ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. **«Ασφάλεια Ψηφιακών Συστημάτων»**

Technical Analysis: Delving into MANET Networks, Routing Protocols, Vulnerability Assessment, and Security Considerations

---

Ξενοφών Ακρίτας
Επιβλεπων: Κώστας Λαμπρινουδάκης

Ιούνιος, 2024

The questions are many, the answers even more, there is only one truth..leave the ordinary and you will find it..the truth is out there

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία αναπτύσσεται στο πλαίσιο του προγράμματος μεταπτυχιακών σπουδών, Ασφάλειας Ψηφιακών Συστημάτων του τμήματος των Ψηφιακών Συστημάτων του πανεπιστημίου Πειραιώς. Οι ασύρματες επικοινωνίες ολοένα έχουν αρχίσει να εισάγωνται στις ζώης μας με την άνοδο της τεχνολογίας καθώς όλο και περισσότεροι χρήστες χρησιμοποιούν ασύρματες συσκευές (πχ smart phones) τους για την πρόσβαση στο internet. Στην παρούσα διπλωματική εργασία θα αναλύσουμε τρόπους επιθέσεων κατά τους οποιούς μια ασύρματη συσκευή βρίσκεται σε ένα decentralize pool απο mobile συσκευές. Θα γίνει περετέρω ανάλυση για το τι είναι τα δίκτυα MANET ,πως λειτουργούν καθώς επίσης και στα είδη δικτύων MANET που υπάρχουν καθώς και τα προτώκολλα με τα οποία μπορεί να πραγματοποιηθεί το routing. Τέλος έχουμε περαιτέρω ανάλυση στα SD-MANET, όπου εξαρχής θα γίνει παρουσίαση και ανάλυση για τα SDN όσον αφορά τον τρόπο λειτουργείας τους αλλά και τα key components της αρχιτεκτονική τους. Επιπρόσθετα θα ακολουθήσει παράδειγμα αρχιτεκτονικής των SD-MANET δικτύων αλλά και πως μπορεί να παίξει σημαντικό ρόλο στην μείωση των ευπαθειών.

ABSTRACT

This thesis is developed in the context of the Master's degree program in Digital Systems Security of the Department of Digital Systems of the University of Piraeus. Wireless communications have increasingly begun to enter our lives with the rise of technology as more and more users use their wireless devices (e.g. smart phones) to access the internet. In this thesis we will analyze ways of attacks in which a wireless device is located in a decentralize pool of mobile devices. Further analysis will be done on what MANET networks are, how they work and also on the types of MANET networks that exist and the protocols with which routing can be performed. Finally we have further analysis on SD-MANET, where from the beginning we will present and analyze SDN in terms of how they work and the key components of their architecture. In addition, we will follow an example of SD-MANET network architecture and how it can play an important role in reducing vulnerabilities.

Πίνακας Περιεχομένων

Εισαγωγή

1.1 Ασύρματες κινητές επικοινωνίες

Ο όρος ασύρματη επικοινωνία εισήχθη τον 19ο αιώνα και έκτοτε,η τεχνολογία των ασύρματων επικοινωνιών έχει εξελιχθεί αξιοσημείωτα. Νέες ασύρματες λύσεις επικοινωνίας υιοθετούνται συνεχώς τις τελευταίες δεκαετίες και η ασύρματη τεχνολογία έχει γίνει βασικό μέρος της ζωής. Σήμερα, η ασύρματη τεχνολογία επικοινωνιών περιλαμβάνει μια ποικιλία συσκευών και τεχνολογιών που κυμαίνονται από από έξυπνα τηλέφωνα έως υπολογιστές, τηλεοράσεις, φορητούς υπολογιστές, τεχνολογία Bluetooth, δορυφόρους και κ.ο.κ. Η ασύρματη επικοινωνία μπορεί να οριστεί ως η μεταφορά πληροφοριών μεταξύ μιας πηγής και ενός προορισμού που χρησιμοποιεί τον "χώρο" ως μέσο διάδοσης του σήματος, χωρίς την ανάγκη για καλώδιο. Τα κύρια στάδια της ασύρματης μετάδοσης είναι η παραγωγή ενός ηλεκτρομαγνητικού σήματος που αντιπροσωπεύει την επιθυμητή πληροφορία από την πηγή, ή πομπού, η διάδοση των ραδιοκυμάτων στο χώρο και η εκτίμηση της πληροφοριών από το λαμβανόμενο σήμα από τον προορισμό, ή αλλιώς, τον δέκτη. Υπάρχουν πολλά πλεονεκτήματα των ασύρματων επικοινωνιών και δικτύων, σε σύγκριση με τις ενσύρματες λύσεις. Ορισμένα από τα σημαντικότερα πλεονεκτήματα περιλαμβάνουν την κινητικότητα, την αυξημένη αξιοπιστία, η ευκολία εγκατάστασης, η ταχεία αποκατάσταση από καταστροφές και το χαμηλότερο κόστος. Η Ασύρματη τεχνολογία έχει επίσης πολλές εφαρμογές σε τομείς, όπως περιβάλλοντα γραφείων,υπηρεσίες υγείας, στρατιωτικές επιχειρήσεις, οικιακή ψυχαγωγία και πολλά άλλα. Η πιο συνηθέστερα χρησιμοποιούμενο σύστημα ασύρματης επικοινωνίας είναι ίσως το κινητό σύστημα επικοινωνίας.Υπάρχουν διάφοροι τύποι ασύρματων δίκτυα. Όπως τα κυψελοειδή δίκτυα, τα δορυφορικά δίκτυα και κινητά δίκτυα ad hoc και πολλά άλλα. Στο πλαίσιο αυτων τα ασύρματα δίκτυα έχουν πολλές κατηγορίες ένα από αυτά είναι το δίκτυο ad hoc (WANET) που χρησιμοποιεί πολλαπλά συνδεδεμένη ραδιοαναμετάδοση καθώς λειτουργεί χωρίς την υποστήριξη κάποιας σταθερής υποδομής όπως στα κλασσικά ασύρματα δίκτυα (infrastructure mode). Τα WANET χαρακτηρίζονται από την αποκεντρωμένη, αυτο-οργανωμένη και ad-hoc φύση τους, γεγονός που τα καθιστά κατάλληλα για δυναμικά και κινητά σενάρια όπου τα παραδοσιακά δίκτυα μπορεί να είναι ανεφάρμοστα. Ωστόσο ιδιαίτερη έμφαση θα πρέπει να δωθεί στην ασφάλεια αυτών δικτύων για την διασφάληση των πληροφοριών μεταξύ των χρηστών και των συσκευών.Υπάρχουν διάφορα είδη WANET, στην παρούσα εργασία θα αναλυθεί το SD-MANET και ακολουθηθεί μελέτη για τις κυριότερα σημεία ελέγχου και ευπαθειών κατά την υλοποίηση αυτών των δικτύων.

1.2 Στόχος της εργασίας

Στόχος της παρούσας διατριβής είναι να παράσχει μια ολοκληρωμένη ανάλυση των Κινητών Ad Hoc Δικτύων (MANETs) στο ευρύτερο πλαίσιο των Ασύρματων Ad Hoc Δικτύων (WANETs), εστιάζοντας στα πρωτόκολλα δρομολόγησής τους, στις προκλήσεις ασφαλείας που αντιμετωπίζουν και στις πιθανές λύσεις μέσω της υλοποίησης Κινητών Ad Hoc Δικτύων που καθορίζονται από λογισμικό (SD-MANETs). Η διατριβή ξεκινά με τη διερεύνηση των βασικών εννοιών, της αρχιτεκτονικής και των εφαρμογών των WANETs και MANETs, τονίζοντας τη σημασία τους στην παροχή αποκεντρωμένων, ευέλικτων και ταχέως αναπτύξιμων λύσεων δικτύωσης. Στη συνέχεια εξετάζει τα διάφορα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται στα MANETs, συμπεριλαμβανομένων των προληπτικών, αντιδραστικών και υβριδικών προσεγγίσεων, αξιολογώντας τις επιδόσεις τους, την επεκτασιμότητα και την καταλληλότητά τους για διαφορετικές συνθήκες δικτύου, δίνοντας έμφαση στις αντισταθμίσεις που συνεπάγεται κάθε τύπος πρωτοκόλλου. Στη συνέχεια διερευνώνται οι ευπάθειες ασφαλείας που ενυπάρχουν στα MANETs, αναλύοντας τις συνήθεις επιθέσεις, όπως οι επιθέσεις blackhole, wormhole, Sybil και denial-of-service (DoS), και αναλύοντας τον αντίκτυπό τους στην απόδοση του δικτύου και την ακεραιότητα των δεδομένων. Για την αντιμετώπιση αυτών των προκλήσεων, η παρούσα εργασία εισάγει την έννοια των Software-Defined Mobile Ad Hoc Networks (SD-MANETs) ως λύση στους περιορισμούς ασφάλειας και απόδοσης των παραδοσιακών MANETs.Εξετάζεται ο τρόπος με τον οποίο τα SD-MANET αξιοποιούν τις αρχές του Software-Defined Networking (SDN) για να βελτιώσουν την αποδοτικότητα της δρομολόγησης, την ασφάλεια και τη διαχείριση του δικτύου μέσω κεντρικού ελέγχου και προγραμματισμού. Με την ενσωμάτωση αυτών των πτυχών, η διατριβή αποσκοπεί στην παροχή μιας ολιστικής άποψης των MANETs, από τις θεμελιώδεις αρχές και τους μηχανισμούς δρομολόγησης έως τις προκλήσεις ασφαλείας και τις πιθανές βελτιώσεις μέσω των SD-MANETs, συμβάλλοντας τελικά στη βαθύτερη κατανόηση και την εξέλιξη της τεχνολογίας των κινητών ad hoc δικτύων.

1.3 Η φύση τους προβλήματος

Η φύση του προβλήματος που εξετάζεται στην παρούσα διατριβή περιστρέφεται γύρω από τις εγγενείς προκλήσεις και τα τρωτά σημεία που σχετίζονται με τα κινητά δίκτυα ad hoc (MANET). Τα MANETs αντιμετωπίζουν σημαντικά προβλήματα λόγω των δυναμικών τοπολογιών τους, οι οποίες περιπλέκουν την ανάπτυξη και τη συντήρηση αποδοτικών πρωτοκόλλων δρομολόγησης, καθώς η δομή του δικτύου αλλάζει συχνά. Επιπλέον, είναι ιδιαίτερα ευάλωτα σε απειλές ασφάλειας, όπως επιθέσεις blackhole, wormhole, Sybil και επιθέσεις άρνησης παροχής υπηρεσιών (DoS), λόγω της αποκεντρωμένης αρχιτεκτονικής τους και της έλλειψης σταθερής υποδομής. Αυτά τα τρωτά σημεία ασφαλείας μπορούν να διαταράξουν τις λειτουργίες του δικτύου, να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων και να υποβαθμίσουν τη συνολική απόδοση. Επιπλέον, οι κόμβοι στα MANET έχουν συχνά περιορισμένους πόρους, όπως η ισχύς της μπαταρίας, η υπολογιστική ικανότητα και το εύρος ζώνης, προσθέτοντας ένα ακόμη επίπεδο πολυπλοκότητας στο σχεδιασμό ισχυρών πρωτοκόλλων δρομολόγησης και μηχανισμών ασφαλείας. Η απουσία κεντρικού ελέγχου στα παραδοσιακά MANET καθιστά δύσκολη την επιβολή συνεπών πολιτικών

ασφαλείας, την αποτελεσματική διαχείριση των πόρων και την ταχεία αντίδραση στις αναδυόμενες απειλές. Για την αντιμετώπιση αυτών των ζητημάτων, η διατριβή προτείνει τη διερεύνηση των Software-Defined Mobile Ad Hoc Networks (SD-MANETs) ως πιθανή στρατηγική μετριασμού. Αξιοποιώντας τις αρχές του Software-Defined Networking (SDN) όπως αναφέρθηκε και στο 1.2, τα SD-MANETs εισάγουν κεντρικό έλεγχο και δυνατότητα προγραμματισμού, ενισχύοντας την αποτελεσματικότητα της δρομολόγησης, την ασφάλεια και τη διαχείριση του δικτύου, παρέχοντας έτσι ένα πιο ευέλικτο, ασφαλές και διαχειρίσιμο περιβάλλον δικτύωσης για την αντιμετώπιση των περιορισμών των παραδοσιακών MANETs. Για την εκτέλεση μιας αξιολόγησεις κινδύνου για SD-MANET, θα πρέπει να ακολουθηθεί μια δομημένη προσέγγιση που περιλαμβάνει τον εντοπισμό πιθανών απειλών, ευπαθειών και των πιθανών επιπτώσεών τους, την αξιολόγηση της πιθανότητας και της σοβαρότητας αυτών των κινδύνων και την ανάπτυξη στρατηγικών μείωσεις του κινδύνου αυτού. Είναι σημαντικό να ληφθεί υπόψη το κάθε use case ξεχωριστά, το μέγεθος του δικτύου και τους διαθέσιμους πόρους κατά την αξιολόγηση και την αντιμετώπιση αυτών των κινδύνων. Οι τακτικές ενημερώσεις και αναθεωρήσεις των μέτρων ασφαλείας είναι επίσης απαραίτητες σε αυτό το διαρκώς μεταβαλλόμενο περιβάλλον.

1.4 Περιεχόμενα Κεφαλαίων

Ακολουθεί σύντομη επισκόπηση των θεμάτων που καλύπτονται σε καθένα από τα ακόλουθα κεφάλαια:

Κεφάλαιο 2: WANET/MANET Networks and Types – Σε αυτό το κεφάλαιο θα γίνει ανάλυση των διαφόρων τύπων WANET με έμφαση το MANET , έπειτα θα παρουσιαστούν βασικές έννοιες του SD-MANET και ανάλυση του τρόπου λειτουργείας του

Κεφαλαιο 3: Routing πρωτόκολλα – Σε αυτό το κεφάλαιο θα πραγματοποιηθεί ανάλυση των προωτοκόλων που χρησιμοποιούνται για routing

Κεφάλαιο 4: Επιθέσεις σε MANET δίκτυα – Σε αυτό το κεφάλαιο θα γίνει ανάλυση των διαφόρων τύπων επιθέσεων στα δίκτυα MANET

Κεφάλαιο 5: SD-MANET A possible mitigation – Σε αυτό το κεφάλαιο θα γίνει ανάλυση του SDN και θα διατυπωθούν βασικοί ορισμοί και έννοιες σχετικά με τον τρόπο λειτουργίας τους ως MANET δίκτυο.

Κεφάλαιο 6: Συμπεράσματα – Το κεφάλαιο αυτό ολοκληρώνει την παρούσα διπλωματική συνοψίζοντας την εργασία, συζήτηση και διεξαγωγή ερωτήσεων των συμπερασμάτων που προέκυψαν από τα προηγούμενα κεφάλαιο.

Κεφάλαιο 2

WANET/MANET

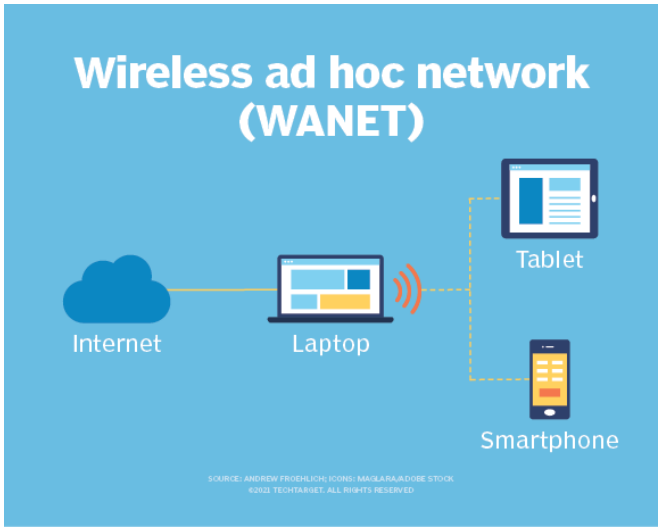
2.1 Βασικές πληροφορίες WANET δικτύων

Ένα ασύρματο δίκτυο ad-hoc (WANET) είναι ένας τύπος τοπικού δικτύου (LAN) που δημιουργείται για να επιτρέπει τη σύνδεση δύο ή περισσότερων ασύρματων συσκευών μεταξύ τους χωρίς να απαιτείται τυπικός εξοπλισμός δικτυακής υποδομής, όπως router ή access point.

Στις περισσότερες περιπτώσεις, ένας υπολογιστής, φορητός υπολογιστής ή ένα smartphone με διεπαφή Wi-Fi χρησιμοποιείται για τη δημιουργία ενός δικτύου ad hoc (Σχήμα 1). Σε άλλες περιπτώσεις, συσκευές όπως οι ασύρματοι αισθητήρες έχουν σχεδιαστεί για να λειτουργούν κυρίως σε λειτουργία ad hoc.

Εικόνα ενός φορητού υπολογιστή συνδεδεμένου στο διαδίκτυο που μεταδίδει συνδεσιμότητα σε ένα smartphone και ένα tablet.

Επειδή οι συσκευές στο δίκτυο ad hoc μπορούν να έχουν άμεση πρόσβαση στους πόρους η μία της άλλης μέσω βασικών ομότιμων (P2P) ή point-to-multipoint λειτουργιών, οι κεντρικοί διακομιστές είναι περιττοί για λειτουργίες όπως η κοινή χρήση αρχείων ή η εκτύπωση. Σε ένα WANET, μια συλλογή συσκευών ή κόμβων, όπως ένας ασύρματος υπολογιστής ή ένα smartphone είναι υπεύθυνη για τις λειτουργίες του δικτύου, όπως η δρομολόγηση, η ασφάλεια, η διευθυνσιοδότηση και η διαχείριση κλειδιών.



Σχήμα 2.1. Σύνδεση συσκευών στο διαδίκτυο με χρήση δικτύου ad hoc.

2.2 Διαφορές και τύποι WANET - MANET

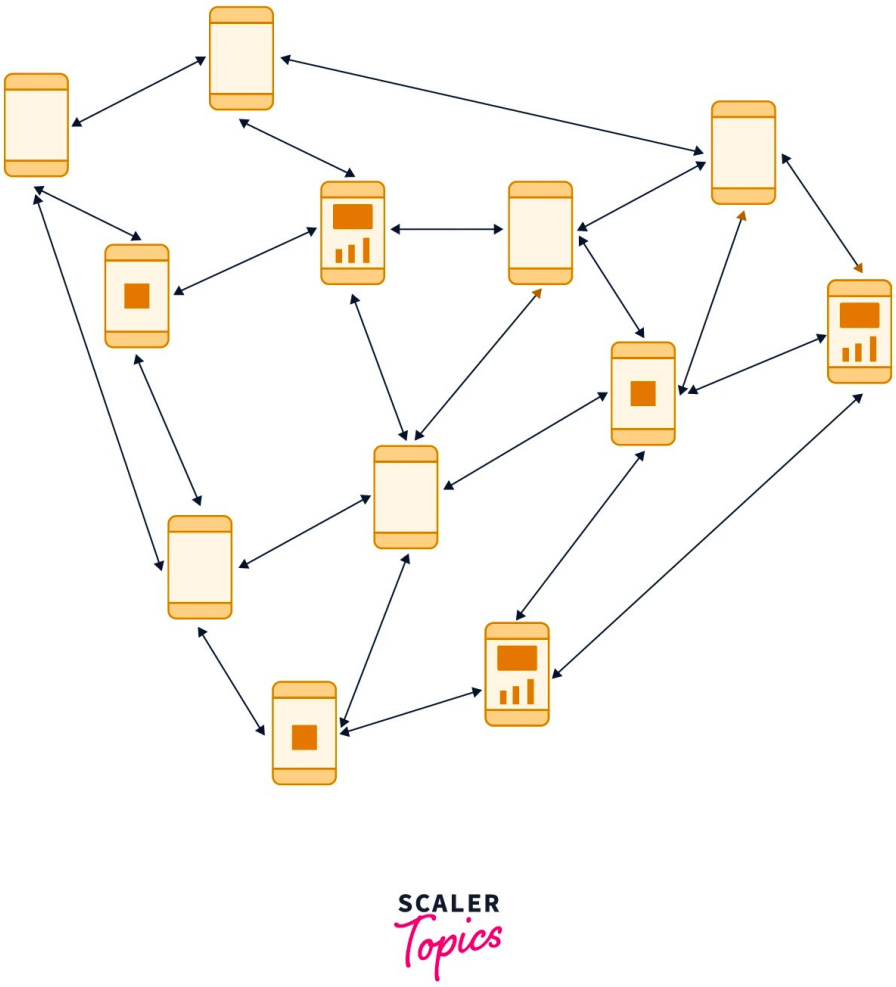
Ένα σημαντικό κομμάτι που πρέπει να τονιστεί είναι ότι το MANET είναι ένας τύπος WANET που δεν απαιτεί σταθερή υποδομή καθώς ένα από τα κύρια χαρακτηριστικά του είναι το mobillity των nodes. Στα WANET δίκτυα και συγκεκριμένα σε έναν άλλο τύπο WANET το WSN δεν είναι απαραίτητο να μην υπάρχει σταθερο infrastructure.

Υπάρχουν περισσότεροι τύποι από αυτούς που θα αναφερθούν στην εργασία, επιγραμματικά γίνεται αναφορά των σημαντικότερών τύπων MANET για την πληρότητα της εργασίας.

- **Vehicular Ad-Hoc Networks (VANETs) :** Το VANET είναι ένας τύπος δικτύων που δημιουργείται από την ιδέα της δημιουργίας ενός δικτύου αυτοκινήτων για μια συγκεκριμένη ανάγκη ή κατάσταση.
- **Wireless Mesh Networks :** Τα ασύρματα δίκτυα πλέγματος (WMN) αποτελούνται από δρομολογητές πλέγματος (mesh routers) και πελάτες πλέγματος (mesh client), όπου οι δρομολογητές πλέγματος έχουν ελάχιστη κινητικότητα και αποτελούν τη ραχοκοκαλιά των WMN.
- **Wireless Body Area Networks (WBANs):** Τα WBAN αφορούν την επικοινωνία μεταξύ συσκευών που είναι τοποθετημένες πάνω ή μέσα στο ανθρώπινο σώμα, συχνά για την παρακολούθηση της υγειονομικής περίθαλψης.
- **Flying Ad-Hoc Networks (FANETs):** Τα FANET αφορούν την επικοινωνία μεταξύ ιπτάμενων συσκευών, όπως τα μη επανδρωμένα αεροσκάφη ή τα μη επανδρωμένα εναέρια οχήματα (UAV).
- **Software Defined Ad-Hoc Networks – SD-MANET:** Τα Software Defined Ad-Hoc Networks (SD-MANETs) αντιπροσωπεύουν ένα καινοτόμο παράδειγμα που συνδυάζει την ευελιξία των κινητών Ad Hoc δικτύων (MANETs) με τη δυνατότητα προγραμματισμού και τον κεντρικό έλεγχο του Software-Defined Networking (SDN). Εκτενέστερη ανάλυση στο κεφαλαιο 5.

2.3 Τι είναι ένα MANET Δίκτυο

Το MANET είναι ακρωνύμιο του Mobile Adhoc Network, επίσης γνωστό ως ασύρματο δίκτυο Adhoc ή Adhoc wireless network, το οποίο είναι ένα περιβάλλον δικτύωσης με δυνατότητα δρομολόγησης που βασίζεται σε ένα ad hoc δίκτυο επιπέδου σύνδεσης. Αποτελούνται από μια συλλογή κινητών κόμβων που συνδέονται ασύρματα σε ένα αυτορυθμιζόμενο, self-healing δίκτυο χωρίς σταθερή υποδομή. Επειδή η αρχιτεκτονική του δικτύου αλλάζει τακτικά, οι κόμβοι MANET επιτρέπεται να μετακινούνται τυχαία. Κάθε κόμβος ενεργεί ως δρομολογητής, προωθώντας την κυκλοφορία σε άλλους κόμβους του δικτύου.Τα MANET χαρακτηρίζονται από τη δυναμική τοπολογία και την αποκεντρωμένη φύση τους.



Σχήμα 2.2. Σύνδεση συσκευών με χρήση δικτύου MANET

Τα MANET μπορούν να λειτουργούν μόνα τους ή ως μέρος ενός ευρύτερου διαδικτύου. Με τη συμπερίληψη ενός ή περισσότερων διαφορετικών πομποδεκτών μεταξύ των κόμβων, δημιουργούν μια ιδιαίτερα δυναμική αυτόνομη τοπολογία. Η θεμελιώδης δυσκολία για το MANET είναι να εξοπλιστεί κάθε συσκευή με τις απαραίτητες πληροφορίες για τη σωστή δρομολόγηση πακέτων. Τα MANET είναι peer-2-peer, αυτοσχηματιζόμενα, αυτοθεραπευόμενα δίκτυα που συνήθως συνδέονται σε ραδιοσυχνότητες (30MHz-5GHz). Αυτό μπορεί να χρησιμοποιηθεί στην οδική ασφάλεια με διάφορους τρόπους, συμπεριλαμβανομένων αισθητήρων για το περιβάλλον, το σπίτι, την υγεία, τις επιχειρήσεις ανακούφισης από καταστροφές, την αεράμυνα/χερσαία/ναυτική άμυνα, τα όπλα, τη ρομποτική κ.ο.κ.

Ad hoc είναι μια λειτουργία επικοινωνίας (ρύθμιση) στο λειτουργικό σύστημα των Windows/Linux που επιτρέπει στις μηχανές να αλληλεπιδρούν απευθείας χωρίς τη χρήση δρομολογητή.

2.4 Πλεονεκτήματα MANET

i). Παρέχουν πρόσβαση σε πληροφορίες και υπηρεσίες ανεξαρτήτως γεωγραφικής θέσης. Αυτό είναι εφαρμόζεται σε στρατιωτικές ή αστυνομικές ασκήσεις, επιχειρήσεις ανακούφισης από καταστροφές, επιχειρήσεις σε χώρους ναρκοπεδίων και επείγουσες επιχειρηματικές συναντήσεις, όπου απαιτείται άμεση επικοινωνία.

ii). Τα δίκτυα αυτά μπορούν να εγκατασταθούν σε οποιοδήποτε τόπο και χρόνο. Μπορούν να εγκατασταθούν χωρίς καλώδια ή βάση σταθμούς και οι κόμβοι είναι ελεύθεροι να μετακινούνται τυχαία και να οργανώνονται αυθαίρετα- έτσι το η ασύρματη τοπολογία των δικτύων μπορεί να αλλάζει γρήγορα και απρόβλεπτα. Οι κινητές συσκευές στα δίκτυο μπορούν να εγκαταλείπουν ή να εντάσσονται στο δίκτυο κατά βούληση.

iii). Τα δίκτυα λειτουργούν χωρίς καμία προϋπάρχουσα υποδομή. Αυτό καθιστά τα MANETs δαπανηρά αποτελεσματικές για περιοχές όπου δεν υπάρχουν τυποποιημένες υποδομές επικοινωνίας. Οι ιδιοκτήτες των συσκευών που είναι εξοπλισμένες με MANET μπορούν να επικοινωνούν μεταξύ τους, να μοιράζονται δεδομένα και βίντεο ροής.

iv) Η χαμηλή κατανάλωση ενέργειας είναι ένα άλλο δυνατό σημείο για τα MANETs. Οι περισσότερες συσκευές που χρησιμοποιούνται είναι επομένως είναι φορητές, καθιστώντας την κινητικότητα εύκολη και τις συσκευές προσιτές. Παραδείγματα είναι τα τηλέφωνα με Bluetooth, οι φορητοί υπολογιστές.

2.5 Challenges στα MANET Δίκτυα

Ορισμένες προκλήσεις που αντιμετωπίζουν τα κινητά δίκτυα ad hoc για την αποτελεσματική παροχή υπηρεσιών περιλαμβάνουν:

1. Η δρομολόγηση(Routing) είναι μια κεντρική λειτουργία σε κάθε δίκτυο. Στα ad hoc δίκτυα, η δρομολόγηση θέτει δύο συγκεκριμένες προκλήσεις. Πρώτον, η δρομολόγηση στα παραδοσιακά δίκτυα (παραδείγματα: το Διαδίκτυο και τα κυψελοειδή δίκτυα) αποσκοπεί στη γρήγορη διάδοση των αλλαγών στην τοπολογία ή την προσβασιμότητα, δημιουργώντας έτσι σταθερά δίκτυα, ενώ στα κινητά ad hoc δίκτυα, η τοπολογία αλλάζει συνεχώς και θεωρείται ασταθής. Δεύτερον, οι παραδοσιακές λύσεις δρομολόγησης βασίζονται σε κάποια μορφή κατανεμημένων βάσεων δεδομένων δρομολόγησης, που συντηρούνται από τους χειριστές είτε στους κόμβους των δικτύων είτε σε εξειδικευμένους κόμβους διαχείρισης. Στο κινητά δίκτυα ad hoc, οι κόμβοι δεν μπορεί να θεωρηθεί ότι διαθέτουν μόνιμη αποθήκευση δεδομένων και δεν είναι πάντα αξιόπιστοι .
2. Διαχείριση κινητικότητας(Mobility Management:): Ένα δίκτυο πρέπει να διαχειρίζεται την κινητικότητα των τερματικών του, και ως εκ τούτου να είναι σε θέση να εντοπίζει οποιοδήποτε από αυτά. Ειδικότερα, εάν ένα τερματικό θέλει να επικοινωνήσει με ένα άλλο, αυτό θα χρησιμοποιήσει τη διεύθυνση του τελευταίου- το δίκτυο θα πρέπει να το εντοπίσει με κάποιο τρόπο. Το απλή λύση της μετάδοσης ενός μηνύματος τηλεειδοποίησης σε όλο το δίκτυο δεν είναι εφικτή. Για το παράδειγμα, στα κυψελοειδή δίκτυα, η θέση των κινητών σταθμών αποθηκεύεται σε κεντρικούς διακομιστές.

   Το self-organised των δικτύων ad hoc αποκλείει την ύπαρξη τέτοιων εξυπηρετητών, οδηγώντας σε άμεση απώλεια/εντοπισμό κάθε κόμβου μόλις βγει εκτός της εμβέλειας του άμεσου δικτύου.
3. Διευθύνσεις IP (Internet Protocol): Για τα μικρά κινητά δίκτυα ad hoc, οι διευθύνσεις είναικατανέμονται με τον παραδοσιακό τρόπο, με ένα πρόθεμα IP που προσδιορίζει το κινητό δίκτυο ad hoc. Για τοδίκτυα μεγάλης κλίμακας, η κατανομή διευθύνσεων με βάση την τοπολογία που χρησιμοποιείται σήμερα στο Διαδίκτυο μπορεί ναδεν είναι η βέλτιστη. Αντίθετα, μια διεύθυνση κόμβου πρέπει να ερμηνεύεται ως σταθερό αναγνωριστικό κόμβου,το οποίο δεν φέρει συγκεκριμένες τοπολογικές πληροφορίες.
4. Το επίπεδο μεταφοράς(Transport Laye) των ad hoc δικτύων απαιτεί επίσης προσοχή. Μετάδοση και έλεγχος Protocol (TCP) σε ad hoc δίκτυα μπορεί να υποβαθμιστεί σημαντικά, καθώς το TCP ερμηνεύει τις απώλειες ως σήμα συμφόρησης και αυτό μειώνει αρνητικά τον ρυθμό αποστολής του, ενώ τα ασύρματα οι ασύρματες συνδέσεις μπορεί να

παρουσιάζουν προσωρινά υψηλά ποσοστά απωλειών λόγω σφαλμάτων μετάδοσης που δεν σχετίζονται με συμφόρηση.

5. Ραδιοδιεπαφή(Radio Interface): αυτή μπορεί να σχεδιαστεί με διάφορους τρόπους, με βάση τις απαιτήσεις ενόςσυγκεκριμένου συστήματος.Τα ζητήματα που πρέπει να ληφθούν υπόψη περιλαμβάνουν:
    - Η μείωση της ισχύος του σήματος ως προς το τετράγωνο της απόστασης.
    - Ορισμένα από τα παραδοσιακά πρωτόκολλα πολλαπλής πρόσβασης που χρησιμοποιούνται για τα ενσύρματα LAN δεν μπορούν να χρησιμοποιηθούν, παράδειγμα: η ανίχνευση σύγκρουσης δεν ενδείκνυται επειδή ένας κόμβος δεν είναι συνήθως σε θέση να ακούσει ενώμεταδίδει.

6. Ασφάλεια(Security): αυτό είναι κρίσιμης σημασίας για τα περισσότερα δίκτυα, και τα κινητά ad hoc δίκτυα δεν είναιεξαίρεση.Μπορούν να απαιτηθούν διάφορα χαρακτηριστικά ασφαλείας, όπως η διαθεσιμότητα της υπηρεσίας παράτις επιθέσεις άρνησης παροχής υπηρεσιών, η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικοποίηση και η μη αποκήρυξη.Η εγγύηση αυτών των χαρακτηριστικών αποτελεί σημαντική πρόκληση. *βλέπε κεφ.6*
7. Η διαχείριση ισχύος(Power Management) είναι σχεδόν πάντα ένα δύσκολο ζήτημα στα ασύρματα δίκτυα. Στην περίπτωση των διαφημιστικών hoc δικτύων, υπάρχουν ουσιαστικά δύο ανησυχίες:
    - Η ισχύς πρέπει να ρυθμίζεται λεπτομερώς προκειμένου να μεγιστοποιείται η απόδοση του δικτύου: όσο υψηλότερη είναι ηισχύς, τόσο μεγαλύτερες είναι οι εμβέλειες μετάδοσης του κόμβου, αλλά και τόσο μεγαλύτερες είναι οι παρεμβολές απόαπό άλλα σήματα. Η αντιστάθμιση επιτυγχάνεται όταν υπάρχει κατά μέσο όρο ακριβώς ένα πακέτο σε διαμετακόμιση πάνω απόκάθε άλμα

Κεφάλαιο 3

Πρωτόκολλα Δρομολόγησης (Routing Protocols)

3.1 Ad hoc Routing Protocols

Η δρομολόγηση στα ασύρματα δίκτυα Ad hoc είναι μια διαδικασία δύο βημάτων: Πρώτον, η εύρεση της διαδρομής μεταξύ πηγής και προορισμού και δεύτερον η μετάδοση πακέτων δεδομένων. Τα πρωτόκολλα δρομολόγησης για τα παραδοσιακά ενσύρματα δίκτυα δεν μπορούν να εφαρμοστούν άμεσα στα MANET λόγω των περιορισμών και των χαρακτηριστικών τους, όπως η δυναμική τοπολογία, το περιορισμένο εύρος ζώνης, η απρόβλεπτη χωρητικότητα των συνδέσεων και ο περιορισμός της ενέργειας. Στο πρόσφατο παρελθόν έχουν προταθεί πολλά πρωτόκολλα δρομολόγησης για MANETs για την ανακάλυψη και τη διατήρηση διαδρομών. Η δρομολόγηση βρίσκει κατάλληλες διαδρομές μεταξύ ζευγών κόμβων πηγής και προορισμού, που ενδεχομένως αποτελούνται από έναν αριθμό ενδιάμεσων κόμβων. Ανάλογα με το υποκείμενο μοντέλο επικοινωνίας, τα πρωτόκολλα δρομολόγησης μπορούν να διακριθούν σε μονοεκπομπή, πολυεκπομπή και δρομολόγηση εκπομπής. Όλοι οι παραπάνω τύποι έχουν έναν αποστολέα, αλλά διαφορετικό αριθμό κόμβων προορισμού και οι κόμβοι προορισμού καθορίζονται με διαφορετική μεθοδολογία σε κάθε έναν από τους παραπάνω τύπους. Στη δρομολόγηση μονοαποστολής, υπάρχει ακριβώς ένας συγκεκριμένος κόμβος προορισμού, ενώ στη δρομολόγηση μονοαποστολής, τα πακέτα παραδίδονται σε ακριβώς έναν προορισμό μεταξύ πολλών πιθανών προορισμών.Η δρομολόγηση πολλαπλής διανομής αποσκοπεί στον καθορισμό μονοπατιών για την παράδοση πακέτων δεδομένων σε πολλαπλούς προορισμούς που συγκεντρώνονται σε μια ομάδα. Η δρομολόγηση εκπομπής αποσκοπεί στην παράδοση πακέτων δεδομένων σε όλους τους κόμβους του δικτύου

3.2 Χαρακτηριστικά των πρωτοκόλλων δρομολόγησης

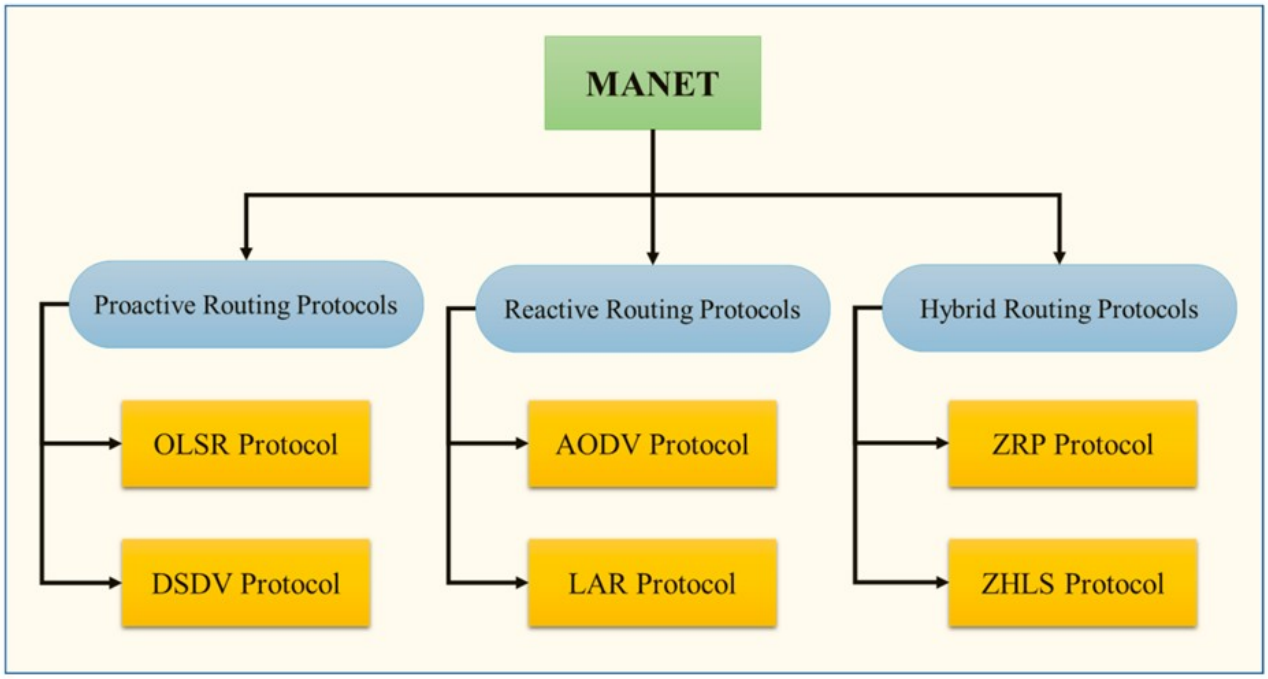
Τα παραδοσιακά πρωτόκολλα δρομολόγησης για σταθερά ενσύρματα δίκτυα, όπως το Πρωτόκολλο Πληροφοριών Δρομολόγησης (RIP) και το Open Shortest Path First (OSPF) , δεν είναι κατάλληλα για τα MANETs, λόγω των built-in χαρακτηριστικά τους, και παρουσιάζουν κακές επιδόσεις.

Ένα πρωτόκολλο δρομολόγησης για MANET θα πρέπει να επιδεικνύει τα ακόλουθα χαρακτηριστικά:

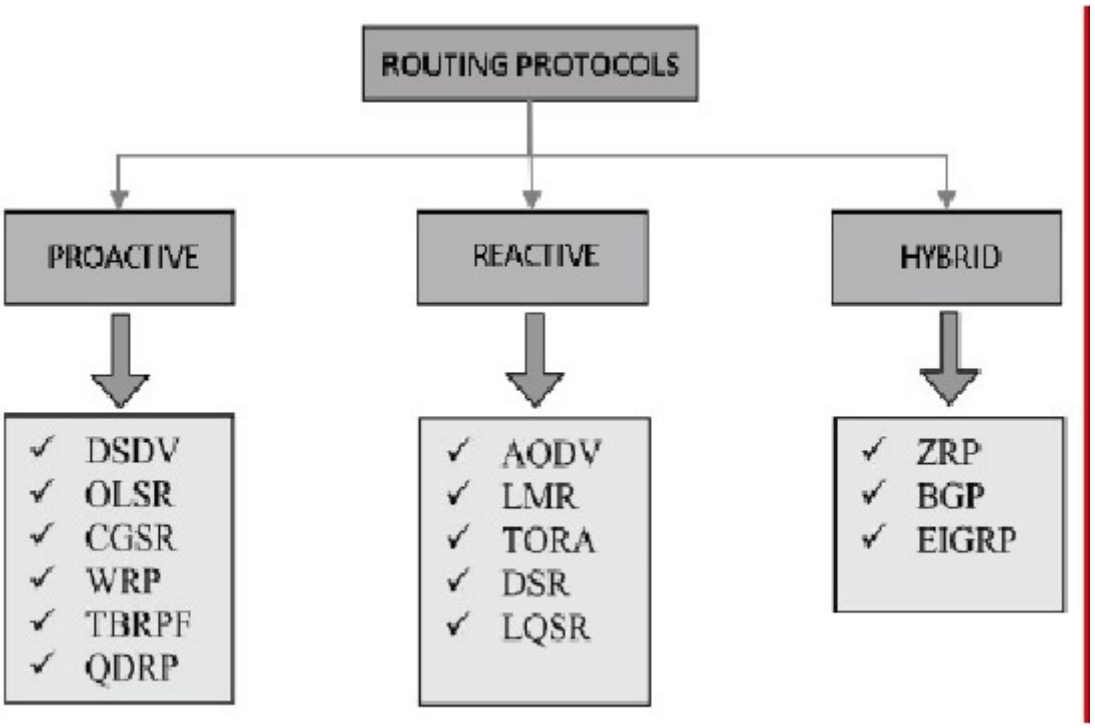
- Θα πρέπει να είναι πλήρως κατανεμημένο και να μην εξαρτάται από κεντρικό κόμβο ελέγχου- η κεντρική δρομολόγηση συνεπάγεται υψηλή επιβάρυνση ελέγχου και δεν είναι
- Στα MANET οι κόμβοι μπορούν να εισέλθουν ή να εξέλθουν από το δίκτυο ανά πάσα στιγμή και λόγω της κινητικότητάς τους το δίκτυο μπορεί να πάρει Ως εκ τούτου το πρωτόκολλο δρομολόγησης πρέπει να προσαρμόζεται στις συχνές αλλαγές της τοπολογίας.
- Για να βελτιωθεί η συνολική απόδοση, το πρωτόκολλο δρομολόγησης θα πρέπει να είναι απαλλαγμένο από βρόχους και από παρωχημένες διαδρομές, ώστε να αποφεύγεται η σπατάλη
- Θα πρέπει επίσης να χρησιμοποιεί τόσο τις μονόδρομες συνδέσεις, όσο και τις αμφίδρομες.
- Θα πρέπει να είναι εντοπισμένο και να περιλαμβάνει ελάχιστο αριθμό κόμβων στον υπολογισμό και τη συντήρηση της διαδρομής.
- Θα πρέπει να ελαχιστοποιεί τον αριθμό των συγκρούσεων πακέτων για τη μείωση των απωλειών
- Θα πρέπει να συγκλίνει σε βέλτιστες διαδρομές γρήγορα, μόλις το δίκτυο αποκτήσει
- Θα πρέπει να χρησιμοποιεί αποτελεσματικά τους σπάνιους πόρους, όπως το εύρος ζώνης, την επεξεργαστική ισχύ, τη μνήμη και την ισχύ της μπαταρίας.
- Θα πρέπει να ενσωματώνει ποιότητα υπηρεσίας (QoS) σύμφωνα με την εφαρμογή.

3.3 Routing Classification

Σε ένα MANET, λόγω της περιορισμένης εμβέλειας ασύρματης μετάδοσης, απαιτείται συχνά ένας ή περισσότεροι ενδιάμεσοι κόμβοι για την προώθηση πακέτων μεταξύ των κινητών κόμβων πηγής και προορισμού. Ως εκ τούτου, κάθε κόμβος στο δίκτυο αναμένεται να έχει τη δυνατότητα δρομολόγησης. Λόγω των διακυμάνσεων των ασύρματων καναλιών και της μετακίνησης των κινητών κόμβων, το MANET έχει εξαιρετικά δυναμική τοπολογία. Λαμβάνοντας υπόψη τις διάφορες απαιτήσεις των εφαρμογών και τα ζητήματα απόδοσης, στη βιβλιογραφία αναφέρονται διάφορες τεχνικές δημιουργίας και διατήρησης διαδρομών για αξιόπιστη μεταφορά δεδομένων από την πηγή στον προορισμό , οι οποίες μπορούν να ταξινομηθούν με πολλούς διαφορετικούς τρόπους



Σχήμα 3.1. Most applied routing algorithms



Σχήμα 3.2. Most applied routing algorithms in total

3.3.1 Reactive routing protocols

Τα Reactive πρωτόκολλα δρομολόγησης καθορίζουν τις διαδρομές μόνο όταν ένας κόμβος πηγής έχει δεδομένα να στείλει σε έναν κόμβο προορισμού. Εάν η διαδρομή από την πηγή προς τον απαιτούμενο προορισμό δεν είναι ήδη διαθέσιμη, ο κόμβος πηγής ξεκινά μια λειτουργία ανακάλυψης διαδρομής για να βρει τις απαραίτητες διαδρομές. Στη λειτουργία ανακάλυψης διαδρομής, ένα μήνυμα αίτησης διαδρομής (RREQ) εκπέμπεται σε ολόκληρο το δίκτυο και ένα μήνυμα απάντησης διαδρομής (RREP) από ένα υποσύνολο κόμβων αποστέλλεται πίσω στον κόμβο-πηγή. Η βέλτιστη διαδρομή από όλες τις διαθέσιμες διαδρομές χρησιμοποιείται για την εγκαθίδρυση σύνδεσης και τη μετάδοση δεδομένων και η επιλεγμένη διαδρομή χρησιμοποιείται μέχρι να καταστεί άκυρη ή να μην είναι διαθέσιμη ή να σπάσει. Τα DSR και AODV είναι τα πιο ευρέως χρησιμοποιούμενα πρωτόκολλα δρομολόγησης που βασίζονται στη στρατηγική On-Demand. Το κύριο πλεονέκτημα των Reactive προσεγγίσεων δρομολόγησης είναι η ικανότητά τους να παρέχουν διαδρομή αμέσως, όταν χρειάζεται. Τα Reactive πρωτόκολλα δρομολόγησης εξαλείφουν κάθε επιπλέον επιβάρυνση από τη διατήρηση στατικών πινάκων δρομολόγησης. Τα

πρωτόκολλα που ανήκουν σε αυτή την κατηγορία ανακαλύπτουν τις διαδρομές όταν απαιτείται ή όταν χρειάζονται, γι' αυτό και ονομάζονται επίσης πρωτόκολλα δρομολόγησης κατά απαίτηση. Τα Reactive πρωτόκολλα δρομολόγησης δεν καταναλώνουν εύρος ζώνης όταν ο κόμβος δεν στέλνει πακέτο δεδομένων, πράγμα που σημαίνει ότι το εύρος ζώνης καταναλώνεται μόνο όταν ο κόμβος έχει κάποια δεδομένα να μεταδώσει σε έναν προορισμό. Τα Reactive πρωτόκολλα δρομολόγησης μειώνουν την επιβάρυνση του εύρους ζώνης του δικτύου και την ισχύ της μπαταρίας, επειδή δεν ανταλλάσσονται περιοδικά μηνύματα ενημέρωσης δρομολόγησης στο δίκτυο.

3.3.2 Proactive routing protocols

Στα Proactive πρωτόκολλα δρομολόγησης, μια διαδρομή είναι πάντα διαθέσιμη μεταξύ κάθε δύο κόμβων στο δίκτυο. Τα περιοδικά μηνύματα ενημέρωσης διαδρομής διαδίδονται στο δίκτυο με σκοπό τη δημιουργία και τη συντήρηση της διαδρομής. Οι περιοδικές ενημερώσεις ανταλλάσσονται μεταξύ των κόμβων σε συγκεκριμένα χρονικά διαστήματα ανεξάρτητα από την κατάσταση της κυκλοφορίας και την κινητικότητα των κόμβων. Από την άλλη πλευρά, οι ενημερώσεις που προκαλούνται από συμβάντα λαμβάνουν χώρα μόνο όταν λαμβάνει χώρα κάποιο συγκεκριμένο συμβάν, όπως η διακοπή σύνδεσης. Δεδομένου ότι η κινητικότητα των κόμβων έχει άμεσο αντίκτυπο στις αλλαγές συνδέσεων, αυξάνεται επίσης η συχνότητα των ενημερώσεων που προκαλούνται από συμβάντα. Σε αυτή την κατηγορία πρωτοκόλλων δρομολόγησης, οι πληροφορίες δρομολόγησης διατηρούνται σε αριθμό πινάκων δρομολόγησης. Αυτοί οι πίνακες ενημερώνονται περιοδικά- ως εκ τούτου, ονομάζονται επίσης πρωτόκολλα δρομολόγησης με βάση τους πίνακες.

Το κύριο πλεονέκτημα των πρωτοκόλλων Proactive δρομολόγησης είναι η διαθεσιμότητα συνεπών και ενημερωμένων διαδρομών στους πίνακες δρομολόγησης μεταξύ όλων των κόμβων ανά πάσα στιγμή στο δίκτυο. Ωστόσο, ένα σημαντικό μειονέκτημα είναι η πρόκληση μεγάλων γενικών εξόδων όσον αφορά τη δημιουργία, την ενημέρωση και τη συντήρηση αυτού του πίνακα δρομολόγησης. Η ενημέρωση του πίνακα δρομολόγησης μπορεί να γίνει αρκετά συχνή σε περίπτωση μεγάλης κινητικότητας των κόμβων. Τα πρωτόκολλα DSDV (Destination-Sequenced Distance Vector) και OLSR (Optimized Link State Routing) είναι σημαντικά πρωτόκολλα για τα MANET.

3.3.3 Hybrid routing protocols

Ένα σχήμα δρομολόγησης που είναι αμιγώς Proactive δεν είναι κατάλληλο για περιβάλλον MANET λόγω των μεγάλων επιβαρύνσεων που σχετίζονται με τους πίνακες δρομολόγησης. Με τον

ίδιο τρόπο, ένα αμιγώς reactive πρωτόκολλο δεν μπορεί να είναι απόλυτα επιτυχημένο στα MANETs λόγω των σχετικών μειονεκτημάτων του. Ως εκ τούτου, ορισμένα χαρακτηριστικά και των δύο αυτών προσεγγίσεων μπορούν να ενσωματωθούν για να σχηματίσουν μια βελτιωμένη κατηγορία πρωτοκόλλων δρομολόγησης κινητών ad-hoc, τα οποία ονομάζονται υβριδικά πρωτόκολλα [3]. Αυτά τα πρωτόκολλα επιδεικνύουν Reactive συμπεριφορά σε ορισμένες περιπτώσεις και Proactive συμπεριφορά σε άλλες περιπτώσεις. Τα υβριδικά πρωτόκολλα δρομολόγησης επιτρέπουν την ευελιξία και την επεκτασιμότητα στο περιβάλλον MANET, θεωρώντας ότι ολόκληρο το δίκτυο χωρίζεται σε ζώνες [8]. Τα ZRP και ZHLS είναι τα παραδείγματα της υβριδικής κατηγορίας.

3.3.4 Source routing versus hop by hop routing

3.3.4.1 Source routing

Τα πρωτόκολλα βασισμένα στη δρομολόγηση by Source δεν είναι κατάλληλα για δίκτυα μεγάλου μεγέθους, επειδή οι πλήρεις πληροφορίες διαδρομής συνδυάζονται με το πακέτο δεδομένων, οπότε δημιουργείται μεγάλο ποσό επιβάρυνσης. Έτσι, στη δρομολόγηση βασισμένη στην πηγή μεγάλου δικτύου αυξάνονται οι πιθανότητες αποτυχίας του δικτύου.Τα πρωτόκολλα CBRP και DSR είναι τα πρωτόκολλα αυτής της κατηγορίας που χρησιμοποιούνται κυρίως.

3.3.4.2 hop by hop routing

Τα πρωτόκολλα δρομολόγησης hop by hop είναι κατάλληλα για τα MANET στα οποία η τοπολογία του δικτύου αλλάζει πολύ συχνά λόγω της κινητικότητας των κόμβων. Στα πρωτόκολλα αυτής της κατηγορίας τα πακέτα δεδομένων δεν μεταφέρουν την πλήρη πληροφορία της διαδρομής, περιέχουν μόνο την πληροφορία του επόμενου άλματος με τη διεύθυνση του κόμβου προορισμού, οπότε μειώνεται η επιβάρυνση και διατίθεται μεγαλύτερο εύρος ζώνης για τη μετάδοση δεδομένων. Τα πακέτα δεδομένων προωθούνται στο δίκτυο με τη βοήθεια των πληροφοριών του πίνακα δρομολόγησης. Οι πίνακες δρομολόγησης ενημερώνονται περιοδικά ή όταν υπάρχουν κάποιες αλλαγές στην τοπολογία λόγω μετακίνησης κόμβων, διακοπής ρεύματος κόμβων κ.λπ. Το AODV είναι το παράδειγμα πρωτοκόλλου αυτής της κατηγορίας.

3.4 Επιλογή routing

Η διαδικασία εύρεσης routing είναι διαφορετική σε κάθε αλγόριθμο. Ο proactive αλγόριθμος δρομολόγησης διατηρεί τις πληροφορίες διαδρομής προς τους άλλους κόμβους στον πίνακα δρομολόγησης, έτσι ώστε να υπάρχει ελάχιστη καθυστέρηση στη μετάδοση πακέτων δεδομένων, ενώ το reactive πρωτόκολλο δρομολόγησης βρίσκει τη διαδρομή κατά απαίτηση, έτσι ώστε να μειώνεται η επιβάρυνση ελέγχου. Το υβριδικό πρωτόκολλο δρομολόγησης είναι το μείγμα του proactive και του reactive πρωτοκόλλου δρομολόγησης που συνδυάζει τα πλεονεκτήματα και των δύο. Η χρήση του πρωτοκόλλου εξαρτάται από τον τύπο των εφαρμογών και τις απαιτούμενες παραμέτρους QoS, όπως ενέργεια, PDR, ρυθμός μετάδοσης και συγχρονισμός. Αυτή η φάση δρομολόγησης έχει συμπεριληφθεί ως ένα αποτελεσματικό πρωτόκολλο δρομολόγησης, το οποίο έχει αποδειχθεί ότι έχει αποδειχθεί με αυτό. Οι βελτιωμένοι αλγόριθμοι QoS είναι συμβατοί με τις αλλαγές στις συνθήκες του δικτύου και παρέχουν καλύτερες επιδόσεις. Στο μέλλον θα σχεδιαστεί ο συνδυασμένος τύπος αλγορίθμων για την αύξηση των παραμέτρων ποιότητας υπηρεσιών, όπως η απόδοση, η καθυστέρηση, η ισχύς και ο λόγος παράδοσης πακέτων.

Κεφάλαιο 4

Επιθέσεις στα MANET

Οι επιθέσεις στα MANET μπορούν να ταξινομηθούν σε active και passive επιθέσεις. Active επίθεση είναι αυτή κατά την οποία ένας επιτιθέμενος που είναι πιστοποιημένος κόμβος διαγράφει ή μεταβάλλει τα δεδομένα που ανταλλάσσονται στο δίκτυο. Ενώ μια passive επίθεση επιτιθέμενου κόμβου ο οποίος είναι μη εξουσιοδοτημένος, παίρνει τα δεδομένα χωρίς να διαταράξει ή να βλάψει τη λειτουργία του δικτύου.

Μια άλλη ταξινόμηση μπορεί να είναι οι external και οι internal επιθέσεις. Στις external επιθέσεις ο επιτιθέμενος κόμβος είναι αυτός που δεν ανήκει στο συγκεκριμένο δίκτυο, ενώ στις internal επιθέσεις ο επιτιθέμενος κόμβος ανήκει σε αυτό το δίκτυο. Οι internal επιθέσεις είναι πιο σοβαρές από τις external επιθέσεις, δεδομένου ότι ο επιτιθέμενος γνωρίζει όλες τις μυστικές πληροφορίες και έχει προνομιακά δικαιώματα πρόσβασης.

Επομένως, ενώ οι active και οι passive επιθέσεις περιγράφουν τον τρόπο με τον οποίο πραγματοποιείται μια επίθεση (είτε μέσω άμεσης παρέμβασης είτε μέσω παρακολούθησης), οι external και οι internal επιθέσεις περιγράφουν από πού προέρχεται η επίθεση (είτε εκτός είτε εντός του δικτύου).

4.1 Ανάλυση Passive-Active

4.1.1 Passive

Μια passive επίθεση δεν μεταβάλλει τα δεδομένα που μεταδίδονται στο δίκτυο.Περιλαμβάνει όμως τη μη εξουσιοδοτημένη "ακρόαση" του δικτύου ή αντλεί δεδομένα από αυτήν. Ο παθητικός επιτιθέμενος δεν διαταράσσει τη λειτουργία ενός πρωτοκόλλου δρομολόγησης αλλά επιχειρεί να ανακαλύψει τις σημαντικές πληροφορίες από τη δρομολογούμενη κυκλοφορία. Η ανίχνευση τέτοιου είδους επιθέσεων είναι δύσκολη, δεδομένου ότι η λειτουργία του ίδιου του δικτύου δεν επηρεάζεται. Προκειμένου να ξεπεραστούν αυτού του είδους οι επιθέσεις ισχυρή κρυπτογράφηση αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων που μεταδίδονται

4.1.2 Active

Οι Active επιθέσεις είναι πολύ σοβαρές επιθέσεις στο δίκτυο που εμποδίζουν τη ροή μηνυμάτων μεταξύ των κόμβων. Ωστόσο, οι Active επιθέσεις μπορεί να είναι external ή internal. Active external επιθέσεις μπορούν να πραγματοποιηθούν από external πηγές που δεν ανήκουν σε στο δίκτυο. Οι internal επιθέσεις προέρχονται από κακόβουλους κόμβους που **ανήκουν** στο δίκτυο, οι internal επιθέσεις είναι πιο σοβαρές και δύσκολα ανιχνεύσιμες σε σχέση με τις external επιθέσεις.

Αυτές οι επιθέσεις δημιουργούν μη εξουσιοδοτημένη πρόσβαση στο δίκτυο που βοηθάει τον επιτιθέμενο να κάνει αλλαγές, όπως η τροποποίηση των πακέτων, DoS, congestion κ.λπ. Οι ενεργές επιθέσεις είναι γενικά από compromised κόμβους ή κακόβουλους κόμβους. Οι κακόβουλοι κόμβοι αλλάζουν τις πληροφορίες δρομολόγησης διαφημίζοντας τον εαυτό τους ως έχοντα τη συντομότερη διαδρομή προς τον προορισμό.

4.2 Τύποι active επιθέσεων

Οι active επιθέσεις ταξινομούνται σε τέσσερις ομάδες:

- ***Dropping Attacks***: Compromised nodes ή selfish nodes μπορούν να απορρίψουν όλα τα πακέτα που δεν προορίζονται για τους. Οι επιθέσεις απόρριψης μπορούν να αποτρέψουν την από άκρο σε άκρο επικοινωνίες μεταξύ των κόμβων, εάν ο κόμβος που απορρίπτει βρίσκεται σε κρίσιμο σημείο. Τα περισσότερα πρωτόκολλα δρομολόγησης έχουν μηχανισμό για να ανιχνεύσει αν τα πακέτα δεδομένων έχουν προωθηθεί ή όχι.
- ***Modification Attacks***: Οι επιθέσεις Sinkhole είναι οι παράδειγμα επιθέσεων τροποποίησης. Αυτές οι επιθέσεις τροποποιούν και διαταράσσουν τη συνολική επικοινωνία μεταξύ των κόμβων του δικτύου. Στην επίθεση sinkhole, ο κόμβος που έχει παραβιαστεί διαφημίζει τον εαυτό του με τέτοιο τρόπο ώστε έχει τη συντομότερη διαδρομή προς τον προορισμό. Ο κακόβουλος κόμβος από το να συλλέγει σημαντικές πληροφορίες δρομολόγησης για να τις χρησιμοποιήσει για περαιτέρω επιθέσεις, όπως η απόρριψη και η επιλεκτική προώθηση.
- ***Fabrication Attacks***: Σε αυτού του είδους τις επιθέσεις, ο επιτιθέμενος στέλνει ένα ψεύτικο μήνυμα στους γειτονικούς κόμβους χωρίς να λαμβάνει κανένα σχετικό μήνυμα. Ο επιτιθέμενος μπορεί επίσης να στείλει ψεύτικο μήνυμα απάντησης διαδρομής ως απάντηση σε σχετικό νόμιμο μηνύματα αίτησης διαδρομής.
- ***Timing Attacks***: Σε αυτόν τον τύπο επιθέσεων, οι επιτιθέμενοι προσελκύουν άλλους κόμβους, διαφημιζόμενοι ως κόμβοι που βρίσκονται πιο κοντά στον πραγματικό κόμβο. Επιθέσεις Rushing και hello flood χρησιμοποιούν αυτή την τεχνική.

4.3 Επιθέσεις per layer

Layer	Attacks
Physical Layer	jamming, interference, Eavesdropping
Data Link Layer	Traffic analysis, monitoring
Network Layer	Wormhole, Black hole, Gray hole, message tempering,Byzantine,Flooding,resource consumption, location disclosure attacks
Transport Layer	Session hijacking, SYN Flooding
Application	Denial of Service (DoS), man-in-the-middle attack,Malicious code, Data corruption, viruses and worm

4.3.1 Επιθέσεις στο φυσικό επίπεδο

Οι επιθέσεις στο φυσικό επίπεδο είναι προσανατολισμένες στο υλικό και χρειάζονται βοήθεια από hardware sources για να υλοποιηθούν. Αυτές οι επιθέσεις είναι απλές στην εκτέλεση σε σύγκριση με άλλες επιθέσεις. Δεν απαιτούν την πλήρη γνώση των τεχνολογίας. Ορισμένες από τις επιθέσεις που εντοπίζονται στο φυσικό επίπεδο περιλαμβάνουν eavesdropping, interference και jamming.

- **Eavesdropping**:

  Eavesdropping μπορεί επίσης να οριστεί ως interception και ανάγνωση μηνυμάτων και συνομιλιών από ακούσιους παραλήπτες. Καθώς η επικοινωνία λαμβάνει χώρα σε ασύρματα μέσο μπορεί εύκολα να υποκλαπεί με δέκτη συντονισμένο στο κατάλληλη συχνότητα. Ο κύριος στόχος αυτών των επιθέσεων είναι η απόκτηση εμπιστευτικών πληροφοριών που πρέπει να παραμείνουν μυστικές κατά τη διάρκεια της επικοινωνίας. Οι πληροφορίες μπορεί να περιλαμβάνουν ιδιωτικό κλειδί, δημόσιο κλειδί, τοποθεσία ή κωδικούς πρόσβασης των κόμβων.

Εικόνα 4.3.1. Eavesdropping

- **Jamming:**

  Η jamming επίθεση είναι μια ειδική κατηγορία επιθέσεων DoS οι οποίες είναι ξεκινούν από κακόβουλο κόμβο μετά τον προσδιορισμό της συχνότητας της επικοινωνίας. Σε αυτόν τον τύπο επίθεσης, ο παρεμβολέας μεταδίδει σήματα.Οι παρεμβολές αποτρέπουν επίσης τη λήψη νόμιμων πακέτων.

- **Active Interference:**

  Μια Active Interference είναι μια επίθεση άρνησης παροχής υπηρεσιών η οποία μπλοκάρει το ασύρματο κανάλι επικοινωνίας, ή παραμορφώνει τις επικοινωνίες. Τα αποτελέσματα τέτοιων επιθέσεων εξαρτώνται από τη διάρκειά τους και το πρωτόκολλο δρομολόγησης που χρησιμοποιείται. Ο επιτιθέμενος μπορεί να αλλάξει τη σειρά των μηνυμάτων ή να επιχειρήσει να αναπαραγωγή παλαιών μηνυμάτων. Τα παλαιά μηνύματα μπορεί να αναπαραχθούν για να επανεισαγάγει ξεπερασμένες πληροφορίες.

4.3.2 Επιθέσεις στο Data link / MAC layer

Οι αλγόριθμοι που χρησιμοποιούνται στο επίπεδο ζεύξης δεδομένων/στρώμα MAC είναι οι εξήσευάλωτοι σε πολλές επιθέσεις DoS. Οι επιθέσεις στο επίπεδο MAC μπορούν να ταξινομούνται ως προς την επίδραση που έχουν στην κατάσταση του δικτύου ως σύνολο. Οι επιπτώσεις μπορούν να μετρηθούν από την αποτυχία route discovery, κατανάλωση ενέργειας, διακοπή σύνδεσης έναρξη route discovery κ.ο.κ. Η κακή συμπεριφορά ενός κόμβου μπορεί να είναι καθαρά εγωιστικού συμφέροντος ή με κακόβουλη σκοπούς.

- **Selfish Misbehaviour of Nodes:**

  Οι επιθέσεις αυτής της κατηγορίας, επηρεάζουν άμεσα την αυτο απόδοση των κόμβων και δεν παρεμβαίνουν στην λειτουργία του δικτύου [4]. Μπορεί να περιλαμβάνει δύο σημαντικούς παράγοντες.

  1. *Conservation of battery power*
  2. *Gaining unfair share of bandwidth*

     Τα selfish nodes μπορεί να αρνηθούν να συμμετάσχουν στη διαδικασία προώθησης ή να απορρίψουν τα πακέτα σκόπιμα για να εξοικονομήσουν πόρους. Αυτές οι επιθέσεις εκμεταλλεύονται το πρωτόκολλο δρομολόγησης προς όφελός τους. Η απόρριψη

πακέτων είναι μια από τις κύριες επιθέσεις από εγωιστές κόμβους που οδηγεί σε συμφόρηση στο δίκτυο. Ωστόσο, τα περισσότερα πρωτόκολλα δρομολόγησης δεν διαθέτουν μηχανισμό για να ανιχνεύουν αν τα πακέτα προωθούνται ή όχι, εκτός από το DSR (δυναμική δρομολόγηση πηγής).

- **Malicious Behaviour of node:**

  Ο κύριος στόχος του κακόβουλου κόμβου είναι να διαταράξει την κανονική λειτουργία του πρωτοκόλλου δρομολόγησης. Ο αντίκτυπος μιας τέτοιας επίθεσης είναι όταν η επικοινωνία λαμβάνει χώρα μεταξύ γειτονικών κόμβων. Οι επιθέσεις αυτού του τύπου διακρίνονται σε ακόλουθες κατηγορίες.

  - ***Άρνηση παροχής υπηρεσιών (DoS)***: Αυτοί οι τύποι απειλών παράγουν μια κακόβουλη ενέργεια με τη βοήθεια συμβιβασμένων κόμβων που αποτελούν σοβαρούς κινδύνους για την ασφάλεια. Στο παρουσία συμβιβασμένων κόμβων, είναι πολύ δύσκολο να εντοπιστεί η συμβιβασμένη δρομολόγηση. Ο συμβιβασμένος διαδρομή φαίνεται σαν μια κανονική διαδρομή, αλλά οδηγεί σε σοβαρές προβλήματα. Για παράδειγμα, ένας συμβιβασμένος κόμβος θα μπορούσε να συμμετέχει στην επικοινωνία, αλλά να απορρίπτει πακέτα που οδηγούν σε υποβάθμιση της ποιότητας της υπηρεσίας που προσφέρεται από το δίκτυο.
  - ***Attacks on Network integrity***: Η ακεραιότητα του δικτύου είναι μια σημαντικό ζήτημα, προκειμένου να παρέχεται ασφαλής επικοινωνίας και ποιότητας υπηρεσιών στο δίκτυο.Υπάρχουν τόσες πολλές απειλές που εκμεταλλεύονται τη δρομολόγηση για την εισαγωγή λανθασμένων πληροφοριών δρομολόγησης.
  - ***Misdirecting traffic*:** Ένας κακόβουλος κόμβος διαφημίζει λανθασμένες πληροφορίες δρομολόγησης προκειμένου να αποκτήσει ασφαλή δεδομένα πριν από την πραγματική διαδρομή. Αυτοί οι κόμβοι λαμβάνουν πληροφορίες που προορίζονταν για τον owner της διεύθυνσης. Ένας κακόβουλος κόμβος μπορεί να διαφημίσει ψεύτικο αίτημα δρομολόγησης, έτσι ώστε ώστε άλλοι κόμβοι να κατευθύνουν τις απαντήσεις διαδρομής στον κόμβο.
  - ***Attacking neighbour sensing protocols***: κακόβουλοι κόμβοι διαφημίζουν ψεύτικα μηνύματα σφάλματος, έτσι ώστε σημαντικοί διασύνδεση συνδέσμων χαρακτηρίζεται ως σπασμένη. Αυτό θα έχει ως αποτέλεσμα μείωση της απόδοσης του δικτύου και της ποιότητας της υπηρεσίας

- **Traffic Analysis:**

  Στα MANETs τα πακέτα δεδομένων καθώς και το μοτίβο κίνησης τόσο είναι σημαντικά για τους αντιπάλους. Για παράδειγμα, εμπιστευτικές πληροφορίες σχετικά με την τοπολογία του

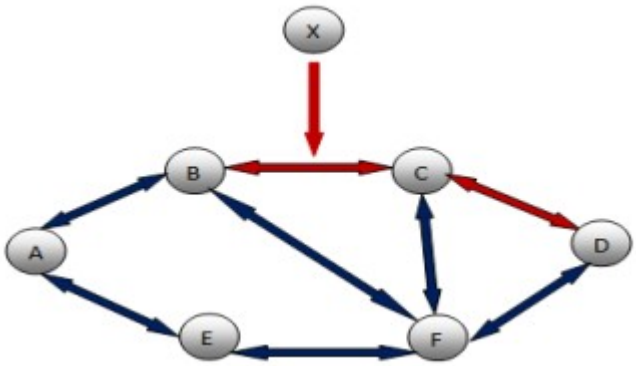
δικτύου μπορούν να αντληθούν αναλύοντας τα μοτίβα κίνησης. Η ανάλυση της κυκλοφορίας μπορεί επίσης να ως ενεργή επίθεση με την καταστροφή κόμβων, οι οποίοι διεγείρει την αυτοοργάνωση του δικτύου, και πολύτιμες δεδομένα σχετικά με την τοπολογία μπορούν να συγκεντρωθούν. Η ανάλυση της κυκλοφορίας σε δίκτυα ad hoc μπορεί να αποκαλύψει τον ακόλουθο τύπο πληροφοριών

- Τοποθεσία των κόμβων
- Τοπολογία δικτύου που χρησιμοποιείται για την επικοινωνία
- Ρόλοι των κόμβων
- Διαθέσιμοι κόμβοι πηγής και προορισμού

4.3.3 Επιθέσεις στο Network layer

Τα *Attacks at Network Layer* επιτρέπουν στους κόμβους MANET να συνδέονται μεταξύ τους μέσω hop-by-hop. Στα MANETs κάθε μεμονωμένος κόμβος λαμβάνει την απόφαση να προωθήσει το πακέτο, οπότε είναι πολύ εύκολο για τον κακόβουλο κόμβο να επιτεθεί σε ένα τέτοιο δίκτυο. Η βασική ιδέα πίσω από αυτές τις επιθέσεις είναι ότι το ίδιο το δίκτυο εισέρχεται στην ενεργή διαδρομή από την πηγή στο προορισμό ή απορροφά την κυκλοφορία του δικτύου. Σε τέτοιες επιθέσεις, οι επιτιθέμενοι μπορούν να δημιουργήσουν βρόχους δρομολόγησης για να προκαλέσουν συμφόρηση.

Γενικά εντοπίζονται διάφοροι τύποι επιθέσεων που ξεκινούν από κακόβουλους κόμβους. Ο κακόβουλος κόμβος "X" μπορεί να «απορροφήσει» σημαντικά δεδομένα, τοποθετώντας τον εαυτό του μεταξύ της πηγής "A" και του προορισμού "D", όπως φαίνεται στην εικόνα 4.3.3.1. Ο "X" μπορεί επίσης να εκτρέψει τα πακέτα δεδομένων που ανταλλάσσονται μεταξύ των "A" και "D", με αποτέλεσμα να οδηγήσει σε σημαντική καθυστέρηση από άκρο σε άκρο μεταξύ των "A" και "D". Σε αυτό τοτύπο επιθέσεων οι επιτιθέμενοι επιτίθενται κατά της επιλογής διαδρομής.

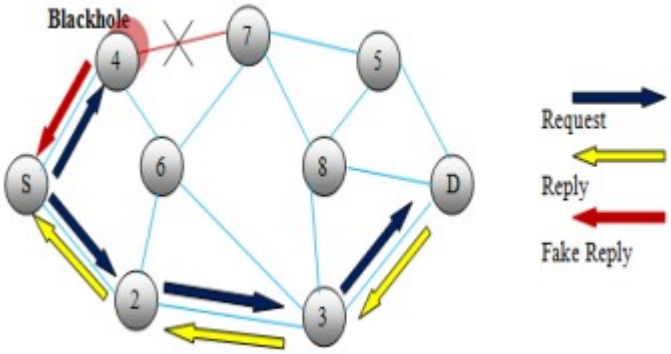


Εικόνα 4.3.3.1: Επίθεση από κακόβουλο κόμβο

- **Blackhole Attack:**

  Σε αυτόν τον τύπο επιθέσεων, ο κακόβουλος κόμβος ισχυρίζεται ότι έχει βέλτιστη διαδρομή προς τον κόμβο του οποίου τα πακέτα θέλει να υποκλέψει. Λαμβάνοντας το αίτημα, ο κακόβουλος κόμβος στέλνει ψεύτικη απάντηση με εξαιρετικά σύντομη διαδρομή. Μόλις ο κόμβος έχει καταφέρει να τοποθετηθεί μεταξύ των κόμβων που επικοινωνούν, είναι σε θέση να κάνει οτιδήποτε με τα πακέτα που περνούν από αυτούς.

  Για παράδειγμα, στην εικόνα 4.3.3.2, ο κακόβουλος κόμβος "4" διαφημίζει τον εαυτό του με τέτοιο τρόπο ώστε να έχει τη συντομότερη διαδρομή προς τον προορισμό. Όταν ο κόμβος πηγής "S" θέλει να στείλει δεδομένα στον προορισμό "D", ξεκινά τη διαδικασία ανακάλυψης διαδρομής. Ο κακόβουλος κόμβος "4" όταν λαμβάνει το αίτημα διαδρομής, στέλνει αμέσως απάντηση στην πηγή. Εάν η απάντηση από τον κόμβο "4" φτάνει πρώτη στην πηγή από τον κόμβο "S", αγνοεί όλα τα άλλα μηνύματα απάντησης και αρχίζει να στέλνει πακέτο, μέσω του κόμβου διαδρομής "2". Έτσι, όλα τα πακέτα δεδομένων χάνονται στον κακόβουλο κόμβο.

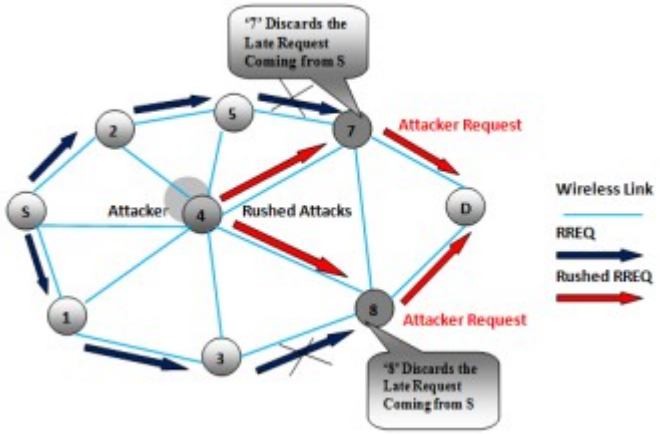


Εικόνα 4.3.3.2: Blackhole attack

- **Rushing Attack:**

Οι επιθέσεις αυτές στρέφονται κυρίως κατά των πρωτοκόλλων δρομολόγησης και ανατρέπουν την διαδικασία ανακάλυψης διαδρομής. Τα *on demand* πρωτόκολλα δρομολόγησης που χρησιμοποιούν διπλότυπη καταστολή κατά τη διαδικασία ανακάλυψης διαδρομής είναι ευάλωτα σε αυτή την επίθεση. Όταν ο συμβιβασμένος κόμβος λαμβάνει ένα αίτημα πακέτου δρομολόγησης από τον κόμβο-πηγή, αυτός προωθεί το πακέτο γρήγορα σε όλο το δίκτυο άλλων κόμβων, οι οποίοι λαμβάνουν επίσης το ίδιο αίτημα, πριν να μπορούν να αντιδράσουν.

Για παράδειγμα, στο σχήμα 4.3.3.3 ο κόμβος "4" αντιπροσωπεύει τον κόμβο επίθεσης, όπου τα "S" και "D" αναφέρονται στους κόμβους πηγής και κόμβους προορισμού. Η βιαστική επίθεση του κόμβου "4" μεταδίδει γρήγορα τα μηνύματα αίτησης διαδρομής για να εξασφαλίσει ότι το μήνυμα RREQ από τον ίδιο θα φτάσει νωρίτερα από ό,τι το μήνυμα RREQ . Αυτό έχει ως αποτέλεσμα όταν ο κόμβος του "D" π.χ. ο"7" και "8" όταν λαμβάνει το πραγματικό (καθυστερημένο) αίτημα δρομολόγησης από την πηγή, απλά να απορρίπτει το αίτημα. Έτσι, παρουσία τέτοιων επιθέσεων, ο "S" αποτυγχάνει να ανακαλύψει οποιοδήποτε χρησιμοποιήσιμη διαδρομή ή ασφαλή διαδρομή χωρίς τη συμμετοχή του επιτιθέμενου.



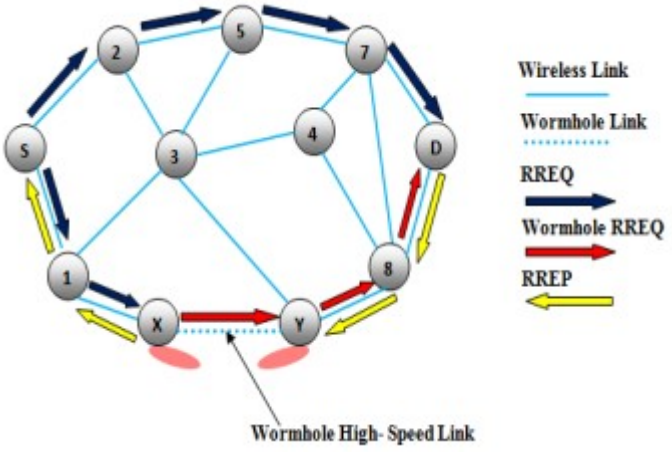
Εικόνα 4.3.3.3: Rushing attack

- **Wormhole attack**

Στην επίθεση *wormhole*, ο κακόβουλος κόμβος λαμβάνει το πακέτο δεδομένων σε ένα σημείο του δικτύου και το διοχετεύει σε ένα άλλο σημείο του δικτύου (κακόβουλο κόμβο). Η σύνδεση μεταξύ δύο κακόβουλων κόμβων αναφέρεται ως wormhole. Οι επιθέσεις αυτές είναι σοβαρές απειλές για τα πρωτόκολλα δρομολόγησης MANET. Οι επιτιθέμενοι χρησιμοποιούν wormholes στο δίκτυο για να κάνουν τους κόμβους τους να φαίνονται πιο ελκυστικοί, ώστε να δρομολογούνται περισσότερα δεδομένα μέσω αυτών. Όταν οι επιθέσεις αυτές χρησιμοποιούνται από τον επιτιθέμενο σε πρωτόκολλο δρομολόγησης όπως το DSR και το AODV, η επίθεση θα μπορούσε να αποτρέψει την ανακάλυψη οποιωνδήποτε διαδρομών εκτός από τις διαδρομές μέσω του wormhole. Εάν δεν υπάρχει αμυντικός μηχανισμός, που να εισάγεται στο δίκτυο μαζί με τα πρωτόκολλα δρομολόγησης, τότε τα υπάρχοντα πρωτόκολλα δρομολόγησης δεν είναι κατάλληλα για την ανακάλυψη έγκυρων διαδρομών.

Για παράδειγμα, στην εικόνα 4.3.3.4, οι κόμβοι "X" και "Y" είναι κακόβουλοι. κόμβοι που σχηματίζουν τούνελ στο δίκτυο. Ο κόμβος πηγής "S" εκκινεί το μήνυμα RREQ για να βρει τη διαδρομή προς τον κόμβο "D" κόμβο προορισμού.

Ο άμεσος γειτονικός κόμβος του κόμβου πηγής "S", δηλαδή "2" και "1" διαβιβάζει το μήνυμα RREQ στους αντιστοιχους γείτονες "5" και "X". Ο κόμβος "X" όταν λάβει το RREQ μοιράζεται αμέσως με τον "Y" και αργότερα ξεκινάει RREQ στον γειτονικό του κόμβο "8", μέσω του οποίου το RREQ παραδίδεται στον κόμβο προορισμού "D". Λόγω της υψηλής ταχύτητας σύνδεσης, αναγκάζει τον κόμβο-πηγή να επιλέξει τη διαδρομή <S-1-8-D> για προορισμό. Αυτό έχει ως αποτέλεσμα το "D" να αγνοεί το RREQ που φτάνει σε μεταγενέστερο χρόνο και έτσι, ακυρώνει τη νόμιμη διαδρομή <S-2-5-7-D>.

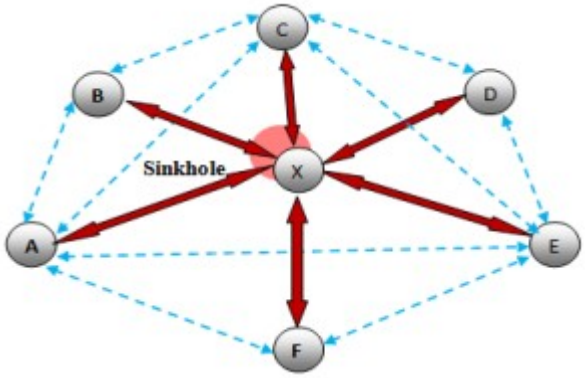


Εικόνα 4.3.3.4: Wormhole attack

- **Sinkhole Attack:**

Η επίθεση *Sinkhole* είναι μία από τις σοβαρές επιθέσεις στα ασύρματα ad hoc δίκτυα. Στην επίθεση αυτή, ένας κακόβουλος κόμβος διαφημίζει λανθασμένες πληροφορίες δρομολόγησης ώστε να εμφανίζεται ως συγκεκριμένος κόμβος και να λαμβάνει ολόκληρη την κίνηση του δικτύου. Έτσι, τροποποιεί μυστικές πληροφορίες, όπως αλλαγές σε πακέτα δεδομένων ή τα απορρίπτει για να κάνει το δίκτυο περίπλοκο. Ένας κακόβουλος κόμβος προσπαθεί να προσελκύσει τα ασφαλή δεδομένα από όλους τους γειτονικούς κόμβους. Οι επιθέσεις *Sinkhole* επηρεάζουν την απόδοση Ad hoc δικτύων, όπως το AODV, χρησιμοποιώντας ελαττώματα όπως τη μεγιστοποίηση του αριθμού ακολουθίας ή την ελαχιστοποίηση του άλματος. Με αυτόν τον τρόπο η διαδρομή που παρουσιάζεται μέσω των κακόβουλων κόμβων φαίνεται να είναι η καλύτερη διαθέσιμη διαδρομή για τους,

κόμβους για να επικοινωνήσουν. Στο πρωτόκολλο DSR, η επίθεση sinkhole τροποποιεί τον αριθμό ακολουθίας στο RREQ.



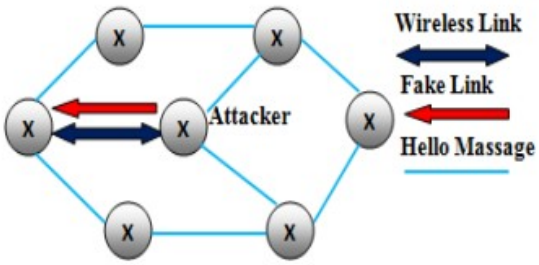
Εικόνα 4.3.3.5: η επίθεση Sinkhole

- **Replay Attacks**

  Στα MANETs, η τοπολογία δεν είναι σταθερή και αλλάζει συχνά λόγω της κινητικότητας των κόμβων. Στην επίθεση επανάληψης, ένας κακόβουλος κόμβος καταγράφει μηνύματα ελέγχου άλλων κόμβων και τα στέλνει εκ νέου αργότερα. Αυτό έχει ως αποτέλεσμα άλλοι κόμβοι να καταγράφουν τον πίνακα δρομολόγησης με παλιές διαδρομές. Αυτές οι επιθέσεις χρησιμοποιούνται για να διαταράξουν τη λειτουργία δρομολόγησης σε ένα MANET.

- **Link Withholding & Link Spoofing Attacks**

  Στην επίθεση αυτή, ο κακόβουλος κόμβος δεν μεταδίδει καμία πληροφορία σχετικά με τις συνδέσεις σε συγκεκριμένους κόμβους. Αυτό έχει ως αποτέλεσμα την απώλεια των συνδέσεων μεταξύ των κόμβων. Έτσι, ένας κακόβουλος κόμβος μεταδίδει ή διαφημίζει τις ψεύτικες πληροφορίες διαδρομής για να διαταράξει τη λειτουργία της δρομολόγησης . Αυτό έχει ως αποτέλεσμα, να ελέγχει τα δεδομένα.



Εικόνα 4.3.3.6: Link Spoofing

- **Resource Consumption Attack**
  Στην περίπτωση αυτή, ένας παραβιασμένος κόμβος μπορεί να προσπαθήσει να καταναλώσει τη διάρκεια ζωής της μπαταρίας ζητώντας υπερβολική ανακάλυψη διαδρομής προωθώντας περιττά πακέτα στον θύμα . Αυτοί οι τύποι επιθέσεων είναι επίσης γνωστοί ως *επιθέσεις sleep deprivation attack* και εκδηλώνονται κυρίως εναντίον των συσκευών που δεν προσφέρουν καμία υπηρεσία στο δίκτυο.

- **Sybil Attack**

  Στην επίθεση Sybil, ο επιτιθέμενος Sybil μπορεί να δημιουργήσει ψεύτικες ταυτότητες ενός αριθμού πρόσθετων κόμβων. Σε αυτό, ένας κακόβουλος κόμβος παράγει μια νέα ταυτότητα του εαυτού του ως μεγάλο αριθμό αντί για έναν κόμβο. Οι πρόσθετες ταυτότητες που αποκτά ο κόμβος ονομάζονται *Sybil nodes*. Ένας κόμβος Sybil μπορεί να κατασκευάσει μια νέα ταυτότητα για να κλέψει μια ταυτότητα του νόμιμου κόμβου. Διάφορες επιπτώσεις που οφείλονται στην παρουσία επιθέσεων Sybil είναι οι εξής:

  - Η παρουσία κόμβων Sybil στο δίκτυο, μπορεί να προκαλέσει τον εντοπισμό ενός κόμβου που δεν συμπεριφέρεται σωστά.

  - Οι επιθέσεις Sybil εμποδίζουν τη δίκαιη κατανομή των πόρων μεταξύ μεταξύ των κόμβων στο δίκτυο.

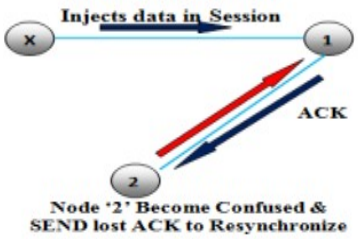
  - Σε ορισμένες εφαρμογές, οι αισθητήρες μπορούν να χρησιμοποιηθούν για τη λήψη αποφάσεων. Λόγω της παρουσίας διπλών ταυτοτήτων το αποτέλεσμα της διαδικασίας ψηφοφορίας μπορεί να ποικίλλει.

  - Οι εικονικοί κόμβοι επηρεάζουν την κανονική λειτουργία της δρομολόγησης πρωτοκόλλων με την εμφάνισή τους σε διάφορες τοποθεσίες σε δικτύου.

4.3.4 Επιθέσεις στο Transport layer

- **Session Hijacking**

Ο επιτιθέμενος στην περίπτωση αυτή, εκμεταλλεύεται την επίθεση μετά την αρχική εγκατάστασή της. Έτσι, παραποιεί τη διεύθυνση IP του κόμβου-θύματος, βρίσκει το σωστό αριθμό ακολουθίας, δηλαδή τον αναμενόμενο από τον στόχο και στη συνέχεια πραγματοποιεί διάφορες επιθέσεις DoS. Έτσι, ο κακόβουλος κόμβος προσπαθεί να συλλέξει ασφαλή δεδομένα (κωδικούς πρόσβασης, μυστικά κλειδιά, ονόματα σύνδεσης κ.λπ.) και άλλες πληροφορίες από τους κόμβους. Οι επιθέσεις αυτές είναι επίσης γνωστές ως επίθεση διεύθυνσης οι οποίες επηρεάζουν το πρωτόκολλο OLSR.



Εικόνα 4.3.4.1: Session hijacking

- **SYN Flooding Attack**

Οι επιθέσεις SYN είναι ο τύπος DoS επιθέσεων, στις οποίες ο επιτιθέμενος δημιουργεί ένα μεγάλο αριθμό μισάνοιχτων συνδέσεων TCP με τον κόμβο-θύμα. Αυτές οι μισάνοιχτες συνδέσεις δεν ολοκληρώνουν ποτέ τη διαδικασία για να ανοίξει πλήρως η σύνδεση.

4.3.5 Επιθέσεις στο Application Layer

Τα πρωτόκολλα επιπέδου εφαρμογής είναι επίσης ευάλωτα σε πολλά DoS επιθέσεις. Το επίπεδο εφαρμογής περιέχει δεδομένα χρήστη. Είναι υποστηρίζει πρωτόκολλα όπως τα HTTP, SMTP, TALNET και FTP, τα οποία παρέχουν πολλά τρωτά σημεία και σημεία πρόσβασης για τους επιτιθέμενους.

- **Malicious code attacks**

  Οι επιθέσεις κακόβουλου κώδικα περιλαμβάνουν ιούς, σκουλήκια, Spywares, και Trojan horses, μπορούν να επιτεθούν τόσο σε λειτουργικούς σύστημα και την εφαρμογή του χρήστη.

- **Repudiation attacks**

  Η αποκήρυξη (**Repudiation**) αναφέρεται στην άρνηση συμμετοχής σε όλες ή μέρος των επικοινωνιών. Πολλοί από τους μηχανισμούς κρυπτογράφησης και τα τείχη προστασίας που χρησιμοποιούνται σε διαφορετικά επίπεδα δεν επαρκούν για για την ασφάλεια των πακέτων. Τα τείχη προστασίας επιπέδου εφαρμογής μπορούν να λάβουν υπόψη υπόψη προκειμένου να παρέχουν ασφάλεια στα πακέτα έναντι πολλών επιθέσεις. Για παράδειγμα, το λογισμικό ανίχνευσης spyware έχει για την παρακολούθηση υπηρεσιών ζωτικής σημασίας.

Κεφάλαιο 5

SD-MANET a possible Mitigation for MANET

Εισαγωγή

Το SDN σημαίνει Software-Defined Networking. Πρόκειται για μια προσέγγιση δικτύωσης που χρησιμοποιεί software-based controllers ή application programming interfaces (APIs) για την καθοδήγηση της κυκλοφορίας στο δίκτυο και την επικοινωνία με την υποκείμενη υποδομή υλικού. Στόχος του SDN είναι να καταστήσει τα δίκτυα πιο ευέλικτα, επεκτάσιμα και προγραμματιζόμενα.

Στις παραδοσιακές αρχιτεκτονικές δικτύων, το επίπεδο ελέγχου(control plane), το οποίο καθορίζει τον τρόπο προώθησης των πακέτων δεδομένων, και το επίπεδο δεδομένων(data plane), το οποίο στην πραγματικότητα προωθεί τα πακέτα, είναι στενά ενσωματωμένα σε συσκευές δικτύου όπως οι μεταγωγείς και οι δρομολογητές. Το SDN διαχωρίζει αυτά τα δύο επίπεδα, συγκεντρώνοντας το επίπεδο ελέγχου και επιτρέποντας στους διαχειριστές να διαχειρίζονται τη συμπεριφορά του δικτύου μέσω εφαρμογών λογισμικού.

5.1 Βασικά στοιχεία λειτουργείας SDN

5.1.1 Control Plane

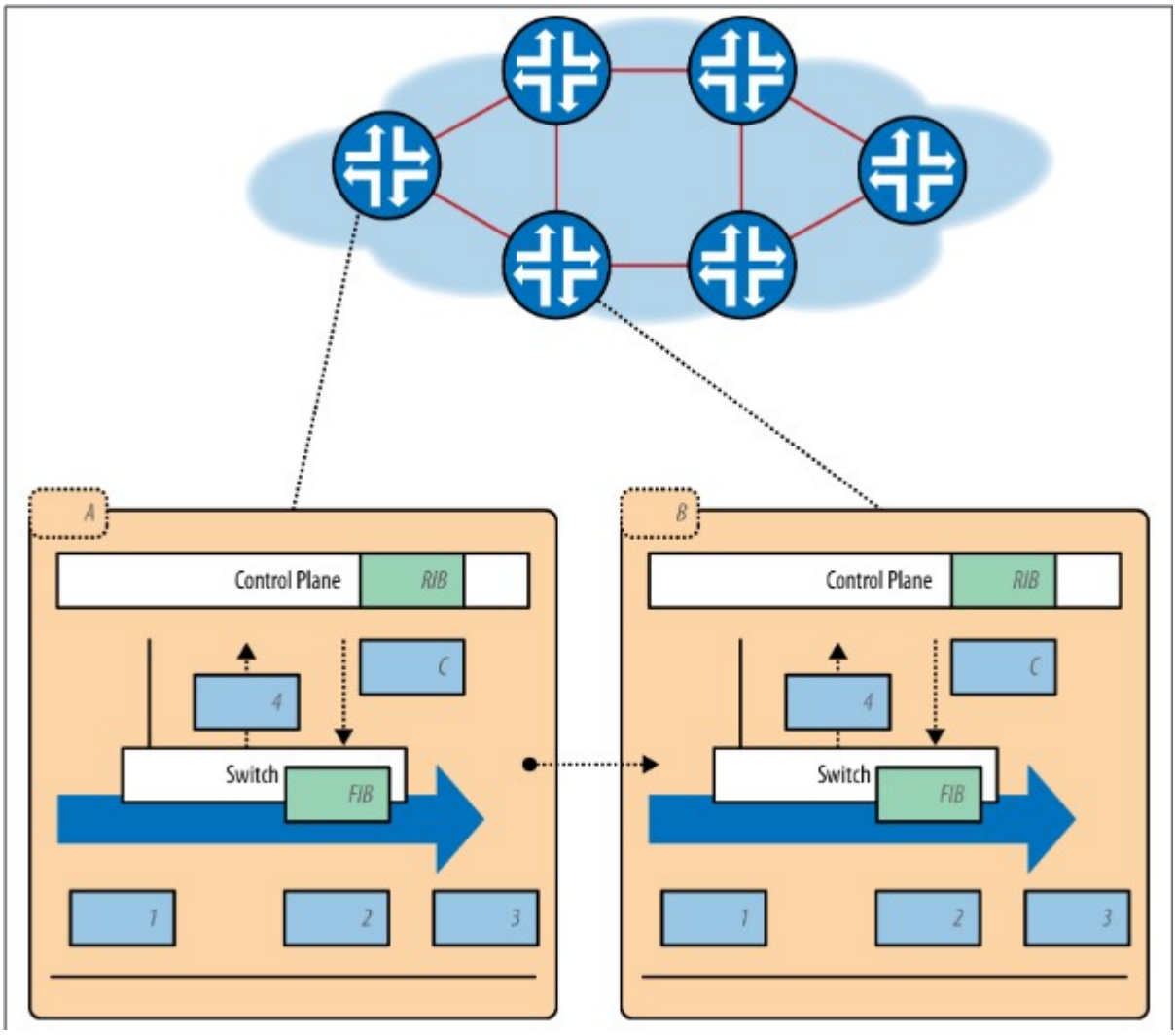
Σε high level, το επίπεδο ελέγχου καθορίζει το τοπικό σύνολο δεδομένων(local data) που χρησιμοποιείται για τη δημιουργία των καταχωρίσεων στο πίνακα προώθησης(forwarding table), οι οποίες με τη σειρά τους χρησιμοποιούνται από το επίπεδο δεδομένων(data plane) για την προώθηση της κίνησης μεταξύ των θυρών εισόδου και εξόδου μιας συσκευής. Το σύνολο δεδομένων που χρησιμοποιείται για την αποθήκευση της τοπολογίας του δικτύου ονομάζεται βάση πληροφοριών δρομολόγησης (RIB). Η RIB συχνά διατηρείται συνεπής (δηλ. χωρίς βρόχους) μέσω της ανταλλαγής πληροφοριών μεταξύ άλλων περιπτώσεων ελέγχου επιπέδων ελέγχου εντός του δικτύου. Οι καταχωρήσεις του πίνακα προώθησης ονομάζονται συνήθως forwarding information base (FIB) και συχνά αντικατοπτρίζονται μεταξύ των επιπέδων ελέγχου και δεδομένων μιας συσκευής. Η FIB προγραμματίζεται μόλις η RIB θεωρηθεί συνεπής και σταθερή.

5.1.2 Data Plane

Το επίπεδο δεδομένων χειρίζεται τα εισερχόμενα datagrams (σε καλώδια, οπτικές ίνες ή ασύρματα μέσα),μέσω μιας σειράς λειτουργιών σε link-level operations που συλλέγουν το datagram και εκτελούν βασικές ελέγχους ορθότητας. Ένα καλά διαμορφωμένο datagram επεξεργάζεται στο επίπεδο δεδομένων(data plane) με τα εξής βήματα εκτελώντας αναζητήσεις στον πίνακα FIB (ή στους πίνακες, σε ορισμένες υλοποιήσεις) το οποίο είναι προγραμματισμένο από το επίπεδο ελέγχου (control plane). Αυτό αναφέρεται μερικές φορές ως η γρήγορη διαδρομή για επεξεργασίας πακέτων, επειδή δεν χρειάζεται περαιτέρω αναζήτηση εκτός από τον εντοπισμό ,του προορισμού του πακέτου χρησιμοποιώντας τον προ-προγραμματισμένο FIB. Η μόνη εξαίρεση σε αυτή την επεξεργασία είναι όταν τα πακέτα δεν μπορούν να ταιριάξουν με αυτούς τους κανόνες, όπως όταν ένας άγνωστος προορισμός εντοπίζεται και τα πακέτα αυτά αποστέλλονται στον επεξεργαστή διαδρομής, όπου το επίπεδο ελέγχου μπορεί να τα επεξεργαστεί περαιτέρω χρησιμοποιώντας το RIB. Είναι σημαντικό να γίνει κατανοητό ότι οι πίνακες FIB θα μπορούσαν να βρίσκονται σε διάφορους στόχους προώθησης-λογισμικό, υλικό-επιταχυνόμενο λογισμικό (GPU/CPU, όπως για παράδειγμα από την Intel ή την ARM), πυρίτιο βασικών προϊόντων (NPU, όπως παράδειγμα της Broadcom, της Intel ή της Marvell, στην αγορά των μεταγωγέων Ethernet), FPGA και εξειδικευμένο πυρίτιο (ASICs όπως το Juniper Trio), ή οποιοσδήποτε συνδυασμός4-ανάλογα με το σχεδιασμό του στοιχείου δικτύου.

5.2 Αναπαράσταση λειτουργείας με παράδειγμα

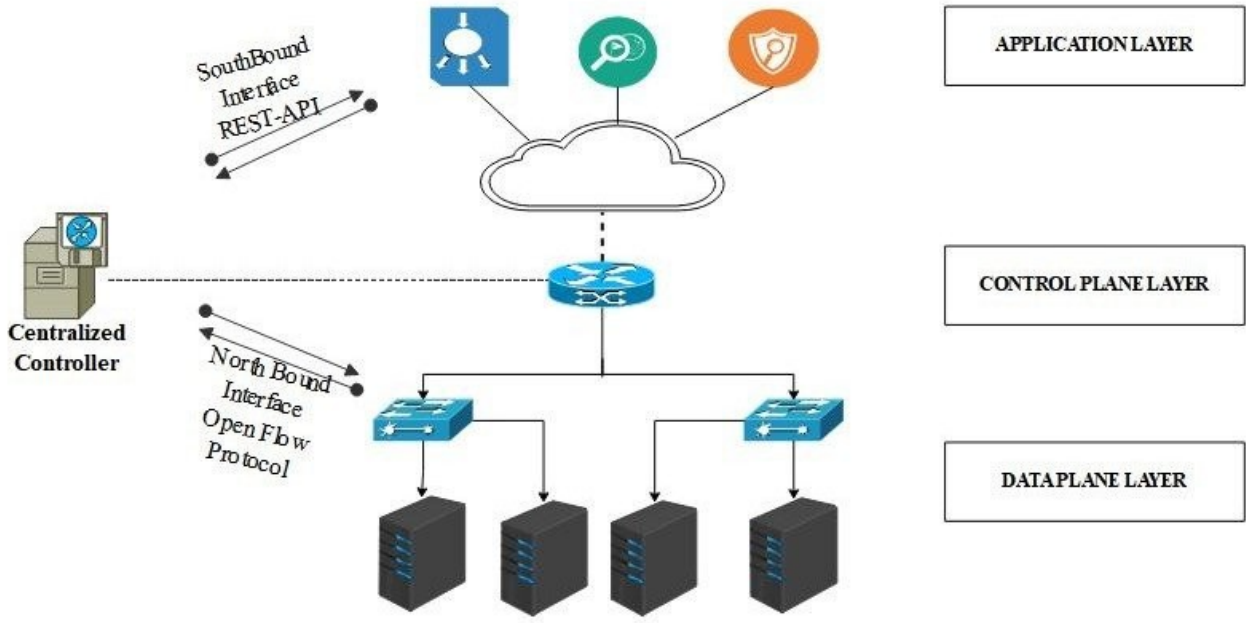
Η μηχανική των control και του data planes παρουσιάζεται στο Σχήμα 2-2, το οποίο αναπαριστά ένα δίκτυο με interconnected switches. Στην κορυφή του σχήματος, ένα δίκτυο από switches, με επέκταση των λεπτομερειών των επιπέδων ελέγχου και δεδομένων δύο από αυτούς τους διακόπτες (σημειωμένα ως A και B). Στο σχήμα, τα πακέτα λαμβάνονται από τον switch A στις στο αριστερότερο επίπεδο ελέγχου και τελικά προωθούνται στον switch B στη δεξιά πλευρά του σχήματος. Στο εσωτερικό κάθε επέκτασης, σημειώστε ότι τα επίπεδα ελέγχου και δεδομένων διαχωρίζονται, με το επίπεδο ελέγχου να εκτελείται στον δικό του επεξεργαστή/κάρτα και το επίπεδο δεδομένων να εκτελείται σε ξεχωριστό. Και τα δύο περιέχονται σε ένα μόνο πλαίσιο. Θα το συζητήσουμε αυτό και άλλες παραλλαγές αυτού του θέματος της φυσικής θέσης των επιπέδων ελέγχου και δεδομένων αργότερα στο κεφάλαιο. Στο σχήμα, τα πακέτα λαμβάνονται στις θύρες εισόδου της κάρτας γραμμής όπου βρίσκεται το επίπεδο δεδομένων. Εάν, για παράδειγμα, λαμβάνεται ένα πακέτο που προέρχεται από μια άγνωστη διεύθυνση MAC, αυτό μεταφέρεται ή ανακατευθύνεται (4) στο επίπεδο ελέγχου της συσκευής, όπου μαθαίνεται, επεξεργάζεται και στη συνέχεια προωθείται. Η ίδια μεταχείριση παρέχεται στην κυκλοφορία ελέγχου, όπως τα μηνύματα του πρωτοκόλλου δρομολόγησης (e.g., OSPF link-state advertise-ments). Μόλις ένα πακέτο παραδοθεί στο επίπεδο ελέγχου, οι πληροφορίες που περιέχονται σε αυτό υποβάλλονται σε επεξεργασία και ενδεχομένως οδηγούν σε τροποποίηση του RIB, καθώς και στη μετάδοση πρόσθετων μηνυμάτων στους ομότιμους χρήστες, ειδοποιώντας τους για την ενημέρωση αυτή (π.χ. μαθαίνεται μια νέα διαδρομή). Όταν το RIB γίνει σταθερό, το FIB ενημερώνεται τόσο στο επίπεδο ελέγχου όσο και στο επίπεδο δεδομένων. Στη συνέχεια, η προώθηση θα ενημερωθεί και θα αντικατοπτρίζει αυτές τις αλλαγές. Ωστόσο, σε αυτή την περίπτωση, επειδή το πακέτο που ελήφθη ήταν ένα από μια μη μαθημένη διεύθυνση MAC, το επίπεδο ελέγχου επιστρέφει το πακέτο (C) στο επίπεδο δεδομένων (2), το οποίο προωθεί το πακέτο αναλόγως (3). Εάν απαιτείται πρόσθετος προγραμματισμός FIB, αυτός πραγματοποιείται επίσης στο βήμα (C), το οποίο θα ήταν η περίπτωση για τώρα που η πηγή των διευθύνσεων MAC έχει μάθει. Ο ίδιος αλγόριθμος για την επεξεργασία των πακέτων συμβαίνει στον επόμενο μεταγωγέα στα δεξιά.



Εικόνα 5.2: Αναπαράσταση λειτουργείας Control & data planes

5.3 Key components of an SDN architecture

- **SDN Controller:** Το control plane είναι centralized στην αρχιτεκτονική SDN και αντιπροσωπεύεται από τον SDN controller. Αυτός ο controller είναι μια οντότητα λογισμικού που διαχειρίζεται τη συνολική συμπεριφορά του δικτύου. Λαμβάνει αποφάσεις σχετικά με τον τρόπο προώθησης της κυκλοφορίας με βάση τη συνολική κατάσταση και τις πολιτικές του δικτύου. Ο SDN controller επικοινωνεί με τους μεταγωγείς ή τους δρομολογητές στο επίπεδο δεδομένων χρησιμοποιώντας **Southbound** API.
- **Northbound APIs:** Αυτα τα interfaces συνδέουν τον SDN controller με τις εφαρμογές ή την επιχειρησιακή λογική που καθορίζουν τη συμπεριφορά του δικτύου. Μέσω **Northbound** API, οι εφαρμογές μπορούν να ζητούν συγκεκριμένες υπηρεσίες δικτύου ή πολιτικές και ο SDN controller μεταφράζει αυτά τα αιτήματα σε διαμορφώσεις για τις υποκείμενες συσκευές δικτύου.
- **Network Devices (Switches/Routers):** Το data plane στο SDN περιλαμβάνει τις φυσικές ή εικονικές συσκευές δικτύου που είναι υπεύθυνες για την προώθηση πακέτων δεδομένων με βάση τις αποφάσεις που λαμβάνει ο SDN controller. Αυτές οι συσκευές είναι συνήθως απλές όσον αφορά την πολυπλοκότητα, επειδή οι πολύπλοκες διαδικασίες λήψης αποφάσεων μεταφέρονται στον κεντρικό SDN controller.
- **Southbound APIs:** Αυτα τα interfaces συνδέουν τον SDN controller με τις συσκευές δικτύου στο επίπεδο δεδομένων, επιτρέποντας στον controller να δίνει οδηγίες στις συσκευές αυτές σχετικά με τον τρόπο προώθησης της κυκλοφορίας. Το πρωτόκολλο OpenFlow είναι ένα παράδειγμα ενός **Southbound** API που χρησιμοποιείται συνήθως στο SDN για την επικοινωνία μεταξύ του controller και των συσκευών δικτύου.Μερικά από τα δημοφιλή **Southbound** API είναι τα OpenFlow, Cisco και OpFlex, ενώ άλλοι προμηθευτές switch και router που υποστηρίζουν το OpenFlow είναι οι IBM, Dell, Juniper, Arista και άλλοι.



Εικόνα 5.3: Key components of an SDN architecture

5.4 Βασικές πληροφορίες SD-MANET δικτύων

Ένα κινητό δίκτυο ad hoc (MANET) είναι μια ομάδα κινητών κόμβων που επικοινωνούν μεταξύ τους χωρίς σταθερή ασύρματη υποδομή. Ένας τυπικός κόμβος MANET έχει περιορισμένη ασύρματη εμβέλεια μετάδοσης και οι ενδιάμεσοι κόμβοι MANET αναμεταδίδουν το δίκτυο πακέτα μέσω πολλαπλών διαδρομών. Επί του παρόντος, κάθε τέτοιος κόμβος υποστηρίζει τις λειτουργίες μιας συσκευής προώθησης και ενός τελικού υπολογιστή, και έχει επίσης ορισμένες λειτουργίες ελέγχου. Κόμβοι μετακινούνται αυθαίρετα, προκαλώντας δυναμικές αλλαγές στην τοπολογία του δικτύου.

Η εφαρμογή των αρχών SDN σε MANET απαιτεί μια αξιόπιστη μετάδοση μεταξύ του SDNC και κάθε κόμβου προώθησης για τον έλεγχο των μηνύματων. Αλλά τα χαρακτηριστικά των MANET, όπως η κινητικότητα των κόμβων, οι διαλείπουσες συνδέσεις και η δυναμική τοπολογία καθιστούν τις συνδέσεις μεταξύ των κόμβων αναξιόπιστες. Κοινό πρωτόκολλα όπως το OpenFlow και το ForCES2 δεν έχουν σχεδιαστεί για τέτοιες συνθήκες.

Οι περισσότερες από τις πρόσφατα προτεινόμενες αρχιτεκτονικές MANET με βάση το SDN (SD-MANET) υποθέτουν ότι το SDNC επικοινωνεί με τον κόμβο μέσω μιας σύνδεσης ενός άλματος μέσω ενός ξεχωριστό κανάλι (π.χ. κινητή τηλεφωνία). Επιπλέον, ένας σταθμός βάσης για τη φιλοξενία του SDNC και ένας υπηρεσία εντοπισμού θέσης (π.χ. GPS) για τον εντοπισμό των θέσεων των κινητών κόμβων είναι επίσης υποτίθεται ότι είναι διαθέσιμοι.

5.4.1 Σχεδίαση ενός SD-MANET

Η πιο σημαντική ερώτηση για τον σχεδιασμό ενός SD-MANET είναι η εξής

- *where to place and how to organize the SDN control logic (controllers) in the network*

Αφού απαντηθεί η ερώτηση αυτή το επόμενο βήμα είναι να εστιάσουμε στο data plane:

Εστιάζοντας στο επίπεδο δεδομένων (δηλαδή, τα δεδομένα σε κόμβους προώθησης). Εδώ, τα ακόλουθα δύο ζητήματα είναι σημαντικά.

Πρώτον, τα τακτικά δίκτυα, και ιδίως τα δίκτυα συνασπισμού, συχνά θα περιλαμβάνουν ένα μεγάλο αριθμό ετερογενών στοιχείων δικτύου. Για παραδείγμα, ορισμένες ομάδες ή στρατιώτες μπορεί να μην να έχουν ραδιοκόμβους με ενίσχυση SDN. Αυτό θα έχει ως αποτέλεσμα σε υβριδικά συστήματα όπου οι κόμβοι του επιπέδου δεδομένων SDN συνυπάρχουν με παλαιούς κόμβους που χρησιμοποιούν δρομολόγηση χωρίς SDN πρωτόκολλα, οπότε η ερώτηση που προκείπτει είναι η εξής

- *where to deploy the SDN forwarding elements and how to use them.*

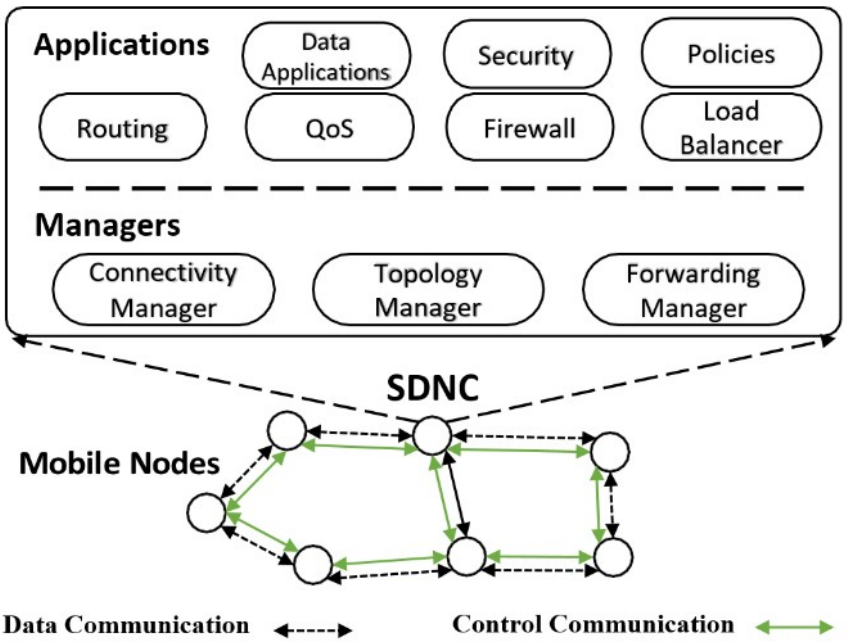
Δεύτερον, η υφηστάμενες προτάσεις SDN βασίζονται στον κεντρικό ελεγκτή για να ενημερώνει όλους τους κανόνες προώθησης στους κόμβους του επιπέδου δεδομένων. Σε τακτικά δίκτυα με υψηλό επίπεδο δυναμισμού και συχνές αποτυχίες δικτύου, αυτή η συγκέντρωση θα έχει ως αποτέλεσμα αργές ενημερώσεις του δικτύου, καθώς και σημαντική επιβάρυνση του ελεγκτή

- *how to make data plane nodes autonomously react to network changes, but at the same time preserve the benefits of centralized control*

5.4.2 Αρχιτεκτονική SD-MANET παράδειγμα

Στην αρχιτεκτονική μας SD-MANET , το SDNC είναι ένας κινητός κόμβος εντός του δικτύου και διαχειρίζεται άλλους κόμβους με κεντρικό τρόπο.Η αρχιτεκτονική μας διαθέτει επίσης το τείχος

προστασίας, τις πολιτικές, το QoS και τις εφαρμογές εξισορρόπησης φορτίου, που εκτελούνται εντός του SDNC για τη διαχείριση του δικτύου και την υλοποίηση των πλεονεκτημάτων του SDN. Ωστόσο, αυτό που κάνει την αρχιτεκτονική μας μοναδική είναι οι τρεις διαχειριστές εντός του SDNC και οι λειτουργίες που εκτελούν.



5.2.1 Παράδειγμα αρχιτεκτονικής SD-MANET

5.5 Ενισχυμένη ασφάλεια στο SD-MANET

Τα δίκτυα SD-MANET (Software-Defined Mobile Ad Hoc Networks) μπορούν να βελτιώσουν σημαντικά την ασφάλεια και να μετριάσουν τα τρωτά σημεία που είναι εγγενή στα παραδοσιακά MANET, αξιοποιώντας τις αρχές του Software-Defined Networking (SDN). Το SDN εισάγει ένα κεντρικό επίπεδο ελέγχου που μπορεί να διαχειρίζεται δυναμικά το δίκτυο, προσφέροντας πιο αποδοτικούς και αποτελεσματικούς τρόπους για την αντιμετώπιση των προκλήσεων ασφαλείας.

5.5.1 Κεντρικός έλεγχος και διαχείριση

Οφέλη από πλευράς ασφάλειας:

- ***Βελτιωμένη παρακολούθηση***: Ο κεντρικός ελεγκτής μπορεί να παρακολουθεί συνεχώς το δίκτυο για ασυνήθιστα μοτίβα και πιθανές παραβιάσεις της ασφάλειας.
- ***Δυναμική επιβολή πολιτικών***: Οι πολιτικές ασφαλείας μπορούν να ενημερώνονται δυναμικά και να επιβάλλονται σε ολόκληρο το δίκτυο σε πραγματικό χρόνο, επιτρέποντας την ταχεία ανταπόκριση σε εντοπισμένες απειλές.
- ***Απλοποιημένη διαχείριση***: Η κεντρική διαχείριση απλοποιεί τη διαμόρφωση και τη συντήρηση των πρωτοκόλλων ασφαλείας, μειώνοντας τον κίνδυνο λανθασμένων ρυθμίσεων που μπορεί να οδηγήσουν σε ευπάθειες.

5.5.2 Ενισχυμένος έλεγχος ταυτότητας και εξουσιοδότηση

Οφέλη από την ασφάλεια:

- ***Κεντρικοποιημένη πιστοποίηση ταυτότητα***ς: Τα SD-MANET μπορούν να εφαρμόσουν ισχυρούς μηχανισμούς ελέγχου ταυτότητας σε επίπεδο ελεγκτή, διασφαλίζοντας ότι μόνο οι νόμιμοι κόμβοι μπορούν να ενταχθούν και να συμμετάσχουν στο δίκτυο.

- ***Έλεγχος πρόσβασης***: Μπορούν να επιβληθούν λεπτής διαβάθμισης πολιτικές ελέγχου πρόσβασης, διασφαλίζοντας ότι οι κόμβοι έχουν πρόσβαση μόνο στους πόρους και τις υπηρεσίες του δικτύου για τις οποίες είναι εξουσιοδοτημένοι.

5.5.3 Αποδοτική ασφάλεια δρομολόγησης

Οφέλη ασφάλειας:

- ***Πρωτόκολλα ασφαλούς δρομολόγησης***: Ο ελεγκτής μπορεί να εφαρμόσει και να επιβάλει ασφαλή πρωτόκολλα δρομολόγησης που είναι λιγότερο ευάλωτα σε συνήθεις επιθέσεις, όπως οι επιθέσεις blackhole, wormhole και Sybil.
- ***Δυναμική διαχείριση διαδρομής***: Σε περίπτωση εντοπισμού απειλής, ο ελεγκτής μπορεί να αναδρομολογήσει δυναμικά την κυκλοφορία για να αποφύγει συμβιβασμένους κόμβους, διατηρώντας ασφαλή και αξιόπιστη επικοινωνία.

5.5.4 Ανίχνευση και μετριασμός απειλών σε πραγματικό χρόνο

Πλεονεκτήματα ασφάλειας:

- ***Ανίχνευση ανωμαλιών***: Ο κεντρικός ελεγκτής μπορεί να χρησιμοποιήσει μηχανική μάθηση και άλλες προηγμένες τεχνικές για την ανίχνευση ανωμαλιών στην κυκλοφορία του δικτύου, υποδεικνύοντας πιθανές απειλές για την ασφάλεια.
- ***Αυτοματοποιημένη απόκριση*:** Με την ανίχνευση μιας απειλής, ο ελεγκτής μπορεί να εφαρμόσει αυτόματα αντίμετρα, όπως η απομόνωση των κόμβων που έχουν τεθεί σε κίνδυνο, η ενημέρωση των κανόνων τείχους προστασίας και η ειδοποίηση των διαχειριστών του δικτύου.

5.5.5 Βελτιωμένη κρυπτογράφηση και ασφαλής επικοινωνία

Οφέλη από την ασφάλεια:

- ***Κεντρική διαχείριση κλειδιών***: Ο ελεγκτής μπορεί να διαχειρίζεται κεντρικά τα κλειδιά κρυπτογράφησης, απλοποιώντας τη διανομή και τη διαχείριση των κλειδιών και εξασφαλίζοντας παράλληλα ασφαλή κανάλια επικοινωνίας μεταξύ των κόμβων.
- ***Συνεπείς πολιτικές κρυπτογράφησης***: Η διασφάλιση της εφαρμογής συνεπών πολιτικών κρυπτογράφησης σε όλο το δίκτυο μπορεί να προστατεύσει από υποκλοπές και αλλοιώσεις δεδομένων.

Τέλος το centralised architech των SD-MANET επιτρέπει την ευκολότερη ανάπτυξη ενημερώσεων λογισμικού και επιδιορθώσεων ασφαλείας σε όλους τους κόμβους, μειώνοντας το παράθυρο ευπάθειας σε γνωστές απειλές, με αποτέλεσμα την διαχείριση ευπαθειών, επιπρόσθετα ο controller μπορεί να παρακολουθεί τις εκδόσεις λογισμικού και τις ευπάθειες όλων των κόμβων, διασφαλίζοντας ότι όλοι οι κόμβοι είναι ενημερωμένοι με τα πιο πρόσφατα μέτρα ασφαλείας.

Συμπεράσματα

Η διερεύνηση των Ασύρματων Ad Hoc Δικτύων (WANETs), ιδίως των Κινητών Ad Hoc Δικτύων (MANETs), διαδραματίζει τον κρίσιμο ρόλο τους στην παροχή αποκεντρωμένων, αυτορυθμιζόμενων δικτύων που λειτουργούν χωρίς σταθερή υποδομή. Τα δίκτυα αυτά, που χαρακτηρίζονται από τις δυναμικές τοπολογίες τους και την κινητικότητα των κόμβων τους, προσφέρουν σημαντικά πλεονεκτήματα σε σενάρια που απαιτούν ταχεία ανάπτυξη και προσαρμοστικότητα, όπως η αποκατάσταση καταστροφών, οι στρατιωτικές επιχειρήσεις και οι κινητές επικοινωνίες. Ωστόσο, τα ίδια τα χαρακτηριστικά που καθιστούν τα MANET ευέλικτα και ευπροσάρμοστα εισάγουν επίσης σημαντικές προκλήσεις, ιδίως όσον αφορά τη δρομολόγηση και την ασφάλεια.Η δρομολόγηση(routing) στα MANETs είναι θεμελιώδης για τη διατήρηση της συνδεσιμότητας και της απόδοσης του δικτύου εν μέσω συνεχών αλλαγών στην τοπολογία του δικτύου. Η ποικιλία των πρωτοκόλλων δρομολόγησης - ενεργητικά, αντιδραστικά και υβριδικά - το καθένα παρουσιάζει ξεχωριστούς συμβιβασμούς. Τα proactive πρωτόκολλα, ενώ εξασφαλίζουν άμεση διαθεσιμότητα διαδρομής, συνεπάγονται υψηλή επιβάρυνση λόγω της συνεχούς συντήρησης των πινάκων δρομολόγησης. Τα reactive πρωτόκολλα, τα οποία ανακαλύπτουν διαδρομές κατ' απαίτηση, μειώνουν την επιβάρυνση αλλά ενδέχεται να εισάγουν καθυστέρηση. Τα υβριδικά πρωτόκολλα προσπαθούν να εξισορροπήσουν αυτά τα αντισταθμιστικά οφέλη, παρέχοντας μια πιο προσαρμόσιμη προσέγγιση δρομολόγησης σε δυναμικά περιβάλλοντα. Η αποδοτικότητα και η αξιοπιστία αυτών των πρωτοκόλλων επηρεάζουν άμεσα τη συνολική απόδοση και την επεκτασιμότητα του δικτύου.Η ασφάλεια παραμένει ένα κρίσιμο ζήτημα στα MANET λόγω της ανοικτής και αποκεντρωμένης φύσης τους. Αυτά τα δίκτυα είναι ευάλωτα σε πολυάριθμες επιθέσεις, όπως επιθέσεις μαύρης τρύπας, σκουληκότρυπας, Sybil και άρνησης παροχής υπηρεσιών (DoS). Τέτοιες ευπάθειες μπορούν να διαταράξουν τις λειτουργίες του δικτύου, να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων και να υποβαθμίσουν την απόδοση. Η αντιμετώπιση αυτών των προκλήσεων ασφαλείας απαιτεί ισχυρούς μηχανισμούς και πρωτόκολλα ικανά να ανιχνεύουν και να μετριάζουν τις απειλές σε πραγματικό χρόνο.Τα καθορισμένα από λογισμικό κινητά Ad Hoc δίκτυα (SD-MANETs) εμφανίζονται ως μια πολλά υποσχόμενη λύση για τις εγγενείς ευπάθειες και τους περιορισμούς των παραδοσιακών MANETs. Ενσωματώνοντας τις αρχές της δικτύωσης καθορισμένου λογισμικού (SDN), τα SD-MANET εισάγουν κεντρικό έλεγχο και δυνατότητα προγραμματισμού, οι οποίες βελτιώνουν σημαντικά τη διαχείριση και την ασφάλεια του δικτύου. Ο κεντρικός ελεγκτής στα SD-MANETs διατηρεί μια σφαιρική άποψη του δικτύου, επιτρέποντας βελτιστοποιημένες αποφάσεις δρομολόγησης, αποτελεσματική διαχείριση πόρων και συνεπή επιβολή πολιτικών ασφαλείας. Αυτή η συγκεντρωτική προσέγγιση επιτρέπει την παρακολούθηση σε πραγματικό χρόνο και την ταχεία αντίδραση σε απειλές ασφαλείας, μετριάζοντας έτσι πολλά από τα τρωτά σημεία που σχετίζονται με τα παραδοσιακά MANET.

Refferences

Gagandeep, Aashima, & Kumar, P. (n.d.). Analysis of different security attacks in Manets on protocol Stack A-Review https://www.ijeat.org/wp-content/uploads/papers/v1i5/E0508061512.pdf

Mishra, V. K., Dusia, A., & Sethi, A. (n.d.). Routing in software-defined mobile ad hoc networks - DTIC. https://apps.dtic.mil/sti/pdfs/AD1059388.pdf

Goyal, M. (n.d.). *Attacks finding and prevention techniques in Manet*. https://www.ripublication.com/awmc17/awmcv10n5_29.pdf.

English, J. (2023, May 2). *SDN controller (software-defined networking controller)*. Networking. https://www.techtarget.com/searchnetworking/definition/SDN-controller-software-defined-networking-controller

Froehlich, A., & Bernstein, C. (2022, November 29). *wireless ad hoc network (WANET)*. Mobile Computing. https://www.techtarget.com/searchmobilecomputing/definition/ad-hoc-network

Okeke, S. S. N., & Nwabueze, C. (2010). MOBILE AD HOC NETWORK (MANET) ARCHITECTURE AND IMPLEMENTATION ANALYSIS. *ResearchGate*. https://doi.org/10.13140/RG.2.2.23447.11680

Pandey, P. (2022, December 19). Mobile Ad hoc Network (MANET) - Scaler Topics. *Scaler Topics*. https://www.scaler.com/topics/manet/

Rehman, S. U., Khan, M. A., Zia, T., & Zheng, L. (2013). Vehicular ad-Hoc networks (VANETs)—An overview and challenges. *ResearchGate*. https://doi.org/10.5923/j.jwnc.20130303.02

SDN-Enabled Tactical ad hoc networks: extending programmable control to the edge. (2018, July 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8419193

Software-Defined architecture for infrastructure-less mobile ad hoc networks. (2021, May 17). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9464002

Southbound vs. Northbound SDN: What are the differences? (2022, November 25). Webwerks. https://www.webwerks.in/blogs/southbound-vs-northbound-sdn-what-are-differences

Suresh Gyan Vihar University. (n.d.). *First Private NAAC A grade University of Rajasthan | SGVU*. NAAC “A” Grade University | Best University in Jaipur Rajasthan - Suresh Gyan Vihar University. https://www.gyanvihar.org/study-of-different-types-of-routing-protocols-in-manet

What is Software-Defined Networking (SDN)? | VMware Glossary. (2024, March 26). VMware. https://www.vmware.com/topics/glossary/content/software-defined-networking.html.html

Wireless SDN mobile ad hoc network: From theory to practice. (2017, May 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7996340

Rehman, S. U., Khan, M. A., Zia, T., & Zheng, L. (2013). Vehicular ad-Hoc networks (VANETs)—An overview and challenges. *ResearchGate*. https://doi.org/10.5923/j.jwnc.20130303.02

Okeke, S. S. N., & Nwabueze, C. (2010). MOBILE AD HOC NETWORK (MANET) ARCHITECTURE AND IMPLEMENTATION ANALYSIS. *ResearchGate*. https://doi.org/10.13140/RG.2.2.23447.11680

Ankur Bawiskar, Dr. B.B. Meshram"Survey of Attacks on Wireless Network", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, March 2013.

Almutairi, L. M., & Shetty, S. (2017). Generalized stochastic Petri Net model based security risk assessment of software defined networks. *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*.

Chahal, M., Harit, S., Mishra, K. K., Sangaiah, A. K., & Zheng, Z. (2017). A Survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. *Sustainable Cities and Society*, *35*, 830–840. https://doi.org/10.1016/j.scs.2017.07.007

Chen, M., Qian, Y., Mao, S., Tang, W., & Yang, X. (2016). Software-defined mobile networks security. *Mobile Networks and Applications*, *21*(5), 729–743. https://doi.org/10.1007/s11036-015-0665-5

Chen, T., Matinmikko, M., Chen, X., Zhou, X., & Ahokangas, P. (2015). Software defined mobile networks: concept, survey, and research directions. *IEEE Communications Magazine*, *53*(11), 126–133. https://doi.org/10.1109/mcom.2015.7321981

Choudhary, S., Narayan, V., Faiz, M., & Pramanik, S. (2022). Fuzzy approach-based stable energy-efficient AODV routing protocol in mobile ad hoc networks. In *Software Defined Networking for Ad Hoc Networks* (pp. 125–139). Springer International Publishing.

Kafetzis, D., Vassilaras, S., Vardoulias, G., & Koutsopoulos, I. (2022). Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 9989–10014. https://doi.org/10.1109/access.2022.3144072

Ku, I., Lu, Y., & Gerla, M. (2014). Software-Defined Mobile Cloud: Architecture, services and use cases. *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*.

Ku, I., Lu, Y., Gerla, M., Gomes, R. L., Ongaro, F., & Cerqueira, E. (2014). Towards software-defined VANET: Architecture and services. *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*.

Mishra, V. K., Dusia, A., Sethi, A., & US Army Research Laboratory Aberdeen Proving Ground United States. (2018). *Routing in Software-defined mobile ad hoc networks (SD-MANET)*.

Polat, H., Polat, O., Sogut, E., & Erdem, O. A. (2019). Performance analysis of between software defined wireless network and mobile ad hoc network under DoS attack. *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*.

Tripathy, B. K., Das, D. P., Jena, S. K., & Bera, P. (2018). Risk based security enforcement in software defined network. *Computers & Security*, *78*, 321–335. https://doi.org/10.1016/j.cose.2018.07.010

Yu, H. C., Quer, G., & Rao, R. R. (2017). Wireless SDN mobile ad hoc network: From theory to practice. *2017 IEEE International Conference on Communications (ICC)*.