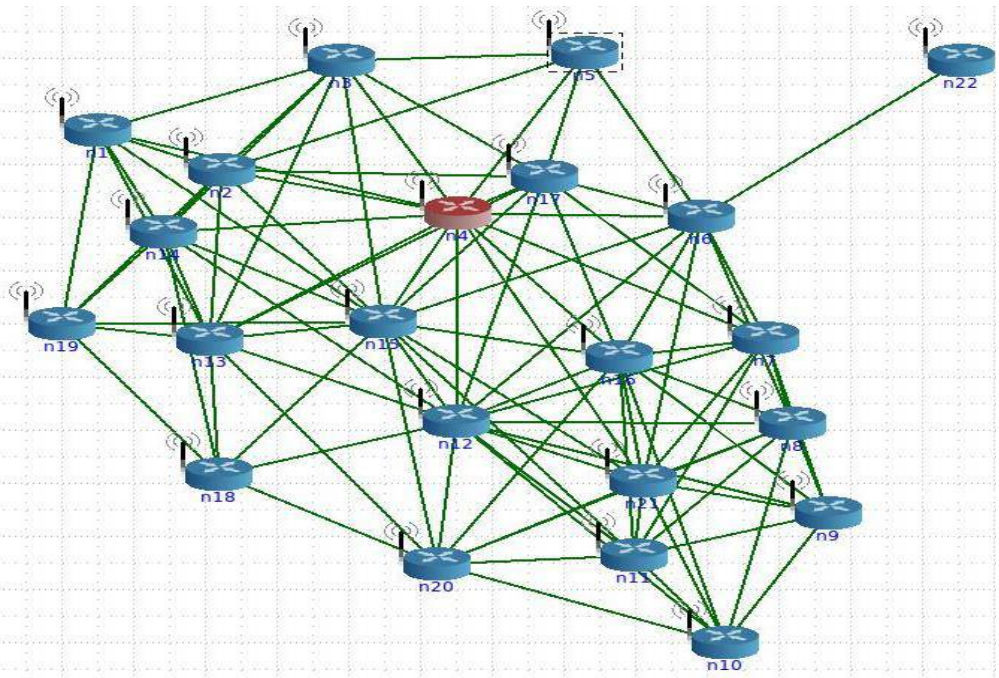
ΠανεπιστήμιοΜακεδονίας
ΔΠΜΣ Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών
Καθηγητής: Α. Α. Οικονομίδης

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

Survivability & Security Aspects in Mobile Ad Hoc Networks

Επιβιωσιμότητα και πτυχές ασφάλειας σε κινητά “κατά περίπτωση” δίκτυα



Φοιτήτρια : Μαϊδου Σεβαστή

Student : Maidou Sevasti

Β’ Εξάμηνο

ΘΕΣΣΑΛΟΝΙΚΗ 2013

Πίνακας περιχομένων

1.Περίληψη-Abstract

Η χρήση των Mobile Ad Hoc Network (MANETs) γίνονται όλο και πιο δημοφιλείς καθώς, εκτός από παλιότερες χρήσεις όπως στρατιωτικά πεδία μαχών και καταστάσεις καταστροφών παρατηρούμε την χρήση τους στην καθημερινότητα μας. Έτσι λοιπόν με την αυξημένη χρήση τους προέρχεται και η ανάγκη για ασφάλεια και αποτελεσματικότητα. Είναι γεγονός πλέον ότι αυτό δεν είναι εύκολα εφικτό καθώς οι απαιτήσεις της ασφάλειας δικτύου συγκρούονται πολλές φορές με τις απαιτήσεις σε κινητά δίκτυα λόγω της φύσης των φορητών συσκευών. Εξαιτίας της υποδομής των MANETs είναι περισσότερο επιρρεπείς στο να δεχτούν πιο εύκολα επιθέσεις στον τομέα τις ασφάλειας. Η παρούσα εργασία περιλαμβάνει μια αναλυτική επεξήγηση των MANETS καθώς επίσης και θέματα που αφορούν την ασφάλεια τους. Τέλος γίνεται ένας λεπτομερείς διαχωρισμός των ειδών επιθέσεων με βασικό κριτήριο το επίπεδο διαστρωμάτωσης και παραθέτονται τρόποι αντιμετώπισης τους.

Abstract

Mobile Ad-Hoc Networks (MANETs) are becoming increasingly popular as more and more mobile devices find their way to the public, besides “traditional” uses such as military battlefields and disaster situations they are being used more and more in every-day situations. With this increased usage comes the need for making the networks secure as well as efficient, something that is not easily done as many of the demands of network security conflicts with the demands on mobile networks due to the nature of the mobile devices. This paper provides a detailed explanation of MANETS as well as issues relating to their safety. Finally becomes a detailed separation of species attacks and includes identifying ways of dealing with them.

2.Εισαγωγή

Στις μέρες μας, χάρη στις διαδικτυακές εγκαταστάσεις και την δυνατότητα μεταφοράς,πολλοί άνθρωποι χρησιμοποιούν κινητή δικτύωση στις επαγγελματικές και καθημερινές δραστηριότητες τους. Η αυξανόμενη ζήτηση των ασύρματων φορητών συσκευών, όπως φορητοί υπολογιστές, PDA, ασύρματα τηλέφωνα ή ασύρματοι αισθητήρες, ανέδειξε τη σημασία των ασύρματων δικτύων.

Όμως, τα τελευταία χρόνια πόλο έλξης στον ερευνητικό τομέα αποτελούν τα κατά περίπτωση δίκτυα (MANETS)[1]. Η διαφορετική υποδομή τους από τα υπόλοιπα δίκτυα, η χρησιμότητα στην καθημερινότητα των ανθρώπων καθώς οι δυνατότητες τις οποίες παρέχουν κάνουν τα MANETS περιζήτητα σε όλους τους τομείς.

3.

1. Ορισμός-MANET

Ένα **MANET (Mobile Ad hoc NETwork - Κινητό ad hoc δίκτυο)** είναι ένα αυτορυθμιζόμενο και χωρίς υποδομή δίκτυο κινητών συσκευών που συνδέονται μέσω ασύρματων ζεύξεων. Ad hoc είναι λατινική φράση που σημαίνει "γι αυτό το σκοπό".

Κάθε συσκευή σε ένα MANET είναι ελεύθερη να κινηθεί σε οποιαδήποτε 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 (mobile ad hoc network (MANET)).

2. Αδυναμίες/Μειονεκτήματα ενός δικτύου MANET

Σύμφωνα με τον παραπάνω ορισμό και μετά από εκτενή και προσεκτική μελέτη παρατηρήθηκαν κάποιες αδυναμίες οι οποίες οφείλονται κυρίως στην φύση και την αρχιτεκτονική ενός δικτύου MANET. Οι αδυναμίες λοιπόν που διαπιστώθηκαν είναι οι εξής:

1 Για λόγους ευκολίας ο όρος κινητά κατά περίπτωση δίκτυα θα χρησιμοποιείται στην συνέχεια με τον αγγλικό όρο

Απουσία ασφαλών ορίων (Lack of Secure Boundaries): Είναι σαφές ότι η ασφάλεια ορίων που εξασφαλίζει ένα παραδοσιακό ενσύρματο δίκτυο δεν μπορεί να συγκριθεί με την αντίστοιχη ασφάλεια των δικτύων MANETs. Η απουσία ασφαλών ορίων προέρχεται απο την φύση και την αρχιτεκτονική των κατα περίπτωση κινητών δικτύων η οποία περιλαμβάνει τα εξής:

- ελευθερία ένταξης
- ελευθερία μετακίνησης,
- ελευθερία εξόδου απο το δίκτυο.

Συγκριτικά με ένα ενσύρματο «παραδοσιακό» δίκτυο ένας αντίπαλος δε χρειάζεται να κερδίσει την φυσική πρόσβαση του για να επισκεφθεί ένα δίκτυο καθώς έχει την δυνατότητα να επικοινωνήσει με οποιονδήποτε κόμβο εντός της εμβέλειας του επιθυμητού δικτύου και συνεπώς να μπει αυτόματα στο δίκτυο. Αυτό έχει σαν αποτέλεσμα το κινητό ad hoc δίκτυο να μην παρέχει την ασφάλεια των ορίων για την προστασία του δικτύου. Ταυτόχρονα το καθιστά επιρρεπή σε οποιοδήποτε κίνδυνο (επιθέσεις) οποιαδήποτε στιγμή (Li& Joshi 2008)

Απειλές από "παραβιασμένους" κόμβους μέσα στο δίκτυο:

Υπάρχουν κάποιες επιθέσεις που στοχεύουν να αποκτήσουν τον έλεγχο των κόμβων και στη συνέχεια τους χρησιμοποιούν για περαιτέρω κακόβουλες ενέργειες. Δεδομένου ότι κόμβοι είναι αυτόνομες μονάδες που μπορούν να ενταχθούν ή να εγκαταλείψουν το δίκτυο με ελευθερία, είναι δύσκολο για τους ίδιους τους κόμβους να εφαρμόσουν αποτελεσματικές πολιτικές για όλους τους κόμβους με τους οποίους επικοινωνούν. Επιπλέον, λόγω της ελευθερίας κίνησης σε ένα δίκτυο ad hoc, ένας παραβιασμένος κόμβος μπορεί να αλλάζει συχνά στόχο επίθεσης και να εκτελέσει κακόβουλη συμπεριφορά σε διαφορετικό κόμβο του δικτύου. Αυτό έχει ως αποτέλεσμα να είναι πολύ δύσκολη η παρακολούθησης μια κακόβουλης συμπεριφοράς ειδικά σε μια μεγάλης κλίμακας δίκτυο ad hoc. Από τα παραπάνω διαπιστώνουμε ότι ιδιαίτερη προσοχή πρέπει να δίνεται και από τους κινητούς

κόμβους οι οποίοι δε θα πρέπει να εμπιστεύονται εύκολα κάποιο κόμβο ενός δικτύου ad hoc ο οποίος ενδέχεται να έχει παραβιαστεί. .(Li& Joshi 2008)

Απουσία κεντρικής διαχείρισης (Lack of Centralized Management) :

Τα κινητά ad hoc δίκτυα δεν έχουν μία κεντρική διαχείρισης όπως ένας διακομιστής (server), κάτι το οποίο δημιουργεί διάφορα προβλήματα τα οποία θα αναλύσουμε παρακάτω.

Πρώτα απ'όλα, η απουσία κεντρικής διαχείρισης καθιστά δύσκολη την ανίχνευση επιθέσεων διότι δεν είναι εύκολη η διαχείρηση της κυκλοφορίας σε ένα δυναμικό και μεγάλης κλίμακας περιβάλλον όπως είναι ένα δίκτυο ad hoc. Είναι κοινός γνωστό σε ένα δίκτυο ad hoc ότι οι καλοήθεις βλάβες, όπως βλάβες μεταφορών και απόρριψη πακέτων, συμβαίνουν συχνά. Ως εκ τούτου, κακόβουλες βλάβες θα είναι πιο δύσκολο να ανιχνευθούν, ειδικά όταν οι αντίπαλοι αλλάζουν τον τρόπο και τον στόχο της επίθεσης τους ανά τακτά χρονικά διαστήματα. Δεύτερον, η έλλειψη κεντρικής διαχείρισης θα εμποδίσει τη διαχείριση εμπιστοσύνης μεταξύ των κόμβων στο δίκτυο ad hoc. Αυτό συμβαίνει διότι όλοι οι κόμβοι απαιτείται να συνεργαστούν για την λειτουργία του δικτύου. Τρίτον, ορισμένοι αλγόριθμοι στο κινητό δίκτυο ad hoc βασίζονται στην συμμετοχή και την συνεργασία όλων των κόμβων και της υποδομής. Έτσι, λοιπόν επειδή δεν υπάρχει κεντρική εξουσία, και η λήψη αποφάσεων είναι μερικές φορές αποκεντρωμένη, ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί αυτου του είδους την ευπάθεια και να προβεί σε επιθέσεις.

Με μια λέξη, η απουσία κεντρικής διαχείρισης οδηγεί σε ευπάθεια που μπορεί να επηρεάσει πολλές πτυχές των δραστηριοτήτων σε ένα δίκτυο ad hoc. (Li& Joshi 2008)

Διαθεσιμότητα πόρων (Resource Availability)- MANETs

Ενώ οι κόμβοι στο ενσύρματο δίκτυο δεν χρειάζεται να ασχοληθούν με το πρόβλημα τροφοδοσίας, διότι έχουν πρόσβαση σε παροχή ηλεκτρικής ισχύος από τις εξόδους, στους αντίστοιχους κόμβους σε κινητό δίκτυο ad hoc δε συμβαίνει κάτι τέτοιοι. Αυτό που θα πρέπει να εξετάζεται κάθε φορά είναι η περιορισμένη ισχύ της μπαταρίας του κάθε κόμβου, η οποία με την σειρά της προκαλεί πολλά προβλήματα. Το πρώτο πρόβλημα που μπορεί να προκληθεί από την περιορισμένη παροχή ηλεκτρικού ρεύματος είναι η εμφάνιση denial - of - service επιθέσεων (τα είδη των επιθέσεων θα

αναλυθούν σε παρακάτω ενότητα). Δεδομένου ότι ο αντίπαλος γνωρίζει ότι ο κόμβος στόχος διαθέτει περιορισμένη ισχύ της μπαταρίας ,μπορεί να στέλνει συνεχώς πρόσθετα πακέτα και να ζητήσει τη δρομολόγηση τους .Με τον τρόπο αυτό, η ισχύς της μπαταρίας του κόμβου στόχου θα εξαντληθεί από αυτά τα ανούσια καθήκοντα, και έτσι ο κόμβος θα τεθεί εκτός λειτουργίας. Επιπλέον, ένας κόμβος στο κινητό δίκτυο ad hoc μπορεί να αρνηθεί να δρομολογήσει τα πακέτα που δέχεται χαρακτηρίζοντας την συμπεριφορά αυτή ως “εγωιστική”. Αυτό γίνεται κυρίως όταν διαπιστωθεί ότι υπάρχει περιορισμένη παροχή ηλεκτρικού ρεύματος, κάτι το οποίο μπορεί να προκαλέσει κάποια προβλήματα ιδιαίτερα όταν απαιτείται η συνεργασία με άλλους κόμβους για την υποστήριξη ορισμένων λειτουργίες του δικτύου. Τέλος, αξίζει να τονιστεί ότι ιδιόμορφες συμπεριφορές των κόμβων δεν πρέπει να θεωρούνται ως κακόβουλες συμπεριφορές, αλλά θα πρέπει να αντιληφθούμε αν η συμπεριφορά προκαλείται από την περιορισμένη ισχύ της μπαταρίας , ή από άρνηση συνεργασίας εκ προθέσεως (Li& Joshi 2008).

Δυνατότητα κλιμάκωσης (Scalability)

Σε αντίθεση με το παραδοσιακό ενσύρματο δίκτυο όπου η κλίμακα της είναι γενικά προκαθορισμένη από τον σχεδιασμό της και δε μπορεί να αλλάξει πολύ κατά τη διάρκεια της χρήσης, το μέγεθος του δικτύου ad hoc αλλάζει συνεχώς. Αυτό συμβαίνει εξαιτίας της κινητικότητας των κόμβων στο κινητό ad hoc δίκτυο και στο οποίο δύσκολα μπορεί να προβλέψει κανείς από πόσους κόμβους θα αποτελείται στο μέλλον. Συνεπώς, τα πρωτόκολλα που εφαρμόζονται στο δίκτυο ad hoc, όπως το πρωτόκολλο δρομολόγησης θα πρέπει να είναι συμβατό με το συνεχώς μεταβαλλόμενο σε κλίμακα δίκτυο ad hoc (Li& Joshi 2008)

4.Ορισμός Survivability of MANET

Μετά από ανάλυση των ορισμού MANET έχει εξεταστεί ότι η βασική υπηρεσία που πρέπει να παρέχει ένα MANET είναι αυτής της επικοινωνίας ανάμεσα σε δυο κόμβους με οποιοδήποτε τρόπο. Έτσι λοιπόν το θέμα της επιβιωσιμότητας (survivability) ορίζεται ως τον βαθμό ικανοποίησης της επικοινωνίας . Από την άλλη πλευρά όμως οι απειλές τις οποίες έχει να αντιμετωπίσει ένα MANET είναι οι εξής :

- Επιρροή δυναμικής τοπολογίας. Οι κόμβοι σε ένα δίκτυο MANET κινούνται αυθαίρετα. Κατά συνέπεια, η τοπολογία δικτύου μπορεί να αλλάξει από την μια στιγμή στην άλλη.
- Δυσλειτουργίες που μπορούν να συμβούν σε κόμβους και συνδέσεις. Για παράδειγμα, ένας κόμβος μπορεί να τερματιστεί για κάποιους λόγους ή μια σύνδεση μπορεί να επηρεαστεί από ένα εμπόδιο.

- Η απειλή επιθέσεων είναι πιθανή σε όλα τα επίπεδα διαστρωμάτωσης ενός δικτύου MANET.

Με την παραπάνω ανάλυση μπορούμε να ορίσουμε την επιβιωσιμότητα ενός κινητού δίκτυο ad hoc ως τη δυνατότητα δημιουργίας μιας επικοινωνίας μεταξύ δύο οποιονδήποτε κόμβων του δικτύου ανά πάσα στιγμή υπό την επίδραση της δυναμική-τοπολογίας, πιθανών σφαλμάτων και επιθέσεων.(Zhou,Xia,Wang & Qi 2009)

5.Αναλυτική περιγραφή της επιβιωσιμότητας ενός δικτύου MANET

Με βάση τον ορισμό της επιβιωσιμότητας του δικτύου MANET παραπάνω, το σύστημα του MANET ως προς την επιβιωσιμότητα μπορεί να χωριστεί σε τρία μέλη: mobile ad hoc network, τις επιπτώσεις(impact) που μπορεί να επηρεάσουν την ικανότητα επιβίωσης των mobile ad hoc δίκτυο, και η βασική υπηρεσία(service) που μπορεί ένα δίκτυο MANET να παρέχει. Κάτι το οποίο περιγράφεται από την παρακάτω σχέση

***SurvivalAdhoc={ADHOC,SERVICE,IMPACT}* (1)**

Το mobile ad hoc δίκτυο αποτελείται από έναν αριθμό κόμβων με ορισμένα χαρακτηριστικά τα οποία σχετίζονται με τις δυνατότητες επιβίωσης. Θεωρούμε ότι ο κάθε κόμβος χαρακτηρίζεται από τα εξής στοιχεία: διεύθυνση IP, θέση (location), radio range, κατάσταση(μετάδοση, λήψη), ισχύς (power), τύπος πρωτοκόλλου (protocol type) και είδος κινητικότητας (mobility type). Η συσχέτιση των παραπάνω χαρακτηριστικών και η επιβιωσιμότητα ενός δικτύου MANET μπορεί να περιγραφεί παρακάτω:

ADHOC::={NODE,LINK} (2)

NODE::={node1,node2,…noden} (3)

LINK::={<nodei,nodej>|nodei,nodej∈NODE} (4)

node=(ip,id,location,R,state,power,
protocoltype,mobilitytype)

Η βασική υπηρεσία από ένα δίκτυο MANET είναι να δημιουργήσει μια υπηρεσία επικοινωνίας μεταξύ δύο κόμβων του δικτύου ανά πάσα στιγμή. Το δίκτυο ad hoc δημιουργεί μια σύνδεση σε δύο βήματα. Πρώτον, στις συνδέσεις μεταξύ δύο οποιωνδήποτε γειτονικών κόμβους που παρέχονται από το επίπεδο σύνδεσης και το φυσικό επίπεδο .Στην συνέχεια οι συνδέσεις επεκτείνονται από το στρώμα δικτύου

υπό μορφή ενός- άλματος (hop) σε πολλαπλά άλματα (multihops). Αυτό που πρέπει να αναφερθεί είναι ότι για ένα δίκτυο MANET με N κόμβους , πρέπει να υπάρχει μια κατευθυντική τροχιά (*Nodei, Nodej….Nodel,Nodm*,) μεταξύ δυο κόμβων . Και η διαδρομή, πρέπει να πληρούν τις ακόλουθες απαιτήσεις:
1) η απόσταση μεταξύ δύο γειτονικών κόμβων, Node i και Node i+1, να είναι μικρότερη από το εύρος μετάδοσης του Nodei.
2) Κάθε κόμβος σε αυτή την πορεία πρέπει να καταλαμβάνει μια διαδρομή εισόδου.
Οι παράγοντες οι οποίοι επηρεάζουν την επιβιωσημότιτα ενός δικτύου MANET είναι η δυναμική τοπολογία , τα λάθη και οι επιθέσεις. Η κύρια σημασία αυτών των παραγόντων είναι να καταστρέψουν την σύνδεση ανάμεσα σε δυο κόμβους με αποτέλεσμα το δίκτυο να αποσυνδεθεί. Κάτι το ποίο περιγράφεται στην παρακάτω σχέση :

$$IMPACT::=\{ a|\ DynamicToplogy(a) \vee Fault\ a \vee Attack(a), a \in Actions\}$$ (Zhou,Xia,Wang & Qi 2009)

Dynamic Topology: Ο παράγοντας της δυναμικής τοπολογίας προκαλείται και επηρεάζεται από δράσεις όπως η κινητικότητα των κόμβων. Αυτό μπορεί να έχει ως αποτέλεσμα την αλλαγή θέσης του κόμβου. Η επιρροή της δυναμικής τοπολογίας εστιάζεται κυρίως στο ότι η νέα απόσταση των γειτονικών κόμβων μπορεί να είναι μεγαλύτερη από το εύρος μετάδοσης του πρώτου κόμβου και έτσι η διαδρομή καταστρέφεται. (Zhou,Xia,Wang & Qi 2009)

Fault: Βλάβες διαχωρίζονται σε βλάβες κόμβων και βλάβες συνδέσμων. Βλάβες κόμβων είναι οι ενέργειες που προκαλούν αλλαγές στην κατάσταση του κόμβου. Εάν η κατάσταση του κόμβου αλλάξει, ταυτόχρονα θα έχουμε αλλαγή και στο εύρος μετάδοσης. Αν το εύρος ζώνης μετά την αλλαγή είναι μικρότερο από το απαιτούμενο τότε θα έχουμε απόρριψη του πακέτου..Στην συνέχεια οι βλάβες συνδέσμων είναι αυτές οι οποίες προκαλούνται από εμπόδια μεταξύ των κόμβων. (Zhou,Xia,Wang & Qi 2009), Αυτό συνοψίζεται στην ακόλουθη σχέση:

$$Fault(a) \rightarrow Node(a) \vee Link(a), a \in Actions$$

Τέλος όσον αφορά τις επιθέσεις που ενδέχεται να δεχθεί ένα κινητό ad hoc δίκτυο ταξινομούνται με βάση την διαστρωμάτωση του δικτύου σε επίπεδα. (αναλυτικότερη περιγραφή στα είδη των επιθέσεων θα γίνει σε παρακάτω ενότητα).Αυτό συνοψίζεται στην παρακάτω σχέση:

$$Attack(a) \rightarrow PhysicalAttack(a) v\ LinkAttack(a)$$
$$NetworkAttack(a)\ TranspAttack(a)\ ApplicationAttack(a)$$

(Y.Zhou,C.XIA , H.Wang,J.Qi 2009)

Layer	**Security Issues**
Application Layer	Detecting and avoiding viruses, worms, and malicious node.
Transport Layer	Authenticating and securing end-to-end interactions through-out data encryption.
Network Layer	Protecting ad-hoc routing and promoting protocols.
Link Layer	Protecting the wireless MAC protocol and provide link-layer security

	support.
Physical Layer	Avoiding signal congestion, denial-of-service attacks.

Εικόνα 1.(Jasmair & Kumar 2012)

6.Στόχοι Ασφάλειας

Υπάρχουν πέντε μεγάλοι στόχοι ασφαλείας που διατηρούν ένα αξιόπιστο και ασφαλές περιβάλλον ad-hoc δικτύου. Η επίτευξη αυτών το στόχων οδηγεί στην πρόληψη και τον εντοπισμό επιθέσεων που αφορούν την ασφάλεια στο δίκτυο. Αυτοί είναι κυρίως:

Διαθεσιμότητα (Availiability)

Ο όρος Διαθεσιμότητα σημαίνει ότι κάθε κόμβος πρέπει να διατηρεί την ικανότητά του να παρέχει όλες τις υπηρεσίες που έχουν σχεδιαστεί ανεξάρτητα από την κατάσταση ασφαλείας του. Όμως αυτός ο όρος αμφισβητείται κυρίως κατά τη διάρκεια των denial-of-service επιθέσεων, κατά την οποία όλοι οι κόμβοι του δικτύου μπορούν να αποτελέσουν στόχος επίθεσης και έτσι μερικές από τις υπηρεσίες δικτύου να μην είναι διαθέσιμες, όπως το πρωτόκολλο δρομολόγησης. (Li& Joshi 2008)

Εμπιστευτικότητα (confidentiality)

Η επίτευξη αυτού του στόχου εξασφαλίζει ότι οι πληροφορίες δεν είναι ποτέ προσπελάσιμες από μη εξουσιοδοτημένους φορείς. Σε MANETs, αυτό είναι πιο δύσκολο να επιτευχθεί, διότι ενδιάμεσοι κόμβοι (routers) δέχονται τα πακέτα για άλλους αποδέκτες. .(Jasmair & Kumar 2012)

Ακεραιότητα (integrity)

Ο όρος αυτός εγγυάται την εξασφάλιση της αξιοπιστίας των μηνυμάτων κατά την αποστολή τους η οποία μπορεί να παραβιαστεί με δυο τρόπους :

- Κακόβουλη αλλοίωση
- Τυχαίας αλλοίωσης

Ένα μήνυμα μπορεί να αφαιρεθεί, να αναπαραχθεί ή να αναθεωρηθεί από έναν αντίπαλο με κακόβουλο στόχο, το οποίο θεωρείται ως κακόβουλη αλλοίωση. Αντιθέτως, αν το μήνυμα έχει χαθεί ή το περιεχόμενό της έχει αλλάξει λόγω κάποιων βλαβών, οι οποίες μπορεί να είναι σφάλματα μετάδοσης στην επικοινωνία ή σφάλματα υλικού, όπως βλάβης του σκληρού δίσκου, τότε κατηγοριοποιούνται ως τυχαία αλλοίωση. . (Li& Joshi 2008)

Ο έλεγχος ταυτότητας (authentication)

Χωρίς έλεγχο ταυτότητας, ένας αντίπαλος μπορεί να δείξει ψευδή κόμβο, αποκτώντας έτσι μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και διαταράσσοντας με αυτόν τον τρόπο τη λειτουργία των άλλων κόμβων. .(Jasmair & Kumar 2012)

Μη αποκήρυξη (non-repudation)

Ιδιαίτερα χρήσιμο για ανίχνευση επικίνδυνων κόμβων. Για παράδειγμα όταν ένας κόμβος Χ λαμβάνει ένα λάθος μήνυμα από έναν κόμβο Υ, με την μη αποκήρυξη(non-repudation) επιτρέπεται ο κόμβος Χ να να κατηγορήσει τον κόμβο Υ χρησιμοποιώντας αυτό το μήνυμα και να πείσει και τους άλλους κόμβους ότι ο κόμβος Υ είναι επικίνδυνος. .(Jasmair & Kumar 2012)

Ανωνυμία (anonymity)

Ο όρος αυτός σημαίνει ότι όλες οι πληροφορίες που μπορούν να χρησιμοποιηθούν για να εντοπιστεί ο ιδιοκτήτης ή ο τρέχοντα χρήστης του κόμβου θα πρέπει να παραμένει ιδιωτικό και να μην διανέμονται από τον ίδιο τον κόμβο ή το λογισμικό του συστήματος. Το κριτήριο αυτό συνδέεται στενά με τη διατήρηση της ιδιωτικότητας, την οποία θα πρέπει να προσπαθήσουμε να την προστατεύσουμε από την αυθαίρετη διαρροή σε άλλες οντότητες. . (Li& Joshi 2008)

Authorization

Εξουσιοδότηση χρησιμοποιείται γενικά για να οριστούν διαφορετικά δικαιώματα πρόσβασης σε διαφορετικό επίπεδο των χρηστών. Για παράδειγμα, πρέπει να διασφαλίσουμε ότι η λειτουργία διαχείρισης του δικτύου είναι προσβάσιμο μόνο από τον διαχειριστή του δικτύου. Ως εκ τούτου, θα πρέπει να υπάρχει μια διαδικασία έγκρισης πριν ο διαχειριστής του δικτύου έχει πρόσβαση στις λειτουργίες διαχείρισης του δικτύου. . (Li& Joshi 2008)

7.Είδη επιθέσεων σε MANET

Τα είδη των επιθέσεων μπορούν να ταξινομηθούν στις εξής κατηγορίες :

A.Internal attack -Εσωτερικές επιθέσεις που προέρχονται από κόμβους που αποτελούν μέρος του δικτύου. Σε μια εσωτερική επίθεση κακόβουλου κόμβου από το δίκτυο επιτυγχάνεται μη εξουσιοδοτημένη επαφή και η προσωποποίηση του σε έγκυρο κόμβο. Οι ζημιές που μπορεί να κάνει είναι να αναλύσει τις συναλλαγές

μεταξύ άλλων κόμβων και να συμμετέχει σε άλλες δραστηριότητες του δικτύου. (Jasmair & Kumar 2012)

B.External attack –Εξωτερικές επιθέσεις. Αυτοί οι τύποι των επιθέσεων προσπαθούν να προκαλέσουν συμφόρηση στο δίκτυο, άρνηση παροχής υπηρεσιών (DoS),λανθασμένες πληροφορίες δρομολόγησης κλπ. Οι επιθέσεις αυτές εμποδίζουν το δίκτυο από την κανονική επικοινωνία και παράγει πρόσθετη επιβάρυνση στο δίκτυο.(Gagandeep, Aashima, Pawan Kumar, 2012) Οι εξωτερικές επιθέσεις μπορούν να διαχωριστούν σε δύο κατηγορίες:

1.Passive attacks-Παθητικές επιθέσεις

Τα MANETS είναι πιο επιρρεπείς σε παθητικές επιθέσεις. Μια παθητική επίθεση δεν μεταβάλλει τα δεδομένα που διαβιβάζονται στο πλαίσιο του δικτύου αλλά περιλαμβάνει τη μη εξουσιοδοτημένη «ακρόαση» στην κίνηση του δικτύου ή συσσωρεύει τα δεδομένα από αυτό. Ένας κακόβουλος χρήστης δεν διαταράσσει τη λειτουργία του πρωτοκόλλου δρομολόγησης, αλλά προσπαθεί να ανακαλύψει τις σημαντικές πληροφορίες από την δρομολόγησης της κίνησης. Ανίχνευση τέτοιου είδους επιθέσεων είναι δύσκολη, δεδομένου ότι η λειτουργία του ίδιου του δικτύου δεν επηρεάζεται. Για να ξεπεραστούν αυτού του είδους οι επιθέσεις χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης για την κρυπτογράφηση των δεδομένων που μεταδίδονται. (Gagandeep, Aashima, Pawan Kumar, 2012)

2.Active attacks-Ενεργές επιθέσεις

Αυτού του είδους οι επιθέσεις είναι πολύ σοβαρές επιθέσεις στο δίκτυο καθώς εμποδίζουν τη ροή μηνυμάτων μεταξύ των κόμβων. Ωστόσο οι ενεργές επιθέσεις μπορούν αν διαχωριστούν σε εσωτερικές ή εξωτερικές. Ενεργές εξωτερικές επιθέσεις μπορεί να πραγματοποιηθούν από εξωτερικές πηγές που δεν ανήκουν στο δίκτυο. Εσωτερικές επιθέσεις προέρχονται από κακόβουλους κόμβους οι οποίοι αποτελούν μέρος του δικτύου.Αποτελούν δύσκολη κατηγορία καθώς είναι δύσκολο να ανιχνευτούν απο ότι οι εξωτερικές επιθέσεις. Οι επιθέσεις αυτές δημιουργούν μη εξουσιοδοτημένη πρόσβαση στο δίκτυο που βοηθά τον εισβολέα να κάνει αλλαγές όπως η τροποποίηση των πακέτων, DoS, την κυκλοφοριακή συμφόρηση κλπ. Πηγή από την οποία ξεκινάνε οι ενεργές επιθέσεις είναι συνήθως οι κακόβουλοι κόμβοι. . (Gagandeep, Aashima, Pawan Kumar, 2012)

Στην συνέχεια οι ενεργές επιθέσεις διαχωρίζονται σε τέσσερις κατηγορίες:

Dropping Attacks: οι ”παραβιασμένοι κόμβοι” μπορεί να απορρίψουν όλα τα πακέτα τα οποία δεν προορίζονται για αυτούς. Τέτοιου είδους επιθέσεις μπορεί να αποτρέψουν την από άκρο σε άκρο επικοινωνία μεταξύ των κόμβων, αν ο

”παραβιασμένος κόμβος”είναι σε ένα κρίσιμο σημείο. Τα περισσότερα πρωτόκολλα δρομολόγησης δε διαθέτουν μηχανισμούς οι οποίοι να ανιχνεύουν αν τα πακέτα δεδομένων έχουν διαβιβαστεί ή όχι. .(Gagandeep, Aashima, Pawan Kumar, 2012)

Modification Attacks: Sinkhole επιθέσεις είναι το παράδειγμα των επιθέσεων τροποποίησης. Αυτές οι επιθέσεις έχουν σκοπό την τροποποίηση των πακέτων και την διατάραξη της συνολικής επικοινωνίας μεταξύ των κόμβων του δικτύου. . (Gagandeep, Aashima, Pawan Kumar, 2012)

Fabrication Attacks: Ο εισβολέας στείλει ψεύτικο μήνυμα στους γειτονικούς κόμβους, χωρίς να λάβει οποιαδήποτε σχετική μήνυμα. Επιπλέον, μπορεί να στέλνει ψεύτικο μήνυμα απάντησης ως απάντηση σε σχετικά αιτήματα διαδρομής. (Gagandeep, Aashima, Pawan Kumar, 2012)

Timing Attacks: Σε αυτό το είδος των επιθέσεων, οι εισβολείς προσελκύουν άλλους κόμβους διαφημίζοντας τον εαυτό τους ότι είναι πιο κοντά σε αυτούς τος κόμβους. Rushing attacks and hello flood είναι δυο από τα παραδείγματα επιθέσεων που χρησιμοποιούν αυτήν την τεχνική. (Gagandeep, Aashima, Pawan Kumar, 2012)

Στην συνέχεια θα γίνει ανάλυση και κατηγοριοποίηση των κίνδυνων με βάση τα επίπεδα του δικτυακού μοντέλου αναφοράς

A. **Attacks at Physical Layer-Επιθέσεις στο φυσικό επίπεδο**
   - **Eavesdroping** σε αυτόν τον κόμβο απλά παρατηρεί τις ιδιωτικές πληροφορίες . Αυτή η πληροφορία μπορεί να χρησιμοποιείται αργότερα από τον κακόβουλο κόμβου. Οι μυστικές πληροφορίες, όπως τοποθεσία, δημόσιο κλειδί, ιδιωτικό κλειδί, περάστε-λέξη κλπ. μπορεί να είναι κάπως τραβηγμένο από eavesdropper. .(Jasmair & Kumar 2012)

   - **Jamming** Είναι μια ειδική κατηγορία επιθέσεις DoS που ξεκινούν από κακόβουλο κόμβο μετά τον καθορισμό της συχνότητας της επικοινωνίας. Σε αυτόν τον τύπο επίθεσης, το jammer μεταδίδει σήματα μαζί με απειλές για την ασφάλεια. Jamming επιθέσεις αποτρέπουν επίσης τη λήψη νόμιμων πακέτων.
   - **Active Interference** Αποτελεί μια επίθεση άρνησης υπηρεσίας η οποία εμποδίζει το ασύρματο κανάλι επικοινωνίας, ή τη νόθευση των επικοινωνιών. Τα αποτελέσματα αυτών των επιθέσεων εξαρτάται από τη διάρκειά τους, καθώς και το πρωτόκολλο δρομολόγησης. Ο εισβολέας έχε την δυνατότητα να αλλάξει τη σειρά των μηνυμάτων και θα προσπαθήσει να επαναλάβει τα παλιά μηνύματα. Gagandeep, Aashima, Pawan Kumar, 2012)

B. **Attacks at Data link / MAC layer**

- **Selfish Misbehaviour of Nodes**

  Οι επιθέσεις σε αυτή την κατηγορία,επηρεάζουν άμεσα την αυτό-απόδοσης των κόμβων και δεν έχουν καμία σχέση με τη λειτουργία του δικτύου. Οι εγωιστές κόμβοι μπορούν να αρνηθούν να λάβουν μέρος στη διαδικασία προώθησης ή ρίχνουν τα πακέτα σκόπιμα, προκειμένου να διαφυλαχθούν οι πόροι. Η απόρριψη πακέτων είναι μια από τις κύριες επιθέσεις εγωιστικών κόμβων που οδηγεί σε συμφόρηση του δικτύου. Gagandeep, Aashima, Pawan Kumar, 2012)

- **Malicious Behaviour of nodes**

  Ο κύριος σκοπός αυτού του κόμβου είναι να διαταράξει την κανονική λειτουργία του πρωτοκόλλου δρομολόγησης. Ο αντίκτυπος αυτής της επίθεσης αυξάνεται όταν η επικοινωνία λαμβάνει χώρα μεταξύ γειτονικών κόμβων. Οι επιθέσεις αυτού του τύπου υπάγονται σε ακόλουθες κατηγορίες:

  - **Denial of Service (DoS):** Αυτοί οι τύποι των απειλών παράγουν κακόβουλες ενέργειες με τη βοήθεια των παραβιασμένων κόμβων. Με την παρουσία τους σε τέτοιου είδους κόμβων , είναι πολύ δύσκολο να ανιχνευθεί η παραβιασμένη δρομολόγηση καθώς φαίνεται σαν μια κανονική διαδρομή , αλλά οδηγεί σε σοβαρά προβλήματα Gagandeep, Aashima, Pawan Kumar, 2012)
  - **Attacks on Network integrity:** η ακεραιότητα του Δικτύου είναι ένα σημαντικό ζήτημα , προκειμένου να παρέχει ασφαλή επικοινωνία και την ποιότητα των υπηρεσιών του δικτύου . Υπάρχουν πολλές απειλές οι οποίες εκμεταλλεύονται το πρωτόκολλο δρομολόγησης και εισαγάγουν λανθασμένες πληροφορίες δρομολόγησης Gagandeep, Aashima, Pawan Kumar, 2012)
  - **Misdirecting traffic:** Ένας κακόβουλος κόμβος διαφημίζει λανθασμένες πληροφορίες δρομολόγησης , προκειμένου να πάρει την ασφάλεια των στοιχείων πριν από την πραγματική διαδρομή. Αυτοί οι κόμβοι λαμβάνουν πληροφορίες που προοριζόταν για τον ιδιοκτήτη της διεύθυνσης . Ένας κακόβουλος κόμβος μπορεί να διαφημίσει ψεύτικο αίτημα διαδρομής , έτσι ώστε να ανταποκριθούν άλλοι κόμβοι. Gagandeep, Aashima, Pawan Kumar, 2012)

- **Attacking neighbour sensing protocols :** κακόβουλοι κόμβοι διαφημίζουν πλαστά μηνύματα λάθους , έτσι ώστε σημαντικές συνδέσεις διασύνδεσης σημειώνονται ως σπασμένα . Αυτό θα οδηγήσει σε μείωση της απόδοσης του δικτύου και της ποιότητας των παρεχόμενων υπηρεσιών . Gagandeep, Aashima, Pawan Kumar, 2012)

- **Traffic Analysis:** Ανάλυση της κίνησης στα δίκτυα ad hoc μπορεί να αποκαλύψουν τις εξής κατηγορίες πληροφοριών:.
  Θέση των κόμβων, τοπολογία δικτύου που χρησιμοποιείται για ρόλους επικοινωνίας που διαδραματίζουν οι κόμβοι και διαθέσιμη πηγή ένα κόμβων προορισμού (Gagandeep, Aashima, Pawan Kumar, 2012)

C. **Attacks at Network Layer**

Η βασική ιδέα πίσω από τις επιθέσεις στο στρώμα δικτύου είναι η εισαγωγή στην ενεργή διαδρομή από την πηγή στον προορισμό ή να απορροφήσουν την κυκλοφορία του δικτύου. Σε αυτές τις επιθέσεις, οι επιτιθέμενοι μπορούν να δημιουργήσουν βρόχους για να σχηματίσουν σοβαρή κυκλοφοριακή συμφόρηση.

- **Blackhole attack** Σε αυτή την επίθεση ένας κακόβουλος κόμβος στέλνει πλαστές ηλεκτρονικές πληροφορίες δρομολόγησης, υποστηρίζοντας ότι έχει βέλτιστη διαδρομή και προκαλεί και άλλους κόμβους να δρομολογήσουν τα πακέτα τους μέσα από την συγκεκριμένη διαδρομή. Στην συνέχεια ο κακόβουλος κόμβος ρίχνει αυτά τα πακέτα αντί να τα διαβιβάσει. (Jasmair & Kumar 2012)
- **Wormhole attack** ένας κακόβουλος κόμβος μπορεί να λάβει πακέτα σε ένα σημείο και να τα μεταφέρει έναν άλλον κακόβουλο κόμβο,που είναι σε ένα άλλο μέρος του δικτύου, εκτός ζώνης καναλιού. Ο δεύτερος κακόβουλος κόμβος επαναλαμβάνει έπειτα τα πακέτα. Αυτό κάνει όλους τους κόμβους που μπορούν να ακούσουν τις μεταδόσεις του δεύτερο κακόβουλου κόμβου να θεωρούν ότι ο κόμβος που έστειλε τα πακέτα στον πρώτο κακόβουλο κόμβο είναι ο γείτονας τους και για το λόγο αυτό λαμβάνουν τα πακέτα άμεσα από αυτόν. Τα Wormholes είναι πολύ δύσκολο να ανιχνευτούν και μπορούν να επηρεάσουν την απόδοση πολλών υπηρεσιών δικτύων όπως ο χρονικός συγχρονισμός, ο εντοπισμός και η μεταφορά δεδομένων. . (Jasmair & Kumar 2012)
- **Sinkhole Attack** ένας κακόβουλος κόμβος διαφημίζει λανθασμένες πληροφορίες δρομολόγησης για να παράγει τον εαυτό του ως ένα συγκεκριμένο κόμβο και λαμβάνει ολόκληρη την κυκλοφορία του

δικτύου. Έτσι με αυτόν τον τρόπο προσπαθεί να προσελκύσει τα ασφαλή δεδομένα από όλες τις γειτονικές κόμβους(Gagandeep, Aashima, Pawan Kumar, 2012)

- **Replay attack-**Ο εισβολέας που εκτελεί μια επίθεση επανάληψης αναμεταδίδει τα έγκυρα δεδομένα επανειλημμένα για να εισάγει την δρομολόγηση του δικτύου κυκλοφορίας που είχε συλληφθεί στο παρελθόν. Αυτή η επίθεση συνήθως μπορεί να χρησιμοποιηθεί για κακό σχεδιασμό λύσεων ασφαλείας. .(Jasmair & Kumar 2012)
- **Link Withholding & Link Spoofing Attacks** ο κακόβουλος κόμβος δεν εκπέμπει καμία πληροφορία σχετικά με τους συνδέσμους σε συγκεκριμένες κόμβους. Αυτό οδηγεί σε απώλεια των δεσμών μεταξύ των κόμβων. Στην συνέχεια ο κακόβουλος κόμβος διαφημίζει ψεύτικες πληροφορίες για να διακόψει την λειτουργία της δρομολόγησης. Αυτό έχει ως αποτέλεσμα τα δεδομένα ή τα δρομολόγια κίνησης να είναι ύπο τον έλεγχο του ίδιου κόμβου(Gagandeep, Aashima, Pawan Kumar, 2012)
- **Resource Consumption Attack**ένας παραβιασμένος κόμβος μπορεί να επιχειρήσει να καταναλώσει τη ισχύ της μπαταρίας προωθώντας για παράδειγμα περιττά πακέτα. Αυτοί οι τύποι των επιθέσεων είναι επίσης γνωστή ως sleep deprivation attack και εμφανίζονται κυρίως στις συσκευές που δεν προσφέρουν υπηρεσίες στο δίκτυο (Gagandeep, Aashima, Pawan Kumar, 2012)
- **Sybil Attack** Σε αυτήν την επίθεση ο εισβολέας προσπαθεί να δημιουργήσει πλαστές ταυτότητες του αριθμού των πρόσθετων κόμβων. Σε αυτό, ένα κακόβουλος κόμβος παράγεται ως μεγάλος αριθμός κόμβων αντί να παραχθεί ένας ενιαίος. Οι πρόσθετες ταυτότητες που αποκτά ο κόμβος ονομάζεται κόμβος Sybil. οι οποίοι μπορούν να κατασκευάσουν μια νέα ταυτότητα για τον εαυτό τους ή να κλέψουν την ταυτότητα ενός νόμιμου κόμβου. (Gagandeep, Aashima, Pawan Kumar, 2012)

D. **Attacks at Transport Layer**

- **Session Hijacking** Σε αυτήν την επίθεση, ο εισβολέας πλαστογραφήσει τη διεύθυνση IP του κόμβου θύματος, βρίσκει την σωστή ακολουθία αριθμών που αναμένεται από το στόχο και στη συνέχεια ξεκινά διάφορες επιθέσεις DoS. Σε αυτήν την περίπτωση ο κακόβουλος κόμβος προσπαθεί να συλλέξει τα ασφαλή δεδομένα (κωδικούς πρόσβασης, τα μυστικά κλειδιά, ονόματα σύνδεσης κλπ)

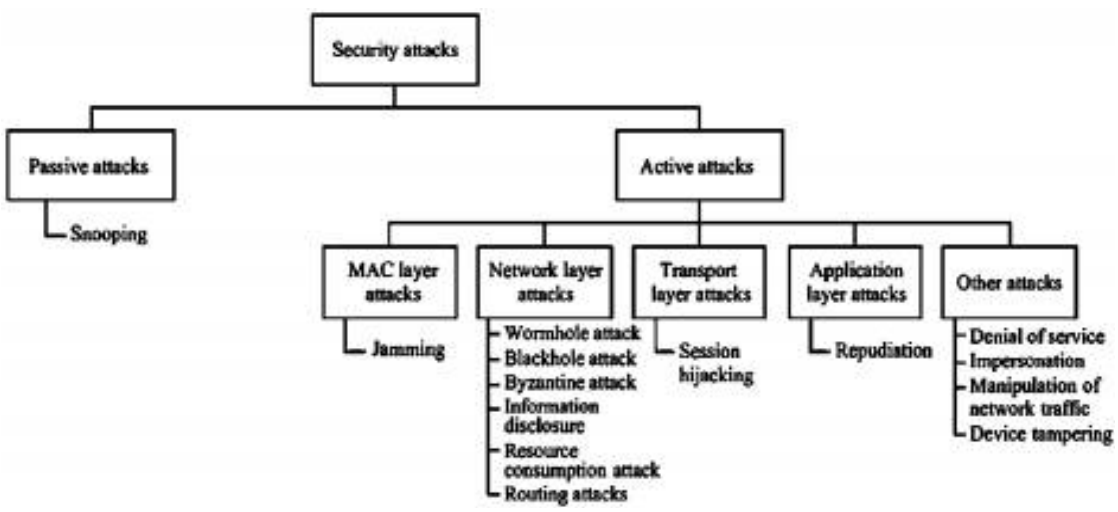
και άλλες πληροφορίες από τους κόμβους. (Gagandeep, Aashima, Pawan Kumar, 2012)

- **SYN Flooding Attack** Αποτελούν το είδος των Denial of Service (DoS) επιθέσεων, στις οποίες ο εισβολέας δημιουργεί ένα μεγάλο αριθμό απο μισάνοιχτες TCP συνδέσεις με τον κόμβο θύμα. (Gagandeep, Aashima, Pawan Kumar, 2012)

E. **Attacks at Application Layer**

- **Malicious code attacks** Σε αυτήν την κατηγορία ανήκουν επιθέσεις απο ιούς, σκουλήκια, Spywares και δούρειους ίππους. Επιπλέον μπορούν να γίνουν επιθέσεις τόσο λειτουργικό σύστημα όσο και στην εφαρμογή του χρήστη. (Gagandeep, Aashima, Pawan Kumar, 2012)
- **Repudiation attacks** Αναφέρεται στην άρνηση της συμμετοχής στο σύνολο ή σε μέρος των επικοινωνιών. Πολλοί από τους μηχανισμούς κρυπτογράφησης και firewalls που χρησιμοποιούνται δεν επαρκούν για την ασφάλεια του πακέτου. (Gagandeep, Aashima, Pawan Kumar, 2012)

Classification of Attacks in Wireless AD Hoc Networks



8. Προκλήσεις για ασφαλή ad hoc πρωτόκολλα δρομολόγησης

Σημαντικές προκλήσεις που αντιμετωπίζει ένα πρωτόκολλο δρομολόγησης σχεδιασμένο για Ad Hoc ασύρματα δίκτυα πρόσωπα είναι τα εξής : την κινητικότητα των κόμβων , περιορισμένων πόροι , κατάσταση καναλιού που κάνει λάθη , και κρυφά και εκτιθέμενα τερματικά προβλήματα.

•**Mobility**: Η τοπολογία του δικτύου σε ένα ασύρματο δίκτυο ad hoc είναι ιδιαίτερα δυναμική λόγω της κίνησης των κόμβων και την προσθήκη νέων κόμβων στο δίκτυο . Διακοπή της υπηρεσίας μπορεί να συμβεί είτε εξαιτίας της κίνησης του ενδιαμέσου κόμβους στη διαδρομή ή λόγω της κίνησης των ακραίων κόμβων(Jangra,Goel,Priyanka,Bhatia 2010) .

•**Bandwidth Constraints**: Στα ασύρματα δίκτυα, η χωρητικότητα της ζώνης των ραδιοσυχνοτήτων είναι περιορισμένη και ως εκ τούτου οι τιμές των δεδομένων που μπορεί να προσφέρει να είναι πολύ λιγότερες από ό,τι ένα ενσύρματο δίκτυο μπορεί να προσφέρει. Αυτός είναι ο λόγος για τον οποίο τα πρωτόκολλα δρομολόγησης θα πρέπει να χρησιμοποιούν το εύρος ζώνης με τον καλύτερο δυνατό τρόπο για να τα επιβαρύνουν όσο το δυνατόν λιγότερο(Jangra,Goel,Priyanka,Bhatia 2010).

•**Error-Prone Channel State**: Οι ασύρματες συνδέσεις έχουν χρονικά μεταβαλλόμενα χαρακτηριστικά όσον αφορά την ικανότητα σύνδεσης και την πιθανότητα σφάλματος σύνδεσης. Απαιτείται λοιπόν το πρωτόκολλο δρομολόγησης ασύρματου δικτύου ad hoc να αλληλεπιδρά με το στρώμα MAC για να υπάρχει δυνατότητα να βρεθούν βρείτε εναλλακτικές διαδρομές μέσα από την καλύτερη ποιότητα σύνδεσης(Jangra,Goel,Priyanka,Bhatia 2010).

•**Hidden Terminal Problem**: Αναφέρεται στη σύγκρουση των πακέτων σε έναν κόμβο υποδοχής, λόγω της ταυτόχρονης μετάδοσης αυτών των κόμβων οι οποίοι δεν είναι εντός της άμεσης μετάδοσης του αποστολέα, αλλά είναι μέσα στην εμβέλεια μετάδοσης της ανάκτησης(Jangra,Goel,Priyanka,Bhatia 2010).

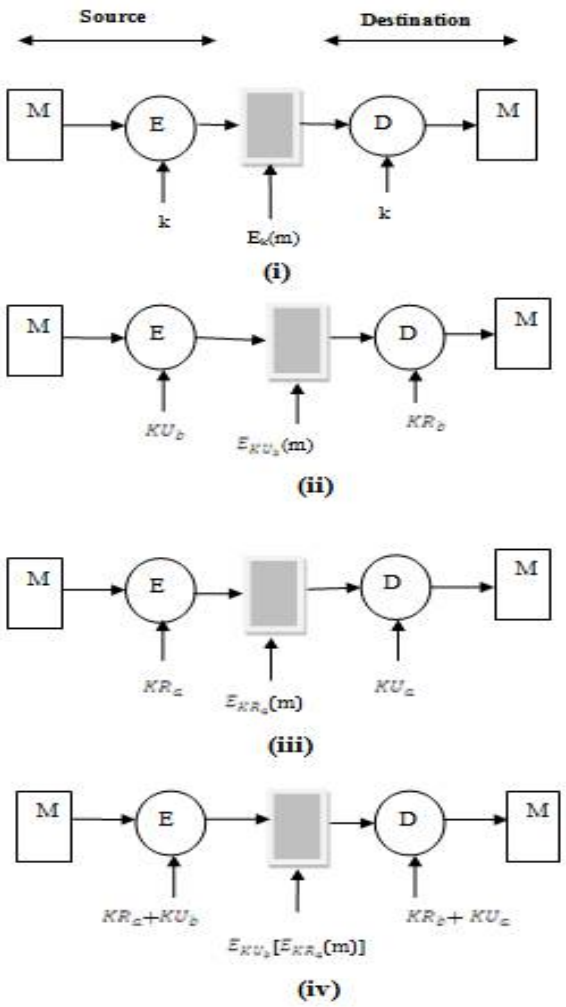
•**Exposed Terminal Problem**: Αναφερόμενοι στην ανικανότητα ενός κόμβου να μεταδώσει προς έναν άλλο κόμβο, όταν το ασύρματο κανάλι δεν είναι ελεύθερο εξ' αιτίας της μετάδοσης από έναν άλλο κοντινό κόμβο (Jangra, Goel, Priyanka, Bhatia 2010)

•**Resource Constraints**: διάρκεια ζωής της μπαταρίας και επεξεργαστική ισχύ είναι δύο απο τους δυο περιορισμένους πόρους που αποτελούν το μεγαλύτερο εμπόδιο για τους κόμβους στο δίκτυο ad hoc . Έτσι , ad hoc ασύρματα πρωτόκολλα δρομολόγησης του δικτύου πρέπει να αποσκοπεί στην βέλτιστη διαχείριση των πόρων(Jangra,Goel,Priyanka,Bhatia 2010).

9.Προτεινόμενη λύση ασφάλειας

Κωδικό γνησιότητας μηνύματος (MAC) είναι μια πιο σύγχρονη τεχνική ελέγχου ταυτότητας για να προστατευτούν τα MANET από επιθέσεις .Βασίζεται σε μια συμμετρική κρυπτογράφηση και χρησιμοποιεί το μυστικό κλειδί k το όποιο μοιράζεται ανάμεσα στον αποστολέα κόμβου και στον δέκτη κόμβου.

Το μυστικό κλειδί k χρησιμοποιείται για να δημιουργήσει ένα κρυπτογραφικό checksum γνωστό ως MAC ή MIC (message integrity code). Το MAC εξαρτάται από το μήνυμα m. Ο Πομπός- κόμβος θέλει να επικοινωνήσει το μήνυμα m στο δέκτη και παράγει έναν αριθμό γνωστών ως MAC χρησιμοποιώντας λειτουργία MAC και μυστικό κλειδί k στο μήνυμα m. Όταν ο δέκτης -κόμβος λαμβάνει το μήνυμα, απαντάει με την ίδια λειτουργία MAC και το μυστικό κλειδί k στο μήνυμα m συγκρίνει την ληφθείσα MAC με την υπολογισμένη MAC. Αν και οι δύο MAC είναι ίδια στο δέκτη τον κόμβο σας διαβεβαιώνεται ότι ο κόμβος είναι του αποστολέα- κόμβου. Και αν οι δύο κόμβοι MAC δεν είναι παρόμοια, τότε αυτός ο κόμβος είναι κακόβουλος κόμβος και τα MANET απορρίπτουν αυτόν τον κόμβο. Στην παρακάτω εικόνα παρουσιάζεται η αρχή λειτουργίας των MAC σε MANET για ασφάλεια.



Μ είναι ένα μήνυμα ότι είναι κρυπτογραφημένα με μυστικό κλειδί k. Εδώ στην εικόνα(i) περιγράφεται συμμετρική κρυπτογράφηση για εμπιστευτικότητα και αυθεντικότητα . Και στην εικόνα(ii) δείχνει κρυπτογράφηση με δημόσιο κλειδί με εμπιστευτικότητα. Σε αυτό ο αποστολέας στέλνει ένα μήνυμα στο δέκτη που είναι κρυπτογραφημένο με το δέκτη δημόσιου κλειδιού KUb. Στο συγκεκριμένο σχ, (iii) είναι για κρυπτογράφηση με δημόσιο κλειδί τόσο για πιστοποίηση και υπογραφή. Και το τελευταίο (iv), δείχνει κρυπτογράφηση με δημόσιο κλειδί χρησιμοποιώντας εμπιστευτικότητα, πιστοποίηση και υπογραφή. Με αυτό το ασύρματο δίκτυο αποφεύγετε κάθε κακόβουλος κόμβος μεταξύ πομπού και δέκτη κόμβο διότι ο κακόβουλος κόμβου δεν γνωρίζει το δημόσιο κλειδί του δέκτη. Οι πληροφορίες διαδίδονται μόνο σε εξουσιοδοτημένο κόμβου. .(Jasmair & Kumar 2012)

10.Συμπεράσματα

Το μέλλον των δικτύων ad hoc είναι πραγματικά εντυπωσιακό, καθώς δίνει την δυνατότητα για ασύρματο δίκτυο σε οποιαδήποτε στιγμή και οποιοδήποτε χώρο. Εξετάζοντας τα χαρακτηριστικά των ad hoc δικτύων παρατηρήσαμε ότι η αρχιτεκτονική τους είναι με τέτοιο τρόπο δομημένη ώστε να είναι επιρρεπής σε κινδύνους στο τομέα της ασφάλειας σε μεγαλύτερο βαθμό από ότι τα ενσύρματα δίκτυα. Έτσι λοιπόν θα πρέπει να μελετήσουμε λεπτομερώς την καθεμία κατηγορία απειλής της ασφαλείας του δικτύου και να προτείνουμε αποτελεσματικούς τρόπους αντιμετώπισης των επιθέσεων. Θα πρέπει λοιπόν να προσπαθήσουμε να εξερευνήσουμε βαθύτερα την περιοχή αυτή που μειονεκτούν τα ad hoc δίκτυα.

Βιβλιογραφία

- ✓ mobile ad hoc network (MANET) . (n.d.). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Mobile_ad_hoc_network
- ✓ Jangra, A., Goel, N., Bhatia, P., & Bhatia, K. (2010). Security Aspects in Mobile Ad Hoc Networks. *International Journal og Neural Networks*.
- ✓ Li, W., & Joshi, A. (2008). Security issues in mobile ad hoc networks-a survey. *Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County*. Retrieved from http://citeseerx.ist.psu.edu/
- ✓ Zhou, Y., Xia, C., Wang, H., & Qi, J. (2009). Research on Survivability of Mobile Ad-hoc Network.*J. Software Engineering and Applications*. Retrieved from http://www.SciRP.org/journal/jsea
- ✓ Jaiswal, P., & Kumar, R. (2012). Preventing Manet From Attacks. *International Journal of Neural Networks*. Retrieved from http://www.bioinfopublication.org/
- ✓ Kunar, G., Kunar, A., & Kunar, P. (2012). Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review. *International Journal of Engineering and Advanced Technology (IJEAT)*.
- ✓ Lidong, Z., & Zygmnut, J. (1999). Securig Ad Hoc Network. *IEEE*.
- ✓ Jawandhiya, P. M., Ghonge, M. M., Ali, M., & Deshpande, J. (2010). A survey of Mobile Ad Hoc Network Attacks. *International Journal og Neural Networks*.
- ✓ Lima, M. N., Aldri, L. D. S., & Pujolle, G. (2009). A survey of Survivability in Mobile Ad Hoc Networks. *IEEE*.
- ✓ Francis, M., Sangeetha, M., & Sabari, A. (2013). A survey key Management Technique for Secure and Reliable Data Transmission in MANET. *International Journal of Advanced Research in Computer Science and Software Enginnering*.
- ✓ Yuan, Y., Chunhe, X., Wang, H., & Jianzhong, Q. (2009). Research on Survivability of MANET. *SciRes*.
- ✓ Acosta, J. C., & Medina, B. G. (n.d.). Survivability Prediction of Ad Hoc Networks under Attack. Retrieved from http://www/jaimeacosta.info/
- ✓ Peng SC, Jia WJ, Wang GJ. Survivability evaluation in large-scale mobile ad-hoc networks. JOURNAL OF COMPUTERSCIENCE AND TECHNOLOGY
- ✓ Azni, A., Ahmad, R., & Azri, Z. (2011). Resilence and Survivability in Manet: Discipline, Issue and Challenge. *ICOCI*.
- ✓ Dabideen, S., Bradley R., S., & Aceves, J. G. (2009). An End-to-End Solution for Secure and Survivable Routing in MANETS. *IEEE*.
- ✓ Wang, T., Huang, C., Xiang, K., & Zhou, K. (n.d.)(2010). Survivability Evaluation for MANET based on Path Reliability. *IEEE*.
- ✓ Lima, M. N., Silva, H. W., Pujolle, G., & Santos, A. (2008). Survival multipath routin for Manets. *IEEE*.
- ✓ Azni, A., Ahmad, R., & Noh, Z. (2013). Suvivability Modeling and Analysis of Mobile Ad Hoc Network with correlated Node Behavior. *SciVerse ScienceDirect*.
- ✓ Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. (n.d.). Trust prediction and trust-based source routing in mobile ad hoc networks. *SciVerse ScienceDirect*. 2013
- ✓ Cho, J.-H., Swami, A., & Chen, I.-R. (2012). Modeling and analysis of trust management with trust chain optimization in MANETS. *SciVerse ScienceDirect*.
- ✓ Ahmad, M., & Mishra, D. K. (2013). Critical Node Detection in Large scale Mobile Ad hoc Networks. *International Journal of Computer Applications*.

- ✓ Cho, J.-H., & Chen, I.-R. (2009). On the Tradeoff between Altrism and Selfishness in MANET Trust Management.
- ✓ Prasant Mohapatra, Chao Gui, Jian L,2009, Group Communication
- ✓