ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

# ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΣΕ AD HOC ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Σπυρίδων Σ. Πουλημένος
Α.Μ. : ΜΕ/07073

Μεταπτυχιακή Διπλωματική Εργασία

Επιβλέπων: Χρήστος Ξενάκης
Λέκτορας Πα.Πει

Πειραιάς, Φεβρουάριος 2010

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους με βοήθησαν και με στήριξαν για την ολοκλήρωση του Μεταπτυχιακού μου τίτλου σπουδών στο Πανεπιστήμιο Πειραιά, και κυρίως τους γονείς μου και την αδελφή μου για την υπομονή και την κατανόηση που έδειξαν καθ'όλη τη διάρκεια των σπουδών μου.

Θα ήθελα να ευχαριστήσω θερμά τον Λέκτορα του Πανεπιστημίου Πειραιά κ. Χρήστο Ξενάκη που μου έδωσε την ευκαιρία να αναπτύξω τη διπλωματική εργασία, και τον υποψήφιο διδάκτορα κ. Χριστόφορο Πάνο, για την υποστήριξή του και την καθοδήγησή του κατά τη διάρκεια της εκπόνησης της παρούσης εργασίας.

# Περίληψη

Η εξέλιξη των ασύρματων επικοινωνιών έχει οδηγήσει στη δημιουργία δικτύων χαμηλού κόστους, χωρίς συγκεκριμένη δομή. Τα δίκτυα αυτά, όπως είναι τα ad hoc δίκτυα αποτελούνται από μικρού μεγέθους κόμβους, οι οποίοι δεν έχουν μια συγκεντρωτική διαχείριση. Καθώς τα συγκεκριμένα δίκτυα γίνονται κομμάτι της καθημερινής ζωής, η ασφάλειά τους αποτελεί πεδίο έρευνας.

Τα θέματα ασφαλείας στα ad-hoc δίκτυα είναι διαφορετικά απ' ότι στα σταθερά δίκτυα. Αυτό οφείλεται στο γεγονός ότι οι απαιτήσεις και οι ιδιαιτερότητες αυτών των δικτύων, όπως είναι η περιορισμένη ενέργεια και η κινητικότητα, διαφέρουν από αυτές των σταθερών.

Στην εργασία αυτή αναφερόμαστε γενικά στα ad-hoc δίκτυα. Συγκεκριμένα παρουσιάζουμε τα δίκτυα αυτά καθώς και τα πρωτόκολλα δρομολόγησης που χρησιμοποιούν. Επίσης παρουσιάζουμε θέματα ασφάλειας των δικτύων αυτών και τρόπους αντιμετώπισης των επιθέσεών τους. Τέλος αναλύουμε τα αποτελέσματα τα οποία απορρέουν από τον σχεδιασμό και την προσομοίωση ενός συστήματος ad-hoc, καθώς και των επιθέσεων προς αυτό, με την βοήθεια του simulation NS-2.

# Abstract

The development of wireless communications has led to the creation of low cost networks, without concrete structure. These networks, as are the ad hoc networks are constituted from small size nodes, which do not have a centralized management. As well as the particular networks become piece of daily life, their safety constitutes field of research.

The subjects of safety in the ad-hoc networks are different from that in the regularly networks. This is owed in the make that the requirements and the particularities of these networks, as are the limited energy and the mobility, differ from those of constants networks.

In this work we were reported as generally speaking in the ad-hoc networks. Concretely we present these networks as well as the protocols of routing that they use. Also we present subjects of safety of this networks and ways of confrontation of their attacks. Finally we analyze the results which arise from the planning and the simulation of system ad-hoc, as well as attack to this, with the help the simulation NS-2.

# Περιεχόμενα

# Πίνακας Σχημάτων και Πινάκων

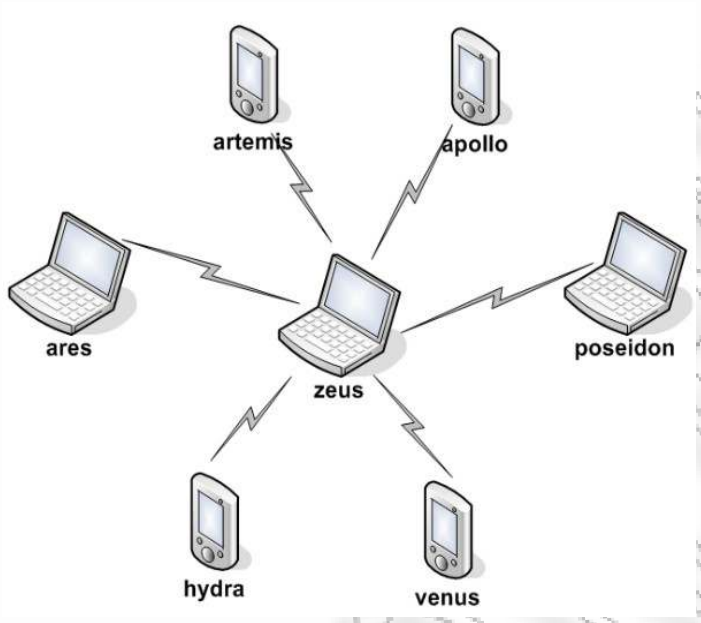
# 1. Εισαγωγή

Οι ψηφιακές ασύρματες επικοινωνίες δεν είναι μια καινούργια ιδέα στον χώρο της τεχνολογίας. Ήδη από το 1901 ο Ιταλός φυσικός Μαρκόνι επέδειξε στο κοινό έναν ασύρματο τηλέγραφο ανάμεσα στα πλοία και στην ξηρά, χρησιμοποιώντας κώδικα Μορς. Αυτά ήταν και τα πρώτα σήματα που ταξίδευαν δια μέσου του Ατλαντικού Ωκεανού. Η ασύρματη τεχνολογία άρχισε να χρησιμοποιείται ευρέως από τις στρατιωτικές δυνάμεις στην μετάδοση των κρυπτογραφημένων πληροφοριών, τόσο εν καιρό πολέμου όσο και σε περιόδους ειρήνης.

Το πρώτο εμπορικό δίκτυο ραδιοτηλεφωνίας δημιουργήθηκε από την εταιρεία Bell Telephone Company στις αρχές της δεκαετίας του 1950. Το πρόβλημα όμως με το συγκεκριμένο δίκτυο ήταν ο μικρός αριθμός χρηστών που θα ήταν συνδεδεμένοι ταυτόχρονα. Το συγκεκριμένο δίκτυο συνέχισε να αναπτύσσεται, ώστε να μπορεί να εξυπηρετεί περισσότερα άτομα με μεγαλύτερη αξιοπιστία.

Το 1971, οι ερευνητές του Πανεπιστημίου της Hawaii ανέπτυξαν το πρώτο παγκόσμιο WLAN (Wireless Local Area Network), το οποίο πήρε το όνομα ALOHAnet. Το 1982, οι προδιαγραφές AMPS (**A**dvanced **M**obile **P**hone **S**ervice) καθορίστηκαν ως το επίσημο πρότυπο της ραδιοτηλεφωνίας στις Ηνωμένες Πολιτείες. Παράλληλα, αρκετές χώρες άρχισαν να αναπτύσσουν κυψελωτά (cellular) δίκτυα, ορισμένα από τα οποία έκαναν χρήση των προτύπων των ΗΠΑ, ενώ άλλα χρησιμοποίησαν διαφορετικά πρότυπα. Τα δίκτυα GSM είναι τα πλέον διαδεδομένα δίκτυα κυψελωτής τηλεφωνίας.

Η βασική δομική μονάδα ενός ασύρματου δικτύου είναι το βασικό σύνολο υπηρεσιών (BSS), το οποίο είναι απλά μια ομάδα σταθμών που επικοινωνούν ο ένας με τον άλλον. Οι επικοινωνίες πραγματοποιούνται μέσα σε μια κάπως συγκεκριμένη περιοχή, τη βασική περιοχή υπηρεσιών, που καθορίζεται από τα χαρακτηριστικά διάδοσης του ασύρματου μέσου. Όταν ένας σταθμός είναι στη βασική περιοχή υπηρεσιών, μπορεί να επικοινωνήσει με τα άλλα μέλη του BSS. Τα BSSs είναι δύο τύπων: ανεξάρτητα (independent) και υποδομής (infrastructure).




**Σχήμα 1** BSS υποδομής

Το παραπάνω σχήμα (σχήμα 1) συνθέτει ένα BSS υποδομής. Τα δίκτυα υποδομής διακρίνονται με την χρήση ενός σημείου πρόσβασης. Τα σημεία πρόσβασης χρησιμοποιούνται για όλες τις επικοινωνίες στα δίκτυα υποδομής, συμπεριλαμβανομένης της επικοινωνίας μεταξύ των κινητών κόμβων στην ίδια περιοχή υπηρεσιών. Εάν ένας κινητός σταθμός σε ένα BSS υποδομής πρέπει να επικοινωνήσει με έναν δεύτερο κινητό σταθμό, η επικοινωνία πρέπει να γίνει σε δύο βήματα. Αρχικά, ο κινητός σταθμός που ξεκινά την επικοινωνία μεταφέρει το πλαίσιο στο σημείο πρόσβασης και μετά το σημείο πρόσβασης μεταφέρει το πλαίσιο στο σταθμό προορισμού. Με όλες τις επικοινωνίες να αναμεταδίδονται μέσω ενός σημείου πρόσβασης, η βασική περιοχή υπηρεσιών που αντιστοιχεί σε μια υποδομή BSS καθορίζεται από τα σημεία στα οποία οι μεταδόσεις από τα σημεία πρόσβασης μπορούν να παραληφθούν. Αν και η μετάδοση πολλών βημάτων καταλαμβάνει περισσότερη ικανότητα μετάδοσης από την μετάδοση ενός πλαισίου απευθείας από τον αποστολέα στο δέκτη, η τεχνική αυτή έχει δύο σημαντικά πλεονεκτήματα:

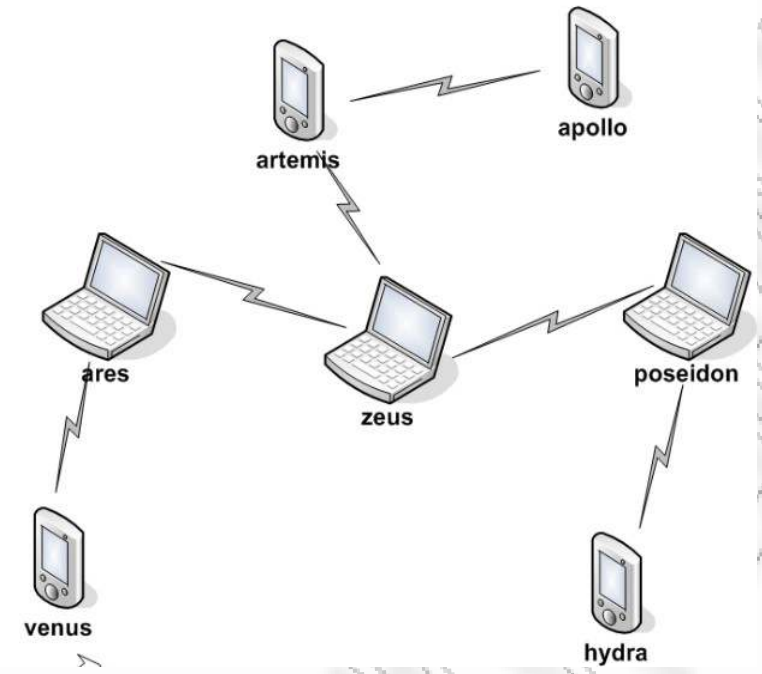
- Μια υποδομή BSS καθορίζεται από την απόσταση από το σημείο πρόσβασης.

Όλοι οι κινητοί σταθμοί πρέπει να είναι προσιτοί στο σημείο πρόσβασης, αλλά κανένας περιορισμός δεν υπάρχει για την απόσταση μεταξύ των κινητών σταθμών. Η άμεση επικοινωνία μεταξύ των κινητών σταθμών θα εξοικονομούσε την ικανότητα μετάδοσης αλλά με κόστος της αυξανόμενης πολυπλοκότητας του φυσικού στρώματος επειδή οι κινητοί σταθμοί είναι ανάγκη να διατηρούν γειτονικές θέσεις με όλους τους άλλους κινητούς σταθμούς μέσα στην περιοχή υπηρεσιών.

- Τα σημεία πρόσβασης στα δίκτυα υποδομής είναι σε θέση να βοηθήσουν τους σταθμούς που προσπαθούν να εξοικονομήσουν ενέργεια. Τα σημεία πρόσβασης μπορούν να προσέξουν πότε ένας σταθμός μπαίνει σε κατάσταση εξοικονόμησης ενέργειας και να τον απομονώσουν. Οι σταθμοί που λειτουργούν με συσσωρευτή μπορούν να κλείσουν τον ασύρματο πομποδέκτη και να τον ανοίξουν για να μεταδώσει και να ανακτήσει αποθηκευμένα πλαίσια από το σημείο πρόσβασης.

Σε ένα δίκτυο υποδομής, οι σταθμοί πρέπει να συνδεθούν σε ένα σημείο πρόσβασης για να λάβουν τις υπηρεσίες δικτύων. Η σύνδεση είναι η διαδικασία με την οποία ο κινητός σταθμός ενώνεται σε ένα ασύρματο δίκτυο και είναι λογικά ισοδύναμη με τη σύνδεση στο καλώδιο ενός δικτύου Ethernet. Δεν είναι μια συμμετρική διαδικασία. Οι κινητοί σταθμοί ξεκινούν πάντα τη διαδικασία σύνδεσης, και τα σημεία πρόσβασης μπορούν να επιλέξουν να επιτρέψουν ή να απαγορεύσουν την πρόσβαση, βασισμένα στο περιεχόμενο του αιτήματος σύνδεσης. Οι συνδέσεις είναι επίσης αποκλειστικές εκ μέρους του κινητού σταθμού: ένας κινητός σταθμός μπορεί να συνδεθεί με μόνο ένα σημείο πρόσβασης. Το πρότυπο 802.11 δεν θέτει κανένα όριο στον αριθμό των κινητών σταθμών που ένα σημείο πρόσβασης μπορεί να εξυπηρετήσει. Θέματα εφαρμογής μπορούν φυσικά να περιορίσουν τον αριθμό κινητών σταθμών που ένα σημείο πρόσβασης μπορεί να εξυπηρετήσει. Στην πράξη, εντούτοις, η σχετικά χαμηλή ρυθμαπόδοση των ασύρματων δικτύων δεν είναι πιθανό να περιορίσει τον αριθμό σταθμών που τοποθετούνται σε ένα ασύρματο δίκτυο.

Στο παρακάτω σχήμα (σχήμα 2) παρατηρούμε ένα ανεξάρτητο BSS (IBSS). Οι σταθμοί σε ένα IBSS επικοινωνούν άμεσα μεταξύ τους και πρέπει να είναι μέσα σε εύρος άμεσης επικοινωνίας. Το μικρότερο πιθανό ασύρματο δίκτυο είναι ένα IBSS με δύο σταθμούς. Χαρακτηριστικά, τα IBSSs αποτελούνται από έναν μικρό αριθμό σταθμών και δημιουργούνται για έναν συγκεκριμένο σκοπό και για μια μικρή χρονική περίοδο. Μια κοινή χρήση είναι να δημιουργηθεί ένα τέτοιο δίκτυο για να υποστηρίξει μια ενιαία συνεδρίαση σε ένα δωμάτιο διασκέψεων. Δεδομένου ότι η συνεδρίαση αρχίζει, οι συμμετέχοντες δημιουργούν ένα IBSS για να μοιραστούν τα στοιχεία. Όταν η συνεδρίαση λήγει το IBSS διαλύεται. Λόγω της σύντομης διάρκειάς τους, το μικρό μέγεθος τους και τον πολύ συγκεκριμένο σκοπό τους τα IBSSs αναφέρονται μερικές φορές ως ad-hoc BSSs ή ad-hoc δίκτυα.




**Σχήμα 2** Ανεξάρτητο BSS

# 2. Περιγραφή Δικτύων Ad-Hoc

## 2.1 Εισαγωγή

Με τις πρόσφατες εξελίξεις στην απόδοση των ασύρματων δικτύων, αναμένεται ευρέα διάδοση και χρήση πιο προχωρημένων ασύρματων δικτύων με κινητούς κόμβους, που θα εξελίξουν κατά πολύ τη χρήση του Internet Protocol (IP). Το όραμα της Ad-Hoc δικτύωσης με κινητούς κόμβους είναι να υποστηρίξει αποτελεσματικά τη χρήση των ασύρματων δικτύων ενσωματώνοντας λειτουργίες δρομολόγησης στους κινητούς κόμβους. Τέτοια δίκτυα θα έχουν δυναμικές, πολλές φορές γρήγορα εναλλασσόμενες και τυχαίες τοπολογίες, που θα αποτελούνται από σχετικά περιορισμένου εύρους ζώνης ασύρματες ζεύξεις.

Στην κοινωνία του Internet, η υποστήριξη δρομολόγησης για κινητούς κόμβους μορφοποιείται ως τεχνολογία “mobile IP”. Αυτή είναι μια τεχνολογία που θα επιτρέπει σε κόμβους να επικοινωνούν με το Internet, συνδεόμενοι σαν φιλοξενούμενοι (hosts) σε κόμβους που θα είναι ήδη συνδεδεμένοι με το Internet με διάφορα μέσα πέρα από την σταθερή τους διεύθυνση (fixed-address). Αυτός ο κόμβος μπορεί να είναι είτε φυσικά συνδεδεμένος με το σταθερό δίκτυο σε ένα ξένο subnet, ή να είναι συνδεδεμένος με μια ασύρματη ζεύξη, ή με μια σύνδεση dial-up, ή με οτιδήποτε άλλο. Αυτή η μορφή του κινητού φιλόξενου κόμβου (host mobility) απαιτεί διαχείριση διευθύνσεων, βελτιώσεις στη διασύνδεση των πρωτοκόλλων και άλλα σχετικά, όμως οι βασικές δικτυακές λειτουργίες όπως η δρομολόγηση από κόμβο σε κόμβο (hop-by-hop routing) ακόμα εξαρτώνται στα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης που λειτουργούν στα σταθερά δίκτυα.

Αντίθετα, ο στόχος των δικτύων MANET είναι να επεκτείνουν αυτή την κινητικότητα σε αυτόνομα, κινητά, ασύρματα domain, όπου ένα σύνολο κόμβων από μόνοι τους αποτελούν την υποδομή για τη δρομολόγηση με έναν Ad-Hoc τρόπο.

## 2.2 Χαρακτηριστικά Δικτύων Ad-Hoc

Ένα δίκτυο Ad Hoc αποτελείται από κινητές μονάδες (π.χ. ένα δρομολογητή με πολλούς hosts και ασύρματες συσκευές, που θα αποκαλούνται κόμβοι) οι οποίες είναι ελεύθερες να μετακινηθούν σε όλη την επιφάνεια του δικτύου. Ένα δίκτυο Ad Hoc, είναι ένα αυτόνομο σύστημα αποτελούμενο από κινητούς κόμβους. Το σύστημα αυτό μπορεί να λειτουργεί απομονωμένο, ή να έχει και διεξόδους (gateways) και να επικοινωνεί με ένα σταθερό δίκτυο. Στον δεύτερο τρόπο λειτουργίας, το σύστημα θα λειτουργεί σαν ένα «αποκομμένο δίκτυο» (“stub” network) που συνδέεται με ένα σταθερό δίκτυο. Τα «αποκομμένα δίκτυα» μεταφέρουν δικτυακή κίνηση που

προέρχεται ή κατευθύνεται προς τους εσωτερικούς κόμβους, αλλά δεν επιτρέπουν την εξωτερική κίνηση να μεταφερθεί μέσω του «αποκομμένου δικτύου».

Οι κόμβοι του δικτύου Ad Hoc είναι εξοπλισμένοι με ασύρματους πομπούς και δέκτες χρησιμοποιώντας κεραίες που μπορεί να είναι μη κατευθυντικές (omnidirectional), πολύ κατευθυντικές (point-to-point), πιθανώς μεταβλητές, ή κάποιος συνδυασμός των παραπάνω. Αυτή η Ad-hoc τοπολογία μπορεί να αλλάξει με την πάροδο του χρόνου, καθώς οι κόμβοι μετακινούνται ή αλλάζουν την ισχύ μετάδοσής τους.

Τα δίκτυα Ad Hoc έχουν πολλά αξιοπρόσεκτα χαρακτηριστικά :

- Καμία σταθερή τοπολογία

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

- Περιορισμένη ενέργεια

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

- Περιορισμένος επεξεργαστής

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

- Περιορισμένη ικανότητα αποθήκευσης και άλλων πόρων

Λόγω των περιορισμών μεγέθους και δαπανών, οι περισσότερες κινητές συσκευές είναι εξοπλισμένες με περιορισμένη ικανότητα αποθήκευσης. Λόγω των ασύρματων τεχνολογιών, το εύρος ζώνης δικτύων είναι επίσης περιορισμένο.

- Παροδική συνεκτικότητα και διαθεσιμότητα

Πολλοί κόμβοι μπορεί να μην είναι προσπελάσιμοι για κάποιο χρόνο ώστε να μπορούν να εξοικονομούν ενέργεια.

- Κάθε κόμβος είναι ένας δρομολογητής

Οι κόμβοι που είναι εκτός εμβέλειας ενός σταθερού κόμβου, δεν μπορούν να προσπελασθούν άμεσα από αυτόν τον κόμβο. Μπορούν μόνο να προσπελασθούν με την αποστολή πακέτων άλλων κόμβων.

- Κοινό φυσικό μέσο

Αντίθετα με τα συνδεδεμένα με καλώδιο δίκτυα, κάθε συσκευή εντός εμβέλειας μπορεί να έχει πρόσβαση στο μέσο μετάδοσης.

- Έλλειψη κεντρικής διαχείρισης

Τα ειδικά δίκτυα μπορούν να συσταθούν παντού και κάθε στιγμή. Γενικά δεν υπάρχει διαθέσιμη καμία κεντρική διαχείριση και δεν μπορούμε επίσης να υποθέσουμε ότι όλες οι πληροφορίες μοιράζονται.

- Περιορισμένη ασφάλεια του φυσικού μέσου μετάδοσης (physical layer)

Τα κινητά ασύρματα δίκτυα είναι γενικά πιο ευπαθή σε θέματα ασφάλειας του φυσικού μέσου μετάδοσης σε σχέση με τα ασύρματα δίκτυα. Οι αυξημένες πιθανότητες για επιθέσεις τύπου eavesdropping, spoofing και DoS (Denial-of-Service) θα πρέπει να ληφθούν σοβαρά υπόψη. Συχνά εφαρμόζονται ήδη υπάρχον τεχνικές ασφάλειας στα ασύρματα δίκτυα για την μείωση των τρωτών σημείων στην ασφάλεια. Η αποκεντρωμένη φύση της διαχείρισης των δικτύων Ad Hoc παρέχει επιπλέον κάλυψη για περιπτώσεις που κάποιος κόμβος βγει εκτός λειτουργίας (single point failure) σε σχέση με τις πιο συγκεντρωμένες (centralized) προσεγγίσεις.

- Κλιμάκωση (Scalability)

Σε κάποια πιθανά δίκτυα Ad Hoc όπως στρατιωτικά δίκτυα ή δίκτυα σε αυτοκινητόδρομους, ο αριθμός των κόμβων ενδέχεται να είναι σχετικά μεγάλος, μερικές δεκάδες ή ακόμα και εκατοντάδες κόμβοι ανά περιοχή δρομολόγησης (routing area), επομένως απαιτείται η υποστήριξη κλιμάκωσης σε αυτά τα δίκτυα.

## 2.3 Εφαρμογές Δικτύων Ad-Hoc

Υπάρχουν κάποιες περιπτώσεις, στις οποίες δεν είναι διαθέσιμη κάποια σταθερή ενσύρματη δικτυακή υποδομή όπως το Internet, είτε επειδή μπορεί να μην είναι οικονομικά και χρονικά πρακτικό είτε φυσικά εφικτό, να παρασχεθεί η απαραίτητη υποδομή. Σε τέτοιες περιπτώσεις, μία συλλογή κινητών χρηστών μπορεί να σχηματίσει ένα προσωρινό δίκτυο, χωρίς να προαπαιτήσει οποιασδήποτε εγκατεστημένης υποδομής ή κεντρικής διαχείρισης.

Τα Ad-hoc δίκτυα χρησιμοποιήθηκαν σε πολλές περιπτώσεις:

- Στρατιωτικές επιχειρήσεις

Οι στρατιώτες με τον τρόπο αυτό μπορούν να αναμεταδίδουν πληροφορίες, για να παρέχουν ενημέρωση για την κατάσταση στο πεδίο της μάχης (σχήμα 3).

- Επιχειρήσεις ομάδων διάσωσης

Τα μέλη της ομάδας, συνήθως κάτω από αντίξοες συνθήκες, πρέπει να βρίσκονται σε συνεχή επικοινωνία για την ανταλλαγή σχετικών πληροφοριών.

- Υποανάπτυκτες περιοχές

Χώρες του τρίτου κόσμου αποτελούμενες από δύσβατα εδάφη, έχουν τη δυνατότητα να εγκαταστήσουν απευθείας ad hoc δίκτυα, χωρίς να πρέπει πρώτα να ξοδέψουν τον χρόνο, το χρήμα και την ενέργεια που απαιτείται κατά την εγκατάσταση ενός ενσύρματου δικτύου.

- Εμπορικά περιβάλλοντα

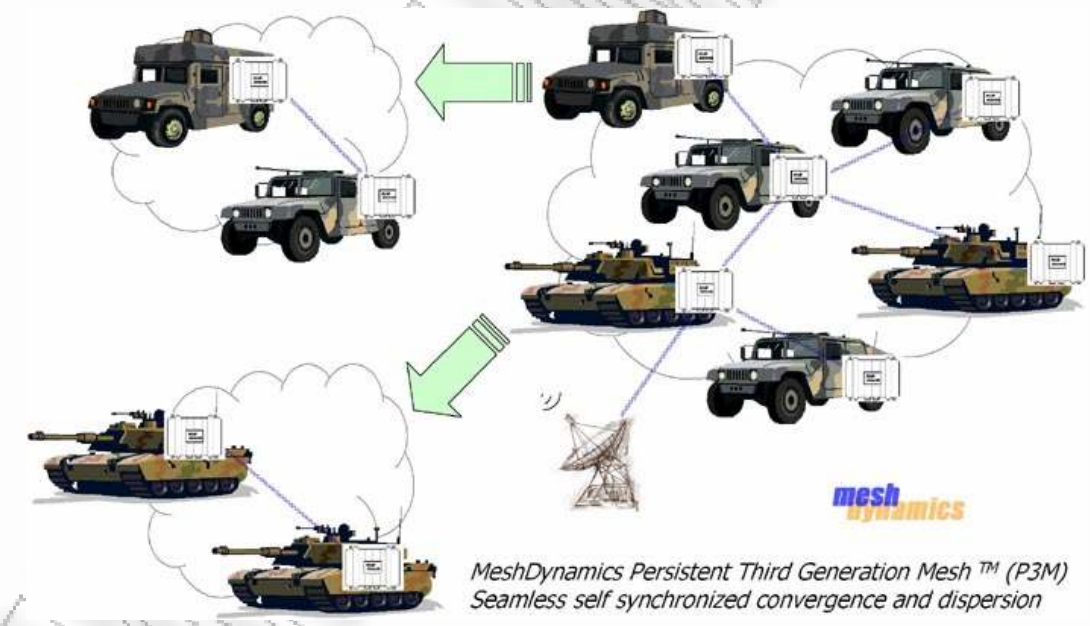
Προσφέρουν υπηρεσίες όπως το ηλεκτρονικό εμπόριο, τη δυναμική πρόσβαση σε στοιχεία πελατών που είναι αποθηκευμένα σε μια κεντρική μονάδα, την παροχή συνεπών βάσεων δεδομένων προς όλους τους πελάτες.

- Εκπαιδευτικές εφαρμογές

Μία ομάδα υπαλλήλων συνδέουν τους φορητούς υπολογιστές τους, ώστε να εξυπηρετηθούν οι ανάγκες μίας on-line σύσκεψης ή παρουσίασης, όπου σε έναν υπολογιστή θα γίνεται η παρουσίαση και οι υπόλοιποι θα μπορούν να την παρακολουθούν από τους προσωπικούς τους υπολογιστές. Επίσης, μία ομάδα ερευνητών της επιστήμης των υπολογιστών, οι οποίοι συγκεντρώνονται σε ένα χώρο για μία διάσκεψη, μπορούν να ενώσουν τους φορητούς υπολογιστές τους σε ένα τοπικό δίκτυο με διαμοιραζόμενα δεδομένα και πόρους εκτύπωσης.

- Υπηρεσίες με γνώση της τοποθεσίας

Περιλαμβάνουν υπηρεσίες πληροφορίας, όπως για παράδειγμα διαφήμιση ειδικών υπηρεσιών της τοποθεσίας ή εμφάνιση σε έναν τουρίστα ενός ταξιδιωτικού οδηγού μόλις εισέρχεται στην συγκεκριμένη περιοχή.




**Σχήμα 3** Στρατιωτικό δίκτυο Ad Hoc

# 3. Πρωτόκολλα Δρομολόγησης Ad-Hoc Δικτύων

## 3.1 Χαρακτηριστικά Πρωτοκόλλων Δρομολόγησης

Επειδή τα δίκτυα Ad-Hoc έχουν μια ιδιαίτερα δυναμική τοπολογία και υπάρχει έλλειψη κεντρικής διαχείρισης, δηλαδή ένα πακέτο για να φτάσει από έναν κόμβο-αποστολέα σε έναν κόμβο-παραλήπτη μπορεί να περάσει από πολλούς ενδιάμεσους κόμβους, χρειάζεται η ύπαρξη ενός πρωτόκολλου δρομολόγησης πακέτων. Λόγω των ζητημάτων που προκύπτουν, ένα πρωτόκολλο δρομολόγησης για τα ασύρματα ad hoc δίκτυα πρέπει να έχει και να ικανοποιεί συγκεκριμένες απαιτήσεις:

- Το πρωτόκολλο θα πρέπει να είναι διανεμημένο και ανεξάρτητο από τη διαχείριση από κάποιον κεντρικό κόμβο.
- Πρέπει να υπάρχουν ελάχιστες περιοδικές εκπομπές πακέτων επιπλέον πληροφορίας, ενώ ταυτόχρονα οι πεσμένες ζεύξεις (broken links) ή οι καινούριες διαδρομές θα πρέπει να ανιχνεύονται όσο το δυνατόν πιο γρήγορα.
- Η ελαχιστοποίηση της απαιτούμενης υπολογιστικής ισχύος και της απαιτούμενης μνήμης στους κόμβους.
- Δε θα πρέπει να δημιουργούνται αέναοι βρόχοι (loop free), αποφεύγοντας προβλήματα όπως το άθροισμα μέχρι το άπειρο (count to infinity problem).
- Θα πρέπει να επεκτείνονται και σε πολύ μεγάλα δίκτυα (scalable).
- Πρέπει να είναι ανεξάρτητα από το φυσικό μέσο μετάδοσης (physical layer), αλλά και του πρωτοκόλλου μετάδοσης (link layer protocol). Επίσης θα πρέπει να λαμβάνονται υπόψη και πρωτόκολλα μετάδοσης περιορισμένης εμβέλειας, όπως οι υπέρυθρες (IrDA) και οι ραδιοσυχνότητες (radio frequency).
- Θα πρέπει να εγκαταλείπονται συνετά οι προσπάθειες εύρεσης ενός κόμβου που είναι εκτός εμβέλειας, ώστε να μη δεσμεύεται αναγκαίο εύρος ζώνης (bandwidth). Έτσι αποφεύγονται προβλήματα όταν μέρος του δικτύου βρεθεί εκτός εμβέλειας ή βγει εκτός λειτουργίας.
- Θα πρέπει, να είναι συμβατό με τα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης των ενσύρματων δικτύων.
- Θα πρέπει ο αλγόριθμος να είναι απλός, ώστε να είναι εύκολος στην κατανόηση και στην εφαρμογή.

## 3.2 Κατηγορίες πρωτοκόλλων Δρομολόγησης

Μπορούμε να ταξινομήσουμε τα πρωτόκολλα δρομολόγησης για τα ad hoc δίκτυα σύμφωνα με διαφορετικά κριτήρια:

- Μηχανισμός πληροφοριών δρομολόγησης με αναπροσαρμογή ή ενημέρωση (update).

Αυτά τα πρωτόκολλα μπορούν να ενεργοποιηθούν είτε από έναν πίνακα δρομολόγησης είτε μετά από αίτηση. Στη πρώτη περίπτωση, κάθε κόμβος αποθηκεύει τις πληροφορίες δικτύων σε έναν πίνακα δρομολόγησης, ο οποίος ενημερώνεται περιοδικά. Προκειμένου να φτάσουμε στον προορισμό, ο κόμβος χρησιμοποιεί έναν κατάλληλο αλγόριθμο εύρεσης πορείας για να βρει την πιο σύντομη διαδρομή. Τα χαρακτηριστικά πρωτόκολλα αυτής της περίπτωσης είναι τα εξής: DSDV, WRP, CGSR, STAR, OLSR, FSR, HSR και GSR. Στη δεύτερη περίπτωση οι κόμβοι δεν χρειάζεται να διατηρήσουν την τοπολογία του δικτύου. Η διαδρομή τους γνωστοποιείται όταν την χρειάζονται, με τη χρησιμοποίηση μιας διαδικασίας σύνδεσης. Το πλεονέκτημα είναι ότι οι κόμβοι δεν χρειάζεται να ανταλλάσουν πληροφορίες δρομολόγησης περιοδικά. Τα χαρακτηριστικά πρωτόκολλα αυτής της περίπτωσης είναι τα: DSR, AODV, ABR, SSA, FORP και PLBR. Μερικά πρωτόκολλα, όπως τα CEDAR, ZRP, ZHLS, συνδυάζουν και τα δύο χαρακτηριστικά γνωρίσματα και ονομάζονται υβριδικά πρωτόκολλα δρομολόγησης.

- Χρήση των χρονικών πληροφοριών για τη δρομολόγηση.

Αυτή η ταξινόμηση είναι βασισμένη στη χρήση των χρονικών πληροφοριών που χρησιμοποιείται για τη διαδικασία δρομολόγησης. Δεδομένου ότι τα ad hoc δίκτυα είναι ιδιαίτερα δυναμικά, είναι πολύ σημαντικό να χρησιμοποιηθούν οι χρονικές πληροφορίες για τη δρομολόγηση. Σύμφωνα με το χρόνο των πληροφοριών, παίρνουμε δύο περαιτέρω ταξινομήσεις σε αυτήν την κατηγορία:

a) Πρωτόκολλα δρομολόγησης που χρησιμοποιούν τις πρότερες χρονικές πληροφορίες, δηλ. κάνουν χρήση πληροφόρησης για την προηγούμενη θέση των συνδέσεων ή τη θέση των συνδέσεων κατά τη διάρκεια της δρομολόγησης, ώστε να λάβουν τις αποφάσεις δρομολόγησης. Τέτοια πρωτόκολλα είναι τα DSDV, WRP, STAR, AODV, FSR, HSR, GSR.

b) Πρωτόκολλα δρομολόγησης που χρησιμοποιούν τις μελλοντικές χρονικές πληροφορίες, δηλ. κάνουν χρήση πληροφόρησης για την αναμενόμενη μελλοντική θέση των ασύρματων συνδέσεων προκειμένου να λάβουν τις αποφάσεις δρομολόγησης. Τέτοια πρωτόκολλα είναι τα FORP, RABR, LBR.

- Οργάνωση πληροφοριών τοπολογίας.

Δεδομένου ότι ο αριθμός κόμβων στα ad hoc δίκτυα είναι γενικά μικρός, είναι πιθανό να χρησιμοποιηθεί είτε μια επίπεδη τοπολογία, είτε μια ιεραρχική τοπολογία για τη δρομολόγηση. Στην πρώτη περίπτωση, πρέπει να υποτεθεί η διαθεσιμότητα ενός μοναδικού μηχανισμού διευθυνσιοδότησης για τους κόμβους στα ad hoc ασύρματα δίκτυα. Πρωτόκολλα όπως τα DSR, AODV, ABR, SSA, FORP, PLBR ανήκουν σε αυτήν την περίπτωση. Τα πρωτόκολλα της δεύτερης περίπτωσης κάνουν χρήση μιας λογικής ιεραρχίας στο δίκτυο και ενός σχετικού σχεδίου διευθυνσιοδότησης. Τα πρωτόκολλα CGSR, FSR, HSR είναι αυτής της περίπτωσης.

- Χρησιμοποίηση συγκεκριμένων πόρων.

Τα πρωτόκολλα αυτής της κατηγορίας μπορούν να ταξινομηθούν περαιτέρω σε δύο τύπους:

a) Πρωτόκολλα δρομολόγησης ενήμερα για την ενέργεια (power aware): Πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία προσπαθούν να ελαχιστοποιήσουν την κατανάλωση ενέργειας από τη μπαταρία. Ένα χαρακτηριστικό πρωτόκολλο είναι το PAR.

b) Πρωτόκολλα δρομολόγησης που υποβοηθούνται από γεωγραφικές πληροφορίες: Τα πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία προσπαθούν να βελτιώσουν την απόδοση της δρομολόγησης και να μειώσουν την επιβάρυνση ελέγχου με αποτελεσματική χρήση των γεωγραφικών πληροφοριών. Ένα χαρακτηριστικό πρωτόκολλο είναι το LAR.

# 4. Ασφάλεια Δικτύων Ad-Hoc

## 4.1 Εισαγωγή

Στα παρακάτω κεφάλαια αναπτύσσονται όλα τα θέματα ασφαλείας των δικτύων. Αυτά είναι τα χαρακτηριστικά της ασφαλείας που πρέπει να εφαρμοστούν για να θεωρείται επιτυχής, τα είδη απειλών και επιθέσεων στα ad-hoc δίκτυα, καθώς και οι τρόποι αντιμετώπισης των απειλών.

## 4.2 Χαρακτηριστικά Ασφάλειας

Ο στόχος της ασφάλειας είναι να παρασχεθούν οι υπηρεσίες ασφάλειας που υπερασπίζουν το ad-hoc δίκτυο ενάντια σε όλα τα είδη απειλής που εξηγούνται σε αυτό το κεφάλαιο. Τα χαρακτηριστικά της ασφάλειας περιλαμβάνουν τα εξής:

- Διαθεσιμότητα

Η διαθεσιμότητα εξασφαλίζει την βιωσιμότητα των υπηρεσιών του δικτύου, παρά τις επιθέσεις denial of services (DoS) που δέχεται. Επίσης, τα συστήματα που εξασφαλίζουν τη διαθεσιμότητα προσπαθούν να καταπολεμήσουν τις επιθέσεις κατανάλωσης ενέργειας, καθώς επίσης την παρεκτροπή των κόμβων και την εγωιστική συμπεριφορά τους κατά την προώθηση μηνυμάτων. Οι παραπάνω απειλές θα παρουσιαστούν στη συνέχεια. Στο φυσικό επίπεδο, ένας αντίπαλος μπορεί να προκαλέσει συνωστισμό (jamming) για να παρέμβει στις επικοινωνίες. Στο επίπεδο δικτύου, μπορεί να διαταραχτεί το πρωτόκολλο προώθησης και να διακοπεί το δίκτυο. Σε ανώτερα επίπεδα μπορούν να ανατραπούν οι αντίστοιχες υπηρεσίες, όπως είναι η υπηρεσία διαχείρισης κλειδιού.

- Εμπιστευτικότητα

Η εμπιστευτικότητα εξασφαλίζει ότι η πληροφορία δεν εκτίθεται σε μη εξουσιοδοτημένες πηγές. Η μετάδοση ευαίσθητων πληροφοριών, όπως είναι στρατηγικές ή τακτικές στρατιωτικές πληροφορίες, απαιτεί εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών σε εχθρούς σε περίοδο πολέμου αλλά και ειρήνης, όπως είναι οι στρατιωτικές ασκήσεις, μπορούν να έχουν καταστροφικές συνέπειες. Η πληροφορία δρομολόγησης πρέπει επίσης να μείνει εμπιστευτική σε ορισμένες περιπτώσεις γιατί αυτή μπορεί να είναι πολύτιμη για τον εχθρό ώστε να εξακριβώσει

και να προσδιορίσει τους στόχους του στο πεδίο της μάχης. Η συνήθης τακτική για να κρατηθούν ευαίσθητα δεδομένα ασφαλή είναι η κρυπτογράφηση των δεδομένων με ένα μυστικό κλειδί, το οποίο μόνο οι επίδοξοι λήπτες κατέχουν. Επειδή η κρυπτογράφηση δημόσιου κλειδιού είναι πολύ ενεργοβόρα σε τέτοιου είδους δίκτυα, τα περισσότερα από τα προτεινόμενα πρωτόκολλα χρησιμοποιούν μεθόδους κρυπτογράφησης συμμετρικού κλειδιού.

- Αυθεντικότητα

Η αυθεντικότητα επιτρέπει σ' ένα κόμβο να διασφαλίσει την ταυτότητα του κάθε κόμβου κατά την διάρκεια της επικοινωνίας τους. Χωρίς την αυθεντικότητα, ένας αντίπαλος μπορεί να μεταμφιέσει έναν κόμβο και έτσι να κερδίσει μη εξουσιοδοτημένη πρόσβαση σε πηγές του δικτύου, σε ευαίσθητες πληροφορίες και να παρέμβει στις λειτουργίες άλλων κόμβων. Έτσι, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς του προγράμματος, όπως εκ νέου προγραμματισμός του δικτύου, έλεγχος κύκλου ασφαλείας σ' ένα κόμβο κ.ά. Η αυθεντικότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε τοπικά από τον πραγματικό αποστολέα. Η αυθεντικότητα μπορεί να επιτευχθεί με έναν καθαρά συμμετρικό μηχανισμό. Ο αποστολέας και ο λήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο υπολογίζουν έναν κώδικα αυθεντικότητας μηνύματος (message authentication code - MAC) για όλα τα αποστελλόμενα δεδομένα. Όταν ένα μήνυμα με τον σωστό MAC φτάσει, ο λήπτης ξέρει την ταυτότητα του αποστολέα. Όμως, κατά την εκπομπή μηνύματος προς πολλούς αποδέκτες, χρειάζονται ισχυρότεροι δεσμοί εμπιστοσύνης. Σε αυτή την περίπτωση, μπορούν να χρησιμοποιηθούν άλλες τεχνικές όπως είναι τα πρωτόκολλα SPINS και LEAP.

- Μη αποποίηση

Η απαίτηση της μη αποποίησης εξασφαλίζει ότι ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα. Η μη αποποίηση είναι χρήσιμη στην επισήμανση και απομόνωση εκτεθειμένων κόμβων. Έτσι, όταν ένας κόμβος Α δέχεται ένα λανθασμένο μήνυμα από έναν κόμβο Β, η μη αποποίηση επιτρέπει στον Α να κατηγορήσει τον Β ότι αυτός έστειλε το μήνυμα και να πείσει τους υπόλοιπους κόμβους του δικτύου ότι ο Β είναι εκτεθειμένος. Οι ψηφιακές υπογραφές μπορεί να είναι μία λύση για την παραπάνω περίπτωση.

- Ανανέωση Δεδομένων

Η απαίτηση για ανανέωση των δεδομένων δηλώνει ότι οι πληροφορίες και τα μηνύματα που ανταλλάσσονται είναι έγκυρα και διαβεβαιώνει ότι δεν επαναλαμβάνεται αναμετάδοση παλαιών μηνυμάτων. Σε όλα τα μηνύματα, συνήθως, παρέχεται ένας καταμετρητής χρόνου. Βάσει του μετρητή μπορούμε να διασφαλίσουμε ότι η πληροφορία που λαμβάνουμε είναι καινούρια. Ένας κοινός τρόπος αντιμετώπισης απειλών είναι να περιλάβουμε έναν αυξανόμενο μετρητή με κάθε μήνυμα το οποίο στέλνεται και να απορρίψουμε μηνύματα με παλαιές τιμές του μετρητή. Επίσης η ανανέωση μπορεί να αφορά στην ανανέωση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Στην περίπτωση αυτή, κάθε κλειδί βεβαιωμένης μεθόδου μπορεί να βεβαιώσει ότι το διαμοιραζόμενο κλειδί ανάμεσα στους εμπλεκόμενους είναι καινούργιο.

- Ακεραιότητα πληροφορίας

Η ακεραιότητα πληροφορίας δηλώνει την γνησιότητα των δεδομένων που στέλνονται μεταξύ εμπλεκομένων. Έτσι, ένα μήνυμα που στέλνεται από έναν κόμβο Α σ' ένα κόμβο Β δεν έχει τροποποιηθεί από έναν κακόβουλο κόμβο Γ κατά τη διάρκεια της μετάδοσης. Ένα μήνυμα μπορεί επίσης να τροποποιηθεί ή να καταστραφεί λόγω εξασθένησης του σήματος. Η υπηρεσία της ακεραιότητας πληροφορίας παρέχεται συχνά από την υπηρεσία της αυθεντικότητας ώστε να εξασφαλιστεί η ασφάλεια του δικτύου. Ένα καλό και ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας ώστε αν μια παράβαση διαπιστωθεί, τότε άμεσα η υπηρεσία να αναφέρει αυτό το πρόβλημα.

- Επεκτασιμότητα

Συνήθως τα δίκτυα που εξετάζουμε χρειάζονται επέκταση με προσθήκη μεγάλου αριθμού νέων κόμβων. Η ανάγκη αυτή απαιτεί δίκτυα τα οποία να μπορούν να έχουν ιδιότητες επέκτασης, είτε ως προς το ενεργειακό μέρος είτε ως προς το θέμα αναδιοργάνωσης του δικτύου. Ο αριθμός των γειτόνων, οι αποστάσεις μεταξύ τους και η απαιτούμενη ισχύς για την αποστολή μηνυμάτων από έναν κόμβο στον άλλο, πιθανόν να μην είναι γνωστά κατά τη διάρκεια ζωής ενός δικτύου. Έτσι οι κόμβοι στα υπό εξέταση δίκτυα πρέπει να είναι ικανοί να αυτό-οργανώνονται και να επιλέγουν τους κατάλληλους μηχανισμούς που ταιριάζουν σε κάθε περίσταση.

- Συνεργασία

Εκτός από την ασφαλή αποστολή και λήψη μηνυμάτων, η υποκίνηση της συνεργασίας είναι ένα σημαντικό θέμα ασφαλείας. Λόγω του περιορισμένου αριθμού πηγών του δικτύου, οι συσκευές του δικτύου τείνουν να γίνουν εγωκεντρικές. Έτσι χρειάζεται ένα είδος υποκίνησης για να παρακινηθεί η συνεργασία στο δίκτυο. Πολλές μέθοδοι δουλεύουν δίνοντας κίνητρο για επιτυχή συνεργασία, ενώ άλλες τιμωρούν την εγωιστική συμπεριφορά.

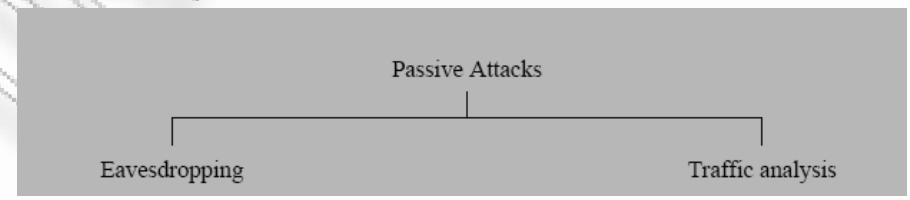
## 4.3 Επιθέσεις κατά δικτύων Ad-hoc

Οι επιθέσεις ασφάλειας μπορούν να ταξινομηθούν σε δύο ευρείες κατηγορίες: ενεργητικές και παθητικές επιθέσεις. Στις παθητικές επιθέσεις, οι αντίπαλοι δεν κάνουν καμιά εκπομπή, είναι κυρίως ενάντια στην εμπιστευτικότητα των στοιχείων του μηνύματος. Στις ενεργές επιθέσεις, οι κακόβουλες πράξεις πραγματοποιούνται όχι μόνο ενάντια στην εμπιστευτικότητα αλλά και στην ακεραιότητα των στοιχείων. Οι ενεργές επιθέσεις μπορούν επίσης να στοχεύσουν τη μη εξουσιοδοτημένη πρόσβαση και τη χρήση των πόρων ή τη διαταραχή των επικοινωνιών ενός αντιπάλου.

Από ένα λάθος, οι χρήστες μπορούν να εκθέσουν τους κόμβους στις απειλές όπως να πειράξουν και να καταστρέψουν ή να εκθέσουν στοιχεία σε όσους δεν έχουν εξουσιοδοτημένη πρόσβαση. Τα συστήματα ασφάλειας πρέπει επίσης να αντιμετωπίσουν τις προκλήσεις προστασίας και ασφάλειας που δημιουργούνται από την απρόσεκτη χρήση κατά την διάρκεια κάποιων γεγονότων

### 4.3.1 Παθητικές Επιθέσεις

Στις παθητικές επιθέσεις οι επιτιθέμενοι είναι χαρακτηριστικά καλυμμένοι και εισέρχονται στις γραμμές επικοινωνίας για να συλλέξουν τα στοιχεία της πληροφορίας που θέλουν. Οι παθητικές επιθέσεις (σχήμα 4) μπορούν να ομαδοποιηθούν σε δύο διαφορετικούς τύπους. Σε αυτούς που «κρυφακούν» και σε αυτούς που αναλύουν την κυκλοφορία.




**Σχήμα 4** Παθητικές Επιθέσεις

#### 4.3.1.1 Eavesdropping

Τα ταξινομημένα στοιχεία μπορούν να κρυφακουστούν με την υποκλοπή των γραμμών επικοινωνίας, για το λόγο αυτό οι ασύρματες συνδέσεις είναι ευκολότερες σε τέτοιου είδους επιθέσεις. Όταν είναι γνωστά τα πρότυπα τα οποία χρησιμοποιούνται για τα δεδομένα, δηλαδή μη κρυπτογραφημένα, ένας αντίπαλος μπορεί εύκολα να λάβει και να διαβάσει τα στοιχεία που μεταδίδονται μέσω των οπτικοακουστικών μεταδόσεων. Παραδείγματος χάριν, ένας αντίπαλος μπορεί εύκολα να κρυφακούσει τους αριθμούς και τους κωδικούς πρόσβασης πιστωτικών καρτών όταν διαβιβάζονται απλά πέρα από τις ανασφαλείς ασύρματες συνδέσεις.

Πραγματικά, τα ad hoc δίκτυα και τα δίκτυα αισθητήρων είναι πιο ασφαλή ενάντια στην υποκλοπή έναντι άλλης ασύρματης τεχνολογίας επειδή τα σήματα δεν στέλνονται πέρα από τις πιο σύντομες αποστάσεις. Ένας αντίπαλος πρέπει να φτάσει αρκετά κοντά στον επιτιθέμενο κόμβο για να είναι σε θέση να υποκλέψει κάποια δεδομένα. Εάν το μέσο όπου αυτές οι ασύρματες τεχνολογίες χρησιμοποιούν έχουν αρκετό διάστημα ελέγχου ενάντια στους εισβολείς, δηλαδή σε ανθρώπους και συσκευές που δεν έχουν εξουσιοδότηση, αυτά γίνονται ασφαλέστερα. Ένα μέλος το οποίο είναι κοντά στο τερματικό που είναι στόχος μπορεί να λάβει όλα τα πλαίσια τα οποία στέλνει ή λαμβάνει, να τα αποθηκεύσει σε κάποιο μέσο και να τα πάρει. Αυτοί οι κίνδυνοι μπορούν να μειωθούν από τις προσεκτικές επιθεωρήσεις ή με τον έλεγχο των ηλεκτρομαγνητικών εκπομπών από το μέσο. Ακόμα, οι κίνδυνοι είναι πολύ υψηλότεροι όταν χρησιμοποιούνται οι ασύρματες τεχνολογίες.

Επιπλέον, η ύπαρξη των ασύρματων επικοινωνιών καθιστά την εφαρμογή των πολλαπλών δικτύων με τα διαφορετικά επίπεδα ασφάλειας σε μια δυσκολότερη ενιαία εγκατάσταση. Παραδείγματος χάριν, εάν υπάρχουν ταξινομημένα δίκτυα και ένα δίκτυο που συνδέεται με το Διαδίκτυο στο ίδιο μέσο και η ασύρματη πρόσβαση στα ταξινομημένα δίκτυα επιτρέπεται, με την αποσύνδεση του Διαδικτύου τα ταξινομημένα δίκτυα μπορούν να γίνουν πολύ δύσκολα στις παθητικές επιθέσεις.

Για την προστασία της μυστικότητας, η ανωνυμία είναι σημαντική. Οι επιθέσεις ενάντια στη μυστικότητα μπορούν να αρχίσουν με τις επιθέσεις ενάντια στην ανωνυμία. Ένας αντίπαλος πρώτα πρέπει να ξέρει ποιος κόμβος εξυπηρετεί ποιο άτομο και για ποιο σκοπό. Ομοίως, πρέπει να ξέρει ποιο πακέτο στοιχείων προέρχεται από ποιο κόμβο. Αφότου επιτυγχάνεται αυτό, τα στοιχεία που συλλέγονται μπορούν να γίνουν σημαντικότερα. Επομένως, η μυστικότητα και η εμπιστευτικότητα μπορούν να ενισχυθούν από την ανωνυμία.

#### 4.3.1.2 Traffic analysis

Όπως και το περιεχόμενο των δεδομένων των πακέτων, η ανάλυση της κυκλοφορίας μπορεί επίσης να είναι πολύ σημαντική για τους αντιπάλους. Παραδείγματος χάριν, οι σημαντικές πληροφορίες για την τοπολογία δικτύωσης μπορούν να παραχθούν με την ανάλυση της κυκλοφορίας. Στα ad hoc δίκτυα και ειδικά στα δίκτυα αισθητήρων, οι κόμβοι που βρίσκονται πιο κοντά στο σταθμό βάσης, κάνουν περισσότερες μεταδόσεις από τους άλλους κόμβους επειδή αναμεταδίδουν περισσότερα πακέτα από τους κόμβους που βρίσκονται μακριά από το σταθμό βάσης. Ομοίως, η ομαδοποίηση (clustering) είναι ένα σημαντικό εργαλείο για την εξελιξιμότητα στα ad hoc δίκτυα και οι επικεφαλείς των ομάδων είναι πιο πολυάσχολοι από τους άλλους κόμβους στο δίκτυο. Οι κόμβοι που βρίσκονται κοντά σε ένα σταθμό βάσης ή οι επικεφαλείς των συστάδων μπορεί να είναι πολύ χρήσιμοι για τους αντιπάλους επειδή μια επίθεση DoS ενάντια σε αυτούς τους κόμβους μπορεί να ασκήσει μεγαλύτερη επίδραση στο δίκτυο. Με την ανάλυση της κυκλοφορίας, αυτό το είδος πολύτιμων πληροφοριών μπορεί να παραχθεί.

Η ανάλυση κυκλοφορίας μπορεί επίσης να χρησιμοποιηθεί για να οργανώσει τις επιθέσεις ενάντια στην ανωνυμία. Η ανίχνευση των κόμβων της πηγής για ορισμένα πακέτα δεδομένων μπορεί επίσης να είναι ένας στόχος για τους αντιπάλους. Αυτές οι πληροφορίες βοηθούν να ανιχνεύσουν τη θέση των γεγονότων, τις αδυναμίες, τις ικανότητες και τις λειτουργίες του δικτύου ή τους ιδιοκτήτες των κόμβων.

Επιπλέον, τα δείγματα της κυκλοφορίας μπορούν να αναφέρονται και σε άλλες εμπιστευτικές πληροφορίες όπως οι ενέργειες και οι προθέσεις. Στις τακτικές επικοινωνίες, η σιωπή μπορεί να δείξει την προετοιμασία για μια επίθεση, μια τακτική κίνηση ή μια διήθηση. Ομοίως, μια ξαφνική αύξηση στο ποσοστό κυκλοφορίας μπορεί να δείξει την έναρξη μιας σκόπιμης επίθεσης ή μιας επιδρομής. Οι παρόμοιες πληροφορίες μπορούν επίσης να παραχθούν από την ανάλυση κυκλοφορίας στα δίκτυα. Η ανάλυση κυκλοφορίας μπορεί να πραγματοποιηθεί για να απαριθμήσει τις συχνές επαφές κάθε τερματικού - αποκαλούμενου friendship trees. Με τον τρόπο αυτό, οι επαφές ενός κόμβου μπορούν να καθοριστούν.

Μια από τις ακόλουθες τεχνικές μπορεί να χρησιμοποιηθεί για την ανάλυση κυκλοφορίας:

Α) **Ανάλυση κυκλοφορίας στο φυσικό στρώμα**: σε αυτήν την επίθεση μόνο ο μεταφορέας αισθάνεται την επίθεση και τα ποσοστά κυκλοφορίας αναλύονται για τους κόμβους σε μια θέση.

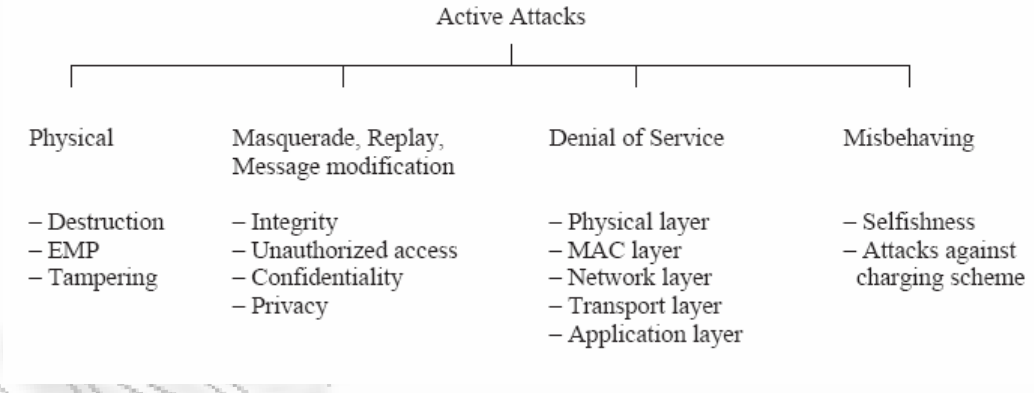
Β) **Ανάλυση κυκλοφορίας στη MAC και τα υψηλότερα στρώματα**: Τα πλαίσια της MAC και τα πακέτα δεδομένων μπορούν να υποπολλαπλασιαστούν και οι επιγραφές μπορούν να αναλυθούν. Αυτό μπορεί να αποκαλύψει διάφορες πληροφορίες δρομολόγησης καθώς και την τοπολογία του δικτύου.

Γ) **Ανάλυση κυκλοφορίας από το συσχετισμό γεγονότος**: γεγονότα όπως η ανίχνευση σε ένα δίκτυο αισθητήρων ή τη μετάδοση από ένα χρήστη μπορεί να συσχετιστεί με την κυκλοφορία και περισσότερες αναλυτικές πληροφορίες, μπορούν να παραχθούν.

Δ) **Ενεργός ανάλυση κυκλοφορίας**: η ανάλυση κυκλοφορίας μπορεί επίσης να διευθυνθεί ως ενεργός επίθεση. Παραδείγματος χάριν, ορισμένοι κόμβοι μπορούν να καταστραφούν, το οποίο υποκινεί το self organize στο δίκτυο, και τα πολύτιμα στοιχεία για την τοπολογία μπορούν να συγκεντρωθούν.

### 4.3.2 Ενεργές Επιθέσεις

Στις ενεργές επιθέσεις ένας αντίπαλος έχει επιπτώσεις πραγματικά στις διαδικασίες στο επιτεθειμένο δίκτυο. Αυτή η επίδραση μπορεί να είναι ο στόχος της επίθεσης και μπορεί να ανιχνευθεί. Παραδείγματος χάριν, οι υπηρεσίες δικτύωσης μπορούν να υποβιβαστούν ή να τερματίσουν ως συνέπεια αυτών των επιθέσεων. Μερικές φορές ο αντίπαλος προσπαθεί να μείνει μη ανιχνεύσιμος, στοχεύοντας να κερδίσει την πρόσβαση στους πόρους των συστημάτων ή απειλώντας την εμπιστευτικότητα ή και την ακεραιότητα του περιεχομένου του δικτύου. Ομαδοποιούμε τις ενεργές επιθέσεις σε τέσσερις κατηγορίες, όπως φαίνεται στο παρακάτω σχήμα (σχήμα 5).




**Σχήμα 5** Ενεργές Επιθέσεις

#### 4.3.2.1 Physical Attack

Ένας αντίπαλος μπορεί φυσικά να βλάψει το hardware προκειμένου να εξοντώσει τους κόμβους. Αυτό είναι μια επίθεση ασφάλειας η οποία μπορεί να θεωρηθεί μέσα στα επιτρεπτά όρια της ανοχής ελαττωμάτων, στην οποία υπάρχει η δυνατότητα να στηριχτούν οι λειτουργίες δικτύωσης χωρίς οποιαδήποτε διακοπή λόγω των αποτυχιών των κόμβων. Οι φυσικές επιθέσεις ενάντια στο hardware είναι ένα σοβαρό ζήτημα, ειδικά στις ad hoc επικοινωνίες και τα δίκτυα αισθητήρων. Οι κόμβοι αισθητήρων μπορούν να επεκταθούν αφύλακτοι σε περιοχές προσιτές από τον αντίπαλο. Επομένως, μπορούν να κινηθούν έξω από την περιοχή αισθητήρων ή να καταστραφούν. Όταν αυτοί οι κίνδυνοι είναι επικείμενοι, οι κόμβοι πρέπει να είναι ελαστικοί στις φυσικές επιθέσεις.

Όταν οι κόμβοι είναι αφύλακτοι και μπορεί ο αντίπαλος να έρθει σε επαφή, οι κόμβοι μπορούν να δεχθούν επίθεση με τεχνικές αλλοίωσης. Επομένως, η ανθεκτικότητα πλαστογραφήσεων είναι ένα ζήτημα που πρέπει να εξεταστεί προσεκτικά τόσο σε δίκτυα αισθητήρων και ad hoc όσο και σε εφαρμογές τακτικών επικοινωνιών.

Μπορούμε να ομαδοποιήσουμε τους κόμβους με βάση την τεχνική της αλλοίωσης σε δύο κατηγορίες: της επεμβατικής και της μη επεμβατικής αλλοίωσης. Οι επεμβατικές τεχνικές στοχεύουν να κερδίσουν την απεριόριστη πρόσβαση σε έναν κόμβο. Στις μη επεμβατικές επιθέσεις, η απεριόριστη πρόσβαση στον κόμβο δεν είναι η πρόθεση. Αντίθετα, αναλύοντας τη συμπεριφορά ενός κόμβου, όπως η κατανάλωση ενέργειας ή τις ρυθμίσεις χρονισμού εκτέλεσης των αλγορίθμων για διάφορες εισροές, μπορούν να προκύψουν εμπιστευτικά δεδομένα σχετικά με τις διαδικασίες και τα κλειδιά που χρησιμοποιούνται από τα συστήματα κρυπτογράφησης.

Οι επιθέσεις ηλεκτρομαγνητικών παλμών (EMP) είναι επίσης μεταξύ των απειλών που μπορούν να παρατίθενται στις επιθέσεις φυσικής ασφάλειας. Μια EMP είναι μια μικρής διάρκειας καταιγισμού υψηλής έντασης ηλεκτρομαγνητική ενέργεια που μπορεί να οδηγήσει σε απότομες αυξομειώσεις της τάσης και να καταστρέψει ηλεκτρονικές συσκευές εντός μιας συγκεκριμένης εμβέλειας. Μια EMP είναι ένα φυσικό αποτέλεσμα πυρηνικών εκρήξεων. Σήμερα, φορητές συσκευές που μπορούν να δημιουργήσουν EMPs είναι διαθέσιμες. Αν και υπάρχουν ακόμη άλυτα ζητήματα που σχετίζονται με το εφικτό EMP τεχνολογιών, είναι μια απειλή για όλα τα είδη των ηλεκτρικών συσκευών σε πεδίο τακτικής. Αυτό μπορεί να θεωρηθεί ως μέρος του τομέα ανοχής σφαλμάτων. Είναι δυνατή η δημιουργία ηλεκτρονικών συσκευών που είναι πιο ανθεκτική σε EMPs. Ως εκ τούτου, θα τοποθετήσουμε τις EMP επιθέσεις ως τύπος επίθεσης ασφαλείας.

#### 4.3.2.2 Masquerade, Replay and Message Modification

Ένας μεταμφιεσμένος κόμβος ενεργεί σαν είναι ένας άλλος κόμβος. Τα μηνύματα μπορούν να ληφθούν και να επαναληφθούν μέσω των κόμβων αυτών. Τέλος, το περιεχόμενο των ληφθέντων μηνυμάτων μπορεί να τροποποιηθεί πριν γίνει η επανάληψη τους. Διάφορα σενάρια και απειλές μπορούν να αναπτυχθούν με βάση αυτές τις προσεγγίσεις.

Τα δίκτυα Ad hoc και τα δίκτυα αισθητήρων εισάγουν τα ιδιαίτερα πλεονεκτήματα για την μεταμφίεση των κόμβων. Στα ad hoc δίκτυα, οι κόμβοι μπορούν να αλλάξουν τη θέση τους στο δίκτυο ανά τακτά χρονικά διαστήματα. Δεδομένου ότι οι αντιδραστικές τεχνικές προτιμώνται για τη δρομολόγηση, η τοπολογία δεν μπορεί να διατηρηθεί, κάνοντάς το δύσκολο να ελεγχθεί και αυτό έχει σαν συνέπεια να είναι δύσκολο το σημείου πρόσβασης ενός κόμβου στο δίκτυο. Επιπλέον, μπορεί να μην είναι δυνατό να ελεγχθεί εάν ο κόμβος έχει πρόσβαση ήδη σε ένα άλλο σημείο του δικτύου. Αντ' αυτού όμως, τεχνικές όπως της στοιχείο-κεντρικής δρομολόγησης και της επαναχρησιμοποίησης διευθύνσεων μπορούν να είναι σχέδιο εξέτασης.

Η μεταμφίεση, η επανάληψη μηνυμάτων και η τροποποίηση περιεχομένου μπορούν να χρησιμοποιηθούν για να επιτεθούν στην ακεραιότητα του περιεχομένου των μηνυμάτων ή των υπηρεσιών σε ένα δίκτυο. Τα δίκτυα αισθητήρων, συγκεκριμένα, έχουν διάφορες λειτουργίες δικτύων οι οποίες είναι ευαίσθητες στα πρόσθετα είδη επίθεσης επειδή είναι βασισμένες σε μια συνεργασμένη προσπάθεια των κόμβων. Παραδείγματος χάριν, τα σχέδια εντοπισμού κόμβων μπορούν να υπόκεινται σε μια από τις ακόλουθες επιθέσεις ασφάλειας:

• Ένας κακόβουλος κόμβος μπορεί να ενεργήσει ως αναγνωριστικό σήμα και να διαδώσει τη θέση του λανθασμένα. Αυτό παρακωλύει τη διαδικασία εντοπισμού του κόμβου όταν αυτός χρησιμοποιεί σήματα τα οποία εκπέμπονται από τον κακόβουλο κόμβο.

• Ένα αναγνωριστικό σήμα μπορεί να αλλαχθεί και να εισαγάγει λανθασμένα στοιχεία θέσης, να διαβιβάσει αναγνωριστικά σήματα με λιγότερη ή περισσότερη ενίσχυση από το αναμενόμενο για να εξασθενίσει την λαμβανόμενη ενίσχυση του σήματος του δέκτη.

• Τα αναγνωριστικά σήματα μπορούν να επαναληφθούν από έναν κακόβουλο κόμβο.

• Οι κόμβοι αναγνωριστικών σημάτων μπορούν να καταστραφούν από τις φυσικές επιθέσεις.

• Ένα εμπόδιο μπορεί να τοποθετηθεί μεταξύ των κόμβων αναγνωριστικών σημάτων και του δικτύου για να εμποδίσει την άμεση σύνδεση.

Μια βελτιωμένη έκδοση της μεταμφίεσης είναι μια επίθεση sybil, όπου ένας κακόβουλος κόμβος εισάγει τον εαυτό του πολλαπλά στο δίκτυο. Η κατοχή των

πολλαπλών προσδιορισμών μπορεί να είναι πολύ χρήσιμη για έναν κακόβουλο κόμβο. Ένας κόμβος που στέλνει πολλαπλές τιμές με τους διαφορετικούς προσδιορισμούς μπορεί να αλλάξει την συνολική αξία σημαντικά. Μια επίθεση sybil μπορεί επίσης να απειλήσει τις πολλαπλές δρομολογήσεις καθώς και τον εντοπισμό των κόμβων, κ.λπ. Τέλος, μπορούν επίσης να βοηθήσουν να κρατήσουν τις επιθέσεις κρυμμένες.

Η μεταμφίεση, η επανάληψη των μηνυμάτων και η τροποποίηση περιεχομένου μπορούν επίσης να χρησιμοποιηθούν ενάντια στην εμπιστευτικότητα κάνοντας τους υπόλοιπους κόμβους να στέλνουν εμπιστευτικά στοιχεία σε έναν κακόβουλο κόμβο και με τον τρόπο αυτό να του παρέχεται πρόσβαση σε όλους τους πόρους του συστήματος.

Ένας αντίπαλος κάνει phishing, το οποίο σημαίνει ότι εξαπατά κάποιον κόμβο προκειμένου να του δώσει τις εμπιστευτικές πληροφορίες εθελοντικά. Ο όρος αυτός είναι ένας συνδυασμός δύο λέξεων - κωδικός πρόσβασης και phishing - που καθορίζουν αυτήν την επίθεση. Ένας κακόβουλος κόμβος υποδύεται ότι είναι ένας εξουσιοδοτημένος κόμβος και μπορεί να ζητήσει από έναν άλλο κόμβο να του δώσει πληροφορίες για τους κωδικούς πρόσβασης, τα κλειδιά, κ.λπ.

Η μεταμφίεση είναι επίσης μια προσέγγιση για τη συντήρηση της ανωνυμίας ενός κακόβουλου κόμβου που παρέχει το παράνομο περιεχόμενο, ή ένας που επιτίθενται ή κερδίζει στην παράνομη πρόσβαση σε ένα μακρινό σύστημα, π.χ. μια σημαντική βάση δεδομένων της κυβέρνησης ή των τραπεζών.

#### 4.3.2.3 Denial of Service Attacks

Μια επίθεση άρνησης υπηρεσιών (DoS) στοχεύει κυρίως στη διαθεσιμότητα των υπηρεσιών δικτύων. Ένα DoS ορίζεται ως οποιοδήποτε γεγονός που μικραίνει την ικανότητα ενός δικτύου να εκτελέσει την αναμενόμενη λειτουργία του σωστά ή κατά τρόπο έγκαιρο (Wood και Stankovic, 2005). Μια επίθεση DoS χαρακτηρίζεται από τις ακόλουθες ιδιότητες:

• Κακόβουλος: πραγματοποιείται για να αποτρέψει το δίκτυο από την πραγματοποίηση των προοριζόμενων λειτουργιών του. Δεν είναι τυχαίο και δεν ανήκει στην περιοχή ανοχής της ασφάλειας και των ελαττωμάτων.

• Αποδιοργανωτικός: υποβιβάζει την ποιότητα των υπηρεσιών που προσφέρονται από το δίκτυο.

• Ασύμμετρος: ο επιτιθέμενος υποβάλλει την λιγότερη προσπάθεια έναντι της κλίμακας του αντίκτυπου που έχει στο δίκτυο. Κάθε υπηρεσία δικτύωσης μπορεί να υπόκειται σε μια επίθεση DoS.

Σε αυτό το τμήμα θα εξετάσουμε τα σημαντικά σενάρια DoS για τα Ad Hoc δίκτυα.

**A) DoS in Physical Layer**

Σε αυτό το τμήμα, το φυσικό στρώμα δείχνει το στρώμα του μοντέλου του OSI που είναι αρμόδιο για να αντιπροσωπεύσει τα σωστά 1s και 0s στο ασύρματο μέσο, και μια επίθεση DoS στο φυσικό στρώμα, που καλείται παρεμβολή παρασίτων, σημαίνει μια απειλή ασφάλειας ενάντια σε αυτό.

Μια κακόβουλη συσκευή μπορεί να φράξει έναν ασύρματο μεταφορέα με τη διαβίβαση ενός σήματος σε εκείνη την συχνότητα. Τα παράσιτα συμβάλλουν στο θόρυβο του φέροντος και η δύναμή τους είναι αρκετή να μειώσει το σήμα κάτω από το επίπεδο που οι κόμβοι που χρησιμοποιούν εκείνη την στιγμή τα κανάλια να παραλαμβάνουν σωστά τα δεδομένα. Η παρεμβολή παρασίτων μπορεί να διευθυνθεί συνεχώς σε μια περιοχή, η οποία ανατρέπει όλους τους κόμβους σε εκείνη την περιοχή από την επικοινωνία. Εναλλακτικά, η παρεμβολή παρασίτων μπορεί να γίνει προσωρινά με τυχαία χρονικά διαστήματα, τα οποία μπορούν ακόμα πολύ αποτελεσματικά να παρακωλύσουν τις μεταδόσεις.

**B) DoS in the Link Layer**

Οι αλγόριθμοι στο στρώμα συνδέσεων, ειδικά της MAC, παρουσιάζουν πολλές ευκαιρίες εκμετάλλευσης για τις επιθέσεις DoS. Παρακάτω θα δούμε τους τρόπους που μπορεί να γίνει αυτό:

• Όποτε ένα σήμα RTS (Request To Send) παραλαμβάνεται, ένα σήμα που συγκρούεται με το σήμα CTS (Clear To Send) διαβιβάζεται. Δεδομένου ότι οι κόμβοι δεν μπορούν να διαβιβάσουν τα στοιχεία πριν λάβουν το CTS, συνεχίζουν τα σήματα RTS.

• Εάν το MAC είναι βασισμένο στις μη ενεργές και τις ενεργές περιόδους, η παρεμβολή των παρασίτων κατά την διάρκεια μόνο των ενεργών περιόδων μπορεί συνεχώς να εμποδίσει το κανάλι.

• Τα ψεύτικα σήματα RTS ή CTS με παραμέτρους τα δεδομένα μετάδοσης που στέλνονται συνεχώς, το οποίο κάνουν τους άλλους κόμβους που κάνουν την εικονική μεταφορά να περιμένουν για πάντα.

• Η εξαπάτηση της βεβαίωση λήψης, όπου ένας αντίπαλος στέλνει τις ψεύτικες βεβαιώσεις λήψης του στρώματος συνδέσεων για τα πακέτα που έχει κρυφακούσει και που απευθύνονται στους γειτονικούς κόμβους, μπορεί επίσης να είναι μια αποτελεσματική επίθεση DoS στρώματος συνδέσεων.

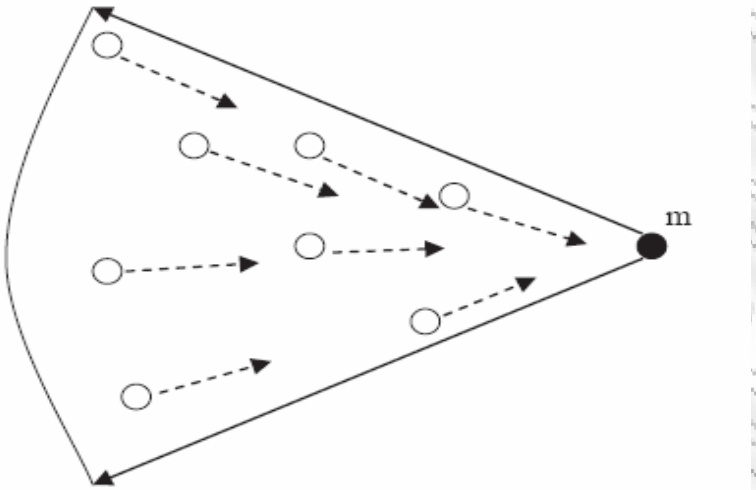
Οι πιο σύνθετες επιθέσεις DoS μπορούν να σχεδιαστούν βασισμένες στο στρώμα της MAC. Παραδείγματος χάριν, στα δίκτυα αισθητήρων, τα πλήρη συστήματα διεύθυνσης δεν χρησιμοποιούνται. Αντ' αυτού, τα θέματα όπως η στοιχείο-κεντρική δρομολόγηση και η επαναχρησιμοποίηση διευθύνσεων μπορούν να χρησιμοποιηθούν.

Ένας κακόβουλος κόμβος μπορεί να διευθύνει μια επίθεση sybil στο στρώμα της MAC για να κάνει τους άλλους κόμβους στην περιοχή να υποθέσουν ότι όλες οι διαθέσιμες διευθύνσεις χρησιμοποιούνται. Αυτό αποτρέπει τους κόμβους από το να γνωρίζουν την ύπαρξη μέρος του δικτύου.

**Γ) DoS against Routing Schemes**

Τα μη δομημένα Ad Hoc δίκτυα και έχουν ειδικές προκλήσεις δρομολόγησης, οι οποίες αντέχουν τους νέους τύπους επιθέσεων DoS ενάντια στα πρωτόκολλα του στρώματος δικτύου. Αυτές οι επιθέσεις εμπίπτουν γενικά σε μια από τις δύο κατηγορίες (Hu et al, 2005): επιθέσεις διάσπασης δρομολόγησης ή επιθέσεις κατανάλωσης των πόρων. Οι επιθέσεις διάσπασης δρομολόγησης στοχεύουν στη δυσλειτουργία της δρομολόγησης, που καθιστά το δίκτυο ανίκανο να παρέχει τις απαραίτητες υπηρεσίες δικτύωσης. Ο στόχος των επιθέσεων κατανάλωσης των πόρων είναι να καταναλωθούν οι πόροι δικτύων όπως το εύρος ζώνης, η μνήμη, η υπολογιστικές δύναμη και η ενέργεια. Και οι δύο είναι επιθέσεις άρνησης υπηρεσιών και τα παραδείγματά τους παρατίθενται παρακάτω (Karlof και Wagner, 2003):

- **Εξαπατημένες ή αλλαγμένες πληροφορίες δρομολόγησης**: οι πληροφορίες δρομολόγησης που ανταλλάσσονται μεταξύ των κόμβων μπορούν από τους κακόβουλους κόμβους να αλλάξουν για να έχουν μια καταστρεπτική επίδραση στο σχέδιο δρομολόγησης.
- **Επίθεση πλημμυρών** (Karlof και Wagner, 2003): ένας κακόβουλος κόμβος μπορεί να μεταδώσει σε όλους τους κόμβους του δικτύου πληροφορίες δρομολόγησης ή οποιεσδήποτε άλλες πληροφορίες με αρκετά υψηλό ρυθμό μετάδοσης έτσι ώστε να πειστεί κάθε κόμβος στο δίκτυο ότι είναι ο γείτονάς τους. Όταν οι άλλοι κόμβοι στέλνουν τα πακέτα τους στον κακόβουλο κόμβο, εκείνα τα πακέτα δεν παραλαμβάνονται από οποιοδήποτε άλλο κόμβο (σχήμα 6).

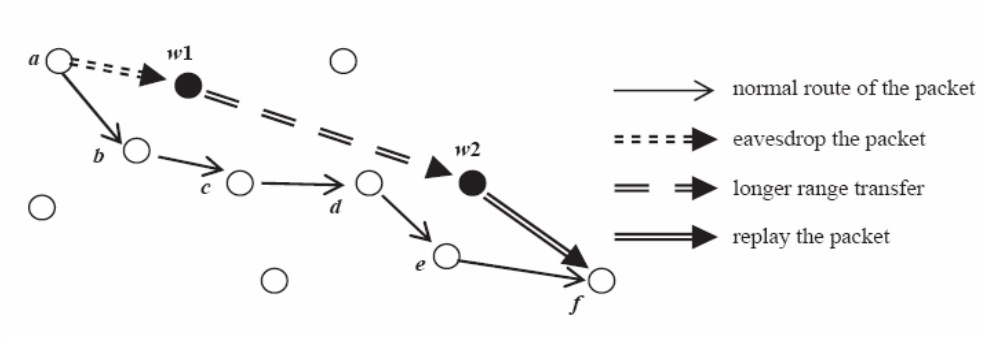



**Σχήμα 6** Επίθεση Πλημμύρας (Flooding Attack)

• **Επίθεση Wormhole**: ένας κακόβουλος κόμβος μπορεί να λάβει πακέτα σε ένα σημείο και να τα μεταφέρει σε έναν άλλο 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 κακόβουλο κόμβο 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. Παραδείγματος χάριν, τα πακέτα που στέλνονται από τον κόμβο α (σχήμα 7) παραλαμβάνονται επίσης από τον κόμβο w1, ο οποίος είναι ένας κακόβουλος. Κατόπιν ο κόμβος w1 διαβιβάζει αυτά τα πακέτα στον κόμβο w2 μέσω ενός καναλιού που είναι εκτός της ζώνη για όλους τους υπόλοιπους κόμβους στο δίκτυο εκτός από τους αντιπάλους. Ο κόμβος w2 επαναλαμβάνει τα πακέτα και ο κόμβος φ τα λαμβάνει σαν τα ελάμβανε άμεσα από τον κόμβο α. Τα πακέτα που ακολουθούν την κανονική διαδρομή, δηλ. το α-β-γ-δ-ε-φ, φτάνουν στον κόμβο φ αργότερα από εκείνα που μεταβιβάστηκαν μέσω του wormhole και επομένως πέφτουν επειδή κάνουν περισσότερα βήματα. 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.

• **Επίθεση αλλαγής δρομολόγησης**: ένας επιτιθέμενος μπορεί να προσπαθήσει την αλλαγή της κυκλοφορίας σε μια υποτιθέμενη διαδρομή ή να χωρίσει το δίκτυο. Διάφορες τεχνικές μπορούν να χρησιμοποιηθούν για αυτό. Παραδείγματος χάριν, ο Hu et al. (2005) καθόρισε μια τέτοια επίθεση, όπου ένας κόμβος σε μια διαδρομή προσθέτει εικονικούς κόμβους στη διαδρομή έτσι ώστε η διαδρομή να γίνεται δαπανηρότερη έναντι μιας άλλης διαδρομής.

• **Επιθέσεις sink hole**: ένας κακόβουλος κόμβος μπορεί να γίνει πολύ ελκυστικός στους περιβάλλοντες κόμβους όσον αφορά τον αλγόριθμο δρομολόγησης. Παραδείγματος χάριν, οι διαφημίσεις δρομολόγησης μπορούν να μεταδίδονται προς όλους και όλοι οι γειτονικοί κόμβοι μπορούν να πειστούν ότι ο κακόβουλος κόμβος είναι ο καλύτερος επόμενος δρόμος για την αποστολή των πακέτων στο σταθμό βάσεων. Όταν ένας κόμβος γίνεται μια sink hole, γίνεται hub για την εγγύτητά της και αρχίζει να λαμβάνει όλα τα πακέτα που πηγαίνουν στο σταθμό βάσεων.




**Σχήμα 7** Επίθεση Wormhole

• **Επίθεση μαύρων τρυπών (Blackhole attack)**: ένας κακόβουλος κόμβος μπορεί να απορρίψει όλα τα πακέτα που λαμβάνει για αποστολή. Αυτή η επίθεση είναι ιδιαίτερα αποτελεσματική όταν ο επιτιθέμενος κόμβος είναι επίσης μια sink hole. Ένας τέτοιος συνδυασμός επίθεσης μπορεί να σταματήσει όλη την κυκλοφορία δεδομένων γύρω από τη μαύρη τρύπα.

• **Επιλεκτική αποστολή (Greyhole attack)**: όταν ένας κακόβουλος κόμβος απορρίπτει όλα τα πακέτα, αυτό μπορεί να ανιχνευθεί εύκολα από τους γείτονές του. Επομένως, μπορεί να απορρίψει μόνο τα επιλεγμένα πακέτα και να διαβιβάσει άλλα.

• **Επίθεση ανακύκλωσης δρομολόγησης (Routing Loop)**: οι sink hole επιθέσεις μπορούν να χρησιμοποιηθούν για να δημιουργήσουν routing loops για να καταναλώσουν την ενέργεια και το εύρος ζώνης καθώς επίσης και να αλλάξουν τη δρομολόγηση.

• **Επίθεση Rushing** (Hu et al., 2005): ένας επιτιθέμενος διαδίδει τα μηνύματα αιτήματος και απάντησης διαδρομών γρήγορα σε όλο το δίκτυο. Αυτό καταστέλλει οποιαδήποτε πιο πρόσφατα νόμιμο μήνυμα αιτήματος διαδρομών, δηλαδή οι κόμβοι τους απορρίπτουν, επειδή οι κόμβοι καταστέλλουν τα άλλα αντίγραφα ενός αιτήματος διαδρομών που έχουν επεξεργαστεί ήδη.

• **Επιθέσεις που εκμεταλλεύονται τους κόμβους τιμωρώντας τα συστήματα**: τα συστήματα που αποφεύγουν τους κόμβους χαμηλής απόδοσης μπορούν να χρησιμοποιηθούν από τους αντιπάλους. Παραδείγματος χάριν, οι κακόβουλοι κόμβοι μπορούν να εκθέσουν μηνύματα λάθους για έναν κόμβο που αποδίδει πραγματικά καλά. Επομένως, το σχέδιο δρομολόγησης μπορεί να αποφύγει μια διαδρομή που περιλαμβάνει αυτόν τον κόμβο. Ομοίως, μια σύνδεση μπορεί να φραχτεί για μια σύντομη περίοδο αλλά δεδομένου ότι τα μηνύματα λάθους παράγονται για τη σύνδεση κατά τη διάρκεια εκείνου του χρονικού διαστήματος, το σχέδιο δρομολόγησης μπορεί να συνεχίσει να αποφεύγει τη σύνδεση ακόμα κι αν δεν είναι φραγμένο άλλο.

**Δ) DoS in the Transport Layer**

Τα πρωτόκολλα στρώματος μεταφοράς είναι επίσης ευαίσθητα στις απειλές ασφάλειας. Μερικά σενάρια επίθεσης εφαρμόσιμα σε αυτό το στρώμα παρατίθενται παρακάτω:

• **Επανάληψη του acknowledgement**: σε μερικά πρωτόκολλα στρώματος μεταφορών, όπως το TCP-Reno, αναγνωρίζοντας το ίδιο τμήμα πολλαπλές φορές στο δίκτυο δείχνει αρνητικό acknowledgement. Ένας κακόβουλος κόμβος μπορεί να επαναλάβει πολλαπλά ένα acknowledgement ώστε να γίνει ο κόμβος πηγής και να θεωρηθεί ότι το μήνυμα δεν παραδόθηκε επιτυχώς.

• **Jamming acknowledgements**: ένας κακόβουλος κόμβος μπορεί να φράξει τα τμήματα που μεταβιβάζουν τα acknowledgement. Αυτό μπορεί να οδηγήσει στη λήξη μιας σύνδεσης.

• **Μεταβαλλόμενος αριθμός ακολουθίας**: στα πρωτόκολλα όπως RMST και PSFQ, ένας κακόβουλος κόμβος μπορεί να αλλάξει τον αριθμό ακολουθίας ενός τεμαχίου και να κάνει τον παραλήπτη να θεωρήσει ότι μερικά πακέτα έχουν χαθεί.

• **Αίτημα spoofing σύνδεσης**: ένας κακόβουλος κόμβος μπορεί να στείλει πολλά αιτήματα σύνδεσης σε έναν κόμβο, καταναλώνοντας τους πόρους του έτσι ώστε δεν μπορεί να δεχτεί οποιοδήποτε άλλο αίτημα σύνδεσης.

Αυτός ο κατάλογος σεναρίων δεν είναι πλήρης. Πολλές διαφορετικές τακτικές μπορούν να αναπτυχθούν βασισμένες στο πρωτόκολλο που χρησιμοποιείται στο στρώμα μεταφορών.

#### 4.3.2.4 Misbehaving

Οι επιθέσεις DoS μπορούν μερικές φορές να προέλθουν από τους κόμβους μέσα στο δίκτυο. Μερικοί κόμβοι μπορούν να συμπεριφερθούν απρεπώς για να κερδίσουν κάποιους εκ των περιορισμένων πόρων της δικτύωσης, δηλαδή μπορούν να φερθούν εγωιστικά. Παραδείγματος χάριν, με τη χρησιμοποίηση του σχεδίου της MAC, ένας κόμβος άπρεπης συμπεριφοράς μπορεί να αναγκάσει τους άλλους κόμβους να περιμένουν περισσότερο έτσι ώστε να μείνουν ελεύθεροι πόροι του συστήματος για δικιά του χρήση. Οι κόμβοι μπορούν επίσης να είναι εγωιστικοί με την άρνηση να αναμεταδώσουν άλλα μηνύματα. Εάν κάθε κόμβος ενεργεί όπως αυτό, κατόπιν ο εγωισμός μπορεί να ασκήσει επίδραση παρόμοια με μια επίθεση DoS.

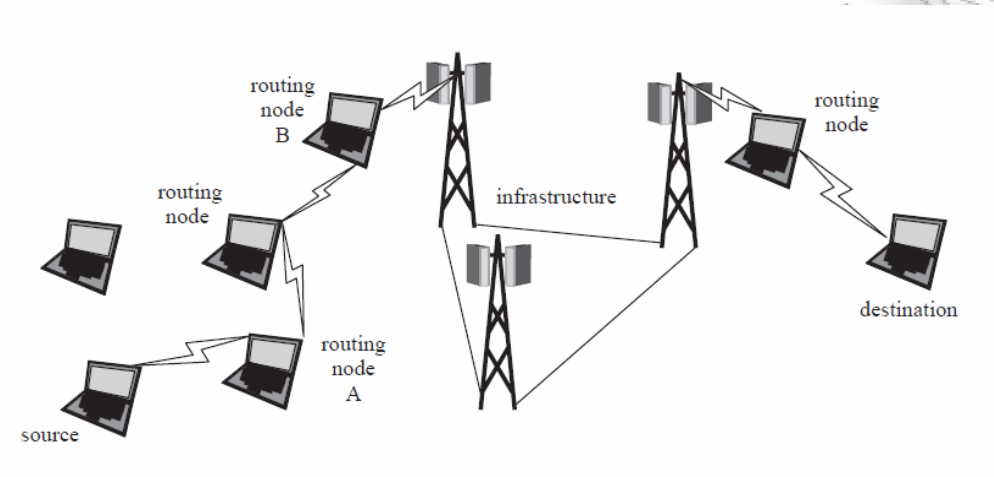
Ένας άλλος σκοπός της συμπεριφοράς αυτής μπορεί να στοχεύσει σε ένα σχέδιο χρέωσης με την άρνηση της πληρωμής για τις λαμβανόμενες υπηρεσίες. Καταρχάς τα ad hoc δίκτυα μπορούν να θεωρηθούν ως περιβάλλοντα όπου κάθε κόμβος συνεργάζεται ώστε να επικοινωνήσει με τον άλλον μέσω ενός ελεύθερου καναλιού. Αυτό όμως δεν συμβαίνει πάντα. Τα δίκτυα πλέγματος (mesh networks) παρέχουν την ασύρματη πρόσβαση multihop στις ευρυζωνικές υπηρεσίες. Ομοίως, μπορούν να υπάρξουν multihop στα κυψελοειδή δίκτυα όπου οι κόμβοι τους επιτρέπεται να έχουν πρόσβαση στο δίκτυο μέσω των ειδικών ασύρματων συνδέσεων multihop όταν είναι εκτός της περιοχή κάλυψης που παρέχεται από την υποδομή, όπως φαίνεται στο σχήμα 8. Στις δύο περιπτώσεις αυτές οι κόμβοι φθάνουν σε έναν φορέα παροχής υπηρεσιών και υποτίθεται ότι πρέπει να πληρώσουν για τις υπηρεσίες που παίρνουν από τον φορέα παροχής υπηρεσιών (Salem et al. 2003). Οι διάφορες επιθέσεις που προβλέπονται ενάντια στα σχέδια χρέωσης σε αυτά τα είδη δικτύου είναι:

• **Refusal to pay**: ο κόμβος της πηγής μπορεί να αρνηθεί ότι πραγματοποίησε κάποια επικοινωνία σχετικά με ένα λογαριασμό.

• **Ανέντιμες ανταμοιβές (Dishonest rewards)**: στη δικτύωση multihop, οι ενδιάμεσοι κόμβοι πρέπει να αναμεταδώσουν τα άλλα πακέτα. Αυτό μπορεί να γίνει παρακινώντας τους ενδιάμεσους κόμβους να διαβιβάσουν τα πακέτα αντί να είναι εγωιστικοί, σχεδιάζοντας μηχανισμούς ανταμοιβής. Σε αυτήν την περίπτωση, ένας κόμβος άπρεπης συμπεριφοράς μπορεί να θελήσει να εμφανιστεί ότι περιλήφθηκε στην αποστολή μερικών πακέτων, ακόμα κι αν δεν ήταν.

• **Ελεύθερη οδήγηση (Free riding)**: οι ενδιάμεσοι κόμβοι ανάμεσα στη διαδρομή μεταξύ της πηγής και του προορισμού μπορούν να τοποθετήσουν τα πακέτα τους προς τις τρέχουσες επικοινωνίες για να αποφύγουν το λογαριασμό. Παραδείγματος χάριν, ο κόμβος δρομολόγησης Α μπορεί να τοποθετήσει το πακέτο του επάνω στα

πακέτα του κόμβου δρομολόγησης Β προκειμένου να πάει στον προορισμό του (Σχήμα 8).




**Σχήμα 8** Multihop cellular network

## 4.4 Συστήματα Ασφάλειας Ad Hoc Δικτύων

### 4.4.1 Τεχνικές ενάντια στις επιθέσεις κατά την Ad Hoc Δρομολόγηση

Η δρομολόγηση είναι μια από τις σημαντικές προκλήσεις ad hoc δίκτυα και γι' αυτό έχουν προσελκύσει πολλούς ερευνητές και τις έχουν μελετήσει εκτενώς. Πολλές εφαρμογές ad hoc και δικτύων αισθητήρων έχουν ως σκοπό να επεκταθούν σε διάφορα περιβάλλοντα, για το λόγο αυτό υπόκεινται σε επιθέσεις. Επομένως, η ασφάλεια πρέπει επίσης να θεωρηθεί ως ένας από τους αρχικούς παράγοντες που επηρεάζουν το σχέδιο της δρομολόγησης των πρωτοκόλλων. Υπάρχουν τρεις προσεγγίσεις στο σχεδιασμό ενός ασφαλούς πρωτοκόλλου δρομολόγησης (Parno et al, 2006):

- πρόληψη επίθεσης
- ανίχνευση και αποκατάσταση επίθεσης από την επίθεση
- ανθεκτικότητα στις επιθέσεις ασφάλειας.

Η δρομολόγηση των πρωτοκόλλων πρέπει να σχεδιαστεί έτσι ώστε ένας αντίπαλος να μη μπορεί να ενεργήσει στους κόμβους και τα μηνύματα ώστε να δημιουργήσει δυσλειτουργία στην δρομολόγηση. Αυτό είναι η αποτελεσματικότερη προσέγγιση όσον αφορά το κόστος του συστήματος και της αποτελεσματικότητας της ασφάλειας στην υπεράσπιση ενάντια στις απειλές. Η δρομολόγηση πρέπει να σχεδιαστεί έτσι ώστε να παραδίδει τα πακέτα των μηνυμάτων στον προορισμό τους ακόμα και όταν υπάρχει μια επίθεση. Τέτοιες τεχνικές θα μελετήσουμε παρακάτω.

#### 4.4.1.1 Τεχνικές ενάντια στα Wormhole Attacks

Οι Wormholes είναι δύσκολο να ανιχνευθούν επειδή ένας αντίπαλος περνά τα πακέτα σε ένα απόμακρο σημείο από το σημείο στο οποίο παραλαμβάνονται με τη χρησιμοποίηση ενός κόμβου που βρίσκεται εκτός ζώνης. Αυτό το κανάλι δεν μπορεί να ανιχνευτεί από το δίκτυο. Οι μηχανισμοί ανίχνευσης ενάντια στις επιθέσεις wormhole μπορούν να βασιστούν στη χρονική και χωρική ανάλυση των πακέτων. Τα γεωγραφικά και χρονικά περιθώρια των πακέτων που εισάγονται ακολουθήθηκε ως προσέγγιση από τον Hu et al. (2003). Τα γεωγραφικά περιθώρια υποθέτουν ότι οι κόμβοι είναι αόριστα συγχρονισμένοι και σε ενήμερη θέση. Ο κόμβος S περιλαμβάνει τη θέση του lS και το πακέτο μετάδοσης στο χρόνο tS ως γεωγραφικό περιθώριο στο πακέτο του PS που στέλνεται στον προορισμό D.

$$S \rightarrow D : lS, tS, P$$

Τα ρολόγια των κόμβων στο δίκτυο είναι συγχρονισμένα μέσα σε ±Δ. Το ανώτερο όριο για την απόσταση μεταξύ δύο κόμβων είναι db, και είναι βασισμένος στη σειρά μετάδοσης των κόμβων. Το ανώτερο όριο λάθους που περιορίζεται από τον κόμβο δίνεται επίσης ως δ. Ομοίως, ένα ανώτερο όριο που δεσμεύεται για την ταχύτητα διαβίβασης των σημάτων v είναι επίσης γνωστό. Κατόπιν κάθε κόμβος i που διαβιβάζει το πακέτο, που είναι στην li θέση και λαμβάνει το πακέτο στο χρόνο ti μπορεί να ελέγξει τον ακόλουθο όρο.

$$db \leq |li - lS| + 2v\ X\ (ti - tS + \_) + \delta$$

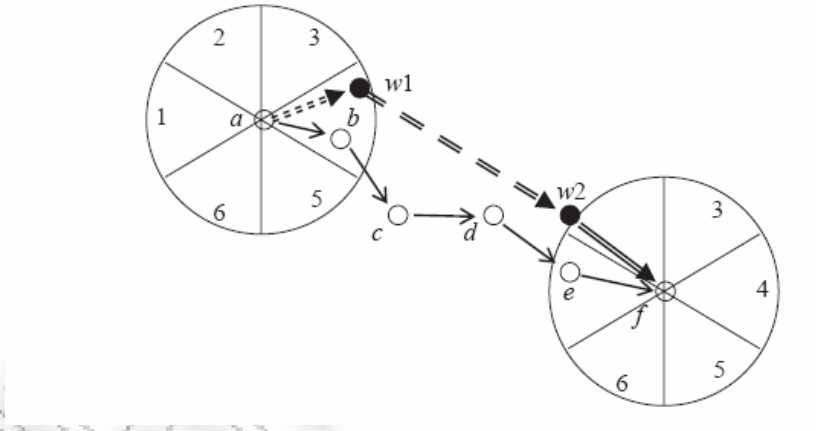
Εάν αυτός ο όρος δεν ισχύει, δείχνει ότι το πακέτο έχει παραληφθεί από τον κόμβο i νωρίτερα από το αναμενόμενο και το δίκτυο μπορεί να υπόκειται σε μια επίθεση wormhole. Όταν η μέση απόσταση μεταξύ των κόμβων δεν είναι αρκετά μακριά, και ο αριθμός των βημάτων στην κανονική πορεία δεν είναι αρκετά υψηλός, αυτή η τεχνική μπορεί να μην ανιχνεύσει wormholes. Τα χρονικά πακέτα συγκράτησης χρησιμοποιούν μόνο τους χρόνους μετάδοσης και υποδοχής των πακέτων για την ανίχνευση wormholes. Όταν ένας κόμβος A διαβιβάζει ένα πακέτο σε έναν άλλο κόμβο B, περιλαμβάνει επίσης το χρόνο tA μετάδοσης στο πακέτο PA.

$$A \rightarrow B : tA, PA$$

Ο κόμβος B ελέγχει τη διαφορά dAB μεταξύ του χρόνου μετάδοσης tA και του χρόνου υποδοχής tB του πακέτου. Εάν dAB είναι πιο κοντά από ένα δεδομένο

κατώτατο όριο θ, μπορεί να δείξει μια επίθεση wormhole. Τα χρονικά περιθώρια απαιτούν το σφιχτό χρονικό συγχρονισμό.

Όταν οι κατευθυντικές κεραίες είναι διαθέσιμες στους κόμβους, μπορούν επίσης να χρησιμοποιηθούν στην ανίχνευση των wormholes (Hu και Evans, 2003), όπως φαίνεται στο σχήμα 9, όπου τα πακέτα στοιχείων που διαβιβάζονται από τον κόμβο α παραλαμβάνονται από έναν κακόβουλο κόμβο w1, μεταβιβάζονται σε έναν άλλο κακόβουλο κόμβο w2 μέσω ενός wormhole και επαναλαμβάνονται από τον κόμβο w2. Τα πακέτα που επαναλήφθηκαν παραλαμβάνονται από τον κόμβο f. Επομένως οι κόμβοι α και f θεωρούν ότι είναι γείτονες. Υποθέστε ότι και οι κόμβοι α και f είναι εξοπλισμένοι με μια κατευθυντική κεραία που έχει έξι τομείς, και οι τομείς και των δύο κόμβων ευθυγραμμίζονται, δηλ. Ο τομέας 1 του κόμβου α είναι στην ίδια κατεύθυνση με τον τομέα 1 του κόμβου f. Επομένως, τα πακέτα που διαβιβάζονται στον τομέα 4 του κόμβου α πρέπει να παραληφθούν στον τομέα 1 του κόμβου f. Εντούτοις, τα πακέτα που επαναλαμβάνονται από το wormhole παραλαμβάνονται στον τομέα 2 του κόμβου f. Αυτό δείχνει μια επίθεση wormhole και μπορεί να ανιχνευθεί από τον κόμβο f εάν τα πακέτα περιλαμβάνουν επίσης τα στοιχεία για τον τομέα από τον οποίο διαβιβάστηκαν.




**Σχήμα 9** Κατευθυντική κεραία για ανίχνευση Wormhole

Οι επιτιθέμενοι μπορούν επίσης να προσαρμοστούν στις κατευθυντικές κεραίες με την επανάληψη των πακέτων στον ίδιο τομέα με αυτόν στον οποίο παραλαμβάνονται. Εντούτοις, οι ικανότητες των επιτιθεμένων μειώνονται ακόμη και με αυτήν την απλούστερη μορφή της προσέγγισης.

#### 4.4.1.2 Τεχνικές ενάντια στα Sybil Attacks

Για να υπερασπίσουν ενάντια στις επιθέσεις sybil, οι ταυτότητες κάθε κόμβου πρέπει να ελεγχθούν. Αυτό μπορεί να γίνει είτε άμεσα είτε έμμεσα. Στην άμεση επικύρωση ένας κόμβος ελέγχει εάν η ταυτότητα ενός γειτονικού κόμβου ισχύει. Παραδείγματος χάριν, ένας κόμβος μπορεί να ορίσει σε κάθε έναν από τους γείτονές του ένα χωριστό κανάλι για να επικοινωνήσει και να ζητήσει να διαβιβάσει κατά τη διάρκεια μιας περιόδου. Κατόπιν ελέγχει αυτά τα κανάλια σε μια τυχαία σειρά εντός εκείνης της περιόδου. Εάν ένας κόμβος διαβιβάζει στο ορισμένο κανάλι του, ο κόμβος είναι ένας φυσικός κόμβος. Εάν καμία μετάδοση δεν ανιχνεύεται σε ένα κανάλι, δείχνει ότι ο κόμβος που ορίζεται σε εκείνο το κανάλι μπορεί να μην είναι ένας φυσικός κόμβος.

Στην έμμεση επικύρωση ένας άλλος εμπιστευμένος κόμβος παρέχει την επαλήθευση για την ταυτότητα του κόμβου. Παραδείγματος χάριν, κάθε κόμβος μπορεί να μοιραστεί ένα μοναδικό κλειδί με το σταθμό βάσεων. Όταν δύο κόμβοι πρέπει να εγκαταστήσουν μια σύνδεση μεταξύ τους, ελέγχει ο ένας την ταυτότητα του άλλου μέσω του σταθμού βάσεων με τη χρησιμοποίηση αυτών των κλειδιών (Karlof και Wagner, 2003). Συγχρόνως μπορεί να τους οριστεί ένα κλειδί συνόδου. Οι κόμβοι μπορούν επίσης να επιτραπούν να εγκαταστήσουν συνδέσεις με έναν περιορισμένο αριθμό γειτονικών κόμβων. Κατά συνέπεια, οι κόμβοι μπορούν μόνο να επικοινωνήσουν με έναν περιορισμένο αριθμό ελεγμένων γειτονικών κόμβων, ο οποίος περιορίζει επίσης τον αντίκτυπο των επιθέσεων sybil.

Τα τυχαία κλειδιά που ορίζονται στους κόμβους παρέχουν επίσης την ασφάλεια ενάντια στις επιθέσεις sybil. Δεδομένου ότι ένας περιορισμένος αριθμός κλειδιών είναι διαθέσιμος σε κάθε κόμβο, οι κόμβοι δεν έχουν αρκετά κλειδιά για να παράγουν πολλαπλάσιες ταυτότητες.

#### 4.4.1.3 Τεχνικές ενάντια στην Επιλεγμένη Προώθηση Πακέτων

Αποτρέποντας τα wormholes, οι sink holes και οι sybil επιθέσεις δεν μπορούν να εγγυηθούν να μετριάσουν τη μαύρη τρύπα και τις εκλεκτικές επιθέσεις αποστολής. Ένας συμβιβασμένος κόμβος μπορεί ακόμα να ενεργήσει ως μαύρη τρύπα ή να απορρίψει τα επιλεγμένα πακέτα. Υπάρχουν δύο προσεγγίσεις υπεράσπισης ενάντια στην εκλεκτική αποστολή: η ανίχνευση των κόμβων που διαβιβάζουν επιλεκτικά πακέτα και η ανάπτυξη των σχεδίων δρομολόγησης, που είναι πιο ελαστικά και μπορούν να παραδώσουν τα πακέτα ακόμα και όταν υπάρχει μια εκλεκτική επίθεση.

Μια προσέγγιση στην ανίχνευση των κόμβων που διαβιβάζουν επιλεκτικά είναι βασισμένη στα acknowledgements (Yu και Xiao, 2006). Κάθε ενδιάμεσος κόμβος που διαβιβάζει ένα πακέτο περιμένει ένα acknowledgement από τον επόμενο κόμβο

(hop). Εάν ο επόμενος κόμβος δεν επιστρέφει τον ίδιο αριθμό acknowledgements με τον αριθμό πακέτων που στέλνονται, ο κόμβος παράγει έναν συναγερμό για τον επόμενο κόμβο. Ο κόμβος μπορεί επίσης να παραγάγει τα acknowledgements για τα πακέτα που απορρίφτηκαν, τα οποία κάνουν αυτό το σχέδιο να αποτύχει. Επιπλέον, ένας κακόβουλος κόμβος μπορεί να παραγάγει τους πλαστούς συναγερμούς για να οργανώσει μια επίθεση DoS. Τα σχέδια και η κρυπτογράφηση επικύρωσης μπορούν να χρησιμοποιηθούν για να αποτρέψουν αυτά τα είδη κακόβουλης συμπεριφοράς (Yu και Xiao, 2006). Τα acknowledgements του στρώματος συνδέσεων μπορούν επίσης να συμπληρωθούν από τα end-to-end σχέδια αξιοπιστίας.

Η πολλαπλών διαδρομών δρομολόγηση μπορεί να είναι ένας αποτελεσματικός τρόπος να μετριαστούν οι επιθέσεις εκλεκτικής αποστολής και μαύρων τρυπών (Karlof και Wagner, 2003). Αυτό απαιτεί τουλάχιστον την σύνδεση αποχώρησης των πορειών, όπου δύο πορείες μπορούν να μοιραστούν μερικούς κόμβους αλλά καμία σύνδεση. Φυσικά, τέτοια μονοπάτια, όπου δύο από αυτά δεν έχουν οποιοδήποτε κόμβο από κοινού, είναι καλύτερα και μειώνουν τον κίνδυνο εκλεκτικής επίθεσης αποστολής πακέτων. Εντούτοις, τέτοια μονοπάτια δεν είναι πάντα διαθέσιμα και όταν οι πορείες δεν πρόκειται να χωρίσουν, εάν ο κόμβος επιλεκτικής αποστολής είναι ο κοινός κόμβος για όλες τις πορείες, η επίθεση μπορεί να γίνει πολύ αποτελεσματική.

#### 4.4.1.4 Τεχνικές ενάντια στην επίθεση Πλημμύρας (Flooding Attack)

Η επίθεση πλημμύρας σε ένα δίκτυο είναι πολύ σημαντική γιατί μπορεί να δημιουργήσει ένα DoS όπου εφαρμοστεί. Για την αντιμετώπισή της έχουν αναπτυχθεί δύο μηχανισμοί οι οποίοι αντιστέκονται ενάντια στις Ad Hoc Flooding Attacks. Οι μηχανισμοί αυτοί είναι η κατάπνιξη από γειτονικούς κόμβους (neighbour suppression) και η διακοπή της διαδρομής (path cut-off).

Η μέθοδος της κατάπνιξης από τους γειτονικούς κόμβους χρησιμοποιείται για να εμποδίσει τα RREQ την επίθεση πλημμύρας. Τα κινητά δίκτυα ad hoc είναι ασύρματα δίκτυα πολλαπλών αλμάτων και συνεπώς ο κάθε κόμβος στέλνει και λαμβάνει πακέτα μέσω των γειτονικών του κόμβων. Εάν όλοι οι γειτονικοί κόμβοι γύρω από τον συγκεκριμένο κόμβο αρνηθούν να προωθήσουν τα πακέτα του τα οποία αυτός στέλνει στο δίκτυο, ο κόμβος αυτός δεν μπορεί να επικοινωνήσει με τους άλλους κόμβους. Στην πράξη, ο κόμβος έχει απομονωθεί από το δίκτυο έστω και αν η θέση του είναι ακόμη εντός του δικτύου.

Όταν ο επιτιθέμενος εξαπολύει μία DATA επίθεση πλημμύρας, οι γειτονικοί κόμβοι είναι δύσκολο να το αναγνωρίσουν διότι ο γειτονικός κόμβος δεν μπορεί να κρίνει εάν ένα πακέτο DATA είναι άχρηστο στο επίπεδο δικτύου. Ο κόμβος προορισμού μπορεί εύκολα να πάρει την απόφαση στο επίπεδο εφαρμογών όταν έχει λάβει αυτά τα άχρηστα DATA πακέτα. Ο επιτιθέμενος θέτει μία διαδρομή από τον

εαυτό του προς τον κόμβο-θύμα για να εξαπολύσει την επίθεση. Όταν το θύμα ανακαλύπτει την DATA Flooding Attack, μπορεί να διακόψει τη διαδρομή από τον επιτιθέμενο και έτσι να τον εμποδίσει από την συνέχιση της επίθεσης. Ο κόμβος-θύμα στέλνει ένα RRER μήνυμα στον επιτιθέμενο. Το μήνυμα αυτό εμφανίζει την IP διεύθυνση του θύματος απρόσιτη. Οι ενδιάμεσοι κόμβοι από τους οποίους περνάει το μήνυμα RRER θα διαγράψουν τη διαδρομή από τον επιτιθέμενο στο θύμα. Έτσι, με την αποκοπή όλων των σχετικών διαδρομών, η DATA Flooding Attack προοδευτικά τερματίζεται. Όταν αυτές οι διαδρομές επίθεσης τελειώσουν, ο επιτιθέμενος μπορεί να δημιουργήσει RREQ προκειμένου να φτιάξει ξανά νέες διαδρομές προς άλλους κόμβους. Οι άλλοι κόμβοι μπορούν να αρνηθούν να ιδρύσουν αυτές τις διαδρομές μέσω μη απάντησης με κάποιο RREP στα συγκεκριμένα RREQ. Στο πρωτόκολλο AODV, οι ενδιάμεσοι κόμβοι μπορούν να απαντήσουν στο RREQ αντί των τελικών κόμβων, εάν αυτοί έχουν μια ενεργό διαδρομή προς τον προορισμό. Για αυτόν τον λόγο, ο επιτιθέμενος μπορεί να ιδρύσει τις διαδρομές προς το θύμα αν και ο κόμβος-θύμα αρνείται να το κάνει. Για να αποφευχθεί αυτό, η λειτουργία κατά την οποία οι ενδιάμεσοι κόμβοι έχουν τη δυνατότητα να απαντούν στα RREQ πρέπει να ανασταλεί. Μόνο ο προορισμός πρέπει να μπορεί να αποκρίνεται σε τέτοια RREQ.

### 4.4.2 Τεχνικές ενάντια στην Ανάλυση Κίνησης

Ένα cluster-based ασύρματο δίκτυο αποτελείται από πολλούς κόμβους με περιορισμένους πόρους, καθώς και κόμβους οι οποίοι είναι οι αρχηγοί στα cluster. Οι head cluster είναι συχνά πιο ισχυροί και έχουν μεγαλύτερες δυνατότητες από τους απλούς κόμβους του δικτύου. Αυτοί διαδραματίζουν σημαντικό ρόλο στο σύστημα και ως εκ τούτου, αποτελούν κύριοι στόχοι για επίθεση.

Εάν ένας αντίπαλος μπορεί να επιτεθεί επιτυχώς στον κεντρικό κόμβο, τότε ολόκληρο το σύστημα μπορεί να καταστεθεί άχρηστο. Επομένως, η εντόπιση ενός κόμβου, ο οποίος είναι και ο αρχηγός του cluster-based δικτύου, θα ήταν πολύ χρήσιμη για έναν αντίπαλο. Οι αντίπαλοι μπορούν να εντοπίσουν αυτούς τους κόμβους και να λάβουν σημαντικές πληροφορίες για το δίκτυο απλά με τον έλεγχο της κίνησης και του όγκου της πληροφορίας, ακόμα και όταν κρυπτογραφούνται τα πακέτα. Στα δίκτυα αισθητήρων, τα στοιχεία που συλλέγονται από τους κόμβους αισθητήρων δρομολογούνται στους σταθμούς βάσης μέσω των σχετικά σταθερών πορειών, και οι κόμβοι κοντά στο σταθμό βάσης προωθούν πολύ περισσότερα πακέτα από τους κόμβους που βρίσκονται μακριά από το σταθμό βάσης. Με βάση αυτά τα χαρακτηριστικά, οι αντίπαλοι μπορούν να αναλύσουν τα σχέδια κυκλοφορίας και να αποκαλύψουν τη θέση του σταθμού βάσης χωρίς να κατανοήσουν το περιεχόμενο των πακέτων. Αυτό είναι γνωστό ως επίθεση ελέγχου rate (Deng et al., 2006). Προκειμένου να εξαπατηθεί και να δοθεί λανθασμένη κατεύθυνση στον επιτιθέμενο,

τα πακέτα που συλλέγονται από τους κόμβους αισθητήρων μπορούν να διαβιβαστούν τυχαία με την ελπίδα ότι ο αντίπαλος δεν θα βρει εύκολα την ακριβή πορεία προς στο σταθμό βάσεων.

Επιπλέον, υπάρχει η επίθεση χρονικού συσχετισμού. Σε αυτήν την επίθεση (Deng et al, 2006), οι αντίπαλοι μπορούν να συναγάγουν τη θέση του σταθμού βάσεων αν απλά παράγουν μερικά γεγονότα και τον έλεγχο όπου οι κόμβοι αισθητήρων διαβιβάζουν τα πακέτα. Μονόδρομη υπεράσπιση ενάντια στην επίθεση χρονικού συσχετισμού είναι να αποθηκευτούν τα εισερχόμενα πακέτα στον κόμβο για έναν τυχαίο χρόνο πριν διαβιβαστούν. Ένας άλλος τρόπος είναι να παραχθεί ένα πλαστό πακέτο και να σταλεί τυχαία σε έναν άλλο κόμβο κάθε φορά που θέλει να στείλει ένας κόμβος ένα πακέτο. Τα πλαστά πακέτα χρησιμοποιούν έναν χρόνο time-to-live (TTL) για να αποφασίσουν πότε η αποστολή πρέπει να σταματήσει.

### 4.4.3 Τεχνικές βασισμένες σε λογισμικό αντι-πλαστογραφήσεων

Αυτήν την περίοδο, το σπάσιμο λογισμικού είναι ένα μεγάλο πρόβλημα για τη βιομηχανία λογισμικού. Για να προστατεύσουν το λογισμικό από το σπάσιμο, τεχνολογίες αντι-πλαστογραφήσεων έχουν αναπτυχθεί. Η προστασία λογισμικού έχει προσελκύσει πρόσφατα την τεράστια προσοχή και όλο και περισσότερο οι τεχνολογίες αντι-πλαστογραφήσεων προτείνονται για αυτόν το λόγο.

Οι τεχνικές αντι-πλαστογραφήσεων γενικά έχουν ως σκοπό να ανιχνεύσουν ή να αισθανθούν οποιοδήποτε τύπο αναρμόδιας τροποποίησης ή χρήσης του λογισμικού. Μόλις ανιχνευθεί κάτι τέτοιο, το μέρος αντι-πλαστογραφήσεων του λογισμικού θα λάβει κάποια μέτρα να καταστεθεί το λογισμικό άχρηστο στον αντίπαλο.

Για να καταπολεμήσει το σπάσιμο του λογισμικού, ένα ευρύ φάσμα μηχανισμών προστασίας αντι-πλαστογραφήσεων έχει μελετηθεί πρόσφατα, συμπεριλαμβανομένου του code obfuscation, του wrapper και της φύλαξης. Είναι σημαντικό να λάβουμε υπόψη ότι καμία από τις ανωτέρω προσεγγίσεις δεν μπορεί να εγγυηθεί την προστασία ενάντια στις επιθέσεις. Ένας συνδυασμός των διαφορετικών τεχνικών προστασίας έτσι ώστε κάθε μια να καλύπτει τις αδυναμίες της άλλης μπορεί να παρέχει την καλύτερη προστασία. Οι τεχνικές βασισμένες στο λογισμικό προστασίας εξηγούνται παρακάτω.

#### 4.4.3.1 Encryption Wrapper

Στα συστήματα κρυπτογράφησης wrapper, το λογισμικό κρυπτογραφείται και πρέπει να αποκρυπτογραφηθεί πριν τη χρήση. Για να είναι αποδοτικά, μόνο τα κρίσιμα μέρη ενός προγράμματος κρυπτογραφούνται. Αυτά τα μέρη

αποκρυπτογραφούνται στο χρόνο εκτέλεσης πριν τη χρήση. Με άλλα λόγια, ένας αντίπαλος πρέπει να τρέξει το πρόγραμμα προκειμένου να αποκτηθεί η αποκρυπτογραφημένη εικόνα του προγράμματος.

Για να αποτρέψει τον επιτιθέμενο από το να πάρει ένα στιγμιότυπο του συνόλου του λογισμικού, μόνο οι κώδικες που θα εκτελεστούν στο σύστημα πρέπει να αποκρυπτογραφηθούν, και τα άλλα μέρη του λογισμικού πρέπει να μείνουν κρυπτογραφημένα. Αυτό δεν μπορεί να εγγυηθεί την προστασία δεδομένου ότι ένας αντίπαλος μπορεί ακόμα να πάρει πολλά στιγμιότυπα συστημάτων.

Επιπλέον, τα κλειδιά αποκρυπτογράφησης πρέπει να προστατευθούν από την κοινοποίηση. Οι κύριες μέθοδοι επίθεσης ενός αντιπάλου είναι run-time εργαλεία, όπως οι debuggers ή οι απορρίψεις μνήμης, ή το τρέξιμο και η ανάλυση του προγράμματος σε ένα εικονικό περιβάλλον. Για να αποτρέψει τις επιθέσεις, η χρήση των run-time εργαλείων πρέπει να περιοριστούν. Συγχρόνως, οι διάφοροι αμυντικοί μηχανισμοί μπορούν να χρησιμοποιηθούν για να το καταστήσουν δυσκολότερο να τρέξουν και να αναλύσουν ένα πρόγραμμα σε ένα εικονικό περιβάλλον. Τα wrappers μπορούν επίσης να χρησιμοποιήσουν τη συμπίεση μαζί με την κρυπτογράφηση για να μειώσουν τη χρήση αποθήκευσης και για να αυξήσουν την ασφάλεια του συστήματος.

Ένα wrapper κρυπτογράφησης είναι μια αποτελεσματική λύση προστασίας. Οι επιτιθέμενοι πρέπει να σχεδιάσουν τα πιο σύνθετα εργαλεία επίθεσης και να καταναλώσουν περισσότερο χρόνο να αναλύσουν και να λάβουν μια εικόνα του αποκρυπτογραφημένου προγράμματος. Εντούτοις, τα wrappers κρυπτογράφησης χρειάζονται επιπλέον ενέργεια του συστήματος για την αποκρυπτογράφηση στο χρόνο εκτέλεσης.

#### 4.4.3.2 Κώδικας Συσκότισης (Code Obfuscation)

Ένα πρόγραμμα μπορεί να μετατραπεί σε κώδικα πηγής με τη βοήθεια των αντίστροφων εργαλείων της εφαρμοσμένης μηχανικής. Ο κώδικας συσκότισης είναι μια τεχνική που μπορεί να αποτρέψει τις επιθέσεις πλαστογράφησης μετασχηματίζοντας το αρχικό πρόγραμμα σε κάποιο κώδικα που δεν έχει μια συνεχή ροή. Οι μετασχηματισμοί αυτοί πρέπει να διατηρήσουν τη λειτουργία του προγράμματος και να ασκήσουν μόνο μέτρια επίδραση στη χρήση της απόδοσης και της μνήμης του κώδικα. Συγχρόνως, πρέπει να είναι ελαστικοί στις διάφορες επιθέσεις πλαστογράφησης. Η ποιότητα της αλλαγής των μετασχηματισμών μπορεί να ταξινομηθεί και να αξιολογηθεί όσον αφορά τη δύναμή τους, την ανθεκτικότητά τους και το κόστος στην κατανάλωση ενέργειας της εφαρμογής

Υπάρχουν διάφορα είδη μετασχηματισμού συσκότισης (Collberg και Thomborson, 2002): μετασχηματισμός σχεδιαγράμματος, μετασχηματισμός δεδομένων,

μετασχηματισμός ελέγχου και προληπτικός μετασχηματισμός. Ο μετασχηματισμός σχεδιαγράμματος τροποποιεί τη φυσική εμφάνιση του κώδικα με την αφαίρεση του σχήματος του κώδικα (π.χ. τοποθετημένες υπό όρους δηλώσεις) και αντικαθιστώντας τα ονόματα των σημαντικών μεταβλητών με τις τυχαίες σειρές. Μόλις χαθεί η αρχική μορφοποίηση, είναι δύσκολο να ανακτηθεί. Αυτό είναι αποτελεσματικό σε σχέση με άλλους μετασχηματισμούς. Ο μετασχηματισμός δεδομένων αλλάζει τις δομές δεδομένων που χρησιμοποιούνται στο πρόγραμμα, το οποίο περιλαμβάνει τις αλλαγές στον τρόπο που τα στοιχεία αποθηκεύονται στη μνήμη, πώς τα αποθηκευμένα στοιχεία ερμηνεύονται, πώς τα στοιχεία ομαδοποιούνται και πώς τα στοιχεία διατάζονται. Η ελεγχόμενη συσκότιση στοχεύει να χειριστεί τη ροή ελέγχου του προγράμματος, π.χ. μεταβάλλοντας τον τρόπο με τον οποίο οι δηλώσεις συγκεντρώνονται και εκτελούνται ή αναδιοργανώνοντας τις δομές βρόχων ή φραγμών σε ένα πρόγραμμα.

Οι προληπτικοί μετασχηματισμοί στοχεύουν να το καταστήσουν δυσκολότερο για τους επιτιθέμενους να πάρουν τον κώδικα του προγράμματος, που καθιστά τις αυτόματες τεχνικές συσκότισης δυσκολότερες και που εκμεταλλεύεται τις γνωστές αδυναμίες τους.

Η συσκότιση μπορεί να γίνει σε επίπεδα κώδικα πηγής και συγκέντρωσης. Οι μετασχηματισμοί στο επίπεδο κώδικα πηγής χρησιμοποιούνται ευρύτερα, αλλά εάν δεν σχεδιάζονται καλά, ένας αντίπαλος μπορεί εύκολα να βρει που οι μετασχηματισμοί εφαρμόστηκαν. Η συσκότιση στο επίπεδο συγκέντρωσης λειτουργεί καλύτερα δεδομένου ότι μπορεί αποτελεσματικά να κρύψει τη δυαδική λειτουργία.

Για να αξιολογήσουν την ποιότητα των μετασχηματισμών συσκότισης, η δύναμη και η ανθεκτικότητα (Collberg et al., 1997) είναι δύο κύριοι παράγοντες που εξετάζονται. Η ποιότητα μετριέται από το βαθμό στον οποίο ο μετασχηματισμένος κώδικας είναι πιο σκοτεινός από τον αρχικό, και από το πόσο καλά ο μετασχηματισμένος κώδικας μπορεί να αντισταθεί σε αυτές τις επιθέσεις. Η μέτρηση της ανθεκτικότητας περιλαμβάνει την προσπάθεια του προγραμματιστή να δημιουργήσει έναν αλγόριθμο από-συσκότισης καθώς και το χρόνο και το διάστημα που απαιτούνται για να τρέξει. Το επίπεδο ασφάλειας που συσκότιση προστίθεται σε μια εφαρμογή εξαρτάται από την εκλέπτυνση των μετασχηματισμών που υιοθετούνται στη συσκότιση, τη δύναμη των διαθέσιμων αλγορίθμων και το ποσό των διαθέσιμων πόρων. Προκειμένου να αποκτηθεί η καλύτερη συσκότιση από άποψη αποτελέσματος, αρκετές από τις τεχνικές μετασχηματισμού συσκότισης μπορούν να συνδυαστούν για να εργαστούν από κοινού.

#### 4.4.3.3 Guarding (Φύλαξη)

Η χρησιμοποίηση μόνο ενός ενιαίου σχεδίου προστασίας προσθέτει ευπάθεια επειδή ένα ενιαίο σημείο προστασίας, ανεξάρτητα από το πόσο αποτελεσματικό είναι, μπορεί να βρεθεί και να κινδυνέψει. Για να παρέχουν γερή προστασία, οι πολλαπλές, ενδεχομένως απλές, τεχνικές προστασίας πρέπει να συνεργαστούν μαζί για να αντισταθούν σε παραποιημένο λογισμικό και για να επιβάλουν τις πολιτικές ασφάλειας. Αυτές οι μικρές μονάδες ασφάλειας καλούνται φρουρές.

Μια φρουρά (Chang και Atallah, 2001) είναι ένα κομμάτι του κώδικα αρμόδιο για την εκτέλεση ορισμένων, σχετικών με την ασφάλεια, ενεργειών κατά τη διάρκεια της εκτέλεσης του προγράμματος. Οι φρουρές παρεμβάλλονται στον κώδικα του λογισμικού για να προστατεύσουν μια διευκρινισμένη περιοχή του κώδικα. Η φύλαξη μπορεί να εφαρμοστεί μεταξύ των τμημάτων κώδικα στο λογισμικό και άλλων αντικειμένων (π.χ. Hardware). Οι φρουρές επεμβαίνουν αν υπάρχει μη εξουσιοδοτημένη παραποίηση του προστατευμένου προγράμματος, διαφορετικά, μια φρουρά δεν πρέπει να παρεμποδίσει τη βασική λειτουργία του προγράμματος.

Οι φρουρές είναι προγραμματισμένες για να παρέχουν προστασία μέσω για παράδειγμα checksum κώδικα προγράμματος. Ένας μεγάλος αριθμός φρουρών μπορεί να διαμορφώσει ένα δίκτυο (Chang και Atallah, 2001) για να ενισχύσει την ασφάλεια ο ένας τον άλλον από την αμοιβαία προστασία. Οι βασισμένες στο λογισμικό φρουρές μπορούν επίσης να χρησιμοποιηθούν μαζί με τις βασισμένες στο hardware προστασίες για να εξασφαλίσουν ότι το προστατευμένο λογισμικό μπορεί μόνο να εκτελεσθεί σε ένα εξουσιοδοτημένο περιβάλλον.

Οι φρουρές μπορούν να παρέχουν πολλαπλάσια στρώματα άμυνας, για παράδειγμα τις αυτοθεραπευόμενες ικανότητες, για να αποβάλουν τις επιθέσεις. Οι φρουρές πρέπει να είναι ελαστικές. Για να παρέχει αντίσταση στις διαφορετικές επιθέσεις, μια αλλαγή του script μπορεί να παραγάγει μια σημαντικά διαφορετική ροή δομών και κώδικα. Χρησιμοποιώντας τα υψηλού επιπέδου script, οι υπεύθυνοι για την ανάπτυξη μπορούν να επιλέξουν ποιες συγκεκριμένες περιπτώσεις φρουράς να παρεμβάλουν και ποια συγκεκριμένη ακολουθία στη χρήση για τους αντίστοιχους μετασχηματισμούς. Οι φρουρές επιτρέπουν στον υπεύθυνο για την ανάπτυξη να έχει τον ακριβή έλεγχο της τοποθέτησης του κώδικα προστασίας. Οι αντιδράσεις φρουρών να επιτεθούν μπορούν να είναι εύκαμπτες εάν είναι απαραίτητο. Με άλλα λόγια, όταν ανιχνεύονται οι επιθέσεις, οι απαντήσεις από τις φρουρές εξαρτώνται από το επιχειρησιακό πρότυπο του εκδότη λογισμικού και τον αναμενόμενο αντίπαλο.

### 4.4.4 Intrusion Detection

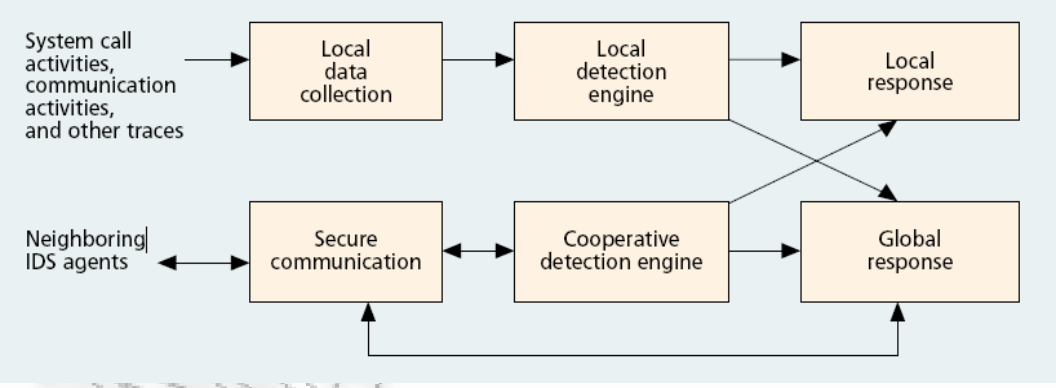
Η ασύρματη ad hoc δικτύωση διαθέτει κάποια τρωτά χαρακτηριστικά όπως η υπαίθρια μετάδοση και η αυτο-οργάνωση χωρίς μια σταθερή υποδομή ή μια συγκεντρωμένη διαχείριση. Συνεπώς, τα ad hoc δίκτυα είναι πιο ευαίσθητα στην επίθεση, και οι προκλήσεις ασφάλειας σε αυτά είναι πιο περίπλοκα. Σαν πρώτη γραμμή υπεράσπισης, οι τεχνικές πρόληψης, όπως η κρυπτογράφηση και η αυθεντικοποίηση, μπορούν να χρησιμοποιηθούν για να υπερασπίσουν το δίκτυο ενάντια στους εισβολείς. Εντούτοις, ακόμη και σε ένα ενσύρματο δίκτυο, η δυναμική υπεράσπιση δεν είναι μόνο επαρκής για να εξασφαλιστεί ένα σύστημα από όλες τις διεισδύσεις. Μια δεύτερη γραμμή αμυντικού συστήματος απαιτείται για να ανιχνεύσει μια τρέχουσα επίθεση στο δίκτυο. Εάν τέτοια ανίχνευση είναι διαθέσιμη, η ζημία μπορεί να ελαχιστοποιηθεί. Η συγκεκριμένη τεχνική θα αναλυθεί εκτενέστερα στο παρακάτω κεφάλαιο.

# 5. Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection System)

## 5.1 Εισαγωγή

Με την αύξηση των παράνομων δραστηριοτήτων και εισβολών στα δικτυωμένα συστήματα υπήρξε παράλληλη ανάπτυξη και στα συστήματα ανίχνευσης εισβολών (IDS), τόσο στον εμπορικό όσο και στον ερευνητικό τομέα.

Ο όρος "Intrusion Detection" σημαίνει "Ανίχνευση Επιθέσεων" και έχει να κάνει με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και την ανάλυσή τους για σημάδια επιθέσεων. Οι επιθέσεις πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω του Internet, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από εξουσιοδοτημένους χρήστες που εκμεταλλεύονται τα δικαιώματα που τους έχουν δοθεί με τρόπο που μπορεί να βλάψει την επιχείρηση, ηθελημένα ή μη. Η εξέλιξη των IDSs είναι ραγδαία τα τελευταία χρόνια και συνεχώς γίνονται προσπάθειες για τη βελτίωσή τους, κυρίως στον τομέα των συμπτωμάτων από False Positives και False Negatives που παρουσιάζουν.




**Σχήμα 10** Intrusion Detection System για δίκτυο MANET

Με την τρέχουσα μορφή τους τα IDSs παρέχουν σημαντική υποστήριξη στα ήδη υπάρχοντα μέτρα προστασίας ενός δικτύου και σε συνδυασμό με άλλους μηχανισμούς ασφάλειας αποτελούν σημαντικό εργαλείο για την αποτροπή δικτυακών επιθέσεων. False Positives ονομάζονται οι λανθασμένες επισημάνσεις που παράγει ένα IDS όταν ανιχνεύει κάποιο γεγονός ως περίπτωση πιθανής επίθεσης ενώ δεν είναι. Τα False Positives είναι δυνατόν να προκύψουν από κακή ρύθμιση ή από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν από μία επίθεση, ως

"συμπεριφορά" των συστημάτων που εμπλέκονται. Από την άλλη μεριά, False Negatives είναι οι περιπτώσεις επιθέσεων τις οποίες το IDS δεν κατάφερε να επισημάνει μετά την εξέτασή τους, κάτι που συνήθως συμβαίνει κατά την εμφάνιση νέας επίθεσης για την οποία δεν υπάρχει προηγούμενη περιγραφή.

Τα εν λόγω συστήματα δεν είναι παντού και πάντα απαραίτητα. Είναι απαραίτητα σε μεγάλες επιχειρήσεις ή σε μικρότερες με ιδιαίτερα εκτεταμένα δίκτυα, πολλούς χρήστες με μεγάλη γεωγραφική διασπορά, σε περιπτώσεις πολλαπλότητας δικτύων, εν ολίγης σε πολύπλοκα περιβάλλοντα. Η Ανίχνευση Επιθέσεων επιτρέπει στις επιχειρήσεις αυτές να προστατεύουν τα συστήματά τους και τις πληροφορίες που βρίσκονται σε αυτά από κινδύνους που προκύπτουν από την αυξημένη δικτυακή διασύνδεση μεταξύ των συστημάτων τους.

Υπάρχουν διάφοροι λόγοι για τους οποίους είναι απαραίτητη η χρήση των IDSs σε αυτές τις περιπτώσεις. Πρώτα και κύρια, τα συγκεκριμένα συστήματα χρησιμεύουν για την ανίχνευση επιθέσεων και άλλων παραβιάσεων ασφάλειας που δεν ανιχνεύονται από άλλα μέτρα προστασίας. Συγκεκριμένα, για την ανίχνευση επιθέσεων στις οποίες ενυπάρχει έντονα ο ανθρώπινος παράγοντας, οπότε οι παράμετροί τους είναι πολλές και συχνά μη ανιχνεύσιμες μέχρι την τελευταία στιγμή. Σε περιβάλλοντα με πολλά συστήματα ο διαχειριστής συνήθως δεν έχει ούτε τη δυνατότητα ούτε το χρόνο να ενημερώνει τα συστήματα που πρέπει με νέες διορθώσεις των αδυναμιών ασφάλειάς τους. Ο συχνότερος κίνδυνος σε ανάλογα περιβάλλοντα προέρχεται από χρήστες των συστημάτων, οι οποίοι κάνουν χρήση διαφόρων λογισμικών που θεωρούνται επικίνδυνα, με την έννοια ότι μπορούν να προκαλέσουν κενά ασφάλειας σε ένα σύστημα. Επιπρόσθετα, τόσο οι διαχειριστές όσο και οι χρήστες κάνουν συχνά λάθη στη ρύθμιση και τη χρήση των συστημάτων και των υπηρεσιών που προσφέρουν.

Τελευταίος λόγος πρέπει να θεωρηθεί η ελλειμματική ενημέρωση με διόρθωση των κενών ασφάλειας από τους οίκους ανάπτυξης λογισμικού. Αυτοί ενημερώνουν συχνά τις λύσεις τους με αναβαθμίσεις. Σε θέματα ασφάλειας, ωστόσο, οι αναβαθμίσεις αυτές προκύπτουν αφού εκδηλωθούν κάποια προβλήματα. Συνεπώς, κανείς διαχειριστής συστήματος δεν μπορεί να αφεθεί στα χέρια τους και να περιμένει ότι οι λύσεις τους θα τον προστατεύσουν απόλυτα. Το ίδιο ισχύει για κάθε σύστημα, όπως και για τα IDSs, αλλά δεδομένου ότι αυτά έχουν διαφορετικούς τρόπους αναγνώρισης των κινδύνων, σε συνεργασία με άλλα προϊόντα μπορούν να φέρουν ένα καλύτερο αποτέλεσμα.

Η χρησιμότητα των IDSs δεν περιορίζονται μονάχα στα παραπάνω, αλλά επεκτείνεται στην ανίχνευση αναγνωριστικών ενεργειών που προηγούνται μίας επίθεσης. Ο επιτιθέμενος συνήθως εξετάζει τον υποψήφιο στόχο του, ώστε να συγκεντρώσει πληροφορίες για αυτόν και να εντοπίσει ένα σημείο εισόδου, το οποίο θα του επιτρέψει να πραγματοποιήσει την επίθεση με επιτυχία. Αυτό επιτυγχάνεται μέσω του scanning. Χωρίς την ύπαρξη ενός IDS ο επιτιθέμενος είναι πολύ πιθανό να

πραγματοποιήσει τις αναγνωριστικές κινήσεις του ανενόχλητος και χωρίς να γίνει αντιληπτός. Ένα IDS θα είχε τη δυνατότητα να εντοπίσει τις κινήσεις αυτές του επιτιθέμενου και να πάρει κάποια μέτρα, όπως να καταγράψει το γεγονός, να ειδοποιήσει σχετικά τους υπεύθυνους ασφάλειας ή και να εμποδίσει τον επιτιθέμενο να τις ολοκληρώσει. Συγχρόνως, τα συστήματα αυτά συμβάλλουν στην αποτελεσματικότερη σχεδίαση και εφαρμογή πολιτικής ασφάλειας. Με τη χρήση των IDSs συλλέγονται πληροφορίες και παρατηρούνται patterns από ενέργειες που πραγματοποιούνται καθημερινά εναντίον ενός δικτύου και των συστημάτων του, τα οποία μπορούν να βοηθήσουν στη σχεδίαση πιο αξιόπιστων μέτρων ασφάλειας, προσαρμοσμένων έτσι ώστε να αντιμετωπίζουν τα γεγονότα και τους κινδύνους που απειλούν το συγκεκριμένο δίκτυο και να οδηγούν στην αποτελεσματικότερη προστασία του.

## 5.2 Χαρακτηριστικά των Συστημάτων Ανίχνευσης Εισβολών

Ένα ιδανικό Σύστημα Ανίχνευσης Εισβολών πρέπει να έχει τα παρακάτω χαρακτηριστικά:

- Ανίχνευση μεγάλου εύρος εισβολών

Τα συστήματα ανίχνευσης εισβολών πρέπει να μπορούν να εντοπίσουν γνωστές και άγνωστες σε αυτά επιθέσεις. Η δυνατότητα αυτή έχει ως προϋπόθεση την ύπαρξη ενός μηχανισμού εκμάθησης στους νέους τύπους επίθεσης και στις αλλαγές της δραστηριότητας των χρηστών.

- Εγκυρότητα στην ανίχνευση των εισβολών

Η ανακάλυψη μιας εισβολής πρέπει να γίνεται σε όσο το δυνατό μικρότερο χρονικό διάστημα, αλλιώς δεν έχει ιδιαίτερη χρησιμότητα ο προσδιορισμός της εισβολής.

- Ακρίβεια στην λειτουργία

Δεν πρέπει να δίνει ψευδές θετικό σήμα, δηλαδή να αναφέρει μια επίθεση ενώ στην πραγματικότητα δεν υπάρχει σχετική επίθεση σε εξέλιξη. Τα ψευδώς θετικά σήματα μειώνουν την αξιοπιστία του συστήματος και αυξάνουν την απαιτούμενη εργασία. Από την άλλη πλευρά, ένα σύστημα ανίχνευσης εισβολών δεν πρέπει να δίνει ψευδώς αρνητικά σήματα, δηλαδή να μην αναφέρει μια πραγματική επίθεση που βρίσκεται σε εξέλιξη. Αυτό είναι ακόμη χειρότερο, αφού σκοπός των συστημάτων ανίχνευσης εισβολών είναι ακριβώς να αναφέρουν τις πραγματικές επιθέσεις.

- Αντιμετώπιση σφαλμάτων

Το σύστημα πρέπει να μπορεί να επανέλθει ακριβώς στην προηγούμενη του κατάσταση μετά από αποτυχίες του συστήματος.

- Πρέπει να τρέχει με ελάχιστη ανθρώπινη παρακολούθηση.

- Προσαρμοστικότητα

Πρέπει να μπορεί να διαμορφώνεται εύκολα, ώστε να προσαρμόζεται με ακρίβεια στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.

- Ανεξάρτητο λειτουργικού συστήματος

Πρέπει να μπορεί να λειτουργεί για ανίχνευση εισβολών σε οποιοδήποτε λειτουργικό σύστημα.

## 5.3 Κατηγορίες Συστημάτων Ανίχνευσης Εισβολών (IDS)

Τα συστήματα ανίχνευσης εισβολών αναπτύχθηκαν για την ανίχνευση της κακόβουλης συμπεριφοράς των χρηστών σε ένα περιβάλλον. Η κακόβουλη συμπεριφορά περιλαμβάνει τους χρήστες που προσπαθούν να λάβουν την μη εξουσιοδοτημένη πρόσβαση στα συστήματα ή τα στοιχεία και ακόμη χρήστες που προσπαθούν να περιορίσουν τη διαθεσιμότητα των πόρων του συστήματος για να νομιμοποιήσει τους χρήστες μέσω της προώθησης των επιθέσεων DoS. Προκειμένου να ανιχνευθεί τέτοια συμπεριφορά, τα συστήματα ανίχνευσης περιέχουν δύο χαρακτηριστικά:

- τμήματα συλλογής δεδομένων
- τμήματα ανάλυσης στοιχείων

Τα τμήματα συλλογής δεδομένων αποτελούνται από τις οντότητες που είναι αρμόδιες για τον έλεγχο και τη συλλογή των δεδομένων για τις δραστηριότητες των χρηστών και της εφαρμογής. Το δεδομένο που λήφθηκε χρησιμοποιείται έπειτα από το δεύτερο τύπο τμημάτων, το οποίο αποκαλείται τμήμα ανάλυσης. Τα τμήματα ανάλυσης δεδομένων είναι αρμόδια για την ανάλυση των δεδομένων και την ανίχνευση οποιασδήποτε κακόβουλης δραστηριότητας.

### 5.3.1 Τμήματα Συλλογής Δεδομένων

Το πρώτο βήμα στην ανίχνευση εισβολών είναι η συλλογή των στοιχείων από το σύστημα που ελέγχεται. Δύο προσεγγίσεις για τη συλλογή δεδομένων έχουν χρησιμοποιηθεί παραδοσιακά στις μεγάλες επιχειρήσεις. Αυτές οι προσεγγίσεις οδηγούν επίσης σε δύο τύπους συστημάτων ανίχνευσης εισβολών:

- Συστήματα Ανίχνευσης Εισβολών Εγκατεστημένα σε Υπολογιστές (HIDS) που τρέχουν σε έναν κόμβο και εστιάζουν να συλλέξουν τα στοιχεία όσον αφορά κάθε κόμβο.

- Δικτυακά Συστήματα Ανίχνευσης Εισβολών (NIDS) που τρέχουν στο δίκτυο και εστιάζουν στη συλλογή των στοιχείων με τον έλεγχο της κυκλοφορίας που τρέχει εντός του δικτύου.

Το πλεονέκτημα του HIDS είναι ότι δεν επηρεάζεται με την χρήση του end-to-end συστήματος κρυπτογραφίας, από τις αλλαγές στην τοπολογία, ή από την δρομολόγηση που μπορεί να προκληθεί από την κινητικότητα των κόμβων σε περίπτωση ad hoc δικτύων. Εντούτοις, το HIDS έχει διάφορα σοβαρά μειονεκτήματα. Αρχικά, ένας εισβολέας μπορεί να αποφύγει την ανίχνευση και να παράγει τη μέγιστη ζημία εκμεταλλευόμενος τις γνώσεις του ότι μόνο ο προορισμός της κυκλοφορίας αναλύει τα πακέτα. Παραδείγματος χάριν εάν ο εισβολέας ξέρει ότι ο προορισμός χρησιμοποιεί μια ιδιαίτερη έκδοση του λειτουργικού συστήματος, κατόπιν μπορεί να προσπαθήσει να διαβιβάσει ένα πακέτο που ακινητοποιεί τη μηχανή μόλις συγκεντρώνει το στρώμα δικτύων του προορισμού το πακέτο και προτού να το αναλύσει το HIDS στο στρώμα εφαρμογής. Δεύτερον, μια επίθεση ενάντια σε έναν host μπορεί να έχει επιπτώσεις στο ίδιο το HIDS. Συχνά αυτό το καθιστά αδύνατο για το IDS να ανιχνεύσει και να αναφέρει την επίθεση δεδομένου ότι ο μηχανισμός ανίχνευσης χρησιμοποιεί τους πόρους υπολογισμού και των διεπαφών του δικτύου. Παραδείγματος χάριν, μια επίθεση DOS σαν στόχο μπορεί ταυτόχρονα να εξαντλήσει το εύρος ζώνης και τον επεξεργαστή του κόμβου.

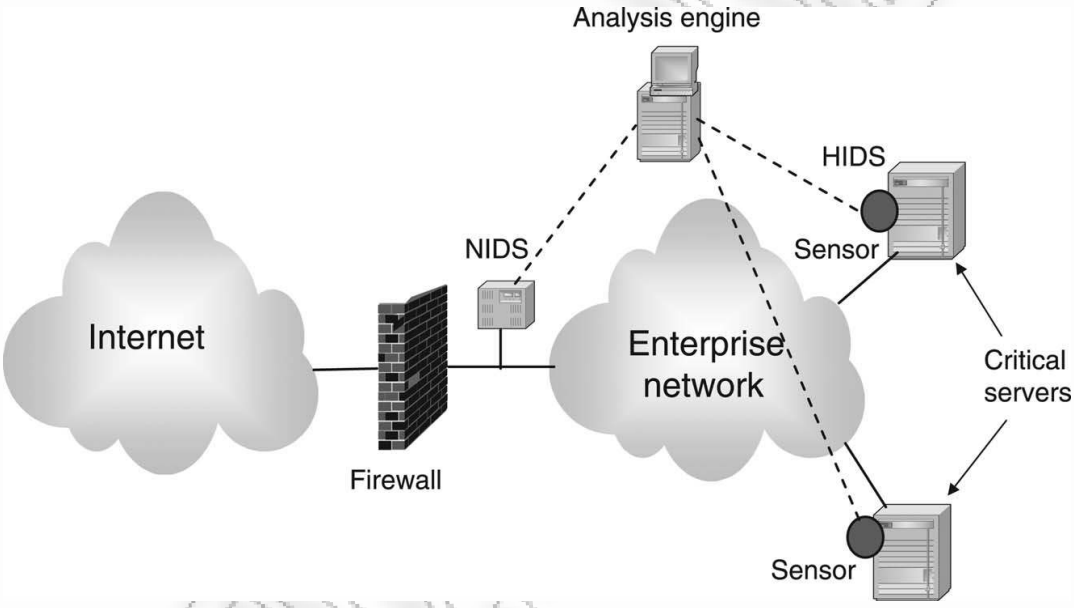
Μερικοί περιορισμοί του HIDS είναι πιο σχετικοί για τα ad hoc δίκτυα απ' ότι για τα επιχειρηματικά δίκτυα. Στα ad hoc δίκτυα, πολλοί από τους κόμβους προορισμού μπορούν να μην είναι σε θέση να εκτελέσουν το IDS λόγω του περιορισμένου υπολογιστικού πόρου και της χαμηλής υπολειπόμενης ενέργειας. Εάν μόνο οι τελικοί χρήστες εκτελέσουν το IDS, τα κακόβουλα πακέτα δεν θα απορριφθούν έως ότου φθάσουν στον προορισμό. Αυτό είναι επικίνδυνο στα ad hoc όπου διάφοροι κόμβοι μπορούν να χρησιμοποιήσουν την περιορισμένη ενέργεια και το εύρος ζώνης τους στην αναμετάδοση των κακόβουλων πακέτων.

Η άλλη προσέγγιση στην ανίχνευση εισβολών είναι το NIDS και έχει διάφορα πλεονεκτήματα. Κατ' αρχάς, ένας εισβολέας δεν μπορεί πλέον να είναι σίγουρος ότι μόνο ο προορισμός εκτελεί το IDS. Επιπλέον, οι ενεργοί κόμβοι IDS μπορούν να επιλεχτούν έτσι ώστε να έχουν διαφορετικά χαρακτηριστικά, διανέμοντας κατά συνέπεια το φορτίο IDS μεταξύ των συσκευών με τις κατάλληλες ικανότητες και καθιστώντας το δυσκολότερο για τους εισβολείς να επινοήσουν τις επιθέσεις για να παρακάμψουν το IDS. Δεύτερον, η προσέγγιση NIDS οδηγεί σε λιγότερες οντότητες, προστατεύοντας τους πολλαπλούς hosts. Αυτό μειώνει το κόστος του IDS. Τρίτον, είναι εύκολο να τοποθετηθούν στα υπάρχοντα δίκτυα με την ελάχιστη προσπάθεια δεδομένου ότι το IDS πρέπει μόνο να εγκατασταθεί σε ένα υποσύνολο των κόμβων. Τέταρτο, οι ενεργοί κόμβοι IDS μπορούν να επιλεχτούν μόνο μεταξύ εκείνων που έχουν την απαραίτητη ικανότητα. Τέλος, το NIDS συλλαμβάνει τα κακόβουλα πακέτα κατά τη μεταφορά και περιορίζει έτσι την απώλεια του εύρους ζώνης και την ενέργεια στην αναμετάδοση τους όπως συζητούνται νωρίτερα. Τα τελευταία δύο πλεονεκτήματα είναι πολύ σημαντικά κατά την εξέταση των ad hoc δικτύων.

Υπάρχουν επίσης διάφορα μειονεκτήματα που συνδέονται με το NIDS. Το NIDS δεν μπορεί να είναι πάντα σε θέση να εργαστεί με τις κρυπτογραφημένες πληροφορίες. Το NIDS μπορεί να αναλύσει την κρυπτογραφημένη κυκλοφορία όταν η κρυπτογράφηση δεν είναι σε ένα στρώμα στο οποίο λειτουργεί και το ίδιο. Παραδείγματος χάριν, όταν κρυπτογραφείται η κυκλοφορία στο στρώμα εφαρμογής, οι ενότητες IDS μπορούν να ανιχνεύσουν τις επιθέσεις στη μεταφορά και τα χαμηλότερα στρώματα, όπως, το ping-of-death, πλημμύρα TCP SYN, smurf. Εάν η κρυπτογράφηση χρησιμοποιείται σε όλα τα στρώματα, το οποίο γίνεται κυρίως στα δίκτυα πεδίων μαχών, τα σχέδια πρέπει να έχουν ως σκοπό να διανείμουν τα κλειδιά ασφαλώς στους ενεργούς κόμβους έτσι ώστε το IDS να μπορεί να αποκρυπτογραφήσει την κυκλοφορία και να αναλύσει την ανίχνευση των επιθέσεων. Η προσέγγιση NIDS σε ένα ασύρματο ειδικό δίκτυο έχει έναν άλλο περιορισμό. Μπορεί να είναι δυνατό να επινοηθούν επιθέσεις βασισμένες στα τεμαχισμένα πακέτα και τις πολλαπλές διαδρομές που στέλνουν τα τεμάχια των επιθέσεων μέσω διαφορετικών πορειών του δικτύου. Οι αισθητήρες του NIDS δεν μπορούν να παρατηρήσουν όλα τα τεμάχια της επίθεσης και επομένως μπορούν να μην είναι σε θέση να ανιχνεύσουν την επίθεση. Τέτοιες επιθέσεις είναι αποτελεσματικότερες σε ένα ασύρματο ad hoc δίκτυο δεδομένου ότι οι κόμβοι κινούνται συχνά και υπάρχει συχνή αλλαγή των διαδρομών. Αυτό το καθιστά πιθανότερο ότι μια ενιαία οντότητα NIDS μπορεί να μην παρατηρήσει όλη τη σχετική κυκλοφορία για την ανίχνευση της επίθεσης.

Είναι σαφές ότι και τα HIDS και οι προσεγγίσεις NIDS έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Επομένως, και οι δύο προσεγγίσεις χρησιμοποιούνται συχνά μαζί σε συμπληρωματικούς ρόλους. Σε ένα χαρακτηριστικό επιχειρηματικό περιβάλλον σήμερα, η δραστηριότητα που θα μπορούσε να ελεγχθεί από ένα IDS

είναι απίστευτα μεγάλη και είναι συχνά μη πρακτικό να ελεγχθεί όλο αυτό. Οι επιχειρήσεις επιλέγουν συνήθως τα βασικά τους σημεία που πρέπει να ελεγχθούν ανάλογα με το πόσο σημαντικό είναι να προστατευτούν. Ως εκ τούτου, είναι χαρακτηριστικό για τις επιχειρήσεις να ελέγξουν τις δραστηριότητες στους κεντρικούς υπολογιστές και τις εφαρμογές μέσω HIDS. Είναι επίσης χαρακτηριστικό για τις επιχειρήσεις να τοποθετήσουν το NIDSs πίσω από τις αντιπυρικές ζώνες που προστατεύουν την επιχείρηση από την εξωτερική κυκλοφορία. Ένα καλά τοποθετημένο NIDS σε ένα επιχειρηματικό δίκτυο μπορεί να ελέγξει το μεγαλύτερο μέρος της κυκλοφορίας στο δίκτυο και να ανιχνεύσουν τις κακόβουλες δραστηριότητες. Αυτή η αρχιτεκτονική προσέγγιση παρουσιάζεται στο σχήμα 11.




**Σχήμα 11** IDS τοποθετημένο σε επιχειρησιακό περιβάλλον

## 5.3.2 Τμήματα Ανάλυσης Στοιχείων

Μόλις γίνει η παραλαβή του στοιχείου από τους αισθητήρες του IDS, πρέπει να αναλυθεί έτσι ώστε η κακόβουλη δραστηριότητα να μπορεί να ανιχνευθεί. Το IDS ενσωματώνει μηχανές ανάλυσης που αναλύουν αυτόματα τα στοιχεία που συλλέγονται από τους διάφορους αισθητήρες για να ανιχνεύσουν τις κακόβουλες δραστηριότητες. Δεδομένου ότι το ποσό των δεδομένων που παραλαμβάνονται συνήθως από τους αισθητήρες είναι πολύ μεγάλο για τους ανθρώπους, οι μηχανές ανάλυσης που μπορούν να εξετάσουν όλα τα διαθέσιμα στοιχεία που συλλέγονται

από το NIDS και το HIDS είναι πολύ σημαντικές. Η ανάλυση των δεδομένων του IDS περιλαμβάνει να παγιώσει τα δεδομένα ενδεχομένως σε μια κεντρική θέση και να προσδιορίσει τις κακόβουλες δραστηριότητες αυτόματα στο μέτρο του δυνατού. Σε μερικές περιπτώσεις οι HIDS και NIDS αισθητήρες περιέχουν μερικές προκαταρκτικές ικανότητες ανάλυσης. Μια τέτοια ικανότητα επιτρέπει στο IDS να ανιχνεύσει την επίθεση τοπικά στον αισθητήρα, την αυξανόμενη ταχύτητα ανίχνευσης και την άδεια της γρηγορότερης αντίδρασης. Μια τέτοια ικανότητα ελαχιστοποιεί επίσης την ανάγκη να μεταφερθούν όλα τα δεδομένα σε μια κεντρικά τοποθετημένη μηχανή ανάλυσης, μειώνοντας με τον τρόπο αυτό τα παραπάνω δεδομένα που παράγονται.

Οι μηχανές ανάλυσης μπορούν να χρησιμοποιήσουν ποικίλες τεχνικές για την κακόβουλη συμπεριφορά. Οι δύο ευρύτατα χρησιμοποιημένες τεχνικές είναι:

- ανίχνευση κακής χρήσης
- ανίχνευση ανωμαλίας

Η τεχνική ανίχνευσης κακής χρήσης περιλαμβάνει την ανάλυση των στοιχείων που έχουν συγκεντρωθεί για συγκεκριμένα σχέδια συμπεριφοράς που είναι γνωστά για συγκεκριμένες επιθέσεις. Αυτά τα σχέδια συμπεριφοράς καλούνται υπογραφές. Παραδείγματος χάριν, ένα πακέτο UDP που προορίζεται στην πόρτα 0 μπορεί να συντρίψει μερικές μηχανές. Η υπογραφή μιας επίθεσης ping-of-death είναι ένα πολύ μεγάλο ping πακέτο. Η υπογραφή μιας επίθεσης RPC locator είναι ένα πακέτο το οποίο προορίζεται για την πόρτα 135 που περιέχει μια εντολή που το σύστημα δεν την αναμένει. Η υπογραφή μιας Bubonic επίθεσης γίνεται από με διάφορες τιμές, όπως ένα TTL 255, μια TOS με τιμή πεδίου 0 _ C9, ακριβή φορτίο 20 byte στο διάγραμμα δεδομένων IP. Η τεχνική ανίχνευσης κακής χρήσης χρησιμοποιείται ευρέως σήμερα από τα εμπορικά συστήματα επειδή παρέχει ακριβή ανίχνευση των επιθέσεων, με αυτόν τον τρόπο με συνέπεια τα χαμηλά ποσοστά ψεύτικων συναγερμών. Όταν μια υπογραφή για μια επίθεση προσδιοριστεί, είναι απλή η ανιχνεύσει της επίθεσης με τη σύγκριση ενός πακέτου με την ακριβή υπογραφή της επίθεσης. Το πρόβλημα με τις τεχνικές ανίχνευσης εισβολών είναι ότι αυτές οι τεχνικές μπορούν μόνο να ανιχνεύσουν τις γνωστές επιθέσεις με τα καθορισμένα σχέδια της κακόβουλης συμπεριφοράς. Οι νέες επιθέσεις δεν μπορούν να ανιχνευθούν έως ότου δημιουργηθεί μια νέα υπογραφή για την επίθεση.

Η τεχνική ανίχνευσης ανωμαλιών περιλαμβάνει την έρευνα της συμπεριφοράς που είναι εκτός της κανονικής αναμενόμενης συμπεριφοράς. Αυτό γίνεται συνήθως με τη χρησιμοποίηση των στατιστικών τεχνικών που συγκρίνουν την παρατηρηθείς συμπεριφορά ενάντια στις στατιστικές της αναμενόμενης κανονικής συμπεριφοράς. Αυτές οι τεχνικές χρησιμοποιούν συχνά τα κατώτατα όρια (όπως το ποσό υπερβολικής φόρτωσης της CPU, κ.λπ.) και αν αυτά ξεπεραστούν δηλώνουν μια

επίθεση. Οι ανιχνευτές που χρησιμοποιούν αυτήν την τεχνική απαιτούν κατάρτιση ώστε τα κατώτατα όρια που χρησιμοποιούνται για την ανίχνευση της ανώμαλης συμπεριφοράς να τίθενται στις κατάλληλες τιμές. Το πλεονέκτημα της anomaly-based ανίχνευσης είναι ότι αυτή η τεχνική δεν απαιτεί την ύπαρξη των ακριβών υπογραφών και μπορεί επομένως να χρησιμοποιηθεί για την ανίχνευση των επιθέσεων που δεν είδαμε κατά το παρελθόν. Το μειονέκτημα της anomaly-based ανίχνευσης είναι ότι, λόγω της στατιστικής φύσης της, είναι περισσότερο επιρρεπής σε ψεύτικους θετικούς συναγερμούς ανάλογα με το πώς τα κατώτατα όρια τίθενται. Υπάρχει πάντα μια ανταλλαγή μεταξύ του καθορισμού των πολύ σφιχτών κατώτατων ορίων (κοντά στην κανονική συμπεριφορά), να προκαλέσουν κατά συνέπεια πολλά ψεύτικα θετικά όταν παρεκκλίνουν οι χρήστες ακόμα και ελαφρώς από την αναμενόμενη συμπεριφορά, και του καθορισμού των πολύ χαλαρών κατώτατων ορίων που ελαχιστοποιούν τα ψεύτικα θετικά αλλά επιτρέπουν στους επιτιθεμένους να αποφύγουν την ανίχνευση. Λαμβάνοντας υπόψη τα μειονεκτήματα, αυτή η τεχνική δεν χρησιμοποιείται ευρέως στα εμπορικά συστήματα.

Μια άλλη τεχνική για την κακόβουλη δραστηριότητα έχει εισαχθεί πρόσφατα αν και δεν χρησιμοποιείται συνήθως ακόμα στα εμπορικά συστήματα. Αυτή η τεχνική, αποκαλούμενη ως προδιαγραφή βασισμένη στην ανίχνευση, υποθέτει την ύπαρξη μιας ακριβούς προδιαγραφής πρωτοκόλλου. Η κακόβουλη συμπεριφορά ανιχνεύεται με τη σύγκριση της κυκλοφορίας του πρωτόκολλου με την προδιαγραφή πρωτόκολλου. Οι ανιχνευτές δημιουργούν χαρακτηριστικά τα ακριβή πρότυπα της αναμενόμενης συμπεριφοράς βασισμένοι στις προδιαγραφές του πρωτόκολλου και συγκρίνουν έπειτα την παρατηρηθείς συμπεριφορά στο δίκτυο ενάντια στο πρότυπο. Το πλεονέκτημα των τεχνικών ανίχνευσης που είναι βασισμένες στις προδιαγραφές είναι ότι λαμβάνοντας υπόψη τις ακριβείς προδιαγραφές της κανονικής συμπεριφοράς (π.χ. οι προδιαγραφές πρωτοκόλλων), η κακόβουλη συμπεριφορά μπορεί να ανιχνευθεί με έναν υψηλό βαθμό βεβαιότητας. Αυτό αποβάλλει τη δυνατότητα ότι ένας ανιχνευτής θα ταξινομήσει μια κανονική συμπεριφορά σαν κακόβουλη, η οποία μειώνει τα ψεύτικα θετικά. Τέτοιοι ανιχνευτές μπορούν επίσης να επισημάνουν τις νέες επιθέσεις δεδομένου ότι αυτοί οι ανιχνευτές δεν εξαρτώνται από την ύπαρξη των συγκεκριμένων υπογραφών επίθεσης. Αφ' ενός, η ανάπτυξη των προτύπων της κανονικής συμπεριφοράς για κάθε πρωτόκολλο είναι συχνά ένας αρκετά σύνθετος στόχος. Περαιτέρω, αυτή η προσέγγιση απαιτεί τα πρότυπα της κανονικής συμπεριφοράς για όλα τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο προκειμένου να ανιχνευθεί ένα ευρύ φάσμα των επιθέσεων. Αυτά τα πρότυπα πρέπει να εκτελεσθούν για κάθε κόμβο στο δίκτυο. Κατά συνέπεια, αυτά τα σχέδια ανίχνευσης απαιτούν σημαντικούς πόρους της CPU για ένα μεγάλο επιχειρηματικό δίκτυο. Ένας άλλος περιορισμός της τεχνικής αυτής είναι ότι οι ανιχνευτές που την χρησιμοποιούν δεν ανιχνεύουν τις επιθέσεις που δεν παραβιάζουν την προδιαγραφή, αλλά εκμεταλλεύονται την επιτρεπόμενη συμπεριφορά για να προωθήσουν μια

επίθεση. Παραδείγματος χάριν, σε μια flooding επίθεση ή μια επίθεση flooding TCP SYN, η συμπεριφορά ενός κόμβου είναι αποδεκτή από την προδιαγραφή πρωτοκόλλου, αλλά η συμπεριφορά είναι πραγματικά επιβλαβής στη λειτουργία της επιχείρησης και είναι επομένως κακόβουλη.

Η ανίχνευση των επιθέσεων δεν είναι χαρακτηριστικά ικανοποιητική για την προστασία μιας επιχείρησης επειδή η επίθεση μπορεί να συνεχίσει να προκαλεί τη ζημιά στο δίκτυο. Επομένως, τα συστήματα ανίχνευσης εισβολών συνδέονται συνήθως με τα συστήματα απάντησης επίθεσης. Μόλις προσδιοριστεί μια επίθεση από το IDS, το σύστημα απάντησης είναι αρμόδιο για την παύση της επίθεσης. Θα μπορούσε να το κάνει αυτό με την απομόνωση της κακόβουλης συμπεριφοράς ή με το να κόψει τον επιτιθέμενο από το δίκτυο και αν είναι δυνατόν αποκαθιστώντας τη ζημία που προκλήθηκε από τον επιτιθέμενο. Οι απαντήσεις είναι δύο τύπων:

- Ενεργή απάντηση
- Παθητική απάντηση

Στην περίπτωση της ενεργού απάντησης, οι ενέργειες λαμβάνονται αυτόματα όταν ανιχνεύονται ορισμένοι τύποι εισβολών. Αυτή περιλαμβάνει τις δραστηριότητες όπως η συλλογή των πρόσθετων πληροφοριών ή η αλλαγή του περιβάλλοντος προκειμένου να σταματήσει η επίθεση. Ο σκοπός της συλλογής των πρόσθετων πληροφοριών θα μπορούσε να είναι η ανάπτυξη της ανησυχία του επιτιθεμένου. Η αλλαγή του περιβάλλοντος θα μπορούσε να οδηγήσει στη στάση μιας υπό εξέλιξη επίθεσης και το μπλοκάρισμα της πρόσβασης του επιτιθέμενου. Αυτό μπορεί να περιπλέκει τις ενέργειες όπως η εισαγωγή των πακέτων rest του TCP, η μετατροπή των δρομολογητών και των αντιπυρικών ζωνών, ανακαλώντας τα πιστοποιητικά των κακόβουλων χρηστών. Στην περίπτωση της παθητικής απάντησης, ο στόχος είναι να προκληθεί πρόσθετος έλεγχος που να μπορεί να παρατηρήσει περισσότερο την κακόβουλη συμπεριφορά και να παρέχει τις πληροφορίες στους χρήστες συστημάτων με την αποστολή συναγερμών και ανακοινώσεων.

## 5.4 Αρχιτεκτονικές Συστημάτων Ανίχνευσης Εισβολών

Η φύση των ασύρματων ad hoc δικτύων τα καθιστά πολύ τρωτά σε επιθέσεις. Καταρχήν, οι κινητοί κόμβοι είναι ανεξάρτητοι και οι μετακινήσεις τους δεν ελέγχονται από το σύστημα, έτσι μπορούν εύκολα να συλληφθούν, να συμβιβαστούν και να τους γίνει κάποια μορφή επίθεσης. Δεδομένου ότι στα ασύρματα δίκτυα δεν υπάρχει κανένα φυσικό εμπόδιο για τον αντίπαλο, οι επιθέσεις μπορούν να προέλθουν από όλες τις κατευθύνσεις και να στοχεύσουν σε οποιοδήποτε κόμβο. Τέλος στα ασύρματα ad hoc δίκτυα οι αντίπαλοι μπορούν να εκμεταλλευτούν την

αποκεντρωμένη διαχείριση για τους νέους τύπους επιθέσεων με σκοπό να σπάσουν τους συνεταιριστικούς αλγορίθμους. Για να αντιμετωπίσουν αυτές τις πρόσθετες προκλήσεις, διάφορες πιθανές αρχιτεκτονικές IDS υπάρχουν συμπεριλαμβανομένου του αυτόνομου IDS, διανεμημένου και συνεταιριστικού IDS και ιεραρχικού IDS.

### 5.4.1 Αυτόνομο IDS

Σε αυτήν την αρχιτεκτονική κάθε κόμβος έχει το IDS του και ανιχνεύει τις επιθέσεις ανεξάρτητα. Δεν υπάρχει καμία συνεργασία μεταξύ των κόμβων και όλες οι αποφάσεις είναι βασισμένες στις πληροφορίες που συλλέγονται από τους μεμονωμένους κόμβους. Αυτή η αρχιτεκτονική δεν είναι αρκετά αποτελεσματική αλλά μπορεί να χρησιμοποιηθεί στα δίκτυα όπου κάθε κόμβος είναι σε θέση να τρέξει ένα IDS.

### 5.4.2 Ιεραρχικό IDS

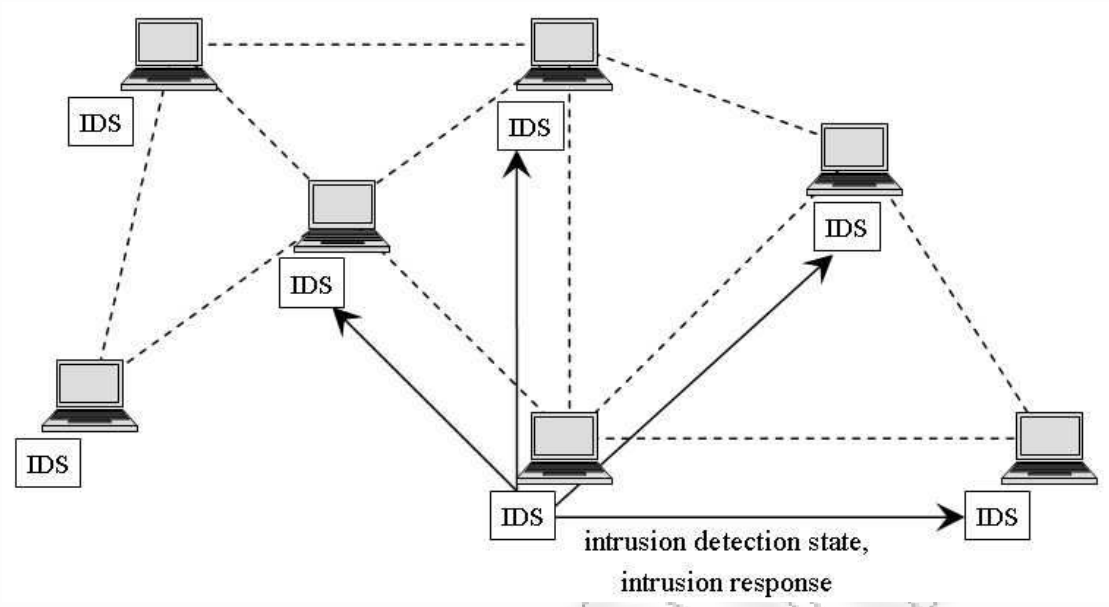
Οι πολυεπίπεδοι ασύρματοι ad hoc κόμβοι δικτύων διαιρούνται σε συστάδες. Για να προσαρμόσουν στις απαιτήσεις, τα ιεραρχικά συστήματα ανίχνευσης εισβολών προτείνουν, κάθε κόμβος να έχει τον δικό του πράκτορα IDS αρμόδιο για την τοπική ανίχνευση εισβολών. Συγχρόνως, ο πράκτορας IDS του αρχηγού των συστάδων είναι αρμόδιος και για την τοπική και σφαιρική ανίχνευση εισβολής. Η συνολική κάλυψη δικτύων βεβαιώνεται με την ενεργοποίηση των σφαιρικών πρακτόρων σε κάθε αρχηγό συστάδων. Εντούτοις, η ομαδοποίηση προσθέτει επίσης πιθανά σημεία επίθεσης, πολυπλοκότητας στη δημιουργία και τη συντήρηση των ομάδων. Μια εναλλακτική διανεμημένη λύση, αποκαλούμενη ως αυθόρμητοι φύλακες, προτείνεται για τις επίπεδες δικτυακές αρχιτεκτονικές αισθητήρων χωρίς την οργάνωση τους σε συστάδες ή προσθήκη των ισχυρότερων κόμβων. Μερικοί κόμβοι αισθητήρων επιλέγονται ανεξάρτητα ως αυθόρμητοι φύλακες για να ελέγξουν τις επικοινωνίες στις ομάδες τους. Η τεχνική στηρίζεται στη φύση της broadcast μετάδοσης των επικοινωνιών αισθητήρων και εκμεταλλεύεται την υψηλή πυκνότητα των κόμβων που επεκτείνονται στον τομέα. Κάθε πακέτο μπορεί να παραληφθεί από ένα σύνολο κόμβων είτε σε μια σειρά broadcast αναμετάδοσης είτε στον επόμενο hop ως πακέτο. Ως εκ τούτου, όλοι αυτοί οι κόμβοι έχουν μια πιθανότητα να ενεργοποιήσουν τους πράκτορές τους προκειμένου να ελέγξουν αυτά τα πακέτα.

### 5.4.3 Κινητός πράκτορας IDS

Ο κινητός πράκτορας IDS μπορεί να θεωρηθεί είτε διανεμημένη και συνεταιριστική τεχνική ανίχνευσης εισβολής ή μπορεί να χρησιμοποιηθεί σε συνδυασμό με ιεραρχικό IDS. Ένας πράκτορας θεωρείται κινητός εξαιτίας της δυνατότητά του να κινηθεί μέσω του δικτύου να αλληλεπιδράσει με τους κόμβους και να συλλέξει τις πληροφορίες από αυτούς. Οι στόχοι της ανίχνευσης διανέμονται και ορίζονται σε αυτούς τους κινητούς πράκτορες. Σε κάθε κινητό πράκτορα ορίζεται ένας συγκεκριμένος στόχος και ενεργεί επάνω στις πληροφορίες που συλλέγει κατά μήκος της κινούμενης πορείας του. Υπάρχουν πολλά πλεονεκτήματα (Mishra et al., 2004) της χρησιμοποίησης των κινητών πρακτόρων. Καταρχήν, η κατανάλωση ισχύος του δικτύου μειώνεται επειδή οι στόχοι διανέμονται και κάθε κόμβος κρατά μόνο μερικούς από τους στόχους και όχι όλους. Αφετέρου, η γενική ανοχή ελαττωμάτων των συστημάτων αυξάνεται επειδή οι στόχοι IDS διανέμονται στα διαφορετικά μέρη του δικτύου όταν μερικοί πράκτορες καταστρέφονται ή τα μέρη του δικτύου χωρίζονται όταν οι άλλοι πράκτορες μπορούν να παραμείνουν λειτουργικοί. Τρίτον, όπως ο κινητός πράκτορας μπορεί να είναι ανεξάρτητος πλατφορμών, το IDS μπορεί να τρέξει στο πλαίσιο των διαφορετικών περιβαλλόντων και λειτουργικών συστημάτων. Επιπλέον, όταν αντικαθίσταται μια μονάδα κεντρικής επεξεργασίας από τους διανεμημένους κινητούς πράκτορες, το υπολογιστικό φορτίο διαιρείται μεταξύ των μηχανών και το φορτίο των δικτύων μειώνεται. Τέλος, αυτοί οι κινητοί πράκτορες πρέπει ακόμα να οργανωθούν σε μια ασφαλή ενότητα σε κάθε κόμβο προκειμένου να προστατευθούν από τους μακρινούς hosts.

### 5.4.4 Διανεμημένο και συνεταιριστικό IDS

Δεδομένου ότι τα ασύρματα ειδικά δίκτυα διανέμονται και βασίζονται στη συνεργασία μεταξύ των κόμβων, το σύστημα ανίχνευσης εισβολών και απάντησης πρέπει επίσης να διανεμηθεί και συνεταιριστικά. Σε αυτήν την αρχιτεκτονική (Zhang et al., 2003), κάθε κόμβος έχει έναν πράκτορα IDS και λαμβάνει τις τοπικές αποφάσεις ανίχνευσης μόνος του. Συγχρόνως, όλοι οι κόμβοι συμμετέχουν σε μια σφαιρική διαδικασία ανίχνευσης. Όπως την αυτόνομη αρχιτεκτονική IDS, η διανεμημένη και συνεταιριστική δομή IDS είναι καταλληλότερη για μια επίπεδη διαμόρφωση δικτύων (σχήμα 12).



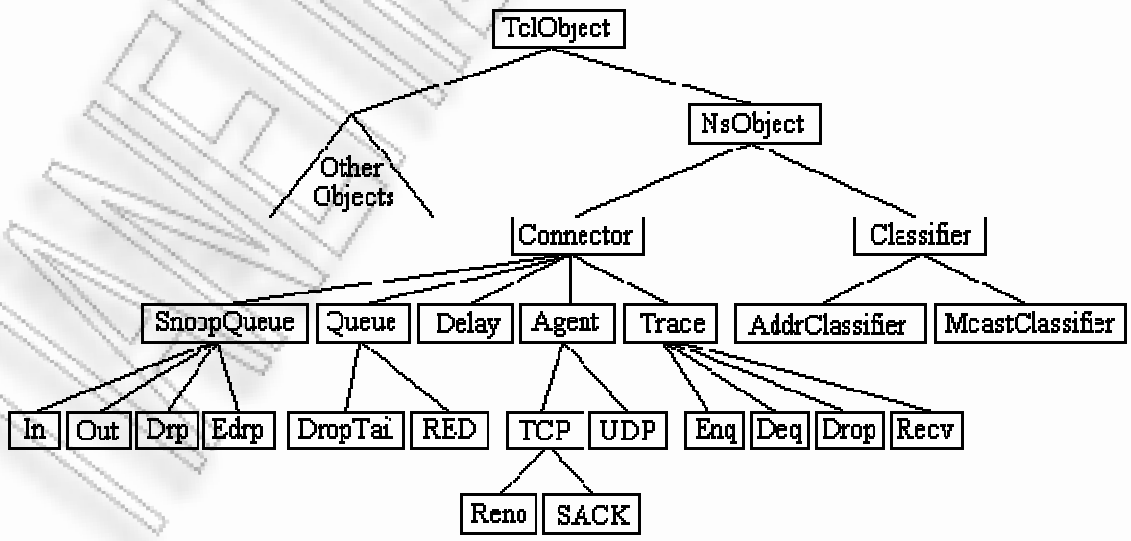

**Σχήμα 12** Διανεμημένο και συνεταιριστικό IDS

# 6. Περιγραφή Network Simulator 2 (NS-2)

## 6.1 Γενική περιγραφή

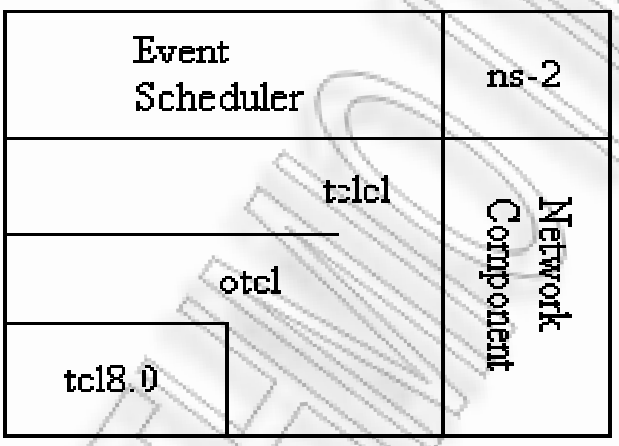
Στο πειραματικό μέρος της διπλωματικής εργασίας, εξομοιώνεται ένα δίκτυο και αναλύονται κάποια από τα μεγέθη που το χαρακτηρίζουν. Η εξομοίωση γίνεται με το πρόγραμμα Network Simulator (NS-2) χρησιμοποιώντας την έκδοση 2.34 για Linux Unix η οποία είναι η νεότερη έκδοση του Network Simulator.

Ο Network Simulator (NS) είναι ένας προσομοιωτής διακριτών γεγονότων (discrete event simulator) ο οποίος στοχεύει στην έρευνα δικτύων. Ο NS παρέχει σημαντική υποστήριξη για προσομοίωση των πρωτοκόλλων TCP/UDP, δρομολόγησης και πολυεκπομπής σε ενσύρματα και ασύρματα (τοπικά και δορυφορικά) δίκτυα. Αυτό σημαίνει ότι υπάρχουν οι κατάλληλες βιβλιοθήκες και συναρτήσεις έτσι ώστε ο κάθε χρήστης του NS να μπορεί να στήσει και να μελετήσει την τοπολογία που αυτός θέλει. Ο NS βρίσκεται σε συνεχή εξέλιξη και βελτίωση καθώς όλο και περισσότερες δυνατότητες και χαρακτηριστικά προστίθενται. Επίσης πρέπει να σημειωθεί ότι στην εξέλιξη αυτή συμβάλλουν διάφορα εκπαιδευτικά ιδρύματα (π.χ. το ISI – Information Sciences Institute, www.isi.edu), όπως και απλοί χρήστες με τις παρατηρήσεις τους ή με ενεργό συμμετοχή στη δημιουργία ή στη βελτίωση των διάφορων συναρτήσεων. Ακόμα και ο χρήστης για τη δική του εφαρμογή μπορεί να δημιουργήσει καινούριους τύπους αντικειμένων όπως είναι οι agents με συγκεκριμένα χαρακτηριστικά και δυνατότητες (σχήμα 13).

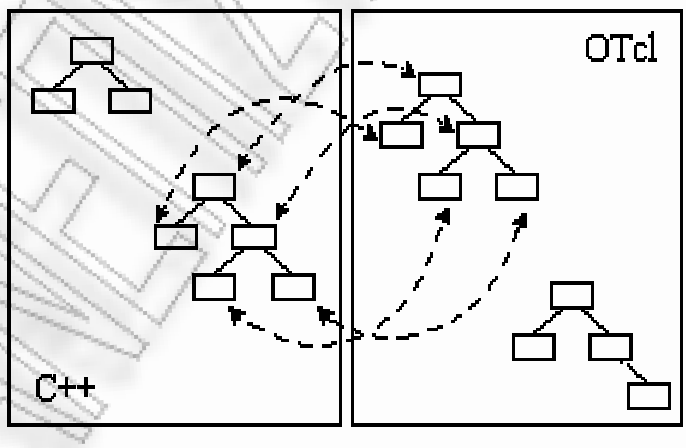


**Σχήμα 13** Αντικείμενα στον Network Simulator

Όπως ήδη προαναφέρθηκε, ο προσομοιωτής στηρίζεται σε διακριτά γεγονότα. Αυτό σημαίνει ότι ο χρήστης προκειμένου να φτιάξει ένα πρόγραμμα που θα το τρέξει με τη βοήθεια του NS και θα βγάλει τα αποτελέσματα που χρειάζεται πρέπει να δώσει ιδιαίτερη έμφαση στα γεγονότα και κυρίως πως αυτά εισάγονται στον NS. Για τη δημιουργία της τοπολογίας και των διάφορων γεγονότων ο NS υποστηρίζει τις γλώσσες προγραμματισμού OTCL (Object TCL) και C++ σε συνεργασία μεταξύ τους (σχήμα 14, σχήμα 15).




**Σχήμα 14** Αρχιτεκτονική του NS




**Σχήμα 15** Συνεργασία C++ και OTcl

Πιο συγκεκριμένα η OTCL χρησιμοποιείται για τη δημιουργία της τοπολογίας, για την δημιουργία κάποιων αντικειμένων επί της τοπολογίας, καθώς και για την εν

δυνάμει αλλαγή των συνθηκών σε κάποιες χρονικές στιγμές της προσομοίωσης. Αντίθετα η C++ χρησιμοποιείται για τον χειρισμό των πακέτων και για το χειρισμό αντικειμένων τα οποία δεν έχουν άμεση σχέση με τη συγκεκριμένη τοπολογία. Σε γενικές γραμμές η C++ προσφέρει πολλές περισσότερες δυνατότητες, λόγω βιβλιοθηκών και ύπαρξη πιο πλούσιων δομών, από ότι η OTCL και είναι πιο γρήγορη στην εκτέλεσή της. Όμως η OTCL έχει τη δυνατότητα να επικοινωνεί καλύτερα με τον NS και να προσομοιώνει τη δημιουργία των διάφορων γεγονότων όποτε εμείς θέλουμε. Επίσης υπάρχουν κάποιες έτοιμες συναρτήσεις αποκλειστικά για τον NS όπως είναι η δημιουργία κόμβων και agents, ενώ η δυνατότητα να εκτελεί των κώδικα δυναμικά ανάλογα με τη δεδομένη κατάσταση του δικτύου είναι ιδιαίτερη χρήσιμη. Πρέπει να αναφέρουμε ότι η σύνδεση μεταξύ των δύο αυτών γλωσσών προγραμματισμού γίνεται ιδιαίτερα αποδοτικά και η απόφαση για το βαθμό στον οποίο ο χρήστης θα χρησιμοποιήσει τη κάθε γλώσσα εξαρτάται κυρίως από την εξοικείωσή του με αυτήν και από τη συγκεκριμένη προσομοίωση. Σε γενικές όμως γραμμές ακολουθείται η τακτική που προαναφέρθηκε. Επίσης η δημιουργία αντικειμένων – κλάσεων που συνδέονται άμεσα με τα βασικά αντικείμενα που χρησιμοποιεί ο NS (κόμβοι, agents, ζεύξεις) είναι ιδιαίτερα βολική, καθώς η όλη υλοποίηση γίνεται πολύ πιο κατανοητή και είναι πιο κοντά στην πραγματικότητα. Στη δημιουργία αυτών των αντικειμένων η χρήση της OTCL και της C++ ενδείκνυται καθώς και οι δύο γλώσσες υποστηρίζουν τον αντικειμενοστραφή προγραμματισμό.

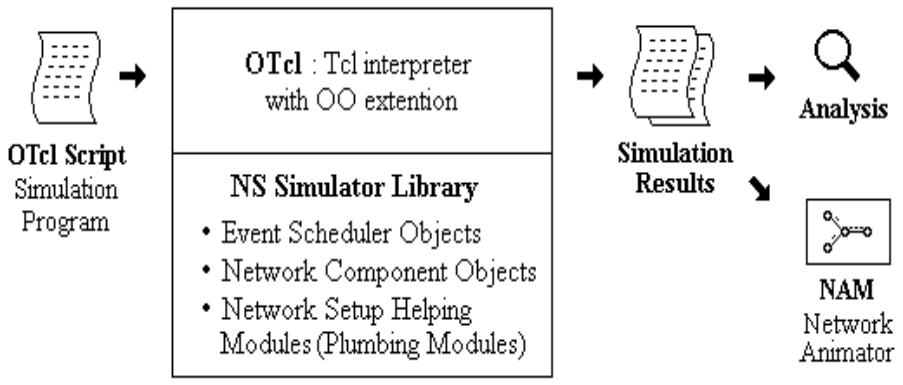
| event | time | from node | to node | pkt type | pkt size | flags | fid | src addr | dst addr | seq num | pkt id |
|---|---|---|---|---|---|---|---|---|---|---|---|

```
r : receive (at to_node)
+ : enqueue (at queue)              src_addr : node.port (3.0)
- : dequeue (at queue)              dst_addr : node.port (0.0)
d : drop    (at queue)
```

**Σχήμα 16** Ανάλυση κίνησης

Το αρχείο το οποίο τρέχουμε με τον NS έχει τη μορφή script.tcl, όπου script είναι το όνομα που εμείς έχουμε δώσει στο αρχείο μας και η κατάληξη *.tcl δηλώνει ότι είναι γραμμένο σε γλώσσα προγραμματισμού OTCL. Κατά την εκτέλεση της προσομοίωσης ο NS έχει τη δυνατότητα να δημιουργεί δύο βασικά αρχεία όπου αποθηκεύονται τα δεδομένα, το myscript.tr και το myscript.nam. Το πρώτο είναι ένα αρχείο απλού κειμένου (plain text) στο οποίο περιγράφονται τα διάφορα γεγονότα (λήψη πακέτου, είσοδος/έξοδος από κάποια ουρά) που αφορούν όλα τα πακέτα που κινούνται στο δίκτυο (σχήμα 16). Αυτό το αρχείο είναι ιδιαίτερα χρήσιμο για τη

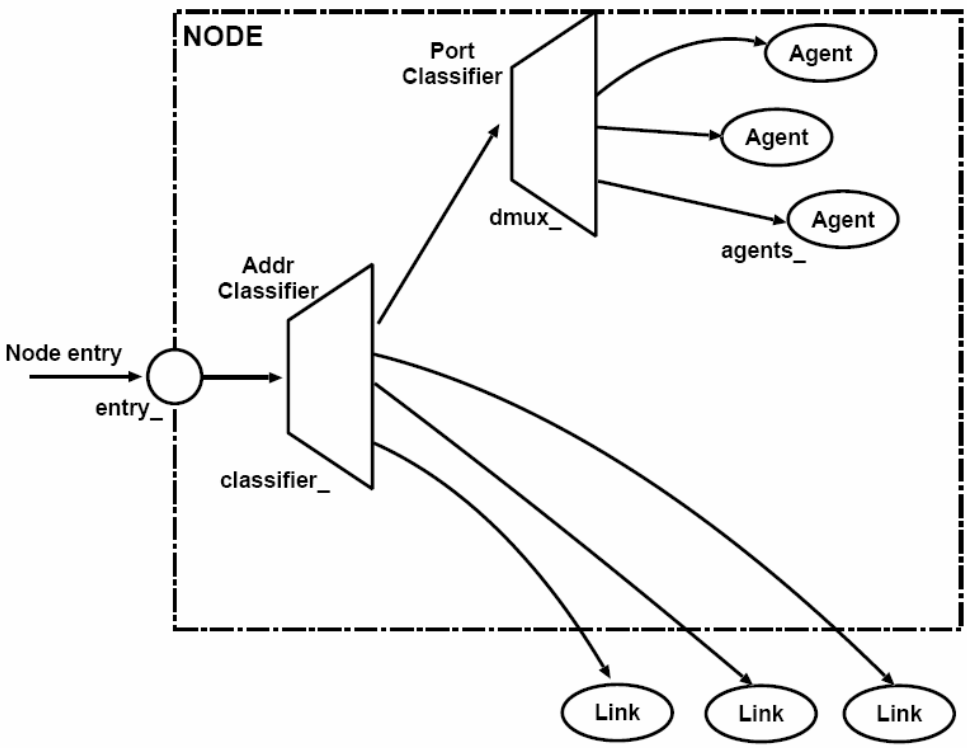
μετέπειτα μελέτη των αποτελεσμάτων καθώς περιέχει λεπτομερώς όλες τις πληροφορίες που θα μπορούσαμε να χρειαστούμε για κάθε είδους υπολογισμό παραμέτρων του δικτύου σχετικά με την κίνηση σε αυτό. Αυτό το αρχείο το επεξεργαζόμαστε με οποιοδήποτε άλλο πρόγραμμα που μπορεί να δεχθεί είσοδο από αρχείο (π.χ. με AWKS, OTCL, C++). Όπου είναι δυνατόν προτιμάται η επεξεργασία με AWKS αφού με αυτόν τον τρόπο η γραμμική ανάλυση του κειμένου (parsing) γίνεται πολύ πιο γρήγορα. Το δεύτερο είναι ένα αρχείο που αποτελεί είσοδο για τον NAM (Network AniMator) ένα πρόγραμμα που συνοδεύει τον NS και δίνει την δυνατότητα για εποπτική παρακολούθηση της προσομοίωσης. Πιο συγκεκριμένα μπορούμε να παρατηρήσουμε στον NAM τους κόμβους και τις συνδέσεις μεταξύ τους, την κίνηση των πακέτων, το αν κάποια ζεύξη είναι ενεργή ή όχι. Επίσης δίνεται η δυνατότητα να γίνει χρωματισμός των πακέτων ανάλογα με τις επιθυμίες του χρήστη (π.χ. τα πακέτα ανάλογα με το είδος τους να έχουν διαφορετικό χρώμα), να παριστάνονται οι κόμβοι με διάφορα σχήματα ανάλογα με το είδος τους, το οποίο καθορίζεται από τον χρήστη, ή να αλλάζουν εν δυνάμει χρώματα ανάλογα το γεγονός (event) που συμβαίνει. Γενικά ο NAM για μικρές τοπολογίες μας δίνει τη δυνατότητα εποπτικής παρακολούθησης της προσομοίωσης έτσι ώστε να διαπιστώνουμε γρήγορα και εύκολα τη σωστή λειτουργία του δικτύου. Βέβαια για μεγάλες τοπολογίες δεν είναι εύκολη η εποπτική παρακολούθηση της κίνησης, καθώς η παρακολούθηση πάνω από 50 κόμβων είναι πρακτικά αδύνατη, ενώ σε κάθε περίπτωση για ακριβή αποτελέσματα είναι απαραίτητη η επεξεργασία του myname.tr με κάποιες από τις μεθόδους που παρουσιάσθηκαν.




**Σχήμα 17** Παράδειγμα χρήσης του NS

## 6.2 Διαμόρφωση κόμβου

Η δομή ενός κόμβου φαίνεται στο επόμενο σχήμα




**Σχήμα 18** Δομή ενός Unicast Node

Όπως φαίνεται στο σχήμα ο κόμβος αποτελείται από δύο **Tcl** αντικείμενα: έναν **address classifier** (classifer_) και ένα **port classifier** (dmux_). Η λειτουργία αυτών των classifier είναι να καθοδηγήσουν τα εισερχόμενα πακέτα στους σωστούς πράκτορες (agents) ή στους συνδέσμους (links).

Όλοι οι κόμβοι περιέχουν τουλάχιστον τα παρακάτω συστατικά.

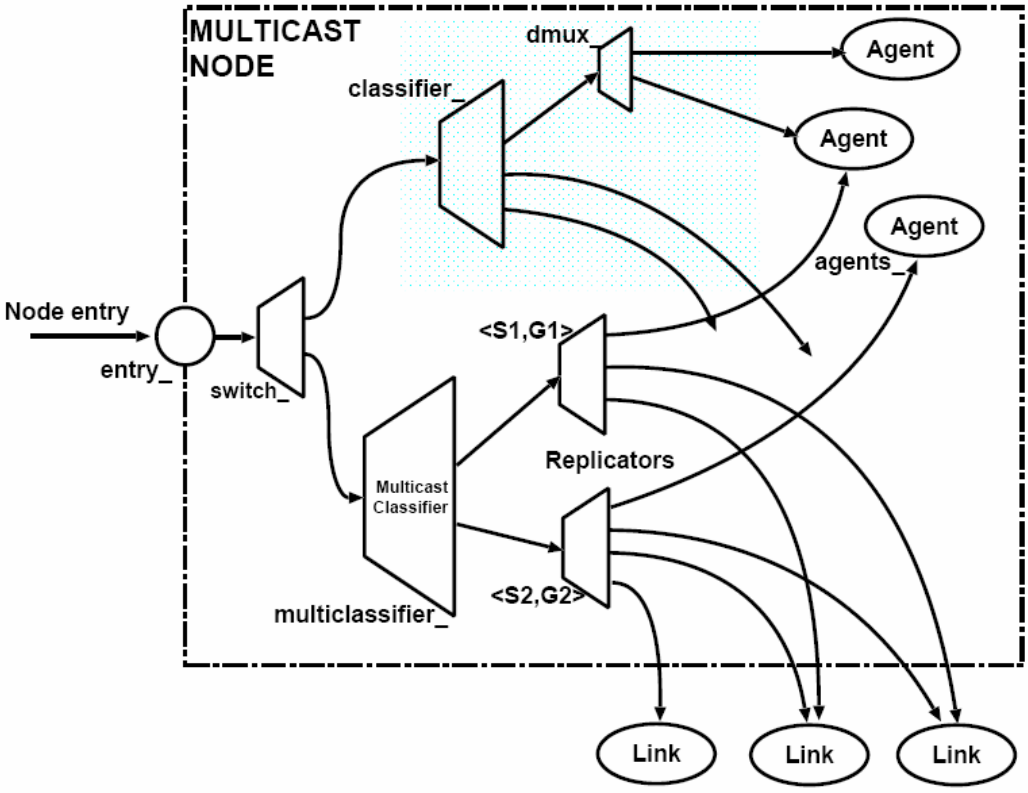
- Μια διεύθυνση ή id_
- Μια λίστα πρακτόρων (agent_)
- Μια λίστα γειτόνων (neighbor_)
- Έναν τύπο που να αναγνωρίζει το είδους του κόμβου (nodetype_)
- Και μια routing module.

**Σημείο εισόδου του κόμβου (entry point)**

Κάθε κόμβος έχει ένα σημείο εισόδου (entry point). Αυτό είναι το πρώτο στοιχείο που χειρίζεται τα πακέτα που φτάνουν σε αυτό τον κόμβο.

Για unicast node το entry point είναι το address classifier (σχήμα 18) το οποίο βλέπει τα πρώτα ψηφία της διεύθυνσης προορισμού.

Για multicast nodes το entry point είναι το switch_ το οποίο βλέπει το πρώτο ψηφίο για να αποφασίσει εάν αυτό πρέπει να διαβιβάσει τα πακέτα στον unicast classifier η στον multicast classifier. Όταν μια προσομοίωση χρησιμοποιεί την multicast δρομολόγηση, το πρώτο ψηφίο δείχνει εάν η διεύθυνση είναι μια multicast διεύθυνση ή μια διεύθυνση unicast. Εάν το κομμάτι είναι 0, η διεύθυνση αντιπροσωπεύει μια διεύθυνση unicast, αλλιώς η διεύθυνση αντιπροσωπεύει μια multicast διεύθυνση.




**Σχήμα 19** Δομή ενός multicast node

## 6.2.1 Classifier

Η λειτουργία του κόμβου όταν αυτό λαμβάνει ένα πακέτο είναι να εξετάσει τα πεδία του πακέτου όπως είναι η διεύθυνση προορισμού και η διεύθυνση πηγής. Τότε πρέπει να μεταδώσει τις τιμές αυτές στον επόμενο δέκτη του πακέτου.

Στον NS αυτό επιτυγχάνεται με ένα simple classifier object. Ένας κόμβος στον NS χρησιμοποιεί πολλούς διαφορετικούς τύπους classifiers για διαφορετικούς σκοπούς.

Ένας classifier παρέχει έναν τρόπο να ταιριαχτεί ένα πακέτο μέσα από μερικά λογικά κριτήρια και να ανακτηθεί μια αναφορά σε ένα άλλο αντικείμενο προσομοίωσης βασισμένο στα αποτελέσματα αντιστοιχιών. Κάθε classifier περιέχει έναν πίνακα των αντικειμένων προσομοίωσης που συντάσσονται από το **slot number**. Η εργασία ενός classifier είναι να καθοριστεί το slot number που συνδέεται με ένα λαμβανόμενο πακέτο και να διαβιβαστεί εκείνο το πακέτο στο αντικείμενο που παραπέμπεται από εκείνο το ιδιαίτερο slot.

### 6.2.2 Address Classifier

Αυτός ο τύπος χρησιμοποιείται για να υποστηρίξει την unicast διαβίβαση πακέτων. Χρησιμοποιεί τις λογικές επεξεργασίες **shift** και **mask** στη διεύθυνση προορισμού για να παράγει ένα slot number.

## 6.3 Mobile Networking in NS

Στο προηγούμενο τμήμα αναλύσαμε και περιγράψαμε πως δημιουργείται ένα δίκτυο. Σε αυτό το κεφάλαιο συζητάμε για τους κινητούς κόμβους (mobile node), τους μηχανισμούς δρομολόγησης και τα διάφορα συστατικά δικτύου που χρησιμοποιούνται για την σύνθεση ενός δικτύου για κινητούς κόμβους. Έτσι θα μπορέσουμε να δούμε τι είναι απαραίτητο ώστε να στήσουμε ένα Ad Hoc δίκτυο.

Συνοπτικά τα συστατικά δικτύου που χρησιμοποιούνται είναι τα Channel, Network-interface, Radio propagation model, MAC protocols, Interface Queue, Link layer και Address Resolution Protocol model (ARP). Παρακάτω περιγράφεται το ασύρματο πρότυπο γνωστό ως CMU model που επιτρέπει την προσομοίωση ασύρματων δικτύων LANs ή multihop ad-hoc δικτύων.

### 6.3.1 Δημιουργώντας μια ασύρματη τοπολογία

Το MobileNode είναι το βασικό αντικείμενο κόμβων NS με πρόσθετες λειτουργίες όπως είναι η μετακίνηση, η δυνατότητα να διαβιβάσει και να λάβει, πακέτα πληροφοριών, σε ένα κανάλι που του επιτρέπει να χρησιμοποιηθεί για να δημιουργήσει τα κινητά και ασύρματα περιβάλλοντα προσομοίωσης.

Τα τέσσερα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται κατά κόρον είναι :

Destination Sequence Distance Vector (DSDV)

Dynamic Source Routing (DSR)
Temporally ordered Routing Algorithm (TORA)
Adhoc On-demand Distance Vector (AODV)

Η διαμόρφωση ενός κινητού κόμβου σε κώδικα Tcl έχει ως εξής:

```
$ns_ node-config -adhocRouting $opt(adhocRouting)
-llType $opt(ll)
-macType $opt(mac)
-ifqType $opt(ifq)
-ifqLen $opt(ifqlen)
-antType $opt(ant)
-propInstance [new $opt(prop)]
-phyType $opt(netif)
-channel [new $opt(chan)]
-topoInstance $topo
-wiredRouting OFF
-agentTrace ON
-routerTrace OFF
-macTrace OFF
```

Οι παραπάνω εντολές διαμορφώνουν έναν κινητό κόμβο ορίζοντας τα στοιχεία adhoc-routing protocol, network stack, channel, topography, propagation model, την ενσύρματη δρομολόγηση ενεργή η ανενεργή (σε περίπτωση που έχουμε τοπολογία με wired και wireless nodes και την καταγραφή (tracing) ενεργή η ανενεργή σε διαφορετικά επίπεδα (router, mac, agent).

Το ανωτέρω API διαμορφώνει ένα mobilenode με όλες τις δεδομένες τιμές της ειδικής-δρομολόγησης του πρωτοκόλλου, σωρός δικτύων, κανάλι, τοπογραφία, πρότυπο διάδοσης και την επισήμανση μακριά σε διαφορετικά επίπεδα (δρομολογητής, MAC, πράκτορας). Στην περίπτωση που η hierarchical addressing χρησιμοποιείται η διεύθυνση του κόμβου πρέπει να περαστεί επίσης.

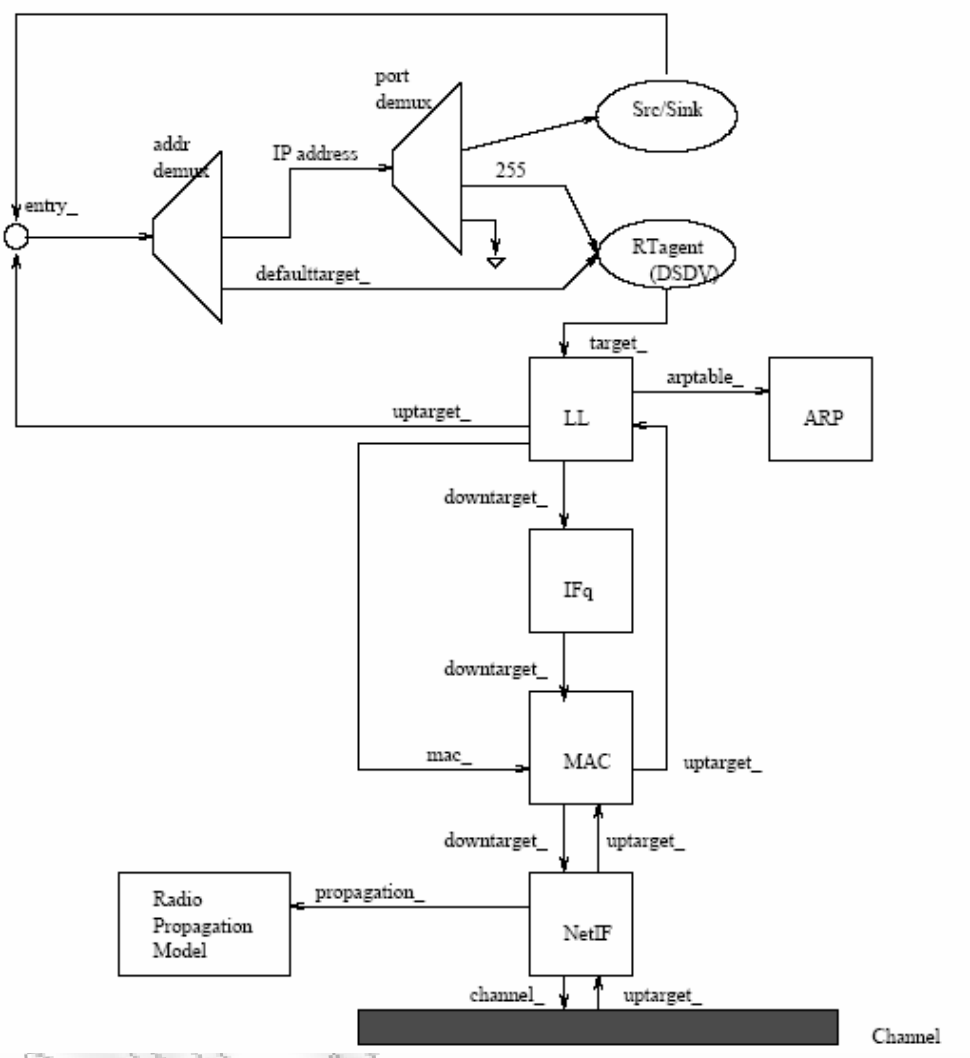
Δημιουργούμε τους κινητούς κόμβους ως εξής

```
for { set j 0 } { $j < $opt(nn)} {incr j} {
set node_($j) [ $ns_ node ]
$node_($i) random-motion 0 ;# disable random motion}
```

Η παραπάνω διαδικασία δημιουργεί ένα mobilenode (split)object, δημιουργεί ένα adhoc-routing agent και δημιουργεί το σωρό δικτύου (network stack) που αποτελείται

από το στρώμα σύνδεσης (link layer), interface queue, mac layer και μια network interface με μια κεραία.

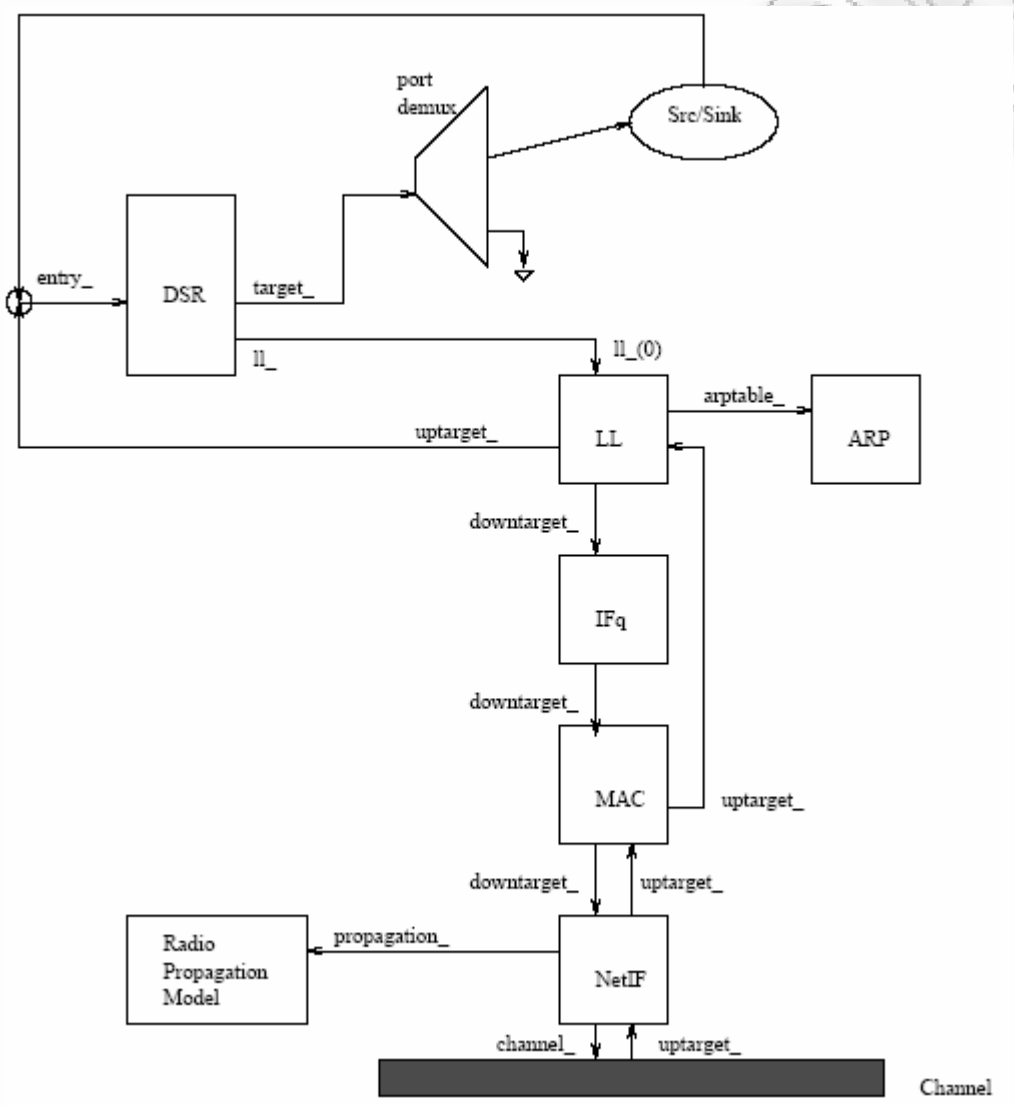
Επίσης χρησιμοποιεί το καθορισμένο πρότυπο διάδοσης, συνδέει αυτά τα συστατικά και συνδέει το σωρό με το κανάλι. Η σχηματική αναπαράσταση του mobilenode φαίνεται στο σχήμα 20.




**Σχήμα 20** Σχηματική δομή ενός κινητού κόμβου

Η δομή του mobilenode που χρησιμοποιείται για τη δρομολόγηση DSR είναι ελαφρώς διαφορετική από το mobilenode που περιγράφεται ανωτέρω. Η κατηγορία SRNode δεν χρησιμοποιεί address demux ή classifiers και όλα τα πακέτα που παραλαμβάνονται από τον κόμβο δίνονται στον DSR routing agent. Ο DSR routing agent είτε λαμβάνει πακέτα για να το μεταδώσει στην πόρτα του dmux είτε διαβιβάζει τα πακέτα σύμφωνα με τις address που αναγράφονται στην επικεφαλίδα του πακέτου

είτε στέλνει τα αιτήματα διαδρομών και τις απαντήσεις διαδρομών για τα νέα πακέτα. Το σχηματικό πρότυπο για ένα SRNode παρουσιάζεται στο σχήμα 21.




**Σχήμα 21** Σχηματική δομή ενός SRnode

## 6.3.2 Μετακινήσεις κόμβου

Το mobilenode σχεδιάζεται με τέτοιο τρόπο ώστε να μπορεί να κινηθεί σε μια τρισδιάστατη τοπολογία. Εντούτοις η τρίτη διάσταση (Z) δεν χρησιμοποιείται. Αυτό γιατί υποτίθεται πως ο mobilenode κινείται πάντα σε μια επίπεδη έκταση με το Z πάντα ίσο με 0. Έτσι ο mobilenode έχει τις συντεταγμένες X, Y, Z(=0) που

μεταβάλλονται συνεχώς καθώς ο κόμβος κινείται. Υπάρχουν δύο μηχανισμοί για να προκαλέσουν τη μετακίνηση στα mobilenodes. Στην πρώτη μέθοδο, η αρχική θέση του κόμβου και οι μελλοντικοί προορισμοί της μπορούν να οριστούν σε ένα ξεχωριστό αρχείο που περιέχει το σενάριο μετακίνησης.

Η αρχική θέση του κόμβου καθώς και οι μετακινήσεις του μπορούν να ορισθούν μέσα στον ίδιο τον κώδικα της Tcl με τη χρησιμοποίηση των ακόλουθων εντολών:

```
$node set X_ <x1>
$node set Y_ <y1>
$node set Z_ <z1>
$ns at $time $node setdest <x2> <y2> <speed>
```

Με την εκτέλεση των παραπάνω εντολών ο κόμβος αρχίζει να κινείται στο χρόνο που ορίζεται από το πεδίο **$time** από την αρχική του θέση (x1,y1) προς έναν προορισμό (x2,y2) με την καθορισμένη ταχύτητα.

Στην δεύτερη μέθοδος η μετακίνηση του κόμβου είναι τυχαία και ενεργοποιείται με την εντολή:

```
$mobilenode start
```

Με την εντολή αυτή ο mobilenode κινείται σε μια τυχαία θέση και έχει επαναλαμβανόμενες αναπροσαρμογές για να αλλάξει την κατεύθυνση και την ταχύτητα του κόμβου. Οι τιμές προορισμού και ταχύτητας παράγονται τυχαία.

Ανεξάρτητα από ποια μέθοδο θα χρησιμοποιήσουμε για την μετακίνηση των κόμβων, η τοπογραφία για τα mobilenodes πρέπει να καθοριστεί. Πρέπει να καθοριστεί πριν την δημιουργία των mobilenode. Η επίπεδη τοπολογία δημιουργείται με τη διευκρίνιση του μήκους και του πλάτους της τοπογραφίας χρησιμοποιώντας την ακόλουθη εντολή:

```
set topo [new Topography]
$topo load_flatgrid $opt(x) $opt(y)
```

Όπου opt(x) και opt(y) είναι τα όρια που χρησιμοποιούνται στην προσομοίωση. Η μετακίνηση των mobilenodes μπορεί να καταγραφεί με τη χρησιμοποίηση μιας διαδικασίας όπως η εξής:

```
proc log-movement {} {

global logtimer ns_ ns
```

```
set ns $ns_
source ../mobility/timer.tcl
Class LogTimer -superclass Timer
LogTimer instproc timeout {} {
global opt node_;
for {set i 0} {$i < $opt(nn)} {incr i} {
$node_($i) log-movement
}
$self sched 0.1
}
set logtimer [new LogTimer]
$logtimer sched 0.1
}
```

Σε αυτήν την περίπτωση οι θέσεις θα καταγράφονται κάθε 0,1 δευτερόλεπτο.

### 6.3.3 Συστατικά δικτύων σε ένα mobilenode

Ο σωρός δικτύου για ένα mobilenode αποτελείται από το link layer (LL), μια ARP μονάδα που συνδέεται στο LL, μια interface priority queue (IFq), ένα mac layer (MAC), ένα network interface (netIF), όλα συνδεόμενα με το κανάλι. Αυτά τα συστατικά δικτύου δημιουργούνται στην OTcl. Η σχετική μέθοδο δείχνεται παρακάτω:

**Link Layer:** Το αντικείμενο Link Layer είναι υπεύθυνο για τη προσομοίωση των πρωτοκόλλων συνδέσεων στοιχείων. Πολλά πρωτόκολλα μπορούν να εφαρμοστούν μέσα σε αυτό το στρώμα όπως ο τεμαχισμός και η επανασυναρμολόγηση πακέτων, και το αξιόπιστο πρωτόκολλο συνδέσεων. Μια άλλη σημαντική λειτουργία του στρώματος συνδέσεων είναι ότι θέτει τη διεύθυνση προορισμού της MAC στην MAC επιγραφή του πακέτου. Στην τρέχουσα εφαρμογή αυτός ο στόχος περιλαμβάνει δύο χωριστά ζητήματα: εύρεση της διεύθυνσης IP του επόμενου κόμβου (δρομολόγηση) και επίλυση αυτής της διεύθυνσης IP στη σωστή διεύθυνση της MAC (ARP). Για πιο μεγάλη ευκολία η προεπιλεγμένη χαρτογράφηση μεταξύ των διευθύνσεων της MAC και IP είναι one-to-one το οποίο σημαίνει ότι οι διευθύνσεις IP είναι σχετικά ξαναχρησιμοποιούμενες στο στρώμα της MAC.

**ARP:** Το Address Resolution Protocol λαμβάνει τις ερωτήσεις από το στρώμα συνδέσεων. Εάν το ARP έχει τη διεύθυνση προορισμού, την γράφει στην επιγραφή MAC του πακέτου. Διαφορετικά μεταδίδει μια ARP ερώτηση, και «κρύβει» το

πακέτο προσωρινά. Για κάθε άγνωστη διεύθυνση προορισμού, υπάρχει ένας buffer για το πακέτο. Στην περίπτωση που πρόσθετα πακέτα στέλνονται στο ARP, το προηγούμενο αποθηκευμένο πακέτο πέφτει. Μόλις είναι γνωστή η διεύθυνση του επόμενου hop ενός πακέτου, το πακέτο παρεμβάλλεται στη σειρά αναμονής διεπαφών (interface queue).

**Interface Queue:** Η κατηγορία PriQueue εφαρμόζεται ως σειρά αναμονής προτεραιότητας που δίνει προτεραιότητα στα πακέτα πρωτοκόλλων δρομολόγησης παρεμβάλλοντας τους στην αφετηρία της σειράς αναμονής. Με την εφαρμογή ενός φίλτρου σε όλα τα πακέτα στη σειρά αναμονής αφαιρεί εκείνα με μια συγκεκριμένη διεύθυνση προορισμού.

**Mac Layer:** Το IEEE 802.11 distributed coordination function (DCF) Mac protocol έχει εφαρμοστεί από την CMU. Χρησιμοποιεί ένα σχέδιο RTS/CTS/DATA/ACK για όλα τα unicast πακέτα και στέλνει απλά τα ΣΤΟΙΧΕΙΑ για όλα τα μεταδιδόμενα πακέτα. Στο NS, δύο πρωτόκολλα στρώματος της MAC εφαρμόζονται για τα κινητά δίκτυα, τα οποία είναι τα 802.11 και TDMA.

**Tap Agents:** Οι πράκτορες καθορίζονται στο mac.h που βρίσκεται μέσα στους υποκαταλόγους του NS και μπορούν να καταχωρηθούν με το αντικείμενο της MAC χρησιμοποιώντας τη μέθοδο installTap (). Εάν το ιδιαίτερο πρωτόκολλο της MAC το επιτρέψει, στο Tap θα δοθούν όλα τα πακέτα που παραλαμβάνονται από το στρώμα της MAC, προτού να γίνει το φιλτράρισμα διευθύνσεων.

**Network Interfaces:** Το Network Interphase layer χρησιμεύει ως μια διεπαφή υλικού που χρησιμοποιείται από το mobilenode για να έχει πρόσβαση στο κανάλι. Η ασύρματη κοινή διεπαφή μέσων εφαρμόζεται ως κατηγορία Phy/WirelessPhy. Αυτή η διεπαφή υποκείμενη στις συγκρούσεις και στο πρότυπο διάδοσης λαμβάνει τα πακέτα που μεταδίδονται από άλλες διεπαφές κόμβων στο κανάλι. Η διεπαφή σφραγίζει κάθε διαβιβασθέν πακέτο με τα δεδομένα σχετικά με τη διεπαφή που το διαβίβασε όπως η δύναμη μετάδοσης, το μήκος κύματος κ.λπ. Αυτά τα δεδομένα στην επιγραφή του πακέτου χρησιμοποιούνται από το πρότυπο διάδοσης στη λήψη της διεπαφής δικτύων για να καθορίσουν εάν το πακέτο έχει την ελάχιστη δύναμη να ληφθεί ή και να ανιχνευθεί από το λαμβάνοντα κόμβο. Το πρότυπο προσεγγίζει τη ράδιο-διεπαφή DSSS.

### 6.3.4 Διαφορετικοί τύποι πρακτόρων δρομολόγησης

Τα τέσσερα διαφορετικά ειδικά πρωτόκολλα δρομολόγησης που εφαρμόζονται αυτήν την περίοδο για την κινητή δικτύωση στο NS είναι τα dsdv, dsr, aodv και tora. Σε αυτό το τμήμα θα συζητήσουμε εν συντομία καθένα από αυτούς.

**DSDV**

Σε αυτό το πρωτόκολλο δρομολόγησης τα μηνύματα δρομολόγησης ανταλλάσσονται μεταξύ των γειτονικών mobilenodes. Αναπροσαρμογές δρομολόγησης μπορούν να προκληθούν ή να επαναληφθούν. Αναπροσαρμογές προκαλούνται σε περίπτωση που πληροφορίες δρομολόγησης από ένα από τους γείτονες αναγκάζει μια αλλαγή στον πίνακα δρομολόγησης. Ένα πακέτο για το οποίο η διαδρομή στον προορισμό της δεν είναι γνωστή αποθηκεύεται ενώ ερωτήσεις δρομολόγησης στέλνονται. Τα πακέτα αποθηκεύονται έως ότου παραληφθούν απαντήσεις για την διαδρομή από τον προορισμό. Υπάρχει ένα μέγιστο μέγεθος αποθήκευσης για τα πακέτα που περιμένουν πληροφορίες δρομολόγησης. Όταν ξεπεραστεί αυτό το μέγεθος τα πακέτα αρχίζουν και απορρίπτονται. Όλα τα πακέτα που προορίζονται για το mobilenode καθοδηγούνται άμεσα από τη διεύθυνση dmux στο port dmux. Το port dmux δίνει τα πακέτα στους αντίστοιχους πράκτορες προορισμού. Το dmux διαθέτει 255 διαθέσιμα port για να συνδέσει τον πράκτορα δρομολόγησης στα mobilenodes. Οι mobilenodes χρησιμοποιούν ένα προεπιλεγμένο στόχο (default-target) στο Classifier τους (ή τη διεύθυνση demux). Στην περίπτωση που ένας στόχος δεν βρίσκεται για τον προορισμό στον ταξινομητή (που συμβαίνει όταν ο προορισμός του πακέτου δεν είναι το ίδιο το mobilenode) τα πακέτα δίνονται στο default-target που είναι ο πράκτορας δρομολόγησης. Ο πράκτορας δρομολόγησης ορίζει το επόμενο hop για το πακέτο και το στέλνει κάτω στο link layer. Το πρωτόκολλο δρομολόγησης εφαρμόζεται κυρίως στη C ++.

**DSR**

Αυτό το τμήμα περιγράφει τη λειτουργία του δυναμικού πρωτοκόλλου δρομολόγησης πηγής. Το SRNode είναι διαφορετικό από το MobileNode. Το σημείο εισόδου (entry_point) του SRNode δείχνει τον πράκτορα δρομολόγησης DSR, αναγκάζοντας κατά συνέπεια όλα τα πακέτα που παραλαμβάνονται από τον κόμβο να παραδοθούν στον πράκτορα δρομολόγησης. Αυτό το πρότυπο απαιτείται για τη μελλοντική εφαρμογή των piggy-backed πληροφοριών δρομολόγησης για τα πακέτα στοιχείων που ειδάλλως δεν θα διέτρεχαν μέσω του πράκτορα δρομολόγησης. Ο πράκτορας DSR ελέγχει κάθε πακέτο στοιχείων για τις πληροφορίες πηγή-διαδρομών. Διαβιβάζει το πακέτο σύμφωνα με τις πληροφορίες δρομολόγησης. Στην

περίπτωση που δεν βρει πληροφορίες δρομολόγησης στο πακέτο, αυτό παρέχει τη διαδρομή πηγής, εάν η διαδρομή είναι γνωστή, ή «κρύβει» το πακέτο και στέλνει ερωτήσεις διαδρομών εάν η διαδρομή στον προορισμό είναι άγνωστη. Οι ερωτήσεις δρομολόγησης, που προκαλούνται πάντα από ένα πακέτο στοιχείων χωρίς τη διαδρομή στον προορισμό του, είναι αρχικά μεταδόσεις σε όλους τους γείτονες. Οι απαντήσεις σχετικά με την διαδρομή στέλνονται πίσω είτε από τους ενδιάμεσους κόμβους είτε από τον κόμβο προορισμού στην πηγή, εάν μπορεί να βρει τις πληροφορίες δρομολόγησης για τον προορισμό στην ερώτηση. Παραδίδει όλα τα πακέτα που προορίζονται για αυτό στο port dmux. Σε SRNode το port 255 δείχνει σε έναν Null Agent δεδομένου ότι το πακέτο έχει περάσει από τον πράκτορα δρομολόγησης.

**TORA**

Το Tora είναι ένα διανεμημένο πρωτόκολλο δρομολόγησης βασισμένο στον αλγόριθμο "αντιστροφή συνδέσεων". Σε κάθε κόμβο ένα ξεχωριστό αντίγραφο του TORA τρέχει για κάθε προορισμό. Όταν ένας κόμβος χρειάζεται μια διαδρομή σε έναν συγκεκριμένο προορισμό μεταδίδει ένα μήνυμα ερώτησης που περιέχει τη διεύθυνση του προορισμού που απαιτεί μια διαδρομή. Αυτό το πακέτο ταξιδεύει μέσω του δικτύου μέχρι να φτάσει στον προορισμό ή σε έναν ενδιάμεσο κόμβο που έχει μια διαδρομή για τον κόμβο προορισμού. Αυτός ο κόμβος μεταδίδει έπειτα ένα πακέτο αναπροσαρμογών που απαριθμεί το ύψος wrt του προορισμού. Δεδομένου ότι αυτός ο κόμβος διαδίδει μέσω του δικτύου κάθε αναπροσαρμογή κόμβου ενημερώνει το ύψος του wrt σε μια αξία μεγαλύτερη από το ύψος του κόμβου από το οποίο λαμβάνει την αναπροσαρμογή. Αυτό προκύπτει σε μία σειρά συνδέσεων από τον κόμβο που δημιουργήθηκε η ερώτηση στον κόμβο προορισμού. Εάν ένας κόμβος ανακαλύπτει έναν ιδιαίτερο προορισμό για να είναι απρόσιτο θέτει μια τοπική μέγιστη αξία του ύψους για εκείνο τον προορισμό. Στην περίπτωση που ο κόμβος δεν μπορεί να βρει οποιοδήποτε γείτονα που να έχει το πεπερασμένο ύψος wrt αυτός ο προορισμός προσπαθεί να βρει μια νέα διαδρομή. Σε περίπτωση χωρίσματος δικτύων, ο κόμβος μεταδίδει ραδιοφωνικά ένα σαφές μήνυμα που να επαναριθμήσει όλα τα μέρη δρομολόγησης και αφαιρεί τις άκυρες διαδρομές από το δίκτυο. Το TORA λειτουργεί πάνω από IMEP (Internet MANET Encapsulation Protocol) που παρέχει την αξιόπιστη παράδοση των μηνυμάτων διαδρομής και ενημερώνει το πρωτόκολλο δρομολόγησης για οποιεσδήποτε αλλαγές των συνδέσεων με τους γείτονές του. Το IMEP προσπαθεί να αθροίσει τα μηνύματα IMEP και TORA σε ένα ενιαίο πακέτο (αποκαλούμενο block) προκειμένου να μειωθεί το overhead. Το IMEP για την επίβλεψη των συνδέσεων και την διατήρηση ενός καταλόγου κοντινών κόμβων στέλνει περιοδικά μηνύματα αναγνωριστικών σημάτων που απαντιούνται από κάθε κόμβο που τα ακούει με ένα HELLO μήνυμα απάντησης.

**AODV**

AODV είναι ένας συνδυασμός των πρωτοκόλλων DSR και DSDV. Έχει τις βασικές λειτουργίες ανακάλυψης διαδρομών και διατήρησης διαδρομών του DSR και χρησιμοποιεί τη δρομολόγηση hop-by-hop, τους αριθμούς ακολουθίας και τα αναγνωριστικά σήματα DSDV. Ο κόμβος που θέλει να ξέρει μια διαδρομή σε έναν συγκεκριμένο προορισμό παράγει ένα αίτημα διαδρομών. Το αίτημα διαδρομών διαβιβάζεται από τους ενδιάμεσους κόμβους που δημιουργούν επίσης μια αντίστροφη διαδρομή για αυτόν από τον προορισμό. Όταν το αίτημα φθάνει σε έναν κόμβο με τη διαδρομή στον προορισμό παράγει μια απάντηση διαδρομών που περιέχει τον αριθμό hop που απαιτείται για να φθάσει στον προορισμό. Όλοι οι κόμβοι που συμμετέχουν στην αποστολή αυτής της απάντησης στον κόμβο πηγής δημιουργούν μια διαδρομή στον προορισμό. Αυτό το μέρος που δημιουργείται από κάθε κόμβο από την πηγή στον προορισμό είναι hop-by-hop μέρος και όχι η ολόκληρη διαδρομή όπως γίνεται στη δρομολόγηση πηγής.

# 7. Σχεδιασμός και Προσομοίωση Επιθέσεων

## 7.1 Εισαγωγή

Σε αυτό το σημείο της διπλωματικής θα περιγράψουμε τα προγράμματα των επιθέσεων που δημιουργήσαμε στο Ad Hoc δίκτυο, δίνοντας ιδιαίτερη έμφαση στον σχεδιασμό τους και στην ανάλυση των αλγορίθμων που πραγματοποιούν τους ελέγχους, καθώς και στα μηνύματα που ανταλλάσσονται ανάμεσα στους κόμβους. Οι επιθέσεις που δημιουργήθηκαν είναι μία Blackhole, ένα Flooding και ένα Worm. Συγκεκριμένα, τα υπάρχοντα πρωτόκολλα δρομολόγησης, όπως DSR , AODV , και μερικά ασφαλή πρωτόκολλα δρομολόγησης, όπως SRP, Ariadne, ARAN, SAODV, δεν μπορούν να είναι άτρωτα από τις παραπάνω επιθέσεις. Στην διπλωματική αυτή θα αναπτύξουμε την προσομοίωση γύρω από το πρωτόκολλο AODV διότι και τα υπόλοιπα είναι τρωτά με τον ίδιο τρόπο.

Στο AODV, η ανακάλυψη πορειών είναι εξ ολοκλήρου on-demand. Όταν ένας κόμβος πηγής πρέπει να στείλει τα πακέτα σε έναν προορισμό στον οποίο δεν έχει καμία διαθέσιμη διαδρομή, μεταδίδει broadcast ένα (αίτημα διαδρομών) πακέτο RREQ στους γείτονές του. Κάθε κόμβος διατηρεί έναν αυξανόμενο αριθμό ακολουθίας για να εξασφαλίσει ελεύθερη δρομολόγηση βρόχων και να εκτοπίσει την πολυδιατηρημένη κρύπτη διαδρομών. Ο κόμβος που είναι αποστολέας περιλαμβάνει το γνωστό αριθμό ακολουθίας του προορισμού στο πακέτο RREQ. Ο ενδιάμεσος κόμβος που λαμβάνει ένα πακέτο RREQ ελέγχει τις καταχωρήσεις των διαδρομών του. Εάν κατέχει μια διαδρομή προς τον προορισμό με μεγαλύτερο αριθμό ακολουθίας από αυτόν στο πακέτο RREQ, στέλνει ένα πακέτο RREP πίσω στο γείτονά του από το οποίο έλαβε το πακέτο RREQ. Διαφορετικά, οργανώνει την αντίστροφη διαδρομή και έπειτα κάνει rebroadcast το πακέτο RREQ. Τα διπλά πακέτα RREQ που παραλαμβάνονται από έναν κόμβο απορρίπτονται. Με τον τρόπο αυτό, το πακέτο RREQ αποστέλλεται με έναν ελεγχόμενο τρόπο στο δίκτυο, και φθάνει τελικά στον προορισμό ο οποίος θα παραγάγει το πακέτο RREP. Δεδομένου ότι το πακέτο RREP διαδίδεται κατά μήκος της αντίστροφης διαδρομής στην πηγή, οι ενδιάμεσοι κόμβοι ενημερώνουν τη δρομολόγησή τους χρησιμοποιώντας τον διανεμημένο αλγόριθμο Bellman-Ford με πρόσθετο περιορισμό στον αριθμό ακολουθίας, και δημιουργούν την διαδρομή.

Το AODV περιλαμβάνει επίσης το μηχανισμό συντήρησης πορειών για να χειριστεί τη δυναμική τοπολογία των δικτύων. Οι συνδέσεις που αποτυγχάνουν μπορούν να ανιχνευθούν είτε από περιοδικά αναγνωριστικά σήματα είτε από acknowledgments του στρώματος συνδέσεων, όπως εκείνα που παρέχονται από το πρωτόκολλο της MAC 802.11. Μόλις μια σύνδεση διακοπεί, ένα εκούσιο πακέτο RRER με έναν φρέσκο αριθμό ακολουθίας και ένα άπειρο hop count διαδίδεται σε

όλους τους ενεργούς κόμβους της πηγής που χρησιμοποιούν την περίοδο αυτήν την σύνδεση. Όταν ο κόμβος της πηγής λαμβάνει την ανακοίνωση μιας σπασμένης σύνδεσης, μπορεί να επανεκκινήσει τη διαδικασία ανακαλύψεων της διαδρομής εάν αυτό χρειάζεται.

## 7.2 Επίθεση Blackhole

### 7.2.1 Σχεδιασμός Επίθεσης Blackhole

Στην διπλωματική μας, έχουμε χρησιμοποιήσει δύο ειδών κόμβους κατάτον σχεδιασμό της Blackhole επίθεσης. Αυτούς που προσομοιώνουν τη συμπεριφορά των μαύρων τρυπών στο ασύρματο Ad Hoc δίκτυο και αυτούς που χρησιμοποιούν το πρωτόκολλο AODV. Δεδομένου ότι οι κόμβοι συμπεριφέρονται ως μαύρη τρύπα πρέπει να χρησιμοποιήσουν ένα νέο πρωτόκολλο δρομολόγησης που μπορεί να χρησιμοποιεί τα μηνύματα του AODV. Όλα τα πρωτόκολλα δρομολόγησης στο NS εγκαθίστανται στον κατάλογο NS-2.34.

Αρχικά δημιουργούμε ένα ακριβές αντίγραφο του πρωτοκόλλου AODV το οποίο το ονομάζουμε ως blackholeaodv. Το βασικό σημείο στην διπλωματική μας είναι ότι το πρωτόκολλο AODV και το πρωτόκολλο blackholeaodv θα ανταλλάσουν μεταξύ τους τα ίδια πακέτα AODV. Επομένως, δεν αντιγράφουμε το αρχείο «aodv_packet.h» στον φάκελο του blackholeaodv. Αυτό γίνεται διότι θέλουμε κατά την σχεδίαση να εκμεταλλευτούμε τα RREQ πακέτα που θα αναλύσουμε παρακάτω.

Έχουμε αλλάξει όλες τις κατηγορίες, τις λειτουργίες, τις δομές, τις μεταβλητές και τα ονόματα σταθερών σε όλα τα αρχεία στον κατάλογο του blackholeaodv εκτός από τις δομές που ανήκουν στον κώδικα AODV packet.h. Με τον τρόπο αυτό έχουμε σχεδιάσει aodv και blackholeoadv πρωτόκολλα να ανταλλάσουν aodv πακέτα.

Μετά από τις ανωτέρω αλλαγές, αλλάζουμε και τα δύο κοινά αρχεία που χρησιμοποιούνται στον NS-2 για να ενσωματώσουν το νέο πρωτόκολλο blackholeaodv στον προσομοιωτή. Το πρώτο αρχείο που τροποποιούμε είναι το ns-lib.tcl όπου οι agents του πρωτοκόλλου κωδικοποιούν την διαδικασία. Όταν οι κόμβοι χρησιμοποιούν το blackholeaodv πρωτόκολλο, αυτός ο agent σχεδιάζεται στην αρχή της προσομοίωσης και ορίζεται στους κόμβους που θα χρησιμοποιήσουν το blackholeaodv πρωτόκολλο. Το δεύτερο αρχείο που τροποποιούμε είναι το makefile. Το αρχείο αυτό τροποποιείται για να δημιουργηθούν τα objects files κατά το compile του αρχείου (σχήμα 22).

```
blackholeaodv/blackholeaodv_logs.o blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o blackholeaodv/blackholeaodv_rqueue.o \
```

**Σχήμα 22** Τροποποίηση αρχείου Makefile

Μέχρι τώρα, έχουμε εφαρμόσει ένα νέο πρωτόκολλο δρομολόγησης που χαρακτηρίζεται ως blackholeaodv. Οι συμπεριφορές των μαύρων τρυπών δεν έχουν εφαρμοστεί ακόμα σε αυτό το νέο πρωτόκολλο δρομολόγησης. Για να προσθέσουμε τη συμπεριφορά μαύρων τρυπών στο νέο πρωτόκολλο AODV κάναμε τις ίδιες αλλαγές στο C++ αρχείο blackholeaodv/blackholeaodv.cc. Όταν ένα πακέτο παραλαμβάνεται από τη λειτουργία «recv» του «aodv/aodv.cc», επεξεργάζεται τα πακέτα με βάση τον τύπο τους. Εάν ο τύπος πακέτων είναι οποιοδήποτε από τα πακέτα των διαδρομών του AODV, στέλνει το πακέτο στη λειτουργία «recvAODV». Εάν το λαμβανόμενο πακέτο είναι ένα πακέτο δεδομένων, κανονικά το πρωτόκολλο AODV το στέλνει στη διεύθυνση προορισμού του, αλλά η συμπεριφορά της μαύρη τρύπα έχει ως αποτέλεσμα να δέχεται και να απορρίπτει όλα τα πακέτα δεδομένων είτε αυτά έχουν σαν προορισμό τους τον blackhole κόμβο είτε όχι.

```
//If destination address is itsself
if ( (u_int32_t)ih->saddr() == index)
   forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY);
else
// For blackhole attack in the wireless adhoc network,
    drop(p, DROP_RTR_ROUTE_LOOP);
```

**Σχήμα 23** Αποδοχή ή απόρριψη πακέτου

Εάν το πακέτο είναι ένα management AODV πακέτο, η «recv» λειτουργία το στέλνει στη λειτουργία «recvblackholeAODV». Η λειτουργία αυτή ελέγχει τον τύπο του AODV πακέτου και τα προωθεί στην κατάλληλη λειτουργία. Για παράδειγμα τα πακέτα RREQ στέλνονται στη «recvRequest» λειτουργία και τα πακέτα RREP στην «recvReply» λειτουργία.

Στην περίπτωσή μας θα εξετάσουμε τη λειτουργία RREQ επειδή η μαύρη τρύπα πραγματοποιείται δεδομένου ότι ο κακόβουλος κόμβος λαμβάνει ένα πακέτο RREQ. Όταν ο κακόβουλος κόμβος λαμβάνει ένα πακέτο RREQ στέλνει αμέσως το πακέτο RREP στον προορισμό σαν να έχει ο ίδιος την γρηγορότερη διαδρομή. Ο κακόβουλος κόμβος προσπαθεί να εξαπατήσει τους κόμβους που στέλνουν ένα τέτοιο πακέτο RREP και αυτό το επιτυγχάνει θέτοντας το υψηλότερο sequence number του πρωτοκόλλου AODV που είναι 4294967295 στον κακόβουλο κόμβο. Με τον τρόπο αυτό ο blackhole κόμβος γίνεται ο next hop του πακέτου το οποίο και παραλαμβάνει. Το ψεύτικο RREP μήνυμα της επίθεσης μαύρων τρυπών παρουσιάζεται στο παρακάτω σχήμα (σχήμα 24).

```
sendReply(rq->rq_src,          // IP Destination
          1,                   // Hop Count
          rq->rq_dst,          // Dest IP Address
          4294967295,          // Highest Dest Sequence Num
        MY_ROUTE_TIMEOUT,      // Lifetime
          rq->rq_timestamp); // timestamp
```

**Σχήμα 24** RREP μήνυμα της επίθεσης blackhole

Στο επόμενο κεφάλαιο θα περιγράψουμε τις προσομοιώσεις και τα αποτελέσματα προσομοίωσης.

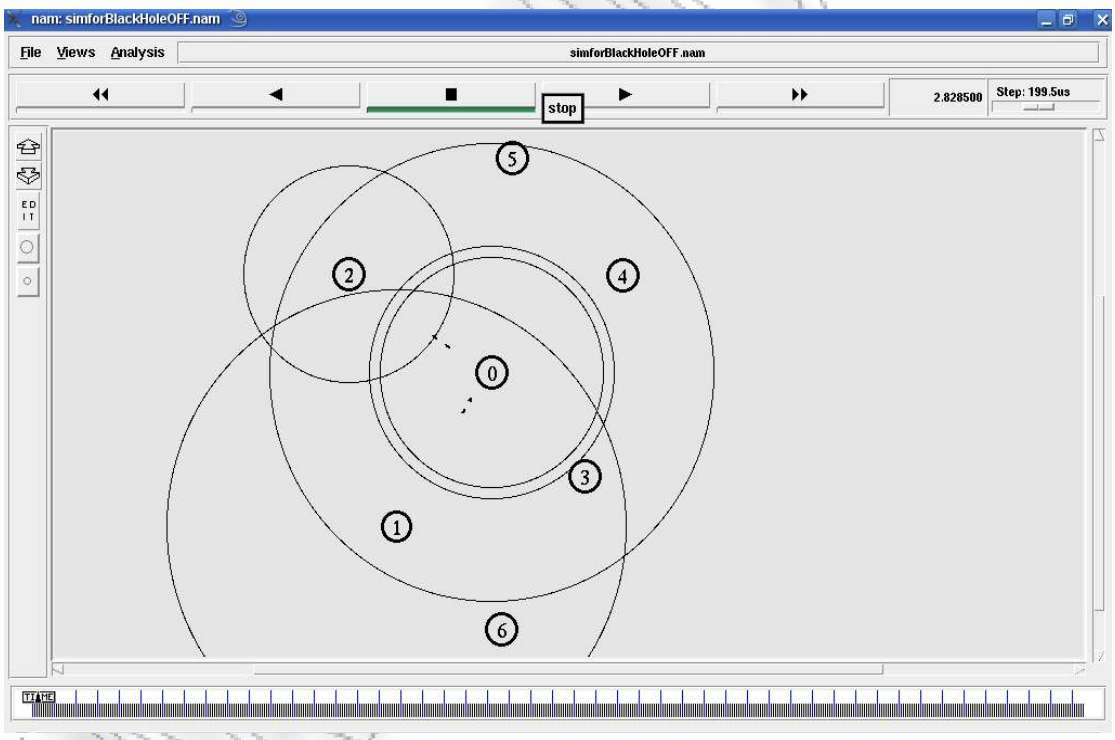
### 7.2.2 Προσομοίωση Επίθεσης Blackhole

Για να εξασφαλίσουμε ότι η εφαρμογή λειτουργεί σωστά, χρησιμοποιήσαμε την εφαρμογή NAM (Network Animator) του NS. Για να εξετάσουμε την εφαρμογή χρησιμοποιήσαμε δύο προσομοιώσεις. Στο πρώτο σενάριο δεν χρησιμοποιήσαμε κάποιον κόμβο να προσομοιώσει την μαύρη τρύπα στο δίκτυο. Στο δεύτερο σενάριο προσθέσαμε έναν κόμβο ο οποίος θα προσομοιώσει την επίθεση της μαύρης τρύπας στο δίκτυο. Κατόπιν συγκρίναμε τα αποτελέσματα των προσομοιώσεων χρησιμοποιώντας το NAM.

Για να πάρουμε ακριβή αποτελέσματα από τις προσομοιώσεις, χρησιμοποιήσαμε το πρωτόκολλο UDP. Ο κόμβος πηγής συνεχίζει την αποστολή των πακέτων UDP, ακόμα κι αν ο κακόβουλος κόμβος τα απορρίπτει, ενώ ο κόμβος σταματά την σύνδεση εάν χρησιμοποιεί το πρωτόκολλο TCP. Με τον τρόπο αυτό μπορούμε να παρατηρήσουμε τη ροή σύνδεσης μεταξύ του αποστολέα και του παραλήπτη κατά τη διάρκεια της προσομοίωσης. Επιπλέον ήμαστε σε θέση να μετρήσουμε χωριστά τα σταλμένα και λαμβανόμενα πακέτα δεδομένου ότι η σύνδεση UDP δεν χάνεται κατά τη διάρκεια της προσομοίωσης. Εάν είχαμε χρησιμοποιήσει το πρωτόκολλο TCP στα σενάριά μας δεν θα μπορούσαμε να μετρήσουμε τα σταλμένα ή λαμβανόμενα πακέτα δεδομένου ότι ο κόμβος που αρχίζει τη σύνδεση TCP θα τελειώσει τη σύνδεση μετά από μια στιγμή εάν δεν έχει λάβει το πακέτο TCP ack. Παράγουμε ένα μικρό δίκτυο μεγέθους επτά κόμβων και δημιουργούμε συνδέσεις UDP μεταξύ των διαφόρων κόμβων του δικτύου. Στους κόμβους αυτούς συνδέουμε την εφαρμογή CBR που παράγει τα σταθερά πακέτα μέσω της σύνδεσης UDP. Το μέγεθος των πακέτων CBR επιλέγεται για να είναι 512 bytes και με ρυθμό μετάδοσης 10Mbps. Η διάρκεια των σεναρίων είναι 500 δευτερόλεπτα και οι συνδέσεις CBR που αρχίζουν στο χρόνο είναι ίσες με 1.0 δευτερόλεπτο και συνεχίζονται μέχρι το τέλος της προσομοίωσης.

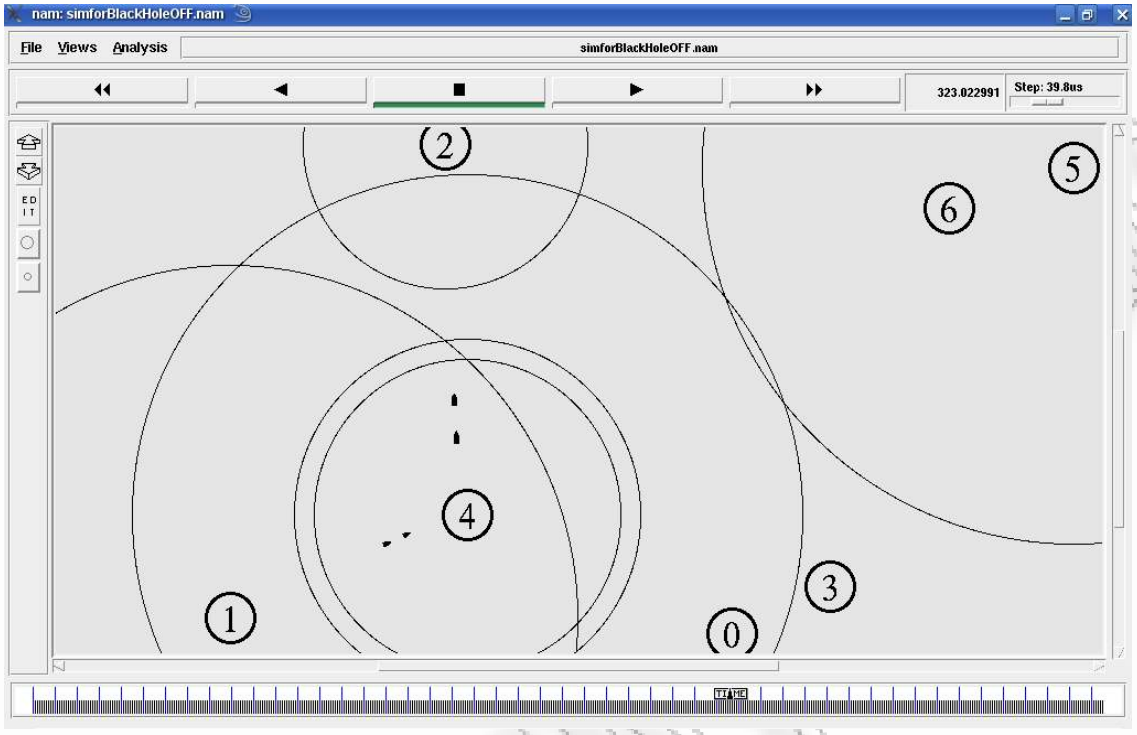
Στα σενάρια που δημιουργήσαμε κάθε ενιαίος κόμβος τοποθετείται σε διαφορετικές συντεταγμένες και εκθέτει διαφορετικές μετακινήσεις. Αυτό μας βοηθά να πάρουμε διαφορετικά αποτελέσματα με τους ίδιους κόμβους. Οι θέσεις και οι μετακινήσεις κόμβων παράγονται τυχαία από το ./setdest, το οποίο είναι μια εφαρμογή του προσομοιωτή για την δημιουργία τυχαίας κίνησης των κόμβων. Κάθε σενάριο ονομάζεται χρησιμοποιώντας τις παραμέτρους ./setdest, παραδείγματος χάριν στην επίθεση της Blackhole scenforAODV-n7-t500-x750-y750. Η εφαρμογή παράγει ένα σενάριο μεταξύ 7 κόμβων που κινούνται από μια τυχαία αφετηρία προς έναν τυχαίο προορισμό με μια ταχύτητα που επιλέγεται τυχαία, κατά τη διάρκεια 500 δευτερολέπτων, οι οποίες λαμβάνουν χώρα σε επίπεδο διάστημα 750x750 μέτρα.

Στο πρώτο σενάριο όπου δεν υπάρχει blackhole κόμβος, η σύνδεση μεταξύ του κόμβου 1 και του κόμβου 2 είναι σωστά δρομολογημένη όταν εξετάζουμε τη ζωτικότητά της χρησιμοποιώντας το NAM. Στο σχήμα 25 παρουσιάζεται η ροή των δεδομένων από τον κόμβο 1 στον κόμβο 2 μέσω του κόμβου 0.



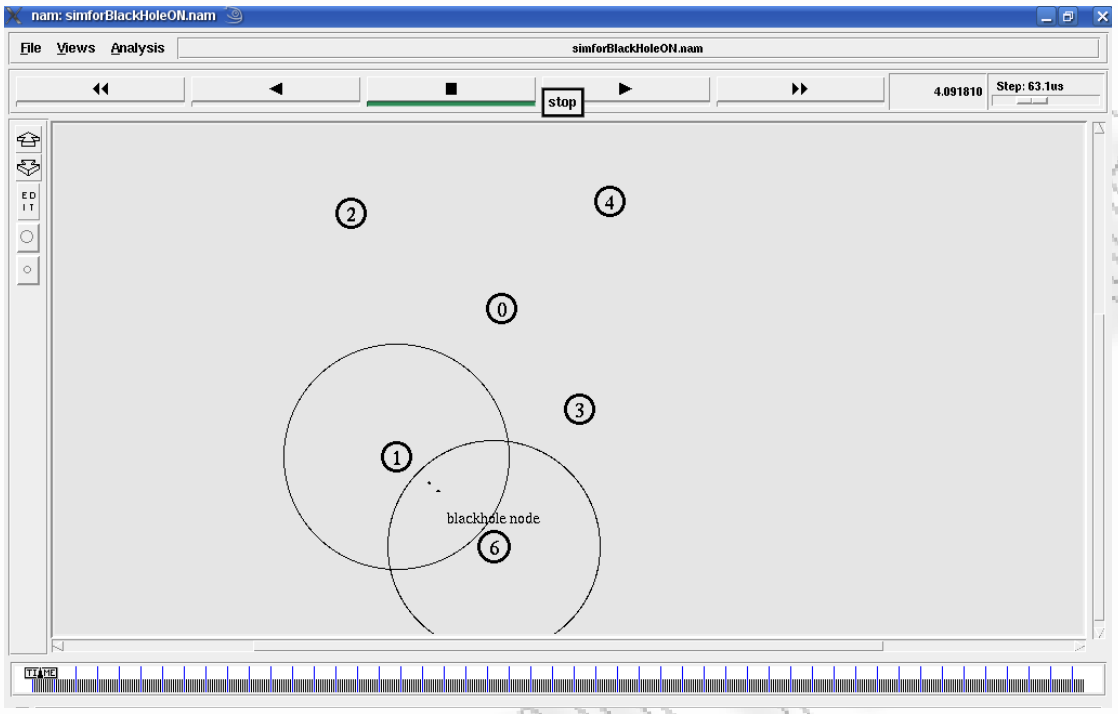

**Σχήμα 25 Ροή** δεδομένων μεταξύ κόμβου 1 και κόμβου 2 μέσω κόμβου 0

Όταν ο κόμβος 0 φεύγει εκτός της εμβέλειας του κόμβου 1 λόγω της κίνησής του, η νέα σύνδεση καθιερώνεται μέσω του κόμβου 4. Η νέα πορεία δρομολόγησης των πακέτων παρουσιάζεται στο σχήμα 26.




**Σχήμα 26** Ροή δεδομένων μεταξύ κόμβου 1 και κόμβου 2 μέσω κόμβου 4

Στο δεύτερο σενάριο που παρουσιάζεται στο σχήμα 27, έχουμε δημιουργήσει την συμπεριφορά της Blackhole επίθεσης στον κόμβο 6. Ο κόμβος αυτός απορροφά τα πακέτα των δεδομένων που δρομολογούνται από τον κόμβο 1 στον κόμβο 2 και τα απορρίπτει. Το παρακάτω σχήμα επιδεικνύει πώς ο κόμβος μαύρων τρυπών απορροφά την κυκλοφορία των πακέτων.




**Σχήμα 27** Ο Blackhole κόμβος 6 απορροφά την κίνηση των κόμβων 1 και 2

### 7.2.3 Αποτελέσματα Προσομοίωσης Επίθεσης Blackhole

Στο τέλος κάθε προσομοίωσης παίρνουμε τα αποτελέσματα από το trace file το οποίο παράγεται στον NS2 και έχει ως κατάληξη *.tr. Τα trace files περιλαμβάνουν όλα τα γεγονότα της προσομοίωσης όπως είναι τα πακέτα που στέλνονται, ποιος κόμβος τα παρήγαγε, ποιος κόμβος έχει τα παραλαμβάνει, ποιος τύπος πακέτου στέλνονται, εάν ένα πακέτο απορρίπτεται και ο λόγος που γίνεται αυτό. Στις προσομοιώσεις μας χρησιμοποιούμε το σχήμα “new-trace” που χρησιμοποιείται ειδικά στα ασύρματα δίκτυα και περιλαμβάνει τις λεπτομερείς πληροφορίες κάθε γεγονότος. Ένα δείγμα trace file παρουσιάζεται στο παράρτημα Α ενώ τα πεδία του εξηγούνται στο παράρτημα Β.

Για να πάρουμε τα αποτελέσματα από τα trace files χρειαστήκαμε μόνο τον τύπο γεγονότος στο πεδίο 1, την ταυτότητα των κόμβων (- Νι), το trace επίπεδο (- Nl) στο πεδίο 19, την διεύθυνση προέλευσης και την διεύθυνση προορισμού καθώς και τις αντίστοιχες πόρτες στα πεδία 31 (-Is) και 33 (-Id) και τέλος τον τύπο των πακέτων στο πεδίο 35 (-It). Για να προσδιορίσουμε τις ανωτέρω πληροφορίες από το trace file δημιουργήσαμε μέσω της γλώσσας προγραμματισμού awk πρόγραμμα το οποίο

απομονώνει τις πληροφορίες και μετράει τα πακέτα τα οποία στέλνονται, λαμβάνονται και απορρίπτονται κατά την διάρκεια της προσομοίωσης.

Η εντολή που χρησιμοποιήσαμε για να τρέξουμε το awk πρόγραμμα είναι η :

**awk –f aodv.awk < simforBlackHoleOFF.tr**

για το σενάριο στο οποίο δεν είχαμε δημιουργήσει την επίθεση της blackhole ενώ αντίστοιχα για την επίθεση ως ενεργή :

**awk –f blackholeaodv.awk < simforBlackHoleON.tr**

Προσπαθούμε αρχικά να αξιολογήσουμε το packet loss στο δίκτυο. Επομένως μετρήσαμε πόσα πακέτα στέλνονται από τους αποστολείς κόμβους και πόσα από αυτά έφθασαν στους παραλήπτες. Στο προηγούμενο τμήμα, περιγράψαμε πώς λαμβάνουμε τους αριθμούς των πακέτων. Οι πίνακες που θα ακολουθήσουν (πίνακας 1 και 2) συγκρίνουν το κανονικό δίκτυο με αυτό της blackhole. Στους πίνακες, η δεύτερη στήλη παρουσιάζει πόσα πακέτα στέλνονται και η τρίτη στήλη παρουσιάζει πόσα από αυτά έφθασαν στους παραλήπτες. Με τον υπολογισμό της διαφοράς μεταξύ των πινάκων προσπαθούμε να αξιολογήσουμε πόσα από τα πακέτα που δεν θα μπορούσαν να φθάσουν στον κόμβο προορισμού απορροφούνται στον κόμβο της blackhole. Το υπόλοιπο των στηλών παρουσιάζει ποσοστό των πακέτων που χάνονται. Στους πίνακες ο κόμβος 6 εμφανίζεται μόνος του γιατί είναι ο blackhole κόμβος και θέλουμε να τον εξετάσουμε μόνο του. Παρατηρήσαμε ότι το ποσοστό της απώλειας στοιχείων της μαύρης τρύπας αυξάνεται περισσότερο από τις κανονικές προσομοιώσεις των δικτύων AODV σε όλα τα σενάρια σε ποσοστό που φθάνει το 78,09 %

| **Κόμβος αποστολέας Κόμβος παραλήπτης** | **Πακέτα που στάλθηκαν** | **Πακέτα που παραλήφθηκαν** | **Packet loss (%)** |
|---|---|---|---|
| Κόμβος1 -> Κόμβος2 | 2718 | 2692 | 0,95 |
| Κόμβος4 -> Κόμβος5 | 3162 | 3123 | 1,23 |
| Κόμβος0 -> Κόμβος3 | 2385 | 2262 | 5,16 |
| Κόμβος6 | | 0 | |
| Συνολικά | 8265 | 8077 | 2,27 |

**Πίνακας 1** Αποτελέσματα ad hoc δικτύου χωρίς blackhole κόμβο

| Κόμβος αποστολέας Κόμβος παραλήπτης | Πακέτα που στάλθηκαν | Πακέτα που παραλήφθηκαν | Packet loss (%) |
|---|---|---|---|
| Κόμβος1 -> Κόμβος2 | 2917 | 1646 | 43,57 |
| Κόμβος4 -> Κόμβος5 | 3770 | 269 | 92,8 |
| Κόμβος0 -> Κόμβος3 | 2965 | 199 | 93,3 |
| Κόμβος blackhole 6 | | 5439 | |
| Συνολικά | 9652 | 2114 | 78,09 |

**Πίνακας 2** Αποτελέσματα ad hoc δικτύου με blackhole κόμβο

## 7.3 Επίθεση Flooding

### 7.3.1 Σχεδιασμός Επίθεσης Flooding

Εισάγουμε μια νέα επίθεση, την οποία καλούμε Flooding, που ενεργεί ως αποτελεσματική επίθεση άρνησης υπηρεσιών (DoS) ενάντια σε όλα τα προτεινόμενα ειδικά πρωτόκολλα δρομολόγησης δικτύων, συμπεριλαμβανομένων των πρωτοκόλλων που σχεδιάστηκαν για να είναι ασφαλή. Στην διπλωματική μας εργασία περιγράφουμε την επίθεση Flooding προκειμένου να δούμε την επίδρασή της στη λειτουργία του AODV πρωτοκόλλου.

Η επίθεση Flooding έχει ως σκοπό τα πακέτα RREQ σε ολόκληρο το δίκτυο να καταναλώσουν όσο το δυνατό περισσότερους πόρους του δικτύου. Για να μειώσει τη συμφόρηση σε ένα δίκτυο, το πρωτόκολλο AODV υιοθετεί μερικές μεθόδους. Ένας κόμβος δεν μπορεί να δημιουργήσει περισσότερα μηνύματα από τα RREQ_RATELIMIT RREQ ανά δευτερόλεπτο. Μετά από ένα broadcast RREQ, ένας κόμβος περιμένει ένα RREP. Εάν μια διαδρομή δεν το παραλάβει, μέσα στα χιλιοστά του δευτερολέπτου, ο κόμβος μπορεί να προσπαθήσει πάλι να ανακαλύψει μια διαδρομή με τη broadcast αναμετάδοση ενός άλλου RREQ, μέχρι ένα μέγιστο αριθμό προσπαθειών στη μέγιστη τιμή του TTL (Time To Live). Οι επαναλαμβανόμενες προσπάθειες από έναν κόμβο πηγής στην ανακάλυψη των διαδρομών προς έναν ενιαίο προορισμό πρέπει να γίνει χρησιμοποιώντας ένα δυαδικό εκθετικό backoff αλγόριθμο. Η πρώτη φορά που ένας κόμβος πηγής μεταδίδει broadcast ένα RREQ, περιμένει τον μετ' επιστροφής χρόνο για την υποδοχή ενός RREP. Εάν ένα RREP δεν παραλαμβάνεται μέσα σε αυτό το χρονικό περιθώριο, ο κόμβος πηγής στέλνει ένα νέο RREQ. Κατά τον υπολογισμό του χρόνου αναμονής για το RREP μετά αποστολή του δεύτερου RREQ, ο κόμβος πηγής πρέπει να χρησιμοποιήσει ένα δυαδικό εκθετικό backoff. Ως εκ τούτου, ο αναμονής χρόνος για το RREP που αντιστοιχεί στο δεύτερο RREQ είναι διπλάσιος του μετ' επιστροφής χρόνου.

Στην Ad Hoc Flooding επίθεση που σχεδιάσαμε σκοπός μας είναι να δημιουργηθούν πακέτα τα οποία θα στέλνονται broadcast από έναν αρχικό κόμβο, τον οποίο έχουμε ορίσει κάθε φορά, σε όλους τους υπόλοιπους προκειμένου να απορριφθούν όσο το δυνατόν περισσότερα πακέτα τα οποία ανταλλάσσουν οι υπόλοιποι κόμβοι την δεδομένη στιγμή. Δημιουργήσαμε έναν agent ο οποίος τοποθετείται σε κάθε κινούμενο κόμβο του συστήματός μας. Ο agent αυτός έχει την ιδιότητα να δεσμεύει μία πόρτα του κόμβου και μία διεύθυνση προκειμένου να δέχεται καθώς και να διαβιβάζει τα πακέτα τα οποία εισέρχονται σε αυτόν(σχήμα 28).

```
set MESSAGE_PORT 42
set BROADCAST_ADDR -1
```

**Σχήμα 28** Ορισμός broadcast port σε έναν agent

Το πακέτο το οποίο στέλνεται σε κάθε κόμβο είναι της μορφής ID:message. Κάθε κόμβος που έχει εγκαταστημένο τον agent λαμβάνει το μήνυμα και αφού το αποσυμπιέσει προκειμένου να δει το ID, προωθεί στον γειτονικό του κόμβο όσα μηνύματα εισέρχονται για πρώτη φορά στον ίδιο και δεν είναι αυτός ο αποδέκτης (σχήμα 29,30).

```
# extract message ID from message
set message_id [lindex [split $data ":"] 0]
puts "\nNode [$node_ node-addr] got message $message_id\n"

if {[lsearch $messages_seen $message_id] == -1} {
lappend messages_seen $message_id
    $ns trace-annotate "[$node_ node-addr] received {$data} from $source"
    $ns trace-annotate "[$node_ node-addr] sending message $message_id"
$self sendto $size $data $BROADCAST_ADDR $sport
} else {
    $ns trace-annotate "[$node_ node-addr] received redundant message $message_id from $source"
}
```

**Σχήμα 29** Αποκωδικοποίηση του πακέτου

```
Agent/MessagePassing/Flooding instproc send_message {size message_id data port} {
    $self instvar messages_seen node_
    global ns MESSAGE_PORT BROADCAST_ADDR
    lappend messages_seen $message_id
    # send the broadcast message
    $ns trace-annotate "[$node_ node-addr] sending message $message_id"
    $self sendto $size "$message_id:$data" $BROADCAST_ADDR $port
}
```

**Σχήμα 30** Δημιουργία agent για την αποστολή του broadcast μηνύματος

Τέλος στην cbr κίνηση που δημιουργήσαμε μέσω μιας γεννήτριας την οποία θα εξηγήσουμε παρακάτω, παράγουμε διαφορετικά μεγέθη πακέτων προκειμένου να έχουμε σε κάθε σενάριο διαφορετικά πακέτα RREQ.

### 7.3.2 Προσομοίωση Επίθεσης Flooding

Για να εξασφαλίσουμε ότι η εφαρμογή λειτουργεί σωστά, χρησιμοποιήσαμε την εφαρμογή NAM (Network Animator) του NS. Για να εξετάσουμε την εφαρμογή χρησιμοποιήσαμε δύο προσομοιώσεις. Στο πρώτο σενάριο δεν δημιουργήσαμε τον agent ο οποίος τοποθετείται στους κόμβους για να κάνει flooding τα πακέτα, ενώ αντίθετα στο δεύτερο σενάριο κάθε κόμβος έχει εγκατεστημένο από έναν τέτοιο agent. Κατόπιν συγκρίναμε τα αποτελέσματα των προσομοιώσεων χρησιμοποιώντας το NAM.

Για την προσομοίωση δημιουργήσαμε UDP agents με πηγές που παράγουν κίνηση CBR και τους προσαρτήσαμε στους κόμβους που έχουμε δημιουργήσει στο δίκτυο. Η γεννήτρια η οποία χρησιμοποιήθηκε για να δημιουργηθεί η κίνηση στο δίκτυο μεταξύ των κόμβων βρίσκεται στον φάκελο *~ns*/indep-utils/cmu-scen-gen και ονομάζεται cbrgen.tcl. Μπορεί να χρησιμοποιηθεί για την παραγωγή συνδέσεων τόσο CBR όσο και TCP. Για να δημιουργήσει τα CBR connection επικαλεστήκαμε την εντολή του NS-2:

**ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]**

Στην συγκεκριμένη επίθεση το μέγεθος των πακέτων CBR επιλέγεται για να είναι 404 bytes, με ρυθμό μετάδοσης 1Mbps. Η διάρκεια των σεναρίων είναι 100 δευτερόλεπτα

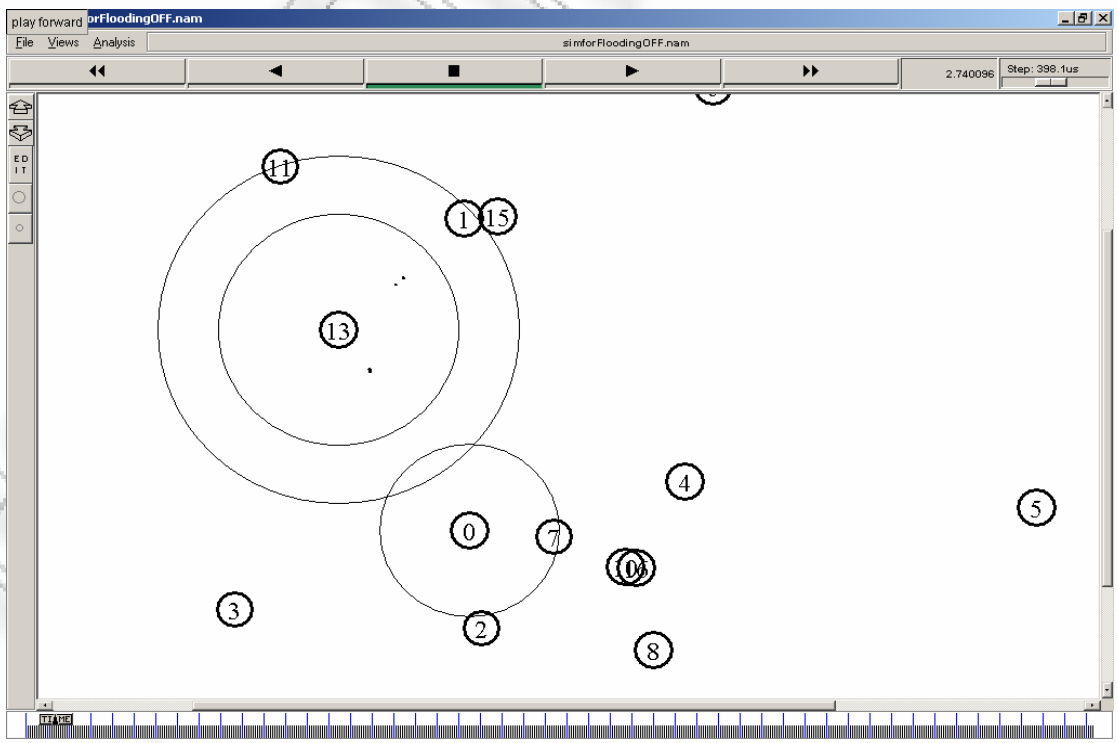
και οι συνδέσεις CBR που αρχίζουν στο 1.0 δευτερόλεπτο και συνεχίζονται μέχρι το τέλος της προσομοίωσης.

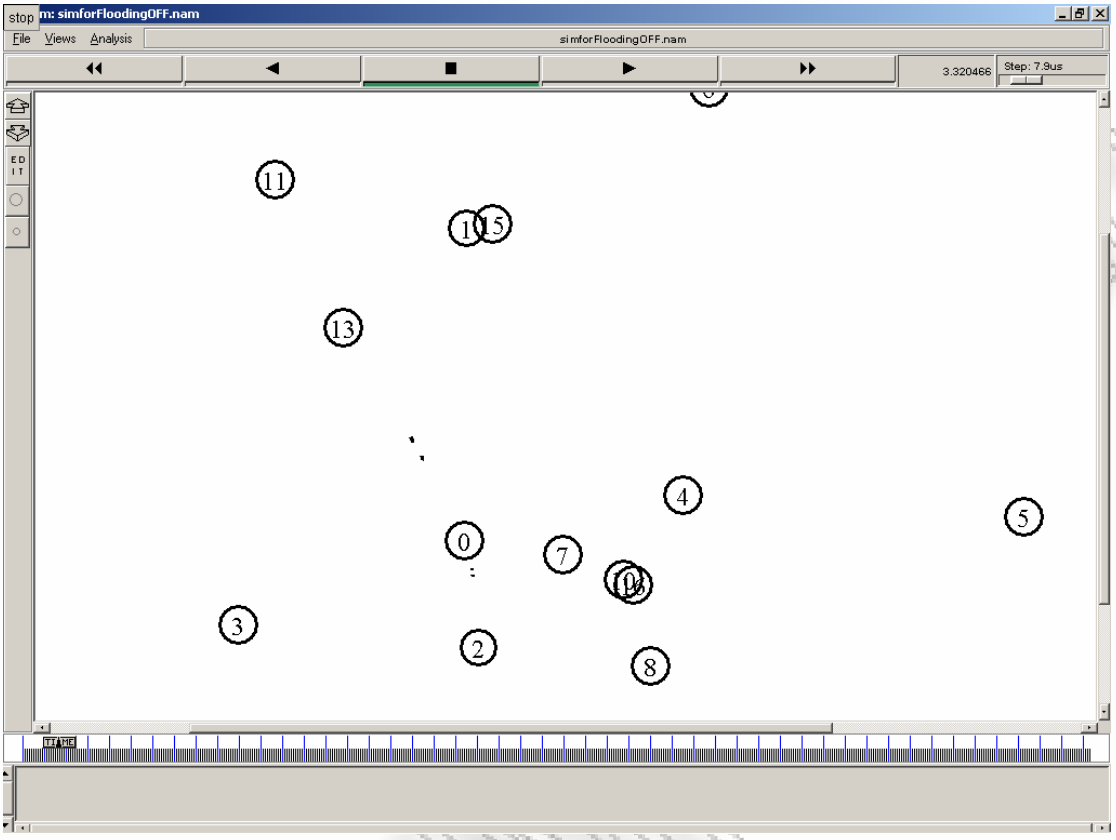
Στα σενάρια που δημιουργήσαμε κάθε ενιαίος κόμβος τοποθετείται σε διαφορετικές συντεταγμένες και εκθέτει διαφορετικές μετακινήσεις. Αυτό μας βοηθά να πάρουμε διαφορετικά αποτελέσματα με τους ίδιους κόμβους. Οι θέσεις και οι μετακινήσεις κόμβων παράγονται τυχαία από μία γεννήτρια η οποία μπορεί να δημιουργήσει κίνηση στους κόμβους του δικτύου. Η γεννήτρια βρίσκεται στον φάκελο *~ns*/indep-utils/cmu-scen-gen/setdest/ του NS-2. Για να δημιουργηθεί η κίνηση αυτή χρησιμοποιούμε την εντολή:

**./setdest -n <num_of_nodes> -p <pausetime> -M <maxspeed> -t <simtime>**
**-x <maxx> -y <maxy> > <outdir>/<scenario-file>**

Στην συγκεκριμένη επίθεση η εφαρμογή παράγει ένα σενάριο μεταξύ 20 κόμβων που κινούνται από μια τυχαία αφετηρία προς έναν τυχαίο προορισμό με μια ταχύτητα που επιλέγεται τυχαία, κατά τη διάρκεια 500 δευτερολέπτων, οι οποίες λαμβάνουν χώρα σε επίπεδο διάστημα 750x750 μέτρα.

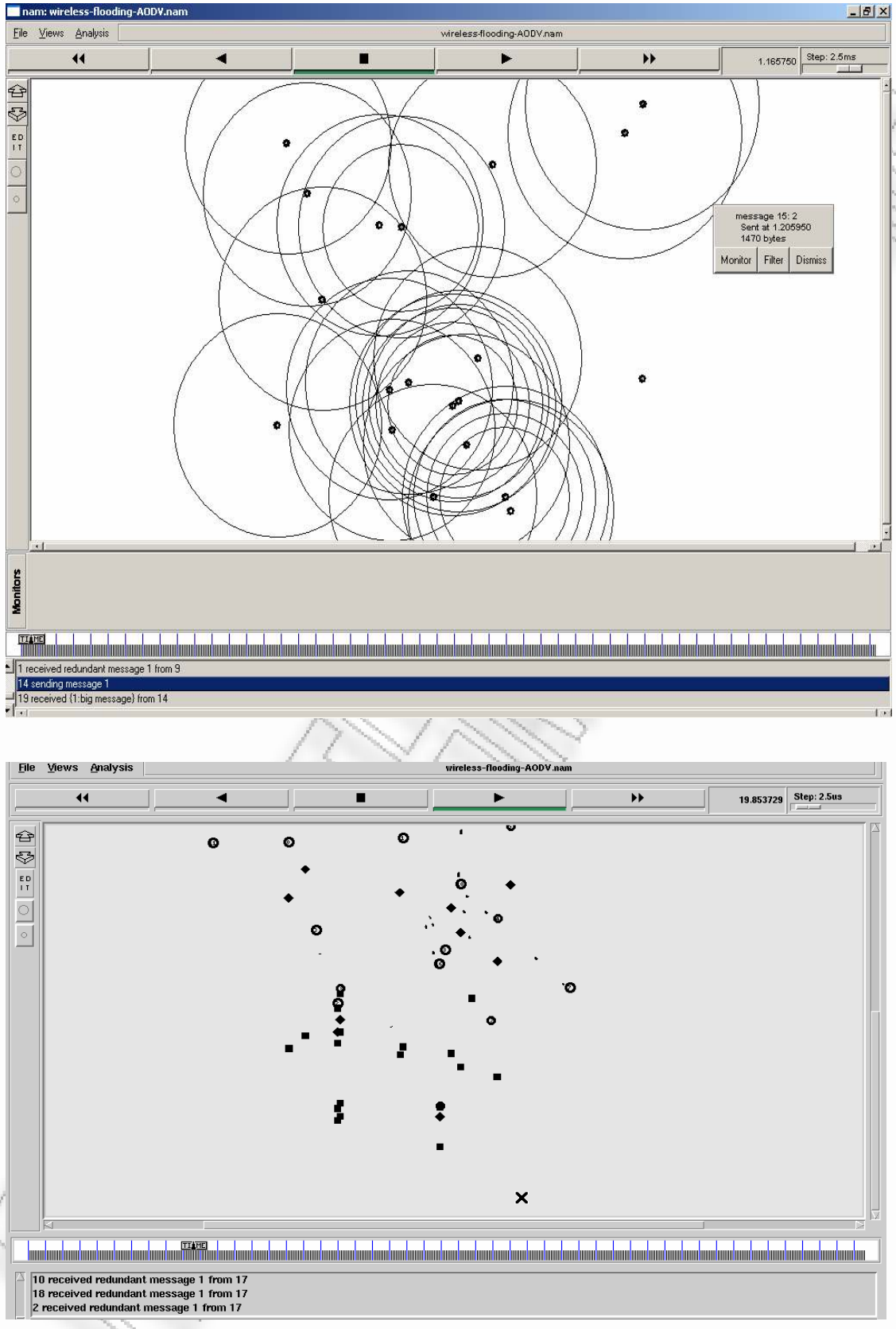
Στο πρώτο σενάριο όπου δεν υπάρχει ο flooding agent ενεργοποιημένος, η σύνδεση μεταξύ των κόμβων είναι σωστά δρομολογημένη όταν εξετάζουμε τη ζωτικότητά της χρησιμοποιώντας το NAM. Στο σχήμα 31 παρουσιάζεται η ροή των δεδομένων από τον κόμβο 1 στον κόμβο 2 μέσω των κόμβων 13 και 0.






**Σχήμα 31** Ροή δεδομένων μεταξύ κόμβων 1 και 2

Στο δεύτερο σενάριο που παρουσιάζεται στο σχήμα 32, έχουμε δημιουργήσει την συμπεριφορά της Flooding επίθεσης στο δίκτυο. Ένας τυχαίος κόμβος αναλαμβάνει να στείλει το αρχικό broadcast πακέτο στους υπόλοιπους. Αυτό έχει ως συνέπεια την καθυστέρηση του δικτύου και την απόρριψη πακέτων κάθε είδους, όπως για παράδειγμα είναι τα πακέτα cbr και acknowledgment. Το παρακάτω σχήμα επιδεικνύει πώς ο εκάστοτε κόμβος ξεκινάει την επίθεση και τα πακέτα τα οποία απορρίπτονται.




**Σχήμα 32** Προσομοίωση Flooding Attack σε Ad-Hoc δίκτυο

Στο κάτω μέρος της προσομοίωσης μπορούμε να παρατηρήσουμε ανά πάσα στιγμή ποίος κόμβος ξεκίνησε την επίθεση και που προωθεί το πακέτο. Στο παραπάνω σχήμα παρατηρούμε ότι ο αρχικός κόμβος είναι ο 14 και ο πρώτος κόμβος που παραλαμβάνει το πακέτο είναι ο 19.

### 7.3.3 Αποτελέσματα Προσομοίωσης Επίθεσης Flooding

Στο τέλος της προσομοίωσης παίρνουμε τα αποτελέσματα από το trace file το οποίο παράγεται στον NS2. Τα trace files, όπως αναλύσαμε και σε προηγούμενο κεφάλαιο, περιλαμβάνουν όλα τα γεγονότα της προσομοίωσης όπως είναι τα πακέτα που στέλνονται, ποιος κόμβος τα παρήγαγε, ποιος κόμβος έχει τα παραλαμβάνει, ποιος τύπος πακέτου στέλνονται, εάν ένα πακέτο απορρίπτεται και ο λόγος που γίνεται αυτό.

Για να πάρουμε τα αποτελέσματα από τα trace files χρειαστήκαμε τον τύπο γεγονότος στο πεδίο 1 (Event type), το trace επίπεδο (- Nl) στο πεδίο 19, τον λόγο του γεγονότος (Nw) στο πεδίο 21 και τέλος τον τύπο των πακέτων στο πεδίο 35 (-It). Για να προσδιορίσουμε τις ανωτέρω πληροφορίες από το trace file δημιουργήσαμε μέσω της γλώσσας προγραμματισμού awk πρόγραμμα το οποίο απομονώνει τις πληροφορίες και μετράει τα πακέτα τα οποία στέλνονται, λαμβάνονται και απορρίπτονται κατά την διάρκεια της προσομοίωσης.

Η εντολή που χρησιμοποιήσαμε για να τρέξουμε το awk πρόγραμμα είναι η :

**awk –f flooding.awk < simforfloodingOFF.tr**

για το σενάριο στο οποίο δεν είχαμε δημιουργήσει την επίθεση flooding ενώ αντίστοιχα θέτοντας την επίθεση ως ενεργή :

**awk –f flooding.awk < wireless-flooding-AODV.tr**

Προσπαθούμε αρχικά να αξιολογήσουμε τον αριθμό τον πακέτων που απορρίφθηκαν στο δίκτυο. Επομένως μετρήσαμε πόσα πακέτα δεν έφθασαν στον προορισμό τους και την αιτία που έγινε αυτό. Οι πίνακες που θα ακολουθήσουν (πίνακας 3 και 4) συγκρίνουν το κανονικό δίκτυο με αυτό της επίθεσης flooding. Στους πίνακες, η δεύτερη στήλη παρουσιάζει πόσα πακέτα απορρίπτονται και η πρώτη στήλη παρουσιάζει τον λόγο της απόρριψης και το είδος του πακέτου. Παρατηρήσαμε ότι το ποσοστό της απώλειας στοιχείων λόγω της επίθεσης αυξάνεται κατακόρυφα σε σχέση με τις κανονικές προσομοιώσεις των δικτύων AODV σε όλα τα σενάρια

| Αιτία απόρριψης / είδος πακέτου | Πακέτα που απορρίφθηκαν |
|---|---|
| Πακέτα CBR | 19 |
| Πακέτα END | 0 |
| Πακέτα COL | 12 |
| Πακέτα DUP | 0 |
| Πακέτα ERR | 0 |
| Πακέτα RET | 8 |
| Πακέτα STA | 0 |
| Πακέτα BSY | 0 |
| Πακέτα NRTE | 1 |
| Πακέτα LOOP | 0 |
| Πακέτα TTL | 16 |
| Πακέτα TOUT | 0 |
| Πακέτα CBK | 10 |
| Πακέτα IFQ | 0 |
| Πακέτα ARP | 0 |
| Πακέτα OUT | 0 |

**Πίνακας 3** Αποτελέσματα ad hoc δικτύου χωρίς επίθεση flooding

| Αιτία απόρριψης / είδος πακέτου | Πακέτα που απορρίφθηκαν |
|---|---|
| Πακέτα CBR | 99870 |
| Πακέτα END | 0 |
| Πακέτα COL | 91290 |
| Πακέτα DUP | 0 |
| Πακέτα ERR | 1650 |
| Πακέτα RET | 0 |
| Πακέτα STA | 0 |
| Πακέτα BSY | 0 |
| Πακέτα NRTE | 8870 |
| Πακέτα LOOP | 0 |
| Πακέτα TTL | 2 |
| Πακέτα TOUT | 0 |
| Πακέτα CBK | 83 |
| Πακέτα IFQ | 3678 |
| Πακέτα ARP | 99 |
| Πακέτα OUT | 0 |

**Πίνακας 4** Αποτελέσματα ad hoc δικτύου με επίθεση flooding

## 7.4 Επίθεση Worm

### 7.4.1 Σχεδιασμός Επίθεσης Worm

Η τρίτη επίθεση που δημιουργήσαμε στην διπλωματική προκειμένου να δούμε την επίδρασή της στην ανάπτυξη που θα έχει μέσα στο Ad Hoc δίκτυο καθώς και στην λειτουργία του AODV πρωτοκόλλου είναι η Worm Attack.

Η επίθεση αυτή κατά τον σχεδιασμό της υποθέτουμε ότι το worm διαδίδεται στο δίκτυο μέσω ενός ενιαίου πακέτου UDP το οποίο το μέγεθός του το έχουμε καθορίσει από την αρχή της προσομοίωσης. Το worm αρχείο, αρχικά, είναι τοποθετημένο σε έναν προεπιλεγμένο κόμβο του δικτύου. Επίσης έχουμε δημιουργήσει έναν πίνακα στον οποίο έχουμε επιλέξει αν ο κόμβος στον οποίο θα γίνει η επίθεση είναι ευπρόσβλητος στην επίθεση αυτή. Με την δημιουργία αυτού του πίνακα γνωρίζουμε εξαρχής σε ποιους κόμβους θα αποσταλεί και θα εγκατασταθεί το worm. Με τον τρόπο αυτό γίνεται ελεγχόμενη η προσομοίωση προκειμένου να έχουμε ακριβή αποτελέσματα.

Για την επίθεση του worm στο δίκτυο ο αρχικός κόμβος, ο οποίος έχει και το μήνυμα που περιέχει το worm, ελέγχει όλους τους one hop κόμβους. Για τον λόγο αυτό δημιουργήσαμε έναν agent ο οποίος τοποθετείται σε κάθε κινούμενο κόμβο του συστήματός μας. Ο agent αυτός έχει ως σκοπό την επικοινωνία μεταξύ των κόμβων προκειμένου να ελέγξει αν ο κόμβος που θα αποσταλεί το μολυσμένο πακέτο είναι ορισμένος ως ευπρόσβλητος ή όχι.

Αν κόμβος είναι ευπρόσβλητος σε τέτοιου είδους επίθεση τότε μέσω UDP στέλνεται το πακέτο του worm. Μόλις το μήνυμα το οποίο περιέχει το worm παραληφθεί από τον αποστολέα τότε ο πίνακας που εμφανίζει σε ποιον κόμβο έχει αποσταλεί το μήνυμα αλλάζει την σύστασή του μεταβάλλοντας την τιμή που αντιστοιχεί στον εκάστοτε κόμβο από μηδέν σε μονάδα εμφανίζοντάς μας ένα μήνυμα στην οθόνη για την αλλαγή που πραγματοποιήθηκε (σχήμα 36). Αν ο κόμβος δεν είναι ευπρόσβλητος σε αυτού του είδους επιθέσεις τότε το πακέτο δεν το λαμβάνει ο προς επίθεση κόμβος και ο παραπάνω ορισμένος πίνακας παραμένει αμετάβλητος.

```
for {set i 0} {$i < $val(nn)} {incr i [expr {5 + $i}]} {

    puts "node ($i)"

set a [lindex $node_weak $i]
set d [lindex $node_worm $i]
if {$a == 1 && $d == 0 } {
set udp(1) [new Agent/UDP]
$udp(1) set class_ 1
$ns_ attach-agent $node_(2) $udp(1)
set null(1) [new Agent/Null]
$null(1) set class_ 1
$ns_ attach-agent $node_($i) $null(1)
set cbr(1) [new Application/Traffic/CBR]
$cbr(1) set packetSize_ 400
$cbr(1) set interval_ 0.1
$cbr(1) attach-agent $udp(1)
$ns_ connect $udp(1) $null(1)
$ns_ at 1.3 "$cbr(1) start"
$ns_ at 1.4 "$cbr(1) stop"

   puts "worm send"
set b [lindex $node_worm $i]
puts "node $i has $b worm  "
set node_worm [lreplace $node_worm $i $i "1"]
set c [lindex $node_worm $i]
puts "node $i has $c worm  "
puts "$node_worm  "
} else {
   puts "worm not send"
puts "$node_worm  "
```

**Σχήμα 33** Έλεγχος κόμβου και αποστολή μηνύματος

### 7.4.2 Προσομοίωση Επίθεσης Worm

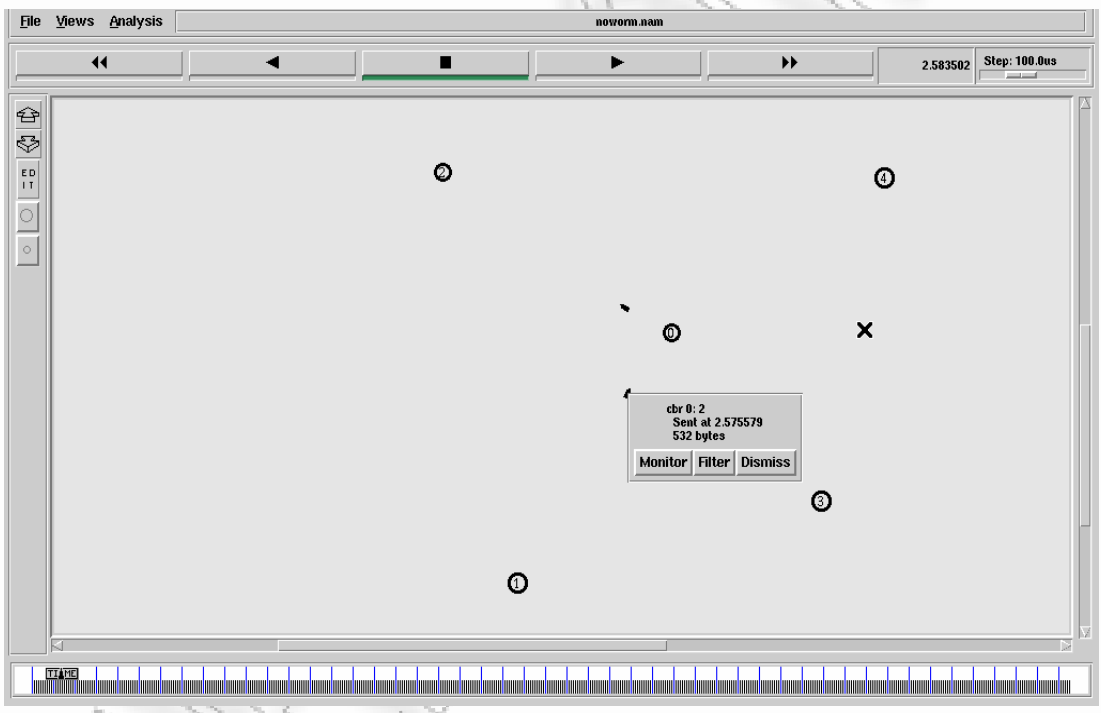
Για την προσομοίωση της επίθεσης Worm στο Ad Hoc δίκτυο χρησιμοποιήσαμε την εφαρμογή NAM του NS. Για να εξετάσουμε την εφαρμογή χρησιμοποιήσαμε δύο προσομοιώσεις. Στο πρώτο σενάριο όλα τα πακέτα τα οποία κυκλοφορούν στο δίκτυο δεν περιέχουν το worm πακέτο, ενώ αντίθετα στο δεύτερο σενάριο κάθε κόμβος έχει εγκατεστημένο από έναν agent ο οποίος βοηθάει στην επικοινωνία των κόμβων για την διάδοση του ιομορφικού πακέτου. Κατόπιν συγκρίναμε τα αποτελέσματα των προσομοιώσεων χρησιμοποιώντας το NAM.

Για την προσομοίωση δημιουργήσαμε UDP agents με πηγές που παράγουν κίνηση CBR και τους προσαρτήσαμε στους κόμβους που έχουμε δημιουργήσει στο δίκτυο. Η γεννήτρια η οποία χρησιμοποιήθηκε δημιούργησε κίνηση με μέγεθος των πακέτων CBR 512 bytes και ο ρυθμός μετάδοσης των δεδομένων στο δίκτυο είναι ίσος με 1Mbps. Η διάρκεια των σεναρίων είναι 500 δευτερόλεπτα και οι συνδέσεις CBR αρχίζουν στο 1.0 δευτερόλεπτο και συνεχίζονται μέχρι το τέλος της προσομοίωσης. Στα σενάρια που δημιουργήσαμε κάθε ενιαίος κόμβος τοποθετείται σε διαφορετικές

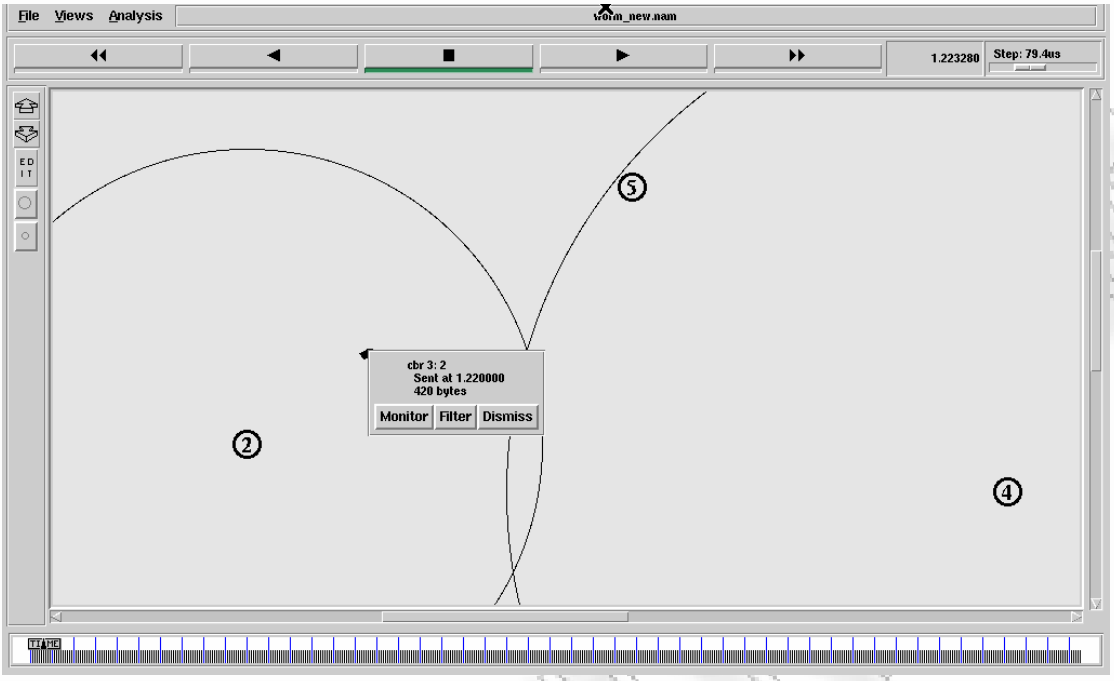
συντεταγμένες και εκθέτει διαφορετικές μετακινήσεις. Αυτό μας βοηθά να πάρουμε διαφορετικά αποτελέσματα με τους ίδιους κόμβους. Οι θέσεις και οι μετακινήσεις κόμβων παράγονται τυχαία από μία γεννήτρια η οποία μπορεί να δημιουργήσει κίνηση στους κόμβους του δικτύου.

Στην συγκεκριμένη επίθεση η εφαρμογή παράγει ένα σενάριο μεταξύ 7 κόμβων που κινούνται από μια τυχαία αφετηρία προς έναν τυχαίο προορισμό με μια ταχύτητα που επιλέγεται τυχαία έχοντας ως maximum τα 20m/s, κατά τη διάρκεια 500 δευτερολέπτων, οι οποίες λαμβάνουν χώρα σε επίπεδο διάστημα 750x750 μέτρα.

Στο πρώτο σενάριο όπου δεν υπάρχει ο worm agent ενεργοποιημένος, η σύνδεση μεταξύ των κόμβων είναι σωστά δρομολογημένη όταν εξετάζουμε τη ζωτικότητά της χρησιμοποιώντας το NAM. Στο σχήμα 34 παρουσιάζεται η ροή των δεδομένων από τον κόμβο 1 στον κόμβο 2 μέσω του κόμβου 0.



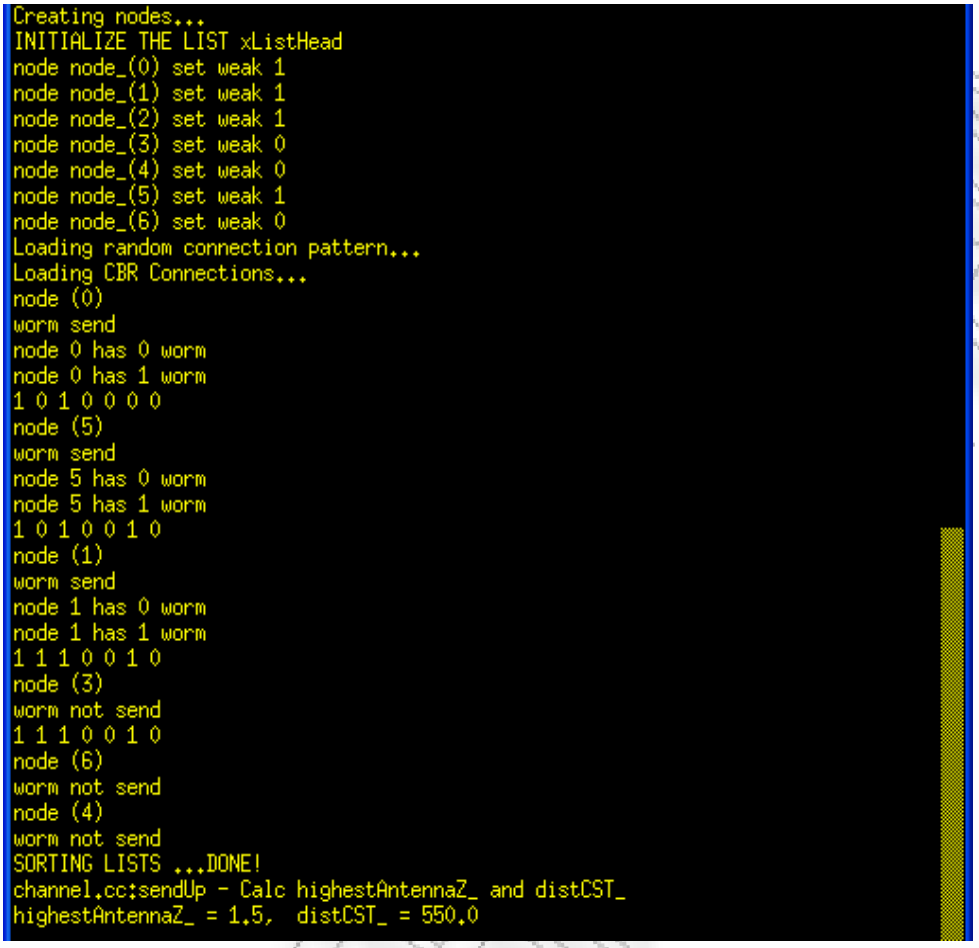

**Σχήμα 34** Ροή δεδομένων μεταξύ κόμβων 1 και 2




**Σχήμα 35** Αποστολή πακέτου worm από τον κόμβο 2 στον κόμβο 5

Στο δεύτερο σενάριο που παρουσιάζεται στο σχήμα 35, έχουμε δημιουργήσει την συμπεριφορά της worm επίθεσης στο δίκτυο. Ένας κόμβος αναλαμβάνει να στείλει το αρχικό πακέτο με το worm, του οποίου το μέγεθος έχει οριστεί στα 400 bytes, στους γειτονικούς του κόμβους. Ο κόμβος αν είναι ευάλωτος σε τέτοιου είδους επιθέσεις λαμβάνει το πακέτο διαφορετικά το απορρίπτει. Μετά την λήψη το προωθεί με την σειρά του στους one hop γειτονικούς του κόμβους εκτός από τον κόμβο που παρέλαβε ο ίδιος το πακέτο του worm. Η διαδικασία ολοκληρώνεται όταν όλοι οι ευάλωτοι κόμβοι του δικτύου προσβληθούν από το worm. Παράλληλα με την διάδοση του worm στο δίκτυο όλοι οι κόμβοι ανταλλάσουν μεταξύ τους κίνηση για να είναι η προσομοίωση πιο αληθοφανής.

Κατά την διάρκεια της προσομοίωσης από το command prompt μπορούμε να δούμε πληροφορίες όπως είναι ποιος κόμβος έχει χαρακτηριστεί ευάλωτος σε αυτές τις επιθέσεις καθώς και ποιος κόμβος παρέλαβε ή απέρριψε το πακέτο με το worm.




**Σχήμα 36** Πληροφορίες από το command prompt της worm προσομοίωσης

### 7.4.3 Αποτελέσματα Προσομοίωσης Επίθεσης Worm

Στο τέλος της προσομοίωσης παίρνουμε τα αποτελέσματα από το trace file το οποίο παράγεται στον NS2. Στην συγκεκριμένη προσομοίωση το στοιχείο το οποίο μας ενδιαφέρει να μετρήσουμε είναι ο χρόνος ο οποίος χρειάζεται για να μολύνει το πακέτο του worm όλους τους ευάλωτους προς αυτό κόμβους του δικτύου. Για να πάρουμε τα αποτελέσματα από τα trace files χρειαστήκαμε τον τύπο γεγονότος στο πεδίο 1 (Event type), τη ταυτότητα του κόμβου στο πεδίο 9 (-Ni), το trace επίπεδο (- Nl) στο πεδίο 19, την διεύθυνση προέλευσης και την διεύθυνση προορισμού καθώς και τις αντίστοιχες πόρτες στα πεδία 31 (-Is) και 33 (-Id), πόσες φορές το πακέτο προωθήθηκε στο πεδίο 49 (Pf) και τέλος το μέγεθος του πακέτου στο πεδίο 37 (Il). Για να προσδιορίσουμε τις ανωτέρω πληροφορίες από το trace file δημιουργήσαμε μέσω της γλώσσας προγραμματισμού awk πρόγραμμα το οποίο απομονώνει τις πληροφορίες και μετράει τα πακέτα τα οποία στέλνονται, λαμβάνονται και απορρίπτονται κατά την διάρκεια της προσομοίωσης.

Η εντολή που χρησιμοποιήσαμε για να τρέξουμε το awk πρόγραμμα είναι η :

**awk –f worm.awk < worm_new.tr**

Προσπαθούμε αρχικά να αξιολογήσουμε τον χρόνο τον οποίο χρειάζεται το πακέτο του worm να εξαπλωθεί σε ολόκληρο το ad hoc δίκτυο. Επομένως μετρήσαμε τον χρόνο αποστολής του πακέτου του worm μέχρι αυτό να παραληφθεί από τον εκάστοτε ευάλωτο παραλήπτη. Ο πίνακας που θα ακολουθεί (πίνακας 5) αναφέρει τον χρόνο που έκανε το πακέτο να φθάσει στον παραλήπτη καθώς και τον συνολικό χρόνο για την εξάπλωση στο δίκτυο.

| **Κόμβος αποστολέας Κόμβος παραλήπτης** | **Πακέτο worm** | **Χρόνος αποστολής πακέτου worm (sec)** |
|---|---|---|
| Κόμβος2 -> Κόμβος5 | NAI | 0.00586383 |
| Κόμβος2 -> Κόμβος0 | NAI | 0.00505779 |
| Κόμβος0 -> Κόμβος1 | NAI | 0.00761520 |
| Κόμβος0 -> Κόμβος3<br>Κόμβος5 -> Κόμβος4<br>Κόμβος1 -> Κόμβος6 | OXI | ------- |
| Συνολικός χρόνος αποστολής | | 0.0166195 |

**Πίνακας 5** Αποτελέσματα ad hoc δικτύου με επίθεση worm

# 8. Συμπεράσματα

Στην παρούσα διπλωματική παρουσιάστηκε και αναλύθηκε ένα πλαίσιο μοντελοποίησης για τη διάδοση κακόβουλων λογισμικών σε ασύρματα ad hoc δίκτυα. Στη συνέχεια το εν λόγω πλαίσιο χρησιμοποιήθηκε για τον χαρακτηρισμό και την αξιολόγηση τριών διαφορετικών μορφών επίθεσης.

Τα αποτελέσματα έδειξαν ότι, στα ασύρματα ad hoc δίκτυα, εν αντιθέσει με τα ενσύρματα, παράμετροι όπως η κινητικότητα των κακόβουλων χρηστών, η γενική συμπεριφορά των κακόβουλων χρηστών, όπως είναι ο έλεγχος της τοπολογίας, η ακτίνα εκπομπής των κόμβων καθώς και η ενεργειακή κατανάλωση αυτών είναι ιδιαίτερα κρίσιμες και ταυτόχρονα οδηγούν σε ιδιαίτερα πολύπλοκα συστήματα, τα οποία μερικές φορές μπορεί να είναι αδύνατον να επιλυθούν θεωρητικά.

Η μελλοντική εργασία, που θα μπορούσε να είναι και η συνέχεια της διπλωματικής αυτής, είναι η ανάπτυξη ενός τρόπου επίλυσης των κακόβουλων κόμβων μέσω ενός συστήματος ανίχνευσης εισβολών το οποίο κύριο μέλημα πρέπει να έχει την απόκριση που θα έχει το σύστημα σε μία τυχόν εισβολή. Η μελέτη της συμπεριφοράς του συστήματος ανίχνευσης εισβολών θα έχει ως βάση του την κινητικότητά του μέσα στο δίκτυο.

# Παράρτημα

## Παράρτημα Α

Προκειμένου να είναι πιο εύκολα αναγνώσιμο το διάβασμα του ασύρματου trace το οποίο χρησιμοποιεί το CMU trace μια νέα βελτιωμένη διάταξη trace έχει εισαχθεί. Αυτή η νέα μορφή trace είναι συμβατή με την παλαιά μορφοποίηση και μπορεί να ενεργοποιηθεί από την ακόλουθη εντολή:

$ns use-newtrace

Αυτή η εντολή πρέπει να κληθεί πριν από την εντολή $ns trace-all <trace-fd>. Η εντολή use-namtrace εγκαθιστά ένα νέο σχήμα για wireless tracing με τον ορισμό μιας νέας μεταβλητής προσομοίωσης αποκαλούμενου newTraceFormat. Προς το παρόν αυτή η νέα υποστήριξη ιχνών είναι διαθέσιμη μόνο για τις ασύρματες προσομοιώσεις.

Ένα παράδειγμα της νέας μορφής που έχει το trace φαίνεται παρακάτω:

s -t 0.267662078 -Hs 0 -Hd -1 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00 –Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.255 -Id -1.255 –It message -Il 32 -If 0 -Ii 0 -Iv 32

s -t 1.511681090 -Hs 1 -Hd -1 -Ni 1 -Nx 390.00 -Ny 385.00 -Nz 0.00 –Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 1.255 -Id -1.255 –It message -Il 32 -If 0 -Ii 1 -Iv 32

s -t 10.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00 –Ne -1.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 -Id 1.0 -It tcp -Il 1000 –If 2 -Ii 2 -Iv 32 -Pn tcp -Ps 0 -Pa 0 -Pf 0 -Po 0

r -t 10.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00 –Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 -Id 1.0 -It tcp -Il 1000 –If 2 -Ii 2 -Iv 32 -Pn tcp -Ps 0 -Pa 0 -Pf 0 -Po 0

r -t 100.004776054 -Hs 1 -Hd 1 -Ni 1 -Nx 25.05 -Ny 20.05 -Nz 0.00 –Ne -1.000000 -Nl AGT -Nw --- -Ma a2 -Md 1 -Ms 0 -Mt 800 -Is 0.0 -Id 1.0 –It tcp -Il 1020 -If 2 -Ii 21 -Iv 32 -Pn tcp -Ps 0 -Pa 0 -Pf 1 -Po 0

s -t 100.004776054 -Hs 1 -Hd -2 -Ni 1 -Nx 25.05 -Ny 20.05 -Nz 0.00 –Ne -1.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 1.0 -Id 0.0 -It ack -Il 40 -If 2 -Ii 22 -Iv 32 -Pn tcp -Ps 0 -Pa 0 -Pf 0 -Po 0

# Παράρτημα Β

**Επεξήγηση της νέας μορφής trace**

Το νέο σχήμα trace όπως φαίνεται ανωτέρω μπορεί να διαιρεθεί στους ακόλουθους τομείς:

**Event type:** στα ίχνη ανωτέρω, το πρώτο πεδίο (όπως με το παλαιότερο σχήμα ιχνών) περιγράφει τον τύπο γεγονότος που πραγματοποιείται στον κόμβο και μπορεί να είναι ένας από τους τέσσερις τύπους:

**s** αποστολή
**r** λήψη
**d** πτώση
**f** προώθηση

**General tag:** Το δεύτερο πεδίο που αρχίζει από "- το t" μπορεί να αντιπροσωπεύσει το χρόνο ή μια σφαιρική ρύθμιση
**-t** χρόνος
**-t** * (σφαιρική ρύθμιση)

**Node property tags**: Αυτό το πεδίο δείχνει τις ιδιότητες κόμβων όπως το id του κόμβου, το επίπεδο στο οποίο η επισήμανση γίνεται όπως τον πράκτορα, το δρομολογητή ή τη MAC. Οι ετικέτες αρχίζουν με μια οδήγηση "-N" και παρατίθενται όπως κατωτέρω:

**-Ni:** id του κόμβου
**-Nx:** συντεταγμένη x του κόμβου
**-Ny:** συντεταγμένη y του κόμβου
**-Nz:** συντεταγμένη z του κόμβου
**-Ne:** ενεργειακό επίπεδο κόμβων
**-Nl:** επίπεδο Trace όπως AGT, RTR, MAC
**-Nw:** αιτία για το γεγονός. Οι διαφορετικοί λόγοι για ένα πακέτο που πέφτει δίνονται παρακάτω.

**"END"** DROP_END_OF_SIMULATION
**"COL"** DROP_MAC_COLLISION
**"DUP"** DROP_MAC_DUPLICATE
**"ERR"** DROP_MAC_PACKET_ERROR
**"RET"** DROP_MAC_RETRY_COUNT_EXCEEDED
**"STA"** DROP_MAC_INVALID_STATE

**"BSY"** DROP_MAC_BUSY
**"NRTE"** DROP_RTR_NO_ROUTE i.e no route is available.
**"LOOP"** DROP_RTR_ROUTE_LOOP i.e there is a routing loop
**"TTL"** DROP_RTR_TTL i.e TTL has reached zero.
**"TOUT"** DROP_RTR_QTIMEOUT i.e packet has expired.
**"CBK"** DROP_RTR_MAC_CALLBACK
**"IFQ"** DROP_IFQ_QFULL i.e no buffer space in IFQ.
**"ARP"** DROP_IFQ_ARP_FULL i.e dropped by ARP
**"OUT"** DROP_OUTSIDE_SUBNET i.e dropped by base stations on receiving routing updates from nodes outside its domain.

**Οι πληροφορίες πακέτων σε επίπεδο IP** οι ετικέτες για αυτό το πεδίο αρχίζει με το γράμμα "- I" και παρατίθενται μαζί με τις εξηγήσεις τους ως ακολούθως:

**-Is:** source address.source port number
**-Id:** dest address.dest port number
**-It:** packet type
**-Il:** packet size
**-If:** flow id
**-Ii:** unique id
**-Iv:** ttl value

**Next hop info:** Αυτό το πεδίο παρέχει πληροφορίες για το επόμενο hop και το πεδίο αρχίζει με το γράμμα "-H".

**-Hs:** id for this node
**-Hd:** id for next hop towards the destination.

**Packet info at MAC level:** Αυτό το πεδίο δίνει πληροφορίες για το στρώμα MAC και αρχίζει με το γράμμα "-M" όπως δείχνεται παρακάτω:

**-Ma:** duration
**-Md:** dst's ethernet address
**-Ms:** src's ethernet address
**-Mt:** ethernet type

**Packet info at "Application level":** Οι πληροφορίες πακέτων σε επίπεδο εφαρμογής αποτελούνται από τον τύπο της εφαρμογής όπως το ARP, το TCP, τον τύπο ad-hoc πρωτοκόλλου δρομολόγησης όπως είναι το DSDV, DSR, AODV κ.λπ.

Αυτό το πεδίο αρχίζει με το γράμμα "-P" και μια λίστα πεδίων για διαφορετικές εφαρμογές φαίνεται παρακάτω:

**-P arp** Address Resolution Protocol. Λεπτομέρειες για το ARP δίνονται παρακάτω:

**-Po:** ARP Request/Reply
**-Pm:** src mac address
**-Ps:** src address
**-Pa:** dst mac address
**-Pd:** dst address

**-P dsr** Αυτό δείχνει το adhoc πρωτόκολλο δρομολόγησης αποκαλούμενο δυναμική δρομολόγηση πηγής. Οι πληροφορίες για το DSR αντιπροσωπεύονται από τις ακόλουθες ετικέτες:

**-Pn:** how many nodes traversed
**-Pq:** routing request flag
**-Pi:** route request sequence number
**-Pp:** routing reply flag
**-Pl:** reply length
**-Pe:** src of srcrouting->dst of the source routing
**-Pw:** error report flag
**-Pm:** number of errors
**-Pc:** report to whom
**-Pb:** link error from linka->linkb

**-P cbr** Constant bit rate. Πληροφορίες για την εφαρμογή CBR παρατίθενται παρακάτω :

**-Pi:** sequence number
**-Pf:** how many times this pkt was forwarded
**-Po:** optimal number of forwards
**-P tcp:** Information about TCP flow is given by the following subtags:
**-Ps:** seq number
**-Pa:** ack number
**-Pf:** how many times this pkt was forwarded
**-Po:** optimal number of forwards

# Βιβλιογραφία

[1] Amitabh Mishra, Ketan Nadkarni, Animesh Patcha, Virginia Tech "Intrusion Detection In Wireless Ad Hoc Networks" IEEE Wireless Communication February 2004

[2] Tiranuch Anantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Wireless/Mobile Network Security" Y.Xiao, X.Shen, and D.-Z. Du (Eds.) pp. 170-196

[3] Asad Amir Pirzada and Chris McDonald, "Detecting and Evading Wormholes in MobileAd-hoc Wireless Networks" International Journal of Network Security, Vol.3, No.2, PP.191–202, Sept. 2006

[4] Bo Sun, Lawrence Osborne, Yang Xiao, Sgaier Guizani "Intrusion Detection Techniques In Mobile Ad Hoc And Wireless Sensor Networks IEEE Wireless Communication October 2007

[5] Andrés Lagar Cavilla, "MANET extensions to ns2"

[6] Farooq Anjum, Petros Mouchtaris, "Security for Wireless Ad Hoc Networks" 2007

[7] Ramón Agüero Calvo, Jesús Pérez Campo, "Adding Multiple Interface Support in NS-2" January 2007

[8] Erdal Cayirci, Chunming Rong, " Security in Wireless Ad Hoc and Sensor Networks" 2009

[9] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless/Mobile Network Security Y.Xiao, X.Shen, and D.-Z. Du (Eds.) Chapter 12, 2006

[10] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks"

[11] Panayiotis Kotzanikolaou, Rosa Mavropodi, Christos Douligeris, "Secure Multipath Routing for Mobile Ad Hoc Networks"

[12] Yongguang Zhang, Wenke Lee, Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks" Mobile Networks and Applications (2003) 1-16

[13] Oleg Kachirski, Ratan Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks" 2002

[14] A. Karygiannis, E Antonakakis, and A. Apostolopoulos, "Detecting Critical Nodes for MANET Intrusion Detection Systems".

[15] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt, "A Specification-based Intrusion Detection System for AODV"

[16] Ioannis Chatzigiannakis, Andreas Strikos, "A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks"

[17] Bo Sun, Doctoral Dissertation " Intrusion Detection in Mobile Ad Hoc Networks" May 2004

[18] Bo Sun, Kui Wu, Udo W. Pooch, "Zone-Based Intrusion Detection for Mobile Ad Hoc Networks"

[19] Ejaz Ahmed, Kashan Samad, Waqar Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks" AusCert 2006 R&D Stream

[20] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless Ad Hoc Networks" Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 6-11,2000

[21] Semih Dokurer, " Simulation of Black Hole Attack in Wireless Ad-Hoc Networks", September 2006

[22] Fei Hu, Neeraj K. Sharma, "Security Considerations in Ad Hoc Sensor Networks" Computer Science (Elsevier), September 2003

[23] Francisco J.Ros, Pedro M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December 2004

[24] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, "An Intrusion Detection Tool for AODV-based Ad Hoc Wireless Networks"

[25] Kevin Fall, Kannan Varadhan, "The ns Manual" , January 6,2009

[26] Paul Brutch, Calvin Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networls" ,

[27] L. Zhou and Z.J. Haas, "Securing ad hoc networks", IEEE Network, November/December 1999

[28] A.D. Wood, J.A. Stankovic, "Denial of Service Attacks", CERT Advisory CA-98, January 1998

[29] Nikos Komninos, Dimitris Vergados, Christos Douligeris, "Layered security design for mobile ad hoc networks", 2005, p.123-124

[30] S. Yi, R Naldurg, and R. Kravets, "Security-aware Ad-hoc routing for Wireless Networks", ACM Wksp. Mobile Ad Hoc Networks, Mobihoc, 2001

[31] Ioanna Stamouli, Master Thesis, "Real-time Intrusion Detection for Ad Hoc Networks", September 12,2003

[32] B. Dahill, B. N. Levine, E. Royer, C. Shields, "A Secure Routing Protocol for Ad hoc Networks", Technical report, UM-CS-2001-037, University of Massachusetts, August 2001

[33] V. Karpijoki, "Security in Ad hoc Networks", In Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland 2000

[34] CMU extensions for ns-2, "http://www.isi.edu/nsnam/ns/", September 2002

[35] C. Perkins, E Belding-Royer, "Ad hoc On-demand Distance Vector (AODV)" Request For Comments (RFC) 3561, July 2003.

[36] M. G. Zapata, N. Asokan, "Secure Ad hoc On-demand Distance Vector Routing" ACM Mobile Computing and Communications Review, Vol 6, no 3, July 2002

[37] Tamilselvan L., Sankaranarayanan V., Prevention of Blackhole Attack in MANET, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007. 27-30 Aug. 2007 Page(s):21 – 21

[38] Perkins C. E., RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing, The Internet Society (2003)

[39] Antony D. Wood, John A. Stankovic, "Denial of Service in Sensor Networks" Computer 35(10): 54-62, 2002

[40] Fei Hu, Neeraj K. Sharma, "Security Considerations in Wireless Sensor Networks", (International Journal) Ad hoc Networks Journal (Elsevier), Volume 3, Issue 1, Pages 69-89, January 2005.

[41] Chris Karlof, David Wagner "Secure routing in wireless sensor networks attacks and countermeasures". Ad Hoc Networks 1(2-3): 293-315 (2003)

[42] Salem Benferhat, Fabien Autrel, Frédéric Cuppens "Enhanced Correlation in an Intrusion Detection Process". MMM-ACNS 2003:157-170

[43] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig "Secure Sensor Network Routing: A Clean-Slate Approach", In Proceedings of the 2nd Conference on Future Networking Technologies (CoNEXT), December 4-7, 2006, Lisboa, Portugal.

[44] Lingxuan Hu and David Evans "Secure Aggregation for Wireless Networks". Workshop on Security and Assurance in Ad hoc Networks. January, 2003

[45] Hoi Chang, Mikhail J. Atallah: "Protecting Software Code by Guards". Digital Rights Management Workshop 2001:160-175

[46] Christian S. Collberg, Clark D. Thomborson: "Watermarking, Tamper-Proofing, and Obfuscation-Tools for Software Protection". IEEE Trans. Software Eng. (TSE) 28(8):735-746 (2002)

[47] B. Sun, F. Yu, K. Wu, Y. Xiao, V. C. M. Leung, "Enhancing Security using Mobility-Based Anomaly Detection in Cellular Mobile Networks", IEEE Transactions on Vehicular Technology, Vol. 55, No. 4, July 2006, pp.1385-1396.

[48] Jing Deng, Richard Han, Shivakant Mishra: "Limiting DoS attacks during multihop data delivery in wireless sensor networks". IJSN 1(3/4):167-178 (2006)

[49] Jieying Zhou, Simeng Wang, Jing Deng, Hongda Feng: ZBMRP: A Zone Based Multicast Routing Protocol for Mobile Ad Hoc Networks. MSN 2005:113-122