβο πηγής και καθορίζει την διαδρομή[8].

Το SRP αντιμετωπίζει την μη συνεννόηση με έναν κακόβουλο κόμβο που είναι σε θέση να τροποποιήσει , να επαναλάβει και να κατασκευάσει πακέτα δρομολόγησης. Αν υποθέσουμε επίσης ότι ο μηχανισμός ανακάλυψης γείτονα διατηρεί πληροφορίες για τον συσχετισμό του μέσου ελέγχου πρόσβασης και τις διευθύνσεις IP των κόμβων, το SRP έχει αποδειχθεί ότι είναι ουσιαστικά άτρωτο σε πλαστογράφηση της IP διευθυνσης[2].

Η βασική έκδοση του SRP είναι ευάλωτη σε επιθέσεις δηλητηρίασης της μνήμης cache κατά την φάση της δρομολόγησης. Το SRP επίσης πάσχει από έλλειψη ενός μηχανισμού επικύρωσης για συντήρηση των μηνυμάτων δρομολόγησης . Το SRP δεν είναι άτρωτο σε επιθέσεις σκουληκότρυπας. Συγκεκριμένα δύο συνεργαζόμενοι κακόβουλοι κόμβοι μπορούν προωθήσουν την δρομολόγηση των πακέτων σε ένα ιδιωτικό δίκτυο αλλάζοντας έτσι την αντίληψη της τοπολογίας του δικτύου από τους νόμιμους κόμβους[2]. Τέλος το SRP όπως γίνεται αντιληπτό παρέχει πολλές μεθόδους για την αντιμετώπιση των διάφορων βυζαντινών επιθέσεων όπως είναι η επίθεση σκουληκότρυπας , η επίθεση μαύρης τρύπας και η επίθεση rushing.

4.3.3 Επίθεση Σκουληκότρυπας

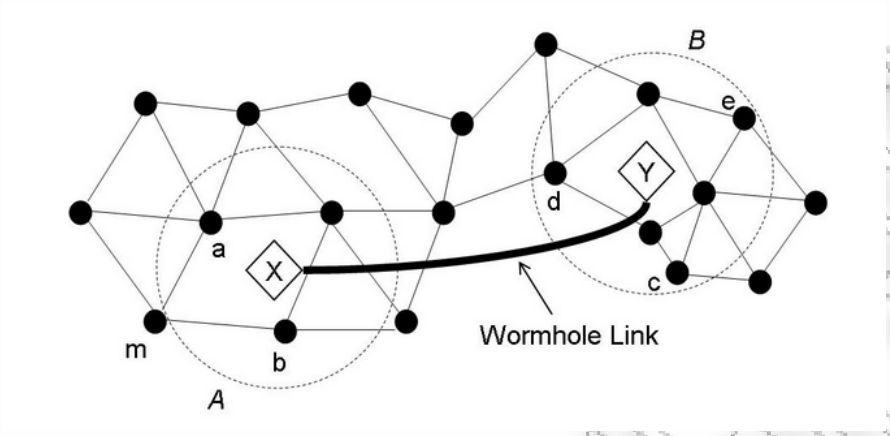
Η επίθεση σκουληκότρυπας (Wormhole Attack) είναι επίσης γνωστή ως “tunneling attack”. Ένας εισβολέας δημιουργεί ένα τούνελ και χρησιμοποιεί ενθυλάκωση (encapsulation) και το αντίθετο (decapsulation) για να δημιουργήσει μια ψευδή διαδρομή μεταξύ δύο κακόβουλων κόμβων. Ένας εισβολέας καταγράφει πακέτα σε ένα σημείο του δικτύου και τα προωθεί σε μια άλλη θέση. Έτσι η δρομολόγηση μπορεί να διαταραχθεί όταν διοχετεύονται τα μηνύματα ελέγχου. Αυτή η σήραγγα μεταξύ δύο συνεργών κακόβουλων κόμβων αναφέρεται ως *σκουληκότρυπα*. Οι επιθέσεις σκουληκότρυπας είναι σοβαρές απειλές για τα Manet πρωτόκολλα

δρομολόγησης. Για παράδειγμα μια επίθεση σκουληκότρυπας εις βάρος ενός on-demand πρωτόκολλου δρομολόγησης όπως το DSR και AODV θα μπορούσε να εμποδίσει την αποκάλυψη τυχόν άλλων οδών πλην αυτών που διέρχονται από το τούνελ.

Συγκεκριμένα σε μια επίθεση «σκουληκότρυπας» ένας επιτιθέμενος λαμβάνει μηνύματα από ένα σημείο του δικτύου, τα διοχετεύει σε άλλο σημείο του δικτύου και στη συνέχεια τα επαναλαμβάνει στο δίκτυο από αυτό το σημείο. Για αποστάσεις διοχέτευσης μεγαλύτερες από την φυσιολογική εμβέλεια ασύρματης μετάδοσης ενός απλού άλματος είναι εύκολο για τον επιτιθέμενο να κάνει τα πακέτα να φτάσουν με καλύτερες παραμέτρους από ότι σε μια φυσιολογική δρομολόγηση. Είναι επίσης δυνατό για τον επιτιθέμενο να προωθήσει κάθε bit στη «σκουληκότρυπα» απευθείας χωρίς να περιμένει ένα ολόκληρο πακέτο να ληφθεί έτσι ώστε να μειώσει τον χρόνο καθυστέρησης που δημιουργείται από τη «σκουληκότρυπα». Λόγω της φύσης της ασύρματης μετάδοσης ο επιτιθέμενος μπορεί να δημιουργήσει μια «σκουληκότρυπα» ακόμα και για πακέτα που δεν απευθύνονται σ' αυτόν αφού μπορεί να τα «ακούσει» κατά την ασύρματη μετάδοση και να τα διοχετεύσει στον συνεργαζόμενο επιτιθέμενο στην άλλη πλευρά της 'σκουληκότρυπας'.

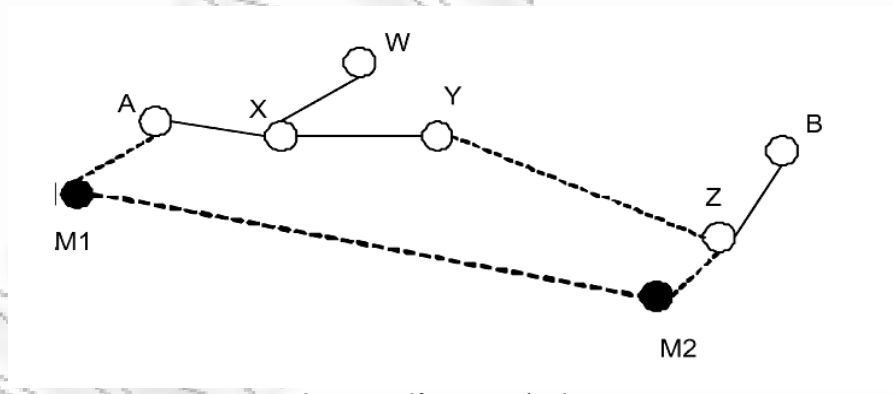
Αν ο επιτιθέμενος εκτελεί αυτήν τη διαδικασία άδολα και αξιόπιστα δεν δημιουργείται κακό. Στην πραγματικότητα ο επιτιθέμενος παρέχει χρήσιμη υπηρεσία συνδέοντας το δίκτυο πιο αποτελεσματικά. Ωστόσο η «σκουληκότρυπα» θέτει τον επιτιθέμενο σε πιο ισχυρή θέση σε σχέση με τους άλλους κόμβους του δικτύου και ο επιτιθέμενος μπορεί να το εκμεταλλευτεί με πολλούς τρόπους. Η επίθεση μπορεί να διαδραματίζεται ακόμα και αν το δίκτυο παρέχει εμπιστευτικότητα και ταυτοποίηση και ακόμα και αν ο επιτιθέμενος δεν έχει κρυπτογραφικά κλειδιά. Επιπλέον ο επιτιθέμενος είναι «αόρατος» σε υψηλότερα επίπεδα.

Ένα παράδειγμα «σκουληκότρυπας» φαίνεται στο παρακάνω σχήμα. Εδώ τα σημεία X και Y είναι τα δύο τελικά σημεία του συνδέσμου του τούνελ (που ονομάζεται ως σκουληκότρυπες). Το σημείο X αναφέρεται στις γειτονικές του περιοχές (περιοχή A) και σε όλα αυτά που «ακούει» το σημείο Y στη γειτονιά του (περιοχή B) και αντιστρόφως. Το καθαρό αποτέλεσμα αυτής της επίθεσης είναι ότι όλοι οι κόμβοι εντός της περιοχής A υποθέτουμε ότι είναι γείτονές των κόμβων στην περιοχή B και αντίστροφα. Αυτό κατά συνέπεια, επηρεάζει τη δρομολόγηση και τη συνδεσιμότητα των άλλων κόμβων με βάση τα πρωτόκολλα του δικτύου. Από τη στιγμή που η νέα διαδρομή καθιερώνεται και η κίνηση στο δίκτυο αρχίζει να χρησιμοποιεί την X Y συντόμευση οι κόμβοι της σκουληκότρυπας μπορούν να ξεκινήσουν την «πτώση» των πακέτων και να προκαλέσουν την διαταραχή του δικτύου. Μπορούν επίσης να κατασκοπεύσουν τα πακέτα που διέρχεται και από την χρήση του μεγάλου όγκου των πληροφοριών που συλλέγονται και να σπάσουν οποιαδήποτε ασφάλεια του δικτύου. Η επίθεση σκουληκότρυπας θα επηρεάσει επίσης τη δυνατότητα σύνδεσης με αλγόριθμους εντοπισμού και ορισμένα πρωτόκολλα που βασίζονται στον εντοπισμό, όπως οι γεωγραφικές μέθοδοι εντοπισμού του δρομολογίου βρίσκοντας συγχρόνως πολλές αντιφάσεις με αποτέλεσμα την περαιτέρω διατάραξη του δικτύου[26].



Εικόνα 21 Επίθεση Σκουλικότρυπας

Συγκεριμένα στο ADOV η επίθεση «σκουλικότρυπας» γίνεται ως εξής: Όπως φαίνεται στην παρακάτω εικόνα ο κόμβος Α θέλει να ανακαλύψει μια διαδρομή προς τον κόμβο Β. Εκπέμπει ένα RREQ μήνυμα που πρώτα φτάνει το Χ και στον M_1.Ενας εισβολέας επίσης θα μπορούσε να είναι διαφανής στο δίκτυο. Ενώ τώρα ο κόμβος Χ αναφέρεται με το RREQ μήνυμα του στους γείτονές W και Y, ο κόμβος M_1 προωθεί το μήνυμα στον M_2 (άλλος εισβολέας) χρησιμοποιώντας μια γρήγορη σύνδεση. Ο κόμβος M_2 μεταδίδει το RREQ μήνυμα στον κόμβο Z, το οποιό με τη σειρά του θα το μεταφέρει στον κόμβο Β. Δεδομένου ότι αυτή η διαδρομή είναι ταχύτερη από την έγκυρη, το έγκυρο RREQ μήνυμα καταστέλλεται, και έτσι επιλέγεται η μικρότερη διαδρομή A-M_1-M_2-Z-B. Επιπλέον, εάν οι κόμβοι κοντά στον κόμβο Α πρόκειται να επικοινωνούν με τους κόμβους κοντά στον Β θα επιλέξουν επίσης αυτή την διαδρομή που περνάει από το M_1-M_2. Στη συνέχεια οι κόμβοι M_1 και M_2 μπορεί να μειωσουν , να καθυστέρησουν ή να τροποποιήσουν τα πακέτα κατά αυτή την μεταφορά[14].



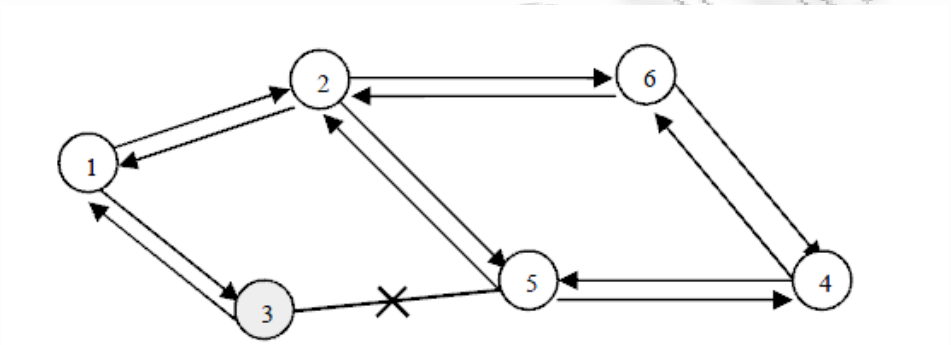
Εικόνα 22 Επίθεση Σκουλικότρυπας

4.3.4 Επίθεση Μαύρης Τρύπας

Η επίθεση μαύρης τρύπας (black hole) γίνεται σε δύο στάδια. Σε πρώτη φάση, ο κακόβουλος κόμβος εκμεταλλεύεται το ασύρματο AdHoc πρωτόκολλο δρομολόγησης όπως το AODV, διαφημίζοντας ότι έχει έγκυρη διαδρομή για έναν κόμβο προορισμού έστω και αν η διαδρομή αυτή είναι πλαστή έχοντας ως πρόθεση την σύλληψη των πακέτων. Σε δεύτερη φάση ο εισβολέας δεν προωθεί τα πακέτα που

έχει προηγουμένως συλλάβει. Σε μια πιο προχωρημένη μορφή ο εισβολέας θα καταστέλλει ή θα τροποποιήσει τα πακέτα που προέρχονται από ορισμένους κόμβους ενώ ταυτόχρονα θα αφήσει ανεπηρέαστα τα δεδομένα από άλλους κόμβους. Με τον τρόπο αυτό, ο εισβολέας ξεγελά τους γειτονικούς κόμβους που παρακολουθούν την εξέλιξη της δρομολόγησης των πακέτων.

Στην παρακάτω εικόνα, ο κόμβος 1 θέλει να στείλει τα πακέτα δεδομένων στον κόμβο 4 και έτσι ξεκινά τη διαδικασία ανακάλυψης διαδρομής. Υποθέτουμε ότι ο κόμβος 3 είναι ένας κακόβουλος κόμβος και ισχυρίζεται κάθε φορά ότι έχει διαδρομή προς τον κόμβο προορισμού και έτσι με το που δέχεται το RREQ μήνυμα αμέσως στέλνει την απάντηση στον κόμβο 1. Εάν η απάντηση από τον κόμβο 3 φτάσει πρώτα στον κόμβο 1 στη συνέχεια ο κόμβος 1 θεωρεί ότι η ανακάλυψη της διαδρομής είναι πλήρης, αγνοεί όλα τα άλλα μηνύματα απαντήσεων (RREQ) και αρχίζει να στείλει τα πακέτα δεδομένων προς τον κόμβο 3. Αυτό έχει ως αποτέλεσμα όλα τα πακέτα να καταναλώνονται ή να χάνονται από το κακόβουλο κόμβο[26].

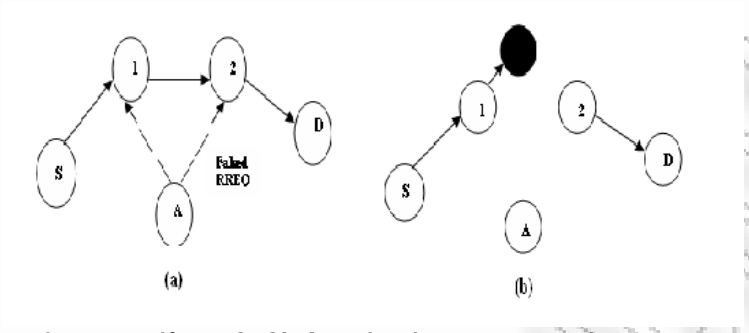


Εικόνα 23 Επίθεση Μαύρης Τρύπας

Η επίθεση της «Μαύρης τρύπας – Black Hole» στο πρωτόκολλο δρομολόγησης AODV μπορεί να ταξινομηθεί σε δύο κατηγορίες: την *RREQ Blackhole επίθεση* και την *RREP Blackhole επίθεση*[18].

Στην RREQ Blackhole επίθεση ένας εισβολέας μπορεί να στείλει ψεύτικα RREQ μηνύματα και να προσποιείται ότι αναμεταδίδει ένα RREQ μήνυμα με ένα μη πραγματικό κόμβο. Οι άλλοι κόμβοι θα ενημερώσουν τις διαδρομές τους με τον μη υπαρκτό κόμβο έτσι ώστε να φτάσουν στον κόμβο προορισμού. Ως εκ τούτου, η κανονική διαδρομή θα καταστραφεί. Ο εισβολέας μπορεί να δημιουργήσει επίθεση μαύρης τρύπας από ψεύτικα RREQ μηνύματα ως εξής:

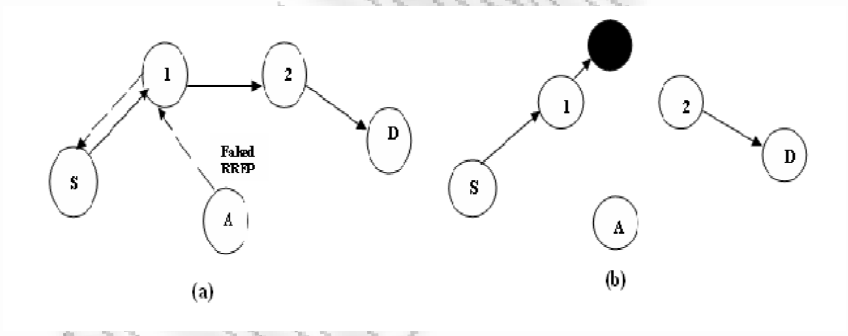
1. Ρύθμιση(Set) του τύπου του πεδίου του RREQ μηνύματος (1).
2. Ρύθμιση της IP διεύθυνσης του εντολέα (originator) με την διεύθυνση IP του εντολέα
3. Ρύθμιση της διεύθυνσης IP προορισμού με την διεύθυνση IP του κόμβου προορισμού
4. Ρύθμιση της διεύθυνσης IP προέλευσης (στην επικεφαλίδα IP) με την μη πραγματική διεύθυνση IP (BlackHole)
5. Αύξηση του αριθμού ακολουθίας της πηγής (source sequence number) κατά τουλάχιστον μια μονάδα(1), ή μείωση της κατά ένα βήμα-άλμα (hop)[18].



Εικόνα χχχ Επίθεση Blackhole από ψεύτικα RREQ μηνύματα

Ο εισβολέας όπως είπαμε και πριν μπορεί να δημιουργήσει ένα μήνυμα RREP για να σχηματίσει μια μαύρη τρύπα ως εξής:

1. Ρύθμιση(Set) του τύπου του πεδίου του RREQ μηνύματος (2)
2. Ρύθμιση του πεδίου των αλμάτων σε 1
3. Ρύθμιση της IP διεύθυνσης του εντολέα (originator) με την διεύθυνση IP του εντολέα και της διεύθυνσης IP προορισμού με την διεύθυνση IP του κόμβου προορισμού.
4. Αύξηση του αριθμού ακολουθίας προορισμού (destination sequence number) τουλάχιστον κατά μια μονάδα (1).
5. Ρύθμιση της διεύθυνσης IP προέλευσης (στην επικεφαλίδα IP) με την μη πραγματική διεύθυνση IP (BlackHole) [18]



Εικόνα χχχ Επίθεση Blackhole από ψεύτικα RREP μηνύματα

Ο επιτιθέμενος στέλνει το ψεύτικο RREP μήνυμα στον αρχικό κόμβο. Όταν ο αρχικός κόμβος (εντολέας) λάβει το ψεύτικο RREP μήνυμα προσαρμόζει την πορεία του προς τον κόμβο προορισμού μέσω του μη-υπαρκτού κόμβου[18].

4.3.5 Rushing Επίθεση

Πρώτα από όλα αναζητώντας την έννοια την ορολογίας «rushing attack» διαπιστώσαμε ότι πρόκειται για «μια ξαφνική επίθεση », ή «μια ξαφνική κίνηση προς τα εμπρός», ή, «μια επίθεση της οποίας η εκτέλεση πρέπει να τελειώσει με μεγάλη ταχύτητα»[19].

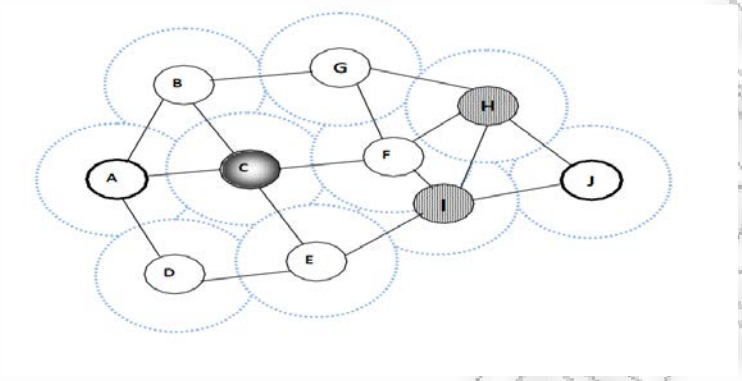
Στη επίθεση σκουληκότρυπας (wormhole), δύο επιτιθέμενοι σχηματίζουν ένα τούνελ για να διαψεύσουν την πραγματική διαδρομή. Στην περίπτωση αυτή η διαδρομή μετάδοσης μέσω του τούνελ είναι αρκετά γρήγορη (για παράδειγμα σε ένα αποκλειστικό κανάλι) και τότε τα πακέτα μπορεί να μεταδοθούν ταχύτερα από αυτά

που μεταδίδονται με τον συνήθη τρόπο των «multihop» διαδρομών και έτσι η επίθεση καταλήγει σε Rushing (βιασύνης).

Στο επίπεδο του δικτύου η "rushing –βιαστική επίθεση" καλείται επίσης ως «novel attack» ή επίθεση «άρνησης υπηρεσίας (Dos)» [5]. Η επίθεση αυτή είναι μια κακόβουλη επίθεση που ενεργεί ως μια αποτελεσματική άρνηση υπηρεσίας σε επιθέσεις εναντίον των on-demand πρωτόκολλων δρομολόγησης (π.χ. DSR, AODV κλπ), συμπεριλαμβανομένων και των πρωτοκόλλων που έχουν σχεδιαστεί για την ασφάλεια (π.χ. ARIANDE, ARAN κλπ). Όπως γνωρίζουμε στα «on-demand» πρωτόκολλα δρομολόγησης η ανακάλυψη της διαδρομής είναι ένας μηχανισμός με τον οποίο ένας κόμβος-πηγής αποκτά ένα δρομολόγιο προς τον κόμβο-προορισμού όταν επιθυμεί να στείλει ένα πακέτο σε αυτόν. Κανονικά, ο κόμβος-πηγής αποκτά την κατάλληλη διαδρομή για ένα προορισμό από την αναζήτηση στην μνήμη cache του αλλά αν η διαδρομή δεν βρίσκεται στην προσωρινή μνήμη του, θα ξεκινήσει την ανακάλυψη δρομολογίου δημιουργώντας (flooding) αιτήματα αναζήτησης της διαδρομής (RREQ) προς όλο το δίκτυο. Προκειμένου να περιοριστεί η επιβάρυνση του δικτύου από αυτά τα μηνύματα, κάθε κόμβος συνήθως υποβάλλει ένα μόνο αίτημα διαδρομής (RREQ) για την ανακάλυψη κάθε διαδρομής. Ειδικότερα, τα υφιστάμενα on-demand πρωτόκολλα δρομολόγησης, όπως το AODV, DSR, ARIANDE, SAODV, ARAN, ασφαλίζονται με τα πρωτόκολλα SUCV και SRP προωθώντας μόνο τα αιτήματα που φθάνουν για πρώτη φορά από την ανακάλυψη κάθε διαδρομής. Στη επίθεση αυτή λοιπόν, ο εισβολέας εκμεταλλεύεται αυτή την ιδιότητα της λειτουργίας της ανακάλυψης της διαδρομής. Τώρα μπορούμε να περιγράψουμε την «rushing επίθεση» από την πλευρά του αποτελέσματός της στη λειτουργία της ανακάλυψης διαδρομής στο πρωτόκολλο DSR. Άλλα πρωτόκολλα όπως το AODV, το ARIANDE, το SAODV και το ARAN είναι ευάλωτα με τον ίδιο τρόπο[19].

Στο δίκτυο που φαίνεται στην παρακάτω εικόνα, οι εσωτερικοί κύκλοι συμβολίζουν τους κόμβους και οι εξωτερικοί (με γαλάζιο χρώμα) συμβολίζουν το εύρος μετάδοσης των κόμβων του δικτύου. Ο κόμβος Α είναι ο κόμβος-πηγής, ο κόμβος J είναι ο κόμβος –προορισμού, ο κόμβος C που συμβολίζεται με μαύρο χρώμα είναι ο κακόβουλος κόμβος και οι κόμβοι Η και Ι είναι οι γείτονες του κόμβου προορισμού στο εν λόγω δίκτυο. Ο κόμβος Α δηλαδή ο κόμβος πηγής ξεκινάει την διαδικασία της ανακάλυψης του δρομολογίου για το τον κόμβο-προορισμού J. Εάν τα μηνύματα αιτήσεων της διαδρομής (RREQ) για αυτήν την ανακάλυψη διαβιβάστηκαν από τον επιτιθέμενο τότε κάθε διαδρομή που θα ανακαλυφθεί θα περιλαμβάνει βήμα (hop) μέσα από τον εισβολέα. Δηλαδή, όταν οι γείτονές του προορισμού-στόχου λαμβάνουν τα αιτήματα από τον εισβολέα θα προωθούν αυτό το αίτημα και δεν θα δημιουργήσουν περαιτέρω αιτήματα για την ανακάλυψη του συγκεκριμένου δρομολογίου. Όταν αργότερα φτάσουν νόμιμα αιτήματα σε αυτούς τους κόμβους, θα τα απορρίψουν. Για παράδειγμα, ας υποθέσουμε ότι ο κόμβος C είναι ένας κακόβουλος κόμβος και έτσι δεν έχει καμία πρόθεση να ελέγξει κατά πόσον η συγκεκριμένη διαδρομή είναι διαθέσιμη. Γι 'αυτό θα μεταδώσει αμέσως σχετικό αίτημα. Όμως σε ένα αίτημα μέσω του κόμβου Β ή σε οποιαδήποτε άλλο νόμιμο κόμβο χρειάζεται κάποιο χρόνο για να ελεγχτεί κατά πόσον η συγκεκριμένη διαδρομή είναι διαθέσιμη. Έτσι ζητούν από τον κακόβουλο κόμβο δηλαδή τον κόμβο C να προωθήσει το αίτημα πρώτος στους κόμβους Η και Ι οι οποίοι είναι πλησίον του κόμβου-στόχου J ώστε ο τελευταίος να συγκρίνει το αίτημα του νόμιμου κόμβου Β. Ως αποτέλεσμα ο αρχικός κόμβος Α δεν θα είναι σε θέση να ανακαλύψει άλλες

διαδρομές (δηλαδή δρομολόγια που δεν περιλαμβάνουν τον επιτιθέμενο) που περιέχουν τουλάχιστον δύο βήματα δηλαδή τρεις κόμβους[19].



Εικόνα 24 Παράδειγμα Rushing Επίθεσης

Εν ολίγοις όταν ο αρχικός κόμβος αρχίζει την διαδικασία εύρεσης της διαδρομής για τον κόμβο-στόχο και η ζητούμενη διαδρομή (Route Requests) διέρχεται από τον εισβολέα τότε αυτός θα είναι ο πρώτος που θα φθάσει σε κάθε γείτονά του στόχου με αποτέλεσμα οποιαδήποτε εύρεση διαδρομής με αυτόν τον τρόπο θα περιλαμβάνει άλματα (hops) μέσα από τον εισβολέα και έτσι όταν ένας γείτονας του στόχου-προορισμού λαμβάνει αίτημα από τον εισβολέα θα διαβιβάσει το αίτημα σε αυτόν και δεν θα υποβάλλει περαιτέρω αιτήματα για αυτή την διαδρομή.

Με άλλα λόγια μπορούμε να πούμε ότι ο εισβολέας μπορεί να διαβιβάζει πιο γρήγορα αιτήματα ανακάλυψης των διαδρομών από ότι οι νόμιμοι κόμβοι μπορούν να το πράξουν. Έτσι μπορεί να αυξήσει την πιθανότητα οι διαδρομές που θα ανακαλυφθούν να περιλαμβάνουν τον εισβολέα και όχι σε άλλα έγκυρα δρομολόγια με νόμιμους κόμβους στηριζόμενος στο γεγονός ότι ο κάθε κόμβος προωθεί ένα αίτημα για την ανακάλυψη μιας διαδρομής. Η rushing επίθεση μπορεί επίσης να χρησιμοποιηθεί εναντίον κάθε πρωτόκολλου που διαβιβάζει αιτήματα για την ανακάλυψη της διαδρομής[19].

4.3.6 Επίθεση Κατανάλωσης Πόρων

Η ενέργεια είναι μια πολύ κρίσιμη παράμετρος στα Manet δίκτυα. Οι συσκευές που λειτουργούν με μπαταρία (Battery-Powered) προσπαθούν να εξοικονομήσουν ενέργεια μεταδίδοντας δεδομένα μόνο όταν είναι απολύτως απαραίτητο. Ο στόχος της επίθεσης *Κατανάλωσης Πόρων* (Resource Consumption) είναι να στέλνει συνεχώς αιτήματα για την ανακάλυψη μιας διαδρομής ή άχρηστα πακέτα στον κόμβο-θύμα ώστε να λιγοστέψει τη διάρκεια ζωής της μπαταρίας του. Η επίθεση αυτή είναι επίσης γνωστή ως επίθεση «στέρησης ύπνου».(deprivation attack).

Συγκεκριμένα σε μια επίθεση κατανάλωσης πόρων οι κακόβουλοι κόμβοι μπορούν να προκαλέσουν επιπλέον έλεγχο των πακέτων δεδομένων στο δίκτυο. Για παράδειγμα, στο πρωτόκολλο AODV ένας κακόβουλος κόμβος μπορεί να στέλνει διαφορετικά μηνύματα ανακάλυψης μιας διαδρομής (RREQ) με τους γείτονές του. Δεδομένου ότι οι αριθμοί ακολουθίας των μηνυμάτων ή οι πλαστές (faked) διευθύνσεις προορισμού μπορουν να αλλάξουν οποιαδήποτε στιγμή και οι γείτονες του εισβολέα δεν είναι σε

θέση να διακρίνουν αν τα μηνύματα αυτά είναι ψεύτικα ή νέα αιτήματα, θα πρέπει και αυτοί με την σειρά τους να τα διαβιβάσουν στους γείτονές τους και ούτω καθεξής. Εάν ο κακόβουλος κόμβος στέλνει αυτά τα πλαστά μηνύματα σε μεγάλο βαθμό, οι γείτονές του πρέπει να δαπανήσουν πολύ περισσότερους πόρους, όπως είναι το εύρος ζώνης, η χρησιμοποίηση του επεξεργαστή και η ενέργεια της μπαταρίας ώστε να χειριστούν αυτά τα πλαστά μηνύματα. Μια ελαφρώς λιγότερο επιθετική εκδοχή αυτής της επίθεσης είναι όταν ένας κακόβουλος κόμβος διατηρεί τα αιτήματα ανακάλυψης της διαδρομής (RREQ) για μεγάλο χρονικό διάστημα αγνοώντας τις απαντήσεις (reply) σε αυτά[20]. Έτσι οι γείτονες τους καταναλώνουν περισσότερους πόρους για να ανακαλύψουν μια διαδρομή.

4.3.7 Επίθεση Αποκάλυψης της Τοποθεσίας

Η επίθεση αυτή (Location Disclosure) είναι μέρος της επίθεσης αποκάλυψης πληροφοριών (Disclosure Attack). Ο κακόβουλος κόμβος διαβάζει πληροφορίες σχετικά με την τοποθεσία ή τη δομή του δικτύου και χρησιμοποιεί τις πληροφορίες αυτές για περαιτέρω επίθεση. Συγκεντρώνει πληροφορίες για την θέση των κόμβων όπως ένα χάρτη πορείας ώστε να γνωρίζει ποιοι κόμβοι βρίσκονται σε κάθε διαδρομή. Η ανάλυση της κυκλοφορίας ή όπως είναι ευρέως γνωστό “traffic analysis” είναι ένα από τα άλυτα πρόβλημα ασφαλείας εναντίον των MANET δικτύων.

Συγκριμένα η επίθεση μπορεί να είναι τόσο απλή όσο η εντολή «traceroute» σε συστήματα τύπου Unix και έτσι ο επιτιθέμενος προβαίνει στις εξής ενέργειες

- Αποστέλλει μηνύματα δρομολόγησης με ανεπαρκές - οριακές τιμές αλμάτων (hop)
- Καταγράφει τις διευθύνσεις των συσκευών αποστολής των μηνυμάτων λάθους του πρωτοκόλλου ICMP
- Τέλος γνωρίζει έτσι ποιοι κόμβοι βρίσκονται στη διαδρομή προς το στόχο.

Τώρα το ICMP (Internet Control Message Protocol) παρέχει την δυνατότητα για μεταφορά μηνυμάτων ανάμεσα στους δρομολογητές που στην περίπτωση μας είναι οι κόμβοι του δικτύου. Προσφέρει στην ουσία ένα τρόπο ανάδρασης για τη διατύπωση προβλημάτων επικοινωνίας. Για παράδειγμα όταν ένας δρομολογητής δεν έχει άλλη χωρητικότητα για να εξυπηρετήσει ένα πακέτο, μπορεί να στείλει στον αποστολέα που έστειλε το πακέτο, ένα ICMP μήνυμα για να τον πληροφορήσει σχετικά. Το ICMP αν και βρίσκεται στο επίπεδο δικτύου που βρίσκεται και το πρωτόκολλο IP είναι στην πραγματικότητα χρήστης του IP. Ένα ICMP μήνυμα δημιουργείται, ενθυλακώνεται (encapsulating) μέσα σε ένα IP header και μεταδίδεται. Επειδή το ICMP μήνυμα μεταδίδεται σαν IP πακέτο.

4.3.8 Επίθεση Καταβόθρας

Σε μια επίθεση «καταβόθρας» (Sinkhole attack) ο στόχος του επιτιθέμενου είναι να παρασύρει όλη την κίνηση μιας συγκεκριμένης περιοχής του δικτύου μέσω ενός εκτεθειμένου κόμβου δημιουργώντας μια μεταφορική καταβόθρα με τον επιτιθέμενο στο κέντρο. Επειδή οι κόμβοι δίπλα ή πάνω στη διαδρομή που ακολουθούν τα πακέτα έχουν μεγάλες δυνατότητες να απασχολούνται με δεδομένα εφαρμογών, οι επιθέσεις καταβόθρας μπορούν να ενεργοποιήσουν και άλλες επιθέσεις. Η επίθεση καταβόθρας αποτελεί βάση για πολλές άλλες επιθέσεις όπως η υποκλοπή(eavesdropping) ή η τροποποίηση στοιχείων. Ακόμα αν και οι εξ ορισμού κόμβοι στο στρώμα δικτύου ενός adhoc δικτύου είναι ίδιοι, οι επιθέσεις καταβόθρας ενδέχεται να είναι πολύ αποτελεσματικές σε επίπεδο εφαρμογής όπου οι κόμβοι μπορεί να έχουν διαφορετικούς ρόλους. Αυτό σημαίνει ότι η επίδραση των επιθέσεων καταβόθρας σε δίκτυα με κεντρικά κόμβους μπορεί να είναι ιδιαίτερα σοβαρή διότι από την απομίμηση του κεντρικού κόμβου ο αντίπαλος μπορεί να πάρει την πρόσβαση στο μεγαλύτερο μέρος των δεδομένων που περιέχονται μέσω του δικτύου[31].

Οι επιθέσεις καταβόθρας συνήθως δουλεύουν κάνοντας έναν εκτεθειμένο κόμβο να φαίνεται ελκυστικός στους γειτονικούς κόμβους ως προς τον αλγόριθμο δρομολόγησης. Για παράδειγμα, ένας επιτιθέμενος μπορεί να παραπλανήσει ή να επαναλάβει μια ανακοίνωση για ένα εξαιρετικά ποιοτικό δρομολόγιο σε έναν σταθμό βάσης. Ορισμένα πρωτόκολλα πιθανόν να προσπαθήσουν να επιβεβαιώσουν την ποιότητα του δρομολογίου με μια ανταπόδοση από άκρη σε άκρη που να περιέχει πληροφορία αξιοπιστίας και χρόνου. Σε αυτή την περίπτωση, ένας επιτιθέμενος με μια ισχυρή κεραία μπορεί να παρέχει υψηλής ποιότητας δρομολόγηση μεταδίδοντας με αρκετή ισχύ για να φτάσει στο σταθμό βάσης με ένα άλμα. Λόγω της αληθινής ή φανταστικής υψηλής ποιότητας της διαδρομής μέσω του εκτεθειμένου κόμβου είναι πιθανό κάθε γειτονικός κόμβος να προωθεί τα πακέτα που κατευθύνονται στο σταθμό βάσης μέσω του επιτιθέμενου κόμβου και επίσης να διαδίδει την ελκυστικότητα της διαδρομής στους γείτονες. Συνοπτικά, ο επιτιθέμενος δημιουργεί μια σφαίρα επιρροής ελκύοντας όλη την κυκλοφορία που κατευθύνεται σε έναν σταθμό βάσης, από κόμβους που βρίσκονται πολλά άλματα μακριά από τον εκτεθειμένο κόμβο.

Ένα κίνητρο για τη δημιουργία μιας επίθεσης «καταβόθρας» είναι ότι κάνει την επιλεκτική προώθηση πακέτων ασήμαντη. Εξασφαλίζοντας ότι όλη η κίνηση στην περιοχή ενδιαφέροντος ρέει μέσω ενός εκτεθειμένου κόμβου, ένας επιτιθέμενος μπορεί επιλεκτικά να τροποποιήσει ή να απορρίψει πακέτα που προέρχονται από οποιοδήποτε κόμβο του δικτύου.

4.3.9 Επίθεση Αναπαραγωγής Κόμβου.

Μια επίθεση αναπαραγωγής κόμβου είναι πολύ απλή με την έννοια ότι ένας επιτιθέμενος προσπαθεί να προσθέσει έναν κόμβο στο υπάρχον δίκτυο αντιγράφοντας (αναπαράγοντας) το ID ενός υπάρχοντος κόμβου. Ένας κόμβος που παράγεται με αυτόν τον τρόπο μπορεί να διαταράξει την ομαλή λειτουργία του δικτύου αλλοιώνοντας τα πακέτα ή οδηγώντας τα σε λάθος διαδρομή. Αυτό μπορεί να οδηγήσει σε ένα δίκτυο που δεν συνδέεται ομαλά και να παρέχει λάθος δεδομένα.

Αν ένας επιτιθέμενος κερδίσει φυσική πρόσβαση στο δίκτυο μπορεί να αντιγράψει τα κρυπτογραφικά κλειδιά και μπορεί να εισάγει αναπαραγόμενους κόμβους σε

στρατηγικά σημεία του δικτύου. Εισάγοντας νέους κόμβους σε συγκεκριμένα σημεία, ο επιτιθέμενος μπορεί να ελέγχει ένα συγκεκριμένο κομμάτι του δικτύου και να εκτελεί επιθέσεις στο υπόλοιπο υγιές δίκτυο[31].

Κεφάλαιο 5

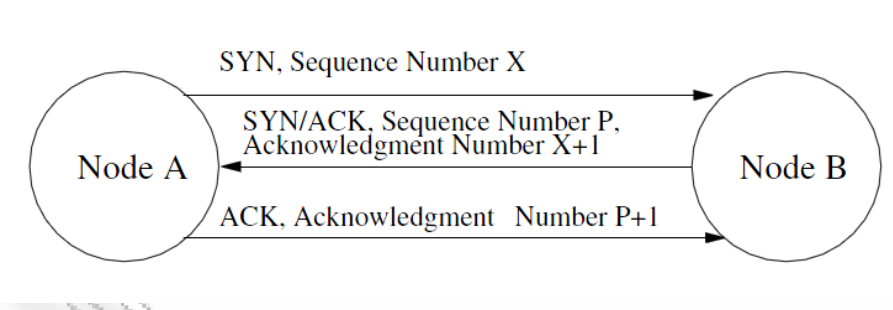
Επιθέσεις στο Επίπεδο Μεταφοράς

5.1 Εισαγωγή

Οι στόχοι του πρωτοκόλλου TCP (πρωτόκολλο επιπέδου μεταφοράς) στα Manet περιλαμβάνουν τη συγκρότηση μιας «end-to-end» σύνδεσης, μιας «end-to-end» αξιόπιστης παράδοσης των πακέτων, έλεγχο ροής, έλεγχο συμφόρησης και συμψηφισμό της «end-to-end» σύνδεσης στο τέλος. Παρομοίως με τα πρωτόκολλα TCP στο Internet, οι κινητοί κόμβοι στα Manet είναι ευάλωτοι στις επιθέσεις SYN Flooding, «Θύελλας» ACK μηνυμάτων κατά την έναρξη μιας συνόδου TCP και Session Hijacking. Ωστόσο τα δίκτυα Manet έχουν υψηλότερο ποσοστό σφάλματος καναλιού σε σύγκριση με τα ενσύρματα δίκτυα. Επειδή το πρωτόκολλο TCP δεν έχει κανένα μηχανισμό για να διακρίνει αν μια ζημία προκλήθηκε από συμφόρηση, τυχαίο σφάλμα, ή κακόβουλες επιθέσεις, το TCP μειώνει πολλαπλασιαστικά το παράθυρο συμφόρησης του όταν παρουσιάζονται ζημίες υποβαθμίζοντας έτσι σημαντικά την απόδοση του δικτύου[32].

5.2 SYN (Synchronize) Flooding Επίθεση

Η επίθεση SYN Flooding είναι μια επίθεση άρνησης υπηρεσίας (Denial Of Service). Ο εισβολέας δημιουργεί ένα μεγάλο αριθμό ελλείπων (Half-Opened) TCP συνδέσεων με έναν κόμβο-θύμα αλλά ποτέ δεν ολοκληρώνει πλήρως την διαδικασία σύνδεσης. Για δύο κόμβους οι οποίοι επικοινωνούν με το TCP πρέπει πρώτα να δημιουργήσουν μια σύνδεση TCP με την διαδικασία της «χειραψίας τριών μερών»(three-way handshake). Τα τρία μηνύματα που ανταλλάσσονται κατά τη διάρκεια χειραψίας απεικονίζονται στην παρακάτω εικόνα, τα οποία επιτρέπουν στους δύο κόμβους να μάθουν αν ο έτερος κόμβος είναι έτοιμος να ανακοινώσει και να συμφωνήσει τους αρχικούς αριθμούς ακολουθίας για τη συνομιλία[32].



Εικόνα 25:Διαδικασία TCP "Χειραψίας" Τριών Μερών

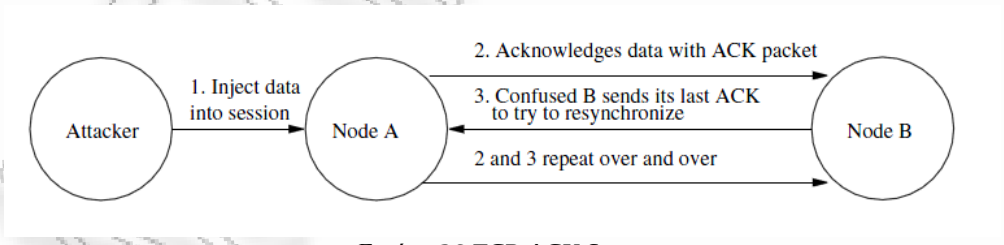
Συγκεκριμένα ο αποστολέας στέλνει ένα SYN μήνυμα στον δέκτη με ένα τυχαίο αριθμό ISN (Initial Sequence Number). Έπειτα ο παραλήπτης δημιουργεί ένα ISN και στέλνει ένα άλλο SYN μήνυμα το οποίο περιέχει το ISN σαν απόδειξη της σωστής

παραλαβής του μηνύματος SYN. Τέλος ο αποστολέας στέλνει ένα ACK μήνυμα στον παραλήπτη.

Κατά τη διάρκεια της επίθεσης ο κακόβουλος κόμβος στέλνει ένα μεγάλο αριθμό από SYN πακέτα σε έναν κόμβο-θύμα παραποιώντας την διεύθυνση επιστροφής των πακέτων SYN. Τα SYN ACK αυτά πακέτα παραλαμβάνονται από τον εισβολέα και στη συνέχεια το θύμα περιμένει την ανταπόκριση των ACK πακέτων από τον εισβολέα. Χωρίς τη λήψη των πακέτων ACK τα δεδομένα παραμένουν στον κόμβο-θύμα. Εάν ο κόμβος-θύμα αποθηκεύει αυτές τις ανεκπλήρωτες (half-opened) συνδέσεις σε ένα πεπερασμένου μεγέθους (fixed size) πίνακα ενώ αναμένει την αναγνώριση των δρόμων «χειραψίας», τότε όλες αυτές οι εν αναμονή συνδέσεις θα μπορούσαν να υπερχειλίσουν τον buffer του θύματος και ο κόμβος-θύμα δεν θα είναι σε θέση να δεχθεί οποιαδήποτε άλλη θεμιτή αναζήτηση για να ανοίξει μια σύνδεση. Συνήθως υπάρχει ένα χρονικό όριο που συνδέεται με την εκκρεμούσα σύνδεση έτσι ώστε οι μισάνοιχτες συνδέσεις (Half-Opened) τελικά να λήξουν και ο κόμβος θύμα να ανακάμψει. Ωστόσο, οι κακόβουλοι κόμβοι μπορεί απλά να συνεχίσουν την αποστολή πακέτων ζητώντας νέες συνδέσεις ταχύτερα από το τη λήξη των εν αναμονή συνδέσεων[32].

5.3 Επίθεση «Θύελλας» ACK μηνυμάτων κατά την έναρξη μιας συνόδου TCP

Όπως φαίνεται στο παρακάτω σχήμα, η επίθεση θύελλας ACK μηνυμάτων (TCP ACK Storm) θα μπορούσε να συμβεί όταν ένας εισβολέας ξεκινά μια σύνοδος TCP. Ο επιτιθέμενος στέλνει τα δεδομένα της συνεδρίας και ο κόμβος Α θα αναγνωρίσει την παραλαβή των δεδομένων με την αποστολή ενός ACK πακέτου στον κόμβο Β. Αυτό το πακέτο δεν θα περιλαμβάνει τον αύξοντα αριθμό που αναμένει ο κόμβος Β και έτσι όταν ο κόμβος Β λάβει αυτό το πακέτο θα προσπαθήσει να συγχρονιστεί εκ νέου με τον κόμβο Α αποστέλλοντας ένα ACK πακέτο και τον αύξων αριθμό που περιμένει. Ο κύκλος έτσι συνεχίζεται και τα πακέτα ACK δημιουργούν μια «θύελλα»[32].



Εικόνα 26 TCP ACK Storm

5.4 Επίθεση Session Hijacking.

Η επίθεση Session Hijacking εκμεταλλεύεται το γεγονός ότι οι επικοινωνίες έχουν μηχανισμούς προστασίας κατά την έναρξή μιας συνόδου και όχι μετέπειτα. Σε μια επίθεση συνόδου “TCP Hijacking” ο εισβολέας αλλοιώνει την διεύθυνση IP του

θύματος, καθορίζει το σωστό αριθμό ακολουθίας (sequence number) που αναμένεται από τον στόχο του και στη συνέχεια εκτελεί μια επίθεση άρνησης υπηρεσιών (DoS) στο θύμα. Έτσι, ο εισβολέας υποδύεται τον κόμβο-θύμα και συνεχίζει τη επικοινωνία του με τον κύριο στόχο[32].

Κεφάλαιο 6

Επιθέσεις στο Επίπεδο Εφαρμογής.

6.1 Εισαγωγή

Οι εφαρμογές θα πρέπει να σχεδιαστούν έτσι ώστε να λειτουργούν με αποσυνδέσεις, επανασυνδέσεις καθώς και με καθυστερήσεις και απώλειες δεδομένων. Οπότε η επικοινωνία στο επίπεδο των εφαρμογών είναι επίσης ευάλωτη όσον αφορά την ασφάλεια σε σύγκριση με τα άλλα στρώματα. Το επίπεδο εφαρμογών περιέχει δεδομένα χρήστη και υποστηρίζει κανονικά πολλά πρωτόκολλα όπως το HTTP, το SMTP, το TELNET και το FTP τα οποία περιέχουν πολλά τρωτά σημεία και σημεία πρόσβασης για τους επιτιθέμενους. Οι επιθέσεις στο επίπεδο εφαρμογών είναι ελκυστικές για τους επιτιθέμενους επειδή οι πληροφορίες που αναζητούν υπάρχουν μέσα στις εφαρμογές και το γεγονός αυτό έχει ένα αντίκτυπο στην επίτευξη των στόχων τους[32].

Οι κύριες επιθέσεις στο επίπεδο των εφαρμογών είναι η επίθεση κακόβουλου κώδικα (malicious code attack), η επίθεση άρνησης συμμόρφωσης(reputation attack) και η επίθεση «Snooping».

6.2 Επίθεση Κακόβουλου Κώδικα

Κακόβουλο κώδικα (malicious code) περιέχουν εφαρμογές όπως οι ιοί (virus), worms, spywares, και οι δούρειοι ίπποι (Trojan Horses) οι οποίες μπορούν να διαβρώσουν τα λειτουργικά συστήματα και κατά συνέπεια τις εφαρμογές των χρηστών. Αυτά τα κακόβουλα προγράμματα μπορούν συνήθως να εξαπλωθούν μέσω του δικτύου και να προκαλέσουν προβλήματα επιβράδυνσης ή ακόμα και καταστροφή σε συστήματα ηλεκτρονικών υπολογιστών και των δικτύων. Στα Manet ένας εισβολέας μπορεί να προκαλέσει παρόμοιες επιθέσεις σε ένα κινητό ad hoc δίκτυο[32].

Όπως γνωρίζουμε τα κακόβουλα προγράμματα είναι ευρέως διαδεδομένα στα δίκτυα. Υπάρχουν διάφορες τεχνικές με τις οποίες ένας ιός τύπου worm (σκουλήκι) μπορεί να ανακαλύψει νέες μηχανές για την εκμετάλλευση. Συνήθως, τα worms δεν τροποποιούν ή διαγράφουν αρχεία αλλά δεσμεύουν μνήμη, καταναλώνουν πόρους του συστήματος και έτσι τα επιβραδύνουν. Ένα παράδειγμα είναι η σάρωση της διεύθυνσης IP (IP address scanning) που χρησιμοποιείται από τους ιούς-worms. Η τεχνική αυτή συνίσταται στην δημιουργία πακέτων σε μια ευάλωτη UDP / TCP θύρα με πολλές διαφορετικές IP διευθύνσεις. Οι κόμβοι που πλήττονται από αυτή την σάρωση λαμβάνουν αντίγραφο του ιού-worm και ως εκ τούτου έχουν μολυνθεί. Ο Code Red worm είναι ένας τέτοιος ιός[21].

Το "Code Red" είναι αυτό-αναπαραγόμενος κακόβουλος κώδικας (worm) που εκμεταλλεύεται μια γνωστή ευπάθεια στον διακομιστή IIS της Microsoft . Το worm "Code Red" διενεργεί την επίθεση με τον εξής τρόπο : Το "Code Red" προσπαθεί να

συνδεθεί στη θύρα TCP 80 σε έναν τυχαία επιλεγμένο κόμβο υποδοχής. Μετά την επιτυχή σύνδεση με τη θύρα 80 ο επιτιθέμενος κόμβος στέλνει μια αίτηση HTTP GET στο θύμα προσπαθώντας να εκμεταλλευθεί την υπερχείλιση της μνήμης του στην Υπηρεσία του Ευρετηρίου (CERT CA-2001-13). Στην συνέχεια η ίδια αίτηση (HTTP GET αίτηση) αποστέλλεται σε καθένα από τους τυχαία επιλεγμένους κόμβους σύμφωνα με τον αυτό-πολλαπλασιαστικό χαρακτήρα του worm. Ωστόσο, ανάλογα με τη διαμόρφωση της υποδοχής του αιτήματος υπάρχουν ποικίλες συνέπειες (απενεργοποίηση του IIS και συνεπώς "ανοιχτή" η πόρτα 80). Τέλος η επίθεση πραγματοποιήθηκε με επιτυχία και το worm αρχίζει την εκτέλεση σου στον κόμβο-θύμα.

Μερικά «σκουλήκια» χρησιμοποιούν μερικές ευπάθειες (loopholes) του συστήματος. Για παράδειγμα, οι worm ιοί «Worm.Blaster και Worm.Sasser » χρησιμοποιούν αυτές τις ευπάθειες. Ο Worm.Blaster χρησιμοποιεί ένα σύστημα RPC DCOM και ο Worm.Sasser χρησιμοποιεί το LSASS σύστημα (υπηρεσία τοπικής ασφάλειας της ταυτότητας του υποσυστήματος)[21].

6.3 Επίθεση Άρνησης Συμμόρφωσης

Σε επίπεδο δικτύου τα τείχη προστασίας (firewalls) μπορεί να εγκατασταθούν για να επιτρέψουν ή όχι των είσοδο ορισμένων πακέτων στο δίκτυο. Στο επίπεδο μεταφοράς το σύνολο των συνδέσεων μπορεί να είναι κρυπτογραφημένο από τον αποστολέα στον παραλήπτη (end-to-end). Οι λύσεις αυτές όμως δεν επιλύουν την εξακρίβωση της γνησιότητας (authentication) ή τη μη άρνηση αναγνώρισης των προβλημάτων (non-repudiation problems). Η επίθεση άρνησης συμμόρφωσης (Reputation Attack) αναφέρεται στην άρνηση της συμμετοχής σε μέρος ή στο σύνολο της επικοινωνίας. Για παράδειγμα, ένα πρόσωπο θα μπορούσε να αρνηθεί τη διεξαγωγή μιας αγοράς με πιστωτική κάρτα από μια επιχείρηση ή να αρνηθεί οποιαδήποτε on-line τραπεζική συναλλαγή, οι οποίες αποτελούν τις πρωτότυπες επιθέσεις άρνησης συμμόρφωσης στο εμπορικό σύστημα. Η επίθεση αυτή μπορεί να γίνει σε συνδυασμό με την Σιβυλλική επίθεση ή την επίθεση της πλαστοπροσωπίας (impersonation).

6.4 Επίθεση Snooping

Η επίθεση αυτή περιλαμβάνει την μη εξουσιοδοτημένη πρόσβαση στα δεδομένα ενός ατόμου. Είναι παρόμοιο με την υποκλοπή (eavesdropping) αλλά η επίθεση «Snooping» δεν περιορίζεται στην πρόσβαση στα δεδομένα κατά τη διάρκεια της μετάδοσής της. Η επίθεση αυτή περιλαμβάνει την περιστασιακή παρακολούθηση του ηλεκτρονικού ταχυδρομείου (email) που εμφανίζεται στην οθόνη κάποιου άλλου υπολογιστή ή την παρακολούθηση της πληκτρολόγησης του άλλου. Πιο εξελιγμένα snooping λογισμικά χρησιμοποιούνται για να παρακολουθούν από απόσταση την δραστηριότητα σε μια συσκευή (υπολογιστή) ή σε κάποιο δίκτυο[16].

Ορισμένοι κακόβουλοι χρήστες (crackers) χρησιμοποιούν συχνά snooping τεχνικές για την παρακολούθηση των κλειδιών κρυπτογραφίας , την σύλληψη κωδικών πρόσβασης και των στοιχείων σύνδεσης.

Παρά το γεγονός ότι γενικά το snooping έχει αρνητική πτυχή στην τεχνολογία των υπολογιστών μπορεί να αναφέρεται σε οποιοδήποτε πρόγραμμα ή βοηθητικό πρόγραμμα που εκτελεί καθήκον παρακολούθησης. Για παράδειγμα ένας διακομιστής που κατασκοπεύει χρησιμοποιείται για την καταγραφή της κίνησης του δικτύου, την ανάλυση και το πρωτόκολλο κατασκοπείας στέλνοντας τις πληροφορίες σε έναν υπολογιστή ώστε να εξασφαλιστεί η αποτελεσματική επεξεργασία.

6.5 Επιθέσεις Άρνησης Παροχής Υπηρεσιών

Στο επίπεδο της εφαρμογής τα διάφορα πρωτόκολλα μπορούν επίσης να αξιοποιηθούν σε DoS (Denial Of Service) επιθέσεις. Τα πρωτόκολλα αυτά ασχολούνται με τον εντοπισμό των κόμβων (node localization), τον συγχρονισμό της ώρας (time synchronization), την άθροιση των δεδομένων (data aggregation), την σύνδεση (association) και τη σύντηξη (fusion) η οποία μπορεί να παρεμποδίζεται. Για παράδειγμα, ένας κακόβουλος κόμβος που υποδύεται έναν έμπιστο κόμβο και δίνει ψευδείς πληροφορίες για τον εντοπισμό ή παρεμποδίζει την μετάδοση της ισχύος του δηλαδή τη μετάδοση με λιγότερη ή περισσότερη δύναμη από ότι έχει την δυνατότητα, μπορεί να εμποδίσει το σύστημα εντοπισμού του κόμβου. Δεδομένου ότι αυτά τα είδη επίθεσης μειώνουν τη σχετική υπηρεσία του δικτύου μπορούν επίσης να χαρακτηριστούν και ως επιθέσεις DoS [4].Ένα παράδειγμα επιθέσεων στο επίπεδο εφαρμογών είναι η επίθεση στα πακέτα της εφαρμογής που διαχειρίζεται τα πακέτα κωδικοποίησης βίντεο (MPEG). Η επίθεση αυτή είναι πολύ διαδεδομένη στις εφαρμογές "video streaming" και κατ επέκταση στις ιστοσελίδες που τις περιέχουν όπως πχ το youtube

Κεφάλαιο 7

Επιθέσεις σε Πολλαπλά Επίπεδά

7.1 Εισαγωγή

Ορισμένες από τις επιθέσεις στα Manet μπορεί να ξεκινήσουν και να εκτελεστούν σε περισσότερα από ένα επίπεδα του προτύπου OSI. Παραδείγματα επιθέσεων πολλαπλών επιπέδων είναι οι επιθέσεις άρνησης εξυπηρέτησης (DoS) οι επιθέσεις πλαστοπροσωπίας-μίμησης(impersonation attacks) κτλ.

7.2 Επιθέσεις Άρνησης Παροχής Υπηρεσιών

Οι επιθέσεις άρνησης εξυπηρέτησης θα μπορούσαν να δρομολογηθούν σε περισσότερα από ένα επίπεδα. Συνοπτικά όπως έχουμε αναφέρει και στα παραπάνω κεφάλαια ένας εισβολέας μπορεί να χρησιμοποιήσει τις παρεμβολές του σήματος στο φυσικό επίπεδο με τις οποίες θα διαταράξει την επικοινωνία. Στο επίπεδο Ζεύξης Δεδομένων οι κακόβουλοι κόμβοι μπορεί να καταλάβουν τα κανάλια μέσω του «capture effect» (ευνοεί τον τελευταίο νικητή μεταξύ των υπόλοιπων κόμβων) το οποίο εκμεταλλεύεται την εκθετική υποχώρηση του δυαδικού συστήματος στα MAC πρωτόκολλα και εμποδίζει τους άλλους κόμβους να έχουν πρόσβαση στο κανάλι. Στο επίπεδο δικτύου η δρομολόγηση μπορεί να διακοπεί μέσω της τροποποίησης του πακέτου έλεγχου (modification), της επιλεκτικής προώθησης, της υπερχείλισης ή της «δηλητηρίασης» του πίνακα δρομολόγησης. Στο επίπεδο μεταφοράς και εφαρμογής, οι επιθέσεις SYN Flooding, Session Hijacking , τα κακόβουλα προγράμματα κ.α μπορεί να προκαλέσουν επιθέσεις DoS.

Στη συνέχεια θα παρουσιάσουμε μια σύντομη ανασκόπηση των DoS επιθέσεων η οποία περιλαμβάνει τους βασικούς μηχανισμούς των επιθέσεων DoS. Οι DoS επιθέσεις έχουν σκοπό να διαταράξουν την κανονική λειτουργία του θύματος και κατά συνέπεια να στερούν από τους λοιπούς χρήστες την νόμιμη πρόσβαση σε υπηρεσίες με τη μείωση των πόρων του θύματος χωρίς όμως να θέσουν σε κίνδυνο την εμπιστευτικότητα ή την ακεραιότητα του στόχου. Από την άλλη οι DoS επιθέσεις σκόπιμα υποβαθμίζουν ή εξαλείφουν την ικανότητά των στόχων να εκτελούν την αναμενόμενη λειτουργία του, δηλαδή τη διαθεσιμότητα τους[22].

Οι DoS επιθέσεις μπορούν να ταξινομηθούν σε DoS επιθέσεις ευπάθειας (vulnerability) και DoS επιθέσεις πλημμύρας (flooding) σύμφωνα με τις στρατηγικές που εκμεταλλεύονται[22].

Οι *DoS επιθέσεις ευπάθειας* εκμεταλλεύονται τα ειδικά χαρακτηριστικά ή τα ελαττώματα των λογισμικών (π.χ. το λειτουργικό σύστημα, τα πρωτόκολλα του δικτύου, καθώς και προγράμματα εφαρμογής) που είναι εγκατεστημένα στο θύμα. Οι επιτιθέμενοι στέλνουν μηνύματα προς το θύμα με στόχο την διαπίστωση της ευπάθειας. Τα μηνύματα αυτά θα μπορούσε να τα δημιουργεί περιοδικά το λογισμικό του στόχου και προκαλέσει άπειρους βρόχους, επιβράδυνση του συστήματος,

επανεκκίνηση τους συστήματος , κατανάλωση τεράστιου ποσού της μνήμης. Ως εκ τούτου, ο στόχος έχει παραλύσει και να αρνείται τις υπηρεσίες του σε νόμιμους χρήστες[22].

Σε αντίθεση με τις επιθέσεις DoS ευπάθειας που απενεργοποιούν τον στόχο χρησιμοποιώντας δημιουργημένα μηνύματα, οι επιθέσεις DoS πλημμύρας επιβαρύνουν βάναυσα το στόχο με υπερβολικά καθήκοντα ώστε να τον παραλύσουν. Τα καθήκοντα αυτά καταναλώνουν τους βασικούς πόρους του στόχου (π.χ. ικανότητα της CPU, της μνήμης, της μπαταρίας και το εύρος ζώνης). Για παράδειγμα, πολύπλοκα μηνύματα μπορούν να απαιτούν μακρά επεξεργασία καταλαμβάνοντας τους κύκλους της CPU, υπερβολική κίνηση για την ανάληψη του εύρους ζώνης και μηνύματα έναρξης επικοινωνίας με τους νέους πελάτες τα οποία καταλαμβάνουν μνήμη[22].

Στις *επιθέσεις πλημμύρας* (address-spoofing flooding) κάθε πακέτο RREQ στέλνεται σε κάθε επιτιθέμενο κόμβο και διατίθεται έτσι ένα τυχαίο ζευγάρι διεύθυνσης πηγής και διεύθυνσης προορισμού. Έτσι καθορίζεται η RREQ ροή ως ένα σύνολο RREQ πακέτων τα οποία μοιράζονται το ζεύγος των διευθύνσεων της πηγής και του προορισμού. Εάν το διάστημα μεταξύ δύο διαδοχικών RREQ είναι πάνω από ένα προκαθορισμένο όριο τότε το δεύτερο RREQ θα ανήκει σε μια νέα ροή RREQ. Ως εκ τούτου, όταν ένας επιτιθέμενος εμφανίζεται, ένας μεγάλος αριθμός RREQ ροών θα δημιουργηθούν μέσα στο δίκτυο. Η πλειοψηφία των ροών αυτών είναι νέα για τους υπάρχοντες κινητούς κόμβους λόγω της αναγνώρισης των ροών αυτών, δηλαδή το ζεύγος διεύθυνσης πηγής και προορισμού είναι αυτό που δημιουργείται τυχαία και εμφανίζονται μόνο μία φορά. Η βασική παραδοχή της επίθεσης αυτής είναι ότι ο επιτιθέμενος κόμβος μπορεί να αποδώσει τυχαία μια διαφορετική διεύθυνση πηγής για τον ίδιο. Έτσι οι RREQ ροές που προέκυψαν από αυτό τον κόμβο θα πρέπει να θεωρηθούν ως μια νέα ροή και συνεπώς αυξάνουν το φορτίο του δικτύου. Ωστόσο, τέτοιου είδους επιθέσεις ενδέχεται να έχουν ορισμένους περιορισμούς ανάλογα με τα πρωτόκολλα που χρησιμοποιούνται. Λαμβάνοντας υπόψη το πρότυπο IEEE 802.11 για την θέσπιση μιας TCP/IP σύνδεσης για παράδειγμα, οποιοσδήποτε κόμβος πηγής μπορεί να αναδιαρθρώνεται για την έναρξη μιας επίθεσης πλημμύρας τότε στα Manet μπορεί να εφαρμοστεί το πρωτόκολλο ARP (Address Resolution Protocol) για τον προσδιορισμό του επιτιθέμενου κόμβου βασιζόμενο στην διεύθυνση MAC του και ως εκ τούτου να εμποδίσει τον επιτιθέμενο κόμβο. Εκτός από αυτά τα στοιχεία του επιπέδου ζεύξης δεδομένων είναι επίσης δυνατό να αναλυθεί η ισχύς του σήματος, η κατεύθυνση του σήματος, η κατάσταση του καναλιού ώστε να προσδιοριστεί ο επιτιθέμενος κόμβος. Λόγω των ιδιοτήτων αυτών είναι πιο δύσκολο για τον επιτιθέμενο κόμβο να προσποιείται την ανωνυμία του και ως εκ τούτου είναι λιγότερο προτιμώμενος τρόπος για την εκκίνηση της επίθεσης[23].

Για τις υπόλοιπες επιθέσεις *(non-address-spoofing flooding (NASF))* οι εισβολείς δεν μπορούν να χρησιμοποιήσουν τυχαίες διευθύνσεις τις οποίες δημιουργούν οι ίδιοι αλλά την δική τους διεύθυνση για τα RREQ πακέτα. Με άλλα λόγια οι εισβολείς μπορούν να χρησιμοποιήσουν μόνο ένα σταθερό ζεύγος διεύθυνσης πηγής και προορισμού για όλα τα κακόβουλα πακέτα RREQ. Συνεπώς σε μια τέτοια επίθεση (NASF) οι κόμβοι του δικτύου θα λάβουν πολλές πανομοιότυπες ροές RREQ για ένα σταθερό αριθμό διαδοχικών διαστημάτων δειγματοληψίας. Επιπλέον, το φαινόμενο αυτό θα παραμείνει για όσο διάστημα διαρκεί η επίθεση[23].

7.3 Επιθέσεις Πλαστοπροσωπίας

Οι επιθέσεις πλαστοπροσωπίας-μίμησης (Impersonation attacks) είναι επιθέσεις οι οποίες χρησιμοποιούν την ταυτότητα άλλου κόμβου όπως την MAC ή την IP διεύθυνση του. Οι επιθέσεις αυτές μερικές φορές είναι το πρώτο βήμα για τις περισσότερες επιθέσεις και χρησιμοποιούνται για τη δρομολόγηση πιο εξελιγμένων επιθέσεων.

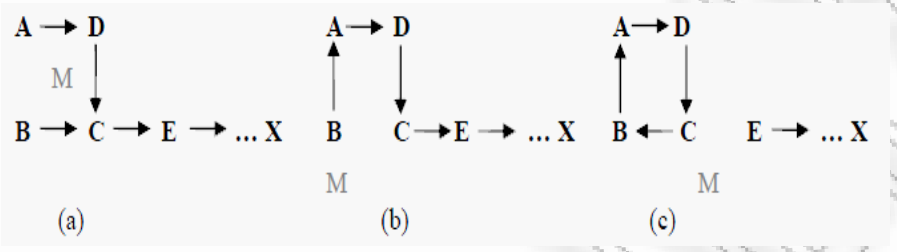
Οι επιθέσεις πλαστοπροσωπίας αποτελούν σοβαρό κίνδυνο για την ασφάλεια σε όλα τα επίπεδα της adhoc δικτύωσης. Εάν η εξακρίβωση της γνησιότητας (authentication) των μερών ενός δικτύου δεν υποστηρίζεται οι εμπλεκόμενοι κόμβοι μπορεί στο επίπεδο δικτύου είναι σε θέση για παράδειγμα να συμμετάσχουν στο δίκτυο και να μην είναι ανιχνεύσιμοι ή να στείλουν ψευδείς πληροφορίες δρομολόγησης όντας "μεταμφιεσμένοι" προς τους αξιόπιστους κόμβους. Στο πλαίσιο της διαχείρισης του δικτύου ο εισβολέας μπορεί να αποκτήσει πρόσβαση στο σύστημα διαχείρισης ως επόπτης (super user). Στο επίπεδο των υπηρεσιών ένας κακόβουλος θα μπορούσε να έχει τα δημόσια κλειδιά των άλλων πιστοποιημένων κόμβων χωρίς ο ίδιος να έχει τα σωστά διαπιστευτήρια (credentials). Έτσι η πλαστοπροσωπία αφορά τις επιθέσεις όλων των κρίσιμων λειτουργιών σε adhoc δίκτυα[24].

Οι επιθέσεις πλαστοπροσωπίας καλούνται επίσης και **επιθέσεις πλαστογράφησης (spoofing attacks).** Ο επιτιθέμενος αναλαμβάνει την ταυτότητα ενός άλλου κόμβου του δικτύου με αποτέλεσμα τη λήψη των μηνυμάτων που κατευθύνονται προς τον κόμβο της απομίμησης. Συνήθως αυτό θα είναι ένα από τα πρώτα βήματα για να εισβάλλουν σε ένα δίκτυο με σκοπό την διενέργεια περαιτέρω επιθέσεων ώστε να διαταράξουν τη λειτουργία του. Ανάλογα με το επίπεδο πρόσβασης του υποδύοντα κόμβου, ο εισβολέας μπορεί ακόμη και να αναδιαμορφώσει το δίκτυο έτσι ώστε άλλοι επιτιθέμενοι να μπορούν (πιο) εύκολα να συμμετάσχουν ή να άρουν τα μέτρα ασφαλείας ώστε να επιτρέψουν επόμενες προσπάθειες εισβολής. Ένας κόμβος μπορεί επίσης να έχει πρόσβαση στα κλειδιά κρυπτογράφησης και στις πληροφορίες γνησιότητας. Σε πολλά δίκτυα ένας κακόβουλος κόμβος θα μπορούσε να εμποδίσει την ορθή δρομολόγηση με την εκχώρηση ψευδών πακέτων δρομολόγησης στο δίκτυο ή να μετατρέψει τις πληροφορίες δρομολόγησης. Οι επιτιθέμενοι ενδέχεται να έχουν ένα πλεονέκτημα στην επιλεκτική προώθηση (selectively forwarding) των πακέτων τους. Έτσι ένας εισβολέας με το στόχο αυτό, πιθανότατα θα προσπαθήσει να μιμηθεί έναν κόμβο στο μονοπάτι της ροής δεδομένων του ενδιαφέροντος του. Θα το επιτύχει αυτό με την τροποποίηση της δρομολόγησης των δεδομένων ή με την προβολή του εαυτό του ως αξιόπιστο συνεργάτη επικοινωνίας με τους γειτονικούς του κόμβους[25].

Ανάλογα με το εκάστοτε επίπεδο που διενεργείται η επίθεση της πλαστογράφησης μπορεί να είναι δύσκολο να αποτραπεί. Με την αξιοποίηση των αδυναμιών του MAC πρωτόκολλου στο επίπεδο Ζεύξης Δεδομένων οι επιτιθέμενοι θα μπορούσαν να θέσουν τον κόμβο τους ανάμεσα σε δύο άλλους κόμβους και να επικοινωνούν μεταξύ τους (man-in-the-middle επιθέσεις). Στις *man-in-the-middle επιθέσεις* ο εισβολέας βρίσκεται μεταξύ του αποστολέα και του παραλήπτη και παρακολουθεί οποιεσδήποτε πληροφορίες αποστέλλονται μεταξύ των δύο άκρων. Σε ορισμένες περιπτώσεις ο εισβολέας μπορεί να μιμηθεί τον αποστολέα και να επικοινωνήσει με το δέκτη ή να μιμηθεί το δέκτη για να απαντήσει στον αποστολέα. Δεδομένου τώρα ότι οι MAC διευθύνσεις μπορεί να αλλοιώνονται με λίγη προσπάθεια, η διαπίστωση της

παράνομης εισβολής μπορεί να μην είναι δυνατή σε αυτό το επίπεδο. Ωστόσο, με τη χρησιμοποίηση καλών αλγορίθμων ελέγχου ταυτότητας, αξιόλογης, κρυπτογράφησης των δεδομένων και ασφαλών πρωτόκολλών δρομολόγησης, οι συνέπειες της πλαστοπροσωπίας μπορεί να μειωθούν σημαντικά[25].

Τέλος θα παρουσιάσουμε την επίθεση πλαστογράφησης (spoofing attack) με ένα παράδειγμα.



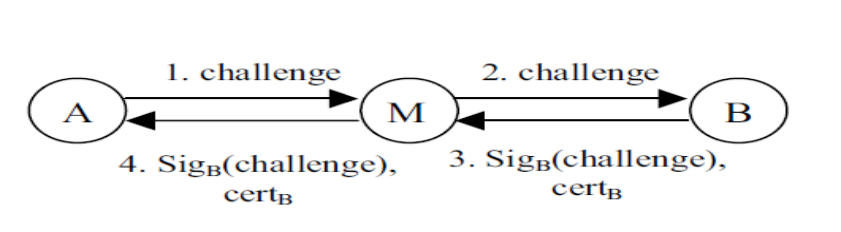
Εικόνα 27 Επίθεση πλαστοπροσωπίας (spoofing attack)[26]

Στην παραπάνω εικόνα (a) υπάρχει ένα μονοπάτι μεταξύ πέντε κόμβων. Ο κόμβος Α μπορεί να ακούσει τον κόμβο Β και τον κόμβο D, ο κόμβος Β μπορεί να ακούσει τον κόμβο Α και τον κόμβο C, ο κόμβος D μπορεί να ακούσει Α και C και κόμβος C μπορεί να ακούσει τους κόμβους Β,D και Ε. Ο κακόβουλος κόμβος Μ μπορεί να ακούσει τους κόμβους Α, Β, C και D ενώ ο κόμβος Ε μπορεί να ακούσει και τον επόμενο κόμβο στην διαδρομή προς τον Χ. Ένας κακόβουλος κόμβος Μ μπορεί να μάθει για την τοπολογία του δικτύου από ανάλυση των πακέτων και στη συνέχεια να σχηματίσει ένα βρόχο δρομολόγησης έτσι ώστε κανείς κόμβος από την σειρά του να μην μπορεί να φτάσει στον προορισμό Χ. Αρχικά ο κακόβουλος κόμβος Μ αλλάζει την MAC διεύθυνση του ώστε να ταιριάζει με αυτή του κόμβου Α προσεγγίζοντας έτσι περισσότερο τον κόμβο Β και αποφεύγοντας την περιοχή του κόμβου Α. Έπειτα στέλνει ένα μήνυμα στο κόμβο Β που περιέχει τον αριθμό των αλμάτων για τον κόμβο Χ η οποία είναι μικρότερη από εκείνη που απέστειλε ο κόμβος C, για παράδειγμα μηδέν. Τώρα ο κόμβος Β αλλάζει την διαδρομή του προς τον προορισμό του (Χ) ώστε να περάσουν από τον κόμβο Α όπως φαίνεται στην εικόνα (b). Ομοίως ο κακόβουλος κόμβος Μ αλλάζει ξανά την MAC διεύθυνση του ώστε να ταιριάζει με αυτή του κόμβου Β και έτσι να κινείται πιο κοντά στον κόμβο C και έξω από την περιοχή του κόμβου Β. Στη συνέχεια στέλνει μήνυμα στον C με τις πληροφορίες ότι η διαδρομή μέσω του κόμβου Β περιέχει μικρότερο αριθμό αλμάτων προς τον Χ από αυτόν του Ε. Τώρα ο κόμβος C αλλάζει τη διαδρομή του προς τον κόμβο Β το οποίο αποτελεί έναν βρόχο όπως φαίνεται στην παραπάνω εικόνα(c). Έτσι ο κόμβος Χ είναι απρόσιτος από τους τέσσερις κόμβους στο δίκτυο[26].

7.3.1 Επίθεση Αόρατου Κόμβου

Στα Manet η επικοινωνία γίνεται μέσω της πολλαπλής μετάδοσης (broadcasting). Αυτό κάνει την δρομολόγηση των Manet πρωτοκόλλων να υπόκεινται σε μία ειδική περίπτωση μιας «Man-in-the-Middle» επίθεσης , της *Επίθεσης Αόρατου Κόμβου (Invisible Node Attack)* . Στην απλούστερη μορφή του ο κακόβουλος αόρατος κόμβος Μ μεταδίδει τα πακέτα ώστε να μην αποκαλύπτει την παρουσία του στην διαδρομή της δρομολόγησης. Αυτή η επίθεση είναι πολύ εύκολο να εφαρμοστεί στα Manet: ο κακόβουλος κόμβος Μ βρίσκεται απλώς μεταξύ δύο κόμβων Α και Β που δεν

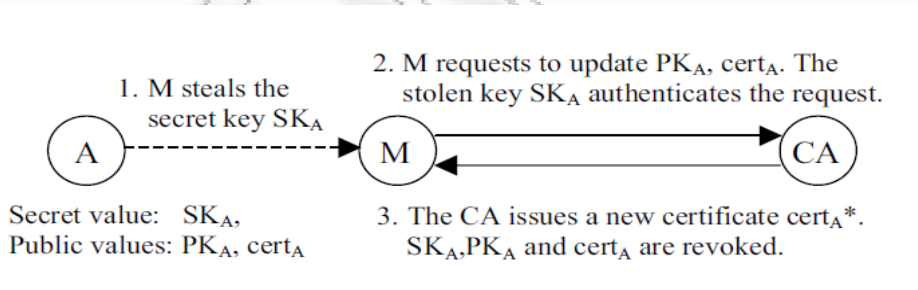
βρίσκονται στην άμεση περιοχή. Ο αόρατος κόμβος επαναλαμβάνει σιωπηλά την επικοινωνία μεταξύ των κόμβων A και B στο μονοπάτι δρομολόγησης που παραπλανητικά οι δυο έμπιστοι κόμβοι υποθέτουν ότι επικοινωνούν απευθείας. Με αυτόν τον τρόπο ο κακόβουλος κόμβος καταφέρνει να μιμείται τον κόμβο A στον κόμβο B και αντιστρόφως[27].



Εικόνα 28 Επίθεση Αόρατου Κόμβου

7.3.2 Επίθεση Κλεμμένων Ταυτοτήτων

Στην επίθεση *Κλεμμένων Ταυτοτήτων (Stolen Identity Attack)* ένας κόμβος καταφέρνει να κλέψει όλα τα πιστοποιητικά αναγνώρισης από έναν νόμιμο κόμβο, όπως τα πιστοποιημένα κλειδιά. Αν ο κακόβουλος κόμβος χρησιμοποιήσει το νόμιμο κόμβο στην ενημέρωση των κλεμμένων διαπιστευτηρίων μέσω της αρχής πιστοποίησης, στη συνέχεια τα διαπιστευτήρια του νόμιμου κόμβου δεν θα ισχύουν πλέον. Έτσι μόνο ο κακόβουλος κόμβος θα είναι σε θέση να χρησιμοποιήσει τα πιστοποιητικά και με αυτό τον τρόπο θα καταφέρει να κλέψει την ταυτότητα του κόμβου θύματος. Η απόκτηση των βασικών υπογραφών ενός κόμβου σε ένα PKI πιστοποιητικό δεν είναι μόνο θέμα για την κλοπή ταυτότητας ενός κόμβου αλλά και ένα θέμα της κατάχρησης των σχέσεων εμπιστοσύνης που άλλοι κόμβοι μπορεί να είχαν καθορίσει με τον κακόβουλο κόμβο[27].



Εικόνα 29 Επίθεση Κλεμμένων Ταυτοτήτων

7.3.3 Η Σιβυλλική επίθεση

Μια επίθεση «Sybil» είναι ουσιαστικά μια επίθεση πλαστογράφησης κατά την οποία ένας κακόβουλος κόμβος κατασκευάζει παράνομα πολλαπλές ταυτότητες και συμπεριφέρεται σαν να ήταν ένας μεγάλος αριθμό από κόμβους. Μια κακόβουλη συσκευή έχει επιπλέον ταυτότητες οι οποίες αναφέρονται ως Sybil ταυτότητές ή Sybil κόμβοι. Υπάρχουν τρεις τρόποι για την Σιβυλλική επίθεση (Sybil attack): η άμεση ή έμμεση επικοινωνία, οι συνθετικές(fabricated) ή οι κλεμμένες ταυτότητες και η σύμπτωση(simultaneity). Στη χειρότερη περίπτωση, ένας εισβολέας μπορεί να

δημιουργήσει έναν απεριόριστο αριθμό Sybil ταυτοτήτων χρησιμοποιώντας μόνο μία μόνο κακόβουλη συσκευή[31].

Άμεση επικοινωνία (Direct Communication). Ένας τρόπος για να εκτελέσει η σιβυλλική επίθεση είναι οι σιβυλλικοί κόμβοι να επικοινωνούν απευθείας με τους νόμιμους κόμβους. Αυτό σημαίνει ότι όταν ένας νόμιμος κόμβος στέλνει ένα μήνυμα σε έναν σιβυλλικό κόμβο, η κακόβουλη συσκευή ακούει το μήνυμα.

Έμμεση επικοινωνία (Indirect Communication). Σε αυτή την εκδοχή της επίθεσης οι νόμιμοι κόμβοι δεν μπορούν απευθείας να επικοινωνούν με τους σιβυλλικούς κόμβους. Μία ή περισσότερες κακόβουλες συσκευές απλώς ισχυρίζονται ότι είναι σε θέση να επιτύχουν μια σειρά από σιβυλλικούς κόμβους. Με αυτό τον τρόπο κάθε μήνυμα που αποστέλλεται σε έναν σιβυλλικό κόμβο διέρχεται από ένα από αυτούς τους κακόβουλους κόμβους οι οποίοι προσποιούνται να το περάσουν στον τελικό προορισμό[31].

Συνθετικές Ταυτότητες (Fabricated Identities). Εάν δεν υπάρχει κάποιος περιορισμός στο δικτύου για τις επιτρεπόμενες ταυτότητες ή κάποιος τρόπος να εξακριβωθεί ότι μια ταυτότητα είναι θεμιτή τότε ένας κακόβουλος κόμβος μπορεί να δημιουργήσει απλά μια αυθαίρετη ταυτότητα και να την χρησιμοποιήσει για να ενταχθεί στο δίκτυο.

Κλεμμένες Ταυτότητες (Stolen Identities). Εάν υπάρχουν μηχανισμοί για να εμποδίσουν τις εικονικές ταυτότητες από την προσχώρηση στο δίκτυο (για παράδειγμα ένας περιορισμένος αριθμός ονομάτων για την αποτροπή επιθέσεων από την προσθήκη νέων ταυτοτήτων), ο εισβολέας μπορεί να προσπαθήσει να εκχωρήσει νόμιμες ταυτότητες στους σιβυλλικούς κόμβους. Αυτή η κλοπή ταυτότητας μπορεί να περάσει απαρατήρητη εάν ο εισβολέας μπορεί με κάποιο τρόπο να απενεργοποιήσει τους κόμβους που υποδύοταν.

Ταυτόχρονες Ταυτότητες (Simultaneous Identities). Ενώ ένας συγκεκριμένος κόμβος μπορεί να διαφημίσει μόνο μία ταυτότητα σε μια στιγμή, μπορεί μέσω 'κύκλων' αυτών των ταυτοτήτων να φανεί ότι είναι παρόντες ταυτόχρονα πολλοί κόμβοι. Με τον τρόπο αυτό ο εισβολέας μπορεί να έχει όλες τις σιβυλλικές ταυτότητες που συμμετέχουν στο δίκτυο την ίδια στιγμή.

Μη Ταυτόχρονες Ταυτότητες (Non Simultaneous Identities). Εναλλακτικά, ο εισβολέας μπορεί να παρουσιάσει ένα μεγάλο αριθμό ταυτοτήτων σε μια χρονική περίοδο όπως επίσης ένα μικρότερο αριθμό ταυτοτήτων σε μια δεδομένη στιγμή. Επίσης, αν ο εισβολέας έχει πολλούς κόμβους σε κίνδυνο, μπορεί να κάνει περιοδική ανταλλαγή των ταυτοτήτων των κόμβων καθιστώντας ακόμη δυσκολότερο τον εντοπισμό τους[31].

Υπάρχουν πολλές εφαρμογές Σιβυλλικών επιθέσεων στα adhoc δίκτυα και αυτές φαίνονται παρακάτω:

Οι σιβυλλικές επιθέσεις δρομολόγησης (Routing Sybil Attacks) έχει αποδειχθεί ότι είναι αποτελεσματικές κατά των πρωτοκόλλων δρομολόγησης στα adhoc δίκτυα. Ένας ειδικά ευάλωτός μηχανισμός πολλαπλών μονοπατιών δρομολόγησης ή δρομολόγησης διασποράς στον οποίο φαινομενικά ασύνδετες πορείες θα μπορούσαν να συνδεθούν από έναν κακόβολό κόμβο ο οποίος διαθέτει πολλές διαφορετικές

σιβυλλικές ταυτότητες. Η γεωγραφική δρομολόγηση είναι ένα άλλος ευάλωτος μηχανισμός όπου ένας σιβυλλικός κόμβος θα μπορούσε να εμφανιστεί ταυτόχρονα σε περισσότερες από μία θέσεις.

Συγκέντρωση Δεδομένων (Data Aggregation). Συνήθως τα αποτελεσματικά πρωτόκολλα συγκεντρώνουν τα διάφορα δεδομένα στο δίκτυο για εξοικονόμηση ενέργειας αντί να κυκλοφορούν διαμοιρασμένα σε όλους τους κόμβους του δικτύου. Χρησιμοποιώντας τη Σιβυλλική επίθεση ένας κακόβουλος κόμβος μπορεί να συνεισφέρει στη συγκέντρωση πολλές φορές. Με αρκετούς Σιβυλλικούς κόμβους ένας επιτιθέμενος μπορεί να αλλάξει τα συγκεντρωμένα δεδομένα.

Ψηφοφορία (Voting). Η σιβυλλική επίθεση θα μπορούσε να χρησιμοποιηθεί για να αλλάξει το αποτέλεσμα ενός συστήματος ψηφοφορίας. Αν για παράδειγμα υπάρχει σε ένα δίκτυο ένα σύστημα ψηφοφορίας για τον προσδιορισμό ενός κόμβου με ανάρμοστη συμπεριφορά, ένας εισβολέας μπορεί να δημιουργήσει αρκετούς σιβυλλικούς κόμβους οι οποίοι θα είναι σε θέση να διαγράψουν κάθε κόμβο-στόχο από το δίκτυο (*blackmail attacks*). Αντιθέτως, αν υπάρχει μια ψηφοφορία για το αν η ταυτότητα ενός κόμβου είναι νόμιμη, ο εισβολέας θα μπορούσε να χρησιμοποιήσει τους σιβυλλικούς κόμβους ώστε εγγυηθεί την νομιμότητα του κατ άλλα κακόβουλου κόμβου.

Ανίχνευση Ανάρμοστης Συμπεριφοράς(Misbehavior Detection). Ας υποθέσουμε ότι ένα ad hoc δίκτυο έχει πιθανότητα να ανακαλύψει μια συγκεκριμένη μορφή κακής συμπεριφοράς. Είναι πιθανό να υπάρχουν ορισμένες πιθανότητες αποτυχίας εντοπισμού. Κατά συνέπεια, πιθανόν να μην ληφθούν μέτρα μέχρι να παρατηρηθούν επανειλημμένες προσπάθειες άμυνας από τον ίδιο κόμβο. Ένας επιτιθέμενος με πολλούς σιβυλλικούς κόμβους μπορεί να εξαπλώσει την αιτία χωρίς να έχει καμία σιβυλλική ταυτότητα με κακή συμπεριφορά ικανή να κάνει το δίκτυο να λάβει μέτρα άμυνας. Επιπλέον, αν η δράση που λαμβάνεται είναι για να ανακαλύψει τον επιτιθέμενο κόμβο, ο επιτιθέμενος μπορεί απλά να χρησιμοποιεί Σιβυλλικές ταυτότητες για να μην αποκαλυφθεί ο ίδιος.

Δίκαιη Κατανομή Πόρων(Fair Resource Allocation). Ορισμένοι πόροι του δικτύου μπορούν να ανατίθενται σε κάθε κάποιο συγκεκριμένο κόμβο. Αν για παράδειγμα, η κατανομή του σήματος γίνεται με τη χρήση για της τεχνικής *TDMA MAC*, με την σιβυλλική επίθεση ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε περισσότερες χρονοθυρίδες (timeslots) σε σχέση με άλλους κόμβους. Αυτό επιτρέπει στον επιτιθέμενο να αποκτήσει επιπλέον πηγές (δηλαδή χρόνο) για να εκτελέσει άλλες επιθέσεις[31].

7.4 Επίθεση Παρακολούθησης & Ανάλυσης Της Κίνησης Του Δικτύου

Η παρακολούθηση και η ανάλυση της κυκλοφορίας (Traffic Monitoring & Analysis) μπορούν να αναπτυχθούν για τον προσδιορισμό των κόμβων ενός δικτύου και των λειτουργιών τους οι οποίες θα μπορούσαν να παράσχουν στοιχεία για να διενεργηθούν επιθέσεις.

Το περιεχόμενο των πακέτων δεδομένων και ο τρόπος διεξαγωγής της κυκλοφορίας μπορεί να αποδειχθεί εξαιρετικά χρήσιμος για τους αντιπάλους. Για παράδειγμα, οι σημαντικές πληροφορίες για την τοπολογία του δικτύου μπορούν να προκύψουν από την ανάλυση των ρευμάτων κυκλοφορίας. Σε AdHoc δίκτυα οι κόμβοι που είναι πιο κοντά στο σταθμό βάσης κάνουν περισσότερές μεταδόσεις από τους άλλους κόμβους διότι αναμεταδίδουν τα πακέτα από τους κόμβους μακρύτερα από το σταθμό βάσης. Ομοίως, η ομαδοποίηση (clustering) αποτελεί ένα σημαντικό εργαλείο για την επεκτασιμότητα των adhoc δικτύων και οι κύριοι κόμβοι (cluster heads) αναλαμβάνουν περισσότερο την διεκπεραίωση της κίνησης από ό, τι οι άλλοι κόμβοι στο δίκτυο. Η ανίχνευση των κύριων αυτών κόμβων όπως επίσης και των κόμβων κοντά σε αυτούς μπορεί να είναι πολύ χρήσιμη για τους αντιπάλους επειδή οι DoS επιθέσεις εναντίον αυτών των κόμβων ή οι υποκλοπές των πακέτων που προορίζονται γι 'αυτούς μπορεί να έχουν μεγαλύτερες επιπτώσεις. Με την ανάλυση της κίνησης λοιπόν μπορούν να εξαχθούν το πολύτιμες πληροφορίες[4].

Η ανάλυση της κίνησης μπορεί επίσης να χρησιμοποιηθεί για την οργάνωση επιθέσεων κατά της ανωνυμίας (anonymity). Η ανίχνευση των κόμβων πηγής για ορισμένα πακέτα δεδομένων μπορεί επίσης να αποτελεί στόχο για τους αντιπάλους. Αυτές οι πληροφορίες βοηθούν να εντοπιστεί η τοποθεσία των εκδηλώσεων, οι αδυναμίες, οι δυνατότητες και οι λειτουργίες των κόμβων[4].

Επιπλέον, τα σχέδια κυκλοφορίας μπορεί να αφορούν και σε άλλες εμπιστευτικές πληροφορίες, όπως τις δράσεις και τις προθέσεις. Σε τακτικές επικοινωνίες, η σιωπή μπορεί να δείξει την προετοιμασία για μια επίθεση. Ομοίως, μια ξαφνική αύξηση του ποσοστό της κυκλοφορίας μπορεί να δηλώνει την έναρξη μιας σκόπιμης επίθεσης ή επιδρομής[4].

Οι παρακάτω τεχνικές μπορούν να χρησιμοποιηθούν για την ανάλυση της κυκλοφορίας στα διάφορα επίπεδα του προτύπου OSI:

- *Ανάλυση της κυκλοφορίας στο φυσικό επίπεδο:* σε αυτήν την επίθεση μόνο ο μεταφορέας ανιχνεύεται και οι συντελεστές της κυκλοφορίας αναλύονται για τους άλλους κόμβους στην περιοχή.

- *Ανάλυση της κίνησης στο επίπεδο ζεύξης δεδομένων (MAC) και σε υψηλότερα επίπεδα:* Τα πλαίσια (frames) του MAC πρωτοκόλλου και τα νέα πακέτα δεδομένων μπορεί να απόπολυπλεκτούν (demultiplexed) και έτσι οι επικεφαλίδες μπορούν να αναλυθούν. Αυτό μπορεί να αποκαλύψει τις πληροφορίες δρομολόγησης και την τοπολογία του δικτύου.

- *Ανάλυση της κίνησης από συσχέτιση ενός γεγονότος:* γεγονότα , όπως η μετάδοση από έναν τελικό χρήστη μπορεί να συσχετιστεί με την κυκλοφορία και πολύ λεπτομερείς πληροφορίες, π.χ. διαδρομές, κλπ., μπορούν να συναχθούν.

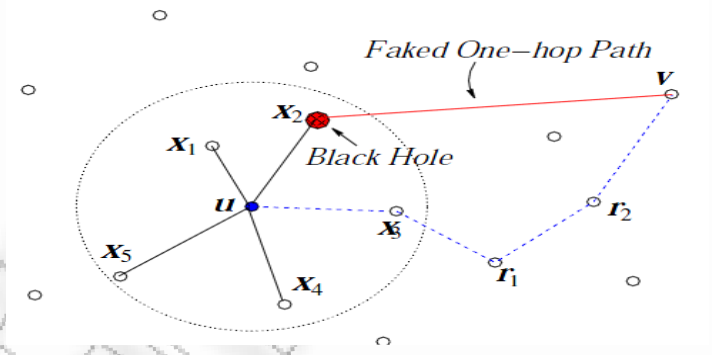
- *Ενεργός ανάλυση της κίνησης:* Η ανάλυση της κυκλοφορίας μπορεί να γίνεται και ως μια ενεργή επίθεση. Για παράδειγμα, ένας ορισμένος αριθμός κόμβων μπορούν να καταστραφούν προκαλώντας εκ νέου οργάνωση (self organization) του δικτύου και έτσι πολύτιμα δεδομένα για την τοπολογία μπορούν να συγκεντρωθούν[4].

7.5 Επίθεση Jellyfish

Ένας κακόβουλος κόμβος σε μια Jellyfish επίθεση μπορεί να δραστηριοποιείται τόσο στην ανακάλυψη της διαδρομής όσο και στην προώθηση των πακέτων προκειμένου να αποτρέψει την ανίχνευση και την διάγνωση τους και έτσι μπορεί να επιτεθεί και να αναδιατάξει, να καταστρέψει περιοδικά τα πακέτα και να αυξήσει τις επικίνδυνες καταστάσεις στο δίκτυο (jitters, πανικός) .Οπότε η jellyfish επίθεση είναι ιδιαίτερα επιβλαβής για την TCP κινητικότητα[20].

Αρχικά ένας jellyfish εισβολέας (μέδουσα) πρέπει πρώτα να εισέρθει στο δίκτυο. Στη συνέχεια για κάποιο χρονικό διάστημα καθυστερεί τα πακέτα δεδομένων χωρίς λόγο. Αυτό οδηγεί σε ιδιαίτερα υψηλή καθυστέρηση από άκρο σε άκρο του δικτύου και ως εκ τούτου υποβαθμίζει την απόδοση των εφαρμογών πραγματικού χρόνου. Ο επιτιθέμενος έτσι υλοποιεί πρώτα την rushing επίθεση για να αποκτήσει πρόσβαση στην διαδικασία δρομολόγησης. Αν η επίθεση είναι επιτυχής τότε καθυστερεί όλα τα πακέτα δεδομένων που λαμβάνει για ένα τυχαίο χρονικό διάστημα που κυμαίνεται από 0 έως 10 s πριν τη διαβίβασή τους[34].

Για παράδειγμα στην παρακάτω εικόνα χρησιμοποιείται το πρωτόκολλο TCP ως το πρωτόκολλο επιπέδου μεταφοράς. Ας υποθέσουμε επίσης ότι ο κόμβος X_2 είναι ο jellyfish κόμβος και ο κόμβος U αρχίζει να επικοινωνεί με τον κόμβο V μέσω του Jellyfish κόμβου. Στη συνέχεια η DoS επίθεση ξεκίνα από τον κόμβο X_2 ο οποίος θα προκαλέσει απώλεια πακέτων και θα διακόψει την επικοινωνία μεταξύ των κόμβων u και v[20].



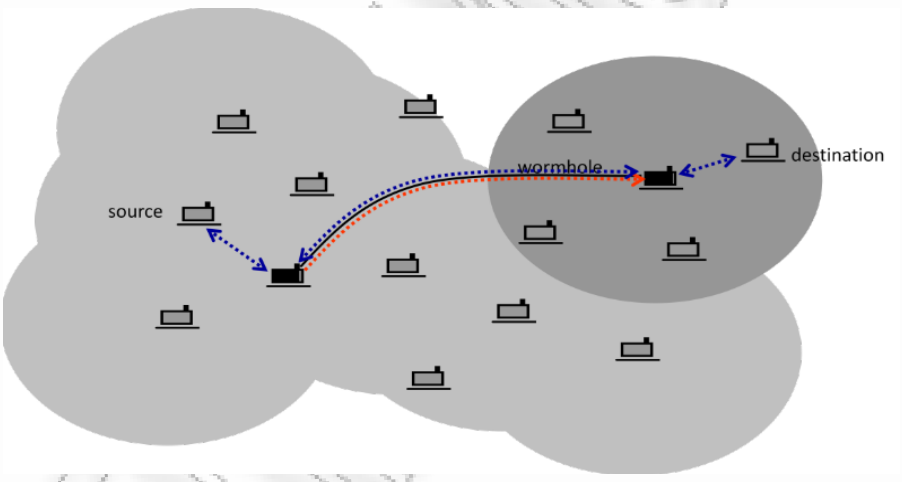
Εικόνα 30 Jellyfish Επίθεση

7.6 Επίθεση Gray Hole

Σε αυτό το είδος της επίθεσης ο επιτιθέμενος παραπλανά το δίκτυο με την υποψία ότι διαβιβάσει τα πακέτα. Μόλις λάβει τα πακέτα από το γειτονικό κόμβο ο επιτιθέμενος προκαλεί πτώση των πακέτων. Αυτό είναι ένα είδος ενεργής επίθεσης. Στην αρχή οι κόμβοι του επιτιθέμενου συμπεριφέρονται φυσιολογικά και απαντούν ορθά στα RREP μηνύματα των κόμβων που ξεκίνησαν τα RREQ μηνύματα. Όταν ο επιτιθέμενος λάβει τα πακέτα ξεκινά την ρίψη των πακέτων και την έναρξη μιας επίθεσης άρνησης παροχής υπηρεσιών (DoS)[38].

Πιο συγκεκριμένα η gray hole επίθεση έχει δύο φάσεις. Στην πρώτη φάση ο κακόβουλος κόμβος εκμεταλλεύεται το πρωτόκολλο AODV διαφημίζοντας τον εαυτό του πως έχει μια έγκυρη διαδρομή προς έναν κόμβο προορισμού έχοντας ως πρόθεση την σύλληψη των πακέτων ακόμη και αν η διαδρομή είναι πλαστή. Στη δεύτερη φάση ο κόμβος με μια ορισμένη πιθανότητα προκαλεί πτώση των παρακολουθούμενων πακέτων. Η επίθεση αυτή είναι πιο δύσκολή να εντοπιστεί από την επίθεση Μαύρης Τρύπας όπου ο κακόβουλος κόμβος προκαλεί με βεβαιότητα πτώση των πακέτων δεδομένων που έλαβε. Η gray hole επίθεση μπορεί να παρουσιάσει κακόβουλη συμπεριφορά με διαφορετικούς τρόπους. Μπορεί να μειώσει τα πακέτα που προέρχονται από (ή προορίζονται για) κάποιο συγκεκριμένο κόμβο-κόμβους στο δίκτυο και να διαβιβάζει όλα τα πακέτα άλλων κόμβων. Ένας άλλος τύπος gray hole κόμβου μπορεί να συμπεριφέρεται κακόβουλα για κάποιο χρονικό διάστημα «ρίχνοντας» τα πακέτα και μπορεί επίσης να στραφεί σε κανονική συμπεριφορά αργότερα. Μια gray hole επίθεση μπορεί να παρουσιάσει επίσης μια συμπεριφορά η οποία να είναι ένας συνδυασμός των δύο παραπάνω καθιστώντας έτσι τον εντοπισμό της ακόμη πιο δύσκολο[39].

Τέλος η επίθεση αυτή είναι γνωστή και ως **επίθεση επιλεκτικής προώθησης** και όπως βλέπουμε στην παρακάτω εικόνα μπορεί να συνδυαστεί με την επίθεση της σκουληκότρυπας.



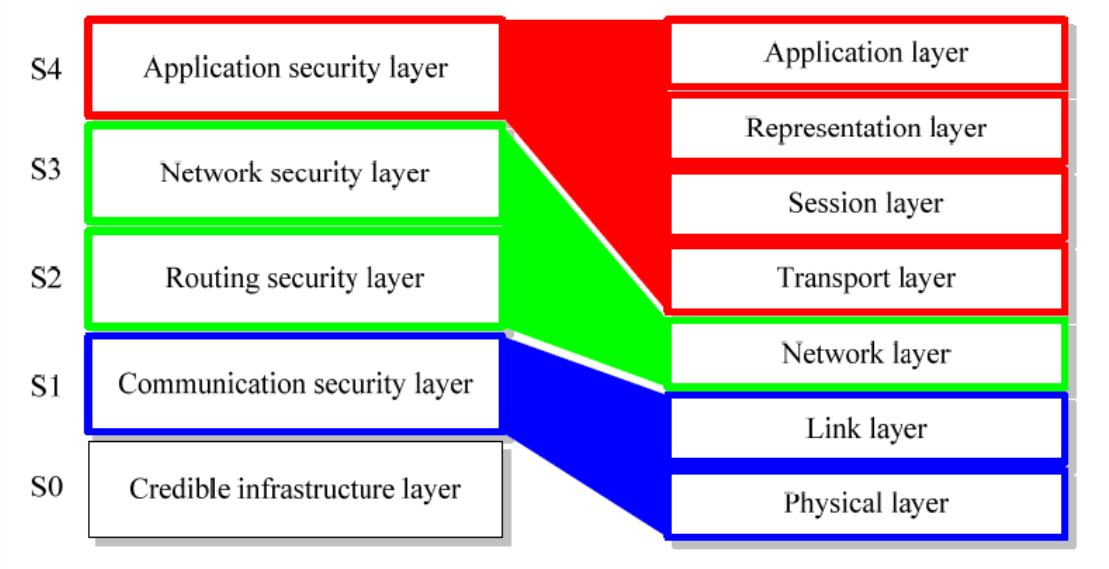
Εικόνα 31 Grayhole Επίθεση

Κεφάλαιο 8

Τρόποι αντιμετώπισης επιθέσεων στα Manet

8.1 Εισαγωγή

Τα πλεονεκτήματα της "σπονδυλωτής" κατασκευής (modularity), της ευελιξίας (flexibility), την τυποποίησης (standardization) του προτύπου OSI έχουν εφαρμοστεί με επιτυχία στο σχεδιασμό πρωτοκόλλων επικοινωνίας τα οποία αποτελούν ένα καλό παράδειγμα για την σχεδίαση πρωτόκολλων ασφαλείας. Σύμφωνα με την ιδέα του μοντέλου OSI η σχέση του στον σχεδιασμό της αρχιτεκτονικής ασφαλείας στα δίκτυα Manet φαίνεται στην παρακάτω εικόνα.



Εικόνα 32 Αρχιτεκτονική ασφαλείας των δικτύων Manet σε σχέση με το πρότυπο OSI

Η επιτυχία των δικτύων Manet εξαρτάται σε μεγάλο βαθμό από το αν οι κανόνες ασφαλείας είναι έμπιστοι. Ωστόσο τα χαρακτηριστικά των Manets δημιουργούν προκλήσεις αλλά και ευκαιρίες για την επίτευξη των στόχων ασφάλειας όπως η εμπιστευτικότητα (confidentiality), η ταυτοποίηση (authentication), η ακεραιότητα (integrity), η διαθεσιμότητα (availability), ο έλεγχος πρόσβασης (access control) και η μη άρνηση αναγνώρισης ή μη αποποίησης ευθυνών (non-repudation)[21].

Οι κινητοί κόμβοι που σχηματίζουν ένα δίκτυο Manet είναι συνήθως κινητές συσκευές με περιορισμένη φυσική προστασία όσο και περιορισμένους πόρους. Ενότητες ασφαλείας όπως οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για την προστασία από φυσικές επιθέσεις. Τα κρυπτογραφικά εργαλεία που χρησιμοποιούνται ευρέως για την παροχή ισχυρών υπηρεσιών ασφαλείας όπως είναι η εμπιστευτικότητα, η επαλήθευση της ακεραιότητας και η μη άρνηση αναγνώρισης. Δυστυχώς η κρυπτογράφηση δεν μπορεί να εγγυηθεί τη διαθεσιμότητα. Για παράδειγμα, δεν μπορεί να αποτρέψει την εμπλοκή με το ραδιόφωνο. Εν τω μεταξύ η ισχυρή κρυπτογράφηση απαιτεί συχνά ένα δύσκολο υπολογισμό ο οποίος ως επί το

πλείστον περιορίζονται από τις δυνατότητες των συσκευών (π.χ. της CPU ή της μπαταρίας)[21].

Τα χαρακτηριστικά και η φύση των Manets απαιτούν τη στενή συνεργασία των κινητών συμμετεχόντων που φιλοξενούν. Ορισμένες τεχνικές ασφαλείας που έχουν εφευρεθεί όπως και ένας κατάλογος πρωτοκόλλων ασφάλειας έχει προτείνει την επιβολή συνεργασίας και την αποφυγή ανάρμοστης συμπεριφοράς με τους εξής τρόπους: 802,11 WEP, IPsec, SEAD, SAODV, SRP, ARAN, SSL κτλ. Ωστόσο καμία από αυτές τις προληπτικές προσεγγίσεις δεν είναι τέλεια ή ικανή να αντικρούσει όλες τις επιθέσεις. Μια δεύτερη γραμμή άμυνας που ονομάζεται Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection Systems) προτείνεται και εφαρμόζεται στα Manet. Τέτοια συστήματα (IDS) είναι μερικά από τα πιο σύγχρονα εργαλεία ασφάλειας στην καταπολέμηση των επιθέσεων. Τα κατανεμημένα IDS εισήχθησαν στα Manet για την παρακολούθηση είτε της ανάρμοστης συμπεριφοράς είτε της ιδιοτέλειας των κινητών κόμβων που φιλοξενούν[21]. Οι μηχανισμοί αυτοί ασφαλείας μπορούν να ταξινομηθούν σε δυο κατηγορίες οι οποίες αναλύονται παρακάτω:

- *Μηχανισμοί Πρόληψης (Preventive Mechanism):* Η συμβατική ταυτοποίηση των συστημάτων κρυπτογράφησης βασίζεται στην κρυπτογραφία η οποία περιλαμβάνει την ασύμμετρη και την συμμετρική κρυπτογραφία. Η λειτουργία της κρυπτογράφησης όπως η hash (message digest) μπορεί να χρησιμοποιηθεί για την ενίσχυση της ακεραιότητας των δεδομένων κατά τη διαβίβαση. Επίσης η κρυπτογραφία μπορεί να χρησιμοποιηθεί για την απόκρυψη στοιχείων χωρίζοντάς τα σε διάφορα μέρη. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για την επίτευξη της ακεραιότητας των δεδομένων και των υπηρεσιών ελέγχου ταυτότητας.

  Είναι επίσης αναγκαίο να εξεταστεί η φυσική ασφάλεια των κινητών συσκευών δεδομένου ότι οι κόμβοι είναι συνήθως μικρές συσκευές οι οποίες είναι «φυσικά» ευάλωτες. Για παράδειγμα, μια συσκευή θα μπορούσε εύκολα να κλαπεί, να απολεσθεί, να καταστραφεί στο πεδίο της μάχης που βρίσκεται, να τεθεί σε κίνδυνο υπό ομηρία κτλ. Η προστασία των ευαίσθητων δεδομένων σε μια φυσική συσκευή μπορεί να επιβληθεί από ορισμένες μονάδες ασφαλείας, όπως οι έξυπνες κάρτες που είναι προσβάσιμες μέσω του PIN, συνθηματικών φράσεων ή χρήσης βιομετρικών στοιχείων. Παρά το γεγονός ότι όλες αυτές οι κρυπτογραφικές τεχνικές συνδυασμένες μπορούν να αποτρέψουν περισσότερες επιθέσεις στη θεωρία, στην πραγματικότητα λόγω του σχεδιασμού, της εκτέλεσης ή της επιλογής των πρωτοκόλλων και των φυσικών περιορισμών της συσκευής, υπάρχουν ακόμη πολλές κακόβουλες επιθέσεις οι οποίες παρακάμπτουν τους μηχανισμούς πρόληψης.

- *Αντιδραστικοί Μηχανισμοί (Reactive Mechanism):* Ένα σύστημα ανίχνευσης εισβολής (Intrusion Detection System) είναι μια δεύτερη γραμμή άμυνας και υπάρχουν ευρέως πολλά που χρησιμοποιούνται για την ανίχνευση της κακής χρήσης και των ανωμαλιών. Ένα σύστημα ανίχνευσης κατάχρησης προσπαθεί να ορίσει την ανάρμοστη συμπεριφορά με βάση τα πρότυπα των γνωστών επιθέσεων αλλά στερείται της δυνατότητας να ανιχνεύει τυχόν επιθέσεις που δεν ελήφθησαν υπόψη κατά τη δημιουργία των μοντέλων. Οι προσπάθειες ανίχνευσης ανωμαλιών για τον καθορισμό της κανονικής ή αναμενόμενης συμπεριφοράς γίνεται με βάση κάποια στατιστικά όπως για παράδειγμα τη

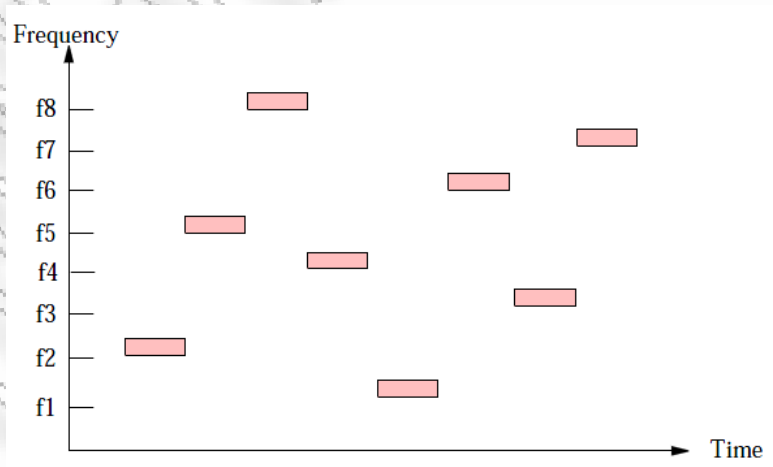
συλλογη στοιχείων από μια νόμιμη συμπεριφορά του χρήστη κατά τη διάρκεια μιας χρονικής περιόδου και στη συνέχεια εφαρμογή των στατιστικών δοκιμών για τον προσδιορισμό της ανώμαλης συμπεριφοράς με ένα υψηλό επίπεδο εμπιστοσύνης. Στην πράξη, οι δύο προσεγγίσεις μπορούν να συνδυαστούν για να είναι πιο αποτελεσματική η καταπολέμηση των επιθέσεων[21].

Τώρα θα αναφερθούμε στην αντιμετώπιση των επιθέσεων στα Manet ταξινομημένων στο πρότυπο OSI

8.2 Αντιμετώπιση Επιθέσεων στο Φυσικό Επίπεδο

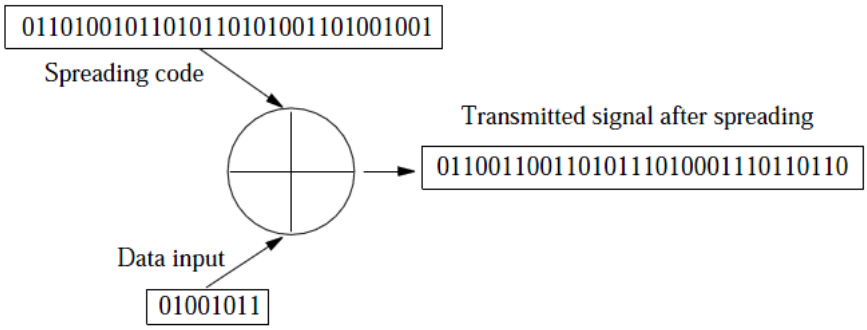
Δεδομένου ότι η ασύρματη επικοινωνία μεταδίδεται από τη φύση και ένα κοινό ραδιοφωνικό σήμα είναι εύκολο να τροποποιηθεί και έτσι η διάδοση της τεχνολογίας του ραδιοφάσματος όπως η συχνότητα hopping (FHSS) ή η άμεση ακολουθία (DSSS) μπορεί να καταστήσει δύσκολο να εντοπιστούν ή να τροποποιηθούν τα σήματα. Οι τεχνολογίες αυτές αλλάζουν την συχνότητα κατά τυχαίο τρόπο κάνοντας έτσι δύσκολη την σύλληψη του σήματος ή την εξάπλωση της ενέργειας σε ένα ευρύτερο φάσμα ώστε η ισχύς μετάδοσης να είναι κρυμμένη πίσω από το επίπεδο θορύβου. Οι κατευθυντικές κεραίες μπορούν επίσης να αναπτυχθούν λόγω του γεγονότος ότι οι τεχνικές επικοινωνίας μπορεί να σχεδιαστούν για να διαδώσουν την ενέργεια του σήματος στο διάστημα.

Frequency Hopping Spread Spectrum (FHSS): Το σήμα είναι διαμορφωμένο με μια φαινομενικά τυχαία σειρά ραδιοσυχνοτήτων οι οποίες μεταπηδούν (hops) από συχνότητα σε συχνότητα σε τακτά χρονικά διαστήματα. Ο δέκτης χρησιμοποιεί τον ίδιο κώδικα εξάπλωσης ο οποίος είναι συγχρονισμένος με τον πομπό ώστε να ανασυνδυάζεται με τα σήματα εξάπλωσης στην αρχική τους μορφή. Η παρακάτω εικόνα δείχνει ένα παράδειγμα μιας FHSS. Με τον πομπό και το δέκτη να συγχρονίζονται σωστά, τα δεδομένα μεταδίδονται πάνω από ένα κανάλι. Ωστόσο, το σήμα φαίνεται στους υποκλοπείς να είναι ένας ακατάληπτος παλμικός θόρυβος διάρκειας. Εν τω μεταξύ η παρεμβολή ελαχιστοποιείται δεδομένου ότι το σήμα έχει διασπαστεί σε πολλές συχνότητες.



Εικόνα 33 Παράδειγμα FHSS

Direct Sequence Spread Spectrum DSSS: Κάθε bit δεδομένων στο αρχικό σήμα αναπαρίσταται με πολλαπλά bits του εκπεμπόμενου σήματος χρησιμοποιώντας τους κώδικες διασκορπισμού (spreading code). Οι κώδικες διασκορπισμού απλώνουν το σήμα σε μια ευρύτερη ζώνη συχνοτήτων άμεσης αναλογίας προς τον αριθμό των χρησιμοποιηθέντων bits. Ο δέκτης μπορεί να χρησιμοποιήσει τους κώδικες διασκορπισμού με το σήμα για να ανακτήσει τα αρχικά δεδομένα. Η παρακάτω εικόνα δείχνει ότι το κάθε αρχικό κομμάτι των δεδομένων εκπροσωπείται από 4 bits του εκπεμπόμενου σήματος. Το πρώτο κομμάτι των δεδομένων, το 0, μεταδίδεται σαν 0110 τα οποία είναι το πρώτο από τα 4 bits του κώδικα που εξαπλώνεται. Το δεύτερο κομμάτι, το 1, μεταδίδεται σαν 0110 το οποίο είναι το δυαδικό συμπλήρωμα του δεύτερου από τα τέσσερα bits του κώδικα διασκορπισμού. Στη συνέχεια, κάθε bit εισόδου είναι συνδυασμός με αποκλειστικό ή (xor) με τα τέσσερα bit του κώδικα διασκορπισμού.



Εικόνα 34 Παράδειγμα DSSS

Τόσο στο FHSS όσο και στο DSSS συνεπάγονται δυσκολίες για τους ξένους που προσπαθούν να αναχαιτίσουν τα ραδιοσήματα. Ο υποκλοπέας πρέπει να γνωρίζει τη ζώνη συχνοτήτων, τους κώδικες διασκορπισμού και τις τεχνικές διαμόρφωσης για να διαβάσει σωστά τα μεταδιδόμενα σήματα. Το γεγονός ότι οι τεχνολογίες ευρέσεως φάσματος δεν συνεργάζονται μεταξύ τους, προσθέτει περαιτέρω δυσκολίες στην υποκλοπέα. Η τεχνολογία των κωδίκων διασκορπισμού του ραδιοφάσματος ελαχιστοποιεί επίσης το ενδεχόμενο παρεμβολών από άλλα ραδιόφωνα και ηλεκτρομαγνητικές συσκευές [21].

8.3 Αντιμετώπιση Επιθέσεων στο Επίπεδο Ζεύξης Δεδομένων

Υπάρχουν κακόβουλες επιθέσεις που στοχεύουν στο επίπεδο ζεύξης δεδομένων με την διακοπή της συνεργασίας των πρωτοκόλλων αυτού του επιπέδου. Τα πρωτόκολλα του επιπέδου ζεύξης δεδομένων βοηθούν στην ανακάλυψη των “κοντινών (1-hop)” γειτόνων, στην δίκαιη πρόσβαση στο κανάλι, στο πλαίσιο ελέγχου σφαλμάτων και διατηρούν τις συνδέσεις με τους γείτονες. Οι κακόβουλοι κόμβοι όπως έχουμε αναφέρει θα μπορούσαν να παρακούσουν τον κανόνα πρόσβασης του καναλιού, να χειριστούν το πεδίο NAV, να εξαπατήσουν τις αξίες του backoff κτλ ώστε να μεγιστοποιηθεί η κυκλοφορία τους. Οι γείτονες οπότε θα πρέπει να παρακολουθούν αυτές τις ανάρμοστες συμπεριφορές. Αν και οι επιθέσεις αυτές εξακολουθούν να είναι μια ανοιχτή πρόκληση και ορισμένα προγράμματα όπως το ERA-802.11 προτείνουν κάποιους αλγόριθμους ανίχνευσης. Η ανάλυση της κίνησης στο επίπεδο ζεύξης δεδομένων εμποδίζεται από κρυπτογράφηση των δεδομένων.

Το Wired Equivalent privacy (WEP) σύστημα κρυπτογράφησης που ορίζεται στο πρότυπο IEEE 802.11 των ασύρματων τοπικών δικτύων LAN χρησιμοποιεί την κρυπτογράφηση συνδέσμου για να κρύψει την «end-to-end» ροή των πληροφοριών. Ωστόσο, το WEP όπως έχουμε δει έχει επικριθεί ευρέως για τις αδυναμίες του. Από την άλλη έχουν προταθεί ορισμένα ασφαλή πρωτόκολλα του επιπέδου ζεύξης δεδομένων όπως το LLSP[21].

Το πρωτόκολλο Link Layer Security Protocol (LLSP) είναι υπεύθυνο για τον έλεγχο της ταυτοποίησης και της κρυπτογράφησης στο επίπεδο Ζεύξης Δεδομένων. Η ταυτοποίηση επιτρέπει στον παραλήπτη ενός ψηφιακού μηνύματος να γνωρίζει την ταυτότητα του αποστολέα. Επίσης, διασφαλίζει την ακεραιότητα των πληροφοριών. Από την άλλη πλευρά, η κρυπτογράφηση διασφαλίζει ότι οι πληροφορίες που μεταδίδονται είναι αναγνώσιμες μόνο από έμπιστους παραλήπτες. Για την ενίσχυση της λειτουργίας ασφαλείας του επιπέδου ζεύξης δεδομένων, ο μηχανισμός «Watchdog» του πρωτοκόλλου LLSP του κάθε γείτονα ενημερώνει το στρώμα MAC ώστε να λάβει τα αναγκαία μέτρα για την εσφαλμένη συμπεριφορά των γειτόνων. Οι υπηρεσίες της ασφάλειας που παρέχονται από LLSP μπορεί να καταταγούν σε πέντε (5) τύπους:

1. Ταυτοποίηση ενός νέου κόμβου,
2. Ενημέρωση της ικανότητας (capability - CAP) του συνδέσμου,
3. Ενημέρωση του κλειδιού (SHK) ενός συνδέσμου,
4. Ταυτοποίηση των ληφθέντων πακέτων
5. Κρυπτογράφηση του ωφέλιμου φορτίου[40].

Συγκριμένα ο έλεγχος ταυτότητας της πρώτης κατηγορίας ανανεώνει περιοδικά την ικανότητα και το κλειδί του συνδέσμου, οι υπηρεσίες ασφαλείας τύπου 2 και 3 βασίζονται σε ένα μηχανισμό ψηφιακής υπογραφής ο οποίος χρησιμοποιεί ένα ασύμμετρο κρυπτογραφικό σύστημα όπως το RSA (Rivest, Shamir and Adleman). Για την τακτική ενημέρωση των πακέτων (πακέτα δηλαδή που δεν χρησιμοποιούνται από τους τύπους 1-3) στον τύπο 4, το πρωτόκολλο LLSP εφαρμόζει συμμετρική κρυπτογραφία π.χ. AES (Advanced Encryption System) σε έναν αριθμό ακολουθίας (SEQ) και το άθροισμα ελέγχου των μηνυμάτων. Η κρυπτογράφηση του τύπου 5 ολοκληρώνεται με ένα συμβολικό μετρικό κρυπτογράφησης (π.χ. AES) χρησιμοποιώντας το περιοδικά ανανεωμένο κλειδί SHK. Η πρόβλεψη για τον κρυπτογραφημένο αύξων αριθμό (encrypted sequence number) και το άθροισμα έλεγχου (checksum) παρέχει καλύτερη προστασία από επιθέσεις επανάληψης (replay attacks)[40].

8.4 Αντιμετώπιση Επιθέσεων στο Επίπεδο Δικτύου

Οι παθητικές επιθέσεις σε πληροφορίες δρομολόγησης μπορεί να αντιμετωπιστούν με τις ίδιες μεθόδους με τις οποίες προστατεύονται τα δεδομένα κίνησης. Ορισμένες ενεργές επιθέσεις όπως η παράνομη τροποποίηση των μηνυμάτων δρομολόγησης μπορούν να προληφθούν με μηχανισμούς ελέγχου προέλευσης της ταυτότητας του μηνύματος όπως και της ακεραιότητας. Οι DoS επιθέσεις μπορούν να περιοριστούν αποτρέποντας τον εισβολέα από την εισαγωγή βρόχων δρομολόγησης, από την επιβολή μέγιστου μήκους διαδρομής που ακολουθεί ένα πακέτο κτλ. Η επίθεση σκουληκότρυπας μπορεί να ανιχνευθεί με την καθυστέρηση του χρόνου ή την

τροποποίηση της γεωγραφικής περιοχής. Για παράδειγμα, τα packet leashes (λουριά πακέτου) χρησιμοποιούνται για την καταπολέμηση των επιθέσεων σκουληκότρυπας.

Σε γενικές γραμμές με ένα είδος μηχανισμού αυθεντικότητας και ακεραιότητας που χρησιμοποιείται , είτε με την «hop-by-hop» ή την «end-to-end» προσέγγιση, εξασφαλίζεται η ορθότητα των πληροφοριών δρομολόγησης. Για παράδειγμα, η ψηφιακή υπογραφή, η μονόδρομη hash συνάρτηση, η αλυσίδα hash, το πρωτόκολλο MAC και ο κρυπτογραφημένος κωδικός πιστοποίησης μηνύματος (Hashed Message Authentication Code) χρησιμοποιούνται ευρέως για το σκοπό αυτό. Τα πρωτόκολλα ασφαλείας του επιπέδου δικτύου IPsec και ESP (Encapsulating Security Protocol) που χρησιμοποιούνται στο διαδίκτυο θα μπορούσαν επίσης να χρησιμοποιηθούν στα Manet υπό ορισμένες περιστάσεις όπως να παράσχουν έλεγχο της ταυτότητας του πακέτου δεδομένων καθώς και ένα ορισμένο επίπεδο εμπιστευτικότητας. Επιπλέον έχουν σχεδιαστεί ορισμένα πρωτόκολλα υπεράσπισης ενάντια κακόβουλων κόμβων οι οποίοι σκοπεύουν να εξοικονομήσουν πόρους και να αποτρέψουν την συνεργασία των δικτύων[21].

Παρακάτω παραθέτουμε ορισμένα μέτρα αντιμετώπισης διάφορων επιθέσεων που συμβαίνουν στο επίπεδο δικτύου.

8.4.1 Αντιμετώπιση Επιθέσεων Σκουληκότρυπας

Ένα πακέτο-λουρί το οποίο περιλαμβάνει τις πληροφορίες που προστίθενται σε ένα πακέτο για να περιορίσει την απόσταση εκπομπής του, έχει σχεδιαστεί ως αντίμετρο στην επίθεση **σκουληκότρυπας** (wormhole attack). Ο μηχανισμός τομέα (Sector mechanism) προτείνεται για να ανιχνεύσει σκουληκότρυπες χωρίς την ανάγκη συγχρονισμού του ρολογιού. Οι κατευθυντικές κεραίες (directional antennas) προτείνονται επίσης για την αποτροπή των επιθέσεων σκουληκότρυπας.

Για να αντιμετωπιστούν οι επιθέσεις σκουληκότρυπας έχουν γίνει κάποιες προσπάθειες στον σχεδιασμό του υλικού και των τεχνικών επεξεργασίας σήματος. Εάν τα bits δεδομένων μεταβιβάζονται με κάποια ειδική μέθοδο διαμόρφωσης γνωστή μόνο στους γειτονικούς κόμβους, τότε αυτοί είναι ανθεκτικοί σε επιθέσεις σκουληκότρυπας. Μια άλλη πιθανή λύση είναι να ενσωματωθούν μέθοδοι πρόληψης σε συστήματα ανίχνευσης κινήσεων (IDS). Ωστόσο, είναι δύσκολο να απομονωθεί ο επιτιθέμενος με μια προσέγγιση λογισμικού δεδομένου ότι τα πακέτα που αποστέλλονται από τη σκουληκότρυπα είναι πανομοιότυπα με τα πακέτα που αποστέλλονται από τους νόμιμο κόμβους.

Παραπάνω αναφέραμε ότι τα πακέτα λουριών (Packet leashes) προτείνονται για την ανίχνευση επιθέσεων σκουληκότρυπας. Πιο συγκεκριμένα αυτά λειτουργούν ως εξής: ένα πακέτο λουριού θέτει τη διάρκεια ζωής ενός πακέτου το οποίο προσθέτει έναν περιορισμό για την απόσταση εκπομπής του. Ένας αποστολέας περιλαμβάνει το χρόνο μετάδοσης και την τοποθεσία του μηνύματος. Ο δέκτης επαληθεύει αν το πακέτο έχει διανύσει την απόσταση μεταξύ του αποστολέα και του ίδιου εντός του χρονικού διαστήματος μεταξύ της λήψης και διαβίβασης του. Τα πακέτα λουριών απαιτούν άρτια συγχρονισμένα ρολόγια και ακριβή γνώση της τοποθεσίας.

Ο μηχανισμός τομέα βασίζεται κατά κύριο λόγο στην εξ αποστάσεως-οριοθέτηση τεχνικών, στην μονόδρομη hash αλυσίδα και στο δέντρο κατακερματισμού Merkle. Ο

τομέας μπορεί να χρησιμοποιηθεί για την πρόληψη των επιθέσεων σκουληκότρυπας στα Manet χωρίς να απαιτείται ρολόι συγχρονισμού ή πληροφορίες τοποθεσίας. Ο τομέας μπορεί επίσης να χρησιμοποιηθεί για να βοηθήσει τα ασφαλή πρωτόκολλα δρομολόγησης στα Manet στην ανίχνευση εξαπάτησης μέσω του εντοπισμού της τοπολογίας.

Τέλος οι κατευθυντικές κεραίες δεν απαιτούν πληροφορίες για τον εντοπισμό ή συγχρονισμό του ρολογιού και είναι πιο αποτελεσματικές με την ενέργεια[21].

8.4.2 Αντιμετώπιση Επιθέσεων Μαύρης Τρύπας.

Μερικά ασφαλή πρωτόκολλα δρομολόγησης, όπως το **Secure-Aware Ad Hoc Routing Protocol (SAR)** μπορούν να χρησιμοποιηθούν για να υπερασπιστούν τις επιθέσεις μαύρης τρύπας (blackhole attacks). Το πρωτόκολλο SAR βασίζεται στα on-demand πρωτόκολλα, όπως το AODV ή το DSR. Στο SAR ένα μετρο ασφαλείας προστίθεται στο πακέτο RREQ και μια διαφορετική διαδικασία ανακάλυψης διαδρομής χρησιμοποιείται. Οι ενδιάμεσοι κόμβοι λαμβάνουν ένα πακέτο RREQ με μια συγκεκριμένη ασφάλεια ή ένα επίπεδο εμπιστοσύνης. Στους ενδιάμεσους κόμβους όταν η εγγύηση της ασφάλειας ή το επίπεδο εμπιστοσύνης είναι ικανοποιητικό, ο κόμβος θα επεξεργάζεται το πακέτο RREQ και θα το διαδίδει στους γείτονές του με ελεγχόμενες πλημμύρες(controlled floodings). Διαφορετικά, το RREQ θα καταστραφεί. Εάν ένα «end-to-end» μονοπάτι με τα απαιτούμενα χαρακτηριστικά ασφαλείας μπορεί να βρεθεί, ο προορισμός θα δημιουργήσει ένα πακέτο RREP με την συγκεκριμένη ασφάλεια. Αν ο κόμβος προορισμού αποτυγχάνει να βρει μια διαδρομή με την απαιτούμενη ασφάλεια ή το επίπεδο εμπιστοσύνης, στέλνει μια ειδοποίηση στον αποστολέα και επιτρέπει στον αποστολέα να ρυθμίσει το επίπεδο ασφαλείας, προκειμένου να βρεθεί μια διαδρομή[21].

Για την εφαρμογή του πρωτοκόλλου SAR είναι απαραίτητο να δεσμευτεί η ταυτότητα του χρήστη με ένα σχετικό επίπεδο εμπιστοσύνης. Για να αποτραπεί η κλοπή της ταυτότητας απαιτούνται ισχυρότεροι μηχανισμοί ελέγχου πρόσβασης, όπως η πιστοποίηση της ταυτότητας. Στο SAR ένα απλό κοινό μυστικό χρησιμοποιείται για να δημιουργήσει ένα συμμετρικό κλειδί κρυπτογράφησης/αποκρυπτογράφησης ανά επίπεδο εμπιστοσύνης. Τα πακέτα είναι κρυπτογραφημένα χρησιμοποιώντας το κλειδί που συνδέεται με το επίπεδο εμπιστοσύνης και οι κόμβοι που ανήκουν σε διαφορετικά επίπεδα δεν μπορούν να διαβάσουν τα πακέτα RREQ ή RREP. Θεωρείται επίσης δεδομένο ότι ένας ξένος δεν μπορεί να αποκτήσει το κλειδί.

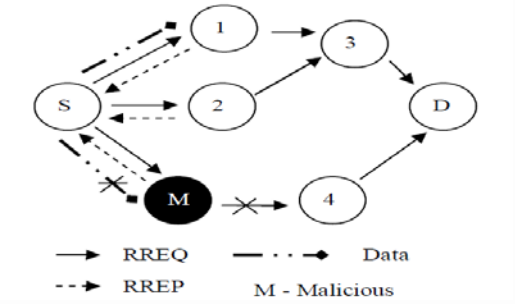
Σε SAR ένας κακόβουλος κόμβος που διακόπτει τη ροή των πακέτων με την αλλαγή του μέτρου της ασφάλειας σε ένα υψηλότερο ή χαμηλότερο επίπεδο δεν μπορεί να προκαλέσει σοβαρές ζημιές επειδή οι ενδιάμεσοι νόμιμοι ή κόμβοι προορισμού υποτίθεται ότι θα μειώσουν το πακέτο και ο εισβολέας δεν είναι σε θέση να αποκρυπτογραφήσει το πακέτο. Το πρωτόκολλο SAR παρέχει μια σειρά από μεθόδους κρυπτογράφησης, όπως η ψηφιακή υπογραφή και η κρυπτογράφηση οι οποίες μπορούν να ενσωματωθούν με βάση την ανάγκη για την πρόληψη της τροποποίησης[21].

Το **SAODV** (Secure Ad hoc On Demand Distance Vector) πρωτόκολλο είναι μια επέκταση του πρωτοκόλλου AODV και είναι και αυτό αποτελεσματικό στις επιθέσεις μαύρης τρύπας. Το ασφαλές (secure) AODV σύστημα βασίζεται στην υπόθεση ότι κάθε κόμβος κατέχει τα πιστοποιημένα δημόσια κλειδιά όλων των κόμβων του δικτύου[2].

Ο δημιουργός των πακέτων ελέγχου της δρομολόγησης προσαρτά την RSA υπογραφή του και το τελευταίο στοιχείο μιας hash αλυσίδας στα πακέτα δρομολόγησης. Με ένα εγκάρσιο πακέτο του δικτύου οι ενδιάμεσοι κόμβοι επικυρώνουν κρυπτογραφικά την υπογραφή και την τιμή hash. Οι ενδιάμεσοι κόμβοι παράγουν το $K_{\text{-ιστό}}$ στοιχείο της αλυσίδας hash, με k να είναι ο αριθμός των εγκάρσιων βημάτων (hops) και έπειτα τοποθετείται στο πακέτο[2].

Το πρωτόκολλο SAODV δίνει δύο εναλλακτικές λύσεις για τα μηνύματα “Route Request” και “Route Reply” . Στην πρώτη περίπτωση, όταν ένα αίτημα “Route Request” αποστέλλεται, ο αποστολέας δημιουργεί μια υπογραφή και την προσθέτει στο πακέτο. Οι ενδιάμεσοι κόμβοι επικυρώνουν την υπογραφή πριν από τη δημιουργία ή την ταυτοποίηση της αντίστροφης διαδρομής προς την πηγή. Η αντίστροφη διαδρομή αποθηκεύεται μόνο όταν η υπογραφή έχει επαληθευτεί. Όταν ο κόμβος φτάσει στον προορισμό του, υπογράφει την απάντηση Route Reply με το ιδιωτικό του κλειδί και την αποστέλλει πίσω. Οι ενδιάμεσοι κόμβοι ελέγχουν πάλι την υπογραφή. Η υπογραφή του αποστολέα αποθηκεύεται πάλι μαζί με την νέα διαδρομή[2].

Στην παρακάτω εικόνα ο κόμβος S θέλει να μεταδώσει στον κόμβο D. Γι 'αυτό μεταδίδει πρώτο το αίτημα RREQ προς όλους τους γειτονικούς του κόμβους. Ο κόμβος 1, ο κόμβος M και ο κόμβος 2 δέχονται το αίτημα αυτό. Ο κακόβουλος κόμβος M δεν έχει καμία πρόθεση να διαβιβάσει τα πακέτα δεδομένων προς τον κόμβο προορισμού D αλλά θέλει να παρακολουθήσει και να συλλέξει τα δεδομένα από τον κόμβο-πηγή S. Έτσι απαντά αμέσως στο αίτημα (M - 4). Αντί να μεταδοθούν τα πακέτα δεδομένων αμέσως μέσω του κόμβου M, ο κόμβος S πρέπει να περιμένει την απάντηση από τους άλλους κόμβους. Μετά από λίγο χρόνο θα λάβει την απάντηση από τον κόμβο 1 σαν (1 - 3) και ο κόμβος 2 σαν (2 - 3). Σύμφωνα με αυτή την προτεινόμενη λύση θα ελέγξει πρώτα τη διαδρομή που περιέχει τα επόμενα επαναλαμβανόμενα βήματα προς τον κόμβο προορισμού. Αν δεν υπάρχει επαναλαμβανόμενος κόμβος επιλέγει τυχαία την διαδρομή και μεταδίδει τα δεδομένα μέσω αυτού του μονοπατιού[37].



Source	Intermediate node	Destination
S	M – 4	D
S	1 – 3 2 – 3	D

Εικόνα 35 Αρχή Λειτουργίας SAODV

Το SAODV μπορεί να χρησιμοποιηθεί για την προστασία του μηχανισμού ανακάλυψης της διαδρομής του πρωτοκόλλου AODV παρέχοντας χαρακτηριστικά ασφαλείας όπως η ακεραιότητα (integrity), η αυθεντικοποίηση (authentication) και η μη άρνηση αναγνώρισης ή μη αποποίησης ευθυνών (non-repudation)[2].

8.4.3 Αντιμετώπιση Επιθέσεων Πλαστοπροσωπίας

Το πρωτόκολλο ARAN μπορεί να χρησιμοποιηθεί για την άμυνα εναντίον επιθέσεων πλαστοπροσωπίας. Το ARAN όπως έχουμε πει παρέχει μηχανισμούς πιστοποίησης της ταυτότητας και της μη άρνηση αναγνώρισης των υπηρεσιών που χρησιμοποιούν προκαθορισμένα κρυπτογραφικά πιστοποιητικά για την «end-to-end» ταυτοποίηση. Επίσης κάθε κόμβος του πρωτοκόλλου ARAN ζητά ένα πιστοποιητικό από έναν αξιόπιστο διακομιστή. Η ανακάλυψη της διαδρομής επιτυγχάνεται με τη μετάδοση ενός μηνύματος ανακάλυψης της διαδρομής RDP από τον κόμβο πηγής. Η απάντηση στο μήνυμα (REP) είναι μονόδρομη από τον τόπο προορισμού προς την πηγή. Τα μηνύματα δρομολόγησης πιστοποιούνται στο κάθε ενδιάμεσο βήμα (hop) -κόμβο και στις δύο κατευθύνσεις.

Επειδή τα μηνύματα RDP δεν περιέχουν τον αριθμό των αλμάτων ή την καταγραφή της διαδρομής από την πηγή και επειδή τα μηνύματα πιστοποιήθηκαν σε κάθε βήμα, οι κακόβουλοι κόμβοι δεν έχουν καμία πιθανότητα να σχηματίσουν έναν βρόχο δρομολόγησης με τον επαναπροσανατολισμό της κυκλοφορίας ή να χρησιμοποιήσουν πλαστοπροσωπία. Το μειονέκτημα του ARAN είναι ότι χρησιμοποιεί βήμα προς βήμα (hop-by-hop) έλεγχο ταυτότητας πράγμα που συνεπάγεται μεγάλη επιβάρυνση υπολογισμού. Εν τω μεταξύ, κάθε κόμβος χρειάζεται να διατηρεί ένα πίνακα ανά ζεύγος πηγής-προορισμού στον οποίο οι διαδρομές να είναι πάντα ενεργές.

8.4.4 Αντιμετώπιση Επιθέσεων Τροποποίησης

Το πρωτόκολλο ασφαλείας SEAD [11], χρησιμοποιείται στον τομέα της άμυνας κατά των επιθέσεων τροποποίησης (modification). Παρόμοια με ένα πακέτο λουριού, το πρωτόκολλο SEAD όπως έχουμε αναφέρει χρησιμοποιεί μια μονόδρομη αλυσίδα hash για να αποτρέψει τους κακόβουλους κόμβους από την αύξηση του αριθμού ακολουθίας ή την μείωση των αλμάτων στη δρομολόγηση των πακέτων διαφήμισης. Στο πρωτόκολλο SEAD οι κόμβοι πρέπει να πιστοποιηθούν από τους γείτονες τους χρησιμοποιώντας την TESLA [12] ταυτότητα εκπομπής ή ένα συμμετρικό κρυπτογραφικό μηχανισμό.

Πρωτόκολλο / **Επίθεση**	**SEAD**	**ARIANDE**	**SRP**	**ARAN**
Άρνηση Υπηρεσίας (DoS)	Ναι	Ναι	Ναι	Ναι
Σκουληκότρυπα	Ναι	Ναι	Ναι	Ναι
Μαύρη Τρύπα	Ναι	Όχι	Όχι	Όχι
Υπερχείλιση του πίνακα δρομολόγησης	Ναι	Όχι	Όχι	Όχι
Spoofing	Ναι	Όχι	Όχι	Όχι

Εικόνα 36 Πρωτόκολλα και Επιθέσεις[9]

8.5 Αντιμετώπιση Επιθέσεων στο Επίπεδο Μεταφοράς

Η «point-to-point» ή «end-to-end» κρυπτογράφηση παρέχει εμπιστευτικότητα στο μήνυμα ή ειδικότερα στο επίπεδο μεταφοράς σε δύο τερματικά συστήματα. Οπως είναι γνωστό το πρωτόκολλο TCP παρέχει μια αξιόπιστη σύνδεση. Το TCP δεν διαπρέπει στα δίκτυα Manet και έτσι η TCP ανάδραση (TCP-F), το πρωτόκολλο TCP ρητής κοινοποίησης ανεπάρκειας (TCP-ELFN), το adhoc πρωτόκολλο μετάδοσης ελέγχου (ATCP) και το ad hoc πρωτόκολλο μεταφορών (ATP) που έχουν εφευρεθεί δεν είναι σχεδιασμένα για την ασφάλεια.

Τα πρωτόκολλα Secure Socket Layer (SSL), Transport Layer Security (TLS) και Private Communications Transport (PCT) έχουν σχεδιαστεί για ασφαλείς επικοινωνίες και βασίζονται στην κρυπτογραφία δημόσιου κλειδιού. Τα πρωτόκολλα TLS / SSL μπορεί να βοηθήσουν στην ασφαλή μετάδοση δεδομένων. Μπορεί επίσης να βοηθήσουν στην προστασία από επιθέσεις πλαστοπροσωπίας, «man-in-the-middle» επιθέσεις και επιθέσεις επανάληψης. Επιπλέον τα πρωτόκολλα TLS / SSL στηρίζονται σε κρυπτογραφία δημόσιου κλειδιού το οποίο απαιτεί αρκετή επεξεργαστική ισχύ και ευρύ σύνολο ρυθμίσεων. Ως εκ τούτου, η εφαρμογή αυτών των συστημάτων στα Manet είναι περιορισμένη. Ακόμα το TLS / SSL πρέπει να τροποποιηθεί προκειμένου να αντιμετωπίσει τις ειδικές ανάγκες των δικτύων Manet[21].

8.6 Αντιμετώπιση Επιθέσεων στο Επίπεδο Εφαρμογής

Όπως και σε όλα τα άλλα επίπεδα και το επίπεδο εφαρμογής πρέπει επίσης να διασφαλιστεί. Σε ένα δίκτυο με εγκατεστημένο ένα τείχος προστασίας (firewall), το τείχος προστασίας μπορεί να παρέχει έλεγχο πρόσβασης, έλεγχο ταυτότητας χρήστη, φιλτράρισμα πακέτων κτλ. Τα διάφορα λογισμικά-τείχη προστασίας μπορεί να αποτρέψουν αποτελεσματικά πολλές επιθέσεις και συγκεκριμένες εφαρμογές όπως για παράδειγμα ένα λογισμικό εντοπισμού spyware τα οποία έχουν αναπτυχθεί για τη διαφύλαξη κρίσιμων υπηρεσιών. Ωστόσο, ένα τείχος προστασίας ως επί το πλείστον περιορίζονται σε βασικά συστήματα ελέγχου της πρόσβασης και δεν είναι σε θέση να επιλύσει όλα τα προβλήματα ασφαλείας. Για παράδειγμα, δεν είναι αποτελεσματικό κατά των επιθέσεων από εσωτερικούς κόμβους. Λόγω της έλλειψης υποδομής στα Manet, ένα τείχος προστασίας δεν είναι ιδιαίτερα χρήσιμο.

Στα Manet ένα IDS μπορεί να χρησιμοποιηθεί ως δεύτερη γραμμή άμυνας. Το IDS μπορεί να εγκατασταθεί στο επίπεδο δικτύου μιας και στο επίπεδο εφαρμογών μπορεί να μην είναι εφικτό αλλά αναγκαίο. Ορισμένες επιθέσεις, όπως η επίθεση που προσπαθεί να κερδίσει την αναρμόδια πρόσβαση σε μια υπηρεσία η οποία μπορεί να φαίνεται νόμιμη στα χαμηλότερα στρώματα, όπως είναι τα πρωτόκολλα MAC του επιπέδου ζεύξης δεδομένων. Επίσης, ορισμένες από τις επιθέσεις μπορεί να είναι πιο προφανές από το επίπεδο εφαρμογών. Για παράδειγμα, το επίπεδο εφαρμογών μπορεί να ανιχνεύσει μια επίθεση DoS πιο γρήγορα από τα χαμηλότερα στρώματα όταν ένας μεγάλος αριθμός εισερχόμενων συνδέσεων παροχής υπηρεσιών δεν έχουν καμία πραγματική δραστηριότητα δεδομένου ότι τα χαμηλότερα στρώματα χρειάζονται περισσότερο χρόνο για να την αναγνωρίσουν[21].

8.7 Αντιμετώπιση Επιθέσεων Πολλαπλών Επιπέδων

Οι επιθέσεις DoS, οι επιθέσεις πλαστοπροσωπίας, οι επιθέσεις «man-in-the-middle» και πολλές άλλες επιθέσεις μπορούν να στοχεύσουν σε πολλαπλά επίπεδα του προτύπου OSI. Τα αντίμετρα για αυτές τις επιθέσεις πρέπει να εφαρμόζονται σε διάφορα επίπεδα. Για παράδειγμα, οι κατευθυντικές κεραίες χρησιμοποιούνται στο επίπεδο ζεύξης δεδομένων για την άμυνα εναντίον επιθέσεων σκουληκότρυπας και πακέτων λουριών που χρησιμοποιούνται ως μέσο άμυνας στο επίπεδο δικτύου κατά των επιθέσεων σκουληκότρυπας. Τα αντίμετρα για τις επιθέσεις πολλαπλών επιπέδων μπορούν επίσης να εφαρμοστούν σε ένα ολοκληρωμένο σύστημα. Για παράδειγμα, εάν ένας κόμβος ανιχνεύσει μια τοπική εισβολή σε υψηλότερο επίπεδο, τα χαμηλότερα επίπεδα ενημερώνονται ώστε να κάνουν περαιτέρω διερεύνηση.

Ως παράδειγμα, δίνουμε μια λεπτομερή περιγραφή για την άμυνα κατά των DoS επιθέσεων.

Στα Manet, δύο είδη DoS επιθέσεων είναι αρκετά συχνές και είναι οι εξής: η μια είναι στο επίπεδο δικτύου και η άλλη στο επίπεδο ζεύξης δεδομένων. Οι επιθέσεις αυτές θα μπορούσε να υφίστανται στο επίπεδο δικτύου αλλά δεν περιορίζονται σε αυτό λόγω των ακόλουθων ανωμαλιών:

1. Ο κακόβουλος κόμβος συμμετέχει σε μια διαδρομή και απλώς καταστρέφει κάποια πακέτα δεδομένων.

2. Ο κακόβουλος κόμβος μεταδίδει ψευδείς ενημερώσεις διαδρομής.

3. Ο κακόβουλος κόμβος θα μπορούσε δυνητικά να επαναλάβει παλιές ενημερώσεις.

4. Ο κακόβουλος κόμβος μειώνει το TTL (time-to-live) πεδίου της επικεφαλίδας IP έτσι ώστε το πακέτο να μην φτάσει ποτέ στον προορισμό.

Αν επιβάλλεται η «end-to-end» ταυτοποίηση οι επιθέσεις από ανεξάρτητους κακόβουλους κόμβους των τύπων (2) και (3) μπορεί να εξουδετερώνονται. Μια επίθεση του τύπου (1), μπορεί να ξεκινάει από την ανάθεση επιπέδων εμπιστοσύνης προς τους κόμβους χρησιμοποιώντας διαδρομές που προσφέρουν υψηλότερο επίπεδο εμπιστοσύνης. Μια επίθεση του τύπου (4) μπορεί να αντιμετωπιστεί καθιστώντας υποχρεωτικά στον κόμβο να εξασφαλίζει ότι το πεδίο TTL έχει οριστεί σε τιμή μεγαλύτερη από τον αριθμό των αλμάτων του προορισμού.

Αν οι κόμβοι συνεργούν, οι μηχανισμοί ελέγχου ταυτότητας αποτυγχάνουν και αυτό είναι ένα ανοικτό πρόβλημα για την παροχή προστασίας από τέτοιες επιθέσεις δρομολόγησης.

Οι DoS επιθέσεις του επιπέδου ζεύξης δεδομένων θα μπορούσαν να περιλαμβάνουν μεταξύ άλλων τις εξής ανωμαλίες:

1. Κρατώντας το κανάλι απασχολημένο στην περιοχή ενός κόμβου αυτό οδηγεί σε άρνηση εξυπηρέτησης σε αυτόν τον κόμβο.

2. Με τη χρήση ενός συγκεκριμένου κόμβου για την αναμετάδοση συνεχώς ψευδών στοιχείων, η διάρκεια ζωής της μπαταρίας του κόμβου μπορεί να ελαττωθεί.

Η «end-to-end» ταυτοποίηση μπορεί να εμποδίσει τις ανωτέρω δύο περιπτώσεις από την επιτυχία τους. Αν ο κόμβος δεν έχει πιστοποιητικό γνησιότητας, μπορεί να αποκλείεται από την πρόσβαση στο κανάλι. Συνήθως οι κόμβοι είναι εξωτερικοί. Ωστόσο, εάν οι κόμβοι συνεργούν και η συνεννόηση των κόμβων περιλαμβάνει τον αποστολέα και τον παραλήπτη οι επιθέσεις του επιπέδου ζεύξης δεδομένων είναι πολύ εφικτές[21].

8.7.1Αντιμετώπιση της Σιβυλλικής Επίθεσης

Για να αντιμετωπιστούν οι Σιβυλλικές επιθέσεις, η ταυτότητα του κάθε κόμβου θα πρέπει να επαληθευθεί. Αυτό μπορεί να γίνει είτε άμεσα είτε έμμεσα. Στην άμεση επικύρωση ενός κόμβου επαληθεύεται άμεσα αν η ταυτότητα ενός γειτονικού κόμβου είναι έγκυρη. Για παράδειγμα ένας κόμβος μπορεί να αναθέσει σε καθένα από τους γείτονές του ένα ξεχωριστό κανάλι για να επικοινωνούν και να τους ζητήσει να εκπέμψουν κατά τη διάρκεια μιας περιόδου. Στη συνέχεια ελέγχει τα κανάλια με τυχαία σειρά εντός της προθεσμίας αυτής. Αν ένας κόμβος τότε μεταδίδει στο ειδικό αυτό κανάλι σημαίνει ότι είναι ένα φυσικός κόμβος. Αν δεν ανιχνευθεί σε ένα κανάλι, αυτό δείχνει ότι ο κόμβος που διατίθενται για το κανάλι δεν μπορεί να είναι ένας φυσικός κόμβος[4].

Στο πλαίσιο της έμμεσης ταυτοποίησης ένας άλλος έμπιστος κόμβος παρέχει τον έλεγχο για την ταυτότητα του κόμβου. Για παράδειγμα, κάθε κόμβος μπορεί να μοιράζεται ένα μοναδικό κλειδί με τον σταθμό βάσης. Όταν δύο κόμβοι πρέπει να δημιουργήσουν μια σύνδεση μεταξύ τους, μέσω του σταθμού βάσης εξακριβώνει ο ένας την ταυτότητα του άλλου χρησιμοποιώντας αυτά τα κλειδιά. Ταυτόχρονα μπορούν να εκχωρήσουν ένα κλειδί συνόδου. Οι κόμβοι μπορούν επίσης να έχουν τη δυνατότητα να δημιουργούν δεσμούς με περιορισμένο αριθμό των γειτονικών κόμβων. Έτσι, οι κόμβοι μπορούν να επικοινωνούν μόνο με ένα περιορισμένο αριθμό ελεγμένων γειτονικών κόμβων, γεγονός που περιορίζει τις επιπτώσεις της Σιβυλλικής επίθεσης.

Τυχαία κλειδιά των κόμβων παρέχουν επίσης ασφάλεια ενάντια στις σιβυλλικές επιθέσεις. Δεδομένου ότι ένας περιορισμένος αριθμός κλειδιών είναι διαθέσιμός σε κάθε κόμβο, οι κόμβοι δεν έχουν αρκετά κλειδιά για τη δημιουργία πολλαπλών ταυτοτήτων[4].

Κεφάλαιο 9

Οι προκλήσεις και το μέλλον των δικτύων Manets

Οι μεγάλες προκλήσεις που αντιμετωπίζουν τα δίκτυα Manet από την αρχιτεκτονική του διαδικτύου μπορούν να ταξινομηθούν ως εξής:

- Στην ενσωμάτωση των αναδυόμενων ασυρμάτων στοιχείων του δικτύου όπως οι φορητές συσκευές, οι ad-hoc δρομολογητές και οι ενσωματωμένοι αισθητήρες στο υφιστάμενο πλαίσιο του πρωτοκόλλου.

- Στην παροχή «end-to-end» υπηρεσιών η οποία διευκολύνει την ανάπτυξη εφαρμογών.

Αυτές οι προκλήσεις τίθενται σε ένα ευρύ φάσμα, όπως είναι οι κυψελωδής υπηρεσίες δεδομένων, τα Wi-Fi hot-spots, οι πληροφορίες των σταθμών, η «peer-to-peer» κινητικότητα, τα AdHoc δίκτυα για την ευρυζωνική πρόσβαση, τα δίκτυα οχημάτων (vanet) και τα δίκτυα αισθητήρων (sensor networks). Αυτά τα σενάρια ασύρματων εφαρμογών μπορούν να οδηγήσουν σε ένα διαφορετικό σύνολο απαιτήσεων παροχής υπηρεσιών για το μέλλον του Διαδικτύου και αυτές συνοψίζονται παρακάτω:

1. Ευελιξία στην ονοματολογία (naming) και στην διευθυνσιοδότηση (addressing).

2. Υποστήριξη της κινητικότητας για την δυναμική μεταφοράς των τελικών χρηστών και των δικτυακών συσκευών.

3. Υπηρεσίες τοποθεσίας που παρέχουν πληροφορίες για τη γεωγραφική θέση.

4. Αυτοργάνωση για τον κατανεμημένο έλεγχο της τοπολογίας του δικτύου.

5. Ασφάλεια και θεώρηση της ιδιωτικής ζωής των κινητών κόμβων και των ανοικτών ασύρματων καναλιών.

6. Αποκεντρωμένη διαχείριση για τον έλεγχο και την απομακρυσμένη παρακολούθηση.

7. Την κατά επίπεδα (cross-layer) υποστήριξη για τη βελτιστοποίηση της απόδοσης των πρωτοκόλλων.

8. Την υποστήριξη των γνωστών τεχνικών ραδιοφώνου για τα δίκτυα όσον αφορά το φυσικό επίπεδο.

9. Οικονομικά κίνητρα για την ενθάρρυνση της αποτελεσματικότερης κατανομής των πόρων[36].

Στο σύνολό τους οι παραπάνω απαιτήσεις των Manet αντιπροσωπεύουν ένα φάσμα προκλήσεων του δικτύου. Κατά τη διάρκεια των τελευταίων ετών σχεδόν κάθε πτυχή των δικτύων Manet έχει διερευνηθεί σε κάποιο επίπεδο λεπτομέρειας. Τα μεγάλα ανοικτά προβλήματα αναφέρονται παρακάτω:

- *Αυτονομία* – Κανένας κεντρικός φορέας *διοίκησης* δεν είναι διαθέσιμος για τη διαχείριση λειτουργίας των διαφόρων κινητών κόμβων.

- *Δυναμική τοπολογία* – Οι κόμβοι είναι κινητοί και μπορεί να συνδεθούν δυναμικά με αυθαίρετο τρόπο. Οι σύνδεσμοι του δικτύου ποικίλλουν και βασίζονται στην εγγύτητα του ενός κόμβου στον άλλο.

- *Συσκευή ανακάλυψης* – Ο εντοπισμός της πρόσφατης μετακίνησης των κόμβων και η ενημέρωση για την ύπαρξή τους πρέπει να είναι δυναμική για να διευκολυνθεί η αυτόματη επιλογή της βέλτιστης διαδρομής.

- *Βελτιστοποίηση του εύρους ζώνης (bandwidth)* – Οι ασύρματοι σύνδεσμοι έχουν σημαντικά χαμηλότερη παραγωγική ικανότητα σε σχέση με τους ενσύρματους.

- *Περιορισμένοι πόροι* – Οι κινητοί κόμβοι βασίζονται στην ισχύ της μπαταρίας τους η οποία είναι ένα αγαθό με ανεπάρκεια. Επίσης, η ικανότητα αποθήκευσης όσον αφορά την χωρητικότητα είναι εξαιρετικά περιορισμένη.

- *Επεκτασιμότητα (scalability)* – Η ευελιξία μπορεί να οριστεί ως προς το αν το δίκτυο είναι σε θέση να παρέχει ένα αποδεκτό επίπεδο υπηρεσιών ακόμη και με την παρουσία μεγάλου αριθμού κόμβων.

- *Περιορισμένη φυσική ασφάλεια* – Η κινητικότητα συνεπάγεται υψηλότερους κινδύνους ασφαλείας, όπως η «peer-to-peer» αρχιτεκτονική του δικτύου ή η ασύρματη επικοινωνία για την πρόσβαση των νόμιμων χρηστών του δικτύου αλλά και των κακόβουλων. Τέτοιες επιθέσεις θεωρούνται οι υποκλοπές, η πλαστοπροσωπία και οι Dos.

- *Η έλλειψη υποδομής και η αυτόνομη λειτουργία* – Η δυνατότητα επούλωσης των αιτημάτων στα Manet θα πρέπει να επαναπροσδιοριστεί σε κάθε κόμβο που διακινείται εκτός της εμβέλειας του δικτύου.

- *Κακή ποιότητα μετάδοσης* – Αυτό είναι ένα πρόβλημα της ασύρματης επικοινωνίας που προκαλείται από διάφορες πηγές σφαλμάτων που έχουν ως αποτέλεσμα την υποβάθμιση του λαμβανόμενου σήματος.

- *Η διευθυνσιοδότηση στα Ad Hoc δίκτυα* – Οι προκλήσεις στο πρότυπο της κανονικής διευθυνσιοδότησης πρέπει να εφαρμοστούν.

- *Η διαμόρφωση του δικτύου* – Το σύνολο της υποδομής στα Manet είναι δυναμικό και αυτός είναι ο λόγος για τη δυναμική σύνδεση και αποσύνδεση των διάφορων συνδέσμων .

- *Η συντήρηση της τοπολογίας* – Η ταυτοποίηση των πληροφοριών των δυναμικών συνδέσεων μεταξύ των κόμβων στα Manets είναι μια μεγάλη πρόκληση[36].

Όσον αφορά το **μέλλον** τα Manet και γενικότερα τα Ad hoc δίκτυα είναι ένας ευρύς τομέας των ασύρματων δικτύων του μέλλοντος και πολλές μελέτες και συζητήσεις γίνονται πάνω σε αυτόν μιας και στις μέρες κυριαρχεί η ανάγκη της «οποτεδήποτε, με οποιονδήποτε & οπουδήποτε» επικοινωνίας. Ολοένα νέες εφαρμογές απαιτούν τόσο μεγάλο εύρος ζώνης όσο και χωρητικότητας το οποίο συνεπάγεται την ανάγκη για υψηλότερη συχνότητα και καλύτερα φασματική επαναχρησιμοποίηση. Η διάδοση, η φασματική επαναχρησιμοποίηση και τα ενεργειακά θέματα υποστηρίζουν στροφή σε μία μακρά ασύρματη σύνδεση (όπως στην κυψελωδή) και σε ένα πλέγμα των αντίστοιχων συνδέσεων (όπως στα Manets). Η ερευνά για την αρχιτεκτονική πολλαπλών βημάτων (multi-hop) έδειξε ότι ήταν μια πολλά υποσχόμενη λύση για την εφαρμογή των AdHoc δικτύων. Καθώς η εξέλιξη συνεχίζεται, ιδίως η ανάγκη της πυκνής ανάπτυξης όπως στο πεδίο της μάχης και τα δίκτυα αισθητήρων, οι κόμβοι στα Manet θα είναι μικρότεροι , φθηνότεροι και πολύ ικανοί.

Η επίγνωση του πλαισίου (context-aware) δρομολόγησης είναι ένας πολλά υποσχόμενος τομέας για μελλοντική έρευνα στα δίκτυα Manet. Η ιδέα είναι ότι το πρωτόκολλο δρομολόγησης από μόνο του μπορεί να είναι πολυμορφικό και να είναι σε θέση να προσαρμόζει τη λειτουργία του σε ένα μεταβαλλόμενο δίκτυο όσον αφορά το πλαίσιο ανάπτυξης του σε πραγματικό χρόνο. Η πιο κατάλληλη πολιτική δρομολόγησης μπορεί να αλλάξει κατά τη διάρκεια ζωής ενός δικτύου ή ακόμη ορισμένες «περιφέρειες» των δικτύων στα Manet μπορεί να επιλέξουν να εφαρμόσουν ταυτόχρονα διαφορετικές πολιτικές δρομολόγησης με τους Manet δρομολογητές κατά μήκος των συνόρων των διαφόρων περιφερειών το οποίο επέχει θέση στην δυναμική δρομολόγηση του πρωτοκόλλου[35].

Η παροχή βαθμού ποιότητας μιας υπηρεσίας (Quality Of Service, QoS) είναι ένα πολύ δύσκολο πρόβλημα στα Manets. Πολλά από αυτά που μπορεί να επιτευχθούν από την άποψη της ποιότητας μιας υπηρεσίας εξαρτώνται σε μεγάλο βαθμό από την τεχνολογία του επιπέδου ζεύξης δεδομένων όπως και από τον τρόπο/βαθμό χρήσης της υπηρεσίας. Ο βαθμός που τα στοιχεία του επιπέδου ζεύξης δεδομένων μπορούν πράγματι να μεταφέρονται σε ένα τυποποιημένο πρότυπο IP πρωτόκολλου δρομολόγησης αποτελεί έναν απαιτητικό τομέα της μελλοντικής έρευνας. Τέλος, ίσως η μεγαλύτερη πρόκληση που αντιμετωπίζει η ποιότητα παροχής υπηρεσιών (QoS) στα Manet είναι ότι πολλά από τα πρωτόκολλα του επιπέδου ζεύξης δεδομένων είναι υπεύθυνα για τη δημοτικότητά σε δίκτυα χωρίς τον έλεγχο του φάσματος. Είναι ακόμα ανέφικτο να παρέχεις ισχυρές εγγυήσεις QoS σε ένα φάσμα που δεν ελέγχεις.

Κεφάλαιο 10

Συμπεράσματα

Καθώς ολοκληρώσαμε την παρουσίαση των επιθέσεων και των τρόπων αντιμετώπισης τους στα δίκτυα Manet , αποκομίσαμε κάποια συμπεράσματα όσον αφορά την καλύτερη αρχιτεκτονική ασφάλειας και δικτύου στα παραπάνω δίκτυα.

Σύμφωνα με την αρχιτεκτονική του δικτύου, ένα δίκτυο μπορεί να είναι έχει υποδομή (σταθερά σημεία πρόσβασης) ή να μην έχει υποδομή (adhoc και δίκτυα αισθητήρων). Η διασφάλιση της αξιόπιστης και της ασφαλής δρομολόγησης καθώς και η διατήρηση ενός επιπέδου εμπιστοσύνης μεταξύ των κόμβων του δικτύου είναι απαραίτητη για τη συνέχιση της παροχής υπηρεσιών μέσω αυτών των δικτύων.

Από την πλευρά του τερματικού σταθμού δηλαδή των κόμβων, είναι σημαντικό να προστατεύσουμε τους πόρους του (μπαταρία, δίσκος, CPU) κατά της κατάχρησης και να διασφαλιστεί το απόρρητο των δεδομένων του. Σε ένα adhoc δίκτυο καθίσταται απαραίτητο να διασφαλιστεί η ακεραιότητα του τερματικού σταθμού δεδομένου ότι διαδραματίζει έναν διπλό ρόλο , αυτού του δρομολογητή (router) και του τερματικού σταθμού.

Η δυσκολία του σχεδιασμού λύσεων ασφαλείας δεν προέρχεται μόνο από τη διασφάλιση της σταθερής αντιμετώπισης των πιθανών επιθέσεων ή από την εξασφάλιση ότι δεν θα επιβραδυνθούν οι επικοινωνίες αλλά πρέπει να βελτιστοποιηθεί η χρήση των πόρων σε εύρος ζώνης, μνήμης, μπαταρίας, κλπ . Ακόμη πιο σημαντικό σε αυτό το ανοικτό πλαίσιο του ασύρματου δικτύου είναι να εξασφαλίζεται η ανωνυμία και η προστασία της ιδιωτικής ζωής επιτρέποντας ταυτόχρονα την ιχνηλασιμότητα για νομικούς λόγους δηλαδή την πληρότητα των πληροφοριών σε κάθε βήμα μιας αλυσίδας διεργασιών παρέχοντας έτσι την δυνατότητα για τον χρονικό συσχετισμό-επαλήθευση των πληροφοριών. Πράγματι, η αυξανόμενη ανάγκη για ιχνηλασιμότητα είναι πλέον αναγκαία για την καταπολέμηση των κακόβουλων επιθέσεων αλλά και την ελαχιστοποίηση της λεηλασίας των πνευματικών δικαιωμάτων. Αντιμετωπίζετε ως εκ τούτου το δίλημμα την παροχής υποστήριξης του δικτύου με ελεύθερη ανταλλαγή πληροφοριών και ταυτόχρονο έλεγχο του περιεχομένου ώστε να αποφεύγονται τα κακόβουλα περιεχόμενα. Στην πραγματικότητα αυτό αφορά τόσο τα ενσύρματα όσο και τα ασύρματα δίκτυα. Όλοι αυτοί οι παράγοντες επηρεάζουν την επιλογή και την εφαρμογή των εργαλείων ασφαλείας και καθοδηγούνται από μια εκ των προτέρων εκτίμηση των κινδύνων και των πολιτικών ασφαλείας.

Επίσης πρέπει τα συστήματα να σχεδιάζονται με μοντέλα εμπιστοσύνης τα οποία θα πρέπει να προσφέρουν υψηλό επίπεδο εμπιστοσύνης έναντι των κλασικών

μηχανισμών ασφαλείας και έτσι τα μελλοντικά δίκτυα θα πρέπει να εφαρμόζουν και τα δύο μοντέλα δηλαδή της ασφάλειας και της εμπιστοσύνης.

Οι μηχανισμοί ασφαλείας που παρουσιάστηκαν παραπάνω είναι μια πρακτική απάντηση σε συγκεκριμένα προβλήματα που ανακύπτουν στα επίπεδα του προτύπου OSI. Ωστόσο, οι λύσεις που προτείνονται καλύπτουν μόνο ένα υποσύνολο όλων των πιθανών απειλών και είναι δύσκολο να ενσωματωθούν μεταξύ τους. Για παράδειγμα, τα ασφαλή πρωτόκολλα δρομολόγησης δεν αντιμετωπίσουν την έλλειψη συνεργασίας των κόμβων του δικτύου και δεν έχουν σχεδιαστεί για να ενσωματώσουν ένα μηχανισμό επιβολής της συνεργασίας. Μια πλήρης υποδομή ασφαλείας πρέπει να εξετάσει ένα ευρύ φάσμα επιθέσεων και έτσι πρέπει να ενσωματώνει πολλά στοιχεία. Επιπλέον, οι ανάγκες ασφάλειας μπορεί να ποικίλλουν ανάλογα με τα διάφορα σενάρια δικτύωσης και τους μηχανισμούς ασφάλειας οι οποίοι εγκρίθηκαν για την καταπολέμηση της εσφαλμένης συμπεριφοράς ή την διαταραχή των κόμβων οι οποίοι πρέπει να είναι αρκετά ευέλικτοι ώστε να χρησιμοποιούνται σε διαφορετικά περιβάλλοντα. Η κατεύθυνση που έχει ληφθεί από την ερευνητική κοινότητα προκειμένου να υποστηρίξει τα adhoc δίκτυα με τους μηχανισμούς ασφαλείας επιβεβαιώνει αυτό το όραμα και οι λύσεις που προτείνονται είναι να ανέλθει σταδιακά σε ώριμο στάδιο καθιστώντας έτσι την adhoc δικτύωση μια ρεαλιστική εναλλακτική λύση για τα ασύρματα δίκτυα και τα δίκτυα 3G.

Βιβλιογραφικές Αναφορές

[1] Marlon McBride, Mustafa Masacioglu, Control Based Mobile Ad Hoc Networking For Survivable - Dynamic -Mobile Special Operation Force Communications, Naval Postgraduate School, Monterey California, September 2009

[2] Anil Kumar Verma, Design And Development Of A Routing Protocol For Mobile Ad Hoc Networks (MANETs), Thapar University, Patalia, Arpil 2007

[3] Deshpande Vivek S, Security in Ad-Hoc Routing Protocols, Maharashtra Institute Of Technology Women Engineering, India

[4] Erdal Çayırcı (NATO Joint Warfare Centre) , Chunming Rong (University of Stavanger),Security in Wireless Ad Hoc and Sensor Networks (Book), Norway, 2009

[5] Al-Sakil Kham Pathan, Security Of Self Organizing Networks (Manet Wsn WMN Vanet), USA, 2011

[6] Yih-Chun Hu (Carnegie Mellon University), Adrian Perrig (Carnegie Mellon University), ARIADNE-A Secure On Demand Routing Protocol for Ad Hoc Networks, David B. Johnson(Rice University), USA, 2002

[7] Yih-Chun Hu (Carnegie Mellon University), Adrian Perrig (Carnegie Mellon University), David B. Johnson(Rice University), SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks , USA, 2003

[8] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, Securing On-Demand Source Routing in MANETs, Department of Computer Science and Engineering, ABV-Indian Institute of Information Technology & Management, Gwalior, India

[9] Tirthraj Ra, Security in Mobile Ad Hoc Networks, Computer Science and Engineering Department ,Thapar University, Patiala, 2009

[10] Peng Ning and Kun Sun, How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols, Computer Science Department, North Carolina State University, March 6, 2003

[11] Animesh K. Trivedi,Rajan Arora,Rishi Kapoor,Sudip Sanyal, Ajith Abraham, Sugata Sanyal, Mobile Ad Hoc Network Security Vulnerabilities, Part from Book: Encyclopedia of Information Science and Technology,

[12] Bridget Dahill, Brian Neil Levine, Elizabeth Royer , Clay Shields, A Secure Routing Protocol for Ad Hoc Networks, August 2001,

[13] Abderrahim Benslimane, Security for Mobile and Vehicular Ad hoc Networks, , Avignon University, Caen, France

[14] Samuel Piere, Michel Barbeau,Evaggelos Kranakis, Ad-Hoc - Mobile and Wireless Networks(Book), New York, 2003

[15] C.Prasanna lakshmi & K.Yasasvi, Secure Routing Protocols for Wireless AdHoc Networks, Sri Venkatesa Perumal College of Engineering and Technology, 2010 (http://www.yuvaengineers.com/?p=699)

[16] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication, Department of Electronics & Communication, University of Allahabad, India

[17] Rutvij H. Jhaveri1, Ashish D. Patel2, Jatin D. Parmar3 ,Bhavin I. Shah4, MANET Routing Protocols and Wormhole Attack against AODV, Department of Computer Engineering and Information Technology, S.V.M. Institute of Technology, Bharuch, India

[18] Sheemu Sharma, Roopam Gupta, Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks, Utara University, Malaysia, 2008

[19] Sushant Kumar, Bibhudatta Sahoo, Effect of Rushing Attack on DSR in wireless Mobile Ad hoc Network, Department of Computer Science & Engineering, NIT Rourkela, Orissa, India

[20] Fei Xing, Wenye Wang, Understanding Dynamic Denial Of Service Attacks in Mobile Ad Hoc Networks, Department Of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695, USA

[21] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Department of Computer Science and Engineering, Florida Atlantic University, 2006

[22] Yibghua Guo, Detecting Manets Against Flooding Attacks By Detective Measures, Institute for telecommunication Research, University Of South Australia, 2008

[23] Yinghua Guo , Ivan Lee, Forensic analysis of DoS attack traffic in MANET, School of Computer and Information Science, University of South Australia, Adelaide, Australia, 2010

[24] Vesa Kärpijoki, Security in Ad Hoc Networks, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology , Finland

[25] Adam Burg, Ad hoc Network Specific Attacks, Technological University of Munich, 2003

[26] Kamanshis Biswas, Md. Liakat Ali, Security Threats in Mobile Ad Hoc Network , Department of Interaction and System Design, School of Engineering Blekinge Institute of Technology , Sweden, 2007

[27] Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris, Preventing Impersonation Attacks in MANET with Multi-factor Authentication, Department of Informatics, University of Piraeus

[28] H Yang H Y. Luo, F Ye S W. Lu L Zhang, Security in Mobile Ad hoc Networks: Challenges and solutions, University of California, 2004

[29] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, Behrang Samadi, A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i), Malaysia

[30] A.Economides, A. Pomportsis, Gkarafli Stamati, Networking Technologies– MANET, University Of Macedonia, 2005

[31] Theologou Mixahl, Koutsoubelas Dimitrios, Kwstoydhs Hlias, Security in ad hoc networks and sensor networks, National Technical University Of Athens, 2008

[32] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey Of Attacks And Countermeasures in Mobile Ad Hoc Networks, Department of Computer Science and Engineering, Florida Atlantic University

[33] Vikram Gupta, Srikanth Krishnamurthy, Michalis Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, UC Riverside

[34] Hoang Lan Nguyen , Uyen Trang Nguyen, A study of different types of attacks on multicast in mobile ad hoc networks, Department of Computer Science and Engineering, York University, Toronto, Canada, 2006

[35] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, Mobile Ad Hoc Networking (Book), Canada, 2004

[36] Kavita Taneja, R. B. Patel, Mobile Ad hoc Networks: Challenges and Future, Mullana, Haryana, India, 2007

[37] Latha Tamilselvan, Dr. V Sankaranarayanan, Prevention of Blackhole Attack in MANET, BSA Crescent Engineering College, Vandalur, Chennai, Tamilnadu, India, 2007

[38] Irshad Ullah, Shoaib Ur Rehman, Analysis of Black Hole attack on Manets using Manet Routing Protocols, School of Computing ,Blekinge Institute of Technology, Sweden, 2010

[39] N. Shanthi, Dr. Lganesan Dr. K .Ramar, Tamil Nadu, Study Of Different Attacks On Multicast Mobile Ad Hoc Network, India, 2009

[40] Muhammad Mahmudul Islam, Ronald Pose, Carlo Kopp, Link Layer Security for SAHN Protocols, School of Computer Science and Software Engineering, Monash University, Australia