Πανεπιστήμιο Μακεδονίας
ΔΠΜΣ Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών
Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia
Master Information Systems
Computer Networks
Professor: A.A. Economides

Attacks on Mobile Ad Hoc Networks

Επιθέσεις σε Mobile Ad Hoc Δίκτυα

Σπύρος Ξανθόπουλος
E-mail: mis114@uom.gr
AEM: 411

Θεσσαλονίκη
Φεβρουάριος 2012

10/2/2012

Abstract

Mobile ad hoc networks (MANETs) are gaining special attention due to their flexibility and independence of network infrastructures. Because of their special characteristics such as the dynamic network topology, the limited bandwidth and battery power, it is a particular challenging task to provide a high level of security in a MANET network in relation to a conventional network. Security is an essential factor in wired and wireless networks, and the success of MANET networks will depend on people's confidence in its security. In this article we attempt to investigate the characteristics and the impact of major attacks in MANET networks with emphasis on attacks at the Network Level.

Περίληψη

Τα Mobile Ad Hoc δίκτυα (MANET) αποκτούν αυξανόμενο ενδιαφέρον εξαιτίας της ευελιξίας και ανεξαρτησίας των δικτυακών τους υποδομών. Λόγω των ιδιαίτερων χαρακτηριστικών τους όπως η δυναμική δικτυακή τοπολογία, το περιορισμένο εύρος μετάδοσης και η περιορισμένη ισχύς μπαταρίας, η παροχή υψηλού επιπέδου ασφάλειας σε ένα δίκτυο MANET αποτελεί μια ιδιαίτερη πρόκληση σε σχέση με ένα συμβατικό δίκτυο. Η ασφάλεια είναι γενικότερα σημαντικότατος παράγοντας τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα, οπότε πέρα από τα όποια πλεονεκτήματα, η ευδοκίμηση αυτών των τύπων δικτύων θα εξαρτηθεί από την εμπιστοσύνη των χρηστών σε θέματα ασφάλειας. Σε αυτή την εργασία γίνεται προσπάθεια έρευνας των χαρακτηριστικά και τον τρόπου επίδρασης των σημαντικότερων επιθέσεων σε δίκτυα MANET με κύρια έμφαση στις επιθέσεις σε Επίπεδο Δικτύου.

Επιθέσεις σε Κινητά Ad Hoc Δίκτυα (MANETs)

Η παρούσα εργασία εκπονήθηκε κατά το δεύτερο εξάμηνο σπουδών στο Διατμηματικό Μεταπτυχιακό Πρόγραμμα Σπουδών στα Πληροφοριακά Συστήματα του Πανεπιστημίου Μακεδονίας στα πλαίσια του μαθήματος «Δίκτυα Υπολογιστών».

Η συγκεκριμένη εργασία καλύπτει θέματα που σχετίζονται με τις επιθέσεις σε Ad Hoc Mobile (MANET) δίκτυα. Δίνεται ιδιαίτερη έμφαση στις επιθέσεις που αναφέρονται στο Επίπεδο Δικτύου (Network Layer) ενώ για λόγους πληρότητας γίνεται παράθεση των σημαντικότερων επιθέσεων στα υπόλοιπα επίπεδα. Τα δίκτυα MANET αποτελούν πόλο έλξης ερευνητικού ενδιαφέροντος για ερευνητικά εργαστήρια και εταιρίες λόγω των ιδιαίτερων πλεονεκτημάτων που προσφέρουν όπως η δυναμική δικτυακή τοπολογία, η ανεξαρτησία από σταθερή υποδομή.

Αρχικά γίνεται αναφορά στα βασικά πρωτόκολλα που χρησιμοποιούνται στα δίκτυα MANET το reactive πρωτόκολλο AODV και το proactive πρωτόκολλο OLSR. Στη συνέχεια γίνεται προσπάθεια κατηγοριοποίησης των διαφόρων τύπων επιθέσεων και ανάλυσης του τρόπου που επενεργούν στα διάφορα επίπεδα του δικτύου δίνοντας έμφαση στο Επίπεδο Δικτύου. Οι βασικές κατηγορίες που καταγράφονται είναι οι επιθέσεις ενεργητικού και παθητικού τύπου ανάλογα με το εάν ο σκοπό της επίθεσης είναι η διατάραξη της ομαλής λειτουργίας του δικτύου ή η υποκλοπή και κατασκοπία δεδομένων. Στις επιθέσεις παθητικού τύπου καταγράφεται η επίθεση snooping και Eavesdropping attack, ενώ στις επιθέσεις ενεργητικού τύπου γίνεται ανάλυση σε εσωτερικές και εξωτερικές επιθέσεις ανάλογα με το εάν ο κακόβουλος κόμβος αποτελεί μέρος ή όχι του δικτύου. Οι εσωτερικές επιθέσεις αναλύονται στα διάφορα επίπεδα και παρατίθενται οι πιο σημαντικές επιθέσεις, όπως wormhole attack, black hole attack, byzantine attack, resource consumption attack, routing attacks, session hijacking και repudiation attack.

Όπου είναι δυνατό επισημαίνονται προτάσεις αντιμετώπισης των επιθέσεων και στην τελική ενότητα παρατίθενται τα γενικά συμπεράσματα και προτάσεις για μελλοντική έρευνα. Συνοψίζοντας, διαπιστώνεται η ανάγκη για την εύρεση συνδυασμένων μηχανισμών και τεχνικών ασφάλειας που να αντιμετωπίζουν στο σύνολό τους, τους τύπους επιθέσεων που αναφέρονται, με στόχο τη μέγιστη αξιοπιστία και ενεργειακή αποδοτικότητα των δικτύων MANET.

Χαρακτηριστικά των Κινητών Ad Hoc Δικτύων

Το κινητό ad hoc δίκτυο (MANET) είναι ένα σύνολο κινητών κόμβων που μπορούν να επικοινωνούν μεταξύ τους χωρίς τη χρήση προκαθορισμένης υποδομής ή κεντρικής διαχείρισης (Hoebeke, Moerman, Dhoedt, & P., 2004). Ένα δίκτυο MANET μπορεί να κατασκευαστεί ταχύτατα και με μικρό κόστος λόγω του ότι δε βασίζεται σε υπάρχουσα δικτυακή υποδομή οπότε καθίσταται κατάλληλο για πληθώρα εφαρμογών όπως οι ναυτικές συγκοινωνίες, δίκτυα οχημάτων, καθημερινές συναντήσεις, πανεπιστημιακά δίκτυα κα (Εικόνα 1).

Σε αντίθεση με ένα συμβατικό ενσύρματο δίκτυο, ένα δίκτυο MANET έχει μια δυναμική και συνεχώς μεταβαλλόμενη τοπολογία λόγω της κινητικότητας των κόμβων που συνθέτουν το δίκτυο (S. Ci et al., 2006). Το γεγονός αυτό μαζί με την περιορισμένη χρήση πόρων, δηλαδή το εύρος μετάδοσης και την ισχύ της μπαταρίας, καθιστούν τη διαδικασία δρομολόγησης εξαιρετικά δύσκολη. Αυτός είναι και ο λόγος που η έρευνα σε δίκτυα MANET λαμβάνει ως βασική αρχή τη δημιουργία υπηρεσιών δρομολόγησης με τις ελάχιστες απαιτήσεις εύρους μετάδοσης και ισχύς μπαταρίας.

Σήμερα, υπάρχουν διάφορα αποδοτικά πρωτόκολλα δρομολόγησης για τα δίκτυα MANET, τα οποία μπορούν να κατηγοριοποιηθούν σε δύο κατηγορίες, τα reactive (on-demand) πρωτόκολλα δρομολόγησης και τα proactive (table-driven) πρωτόκολλα δρομολόγησης.

Στα **reactive πρωτόκολλα** δρομολόγησης, όπως το AODV (Ad hoc On Demand Distance Vector) η διαδικασία εύρεσης μιας διαδρομής ενεργοποιείται μόνο όταν είναι απαραίτητο, στην περίπτωση δηλαδή, που ένας κόμβος-αποστολέας θέλει να στείλει πακέτα σε έναν κόμβο-προορισμό για τον οποίο δε γνωρίζει τη διαδρομή (C.Perkins, E.Belding-Royer, and S.Das, 2003).

Στα **proactive πρωτόκολλα** δρομολόγησης, όπως το OLRS (Optimized Link State Routing), κάθε κόμβος συντηρεί έναν ειδικό πίνακα με πληροφορίες δρομολόγησης (routing table) για κάθε κόμβο που ανήκει στο δίκτυο. Οι κόμβοι ανταλλάσουν τακτικά πληροφορίες σχετικά με την τοπολογία του δικτύου με σκοπό την επικαιροποίηση του πίνακα ώστε όταν χρειαστεί να προωθηθεί ένα πακέτο σε κάποιον προορισμό η διαδρομή να είναι γνωστή εκ των προτέρων (Th. Clausen et al., 2003).

Τα περισσότερα πρωτόκολλα δρομολόγησης στα δίκτυα MANET βασίζονται στη συνεργασία μεταξύ των κόμβων λόγω της έλλειψης κεντρικής διαχείρισης και υποθέτουν ότι όλοι οι κόμβοι είναι έμπιστοι και καλόβουλοι. Σε ένα εχθρικό περιβάλλον όμως, ένας

κακόβουλος κόμβος μπορεί να κάνει χρήση του δικτύου με σκοπό είτε τη διαταραχή και διακοπή των υπηρεσιών δρομολόγησης (ενεργητικού τύπου επίθεση) είτε την υποκλοπή και κατασκοπία των δεδομένων (παθητικού τύπου επίθεση) (Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, 2010).

Τα Πρωτόκολλα Δρομολόγησης AODV και OLSR

Σκοπός της διαδικασίας δρομολόγησης σε ένα δίκτυο MANET είναι η εύρεση της σωστής διαδρομής από ένα κόμβο-αποστολέα προς ένα κόμβο-παραλήπτη λαμβάνοντας υπόψη την πιο πρόσφατη τοπολογία σε ένα δίκτυο που συνεχώς βρίσκεται σε μεταβολή. Σε αυτή την ενότητα γίνεται αναφορά σε δύο τυποποιημένα πρωτόκολλα δρομολόγησης που είναι αντικείμενα ενεργής έρευνας το AODV και το OLSR.

Πρωτόκολλο Δρομολόγησης AODV

Το πρωτόκολλο AODV δημιουργήθηκε το 1997 και είναι ένα reactive πρωτόκολλο δρομολόγησης βασισμένο στο πρωτόκολλο DSDV. Όταν ένας κόμβος S θέλει να αποστείλει ένα πακέτο στον κόμβο D και δε γνωρίζει τη διαδρομή, αποστέλλει μαζικά (broadcasting) μια αίτηση δρομολόγησης PREQ σε όλους τους γειτονικούς κόμβους. Ο γειτονικός κόμβος, αποστέλλει και αυτός με τη σειρά του το ίδιο PREQ αίτημα στους δικούς του γειτονικούς κόμβους και η ίδια διαδικασία επαναλαμβάνεται μέχρι το αίτημα να φτάσει στον ζητούμενο κόμβο. Όταν ο κόμβος-προορισμός παραλάβει το αίτημα PREQ αποστέλλει μια απάντηση PREP (unicasting) προς τον αρχικό κόμβο-αποστολέα μέσω της ίδιας διαδρομής που χρησιμοποιήθηκε για να παραλάβει το αίτημα. Τα ίδια αιτήματα που θα παραληφθούν από τον κόμβο-προορισμό θα αγνοηθούν.

Επιπρόσθετα, το πρωτόκολλο AODV επιτρέπει στους ενδιάμεσους κόμβους που έχουν επίκαιρη πληροφορία δρομολόγησης να απαντήσουν οι ίδιοι στο αίτημα με απάντηση PREP προς τον αρχικό κόμβο-αποστολέα. Στο παράδειγμα της εικόνας 3, ο κόμβος S θέλει να επικοινωνήσει με τον κόμβο D. Μια διαδρομή ορίζεται όταν το αίτημα PREQ φτάσει στον κόμβο-προορισμό, και έπειτα ληφθεί η απάντηση PREP πίσω στον κόμβο-αποστολέα. Η διαδρομή καταγράφεται στον πίνακα δρομολόγησης του S.

Πρωτόκολλο Δρομολόγησης OLSR

Στο πρωτόκολλο OLSR βασίζεται στην περιοδική ανταλλαγή πληροφορίας που αφορά την τοπολογία του δικτύου. Η πληροφορία που ανταλλάσσεται περιέχει την IP διεύθυνση κάθε

κόμβου, τον αριθμό ακολουθίας και μια λίστα με τις αποστάσεις από τους γειτονικούς κόμβους. Η βασική ιδέα και βασική διαφορά με το από LSR πρωτόκολλο είναι η χρήση των κόμβων MPR (multi-point relays). Ένας κόμβος MPR επιλέγεται από τους άμεσα γειτονικούς κόμβους (one hop). Το πρωτόκολλο δημιουργηθεί ένα μηχανισμό πλημύρας, προσπαθώντας ελαχιστοποιήσει τον αριθμό των **απαιτούμενων αναμεταδόσεων**, δηλαδή ένα πακέτο δε θα έπρεπε να σταλεί δύο φορές στην ίδια περιοχή δικτύου. Κάθε κόμβος διατηρεί μια λίστα των επιλεγμένων MPR κόμβων του, την οποία κοινοποιεί και στους άμεσους γείτονές του. Κάθε επιλεγμένος MPR κόμβος καταγράφει τους MPR κόμβους. Επίσης το πρωτόκολλο επιτρέπει τη μείωση του **μεγέθους των μηνυμάτων** που ανταλλάσσονται γιατί περιέχει μόνο τους γείτονες που επιλέγουν τον κόμβο ως ένα δικό τους MPR κόμβο. Έτσι, μόνο μέρος της πληροφορίας που αφορά την τοπολογία του δικτύου μεταδίδεται. Ο κόμβος μπορεί να προσεγγιστεί μόνο από τους MPR Selectors. Μόνο οι κόμβοι που επιλέχθηκαν ως MPR έχουν δυνατότητα δημοσίευσης και προώθησης μιας MPR λίστας επιλογής δημοσιευμένης από άλλους MPR κόμβους. Στο παράδειγμα της εικόνας 4, ο κόμβος N2 επέλεξε τους γειτονικούς κόμβους N1 και N6 ως multi-point relays, οι οποίοι θα στείλουν N2-πακέτα. Ο N2 επιλέγει τους κόμβους MPR για να καλύψει τους κόμβους που απέχουν ακριβώς δύο hop από τον ίδιο, δηλαδή τους N7, N8, N9 και N4. Ένας κόμβος που είναι MPR μπορεί να διαβάζει τα πακέτα που στέλνονται από τον κόμβο N2, αλλά δε μπορεί να τα προωθεί.

Σε αντίθεση με τη απλή μέθοδο πλημμύρας όπου κάθε κόμβος προωθεί το μήνυμα σε όλες τις συνδέσεις του, στο πρωτόκολλο OLSR μόνο οι MPR κόμβοι προωθούν τα μηνύματα. Στην εικόνα 2 δίνεται σχηματικό παράδειγμα της απλής μεθόδου πλημμύρας σε σχέση με την MPR προώθηση.

Κάθε κόμβος, όταν συγκεντρώσει την απαιτούμενη πληροφορία της τοπολογίας του δικτύου συντηρεί έναν πίνακα δρομολόγησης προς κάθε άλλο κόμβο του δικτύου. Ο πίνακας αυτό χρησιμοποιείται μαζί με έναν κατάλληλο αλγόριθμο για την εύρεση της ελάχιστης διαδρομής προσέγγισης ενός άλλου κόμβου.

Μηνύματα Δρομολόγησης στο Πρωτόκολλο OLSR. – Γενικά, στο πρωτόκολλο OLSR χρησιμοποιούνται δύο τύποι μηνυμάτων, το μήνυμα HELLO και το μήνυμα ελέγχου τοπολογίας (topology control message, TC). Το μήνυμα HELLO χρησιμοποιείται για την επιλογή MPR κόμβων και περιέχει τη διεύθυνση του κόμβου και τη λίστα με τους 1-hop γείτονες. Ανταλλάσσοντας μηνύματα HELLO κάθε κόμβος μπορεί να ενημερωθεί για την τοπολογία του δικτύου έως 2 hops. Τα μηνύματα HELLO ανταλλάσσονται τοπικά από γειτονικούς κόμβους και δεν προωθούνται περαιτέρω σε άλλους κόμβους. Το μήνυμα TC χρησιμοποιείται για τον υπολογισμό της διαδρομής. Στο πρωτόκολλο OLSR κάθε MPR κόμβος στέλνει μηνύματα TC περιοδικά.

Η επιλογή των MPR. Ο κάθε κόμβος επιλέγει ένα σετ MPR κόμβων στα οποία προωθεί τα μηνύματα δρομολόγησης. Στο πρωτόκολλο OLSR, ένας κόμβος επιλέγει τους MPR κόμβους έτσι ώστε να μπορεί να προσεγγίζει όλους του κόμβους που βρίσκονται σε 2-hops απόσταση. Σε περίπτωση που υπάρχουν διάφορες επιλογές, επιλέγεται το ελάχιστο σετ κόμβων.

Επιθέσεις εναντίον των δικτύων MANET

Σε αντίθεση με το παρελθόν όπου οι περισσότερες προσπάθειες εστίαζαν στην παροχή προληπτικών μέτρων για την προστασία του πρωτοκόλλου δρομολόγησης στα δίκτυα MANET, σήμερα υπάρχει διαφορετική προσέγγιση στις προσπάθειες έρευνας για την αντιμετώπιση τέτοιων κακόβουλων επιθέσεων. Οι περισσότερες τεχνικές είναι βασισμένες στη διαχείριση κλειδιού (key management) ή σε τεχνικές κωδικοποίησης για να αποτρέψουν μη εξουσιοδοτημένους κόμβους να συνδεθούν στο δίκτυο (Boundpadith Kannhavong et al., 2007). Γενικά, το κύριο μειονέκτημα αυτών των προσεγγίσεων είναι ότι επιβαρύνουν με κυκλοφοριακό φορτίο απαραίτητο για την ανταλλαγή και επαλήθευση των κλειδιών, κάτι που κοστίζει πολύ σε εύρος σε MANET κόμβους με περιορισμένη ισχύ μπαταρίας και περιορισμένες υπολογιστικές δυνατότητες (Y-C Hu and A. Perrig, 2005).

Οι επιθέσεις σε δίκτυα MANET ενδέχεται να εμφανιστούν σε όλα τα επίπεδα, από το επίπεδο εφαρμογών έως και το φυσικό επίπεδο (Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, 2006).

Στον Πίνακα 1 παρατίθενται συνοπτικά διαφορετικοί τύποι επιθέσεων ανά επίπεδο. Οι επιθέσεις σε MANET δίκτυα μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες, τις

επιθέσεις ενεργητικού χαρακτήρα (active attacks) και τις επιθέσεις παθητικού χαρακτήρα (passive attacks).

Επιθέσεις Παθητικού Χαρακτήρα (Passive Attacks)

Οι επιθέσεις παθητικού χαρακτήρα δεν έχουν σκοπό την διατάραξη της ομαλής λειτουργίας του δικτύου αλλά την κατασκοπία των δεδομένων που ανταλλάσσονται μέσω του δικτύου. Σε αυτή την κατηγορία μπορεί να γίνει παραβίαση της αρχής της εμπιστευτικότητας (confidentiality) εφόσον ένας κακόβουλος κόμβος μπορέσει να ερμηνεύσει τα δεδομένα που συγκεντρώνει από το δίκτυο. Ο εντοπισμός των επιθέσεων αυτού του τύπου είναι εξαιρετικά δύσκολος γιατί η ίδια η λειτουργία του δικτύου δε διαταράσσεται. Από τους καλύτερους τρόπος προστασίας από τέτοιες επιθέσεις αποτελεί η χρήση ισχυρών μηχανισμών κρυπτογράφησης των δεδομένων που μεταδίδονται, ώστε να καθίσταται αδύνατη η απόσπαση χρήσιμης πληροφορίας. Τύποι επίθεσης που ανήκουν στη συγκεκριμένη κατηγορία είναι η επίθεση snooping και η επίθεση eavesdropping.

Επίθεση Snooping

Η επίθεση Snooping συνίσταται στην μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Στη γενική της μορφή αυτού του τύπου η επίθεση δεν περιορίζεται μόνο στην προσπάθεια πρόσβασης σε δεδομένα κατά τη διάρκεια της μετάδοσης αλλά έχει χαρακτήρα παρακολούθησης των επιτελούμενων ενεργειών και δραστηριοτήτων που λαμβάνουν χώρα σε ένα κόμβο δικτύου. Για παράδειγμα κακόβουλοι χρήστες συχνά χρησιμοποιούν τεχνικές snooping για την παρακολούθηση δεδομένων που εισάγονται κατά την πληκτρολόγηση των passwords, κατά τη μετάδοση ευαίσθητων δεδομένων, αλλά και μεγάλες εταιρίες χρησιμοποιούν τέτοιες τεχνικές για την νόμιμη παρακολούθηση της χρήσης των παρεχόμενων υπολογιστικών πόρων και του διαδικτύου.

Επίθεση Eavesdropping

Η επίθεση eavesdropping συνίσταται στην υποκλοπή μηνυμάτων και συναλλαγών από μη εξουσιοδοτημένους χρήστες. Στα δίκτυα MANET οι κόμβοι επικοινωνούν ασύρματα (RF spectrum) μέσω broadcasting οπότε είναι εύκολη η παρεμβολή από συντονισμένους δέκτες. Η υποκλοπή των δεδομένων από το δίκτυο είναι δυνατή όπως επίσης και η εισαγωγή μη νόμιμων δεδομένων στο δίκτυο. Προβλήματα μπορεί ακόμη να δημιουργηθούν ακόμη και από την ισχυρή

ισχύ εκπομπής ενός κακόβουλου κόμβου όπου το σήμα μπορεί να αλλοιώσει τα σήματα-στόχο με αποτέλεσμα τη διακοπή των επικοινωνιών. Γνωστές τεχνικές παρεμβολής σήματος είναι η τυχαίος (random noise) και παλμικός (pulse) θόρυβος.

Επιθέσεις Ενεργητικού Χαρακτήρα (Active Attacks)

Οι επιθέσεις ενεργητικού χαρακτήρα έχουν σκοπό την αλλοίωση και την καταστροφή των δεδομένων που ανταλλάσσονται στο δίκτυο ώστε να διαταραχθεί η ομαλή λειτουργία του δικτύου. Οι επιθέσεις αυτής της κατηγορίας μπορούν να αναλυθούν σε δύο υποκατηγορίες, τις **εξωτερικές επιθέσεις** (active external attacks) και τις **εσωτερικές επιθέσεις** (active internal attacks). Οι εξωτερικές επιθέσεις πραγματοποιούνται από κόμβους που δεν ανήκουν στο δίκτυο. Επιθέσεις αυτού του τύπου μπορούν να αντιμετωπιστούν με τη χρήση συμβατικών τεχνικών ασφάλειας όπως τεχνικές κρυπτογράφησης και χρήση τείχους προστασίας. Οι εσωτερικές επιθέσεις πραγματοποιούνται από κόμβους που αποτελούν ήδη μέρος του δικτύου. Επειδή οι κακόβουλοι κόμβοι είναι ήδη εξουσιοδοτημένοι χρήστες του δικτύου, οι εσωτερικές επιθέσεις είναι σοβαρότερες και δυσκολότερο να εντοπιστούν σε σχέση με τις εξωτερικές επιθέσεις. Στη συνέχεια ακολουθεί σύντομη περιγραφή των σημαντικότερων επιθέσεων ενεργητικού χαρακτήρα στα πιο σημαντικά επίπεδα του δικτύου.

Επίθεση Wormhole Attack

Η επίθεση wormhole attack είναι μια από τις πιο εξελιγμένες και επικίνδυνες επιθέσεις σε δίκτυα MANET σε Επίπεδο Δικτύου (Network Layer). Σε αυτή την επίθεση ζεύγος κακόβουλων κόμβων συνωμοτεί και καταγράφει πακέτα τα οποία και προωθεί χρησιμοποιώντας ένα δίκτυο υψηλής ταχύτητας. Ο πρώτος κόμβος καταγράφει τα αιτήματα PREQ και τα μεταβιβάζει αυτούσια στον άλλο. Λόγω της υψηλής ταχύτητας μετάδοσης ο προορισμός προσεγγίζεται πρώτος, οπότε και επιλέγει εσφαλμένα τη διαδρομή που περιέχει το ζεύγος των κακόβουλων κόμβων. Η σοβαρότητα της επίθεσης έγκειται στο γεγονός ότι μπορεί να χρησιμοποιηθεί εναντίον όλων των επικοινωνιών που παρέχουν αυθεντικοποίηση (authenticity) και εμπιστευτικότητα (confidentiality). Στην Εικόνα 5 παρατίθεται παράδειγμα επίθεσης σε reactive πρωτόκολλο δρομολόγησης. Οι A1 και A2 είναι οι κακόβουλοι κόμβοι, ενώ ο S είναι ο στόχος της επίθεσης. Ο S αποστέλλει μαζικά (broadcast) ένα PREQ αίτημα για να εντοπίσει τον προορισμό D. Οι γειτονικοί του κόμβοι J και K αναμεταδίδουν το PREQ αίτημα, σύμφωνα με το πρωτόκολλο. Ο A1 όμως που λαμβάνει το αίτημα από τον J, το καταγράφει και το προωθεί αυτούσιο στον A2, και ο A2 με τη σειρά του στον P. Δεδομένης της υψηλής ταχύτητα

μετάδοσης, το αίτημα PREQ θα φτάσει πρώτο στον προορισμό D. Συνεπώς ο προορισμός D θα επιλέξει τη διαδρομή D-P-J-S για να απαντήσει (unicast) με ένα PREP μήνυμα στον κόμβο-αποστολέα S, αγνοώντας όλα τα αιτήματα PREQ που θα φτάσουν αργότερα. Τελικά, ο κόμβος-αποστολέας S θα επιλέξει τη διαδρομή δρομολόγησης S-J-P-D για τη μετάδοση των δεδομένων που περνά όμως και από τους κακόβουλους κόμβους A1 και A2.

Επίθεση Blackhole Attack

Αυτός ο τύπος επίθεσης επιδρά σε Επίπεδο Δικτύου (Network Layer). Σε μια επίθεση blachkhole attack , ένας κακόβουλος κόμβος στέλνει ψεύτικη πληροφορία δρομολόγησης ισχυριζόμενος ότι κατέχει τη βέλτιστη διαδρομή, προκαλώντας έτσι τη δρομολόγηση των πακέτων μέσω αυτού. Για παράδειγμα, στο πρωτόκολλο AODV, ο κακόβουλος κόμβος στέλνει ψεύτικα PREP μηνύματα (περιλαμβάνοντας έναν ψεύτικο αριθμό ακολουθίας ίσο ή μεγαλύτερο από αυτόν που περιέχεται στο PREQ) προς τον κόμβο-πηγή, ισχυριζόμενος ότι έχει την πιο πρόσφατη διαδρομή προς τον κόμβο-προορισμό. Σαν συνέπεια, ο κόμβος πηγής επιλέγει την προτεινόμενη διαδρομή, η οποία όμως περιλαμβάνει και τον κακόβουλο κόμβο. Όλη η κυκλοφορία περνά λοιπόν και από τον κακόβουλο κόμβο, ο οποίος είναι πια σε θέση να τη μεταχειριστεί όπως θέλει ή να την απορρίψει εντελώς. Στο παράδειγμα της εικόνας 6 ο κακόβουλος κόμβος A στέλνει ένα ψεύτικο PREP μήνυμα στον κόμβο πηγής S, ισχυριζόμενος ότι έχει την πιο πρόσφατη διαδρομή προς τον προορισμό σε σχέση με τους άλλους κόμβους.

Επίθεση Link Withholding Attack.

Σε αυτή τη σοβαρή μορφή επίθεσης που επιδρά σε Επίπεδο Δικτύου (Network Layer), ο κακόβουλος κόμβος δεν κοινοποιεί τη σύνδεση συγκεκριμένων κόμβων ή ομάδας κόμβων, οπότε προκύπτει αδυναμία σύνδεσης με αυτούς τους κόμβους.

Επίθεση Link Spoofing Attack.

Σε μια επίθεση link spoofing attack η οποία επιδρά σε Επίπεδο Δικτύου (Network Layer), ένας κακόβουλος κόμβος κοινοποιεί ψεύτικες συνδέσεις με μη υπάρχοντες γειτονικούς κόμβους για να διασπάσει τη διαδικασία δρομολόγησης. Για παράδειγμα, στο πρωτόκολλο OLSR, μπορεί να κοινοποιήσει ένα ψεύτικο σύνδεσμο προς έναν 2-hop γείτονα. Σαν συνέπεια, επιλέγεται ως MPR κόμβος και στη συνέχεια είναι πλέον σε θέση να χειριστεί τα δεδομένα, να αλλάξει ή να απορρίψει την κυκλοφορία ή να εφαρμόσει άλλα είδη denial-of-service επιθέσεων. Στο παράδειγμα της εικόνας 7 ο A είναι ο κακόβουλος κόμβος και στόχος ο κόμβος T. Πριν την επίθεση, οι κόμβοι A και B είναι οι MPRs του T. Ο A επιτίθεται κοινοποιώντας στον T την

ψεύτικη σύνδεση με τον 2-hop D γείτονα του T. Ο B δεν είναι πλέον απαραίτητος MPR κόμβος για τον T, αφού μπορεί να προσεγγίσει πλέον και τους δύο 2-hop κόμβους D και C μέσω του κακόβουλου κόμβου A.

Επίθεση Replay Attack.

Η επίθεση replay attack εκμεταλλεύεται το γεγονός ότι η τοπολογία του δικτύου MANET μεταβάλλεται συνεχώς λόγω της κινητικότητας των κόμβων του και επιδρά σε Επίπεδο Δικτύου (Network Layer). Ένας κακόβουλος κόμβος καταγράφει έγκυρα μηνύματα ελέγχου άλλων κόμβων με σκοπό να τα αναμεταδώσει αργότερα. Έτσι, προκαλεί την ενημέρωση των πινάκων δρομολόγησης των άλλων κόμβων με παρωχημένη πληροφορία. Η επίθεση replay attack χρησιμοποιείται για impersonation ενός συγκεκριμένου κόμβου ή για τη διατάραξη της διαδικασίας δρομολόγησης σε ένα δίκτυο MANET.

Επίθεση Byzantine Attack

Αυτός ο τύπος επίθεσης επιδρά σε Επίπεδο Δικτύου (Network Layer). Σε αυτόν τον τύπο επιθέσεων ένας ή σύνολο κακόβουλων κόμβων συνεργάζονται για να επιτελέσουν ενέργειες με σκοπό την διατάραξη και υποβάθμιση των υπηρεσιών δρομολόγησης. Για παράδειγμα γίνεται προσπάθεια να δημιουργήσουν ατέρμονους βρόχους δρομολόγησης, να δρομολογήσουν πακέτα μέσω μη βέλτιστων διαδρομών, ή να καταστρέψουν επιλεκτικά πακέτα. Ο εντοπισμός της συγκεκριμένης επίθεσης από τους ίδιους τους κόμβους είναι εξαιρετικά δύσκολος γιατί από τη δική τους οπτική το δίκτυο φέρεται να λειτουργεί κανονικά, ενώ στην πραγματικότητα η συνολική απόδοση του δικτύου να υποβαθμίζεται λόγω της συγκεκριμένης επίθεσης.

Επιθέσεις Resource Consumption και Flooding Attack

Ο σκοπός των συγκεκριμένων επιθέσεων είναι η εξάντληση των πόρων του δικτύου και επιδρά σε Επίπεδο Δικτύου (Network Layer). Οι σημαντικότεροι πόροι που βρίσκονται στο στόχαστρο και αποτελούν και την αχίλλειο πτέρνα των δικτύων MANET είναι το εύρος μετάδοσης, η υπολογιστική ισχύς και η ισχύς της μπαταρίας, εμποδίζοντας τελικά τη διαδικασία δρομολόγησης και προκαλώντας σοβαρή υποβάθμιση στην απόδοση του δικτύου. Για παράδειγμα, στο AODV πρωτόκολλο, ένας κακόβουλος κόμβος μπορεί να αποστείλει μεγάλο αριθμό PREQ αιτημάτων σε μικρό χρονικό διάστημα προς ένα μη υπαρκτό κόμβο. Επειδή κανένας κόμβος δε θα απαντήσει, τα αιτήματα PREQ θα πλημυρίσουν όλο το δίκτυο. Ως συνέπεια, η ισχύς των μπαταριών των κόμβων αναλώνεται, όπως και το εύρος μετάδοσης

οδηγώντας έτσι σε denial of service και sleep deprivation. Η συγκεκριμένη επίθεση μπορεί να υποβαθμίσει την απόδοση του συστήματος έως και 84%.

Επιθέσεις Δρομολόγησης (Routing Attacks)

Υπάρχει μεγάλη ποικιλία σε επιθέσεις αυτού του τύπου και επιδρούν σε Επίπεδο Δικτύου (Network Layer). Οι σημαντικότερες παρατίθενται στη συνέχεια.

***Routing Table Overflow*:** σε αυτόν τον τύπο επίθεσης ο κακόβουλος κόμβος δημιουργεί πληθώρα διαδρομών προς μη υπάρχοντες κόμβους. Τελικός σκοπός είναι να δημιουργηθεί μεγάλο πλήθος τέτοιων διαδρομών ώστε να εμποδίζεται η δημιουργία νέων ή να συντριβεί εντελώς η λειτουργία του πρωτοκόλλου δρομολόγησης. Στα proactive πρωτόκολλα η διαδρομή αναζητείται πριν χρειαστεί ενώ στα reactive πρωτόκολλα η διαδρομή αναζητείται μόνο όταν χρειάζεται. Στόχος λοιπόν της επίθεσης είναι η υπερχείλιση των πινάκων δρομολόγησης ώστε στη συνέχεια να εμποδίζεται η δημιουργία νέων καταχωρήσεων που αντιστοιχούν σε νέες διαδρομές προς εξουσιοδοτημένους κόμβους.

***Packet replication*:** σε αυτόν τον τύπο επίθεσης ο κακόβουλος κόμβος αναπαράγει πακέτα τα οποία είναι παρωχημένα καταναλώνοντας εύρος δικτύου και ισχύ μπαταρίας, καθώς και γενικότερη σύγχυση στο δίκτυο.

Rushing attack: σε αυτόν τον τύπο επίθεσης είναι ευάλωτα τα on demand πρωτόκολλα δρομολόγησης που κάνουν χρήση απόρριψης διπλοτύπων κατά τη διαδικασία εύρεσης διαδρομής. Η βασική ιδέα είναι ότι ο κακόβουλος κόμβος που λαμβάνει μια αίτηση από κάποιον κόμβο πηγή προσπαθεί να απαντήσει την αίτηση προτού απαντήσουν οι υπόλοιποι κόμβοι. Οι νόμιμες απαντήσεις που φθάνουν αργότερα θεωρούνται διπλότυπα που έχουν ήδη ληφθεί (από τον κακόβουλο κόμβο) και απορρίπτονται. Ως συνέπεια η διαδρομή που λαμβάνει ο κόμβος πηγή εμπεριέχει και τον κακόβουλο κόμβο.

Επίθεση Session hijacking

Η επίθεση Session Hijacking είναι εξαιρετικά επικίνδυνη και δίνει τη δυνατότητα στον κακόβουλο κόμβο να έχει τη συμπεριφορά ενός νόμιμου συστήματος εκμεταλλευόμενος το γεγονός ότι γενικότερα όλες οι επικοινωνίες πιστοποιούνται μόνο στην εκκίνηση της διαδικασίας συνόδου (session). Επιδρά σε Επίπεδο Μεταφοράς (Transport Layer) και ο κακόβουλος κόμβος επιτίθεται αρχικά στον κόμβο στόχο μέσω IP address spoofing και DoS

καθιστώντας τον μη διαθέσιμο για κάποιο χρονικό διάστημα. Στην συνέχεια παίρνει τη θέση του κόμβου στόχου διατηρώντας τη συνεδρία με τα άλλα συστήματα ενεργή.

Repudiation

Η μη αποποίηση ευθύνης αναφέρεται στο γεγονός ότι ένας κόμβος που συμμετέχει σε μια διαδικασία δεν μπορεί να αρνηθεί ότι πήρε μέρος στη διαδικασία. Η μη αποποίηση ευθύνης είναι μια από τις σημαντικότερες προϋποθέσεις των πρωτοκόλλων ασφάλειας. Η συγκεκριμένη επίθεση επιδρά στο επίπεδο εφαρμογών (Application Layer).

Συμπεράσματα και Προτάσεις για Μελλοντική Έρευνα

Στην παρούσα εργασία μελετήθηκαν θέματα που σχετίζονται με τις επιθέσεις σε Mobile Ad Hoc (MANET) δίκτυα με ιδιαίτερη έμφαση στις επιθέσεις που αναφέρονται στο Επίπεδο Δικτύου (Network Layer).

Αρχικά αναλύθηκαν τα βασικά πρωτόκολλα που χρησιμοποιούνται στα δίκτυα MANET το reactive πρωτόκολλο AODV και το proactive πρωτόκολλο OLSR. Στη συνέχεια έγινε κατηγοριοποίηση των διαφόρων τύπων επιθέσεων σε ενεργητικού και παθητικού τύπου ανάλογα με το εάν ο σκοπός της επίθεσης είναι η διατάραξη της ομαλής λειτουργίας του δικτύου ή η υποκλοπή και κατασκοπία δεδομένων. Οι επιθέσεις ενεργητικού τύπου αναλυθήκαν περαιτέρω σε εσωτερικές και εξωτερικές επιθέσεις ανάλογα με το εάν ο κακόβουλος κόμβος αποτελεί μέρος ή όχι του δικτύου και τέλος έγινε παράθεση των σημαντικότερων επιθέσεων στα διάφορα επίπεδα επισημαίνοντας τα ιδιαίτερα χαρακτηριστικά τους.

Όπως διαπιστώνεται, οι επιθέσεις στα δίκτυα MANET μπορεί να εκδηλωθούν σε όλα τα επίπεδα, από το Φυσικό Επίπεδο έως και το Επίπεδο Εφαρμογών με βασικούς στόχους των επιθέσεων είτε τη εξάντληση των πόρων του δικτύου και την υποβάθμιση της απόδοσης και των παρεχόμενων υπηρεσιών, είτε την υποκλοπή και κατασκοπία των δεδομένων. Επίσης, οι περισσότερες τεχνικές ασφάλειας είναι βασισμένες στη διαχείριση κλειδιού (key management) ή σε τεχνικές κωδικοποίησης με κύριο μειονέκτημα την επιβάρυνση με κυκλοφοριακό φορτίο, απαραίτητο για την ανταλλαγή και επαλήθευση των κλειδιών, κάτι που κοστίζει πολύ σε εύρος σε MANET κόμβους με περιορισμένη ισχύ μπαταρίας και περιορισμένες υπολογιστικές δυνατότητες.

Σαν μελλοντική έρευνα διαπιστώνεται η ανάγκη για την εύρεση συνδυασμένων μηχανισμών και τεχνικών ασφάλειας που να αντιμετωπίζουν στο σύνολό τους, τους τύπους επιθέσεων που αναφέρονται, με στόχο τη μέγιστη αξιοπιστία και την ενεργειακή αποδοτικότητα των δικτύων MANET.

Ειδικότερα, μια προσέγγιση θα μπορούσε να εστιάσει στην ελαχιστοποίηση της χρήσης public key κρυπτογράφησης κάνοντας χρήση υβριδικών τεχνικών κρυπτογράφησης. Για παράδειγμα, μετάδοση κλειδιού κρυπτογράφησης με ECC Public Key αλγορίθμους επιτυγχάνοντας μεγάλη ασφάλεια με μικρό μήκος κλειδιού (αποφεύγοντας την υπερφόρτωση του δικτύου) και στη συνέχεια χρήση του κλειδιού για shared key κρυπτογράφηση.

Επίσης, η ανάπτυξη εύρωστων τεχνικών και επεκτάσεων των υπαρχόντων πρωτοκόλλων θα πρέπει να συνδυάζεται με χρήση NS-2 εξομοιώσεων, εφαρμόζοντας καταστάσεις του πραγματικού κόσμου δεδομένων των ιδιαιτεροτήτων και περιορισμών των δικτύων MANET.

Σε κάθε περίπτωση, η παροχή υψηλού επιπέδου ασφάλειας σε ένα δίκτυο MANET αποτελεί μια ιδιαίτερη πρόκληση σε σχέση με ένα συμβατικό δίκτυο, και πέρα από τα όποια πλεονεκτήματα των συγκεκριμένων δικτύων, η ευδοκίμησή τους θα εξαρτηθεί σε μεγάλο βαθμό από την εμπιστοσύνη των χρηστών σε θέματα που αφορούν στην ασφάλειά τους.

Βιβλιογραφία

Nishu Garg, Mahapatra R.P. (2009). MANET Security Issues. *IJCSNS International Journal of Computer Science and Network Security, 9*, 241-246. Retrieved from http://paper.ijcsns.org/07_book/200908/20090834.pdf

Hoang Lan Nguyen, Uyen Trang Nguyen. (2008) A study of different types of attacks on multicast in mobile ad hoc networks, *Journal of Ad-Hoc Networks, 6,* 32-46. DOI:10.1016/j.adhoc.2006.07.005

Kargl F., Geiß A., Schlott S., Weber M. (2005) Secure Dynamic Source Routing. *System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference*. DOI: 10.1109/HICSS.2005.531

Jihye Kim, Tsudik Gene. (2009) SRDP: Secure route discovery for dynamic source routing in MANETs, *Journal of Ad-Hoc Networks, 7*, 1097-1109. DOI:10.1016/j.adhoc.2008.09.007

David B. Johnson and David Maltz A. (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. Retrieved from http://www.cs.cornell.edu/people/egs/615/johnson-dsr.pdf

Perkins, C.E. and Royer, E.M. (1999) Ad-hoc on-demand distance vector routing. *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, 90-100. DOI: 10.1109/MCSA.1999.749281

Awerbuch, B. and Holmer, D. and Nita-Rotaru, C. and Rubens, H. (2002) An on-demand secure routing protocol resilient to byzantine failures. *Proceedings of the 1st ACM workshop on Wireless security*, 21-30. DOI:10.1145/570681.570684

Hu, Y.C. and Perrig, A. and Johnson, D.B. (2003) Rushing attacks and defense in wireless ad hoc network routing protocols. *Proceedings of the 2nd ACM workshop on Wireless security*, 30-40. DOI:10.1145/941311.941317

Hoebeke, J. and Moerman, I. and Dhoedt, B. and Demeester, P. (2004) An overview of mobile ad hoc networks: applications and challenges. *JOURNAL-COMMUNICATIONS NETWORK*, *3*, 60-66. Retrieved from http://www-di.inf.puc-rio.br/~endler/courses/Mobile/papers/MANET-Challenges.pdf

Perkins, C.E. Royer, E.M. (1999) Ad-hoc on-demand distance vector, *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, DOI:10.1109/MCSA.1999.749281

Jacquet P., Muhlethaler P., Clausen T., Laouiti A., Qayyum A., Viennot L. (2001) Optimized link state routing protocol for ad hoc networks, *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*, DOI: 10.1109/INMIC.2001.995315

Rai, A.K. and Tewari, R.R. and Upadhyay, S.K. (2010) Different Types of Attacks on Integrated MANET-Internet Communication, *International Journal of Computer Science and Security (IJCSS)*, *4*, 265-274. Retrieved from http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume4/Issue3/IJCSS-292.pdf

Kannhavong, B. and Nakayama, H. and Nemoto, Y. and Kato, N. and Jamalipour, A. (2007) A survey of routing attacks in mobile ad hoc networks, *Wireless Communications, IEEE, 14*, 85-91. DOI: 10.1109/MWC.2007.4396947

Wu, B. and Chen, J. and Wu, J. and Cardei, M. (2007) A survey of attacks and countermeasures in mobile ad hoc networks, *Wireless Network Security*, 103-135. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.8143&rep=rep1&type=pdf

Peng Ning, KunSun (2005) How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols, *Journal of Ad-Hoc Networks, 3.* DOI: 10.1016/j.adhoc.2004.04.001

Verbree, Jan-Maarten, de Graaf, Maurits and Hurink, Johann (2010) An analysis of the lifetime of OLSR networks, *Journal of Ad-Hoc Networks, 8.* DOI: 10.1016/j.adhoc.2009.09.003

Mohammad Al-Shurman, Seong-Moo Yoo,Seungjin Park (2004) Black hole attack in mobile Ad Hoc networks, *ACM-SE 42 Proceedings of the 42nd annual Southeast regional conference*. DOI: 10.1145/986537.986560

Optimized Link State Routing Protocol. (n.d.) Retrieved February 6, 2012 from Wikipedia: http://en.wikipedia.org/wiki/Optimized_Link_State_Routing_Protocol

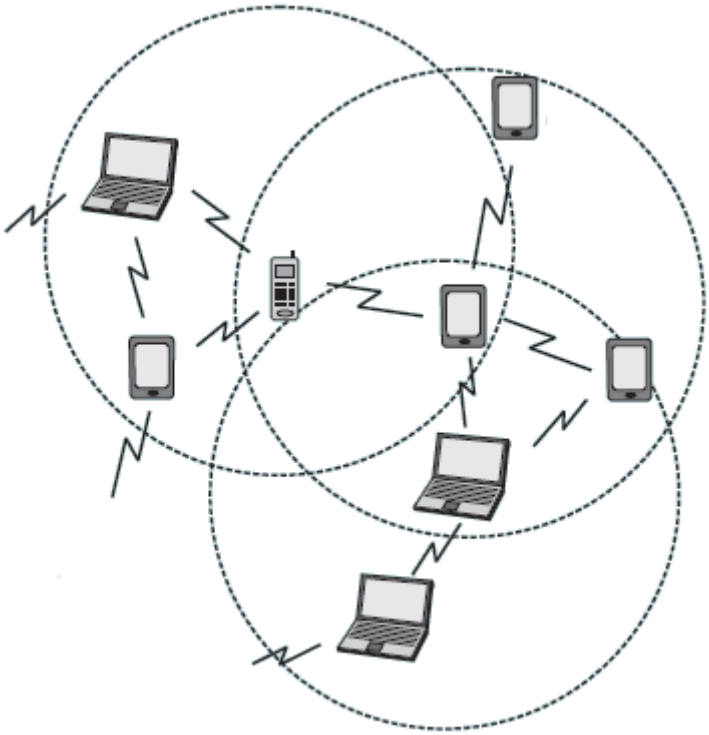
Ad hoc On-Demand Distance Vector Routing. (n.d.) Retrieved February 6, 2012 from Wikipedia: http://en.wikipedia.org/wiki/AODV

Mobile ad hoc network. (n.d.) Retrieved February 6, 2012 from Wikipedia: http://en.wikipedia.org/wiki/MANET

Πίνακας 1

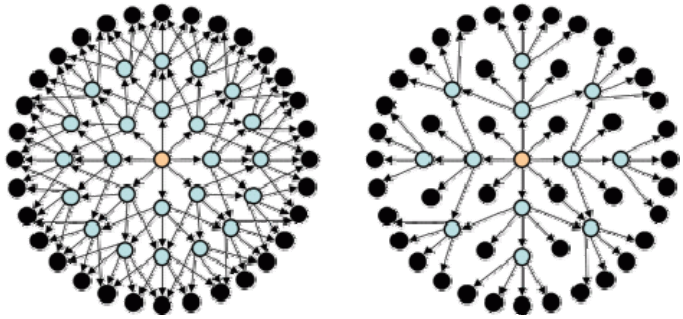
Συνοπτικός πίνακας επιθέσεων σε δίκτυα MANET, από το Φυσικό μέχρι το Επίπεδο Εφαρμογών

Επίπεδο	**Επίθεση**
Application layer	Repudiation,
	Data corruption
Transport layer	Session hijacking,
	SYN flooding
Network layer	Wormhole, Blackhole, Byzantine, Flooding, Resource consumption,
	Location disclosure attacks
Data link layer	Traffic analysis,
	Monitoring,
	Disruption MAC (802.11),
	WEP weakness
Physical layer	Jamming,
	Interceptions,
	Eavesdropping
Multi-layer attacks	DoS, impersonation,
	Replay,
	Man-in-the-middle



Εικόνα 1 Mobile Ad Hoc Network

(Hoebeke, J. and Moerman, I. and Dhoedt, B. and Demeester, P., 2004)



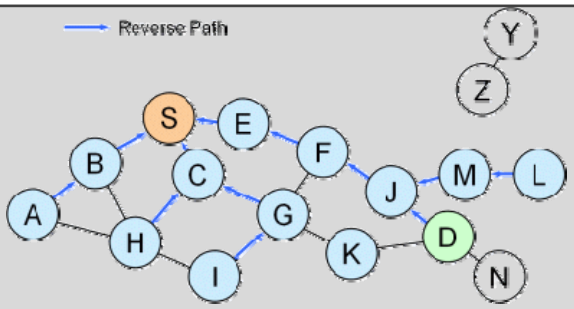
Εικόνα 2 Η απλή μέθοδος πλημμύρας (στα αριστερά)

σε αντίθεση με την MPR προώθηση (στα δεξιά)

(Traditional vs. optimized flooding with MPRs (2007) Retrieved from

http://geodes.ict.tuwien.ac.at/PowerSavingHandbook/D3.5.html)

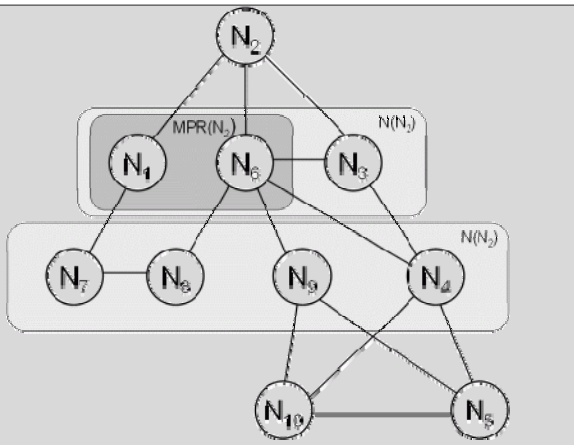
Στο παράδειγμα της εικόνας ο κόμβος S θέλει να επικοινωνήσει με τον κόμβο D. Μια διαδρομή ορίζεται όταν το αίτημα PREQ φτάσει στον κόμβο-προορισμό, και έπειτα ληφθεί η απάντηση PREP πίσω στον κόμβο-αποστολέα. Η διαδρομή καταγράφεται στον πίνακα δρομολόγησης του S.



(Bounpadith Kannhavong et al., 2007)

Εικόνα 3 Παράδειγμα εύρεσης διαδρομής στο πρωτόκολλο AODV

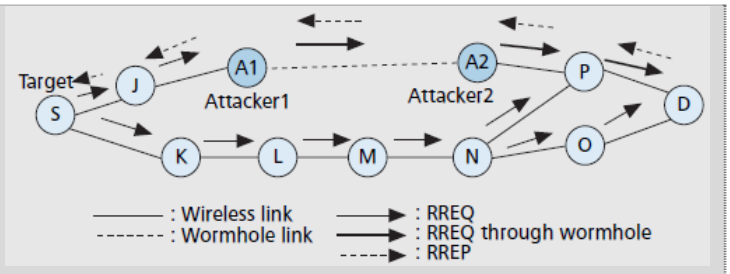
Στο παράδειγμα της εικόνας ο κόμβος N2 επέλεξε τους γειτονικούς κόμβους N1 και N6 ως multi-point relays, οι οποίοι θα στείλουν N2-πακέτα. Ο N2 επιλέγει τους κόμβους MPR για να καλύψει τους κόμβους που απέχουν ακριβώς δύο hop από τον ίδιο, δηλαδή τους N7, N8, N9 και N4. Ένας κόμβος που είναι MPR μπορεί να διαβάζει τα πακέτα που στέλνονται από τον κόμβο N2, αλλά δε μπορεί να τα προωθεί.



(Bounpadith Kannhavong et al., 2007)

Εικόνα 4 Παράδειγμα εύρεσης διαδρομής στο πρωτόκολλο OLSR

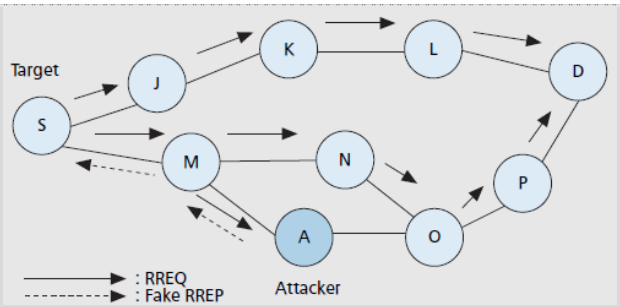
Στην εικόνα παρατίθεται παράδειγμα επίθεσης σε reactive πρωτόκολλο δρομολόγησης. Οι A1 και A2 είναι οι κακόβουλοι κόμβοι, ενώ ο S είναι ο στόχος της επίθεσης. Ο S αποστέλλει μαζικά (broadcast) ένα PREQ αίτημα για να εντοπίσει τον προορισμό D.



(Bounpadith Kannhavong et al., 2007)

Εικόνα 5 Παράδειγμα επίθεσης τύπου Wormhole Attack

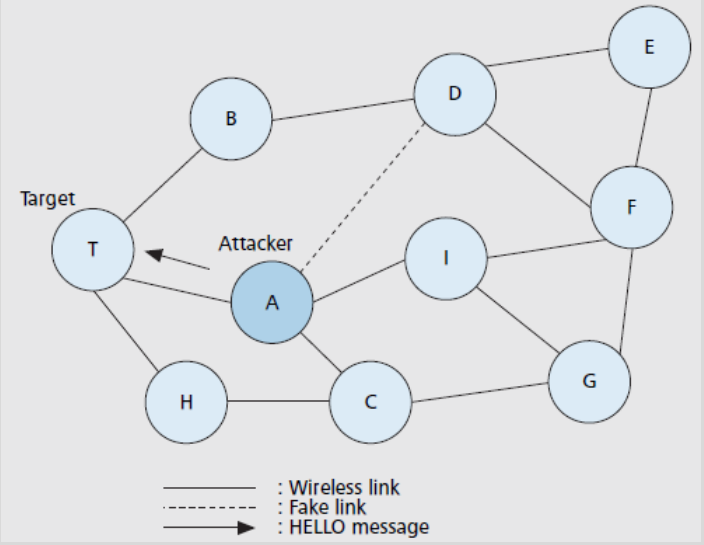
Στο παράδειγμα της εικόνας ο κακόβουλος κόμβος A στέλνει ένα ψεύτικο PREP μήνυμα στον κόμβο πηγής S, ισχυριζόμενος ότι έχει την πιο πρόσφατη διαδρομή προς τον προορισμό σε σχέση με τους άλλους κόμβους.



(Bounpadith Kannhavong et al., 2007)

Εικόνα 6 Παράδειγμα επίθεσης τύπου Blackhole Attack

Στο παράδειγμα της εικόνας ο A είναι ο κακόβουλος κόμβος και στόχος ο κόμβος T. Πριν την επίθεση, οι κόμβοι A και B είναι οι MPRs του T. Ο A επιτίθεται κοινοποιώντας στον T την ψεύτικη σύνδεση με τον 2-hop D γείτονα του T. Ο B δεν είναι πλέον απαραίτητος MPR κόμβος για τον T, αφού μπορεί να προσεγγίσει πλέον και τους δύο 2-hop κόμβους D και C μέσω του κακόβουλου κόμβου A.



(Bounpadith Kannhavong et al., 2007)

Εικόνα 7 Παράδειγμα επίθεσης Link Spoofing Attack