Πανεπιστήμιο Μακεδονίας
ΔΠΜΣ στα Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών
Καθ. Αναστάσιος Α. Οικονομίδης

University of Macedonia
Master in Information Systems
Computer Networks
Prof. Anastasios A. Economides

Attacks Happened at More Significant Layers of Mobile Ad Hoc Networks and Some Countermeasures

Επιθέσεις στα σημαντικότερα επίπεδα των κινητών δικτύων και ορισμένα μέτρα αντιμετώπισης

Παλπάνα Κρυσταλία
Palpana Krystalia

MIS Student ID: MIS 13/10, University of Macedonia
mis1310@uom.edu.gr

9 Ιανουαρίου 2014

Περιεχόμενα

Περίληψη

Τα Mobile Ad Hoc Networks (Κινητά δίκτυα) παρουσιάζουν ιδιαίτερο ενδιαφέρον για περαιτέρω έρευνα λόγω της δικτυακής τους υποδομής, η οποία τα καθιστά ικανά να λειτουργούν αυτόνομα. Λόγω της δυναμικής τους φύσης, τα κινητά δίκτυα δεν είναι συνήθως πολύ ασφαλείς, για αυτό είναι πολύ σημαντικό να δοθεί ιδιαίτερη έμφαση στο είδος των δεδομένων που στέλνονται μέσω αυτών. Όσον αφορά τις επιθέσεις στα Manets στο φυσικό επίπεδο του μοντέλου OSI είναι αυξημένες εξαιτίας της ασύρματης ιδιότητας των παραπάνω δικτύων, τα οποία έχουν σαν μέσο μετάδοσης τον αέρα. 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 του. Η επιτυχία των δικτύων Manets εξαρτάται σε μεγάλο βαθμό από το αν οι κανόνες ασφαλείας είναι έμπιστοι. Σε αυτήν την εργασία γίνεται προσπάθειας έρευνας των επιθέσεων που συμβαίνουν στα κινητά δίκτυα, καθώς και των διαφόρων τρόπων αντιμετώπισής τους με κύρια έμφαση στο φυσικό επίπεδο, στο επίπεδο ζεύξης δεδομένων και στο επίπεδο δικτύου του προτύπου OSI.

Abstract

The Mobile Ad Hoc Networks (Mobile Networks) are of particular interest for further investigation due to their network infrastructure, which enables them to configure itself on the fly. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a 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 attacks may also be made on 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. The success of Manet networks depends largely on whether safety standards are trusted. In this article we attempt to investigate the attacks in Manet networks, and some countermeasures with emphasis on the physical level, the data link layer and the network layer.

1. Εισαγωγή

Στη παρούσα εργασία θεωρήθηκε σκόπιμο να δοθεί ένας ορισμός σχετικά με το τι είναι ένα κινητό δίκτυο ή αλλιώς mobile ad hoc network. Ένα **MANET (Mobile Ad hoc Network - Κινητό δίκτυο)** είναι ένα αυτορυθμιζόμενο και χωρίς υποδομή δίκτυο κινητών συσκευών που συνδέονται μέσω ασύρματων ζεύξεων. Κάθε συσκευή σε ένα MANET είναι ελεύθερη να κινηθεί σε κάθε κατεύθυνση, και ως εκ τούτου να αλλάζει συχνά τις ζεύξεις της με άλλες συσκευές. Καθεμιά θα πρέπει να προωθεί την κυκλοφορία των δεδομένων που δε σχετίζονται με τη δική της χρήση, και συνεπώς να λειτουργεί ως δρομολογητής. Η κύρια πρόκληση για την οικοδόμηση ενός Manet είναι ο εφοδιασμός κάθε συσκευής έτσι ώστε να διατηρεί συνεχώς τις πληροφορίες που απαιτούνται για να δρομολογεί κατάλληλα την κυκλοφορία. Τα εν λόγω δίκτυα μπορούν είτε να λειτουργήσουν αυτόνομα είτε να συνδεθούν στο Internet. (MANET, 2013).

Εικόνα 1: Mobile Ad Hoc Network-Κινητό δίκτυο

Στη συνέχεια παρατίθενται τα βασικά χαρακτηριστικά των κινητών δικτύων, τα οποία αποτελούν και τους σημαντικότερους λόγους για τους οποίους ένα κινητό δίκτυο θεωρείται πιο ευάλωτο σε επιθέσεις από ένα ενσύρματο δίκτυο.

- *Μη ύπαρξη καλωδίωσης*: Η χρήση των ασύρματων ζεύξεων στα κινητά δίκτυα τα καθιστά ευαίσθητα σε επιθέσεις, επομένως οι επιτιθέμενοι δεν χρειάζεται να έχουν φυσική πρόσβαση στο δίκτυο ώστε να εισβάλλουν.
- *Δυναμική τοπολογία*: Όπως αναφέρθηκε και προηγουμένως στον ορισμό των κινητών δικτύων οι κόμβοι μπορούν να φεύγουν και να εντάσσονται από και προς ένα άλλο δίκτυο ανεξάρτητα. Αυτό έχει ως αποτέλεσμα την συχνή αλλαγή της τοπολογίας του δικτύου και επομένως την αύξηση του βαθμού δυσκολίας όσον αφορά τον τρόπο διαχείρισης του δικτύου.
- *Χρήση αλγόριθμων δρομολόγησης αμοιβαίας συνεργασίας(cooperative algorithms):* Συνήθως οι αλγόριθμοι δρομολόγησης σε ένα Manet δίκτυο απαιτούν την αμοιβαία συνεργασία μεταξύ των κόμβων, το οποίο παραβιάζει τις αρχές ασφάλειας των δικτύων. Επομένως, ένας κακόβουλος εισβολέας μπορεί εύκολα να μετατραπεί σε ένα σημαντικό παράγοντα δρομολόγησης και με αυτό τον τρόπο να διαταράξει τις λειτουργίες του δικτύου μέσω της ανυπακοής στις προδιαγραφές του πρωτοκόλλου.
- *Η έλλειψη σαφούς γραμμή άμυνας*: Τα κινητά δίκτυα δεν έχουν μια σαφή γραμμή άμυνας επομένως οι επιθέσεις σε αυτά μπορούν να προέλθουν από όλες τις κατευθύνσεις. Το όριο που διαχωρίζει το εσωτερικό δίκτυο από τον έξω κόσμο δεν είναι ξεκάθαρο και δε μπορεί να εξασφαλίσει τη πρόληψη από ένας είδος επίθεσης.
- *Περιορισμένη ικανότητα αποθήκευσης και άλλων πόρων*: Οι περιορισμοί πόρων σε ένα κινητό δίκτυο είναι ένα ακόμη θέμα ευπάθειας σε επιθέσεις, διότι οι περισσότερες συσκευές που υπάρχουν σε ένα τέτοιο δίκτυο είναι με

περιορισμένη ικανότητα αποθήκευσης, όπως φορητοί υπολογιστές μέχρι συσκευές χειρός. Επομένως, αυτές οι συσκευές μπορούν να γίνουν το επίκεντρο για νέες επιθέσεις λόγω του ότι ποικίλλουν όσον αφορά την υπολογιστική δυνατότητα και τη δυνατότητα αποθήκευσης της κάθε μίας. (Abhay, Rajiv, Saurabh, K. (2010)).

Αργότερα θα αναλυθούν περαιτέρω και τα διάφορα είδη των επιθέσεων στα πιο κρίσιμα επίπεδα του μοντέλου OSI αλλά και ορισμένα μέτρα αντιμετώπισής τους. Επιπλέον αναφέρονται συνοπτικά και κάποια από τα πλεονεκτήματα και τα μειονεκτήματα των δικτύων Manets και τέλος παρατίθενται μερικές προτάσεις για μελλοντική έρευνα.

2. Είδη επιθέσεων σε δίκτυα MANETs

Οι επιθέσεις στα κινητά δίκτυα μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες: στις **παθητικές** και στις **ενεργές επιθέσεις**. Στις παθητικές επιθέσεις ο επιτιθέμενος δεν διαταράσσει το πρωτόκολλο δρομολόγησης, αλλά προσπαθεί να εξάγει από αυτό τις πιο πολύτιμες πληροφορίες, όπως την ιεραρχία του κόμβου και την τοπολογία του δικτύου. Στην πραγματικότητα μια παθητική επίθεση περιλαμβάνει την παρακολούθηση και την υποκλοπή της μετάδοσης των δεδομένων και κύριος στόχος του επιτιθέμενου είναι να λαμβάνει όλες τις πληροφορίες που μεταδίδονται στο δίκτυο. Αυτού του είδους οι επιθέσεις είναι πολύ δύσκολο να ανιχνευτούν, διότι δεν αλλοιώνουν τα δεδομένα. Παραδείγματα παθητικών επιθέσεων είναι οι υποκλοπές (eavesdropping), η ανάλυση της κίνησης των δεδομένων(traffic analysis) καθώς και η παρακολούθηση της κυκλοφορίας. (Chaudhary, P. (2013)). Στις ενεργές επιθέσεις οι επιτιθέμενοι έχουν ως στόχο την διακοπή της μετάδοσης των δεδομένων, ή την τροποποίηση αυτών, διαταράσσοντας έτσι την ομαλή λειτουργία του κινητού δικτύου. Παραδείγματα των ενεργητικών 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). (Μητρόπουλος. (2011)).

Επιπλέον οι επιθέσεις στα Manet δίκτυα μπορούν να ταξινομηθούν σε **εξωτερικές** και **εσωτερικές** ανάλογα με τον τομέα των επιθέσεων. Οι εξωτερικές επιθέσεις πραγματοποιούνται από κόμβους που δεν ανήκουν στην περιοχή του δικτύου και έχουν ως στόχο να προκαλέσουν συμφόρηση, να αναπαράγουν λανθασμένες πληροφορίες δρομολόγησης ή ακόμη και να εμποδίσουν τις υπηρεσίες να λειτουργήσουν σωστά. Οι εσωτερικές επιθέσεις πραγματοποιούνται από κόμβους που στην πραγματικότητα είναι μέρος του δικτύου και θεωρούνται πιο σοβαρές από τις εξωτερικές από την άποψη ότι οι εσωτερικοί-κακόβουλοι κόμβοι γνωρίζουν εμπιστευτικές και απόρρητες πληροφορίες.

Στην παρούσα εργασία όμως θα επικεντρωθούμε στις επιθέσεις και στους τρόπους αντιμετώπισής τους στα πιο κρίσιμα **επίπεδα του μοντέλου OSI**, οι οποίες θα αναλυθούν περαιτέρω και κυρίως στα επίπεδα δικτύου, ζεύξης δεδομένων και στο φυσικό επίπεδο. Οι απειλές στα επίπεδα μεταφοράς και εφαρμογών είναι κατά βάση όμοιες με αυτές των ενσύρματων δικτύων και επιπλέον σε ένα κινητό δίκτυο τα είδη των επιθέσεων στα συγκεκριμένα επίπεδα δε μπορούν να θεωρηθούν κοινά διότι ο κάθε χρήστης χρησιμοποιεί διαφορετικό μέσο μετάδοσης που συνεπάγεται και διαφορετικούς τύπους εφαρμογών.

2.1 Επιθέσεις στο Φυσικό επίπεδο

Η ασφάλεια στο φυσικό επίπεδο είναι σημαντική σε ένα κινητό δίκτυο, διότι πολλές επιθέσεις μπορούν να λάβουν χώρα λόγω της ασύρματης ιδιότητας του δικτύου, το οποίο έχει σαν μέσο μετάδοσης τον αέρα. Έτσι, ένας κακόβουλος εισβολέας μπορεί εύκολα να διακόψει ή να «κρυφακούσει» την υπηρεσία των ασύρματων δικτύων. Οι πιο συχνές επιθέσεις που μπορούν να συμβούν στο φυσικό επίπεδο σε ένα manet δίκτυο είναι:

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

2.1.1 Υποκλοπές (Eavesdropping)

Η υποκλοπή είναι μια παθητική επίθεση και ως κύριο στόχο έχει την ανάγνωση μηνυμάτων και συνομιλιών εντός του κινητού δικτύου μέσω της εισαγωγής στο δίκτυο παραποιημένων μηνυμάτων, τα οποία παρακολουθούν και λαμβάνουν τα δεδομένα που ανταλλάσσονται μεταξύ δύο εξουσιοδοτημένων χρηστών στο δίκτυο. Μία τέτοιου είδους επίθεση μπορεί εύκολα να υλοποιηθεί σε ένα manet δίκτυο, διότι οι κόμβοι του μοιράζονται ένα ασύρματο μέσο και επικοινωνούν χρησιμοποιώντας ένα φάσμα ραδιοσυχνοτήτων που από τη φύση του μπορεί εύκολα να υποκλαπεί με δέκτες συντονισμένους στη κατάλληλη συχνότητα. Στην πραγματικότητα, ένα ad hoc δίκτυο είναι λίγο πιο ασφαλές από τις υποκλοπές σε σύγκριση με τα υπόλοιπα είδη ασύρματων τεχνολογιών, διότι τα σήματα αποστέλλονται σε μικρές αποστάσεις και επομένως ένας κακόβουλος εισβολέας θα πρέπει να πλησιάσει αρκετά τους κόμβους του δικτύου προκειμένου να εισβάλλει σε αυτό.

2.1.2 Παρεμβολές (Interference-Jamming)

Η παρεμβολή θεωρείται ενεργητική επίθεση και όταν εισβάλλει σε ένα ραδιοφωνικό σήμα μπορεί να προκαλέσει την απώλεια ή την καταστροφή των μηνυμάτων μέσα σε ένα κινητό δίκτυο. Εάν ο εισβολέας διαθέτει έναν ισχυρό πομπό μπορεί να παράγει ένα σήμα αρκετά ισχυρό, έτσι ώστε να παρεμποδίσει τα σήματα του κινητού δικτύου και να διαταράξει την επικοινωνία. Οι πιο συνηθισμένοι τύποι παρεμβολών ενός σήματος είναι ο παλμός και ο θόρυβος. Σε αυτόν τον τύπο επίθεσης ανήκει και η επίθεση άρνησης παροχής υπηρεσιών (Denial of Service-DOS), διότι στην ουσία παρεμποδίζει την εκτέλεση των αναμενόμενων λειτουργιών του δικτύου. (Mohammad, W. (2011)).

2.1.3 Φυσικές επιθέσεις

Ως φυσικές επιθέσεις θεωρούνται απειλές που επιφέρουν τη φυσική καταστροφή των κόμβων και τους καταστρέφουν μόνιμα σε αντίθεση με τα είδη των επιθέσεων που αναφέρθηκαν παραπάνω.

Οι επιτιθέμενοι μπορούν να εξάγουν κρυπτογραφικά μυστικά, να αλλάξουν τη διάταξη των κυκλωμάτων των κόμβων, να τροποποιήσουν τον προγραμματισμό των κόμβων ή να αντικαταστήσουν τους κόμβους με άλλους κακόβουλους. Πιο συγκεκριμένα όταν οι κόμβοι δεν είναι σωστά «προστατευμένοι» και οι εισβολείς μπορούν να φτάσουν φυσικά σε αυτούς, μπορούν να δεχθούν επίθεση με τεχνικές αλλοίωσης.

Οι ηλεκτρομαγνητικοί παλμοί (EMP) είναι επίσης μεταξύ των απειλών που μπορούν να ταξινομηθούν στις φυσικές επιθέσεις ασφαλείας. Οι EMP είναι μια έκρηξη

μικρής διάρκειας και υψηλής έντασης ηλεκτρομαγνητική ενέργεια που μπορεί να παράγει κύματα τάσης και έτσι να βλάψει τις ηλεκτρονικές συσκευές εντός εμβέλειας του δικτύου.

2.2 Επιθέσεις στο Επίπεδο Ζεύξης Δεδομένων

Τα κινητά δίκτυα βασίζονται στην ανοικτή αρχιτεκτονική «peer to peer» πολλαπλών βημάτων «multihops», κατά την οποία τα πρωτόκολλα επιπέδου ζεύξης δεδομένων διατηρούν τη σύνδεση ενός βήματος (one hop) μεταξύ των γειτονικών κόμβων. Επομένως οι επιθέσεις μπορούν να πραγματοποιηθούν σε αυτό το επίπεδο διαταράσσοντας τη συνεργασία μεταξύ των πρωτοκόλλων.

Τα ασύρματα πρωτόκολλα για τον έλεγχο της πρόσβασης στο μέσο (MAC) πρέπει να συντονίζουν τη μετάδοση των κόμβων στο κοινό μέσο μετάδοσης. Το πρωτόκολλο IEEE 802.11 MAC χρησιμοποιεί ειδικού μηχανισμούς επίλυσης της διανομής του ασύρματου καναλιού που βασίζονται σε δύο διαφορετικούς αλγορίθμους. Ο ένας είναι ένα πλήρως κατανεμημένο πρωτόκολλο πρόσβασης (Distributed Coordination Function-DCF)και ο άλλος είναι ένα κεντρικό πρωτόκολλο πρόσβασης (Point Coordination Function-PCF), το οποίο απαιτεί ένα 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. (Ajay, D. (2010)).

2.2.1 Επιθέσεις στο πρωτόκολλο IEEE 802.11 MAC

Το πρωτόκολλο IEEE 802.11 MAC είναι ευάλωτο σε επιθέσεις άρνησης παροχής υπηρεσιών (DoS). Για να πραγματοποιηθεί μία επίθεση DoS στο πρωτόκολλο, ο εισβολέας θα πρέπει να εκμεταλλευτεί την εκθετική υποχώρηση του δυαδικού συστήματος (binary exponential backoff scheme). Για παράδειγμα, ο εισβολέας μπορεί να καταστρέψει τα πλαίσια εύκολα με την προσθήκη ορισμένων bits ή αγνοώντας τη συνεχιζόμενη μετάδοση. Μεταξύ των αντιμαχόμενων κόμβων, το δυαδικό εκθετικό σύστημα ευνοεί τον τελευταίο νικητή και οι κόμβοι που έχουν μεγάλο φόρτο τείνουν να συλλάβουν το κανάλι μέσα από τη συνεχή διαβίβαση δεδομένων, προκαλώντας έτσι ελαφρύ φορτίο στους γείτονες με ατελείωτα backoffs. Οι κακόβουλοι κόμβοι θα μπορούσαν αν επωφεληθούν από αυτήν την ευπάθεια και επιπλέον να προκληθεί μια αλυσιδωτή αντίδραση στα πρωτόκολλα των ανώτερων επιπέδων που χρησιμοποιούν ένα σύστημα υποχώρησης, όπως η διαχείριση παραθύρου στο TCP πρωτόκολλο.

2.2.2 DoS επίθεση λόγω αδυναμίας του πεδίου NAV(Network Allocation Vector)

Μια άλλη αδυναμία και κατ' επέκταση μια άλλη DoS επίθεση στο επίπεδο ζεύξης δεδομένων εκτίθεται μέσω του πεδίου του φορέα χορήγησης δικτύου (NAV) που υπάρχει στα πλαίσια RTS/CTS(Ready to Send/Clear to Send). Κατά τη διάρκεια RTS/CTS χειραψίας, ένα μικρό πλαίσιο RTS αποστέλλεται από τον αποστολέα και περιέχει το χρόνο που απαιτείται για την ολοκλήρωση της CTS, της μεταφοράς δεδομένων και των πλαισίων ACK.

Κάθε γείτονας του αποστολέα και του παραλήπτη ενημερώνει το πεδίο NAV και αναβάλει τη διαβίβαση κατά τη διάρκεια της μελλοντικής συναλλαγής σύμφωνα με το χρόνο που άκουσε «τυχαία». Επομένως, ένας εισβολέας μπορεί να ακούσει τις

πληροφορίες του πεδίου NAV και στη συνέχεια να αλλοιώσει το πλαίσιο του επιπέδου ζεύξης δεδομένων μέσω ασύρματων παρεμβολών στη συνεχιζόμενη μετάδοση.

2.2.3 Επίθεση στο πρωτόκολλο IEEE 802.11 WEP

Το πρώτο σύστημα ασφάλειας που παρέχεται από το πρωτόκολλο IEEE 802.11 στα WLAN συστήματα είναι η τεχνολογία Wired Equivalent Privacy(WEP). Είναι πλέον γνωστό ότι το WEP είναι ευάλωτο σε επιθέσεις σχετικά με την ασφάλεια και την ακεραιότητα των μηνυμάτων, καθώς και σε επιθέσεις σχετικά με το κλειδί κρυπτογράφησης των δεδομένων μέσα στο δίκτυο. Πλέον το WEP έχει αντικατασταθεί από το AES στο 802.11i. Ορισμένες από τις αδυναμίες του WEP περιγράφονται παρακάτω:

- Το WEP πρωτόκολλο δε προσδιορίζει τη διαχείριση κλειδιών, γεγονός το οποίο αποτελεί κρίσιμο παράγοντα μιας επίθεσης στο δίκτυο.
- Το διάνυσμα αρχικοποίησης (IV) που χρησιμοποιείται σε ένα WEP είναι ένα πεδίο 24-Bit, το οποίο αποστέλλεται 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 ενός μη-κρυπτογραφημένου αλγορίθμου ακεραιότητας CRC32 με τη κρυπτογράφηση ροής, αποτελεί κίνδυνο για την ασφάλεια και μπορεί να προκαλέσει επιθέσεις όσον αφορά την ασφάλεια και την ακεραιότητα των μηνυμάτων.

2.3 Επιθέσεις στο Επίπεδο δικτύου

Όπως ειπώθηκε και προηγουμένως, στη παρούσα εργασία θα δοθεί μεγάλη έμφαση στο συγκεκριμένο επίπεδο, διότι τα είδη των επιθέσεων που συμβαίνουν στο επίπεδο δικτύου ποικίλλουν λόγω της αδυναμίας των πρωτοκόλλων του.

Πιο συγκεκριμένα, τα πρωτόκολλα του επιπέδου δικτύου διευκολύνουν τη συνδεσιμότητα των γειτονικών κόμβων και όχι μόνο σε ένα δίκτυο manet. Επομένως, σε μια ιδανική κατάσταση θεωρούμε ότι όλοι οι κόμβοι μέσα σε ένα κινητό δίκτυο είναι έμπιστοι και συνεργάζονται μεταξύ τους, γεγονός το οποίο μπορεί να εκμεταλλευτεί οποιοσδήποτε κακόβουλος κόμβος θέλει να εισβάλλει στο δίκτυο. Επειδή κάθε κόμβος είναι υπεύθυνος για τη λήψη αποφάσεων όσον αφορά τη δρομολόγηση των πακέτων, γίνεται σχετικά εύκολα αντιληπτό ότι με μια εσφαλμένη συμπεριφορά ενός κόμβου μπορεί να πραγματοποιηθεί μια επίθεση σε ένα δίκτυο manet.

Πολλές μέθοδοι χρησιμοποιούνται από τους δράστες για να επιτευχθεί ο απώτερος σκοπός τους που είναι η διακοπή της κυκλοφορίας στο δίκτυο. Τα πακέτα της κυκλοφορίας έτσι διαβιβάζονται σε μη βέλτιστα μονοπάτια, γεγονός το οποίο εισάγει σημαντικές απώλειες και καθυστέρηση στο δίκτυο. Επιπλέον, τα πακέτα θα μπορούσαν να διαβιβαστούν σε ένα ανύπαρκτο μονοπάτι και να χαθούν. Οι επιτιθέμενοι μπορούν να αποτρέψουν από ένα κόμβο-πηγή από την εξεύρεση μιας διαδρομής για το προορισμό, προκαλώντας έτσι το διαχωρισμό του δικτύου, γεγονός το οποίο εντείνει τη συμφόρηση του δικτύου και την υποβάθμιση των επιδόσεων.

Οι επιτιθέμενοι εναντίον ενός δικτύου μπορούν να ταξινομηθούν, όπως αναφέραμε και προηγουμένως, σε δύο κατηγορίες: 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 στο μηχανισμό δρομολόγησης των δικτύων MANETs. Οι αλγόριθμοι δρομολόγησης έχουν χαρακτήρα συνεργασίας και έτσι μπορούν να επηρεάσουν ολόκληρο το σύστημα. Τα κυριότερα είδη των επιθέσεων που μπορούν να συμβούν στο επίπεδο δικτύου ενός manet δικτύου είναι τα εξής:

- Επιθέσεις κατά τη φάση ανακάλυψης της διαδρομής (RREQ Επίθεση)
- Επίθεση σκουληκότρυπας
- Επίθεση μαύρης τρύπας
- Rushing επίθεση
- Επίθεση κατανάλωσης πόρων
- Επίθεση αποκάλυψης της τοποθεσίας

2.3.1 Επιθέσεις κατά τη φάση της ανακάλυψης της διαδρομής (RREQ)

Υπάρχουν κακόβουλες επιθέσεις που στοχεύουν στην ανακάλυψη ή στη φάση συντήρησης της δρομολόγησης, μη ακολουθώντας τις προδιαγραφές των πρωτοκόλλων δρομολόγησης και οι οποίες έχουν ως στόχο την ανακάλυψη της διαδρομής. Ορισμένες επιθέσεις τέτοιου τύπου παρουσιάζονται παρακάτω.

(α) Επίθεση υπερχείλισης (overflow) του πίνακα δρομολόγησης:

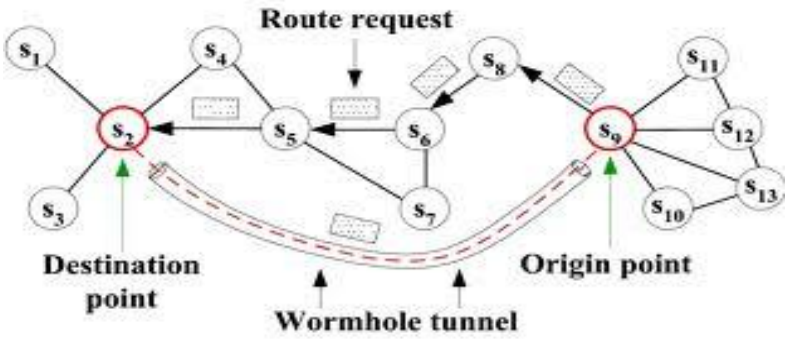
Αυτού του είδους η επίθεση συμβαίνει συνήθως σε προληπτικούς (proactive) αλγορίθμους που στοχεύουν στη περιοδική επαλήθευση των πληροφοριών δρομολόγησης. Για την πραγματοποίηση μιας τέτοιας επίθεσης σε ένα κινητό δίκτυο, ο επιτιθέμενος προσπαθεί να δημιουργήσει διαδρομές για μη υπαρκτούς κόμβους στο δίκτυο. Έτσι στέλνει μεγάλο αριθμό αιτήσεων και προκαλεί υπερχείλιση του πίνακα δρομολόγησης, εφόσον και οι proactive αλγόριθμοι προσπαθούν συνεχώς να ανακαλύψουν πληροφορίες δρομολόγησης πριν να υπάρξει πραγματική ανάγκη. Ο στόχος των επιτιθέμενων είναι να υπάρχουν τόσα δρομολόγια, ώστε η δημιουργία νέων να αποτρέπεται.

(β) Επίθεση «δηλητηρίασης» της κρυφής μνήμης (cache) δρομολόγησης:

Σε αυτού του είδους την επίθεση οι επιτιθέμενοι επωφελούνται από το γεγονός ότι οι πίνακες δρομολόγησης ανανεώνονται με ανομοιογενή τρόπο και αυτό συμβαίνει όταν οι πληροφορίες που φυλάσσονται στους πίνακες αυτούς σβήνονται, μεταβάλλονται ή εμπλουτίζονται με λανθασμένες πληροφορίες. Ας υποθέσουμε για παράδειγμα ότι ο κακόβουλος κόμβος Μ, θέλει να επηρεάσει τις διαδρομές προς τον κόμβο Χ. Ο Μ μπορεί να μεταδώσει πακέτα με αλλοιωμένες πληροφορίες με κόμβο πηγής τον Χ, επομένως οι γειτονικοί του κόμβοι θα προσθέσουν αυτή τη διαδρομή στη δική τους κρυφή μνήμη (route cache), την οποία πρότεινε ο Μ.

2.3.2 Επίθεση Σκουληκότρυπας (Wormhole attack) :

Η επίθεση σκουληκότρυπας είναι μία από τις πιο εξελιγμένες και σοβαρές επιθέσεις στα δίκτυα Manets. Αυτού του είδους η επίθεση είναι δυνατόν να συμβεί ακόμη και αν ο επιτιθέμενος δεν φιλοξενεί κανένα κόμβο και ακόμη και αν όλη η επικοινωνία παρέχει αυθεντικότητα και εμπιστευτικότητα. Σε αυτήν την επίθεση ένα ζευγάρι από επιτιθέμενους λαμβάνει μηνύματα από ένα σημείο του δικτύου και τα αναπαράγει σε ένα άλλο σημείο, χρησιμοποιώντας ένα ιδιωτικό δίκτυο υψηλών ταχυτήτων. Στην *Εικόνα 2* απεικονίζεται η επίθεση σκουληκότρυπας σε ένα κινητό δίκτυο. (Raghavendran, C. (2013)).

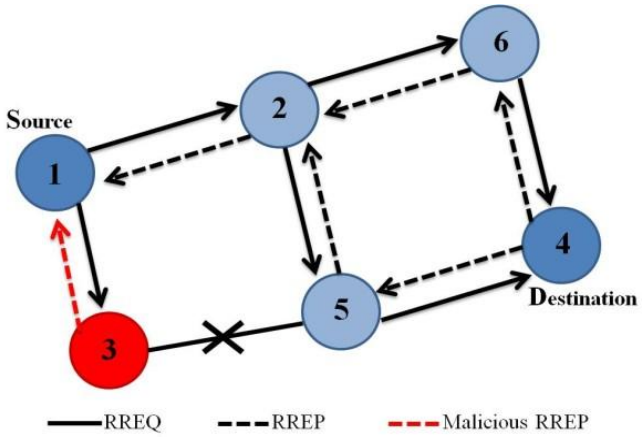


Εικόνα 2: Wormhole attack-Επίθεση σκουληκότρυπας

Είναι επίσης δυνατό για τον εισβολέα να προωθήσει κάθε bit στη «σκουληκότρυπα» απευθείας, χωρίς να περιμένει ένα ολόκληρο πακέτο να ληφθεί έτσι ώστε να μειώσει το χρόνο καθυστέρησης που δημιουργείται από τη σκουληκότρυπα. Επιπλέον ο εισβολέας είναι αόρατος στα υψηλότερα επίπεδα, σε αντίθεση με ένα κακόβουλο κόμβο σε ένα πρωτόκολλο δρομολόγησης, ο οποίος μπορεί εύκολα να φανερωθεί. Λόγω της φύσης της ασύρματης μετάδοσης, ο επιτιθέμενος μπορεί να δημιουργήσει μία «σκουληκότρυπα» ακόμη 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».

2.3.3 Επίθεση Μαύρης Τρύπας (Blackhole attack):

Σε αυτήν την επίθεση ένας κακόβουλος κόμβος προσπαθεί να «ξεγελάσει» τους γειτονικούς του κόμβους, έτσι ώστε να προσελκύσει όλα τα πακέτα δρομολόγησης σε αυτούς. Εκμεταλλεύεται το πρωτόκολλο δρομολόγησης με σκοπό να διαφημίσει ότι έχει μια έγκυρη διαδρομή για ένα κόμβο προορισμού, έστω και αν η διαδρομή αυτή είναι πλαστή, έχοντας ως πρόθεση τη σύλληψη των πακέτων. Όπως και στην επίθεση σκουληκότρυπας, έτσι και στις επιθέσεις μαύρης τρύπας, οι κακόβουλοι κόμβοι ξεκινάν την εισβολή στο δίκτυο διαφημίζοντας τους ίδιους στους γειτονικούς τους κόμβους, ότι κατέχουν την πιο βέλτιστη διαδρομή για τους προορισμούς που τους έχουν ζητηθεί. Η επίθεση της μαύρης τρύπας παρουσιάζεται στην *Εικόνα 3*.



Εικόνα 3: Blackhole attack-Επίθεση μαύρης τρύπας

Η επίθεση αυτή διαδραματίζεται σε δύο στάδια. Στο πρώτο στάδιο, ο κακόβουλος κόμβος εκμεταλλεύεται το πρωτόκολλο δρομολόγησης του κινητού δικτύου ώστε να διαφημίσει τον ίδιο ότι έχει μια έγκυρη διαδρομή προς ένα κόμβο προορισμού, με σκοπό να παρακολουθεί τα πακέτα. Σε δεύτερο στάδιο, ο εισβολέας δε προωθεί τα πακέτα που έχει προηγουμένως συλλάβει. Σε μια πιο προχωρημένη μορφή, ο εισβολέας καταστέλλει ή τροποποιεί τα πακέτα που προέρχονται από ορισμένους κόμβους, ενώ ταυτόχρονα θα αφήσει ανεπηρέαστα τα δεδομένα που προέρχονται από άλλους κόμβους.

2.3.4 Byzantine attack:

Η βυζαντινή επίθεση μπορεί να δημιουργηθεί σε ένα κινητό δίκτυο είτε από ένα μόνο κακόβουλο κόμβο ή ακόμη και από μία ομάδα κόμβων οι οποίοι συνεργάζονται μεταξύ τους. Μια ομάδα από κόμβους που έχουν σκοπό να παρεμποδίσουν τη σωστή λειτουργία του δικτύου, μπορούν για παράδειγμα να δημιουργούν αλυσίδες στη διαδρομή των πακέτων, να προωθούν τα πακέτα σε μακρινές διαδρομές αντί να επιλέγουν τις σωστές, ακόμη και να απορρίπτουν τα πακέτα. Η επίθεση αυτή μειώνει την απόδοση του δικτύου, και επίσης διαταράσσει τις υπηρεσίες δρομολόγησης.

2.3.5 Rushing attack:

Στην επίθεση σκουληκότρυπας, δύο επιτιθέμενοι κόμβοι σχηματίζουν μεταξύ τους ένα τούνελ για να αλλοιώσουν την πραγματική διαδρομή. Αν για παράδειγμα η μετάδοση στο τούνελ είναι αρκετά γρήγορη, τότε τα πακέτα σε αυτό μεταδίδονται γρηγορότερα σε σύγκριση με αυτά που μεταδίδονται μέσα από μια «multi-hop» διαδρομή και έτσι η επίθεση καταλήγει σε rushing. Ουσιαστικά, είναι μια άλλη μορφή της επίθεσης DoS(Denial of Service), η οποία μπορεί να τεθεί σε λειτουργία εναντίον όλων των ως τώρα γνωστών πρωτοκόλλων δρομολόγησης, όπως τα ARAN και Ariadne.

2.3.6 Resource Consumption Attack - Επίθεση κατανάλωσης πόρων:

Σε ένα κινητό δίκτυο η ενέργεια αποτελεί κρίσιμο παράγοντα, διότι οι συσκευές που έχουν σαν μόνη πηγή ενέργειας τη μπαταρία προσπαθούν να εξοικονομήσουν ενέργεια, εκπέμποντας δεδομένα μόνο όταν αυτό κριθεί απολύτως απαραίτητο. Ο στόχος της επίθεσης κατανάλωσης πόρων είναι να αναγκάσει το θύμα με διάφορες μεθόδους να μεταδίδει ή να λαμβάνει πακέτα συνεχώς, έτσι ώστε να εξαντληθούν οι ενεργειακοί του πόροι. Έτσι ένας εισβολέας ή ένας κακόβουλος κόμβος μπορεί να διαταράξει τις κανονικές λειτουργίες του κινητού δικτύου. Αυτή η επίθεση είναι γνωστή και ως επίθεση στέρησης ύπνου (sleep deprivation attack).

2.3.7 Location Disclosure attacks – Επίθεση αποκάλυψης της τοποθεσίας:

Το είδος αυτό της επίθεσης είναι ένα μέρος της επίθεσης αποκάλυψης πληροφοριών (Information Disclosure). Ο κακόβουλος κόμβος διαβάζει πληροφορίες σχετικά με τη τοποθεσία ή τη δομή του κινητού δικτύου και χρησιμοποιεί τις πληροφορίες αυτές για περαιτέρω επιθέσεις. Συγκεντρώνει τις πληροφορίες σχετικά με τη θέση των κόμβων στο δίκτυο και γνωρίζει ποιοι κόμβοι εμπεριέχονται σε κάθε διαδρομή. Η ανάλυση της κυκλοφορίας ή όπως είναι ευρέως γνωστό «traffic analysis», είναι ένα από τα άλυτα προβλήματα ασφάλειας εναντίον των MANET δικτύων.

3. Τρόποι αντιμετώπισης επιθέσεων στα Manet

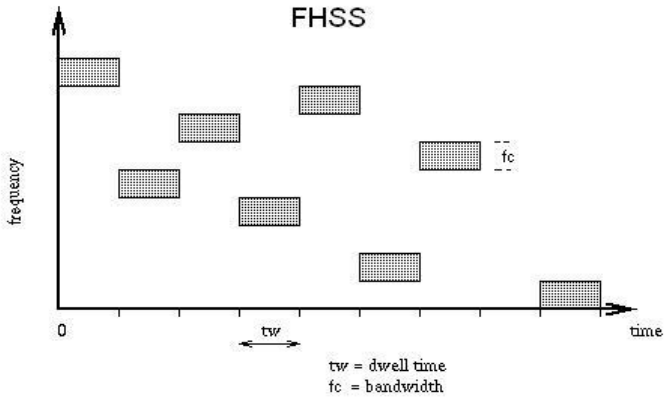
Στη παρούσα εργασία θα αναφερθούμε επίσης και σε ορισμένους τρόπους αντιμετώπισης των επιθέσεων στα κινητά δίκτυα και συγκεκριμένα σε τεχνικές ασφάλειας για τα είδη των επιθέσεων που μπορούν να συμβούν στα πιο κρίσιμα επίπεδα του μοντέλου OSI. Αρχικά, είναι γνωστό ότι οι κινητοί κόμβοι που σχηματίζουν ένα δίκτυο Manet είναι συνήθως κινητές συσκευές με περιορισμένη φυσική προστασία όσο και περιορισμένους πόρους. Ενότητες ασφάλειας όπως οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για την προστασία από φυσικές επιθέσεις. Επιπλέον τα κρυπτογραφικά εργαλεία χρησιμοποιούνται ευρέως για την παροχή ισχυρών υπηρεσιών ασφάλειας των κινητών δικτύων, όπως είναι η εμπιστευτικότητα, η επαλήθευση της ακεραιότητας και η μη άρνηση αναγνώρισης. Δυστυχώς όμως η κρυπτογράφηση δε μπορεί να εγγυηθεί τη διαθεσιμότητα. Για παράδειγμα, δε μπορεί να αποτρέψει την εμπλοκή με το ραδιόφωνο. Ακόμη η κρυπτογράφηση απαιτεί έναν δύσκολο υπολογισμό, ο οποίος περιορίζεται από τις δυνατότητες των συσκευών (π.χ. της CPU ή της μπαταρίας). Τα τωρινά πρωτόκολλα δρομολόγησης για τα κινητά δίκτυα είναι ανασφαλής και για αυτό το λόγο ο σχεδιασμός ενός πρωτοκόλλου δρομολόγησης, το οποίο να ικανοποιεί τους προτεινόμενους στόχους ασφαλείας, αποτελεί ακόμη ένα ανοιχτό πρόβλημα. Η πιθανή παρουσία εχθρών με lap-top, insiders και η περιορισμένη συσχέτιση μηχανισμών ασφαλείας end-to-end, απαιτούν προσεκτικό σχεδιασμό πρωτοκόλλων.

3.1 Αντιμετώπιση επιθέσεων στο Φυσικό επίπεδο:

Το φυσικό επίπεδο των δικτύων Manet είναι πιο ευάλωτο στην τροποποίηση των σημάτων (signal jamming), στην DoS επίθεση καθώς και σε ορισμένες παθητικές επιθέσεις, διότι η ασύρματη επικοινωνία ενός κινητού δικτύου μεταδίδεται από τη φύση και ένα ραδιοφωνικό σήμα είναι πολύ εύκολο να τροποποιηθεί. Δύο τεχνολογίες του ραδιοφάσματος μπορούν να χρησιμοποιηθούν για να καταστήσουν πιο δύσκολη την ανίχνευση ή τη τροποποίηση των σημάτων και αυτές είναι η συχνότητα hopping (FHSS) ή η άμεση ακολουθία (DSSS). Οι τεχνολογίες αυτές αλλάζουν τη συχνότητα κατά τυχαίο τρόπο κάνοντας έτσι δύσκολη τη σύλληψη του σήματος ή την εξάπλωση της ενέργειας σε ένα ευρύτερο φάσμα, έτσι ώστε η ισχύς μετάδοσης να είναι «κρυμμένη» πίσω από το επίπεδο θορύβου.

3.1.1 Frequency Hopping Spread Spectrum (FHSS)

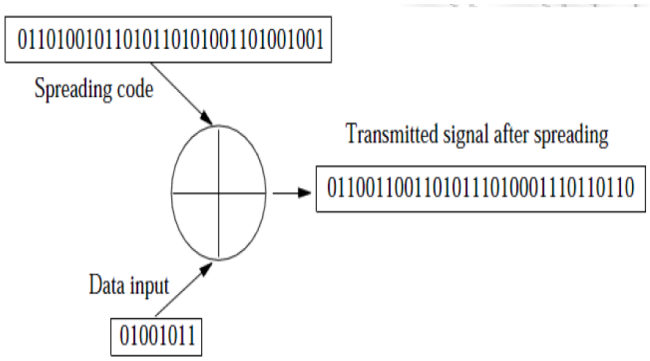
Η τεχνολογία FHSS κάνει το σήμα να φαίνεται στους υποκλοπείς ως ένας ακατάληπτος παλμικός θόρυβος διάρκειας. Αυτό συμβαίνει διότι το σήμα είναι διαμορφωμένο με μια τυχαία σειρά ραδιοσυχνοτήτων, οι οποίες μεταπηδούν (hops) από συχνότητα σε συχνότητα σε τακτά χρονικά διαστήματα. Ο δέκτης χρησιμοποιεί τον ίδιο κώδικα εξάπλωσης, ο οποίος είναι συγχρονισμένος με τον πομπό, ώστε τα δεδομένα να μεταδίδονται πάνω από ένα κανάλι. Έτσι η παρεμβολή ελαχιστοποιείται δεδομένου ότι το σήμα έχει διασπαστεί σε πολλές συχνότητες. Η παρακάτω εικόνα (*Εικόνα 4*) δείχνει ένα παράδειγμα μιας τεχνολογίας FHSS.



Εικόνα 4: Τεχνολογία Frequency Hopping Spread Spectrum

3.1.2 Direct Sequence Spread Spectrum (DSSS):

Με βάση αυτή τη τεχνολογία 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 μία 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. Στη παρακάτω εικόνα (*Εικόνα 5*) φαίνεται πως μπορεί να εφαρμοστεί η τεχνολογία DSSS σε ένα εκπεμπόμενο σήμα. Μπορούμε λοιπόν να παρατηρήσουμε 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 τέσσερα bits του κώδικα που εξαπλώνεται (spreading code).



Εικόνα 5: Direct Sequence Spread Spectrum-DSSS

3.2 Αντιμετώπιση επιθέσεων στο επίπεδο ζεύξης δεδομένων

Τα πρωτόκολλα στο συγκεκριμένο επίπεδο των κινητών δικτύων βοηθούν στην εύρεση των «κοντινών (1-hop)» γειτόνων, στη δίκαιη πρόσβαση στο κανάλι, στο πλαίσιο ελέγχου σφαλμάτων και διατηρούν τις συνδέσεις με τους γείτονες. Παρ' όλα αυτά, υπάρχουν κακόβουλες επιθέσεις που στοχεύουν στη διακοπή της συνεργασίας των πρωτοκόλλων σε αυτό το επίπεδο. Όπως αναφέρθηκε και προηγουμένως, οι επιθέσεις κατανάλωσης πόρων (χρησιμοποιώντας το πεδίο NAV) εξακολουθούν να αποτελούν μια ανοικτή πρόκληση αν και ορισμένα προγράμματα, όπως το ERA-802.11, προτείνουν κάποιους αλγόριθμους ανίχνευσης. Επίσης, είναι ευρέως γνωστό ότι το σύστημα κρυπτογράφησης (WEP) έχει

επικριθεί για τις αδυναμίες του και για αυτό έχουν προταθεί άλλα πρωτόκολλα του επιπέδου ζεύξης δεδομένων όπως είναι το LLSP. (Pankajini, P. (2013)).

3.2.1 Πρωτόκολλο Link Layer Security Protocol (LLSP):

Το πρωτόκολλο LLSP παρέχει μία σειρά από υπηρεσίες ασφάλειας στο επίπεδο ζεύξης ενός κινητού δικτύου και είναι υπεύθυνο για τον έλεγχο της ταυτοποίησης και της κρυπτογράφησης σε αυτό το επίπεδο. Η ταυτοποίηση επιτρέπει στον παραλήπτη ενός ψηφιακού μηνύματος να γνωρίζει την ταυτότητα του αποστολέα και εξασφαλίζεται έτσι η 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 ασφάλειας του επιπέδου ζεύξης, ο μηχανισμός «Watchdog» του πρωτοκόλλου LLSP του κάθε γείτονα ενημερώνει το στρώμα MAC ώστε να λάβει τα αναγκαία μέτρα για την εσφαλμένη συμπεριφορά των γειτονικών του κόμβων.

3.3 Αντιμετώπιση επιθέσεων στο επίπεδο δικτύου:

Το επίπεδο του δικτύου είναι το πιο ευάλωτο σε επιθέσεις σε ένα manet δίκτυο, από τα υπόλοιπα επίπεδα του μοντέλου OSI. Μια ποικιλία από μηχανισμούς ασφαλείας επιβάλλεται σε αυτό το επίπεδο αλλά και μέσω της χρήσης ασφαλών πρωτοκόλλων δρομολόγησης εξασφαλίζεται η πρώτη γραμμή άμυνας του δικτύου. Οι παθητικές επιθέσεις σε πληροφορίες δρομολόγησης μπορούν να αντιμετωπιστούν με τις ίδιες μεθόδους με τις οποίες προστατεύονται τα δεδομένα κίνησης. Από την άλλη, ορισμένες ενεργές επιθέσεις όπως η παράνομη τροποποίηση των μηνυμάτων δρομολόγησης, μπορούν να προληφθούν με μηχανισμούς ελέγχου προέλευσης της ταυτότητας του μηνύματος καθώς και της ακεραιότητας. Παρακάτω παρατίθενται ορισμένοι τρόποι αντιμετώπισης διαφόρων επιθέσεων που συμβαίνουν στο επίπεδο δικτύου.

3.3.1 Αντιμετώπιση επιθέσεων σκουληκότρυπας (Wormhole attack):

Ένα πακέτο–λουρί (packet leashes) προτείνεται ως αντίμετρο για την επίθεση σκουληκότρυπας, το οποίο περιλαμβάνει πληροφορίες που προστίθενται σε ένα πακέτο για να περιορίσει την απόσταση εκπομπής του. Επιπλέον μπορούν να εφαρμοστούν δύο άλλες χρήσιμες τεχνικές ασφάλειας για την επίθεση αυτή, εκ των οποίων η μία ονομάζεται μηχανισμός τομέα (sector mechanism) και προτείνεται για την ανίχνευση μιας σκουληκότρυπας χωρίς την ανάγκη συγχρονισμού του ρολογιού, και η άλλη είναι γνωστή ως κατευθυντήριες κεραίες (directional antennas). Πιο αναλυτικά:

3.3.1.1 Πακέτα λουριών (Packet leashes):

Ένα πακέτο λουριών θέτει τη διάρκεια ζωής ενός πακέτου το οποίο προσθέτει ένα περιορισμό για την απόσταση εκπομπής του. Ο αποστολέας κατέχει πληροφορίες σχετικά με το χρόνο μετάδοσης και την τοποθεσία του μηνύματος και στη συνέχεια ο δέκτης επαληθεύει αν το πακέτο έχει διανύσει την απόσταση μεταξύ του αποστολέα και του ίδιου, εντός του χρονικού διαστήματος μεταξύ της λήψης και της διαβίβασης του. Για αυτό το λόγο τα πακέτα λουριών απαιτούν άρτια συγχρονισμένα ρολόγια και ακριβή γνώση της τοποθεσίας.

3.3.1.2 Μηχανισμός τομέα (Sector mechanism):

Ο μηχανισμός τομέα βασίζεται στην εξ αποστάσεως οριοθέτηση τεχνικών, στην μονόδρομη hash αλυσίδα, και στο δέντρο κατακερματισμού Merkle. Ο συγκεκριμένος μηχανισμός μπορεί να χρησιμοποιηθεί για να βοηθήσει τα ασφαλή πρωτόκολλα δρομολόγησης στα Manets, ώστε να μπορούν να ανιχνεύουν τυχών επιθέσεις, μέσω του εντοπισμού της τοπολογίας.

3.3.1.3 Κατευθυντήριες κεραίες (Directional antennas):

Οι κατευθυντήριες κεραίες δεν απαιτούν πληροφορίες για τον εντοπισμό ή το συγχρονισμό του ρολογιού και είναι πιο αποτελεσματικές με την ενέργεια. (Sivakumar, K. (2013)).

3.3.2 Αντιμετώπιση επιθέσεων Μαύρης τρύπας (Blackhole attack):

Μερικά ασφαλή πρωτόκολλα όπως το Secure Aware Ad Hoc Routing Protocol (SAR) καθώς και το Secure Ad Hoc On Demand Distance Vector (SAODV), μπορούν να χρησιμοποιηθούν σε ένα κινητό δίκτυο ώστε να το προστατέψουν από την επίθεση της μαύρης τρύπας. Πιο αναλυτικά:

3.3.2.1 Secure Aware Ad Hoc Routing Protocol (SAR):

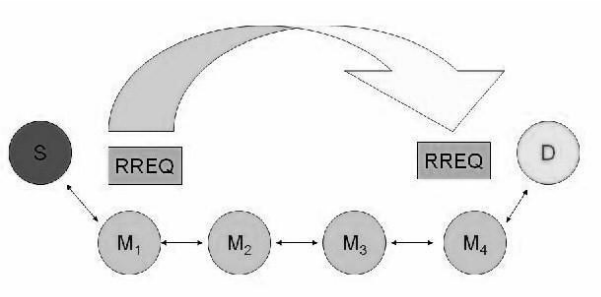
Το πρωτόκολλο SAR βασίζεται στα on-demand πρωτόκολλα, όπως το AODV και το DSR. Στο SAR ένα μέτρο ασφάλειας προστίθεται στο πακέτο RREQ, και χρησιμοποιείται μια διαφορετική διαδικασία ανακάλυψης της διαδρομής. Οι ενδιάμεσοι κόμβοι λαμβάνουν ένα πακέτο RREQ με μια συγκεκριμένη ασφάλεια ή ένα επίπεδο εμπιστοσύνης. Στους ενδιάμεσους κόμβους, εφόσον πληρούνται τα μέτρα ασφάλειας και το επίπεδο εμπιστοσύνης, ο κόμβος θα επεξεργαστεί το πακέτο RREQ και θα το διαδώσει στους γείτονές του με ελεγχόμενες πλημμύρες (controlled floodings). Σε αντίθετη περίπτωση, 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 τη συγκεκριμένη ασφάλεια. Αν ο κόμβος προορισμού αποτύχει να βρει μια διαδρομή με την απαιτούμενη ασφάλεια ή το επίπεδο εμπιστοσύνης, στέλνει μια ειδοποίηση στον αποστολέα και τον επιτρέπει να ρυθμίσει το επίπεδο ασφαλείας του, έτσι ώστε να ανακαλύψει μία νέα διαδρομή.(Rajib, D. (2011)).

3.3.2.2 Secure Ad Hoc On Demand Distance Vector (SAODV):

Το πρωτόκολλο SAODV είναι μια επέκταση του πρωτοκόλλου AODV και είναι και αυτό αποτελεσματικό στις επιθέσεις μαύρης τρύπας. Το ασφαλές AODV σύστημα βασίζεται στην υπόθεση ότι κάθε κόμβος κατέχει τα πιστοποιημένα δημόσια κλειδιά όλων των κόμβων του δικτύου. 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 καταφτάσει στον προορισμό του, υπογράφει την απάντηση «Route Reply» με το ιδιωτικό του κλειδί και την αποστέλλει πίσω. Οι ενδιάμεσοι κόμβοι ελέγχουν πάλι την υπογραφή και εν τέλει η

υπογραφή του αποστολέα αποθηκεύεται πάλι μαζί με τη νέα διαδρομή. Στη παρακάτω εικόνα παρουσιάζεται η αρχή λειτουργίας του πρωτοκόλλου SAODV (Εικόνα 6).



Εικόνα 6: Secure Ad Hoc On Demand Distance Vector (SAODV)

4. Πλεονεκτήματα-Μειονεκτήματα των Manet

- **Πλεονεκτήματα:**
  - Ένα κινητό δίκτυο μπορεί να αναπτυχθεί και με την ελάχιστη τηλεπικοινωνιακή υποδομή, που σημαίνει ότι για τη δημιουργία του δεν απαιτούνται πολλά περιττά έξοδα.
  - Τα δίκτυα αυτά μπορούν να δημιουργηθούν σε κάθε τόπο και χρονική στιγμή.
  - Τα manets δίκτυα μπορούν να λειτουργήσουν χωρίς καμία προϋπάρχουσα υποδομή και δεν απαιτούν μεγάλο χρονικό διάστημα για να υλοποιηθούν.
  - Παρέχουν πρόσβαση στους χρήστες τους σε πληροφορίες και υπηρεσίες ανεξάρτητα από τη γεωγραφική θέση.
  - Τα εν λόγω δίκτυα μπορούν είτε να λειτουργήσουν αυτόνομα, είτε να συνδεθούν στο Internet.
  - Κάθε συσκευή σε ένα MANET είναι ελεύθερη να κινηθεί προς κάθε κατεύθυνση, και ως εκ τούτου να αλλάζει συχνά τις ζεύξεις της με άλλες συσκευές.

- **Μειονεκτήματα:**
  - Τα κινητά δίκτυα έχουν περιορισμένους πόρους και περιορισμένες τεχνικές ασφάλειας
  - Λόγω των αλγορίθμων δρομολόγησης που χρησιμοποιούνται από τα εν λόγω δίκτυα, επιβάλλεται από τους κόμβους να έχουν αμοιβαία εμπιστοσύνη μεταξύ τους και να συνεργάζονται, γεγονός το οποίο τα καταστεί πολύ ευάλωτα σε επιθέσεις.
  - Συνήθως πολλά δίκτυα manets εγκαθίστανται χωρίς άδεια.
  - Η τοπολογία αυτών των δικτύων καθιστά δύσκολη την ανίχνευση των κακόβουλων κόμβων σε αυτά.
  - Τα πρωτόκολλα ασφαλείας για τα ενσύρματα δίκτυα δε μπορούν να εφαρμοστούν και στα ad hoc δίκτυα.

5. Συμπεράσματα – Προτάσεις για μελλοντική έρευνα

Η ασφάλεια των κινητών δικτύων αποτελεί ένα κρίσιμο θέμα ακόμη και σήμερα για πολλούς ερευνητές, διότι εάν κάποια στιγμή καταφέρουν να εξασφαλισθεί μπορεί να έχει ως αποτέλεσμα την ευρεία ανάπτυξη τους. Οι περισσότερες από τις ερευνητικές εργασίες επικεντρώνονται στην ανάλυση των επιθέσεων στο επίπεδο δικτύου, διότι θεωρείται το πιο ευάλωτο επίπεδο του μοντέλου OSI. Παρ' όλα αυτά, υπάρχουν ορισμένες απρόβλεπτες ή πιο περίπλοκες επιθέσεις οι οποίες παραμένουν ανεξερεύνητες.

Περισσότερη έρευνα μπορεί να πραγματοποιηθεί σε θέματα που αφορούν τα συστήματα διαχείρισης των κλειδιών κρυπτογράφησης, στα πρωτόκολλα δρομολόγησης των δικτύων, στις τεχνικές ασφάλειας δρομολόγησης των δικτύων καθώς και στην ασφάλεια των δεδομένων στο επίπεδο του δικτύου. Η ***επίγνωση του πλαισίου δρομολόγησης (context-awareness)*** είναι ένας πολλά υποσχόμενος τομέας για μελλοντική έρευνα των κινητών δικτύων, διότι λόγω της πολυμορφίας του μπορεί να προσαρμόζει τη λειτουργία του σε ένα μεταβαλλόμενο δίκτυο όσον αφορά το πλαίσιο ανάπτυξής του σε πραγματικό χρόνο. Η έννοια της επίγνωσης του πλαισίου δρομολόγησης (context-awareness) αναφέρεται στην ικανότητα υπηρεσιών κινητού υπολογισμού, να μετρούν, να ανακτούν και να συμπεραίνουν πληροφορία πλαισίου (πολυδιάστατα δεδομένα) από το περιβάλλον που ενεργεί ο χρήστης και να προσαρμόζονται σε αυτό. Η πιο κατάλληλη δρομολόγηση μπορεί να αλλάξει κατά τη διάρκεια ζωής ενός δικτύου ή ακόμη ορισμένες «περιφέρειες» των δικτύων στα Manet μπορούν να επιλέξουν να εφαρμόσουν διαφορετικές πολιτικές δρομολόγησης με τους manet δρομολογητές.(Νικητίδης, Μ. (2009)).

Εν τέλει σα μελλοντική έρευνα μπορεί να θεωρηθεί η ανάγκη για την ανάπτυξη νέων τεχνικών ασφαλείας καθώς και ο κατάλληλος συνδυασμός τους με τις ήδη υπάρχουσες, οι οποίες θα είναι ικανές να αντιμετωπίζουν τα είδη των επιθέσεων που αναφέρθηκαν. Όλα αυτά μπορούν να υλοποιηθούν με βασική προϋπόθεση όλες οι τεχνικές ασφαλείας να μπορούν να σχεδιάζονται σωστά ώστε να εξασφαλίζουν υψηλό επίπεδο εμπιστοσύνης στα κινητά δίκτυα έναντι των κλασικών μηχανισμών ασφάλειας.

Βιβλιογραφικές αναφορές

Abhay, Rajiv, Saurabh, K. (2010, 31 Ιουλίου). Different Types of Attacks on Integrated MANET-Inte rnet Communication *International Journal of Computer Science and Security (IJCSS) 4, (3)*. Ανακτήθηκε 28 Δεκεμβρίου, 2013, από http://www.cscjournals.org/csc/download/issuearchive/IJCSS/volume4/IJCSS_V4_I3.pdf

Ankita, Sanjay, G. (2012, 4 Ιουλίου). Various Routing Attacks In Mobile Ad-Hoc Networks *International Journal Of Computing & Corporate Research 2, (4)*. Ανακτήθηκε 13 Δεκεμβρίου, 2013, από http://www.ijccr.com/july2012/6.pdf.

Ajay, Aman, Meha, D. (2010). IEEE 802.11 Based MAC Improvements for MANET *International Journal Computer Applications 1, (2)*. Ανακτήθηκε 6 Δεκεμβρίου, 2013, από http://www.ijcaonline.org/manets/number2/SPE66T.pdf.

Chaudhary, P. (2013). Classification Of Security Attacks In Manet *Asian Journal Of Computer Science And Information Technology 3, (5)*. Ανακτήθηκε 22 Δεκεμβρίου, 2013, από http://www.innovativejournal.in/index.php/ajcsit/article/view/365.

Danailov, Z. (2012). *Attacks on mobile ad hoc networks*. Μη εκδεδομένη διδακτορική διατριβή, Ruhr-University Bochum, http://www.slideshare.net/xeon40/attacks-on-mobile-ad-hoc-networks-12619703.

Dhruvi, M. (2013). A Review Paper on Network Layer attacks in MANETs *International Journal for Scientific Research & Development 1, (9)*. Ανακτήθηκε 16 Δεκεμβρίου, 2013, από http://ijsrd.com/index.php?p=aboutus.

International Conference On Ongoing Research In Management & It. (2013). *Security Aspects In Mobile Ad Hoc Network (Manets)*. Ανακτήθηκε 15 Δεκεμβρίου, 2013, από http://www.asmedu.org/incon/publication/INCON13-IT-006.pdf.

Mamatha, Sharma, G. (2010). Network Layer Attacks and Defense Mechanisms in MANETS-A Survey *International Journal of Computer Applications 9, (9)*. Ανακτήθηκε 14 Δεκεμβρίου, 2013, από http://www.ijcaonline.org/volume9/number9/pxc3871911.pdf.

Mangesh, Pradeep, Ali, M. (2011). *Countermeasures of Network Layer Attacks in MANETs*. Ανακτήθηκε 15 Δεκεμβρίου, 2013, από http://research.ijcaonline.org/nsc/number1/SPE002T.pdf.

Mohammad, Rajesh, Goudar, W. (2011). *A Survey of Attacks Happened at Different Layers of Mobile Ad - Hoc Network & Some Available Detection Techniques*. Ανακτήθηκε 21 Δεκεμβρίου, 2013, από http://research.ijcaonline.org/comnet/number1/comnet1010.pdf.

Pankajini, Khitish, Niranjan, P. (2013). Manet Attacks and their Countermeasures: A Survey *International Journal of Computer Science and Mobile Computing 2, (11)*. Ανακτήθηκε 19 Δεκεμβρίου, 2013, από http://paper.researchbib.com/?action=viewPaperDetails&paperid=9887.

Purushottam, Rupali, P. (2012). A survey on Selfishness and Countermeasure in MANET *International Journal of Advanced Research in Computer Science and Electronics Engineering 1, (4)*. Ανακτήθηκε 7 Δεκεμβρίου, 2013, από http://www.ijarcsee.org/index.php/IJARCSEE/article/view/100/100.

Raghavendran, Satish, Varma, C. (2013, 1 Σεπτεμβρίου). Security Challenges and Attacks in Mobile Ad Hoc Networks *International Journal of Information Engineering and Electronic Business(IJIEEB) 5, (3)*. Ανακτήθηκε 17 Δεκεμβρίου, 2013, από http://www.mecs-press.org/ijieeb/ijieeb-v5-n3/IJIEEB-V5-N3-6.pdf.

Rajib, Bipul, Prodipto, D. (4 Απριλίου, 2011). *Security Measures for Black Hole Attack in MANET: An Approach*. Ανακτήθηκε 7 Δεκεμβρίου, 2013, από http://arxiv.org/find/all/1/all:+AND+manets+AND+attacks+in/0/1/0/all/0/1.

Rajni, Alisha, S. (2011). A Study of Various Security Attacks and their Countermeasures in MANET *International Journal of Advanced Research in Computer Science and Software Engineering 1, (1)*. Ανακτήθηκε 8 Δεκεμβρίου, 2013, από http://www.ijarcsse.com/docs/papers/december2011/V1I102.pdf.

Sivakumar, Selvaraj, K. (2013, 1 Ιανουαρίου). Overview Of Various Attacks In Manet And Countermeasures For Attacks *International Journal of Computer Science and Manag ement Research 2, (1)*. Ανακτήθηκε 14 Δεκεμβρίου, 2013, από http://www.ijcsmr.org/vol2issue1/paper201.pdf.

Sivakumar, Selvaraj, K. (2013, 1 Ιανουαρίου). Analysis o f Worm Hole Attack In M ANET And Avoidance Using Robust Secure Routing Method *International Journal of Advanced Research in Computer Science and Software Engineering 3, (1)*. Ανακτήθηκε 14 Δεκεμβρίου, 2013, από http://www.ijarcsse.com/docs/papers/Volume_3/1_January2013/V3I1-0241.pdf.

Sudhir, Sanjeev J., Sanjeev S., A. (2011, 1 Ιανουαρίου). A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks *Journal Of Computing 3, (1)*. Ανακτήθηκε 6 Δεκεμβρίου, 2013, από http://arxiv.org/ftp/arxiv/papers/1105/1105.5623.pdf.

Wikipedia. (21 Μαρτίου, 2013). *MANET*. Ανακτήθηκε 30 Δεκεμβρίου, 2013, από http://el.wikipedia.org/wiki/MANET.

Μητρόπουλος, Γ. (4 Ιουλίου, 2011). *Αδυναμίες Ασφάλειας και Επιθέσεις σε Manet Δ ίκτυα*. Ανακτήθηκε 18 Δεκεμβρίου, 2013, από http://digilib.lib.unipi.gr/dspace/handle/unipi/4108.

Νικητίδης, Μ. (2009). *Μηχανισμός Ανακάλυψης Πληροφορίας Πλαισίου με χρήση Αλγορίθμων Διάχυσης Πληροφορίας*. Μη εκδεδομένη διδακτορική διατριβή, Ελληνικό Ανοικτό Πανεπιστήμιο Σχολή Θετικών Επιστημών Και Τεχνολογίας, Πάτρα.