ΤΖΑΦΟΛΙΑΣ ΔΗΜΗΤΡΙΟΣ

Διπλωματική Εργασία

Μελέτη συνεργατικών αρχιτεκτονικών συστημάτων ανίχνευσης εισβολών

Μεταπτυχιακή Διπλωματική Εργασία

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Ιούνιος 2011

Ευχαριστίες

Ευχαριστώ πολύ τον καθηγητή μου Δρ. Λαμπρινουδάκη για την καθοδήγηση του σε όλη τη διάρκεια εκπόνησης της διπλωματικής αυτής μελέτης.

" ...Αφιερώνεται στην Οικογένεια μου,

και σε όσους με στήριξαν τα χρόνια των σπουδών μου! "

Τραφόλας Δημήτριος.

Abstract

Intrusion Detection Systems (IDS) are systems comprised of software and hardware and their role is to automatically detect network intrusions. Ad hoc networks are autonomous self-organized wireless networks without steady infrastructure where devices are using their wireless interfaces to communicate. Due to the absence of steady infrastructure these networks are vulnerable to a number of attacks.

The current IDS architectures proposed for Ad Hoc networks are based on cooperative methodologies: hierarchical and cooperative architectures. In this dissertation an extensive study on suggested cooperative IDS architectures will be presented and their advantages and disadvantages will be thoroughly analyzed.

Περίληψη

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems-IDS) είναι συστήματα που συντίθενται από υλικό και λογισμικό και έχουν ως στόχο την αυτοματοποίηση της ανίχνευσης εισβολών. Τα Ad-Hoc δίκτυα είναι δίκτυα τυχαία διαμορφωμένα, χωρίς σταθερή υποδομή δικτύου και βασίζονται σε ασύρματες συνδέσεις ώστε να μπορούν να επικοινωνούν μεταξύ τους οι συσκευές. Λόγω της έλλειψης σταθερής υποδομής δικτύου, τα εν λόγω δίκτυα είναι τρωτά σε διάφορες επιθέσεις.

Οι πιο σύγχρονες αρχιτεκτονικές IDS πού έχουν προταθεί για Ad-Hoc δίκτυα βασίζονται σε διάφορες συνεργατικές μεθόδους όπως, λόγου χάρη, οι hierarchical και cooperative αρχιτεκτονικές. Στην διπλωματική αυτή εργασία, θα γίνει μια εκτενής μελέτη των προτεινόμενων συνεργατικών αρχιτεκτονικών IDS, με σκοπό να εντοπιστούν και να αναλυθούν τα πλεονεκτήματα και τα μειονεκτήματα τους.

Πίνακας περιεχομένων

Πίνακας Εικόνων

Κεφάλαιο 1

Εισαγωγή στα δίκτυα Ad Hoc

1.1 Εισαγωγή

Ο όρος "Ad-Hoc" χρησιμοποιείται στα δίκτυα υπολογιστών για να δηλώσει μια μέθοδο διασύνδεσης. Ελληνική ορολογία για τα δίκτυα αυτά δεν υπάρχει αλλά συνήθως ονομάζονται αδόμητα είτε «κατ' απαίτηση δίκτυα», με τον δεύτερο όρο να επικρατεί στη βιβλιογραφία. Τα δίκτυα αυτά δεν έχουν σταθερή υποδομή και εντάσσονται στην ευρύτερη κατηγορία δικτύων (Distributed Transient Networks) και είναι αποκεντρωμένα και αποτελούνται κυρίως από κόμβους οι οποίοι δεν ανήκουν εξ ορισμού και διαρκώς στο δίκτυο αλλά έχουν τη δυνατότητα να εισέρχονται ή να αποχωρούν από αυτό, οποιαδήποτε στιγμή και από οποιοδήποτε σημείο του. Η απουσία σταθερής υποδομής καθιστά αυτά τα δίκτυα ευέλικτα. Η τοπολογία τους αυτό-οργανώνεται διαρκώς και δυναμικά κάτι το οποίο τα κάνει ιδανικά για τη δικτύωση μεταξύ αυτοκινήτων που κινούνται και η θέση τους μεταβάλλεται (τεχνολογίες VANET – Vehicular Ad Hoc Networks και inVANAET) και γενικότερα κινητών πρακτόρων με δυνατότητες ασύρματης διασύνδεσης. Η φιλοσοφία της απουσίας σταθερής υποδομής δημιουργεί ένα σύνολο από νέες απαιτήσεις τόσο σχετικά με τη λειτουργία τους όσο και σχετικά με την ασφάλεια.

Στο κεφάλαιο που ακολουθεί θα παρουσιάσουμε τα βασικά χαρακτηριστικά των Ad Hoc δικτύων, οι ιδιαιτερότητές τους, θέματα διευθυνσιοδότησης και δρομολόγησης καθώς και τα κύρια πρωτόκολλα που χρησιμοποιούνται σε αυτά.

1.2 Ιδιότητες των Ad-Hoc δικτύων

Οι κινητοί κόμβοι από τους οποίους αποτελείται ένα Ad Hoc δίκτυο έχουν τη δυνατότητα λήψης και αποστολής δεδομένων τόσο με τους συνδεδεμένους σε αυτούς κόμβους όσο και με αυτούς που είναι συνδεδεμένοι στους γειτονικούς τους κόμβους. Η απευθείας επικοινωνία είναι γενικώς μια απλή διαδικασία αλλά η επικοινωνία με απομακρυσμένους κόμβους προϋποθέτει ότι ένας ή περισσότεροι ενδιάμεσοι κόμβοι θα αναλάβουν την μεταγωγή και δρομολόγηση των δεδομένων από τον αποστολέα στον παραλήπτη.

Στα Ad Hoc δίκτυα η τοπολογία μεταβάλλεται διαρκώς καθώς νέοι κόμβοι συνδέονται και άλλοι κόμβοι αποχωρούν από αυτό. Οι κόμβοι για να συμμετάσχουν σε ένα τέτοιο δίκτυο θα πρέπει να μπορούν να αντιλαμβάνονται την παρουσία νέων υποψηφίων κόμβων και να ενεργοποιούν πρωτόκολλα διασύνδεσης, δρομολόγησης αλλά και ενημέρωσης του δικτύου για τη σύνδεση του κάθε νέου κόμβου. Τέλος είναι σαφές ότι η δημιουργία και λειτουργία ενός Ad Hoc δικτύου πρέπει να γίνεται αυτόματα χωρίς τη διαχείριση εκ μέρους των χρηστών του ή χρήση ειδικευμένου υλικού.

Μια από τις βασικότερες λειτουργίες των δικτύων αυτών είναι η καταγραφή των βέλτιστων διαδρομών για τη μεταγωγή δεδομένων. Τα υπάρχοντα πρωτόκολλα δρομολόγησης των σταθερών δικτύων δεν μπορούν να χρησιμοποιηθούν για το σκοπό αυτό αλλά υπάρχουν πολλά πρωτόκολλα που σχεδιάστηκαν για ακριβώς αυτά τα αδόμητα δίκτυα. Σχετικές μελέτες και προσομοιώσεις έχουν αποδείξει ότι η απόδοση των πρωτοκόλλων αυτών υπολείπεται αρκετά από την απόδοση των πρωτοκόλλων σταθερών δικτύων.

1.3 Σύγκριση με σταθερά δίκτυα

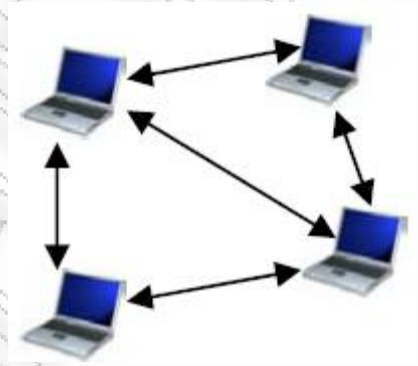
Οι κύριες διαφορές μεταξύ των σταθερών δικτύων και των δικτύων Ad Hoc αφορούν το Hardware, την διευθυνσιοδότηση, την ονοματοδοσία και το πιο σημαντικό τη δρομολόγηση.

1.3.1 Σχετικά με την υποδομή (Infrastructure)

Ένα χαρακτηριστικό των δικτύων Ad Hoc είναι ότι αποτελούνται από ένα σχετικά μικρό αριθμό ετερογενών κόμβων. Διαφορετικοί τύπου συσκευών είναι μέλη του δικτύου αυτού, με διαφορετικές δυνατότητες η κάθε μια (συσκευές PDA, laptop, embedded devices κτλ). Η ανομοιογένεια είναι υπαρκτή σε πολλά από τα χαρακτηριστικά των κόμβων όπως η διάρκεια ζωής των μπαταριών, η υπολογιστική ισχύς, η ακτίνα εκπομπής, η ταχύτητα του ρυθμού επικοινωνίας, η δυνατότητα αποστολής broadcast ή multicast καθώς και η υποστήριξη κινητικότητας.

Στα δίκτυα Ad Hoc η εμβέλεια αποστολής ή λήψης μιας συσκευής παίζει καθοριστικό ρόλο. Όσο μεγαλύτερη είναι τόσο λιγότεροι ενδιάμεσοι κόμβοι χρειάζεται να χρησιμοποιηθούν για τη μετάδοση δεδομένων. Από την άλλη, μια μεγάλη εμβέλεια σημαίνει ότι οι παρεμβολές μεταξύ των συσκευών θα είναι μεγαλύτερη με αποτέλεσμα την ύπαρξη πολλών συγκρούσεων πακέτων κατά τη μεταγωγή.

Αναλόγως των πρωτοκόλλων που χρησιμοποιούνται, δύο τύποι υποδομών μπορεί να δημιουργηθούν. Στην ισοδύναμη τοπολογία κάθε κόμβος θεωρείται ίσος με κάθε άλλο κόμβο του δικτύου και συνδέεται με όσους κόμβους μπορεί και δρομολογεί τα πακέτα του δικτύου.

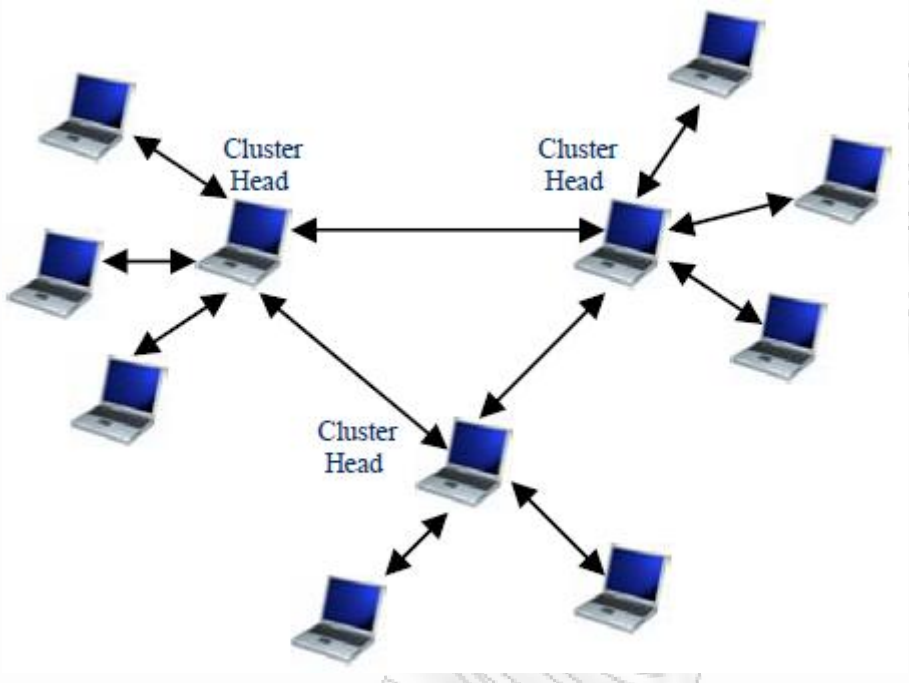


Εικόνα 1.1 Ισοδύναμη τοπολογία κόμβων

Στην πολύ-επίπεδη τοπολογία ορισμένοι κόμβοι που διαθέτουν είτε δυνατότερους πομποδέκτες είτε πιο ισχυρό hardware δημιουργούν την «*σπονδυλική στήλη*» του δικτύου και οι υπόλοιποι κόμβοι συνδέονται σε έναν από αυτούς. Στην περίπτωση αυτή οι πιο ισχυροί κόμβοι (Cluster Heads) ουσιαστικά αναλαμβάνουν το μεγαλύτερο μέρος της δρομολόγησης.

Πρέπει να σημειωθεί ότι από πλευράς συστημάτων ανίχνευσης παρεισφρήσεων η πολύ-επίπεδη τοπολογία μπορεί να υποστηρίξει πολλές περισσότερες υποδομές ασφαλείας

σχετικά τόσο με την εμπιστοσύνη μεταξύ κόμβων όσο και την χρήση κρυπτογράφησης στο δίκτυο.



Εικόνα 1.2 Πολύ-επίπεδη τοπολογία κόμβων

Για την περιγραφή ενός δικτύου Ad Hoc, οι Micah Adler και Christian Scheideler, προτείνουν ένα μοντέλο τριών επιπέδων [12]. Αρχικά, έχουμε το **επίπεδο ελέγχου προσπέλασης μέσου** (Medium Access Control layer), το οποίο είναι υπεύθυνο για την επικοινωνία από κόμβο σε κόμβο (node-to-node) στο φυσικό μέσο. Ακολούθως έχουμε το **επίπεδο επιλογής διαδρομής**, (route selection layer), το οποίο είναι υπεύθυνο για την εύρεση κατάλληλων διαδρομών για τα πακέτα. Τέλος, έχουμε το **επίπεδο χρονοπρογραμματισμού** (scheduling layer), που είναι υπεύθυνο για τον καθορισμό της σειράς αποστολής των πακέτων.

Για τη μέτρηση της απόδοσης ενός δικτύου Ad Hoc έχουν οριστεί ορισμένες μετρικές οι οποίες είναι:

- ALM – Application Layer Metrics
- NLM – Network Layer Metrics
- MLM – MAC Layer Metrics

Χρησιμοποιώντας τις παραπάνω μετρικές, στο επίπεδο εφαρμογών, η συνολική καθυστέρηση επικοινωνίας και ο ρυθμός μετάδοσης δεδομένων επηρεάζουν τα ALM. Στο επίπεδο δικτύου παράμετροι όπως το buffer size, η δυνατότητα διόρθωσης λαθών μετάδοσης (error correction), η κατανάλωση ισχύος και άλλα χαρακτηριστικά αποτελούν τις μετρικές NLM. Τέλος στο επίπεδο διασύνδεσης (MAC Layer) το σημαντικότερο χαρακτηριστικό το οποίο μπορεί να μετρήσει την ποιότητα αποτελεί το Signal To Noise ratio.

1.3.2 Σχετικά με την διευθυνσιοδότηση (Addressing)

Στα παραδοσιακά δίκτυα οι διασυνδεμένες συσκευές λαμβάνουν ως διεύθυνση δικτύου (IP Address) είτε στατικά νούμερα που δίδονται από το διαχειριστή του δικτύου είτε δυναμικά δέχονται τη διεύθυνση τους μέσω τη χρήση πρωτοκόλλων όπως το DHCP (Dynamic Host Configuration Protocol). Εξυπηρετητές DHCP ενημερώνονται για τη σύνδεση μιας νέας συσκευής στο δίκτυο που εξυπηρετούν και αυτόματα δίνουν μια τυχαία ή μια συγκεκριμένη διεύθυνση σε κάθε συσκευή. Πέρα από τη διεύθυνση αυτή, αποστέλλονται και άλλες πληροφορίες όπως η τοποθεσία των DNS servers, το μέγεθος του τοπικού δικτύου (netmask) καθώς και η διεύθυνση του δρομολογητή που εξυπηρετεί το δίκτυο (default gateway).

Μόνο όμως σε ένα σταθερό δίκτυο είναι εγγυημένο ότι κάθε συσκευή διαθέτει μια μοναδική και ξεχωριστή διεύθυνση δικτύου. Στα Ad Hoc δίκτυα, δεν υπάρχει κάποια κεντρική υποδομή η οποία θα αναλαμβάνει την επιστασία της διαδικασίας διευθυνσιοδότησης. Έτσι η διεύθυνση η οποία δόθηκε στη συσκευή ενός κόμβου δεν αντικατοπτρίζει την γεωγραφική θέση της συσκευής και ούτε τη μοναδικότητα της διεύθυνσης αυτής. Έτσι υπάρχει μια πολύ μεγαλύτερη πολυπλοκότητα στην κατανόηση και χρήση ενός τέτοιου δικτύου.

1.3.3 Σχετικά με τη δρομολόγηση (Routing)

Στα σταθερά δίκτυα η δρομολόγηση πακέτων από τον αποστολέα μέχρι τον παραλήπτη αναλαμβάνεται αποκλειστικά από συσκευές ειδικά ρυθμισμένες για τον σκοπό αυτό όπως Routers και Switches ή από υπολογιστές με πολλαπλά interfaces που διαθέτουν καταλλήλως παραμετροποιημένο λογισμικό. Η διευθυνσιοδότηση των σταθερών δικτύων λειτουργεί με τέτοιο τρόπο ώστε ομάδες διευθύνσεων να εξυπηρετούνται από συγκεκριμένους δρομολογητές. Έτσι κάθε συσκευή δρομολόγησης μπορεί με πολύ λίγες πληροφορίες να δρομολογήσει δεδομένα σε κάθε πιθανό δίκτυο (Παράδειγμα: Κανόνας1 «Δρομολόγησε ότι πακέτα έχουν προορισμό το δίκτυο 192.168.1.0/24 στο interface1. Κανόνας2 «Δρομολόγησε όλα τα υπόλοιπα πακέτα στο interface2.)

Στα Ad Hoc δίκτυα, κάθε συσκευή διαθέτει ένα μόνο ασύρματο interface επικοινωνίας και όλη η επικοινωνία αλλά και δρομολόγηση πρέπει να λειτουργεί μέσα από αυτό το μοναδικό κανάλι το οποίο από τη φύση του είναι τύπου broadcast. Επιπλέον στα Ad Hoc δίκτυα δεν υπάρχουν προκαθορισμένες συσκευές δρομολόγησης αλλά πρέπει η κάθε συσκευή να βοηθά στην διαδικασία δυναμικής δρομολόγησης, διαρκώς κατά τη διάρκεια ύπαρξης της μέσα σε ένα τέτοιο δίκτυο. Η διευθυνσιοδότηση των Ad Hoc δικτύων δεν βοηθά τη διαδικασία δρομολόγησης. Κάθε συσκευή διαθέτει ξεχωριστή διεύθυνση στο δίκτυο η οποία δεν παραπέμπει στην πιθανή της θέση. Έτσι οι πίνακες δρομολόγησης δεν μπορούν να είναι ομαδοποιημένοι όπως στο παράδειγμα των σταθερών δικτύων στην προηγούμενη παράγραφο. Οι πίνακες δρομολόγησης στις Ad Hoc συσκευές πρέπει να είναι πολύ αναλυτικοί (για κάθε IP διεύθυνση πρέπει να γνωρίζει σε ποια συσκευή να απευθυνθεί). Επίσης λόγο της αποσύνδεσης και σύνδεσης αλλά και της κινητικότητας των συσκευών οι πίνακες αυτοί πρέπει διαρκώς να ενημερώνονται.

1.4 Πρωτόκολλα δρομολόγησης Ad-Hoc δικτύων

Στα δίκτυα Ad Hoc ένα πακέτο πολλές φορές θα χρειαστεί να ταξιδέψει ανάμεσα σε διάφορους κόμβους μέχρι να φτάσει στον προορισμό του. Ο κύριος σκοπός του πρωτόκολλου δρομολόγησης είναι να διατηρεί έναν πίνακα δρομολόγησης με πληροφορίες σχετικά με την κατεύθυνση στην οποία πρέπει να αναμεταδώσει το κάθε πακέτο πληροφοριών.

Τα προβλήματα δρομολόγησης στα παραδοσιακά δίκτυα έχουν επιτυχώς αντιμετωπιστεί από δυναμικά πρωτόκολλα όπως το OSPF (Open Shortest Path First) και το RIP (Routing Information Protocol). Τα πρωτόκολλα αυτά είναι ικανά να λειτουργήσουν πολύ αποδοτικά σε περιβάλλοντα όπου η τοπολογία του δικτύου είναι σχετικά σταθερή. Στα Ad Hoc δίκτυα όπου υπάρχει πλήρη ελευθερία κινήσεως για τους κόμβους, υπάρχουν και άλλα χαρακτηριστικά που κάνουν τη χρήση των πρωτοκόλλων αυτών αδύνατη. Λόγω του διαθέσιμου εύρους φάσματος στα ασύρματα δίκτυα ένα κόμβος μπορεί να λειτουργεί unidirectional (μόνο να στέλνει ή μόνο να δέχεται δεδομένα).

Για τους παραπάνω λόγους μια σειρά από πρωτόκολλα δρομολόγησης ειδικά για Ad Hoc δίκτυα έχουν αναπτυχθεί. Παρακάτω ακολουθεί μια λίστα χαρακτηριστικών που υλοποιούνται από τα πρωτόκολλα αυτά.

- Κατανεμημένη λειτουργία.
- Απουσία βρόγχων. Η απουσία βρόγχων (loops) στη δρομολόγηση επιτυγχάνει καλύτερη απόδοση στο δίκτυο.
- Λειτουργία on-demand: Αντί για να διατηρεί τεράστιους πίνακες δρομολόγησης σε κάθε κόμβο και διαρκώς να τους ενημερώνει, το πρωτόκολλο θα πρέπει να εντοπίζει τους απαραίτητους κανόνες δρομολόγησης την στιγμή που θα χρειαστεί να δρομολογηθεί ένα πακέτο. Έτσι γίνεται οικονομία τόσο ενέργειας όσο και εύρους ζώνης (bandwidth).
- Λειτουργία pro-active: Σε ένα δίκτυο πολλοί κόμβοι στέλνουν διαρκώς λίγα δεδομένα σε πολλούς κόμβους η λειτουργία on-demand δημιουργεί ιδιαίτερο overhead στο δίκτυο. Στην περίπτωση αυτή η pro-active λειτουργία, δηλαδή η διαρκή διατήρηση δεδομένων πρωτοκόλλησης είναι προτιμότερη.
- Ασφάλεια: Απαραίτητη προϋπόθεση αποτελεί η ύπαρξη μηχανισμών ασφαλείας έτσι ώστε ένας κακόβουλος χρήστης χρησιμοποιώντας έναν κόμβο να μην μπορεί να αποδιοργανώσει το δίκτυο στέλνοντας εσφαλμένες πληροφορίες.
- Κατάσταση διατήρησης ενέργειας (sleep): Η άσκοπη κατανάλωση ενέργειας πρέπει να αποφεύγεται και τα πρωτόκολλα δρομολόγησης θα πρέπει να σέβονται όσο το δυνατόν τη συνθήκη αυτή.
- Χρήση πολλαπλών μονόδρομων διαδρομών: Επειδή ορισμένοι κόμβοι μπορεί να λειτουργούν μόνο προς μια κατεύθυνση θα πρέπει το πρωτόκολλο να μπορεί να χρησιμοποιεί διαφορετικούς κόμβους ώστε να επιτυγχάνει αμφίδρομη επικοινωνία.

1.4.1 Πρωτόκολλα βασισμένα σε πίνακες

Τα πρωτόκολλα που βασίζονται σε πίνακες δρομολόγησης υλοποιούν την pro-active λειτουργία. Όταν ένα τέτοιο πρωτόκολλο χρησιμοποιείται, κάθε κόμβος γνωρίζει που να δρομολογήσει για κάθε άλλο κόμβο που είναι συνδεδεμένος στο δίκτυο αυτό. Περιοδικά για κάθε αλλαγή στην τοπολογία, ένα μήνυμα ανανέωσης αποστέλλεται σε κάθε κόμβο, έτσι ώστε όλοι οι κόμβοι να γνωρίζουν με λεπτομέρεια την τρέχουσα τοπολογία.

Το μειονέκτημα των πρωτοκόλλων αυτών είναι ότι πολύ συχνά μια σύνδεση ανάμεσα σε δύο κόμβους μεταβάλλεται, με αποτέλεσμα πολλά μηνύματα να δημιουργούνται στο δίκτυο. Οι κόμβοι αυτοί μπορεί να μη συμμετέχουν ενεργά στο δίκτυο τη χρονική αυτή στιγμή. Παρόλα αυτά μηνύματα αποστέλλονται σε κάθε κόμβο για τη διατήρηση της γνώσης της τοπολογίας. Παρακάτω παρουσιάζονται δύο από τα πιο πετυχημένα τέτοια πρωτόκολλα το DSDV και το OLSR.

1.4.1.1 Destination-Sequenced Distance Vector (DSDV)

Το πρωτόκολλο αυτό βασίζεται στον αλγόριθμο Bellman-Ford [13]. Το πρόβλημα του αλγορίθμου αυτού είναι πως κάτω από ορισμένες συνθήκες ένας κόμβος μπορεί να αποσυνδεθεί από το δίκτυο και τα πακέτα που προορίζονταν για αυτόν να κυκλοφορούν διαρκώς στο δίκτυο για πάντα χωρίς να βρίσκουν ποτέ τον παραλήπτη:

Εικόνα 1.3 Πρόβλημα επαναληπτικής κυκλικής κίνησης πακέτων

Στο παραπάνω παράδειγμα, όλοι οι κόμβοι αρχικά διαθέτουν πλήρεις πίνακες δρομολόγησης. Ο κόμβος Β γνωρίζει ότι η απόσταση από τον Α είναι 1, ο κόμβος Γ ότι είναι 2 και ο κόμβος Δ ότι είναι 3. Η σύνδεση μεταξύ Α και Β κόμβου ξαφνικά διακόπτεται. Στη συνέχεια καταφθάνει ένα πακέτο στον κόμβο Β με προορισμό τον Α. Ο Β γνωρίζει ότι δεν είναι συνδεδεμένος πλέον με τον Α, αλλά βλέπει ότι ο κόμβος Γ δηλώνει (εσφαλμένα βέβαια) ότι έχει απόσταση 2 από τον Α. Ο κόμβος Β θεωρεί ότι ο Α συνδέθηκε στον Γ και η παρεξήγηση αυτή μεταξύ κόμβων συνεχίζεται για πάντα καθώς ο ένας κόμβος θεωρεί ότι ο Α συνδέθηκε στο γειτονικό του.

Το παραπάνω πρόβλημα που ονομάζεται count-to-infinity αντιμετωπίζεται από τον DSDV με τη χρήση sequence number.

Ο πίνακας που διατηρεί ο DSDV σε κάθε κόμβο περιέχει για κάθε άλλο κόμβο:

α) Την IP διεύθυνση του κάθε κόμβου του δικτύου
β) Την απόσταση σε κόμβους
γ) Σε ποιον από τους γειτονικούς κόμβους πρέπει να απευθυνθεί για επικοινωνία

Για την ενημέρωση των πινάκων δρομολόγησης δύο τύποι πακέτων χρησιμοποιούνται. Το full dump σημαίνει την ριζική ανανέωση εκ του μηδενός του πίνακα, ενώ το incremental update αφορά μόνο μικρές αλλαγές. Το full dump γίνεται όταν ένας κόμβος αλλάζει ριζικά

θέση ή αν ο κόμβος συνδέεται για πρώτη φορά στο δίκτυο και απαιτεί ιδιαίτερο bandwidth. Το incremental update από την άλλη είναι το πλέον χρησιμοποιούμενο πακέτο και έχει πολύ μικρό overhead στο δίκτυο. Τα παραπάνω εφιστούν ιδανικό το πρωτόκολλο DSDV σε δίκτυα όπου η κινητικότητα των κόμβων είναι σχετικά μικρή.

1.4.1.2 Optimized Link State Routing (OLSR)

Το OLSR είναι και αυτό ένα pro-active πρωτόκολλο και έχει βασιστεί στο επιτυχημένο OSPF πρωτόκολλο, άρα στον αλγόριθμο του Dijkstra. Το OLSR ελαχιστοποιεί την επιβάρυνση του δικτύου από την κίνηση πολυάριθμων μηνυμάτων ελέγχου, χρησιμοποιώντας μονάχα επιλεγμένους κόμβους (τους επονομαζόμενους MPRs) για την αναμετάδοση των μηνυμάτων ελέγχου.

Τα χαρακτηριστικό του γνώρισμα είναι ότι σχεδιάζει τους χάρτες δρομολόγησης βάση του packet loss και του latency, και όχι βάση του αριθμού των hops που είναι και το πλέον σύνηθες για αρκετά πρωτόκολλα δυναμικής δρομολόγησης. Αυτό θα πει ότι για να φτάσει σε ένα προορισμό θα επιλέξει την πιο γρήγορη διαδρομή και όχι αυτή που έχει τα λιγότερα hops (ενδιάμεσους κόμβους), όπως κάνει το απλό BGP δηλαδή.

Η επικοινωνία μεταξύ των δρομολογητών γίνεται μέσω UDP broadcasts και σε κάθε πακέτο εμπεριέχεται μια ομάδα από OLSR μηνύματα. Το κάθε ένα από αυτά τα μηνύματα περιέχει πληροφορίες δρομολόγησης αλλά και μια παράμετρο σχετικά με τον χρόνο εγκυρότητας. Αν ο χρόνος αυτός περάσει τότε οι πληροφορίες απορρίπτονται. Το OLSR χρησιμοποιώντας τους MPR είναι ιδανικό για μεγάλα και πυκνά δίκτυα όπου μεγάλος αριθμός κόμβων κινούνται.

1.4.2 Πρωτόκολλα λειτουργίας κατά παραγγελία (on-demand)

Η εναλλακτική προσέγγιση είναι τα πρωτόκολλα κατά παραγγελία (on-demand). Τα πρωτόκολλα που ανήκουν στην κατηγορία αυτή εντοπίζουν τις πιθανές δρομολογήσεις μόνο όταν αυτές είναι απαραίτητες. Όταν μια αποστολή δεδομένων πρέπει να ξεκινήσει τα πακέτα που παράγονται τοποθετούνται προσωρινά σε ένα buffer και ταυτόχρονα ξεκινά μια διαδικασία αναζήτησης της διαδρομής που θα ακολουθηθεί. Τα δεδομένα ρέουν κανονικά από τον αποστολέα στον παραλήπτη μέσω της διαδρομής αυτής μέχρι η διαδρομή, λόγω της κίνησης των κόμβων, να διασπαστεί. Στην περίπτωση αυτή, μια νέα διαδρομή αναζητιέται από το πρωτόκολλο. Τα πιο γνωστά πρωτόκολλα κατά παραγγελία στα Ad Hoc δίκτυα είναι τα: AODV, DSR και το TORA.

1.4.2.1 Ad hoc On-demand Distance Vector (AODV)

Το πρωτόκολλο δρομολόγησης AODV χρησιμοποιεί την υλοποίηση του DSDV, βελτιώνει τη λειτουργία του και χρησιμοποιεί πολύ λιγότερα broadcasts, καθώς ενημερώνει τους πίνακες δρομολόγησης μόνο με τις πληροφορίες των διαδρομών που πραγματικά χρειάζονται.

Στο πρωτόκολλο AODV, το δίκτυο παραμένει “σιωπηλό” έως ότου απαιτηθεί μια νέα σύνδεση. Σε αυτό το σημείο ο κόμβος του δικτύου που χρειάζεται μια νέα σύνδεση μεταδίδει αίτημα νέας σύνδεσης. Οι υπόλοιποι κόμβοι έπειτα διαβιβάζουν αυτό το μήνυμα,

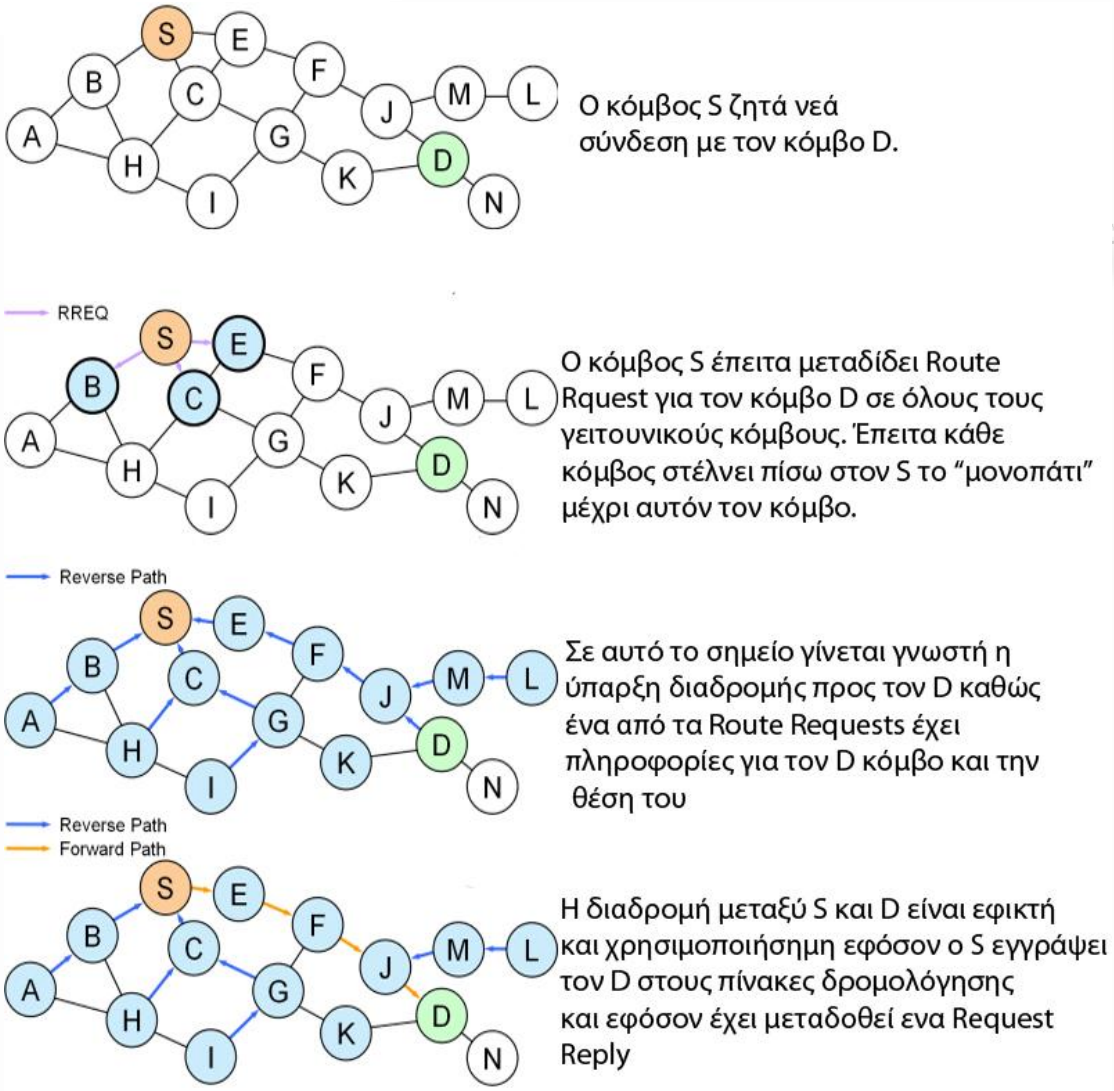
και καταγράφουν τον κόμβο από τον οποίο το έλαβαν. Όταν κάποιος κόμβος λάβει το συγκεκριμένο μήνυμα και γνωρίζει μια διαδρομή προς τον επιθυμητό κόμβο, στέλνει ένα μήνυμα προς τον αιτηθέντα κόμβο μέσω μιας προσωρινής διαδρομής. Έπειτα πραγματοποιείται η σύνδεση χρησιμοποιώντας την διαδρομή με τις λιγότερες "αναπηδήσεις" (hops) σε σχέση με άλλους κόμβους. Να σημειωθεί πως οι αχρησιμοποίητες εγγραφές στους πίνακες δρομολόγησης διαγράφονται μετά από κάποιο συγκεκριμένο χρονικό διάστημα. Στην περίπτωση στην οποία αποτυγχάνει μία σύνδεση, αποστέλλεται ένα μήνυμα λάθους δρομολόγησης πίσω στον κόμβο που ζητά σύνδεση και η διαδικασία επαναλαμβάνεται.

Το AODV πρωτόκολλο είναι ιδιαίτερα πολύπλοκο και ένα μεγάλο μέρος της πολυπλοκότητας του πρωτοκόλλου οφείλεται στην προσπάθεια μείωσης των μεταδιδόμενων μηνυμάτων, έτσι ώστε να συντηρείται σταθερή η χωρητικότητα του δικτύου.

Για παράδειγμα, κάθε αίτημα για μια διαδρομή έχει έναν αριθμό ακολουθίας. Οι κόμβοι χρησιμοποιούν αυτόν τον αριθμό ακολουθίας έτσι ώστε να μην επαναλαμβάνουν τα αιτήματα διαδρομών που έχουν ήδη δοθεί.

Το κύριο πλεονέκτημα του AODV είναι ότι δεν δημιουργεί πρόσθετη κίνηση στο δίκτυο για την επικοινωνία των συνδέσεων. Επίσης αυτού του είδους η δρομολόγηση είναι απλή και δεν απαιτεί πολύ μνήμη ή υπολογιστική ισχύ. Εντούτοις το AODV απαιτεί περισσότερο χρόνο προκειμένου να δημιουργηθεί μια νέα σύνδεση, και η αρχική επικοινωνία για να δημιουργηθεί μια διαδρομή μπορεί μερικές φορές να είναι πιο απαιτητική από μερικές άλλες προσεγγίσεις

Το πρωτόκολλο δρομολόγησης AODV χρησιμοποιεί, όπως προαναφέρθηκε, μια on-demand προσέγγιση για την εύρεση των διαδρομών. Δηλαδή μια διαδρομή καθιερώνεται μόνο όταν απαιτηθεί από κάποιον κόμβο. Υιοθετεί τους "αριθμούς ακολουθίας προορισμού" για να προσδιορίσει την πιο πρόσφατη διαδρομή προς έναν συγκεκριμένο κόμβο. Η μεγαλύτερη διαφορά μεταξύ AODV και του DSR είναι ότι τα πακέτα που μεταβιβάζονται σε ένα δίκτυο βασισμένο στο DSR διαθέτουν πληροφορίες για την πλήρη πορεία τους προς τον προορισμό. Εντούτοις, στο AODV, ο κόμβος πηγής και οι ενδιάμεσοι κόμβοι αποθηκεύουν πληροφορίες για τους επόμενους κόμβους που αντιστοιχούν σε κάθε ροή μετάδοσης δεδομένων.



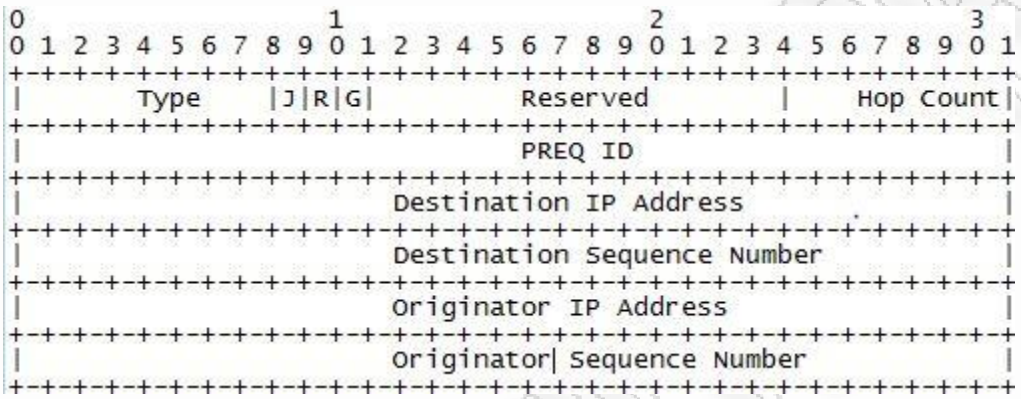
Εικόνα 1.4 Διαδικασία δημιουργίας νέας σύνδεσης μέσω του AODV πρωτοκόλλου

Σε ένα on-demand πρωτόκολλο δρομολόγησης, ο κόμβος που αιτείται νέας σύνδεσης πλημμυρίζει το δίκτυο με πακέτα "RouteRequest", εφόσον δεν υπάρχει διαθέσιμη διαδρομή για τον επιθυμητό προορισμό. Με μια τέτοια ενέργεια, το πιθανότερο είναι ο αρχικός κόμβος να λάβει πολλαπλές διαδρομές για τον τελικό κόμβο, από ένα ενιαίο RouteRequest. Η μεγαλύτερη διαφορά μεταξύ AODV και των άλλων on-demand πρωτοκόλλων δρομολόγησης, είναι ότι χρησιμοποιεί έναν "αριθμό ακολουθίας προορισμού" (DestSeqNum), για να καθορίσει την πιο πρόσφατη πορεία προς τον προορισμό. Ένας κόμβος ενημερώνει τις πληροφορίες σχετικά με τις διαδρομές που διαθέτει, μόνο εάν η τιμή του DestSeqNum του τρέχοντος λαμβανόμενου πακέτου είναι μεγαλύτερη από την τελευταία αποθηκευμένη τιμή DestSeqNum στον κόμβο.

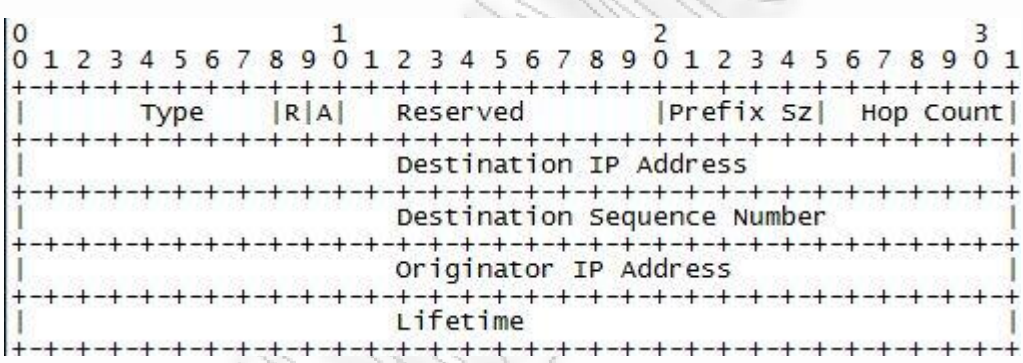
Ένα RouteRequest φέρει τα εξής:

- ταυτότητα πηγής (SrcID)
- ταυτότητα προορισμού (DestID)

- αριθμό ακολουθίας πηγής (SrcSeqNum)
- αριθμό ακολουθίας προορισμού (DestSeqNum)
- ταυτότητα μετάδοσης (BcastID)
- χρόνο ζωής (TTL)



Εικόνα 1.5 Δομή ενός RREQ πακέτου



Εικόνα 1.6 Δομή ενός RREP πακέτου

Η μεταβλητή DestSeqNum αντιπροσωπεύει την "φρεσκάδα" της διαδρομής που λαμβάνεται από την πηγή. Όταν ένας ενδιάμεσος κόμβος λάβει ένα RouteRequest, είτε μεταδίδει και αυτός RouteRequest προς επόμενο κόμβο, είτε προετοιμάζει ένα RouteReply, εάν έχει έγκυρη διαδρομή προς τον αρχικό προορισμό. Η πιστότητα μιας διαδρομής στον ενδιάμεσο κόμβο, καθορίζεται με τη σύγκριση του αριθμού ακολουθίας του ενδιάμεσου κόμβου, με τον αριθμό ακολουθίας προορισμού στο πακέτο RouteRequest.

Εάν ένα RouteRequest ληφθεί πολλές φορές, το οποίο υποδεικνύεται από τις τιμές των BcastID-SrcID, τότε οι διπλοεγγραφές απορρίπτονται. Όλοι οι ενδιάμεσοι κόμβοι που έχουν έγκυρες διαδρομές προς τον προορισμό, είτε ο ίδιος ο κόμβος προορισμού, επιτρέπεται να στείλουν πακέτα RouteReply προς την πηγή.

Όταν ένας κόμβος λάβει ένα πακέτο RouteReply, αποθηκεύει στο πακέτο αυτό πληροφορίες για τον προηγούμενο κόμβο από τον οποίο το πακέτο παραλήφθηκε,

προκειμένου να διαβιβαστούν στον επόμενο κόμβο και ούτε καθεξής, έτσι ώστε να δημιουργηθεί η διαδρομή μεταξύ πηγής και προορισμού.

1.4.2.2 Dynamic Source Routing (DSR)

Το πρωτόκολλο DSR βασίζεται σε μια μεθοδολογία που είναι γνωστή ως source routing [14]. Στη μεθοδολογία αυτή η δρομολόγηση ενός πακέτου γίνεται στην πηγή (source) και τοποθετούνται πληροφορίες με τις διευθύνσεις του κάθε διαδοχικού κόμβου από όπου το πακέτο αυτό θα περάσει μέχρι να φτάσει στον προορισμό του, στην επικεφαλίδα του.

Τα Ad Hoc δίκτυα που χρησιμοποιούν το πρωτόκολλο DSR λειτουργούν σε promiscuous mode. Έτσι κάθε κόμβος μέσα από τον οποίο περνάει ένα πακέτο, μπορεί να διαβάσει τις πληροφορίες που περιέχονται στην επικεφαλίδα του, ώστε να ενημερώσει την cache μνήμη του κόμβου τοποθετώντας πληροφορίες δρομολόγησης για μελλοντική χρήση.

Το DSR διαθέτει μηχανισμούς ανεύρεσης διαδρομών και διόρθωσης τους, σε περίπτωση που η τοπολογία αλλάξει, κάτι το οποίο επιτυγχάνεται με τον παρακάτω μηχανισμό: Κάθε κόμβος που επιβεβαιώνει ότι το πακέτο έφτασε στον παραλήπτη, αποστέλλει μήνυμα επιβεβαίωσης, σε διαφορετική περίπτωση το πακέτο ξαναστέλνεται. Παρά την μεγάλη επιτυχία του, το πρωτόκολλο αυτό απαιτεί πολλές πληροφορίες να αποθηκεύονται στις επικεφαλίδες των πακέτων, δημιουργώντας μεγάλο overhead στο δίκτυο.

1.4.3 Χρήση πρωτοκόλλων στο Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών (AWMN)

Το Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών είναι ένα πεδίο όπου μπορεί κανείς να πειραματιστεί με πρωτόκολλα δρομολόγησης και να ερευνήσει την αποτελεσματικότητά τους. Αποτελείται από σταθερούς κατά κύριο λόγο κόμβους και άρα δεν μπορεί να χαρακτηριστεί ως Ad Hoc δίκτυο. Το χαρακτηριστικό που διαθέτει το δίκτυο αυτό, είναι ότι οι κατευθυντικές ή πολυκατευθυντικές συνδέσεις ανάμεσα στους κόμβους που απαρτίζουν το δίκτυο αυτό μεταβάλλονται πολύ συχνά. Αυτό μπορεί να γίνει είτε γιατί λόγω καιρικών συνθηκών ή παρεμβολών στην ελεύθερη μπάντα των 2.4GHz, αρκετές ασύρματες ζεύξεις αδρανοποιούνται συχνά για λίγες ώρες. Επίσης η συντήρηση, αναβάθμιση των κόμβων, αλλά ακόμα και διακοπές ρεύματος σε περιοχές του λεκανοπεδίου της Αττικής μεταβάλλουν διαρκώς την τοπολογία του δικτύου.

Η χρήση δυναμικών πρωτοκόλλων δρομολόγησης είναι απαραίτητη στο δίκτυο αυτό που φέρει χαρακτηριστικά Ad Hoc δικτύου. Πέρα από παραλλαγές πρωτοκόλλων που έχουν σχεδιαστεί για σταθερά δίκτυα όπως BGP και OSPF, το OLSR πρωτόκολλο έχει χρησιμοποιηθεί με επιτυχία σε μέρη του δικτύου για ερευνητικούς σκοπούς. Η συνεργασία του πρωτοκόλλου αυτού με το BGP έχει επιτευχθεί και τα αποτελέσματα της σχετικής έρευνας [16] είναι: «*το μεγαλύτερο ίσως πρόβλημα του OLSR (και γενικά κάθε πρωτόκολλο που παίζει σε IGP θέση) έρχεται όταν το confederation που ελέγχεται από το OLSR σπάσει σε δύο μέρη και διαφημιστεί δύο φορές στους EGP πίνακες δρομολόγησης του ευρύτερου δικτύου. Τότε το ένα τμήμα του Confederation δε θα μπορεί να επικοινωνήσει απευθείας με*

το άλλο. Για αυτό το πρόβλημα, μόνη λύση είναι τα πολλαπλά links εντός του confederation σε ρόλο back-up.»

Κεφάλαιο 2

Χαρακτηριστικά ασφαλείας σε δίκτυα Ad-Hoc

2.1 Εισαγωγή

Τα θέματα ασφάλειας που αφορούν τα παραδοσιακά δίκτυα αφορούν και τα δίκτυα Ad Hoc. Από τη φύση τους όμως τα δίκτυα Ad Hoc (αποτελούν αυτό-οργανωμένα δίκτυα) δημιουργούν πολλούς νέους προβληματισμούς σχετικά με την ασφάλεια τους. Πως μπορεί ένας κόμβος να πιστοποιήσει ότι είναι πράγματι αυτός που ισχυρίζεται ότι είναι, όταν κινείται, συνδέεται και αποσυνδέεται σε δίκτυα κόμβων με τους οποίους δεν έχει επικοινωνήσει ποτέ;

Ποια είναι η χρήση των Ad Hoc δικτύων σε πραγματικές συνθήκες. Μπορεί να είναι αυτοκίνητα που επικοινωνούν καθώς κινούνται στο οδικό δίκτυο, μπορεί να είναι μηχανήματα σε ένα εργοστάσιο, μπορεί να είναι στρατιωτικές εφαρμογές σε πεδίο μάχης ή μπορεί να είναι ομάδα από laptop που δημιουργεί ένα τέτοιο δίκτυο, με σκοπό να μπορεί να αποκτήσει πρόσβαση σε υπηρεσίες ή στο Ιντερνέτ (περίπτωση one laptop per child).

Πως μπορεί ο ένας κόμβος να εμπιστευτεί τις πληροφορίες που δέχεται από ένα γειτονικό κόμβο; Αυτό που μπορεί να καταλάβει κανείς μετά την ανάγνωση του πρώτου κεφαλαίου της διπλωματικής εργασίας είναι ότι ένα από τα δυσκολότερα σημεία των δικτύων αυτών είναι η δρομολόγηση αλλά και η διασφάλιση της ακεραιότητας. Αυτές και πολλές άλλες ερωτήσεις αφορούν αποκλειστικά τα δίκτυα Ad Hoc και θα αναλυθούν στα επόμενα κεφάλαια.

2.2 Ορισμός της ασφάλειας στα Ad-Hoc δίκτυα

Τα χαρακτηριστικά ασφαλείας που πρέπει να διαθέτει ένα Ad Hoc δίκτυο είναι επιγραμματικά τα εξής:

1. **Διαθεσιμότητα** (Availability): Ακόμα και στην περίπτωση που μια επίθεση ενάντια στους πόρους του δικτύου (denial of service attack) λαμβάνει χώρα, το δίκτυο θα πρέπει να παραμένει διαθέσιμο και λειτουργικό. Στην πράξη αυτό είναι πραγματικά δύσκολο, ειδικά αν αναλογιστεί κανείς όλα τα επίπεδα στα οποία μπορεί να συμβεί μια τέτοια επίθεση: α) σε physical επίπεδο με δημιουργία παρεμβολών μέσω jammers στις συχνότητες λειτουργίας των ασύρματων ζεύξεων, β) σε επίπεδο δρομολόγησης (network layer), επιθέσεις που θα αναλυθούν εκτενέστερα στη συνέχεια, γ) σε επίπεδο εφαρμογών και υπηρεσιών.
2. **Εμπιστευτικότητα** (Confidentiality): Οι πληροφορίες που μεταδίδονται δεν θα πρέπει να μπορούν να υποκλαπούν από τους κόμβους που συμμετέχουν στην αναμετάδοση των ενδιάμεσων πακέτων. Επιπροσθέτως από ότι συμβαίνει σε άλλα δίκτυα, στα Ad Hoc δίκτυα ακόμα και η γνώση της θέσης ενός κόμβου μπορεί να είναι εμπιστευτική, οπότε απαιτείται πολλές φορές εμπιστευτικότητα ακόμα και σχετικά με τις πληροφορίες δρομολόγησης!
3. **Ακεραιότητα** (Integrity): Τα δεδομένα που αποστέλλονται θα πρέπει να φτάνουν στον παραλήπτη χωρίς να έχουν μετατραπεί κακόβουλα ή μη.
4. **Πιστοποίηση** (Authentication): Κάθε κόμβος θα πρέπει να γνωρίζει πιστοποιημένα την ταυτότητα του κάθε κόμβου με τον οποίο έχει συνδεθεί. Όταν κάποιο authentication scheme δεν βρίσκεται σε λειτουργία, ένα κακόβουλος χρήστης μπορεί να προσποιηθεί ότι ο κόμβος του είναι κάποιος άλλος (το αντίστοιχο της πλαστοπροσωπίας) και να αποκτήσει πρόσβαση σε δεδομένα και υπηρεσίες στα οποία δεν θα έπρεπε να είχε πρόσβαση.
5. **Μη άρνηση μετάδοσης** (Non-Repudiation): Ένας κόμβος μπορεί να αρνείται να αποστείλει πακέτα που προορίζονται σε γειτονικό του κόμβο, δημιουργώντας πρόβλημα στο δίκτυο. Με κάποιο μηχανισμό τέτοιοι απομονωμένοι κόμβοι θα πρέπει να μπορούν να εντοπιστούν.

2.3 Κύριες δυσκολίες στην παροχή ασφάλειας

Πρωταρχική δυσκολία στην παροχή ασφάλειας σε δίκτυα Ad Hoc αποτελεί το μέσο επικοινωνίας που αποτελείται από ασύρματες ζεύξεις. Μια σειρά από επιθέσεις μπορούν να λάβουν χώρα, συμπεριλαμβανομένων και των: παθητική υποκλοπή δεδομένων (passive eavesdropping), ενεργή πλαστοπροσωπία, επανεκπομπή πακέτων και αλλοίωση πακέτων.

Η παθητική υποκλοπή δεδομένων μπορεί να γίνει με την τοποθέτηση ενός μη ενεργού κόμβου στην εμβέλεια του Ad Hoc δικτύου και στη συνέχεια μέσω της καταγραφής των πληροφοριών δρομολόγησης αλλά και των δεδομένων μπορεί κανείς να διασπάσει την εμπιστευτικότητα της επικοινωνίας, αλλά και να αποκτήσει γνώσεις σχετικά με την τοπολογία και τη θέση των κόμβων. Μάλιστα όλα αυτά χωρίς να μπορεί κανείς να εντοπίσει τον επιτιθέμενο, καθώς ο κόμβος που συμμετέχει στην επίθεση δεν αποστέλλει καμία πληροφορία.

Οι ενεργητικές επιθέσεις από την άλλη μπορούν να αφαιρέσουν σημαντικά πακέτα από το δίκτυο ή να εισάγουν πακέτα που περιέχουν μια σειρά λανθασμένων πληροφοριών, που σκοπό έχουν την αποδιοργάνωση του δικτύου. Ενεργητική είναι και η επίθεση πλαστοπροσωπίας, που σκοπό έχει την λήψη δεδομένων που δεν αποστάλθηκαν εξ αρχής για τον κόμβο αυτό, αλλά για κάποιον άλλο. Σε κάθε περίπτωση μηχανισμοί ασφαλείας μπορούν να τεθούν σε λειτουργία, ώστε τέτοιοι κόμβοι να εντοπίζονται και να απομακρύνονται από το δίκτυο.

Επιπροσθέτως, σε στρατιωτικές εφαρμογές των Ad Hoc δικτύων, μπορεί ο αντίπαλος να αποκτήσει πρόσβαση σε έναν κόμβο και να ξεκινήσει μια επίθεση από το εσωτερικό του δικτύου, με σκοπό την καταστροφή του. Έτσι οι μηχανισμοί κρυπτογράφησης με χρήση πιστοποιητικών ασφαλείας δεν είναι επαρκείς για τα Ad Hoc δίκτυα. Τα δίκτυα αυτά θα πρέπει να διαθέτουν αποκεντρωμένα και κατανεμημένα συστήματα ανίχνευσης εισβολέων που να αντιδρούν συντονισμένα σε κάθε περίπτωση όπου ύποπτη συμπεριφορά παρατηρείται, αποκλείοντας διαρκώς τους κακόβουλους κόμβους από το δίκτυο. Τέλος ένα Ad Hoc δίκτυο μπορεί να αποτελείται από λίγους μέχρι και εκατοντάδες κόμβους. Έτσι οι κατανεμημένοι μηχανισμοί ασφαλείας θα πρέπει να μπορούν να λειτουργούν σε μεγάλης κλίμακας δίκτυα χωρίς να τα επιφορτίζουν ιδιαίτερα.

Οι παραπάνω περιπτώσεις αποτελούν συγκεντρωτικά το έναυσμα της διπλωματικής αυτής εργασίας όπου θα παρουσιαστούν τα ευρήματα ερευνητικών μελετών στα ζητήματα αυτά.

2.4 Ενεργητικές (active) επιθέσεις

Οι παθητικές επιθέσεις στο δίκτυο δεν μπορούν να εντοπιστούν και για αυτό δεν θα μελετηθούν περισσότερο. Οι ενεργητικές όμως επιθέσεις αφήνουν ίχνη σε ένα δίκτυο, τα οποία αν συνεργατικά οι κόμβοι παρακολουθήσουν προσεκτικά, μπορούν να καταλήξουν σε ένα ασφαλές συμπέρασμα σχετικά με την προέλευση μιας επίθεσης. Παρακάτω παρουσιάζονται οι κυριότερες κατηγορίες ενεργητικών επιθέσεων:

- **Μαύρη τρύπα**: Σε αυτού του είδους την επίθεση, ένας κακόβουλος κόμβος παρακολουθεί τα πακέτα που περνάν μέσα από αυτόν και αποστέλλει ψευδείς πληροφορίες δρομολόγησης στους γειτονικούς κόμβους ότι βρίσκεται ιδιαίτερα κοντά στους παραλήπτες των μηνυμάτων. Αυτή η επίθεση μπορεί να υλοποιηθεί εύκολα για το πρωτόκολλο AODV. Από την στιγμή που ο κόμβος αυτός εξαναγκάσει όλη η επικοινωνία που απευθύνεται σε έναν άλλο κόμβο να περνάει μέσα από αυτόν, τότε υπάρχουν οι παρακάτω επιλογές στον επιτιθέμενο: Μπορεί να μην προωθεί κανένα πακέτο στον πραγματικό παραλήπτη κάνοντας ουσιαστικά επίθεση denial-of-service, μπορεί να συνεχίζει να δίνει λανθασμένες πληροφορίες δρομολόγησης στο δίκτυο με σκοπό να το αποδιοργανώσει ή μπορεί να ξεκινήσει μια επίθεση τύπου man-in-the-middle.
- **Υπερχείλιση πινάκων δρομολόγησης** (routing table overflow): Σε αυτού του τύπου την επίθεση, ο επιτιθέμενος δημιουργεί διαρκώς δρομολόγια για κόμβους που στην πραγματικότητα δεν υπάρχουν στο δίκτυο. Τα proactive πρωτόκολλα είναι πιο ευπαθή σε αυτή την επίθεση και ο επιτιθέμενος μπορεί να δημιουργήσει τεράστια προβλήματα στο δίκτυο τοποθετώντας ακόμα και χιλιάδες πλαστές δρομολογήσεις.

Ένα reactive πρωτόκολλο όπως το AODV είναι πιο δύσκολο να ξεγελαστεί, καθώς πρέπει να υπάρχει τόσο εικονικός αποστολέας, όσο και εικονικός παραλήπτης για να δημιουργηθεί η ανάγκη έναρξης διαδικασιών δρομολόγησης.

- **Κατανάλωση πόρων** (Resource consumption): Σε αυτού του είδους την επίθεση ο επιτιθέμενος ζητά διαρκώς πληροφορίες δρομολόγησης από το δίκτυο, ώστε οι υπόλοιποι κόμβοι να παραμένουν διαρκώς ενεργοί, καταναλώνοντας τόσο την μπαταρία όσο και εύρος ζώνης (bandwidth).
- **Καταστροφή πληροφοριών δρομολόγησης**: Ενώ κάθε κόμβος πρέπει να συμμετέχει στην διαδικασία δρομολόγησης, ένας κόμβος μπορεί να καταστρέφει πληροφορίες δρομολόγησης (επιλέγοντας να μην προωθεί συγκεκριμένες πληροφορίες ή επιλέγοντας να προωθεί μόνο πληροφορίες δρομολόγησης που εξυπηρετούν τις δικές του ανάγκες). Μια τέτοια επίθεση μπορεί ακόμα και να διχοτομήσει ένα δίκτυο σε δύο ή περισσότερα υποδίκτυα.
- **Γνωστοποίηση τοποθεσίας** (location disclosure): Ο επιτιθέμενος κατά τη διάρκεια της επίθεσης αυτής αποστέλλει πακέτα τύπου ICMP διαδοχικά σε κοντινούς και κατόπιν σε πιο απομακρυσμένους κόμβους. Το κάθε πακέτο ICMP διαθέτει μια μεταβλητή που ονομάζεται time-to-live. Κάθε φορά που ένα πακέτο ICMP περνάει από έναν κόμβο, η τιμή του time-to-live μικραίνει κατά ένα. Όταν η τιμή μηδενιστεί το πακέτο αυτό σταματά να προωθείται. Το ICMP πρωτόκολλο απαιτεί την αποστολή πακέτου επιβεβαίωσης (acknowledgment). Χρησιμοποιώντας την λειτουργία του ICMP ο επιτιθέμενος μπορεί να σχηματίσει μια αρκετά καλή εικόνα της τοπολογίας ενός δικτύου. Αν μάλιστα γνωρίζει την πραγματική θέση ορισμένων από τους κόμβους (γεωγραφικές συντεταγμένες) τότε μπορεί με σχετική ακρίβεια να υπολογίσει την πραγματική γεωγραφική θέση πολλών από τους υπόλοιπους κόμβους.

Παρακάτω ακολουθεί ένας επιγραμματικός πίνακας με αρκετά άλλα είδη επιθέσεων που μπορούν να συμβούν:

Επίθεση στις πληροφορίες κατά τη διάδοση.	Οι πληροφορίες μπορούν να μεταλλαχθούν, να τροποποιηθούν, να αποσταλούν περισσότερο από μια φορές, ή ακόμα και να διαγραφούν.
Hello flood	Ένας επιτιθέμενος με ισχυρή συσκευή εκπομπής ράδιο στέλνει πολλά Hello πακέτα, ακόμα και σε πολύ απομακρυσμένους κόμβους, ενημερώνοντας τους ότι είναι γειτονικός τους και έτσι αποκτά κομβικό ρόλο στο σύνολο του δικτύου.
Επίθεση Sylib	Ο επιτιθέμενος δημιουργεί δεκάδες ψευδείς ταυτότητες και τις χρησιμοποιεί ώστε να επηρεάσει το σύνολο του δικτύου. Αν για παράδειγμα ένα Ad-Hoc δίκτυο λειτουργεί δημοκρατικά και περιλαμβάνει 50 κόμβους, ένας κακόβουλος κόμβος μπορεί να δημιουργήσει 50-60 ψευδείς ταυτότητες και να αποκτήσει μέσω αυτών την δυνατότητα να παραπλανεί το σύνολο του δικτύου.

Wormhole επίθεση	Ένας κόμβος δρομολογεί πληροφορίες ανάμεσα σε δύο Ad-Hoc δίκτυα ή δύο μέρη ενός δικτύου, κρατώντας την παρουσία του εντελώς κρυφή.
Επίθεση network partition	Ένας κόμβος με αυτή την επίθεση κατακερματίζει το αρχικό δίκτυο σε μικρότερα υποδίκτυα.
Επίθεση Black Hole	Ο κόμβος καταστρέφει κάθε πληροφορία που προσπαθεί να περάσει μέσα από αυτόν.
Επίθεση Sink Hole	Ο κόμβος καταστρέφει κάθε πληροφορία δρομολόγησης που προσπαθεί να περάσει μέσα από αυτόν.
Selective Forwarding	Ο κόμβος προωθεί μόνο επιλεγμένες πληροφορίες.
Simple Broadcast Flooding	Ο επιτιθέμενος κατακλύζει το δίκτυο με broadcast μηνύματα.
Simple Target Flooding	Ο επιτιθέμενος κατακλύζει ένα συγκεκριμένο κόμβο.
False Identity Broadcast Flooding	Ο επιτιθέμενος κατακλύζει το δίκτυο με broadcast μηνύματα χρησιμοποιώντας ψεύτικη ταυτότητα κάθε φορά.
Misdirection Attack	Ο επιτιθέμενος τροποποιεί την διεύθυνση αποστολής ενός πακέτου σε έναν απομακρυσμένο παραλήπτη.

2.5 Byzantine Failure και ODSBR

Το "*βυζαντινό σφάλμα*" - Byzantine failure, είναι ένα αυθαίρετο σφάλμα που εμφανίζεται κατά τη διάρκεια της εκτέλεσης ενός αλγορίθμου από ένα διανεμημένο σύστημα. Μπορεί να είναι είτε omission failure (αποτυχία παράλειψης, όπως για παράδειγμα αποτυχία λήψης αιτήματος), είτε commission failures, όπως για παράδειγμα λάθος επεξεργασία αιτήματος ή αποστολή λανθασμένου αιτήματος. Όταν εμφανιστεί ένα byzantine fault, το σύστημα μπορεί να αποκριθεί με απρόβλεπτο τρόπο, εκτός αν έχει σχεδιαστεί με την προοπτική της αντοχής στα βυζαντινά σφάλματα

Για να κατανοήσει κανείς το παραπάνω, αρκεί να φέρει στο νου του μια περίπτωση όπου το αποτέλεσμα μιας συνάρτησης αποτελεί εισαγωγή σε μια άλλη. Τότε μικρά λάθη στην πρώτη συνάρτηση είναι πολύ πιθανό να παραγάγουν πολύ μεγαλύτερα λάθη στην δεύτερη. Εάν η δεύτερη συνάρτηση αποτελούσε είσοδο για μια τρίτη, το πρόβλημα θα μπορούσε να γίνει ακόμα μεγαλύτερο.

Σε έναν αλγόριθμο που έχει σχεδιαστεί λαμβάνοντας υπόψη και τις βυζαντινές αποτυχίες (Byzantine fault tolerant), λαμβάνονται διάφορα μέτρα προφύλαξης σε κάθε επιμέρους διαδικασία. Σε αυτή την περίπτωση μια διαδικασία θεωρείται ελαττωματική, όταν έχει σε οποιονδήποτε βαθμό μια αποτυχία. Μια διαδικασία που δεν είναι ελαττωματική θεωρείται αυτόματα σωστή.

Βυζαντινές επιθέσεις πραγματοποιούνται και στα ασύρματα δίκτυα και κυρίως στα Ad-Hoc, στα οποία η ασφάλεια τους είναι μειωμένη. Στην περίπτωση αυτή, βυζαντινές επιθέσεις πραγματοποιούνται από εσωτερικούς κόμβους του δικτύου οι οποίοι έχουν δεχθεί επίθεση και είναι πλέον στον έλεγχο ενός κακόβουλου κόμβου, ο οποίος έχει σκοπό να διαταράξει την ομαλή λειτουργία του δικτύου. Τέτοια παραδείγματα είναι: η δημοσίευση στο δίκτυο λανθασμένων δεδομένων σχετικών με την δρομολόγηση ή ακόμα και η διαγραφή διερχόμενων πακέτων.

2.5.1 Παρουσίαση του ODSBR

Τα Byzantine attacks μπορούν να αντιμετωπιστούν με διάφορους τρόπους όπως η χρήση αλγορίθμων που ελέγχουν την δρομολόγηση του δικτύου, με τροποποιημένα συστήματα ανίχνευσης παρεισφρήσεων αλλά και με ανανεωμένα πρωτόκολλα δρομολόγησης. Ένα τέτοιο πρωτόκολλο είναι το ODSBR (*On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks*), που αποτελεί ένα on-demand πρωτόκολλο δρομολόγησης σε Ad-Hoc δίκτυα, το οποίο σύμφωνα και με αποτελέσματα μερικών συγκρίσεων, παρουσιάζει αυξημένη αποδοτικότητα σε σχέση με άλλα πρωτόκολλα και μεθόδους ενάντια σε βυζαντινές επιθέσεις. Η αυξημένη αποδοτικότητα του ODSBR βασίζεται στο ότι μπορεί να παρακολουθεί πολλαπλούς κόμβους που πραγματοποιούν ταυτόχρονα βυζαντινές επιθέσεις, ενώ παράλληλα δεν περιορίζεται η αποδοτικότητα της ανταλλαγής δεδομένων μεταξύ των κόμβων του δικτύου. Να σημειωθεί πως σκοπός αυτού του κεφαλαίου δεν είναι η εκτενής και σε βάθος ανάλυση του ODSBR αλλά η παρουσίασή του και η σύγκριση του με άλλα.

2.5.2 Δομή του ODSBR

Το ODSBR δεν στοχεύει στην ανίχνευση εισβολών σε χαμηλά επίπεδα του δικτύου, αλλά παρακολουθεί το network layer. Επιπλέον δεν είναι αποδοτικό σε ανοικτά δίκτυα. Υποθέτει δηλαδή πως υπάρχει μια πρόχειρη δικτυακή υποδομή και η σύνδεση στο δίκτυο απαιτεί την χρήση ενός κλειδιού. Θεωρεί επίσης ως εμπιστευόμενα μέλη του δικτύου, μόνο την πηγή και τον προορισμό κάθε φορά. Επιπλέον κάθε κόμβος επικυρώνεται σύμφωνα με *public key-based* τεχνικές, κατά το στάδιο της ανίχνευσης της δρομολόγησης του δικτύου και *symmetric key-based* τεχνικές, στα επόμενα στάδια του ODSBR. Τα μηνύματα που δεν μπορούν να επικυρωθούν απορρίπτονται.

Οποιοσδήποτε ενδιάμεσος κόμβος στην πορεία μεταξύ της πηγής και του προορισμού μπορεί να εκθέσει βυζαντινή συμπεριφορά. Στόχος του πρωτοκόλλου είναι να ανιχνευθεί η βυζαντινή συμπεριφορά και να αποφευχθεί, ή να περιορίσει την επίδρασή της στο δίκτυο.

Βυζαντινή συμπεριφορά καθορίζεται οποιαδήποτε ενέργεια από έναν επικυρωμένο κόμβο του δικτύου που καταλήγει στην διάσπαση ή την διατάραξη της δρομολόγησης του δικτύου. Γενικά οποιαδήποτε ενέργεια που προκαλεί καθυστερήσεις και απώλειες πακέτων.

Αντίθετα από άλλα πρωτόκολλα, το ODSBR δεν χρησιμοποιεί τον αριθμό των κόμβων για την επιλογή μιας διαδρομής. Η μέθοδος αυτή (hop-count) έχει αποδειχθεί ότι δεν είναι το πλέον κατάλληλο μέτρο σύγκρισης για ασύρματα δίκτυα πολλών κόμβων. Η προσέγγιση

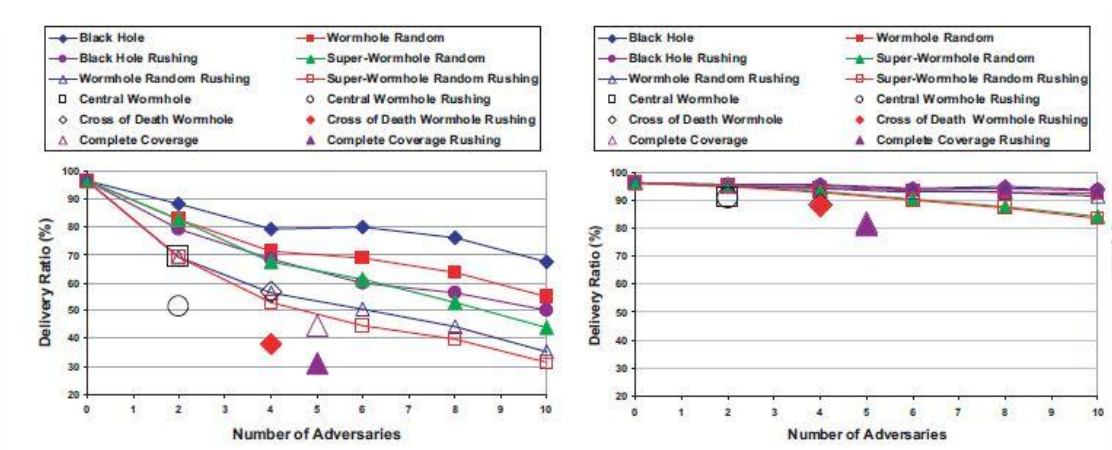
ODSBR είναι να καθορίζει ένα νέο μετρικό το οποίο "συλλαμβάνει" την αξιοπιστία και τη συμπεριφορά μιας διαδρομής, βασιζόμενη στο ιστορικό της. Το μετρικό αντιπροσωπεύεται από μια λίστα με «ζυγισμένες συνδέσεις» όπου χαμηλό βάρος σύνδεσης συνεπάγεται χαμηλή αξιοπιστία. Κάθε κόμβος στο δίκτυο διατηρεί την δική του μοναδική λίστα και την ενημερώνει δυναμικά όταν ανιχνευθεί κάποιο σφάλμα στο δίκτυο. Οι ελαττωματικές συνδέσεις αποφεύγονται, χρησιμοποιώντας ένα ασφαλές πρωτόκολλο ανακάλυψης δρομολόγησης που ενσωματώνει τις λίστες αξιοπιστίας που προαναφέρθηκαν.

Πιο συγκεκριμένα, το ODSBR μπορεί να χωριστεί σε τρία διαδοχικά στάδια, όπου κάθε στάδιο χρησιμοποιεί ως είσοδο την έξοδο από το προηγούμενο στάδιο:

- **Ανακάλυψη διαδρομών - *Route discovery***: Το ODSBR χρησιμοποιεί μεθόδους που εξασφαλίζουν την σίγουρη μετάβαση πακέτων από τον αποστολέα προς τον προορισμό, αλλά και την σίγουρη μετάβαση από τον προορισμό πίσω προς τον αποστολέα. Αυτό πραγματοποιείται με την απαίτηση του ODSBR από κάθε κόμβο, να υπογράφει ψηφιακά κάθε πακέτο που διέρχεται από αυτόν. Σε περίπτωση που αυτή η διαδικασία αποτύχει, τότε αυτόματα ο αντίστοιχος κόμβος απομακρύνεται από το δίκτυο.
- **Ανίχνευση βυζαντινών σφαλμάτων - *Byzantine fault detection*:** Στο συγκεκριμένο στάδιο ανακαλύπτονται οι προβληματικές συνδέσεις στην διαδρομή από την πηγή προς τον προορισμό, χρησιμοποιώντας ως είσοδο στον αλγόριθμο την συγκεκριμένη διαδρομή που έχει ως έξοδο την τυχόν ελαττωματική σύνδεση. Η πηγή απαιτεί κρυπτογραφημένη απόδειξη, ότι τα πακέτα παραδίδονται επιτυχώς και αναλλοίωτα στον προορισμό.
- **Διαχείριση συνδέσεων - *Link weight management*:** Στόχος του πρωτοκόλλου είναι η αποφυγή σφαλμάτων. Αυτό επιτυγχάνεται από το στάδιο ανακάλυψης της δρομολόγησης το οποίο λαμβάνει υπόψη το «βάρος» κάθε σύνδεσης. Επιπλέον, το ODSBR χρησιμοποιεί έναν μηχανισμό αποκατάστασης, που από τη μια πλευρά περιορίζει το μέγεθος ζημίας που προκαλεί κάποια εισβολή ή μια ομάδα επιτιθεμένων, ενώ μειώνει παράλληλα το αντίκτυπο των λανθασμένων μηνυμάτων εισβολής χωρίς να αποσυνδέει κόμβους από το δίκτυο.

2.5.3 Αξιολόγηση του ODSBR

Παραθέτουμε στην συνέχεια κάποια αποτελέσματα τα οποία προέκυψαν από την σύγκριση μεταξύ του πρωτοκόλλου AODV και του ODSBR. Τα αποτελέσματα αποτελούν απόσπασμα από την επίσημη παρουσίαση του ODSBR [17]. Από το παρακάτω διάγραμμα γίνεται σαφές πως το πρωτόκολλο ODSBR παρουσιάζει αυξημένη αποδοτικότητα σε byzantine failures. Στην πραγματικότητα μόνο δύο βυζαντινές επιθέσεις κατάφεραν να μειώσουν την αποδοτικότητα της παράδοσης δεδομένων στο 51%.



Εικόνα 2.1 Σύγκριση απόδοσης μεταξύ AODV και ODSBR σε Byzantine Attacks

2.6 Προτεινόμενες πολιτικές ασφάλειας (security schemas)

Οι κύριες προσεγγίσεις σχετικά με πολιτικές ασφάλειας στα δίκτυα Ad Hoc αφορούν α) τη χρήση συστημάτων ανίχνευσης εισβολέων ή β) την ανάπτυξη νέων πρωτοκόλλων δρομολόγησης όπου η ασφάλεια θα αποτελεί πρωταρχικό συστατικό την υλοποίησης τους.

Τα συστήματα ανίχνευσης εισβολέων σε δίκτυα που αυτό-οργανώνονται αποτελούν ένα νέο πεδίο ερευνητικής δραστηριότητας και πολλά προβλήματα ακόμα δεν έχουν αντιμετωπιστεί επιτυχώς. Από την άλλη, τα ασφαλή πρωτόκολλα δρομολόγησης που προτείνονται βασίζονται κυρίως στα υπάρχοντα πρωτόκολλα όπως το AODV και το DSR. Οι προτεινόμενες αυτές πολιτικές ασφαλείας παρουσιάζονται στη συνέχεια.

2.6.1 Ασφάλεια πρωτοκόλλων δρομολόγησης

Στην προσέγγιση αυτή η δημιουργία ασφαλών πρωτοκόλλων δρομολόγησης θεωρείται ότι μπορεί να λύσει τα προβλήματα που παρουσιάζονται στα δίκτυα Ad Hoc. Τα περισσότερα ασφαλή πρωτόκολλα βασίζονται είτε στη χρήση των hash-chains, είτε βασίζονται σε σχέσεις εμπιστοσύνης.

Το πρωτόκολλο **SEAD** (Secure Efficient Ad Hoc Distance Vector) βασίζεται στο DSDV και αξιοποιεί τα hash-chains για να επικυρώσει την αυθεντικότητα, τόσο της σειρά των κόμβων, όσο και των sequence numbers μέσα σε κάθε πακέτο. Για να μπορεί να λειτουργήσει η αυθεντικοποίηση, πρέπει όλοι οι κόμβοι να έχουν συγχρονισμένα ρολόγια ή διαφορετικά να έχουν ένα κοινό μυστικό κλειδί αυθεντικοποίησης. Με τον τρόπο λειτουργίας του, επιτρέπει μεγάλο αριθμό κόμβων να σχηματίσουν ένα Ad Hoc δίκτυο, αλλά αποτρέπει έναν κόμβο να προσποιηθεί ότι είναι ένας άλλος και αποτρέπει και άλλες επιθέσεις.

Το πρωτόκολλο **Ariadne** βασίζεται πάνω στο DSR και προϋποθέτει την ύπαρξη ενός κοινού μυστικού κλειδιού αυθεντικοποίησης ανάμεσα σε κάθε ζευγάρι διασυνδεμένων κόμβων, το οποίο και χρησιμοποιεί για να επικυρώνει την αυθεντικότητα στην πλήρη διαδρομή μεταξύ δύο κόμβων του δικτύου.

Το **SAODV** (Secure Ad Hoc On Demand Distance Vector) προσθέτει μηχανισμούς ασφαλείας στο AODV και χρησιμοποιεί και αυτό κλειδιά κρυπτογράφησης για να διασφαλίσει κάθε

διαδρομή δρομολόγησης μέσω ασύμμετρης κρυπτογραφίας. Απαιτείται βέβαια ένας μηχανισμός διαχείρισης των κλειδιών.

Το **ARAN** (Authenticated Routing for Ad Hoc Networks) πρωτόκολλο ανήκει στη δεύτερη κατηγορία ασφαλών πρωτοκόλλων και απαιτεί σχέσεις εμπιστοσύνης. Για να υπάρχει σχέση εμπιστοσύνης ανάμεσα σε δύο κόμβους θα πρέπει ο κάθε ένας να γνωρίζει το δημόσιο κλειδί του κόμβου επιβεβαίωσης της εμπιστοσύνης.

Το πρωτόκολλο **SAR** (Security-aware Ad Hoc Routing) έχει εντελώς διαφορετική φιλοσοφία. Κάθε κόμβος αποκτά μια τιμή σχετικά με το πόσο ασφαλής και έμπιστος θεωρείται. Έτσι προτιμάται η χρήση μιας διαδρομής που αποτελείται από έμπιστους κόμβους, παρά μια πιο κοντινή διαδρομή. Ένας κόμβος που μόλις συνδέθηκε στο δίκτυο αρχικά δεν θεωρείται έμπιστος. Όσο ο χρόνος περνά η τιμή της ασφάλειας του σταδιακά βελτιώνεται, όσο επιβεβαιώνεται ότι λειτουργεί νομότυπα.

Στο **SRP** (Secure Routing Protocol) ο αποστολέας με τον παραλήπτη δεδομένων δημιουργούν αρχικά ένα μυστικό κλειδί κρυπτογραφίας. Κατόπιν το κλειδί αυτό χρησιμοποιείται από το πρωτόκολλο, σε κάθε ξεχωριστό κόμβο, για να επικυρώνει την σωστή μεταφορά των μηνυμάτων.

2.6.2 Χρήση IDS

Η πρώτη γραμμή άμυνας ενάντια σε οποιαδήποτε επίθεση είναι η απόκρουσή της από το σύστημα. Στην περίπτωση όμως που μια επίθεση δεν μπορεί να αποκρουστεί, το δεύτερο επίπεδο άμυνας είναι ο εντοπισμός του επιτιθέμενου ώστε το σύστημα να μπορεί να αντιδράσει σε αυτή. Για να εντοπιστεί μια επίθεση έναντι είτε του συστήματος, είτε ενός συγκεκριμένου κόμβου, συνήθως χρειάζεται το σύνολο των κόμβων που αποτελούν το δίκτυο να παρακολουθούν προσεκτικά τα δεδομένα που κυκλοφορούν. Στην περίπτωση που ανάρμοστη συμπεριφορά παρατηρηθεί, τότε το δίκτυο μπορεί να ενημερώσει όλους τους κόμβους ώστε τα απαραίτητα αντίμετρα να λειτουργήσουν.

Αρκετοί τύπων συστήματος ανίχνευσης εισβολέων υπάρχουν. Ένας τύπος που ονομάζεται **host-based IDS**, λειτουργεί σε κάθε κόμβο του δικτύου ξεχωριστά και προσπαθεί να εντοπίσει επιθέσεις που στοχεύουν το συγκεκριμένο κόμβο. Ένας άλλος τύπος που ονομάζεται **network-based IDS**, εκτελείται σε σημεία-κλειδιά ενός δικτύου και παρακολουθεί το σύνολο της δικτυακής κίνησης που προωθείται προς και από το δίκτυο αυτό και συμπερασματικά προσπαθεί να εντοπίσει επιθέσεις που προορίζονται σε οποιαδήποτε κόμβο του δικτύου. Και οι δύο αυτοί τύποι συστημάτων ανίχνευσης εισβολέων είναι αναποτελεσματικοί σε δίκτυα Ad Hoc.

Ένα σύστημα ανίχνευσης εισβολέων μπορεί να επιτελέσει δύο κύριες λειτουργίες. Η πρώτη είναι να αξιοποιήσει **τεχνικές pattern-matching**, όπου τα περιεχόμενα των πακέτων δεδομένων διασταυρώνονται έναντι πληροφοριών από μια βάση δεδομένων που περιέχει δείγματα πακέτων επιτιθέμενων. Αν αναλυθεί μια δικτυακή επίθεση, μπορούν να βρεθούν μοτίβα στα πακέτα που χρησιμοποιούνται στην επίθεση αυτή. Τα μοτίβα αυτά αν χρησιμοποιηθούν μπορούν να προβλέψουν με μεγάλη ακρίβεια ότι μια συγκεκριμένη επίθεση λαμβάνει χώρα. Η τεχνική αυτή όμως μπορεί να εντοπίσει μόνο γνωστές επιθέσεις

που έχουν αναλυθεί διεξοδικά. Η δεύτερη λειτουργία των συστημάτων ανίχνευσης εισβολέων είναι ο **εντοπισμός ανωμαλιών** στο δίκτυο. Σε αυτή τη λειτουργία, το σύστημα ανίχνευσης εισβολέων παρακολουθεί διεξοδικά την κίνηση του δικτύου για μεγάλα χρονικά διαστήματα και καταγράφει στατιστικά σχετικά με τη συνηθισμένη χρήση του δικτύου. Ένα εταιρικό δίκτυο για παράδειγμα μπορεί να είναι εντελώς ανενεργό κατά τη διάρκεια της νύχτας και των αργιών, και τις καθημερινές η κίνηση να απαρτίζεται από Voice Over IP δεδομένα και Web & Email πληροφορίες. Αν ξαφνικά μια ημέρα παρατηρηθεί τεράστια χρήση πακέτων UDP ή ICMP μπορεί κανείς εύκολα να αναρωτηθεί για τις αιτίες της ξαφνικής αυτής αλλαγής χρήσης του δικτύου και σταδιακά να οδηγηθεί σε συμπεράσματα, όπως για παράδειγμα ότι κάποιος υπάλληλος χρησιμοποιεί το πρωτόκολλο torrent για ανταλλαγή ταινιών και λογισμικού ή ότι ένας ιός έχει εισβάλει σε κάποιον υπολογιστή της εταιρίας.

Η παρακολούθηση ανωμαλιών δημιουργεί alarms, συναγερμούς για πιθανή επίθεση και οι συναγερμοί αυτοί ορισμένες φορές είναι σωστοί και ορισμένες λάθος. Η τεχνική αυτή μπορεί να εντοπίσει και επιθέσεις οι οποίες είναι άγνωστες και δεν έχουν αναλυθεί ακόμα. Οπότε, συνήθως κάθε σύστημα ανίχνευσης εισβολέων παρακολουθεί τόσο τα μοτίβα/υπογραφές επιθέσεων όσο και τα στατιστικά της κίνησης του δικτύου, για εντοπισμό ανωμαλιών.

2.7 Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκαν οι κυριότερες απειλές που αντιμετωπίζει ένα δίκτυο Ad Hoc, κυρίως λόγω της διαφορετικότητας του σε σχέση με τα υπόλοιπα δίκτυα. Η υλοποίηση μιας επίθεσης που εκμεταλλεύεται τα κενά ασφαλείας των πρωτοκόλλων δρομολόγησης μπορεί σχετικά εύκολα να υλοποιηθεί. Για τον λόγο αυτό, ένα μεγάλο μέρος της έρευνας σχετικά με τα δίκτυα αυτά, κατευθύνεται προς την κατασκευή ασφαλών πρωτοκόλλων δρομολόγησης. Τα περισσότερα όμως από αυτά τα πρωτόκολλα απαιτούν την εκ προτέρου ύπαρξη σχέσεων εμπιστοσύνης ανάμεσα στους κόμβους, κάτι το οποίο τα καθιστά μη συμβατά για χρήση στα περισσότερα δίκτυα, αλλά άκρως χρήσιμα σε Ad Hoc δίκτυα στρατιωτικής χρήσης ή ρομποτικών συστημάτων που χρησιμοποιούνται για παράδειγμα για τη διάσωση επιζώντων από καταστροφές. Επιπρόσθετα η χρήση κλειδιών κρυπτογράφησης επιβαρύνει τους υπολογιστικούς πόρους και τις ενεργειακές απαιτήσεις των κόμβων.

Από την άλλη η χρήση συστημάτων ανίχνευσης εισβολέων φαίνεται να έχει ιδιαίτερο μέλλον στα δίκτυα Ad Hoc και ο προσεκτικός σχεδιασμός τους και η αποκεντρωμένη λειτουργία τους μπορεί να δώσει ισχύ σε κάθε κόμβο να λειτουργήσει ως «*ένα κύτταρο του ανοσοποιητικού συστήματος του δικτύου*».

Κεφάλαιο 3

Εισαγωγή στα συστήματα ανίχνευσης παρεισφρήσεων

3.1 Εισαγωγή στην ανίχνευση παρεισφρήσεων και το Snort

Για να μπορεί κανείς να κατανοήσει πλήρως τα εξελιγμένα κατανεμημένα συστήματα ανίχνευσης εισβολέων, θα πρέπει πρώτα να αναλύσει την λειτουργία ενός IDS. Το λογισμικό Snort επιλέχθηκε επειδή είναι ανοιχτού κώδικα και διατίθεται δωρεάν για πολλές πλατφόρμες.

Το Snort, κάνει την χρήση κανόνων που είναι αποθηκευμένοι σε αρχεία κειμένων που μπορούν να τροποποιηθούν ακόμα και από έναν συντάκτη κειμένων. Οι κανόνες αυτοί ομαδοποιούνται σε διάφορες κατηγορίες. Οι κανόνες της κάθε κατηγορίας αποθηκεύονται σε ξεχωριστά αρχεία. Αυτά τα αρχεία έπειτα συμπεριλαμβάνονται σε ένα κύριο αρχείο, το snort.conf. Το λογισμικό διαβάζει αυτούς τους κανόνες κατά την εκκίνηση του και διαμορφώνει τις εσωτερικές δομές δεδομένων ή "τις αλυσίδες" προκειμένου στην συνέχεια να εφαρμόσει αυτούς τους κανόνες στα δεδομένα που θα εξετάσει.

Η εύρεση των υπογραφών και η χρήση τους στους κανόνες είναι μια απαιτητική εργασία, δεδομένου ότι όσο περισσότεροι κανόνες χρησιμοποιούνται, τόσο περισσότερη επεξεργαστική ισχύς απαιτείται για να εξεταστούν τα δεδομένα που θα συλλέξει το σύστημα, σε πραγματικό χρόνο. Είναι σημαντικό να εφαρμοστούν τόσες υπογραφές όσες κάποιος χρειάζεται αλλά με όσο το δυνατόν λιγότερους κανόνες. Το Snort έρχεται με ένα πλούσιο σύνολο προκαθορισμένων κανόνων για να ανιχνεύσει την δραστηριότητα παρεισφρήσεων, ενώ δίνεται παράλληλα η δυνατότητα να προστεθούν και άλλοι κανόνες. Υπάρχει επίσης και η δυνατότητα να διαγραφούν – απενεργοποιηθούν μερικοί από τους ενσωματωμένους κανόνες για να αποφευχθούν λανθασμένες ειδοποιήσεις.

3.2 Πολιτική των IDS

Προτού να εγκατασταθεί ένα σύστημα ανίχνευσης παρεισφρήσεων στο δίκτυό, θα πρέπει να υπάρχει μια πολιτική για την ανίχνευση των επιθέσεων και μια πολιτική για τα μέτρα που θα πρέπει να ληφθούν όταν εντοπιστεί μία επίθεση. Μια πολιτική είναι απαραίτητο να «υπαγορεύσει» τους κανόνες του IDS και πώς αυτοί θα εφαρμοστούν. Μία ορθή και γενικευμένη πολιτική των IDS θα πρέπει να περιέχει τουλάχιστον τα ακόλουθα:

1. Ποιος θα ελέγχει το IDS; Ανάλογα με το IDS, οι ειδοποιήσεις διαφέρουν για τις ίδιες επιθέσεις σε ένα σύστημα. Αυτές οι ειδοποιήσεις μπορεί να είναι σε μορφή απλών αρχείων κειμένων, ή μπορεί να είναι περισσότερο περίπλοκες, ή ενσωματωμένες σε συστήματα διαχείρισης όπως σε κάποια βάση δεδομένων OpenView ή MySQL. Παρόλα αυτά απαιτείται κάποιος να ελέγχει την δραστηριότητα των εισβολέων και πρέπει να καθοριστεί ένα αρμόδιο πρόσωπο για αυτήν την δραστηριότητα. Επίσης οι επιθέσεις μπορούν να ελεγχθούν σε πραγματικό χρόνο χρησιμοποιώντας pop-up windows ή web interfaces. Σε αυτήν την περίπτωση οι χρήστες πρέπει να έχουν γνώση για την ερμηνεία και την αντιμετώπιση αυτών των μηνυμάτων.

2. Ποίος θα συντηρεί το σύστημα; Όπως με όλα τα συστήματα, έτσι και με τα IDS πρέπει να καθιερωθούν περιοδικοί έλεγχοι στα συστήματα από αρμόδιους φορείς.

3. Ποιος θα χειρίζεται τις ειδοποιήσεις και πώς;

4. Ποια θα είναι η διαδικασία κλιμάκωσης (επίπεδο 1, επίπεδο 2 και ούτω καθεξής); Η διαδικασία κλιμάκωσης είναι βασική στρατηγική για την αντιμετώπιση μιας επίθεσης. Η πολιτική αυτή επίσης πρέπει να περιγράφει σαφώς ποιες από τις ειδοποιήσεις θα πρέπει να μεταφερθούν σε ανώτερους διαχειριστές.

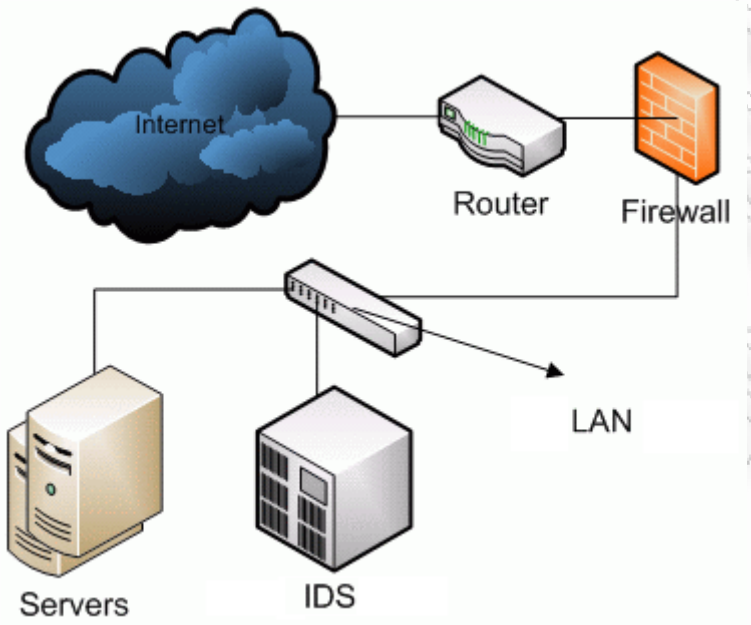
5. Υποβολή αναφορών. Οι εκθέσεις-αναφορές θα πρέπει να δημιουργούνται ανά τακτά χρονικά διαστήματα (κάθε μέρα, εβδομάδα κλπ) προκειμένου να υπάρχει μια πλήρης εικόνα των κινδύνων του συστήματος.

6. Αναπροσαρμογές των υπογραφών (*Signature updates*). Οι επιτιθέμενοι δημιουργούν συνεχώς νέους τύπους επιθέσεων. Αυτές οι επιθέσεις ανιχνεύονται από τα IDS μόνο εάν το σύστημα γνωρίζει τις υπογραφές των νέων αυτών επιθέσεων. Λόγω της συχνής μεταβολής της φύσης των επιθέσεων, πρέπει να ενημερώνεται συχνά το σύστημα ανίχνευσης παραφράσεων με νέες υπογραφές και κανόνες.

3.3 Θέση ενός IDS στην τοπολογία ενός δικτύου

Ανάλογα με την τοπολογία ενός δικτύου, μπορεί κανείς να τοποθετήσει ένα σύστημα ανίχνευσης παρεισφρήσεων σε μία ή περισσότερες θέσεις. Εξαρτάται επίσης από το ποιου τύπου παρεισφρήσεων θέλει κανείς να ανιχνεύσει: εσωτερικές, εξωτερικές ή και τα δύο είδη. Παραδείγματος χάριν, εάν θέλει κανείς να ανιχνεύσει μόνο τις εξωτερικές δραστηριότητες παρείσφρησης και υπάρχει μόνο ένας δρομολογητής που συνδέει το

σύστημα με το διαδίκτυο, τότε η καλύτερη θέση για το IDS είναι ακριβώς "μέσα" στο δρομολογητή ή το firewall. Εάν υπάρχουν πολλαπλές συνδέσεις διαδικτύου, τότε η καλύτερη λύση για να τοποθετηθεί ένα IDS σε κάθε σημείου εισόδου στο διαδίκτυο.



Εικόνα 3.1 Τοποθέτηση του IDS στο σημείο διασύνδεσης του τοπικού δικτύου και του Ιντερνέτ

Εντούτοις, ίσως να χρειάζεται να ανιχνεύονται και οι εσωτερικές επιθέσεις του συστήματος επομένως είναι απαραίτητο να τοποθετηθεί ένα IDS σε κάθε τομέα του δικτύου. Άλλες φορές πάλι ίσως δεν είναι απαραίτητο να τοποθετηθεί ένα σύστημα ανίχνευσης παρεισφρήσεων σε κάθε δικτυακό τομέα, αλλά μόνο στις ευαίσθητες περιοχές του. Αξίζει να σημειωθεί ότι όσο περισσότερα IDS υπάρχουν τόσο περισσότερη εργασία χρειάζεται, καθώς και το ότι το κόστος συντήρησης αυξάνεται.

3.4 Ορολογία συστημάτων παρεισφρήσεων

Προτού προχωρήσουμε στις λεπτομέρειες της ανίχνευσης παρεισφρήσεων και του Snort, θα αναλυθούν μερικοί από τους βασικούς ορισμούς που χρησιμοποιούνται συχνά στα συστήματα ανίχνευσης εισβολέων.

IDS (Intrusion Detection Systems)

Το σύστημα ανίχνευσης παρεισφρήσεων ή IDS είναι ένα λογισμικό, υλικό ή συνδυασμός και των δυο που χρησιμοποιείται για να ανιχνεύσει την δραστηριότητα εισβολέων. Ένα IDS μπορεί να έχει διαφορετικές ικανότητες ανάλογα με το πόσο σύνθετο είναι αυτό και τα συστατικά του μέρη. Οι συσκευές IDS, που είναι ένας συνδυασμός υλικού και λογισμικού είναι διαθέσιμες από πολλές εταιρίες. Όπως αναφέρθηκε και νωρίτερα, ένα IDS μπορεί να χρησιμοποιεί υπογραφές ή αλλιώς μοτίβα επιθέσεων (signatures) ή να παρατηρεί ανωμαλίες στην κίνηση του δικτύου (anomaly-based techniques) ή και τα δύο.

Δικτυακό (Network) IDS ή NIDS

Το NIDS είναι συστήματα ανίχνευσης παρεισφρήσεων που «συλλαμβάνει» πακέτα δεδομένων που μεταδίδονται μέσα στα δίκτυα (ενσύρματα και ασύρματα) και τα αντιστοιχεί με μια βάση δεδομένων των υπογραφών τους. Ανάλογα με το εάν ένα πακέτο αντιστοιχίζεται με μια υπογραφή εισβολέων (intruder signature), τότε ειδοποιούνται τα κατάλληλα στελέχη. Διαφορετικά το πακέτο καταγράφεται σε ένα αρχείο ή σε μια βάση δεδομένων. Μια σημαντική χρήση του Snort είναι και η λειτουργία του ως NIDS.

Host IDS ή HIDS

Στα συστήματα Host-based intrusion detection ή HIDS το λογισμικό εγκαθίσταται ως "πράκτορας" σε έναν κόμβο. Αυτά τα συστήματα ανίχνευσης παρεισφρήσεων μπορούν να εξετάσουν τα δεδομένα για να ανιχνεύσουν οποιαδήποτε δραστηριότητα εισβολέων. Μερικά από αυτά τα συστήματα είναι αντιδραστικά, που σημαίνει ότι ειδοποιούν για οποιαδήποτε δραστηριότητα, μόνο όταν κάτι έχει συμβεί. Μερικά HIDS είναι δυναμικά: μπορούν να ελέγχουν διαρκώς την κυκλοφορία των δικτύων και των πακέτων που μεταδίδονται στον κόμβο στον οποίο το HIDS είναι εγκατεστημένο και να ειδοποιεί με αυτό τον τρόπο σε πραγματικό χρόνο.

Υπογραφές (Signatures)

Η υπογραφή είναι το μοτίβο (pattern) που αναζητείται μέσα σε ένα πακέτο δεδομένων. Μια υπογραφή χρησιμοποιείται προκειμένου να ανιχνευτούν διάφοροι τύποι επιθέσεων. Παραδείγματος χάριν, η παρουσία "scripts/iisadmin" σε ένα πακέτο δεδομένων που κατευθύνεται προς κάποιο κεντρικό υπολογιστή ενός δικτύου μπορεί να αναδείξει δραστηριότητα εισβολέων.

Οι υπογραφές μπορούν να είναι παρούσες σε διαφορετικά μέρη ενός πακέτου δεδομένων, ανάλογα με την φύση της επίθεσης. Συνήθως τα IDS βασίζονται στις υπογραφές για να αναγνωρίσουν την δραστηριότητα των εισβολέων-επιθέσεων. Μερικά IDS από διάφορους προμηθευτές ενημερώνονται και προσθέτουν αυτόματα νέες υπογραφές, όταν ένας νέος τύπος επίθεσης ανακαλύπτεται. Σε άλλα IDS, όπως το Snort, η ενημέρωση δεν γίνεται αυτόματα, αλλά από τον διαχειριστή του συστήματος

Ειδοποιήσεις (Alerts)

Οι ειδοποιήσεις είναι οποιουδήποτε είδους ανακοίνωση προς τους χρήστες και τους αρμόδιους φορείς (διαχειριστές) για διάφορες επιθέσεις που αναγνωρίζονται σε ένα σύστημα. Όταν ένα IDS ανιχνεύει μία επίθεση, τότε αυτό ενημερώσει τον διαχειριστή ασφάλειας με αυτές τις ειδοποιήσεις. Αυτές οι ειδοποιήσεις αποθηκεύονται επίσης σε αρχεία συμβάντων (log) ή σε βάσεις δεδομένων, όπου μπορούν να επεξεργαστούν αργότερα από τους ειδικούς ασφάλειας. Το Snort μπορεί να παραγάγει τέτοιου είδους ειδοποιήσεις, ενώ έχει παράλληλα την δυνατότητα να τις στείλει σε πολλαπλούς προορισμούς. Για παράδειγμα, είναι δυνατό να καταγραφούν τα alerts σε μια βάση δεδομένων ενώ παράλληλα να σταλούν και emails με αυτές τις ειδοποιήσεις.

Συμβάντα (Logs)

Τα log messages σώζονται συνήθως σε κάποιο αρχείο. Εξ ορισμού το Snort αποθηκεύει αυτά τα μηνύματα στον κατάλογο του `/var/log/snort`. Εντούτοις, η θέση που αποθηκεύονται αυτά τα μηνύματα μπορεί να αλλάξει κατά την εκκίνηση του Snort, από την γραμμή εντολών του. Τα log messages μπορούν να αποθηκευτούν σε μορφή κειμένου είτε σε δυαδική μορφή. Τα δυαδικά αρχεία μπορούν έπειτα να επεξεργαστούν χρησιμοποιώντας το λογισμικό «tcpdump».

Ένα αποδοτικό λογισμικό αποκαλούμενο Barnyard είναι διαθέσιμο προκειμένου να αναλύει τα δυαδικά αρχεία που παράγει το Snort. Να σημειωθεί μάλιστα ότι τα αρχεία των log messages σε δυαδική μορφή είναι γενικώς αποδοτικότερα.

False Alarms

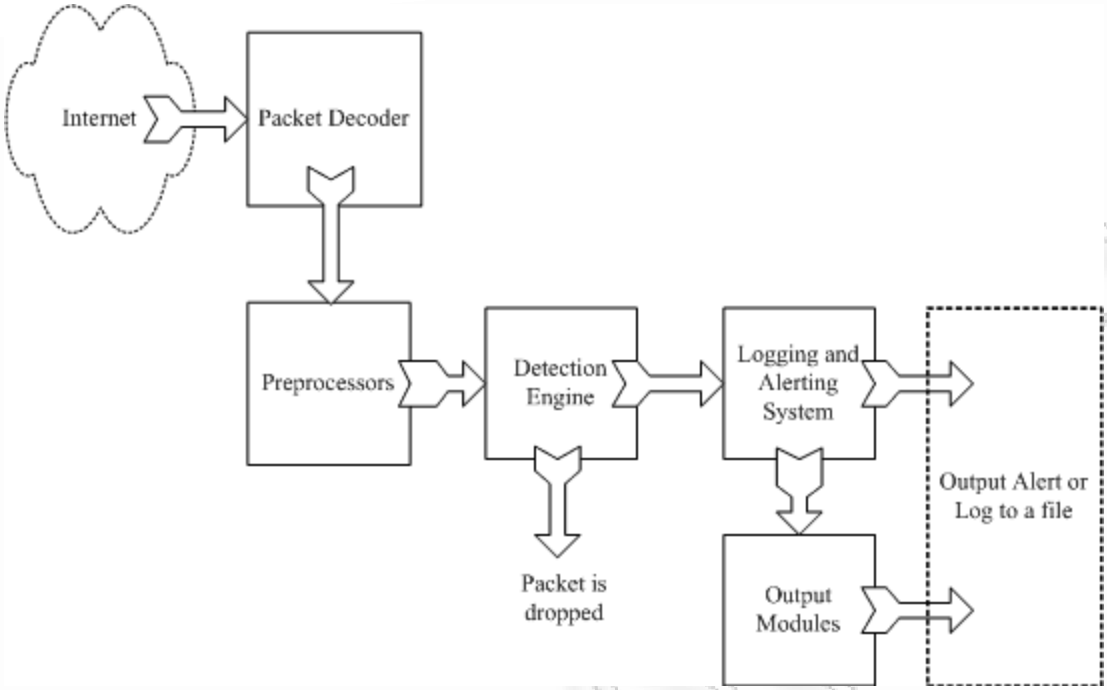
Τα False Alarms παράγονται λόγω μιας λανθασμένης ένδειξης επίθεσης στο σύστημα. Παραδείγματος χάριν, εσωτερικοί κόμβοι ενός δικτύου μπορεί μερικές φορές να μεταδώσουν μηνύματα τα οποία να "αφυπνίσουν" το σύστημα χωρίς λόγο. Για να αποφευχθούν οι ψεύτικες ειδοποιήσεις, πρέπει να τροποποιηθούν προσεκτικά οι διαφορετικούς κανόνες προεπιλογής. Σε μερικές περιπτώσεις ίσως να χρειάζεται να απενεργοποιηθούν εντελώς κάποιοι από αυτούς τους κανόνες, προκειμένου να αποφευχθούν αυτού του είδους οι συναγερμοί.

3.5 Συστατικά μέρη του Snort

Η λειτουργία του Snort διαιρείται σε 5 μέρη. Σε κάθε ένα εκτελείται μια λειτουργία προκειμένου να ανιχνεύονται οι επιθέσεις στο δίκτυο. Τα μέρη από τα οποία απαρτίζεται το Snort είναι τα ακόλουθα:

- Αποκωδικοποιητής πακέτων
- Προεπεξεργαστές (Preprocessor)
- Μηχανή ανίχνευσης
- Σύστημα καταγραφής και ειδοποιήσεων
- Output Modules

Το παρακάτω σχήμα επιδεικνύει πώς αυτά τα συστατικά μέρη του Snort κατανέμονται. Τα εισερχόμενα πακέτα δεδομένων από το διαδίκτυο εισάγονται αρχικά στον αποκωδικοποιητή πακέτων και στην συνέχεια το κάθε πακέτο δεδομένων επεξεργάζεται από το κάθε κομμάτι του Snort όπως φαίνεται παρακάτω.



Εικόνα 3.2 Τα συστατικά μέρη του Snort

Στην συνέχεια παρουσιάζεται μια συνοπτική εισαγωγή στα 5 μέρη του Snort:

1. ***Αποκωδικοποιητής πακέτων***

   Ο αποκωδικοποιητής πακέτων παίρνει τα πακέτα από τους διαφορετικούς τύπους δικτύων (ενσύρματα και ασύρματα) και τα προετοιμάζει έτσι ώστε να μπορούν να επεξεργαστούν ή να σταλούν στη μηχανή ανίχνευσης.

2. ***Προεπεξεργαστές***

   Προεπεξεργαστές ή Preprocessors είναι components που μπορούν να χρησιμοποιηθούν για να τροποποιήσουν τα διάφορα πακέτα δεδομένων, προτού η μηχανή ανίχνευσης αναλάβει δράση για να ανιχνεύσει τυχόν επιθέσεις. Επιπλέον μερικοί από τους preprocessors σε ένα IDS έχουν και αυτοί την δυνατότητα να ειδοποιήσουν τους διαχειριστές του συστήματος για τυχόν επιθέσεις. Οι Preprocessors είναι πολύ σημαντικοί για οποιοδήποτε IDS, προκειμένου να προετοιμάσουν τα πακέτα δεδομένων που προορίζονται για ανάλυση από τις μηχανές ανίχνευσης. Οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές για να «ξεγελάσουν» ένα IDS. Για παράδειγμα, σε κάποιο σύστημα ίσως υπάρχει ένας κανόνας για την ανίχνευση της υπογραφής, *"scripts/iisadmin".* Ένας επιτιθέμενος για να *ξεγλιστρήσει* από ένα σύστημα ανίχνευσης εισβολέων μπορεί να χρησιμοποιήσει παραλλαγές όπως:

   ```
   "scripts/./iisadmin"  ή
   "scripts/examples/../iisadmin" ή
   "scripts\iisadmin" ή
   "scripts/.\iisadmin"
   ```

Αν το IDS ψάχνει για ακριβή αντιστοιχία μεταξύ των υπογραφών τότε δεν θα είναι ικανό να εντοπίσει αυτές τις παραλλαγές επομένως ούτε και τις αντίστοιχες επιθέσεις.

Οι Preprocessors χρησιμοποιούνται επίσης για την επανένωση πακέτων. Όταν ένα μεγάλο πακέτο δεδομένων μεταφέρεται σε έναν άλλο υπολογιστή μέσω ενός δικτύου, το πακέτο αυτό συνήθως διασπάται σε μικρότερα. Παραδείγματος χάριν, το μέγιστο μήκος ενός οποιοιδήποτε πακέτου σε ένα δίκτυο Ethernet είναι συνήθως 1500 bytes. Αυτή η τιμή ελέγχεται από το Transfer Unit (MTU). Αυτό σημαίνει ότι αν αποσταλεί ένα αρχείο μεγαλύτερο των 1500 bytes, αυτό θα χωριστεί σε πολλαπλάσια πακέτα δεδομένων έτσι ώστε κάθε πακέτο να έχει μέγεθος μικρότερο ή ίσο με 1500 bytes. Έτσι το σύστημα το οποίο λαμβάνει αυτά τα πακέτα, τα αναδιαμορφώνει σε ένα ενιαίο πακέτο.

Σε ένα IDS, προτού να γίνει οποιοσδήποτε έλεγχος πρέπει αυτά τα διασπασμένα πακέτα να επανενωθούν, έτσι ώστε να είναι δυνατή η ανάλυσή τους. Για παράδειγμα πολλές φορές ίσως, ένα κομμάτι της υπογραφής βρίσκεται σε ένα πακέτο δεδομένων και η υπόλοιπη σε ένα άλλο. Έτσι λοιπόν για να ανιχνευτεί αυτή η υπογραφή σωστά, πρέπει πρώτα να συνδυαστούν σωστά όλα τα τμήματα των πακέτων. Οι επιτιθέμενοι χρησιμοποιούν συχνά την μέθοδο της διάσπασης πακέτων προκειμένου να μην γίνουν αντιληπτοί από ένα σύστημα ανίχνευσης εισβολέων.

Οι Preprocessors στο Snort έχουν την δυνατότητα να επανασυνδέσουν πακέτα δεδομένων, να αποκωδικοποιήσουν το HTTP URI και ούτω καθεξής. Αυτές οι λειτουργίες αποτελούν πολύ σημαντικό μέρος του συστήματος ανίχνευσης παρεισφρήσεων.

3. ***Μηχανή ανίχνευσης (Detection Engine)***

Η μηχανή ανίχνευσης είναι το σημαντικότερο μέρος ενός IDS. Η ευθύνη της είναι να ανιχνεύει πιθανές προσπάθειες εισβολής σε κάποιο από τα πακέτα που εξετάζει. Η μηχανή ανίχνευσης χρησιμοποιεί τους κανόνες για τον λόγο αυτό. Οι κανόνες διαβάζονται σε εσωτερικές δομές δεδομένων και έπειτα σύμφωνα με αυτούς εξετάζονται τα πακέτα δεδομένων. Εάν ένα πακέτο ανταποκρίνεται στις απαιτήσεις κάποιου κανόνα, τότε η κατάλληλη ενέργεια λαμβάνεται για το πακέτο αυτό.

Ανάλογα με το πόσο ισχυρό είναι το υπολογιστικό σύστημα στο οποίο είναι εγκατεστημένο το Snort και ανάλογα με το πόσοι κανόνες έχουν καθοριστεί, διαφέρει και ο χρόνος επεξεργασίας των διαφόρων πακέτων που δέχεται το Snort για έλεγχο. Εάν η κυκλοφορία σε ένα δίκτυο είναι πάρα πολύ υψηλή όταν το Snort εργάζεται σε NIDS mode, τότε ο έλεγχος για τυχόν επιθέσεις ίσως να καθυστερήσει σημαντικά. Το “φορτίο” στη μηχανή ανίχνευσης εξαρτάται από τους ακόλουθους παράγοντες:

- Αριθμός κανόνων
- Επεξεργαστική ισχύς του συστήματος που είναι εγκατεστημένο το Snort
- Ταχύτητα επικοινωνίας των διαύλων του συστήματος του Snort

- Το φορτίο του δικτύου

Κατά το σχεδιασμό ενός συστήματος ανίχνευσης παρεισφρήσεων, όλοι οι παραπάνω παράγοντες θα πρέπει να λαμβάνονται υπόψη. Να σημειωθεί επίσης ότι το σύστημα ανίχνευσης μπορεί να διασπάσει ένα πακέτο σε άλλα μικρότερα και να εφαρμόσει τους κανόνες στα διασπασμένα πλέον μέρη. Αυτά τα μέρη μπορεί να είναι:

- Η IP διεύθυνση του πακέτου.
- Τα πρωτόκολλα TCP,UDP, ICMP ή σε άλλα πρωτόκολλα.
- Οι "επικεφαλίδες» της επιγραφής του DNS, του FTP, του SNMP και του SMTP.

Η μηχανή ανίχνευσης του Snort λειτουργεί διαφορετικά για τις διάφορες εκδόσεις του. Σε όλες τις εκδόσεις 1.x, η μηχανή ανίχνευσης σταματά την περαιτέρω επεξεργασία ενός πακέτου όταν αντιστοιχείται με έναν κανόνα. Ανάλογα με τον κανόνα, η μηχανή ανίχνευσης παίρνει τη κατάλληλη ενέργεια. Δηλαδή είτε καταγράφει το πακέτο, είτε ειδοποιεί τους αρμόδιους φορείς. Αυτό σημαίνει ότι εάν ένα πακέτο ταιριάζει με τα κριτήρια παραπάνω από ενός κανόνα, τότε μόνο ο πρώτος κανόνας εφαρμόζεται στο πακέτο χωρίς να γίνεται έρευνα άλλων αντιστοιχιών με άλλους κανόνες. Αυτή η μέθοδος παρουσιάζει ένα πρόβλημα. Ένας κανόνας χαμηλής προτεραιότητας παράγει "μια χαμηλής επικινδυνότητας ειδοποίηση", ακόμα κι αν στην συνέχεια βρεθεί κάποιος κανόνας υψηλότερης επικινδυνότητας.

Αυτό το πρόβλημα αποκαθίσταται στο Snort στην έκδοση 2 όπου όλοι οι κανόνες αντιστοιχούνται ενάντια σε ένα πακέτο πριν γίνει οποιαδήποτε ειδοποίηση ή καταγραφή. Η μηχανή ανίχνευσης στην έκδοση 2.0 του Snort έχει δημιουργηθεί εξολοκλήρου από την αρχή έτσι ώστε να είναι πολύ γρηγορότερη στην ανίχνευση των απειλών από τις προηγούμενες εκδόσεις.

4. ***Σύστημα καταγραφής και ειδοποιήσεων***

Ανάλογα με το τι εντοπίζει το σύστημα ανίχνευσης μέσα σε ένα πακέτο, το πακέτο ίσως να καταγραφεί, ή εξαιτίας αυτού να ειδοποιηθεί ο διαχειριστής του συστήματος. Οι καταγραφές για τα συμβάντα που αντιμετωπίζει το Snort αποθηκεύονται σε μορφή απλών αρχείων κειμένων ή αρχείων τύπου tcpdump-style ή σε κάποια άλλη μορφή. Όλα αυτά τα αρχεία αποθηκεύονται εξ ορισμού στον κατάλογο `/var/log/`. Βέβαια είναι δυνατή η αλλαγή αυτής της τοποθεσίας μέσω της γραμμής εντολών του Snort και της χρήσης της παραμέτρου – l.

5. ***Output modules***

Τα **Output Modules** μπορούν να κάνουν διαφορετικές διαδικασίες ανάλογα με το αν επιθυμεί κάποιος να αποθηκεύει τις "εξόδους" του Snort. Δηλαδή τις προειδοποιήσεις και τις καταγραφές των απειλών. Στην πραγματικότητα ελέγχουν τον τύπο των εξόδων

αυτών. Ανάλογα με την παραμετροποίηση, τα output modules μπορούν να κάνουν πράγματα όπως:

- Απλή καταγραφή στα αρχεία /var/log/snort/alerts ή σε κάποιο άλλο αρχείο
- Αποστολή SNMP traps
- Αποστολή των μηνυμάτων στο syslog
- Καταγραφή σε μια βάση δεδομένων όπως την MySQL ή την Oracle
- Παραγωγή αρχείων τύπου XML
- Τροποποίηση των ρυθμίσεων στους δρομολογητές και τα firewalls
- Αποστόλη μηνυμάτων με την μορφή pop-up windows σε windows-based συστήματα
- Αποστολή ειδοποιήσεων σε μορφή e-mail
- Αποστολή ειδοποιήσεων σε web-interfaces

3.6 Κανόνες συστήματος ανίχνευσης παρεισφρήσεων Snort

Στην συνέχεια παρουσιάζονται κάποια βασικά παραδείγματα κανόνων που χρησιμοποιούνται στο Snort καθώς επίσης και ο τρόπος γραφής νέων κανόνων.

Παράδειγμα 1

Παρακάτω παρουσιάζεται ο πρώτος κανόνας. Δεν υπάρχει λόγος το Snort να ελέγχει για έναν τέτοιο κανόνα, καθώς όχι μόνο δεν προσφέρει κάποια ειδοποίηση αλλά και καταστρέφει το συστήματα. Στην συνέχεια αναλύεται γιατί συμβαίνει αυτό:

```
alert ip any any -> any any (msg: "IP Packet detected";)
```

Για να χρησιμοποιηθεί αυτός ο κανόνας πρέπει να προστεθεί στο τέλος του αρχείου snort.conf, την πρώτη φορά αφού γίνει εγκατάσταση. Αφού γίνει αυτό, το Snort θα παραγάγει συνεχώς ειδοποιήσεις για κάθε πακέτο IP που ελέγχει είτε πρόκειται για κακόβουλα δεδομένα, είτε όχι. Επομένως αυτό θα καταλήξει αναπόφευκτα στην “κατάληψη” ολόκληρου του ελεύθερου χώρου στο σκληρό δίσκο. Συνήθως αυτή η εντολή χρησιμοποιείται προκειμένου να διαπιστωθεί εάν όντως το Snort λειτουργεί σωστά.

Παράδειγμα 2

Ο παρακάτω κανόνας ειδοποιεί το σύστημα μόνο για τα πακέτα που έχουν την IP 192.168.1.113 ως παραλήπτη.

```
alert icmp any any -> 192.168.1.113/32 any \ (msg: "Ping with
TTL=100"; ttl:100;)
```

Δομή ενός κανόνα

Η γενική δομή ενός κανόνα που αναγνωρίζει το Snort είναι της μορφής που φαίνεται στο παρακάτω σχήμα.

Εικόνα 3.3 Η δομή των κανόνων του Snort

Στην συνέχεια αναλύεται κάθε ένα από τα τμήματα ενός κανόνα που φαίνονται στο παραπάνω σχήμα.

- ***Action***

  Καθορίζει τον τύπο της ενέργειας που θα γίνει όταν ένα πακέτο πληροί τις προϋποθέσεις του συγκεκριμένου κανόνα. Ένα τυπικό όρισμα σαν action συνήθως ειδοποιεί το σύστημα ή καταγράφει το συμβάν.

- ***Protocol***

  Χρησιμοποιείται για να ορίσει ποιο τύπο πρωτοκόλλου θα έχουν τα δεδομένα που θα εξετάσει το Snort και όπου θα εφαρμοστεί ο συγκεκριμένος κανόνας. Για παράδειγμα μερικά από τα ορίσματα είναι τα: IP, ICMP, UDP κ.α..

- ***Address***

  Καθορίζει την IP προέλευσης και την IP προορισμού. Σαν όρισμα μπορεί να είναι ένας μόνο κόμβος, περισσότεροι από ένας ή ακόμα και ένα δίκτυο υπολογιστών. Να σημειωθεί πως υπάρχουν δύο πεδία αυτού του τύπου. Το ένα, όπως αναφέρθηκε και προηγουμένως, είναι για την διεύθυνση προέλευσης και το άλλο για τον προορισμό. Το ποιο πεδίο από τα δύο θα είναι προορισμού και ποιο προέλευσης καθορίζεται από το πεδίο *Direction*. Για παράδειγμα εάν το πεδίο *Direction* είναι "->", τότε η διεύθυνση στα αριστερά είναι αυτή της προέλευσης και αντίστοιχα αυτή στα δεξιά, της αποστολής.

- ***Port***

  Στην περίπτωση που το πρωτόκολλο είναι TCP ή UDP, τότε το πεδίο αυτό καθορίζει την θύρα προορισμού και προέλευσης του πακέτου, το οποίο θα εξεταστεί σύμφωνα με τον συγκεκριμένο κανόνα. Στην περίπτωση που το πεδίο protocol είναι διαφορετικό από TCP ή UDP, τότε ο καθορισμός στον κανόνα κάποιας πόρτας, δεν έχει κανένα νόημα.

Κεφάλαιο 4

Κατανεμημένα συστήματα ανίχνευσης παρεισφρήσεων

4.1 Εισαγωγή

Είναι ιδιαίτερα δύσκολο οι τεχνικές ενός συστήματος ανίχνευσης παρεισφρήσεων των κλασσικών δικτύων να χρησιμοποιηθούν σε ένα δίκτυο Ad Hoc, λόγω της μεγάλης διαφοράς των δύο τύπων δικτύων. Τα Ad Hoc δίκτυα, εν αντιθέσει με τα δίκτυα σταθερών υποδομών, δεν διαθέτουν συγκεκριμένους κόμβους μέσα από τους οποίους δρομολογείται το σύνολο της κίνησης του δικτύου (switches και routers). Κάθε IDS ενός κόμβου μπορεί να παρατηρήσει μόνο τα δεδομένα που κινούνται μέσα από τον ίδιο ή, στην καλύτερη των περιπτώσεων, όλα τα δεδομένα τα οποία διακινούνται στην εμβέλεια της ασύρματης συσκευής που διαθέτει.

Επιπροσθέτως τα μοτίβα κίνησης που βασίζονται στην στατιστική δεν μπορούν πλέον να λειτουργήσουν. Καθώς η θέση ενός κόμβου μεταβάλλεται στο δίκτυο διαφορετικού τύπου και ποσότητας δεδομένων περνούν μέσα από αυτόν. Έτσι υπάρχουν διαρκώς ανωμαλίες στην κίνηση του δικτύου και οι τεχνικές που βασίζονται στον εντοπισμό τέτοιων ανωμαλιών (anomaly-based techniques) δεν μπορούν να αξιοποιηθούν.

Ακόμα πιο σύνθετη είναι η διαδικασία ανίχνευσης παρεισφρήσεων καθώς ένας κόμβος που αποστέλλει λανθασμένα δεδομένα δρομολόγησης μπορεί να είναι όντως κακόβουλος, αλλά μπορεί να έχει προσωρινά αποσυγχρονιστεί από το υπόλοιπο δίκτυο.

4.2 Δυσκολίες και συγκριτικά πλεονεκτήματα λειτουργίας IDS σε Ad-Hoc Δίκτυα

Παρά τις δυσκολίες που παρουσιάζουν τα δίκτυα Ad Hoc η καλύτερη στρατηγική παραμένει ο εντοπισμός ανωμαλιών (anomaly detection). Για να εντοπιστεί μια ανωμαλία θα πρέπει οι κόμβοι να παρακολουθούν τα δεδομένα που διέρχονται από αυτούς, αλλά και να συνεργάζονται και με άλλους κόμβους του δικτύου, ζητώντας επιπρόσθετες αποδείξεις ώστε να σιγουρευτούν ότι όντως μια ανωμαλία του δικτύου λαμβάνει χώρα.

Οι δυσκολίες που εμφανίζουν τα Ad-Hoc δίκτυα στην λειτουργία ενός συστήματος IDS μπορούν να τοποθετηθούν στις παρακάτω κατηγορίες.

- **Δυνατότητες υλικού.** Οι κόμβοι που συνδέονται σε ένα Ad-Hoc δίκτυο διαθέτουν διαφορετικό υλικό και διαφορετικό λογισμικό. Μπορεί ένας κόμβος να αποτελεί το κινητό τηλέφωνο ενός χρήστη, το PDA, το NetBook ενός άλλου, κάποιο laptop ή κάποια embedded συσκευή που λειτουργεί ως μέρος ενός αυτοκινήτου ή μιας μηχανής. Κάθε μια από αυτές τις συσκευές διαθέτει επεξεργαστή και μνήμη, σχετικά μειωμένων δυνατοτήτων και ενεργειακά βασίζεται στη χρήση μπαταριών. Για την αύξηση της διάρκειας λειτουργίας τους, οι συσκευές αυτές συνήθως διαθέτουν μηχανισμούς εξοικονόμησης ενέργειας και πρέπει να σεβαστούν οι μηχανισμοί αυτοί ακόμα και αν αυτό είναι εις βάρος της συνολικής απόδοσης του συστήματος ανίχνευσης παρεισφρήσεων.

- **Ανομοιογένεια κόμβων.** Κάθε κόμβος έχει πληθώρα διαφορετικών χαρακτηριστικών. Για την άριστη λειτουργία του IDS θα πρέπει λοιπόν ο κάθε κόμβος να λειτουργεί όσο το δυνατόν καλύτερα μπορεί στα πλαίσια των δυνατοτήτων του.

- **Δυναμική τοπολογία.** Η τοπολογία ενός Ad-Hoc δικτύου είναι μεταβλητή. Οι κόμβοι κινούνται σε απρόβλεπτες κατευθύνσεις και δημιουργούν ασύρματες συνδέσεις κατά βούληση. Η έλλειψη τοπολογίας σημαίνει ότι δεν μπορούν να εντοπιστούν συγκεκριμένα κομβικά σημεία, ώστε σε αυτά να δοθεί η μεγαλύτερη βαρύτητα στην ανίχνευση εισβολέων.

Από την άλλη, η φύση των Ad-Hoc δικτύων αναγκάζει τους κόμβους να χρησιμοποιούν συνεργατικά IDS. Το πλήθος των συστημάτων IDS που λειτουργούν σε ένα δίκτυο είναι όσος και ο αριθμός των κόμβων. Αυτό παρέχει κάποια πλεονεκτήματα συγκριτικά με τα IDS των δικτύων με σταθερές υποδομές.

Ακόμα και στο πιο ασφαλές εταιρικό δίκτυο, στο οποίο έχουν τοποθετηθεί συστήματα IDS σε επιλεκτικά σημεία, ένας υπάλληλος μπορεί να εκτελέσει αρκετές επιθέσεις σε γειτονικά του συστήματα χωρίς αυτό ποτέ να ανιχνευθεί. Αν για παράδειγμα η διαδρομή των δεδομένων δεν περιλαμβάνει ένα σύστημα IDS, τότε η επίθεση αυτή πιθανώς να μην ανιχνευθεί. Στα Ad-Hoc δίκτυα όμως κάθε επίθεση μπορεί να ανιχνευθεί καθώς κάθε κόμβος του δικτύου αποτελεί ένα IDS.

Το κυριότερο ερώτημα είναι ποιες τεχνικές να χρησιμοποιηθούν ώστε μια επίθεση α) να ανιχνευθεί ταχύτατα και β) να αντιμετωπιστεί όσο το δυνατόν πιο αποτελεσματικά.

4.3 Αλγόριθμοι και τεχνικές για κατανεμημένα συστήματα ανίχνευσης παρεισφρήσεων

Αλγόριθμος Haystack

Ο αλγόριθμος Haystack βασίζεται στην στατιστική μεθοδολογία. Αρχικά παρακολουθεί τα δεδομένα που μεταδίδονται από τον κόμβο και δημιουργεί ένα αρχείο CAT (canonical audit trail), το οποίο περιέχει δείκτες που δείχνουν την δραστηριότητα του χρήστη του κόμβου. Αυτοί οι δείκτες αναλύονται διαρκώς και λαμβάνουν μια *τιμή ανωμαλίας*. Όταν μια τιμή ξεπεράσει κάποια προκαθορισμένα όρια δημιουργούνται προειδοποιήσεις στο χρήστη. Ο αλγόριθμος αυτός χρησιμοποιείται για Host Based IDS και μπορεί να εντοπίσει επιθέσεις όπως denial of service, masquerading και άλλες και δημιουργήθηκε αρχικά ώστε να χρησιμοποιηθεί από στρατιωτικές υπηρεσίες. Επειδή αναπτύχθηκε αρχικά για δίκτυα με σταθερές υποδομές, για να χρησιμοποιηθεί σε Ad Hoc δίκτυα, ένας κόμβος (που θα πρέπει να προκαθοριστεί από τον αρχικό δημιουργό του δικτύου) θεωρείται διαχειριστής του IDS και όλοι οι υπόλοιποι κόμβοι ενημερώνονται έτσι ώστε να αποστέλλουν περιοδικά του δείκτες που περιέχουν.

Αλγόριθμος Indra

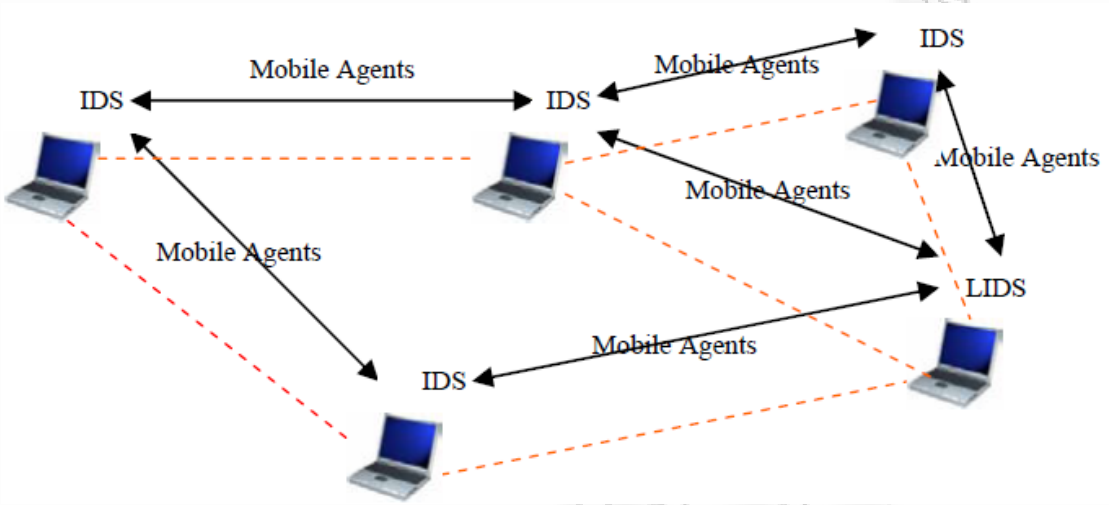
Ο αλγόριθμος Indra απέκτησε την ονομασία αυτή από το “INtrusion Detection and Rapid Action” και αφορά ένα κατανεμημένο (distributed) IDS. Η βασική ιδέα είναι ο κάθε κόμβος να παρακολουθεί διαρκώς τους γειτονικούς του και να τους υποπτεύεται ότι είναι κακόβουλοι. Κάθε κόμβος που εντοπίζει μια ανωμαλία ενημερώνει αμέσως τον κόμβο ο οποίος είναι στόχος της επίθεσης. Αν ο κόμβος επιβεβαιώσει την επίθεση τότε δημιουργεί έναν συναγερμό και όλοι οι υπόλοιποι κόμβοι είναι προετοιμασμένοι για τυχόν παρόμοια επίθεση. Έτσι λειτουργεί παρομοίως με το ανοσοποιητικό σύστημα.

Στον Indra το πιο σημαντικό είναι η εμπιστοσύνη ανάμεσα στους κόμβους ότι τα δεδομένα που λαμβάνουν είναι αξιόπιστα και καλόβουλα. Στα δίκτυα με σταθερές υποδομές αυτό δεν αποτελεί πρόβλημα καθώς ένα Certification Authority (CA) δημιουργεί πιστοποιητικά ασφαλείας για τους κόμβους του δικτύου. Στην περίπτωση των Ah Hoc δικτύων κάθε κόμβος εμπιστεύεται μόνο τον εαυτό του και κανέναν άλλο. Μια αποκεντρωμένη CA που ονομάζεται μοντέλο **web-of-trust** [15] μπορεί όμως να χρησιμοποιηθεί. Στο μοντέλο αυτό όσο οι πληροφορίες που αποστέλλει ένας κόμβος επιβεβαιώνονται ότι είναι ορθές, τόσο ο κόμβος αρχίζει να αποκτά μεγαλύτερη υπόληψη. Βέβαια το σύστημα θα πρέπει να προφυλάσσεται από κόμβους οι οποίοι μπορεί να λειτουργούν νομότυπα για μεγάλο χρονικό διάστημα ώστε να θεωρηθούν ως έμπιστοι και κατόπιν να αρχίζουν την κακόβουλη συμπεριφορά τους.

Κινητοί πράκτορες

Η προσέγγιση των mobile agents προσπαθεί να δημιουργήσει ένα καθολικό κατανεμημένο IDS που αποτελείται από επιμέρους τοπικά IDS τα οποία συνεργάζονται μεταξύ τους. Οι

κινητοί πράκτορες λειτουργούν κατανεμημένα και συνεργατικά. Σε κάθε νέο κόμβο που συνδέεται σε ένα τέτοιο Ad Hoc δίκτυο θα πρέπει να εκτελείται το τοπικό IDS εκ των προτέρων, ώστε αμέσως να γίνεται μέρος του καθολικού IDS του δικτύου.



Εικόνα 4.1 Κινητοί πράκτορες για ανίχνευση εισβολέων

Κάθε κινητός πράκτορας διαθέτει τρία υποσυστήματα: ένα μηχανισμό συλλογής δεδομένων, ένα μηχανισμό ανάλυσης και ένα μηχανισμό ειδοποίησης των υπολοίπων κόμβων. Ο μηχανισμός ανάλυσης δεδομένων παρακολουθεί τόσο για μοτίβα (patterns), όσο και στατιστικά τα δεδομένα (hybrid mechanism). Κάθε πράκτορας ουσιαστικά προστατεύει τον κόμβο του, αλλά ταυτόχρονα μπορεί να εντοπίσει και επιθέσεις εναντίων άλλων κόμβων. Στην περίπτωση αυτή στέλνει προειδοποιητικές ειδοποιήσεις.

Εξόρυξη δεδομένων

Τεχνικές data mining μπορούν να χρησιμοποιηθούν και για την ανίχνευση εισβολέων. Κάθε κόμβος μπορεί να αναλύσει δεδομένα και να δημιουργήσει μοντέλα ανίχνευσης παρεισφρήσεων.

Η πλέον γνωστή τεχνική στην εξόρυξη δεδομένων είναι το classification. Σε αυτή την διαδικασία, κάθε δεδομένο κατηγοριοποιείται σε μια προκαθορισμένη κατηγορία. Η κατηγοριοποίηση μπορεί να βασιστεί είτε σε απλούς κανόνες, είτε σε πιο σύνθετα decision trees (δέντρα αποφάσεων). Για να λειτουργήσει επιτυχώς πρέπει αρκετά δεδομένα να συλλεχθούν τόσο φυσιολογικής κίνησης όσο και κακόβουλης χρήσης. Μελετώντας τα δεδομένα αυτά, ο αλγόριθμος μπορεί να «εκπαιδευτεί» ώστε να είναι σε θέση να κατηγοριοποιήσει μελλοντικά δεδομένα σε είτε φυσιολογική είτε κακόβουλη χρήση.

Κεφάλαιο 5

Ιεραρχικά IDS στα Ad-Hoc δίκτυα

5.1 Εισαγωγή

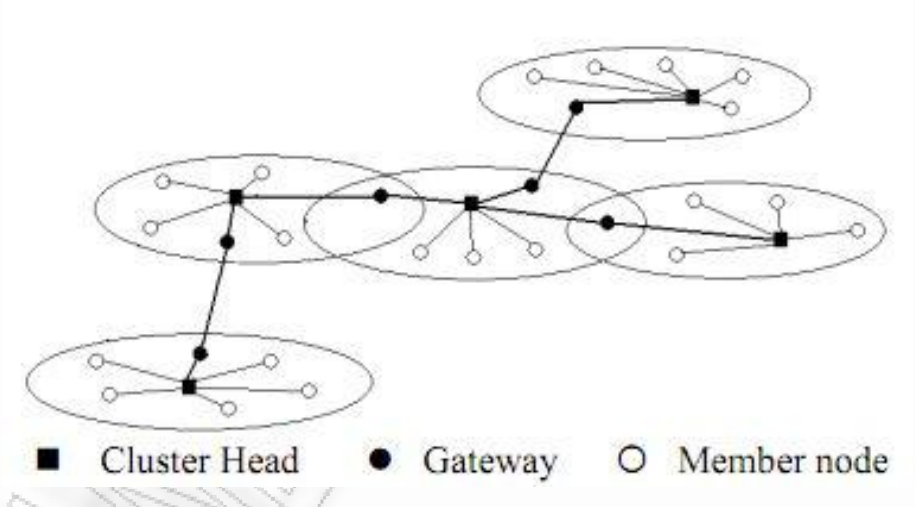
Οι ιεραρχικές αρχιτεκτονικές συστημάτων ανίχνευσης παρεισφρήσεων έχουν προταθεί για τα πολυστρωματικά (multi-layered), ασύρματα ad-hoc δίκτυα. Σε ένα multi-layered ασύρματο ad-hoc δίκτυο, οι cluster-head κόμβοι συγκεντρώνουν τις ενέργειες δρομολόγησης και είναι αυτοί οι κόμβοι που μπορούν να υποστηρίξουν πρόσθετους μηχανισμούς ασφάλειας, όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο. Στην συνέχεια αυτού του κεφαλαίου αναλύεται η γενική δομή και λειτουργία ενός Hierarchical IDS το οποίο βασίζεται στο πρωτόκολλο επικοινωνίας CBRP. Μετά την ανάλυση αυτή ακολουθεί μια εκτενής παρουσίαση ενός Hierarchical IDS το οποίο βασίζεται σε cluster δίκτυο με την διαφορά ότι οι cluster head κόμβοι συνεχώς εναλλάσσονται μεταξύ τους, προσδίδοντας έτσι στο σύστημα αυξημένη ασφάλεια και κατά συνέπεια αυξημένη αποδοτικότητα.

5.2 Hierarchical IDS με πρωτόκολλο CBRP

Σε αυτή την παράγραφο παρουσιάζεται μία δομή Hierarchical IDS η οποία βασίζεται στο πρωτόκολλο δρομολόγησης CBRP. Αναλύεται αρχικά το πρωτόκολλο CBRP, στην συνέχεια παρουσιάζονται τα συστατικά μέρη του συγκεκριμένου IDS και τέλος ο γενικός τρόπος λειτουργίας του.

5.2.1 Πρωτόκολλο δρομολόγησης βασισμένο σε συμπλέγματα (Cluster Based Routing Protocol)

Το CBRP είναι ένα πρωτόκολλο δρομολόγησης που έχει δημιουργηθεί με σκοπό να χρησιμοποιείται σε ad-hoc δίκτυα. Το πρωτόκολλο διαιρεί τους κόμβους σε συμπλέγματα - clusters με “διάμετρο” δύο κόμβων με έναν διανεμημένο τρόπο. Σε κάθε cluster επιλέγεται ο cluster-head κόμβος, ο οποίος διατηρεί τις πληροφορίες του συμπλέγματός του. Με βάση τις πληροφορίες που διαθέτει ο cluster-head κόμβος, διαμορφώνεται δυναμικά η δρομολόγηση του δικτύου του συμπλέγματος και σταδιακά ολόκληρου του δικτύου. Το συγκεκριμένο πρωτόκολλο ελαχιστοποιεί αποτελεσματικά την υπέρ-τροφοδότηση με μη χρήσιμες πληροφορίες σχετικά με την δρομολόγηση του δικτύου και επιταχύνει παράλληλα αυτή την διαδικασία με τη συγκέντρωση των κόμβων σε συμπλέγματα. Ένα παράδειγμα ενός τέτοιου δικτύου παρουσιάζεται στην εικόνα 5.1. Οι κόμβοι οργανώνονται σε πέντε συμπλέγματα και κάθε ένα διαθέτει έναν κόμβο cluster-head.



Εικόνα 5.1 Cluster Based Ad-Hoc Network

Αντίθετα από τα on-demand πρωτόκολλα δρομολόγησης, στο CBRP οι κόμβοι οργανώνονται σε μια ιεραρχία. Ο cluster-head κόμβος συντονίζει την μετάδοση των δεδομένων από το σύμπλεγμα στο οποίο ηγείται στα άλλα συμπλέγματα. Το πλεονέκτημα του CBRP είναι ότι μόνο οι cluster-head κόμβοι ανταλλάσσουν πληροφορίες δρομολόγησης, επομένως ο όγκος των δεδομένων που διαβιβάζονται στο δίκτυο, είναι σημαντικά μικρότερος σε σχέση με άλλα πρωτόκολλα.

Οι πληροφορίες για την κατάσταση των συνδέσεων διατηρούνται σε ένα πίνακα. Ένας κόμβος cluster-head διατηρεί πληροφορίες για την κατάσταση των γειτονικών του συμπλεγμάτων, παράλληλα με τις πληροφορίες για τα μέλη της δικής του συστάδας. Μέσα

σε αυτές τις πληροφορίες περιλαμβάνονται εκτός των άλλων δεδομένα για τους cluster-head κόμβους των γειτονικών clusters αλλά και δεδομένα για τους gateway κόμβους του δικτύου.

Κύριος ρόλος επομένως του CBRP είναι να προτείνει κάθε φορά την συντομότερη διαδρομή καταλήγοντας έτσι στην βέλτιστη απόδοση του δικτύου. Μερικά από τα κυριότερα χαρακτηριστικά αυτού του πρωτοκόλλου είναι:

- Πλήρως κατανεμημένη λειτουργία.
- Μειωμένη κίνηση στο δίκτυο κατά την διάρκεια της δυναμικής δρομολόγησής του.
- Τοπικά σφάλματα δρομολόγησης μπορούν να λυθούν χωρίς την ανάγκη επανάληψης ολικής δρομολόγησης .

5.2.2 Δομή του HIDS

Το παραπάνω ιεραρχικό IDS βασίζεται στο πρωτόκολλο CBRP. Εστιάζει δηλαδή κυρίως στους cluster-head κόμβους ενός ad-hoc δικτύου.

Το μοντέλο αποτελείται από δύο επίπεδα (layers). Το επίπεδο cluster member και το επίπεδο cluster head. Αναπαρίσταται η δομή του HIDS με την χρήση των δύο τελευταίων επιπέδων. Ανάλογα με την λειτουργία την οποία πρέπει να εκτελέσει κάθε κόμβος χρησιμοποιούνται και διαφορετικοί πράκτορες (agents). Πιο συγκεκριμένα:

- **Intrusion Detection Agent (IDA):** Ένας intrusion detection agent χρησιμοποιείται σε κάθε cluster-head κόμβο που όχι απλά ανιχνεύει κάποια γενική παρείσφρηση, αλλά και έχει την δυνατότητα να ανιχνεύσει το είδος της εισβολής και επιπλέον να ειδοποιήσει όλα τα μέλη του συμπλέγματος σχετικά με αυτή. Να σημειωθεί πως η χρήση των IDAs δεν επηρεάζει αισθητά το bandwidth του συμπλέγματος. Όλα τα παραπάνω έχουν ως αποτέλεσμα την μείωση εάν όχι την ολοκληρωτική κατάργηση των βλαβών που προκαλούνται από τις εισβολές στο δίκτυο. Ένας πράκτορας τύπου Intrusion Detection αποτελείται από τα εξής μέρη:

  1. **Pre-Processor:** Συλλέγει είτε δεδομένα της κίνησης στο σύμπλεγμα του, είτε δέχεται αναφορές από τους υπολοίπους κόμβους σχετικά με την λειτουργία του δικτύου. Είναι επίσης υπεύθυνος για την μετατροπή των δεδομένων που συλλέγει σε μορφή κατανοητή από τα ανώτερα μέρη του IDA.

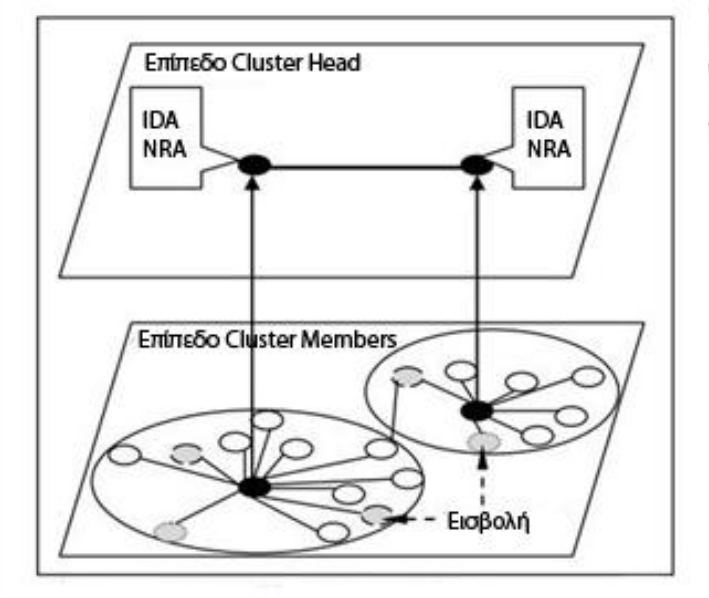
  2. **Signature Processor:** Συγκρίνει τα κατανοητά πλέον δεδομένα που προκύπτουν από την λειτουργία του Pre-Processor, με δεδομένα που βρίσκονται σε μία βάση δεδομένων που καλείται συνήθως Signature Record. Στην βάση αυτή είναι αποθηκευμένες συνήθως γνωστές επιθέσεις και υψηλού κινδύνου ενέργειες. Εάν δεν βρεθεί κάποια αντιστοιχία των δεδομένων προς επεξεργασία με την βάση, τότε τα δεδομένα αυτά μεταβιβάζονται στο αμέσως επόμενο επίπεδο για περαιτέρω επεξεργασία.

  3. **Anomaly Processor:** Αποτελεί το επόμενο στάδιο επεξεργασίας, αμέσως μετά το στάδιο “Signature Processor” και χρησιμοποιεί στατιστικές μεθόδους ή

μεθόδους τεχνητής νοημοσύνης. Εάν κάποιες συγκεκριμένες τιμές των δεδομένων υπερβούν κάποια όρια τότε θεωρείται πως το δίκτυο έχει δεχθεί εισβολή.

4. **Post Processor:** Είναι το στάδιο το οποίο είναι υπεύθυνο για να στέλνει αναφορές στα μέλη-κόμβους του συμπλέγματος.

- ***Network Response Agent (NRA):*** Ένας network response agent χρησιμοποιείται αφού έχει ανιχνευθεί κάποια απειλή στο δίκτυο. Δηλαδή όταν έχει ενεργοποιηθεί ο IDA. Σκοπός του είναι να ενημερώσει τους υπολοίπους cluster-head κόμβους για την εισβολή μόνο στην περίπτωση κατά την οποία ο εισβολέας αποτελεί gateway κόμβο.



Εικόνα 5.2 Δομή ενός HIDS

5.3 Voting Based Hierarchical IDS

Σε ένα Cluster Based δίκτυο οι επιθέσεις μπορεί να λάβουν χώρα σε οποιοδήποτε κόμβο. Είτε αυτός είναι cluster head κόμβος είτε απλό μέλος ενός συμπλέγματος. Επιπλέον με το πέρασμα του χρόνου θέλουμε να αποσυμπιέζουμε τον cluster – head κόμβο από τις λειτουργίες και τον φόρτο εργασίας που απαιτεί το IDS. Για αυτούς τους λόγους κυρίως, είναι απαραίτητο να αλλάζουν περιοδικά με την πάροδο του χρόνου οι cluster head κόμβοι του δικτύου.

Σε αυτή την παράγραφο λοιπόν, αναλύεται ένα HIDS το οποίο βασίζεται στο CBRP. Στην μέθοδο αυτή οι cluster head κόμβοι αλλάζουν συνεχώς στο χρόνο. Η επιλογή τους βασίζεται σε μια ψηφοφορία που λαμβάνει χώρα ανά συγκεκριμένα χρονικά διαστήματα και με βάση κάποιων συγκεκριμένων χαρακτηριστικών των κόμβων.

Η υλοποίηση μπορεί να διαιρεθεί και να αναλυθεί στα ακόλουθα στάδια:

1. Αλγόριθμος εκλογής (Election Algorithm)
2. Ενημέρωση της αρχιτεκτονική του IDS (IDS architecture)
3. Απάντηση σχετικά με την εισβολή (Intrusion response)
4. Διαμοιρασμός δεδομένων (Sharing of data)

5.3.1 Αλγόριθμος Εκλογής

Είναι απαραίτητο ο αλγόριθμος εκλογής για τον επόμενο cluster-head κόμβο να είναι δίκαιος. Έχουν προταθεί αρκετοί αλγόριθμοι εκλογής σε ad-hoc ασύρματα δίκτυα [18], αλλά ελάχιστοι εξετάζουν παραμέτρους, όπως για παράδειγμα την υπολογιστική δύναμη κάθε κόμβου και το τρέχον επίπεδο της μπαταρίας. Παρατηρείται λοιπόν πως αυτές οι δύο παράμετροι είναι αρκετοί, εφόσον δεν υπολογιστούν κατά την διαδικασία εκλογής, για να υπάρξει μια μη δίκαιη ψηφοφορία μεταξύ των κόμβων του δικτύου. Είναι σημαντικό δηλαδή να ληφθεί υπόψη η υπολογιστική δύναμη των υποψηφίων κόμβων καθώς και το επίπεδο της ενέργειας της μπαταρίας κάθε κόμβου. Το τελευταίο αποτελεί ιδιαίτερα καθοριστικό παράγοντα κατά την εκλογή του cluster-head, διότι εάν το επίπεδο μπαταρίας είναι χαμηλό οι απαιτήσεις του IDS, δεδομένου ότι ο αντίστοιχος κόμβος έχει εκλεγεί ως cluster head, θα μειώσουν σε πολύ λιγότερο χρόνο την διάρκεια ζωής της μπαταρίας.

Ως εκ τούτου, στην μέθοδο που παρουσιάζεται στην συνέχεια, έχουν επιλεγεί ως κριτήρια για την επιλογή του νέου cluster head κόμβου: η υπολογιστική δύναμη και το επίπεδο της μπαταρίας των κόμβων. Επίσης για να εξασφαλιστεί η μη προβλεψιμότητα στα αποτελέσματα, χρησιμοποιείται και ένας τυχαίος αριθμός κάθε φορά.

Για να εξασφαλίσει η ακεραιότητα των δεδομένων, δηλαδή ότι οι κόμβοι δεν αλλοιώνουν τα δεδομένα που μεταδίδουν, η διαδικασία της εκλογής αποτελείται από δύο φάσεις, όπου στην δεύτερη φάση πιστοποιούνται οι τιμές που μεταδόθηκαν κατά την πρώτη.

Ο αλγόριθμος εκλογής διαθέτει τα εξής βήματα:

1. Κάθε κόμβος λαμβάνει περιοδικά πληροφορίες για την κατάσταση των γειτονικών του κόμβων.
2. Κατά την έναρξη του αλγορίθμου, κάθε κόμβος αποτελεί ένα αυτόνομο και αυτοτελές σύστημα ανίχνευσης παρείσφρησης.
3. Μια `*κλίκα*` ορίζεται ως μια ομάδα κόμβων όπου κάθε ζευγάρι των μελών της μπορεί να επικοινωνήσει μέσω μιας άμεσης ασύρματης σύνδεσης. Όταν ο βρεθεί ποιος θα είναι ο cluster head κόμβος κάθε φορά, τότε ο θεσμός των κλικών χαλαρώνει.
4. Όλοι οι κόμβοι υπολογίζουν μια τιμή hash μέσω μιας hash function. Η τιμή αυτή προκύπτει από τον υπολογισμό της υπολογιστικής δύναμης, το επίπεδο ενέργειας της μπαταρίας και ενός τυχαίου αριθμού.
5. Αναμεταδίδονται οι αρχικές τιμές των παραμέτρων εκλογής
6. Κάθε κόμβος συγκρίνει τις τιμές που λαμβάνει στο βήμα 4 και 5 και εξασφαλίζει ότι είναι οι ίδιες.
7. Όλοι οι κόμβοι τρέχουν τον αλγόριθμο εκλογής και υπολογίζουν τις ίδιες τιμές για τον κύριο και εφεδρικό κόμβο.

8. Ο κύριος κόμβος (master node) διατηρεί έναν κατάλογο μελών που χρησιμοποιείται για την αποθήκευση πληροφοριών για κάθε κόμβο.
9. Cluster Valid Assertion: Το πρωτόκολλο αυτό χρησιμοποιείται όταν έχει πλέον εκλεχθεί ο cluster head κόμβος και ελέγχει περιοδικά την κατάσταση των συνδέσεων και είναι επίσης αρμόδιο για τον έλεγχο του χρόνου της επόμενης εκλογής.
10. Η αποτυχία των συνδέσεων μεταξύ των κόμβων έχει ως αποτέλεσμα την ενεργοποίηση του πρωτοκόλλου Cluster recovery.
11. Cluster recovery: Έχει ως αποτέλεσμα την επανέναρξη της διαδικασίας εκλογής νέου cluster head κόμβου.

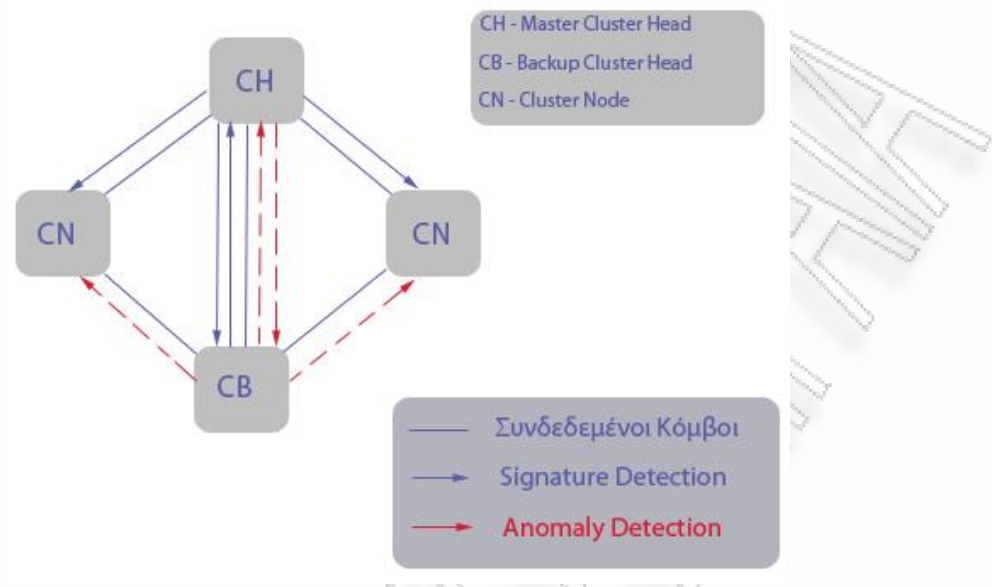
Κατά την λειτουργία του δικτύου διακρίνονται μερικά σενάρια όπως:

- Αρχικός σχηματισμός δικτύου: Όλοι οι κόμβοι ανταλλάσσουν μηνύματα «Hello» ζητώντας πληροφορίες για γειτονικούς κόμβους. Αυτή η λειτουργία οδηγεί έπειτα στο σχηματισμό των `*κλικών*` όπως αναφέρθηκε παραπάνω και μόλις οι κλίκες δημιουργηθούν, ανταλλάσσονται οι παράμετροι εκλογής μεταξύ των κόμβων, για να καθοριστεί ο κύριος και ο εφεδρικός cluster-head.
- Ο κύριος cluster-head εγκαταλείπει το δίκτυο: Όταν ο κύριος cluster-head κόμβος κινείται εκτός του δικτύου, τότε όλοι οι κόμβοι στο σύμπλεγμα επικοινωνούν για να πραγματοποιηθεί νέα εκλογή.
- Ο εφεδρικός cluster-head εγκαταλείπει το δίκτυο: Όταν ο εφεδρικός cluster-head κόμβος κινείται εκτός του δικτύου και σε αυτή την περίπτωση πραγματοποιείται επανεκλογή.
- Ο κύριος cluster-head δέχεται επίθεση: Όταν ο εφεδρικός cluster head έχει επαρκή στοιχεία ότι ο κύριος κόμβος έχει δεχθεί επίθεση, είτε μέσω των αποτελεσμάτων της ανίχνευσης υπογραφών είτε μέσω της κοινής συναίνεσης με άλλους κόμβους, τότε πραγματοποιείται άμεσα επανεκλογή αφού απομονωθεί ο πρώην κύριος κόμβος.
- Ο εφεδρικός cluster-head δέχεται επίθεση: Όταν ο κύριος έχει επαρκή στοιχεία πως ο εφεδρικός έχει δεχθεί επίθεση και σε αυτή την περίπτωση πραγματοποιείται επανεκλογή, αφού πρώτα αφαιρεθεί από την λίστα των υποψηφίων κόμβων ο εφεδρικός cluster-head.
- Περιοδική επανεκλογή: Πραγματοποιείται μετά από συγκεκριμένο χρόνο προκειμένου να αποφευχθεί, η από ένα και μόνο κόμβο ανίχνευση παρεισφρήσεων.

5.3.2 Αρχιτεκτονική του IDS (IDS architecture)

Στο παραπάνω μοντέλο οι κόμβοι έχουν άμεσες συνδέσεις ο ένας με τον άλλο (*κλίκες*) κατά την διαδικασία σχηματισμού συμπλέγματος, έτσι ώστε να ανιχνεύονται αλλοιωμένα μηνύματα. Επίσης κάθε κόμβος διαθέτει ένα εκπαιδευμένο, προ-εγκατεστημένο IDS που λειτουργεί τόσο σε επίπεδο υπογραφών όσο και ανωμαλιών (anomaly & signature). Θα ενεργοποιηθεί μόνο στην περίπτωση που ο αντίστοιχος κόμβος επιλέγεται ως κύριος ή εφεδρικός cluster-head. Ο κύριος cluster head κόμβος πραγματοποιεί έλεγχο υπογραφών ενώ παράλληλα θα πραγματοποιεί ανίχνευση ανωμαλιών (anomaly detection) σε όλους του

κόμβους. Ομοίως ο εφεδρικός κόμβος πραγματοποιεί έλεγχο υπογραφών ενώ παράλληλα πραγματοποιεί anomaly detection μόνο στον τρέχον κύριο cluster head κόμβο.



Εικόνα 5.3 Λειτουργία του HIDS που αναλύεται

1. *Ανίχνευση υπογραφών από τον Cluster Head:*

Η ανίχνευση υπογραφών απαιτεί όπως έχει αναφερθεί νωρίτερα, τη συντήρηση μιας εκτενούς βάσης δεδομένων με υπογραφές επιθέσεων, η οποία στην περίπτωση του ad-hoc δικτύου θα έπρεπε να αντιγραφεί μεταξύ όλων των κόμβων. Κάθε πακέτο στο οποίο συγκρίνεται η υπογραφή του πρέπει να συγκριθεί με τη βάση δεδομένων υπογραφών επίθεσης. Αυτή η διαδικασία απαιτεί O(n) χρόνο, όπου το n είναι ο αριθμός των υπογραφών στη βάση δεδομένων. Η βάση δεδομένων υπογραφών έχει συνήθως εκατοντάδες σχέδια επίθεσης.

Η διαδικασία της anomaly detection, απαιτεί λιγότερες συγκρίσεις. Χαρακτηριστικά, λιγότερες από είκοσι παράμετροι χρησιμοποιούνται. Κατά συνέπεια καταλήγουμε στο συμπέρασμα ότι η ανίχνευση υπογραφών απαιτεί μεγαλύτερη υπολογιστική δύναμη σε σύγκριση με την ανίχνευση ανωμαλιών.

Στον αλγόριθμο εκλογής που χρησιμοποιείται σε αυτή την υλοποίηση ευνοούνται οι κόμβοι που έχουν μεγαλύτερη υπολογιστική δύναμη και μεγαλύτερη διάρκεια ζωής της μπαταρίας σε σύγκριση με άλλους κόμβους στο σύμπλεγμα. Για αυτούς τους λόγους τα συστήματα ανίχνευσης παρεισφρήσεων λειτουργούν μόνο στους cluster head κόμβους.

Για ένα προ-αποφασισμένο χρονικό διάστημα, ο cluster head ελέγχει κάθε κόμβο για πιθανές υπογραφές σχετικές με κάποια επίθεση. Αυτό γίνεται κατά τρόπο κυκλικό για όλα τα μέλη του συμπλέγματος. Να σημειωθεί πως η βάση δεδομένων των υπογραφών δεν χρειάζεται συχνή αναπροσαρμογή. Αναπροσαρμογή απαιτείται μόνο όταν ανακαλυφθεί μια νέα επίθεση και η υπογραφή της πρέπει να προστεθεί στη βάση δεδομένων.

2. *Ανίχνευση ανωμαλίας από τον εφεδρικό Cluster Head:*

Το σύστημα ανίχνευσης ανωμαλιών στηρίζεται σε μια μακροπρόθεσμη έρευνα και ταξινόμηση η οποία πραγματοποιείται κατά την ομαλή λειτουργία του δικτύου. Όπως έχει αναφερθεί, τα ad-hoc ασύρματα δίκτυα είναι ιδιαίτερα δυναμικά στη δομή, δίνοντας έτσι αφορμή για τυχαία σχεδιαστικά μοτίβα, καθιστώντας κατά συνέπεια δύσκολο να διαμορφωθεί ένα IDS με λιγοστά λανθασμένα αποτελέσματα. Επομένως σε ένα τέτοιο ιδιαίτερα δυναμικό περιβάλλον, η απλούστερη και πιο αξιόπιστη τεχνική για ένα τέτοιο IDS είναι το threshold based detection [19]. Τα αρχικά κατώτατα όρια τίθενται στο προ εγκατεστημένο IDS για τις τοπικές και τις δικτυακές παραμέτρους που πρόκειται να ελεγχθούν. Έπειτα τα απαιτούμενα δεδομένα για τις δικτυακές παραμέτρους συλλέγονται μέσω του SNMP Simple network management protocol [20,21] και τα δεδομένα για τις τοπικές παραμέτρους μέσω του πυρήνα του λειτουργικού συστήματος. Τέλος τα κατώτατα όρια μπορούν να τροποποιηθούν από κοινού με όλους τους κόμβους-μέλη της συστάδας.

Μερικές από τις γενικές παραμέτρους του δικτύου (παράμετροι κίνησης) που μπορούν να ελέγχονται και να τροποποιούνται είναι:

- ✓ *Forward Percentage (FP):* Το FP καθορίζει την αναλογία των διαβιβασμένων πακέτων προς τα πακέτα που πρέπει να διαβιβαστούν.

$$FP_m = \frac{διαβιβασμένα\ πακέτα}{πακέτα\ προς\ διαβίβαση}$$

- ✓ Επίσης το FP μπορεί να διαιρεθεί περαιτέρω σε τοπικό FP και στο καθολικό FP [22].
- ✓ *Malicious Flooding* σε συγκεκριμένο στόχο: Ελέγχεται ο συνολικός αριθμός των πακέτων για μια χρονική περίοδο για κάθε προορισμό. Εάν είναι μεγαλύτερος από ένα κατώτατο όριο, η επίθεση θεωρείται ως *Malicious Flooding*.
- ✓ Αναπροσαρμογές του πίνακα δρομολόγησης: Ο αριθμός αναπροσαρμογών στον πίνακα δρομολόγησης μπορεί να ελέγχεται σε ανά μια χρονική περίοδο προκειμένου να ανιχνευθούν επιθέσεις [23,24] στην δρομολόγηση του δικτύου.
- ✓ Άλλες παράμετροι όπως το μέγιστο μέγεθος των πακέτων κ.λπ.

3. *Ανίχνευση μεταξύ των κύριων και εφεδρικών Cluster Heads:*

Ο κύριος cluster head εκτελεί την signature detection σε όλους τους κόμβους συμπεριλαμβανομένου και του ίδιου. Ομοίως ο εφεδρικός cluster head εκτελεί anomaly detection σε όλους τους κόμβους συμπεριλαμβανομένου του ίδιου. Ίσως όμως ο κύριος ή ο εφεδρικός cluster head έχει απενεργοποιημένο το IDS του λόγω κάποιας εισβολής που έχει υποστεί. Έτσι απαιτείται ένας δεύτερος βαθμός εξακρίβωσης της αξιοπιστίας επιτρέποντας την signature detection στον κύριο cluster head από τον εφεδρικό και αντίστοιχα anomaly detection από τον κύριο στον εφεδρικό. Να σημειωθεί επίσης πως ο εφεδρικός cluster-head μπορεί να εκτελέσει signature detection σε προκαθορισμένο χρόνο αλλά με υψηλότερη συχνότητα από την ανίχνευση που εκτελείται από τον κύριο cluster head στους κόμβους του συμπλέγματος, ενώ ο master cluster head μπορεί να ελέγξει τον εφεδρικό σε τυχαία βάση.

5.3.3 Intrusion response

Η ιδανική "απάντηση" σε οποιαδήποτε είδους παρείσφρησης για ένα ασύρματο ad-hoc δίκτυο θα ήταν να απομονωθεί ο κόμβος που βρίσκεται υπό επίθεση από το υπόλοιπο δίκτυο. Το παραπάνω συμβαίνει στα σταθερά δίκτυα που εφαρμόζουν την τεχνική αυτή ενημερώνοντας το firewall του δικτύου να αποκλείει τον εκάστοτε κόμβο από τα να εισέλθει στο δίκτυο. Παρόλα αυτά σε μια δυναμικά μεταβαλλόμενη ασύρματη ad-hoc τοπολογία, αυτή η λύση δεν είναι ούτε αποτελεσματική ούτε και η εφαρμογή του firewall εφικτή επίσης.

Προτείνεται λοιπόν η χρήση ενός "counter" πιστοποιητικού, με το οποίο ο master και ο backup cluster head θα μπορούν να απομονώσουν έναν κόμβο από το υπόλοιπο του δικτύου μεταδίδοντας αυτό το πιστοποιητικό για τον συγκεκριμένο κόμβο.

Στην προσέγγιση που προτείνεται συναντώνται οι εξής καταστάσεις:

1) Ο κόμβος Master Cluster Head έχει δεχθεί επίθεση: Αυτή η κατάσταση ανιχνεύεται από τον εφεδρικό cluster head με βάση είτε τα αποτελέσματα της anomaly detection είτε της signature detection. Σε κάθε περίπτωση θα πραγματοποιηθεί εκ νέου επανεκλογή για τους δύο cluster head κόμβους. Ανάλογα με την κατηγορία ανίχνευσης ακολουθούνται οι ανάλογες διαδικασίες:

   - Anomaly Detection: Εάν ο backup cluster head "υποψιαστεί" ότι ο master έχει δεχθεί επίθεση, μεταδίδεται ένα είδος "συναγερμού" στο δίκτυο και ζητείται από τα μέλη του συμπλέγματος η συναίνεσή τους. Έπειτα διεξάγεται ψηφοφορία από τα μέλη του συμπλέγματος σχετικά με την κατάσταση του master cluster head. Η ψηφοφορία μεταξύ των κόμβων διεξάγεται προκειμένου να μειωθούν τα λανθασμένα μηνύματα (λάθος συμπεράσματα) που παράγονται από τα εν ενεργεία IDS. Η τελική λοιπόν απόφαση διαμορφώνεται από την παραπάνω ψηφοφορία. Εάν αποφασιστεί πως ο master cluster head βρίσκεται υπό επίθεση τότε καταργείται από την λίστα των υποψηφίων κόμβων για cluster head (master και backup) στην επόμενη εκλογή.
   - Signature Detection: Δεδομένου ότι η ανίχνευση υπογραφών βασίζεται στις υπογραφές των προηγούμενων επιθέσεων, το αποτέλεσμα της ανίχνευσης θα είναι σίγουρα σωστά και επομένως στην περίπτωση που ανιχνευθεί επίθεση στον master cluster head θα απορριφθεί από την επόμενη εκλογή χωρίς την συναίνεση των υπολοίπων μελών του συμπλέγματος.

2) Ο κόμβος Backup Cluster Head έχει δεχθεί επίθεση: Αυτή η κατάσταση αντίστοιχα με την προηγούμενη περίπτωση, ανιχνεύεται από τον master cluster head με βάση είτε τα αποτελέσματα της anomaly detection είτε της signature detection. Σε κάθε περίπτωση θα πραγματοποιηθεί εκ νέου επανεκλογή για τους δύο cluster head κόμβους. Ανάλογα με την κατηγορία ανίχνευσης ακολουθούνται οι ανάλογες διαδικασίες:

- Anomaly Detection: Εάν ο master cluster head υποψιάζεται ότι ο εφεδρικός έχει δεχθεί επίθεση, μεταδίδεται και σε αυτή την περίπτωση ένα είδος "συναγερμού" στο δίκτυο και ζητείται από τα μέλη του συμπλέγματος η συναίνεσή τους. Ανάλογα με την τελική απόφαση ο εφεδρικός είτε αποκλείεται από την επόμενη εκλογή είτε όχι.
- Signature Detection: Δεδομένου ότι η ανίχνευση υπογραφών βασίζεται στις υπογραφές των προηγούμενων επιθέσεων, το αποτέλεσμα της ανίχνευσης θα είναι απόλυτα σωστό και επομένως στην περίπτωση που ανιχνευθεί επίθεση στον master cluster head θα απορριφθεί από την επόμενη εκλογή χωρίς την συναίνεση των υπολοίπων μελών του συμπλέγματος.

5.3.3 Διαμοιρασμός Δεδομένων (Sharing of data)

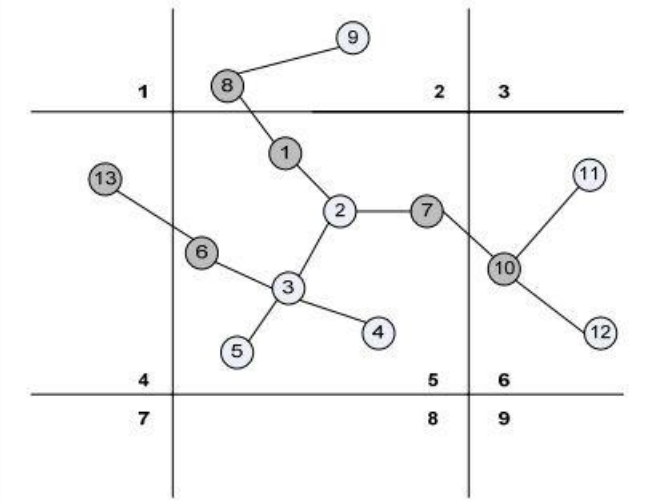
Για να έχουμε συγχρονισμένες βάσεις δεδομένων των υπογραφών (signature) και των ανωμαλιών (anomaly) στο τέλος κάθε εκλογής μεταδίδονται ανανεώσεις από τον master και τον backup cluster head για τις βάσεις δεδομένων προς όλους τους κόμβους. Η αναπροσαρμογή στις βάσεις δεδομένων γίνεται στο τέλος κάθε εκλογής βασιζόμενοι στο γεγονός ότι η ανακάλυψη μιας νέα επίθεσης κατά την διάρκεια μια συγκεκριμένης περιόδου της λειτουργίας του ad-hoc δικτύου είναι ιδιαίτερα σπάνια.

5.3.4 Συμπεράσματα

Το Hierarchical Intrusion Detection System μοντέλο που αναλύθηκε παραπάνω βασίζεται σε ένα Cluster Based δίκτυο δύο επιπέδων. Στο επίπεδο των cluster head κόμβων (backup και master) και στο επίπεδο των απλών μελών-κόμβων του συμπλέγματος. Ιδιαίτερη σημασία έχει το επίπεδο των cluster head κόμβων διότι αποδίδει ιδιαίτερα αυξημένη ασφάλεια στο δίκτυο. Αυτό συμβαίνει διότι ο master cluster head ελέγχεται συνεχώς από τον backup ενώ αντίστοιχα ο master ελέγχει παράλληλα και καθόλη την διάρκεια λειτουργίας του δικτύου, τον backup cluster head. Επιπλέον ο αλγόριθμος επιλογής των backup και master cluster head κόμβων λαμβάνει υπόψη διάφορους παράγοντες των κόμβων του δικτύου προσδίδοντας έτσι αυξανόμενη αποδοτικότητα στην ασφάλεια του ad-hoc δικτύου . Στην υλοποίηση λαμβάνεται υπόψη η υπολογιστή ισχύς και η διάρκεια ζωής της μπαταρίας. Παρόλα αυτά, δίνεται η δυνατότητα τροποποίησης των λαμβανόμενων υπόψη παραμέτρων κατά την διάρκεια της εκλογής. Για παράδειγμα μπορεί να ληφθεί υπόψη η ποιότητα της ζεύξης των κόμβων.

5.4 Zone-Based Intrusion Detection System

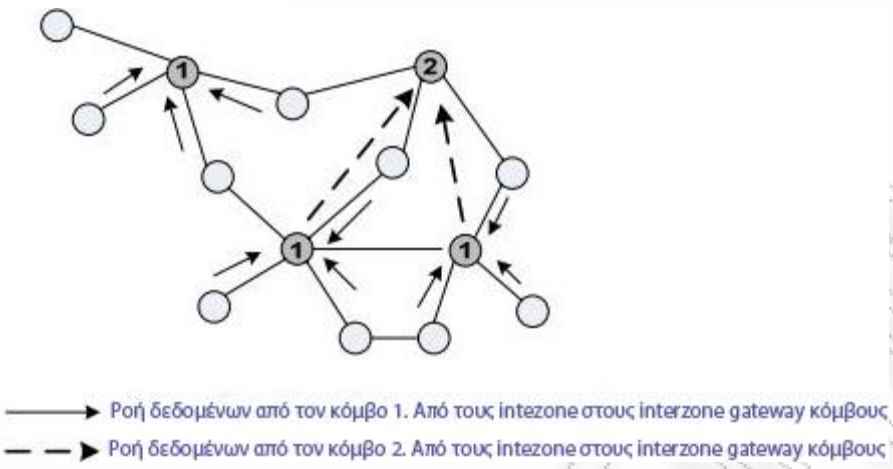
Στην συνέχεια περιγράφεται ένα σύστημα ανίχνευσης παρεισφρήσεων το οποίο βασίζεται σε “δικτυακές ζώνες”. Σε αυτήν την αρχιτεκτονική, το δίκτυο διαιρείται σε ζώνες οι οποίες βασίζονται στον γεωγραφική θέση κάθε κόμβου προκειμένου να ελαττωθεί το “φορτίο” κάθε καναλιού επικοινωνίας βελτιώνοντας παράλληλα την απόδοση της ανίχνευσης εισβολών με την λήψη δεδομένων από πολλούς κόμβους.



Εικόνα 5.4 Δομή ενός Zone-Based IDS σε Ad-Hoc δίκτυο

Οι κόμβοι εντός μιας ζώνης καλούνται “intrazone” κόμβοι, και οι κόμβοι που λειτουργούν ως γέφυρες μεταξύ των ζωνών του δικτύου καλούνται “interzone (gateway)” κόμβοι. Όπως φαίνεται στην εικόνα 5.4 είναι δυνατόν να υπάρξουν περισσότεροι από ένας interzone-gateway κόμβοι σε μια ζώνη, όπως για παράδειγμα οι κόμβοι 1, 6, 7 οι οποίοι λειτουργούν ως γέφυρες για την ζώνη 5 με τις άλλες ζώνες. Κάθε κόμβος στη ζώνη είναι αρμόδιος για τοπική ανίχνευση και αποστολή δεδομένων ασφαλείας στους υπολοίπους interzone κόμβους.

Στόχος της αρχιτεκτονικής αυτής είναι η εύκολη χρήση διαφορετικών τεχνικών ανίχνευσης παρεισφρήσεων σε κάθε έναν πράκτορα του IDS. Να σημειωθεί πως στους πράκτορες των IDSs ανανεώνονται περιοδικά οι πίνακες δρομολόγησης.



Εικόνα 5.5 Ιεραρχία ενός IDS με 2 gateway κόμβους σε μια ζώνη

Οι interzone κόμβοι πραγματοποιούν τοπικό έλεγχο, ενώ οι gateway κόμβοι είναι αρμόδιοι για τον "σφαιρικό" έλεγχο και για την λήψη των τελικών αποφάσεων σχετικά με μια απειλή. Επομένως οι κόμβοι – γέφυρες απαρτίζουν και λειτουργούν σε τελικό στάδιο στην ανίχνευση του δικτύου. Τα δεδομένα που στέλνονται από τους interzone κόμβους παρουσιάζουν απλά μια αξιολόγηση της πιθανότητας εισβολής του δικτύου. Στον αλγόριθμο συνάθροισής για τον προσδιορισμό μιας απειλής - εισβολής, οι gateway κόμβοι εξετάζουν τις ακόλουθες παραμέτρους:

- Classification of attacks. Πιστοποίηση του τύπου εισβολής.
- Time similarity. Αναφέρεται στον χρόνο που συνέβη η εισβολή και στον χρόνος της ανίχνευσης της επίθεσης.
- Source similarity. Έλεγχος του σημείου στο οποίο ανιχνεύθηκε εισβολή. Η παράμετρος αυτή εξετάζεται πρώτα από τις υπόλοιπες έτσι ώστε να μην μειώνεται η απόδοση της ανίχνευσης με την αύξηση των εισβολών.

5.5 Άλλες προσεγγίσεις

5.5.1 Case-Based Agents for Packet-Level Intrusion Detection

Σε μια δημοσίευση του Guha [25] προτάθηκε ένα case-based (ανάλογα την περίπτωση) σύστημα για την ανίχνευση παρεισφρήσεων βασιζόμενα στα ιεραρχικά συστήματα IDSs. Στην προσέγγιση case based γνωστές επιθέσεις διαμορφώνονται ως περιπτώσεις στο αρχείο περιπτώσεων, το οποίο αποθηκεύει χαρακτηριστικά γνωστών προβλημάτων καθώς επίσης και τις ενέργειες προκειμένου να λυθούν τέτοια προβλήματα. Η βασική ιδέα στηρίζεται στην αναζήτηση για παρόμοιες περιπτώσεις στο αρχείο, όταν ανιχνεύεται ένα πρόβλημα στο δίκτυο. Οι επιστρεφόμενες παρόμοιες περιπτώσεις χρησιμοποιούνται καθεμία ως άμεση λύση στο πρόβλημα ειδάλλως ως βάσεις στις οποίες θα διατυπωθεί μια καινούρια περίπτωση.

Στην εκδοχή των Guha και λοιπών, χρησιμοποιούνται οι κανόνες του Snort ως περιπτώσεις και κάθε κόμβος έχει τη δική του βάση δεδομένων από αυτούς τους κανόνες (θεωρείται ότι το μέγεθος της βάσης είναι μικρό). Οι λειτουργίες του διανέμονται σε διαφορετικούς πράκτορες. Μερικές απ' αυτές τις λειτουργίες πραγματοποιούνται σε όλους κόμβους, ενώ άλλοι διανέμονται μόνο σε έναν επίλεκτους.

5.5.2 Specification-Based IDS for AODV

Το πρώτο ***Specification-Based IDS*** σε Ad-Hoc δίκτυο προτάθηκε από τον Tsen [26]. Χρησιμοποιεί ελεγκτές δικτύου (Network Monitors) οι οποίοι καλύπτουν όλους τους κόμβους. Η αρχιτεκτονική αυτή υποθέτει τα εξής:

- Οι network monitors γνωρίζουν τις διευθύνσεις IP και τις MAC addresses όλων των κόμβων, και οι διευθύνσεις MAC δεν μπορούν να επεξεργαστούν - αλλοιωθούν.
- Οι network monitors και τα μηνύματά που διαβιβάζουν είναι ασφαλή.
- Εάν μερικοί κόμβοι δεν αποκρίνονται στην μετάδοση μηνυμάτων, τότε δεν θα προκληθούν σοβαρά προβλήματα.

Οι ελεγκτές δικτύου χρησιμοποιούν Finite State Machines ως προδιαγραφές για την χρήση του AODV, ειδικά για τη διαδικασία ανακάλυψης νέων διαδρομών και για την διατήρηση ενός πίνακα δρομολόγησης για όλους του ελεγχόμενους κόμβους. Κάθε Route Request και Route Reply ελέγχεται από τους network monitors. Όταν ένας ελεγκτής χρειαστεί πληροφορίες για προηγούμενα μηνύματα ή για άλλους κόμβους που δεν βρίσκονται στην αρμοδιότητά του, ρωτάει τους γειτονικούς ελεγκτές δικτύου. Σε περιπτώσεις υψηλής κινητικότητας η επικοινωνία μεταξύ των network monitors

αυξάνεται προκειμένου να υπάρχει πλήρης εικόνα της συνολικής κατάστασης του δικτύου.

Η αρχιτεκτονική αυτή δεν έχει επιβεβαιωθεί πειραματικά ότι είναι αποτελεσματική οπότε μελλοντική εργασία σε αυτή την αρχιτεκτονική περιλαμβάνει τον πειραματισμό με NS-2 δίκτυα, χρήση QoS (Quality of Service) για να μειωθούν λανθασμένα μηνύματα με το διαχωρισμό για παράδειγμα των packet loss, και των packet errors.

Η παραπάνω προσέγγιση όμως φαίνεται ελπιδοφόρα, καθώς μπορεί να ανιχνεύσει γνωστές και άγνωστες επιθέσεις ενάντια στη δρομολόγηση των πρωτοκόλλων που έχουν σαφώς καθορισμένες προδιαγραφές. Όπως υποστηρίζεται είναι ικανό ένα τέτοιο σύστημα να ανιχνεύσει περισσότερες επιθέσεις με ελάχιστους υπολογιστικούς και δικτυακούς πόρους σε πραγματικό χρόνο. Εντούτοις, μερικές από τις υποθέσεις στις οποίες στηρίζεται ένα τέτοιο IDS δεν είναι ιδιαίτερα ρεαλιστικές. Παραδείγματος χάριν, η υπόθεση πως καμία από τις MAC διευθύνσεις δεν μπορεί να αλλοιωθεί από εξωτερικούς παράγοντες. Επιπλέον, η “εξαφάνιση” κάποιων μεταδιδόμενων μηνυμάτων στο δίκτυο μπορεί να έχει σημαντικές επιπτώσεις σε πολλές υπηρεσίες του δικτύου ανάλογα την περίπτωση.

5.5.3 An IDS Architecture with Stationary Secure Database

Η αρχιτεκτονική αυτή αφορά ένα διανεμημένο-ιεραρχικό σύστημα που αποτελείται από πράκτορες ανίχνευσης εισβολών και από μια σταθερή ασφαλή βάση δεδομένων (SSD) [27]. Όλοι οι κόμβοι παρέχουν τοπική ανίχνευση και συνεργάζονται με άλλους πράκτορες εάν χρειαστεί. Οι πράκτορες των IDSs έχουν πέντε συστατικά:

- Τοπικός έλεγχος διαδρομών. Συγκεντρώνει και αποθηκεύει τοπικά δεδομένα δρομολόγησης, δικτυακά πακέτα και δεδομένα συστήματος.
- Τοπική βάση δεδομένων παρεισφρήσεων (LID). Είναι μια βάση δεδομένων που κρατά πληροφορίες διαθέσιμες στους IDS πράκτορες όπως υπογραφές επίθεσης, πρότυπα κανονικής συμπεριφοράς χρηστών, κ.λπ.
- Ασφαλές κανάλι επικοινωνίας. Χρησιμοποιείται μόνο από τους IDS προκειμένου επικοινωνήσουν με ασφάλεια με άλλους πράκτορες.
- Ανιχνευτές ανωμαλιών (ADMs). Χρησιμοποιούνται για την ανίχνευση παρεισφρήσεων. Μπορούν να υπάρξουν περισσότεροι από ένας ADM σε έναν πράκτορα IDS. Παραδείγματος χάριν μπορούν να χρησιμοποιούν διαφορετικές τεχνικές για τον έλεγχο διαφορετικών δεδομένων.
- Ανιχνευτές κακόβουλης χρήσης (MDMs). Χρησιμοποιούνται συνήθως για την ανίχνευση γνωστών εισβολών.

Η σταθερή ασφαλής βάση δεδομένων (SSD) διατηρεί τις πιο πρόσφατες υπογραφές επίθεσης και τα πιο πρόσφατα σχέδια κανονικής συμπεριφοράς των χρηστών. Υποτίθεται πως διατηρείται σε ένα ασφαλές περιβάλλον. Οι κινητοί κόμβοι λαμβάνουν πληροφορίες από την SSD και μεταφέρουν τα logs τους στην SSD για περαιτέρω

επεξεργασία. Η SSD έχει μεγαλύτερη χωρητικότητα αποθήκευσης και υπολογισμού από τους κινητούς κόμβους, έτσι είναι ικανή για γρηγορότερη επεξεργασία των κανόνων συμπεριφοράς. Επιπλέον, η ενημέρωση της SSD πραγματοποιείται ευκολότερα από την ενημέρωση κάθε κόμβου ξεχωριστά. Εντούτοις, μια σταθερή βάση δεδομένων δεν είναι πάντα υλοποιήσιμη σε κάθε δίκτυο. Λύση σε αυτό το πρόβλημα είναι η διατήρηση ξεχωριστών βάσεων δεδομένων σε κάθε κόμβο με αποτέλεσμα όμως την κατανάλωση σημαντικής χωρητικότητας του καναλιού επικοινωνίας.

Κεφάλαιο 6

Cooperative IDS στα Ad-Hoc δίκτυα

6.1 Εισαγωγή

Σε αυτό το κεφάλαιο αναλύεται η δομή ενός Cooperative Intrusion Detection System (CIDS) καθώς και το αντίστοιχο δίκτυο στο οποίο εφαρμόζεται αυτή η μέθοδος ανίχνευσης παρεισφρήσεων. Στην αρχιτεκτονική CIDS κάθε κόμβος στο ασύρματο Ad-Hoc δίκτυο συμμετέχει στην ανίχνευση τυχόν επιθέσεων. Επομένως κάθε κόμβος συνεισφέρει ανεξάρτητα αλλά συνεργάζεται ταυτοχρόνως με τους υπόλοιπους κόμβους προκειμένου να ερευνάται μια μεγαλύτερη περιοχή.

Από τεχνική άποψη, ατομικοί IDS πράκτορες τοποθετούνται σε κάθε κόμβο του δικτύου. Καθένας από τους παραπάνω πράκτορες δραστηριοποιείται ανεξάρτητα και ελέγχει τοπικές δραστηριότητες (συμπεριλαμβανομένων εργασιών του συστήματος και δραστηριοτήτων του δικτύου εντός του πεδίου επικοινωνίας). Επομένως βρίσκεται σε θέση να εντοπίσει τοπικούς συναγερμούς και να ξεκινήσει μια έρευνα. Εάν λοιπόν ανιχνευτεί κάποια ανωμαλία στα δεδομένα, ή έστω ανιχνευθεί κάποιο ίχνος εισβολής και απαιτείται περαιτέρω έρευνα, γειτονικοί IDS πράκτορες θα συνεργαστούν ως ένα καθολικό IDS. Επομένως αυτά τα υποσυστήματα (IDS agents) διαμορφώνουν την συνολική ασφάλεια του ασύρματου Ad-Hoc δικτύου.

6.2 Προκλήσεις κατά την δημιουργία ενός Cooperative IDS

Οι διάφορες μέθοδοι συνεργασίας για την αντιμετώπιση εισβολών σε ένα δίκτυο φαίνεται να είναι ικανές να "αναζωογονήσουν" τις υπάρχουσες τεχνικές προστασίας των δικτύων προσφέροντας δεδομένα και πληροφορίες από πολλές οπτικές γωνίες. Για παράδειγμα πληροφορίες ακόμη σχετικά και με ηλεκτρονικές υπογραφές. Η ανταλλαγή λοιπόν πληροφοριών ασφάλειας μέσα σε ένα δίκτυο μπορεί αποτελεσματικά να αυξήσει την αποτελεσματικότητα της ασφάλειας.

Παρόλα αυτά πρέπει να ικανοποιηθούν διάφορες απαιτήσεις σχετικά με την ανίχνευση της ασφάλειας πριν αυτή δημοσιευθεί στους υπόλοιπους κόμβους του δικτύου. Καταρχήν ο όγκος και μόνο των υπό εξέταση δεδομένων ίσως να οδηγεί μερικές φορές στο να μην αναγνωρίζονται διάφορες απειλές. Να προσπελαύνονται δηλαδή απαρατήρητες. Επιπλέον η συνεχής ανταλλαγή πληροφοριών αυξάνει σημαντικά την πολυπλοκότητα της επικοινωνίας καθώς επίσης και τις ανάγκες για εύρος ζώνης. Τέλος σημαντικές πληροφορίες σχετικά με την ασφάλεια του δικτύου που ανταλλάσσονται μεταξύ των κόμβων, ίσως "δραπετεύσουν" εκτός των επιθυμητών στόχων τους.

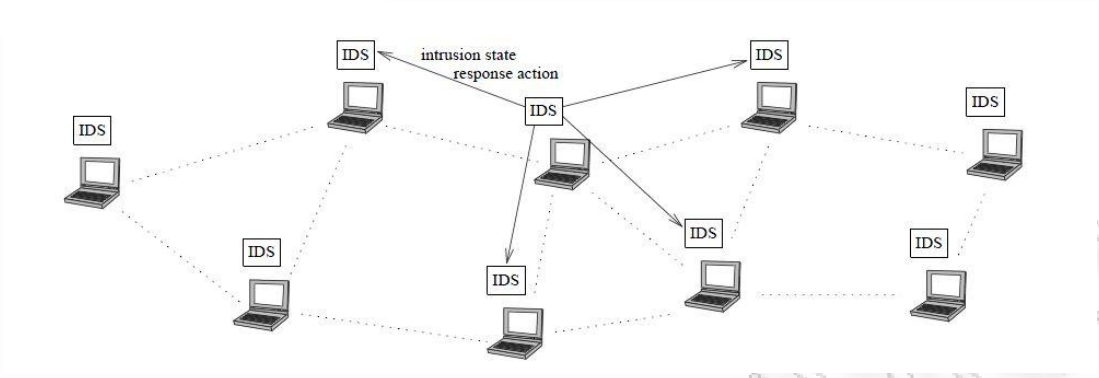
6.3 Αρχιτεκτονική δομής ενός Cooperative IDS

Σε αυτή την ενότητα θα παρουσιαστεί η low-level δομή ενός CIDS η οποία περιλαμβάνει τα ακόλουθα συστατικά μέρη:

- ✓ Στοιχειώδεις ανιχνευτές - Elementary Detectors (EDS)
- ✓ Σειρά αναμονής μηνυμάτων - Message Queue (MQ)
- ✓ Συνδέσμους ιχνηλατών - Connection Tracker
- ✓ Διαχειριστή – Manager
- ✓ Σύστημα απαντήσεων – Response Engine

6.3.1 Elementary Detectors

Οι στοιχειώδεις ανιχνευτές είναι εξειδικευμένοι ανιχνευτές παρεισφρήσεων που διανέμονται εντός του συστήματος σε κάθε πράκτορα. Οι EDs και ο manager μπορούν να βρίσκονται σε διαφορετικούς πράκτορες αλλά επικοινωνούν μέσω μιας γενικευμένης Message Queue που επιτρέπει την επικοινωνία τους, ανεξάρτητα με την τοποθεσία προέλευσης των μηνυμάτων.



Εικόνα 6.1 Δομή ενός Ad-Hoc με Cooperative Intrusion Detection System

Διαφορετικοί πράκτορες έχουν την δυνατότητα να διαθέτουν διαφορετική μορφοποίηση στους EDs. Αυτό αποτελεί μια ιδιαίτερα σημαντική επιλογή δεδομένου ότι σε ένα διανεμημένο-συνεργατικό σύστημα με ετερογενείς υπηρεσίες, αυτές οι διαφορετικές υπηρεσίες στους διαφορετικούς πράκτορες μπορεί να χρειαστούν και διαφορετικά είδη ανιχνευτών.

6.3.2 Message Queue

Οι πράκτορες στους διάφορους κόμβους του συστήματος επικοινωνούν μεταξύ τους χρησιμοποιώντας το Message Queue (MQ). Το τελευταίο χρησιμοποιεί το TCP πρωτόκολλο για να μεταφέρει τα δεδομένα. Κάθε μήνυμα έχει ένα μοναδικά αυξανόμενο σειριακό αριθμό, μια υπογραφή και ένα μυστικό κλειδί το οποίο το μοιράζεται αποκλειστικά με τον manager. Επομένως χωρίς την γνώση του κλειδιού δεν είναι δυνατή η ανάγνωση ενός μηνύματος.

6.3.3 Connection Tracker

Ο Connection Tracker αποτελεί συστατικό μέρος το οποίο αντιστοιχίζει port numbers σε ID ενεργειών, οι οποίες ενέργειες έχουν ενεργές συνδέσεις με τις αντίστοιχες πόρτες. Για αυτό το λόγο παρεμβαίνει συχνά στις δραστηριότητες του συστήματος προκειμένου να δεχτεί νέες συνδέσεις και να τερματίσει όταν αυτό απαιτείται. Για παράδειγμα, ο manager ίσως ζητήσει από τον Connection Tracker να συλλέξει πληροφορίες σχετικά με μια εισβολή (ή έστω και για μια ειδοποίηση) από τον πράκτορα ο οποίος γνωστοποίησε το παραπάνω γεγονός. Επομένως η διαδικασία αυτή πραγματοποιείται ευκολότερα και σε μικρότερο χρόνο δεδομένης της μηχανογράφησης που έχει πραγματοποιήσει ο Connection Tracker.

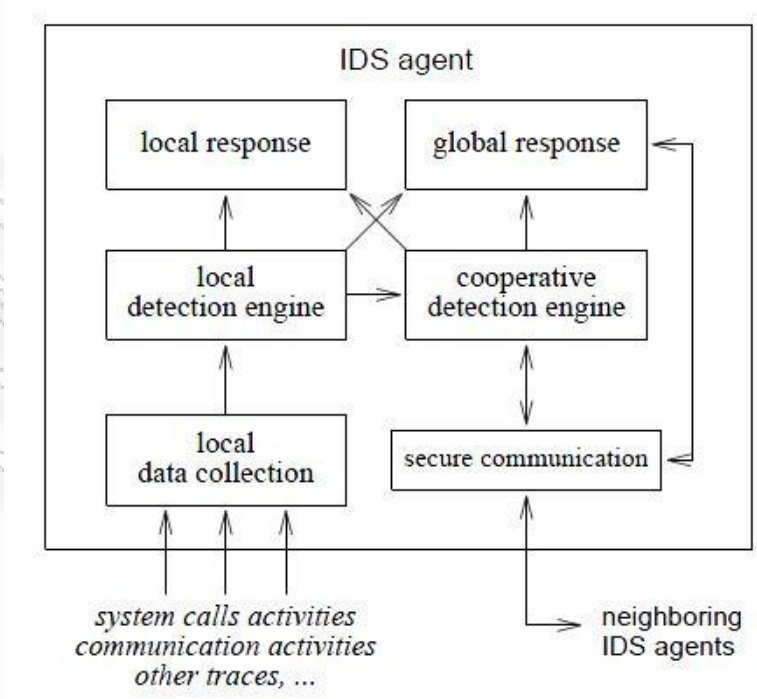
6.3.4 Manager

Ο manager είναι το σημαντικότερο στοιχείο των CIDS και παράλληλα αποτελεί το κλειδί διαφοροποίησης μεταξύ αυτών. Ο manager είναι υπεύθυνος για την συσχέτιση των πληροφοριών από τους διαφορετικούς πράκτορες γεγονός που έχει ως αποτέλεσμα την παραγωγή μιας καθολικά συνδυασμένης απόφασης σχετικά με την ύπαρξη παρείσφρησης. Επομένως από τον manager απαιτούνται εξειδικευμένες λειτουργίες υψηλής αποδοτικότητας και για αυτό το λόγο διαθέτει τα εξής:

- **Translation Engine**: Μετατρέπει την ειδοποίηση που παράγει κάποιος κόμβος, σε μορφή κατανοητή και επεξεργάσιμη από το CIDS.
- **Event Dispatcher**: Αποστέλλει δεδομένα-γεγονότα στους κατάλληλους κάθε φορά κόμβους
- **Inference Engine**: Ο μηχανισμός αυτός αντιστοιχίζει τα εισερχόμενα μηνύματα σε Rules προκειμένου να προκύψει θετική ή αρνητική απάντηση σχετικά με παρείσφρηση.
- **Combining Engine**: Συλλέγει τα διάφορα αποτελέσματα από το Inference Engine και αποφασίζει σχετικά με καθολική απάντηση προς όλους του πράκτορες.

6.4 Δομή πράκτορα

Η εσωτερική δομή ενός πράκτορα συστήματος CIDS είναι αρκετά περίπλοκη αλλά μπορεί να αναπαρασταθεί γενικά σε έξι ενότητες όπως φαίνεται στην εικόνα 6.2. Το component "data collection" είναι υπεύθυνο για την συλλογή των τοπικών δραστηριοτήτων και των καταγεγραμμένων ενεργειών. Έπειτα η μηχανή ανίχνευσης "local detection engine" θα χρησιμοποιήσει τα δεδομένα από το "data collection" για να αναζητήσει τυχόν ανωμαλίες. Στη συνέχεια η μηχανή ανίχνευσης "cooperative detection engine" χρησιμοποιείται σε συστήματα IDS που απαιτούν συνεργασία μεταξύ των πρακτόρων, δηλαδή στα συστήματα ανίχνευσης παρεισφρήσεων που μελετώνται σε αυτό το κεφάλαιο. Η απάντηση σε μια παρείσφρηση προκύπτει από τα components "local response" και "global response". Πιο συγκεκριμένα το "local response" είναι υπεύθυνο για να ειδοποιεί τοπικούς κόμβους, ενώ η δεύτερη για να ειδοποιεί γειτονικούς κόμβους. Τέλος η ενότητα "secure" είναι υπεύθυνη για την ασφαλή μεταγωγή δεδομένων του συστήματος CIDS μεταξύ των κόμβων.



Εικόνα 6.2 Δομή πράκτορα σε co-operative intrusion detection system

6.4.1 Data Collection

Κατά την διαδικασία αυτή συλλέγονται δεδομένα σε πραγματικό χρόνο από διάφορες πηγές. Ανάλογα με τον αλγόριθμο εντοπισμού απειλών, αυτά τα δεδομένα μπορεί να περιλαμβάνουν ενέργειες του συστήματος και των χρηστών στο κόμβο και ενέργειες εντός του πεδίου επικοινωνίας που αφορούν την επικοινωνία μεταξύ άλλων κόμβων. Επομένως μπορεί να συνυπάρχουν πολλές ενότητες "data collection" στον ίδιο κόμβο για ταυτόχρονη συλλογή πολλαπλών τύπων δεδομένων, από πολλαπλές πηγές και τέλος διαφόρων τύπων.

6.4.2 Local Collection

Κατά την διαδικασία αυτή αναλύονται τα δεδομένα τα οποία παρέχονται από την προηγούμενη ενότητα προκειμένου να εντοπιστούν τυχόν ανωμαλίες. Γίνεται εύκολα αντιληπτό πως ο αριθμός των νεοδημιουργηθέντων τύπων επιθέσεων προοριζόμενες για τα ασύρματα δίκτυα αυξάνεται με ταχύτατο ρυθμό όσο συσκευές αποκτούν ασύρματες ιδιότητες. Επομένως δεν είναι εφικτό να δημιουργηθούν απλά μερικοί κανόνες που να αναλύουν τα δεδομένα και να ανιχνεύουν όλες τις υπάρχουσες απειλές. Να σημειωθεί πως δύσκολη και απαιτητική εργασία είναι επίσης η περιοδική ανανέωση αυτών των κανόνων σε ένα ασύρματο δίκτυο Ad-Hoc. Σύμφωνα με τα παραπάνω προκύπτει πως σε ενός τέτοιου τύπου δίκτυο είναι προτιμότερο να διατηρούνται τεχνικές στατικής ανίχνευσης παρεισφρήσεων. Τέτοιες τεχνικές και διαδικασίες περιλαμβάνουν:

- Συνηθισμένα προφίλ – μοντέλα κίνησης: Υπολογίζονται χρησιμοποιώντας δεδομένα από το Data Collection τα οποία έχουν προέλθει από διαδικασία "εκπαίδευσης" του δικτύου όπου όλες οι διαδικασίες συμπεριφέρονται απολύτως "συνηθισμένα".
- Αποκλίσεις: Οι αποκλίσεις από το συνηθισμένο προφίλ καταγράφονται κατά το στάδιο της "δοκιμής" όπου στο στάδιο αυτό καταχωρούνται συνηθισμένες και ασυνήθιστες συμπεριφορές του δικτύου.
- Ανιχνεύσεις: Ένα μοντέλο ανιχνεύσεων σχεδιάζεται από τις αποκλίσεις του συστήματος σε συνεργασία με την συνηθισμένη συμπεριφορά. Να σημειωθεί πως πάντα καθώς επανασχεδιάζεται ένα μοντέλο ανιχνεύσεων, θα υπάρχουν και νέες προσθήκες.

6.4.3 Cooperative Detection

Κάθε κόμβος ο οποίος εντοπίζει κάποιου είδους παρείσφρηση ή ανωμαλία και είναι "πεπεισμένος" πως αποτελεί απειλή στο σύστημα τότε του δίνεται το δικαίωμα να καθορίσει ανεξάρτητα τον τύπο της απειλής και να το γνωστοποιήσει στο δίκτυο. Παρόλα αυτά αν ο πράκτορας εντοπίσει απειλή για την οποία δεν είναι σίγουρος για την επικινδυνότητα της, τότε ξεκινά την διαδικασίας της ανίχνευσης της απειλής σε συνεργασία με γειτονικούς κόμβους, γεγονός το οποίο αποτελεί και το κύριο χαρακτηριστικό των CIDSs.

Το επίπεδο εμπιστοσύνης για κάθε απειλή διαμορφώνεται ως εξής:

- "p% εμπιστοσύνη, ο κόμβος A συμπεραίνει σε συνεργασία με τους τοπικούς πράκτορες πως το δίκτυο έχει δεχθεί εισβολή"

- “p% εμπιστοσύνη, ο κόμβος Α συμπεραίνει από το τοπικά δεδομένα που του παρέχονται αλλά και από τις γειτονικές καταστάσεις πως υπάρχει παρείσφρηση στο δίκτυο.”
- “p% εμπιστοσύνη, οι κόμβοι A,B,C … σταδιακά συμπεραίνουν πως υπάρχει εισβολή στο δίκτυο.”

και με περισσότερα στοιχεία:

- “p% εμπιστοσύνη, ο κόμβος Α συμπεραίνει από γειτονικά δεδομένα πως ο κόμβος Χ βρίσκεται σε κίνδυνο.”

Το επόμενο βήμα του component αυτού είναι η κατασκευή ενός αλγορίθμου για να αναπροσαρμόσει τις τεχνικές ανίχνευσης παρεισφρήσεων του υπάρχοντος κόμβου για να συμπεριλαμβάνει και τον πιο πρόσφατο κίνδυνο. Να σημειωθεί πως ο εκάστοτε αλγόριθμος μπορεί να περιλαμβάνει μεθόδους “βαρύτητας”. Δηλαδή ένας κόμβος επηρεάζεται περισσότερο (κατά την λήψη μιας απόφασης σχετικά με απειλή ή ανωμαλία) από τοπικούς κόμβους ή γενικότερα από τους πλέον πλησιέστερους.

Για παράδειγμα ένα σύστημα ανίχνευσης παρεισφρήσεων που περιλαμβάνει μεθόδους “πλειοψηφίας” μπορεί να συμπεριλαμβάνει τα ακόλουθα στάδια:

1 Ο κόμβος στέλνει σε γειτονικό κόμβο μια “αίτηση κατάστασης απειλής ή ανωμαλίας”.

2 Κάθε κόμβος (συμπεριλαμβανομένου του αιτηθέντος) διαμορφώνει την κατάσταση των πληροφοριών, δείχνοντας με αυτό τον τρόπο την πιθανότητα σε τοπικούς και γειτονικούς κόμβους για το εάν πρόκειται για απλή ανωμαλία ή για απειλή.

3 Έπειτα κάθε κόμβος καθορίζει εάν η πλειοψηφία των ληφθέντων αναφορών δείχνει εάν πρόκειται για απειλή ή για ανωμαλία. Εάν ναι τότε ανακοινώνει στο δίκτυο πως αυτό βρίσκεται υπό επίθεση.

4 Κάθε κόμβος που ανιχνεύει την απειλή μπορεί να ξεκινήσει τις διαδικασίες που περιέχονται στα components “global response” και “local response”.

Η λογική πίσω από αυτή τη μεθοδολογία έχει ως εξής: Δεδομένα από άλλους κόμβους δεν μπορούν εύκολα να εμπιστευθούν και δεν πρέπει, επειδή οι έχοντες υποστεί εισβολή κόμβοι ίσως στέλνουν παραποιημένα δεδομένα. Επομένως απαιτείται η πλειοψηφία των κόμβων προτού να εκδοθεί κάποια απόφαση σχετική με την ασφάλεια του δικτύου.

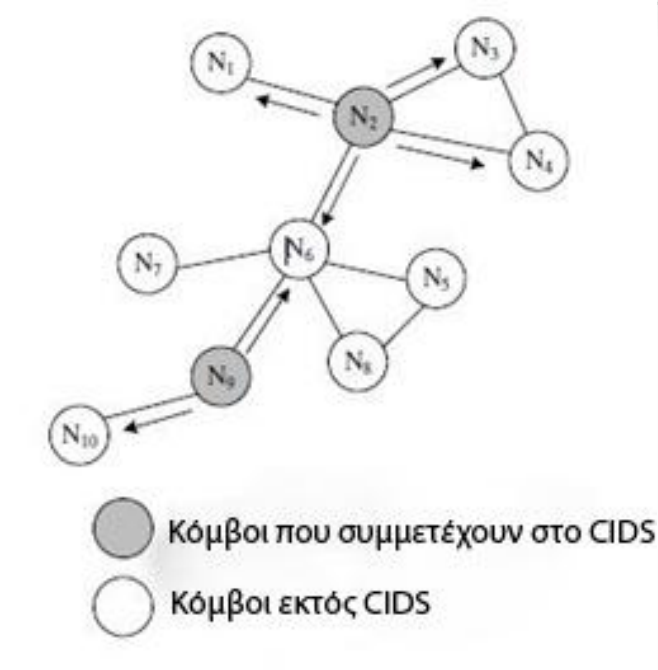
Στα ασύρματα δίκτυα που μελετώνται βέβαια, η τοπολογία είναι δυναμική επειδή κόμβοι εισέρχονται και εξέρχονται συνεχώς εντός του και εκτός του δικτύου αντίστοιχα. Για αυτό το λόγο ενώ κάθε κόμβος βασίζεται συνήθως σε τοπικούς και γειτονικούς προκειμένου να αποφανθεί κάποιο αποτέλεσμα δεν βασίζεται ποτέ αποκλειστικά σε συγκεκριμένους κόμβους αλλά στις αναφορές της πλειοψηφίας αυτών.

6.4.4 Intrusion Response

Ο τύπος της απάντησης σε μία εισβολή σε ένα ασύρματο δίκτυο Ad-Hoc εξαρτάται από τον τύπο της ίδιας της εισβολής, τον τύπο των πρωτοκόλλων του δικτύου και την σιγουριά για την εισβολή-απειλή. Για παράδειγμα απάντηση σε μία εισβολή μπορεί να είναι ένα από τα παρακάτω:

- Επαναρχικοποίηση του καναλιού επικοινωνίας μεταξύ 2 κόμβων.
- Αναγνώριση των υπό εισβολή κόμβων και αναδιοργάνωση του δικτύου προκειμένου να αποκλειστούν από το δίκτυο.

Πιο συγκεκριμένα, ένας IDS πράκτορας μπορεί να ειδοποιήσει έναν τελικό χρήστη, ο οποίος με την σειρά του ίσως διεξάγει την δική του έρευνα σχετικά με κάποια προειδοποίηση – απειλή. Επίσης μπορεί να σταλθεί αίτηση "επαλήθευσης ταυτότητας" απαιτώντας από τους τελικούς χρήστες να πιστοποιήσουν την ταυτότητά τους. Επομένως έπειτα από αυτή την ενέργεια μόνο πιστοποιημένοι χρήστες θα μπορούν να εισέλθουν στο δίκτυο.



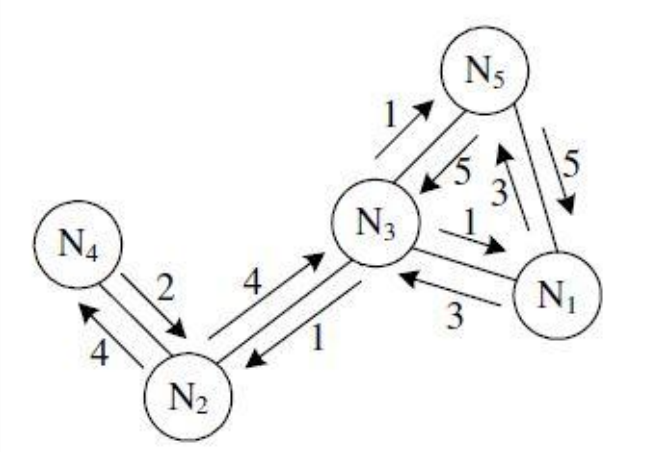
Εικόνα 6.3 Εναλλακτική δομή δικτύου βασισμένου σε CIDS

6.5 Μείωση παραγόμενων λανθασμένων συναγερμών (CIDS)

Υποθέτουμε πως το δίκτυο μας διαμορφώνεται ως μια μη ευθυγραμμισμένη γραφική παράσταση G=(N, E), όπου N = {N1,…, Nx} είναι το σύνολο των κινητών κόμβων. Χρησιμοποιούμε όπως είναι φυσικό CIDS όπου κάθε κόμβος στο δίκτυο συμμετέχει στην ανίχνευση των παρεισφρήσεων . Επιπλέον, κάθε κόμβος τρέχει ένα IDS για να εκτελέσει διαδικασίες τοπικής συλλογής δεδομένων και ανίχνευσης ανωμαλιών. Στην περιγραφή και μελέτη που ακολουθεί λαμβάνουμε υπόψη δύο κοινές παρεισφρήσεις:

- **Cache poisoning**: Ο εισβολέας έχει τη δυνατότητα να αλλοιώσει τον πίνακα δρομολόγησης, να τροποποιήσει το περιεχόμενο του διαγράφοντας πληροφορίες ή ενημερώνοντάς τον με ψεύτικες.
- **Malicious flooding**: Ο εισβολέας πλημμυρίζει τον εκάστοτε κόμβο ή ολόκληρο το δίκτυο με μεγάλου μεγέθους πακέτα. Αυτό έχει ως αποτέλεσμα την απορρόφηση των πόρων του κάθε συστήματος. Το τελευταίο είναι ιδιαίτερα ενοχλητικό σε περιπτώσεις όπου το hardware των κόμβων λειτουργεί με μπαταρία μόνο, όπου και η διάρκεια ζωής της καταναλώνεται γρηγορότερα.

Το μοντέλο του δικτύου το οποίο αναλύουμε παρουσιάζεται στο σχήμα 6.4:



Εικόνα 6.4 Ενδεικτική δομή μελετώμενου δικτύου

Καθορίζουμε αντίστοιχα τα σύνολα cache poisoning και malicious flooding ως εξής: C = {0, 1} και M = {0, 1}. Κάθε κόμβος είναι σε θέση να ανιχνεύσει και τις δύο παραπάνω παρεισφρήσεις. Καθορίζουμε μία «ένα προς ένα χαρτογράφηση» για το O από το σύνολο των κόμβων N μέχρι το C × M. Για παράδειγμα το O: N → C × M, όπου O (Ni) = (Ci, mi) σημαίνει πως ο Ni κόμβος έχει ανιχνεύσει cache poisoning επίθεση, εάν το Ci (mi) είναι ίσο με το ένα ειδάλλως δεν έχει ανιχνεύσει.

Τα παραπάνω σύνολα θα χρησιμοποιηθούν αργότερα προκειμένου να υποδεικνύουν εάν ο αντίστοιχος κόμβος έχει ανιχνεύσει παρείσφρηση ή όχι. Παραδείγματος χάριν, εάν έχει ανιχνευθεί εισβολή τύπου cache poisoning από έναν κόμβο τότε το c θα ισούται με το ένα διαφορετικά με το 0. Το αποτέλεσμα αυτό θα ποικίλλει από έναν κόμβο σε άλλο σύμφωνα με το πόσο ο αντίστοιχος κόμβος ενδιαφέρεται για την ανίχνευση μια παρείσφρησης που παρόλο που δεν την δέχτηκε ο ίδιος ο κόμβος θα μπορούσε να είχε κάποια επίδραση σε αυτόν.

6.5.1 Κατηγορίες ασφάλειας του CIDS

Οι λανθασμένοι συναγερμοί θεωρούνται ως ένα από τα κυριότερα προβλήματα το οποίο πρέπει να αντιμετωπιστεί από τα σημερινά IDS καθώς τα καθιστά λιγότερο αξιόπιστα. Σε αυτή την παράγραφο παρουσιάζονται τεχνικές προκειμένου να αυξηθεί η αποδοτικότητα ενός Cooperative IDS με την μείωση των λανθασμένων συναγερμών. Αυτό αρχικά επιτυγχάνεται με την λειτουργίας μιας συνάρτησης (f) που αντιπροσωπεύει και τις δύο

επιθέσεις (*cache poisoning* και *malicious flooding*) και χαρτογραφεί την σοβαρότητα μιας παρείσφρησης στην αντίστοιχη κατηγορία ασφάλειάς της. Επιπλέον, ένα σύνολο κατώτατων ορίων χρησιμοποιείται προκειμένου να συντονιστούν οι κατηγορίες ασφαλείας έτσι ώστε να υπάρξει ένα αξιόπιστο IDS.

Η συνάρτηση f ορίζεται ως εξής:

$$f(N_i) = c_i \frac{NFP(N_i)}{NR\_ack(N_i)} + m_i \frac{NRP(N_i)}{ENRP(N_i)} \qquad (6.1)$$

Όπου:

- $NFP(N_i)$ είναι ο αριθμός των πακέτων που διαβιβάζονται από τον κόμβο Ni.
- $NR\_ack(N_i)$ είναι ο αριθμός των λαμβανόμενων εξακριβώσεων από τον Ni κόμβο.
- $NRP(N_i)$ είναι ο αριθμός των λαμβανόμενων πακέτων από τον κόμβο Ni.
- $ENRP(N_i)$ είναι ο αναμενόμενος αριθμός λαμβανόμενων πακέτων από τον Ni κόμβο.

Όπως αναφέρθηκε προηγουμένως, η συνάρτηση είναι ικανή να ανιχνεύει και τα δύο είδη περιπτώσεων εισβολών τα οποία μελετώνται.

Εάν ο κόμβος δεν λάβει οποιαδήποτε εξακρίβωση για τα πακέτα που έστειλε, υποθέτει πως τα πακέτα δεν έφθασαν στους προορισμούς τους και επομένως το NR_ack θα είναι μικρότερο από το NFP. Αυτό σημαίνει πως υπάρχει πρόβλημα στο πρωτόκολλο δρομολόγησης και θα μπορούσε να οφείλεται σε μια επίθεση cache poisoning. Όσο υψηλότερο είναι το ποσοστό απωλειών, τόσο μεγαλύτερη και η πιθανότητα της απειλής τύπου cache poisoning. Παραδείγματος χάριν, εάν NFP του κόμβου 1 είναι ίσο με 20 και NR_ack του ίδιου κόμβου είναι ίσο με 5 συνεπάγεται πως η αναλογία είναι 4 ενώ σε κανονικές περιπτώσεις η αναλογία αυτή θα πρέπει να είναι ίση με 1.

Εάν ο κόμβος λάβει πακέτα με ένα ποσοστό που είναι μεγαλύτερο από το αναμενόμενο ποσοστό, δηλ., NRP(Ni) > ENRP(Ni), τότε είναι πιθανό πως το δίκτυο έχει υποστεί εισβολή τύπου malicious flooding. Όσο υψηλότερο το ποσοστό απώλειας, τόσο μεγαλύτερη και η πιθανότητα εισβολής τύπου malicious flooding. Παραδείγματος χάριν, εάν το NRP του κόμβου 1 είναι ίσο με 40 και το ENRP_ack του ίδιου κόμβου είναι ίσο με 10 συνεπάγεται πως η αναλογία είναι ίση με 4, ενώ σε κανονικές περιπτώσεις η αναλογία πρέπει ισούται με 1. Αυτό δείχνει την πιθανότητα ύπαρξης κακόβουλου κόμβου που επιτίθεται πλημμυρίζοντας το δίκτυο (malicious flooding επίθεση). Να σημειωθεί πως η τιμή του ENRP (Ni) εξαρτάται από την φάση εκπαίδευσης του δικτύου.

Η συνάρτηση f(Ni) απεικονίζει τη δριμύτητα μιας επίθεση που αντιλαμβάνεται ο κόμβος Ni. Να σημειωθεί πως η συνάρτηση αυτή παραμετροποιείται ιδιαίτερα εύκολα, στην περίπτωση που χρειάζεται να μελετηθούν άλλα είδη επιθέσεων. Παρόλα αυτά στην διπλωματική αυτή εργασία παρουσιάζονται μόνο οι δύο αυτοί τύποι επιθέσεων δεδομένου

πως θέλουμε απλά να περιγράψουμε πως μειώνονται οι λανθασμένοι συναγερμοί που παράγει ένα CIDS από μία πιο γενικευμένη άποψη.

Για να μειωθούν τα παραγόμενα λανθασμένα μηνύματα, η κατηγορία των κλάσεων θα πρέπει να είναι CL = {cl1,…, clk}. Αυτό θα έχει ως αποτέλεσμα την καλύτερη απόκριση του συστήματος, δεδομένης της γνώσης της κατηγορίας ασφάλειας στην οποία βρίσκεται η εκάστοτε απειλή. Το CIDS που παρουσιάζεται, αποτελείται από k κατηγορίες κλάσεων και κάθε κατηγορία αντιπροσωπεύει τη δριμύτητα της επίθεσης.

Στη συνέχεια παρουσιάζεται το σύνολο των κ-1 κατωτάτων ορίων T, προκειμένου να κατηγοριοποιηθούν οι κατηγορίες ασφαλείας όπου $T=\{t_1,\ldots,t_{k-1}\}$. Επομένως η συνολική συνάρτηση F διαμορφώνεται ως εξής:

$$F(N) = \sum_{N_i \in N} r_{N_i} xf(N_i) \qquad (6.2)$$

Όπου το r_{N_i} αντιπροσωπεύει την "φήμη" του κόμβου Ni. Η παραπάνω συνάρτηση χρησιμοποιείται από έναν κόμβο όταν υποπτεύεται κάποιου είδους εισβολή και ζητά από τους υπόλοιπους κόμβους του δικτύου να εξετάσουν και αυτοί για την συγκεκριμένη απειλή. Επιπλέον συνοψίζει την σοβαρότητα των επιθέσεων που δημοσιεύονται από κάθε κόμβο N_i, ενώ παράλληλα υπολογίζεται και η "φήμη" κάθε κόμβου. Να σημειωθεί πως η φήμη του κάθε κόμβου υπολογίζεται από στατιστικά δεδομένα του κάθε κόμβου από προηγούμενες συμπεριφορές του και παίρνει τιμές από το 0 έως το 1. Οι κατηγορίες ασφαλείας διαμορφώνονται ως:

$$CL=\begin{cases} cl_1 \text{ εάν } F(N) < t_1 \\ cl_i \text{ εάν } t_{i-1} \leq F(N) < t_i : i \in [2, k-1] \\ cl_k \text{ εάν } F(N) < t_{k-1} \end{cases} \qquad (6.3)$$

Κατηγοριοποιώντας λοιπόν την σημασία μιας εισβολής στις αντίστοιχες κατηγορίες ασφαλείας, βοηθά στην μείωση των πιθανών λανθασμένων μηνυμάτων και δίνει στο σύστημα αρκετά ακριβέστερες πληροφορίες για την εκάστοτε εισβολή.

Όλα τα παραπάνω αποτελούν ένα μεγάλο κομμάτι της θεωρητικής ανάλυσης ενός CIDS. Προκειμένου να αναπαρασταθεί αυτό το μοντέλο θα χρησιμοποιηθεί το μοντέλο των συνεργατικών παιχνιδιών.

6.5.2 Cooperative Game Theory

Ο σχεδιασμός και η ανάλυση του προτεινόμενου μοντέλου θα πραγματοποιηθεί όπως αναφέρθηκε και προηγουμένως με την θεωρία «Cooperative Game Theory». Οι l κινητοί

κόμβοι θα μοντελοποιηθούν ως ένα σύνολο *N από l* παίκτες και σε ένα παιχνίδι *N-παικτών* με *N={N1,…Nl}.*

Στην συνέχεια παρουσιάζονται οι σχέσεις μεταξύ των στοιχείων στο μοντέλο των συνεργατικών παιχνιδιών:

$$\Delta \subseteq \mathrm{N} \text{ και } x \in \Delta,$$

$$O(x)=(1,1) \text{ ή } O(x)=(0,1) \text{ ή } O(x)=(1,0) \qquad (6.4)$$

Παραπάνω καθορίζεται μια συνάθροιση από ένα σύνολο κόμβων, όπου κάθε κόμβος αναφέρει τουλάχιστον ενός είδους επίθεση. Επομένως κάθε κόμβος στο Δ αναφέρει απειλές στο δίκτυο. Επιπλέον το δ αντιπροσωπεύει τον αριθμό των συναθροίσεων στο δίκτυο. Εφαρμόζοντας την συνολική σχέση στο σύνολο Δ, έχουμε

$$\sum_{x \in \Delta} r_x \, x \, f(x)$$

,προκειμένου να αναθέσουμε την εκάστοτε εισβολή στην αντίστοιχη κατηγορία ασφαλείας cl_j. Η εφαρμογή του προσδοκώμενου ορίου συνεισφοράς του κάθε παίκτη (κόμβου) στο παιχνίδι αναπαριστάται από την τιμή Shapley [Αναφορά 28 κεφάλαιο 6].

Προκειμένου να υπολογιστεί η συνεισφορά του κόμβου N_i στην συνάθροιση Δ, θεωρούμε όλες τις διαφορετικές μεταθέσεις για τους κόμβους Π_Δ, στην συνάθροιση. Έπειτα υπολογίζεται η διαφορά μεταξύ της συνάρτησης που περιλαμβάνει όλες τις μεταθέσεις μέχρι και τον κόμβο N_i και της συνάρτησης που περιλαμβάνει όλες τις μεταθέσεις μέχρι πριν τον κόμβο N_i . Καθορίζεται επίσης ως $P_\pi^{N_i}$ το σύνολο από κόμβους πριν τον N_i με $\pi \in \Pi_\Delta$. Έπειτα υπολογίζοντας τον μέσο όρο από τις παραπάνω διαφορές προκύπτει το όριο συνεισφοράς του κόμβου N_i στην συνάθροιση Δ. Δηλαδή η συνεισφορά έχει ως εξής:

$$\Phi_{\mathrm{N}_i}(\Delta) = \frac{1}{\delta!} \sum_{\pi \in \Pi_\Delta} F(P_\pi^{Ni} \cup \{\mathrm{N}_i\}) - F(P_\pi^{Ni}) \qquad (6.5)$$

Αντικαθιστώντας το $F(P_\pi^{Ni} \cup \{\mathrm{N}_i\})$ με $\sum_{x \in P_\pi^{Ni} \cup \{\mathrm{N}_i\}} r_x x f(x)$

και το $F(P_\pi^{Ni})$ με $\sum_{x \in P_\pi^{Ni}} r_x x f(x)$ η εξίσωση (6.5) διαμορφώνεται πλέον ως:

$$\Phi_{\mathrm{N}i}(\Delta) = \frac{1}{\delta!} \sum_{\pi \in \Pi_\Delta} F(\{\mathrm{N}_i\}) \qquad (6.6)$$

η οποία γράφεται και ως:

$$\Phi_{\mathrm{N}i}(\Delta) = F(\{N_i\}) \qquad (6.7)$$

Προκείμενου να υπολογιστεί το όριο συνεισφοράς (τιμή Shapley) του κόμβου N_i στο δίκτυο πρέπει να υπολογιστεί ο μέσος όρος όλων των πιθανών συναθροίσεων ο οποίος δίνεται από:

$$\Phi_{Ni} = \frac{1}{\gamma} \sum_{N_i \in \Delta, \Delta \in N} F(\{N_i\}) \qquad (6.8)$$

Όπου το γ είναι ο αριθμός των πιθανών συναθροίσεων στο δίκτυο. Συναθροίσεις με αρκετή ισχύ έτσι ώστε να εναντιωθούν σε μια απόφαση ονομάζονται «winning coalitions». Στο συγκεκριμένο παράδειγμα *winning coalitions* υπάρχει όταν η τιμή της σχέσης αυτής μπορεί να αλλάξει την κατηγορία ασφάλειας. Επομένως, η τιμή της κάθε συνάθροισης είναι είτε 1 είτε 0. 1 είναι στην περίπτωση που υπάρχει winning coalitions και 0 διαφορετικά. Έτσι η επίδραση του κόμβου N_i στην κατηγορία ασφάλειας cl_i μπορεί να γραφτεί ως $\frac{1}{\gamma}|\Delta'|$, όπου $|\Delta'|$ είναι το σύνολο των winning coalitions. Για παράδειγμα $\Sigma_{N_i \in \Delta'} F(\Delta') \geq t_i$.

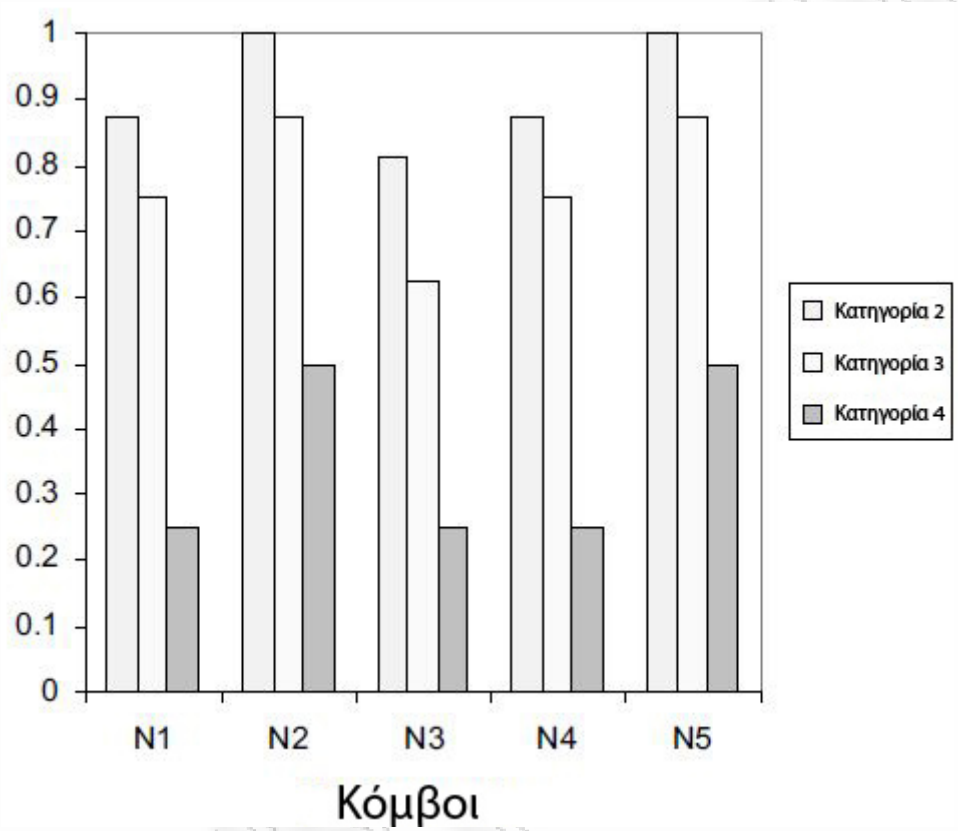
Η τιμή Shapley του κόμβου N_i αναπαριστά την σχετική συνεισφορά για ένα δοσμένο κατώτατο όριο t_i. Επομένως οι τιμές των κατωτάτων ορίων μπορούν να διαμορφωθούν χρησιμοποιώντας στατιστικά δεδομένα και αυτό γίνεται προκειμένου να μειωθούν τα λανθασμένα μηνύματα των κόμβων. Η παραπάνω διαδικασία αποδεικνύει την σημαντικότητα της ανάλυσης της σχετικής συνεισφοράς ενός κόμβου σχετικά με την απόφαση για μια κατηγορία ασφαλείας. Το παράδειγμα που αναλύεται παρουσιάζεται στην επόμενη παράγραφο με γραφήματα και περιορισμένα θεωρητικά στοιχεία:

Έστω 5 κινητοί κόμβοι οι οποίοι επικοινωνούν σε ένα ασύρματο δίκτυο όπως αυτό παρουσιάστηκε στην εικόνα 6.4. Θεωρούμε ότι ένας από τους κόμβους έλαβε ασυνήθιστο αριθμό από αιτήματα σχετικά με την δρομολόγηση των πληροφοριών και του δικτύου. Ο κόμβος που αναγνώρισε αυτό το ασυνήθιστο φαινόμενο πρέπει να ελέγξει εάν αυτό το ποσό των αιτημάτων οφείλεται στην απώλεια συνδέσεων του δικτύου, στην αποχή πολλών κόμβων από το δίκτυο ή σε εισβολή τύπου malicious flooding. Έτσι, ο συγκεκριμένος κόμβος πρέπει να συνεργαστεί με τους γειτονικούς έτσι ώστε να αποφασίσει εάν έχει υπάρξει επίθεση ή όχι.

Έστω πως υπάρχουν οι ακόλουθες κατηγορίες ασφάλειας CL = {cl_1, cl_2, cl_3, cl_4} και έστω επίσης πως το κατώτατο όριο καθορίζεται ως T = {2, 4, 6}. Επιπλέον οι κατηγορίες ασφάλειας ταξινομούνται ως εξής: $cl_1 < 2$, $2 \leq cl_2 < 4$, $4 \leq cl_3 < 6$, $cl_4 \geq 6$. Η φήμη των κόμβων αντίστοιχα για κάθε κόμβο είναι: $r_1 = 0.5$, $r_2 = 0.8$, $r_3 = 0.2$, $r_4 = 0.5$, $r_5 = 0.6$, και f(1) = 3, f(2) = 4, f(3)=1, f(4)=2, f(5)=5. Με χρήση της σχέση (8), προκύπτει στον ακόλουθο πίνακα η συμμετοχή κάθε κόμβου στην ανίχνευση της παρείσφρησης.

Κόμβος	*N1*	*N2*	*N3*	*N4*	*N5*
Τιμή Συνεισφοράς	*19.2*	*40.96*	*2.56*	*12.8*	*38.4*

Χρησιμοποιώντας το $\frac{1}{\gamma}|\Delta'|$, προκύπτει η συνεισφορά του κάθε κόμβου σε κάθε κατηγορία ασφάλειας όπως φαίνεται στην παρακάτω εικόνα 6.5. Εκεί φαίνεται ότι η συνεισφορά του N3, μαζί με άλλους κόμβους στην συνάθροιση, αλλάζει την κατηγορία ασφάλειας στου CIDS από cl_3, σε cl_4, το οποίο πρακτικά σημαίνει πως το ρίσκο από μια εισβολή είναι μεγάλο και απαιτείται άμεση τοπική ή γειτονική απάντηση για την συγκεκριμένη εισβολή.



Εικόνα 6.5 Συνεισφορά κάθε κόμβου σε κάθε κατηγορία ασφάλειας

Έπειτα χρησιμοποιώντας την σχέση $\Sigma_{N_i \in \Delta'} F(\Delta') \geq t_i$ προκύπτει το winning coalition, το οποίο αποφασίζει για την αλλαγή από την κατηγορία ασφάλειας cl_3 στην cl_4 όπου το N_3 ανήκει στις ακόλουθες συναθροίσεις: {{N2,N3,N5}, {N1,N2,N3,N5}, {N2,N3,N4,N5} και {N1,N2,N3,N4,N5}}.

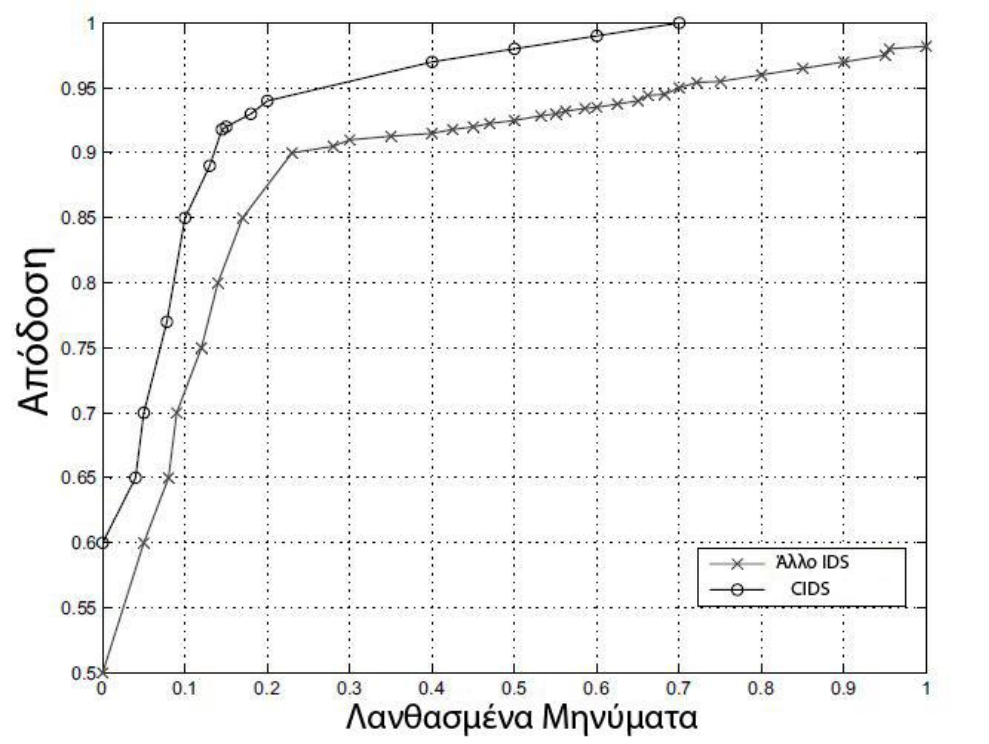
6.5.2 Αποτελέσματα ανάλυσης

Για την προσομοίωση του μοντέλου που περιγράφεται παραπάνω χρησιμοποιήθηκε σε μια δημοσίευση εφαρμογή GloMoSim (έκδοση 2) και το πρωτόκολλο δρομολόγησης AODV. Η τοπολογία του δικτύου κάλυπτε τετράγωνο 500 μέτρων μήκους και πλάτους με 30 κινητούς κόμβους. Ο χρόνος προσομοίωσης ήταν 300 δευτερόλεπτα. Το συγκεκριμένο πρότυπο (CIDS) συγκρίθηκε με ένα κλασσικό πρότυπο ανίχνευσης παρεισφρήσεων. Δηλαδή κάθε κόμβος διαθέτει το δικό του IDS και όταν ανιχνεύσει κάποια ανωμαλία με λίγα διαθέσιμα δεδομένα ενημερώνει και ενημερώνεται παράλληλα από τους διπλανούς κόμβος. Θεωρείται επίσης πως υπάρχουν 4 κατηγορίες ασφαλείας.

Κατά την φάση εκπαίδευσης του συστήματος, κάτι το οποίο έχει αναφερθεί νωρίτερα σε αυτό το κεφάλαιο, χρησιμοποιούνται δεδομένα από την συνηθισμένη και σταθερή λειτουργία του δικτύου.

Κατόπιν, πραγματοποιείται μια από τις δύο επιθέσεις (malicious flooding και cache poisoning) και συλλέγονται τα στοιχεία για την αξιολόγηση του συγκεκριμένου μοντέλου. Το μετρικό σε αυτή την υλοποίηση είναι η αποδοτικότητα του CIDS στην ανίχνευση των παρεισφρήσεων και το ποσοστό των λανθασμένων μηνυμάτων εισβολής που παράγονται από το σύστημα. Κατά την αξιολόγηση των δεδομένων, υπολογίζεται πόσες από τις ανιχνευμένες παρεισφρήσεις που προσδιορίζονται, πραγματικά αποτελούν απειλή για το σύστημα και πόσες από αυτές ήταν απλά λανθασμένα αποτελέσματα του συστήματος. Τα κατώτατα όρια ρυθμίζονται προκειμένου να υπάρξουν καλύτερα αποτελέσματα όσον αφορά τα λανθασμένα μηνύματα των κόμβων.

Τα αποτελέσματα της προσομοίωσής αναπαριστώνται στην παρακάτω εικόνα 6.6. Στο σχήμα αυτό απεικονίζεται η σύγκριση μεταξύ του προτύπου που παρουσιάστηκε σε αυτή την παράγραφο και ενός συνηθισμένου IDS. Είναι σαφές λοιπόν από την γραφική παράσταση πως το CIDS επιφέρει καλύτερα αποτελέσματα όσον αφορά τα λάθος παραγόμενα μηνύματα και την αποδοτικότητα στην ανίχνευση των παρεισφρήσεων.



Εικόνα 6.6 Η απόδοση του CIDS σε σχέση με τα λανθασμένα μηνύματα

Το συγκεκριμένο σύστημα CIDS που παρουσιάζεται φαίνεται να έχει αυξημένη αποδοτικότητα και λειτουργικότητα για τους εξής λόγους κυρίως:

- Κατηγοριοποίηση των εισβολών σε κατηγορίες ασφαλείας.
- Στη χρήση δεδομένων δικτύου σε φυσιολογική κατάσταση (εκπαίδευση συστήματος).

Κεφάλαιο 7

Συμπεράσματα

7.1 Σύνοψη χαρακτηριστικών IDS για Ad-Hoc δίκτυα

Το ad-hoc δίκτυα είναι ένας νέος τύπος διανεμημένων δικτύων του οποίου οι ιδιότητες είναι σύνθετες και δύσκολα κατανοητές. Η ανίχνευση παρεισφρήσεων σε αυτά τα πολυσύνθετα συστήματα είναι προς το παρόν ένας μη ώριμος ερευνητικός τομέας. Υπάρχουν πολύ λιγότερα προτεινόμενα IDSs για τα ad-hoc από ότι για τα συμβατικά δίκτυα. Οι ερευνητές μπορούν να εστιάσουν είτε στην δημιουργία και εισαγωγή νέων IDSs για να χειριστούν την ασφάλεια συγκεκριμένων χαρακτηριστικών στα ad-hoc είτε μπορούν να προσαρμόσουν τα υπάρχοντα συστήματα ανίχνευσης. Σημαντικές ίσως αποδειχθούν επίσης και οι υβριδικές προσεγγίσεις.

Όπως συμπεραίνουμε από την ανάλυση που έχει προηγηθεί κάθε IDS δημιουργεί πρόσθετες απαιτήσεις και δημιουργεί νέα προβλήματα προς επίλυση. Ο πίνακας 7. 1 συνοψίζει κάθε προτεινόμενο IDS που παρουσιάστηκε σε προηγούμενα κεφάλαια, την συνεισφορά του καθενός σε νέους τομείς μαζί με μια ένδειξη των συγκεκριμένων ζητημάτων που δεν εξετάζουν. Σε γενικό επίπεδο κανένα από αυτά τα IDSs δεν είναι πλήρες. Συνήθως κάθε ένα εστιάζει σε συγκεκριμένα ζητήματα ασφάλειας. Επομένως θα πρέπει να ληφθεί υπόψη όλο το εύρος των πιθανών προβλημάτων προκειμένου να υπάρξει ένα αποτελεσματικό και αποδοτικό σύστημα ανίχνευσης παρεισφρήσεων.

Συνοπτικά επομένως παρατηρούμε τα εξής για τα υπάρχοντα IDSs.

- Καλύπτουν περιορισμένο αριθμό απειλών
- Χρησιμοποιούν συγκεκριμένα πρωτόκολλα δρομολόγησης
- Μερικά IDSs δεν λαμβάνουν ολοκληρωτικά υπόψη την κινητικότητα του δικτύου.
- Μερικά συστήματα αγνοούν την δυναμική φύση των ad-hoc δικτύων.
- Πιο εκτεταμένη έρευνα και αξιολόγηση των συστημάτων είναι απαραίτητη.

Τα προτεινόμενα συστήματα επιδιώκουν να εξετάσουν την έλλειψη κεντρικών συστημάτων ανίχνευσης εισβολών στα δίκτυα Ad-Hoc με την πρόταση διανεμημένων (distributed) και συνεταιριστικών (cooperative) αρχιτεκτονικών. Τέτοιες αρχιτεκτονικές παρόλα αυτά δημιουργούν ερωτήματα για την αποδοτικότητα της ασφάλειας, της επικοινωνίας και της διαχείρισης. Η καταλληλότητα της αρχιτεκτονικής στο εκάστοτε δίκτυο είναι μια σημαντική εκτίμηση κατά τον σχεδιασμό και την χρήση ενός IDS. Μια αρχιτεκτονική δεν πρέπει να εισαγάγει νέες αδυναμίες στα δίκτυα Ad-Hoc. Για παράδειγμα, μερικές από τις προτεινόμενες αρχιτεκτονικές όπως αυτή που βασίζεται σε cluster-head κόμβους είναι

χρονοβόρες προκειμένου να εγκατασταθούν ενώ επίσης είναι αρκετά δαπανηρές για δίκτυα υψηλής κινητικότητας.

Πρέπει να δοθεί ιδιαίτερη σημασία στην κινητικότητα των δικτύων κατά την χρήση των IDSs. Τα ποσοστά λανθασμένων μηνυμάτων (false positives) μπορούν να επηρεαστούν πολύ από το επίπεδο κινητικότητας. Το εκάστοτε χρησιμοποιούμενο σύστημα ανίχνευσης πρέπει να γνωρίζει την κινητικότητα και την τρέχουσα τοπολογία δικτύου που παρακολουθεί. Έτσι, χαρακτηριστικά γνωρίσματα όπως πληροφορίες σχετικές με την δυναμικότητα του δικτύου πρέπει να περιληφθούν κατά τον σχεδιασμό και την ανάπτυξη ενός IDS.

Η επικοινωνία μεταξύ των πρακτόρων ενός IDS πρέπει να ελαχιστοποιηθεί λόγω του περιορισμένου αριθμού ασύρματων συνδέσεων. Αυτό είναι ένας από τους στόχους της προσέγγισης που περιγράφεται στη μελέτη «Distributed Evidence Driven Message Exchange Intrusion Detection Model». Τα περισσότερα από τα υπάρχοντα συστήματα συνήθως δεν δίνουν όμως προσοχή σε αυτό το ζήτημα.

Δεδομένου ότι οι κόμβοι είναι οι μόνες πηγές δεδομένων στο δίκτυο, όλοι οι κόμβοι πρέπει να συμβάλουν στο IDS με την πραγματοποίηση τοπικής επίβλεψης και ανίχνευσης ενώ να παρέχουν παράλληλα δεδομένα σε άλλους κόμβους όταν απαιτείται. Εντούτοις, οι διάφοροι κόμβοι έχουν και συνήθως και διαφορετικές υπολογιστικές ικανότητες. Επιπλέον κάποιοι κόμβοι, δεν είναι αρκετά ισχυροί για να εκτελέσουν σύνθετους ή μεγάλους αλγορίθμους ανίχνευσης παρεισφρήσεων. Για αυτό το λόγο θα πρέπει ο παράγοντας αυτός να βρίσκεται υψηλά στην λίστα απαιτήσεων του συστήματος.

Λόγω της έλλειψης σαφών χαρακτηριστικών γνωρισμάτων της αμυντικής γραμμής του δικτύου και του δικτύου συνεργατών οι ίδιοι οι IDS πράκτορες είναι εύκολοι στόχοι των επιτιθεμένων. Τα προτεινόμενα συστήματα συνήθως υποθέτουν ότι οι πράκτορες ενός συστήματος ανίχνευσης εισβολών καθώς και η επικοινωνία μεταξύ τους είναι ασφαλείς. Οι ερευνητές λοιπόν πρέπει να εξετάσουν την ασφάλεια των ίδιων των IDSs.

IDS	Συνεισφορά	Σημειώσεις
Distributed και Cooperative IDS	Διανεμημένα Λαμβάνουν υπόψη τη δυναμικότητα του δικτύου	Σχεδιάστηκαν με βάση μόνο την τοπική κινητικότητα
Zone-Based IDS	Δυναμικότητα του δικτύου βασιζόμενα σε γειτονικούς κόμβους	Προκαλεί καθυστερήσεις στο δίκτυο κατά τον έλεγχο εισβολής
General Cooperative IDS Architectures	Χρήση πολλαπλών επιπέδων δικτύου	Υψηλό κόστος συντήρησης ειδικά υπό συνθήκες υψηλής κινητικότητας
Specification-Based	Το πρώτο Specification-	Μεγάλη κίνηση στο δίκτυο

IDS με AOD	Based IDS για ad-hoc δίκτυο	όταν υπάρχει υψηλή κινητικότητα
Case-Based Agents for Packet-Level IDS	Χρήση της τεχνικής Cased-Based και Anomaly-Based	Δυσκολία στην ανανέωση των περιπτώσεων όταν το σύστημα είναι διανεμημένο και αρκετά δυναμικό
IDS Architecture with Stationary Database	Στατική βάση για την αποθήκευση γνωστών προτύπων συνηθισμένης λειτουργίας του δικτύου	Έχει ένα κεντρικό σημείο όπου και αποθηκεύεται η βάση

Πινάκας 7.1 Σύνοψη χαρακτηριστικών IDS για Ad-Hoc δίκτυα

7.2 Τα χαρακτηριστικά ενός ιδανικού κατανεμημένου IDS

Ένα ιδανικό IDS για δίκτυα Ad Hoc θα πρέπει να εκτελείται **σε κάθε κόμβο**. Κάθε κόμβος αναλόγως των **δυνατοτήτων** του θα πρέπει συνεισφέρει όσο το δυνατόν περισσότερο μπορεί. Κάθε κόμβος θα αξιοποιεί αρχικά τα δεδομένα τα οποία μπορεί τοπικά να συλλέξει και θα συνεργάζεται με τους γειτονικούς κόμβους, ώστε να λαμβάνει επιπλέον πληροφορίες όταν αυτό είναι απαραίτητο για καλύτερη ανίχνευση. Η επικοινωνία αυτή μεταξύ κόμβων θα πρέπει να χρησιμοποιεί ένα **ασφαλές** κανάλι επικοινωνίας.

Κάθε IDS module θα πρέπει να χρησιμοποιεί τόσο τεχνικές βασισμένες σε **υπογραφές** (μοτίβα επιθέσεων) όσο και να παρατηρεί **ανωμαλίες** στην κίνηση του δικτύου (anomaly-based techniques).

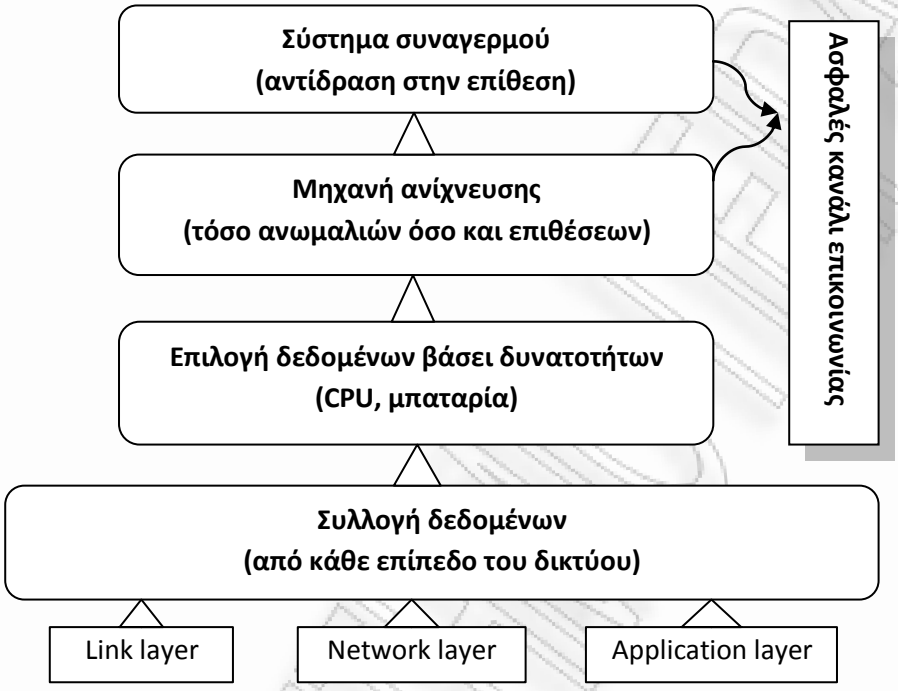
Η λειτουργία του IDS θα πρέπει να είναι τόσο σε **πραγματικό χρόνο** (ώστε να εντοπίζει ταχύτατα τις επιθέσεις που λαμβάνουν χώρα) όσο και σε **δεδομένα που έχουν συλλεχθεί στην πάροδο του χρόνου**. Τα ιστορικά αυτά δεδομένα μπορούν να χρησιμοποιούνται για τη δημιουργία νέων μοντέλων που θα τροφοδοτούν τις μηχανές πραγματικού χρόνου.

Εικόνα 7.1 Αναπαράσταση ταυτόχρονης παρακολούθησης δεδομένων και δεδομένων πραγματικού χρόνου

Επιπλέον ένα ιδανικό IDS Ad Hoc δικτύων θα πρέπει να μπορεί να συνεργαστεί με υπάρχοντες υποδομές IDS. Για παράδειγμα ένα Ad Hoc δίκτυο μπορεί να δημιουργηθεί σε

ένα σχολείο ή ένα πανεπιστήμιο για να εξυπηρετεί τις κινητές συσκευές. Το δίκτυο που δημιουργείται μπορεί να συνδέεται με τις υπάρχουσες δικτυακές υποδομές με σκοπό την παροχή υπηρεσιών. Σε αυτή την περίπτωση η ανταλλαγή δεδομένων ανάμεσα στο υπάρχον IDS και στο νέο κατανεμημένο Ad-Hoc IDS μπορεί να βοηθήσει πολύ τη διαδικασία ανίχνευσης εισβολέων.

Το παρακάτω σχήμα αναπαριστά ένα τέτοιο συνεργατικό IDS σύστημα.



Εικόνα 7.2 Αρχιτεκτονική του προτεινόμενου υβριδικού κατανεμημένου IDS

Βιβλιογραφία & Αναφορές

[1] Dardari D., Chong C., Damien B., Mucchi L. (2008) "*Cooperative Localization in Wireless Ad Hoc and Sensor Networks*" EURASIP Journal on Advances in Signal Processing
[Πηγή από Internet – Τελευταία πρόσβαση 28/9/2010]
http://downloads.hindawi.com/journals/specialissues/0012008010.pdf

[2] Huang Y., Wenke L. (2004) "A Cooperative Intrusion Detection System for Ad Hoc Networks"
[Πηγή από Internet – Τελευταία πρόσβαση 28/9/2010]
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.8768&rep=rep1&type=pdf

[3] Yu-Sung W., Bingrui F., Yongguo M., Saurabh B. (2003) "Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS"
[Πηγή από Internet – Τελευταία πρόσβαση 28/9/2010]
http://cobweb.ecn.purdue.edu/~dcsl/publications/papers/2003/cids_acsac03_cameraready.pdf

[4] Pahlevanzadeh B., Samsudin A. (2007) "Distributed Hierarchical IDS for MANET over AODV+" Proceedings of the 2007 IEEE Intemational Confbrence on Telecommunications
[Πηγή από Internet – Τελευταία πρόσβαση 5/10/2010]
http://eprints.usm.my/9410/1/Distributed_Hierarchical_IDS_for_MANET_over_AODV%2B.pdf

[5] Stamouli I. (2003) "*Real-time Intrusion Detection for Ad hoc Networks*" Dissertation submitted to the University of Dublin.
[Πηγή από Internet – Τελευταία πρόσβαση 6/10/2010]
http://www.scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-54.pdf

[6] Anne Aaron and Jie Weng. (2001) "Performance Comparison of Ad-hoc Routing Protocols for Networks with Node Energy Constraints"
[Πηγή από Ιντερνετ – Τελευταία πρόσβαση 7/10/2010]
http://ivms.stanford.edu/~amaaron/ee360/EE360_FINAL_PAPER.pdf

[7] Saiful M and Kabir S. (2010) "*Hierarchical design based Intrusion Detection System for wireless Ad Hoc sensor network*" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010
[Πηγή από Internet – Τελευταία πρόσβαση 8/10/2010]
http://airccse.org/journal/nsa/0710ijnsa07.pdf

[8] Ritonga M. A. (2008) “A study on Efficient Architecture for Intrusion Detection System in Ad Hoc Networks”
[Πηγή από Internet – Τελευταία πρόσβαση 9/10/2010]
http://repository.dl.itc.u-tokyo.ac.jp/dspace/bitstream/2261/24331/1/K-01476.pdf

[9] Σιδηρόπουλος Α. (2009) «Δίκτυα Υπολογιστών υπό κακόβουλο Έλεγχο (Botnets). Τεχνικές ανίχνευσης και απόκρυψης». Διπλωματική Εργασία Μεταπτυχιακού Οικονομικού πανεπιστημίου Αθηνών. Κεφάλαιο 3 , 5.2 και 6.2
[Πηγή από Internet – Τελευταία πρόσβαση 9/10/2010]
http://www.mm.aueb.gr/master_theses/polyzos/2009_sidiropoulos.pdf

[10] Κουτσουβέλας Δ., Κωστούδης Η. (2008) «*Ασφάλεια σε δίκτυα Ad Hoc και δίκτυα αισθητήρων*» Διπλωματική Εργασία Εθνικού Μετσόβιου Πολυτεχνείου. Κεφάλαιο 4 και 5.
[Πηγή από Internet – Τελευταία πρόσβαση 10/10/2010]
http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2008-0266/DT2008-0266.pdf

[11] Heng W., Nwe Y., Hian J. (2004) “Intrusion Detection in Wireless Ad-Hoc Networks”
[Πηγή από Internet – Τελευταία πρόσβαση 10/10/2010]
http://www.projapps.com/CS4274.pdf

[12] Micah Adler and Christian Scheideler, Efficient Communication Strategies for Ad-Hoc Wireless Networks, in Proceedings of 10th ACM Symposium on Parallel Algorithms and Architectures (SPAA) 1998.

[13] R. Perlman, “Interconnections: Bridges, Routers, Switches and Internetworking Protocols”, 2nd Edition, Addison-Wesley, 2000.

[14] D. B. Johnson, D. A. Maltz, Y-C Hu, J. G. Jetcheva, “The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR), Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, February 2002.

[15]A Survey of Distributed Intrusion Detection Approaches – Web of Trust
http://arxiv.org/PS_cache/cs/pdf/0501/0501001v1.pdf

[16] Λίγα λόγια για το OLSR Routing - AWMN, Μιχάλης Τοπαλούδης
http://routing.explode.gr/node/36

[17] Πρωτόκολλο ODSBR: ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks
http://cs.njit.edu/~crix/publications/ODSBR-TISSEC.pdf

[18] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," *Proceedings of the 6th Annual Int'l Conference on Mobile Computing and Networking (MobiCom'00)*, pp. 275–283,2000.

[19] Anand Patwardhan, Jim.Parker., Anupam Joshi, Michaela Iorga and Tom Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks". *Proceedings of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom 2005),* 2005.

[20] P. Albers et al., "Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches," 1st Int'l. Workshop on Wireless Info. Sys. Apr. , 2002.

[21] An Overview of SNMP Protocol, http://www.asg-sentry.com/Resources/SNMP-Overview.pdf

[22] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari, "Real-time Intrusion Detection for Ad hoc Networks**"**

[23] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," Proceedings of the 6th Annual Int'l Conference on Mobile Computing and Networking (MobiCom'00), pp. 275–283, 2000.

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

[25] Guha R, Kachirski O et al (2002) Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks. In Proc of 17th Int Symp on Comput & Inf Sci:315-230

[26] Tseng C-Y, Balasubramayan P et al (2003) A Specification-Based Intrusion Detection System for AODV. In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Netw (SASN)

[27] Smith AB (2001) An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks. In Proc of 5th Natl Colloq for Inf Syst Secur Educ

[28] A. E.Roth,"The Shapley Value: Essays in Honor of Lloyd S.Shapley", Cambridge University Press, 1988.

[29] Καραμπότση, Νικολέτα, 2007, Πτυχιακή ΤΕΙ Κρήτης, Ασύρματα Ad Hoc Δίκτυα: Πρωτόκολλα – Εφαρμογές http://nefeli.lib.teicrete.gr/browse/stef/epp/2007/Karampotsi,Nikoleta/document.tkl

[30] Dimitra Kampitaki, Ad-Hoc and Sensor Networks: Technology and Applications, Master Thesis in University of Macedonia http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/erga

sies/2007/Ad-Hoc%20and%20Sensor%20Networks.pdf

[31] OLSR Protocol – AWMN:
http://routing.explode.gr/node/87

[32] Kong, J., Luo, H., Xu, K., Gu, D., Gerla, M., and Lu, S.,"Adaptive Security for Multi-layer Ad-hoc Networks," *Special Issue of Wireless Communication and Mobile Computing*, 2002.

[33] Snort :: HomePage
http://www.snort.org/

[34] Snort :: Snort Rules
http://www.snort.org/snort-rules/

[35] Introduction to Snort
http://www.seren.net/documentation/unix%20utilities/Snort.pdf

[36] Snort tutorial
http://luctus.es/wp-content/uploads/2010/03/Snort.ppt

[37] Data Sets from DARPA Intrusion Detection Evaluation.
http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html

[38] Investigating the problem of IDS false alarms: An experimental study using Snort
http://www.springerlink.com/content/e490276x0h804504/

[39] Συστήματα Ανίχνευσης Παρεισφρήσεων IDS
http://digilib.lib.unipi.gr/dspace/bitstream/unipi/2462/3/Michailidis.pdf

[40] ISLAB HACK: Βασικές Έννοιες & Προγραμματισμός του Snort 2.0
http://www.islab.demokritos.gr/gr/html/Snort2_dpritsos/Snort2&Snort_Preprocessors.pdf

[41] SECURITY CONTROLS FOR COMPUTER SYSTEMS: Report of Defense Science Board Task Force on Computer Security
http://cryptome.org/sccs.htm

[42] Συστήματα Ανίχνευσης & Ειδοποίησης Κακόβουλων Ενεργειών Σε Περιβάλλοντα Προσωπικών Δικτύων
http://artemis.cslab.ntua.gr/Dienst/UI/1.0/Download/artemis.ntua.ece/PD2009-0082

[43] GIoMoSim website, http://pcl.cs.ucla.edu/projects/glomosim/