ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ ΣΕ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΜΕ ΑΛΓΟΡΙΘΜΟΥΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ

Αικατερίνη Β. Μητροκώτσα

Διδακτορική Διατριβή

Πειραιάς, Αύγουστος 2007

Ευχαριστίες

Θα ήθελα να εκφράσω την ευγνωμοσύνη μου σε όλους αυτούς που με βοήθησαν να ολοκληρώσω αυτή τη διδακτορική διατριβή. Θα ήθελα να ευχαριστήσω το Ίδρυμα Μποδοσάκη για την υποστήριξη και την υποτροφία που μου παρείχε κατά τη διάρκεια της έρευνάς μου.

Είμαι ιδιαίτερα ευγνώμων στον επιβλέποντα μου, Δρ. Χρήστο Δουληγέρη, Καθηγητή του τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς, που ήταν πάντα δίπλα μου να με ενθαρρύνει και να με καθοδηγεί κατά τη διάρκεια αυτής της ερευνητικής εργασίας. Η οξεία ερευνητική του ματιά, η ορθή του κρίση, οι προτάσεις και η καθοδήγησή του έκαναν δυνατή την ολοκλήρωση αυτής της διδακτορικής διατριβής. Θα ήθελα επίσης να ευχαριστήσω τον Δρ. Χρήστο Δημητρακάκη, τον Δρ. Νίκο Κομνηνό, την υποψήφια διδάκτορα Ρόζα Μαυροπόδη και τον μεταπτυχιακό φοιτητή Μανώλη Τσάγκαρη που μου πρόσφεραν τον χρόνο τους, τις συμβουλές τους και τη βοήθειά τους.

Θα ήθελα επίσης να ευχαριστήσω τους συνεργάτες μου άλλους υποψήφιους διδάκτορες του τμήματος Πληροφορικής που μου παρείχαν ένα άριστο ακαδημαϊκό περιβάλλον με την υποστήριξη και τις προτάσεις τους και ήταν πάντα δίπλα μου για να προσφέρουν τη βοήθειά τους και να με εμψυχώσουν όποτε χρειαζόταν. Τέλος, θα ήθελα να εκφράσω τη βαθιά ευγνωμοσύνη μου στους γονείς μου, και τα αδέρφια μου, που μου παρείχαν απεριόριστη ενθάρρυνση και υποστήριξη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Συμβουλευτική Επιτροπή

Επιβλέπων:

Χρήστος Δουληγέρης
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Γεώργιος Τσιχριντζής
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Πανεπιστήμιο Πειραιώς

Τμήμα Πληροφορικής

Διατριβή

Για την απόκτηση Διδακτορικού Διπλώματος του τμήματος Πληροφορικής

Αικατερίνης Β. Μητροκώτσα

«Ανίχνευση Εισβολών σε Δίκτυα Υπολογιστών με Αλγόριθμους Μηχανικής Μάθησης»

Εξεταστική Επιτροπή:

Νικόλαος Αλεξανδρής,
Καθηγητής Πανεπιστημίου Πειραιώς

Ιάκωβος Βενιέρης
Καθηγητής Ε.Μ. Πολυτεχνείου

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Χρήστος Δουληγέρης
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Γεώργιος Τσιχριντζής
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Αθανασία Αλωνιστιώτη
Λέκτορας Πανεπιστημίου Πειραιώς

Δέσποινα Πολέμη
Λέκτορας Πανεπιστημίου Πειραιώς

Πρόλογος

Η αύξηση της συνδεσιμότητας των υπολογιστικών επικοινωνιών σε ενσύρματα και ασύρματα δίκτυα καθιστά επιτακτική την ανάγκη για διασφάλιση των υπολογιστικών και δικτυακών συστημάτων. Η ανίχνευση εισβολών αποτελεί ένα από τα σημαντικότερα μέσα για τη διασφάλιση και προστασία των υπολογιστικών συστημάτων από κακόβουλους επιτιθέμενους, καθώς επιτυγχάνει την ανίχνευση επιθέσεων, περιορίζει την επίδρασή τους και είναι απαραίτητη προκειμένου να επιτύχουμε μεγάλη επιβιωσιμότητα σε ένα δίκτυο. Στη διατριβή αυτή εξετάζουμε το πρόβλημα των δικτυακών επιθέσεων και προσεγγίσουμε τη δυνατότητα διασφάλισης υπολογιστικών και δικτυακών επικοινωνιών προτείνοντας προσεγγίσεις ανίχνευσης εισβολών που βασίζονται σε μηχανισμούς ταξινόμησης και μηχανικής μάθησης.

Αρχικά ερευνούμε το πρόβλημα μίας από τις σοβαρότερες απειλές της διαθεσιμότητας πληροφοριών, τις επιθέσεις *άρνησης εξυπηρέτησης (Denial of Service (DoS))*. Παρουσιάζουμε μία πλήρη επισκόπηση της υπάρχουσας γνώσης στο πεδίο των επιθέσεων αυτών προτείνοντας ταξινομήσεις τόσο για τις επιθέσεις αυτές όσο και για τους μηχανισμούς που έχουν προταθεί για την αντιμετώπισή τους. Στόχος μας είναι να περιγράψουμε τα υπάρχοντα προβλήματα ώστε να επιτύχουμε καλύτερη κατανόηση του προβλήματος των επιθέσεων DoS και να σχεδιάσουμε πιο αποτελεσματικούς μηχανισμούς αντιμετώπισης. Σημειώνουμε τη σοβαρότητα που έχουν οι επιθέσεις DoS για τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης, έναν τομέα ιδιαίτερα κρίσιμο και σημαντικό. Επιπλέον, προτείνουμε πρακτικές και πολιτικές που μπορούν να χρησιμοποιηθούν από τους οργανισμούς προκειμένου να ενδυναμώσουν περισσότερο την ασφάλεια στα συστήματά τους και να τα προστατέψουν από το ενδεχόμενο να γίνουν θύμα μίας επίθεσης DoS.

Προτείνουμε μία μέθοδο ανίχνευσης των δικτυακών εισβολών περιλαμβανομένων των επιθέσεων DoS, η οποία βασίζεται στην ακριβή και αποτελεσματική διάκριση μεταξύ της παράνομης ("μη-φυσιολογικής") και της νόμιμης ("φυσιολογικής") δικτυακής κυκλοφορίας. Η προτεινόμενη προσέγγιση εφαρμόζεται τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα και βασίζεται στην κατάλληλη επεξεργασία αρχείων καταγραφής δικτυακής κυκλοφορίας χρησιμοποιώντας μία κατηγορία νευρωνικών δικτύων που είναι γνωστά ως *αναδυόμενοι Αυτό-Οργανούμενοι Χάρτες (emergent Self-Organizing Maps (eSOM))*. Χρησιμοποιώντας τεχνικές απεικόνισης πληροφοριών αποκτούμε μία ξεκάθαρη εικόνα της δικτυακής δραστηριότητας και το πλεονέκτημα απόκρισης σε πραγματικό χρόνο.

Προτείνουμε επίσης μία αποτελεσματική μηχανή *Απόκρισης σε Εισβολές* για τα ασύρματα δίκτυα κατά περίσταση που στόχο έχει τον περιορισμό των επιδράσεων πιθανών εισβολών. Η προτεινόμενη μηχανή *Απόκρισης σε Εισβολές* κρίνεται απαραίτητη ειδικά στα ασύρματα δίκτυα που παρουσιάζουν πολλά

έμφυτα προβλήματα και αδυναμίες συμπεριλαμβανομένων των περιορισμένων πόρων. Επιπλέον, χρησιμοποιούμε τεχνικές υδατογράφησης προκειμένου να διασφαλίσουμε την ακεραιότητα και να εντοπίσουμε πιθανές τροποποιήσεις στους χάρτες eSOM που παράγονται από τη μηχανή ανίχνευσης εισβολών.

Τέλος, λαμβάνοντας υπόψη μας το γεγονός ότι στην ανίχνευση εισβολών η απαίτηση δεν είναι απλά να προβλέψουμε την πιο πιθανή ετικέτα κλάσης (επίθεση - "φυσιολογική" συμπεριφορά), αφού διαφορετικοί τύποι λαθών επιφέρουν διαφορετικό κόστος, προτείνουμε την υλοποίηση μίας προσέγγισης ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος και την εφαρμόζουμε σε μερικούς πολύ γνωστούς και αποτελεσματικούς ταξινομητές, τόσο για ενσύρματα όσο και ασύρματα δίκτυα. Εξετάζουμε την απόδοση των αλγόριθμων αυτών ταξινόμησης στην ανίχνευση εισβολών με και χωρίς ευαισθησία στο κόστος.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1ο
Εισαγωγή

1. Εισαγωγή

Καθώς η συνδεσιμότητα των υπολογιστών αυξάνεται συνεχώς, η ανάγκη για ασφάλεια των υπολογιστικών συστημάτων και δικτύων γίνεται επιτακτική. Η ασφάλεια των υπολογιστικών συστημάτων μπορεί να οριστεί ως η ικανότητα ενός συστήματος να προστατεύσει τις πληροφορίες του συστήματος από επιτιθέμενους. Προκειμένου να υπάρχει ασφάλεια σε μία δικτυακή επικοινωνία είναι απαραίτητο να ικανοποιούνται οι ακόλουθες βασικές αρχές [Stallings, 1999] *διαθεσιμότητα (availability), εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity), πιστοποίηση (authentication)* και *καταλογισμός ευθύνης (non – repudiation).*

Η ***διαθεσιμότητα*** επιβεβαιώνει ότι οι δικτυακές υπηρεσίες είναι διαθέσιμες στους συμμετέχοντες, όταν χρειάζονται.

Η ***εμπιστευτικότητα*** επιβεβαιώνει ότι στις πληροφορίες που μεταφέρονται έχουν πρόσβαση μόνο οι εξουσιοδοτημένοι συμμετέχοντες και δεν αποκαλύπτονται ποτέ σε μη-εξουσιοδοτημένους χρήστες.

Η ***πιστοποίηση*** επιβεβαιώνει την ταυτότητα του συμμετέχοντα που μεταδίδει πληροφορίες.

Η ***ακεραιότητα*** εξασφαλίζει την ασφαλή μεταφορά πληροφοριών χωρίς τροποποιήσεις.

Ο *καταλογισμός ευθύνης* επιβεβαιώνει ότι μία οντότητα μπορεί να αποδείξει τη μεταφορά ή τη λήψη πληροφοριών από μία άλλη οντότητα (αποστολέας/παραλήπτης) και δεν μπορεί να αρνηθεί το γεγονός ότι έλαβε ή έστειλε συγκεκριμένα δεδομένα.

Συχνά όμως οι παραπάνω βασικές αρχές ασφάλειας δεν διατηρούνται με αποτέλεσμα τα υπολογιστικά συστήματα/δίκτυα να είναι εκτεθειμένα σε ένα μεγάλο αριθμό απειλών. Ο Anderson [Anderson, 1980] ταξινόμησε τις απειλές εναντίον ενός υπολογιστικού συστήματος στις ακόλουθες κατηγορίες:

- **Κίνδυνος (Risk):** Τυχαία ή απρόβλεπτη έκθεση πληροφοριών ή παραβίαση της ακεραιότητας λειτουργιών λόγω κακής λειτουργίας υλικού, ελλιπούς ή λανθασμένου σχεδιασμού λογισμικού.
- **Ευπάθεια (Vulnerability)**: Ένα γνωστό ή ύποπτο σφάλμα στο υλικό ή το λογισμικό ή τη λειτουργία ενός συστήματος που εκθέτει το σύστημα σε επιτυχείς επιθέσεις ή τις πληροφορίες του σε τυχαία αποκάλυψη.
- **Επίθεση (Attack)** : Μία συγκεκριμένη εκτέλεση ενός σχεδίου προκειμένου να πραγματοποιηθεί μία προσπάθεια απειλής.
- **Εισβολή (Penetration)**: Μία επιτυχής επίθεση – η ικανότητα να λαμβάνεται μη-εξουσιοδοτημένη και μη-ανιχνεύσιμη πρόσβαση σε αρχεία και προγράμματα ή την κατάσταση ελέγχου ενός υπολογιστικού συστήματος.

Σύμφωνα όμως με τους Heady και άλλους [Heady, 1990]: "Εισβολή ορίζεται κάθε σύνολο ενεργειών που προσπαθούν να διαβάλουν την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός υπολογιστικού πόρου". Αυτός ο ορισμός δεν διαχωρίζει την επιτυχία ή την αποτυχία αυτών των ενεργειών. Στη συνέχεια αυτής της διατριβής δεν διαχωρίζουμε τις έννοιες επίθεση και εισβολή.

Ο Anderson [Anderson, 1980] επίσης ταξινόμησε τους επιτιθέμενους σε δύο τύπους:

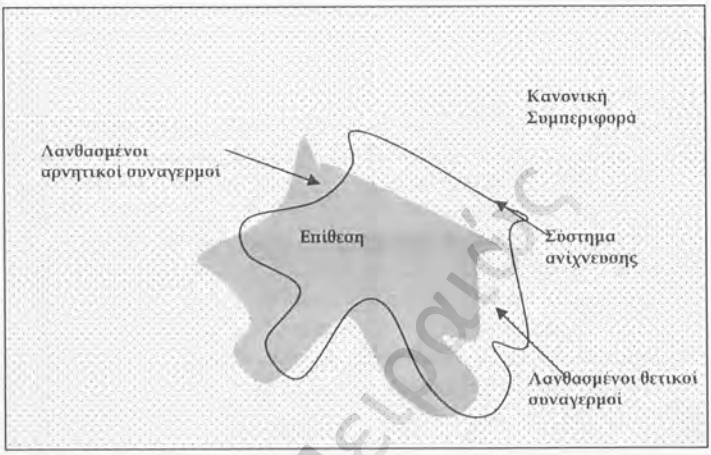
- τους *εξωτερικούς επιτιθέμενους* η οποίοι είναι μη-εξουσιοδοτημένοι χρήστες των μηχανημάτων στα οποία πραγματοποιούν επίθεση, και
- τους *εσωτερικούς επιτιθέμενους*, οι οποίοι είναι εξουσιοδοτημένοι χρήστες του συστήματος και υπερβαίνουν τα νόμιμα δικαιώματα πρόσβασης που έχουν. Οι επιτιθέμενοι αυτής της κατηγορίας διαχωρίζονται σε:
  - *μεταμφιεσμένους (*

2. Ανίχνευση Εισβολών

Προκειμένου να επιτευχθούν οι απαιτούμενοι στόχοι ασφάλειας και να διαφυλαχθούν τα υπολογιστικά συστήματα, έχουν προταθεί και εφαρμοστεί πολλοί μηχανισμοί ασφάλειας. Η *παρεμπόδιση εισβολών*, μέσω της κρυπτογράφησης και της πιστοποίησης μπορεί να χρησιμοποιηθεί σαν μία πρώτη γραμμή προστασίας προκειμένου να περιοριστούν οι εισβολές αλλά σίγουρα δεν μπορεί να τις εξαλείψει. Ανεξάρτητα από το πόσοι μηχανισμοί παρεμπόδισης εισβολών εφαρμόζονται σε ένα δίκτυο, υπάρχουν πάντα κάποιες αδυναμίες και ευπάθειες, τις οποίες μπορεί να εκμεταλλευτεί ένας κακόβουλος χρήστης. Ένα δεύτερο τείχος προστασίας είναι απαραίτητο προκειμένου να παρεμποδίσουμε μία επίθεση ή να μετριάσουμε την επίδρασή της.

Τα *συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems (IDS))* είναι η δεύτερη γραμμή προστασίας από κακόβουλους επιτιθέμενους καθώς βοηθούν στην ανίχνευση επιθέσεων, περιορίζουν την επίδρασή τους και είναι απαραίτητα προκειμένου να επιτύχουμε μεγάλη επιβιωσιμότητα σε ένα δίκτυο. Η ανίχνευση εισβολών μπορεί να οριστεί σαν τη διαδικασία ανίχνευσης ανάρμοστης λανθασμένης ή ανώμαλης δραστηριότητας. Ο στόχος ενός συστήματος ανίχνευσης εισβολών είναι η διάκριση μεταξύ της παράνομης ("μη-φυσιολογικής") συμπεριφοράς και της νόμιμης ("φυσιολογικής") συμπεριφοράς. Επομένως, ένα σύστημα ανίχνευσης εισβολών μπορεί να οριστεί ως ένα σύστημα ταξινόμησης το οποίο μπορεί να αναλύσει τις συμπεριφορές του συστήματος ή των γεγονότων ασφαλείας και να αναγνωρίσει κακόβουλες συμπεριφορές. Στο Σχήμα 1.1 [Li, 2001] κάθε σημείο στο επίπεδο αναπαριστά ένα πρότυπο. Εάν το σημείο βρίσκεται μέσα στη σκιασμένη περιοχή θεωρείται επίθεση. Διαφορετικά είναι "φυσιολογική" συμπεριφορά. Ένα σύστημα ανίχνευσης εισβολών προσπαθεί να κωδικοποιήσει το όριο ανάμεσα στις δύο περιοχές ταξινομώντας τα πρότυπα ως "φυσιολογικά" ή "μη-φυσιολογικά". Στην προσπάθεια του συστήματος ανίχνευσης να πραγματοποιήσει επιτυχή και ακριβή ανίχνευση επιθέσεων μπορεί να αναγνωρίσει νόμιμη δικτυακή κυκλοφορία σαν επίθεση και να δημιουργήσει *λανθασμένους θετικούς συναγερμούς*. Αντίστοιχα, μπορεί να αποτύχει στην ανίχνευση δικτυακής κυκλοφορίας επίθεσης (δημιουργία *λανθασμένων αρνητικών συναγερμών*). Στόχος ενός συστήματος ανίχνευσης είναι να επιτύχει όσο δυνατόν υψηλότερο ποσοστό ανίχνευσης χωρίς όμως να δημιουργεί πολλούς λανθασμένους αρνητικούς συναγερμούς.

Η ανίχνευση εισβολών διακρίνεται σε δύο κύριες κατηγορίες: την ανίχνευση εισβολών που βασίζεται στην *ανίχνευση ανωμαλιών (anomaly detection)* και την ανίχνευση εισβολών που βασίζεται στην *ανίχνευση κακής χρήσης (misuse detection)*.



Σχήμα 1. 1 Η Ανίχνευση Εισβολών ως Ταξινομητής Συμπεριφοράς

2.1. Ανίχνευση Κακής Χρήσης

Τα συστήματα που βασίζονται στην *ανίχνευση κακής χρήσης*, διατηρούν μία βάση δεδομένων με υπογραφές εισβολών. Χρησιμοποιώντας αυτές τις υπογραφές το σύστημα μπορεί εύκολα να ανιχνεύσει εισβολές στα υπολογιστικά συστήματα.

Η *ανίχνευση κακής χρήσης* χρησιμοποιεί "εκ των προτέρων" γνώση για εισβολές και προσπαθεί να ανιχνεύσει επιθέσεις βασιζόμενη σε συγκεκριμένα πρότυπα ή υπογραφές γνωστών επιθέσεων. Τα συστήματα ανίχνευσης εισβολών που βασίζονται στην *ανίχνευση κακής χρήσης* είναι πολύ ακριβή καθώς οι υπογραφές των εισβολών ορίζονται με στενά όρια. Το βασικό μειονέκτημα που παρουσιάζουν αυτά τα συστήματα είναι η αδυναμία τους να αποκαλύψουν νέες -άγνωστες επιθέσεις καθώς οι μηχανισμοί επίθεσης βρίσκονται σε συνεχή εξέλιξη, κάτι το οποίο οδηγεί στην ανάγκη για μία βάση γνώσης. Αυτό το μειονέκτημα μπορεί να μετριαστεί αν διατηρείται μία ενημερωμένη βάση υπογραφών. Από την άλλη πλευρά, η διατήρηση μίας ενημερωμένης βάσης υπογραφών απαιτεί προσεκτική ανάλυση κάθε ευπάθειας και είναι μία ιδιαίτερα χρονοβόρα διαδικασία. Επιπλέον, τα συστήματα *ανίχνευσης κακής χρήσης* έχουν να αντιμετωπίσουν το μειονέκτημα ότι κάθε επίθεση επικεντρώνεται σε συγκεκριμένα λειτουργικά συστήματα, εκδόσεις, πλατφόρμες και εφαρμογές. Επομένως υπάρχει πρόβλημα όσον αφορά στη γενίκευση της προσέγγισης που χρησιμοποιείται.

Η *ανίχνευση κακής χρήσης* μπορεί να ταξινομηθεί σε τρεις κύριες κατηγορίες:

- Ανίχνευση Κακής Χρήσης με χρήση *έμπειρων συστημάτων*,
- Ανίχνευση Κακής Χρήσης με μεθόδους *ταιριάσματος προτύπου*,
- Ανίχνευση Κακής Χρήσης με μεθόδους *ανάλυσης μετάβασης καταστάσεων*.

2.1.1 Ανίχνευση Κακής Χρήσης με Χρήση Έμπειρων Συστημάτων

Ένα έμπειρο σύστημα που χρησιμοποιείται στην ανίχνευση εισβολών κωδικοποιεί γνώση για παλιότερες εισβολές, γνωστές ευπάθειες των συστημάτων και πολιτικών ασφάλειας και δημιουργεί ένα σύνολο κανόνων που περιγράφουν επιθέσεις. Καθώς συλλέγονται πληροφορίες, το έμπειρο σύστημα μπορεί να καθορίσει αν οι υπάρχοντες κανόνες ικανοποιούνται. Χαρακτηριστικά παραδείγματα μεθόδων ανίχνευσης εισβολών που χρησιμοποιούν έμπειρα συστήματα είναι αυτές που προτάθηκαν από τους Habra και άλλους [Habra, 1992], και Garvey και άλλους [Garvey, 1991]. Τα κύρια μειονεκτήματα που παρουσιάζουν αυτά τα συστήματα είναι ότι δεν μπορούν να διαχειριστούν πολύ μεγάλες ποσότητες δεδομένων. Μπορούν να ανιχνεύσουν μόνο γνωστές επιθέσεις και δεν μπορούν να επεξεργαστούν περιπτώσεις που παρουσιάζουν αβεβαιότητα.

2.1.2 Η Ανίχνευση Κακής Χρήσης με Μεθόδους Ταιριάσματος Προτύπου

Η ανίχνευση εισβολών με μεθόδους *ταιριάσματος προτύπου* [Debar, 1999] ακολουθεί ακριβώς την ίδια προσέγγιση απόκτησης γνώσεων με τα έμπειρα συστήματα, αλλά σε αυτή την περίπτωση η γνώση που λαμβάνεται χρησιμοποιείται με άλλο τρόπο. Η σημασιολογική περιγραφή των επιθέσεων μετατρέπεται σε πληροφορίες που μπορεί να βρεθούν μέσα στα καταγεγραμμένα αρχεία με άμεσο τρόπο. Για παράδειγμα, τα σενάρια επιθέσεων μπορούν να αντιστοιχηθούν με ακολουθίες των καταγεγραμμένων γεγονότων (audit events) που παράγουν ή με τα πρότυπα των δεδομένων που μπορούν να βρεθούν μέσα στα αρχεία καταγραφής τα οποία παράγονται από το σύστημα. Αυτή η μέθοδος παρουσιάζει ιδιαίτερα αποτελεσματική υλοποίηση και για το λόγο αυτό χρησιμοποιείται ευρέως στα εμπορικά συστήματα ανίχνευσης εισβολών ([Landwehr, 1994], [ISS, 2007]). Το κύριο μειονέκτημα αυτής της προσέγγισης όπως και όλων των συστημάτων ανίχνευσης κακής χρήσης είναι ότι χρειάζονται συχνές ανανεώσεις των προτύπων με βάση τις νέες επιθέσεις. Ιδιαίτερα επίπονη χαρακτηρίζεται η διαδικασία αν σκεφτούμε ότι κάθε επίθεση παρουσιάζει διαφορετικό πρότυπο ανάλογα με το λειτουργικό σύστημα στο οποίο εφαρμόζεται το σύστημα ανίχνευσης.

2.1.3 Ανίχνευσης Κακής Χρήσης με τη Χρήση Μεθόδων Ανάλυσης Μετάβασης Καταστάσεων

Τα συστήματα ανίχνευσης εισβολών που χρησιμοποιούν μεθόδους *ανάλυσης μετάβασης καταστάσεων* χρησιμοποιούν γραφήματα μηχανών πεπερασμένων καταστάσεων (finite state machine graphs) (πεπερασμένα αυτόματα) προκειμένου να μοντελοποιήσουν τις επιθέσεις. Μία εισβολή αποτελείται από μία ακολουθία ενεργειών που οδηγούν από κάποια αρχική κατάσταση του συστήματος σε μία κατάσταση εισβολής [Bace, 2000]. Η αρχική κατάσταση αναπαριστά την κατάσταση του συστήματος πριν δεχτεί την εισβολή, ενώ η κατάσταση εισβολής περιγράφει την κατάσταση του συστήματος μετά την

ολοκλήρωση της επίθεσης. Η κατάσταση του συστήματος περιγράφεται με χαρακτηριστικά του συστήματος ή/και δικαιώματα του χρήστη. Η μετάβαση των καταστάσεων καθορίζεται από τις ενέργειες του χρήστη. Μία μηχανή *μετάβασης καταστάσεων* διατηρεί ένα σύνολο διαγραμμάτων μετάβασης καταστάσεων, κάθε ένα από τα οποία περιγράφει ένα σενάριο εισβολής. Σε μία δεδομένη στιγμή, θεωρείται ότι κάποια ακολουθία ενεργειών οδήγησε το σύστημα σε μία συγκεκριμένη κατάσταση σε κάθε διάγραμμα. Όταν πραγματοποιείται μία ενέργεια, η μηχανή ελέγχει αν αυτή η ενέργεια οδηγεί κάποιο σενάριο εισβολής σε επόμενη κατάσταση. Εάν η ενέργεια οδηγήσει ένα σενάριο εισβολής σε τελική κατάσταση, η πληροφορία μετάβασης κατάστασης αποστέλλεται στη μηχανή ανίχνευσης, η οποία ενημερώνει τον διαχειριστή του συστήματος για την ύπαρξη εισβολής. Χαρακτηριστικό παράδειγμα μεθόδου ανίχνευσης εισβολών που χρησιμοποιεί την *ανάλυση μετάβασης καταστάσεων* είναι αυτό που προτάθηκε από τους Porras και άλλους [Porras, 1992].

Τα συστήματα ανίχνευσης εισβολών που βασίζονται σε μεθόδους ανάλυσης μετάβασης καταστάσεων αποτελούν μία υψηλού επίπεδου αναπαράσταση των σεναρίων εισβολών. Παρόλα αυτά η λίστα των καταστάσεων των σεναρίων εισβολών μπορεί να μην αρκεί προκειμένου να εκφραστούν πιο πολύπλοκα σενάρια εισβολών. Αυτό έχει ως αποτέλεσμα τέτοιου είδους συστήματα να μη μπορούν να ανιχνεύσουν κοινές επιθέσεις. Οπότε είναι απαραίτητο να συνδυαστούν με άλλα συστήματα ανίχνευσης.

2.2. Ανίχνευση Ανωμαλιών

Η *ανίχνευση ανωμαλιών* υιοθετεί την προσέγγιση με βάση την οποία γνωρίζει τι είναι "φυσιολογικό" και στη συνέχεια προσπαθεί να ανιχνεύσει αποκλίσεις από τη "φυσιολογική" συμπεριφορά τις οποίες θεωρεί ανωμαλίες ή πιθανές εισβολές. Αυτό πραγματοποιείται αφού πρώτα δημιουργηθεί ένα προφίλ του συστήματος σε κανονική χρήση. Ένα σύστημα ανίχνευσης ανωμαλιών τυπικά αποτελείται από δύο φάσεις: μία *φάση εκπαίδευσης* και μία *φάση ελέγχου*. Στην πρώτη φάση ορίζεται το προφίλ της "φυσιολογικής" συμπεριφοράς ενώ στη δεύτερη φάση το προφίλ που έχει δημιουργηθεί με την εκπαίδευση εφαρμόζεται σε νέα δεδομένα. Το κύριο πλεονέκτημα της *ανίχνευσης ανωμαλιών* είναι ότι παρέχει τη δυνατότητα να ανιχνεύσουμε άγνωστες επιθέσεις βασιζόμενοι στο γεγονός ότι το σύστημα παρουσιάζει "μη-φυσιολογική" συμπεριφορά.

Παρόλα αυτά, η *ανίχνευση ανωμαλιών* παρουσιαζει κάποια σοβαρά μειονεκτήματα. Το πρώτο είναι ότι παρουσιάζει μεγάλο αριθμό λανθασμένων θετικών συναγερμών. Αυτό οφείλεται κυρίως στο γεγονός ότι είναι πολύ δύσκολο να καθοριστεί η "φυσιολογική" συμπεριφορά ενός συστήματος. Προκειμένου να αντιμετωπιστεί αυτό, νέα προφίλ "φυσιολογικής" συμπεριφοράς πρέπει να λαμβάνονται από το δίκτυο σε τακτά χρονικά διαστήματα προκειμένου το προφίλ που χρησιμοποιείται να είναι ανανεωμένο. Παρόλα αυτά αυτή είναι χρονοβόρα διαδικασία, αλλά ακόμα και αν επιτευχθεί είναι δύσκολο να υπάρχει

ένα πάντα ενημερωμένο προφίλ που να κάνει εύκολο το διαχωρισμό μεταξύ ασυνήθιστης συμπεριφοράς αλλά νόμιμης και ασυνήθιστης συμπεριφοράς που αποτελεί εισβολή. Επιπλέον ένας εισβολέας που γνωρίζει ότι οι ενέργειές του παρακολουθούνται μπορεί να εκπαιδεύσει το σύστημα για ένα χρονικό διάστημα προκειμένου να παγιδεύσει το σύστημα ανίχνευσης εισβολών ώστε να θεωρήσει ότι δεδομένα επίθεσης είναι "φυσιολογικά".

Η *ανίχνευση ανωμαλιών* σύμφωνα με τους Patcha και άλλους [Patcha, 2007] μπορεί να κατηγοριοποιηθεί σε τρεις βασικές κατηγορίες:

- Ανίχνευση Ανωμαλιών με τη χρήση *στατιστικών μεθόδων*.
- Ανίχνευση Ανωμαλιών με τη χρήση *μηχανικής εκμάθησης*.
- Ανίχνευση Ανωμαλιών με τη χρήση *εξόρυξης δεδομένων*.

Πρέπει να σημειώσουμε εδώ ότι οι τεχνικές αυτές ανίχνευσης ανωμαλιών παρουσιάζουν πολλά κοινά στοιχεία και συχνά δεν υπάρχει σαφής διαχωρισμός για την κατηγορία στην οποία ανήκει ένα σύστημα ανίχνευσης ανωμαλιών. Οι έννοιες της στατιστικής ανάλυσης, της μηχανική μάθησης και της εξόρυξης δεδομένων στην ανίχνευση εισβολών παρουσιάζουν πολλά στοιχεία αλληλο-κάλυψης και αλληλο-εξάρτησης. Αν θελήσουμε όμως να εφαρμόσουμε μία κατηγοριοποίηση τότε ο παραπάνω διαχωρισμός [Patcha, 2007] παρέχει μία ικανοποιητική προσέγγιση. Στις ακόλουθες παραγράφους περιγράφεται αναλυτικά κάθε κατηγορία.

2.2.1 Ανίχνευση Εισβολών με τη Χρήση Στατιστικών Μεθόδων

Στις μεθόδους ανίχνευσης ανωμαλιών που χρησιμοποιούν *στατιστικές τεχνικές*, το σύστημα παρατηρεί την υπάρχουσα δικτυακή δραστηριότητα και παράγει προφίλ για την αναπαράσταση της συγκεκριμένης συμπεριφοράς. Το προφίλ περιλαμβάνει μετρήσιμες μεταβλητές όπως είναι η ένταση της δραστηριότητας, η κατανομή των καταγεγραμμένων εγγραφών, ο χρόνος σύνδεσης και αποσύνδεσης κάθε συνεδρίας αλλά και η ποσότητα πόρων επεξεργαστής-μνήμη και δίσκος που καταναλώθηκαν κατά τη διάρκεια μίας συνεδρίας. Τυπικά το σύστημα ανίχνευσης εισβολών διατηρεί δύο προφίλ, το τρέχον και το αποθηκευμένο προφίλ. Καθώς πραγματοποιείται η επεξεργασία των δεδομένων του δικτύου και του συστήματος, το σύστημα ανίχνευσης εισβολών ανανεώνει το τρέχον προφίλ και περιοδικά υπολογίζει ένα βαθμό ανωμαλίας συγκρίνοντας το τρέχον προφίλ με το αποθηκευμένο. Εάν ο βαθμός ανωμαλίας είναι υψηλότερος από ένα συγκεκριμένο όριο, το σύστημα ανίχνευσης εισβολών παράγει ένα συναγερμό. Οι μέθοδοι ανίχνευσης εισβολών που βασίζονται σε στατιστικές μεθόδους είναι ιδιαίτερα αποτελεσματικές και ακριβείς για επιθέσεις που πραγματοποιούνται σε εκτεταμένες χρονικές περιόδους (π.χ. επιθέσεις άρνησης εξυπηρέτησης). Παρόλα αυτά επιδέξιοι επιτιθέμενοι μπορούν να εκπαιδεύσουν το σύστημα ανίχνευσης εισβολών που βασίζεται σε στατιστικές μεθόδους ώστε να δεχτεί τη "μη-φυσιολογική" συμπεριφορά ως "φυσιολογική". Επιπλέον δεν είναι δυνατόν όλες οι συμπεριφορές να μοντελοποιηθούν απόλυτα από στατιστικές μεθόδους. Χαρακτηριστικά παραδείγματα συστημάτων ανίχνευσης εισβολών

που βασίζονται σε στατιστικές μεθόδους είναι το Haystack [Smaha, 1998], το NIDES [Anderson, 1994], το SPADE [Staniford, 2002] αυτό που προτάθηκε από τους Ye και άλλους [Ye, 2002].

2.2.2 Ανίχνευση Ανωμαλιών με τη Χρήση Μηχανικής Εκμάθησης.

Η *μηχανική εκμάθηση* μπορεί να οριστεί ως η ικανότητα ενός συστήματος ή προγράμματος να μάθει και να βελτιώσει την απόδοσή του σε ένα συγκεκριμένο τομέα με την πάροδο του χρόνου. Η *μηχανική εκμάθηση* προσπαθεί να απαντήσει σε σημαντικό βαθμό στα ίδια θέματα με τις στατιστικές μεθόδους και την εξόρυξη δεδομένων. Παρόλα αυτά, σε αντίθεση με τις στατιστικές μεθόδους που προσπαθούν να κατανοήσουν τη διαδικασία με την οποία παράγονται τα δεδομένα, η *μηχανική εκμάθηση* επικεντρώνεται στη δημιουργία ενός συστήματος που βελτιώνει την απόδοσή του με βάση προηγούμενα αποτελέσματα. Με άλλα λόγια τα συστήματα που βασίζονται στη *μηχανική εκμάθηση* έχουν την ικανότητα να αλλάζουν τη στρατηγική τους με βάση τις νέες πληροφορίες που λαμβάνουν. Έχουν προταθεί πολλές μέθοδοι ανίχνευσης εισβολών που βασίζονται στη *μηχανική εκμάθηση* όπως είναι:

- Ανίχνευση εισβολών με *ανάλυση ακολουθίας κλήσεων συστήματος* που βασίζεται στην εκμάθηση της συμπεριφοράς ενός προγράμματος και την αναγνώριση σημαντικών αποκλίσεων από το "φυσιολογικό". Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας μεθόδου ανίχνευσης εισβολών είναι η μέθοδος που προτάθηκε από τους Forrest και άλλους [Forrest, 1996] με βάση την αναλογία ανάμεσα στο ανθρώπινο ανοσοποιητικό σύστημα και τα υπολογιστικά συστήματα.
- Ανίχνευση εισβολών με τη χρήση *Μπαυεζιανών δικτύων* τα οποία είναι γραφικά μοντέλα που κωδικοποιούν πιθανοθεωρητικές σχέσεις ανάμεσα στις μεταβλητές που μας ενδιαφέρουν [Ye, 2000].
- Ανίχνευση εισβολών με *ανάλυση κύριων στοιχείων (Principal component analysis (PCA))* μία τεχνική που βασίζεται στη μείωση των διαστάσεων των δεδομένων [Shyu, 2003].
- Ανίχνευση εισβολών με τη χρήση *κρυφών μαρκοβιανών μοντέλων (Hidden Markov Models (HMM))*, δηλαδή ενός στατιστικού μοντέλου όπου το σύστημα που μοντελοποιείται θεωρείται ότι είναι μία *Μαρκοβιανή* διαδικασία με άγνωστες παραμέτρους [Yeung, 2003].

2.2.3 Ανίχνευση Ανωμαλιών με τη Χρήση Εξόρυξης Δεδομένων

Η *εξόρυξη δεδομένων* μπορεί να οριστεί ως η διαδικασία αποκάλυψης προτύπων, συσχετίσεων, αλλαγών ανωμαλιών, και στατιστικά σημαντικών δομών και γεγονότων από τα δεδομένα [Grossman, 1997]. Με άλλα λόγια, η *εξόρυξη δεδομένων* έχει τη δυνατότητα να λάβει δεδομένα ως είσοδο, και να παράγει από αυτά πρότυπα ή αποκλίσεις, που δεν μπορούν να εντοπιστούν εύκολα με γυμνό μάτι. Ένας άλλος όρος που χρησιμοποιείται συχνά για την εξόρυξη δεδομένων είναι η *ανακάλυψη γνώσης (discovery knowledge)*. Η *εξόρυξη*

δεδομένων μπορεί να βοηθήσει σημαντικά προκειμένου να βελτιωθεί η διαδικασία της ανίχνευσης εισβολών με μεγαλύτερη εστίαση στην ανίχνευση ανωμαλιών. Αναγνωρίζοντας τα όρια της έγκυρης δικτυακής δραστηριότητας, η *εξόρυξη δεδομένων* βοηθά σημαντικά έναν διαχειριστή δικτύου/αναλυτή να διακρίνει την δικτυακή δραστηριότητα επίθεσης από τη συνηθισμένη καθημερινή δικτυακή κυκλοφορία. Η ανίχνευση εισβολών με τη χρήση *εξόρυξης δεδομένων* μπορεί να διακριθεί στις ακόλουθες βασικές κατηγορίες:

- Την ανίχνευση εισβολών με τη χρήση μεθόδων *ταξινόμησης (classification)* η οποία μπορεί να πραγματοποιηθεί με τη χρήση τεχνικών παραγωγής κανόνων ([Cohen, 1995], [Quinlan, 1993]) με ασαφή λογική [Dickerson, 2000], γενετικούς αλγόριθμους ([Li, 2004], [Pillai, 2004]) και τεχνικές που βασίζονται σε νευρωνικά δίκτυα ([Ghosh, 2000], [Ramadas, 2003]).
- Την ανίχνευση εισβολών με *ομαδοποίηση (clustering)* [Portnoy, 2001] και ανίχνευση εκτοπών (*outlier detection)* ([Hautamaki, 2004], [Ertöz, 2004]). Η τεχνική της ομαδοποίησης βασίζεται στην εύρεση προτύπων σε δεδομένα που δεν έχουν ετικέτες (unlabeled) και παρουσιάζουν πολλές διαστάσεις. Ενώ η ανίχνευση εκτοπών (*outlier detection)* βασίζεται στις αποστάσεις ανάμεσα στα σημεία και την πυκνότητα των τοπικών γειτονιών.
- Την ανίχνευση εισβολών με τη χρήση *κανόνων συσχέτισης (association rules discovery)* [Lee, 1999] η οποία βασίζεται στην εύρεση γεγονότων που τείνουν να συμβαίνουν μαζί.

3. Ανίχνευση Εισβολών με τη Χρήση Αλγόριθμων Ταξινόμησης

Από τις παραπάνω κατηγορίες ανίχνευσης εισβολών επιλέξαμε να χρησιμοποιήσουμε την ανίχνευση εισβολών με χρήση αλγόριθμων ταξινόμησης. Τα περισσότερα συστήματα ανίχνευσης εισβολών παρουσιάζουν μεγάλη δυσκολία στην επιτυχημένη ταξινόμηση και διάκριση των εισβολών από τη "φυσιολογική" δικτυακή συμπεριφορά, καθιστώντας δύσκολη τη δημιουργία ενός ανθεκτικού συστήματος ανίχνευσης εισβολών σε πραγματικό χρόνο. Οι αλγόριθμοι ταξινόμησης χρησιμοποιούνται στην ανίχνευση εισβολών προκειμένου να βελτιώσουν την απόδοσή της στην αναζήτηση και ανάλυση δεδομένων από ήδη καταγεγραμμένα αρχεία υπολογιστικών συστημάτων. Ένα σύστημα ανίχνευσης εισβολών που ταξινομεί τα καταγεγραμμένα δεδομένα χρησιμοποιώντας ένα σύνολο κανόνων, πρότυπα ή κάποια άλλη τεχνική ταξινόμησης μπορεί γενικά να οριστεί σαν ένα σύστημα ανίχνευσης εισβολών που βασίζεται στην ταξινόμηση.

Επιλέγουμε λοιπόν τους αλγόριθμους ταξινόμησης και εκμεταλλευόμαστε τα πλεονεκτήματά τους προκείμενου να επιτύχουμε αξιόπιστη και αποτελεσματική ανίχνευση εισβολών. Οι αλγόριθμοι ταξινόμησης είναι ιδιαίτερα απλοί στη λειτουργία και χρήση τους, αυτοματοποιημένοι, παράγουν άμεσα και ακριβή αποτελέσματα και έχουν εκτεταμένες εφαρμογές, μεγάλη βιβλιογραφική κάλυψη

και εκτενή πειραματική εμπειρία που καταδεικνύει την αποτελεσματικότητα τους.

Η ιδανική εφαρμογή της ανίχνευσης εισβολών με αλγόριθμους ταξινόμησης βασίζεται στη συγκέντρωση αρκετών "φυσιολογικών" και "μη-φυσιολογικών" καταγεγραμμένων δεδομένων που αντιστοιχούν στη συμπεριφορά ενός χρήστη ή ενός προγράμματος. Στη συνέχεια εφαρμόζεται ο αλγόριθμος ταξινόμησης προκειμένου να εκπαιδευθεί ο ταξινομητής και να μπορέσει να προβλέψει την κλάση ("φυσιολογικά" ή "μη-φυσιολογικά") νέων καταγεγραμμένων δεδομένων.

Ένας ταξινομητής δημιουργείται όταν εφαρμοστεί ένας αλγόριθμος εκμάθησης σε ένα σύνολο δεδομένων. Το σύνολο δεδομένων εκπαίδευσης αποτελείται από έναν αριθμό εγγραφών, και διανυσμάτων, όπου κάθε διάνυσμα αποτελείται από ένα σύνολο πεδίων-χαρακτηριστικών. Ο στόχος ενός ταξινομητή είναι να χρησιμοποιήσει ένα διάνυσμα χαρακτηριστικών και να αντιστοιχίσει σε κάθε διάνυσμα μία κατηγορία. Προκειμένου να χρησιμοποιήσουμε έναν ταξινομητή σε ένα πρόβλημα ακολουθούμε μία διαδικασία αναγνώρισης προτύπου. Ο σχεδιασμός του συστήματος αναγνώρισης προτύπου (Σχήμα 1.2) [Duda, 2001] συνήθως περιλαμβάνει την επανάληψη ενός αριθμού διαφορετικών δραστηριοτήτων: τη *συλλογή δεδομένων*, την *επιλογή πεδίων-χαρακτηριστικών*, την *επιλογή μοντέλου*, την *εκπαίδευση του ταξινομητή* και την *δοκιμή και αξιολόγησή του*.

Τα βασικά βήματα που περιλαμβάνει ένα σύστημα ανίχνευσης εισβολών που βασίζεται σε αλγόριθμους ταξινόμησης είναι τα ακόλουθα:

Συλλογή Δεδομένων: Η συλλογή δεδομένων έχει να κάνει με το πρόβλημα που θέλουμε να λύσουμε και είναι ιδιαίτερα σημαντική η συλλογή ενός αρκετά μεγάλου και αντιπροσωπευτικού συνόλου παραδειγμάτων για την εκπαίδευση και τη δοκιμή του ταξινομητή.

Επιλογή Πεδίων: Η επιλογή των κατάλληλων πεδίων που βοηθά στο διαχωρισμό των κλάσεων, τα οποία είναι αντιπροσωπευτικά για κάθε πρόβλημα, είναι ένα ιδιαίτερα σημαντικό βήμα. Στην επιλογή των πεδίων σαν κριτήριο χρησιμοποιείται το γεγονός, τα πεδία να μπορούν να ληφθούν εύκολα από το σύνολο δεδομένων, να μην επηρεάζονται από το θόρυβο και να είναι χρήσιμα για το διαχωρισμό των προτύπων σε διαφορετικές κατηγορίες.

Επιλογή Μοντέλου: Προκειμένου να επιλέξουμε το κατάλληλο μοντέλο χρησιμοποιούμε συγκεκριμένες μεθόδους για τη ρύθμιση των παραμέτρων του μοντέλου εκπαίδευσης έτσι ώστε να επιτυγχάνεται ένας συγκεκριμένος στόχος, για παράδειγμα να ελαχιστοποιείται το λάθος ταξινόμησης.

Εκπαίδευση Ταξινομητή: Έχοντας επιλέξει το κατάλληλο μοντέλο και τις κατάλληλες παραμέτρους εκπαιδεύουμε τον ταξινομητή μας.

Δοκιμή και Αξιολόγηση Ταξινομητή: Δοκιμάζουμε τον ταξινομητή μας σε ένα σύνολο δεδομένων δοκιμής και εξετάζουμε την αποτελεσματικότητα του ταξινομητή μας. Τα αποτελέσματα της αξιολόγησης μπορεί να οδηγήσουν σε επανάληψη διάφορων προηγούμενων βημάτων προκειμένου να λάβουμε ικανοποιητικά αποτελέσματα.

Σχήμα 1. 2 Διαδικασία Αναγνώρισης Προτύπου

4. Περιγραφή του Προβλήματος – Στόχος της Διατριβής

Το πρόβλημα που καλούμαστε να λύσουμε είναι σύνθετο και πολυδιάστατο:

- Οι επιθέσεις εναντίον των υπολογιστικών και δικτυακών τεχνολογιών απειλούν καθημερινά τη ζωή μας, όχι μόνο τον εργασιακό τομέα αλλά ακόμα και τον τομέα επικοινωνίας, μετακινήσεων ακόμα και διασκέδασης. Δεχόμαστε μία πληθώρα επιθέσεων και αναρωτιόμαστε πως μπορούμε να τις αντιμετωπίσουμε. Πριν όμως αναζητήσουμε τρόπους αντιμετώπισης πρέπει να κατανοήσουμε τις ίδιες τις επιθέσεις τον τρόπο λειτουργίας τους και τα μέσα που χρησιμοποιούν. Επιπλέον, καλούμαστε να εξετάσουμε τις αδυναμίες που παρουσιάζουν οι υπάρχοντες μηχανισμοί αντιμετώπισης επιθέσεων, οι οποίες παρεμποδίζουν την αποτελεσματικότητα των μηχανισμών αντιμετώπισης επιθέσεων.
- Είναι σημαντικό να κατανοήσουμε τη ευαρότητα των επιθέσεων ενάντια των υπολογιστικών και δικτυακών επικοινωνιών και να εξετάσουμε την ύπαρξη κάποιων βασικών βημάτων που θα μπορούσαν να εφαρμοστούν στους σύγχρονους οργανισμούς προκειμένου να διασφαλιστεί σε κάποιο βαθμό η ομαλή λειτουργία τους.

- Καλούμαστε επίσης να βρούμε αποτελεσματικούς τρόπους ανίχνευσης εισβολών που θα έχουν τη δυνατότητα να διακρίνουν με ακρίβεια τη "φυσιολογική" από τη "μη-φυσιολογική" δικτυακή κίνηση.
- Αφού στόχος μας είναι η χρησιμοποίηση αλγόριθμων ταξινόμησης προκείμενου να ανιχνεύουμε επιθέσεις, καλούμαστε να βρούμε τους κατάλληλους ταξινομητές και τα κατάλληλα πεδία (χαρακτηριστικά) δικτυακής κίνησης που θα μας βοηθήσουν να κάνουμε διαχωρισμό μεταξύ επίθεσης και "φυσιολογικής" δικτυακής κίνησης.
- Η προτεινόμενη μέθοδος ανίχνευσης εισβολών θα πρέπει να παρέχει αξιόπιστα αποτελέσματα τα οποία δεν μπορούν να τροποποιούν οι κακόβουλοι επιτιθέμενοι. Επομένως, ο συνδυασμός με μηχανισμούς παρεμπόδισης εισβολών είναι επιθυμητός.
- Στόχος του συστήματος ανίχνευσης εισβολών είναι η αξιόπιστη ανίχνευση εισβολών. Το σύστημα ανίχνευσης εισβολών θα πρέπει να δίνει όσο το δυνατόν λιγότερους λανθασμένους συναγερμούς για τη νόμιμη δικτυακή κυκλοφορία που την αναγνωρίζει σαν επίθεση (λανθασμένοι θετικοί συναγερμοί). Παράλληλα το σύστημα ανίχνευσης εισβολών δεν πρέπει να αποτυγχάνει στην ανίχνευση δικτυακής κυκλοφορίας επίθεσης (λανθασμένοι αρνητικοί συναγερμοί).
- Είναι σημαντικό τα αποτελέσματα που παράγει το σύστημα ανίχνευσης εισβολών να είναι εύκολα αντιληπτά και να διευκολύνουν το έργο του διαχειριστή δικτύου στον εντοπισμό των επιθέσεων.
- Η ανίχνευση των εισβολών να πραγματοποιείται σε πραγματικό χρόνο ώστε να υπάρχει άμεση απόκριση.
- Το σύστημα ανίχνευσης εισβολών θα πρέπει να αναλύει και να αποκωδικοποιεί δικτυακά γεγονότα για ορισμένα πρωτόκολλα και υπηρεσίες που δεν είναι αναγνώσιμες από τον άνθρωπο και να τα παρέχει σε μορφή αναγνώσιμη.
- Το σύστημα ανίχνευσης εισβολών δεν πρέπει να χάνει τη "γενική εικόνα" όταν εξετάζει λεπτομέρειες χαμηλού επιπέδου.
- Δεν πρέπει να απαιτείται ο διαχειριστής του συστήματος ανίχνευσης εισβολών να έχει υπερβολική ειδίκευση προκειμένου να το διαχειριστεί. Θα πρέπει λοιπόν ο χειριστής να μπορεί εύκολα να το χρησιμοποιήσει και να το κατανοήσει.
- Πρέπει να είναι απλό στην εφαρμογή του. Αυτό μπορεί να επιτευχθεί εάν μπορεί εύκολα να μεταφερθεί σε διαφορετικές αρχιτεκτονικές και λειτουργικά συστήματα, μέσω απλών μηχανισμών εγκατάστασης.
- Δεν πρέπει να προκαλεί υψηλή υπερφόρτωση του συστήματος στο όποιο λειτουργεί προκειμένου να αποφευχθεί ή παρέμβασή του στην ομαλή λειτουργία του συστήματος.
- Καλούμαστε να εξετάσουμε τη δυνατότητα εφαρμογής της μεθόδου ανίχνευσης και στα ασύρματα δίκτυα, τα οποία παρουσιάζουν

ιδιαίτερες αδυναμίες και ευπάθειες κυρίως λόγω των περιορισμένων διαθέσιμων πόρων.

- Είναι σημαντικό η ανίχνευση εισβολών να πραγματοποιείται με τέτοιο τρόπο ώστε να επιτρέπει την άμεση και αποτελεσματική απόκριση προκειμένου να παρεμποδίζονται οι εκτεταμένες απώλειες που μπορούν να προκληθούν από τις επιθέσεις.
- Στα ασύρματα δίκτυα το πρόβλημα καθίσταται ακόμα πιο δύσκολο καθώς οι περιορισμένοι πόροι των ασύρματων δικτυακών συσκευών και η ανύπαρκτη φυσική ασφάλεια καθιστούν επιτακτική και άμεση την απόκριση σε πιθανές εισβολές και την προστασία των συστημάτων ανίχνευσης εισβολών ώστε να μην διαβληθούν και χρησιμοποιηθούν από κακόβουλους χρήστες.
- Η απόκριση και ενημέρωση των δικτυακών κόμβων θα πρέπει να πραγματοποιείται με τέτοιο τρόπο ώστε να μη προκαλεί προβλήματα στη δικτυακή κυκλοφορία (π.χ. πλημμύρα μηνυμάτων συναγερμών-ενημέρωσης).
- Το σύστημα ανίχνευσης εισβολών θα πρέπει να έχει τη δυνατότητα ανανέωσης ώστε να ανταποκρίνεται σε νέες δικτυακές συνθήκες και επιθέσεις. Πρέπει λοιπόν να είναι προσαρμόσιμο σε αλλαγές του συστήματος και της συμπεριφοράς του χρήστη με την πάροδο του χρόνου. Για παράδειγμα, συχνά νέες εφαρμογές εγκαθίστανται, οι χρήστες αλλάζουν τις δραστηριότητές τους, νέοι πόροι είναι διαθέσιμοι, ενώ στα ασύρματα δίκτυα η δικτυακή τοπολογία αλλάζει είτε λόγω κινητικότητας είτε λόγω των περιορισμένων πόρων. Όλα αυτά επηρεάζουν σημαντικά τα πρότυπα που χρησιμοποιεί το σύστημα και είναι σημαντικό το σύστημα ανίχνευσης εισβολών να μπορεί να ανταποκριθεί στις νέες συνθήκες.
- Το σύστημα ανίχνευσης εισβολών θα πρέπει να είναι προσαρμόσιμο όχι μόνο στις δικτυακές συνθήκες αλλά και στις δικτυακές επιθέσεις οι οποίες εξελίσσονται καθημερινά. Οι αλλαγές στις δικτυακές επιθέσεις πρέπει να ενσωματώνονται στο σύστημα.
- Το σύστημα ανίχνευσης εισβολών θα πρέπει να είναι αρκετά γενικό ώστε να ανιχνεύει διαφορετικούς τύπους επιθέσεων.
- Ένα επίσης σημαντικό πρόβλημα που καλούμαστε να εξετάσουμε είναι ο περιορισμός του αναμενόμενου κόστους ενός συστήματος ανίχνευσης εισβολών. Επιθυμητό είναι το σύστημα ανίχνευσης εισβολών να λειτουργεί λαμβάνοντας υπόψη ότι κάθε απόφαση που λαμβάνει έχει και το αντίστοιχο κόστος. Είναι επιθυμητό να επιτύχουμε ένα συμβιβασμό ανάμεσα στο μικρότερο δυνατό κόστος ενός συστήματος ανίχνευσης εισβολών με αξιόπιστη ανίχνευση εισβολών και περιορισμένο αριθμό λανθασμένων συναγερμών.

5. Προτεινόμενη Λύση – Μεθοδολογία της Διατριβής

Προκειμένου να επιλύσουμε αυτό το πολύπλοκο πρόβλημα που περιγράφεται στην προηγούμενη ενότητα, ακολουθήσαμε μία προσέγγιση πολλαπλών κατευθύνσεων ώστε να καλύψουμε όλες τις διαστάσεις του προβλήματος. Συγκεκριμένα οι συνεισφορές της προσέγγισής μας είναι οι ακόλουθες:

- Επιλέξαμε μία από τις πιο μεγάλες απειλές των δικτυακών και υπολογιστικών επικοινωνιών, των επιθέσεων Άρνησης Εξυπηρέτησης (Denial of Service (DoS)) προκειμένου να πραγματοποιήσουμε μία πλήρη επισκόπηση της υπάρχουσας γνώσης στο πεδίο των επιθέσεων αυτών. Στόχος είναι η κατανόηση αυτών των επιθέσεων του τρόπου λειτουργίας τους και η πλήρης ανάλυση των μέσων που χρησιμοποιούν προκειμένου να προκαλέσουν καταστρεπτικές επιδράσεις στα θύματα τους. Συγκεκριμένα, παρουσιάζουμε μία γενικότερη ολοκληρωμένη και δομημένη εικόνα στο πεδίο των επιθέσεων DoS παρουσιάζοντας το πρόβλημα των επιθέσεων και προτείνοντας ταξινομήσεις τόσο για τις επιθέσεις όσο και για τους μηχανισμούς που έχουν προταθεί για την αντιμετώπιση των επιθέσεων αυτών.

- Η κατηγοριοποίηση των επιθέσεων περιλαμβάνει τόσο γνωστούς όσο και πιθανούς μηχανισμούς επίθεσης. Επιπλέον, περιγράφουμε τα σημαντικά χαρακτηριστικά κάθε επίθεσης και κατηγορίας μηχανισμών προστασίας και αναλύουμε τα πλεονεκτήματα και μειονεκτήματα κάθε προτεινόμενου σχήματος αντιμετώπισης των επιθέσεων. Στόχος μας είναι να περιγράψουμε τα υπάρχοντα προβλήματα ώστε να επιτύχουμε καλύτερη κατανόηση του προβλήματος των επιθέσεων DoS και να σχεδιάσουμε πιο αποτελεσματικούς μηχανισμούς αντιμετώπισης.

- Σημειώνουμε τη σοβαρότητα που έχουν οι επιθέσεις DoS για τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης έναν τομέα ιδιαίτερο κρίσιμο και σημαντικό. Για το σκοπό αυτό παρουσιάζουμε στατιστικά στοιχεία και χαρακτηριστικά περιστατικά των επιθέσεων DoS στις υπηρεσίες ηλεκτρονικής διακυβέρνησης που υποδηλώνουν ξεκάθαρα το μέγεθος της απειλής και των καταστρεπτικών συνεπειών που μπορούν να επιφέρουν. Επιπλέον, παρουσιάζουμε μία λίστα με τις καλύτερες πρακτικές που μπορούν να χρησιμοποιηθούν από τους κυβερνητικούς οργανισμούς προκειμένου να ενδυναμώσουν περισσότερο την ασφάλεια στα συστήματά τους και να τους βοηθήσουμε να προστατέψουν τα συστήματά τους από το ενδεχόμενο να συμμετάσχουν σε μία επίθεση DDoS ή να γίνουν θύμα μίας επίθεσης DoS/DDoS. Μακροχρόνια μέτρα αντιμετώπισης προτείνονται επίσης που πρέπει να υιοθετηθούν για πιο αποτελεσματικές λύσεις στο πρόβλημα.

- Προτείνουμε τη χρήση μοντέλων ταξινόμησης και ταξινομητών προκειμένου να πραγματοποιήσουμε ανίχνευση εισβολών σε ενσύρματα και ασύρματα δίκτυα.
- Προκειμένου να απαλλάξουμε τους διαχειριστές δικτύων από την ιδιαίτερα δύσκολη και χρονοβόρα εργασία εξέτασης της δικτυακής κυκλοφορίας και να αποφύγουμε μεγάλη επιβάρυνση επεξεργασίας, προτείνουμε μία προσέγγιση ανίχνευσης εισβολών που βασίζεται σε μία κατηγορία νευρωνικών δικτύων που είναι γνωστά σαν αναδυόμενοι *Αυτό-Οργανούμενοι Χάρτες (emergent Self-Organizing Maps (eSOM))*. Συνδυάζοντας τις τεχνικές μηχανικής μάθησης και απεικόνισης πληροφοριών έχουμε τη δυνατότητα να έχουμε μία πιο ξεκάθαρη εικόνα της δικτυακής δραστηριότητας.
- Η προτεινόμενη μέθοδος ανίχνευσης εισβολών με τη χρήση eSOM παράγει μία απεικόνιση πληροφοριών που είναι τοπολογικά διατηρήσιμη και δίνει στους διαχειριστές δικτύου τη δυνατότητα να παρατηρήσουν την δικτυακή κυκλοφορία σε ένα ανώτερο, συνολικό επίπεδο, χωρίς να λαμβάνουν υπόψη τις τμηματικές δομές, παρέχοντας τους οπτικά πληροφορίες που διαφορετικά θα ήταν αόρατες.
- Η προτεινόμενη μέθοδος ανίχνευσης εισβολών με τη χρήση eSOM εκμεταλλεύεται την φυσική ικανότητα του ανθρώπου να αναλύει οπτικά πολύπλοκες πληροφορίες.
- Η προτεινόμενη μεθοδολογία ανίχνευσης εισβολών εφαρμόζεται τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα κατά περίσταση (ad hoc networks) και παράγει υποσχόμενα αποτελέσματα στην ικανότητά της να ταξινομεί τη "φυσιολογική" απέναντι στη "μη-φυσιολογική" συμπεριφορά.
- Στα ασύρματα δίκτυα κατά περίσταση στα οποία το πρόβλημα διασφάλισής τους καθίσταται ιδιαίτερα δύσκολο λόγω των περιορισμένων πόρων τους προτείνουμε έναν αποτελεσματικό μηχανισμό απόκρισης σε εισβολές προκειμένου να περιορίσουμε τις καταστρεπτικές συνέπειες των επιθέσεων.
- Ο προτεινόμενος μηχανισμός απόκρισης βασίζεται στην ασφαλή διανομή των χαρτών που παράγονται από το eSOM στους γειτονικούς κόμβους του θύματος-κόμβου προκειμένου να επιτύχουμε άμεση και πραγματικού χρόνου απόκριση. Η απόκριση βασίζεται στην ασφαλή και αποτελεσματική δρομολόγηση αποφεύγοντας μονοπάτια που περιλαμβάνουν κόμβους οι οποίοι είναι θύματα επιθέσεων.
- Ο τρόπος λειτουργίας της μονάδας απόκρισης είναι αξιόπιστος και βασίζεται στη χρήση ενός προτεινόμενου πιστοποιημένου πρωτοκόλλου δημιουργίας ομαδικού κλειδιού. Κατά αυτό τον τρόπο διασφαλίζεται η αξιόπιστη λειτουργία και προστατεύεται από επίδοξους κακόβουλους επιτιθέμενους χρήστες, που πιθανόν να προσπαθήσουν να τη διαβάλλουν.

- Προκείμενου να αποφευχθούν πιθανά προβλήματα (π.χ. πλημμύρα μηνυμάτων συναγερμών- ενημέρωσης) από τη λειτουργία της μονάδας απόκρισης, διακρίνουμε δύο είδη μονάδων απόκρισης, την *Καθολική Μονάδα Απόκρισης* και την *Τοπική Μονάδα Απόκρισης*. Η μονάδα Καθολικής Απόκρισης παρέχει ενημέρωση σε όλους τους κόμβους που βρίσκονται στην εμβέλεια του θύματος-κόμβου και ενεργοποιείται μόνο σε πολύ σοβαρές και εκτεταμένες επιθέσεις.
- Προκειμένου να διασφαλίσουμε την ομαλή λειτουργία της ανίχνευσης εισβολών με τη χρήση eSOM προτείνουμε μία καινοτόμα μέθοδο υδατογράφησης, η οποία δεν επιτρέπει σε κακόβουλους επιτιθέμενους να τροποποιήσουν τα αποτελέσματα της μηχανής ανίχνευσης εισβολών.
- Εξετάζουμε την απόδοση και άλλων αλγόριθμων ταξινόμησης εκτός από το eSOM για το πρόβλημα της ανίχνευσης εισβολών τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα. Συγκεκριμένα, εξετάζουμε την απόδοση του *πολυ-επίπεδου Perceptron (MultiLayer Perceptron (MLP) αλγόριθμου*, του *Γραμμικού (Linear)* ταξινομητή, του αλγόριθμου *Γκαουσσιανών μειγμάτων (Gaussian Mixture Model (GMM))*, του ταξινομητή *απλοϊκού μοντέλου (Naïve Bayes)* και των *Μηχανών Υποστήριξης Αποφάσεων (Support Vector Machines (SVM))*.
- Λαμβάνοντας υπόψη μας το γεγονός ότι στην ανίχνευση εισβολών η απαίτηση δεν είναι απλά να προβλέψουμε την πιο πιθανή ετικέτα κλάσης (label), αφού διαφορετικοί τύποι λαθών επιφέρουν διαφορετικό κόστος προτείνουμε την υλοποίηση μίας προσέγγισης ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος και την εφαρμόζουμε σε μερικούς πολύ γνωστούς και αποτελεσματικούς ταξινομητές.
- Η απόδοση της χρήσης των αλγόριθμων ταξινόμησης στην ανίχνευση εισβολών τόσο με ευαισθησία ως προς το κόστος όσο και χωρίς εξετάζεται σε διαφορετικές πειραματικές συνθήκες τόσο για ενσύρματα όσο και για ασύρματα δίκτυα και μοντέλα ταξινόμησης όσον αφορά στο αναμενόμενο κόστος, στην ανίχνευση εισβολών και στους λανθασμένους συναγερμούς.
- Οι προτεινόμενοι μηχανισμοί ανίχνευσης εισβολών μπορούν να επεκταθούν στην ανίχνευση πολλών διαφορετικών τύπων επίθεσης.
- Οι προτεινόμενοι μηχανισμοί ανίχνευσης έχουν τη δυνατότητα ανανέωσης ώστε να ανταποκρίνονται σε νέες δικτυακές συνθήκες αλλά και σε εξελιγμένες μορφές επιθέσεων.
- Τα προτεινόμενα συστήματα ανίχνευσης εισβολών είναι απλά στην εφαρμογή τους και μπορούν εύκολα να μεταφερθούν σε διαφορετικές αρχιτεκτονικές και λειτουργικά συστήματα.

6. Οργάνωση της Διατριβής

Στο πρώτο κεφάλαιο περιγράφεται η ανίχνευση εισβολών και οι βασικές μεθοδολογίες που χρησιμοποιεί. Περιγράφεται αναλυτικά το πρόβλημα και ο στόχος της διατρβής αλλά και η προτεινόμενη λύση και μεθοδολογία.

Στο δεύτερο κεφάλαιο παρουσιάζεται μία πλήρης επισκόπηση της υπάρχουσας γνώσης στο πεδίο των επιθέσεων *Άρνησης Εξυπηρέτησης (Denial of Service (DoS))*. Στο κεφάλαιο αυτό ερευνούμε το πρόβλημα των επιθέσεων DoS και των κατανεμημένων επιθέσεων DoS (DDoS) και παρουσιάζουμε κατηγοριοποιήσεις για τις επιθέσεις DoS και DDoS. Επιπλέον, δίνουμε τα βασικά χαρακτηριστικά γνωστών εργαλείων DDoS, παρουσιάζουμε τα προβλήματα αντιμετώπισης των επιθέσεων DDoS και προτείνουμε μία κατηγοριοποίηση των μηχανισμών αντιμετώπισής τους.

Στο τρίτο κεφάλαιο παρουσιάζουμε περιστατικά επιθέσεων DoS/DDoS, καθώς και αποτελέσματα από έρευνες που σχετίζονται με τις επιθέσεις DoS/DDoS. Επιπλέον παρουσιάζουμε τις καλύτερες πρακτικές για την αντιμετώπιση των επιθέσεων DoS που μπορούν να χρησιμοποιηθούν από τις κυβερνητικές οργανώσεις αλλά και μακροχρόνια μέτρα αντιμετώπισης τους.

Στο τέταρτο κεφάλαιο περιγράφουμε τη μέθοδο ανίχνευσης εισβολών προκειμένου να ανιχνεύσουμε δικτυακές επιθέσεις που βασίζεται στη χρήση *αναδυόμενων Αυτο-Οργανούμενων Χαρτών (emergent Self-Organizing Maps (eSOM))*. Συγκεκριμένα περιγράφεται ο αλγόριθμος Kohonen SOM στον οποίο βασίζονται τα eSOM, παρουσιάζονται σχετικές εργασίες προτεινόμενων μεθόδων ανίχνευσης εισβολών που βασίζονται στα KSOM και περιγράφονται τα eSOM και οι διαφορές τους από τα απλά KSOM. Παρουσιάζεται αναλυτικά η προτεινόμενη μέθοδος ανίχνευσης εισβολών και η αξιολόγηση της απόδοσής της με πειραματικά αποτελέσματα για την ανίχνευση των επιθέσεων DoS, Probe, R2L (Remote To Local) και U2R (User to Root).

Στο πέμπτο κεφάλαιο περιγράφουμε την προσέγγισή μας προκειμένου να διασφαλίσουμε τα ασύρματα δίκτυα κατά περίσταση, η οποία βασίζεται στην ανίχνευση και απόκριση σε εισβολές. Συγκεκριμένα περιγράφουμε τον τρόπο λειτουργίας των ασυρμάτων δικτύων κατά περίσταση αλλά και τα προβλήματα ασφάλειας που παρουσιάζουν. Περιγράφουμε σχετική εργασία για την ανίχνευση εισβολών στα ασύρματα δίκτυα κατά περίσταση και σχετική εργασία για την ανίχνευση εισβολών με τη χρήση πρωτοκόλλων συμφωνίας κλειδιού. Στη συνέχεια περιγράφουμε την προσέγγισή μας για την διαφύλαξη των ασύρματων δικτύων η οποία βασίζεται στη χρήση eSOM για την ανίχνευση των εισβολών και σε ένα προτεινόμενο πιστοποιημένο πρωτόκολλο συμφωνίας κλειδιού για την αξιόπιστη απόκριση σε εισβολές. Παρουσιάζεται επίσης η αξιολόγηση της προσέγγισής για διαφορετικές πειραματικές συνθήκες όσον αφορά στην ανίχνευση εισβολών και στους λανθασμένους συναγερμούς.

Στο έκτο κεφάλαιο περιγράφεται η προτεινόμενη προσέγγισή μας για τη διασφάλιση των χαρτών eSOM που παράγει η μηχανή ανίχνευσης εισβολών, με τη χρήση τεχνικών υδατογράφησης. Συγκεκριμένα περιγράφεται αναλυτικά η προτεινόμενη προσέγγιση υδατογράφησης και ο τρόπος εφαρμογής της στη μηχανή ανίχνευσης εισβολών που προτάθηκε για τα ασύρματα δίκτυα κατά περίσταση. Περιγράφονται αναλυτικά οι μέθοδοι ενσωμάτωσης Lattice και Block-Wise στις οποίες βασίζεται και παρουσιάζεται η αξιολόγηση της απόδοσής της.

Στο έβδομο κεφάλαιο εξετάζουμε τη δυνατότητα των συστημάτων ανίχνευσης εισβολών να μεγιστοποιήσουν την παρεχόμενη ασφάλεια ελαχιστοποιώντας το αναμενόμενο κόστος. Εξετάζουμε λοιπόν, τη δυνατότητα κατασκευής ενός συστήματος ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος. Μελετάμε την απόδοση αυτής της προσέγγισης τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα και την εφαρμογή της σε κάποιους πολύ γνωστούς αλγόριθμους ταξινόμησης, το πολυ-επίπεδο Perceptron (Multilayer Perceptron (MLP)), τον αλγόριθμο Γκαουσιανών μειγμάτων (Gaussian Mixture Model (GMM)), το γραμμικό (Linear) ταξινομητή και τον ταξινομητή απλοϊκού μοντέλου Bayes (Naïve Bayes). Επιπλέον, εξετάζουμε την απόδοση των παραπάνω αλγόριθμων και των μηχανών υποστήριξης αποφάσεων (Support Vector Machines (SVM)) στην ανίχνευση των επιθέσεων χωρίς τη χρήση κόστους σε ενσύρματα και ασύρματα δίκτυα κατά περίσταση για διάφορες δικτυακές συνθήκες.

Τέλος, στο όγδοο κεφάλαιο παρουσιάζουμε τα συμπεράσματα αυτής της διατριβής, τα θέματα μελλοντικής έρευνας και τις πιθανές επεκτάσεις.

Βιβλιογραφία

[Anderson, 1980] J.P Anderson, *"Computer Security Threat Monitoring and Surveillance"*, Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.

[Anderson, 1994] D. Anderson, T. Frivold, A. Tamaru, A. Valdes, *"Next generation intrusion detection expert system (NIDES)"*, Software Users Manual, Beta-Update release, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, Technical Report SRI-CSL-95-0, May 1994.

[Bace, 2000] R. G. Bace, *"Intrusion Detection"*, Macmillan Technical Publishing, 2000.

[Cohen, 1995] W.W. Cohen, *"Fast Effective Rule Induction"*, In Proceedings of the 12th International Conference on Machine Learning, Tahoe City, CA, 1995, pp. 115-123.

[Debar, 1999] H. Debar, M. Dacier, A. Wespi, *"Towards a Taxonomy of Intrusion Detection Systems"*, Computer Networks (31), 1999, pp. 805-822.

[Dickerson, 2000] J.E. Dickerson, J.A. Dickerson, *"Fuzzy network profiling for intrusion detection"*, In Proceedings of the 19th International Conference of the

North American Fuzzy Information Processing Society (NAFIPS), Atlanta, GA, 2000, pp. 301–306.

[Duda, 2001] R.O. Duda, P.E. Hart, D.G. Stork, *"Pattern Classification"*, A Wiley-Interscience Publication, John Wiley & Sons, Inc. 2001, Second Edition.

[Ertöz, 2004] L. Ertöz, E. Eilertson, A. Lazarevic, P.-N. Tan, V. Kumar, J. Srivastava, P. Dokas, *"The MINDS - Minnesota INtrusion Detection System"*, In Next Generation Data Mining, MIT Press, Boston, 2004.

[Forrest, 1996] S. Forrest, S.A. Hofmeyr, A. Somayaji, T.A. Longstaff, *"A Sense of Self for Unix Processes"*, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, USA, 1996, pp. 120–128.

[Garvey, 1991] T. Garvey, T. Lunt, *"Model-Based Intrusion Detection"*, In Proceedings of 14th National Computer Security Conf., October 1991, pp. 372–385.

[Ghosh, 2000] A.K. Ghosh, C. Michael, M. Schatz, *"A Real-Time Intrusion Detection System Based on Learning Program Behavior"*, In Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection Toulouse, France, 2000, pp. 93–109.

[Grossman, 1997] R. Grossman, *"Data Mining: Challenges and Opportunities for Data Mining During the Next Decade"*, 1997.

[Habra, 1992] N. Habra, B. Le Charlier, A. Mounji, I. Mathieu, *"Asax: Software Architecture and Rule-Based Language for Universal Audit Trail Analysis"*, In Proceedings of 2nd European Symposium on Research in Computer Security (ESORICS, 1992), Toulouse, Berlin, Lecture Notes in Computer Science, vol. 648, Springer, Berlin, November 1992.

[Hautamaki, 2004] V. Hautamaki, I. Karkkainen, P. Franti, *"Outlier detection Using k-Nearest Neighbour Graph"*, In Proceedings of the 17th International Conference on Pattern Recognition Los Alamitos, CA, USA, 2004, pp. 430–433.

[Heady, 1990] R. Heady, G. Luger, A. Maccabe, and M. Servilla, *"The Architecture of a Network Level Intrusion Detection System"*, Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 1990.

[ISS, 2007] Internet Security Systems, *"IBM RealSecure Server Sensor"*, Last Check August 2007, Available from <http://www.iss.net/products/RealSecure_ServerSensor/product_main_page.html>.

[Landwehr, 1994] C.E. Landwehr, A.R. Bull, J.P. McDermott, W.S. Choi, *"A Taxonomy of Computer Program Security Flaws"*, ACM Computing Surveys 26 (3). (September 1994), pp. 211–254.

[Lee, 1999] W. Lee, S.J. Stolfo, K.W. Mok, *"A Data Mining Framework for Building Intrusion Detection Models"*, In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, 1999, pp. 120–132.

[Li, 2001] H. Li, L. Chang and X. Wang, *"A Useful Intrusion Detection System Prototype to Monitor Multi-processes Based on System Calls"*, Lecture Notes In Computer Science; Vol. 2229, Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001), pp. 441-450.

[Li, 2004] W. Li, *"Using Genetic Algorithm for Network Intrusion Detection"*, C.S.G. Department of Energy, 2004, pp. 1–8.

[Patcha, 2007] A. Patcha, J.-M. Park,*"An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends"*, Computer Networks 51 (2007), pp. 3448-3470.

[Pillai, 2004] M.M. Pillai, J.H.P. Eloff, H.S. Venter, *"An Approach to Implement a Network Intrusion Detection System Using Genetic Algorithms"*, In Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, Stellenbosch, Western Cape, South Africa, 2004, pp. 221–228.

[Porras, 1992] P. Porras, R. Kemmerer, *"Penetration State Transition Analysis – a Rule-Based Intrusion Detection Approach"*, In Proceedings of 8th Annual Computer Security Applications Conf., November 1992, pp. 220–229.

[Portnoy, 2001] L. Portnoy, E. Eskin, S.J. Stolfo, *"Intrusion Detection with Unlabeled Data Using Clustering"*, In Proceedings of the ACM Workshop on Data Mining Applied to Security, Philadelphia, PA, 2001.

[Quinlan, 1993] J.R. Quinlan, *"C4.5: Programs for Machine Learning"*, Morgan Kaufman, Los Altos, CA, 1993.

[Ramadas, 2003] M. Ramadas, S.O.B. Tjaden, *"Detecting Anomalous Network Traffic with Self-Organizing Maps"*, In Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, USA, 2003, pp. 36–54.

[Smaha, 1988] S.E. Smaha, *"Haystack: An Intrusion Detection System"*, In Proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, 1988, pp. 37–44.

[Shyu, 2003] M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, L. Chang, *"A Novel Anomaly Detection Scheme Based on Principal Component Classifier"*, In Proceedings of the IEEE Foundations and New Directions of Data Mining Workshop, Melbourne, FL, USA, 2003, pp. 172–179.

[Stallings, 1999] W. Stallings, *"Cryptography and Network Security, Principles and Practice"*, Second Edition, Prentice Hall, Inc., New Jersey, 1999.

[Staniford, 2002] S. Staniford, J.A. Hoagland, J.M. McAlerney, *"Practical Automated Detection of Stealthy Portscans"*, Journal of Computer Security 10 (2002) 105–136.

[Ye, 2000] N. Ye, M. Xu, S.M. Emran, *"Probabilistic Networks with Undirected Links for Anomaly Detection"*, In Proceedings of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop, West Point, NY, 2000.

[Ye, 2002] N. Ye, S.M. Emran, Q. Chen, S. Vilbert, *"Multivariate Statistical Analysis of Audit Trails for Host-based Intrusion Detection"*, IEEE Transactions on Computers 51 (2002) pp. 810–820.

[Yeung, 2003] D.-Y. Yeung, Y. Ding, *"Host-based Intrusion Detection Using Dynamic and Static Behavioral Models"*, Pattern Recognition 36 (2003), pp. 229–243.

Κεφάλαιο 2ο
Επιθέσεις Άρνησης Εξυπηρέτησης

1. Εισαγωγή

Η ανάπτυξη των υπολογιστικών και τεχνολογικών επικοινωνιών καθημερινά πλήττεται από ένα πλήθος απειλών που εμποδίζουν την ομαλή λειτουργία τους. Η διαθεσιμότητα είναι απαραίτητη προκειμένου τα υπολογιστικά συστήματα να λειτουργούν κανονικά χωρίς απώλεια πόρων για τους νόμιμους χρήστες τους. Ένα από τα πιο προκλητικά θέματα όσον αφορά στη διαθεσιμότητα είναι οι επιθέσεις *Άρνησης Εξυπηρέτησης (Denial of Service (DoS))*. Πριν αναζητήσουμε νέους αποτελεσματικούς τρόπους αντιμετώπισης των επιθέσεων αυτών, κρίνεται απαραίτητο να κατανοήσουμε σε βάθος και να αποκτήσουμε μία βάση γνώσης για το ίδιο το πρόβλημα των επιθέσεων, τον τρόπο λειτουργίας τους και των αδυναμιών που εκμεταλλεύονται. Ιδιαίτερα σημαντικό είναι να αναλύσουμε τους υπάρχοντες μηχανισμούς αντιμετώπισης. Με αυτό τον τρόπο κατανοούμε πλήρως το πρόβλημα και μπορούμε να σχεδιάσουμε πιο αποτελεσματικούς μηχανισμούς αντιμετώπισής τους.

Οι επιθέσεις *DoS* αποτελούν μία από τις κύριες απειλές και μεταξύ των δυσκολότερων προβλημάτων ασφάλειας στο σημερινό Διαδίκτυο και η επίδρασή τους καταδεικνύεται στη βιβλιογραφία που αφορά τα δίκτυα υπολογιστών. Ο κύριος στόχος των επιθέσεων *DoS* είναι η διακοπή των υπηρεσιών προσπαθώντας

να περιορίσουν την πρόσβαση σε μία μηχανή ή σε μία υπηρεσία αντί να υπονομεύσουν την ίδια την υπηρεσία. Αυτό το είδος επίθεσης προσπαθεί να θέσει ένα δίκτυο ανίκανο να παρέχει κανονική υπηρεσία στοχεύοντας είτε στο εύρος ζώνης είτε στη συνδεσιμότητα του δικτύου. Οι επιθέσεις αυτού του τύπου επιτυγχάνουν το στόχο τους στέλνοντας μία μεγάλη ροή πακέτων που πλημμυρίζει το δίκτυο του θύματος ή εκμεταλλεύονται όλη τη διαθέσιμη χωρητικότητα με αποτέλεσμα να αρνείται την πρόσβαση στους νόμιμους πελάτες. Στο όχι και τόσο μακρινό παρελθόν, κάποιες επιθέσεις μεγάλης κλίμακας είχαν ως στόχο δικτυακούς τόπους υψηλού προφίλ ([CERT, 1997], [CSI/FBI, 2001], [Moore, 2001]).

Ιδιαίτερη ανησυχία προκαλούν οι *Κατανεμημένες επιθέσεις Άρνησης Εξυπηρέτησης (Distributed Denial of Service Attacks (DDoS))*, των οποίων η επίδραση μπορεί να είναι αναλογικά πιο σοβαρή. Χωρίς καμία ή με μικρή προειδοποίηση, μία επίθεση DDoS μπορεί εύκολα να εξαντλήσει τους υπολογιστικούς και επικοινωνιακούς πόρους του θύματός της μέσα σε σύντομο χρονικό διάστημα. Λόγω της σοβαρότητας του προβλήματος έχουν προταθεί πολλοί μηχανισμοί προκειμένου να αντιμετωπισθούν αυτές οι επιθέσεις.

Οι επιθέσεις *DDoS*, είναι μία σχετικά απλή, αλλά πάρα πολύ δυναμική τεχνική ενάντια των πόρων του Διαδικτύου. Οι επιθέσεις DDoS προσθέτουν τη διάσταση πολλά-προς-ένα στο πρόβλημα των επιθέσεων DoS κάνοντας πιο δύσκολη την παρεμπόδιση και τον μετριασμό των επιθέσεων αυτών, αναλογικά πιο οδυνηρή την επίδρασή τους. Οι επιθέσεις DDoS εκμεταλλεύονται τις έμφυτες αδυναμίες της αρχιτεκτονικής του Διαδικτύου, και συγκεκριμένα το μοντέλο ανοιχτής πρόσβασης στο Διαδίκτυο, το οποίο συμβαίνει να είναι και ένα από τα μεγαλύτερα πλεονεκτήματά του.

Οι επιθέσεις DDoS δημιουργούν ροές πακέτων που προέρχονται από διάφορες πηγές. Αυτές οι επιθέσεις δεσμεύουν τις δυνάμεις ενός τεράστιου αριθμού συντονισμένων κόμβων του Διαδικτύου προκειμένου να καταναλώσουν κρίσιμους πόρους στο θύμα και να προκαλέσουν άρνηση εξυπηρέτησης στους νόμιμους πελάτες. Η δικτυακή κίνηση είναι συνήθως στις περιπτώσεις αυτές άθροισμα πολλών ροών με αποτέλεσμα να είναι αδύνατο να διακρίνουμε τα νόμιμα πακέτα από τα πακέτα επίθεσης. Ακόμα πιο σημαντικό είναι το γεγονός ότι το μέγεθος της επίθεσης μπορεί να είναι μεγαλύτερο από το μέγεθος που μπορεί να χειριστεί το σύστημα. Αν δεν αντιμετωπιστεί με σοβαρότητα η επίθεση ένα θύμα επίθεσης DDoS μπορεί να υποφέρει από ζημιές που ποικίλουν από το κλείσιμο του συστήματος και την αλλοίωση των αρχείων, μέχρι την ολική ή τη μερική απώλεια υπηρεσιών.

Δεν υπάρχουν προφανή χαρακτηριστικά των ροών των πακέτων DDoS που θα μπορούσαν άμεσα και γενικά να χρησιμοποιηθούν για την ανίχνευση και το φιλτράρισμά τους. Οι επιθέσεις DDoS επιτυγχάνουν το επιθυμητό αποτέλεσμα στέλνοντας ένα μεγάλο ποσοστό δικτυακής κυκλοφορίας, και τροποποιώντας

συγκεκριμένα πεδία των πακέτων προκειμένου να αποφύγουν τον χαρακτηρισμό τους και την ανίχνευσή τους. Ιδιαίτερα πολύπλοκα, "φιλικά-προς–το-χρήστη" και ισχυρά εργαλεία DDoS είναι διαθέσιμα στους πιθανούς επιτιθέμενους, αυξάνοντας τον κίνδυνο να πραγματοποιηθεί μία επίθεση DoS ή DDoS, αφού πολύ σημαντικά συστήματα δεν είναι κατάλληλα προετοιμασμένα προκειμένου να προστατέψουν τον εαυτό τους. Τα προγράμματα επίθεσης DDoS έχουν πολύ απλή λογική δομή και μικρό μέγεθος μνήμης με αποτέλεσμα να είναι σχετικά εύκολο να υλοποιηθούν και να κρυφτούν. Οι επιτιθέμενοι συνεχώς αλλάζουν τα εργαλεία τους προκειμένου να ξεπεράσουν τα συστήματα ασφάλειας που αναπτύσσονται από τους διαχειριστές συστημάτων και τους ερευνητές, οι οποίοι είναι σε συνεχή εγρήγορση προκειμένου να τροποποιήσουν τις προσεγγίσεις τους και να αντιμετωπίσουν νέες επιθέσεις.

Το πεδίο των επιθέσεων DDoS εξελίσσεται γρήγορα, με αποτέλεσμα να γίνεται ιδιαίτερα δύσκολο να συλλάβουμε μία καθολική εικόνα του προβλήματος. Αν και δεν υπάρχει μία λύση-πανάκεια για όλα τα είδη των επιθέσεων DDoS, υπάρχουν διάφορα μέτρα αντιμετώπισης που στόχο έχουν, να κάνουν πιο δύσκολη την πραγματοποίηση μίας επίθεσης.

Σε αυτό το κεφάλαιο παρουσιάζουμε μία πλήρη επισκόπηση της υπάρχουσας γνώσης στο πεδίο των επιθέσεων DoS μέσω μίας παρουσίασης διάφορων τύπων επιθέσεων DoS/DDoS και μηχανισμών που μπορεί να χρησιμοποιηθούν προκειμένου να αντιμετωπιστούν αυτές οι επιθέσεις. Η κατηγοριοποίηση των επιθέσεων περιλαμβάνει τόσο γνωστούς όσο και πιθανούς μηχανισμούς επίθεσης. Σε κάθε κατηγορία επίθεσης ορίζουμε ειδικά και σημαντικά στοιχεία και χαρακτηριστικά. Επιπλέον, περιγράφονται σημαντικά χαρακτηριστικά κάθε επίθεσης και κατηγορίας μηχανισμών προστασίας περιγράφονται καθώς επίσης αναλύονται και τα πλεονεκτήματα και μειονεκτήματα κάθε προτεινόμενου σχήματος.

Ακολουθώντας αυτή την εισαγωγή, αυτό το κεφάλαιο οργανώνεται ως εξής. Η δεύτερη ενότητα ερευνά το πρόβλημα των επιθέσεων DoS και στη συνέχεια παρουσιάζει μία κατηγοριοποίηση των επιθέσεων DoS. Η τρίτη ενότητα εισάγει το πρόβλημα των επιθέσεων DDoS και δίνει τα βασικά χαρακτηριστικά γνωστών εργαλείων DDoS και παρουσιάζει μία ταξινόμηση των επιθέσεων DDoS. Η τέταρτη ενότητα παρουσιάζει τα προβλήματα αντιμετώπισης των επιθέσεων DDoS και προτείνει μία κατηγοριοποίηση των μηχανισμών αντιμετώπισής τους, ενώ η πέμπτη ενότητα ολοκληρώνει το κεφάλαιο.

2. Επιθέσεις Άρνησης Εξυπηρέτησης

2.1 Ορίζοντας της Επιθέσεις Άρνησης Εξυπηρέτησης

Σύμφωνα με το World Wide Web Security FAQ [Stein, 2002] μία επίθεση DoS μπορεί να περιγραφεί σαν μία επίθεση που σχεδιάστηκε για να καταστήσει έναν υπολογιστή ή ένα δίκτυο ανίκανο να παρέχει τις "φυσιολογικές" (κανονικές) του

υπηρεσίες. Μία επίθεση DoS θεωρείται ότι πραγματοποιείται μόνο όταν η πρόσβαση σε ένα υπολογιστή ή σε έναν πόρο δικτύου σκοπίμως παρεμποδίζεται ή μειώνεται σαν αποτέλεσμα κακόβουλης πράξης που πραγματοποιείται από κάποιον άλλο χρήστη. Αυτές οι επιθέσεις δεν φθείρουν απαραίτητα δεδομένα, άμεσα ή μόνιμα, αλλά σκοπίμως διακινδυνεύουν τη διαθεσιμότητα των πόρων.

Οι πιο συνηθισμένες επιθέσεις DoS στόχο έχουν το εύρος ζώνης ή τη συνδεσιμότητα ενός δικτύου υπολογιστών. Οι επιθέσεις που στόχο έχουν το εύρος ζώνης πλημμυρίζουν το δίκτυο με τεράστιο κυκλοφοριακό όγκο με αποτέλεσμα όλοι οι διαθέσιμοι πόροι δικτύου να καταναλώνονται ώστε να μην μπορούν να εξυπηρετηθούν οι νόμιμες αιτήσεις χρηστών, οδηγώντας το δίκτυο και το σύστημα σε αισθητά μειωμένη παραγωγικότητα. Οι επιθέσεις που στοχεύουν στη συνδεσιμότητα πλημμυρίζουν έναν υπολογιστή με τόσο πολλές αιτήσεις σύνδεσης, ώστε όλοι οι πόροι του λειτουργικού συστήματος να καταναλώνονται και ο υπολογιστής να μην μπορεί πια να επεξεργαστεί τις νόμιμες αιτήσεις χρηστών.

2.2 Κατηγοριοποίηση Επιθέσεων Άρνησης Εξυπηρέτησης

Οι επιθέσεις DoS μπορούν να κατηγοριοποιηθούν σε πέντε κατηγορίες με βάση το επίπεδο του πρωτοκόλλου στο οποίο πραγματοποιείται η επίθεση, όπως απεικονίζεται στο Σχήμα 2.1 [Karig, 2001].

Σχήμα 2. 1 Κατηγοριοποίηση Επιθέσεων Άρνησης Εξυπηρέτησης

Οι επιθέσεις *Άρνησης Εξυπηρέτησης (DoS)* στο *Επίπεδο Δικτυακής Συσκευής (Network Device Level)* περιλαμβάνουν επιθέσεις που μπορεί να προκληθούν είτε αν ο επιτιθέμενος εκμεταλλευτεί λάθη ή αδυναμίες στο λογισμικό, είτε αν προσπαθήσει να εξαντλήσει τους υλικούς πόρους των δικτυακών συσκευών. Ένα παράδειγμα μίας αδυναμίας συσκευών δικτύου είναι αυτό που προκαλείται από ένα σφάλμα υπερχείλισης μνήμης στη διαδικασία ελέγχου των συνθηματικών. Εκμεταλλευόμενοι τέτοιου είδους αδυναμίες συγκεκριμένοι δρομολογητές Cisco 7xx [CIAC, 1997a] μπορούν να διακόψουν την λειτουργία τους αν ο επιτιθέμενος

συνδεθεί με τους δρομολογητές μέσω telnet και εισάγει ιδιαίτερα μεγάλα συνθηματικά.

Στο *επίπεδο Λειτουργικού Συστήματος (OS level)* οι επιθέσεις DoS εκμεταλλεύονται τους τρόπους με τους οποίους τα λειτουργικά συστήματα υλοποιούν τα διάφορα πρωτόκολλα. Ένα παράδειγμα αυτής της κατηγορίας επιθέσεων DoS είναι η επίθεση Ping of Death [Kenney, 1997]. Σε αυτή την επίθεση, στέλνονται στο θύμα στόχο αιτήσεις ηχούς ICMP που έχουν συνολικό μέγεθος δεδομένων μεγαλύτερο από το μέγιστο μέγεθος με βάση το πρότυπο IP. Όταν στέλνονται τέτοιου είδους πακέτα τμηματοποιούνται και στη συνέχεια επανενώνονται στον προορισμό. Πολλά λειτουργικά συστήματα όμως αποτυγχάνουν να δεσμεύσουν αρκετή μνήμη για τα υπερμεγέθη επανενωμένα πακέτα ICMP με αποτέλεσμα την υπερχείλιση της προσωρινής μνήμης.

Οι *επιθέσεις στο επίπεδο εφαρμογής (application-based attacks)* προσπαθούν να θέσουν μία μηχανή ή μία υπηρεσία εκτός λειτουργίας είτε εκμεταλλευόμενοι συγκεκριμένα λάθη στις εφαρμογές δικτύων που "τρέχουν" στον κόμβο στόχο, είτε χρησιμοποιώντας τέτοιες εφαρμογές προκειμένου να εξαντλήσουν τους πόρους του θύματός τους. Είναι επίσης πιθανό ο επιτιθέμενος να βρει σημεία υψηλής αλγοριθμικής πολυπλοκότητας και να τα εκμεταλλευτεί προκειμένου να καταναλώσει όλους τους διαθέσιμους πόρους σε έναν απομακρυσμένο κόμβο. Ένα παράδειγμα επίθεσης που βασίζεται στο επίπεδο εφαρμογής είναι η επίθεση finger bomb [Xforce, 2006]. Ένας κακόβουλος χρήστης μπορεί να προκαλέσει την επαναλαμβανόμενη εκτέλεση της ρουτίνας finger στον κόμβο-θύμα, οδηγώντας πιθανότατα στην εξάντληση των πόρων των δικτύων.

Στις επιθέσεις *πλημμύρας δεδομένων (data flooding)*, ο επιτιθέμενος προσπαθεί να χρησιμοποιήσει το διαθέσιμο εύρος ζώνης σε έναν κόμβο ή συσκευή δικτύου στο μεγαλύτερο δυνατό βαθμό, στέλνοντας μαζικές ποσότητες δεδομένων και προκαλώντας την επεξεργασία ιδιαίτερα μεγάλων ποσοτήτων δεδομένων.

Οι *επιθέσεις DoS που βασίζονται σε χαρακτηριστικά πρωτοκόλλων* εκμεταλλεύονται συγκεκριμένα χαρακτηριστικά των πρωτοκόλλων. Για παράδειγμα διάφορες επιθέσεις εκμεταλλεύονται το γεγονός ότι μπορεί να παραποιηθούν οι διευθύνσεις πηγής IP. Διάφορα είδη επιθέσεων DoS έχουν επικεντρωθεί στην υπηρεσία διάθεσης ονομάτων και διευθύνσεων που χρησιμοποιούνται στο Διαδίκτυο (Domain Name Service (DNS)). Πολλές από αυτές περιλαμβάνουν την επίθεση στη γρήγορη μνήμη των εξυπηρετητών ονομάτων. Ένα πρόβλημα που υπάρχει σε πολλές υλοποιήσεις των DNS, είναι ότι δεν ελέγχεται η ορθότητα των απαντήσεων που λαμβάνουν σε αιτήσεις. Ένας παραβιασμένος εξυπηρετητής ονομάτων μπορεί να ανταποκριθεί σε μία αίτηση με ψευδείς πληροφορίες, οι οποίες μπορούν να αποθηκευτούν στον εξυπηρετητή ονομάτων που λαμβάνει την απάντηση της αίτησης. Ένας επιτιθέμενος που έχει παραβιάσει έναν εξυπηρετητή ονομάτων μπορεί να αναγκάσει ένα θύμα να αποθηκεύει λανθασμένες εγγραφές ρωτώντας το θύμα για το δικτυακό τόπο του ίδιου του

επιτιθέμενου. Αυτό θα έχει σαν αποτέλεσμα ένα ευπαθές θύμα εξυπηρετητή ονομάτων να αναφέρεται στον απατεώνα εξυπηρετητή και θα αποθηκεύει την απάντηση, η οποία πιθανότατα θα είναι πλαστή [Davidowicz, 1999].

2.3 Κίνητρα των Επιθέσεων DoS και Προβλήματα Αντιμετώπισής τους

Υπάρχουν πολλά κίνητρα για την πραγματοποίηση επιθέσεων DoS. Συγκεκριμένα άτομα συχνά εκκινούν επιθέσεις DoS προκειμένου να τραβήξουν την προσοχή και να γίνουν δημοφιλής. Άλλες επιθέσεις έχουν πολιτικά κίνητρα. Ιστοσελίδες που ανήκουν σε επίμαχες οντότητες συχνά έγιναν στόχοι επιθέσεων άρνησης εξυπηρέτησης. Προσωπικοί λόγοι είναι ένα άλλο κίνητρο για τις επιθέσεις DoS. Άλλα άτομα μπορεί να πραγματοποιήσουν επιθέσεις με σκοπό να προκληθεί κάποια ταπείνωση ή απλά σαν αστείο. Αυτές οι επιθέσεις γενικά δεν είναι πολύ ισχυρές και συνήθως δεν διαρκούν πολύ. Οι επιθέσεις DoS έχουν κάποια χαρακτηριστικά που κάνουν ακόμα πιο δύσκολη την αντιμετώπισή τους. Για αυτό το λόγο, στη συνέχεια παρουσιάζουμε κάποια θέματα που εξηγούν γιατί η προστασία από τις επιθέσεις DoS είναι πολύ δύσκολη.

Η ασφάλεια του Διαδικτύου είναι αλληλεξαρτώμενη [Zaroo, 2002]: Το Διαδίκτυο έχει λίγους ενσωματωμένους μηχανισμούς προστασίας προκειμένου να αντιμετωπιστούν οι επιθέσεις DoS. Ο σχεδιασμός τους δημιουργεί κενά ασφάλειας τα οποία μπορεί να εκμεταλλευτούν οι επιτιθέμενοι. Είναι σημαντικό να σημειώσουμε ότι ανεξάρτητα από το πόσο ασφαλής είναι ένας κόμβος, είναι πάντα υπό απειλή αφού το υπόλοιπο Διαδίκτυο δεν είναι ασφαλές [CERT, 2001a].

Οι επιθέσεις DoS είναι από τη φύση τους δύσκολο να ανιχνευθούν [Xuan, 2001]: Η ανίχνευση της πηγής των επιθέσεων DoS είναι αρκετά δύσκολη. Εκμεταλλευόμενοι την ασταθή φύση του Διαδικτύου, οι επιτιθέμενοι χρησιμοποιούν παραποιημένες διευθύνσεις πηγής IP προκειμένου να κρύψουν την ταυτότητά τους πίσω από άλλες μηχανές που έχουν θέσει υπό τον έλεγχο τους. Επιπλέον, οι ροές των πακέτων DoS δεν παρουσιάζουν κοινά χαρακτηριστικά, με αποτέλεσμα να καθιστούν ιδιαίτερα δύσκολη την ανίχνευση τους [Xuan, 2001] και ακόμα πιο δύσκολη τη διαφοροποίηση των πακέτων επίθεσης από τα νόμιμα πακέτα [Zaroo, 2002].

Περιορισμένοι πόροι [Xuan, 2001]: Ο υψηλός ρυθμός πακέτων ο οποίος χρειάζεται για να δημιουργηθούν μαζικές επιθέσεις DoS απαιτεί μεγάλο αριθμό πόρων. Τα συστήματα και τα δίκτυα που αποτελούν το Διαδίκτυο έχουν περιορισμένους πόρους οι οποίοι μπορεί εύκολα να εξαντληθούν κατά τη διάρκεια της ανίχνευσης των επιθέσεων.

Αυτοματοποιημένα εργαλεία: Τα εργαλεία DoS τα οποία είναι διαθέσιμα στο Διαδίκτυο συνοδεύονται από οδηγίες οι οποίες επιτρέπουν την εύκολη και αποτελεσματική χρήση τους ακόμα και από όχι τεχνικά καταρτισμένους χρήστες. Οι επιτιθέμενοι συνεχώς προσπαθούν να αναπτύξουν πιο αποτελεσματικά

εργαλεία προκειμένου να ξεπεράσουν τα συστήματα ασφαλείας που αναπτύσσονται από τους ερευνητές.

Ένα περιβάλλον γεμάτο στόχους [Zaroo, 2002]: Υπάρχει ένας μεγάλος αριθμός κόμβων και δικτύων στο Διαδίκτυο που είναι ευπαθή, τα οποία μπορεί να τα εκμεταλλευτούν και τα οποία παρέχουν γόνιμο έδαφος προκειμένου να πραγματοποιηθούν επιθέσεις DoS. Υπάρχουν επίσης πολλοί χρήστες του Διαδικτύου οι οποίοι δεν έχουν την απαιτούμενη τεχνική κατάρτιση προκειμένου να προστατέψουν τα συστήματά τους από επιθέσεις DoS. Επιπλέον, ο σχεδιασμός ενός αποτελεσματικού συστήματος αμύνης απέναντι στις επιθέσεις DoS αντιμετωπίζει πολλές προκλήσεις, γιατί οι απαιτήσεις για μία αποτελεσματική απόκριση στις επιθέσεις DoS είναι πολλαπλές [Criscuolo, 2000]:

- Ένα από τα κύρια χαρακτηριστικά των συστημάτων προστασίας απέναντι στις επιθέσεις DoS είναι η υψηλή ασφάλεια. Πρέπει να επιβεβαιωθεί ότι το σύστημα προστασίας δεν μπορεί να χρησιμοποιηθεί σαν θύμα μίας επίθεσης DoS.
- Ένα σύστημα προστασίας απέναντι στις επιθέσεις DoS πρέπει να είναι αξιόπιστο στην ανίχνευση επιθέσεων DoS και να μην εμφανίζει λανθασμένους θετικούς συναγερμούς. Αυτό μπορεί να έχει σαν αποτέλεσμα υψηλό κόστος, επομένως ίσως θα ήταν καλύτερο να υπάρχει μεγάλη αυστηρότητα ως προς αυτή την απαίτηση.
- Ένα σύστημα προστασίας απέναντι στις επιθέσεις DoS πρέπει να είναι αποτελεσματικό στην ανίχνευση και την απόκριση σε μία επίθεση DoS προκειμένου να περιορίσει την αποτελεσματικότητα της επίθεσης.
- Ένας μηχανισμός προστασίας από επιθέσεις DoS πρέπει να είναι ρεαλιστικός στο σχεδιασμό του και να μπορεί να εφαρμοστεί στις υπάρχουσες υποδομές ασφάλειας, χωρίς να απαιτεί σημαντικές αλλαγές στην υποδομή του Διαδικτύου.
- Ένας μηχανισμός προστασίας από επιθέσεις DoS δεν πρέπει να απαιτεί πολλούς πόρους και πρέπει να έχει μειωμένο κόστος απόδοσης, προκειμένου να αποφύγει τη μείωση της απόδοσης του δικτύου το οποίο δέχεται την επίθεση.

3. Κατανεμημένες Επιθέσεις Άρνησης Εξυπηρέτησης

3.1 Ορίζοντας τις Επιθέσεις DDoS

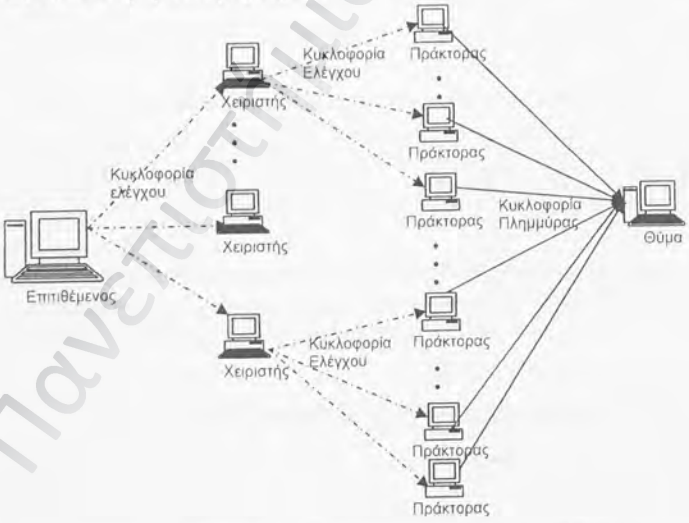
Σύμφωνα με το WWW Security FAQ [Stein, 2002] "Μία κατανεμημένη επίθεση *Άρνησης Εξυπηρέτησης (DDoS)* χρησιμοποιεί πολλούς υπολογιστές για να πραγματοποιήσει μία κατευθυνόμενη επίθεση *Άρνησης Εξυπηρέτησης (DoS)* ενάντια ενός ή περισσότερων στόχων. Χρησιμοποιώντας την τεχνολογία πελάτη/εξυπηρετητή, ο επιτιθέμενος μπορεί να πολλαπλασιάσει σημαντικά την

αποτελεσματικότητα της επίθεσης DoS θέτοντας υπό τον έλεγχό του, τους πόρους πολλαπλών ακούσιων συνεργών υπολογιστών, οι οποίοι χρησιμοποιούνται σαν πλατφόρμες επίθεσης". Η επίθεση DDoS είναι η πιο εξελιγμένη μορφή των επιθέσεων DoS. Διαχωρίζεται από τις άλλες επιθέσεις, από την ικανότητά της να αναπτύσσει τα όπλα της με ένα κατανεμημένο τρόπο στο Διαδίκτυο και να αθροίζει αυτές τις δυνάμεις ώστε να δημιουργηθεί πολύ επικίνδυνη κυκλοφορία. Οι επιθέσεις DDoS ποτέ δεν προσπαθούν να μπουν στο σύστημα του θύματος, καθιστώντας κατά αυτό τον τρόπο κάθε παραδοσιακό μηχανισμό προστασίας ασφάλειας μη αποτελεσματικό. Ο κύριος στόχος μίας επίθεσης DDoS είναι να προκαλέσει ζημιά στο θύμα είτε για προσωπικούς λόγους, είτε για υλικό κέρδος είτε για δημοτικότητα.

3.2 Στρατηγική Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης

Μία επίθεση DDoS αποτελείται από τέσσερα στοιχεία όπως φαίνεται και στο Σχήμα 2.2.

1. Τον επιτιθέμενο.
2. Τους χειριστές (handlers) ή επιτελείς (masters) κόμβους, οι οποίοι είναι κόμβοι που έχουν παραβιαστεί από τον επιτιθέμενο και "τρέχει" ένα ειδικό πρόγραμμα σε αυτούς, δίνοντάς τους τη δυνατότητα να ελέγχουν πολλαπλούς πράκτορες (agents).



Σχήμα 2. 2 Αρχιτεκτονική των Επιθέσεων DDoS

3. Τους επιτιθέμενους πράκτορες (daemon agents ή κόμβους zombie), οι οποίοι είναι παραβιασμένοι κόμβοι, στους οποίους τρέχει ένα ειδικό πρόγραμμα και

οι κόμβοι αυτοί είναι υπεύθυνοι για την παραγωγή μίας ροής πακέτων προς το μελλοντικό θύμα. Αυτές οι μηχανές είναι συνήθως έξω από το δίκτυο του θύματος, προκειμένου να αποφεύγουν αποτελεσματική απόκριση από το θύμα, και εξωτερικές από το δίκτυο του επιτιθέμενου, προκειμένου να αποφεύγεται η ευθύνη εάν γίνει προσπάθεια εύρεσης της πηγής της επίθεσης.

4. Ένα θύμα ή κόμβο-στόχο.

Καθώς ετοιμάζεται και πραγματοποιείται μία επίθεση DDoS πραγματοποιούνται τα ακόλουθα βήματα:

1. *Επιλογή των πρακτόρων.* Ο επιτιθέμενος επιλέγει τους πράκτορες που θα πραγματοποιήσουν την επίθεση. Αυτές οι μηχανές πρέπει να έχουν κάποιες αδυναμίες ή ευπάθειες που ο επιτιθέμενος εκμεταλλεύεται προκειμένου να αποκτήσει πρόσβαση σε αυτές. Επιπλέον πρέπει να έχουν πλούσιους πόρους έτσι ώστε να είναι ικανοί να παράγουν ισχυρές ροές πακέτων επίθεσης. Στην αρχή αυτή η διαδικασία πραγματοποιούνταν χειρωνακτικά, αλλά σύντομα αυτοματοποιήθηκε με ειδικά εργαλεία σάρωσης.
2. *Παραβίαση.* Ο επιτιθέμενος εκμεταλλεύεται τις "τρύπες" ασφαλείας και τις υπάρχουσες αδυναμίες των μηχανών-πρακτόρων και εγκαθιστά εκεί τον κώδικα επίθεσης. Επιπλέον, προσπαθεί να προστατέψει τον κώδικα από αποκάλυψη και απενεργοποίηση. Εργαλεία αυτο-αναπαραγωγής όπως το σκουλήκι Ramen [CIAC, 2001] και το Code Red [CERT, 2001b] σύντομα αυτοματοποίησαν αυτή τη φάση. Οι ιδιοκτήτες και χρήστες των συστημάτων πρακτόρων τυπικά δεν έχουν γνώση ότι το σύστημά τους έχει καταληφθεί και ότι θα συμμετάσχουν σε μία επίθεση DDoS. Όταν συμμετέχουν σε μία επίθεση DDoS, κάθε πρόγραμμα πράκτορα χρησιμοποιεί μόνο ένα μικρό τμήμα πόρων (τόσο στη μνήμη όσο και στο εύρος ζώνης), με αποτέλεσμα οι χρήστες των υπολογιστών-χειριστών να παρατηρούν μικρή αλλαγή στην απόδοση των συστημάτων τους.
3. *Επικοινωνία.* Ο επιτιθέμενος επικοινωνεί με όλους τους χειριστές-κόμβους προκειμένου να αναγνωρίσει ποιοι πράκτορες μπορεί να χρησιμοποιηθούν σε μία επίθεση, εάν είναι απαραίτητο να πραγματοποιήσει αναβάθμιση στους πράκτορες και πότε είναι η κατάλληλη στιγμή να πραγματοποιήσει την επίθεση. Οι πράκτορες μπορούν να επικοινωνούν με έναν ή πολλούς χειριστές-κόμβους ανάλογα με τη διαμόρφωση του δικτύου επίθεσης DDoS. Τα πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία ανάμεσα στους χειριστές και τους πράκτορες είναι τα TCP, UDP ή ICMP.
4. *Επίθεση.* Σε αυτό το βήμα ο επιτιθέμενος διατάσσει την εκκίνηση της επίθεσης. Το θύμα, η διάρκεια της επίθεσης καθώς και ειδικά χαρακτηριστικά της επίθεσης όπως ο τύπος, το μήκος, το πεδίο TTL (Time To Live), οι αριθμοί των θυρών κ.τ.λ., μπορεί να ρυθμιστούν. Η ποικιλία αυτή των ιδιοτήτων των πακέτων επίθεσης μπορεί να είναι ευεργετική για τον επιτιθέμενο, ώστε να καταφέρει να αποφύγει την ανίχνευση.

Η τελευταία γενιά των επιθέσεων DDoS δεν αναμένει την εκκίνηση της επίθεσης από τον επιτιθέμενο αλλά παρακολουθεί μία δημόσια τοποθεσία του Διαδικτύου. Για παράδειγμα, ένα δωμάτιο συζητήσεων (chat room) μπορεί να παρακολουθείται και η επίθεση να ξεκινά αυτόματα όταν πληκτρολογείται μία συγκεκριμένη λέξη-κλειδί ή φράση. Με αυτόν τον τρόπο είναι ακόμα πιο δύσκολο να ανιχνευθεί ο επιτιθέμενος. Ακόμα πιο τρομακτικό είναι το γεγονός ότι σαν λέξη εκκίνησης της επίθεσης μπορεί να έχει τεθεί μία συχνά χρησιμοποιούμενη λέξη, και ο επιτιθέμενος δεν χρειάζεται να κάνει το παραμικρό προκειμένου να πραγματοποιηθεί η επίθεση.

Πρόσφατα τα πολυ-χρηστικά, απευθείας συνδεδεμένα συστήματα συνομιλίας που είναι γνωστά σαν κανάλια Internet Relay Chat (IRC), χρησιμοποιούνται για επικοινωνία μεταξύ του επιτιθέμενου και των πρακτόρων [Lo, 1998], καθώς τα κανάλια IRC επιτρέπουν στους χρήστες τους να δημιουργήσουν δημόσια και ιδιωτικά μυστικά κανάλια. Ένα δίκτυο επίθεσης DDoS το οποίο βασίζεται σε κανάλια IRC και ένα που βασίζεται στο μοντέλο πράκτορα-χειριστή έχουν πολλές ομοιότητες. Σύμφωνα με το [Lee, 2003] η ειδοποιός διαφορά ανάμεσα στα δύο δίκτυα επιθέσεων DDoS είναι ότι αντί να χρησιμοποιείται ένα πρόγραμμα χειριστή που είναι εγκατεστημένο σε έναν εξυπηρετητή δικτύου, ένας εξυπηρετητής καναλιών IRC ανιχνεύει τις διευθύνσεις των συνδεδεμένων πρακτόρων και χειριστών και διευκολύνει την επικοινωνία ανάμεσα τους. Το κύριο πλεονέκτημα των δικτύων επίθεσης που βασίζονται σε IRC σε σχέση με τα μοντέλα επίθεσης που βασίζονται σε πράκτορες - χειριστές είναι το γεγονός ότι αν και η αποκάλυψη ενός συμμετέχοντος μπορεί να οδηγήσει στην αποκάλυψη του καναλιού επικοινωνίας, προστατεύονται οι ταυτότητες των άλλων συμμετεχόντων. Επιπλέον, τα μοντέλα επιθέσεων DDoS που βασίζονται σε κανάλια IRC παρέχουν ανωνυμία κάνοντας ακόμα πιο δύσκολη την ανίχνευση των πρακτόρων και την πηγή της επίθεσης. Ένα άλλο πλεονέκτημα των μοντέλων των επιθέσεων DDoS που βασίζονται σε κανάλια IRC είναι ότι ο επιτιθέμενος δεν χρειάζεται πια να διατηρεί μία λίστα των πρακτόρων, καθώς μπορεί απλά να συνδέεται στον εξυπηρετητή IRC και να βλέπει μία λίστα όλων των διαθέσιμων πρακτόρων [Criscuolo, 2000]. Το λογισμικό των πρακτόρων που έχει εγκατασταθεί στο δίκτυο IRC συνήθως επικοινωνεί με το κανάλι IRC και ενημερώνει τον επιτιθέμενο όταν ο πράκτορας είναι σε λειτουργία.

3.3 Εργαλεία Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης

Υπάρχουν αρκετά γνωστά εργαλεία *Κατανεμημένων επιθέσεων Άρνησης Εξυπηρέτησης (DDoS)*. Η αρχιτεκτονική αυτών των εργαλείων είναι παρόμοια και πολλά από τα εργαλεία αυτά έχουν κατασκευαστεί μέσω μικρών τροποποιήσεων άλλων εργαλείων. Σε αυτή την ενότητα, παρουσιάζουμε τη λειτουργικότητα κάποιων από αυτά τα εργαλεία. Για λόγους παρουσίασης τα ορίζουμε σε αυτά που βασίζονται σε πράκτορες και σε αυτά που βασίζονται σε κανάλια IRC.

3.3.1 Εργαλεία που Βασίζονται σε Πράκτορες

Τα εργαλεία DDoS που βασίζονται σε πράκτορες λειτουργούν με βάση το μοντέλο επίθεσης DDoS πράκτορα – χειριστή το οποίο αποτελείται από χειριστές, πράκτορες και θύματα όπως έχει ήδη περιγραφεί στην ενότητα που αφορά την στρατηγική DDoS. Κάποια από τα πολύ γνωστά εργαλεία DDoS που βασίζονται σε πράκτορες είναι το *Trinoo*, το *TFN*, το *TFN2K*, το *Stacheldraht*, το *mstream* και το *Shaft*.

Το *Trinoo* ([Criscuolo, 2000], [Dittrich, 1999a]) είναι το πρώτο ευρέως διαδεδομένο εργαλείο επίθεσης DDoS. Είναι ένα εργαλείο που οδηγεί στην εξάντληση του εύρους ζώνης και μπορεί να χρησιμοποιηθεί για την πραγματοποίηση κατευθυνόμενων επιθέσεων πλημμύρας UDP ενάντια μίας ή περισσότερων διευθύνσεων IP. Η επίθεση χρησιμοποιεί σταθερού μεγέθους πακέτα UDP και στοχεύει σε τυχαίες θύρες στη μηχανή του θύματος. Νεώτερες εκδόσεις του *Trinoo* παρέχουν υποστήριξη σε παραποιημένες διευθύνσεις πηγής IP. Τυπικά, ο πράκτορας trinoo εγκαθίσταται σε ένα σύστημα το οποίο υποφέρει από την αδυναμία υπερφόρτωσης προσωρινής μνήμης (buffer overrun). Αυτό το "σφάλμα" στο λογισμικό επιτρέπει στον επιτιθέμενο να πραγματοποιήσει απομακρυσμένα την εγκατάσταση στον πράκτορα χρησιμοποιώντας το σύστημα προσωρινής μνήμης ενός δευτερεύοντος θύματος. Ο χειριστής χρησιμοποιεί UDP ή TCP για να επικοινωνήσει με τους πράκτορες με αυτό τον τρόπο τα συστήματα ανίχνευσης εισβολών μπορούν να ανιχνεύσουν τους χειριστές μόνο παρακολουθώντας την κυκλοφορία UDP. Αυτό το κανάλι μπορεί επίσης να είναι κρυπτογραφημένο και να προστατεύεται με συνθηματικά. Παρόλα αυτά, επί του παρόντος το συνθηματικό δεν στέλνεται σε κρυπτογραφημένη μορφή, επομένως μπορεί να ανιχνευθεί και να υποκλαπεί. Το *Trinoo* δεν δημιουργεί παραποιημένες διευθύνσεις πηγής αν και μπορεί εύκολα να επεκταθεί ώστε να χρησιμοποιήσει αυτή τη δυνατότητα. Οι επιτιθέμενοι πράκτορες του *Trinoo* υλοποιούν επιθέσεις πλημμύρας UDP ενάντια του στόχου-θύματος.

Το *Tribe Flood Network* (TFN) [Dittrich, 2000a], είναι ένα εργαλείο επίθεσης DDoS που παρέχει στον επιτιθέμενο την ικανότητα να πραγματοποιήσει τόσο επιθέσεις εξάντλησης εύρους ζώνης όσο και επιθέσεις εξάντλησης πόρων. Χρησιμοποιεί μία διεπαφή γραμμής εντολών προκειμένου να πραγματοποιήσει την επικοινωνία μεταξύ επιτιθέμενου και χειριστή αλλά δεν παρέχει κρυπτογράφηση μεταξύ πρακτόρων και χειριστών ή ανάμεσα στους χειριστές και τον επιτιθέμενο. Επιπλέον εκτός από την επίθεση πλημμύρας UDP που μπορεί να πραγματοποιήσει το Trinoo, το *TFN* μπορεί να πραγματοποιήσει πλημμύρες TCP SYN και ICMP καθώς επίσης και επιθέσεις Smurf. Στους χειριστές η πρόσβαση επιτυγχάνεται χρησιμοποιώντας πρότυπες συνδέσεις TCP όπως είναι το telnet ή το ssh (secure shell). Η επικοινωνία ανάμεσα στον χειριστή και τους πράκτορες ολοκληρώνεται με πακέτα ICMP ECHO REPLY, που είναι δυσκολότερο να ανιχνευθούν σε σχέση με τα πακέτα UDP και μπορούν συχνά να περάσουν συστήματα αντι-πύρινων ζωνών (firewalls). Το *TFN* πραγματοποιεί

κατευθυνόμενες επιθέσεις DoS που είναι ιδιαίτερα δύσκολο να αντιμετωπιστούν καθώς παράγουν πολλαπλούς τύπους επιθέσεων και μπορούν να παράγουν πακέτα με παραποιημένες διευθύνσεις πηγής IP καθώς επίσης αλλάζει με τυχαίο τρόπο τις θύρες στόχους. Είναι ικανό να πραγματοποιήσει παραποίηση είτε σε ένα είτε και στα 32 bit της διεύθυνσης πηγής IP ή μόνο στα τελευταία οκτώ. Μερικές από τις επιθέσεις που μπορούν να πραγματοποιηθούν από το *TFN* περιλαμβάνουν: την επίθεση Smurf, την πλημμύρα UDP, την πλημμύρα TCP SYN, την πλημμύρα αιτήσεων ηχούς ICMP και την κατευθυνόμενη ανοικτή εκπομπή ICMP.

Το *TFN2K* [Barlow, 2000] είναι ένα εργαλείο επίθεσης DDoS που βασίζεται στην αρχιτεκτονική TFN. Το *TFN2K* προσθέτει κρυπτογραφημένα μηνύματα στις επικοινωνίες ανάμεσα σε όλα τα συμμετέχοντα στοιχεία [CERT, 1999]. Η επικοινωνία ανάμεσα στον πραγματικό επιτιθέμενο και το πρόγραμμα διαχείρισης πραγματοποιείται χρησιμοποιώντας έναν αλγόριθμο που βασίζεται σε κλειδιά, τον CAST-256 [Adams, 1999]. Επιπλέον, το *TFN2K* πραγματοποιεί μυστικές λειτουργίες προκειμένου να μη γίνει αντιληπτό από τα συστήματα ανίχνευσης εισβολών. Οι επιτιθέμενοι πράκτορες του *TFN2K* πραγματοποιούν επιθέσεις πλημμύρας Smurf, SYN, UDP και ICMP και ο τύπος της επίθεσης μπορεί να ποικίλλει κατά τη διάρκεια της επίθεσης. Οι εντολές στέλνονται από τον χειριστή στον πράκτορα μέσω TCP, UDP, ICMP ή και τα τρία τυχαία, καθιστώντας ακόμα πιο δύσκολη την ανίχνευση του *TFN2K* παρακολουθώντας το δίκτυο.

Τα πακέτα εντολών μπορούν να διασκορπιστούν με οποιοδήποτε αριθμό πακέτων παγίδας και να σταλούν σε τυχαίες διευθύνσεις IP προκειμένου να αποφύγουν την ανίχνευση. Σε δίκτυα που εφαρμόζουν φιλτράρισμα εισόδου όπως περιγράφεται στο [Ferguson, 2000], το *TFN2K* μπορεί να παραποιήσει (forge) πακέτα που προέρχονται από γειτονικούς υπολογιστές. Η επικοινωνία ανάμεσα στους χειριστές και τους πράκτορες είναι κρυπτογραφημένη και κωδικοποιημένη με βάση το 64 (base-64 encoded). Υπάρχει μία επιπλέον μορφή επίθεσης που ονομάζεται TARGA. Η TARGA λειτουργεί στέλνοντας παραποιημένα πακέτα IP προκειμένου να καθυστερήσει ή να επιβαρύνει πολλές στοίβες TCP/IP δικτύων. Μία άλλη επιλογή είναι οι καλούμενες επιθέσεις MIX, οι οποίες ανακατεύουν πλημμύρες UDP, SYN και ICMP ECHO REPLY [Bellovin, 2000].

Το *Stacheldraht* [Dittrich, 1999b] (γερμανικός όρος για το "αγκαθωτό καλώδιο") βασίζεται σε νεώτερες εκδόσεις του TFN και προσπαθεί να περιορίσει μερικά από τα αδύναμα σημεία του. Συνδυάζει χαρακτηριστικά του Trinoo (αρχιτεκτονική χειριστή/πράκτορα) με αυτά του πρωτότυπου TFN. Επιπλέον, έχει την ικανότητα να πραγματοποιεί αυτόματα ενημερώσεις στους πράκτορες. Αυτό σημαίνει ότι ο επιτιθέμενος μπορεί να παρέχει το αρχείο εγκατάστασης ή έναν ανώνυμο εξυπηρετητή και όταν κάθε σύστημα πράκτορα ενεργοποιείται (ή συνδέεται με το Διαδίκτυο), ο πράκτορας αυτόματα αναζητά ενημερώσεις και τις

εγκαθιστά. Το *Stalchedraht* επίσης παρέχει μία ασφαλή σύνδεση telnet μέσω συμμετρικής κρυπτογράφησης κλειδιού ανάμεσα στα συστήματα του επιτιθέμενου και του χειριστή. Η επικοινωνία πραγματοποιείται μέσω πακέτων TCP και ICMP. Μερικές από τις επιθέσεις που μπορούν να πραγματοποιηθούν με το *Stacheldraht* περιλαμβάνουν τις πλημμύρες UDP, TCP SYN, αιτήσεων ηχούς ICMP και κατευθυνόμενης ανοικτής εκπομπής ICMP.

Το εργαλείο *mstream* [Dittrich, 2000b] χρησιμοποιεί παραποιημένα πακέτα TCP θέτοντας τη σημαία ACK ώστε να επιτεθεί στο στόχο. Το *mstream* είναι ένα απλό σημείο-προς-σημείο εργαλείο πλημμύρας TCP ACK. Η επικοινωνία η οποία δεν κρυπτογραφείται πραγματοποιείται μεταξύ πακέτων TCP και UDP. Ο χειριστής επικοινωνεί με τους πράκτορες μέσω telnet. Η πρόσβαση στον χειριστή προστατεύεται με συνθηματικό. Το θύμα στόχος λαμβάνει πακέτα ACK και στέλνει πακέτα TCP RST (ReSeT) σε μη υπάρχουσες διευθύνσεις IP. Οι δρομολογητές στέλνουν πακέτα ICMP "απρόσιτου προορισμού" καταναλώνοντας ακόμα περισσότερο εύρος ζώνης. Το *mstream* έχει περιορισμένα χαρακτηριστικά ελέγχου και μπορεί να εφαρμόσει την τεχνική παραποίησης τυχαία και στα 32 bit της διεύθυνσης πηγής IP.

Το *Shaft* [Dietrich, 2000] είναι ένα παράγωγο του εργαλείου Trinoo. Χρησιμοποιεί επικοινωνία UDP ανάμεσα στους χειριστές και τους πράκτορες χωρίς να κρυπτογραφούνται τα μηνύματα. Το *Shaft* μπορεί να πραγματοποιήσει επιθέσεις πλημμύρας UDP, ICMP και TCP. Οι επιθέσεις μπορούν να πραγματοποιηθούν ξεχωριστά, ή μπορεί να συνδυαστούν για να πραγματοποιηθεί μία επίθεση πλημμύρας UDP/TCP/ICMP. Το *Shaft* δημιουργεί τυχαίες διευθύνσεις πηγής IP και θύρες πηγής στα πακέτα. Το μέγεθος των πακέτων παραμένει σταθερό κατά τη διάρκεια της επίθεσης. Ένα σημαντικό χαρακτηριστικό του *Shaft* είναι η ικανότητα να αλλάζει τη διεύθυνση IP και τη θύρα του χειριστή σε πραγματικό χρόνο, κάνοντας ιδιαίτερα δύσκολη την αποτελεσματικότητα των εργαλείων ανίχνευσης εισβολών. Επιπλέον το *Shaft* παρέχει στατιστικά στοιχεία για τις επιθέσεις πλημμύρας. Αυτά τα στατιστικά στοιχεία είναι χρήσιμα στον επιτιθέμενο προκειμένου να γνωρίζει πότε το σύστημα του θύματος είναι εκτός λειτουργίας και πότε να σταματήσει να προσθέτει μηχανές-πράκτορες στην επίθεση.

3.3.2 Εργαλεία Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης που Βασίζονται σε Κανάλια IRC

Τα εργαλεία *Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης* που βασίζονται σε κανάλια IRC αναπτύχθηκαν μετά την εμφάνιση των εργαλείων επίθεσης που βασίζονται στο μοντέλο πράκτορα-χειριστή. Αυτό είχε σαν αποτέλεσμα πολλά εργαλεία που βασίζονται σε κανάλια IRC να είναι πιο εξεζητημένα καθώς περιλαμβάνουν μερικά σημαντικά χαρακτηριστικά που μπορεί να βρεθούν σε πολλά εργαλεία επίθεσης τα οποία ακολουθούν το μοντέλο πράκτορα-χειριστή.

Ένα από τα πιο γνωστά εργαλεία DDoS που βασίζονται σε κανάλια IRC είναι το *Trinity*. Το *Trinity v3* [Hancock, 2000] εκτός από τις πολύ γνωστές επιθέσεις πλημμύρας UDP, TCP SYN, TCP ACK και TCP NUL εισάγει τις πλημμύρες τυχαίων σημαίων πακέτων TCP, τις πλημμύρες κατάτμησης TCP, τις εγκαταστημένες πλημμύρες TCP και τις πλημμύρες πακέτων TCP RST. Δημιουργεί τυχαίες διευθύνσεις πηγής IP χρησιμοποιώντας και τα 32 bit [CERT, 2001c]. Επίσης παράγει πακέτα πλημμύρας TCP με τυχαίες σημαίες ελέγχου και κατά αυτόν τον τρόπο το Trinity παρέχει ένα μεγάλο σύνολο επιθέσεων που βασίζονται στο TCP. Στην ίδια γενιά με το *Trinity* είναι το *myServer* [Dietrich, 2000], το οποίο βασίζεται σε εξωτερικά προγράμματα προκειμένου να παρέχει επιθέσεις άρνησης εξυπηρέτησης και το *Plague* [Dietrich, 2000], το οποίο παρέχει επιθέσεις πλημμύρας TCP ACK και TCP SYN.

Το *Knight* είναι ένα εργαλείο DDoS που βασίζεται σε κανάλια IRC. Το *Knight* δεν προκαλεί υπολογιστική επιβάρυνση αλλά είναι αποτελεσματικό στην πραγματοποίηση επιθέσεων DDoS [CERT, 2001c]. Το *Knight* μπορεί να προκαλέσει επιθέσεις SYN και πλημμύρας UDP [Bysin, 2001]. Σχεδιάστηκε για τα λειτουργικά συστήματα Windows και έχει σημαντικά χαρακτηριστικά όπως την αυτόματη ανανέωση μέσω http ή ftp. Το *Knight* τυπικά εγκαθίσταται χρησιμοποιώντας ένα πρόγραμμα Δούρειου Ίππου (Trojan horse) που ονομάζεται Back Orifice [CERT, 2001c]. Άλλο ένα εργαλείο DDoS που βασίζεται στο *Knight* είναι το *Kaiten* [Dietrich, 2000], το οποίο περιλαμβάνει επιθέσεις πλημμύρας UDP και TCP, επιθέσεις SYN και επιθέσεις PUSH+ACH και αλλάζει με τυχαίο τρόπο και τα 32 bit της διεύθυνσης πηγής.

3.4 Κατηγοριοποίηση των Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης

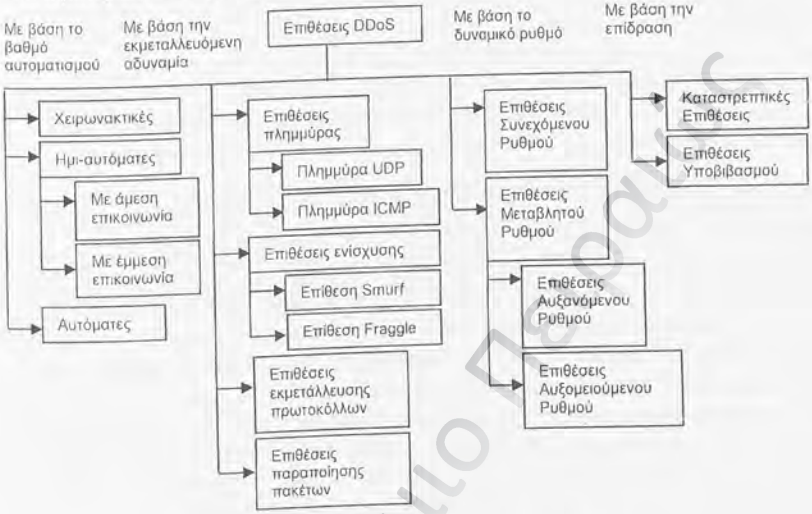
Προκειμένου να κατανοήσουμε τις επιθέσεις DDoS είναι σημαντικό να έχουμε μία επίσημη κατηγοριοποίηση των επιθέσεων αυτών. Προτείνουμε μία κατηγοριοποίηση των επιθέσεων DDoS που συνδυάζει αποτελεσματικά τις κατηγοριοποιήσεις που προτείνονται από τους Mirkovic και άλλους [Mirkovic, 2002a] και Lee και άλλους [Lee, 2003] καθώς και πιο πρόσφατα αποτελέσματα έρευνας. Αυτή η κατηγοριοποίηση απεικονίζεται στο σχήμα 2.3 και αποτελείται από δύο επίπεδα. Στο πρώτο επίπεδο οι επιθέσεις κατηγοριοποιούνται με βάση το βαθμό αυτοματισμού, την εκμεταλλευόμενη αδυναμία, το δυναμικό ρυθμό της επίθεσης και την επίδρασή της. Στο δεύτερο επίπεδο αναγνωρίζονται ειδικά χαρακτηριστικά κάθε κατηγορίας πρώτου επιπέδου.

3.4.1 Κατηγοριοποίηση με Βάση το Βαθμό Αυτοματισμού

Με βάση το *βαθμό αυτοματισμού*, οι επιθέσεις DDoS μπορεί να κατηγοριοποιηθούν σε *χειρωνακτικές*, *ημί-αυτόματες* και *αυτόματες*.

- Οι αρχικές επιθέσεις DDoS ήταν *χειρωνακτικές*. Αυτό σημαίνει ότι η στρατηγική DDoS περιελάμβανε τη σάρωση των απομακρυσμένων μηχανών

για την εύρεση αδυναμιών, αποκτώντας πρόσβαση σε αυτά και εγκαθιστώντας τον κώδικα επίθεσης. Όλα αυτά τα βήματα αργότερα αυτοματοποιήθηκαν, χρησιμοποιώντας *ημι-αυτόματες* επιθέσεις DDoS και *αυτόματες* επιθέσεις DDoS.



Σχήμα 2. 3 Κατηγοριοποίηση των Επιθέσεων DDoS

- Στις *ημι-αυτόματες* επιθέσεις, οι επιθέσεις DDoS ανήκουν στο μοντέλο επίθεσης πράκτορα-χειριστή. Ο επιτιθέμενος εξετάζει και καταλαμβάνει τους χειριστές και τους πράκτορες χρησιμοποιώντας αυτοματοποιημένα σενάρια. Ο τύπος της επίθεσης, η διεύθυνση του θύματος και η έναρξη της επίθεσης καθορίζεται από τις μηχανές-χειριστές. Οι *ημι-αυτόματες* επιθέσεις μπορεί επιπλέον να διαχωριστούν σε επιθέσεις *με άμεση επικοινωνία* και σε επιθέσεις *με έμμεση επικοινωνία*. Οι επιθέσεις *με άμεση επικοινωνία* περιλαμβάνουν επιθέσεις κατά τη διάρκεια των οποίων ο πράκτορας και ο χειριστής χρειάζεται να γνωρίζουν ο ένας την ταυτότητα του άλλου προκειμένου να επικοινωνήσουν. Αυτή η προσέγγιση περιλαμβάνει την αντιγραφή στο υλικό της διεύθυνσης IP των μηχανών-χειριστών. Το κύριο μειονέκτημα αυτής της προσέγγισης είναι ότι η αποκάλυψη μίας κατειλημμένης μηχανής μπορεί να εκθέσει ολόκληρο το δίκτυο DDoS. Οι επιθέσεις *με έμμεση επικοινωνία* χρησιμοποιούν την ανακατεύθυνση προκειμένου να επιτύχουν μεγαλύτερη επιβιωσιμότητα των επιθέσεων DDoS. Ένα χαρακτηριστικό παράδειγμα αυτού του τύπου επιθέσεων είναι οι επιθέσεις DDoS που βασίζονται σε κανάλια IRC, οι οποίες αναλύθηκαν ήδη σε προηγούμενη ενότητα.

- Στις *αυτόματες* επιθέσεις DDoS αποφεύγεται η επικοινωνία ανάμεσα στον επιτιθέμενο και τους πράκτορες. Στις περισσότερες περιπτώσεις η φάση της επίθεσης περιορίζεται σε μία απλή εντολή. Όλα τα χαρακτηριστικά της επίθεσης, για παράδειγμα ο τύπος της επίθεσης, η διάρκεια και η διεύθυνση του θύματος, καθορίζονται στον κώδικα της επίθεσης. Με αυτόν τον τρόπο, ο επιτιθέμενος εκτίθεται ελάχιστα και η πιθανότητα να αποκαλυφθεί η ταυτότητά του είναι μικρή. Το μειονέκτημα αυτής της προσέγγισης είναι ότι οι μηχανισμοί διάδοσης μπορεί να αφήσουν το κατειλημμένο μηχάνημα ευπαθές, κάνοντας δυνατή με αυτό τον τρόπο τη μελλοντική πρόσβαση και τροποποίηση του κώδικα επίθεσης.

3.4.2 Κατηγοριοποίηση με Βάση την Εκμεταλλευόμενη Αδυναμία

Οι επιθέσεις DDoS με βάση την εκμεταλλευόμενη αδυναμία μπορεί να διαχωριστούν στις ακόλουθες κατηγορίες: επιθέσεις *πλημμύρας*, επιθέσεις *ενίσχυσης*, επιθέσεις *εκμετάλλευσης πρωτοκόλλου* και επιθέσεις *παραποίησης πακέτων*.

- Σε μία *επίθεση πλημμύρας*, οι πράκτορες στέλνουν μεγάλη ποσότητα κυκλοφορίας IP στο σύστημα του θύματος προκειμένου να προκαλέσουν συμφόρηση στο εύρος ζώνης στο σύστημα του θύματος. Η επίδραση των ροών των πακέτων που στέλνονται από τους πράκτορες στο θύμα ποικίλουν από καθυστέρηση ή κλείσιμο του συστήματος μέχρι εξάντληση του εύρους ζώνης του δικτύου. Μερικές από τις πιο γνωστές επιθέσεις πλημμύρας είναι οι *επιθέσεις πλημμύρας UDP* και οι *επιθέσεις πλημμύρας ICMP*.

  Η επίθεση *πλημμύρας UDP* είναι δυνατή όταν ένας μεγάλος αριθμός πακέτων UDP στέλνεται στο σύστημα του θύματος. Αυτό έχει σαν αποτέλεσμα τον βομβαρδισμό του δικτύου και την εξάντληση του διαθέσιμου εύρους ζώνης για νόμιμες αιτήσεις του συστήματος του θύματος. Σε μία επίθεση *πλημμύρας UDP*, τα πακέτα UDP στέλνονται είτε σε τυχαίες ή σε καθορισμένες θύρες στο σύστημα του θύματος. Τυπικά, οι επιθέσεις *πλημμύρας UDP* σχεδιάζονται έτσι ώστε να επιτίθενται σε τυχαίες θύρες του θύματος. Μία επίθεση *πλημμύρας UDP* είναι δυνατή όταν ο επιτιθέμενος στέλνει ένα πακέτο UDP σε τυχαία θύρα του θύματος. Όταν το σύστημα του θύματος λαμβάνει ένα πακέτο UDP, θα καθορίσει ποια εφαρμογή περιμένει στη θύρα προορισμού. Όταν συνειδητοποιήσει ότι δεν υπάρχει εφαρμογή που να περιμένει στη θύρα, θα παράγει ένα πακέτο ICMP "απρόσιτου προορισμού" [Houle, 2001] προς την παραποιημένη διεύθυνση πηγής. Εάν αρκετά πακέτα UDP φτάσουν στις θύρες του θύματος, το σύστημα θα τεθεί εκτός λειτουργίας. Χρησιμοποιώντας ένα εργαλείο DDoS η διεύθυνση πηγής IP είναι παραποιημένη και με αυτό τον τρόπο προστατεύεται από αποκάλυψη η πραγματική ταυτότητα των δευτερευόντων θυμάτων και δεν φτάνουν στους πράκτορες τα πακέτα που στέλνονται από το σύστημα του θύματος.

Οι *επιθέσεις πλημμύρας ICMP* εκμεταλλεύονται το Internet Control Message Protocol (ICMP), ενεργοποιώντας τους χρήστες να στείλουν ένα πακέτο ηχούς σε ένα απομακρυσμένο κόμβο για να ελέγξουν εάν είναι σε λειτουργία. Πιο συγκεκριμένα κατά τη διάρκεια μίας επίθεσης *πλημμύρας ICMP* οι πράκτορες στέλνουν μεγάλο αριθμό από πακέτα ("ping") ICMP_ECHO_REPLY στο θύμα. Αυτά τα πακέτα ζητούν απάντηση από το θύμα, γεγονός το οποίο έχει σαν αποτέλεσμα την εξάντληση του εύρους ζώνης του δικτύου σύνδεσης του θύματος [Criscuolo, 2000]. Κατά τη διάρκεια μίας επίθεσης *πλημμύρας ICMP* η διεύθυνση πηγής IP μπορεί να είναι παραποιημένη.

- Στις *επιθέσεις ενίσχυσης* ο επιτιθέμενος ή οι πράκτορες εκμεταλλεύονται το χαρακτηριστικό διεύθυνσης IP ανοικτής εκπομπής, που υπάρχει στους περισσότερους δρομολογητές, για να ενισχύσουν και να ανακλάσουν την επίθεση και να στείλουν μηνύματα σε μία διεύθυνση IP ανοικτής εκπομπής. Αυτό καθοδηγεί τους δρομολογητές που εξυπηρετούν τα πακέτα μέσα στο δίκτυο να τα στείλουν σε όλες τις διευθύνσεις IP μέσα στο εύρος ανοικτής εκπομπής της διεύθυνσης. Κατά αυτόν τον τρόπο, η κακόβουλη κυκλοφορία που παράγεται μειώνει το εύρος ζώνης στο σύστημα του θύματος. Σε αυτό τον τύπο επίθεσης DDoS, ο επιτιθέμενος μπορεί να στείλει το μήνυμα ανοικτής εκπομπής προκειμένου να αυξήσει την ποσότητα της επιτιθέμενης κυκλοφορίας. Εάν το μήνυμα ανοικτής εκπομπής στέλνεται άμεσα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει τα συστήματα μέσα στο δίκτυο ανοικτής εκπομπής σαν πράκτορες χωρίς να χρειάζεται να εγκαταστήσει λογισμικό πρακτόρων σε αυτά. Οι ενδιάμεσοι κόμβοι που χρησιμοποιούνται σαν εκκινητές στις *επιθέσεις ενίσχυσης* ονομάζονται ανακλαστήρες [Paxson, 2001]. Ένας ανακλαστήρας είναι οποιοσδήποτε κόμβος IP που θα επιστρέψει ένα πακέτο εάν λάβει ένα πακέτο. Επομένως, οι εξυπηρετητές ιστού, οι εξυπηρετητές υπηρεσίας διάθεσης ονομάτων και διευθύνσεων που χρησιμοποιούνται στο διαδίκτυο (Domain Name Service (DNS)) και οι δρομολογητές είναι ανακλαστήρες, καθώς επιστρέφουν πακέτα SYN ACK ή RST σαν απόκριση σε πακέτα SYN ή άλλα TCP.

  Κατά τη διάρκεια μίας *επίθεσης ενίσχυσης* ο επιτιθέμενος στέλνει στους ανακλαστήρες πακέτα που απαιτούν αποκρίσεις. Τα πακέτα έχουν παραποιημένες διευθύνσεις, με τη διεύθυνση πηγής να έχει τεθεί ίση με τη διεύθυνση του θύματος. Οι ανακλαστήρες επιστρέφουν πακέτα απόκρισης στο θύμα σύμφωνα με τους τύπους των πακέτων επίθεσης. Τα πακέτα επίθεσης ανακλώνται προς το θύμα. Τα ανακλώμενα πακέτα μπορούν να πλημμυρίσουν τη ζεύξη του θύματος εάν ο αριθμός των ανακλαστήρων είναι αρκετά μεγάλος. Σημειώνεται ότι οι ανακλαστήρες αναγνωρίζονται εύκολα σαν διευθύνσεις πηγής στα πακέτα πλημμύρας που λαμβάνονται από το θύμα. Από την άλλη πλευρά, ο διαχειριστής του ανακλαστήρα δεν μπορεί εύκολα να εντοπίσει τον υποτελή κόμβο που βομβαρδίζει με πακέτα τον

ανακλαστήρα, καθώς η κυκλοφορία που στέλνεται στον ανακλαστήρα δεν έχει ως διεύθυνση πηγής τη διεύθυνση του υποτελή κόμβου, αλλά τη διεύθυνση του θύματος.

Τα κύρια χαρακτηριστικά που διαφοροποιούν μία επίθεση ενίσχυσης από μία άμεση επίθεση είναι τα ακόλουθα [Chang, 2002]:

- Σε μία *επίθεση ενίσχυσης* είναι απαραίτητοι κάποιοι προκαθορισμένοι ανακλαστήρες.
- Οι ανακλαστήρες μπορεί επίσης να διασκορπιστούν στο Διαδίκτυο, καθώς ο επιτιθέμενος δεν χρειάζεται να εγκαταστήσει λογισμικό πρακτόρων.
- Τα ανακλώμενα πακέτα είναι φυσιολογικά πακέτα με νόμιμη προέλευση, που δεν μπορεί να συλληφθούν και να περιοριστούν μέσω φιλτραρίσματος και μηχανισμούς δρομολόγησης.

Χαρακτηριστικά παραδείγματα επιθέσεων *ενίσχυσης* είναι οι επιθέσεις *Smurf* και *Fraggle*.

Οι επιθέσεις *Smurf* στέλνουν κυκλοφορία αιτήσεων ηχούς ICMP με παραποιημένες διευθύνσεις πηγής [Daemon9, 1996] ίδια με αυτή του θύματος στόχου σε ένα αριθμό διευθύνσεων IP ανοικτής εκπομπής. Οι περισσότεροι κόμβοι σε ένα δίκτυο IP οι οποίοι θα δεχθούν αιτήσεις ηχούς ICMP [Daemon9, 1996] απαντούν στη διεύθυνση πηγής αυτών των αιτήσεων. Στην περίπτωση των επιθέσεων *Άρνησης Εξυπηρέτησης* η διεύθυνση πηγής είναι η διεύθυνση του θύματος-στόχου. Στην περίπτωση ενός δικτύου ανοικτής εκπομπής οι απαντήσεις σε κάθε ένα πακέτο ICMP θα μπορούσαν να είναι εκατοντάδες. Σε αυτό τον τύπο επίθεσης πλήττεται όχι μόνο το θύμα αλλά και ενδιάμεσες συσκευές εκπομπής (ανακλαστήρες) [CERT, 2001c]. Η επίθεση *Fraggle* είναι ένας παρόμοιος τύπος επιθέσεων με τη *Smurf* με εξαίρεση ότι χρησιμοποιεί πακέτα ηχούς *UDP* αντί για πακέτα ηχούς ICMP. Οι επιθέσεις *Fraggle* παράγουν ακόμα περισσότερη κακή κυκλοφορία και μπορούν να δημιουργήσουν ακόμα πιο καταστρεπτικά αποτελέσματα από μία επίθεση *Smurf*.

- Οι *επιθέσεις εκμετάλλευσης πρωτοκόλλων* [Mirkovic, 2004] εκμεταλλεύονται ένα συγκεκριμένο χαρακτηριστικό ή σφάλμα υλοποίησης κάποιου πρωτοκόλλου που έχει εγκατασταθεί στο θύμα, προκειμένου να καταναλώσουν υπερβολικές ποσότητες από τους πόρους του θύματος. Ένα χαρακτηριστικό παράδειγμα των επιθέσεων εκμετάλλευσης πρωτοκόλλων είναι οι επιθέσεις *TCP SYN*.

  Οι *επιθέσεις TCP SYN* εκμεταλλεύονται τις έμφυτες αδυναμίες της χειραψίας τριών τρόπων (three-way handshake) που περιλαμβάνεται στην έναρξη μίας σύνδεσης TCP. Ένας εξυπηρετητής, λαμβάνοντας μία αρχική αίτηση σύνδεσης SYN (συγχρονισμός/εκκίνηση) από έναν πελάτη, ανταποκρίνεται με ένα πακέτο SYN/ACK (συγχρονισμό/επιβεβαίωση) και περιμένει από τον πελάτη να στείλει την τελική επιβεβαίωση ACK.

Μία επίθεση *πλημμύρας SYN* ξεκινά με την αποστολή ενός μεγάλου αριθμού πακέτων SYN, χωρίς να παρέχεται επιβεβαίωση σε καμία από τις απαντήσεις που δέχεται, ενώ ο εξυπηρετητής περιμένει για επιβεβαιώσεις ACK [Bellovin, 1989]. Λαμβάνοντας υπόψη το γεγονός ότι ο εξυπηρετητής έχει περιορισμένη ουρά ενδιάμεσης μνήμης για νέες συνδέσεις, η επίθεση *πλημμύρας SYN* έχει σαν αποτέλεσμα ο εξυπηρετητής να μην μπορεί να επεξεργαστεί τις εισερχόμενες συνδέσεις καθώς η ουρά υπερφορτώνεται [Cisco, 1999]. Άλλα παραδείγματα επιθέσεων που εκμεταλλεύονται πρωτόκολλα είναι οι επιθέσεις PUSH+ACK, οι επιθέσεις αιτήσεων CGI και οι επιθέσεις αυθεντικοποίησης του εξυπηρετητή.

- *Οι επιθέσεις τροποποιημένων πακέτων* [Lee, 2003] βασίζονται σε λανθασμένα τροποποιημένα πακέτα IP τα οποία στέλνονται από τους πράκτορες στο θύμα προκειμένου να καταρρεύσει το σύστημα του θύματος. Οι επιθέσεις *τροποποιημένων πακέτων* μπορεί να διαχωριστούν σε δύο τύπους επιθέσεων: επιθέσεις *διεύθυνσης IP* και επιθέσεις *επιλογών πακέτων IP*. Σε μία επίθεση *διεύθυνσης IP*, το πακέτο περιέχει την ίδια διεύθυνση πηγής και προορισμού. Αυτό έχει σαν αποτέλεσμα τη σύγχυση του λειτουργικού συστήματος του θύματος και την κατάρρευσή του. Ένα ιδιαίτερο χαρακτηριστικό των τροποποιημένων πακέτων που χρησιμοποιείται προκειμένου να πραγματοποιηθούν οι επιθέσεις *επιλογών πακέτων IP* είναι η αλλαγή με τυχαίο τρόπο των προαιρετικών πεδίων μέσα σε ένα πακέτο IP και επιπλέον να τίθενται όλα τα bit ποιότητας υπηρεσίας ίσα με ένα. Αυτό μπορεί να έχει σαν αποτέλεσμα τη χρήση πρόσθετου χρόνου επεξεργασίας από το θύμα προκειμένου να αναλυθεί η κυκλοφορία. Εάν η επίθεση συνδυάζεται με τη χρήση πολλαπλών πρακτόρων, μπορεί να οδηγήσει στην κατάρρευση του συστήματος του θύματος.

3.4.3 Κατηγοριοποίηση με Βάση το Δυναμικό Ρυθμό του Θύματος

Ανάλογα με το δυναμικό ρυθμό της επίθεσης οι επιθέσεις DDoS μπορεί να διαχωριστούν σε επιθέσεις *συνεχόμενου ρυθμού* και *επιθέσεις μεταβλητού ρυθμού*.

- Οι επιθέσεις *συνεχόμενου ρυθμού* αποτελούνται από επιθέσεις που μετά από την έναρξη της επίθεσης εκτελούνται με πλήρη ισχύ χωρίς διακοπή ή ελάττωση της έντασης. Η επίδραση μίας τέτοιας επίθεσης είναι πολύ γρήγορη.
- Οι επιθέσεις *μεταβλητού ρυθμού* όπως υποδεικνύεται και από το όνομά τους, μεταβάλλουν το ρυθμό επίθεσης και κατά αυτόν τον τρόπο αποφεύγουν την ανίχνευση και την άμεση απόκριση. Βασιζόμενοι στο μηχανισμό αλλαγής ρυθμού διαφοροποιούνται σε επιθέσεις *αυξανόμενου ρυθμού* και *αυξομειούμενου ρυθμού*. Οι επιθέσεις *αυξανόμενου ρυθμού* οδηγούν σταδιακά στην εξάντληση των πόρων του θύματος, με αποτέλεσμα να καθυστερούν την ανίχνευση της επίθεσης. Οι επιθέσεις *αυξομειούμενου ρυθμού* έχουν ένα κυματιστό ρυθμό που ορίζεται από τη συμπεριφορά του θύματος και την απόκριση στην επίθεση,

ελαττώνοντας κατά καιρούς το ρυθμό προκειμένου να αποφύγουν την ανίχνευση.

3.4.4 Κατηγοριοποίηση με Βάση την Επίδραση

Βασιζόμενοι στην επίδραση μίας επίθεσης DDoS μπορούμε να διαχωρίσουμε μία επίθεση DDoS σε *καταστρεπτική* και σε επίθεση *υποβιβασμού*.

- Οι *καταστρεπτικές* επιθέσεις μπορούν να οδηγήσουν σε πλήρη άρνηση εξυπηρέτησης του θύματος στους πελάτες του.
- Ο στόχος των επιθέσεων *υποβιβασμού* είναι η κατανάλωση ενός τμήματος των πόρων του θύματος. Αυτό έχει σαν αποτέλεσμα την καθυστέρηση της ανίχνευσης της επίθεσης και την ίδια στιγμή μία τεράστια καταστροφή στο θύμα.

4. Κατηγοριοποίηση των Μηχανισμών Αντιμετώπισης των Επιθέσεων DDoS

Οι επιθέσεις DDoS είναι ένα ιδιαίτερα δύσκολο πρόβλημα να λυθεί. Πρώτα από όλα δεν υπάρχουν κοινά χαρακτηριστικά μεταξύ των ροών πακέτων DDoS που μπορούν να χρησιμοποιηθούν για την ανίχνευσή τους. Επιπλέον, η κατανεμημένη φύση των επιθέσεων DDoS κάνει ιδιαίτερα δύσκολη την ανίχνευση ή εύρεση της προέλευσης της πηγής. Τα αυτοματοποιημένα εργαλεία που κάνουν την εφαρμογή μίας επίθεσης DDoS δυνατή μπορούν εύκολα να ληφθούν από το Διαδίκτυο. Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιήσουν παραποιημένες διευθύνσεις IP προκειμένου να κρύψουν την αληθινή τους ταυτότητα, και αυτό κάνει ιδιαίτερα δύσκολη την εύρεση της πηγής των επιθέσεων DDoS. Τέλος, δεν υπάρχει αρκετά υψηλό επίπεδο ασφάλειας σε όλους τους κόμβους του Διαδικτύου, καθώς υπάρχουν σημαντικά κενά ασφάλειας σε αυτούς.

Μπορούμε να κατηγοριοποιήσουμε τους μηχανισμούς αντιμετώπισης των επιθέσεων DDoS χρησιμοποιώντας δύο διαφορετικά κριτήρια. Η πρώτη κατηγοριοποίηση ταξινομεί τους μηχανισμούς αντιμετώπισης των επιθέσεων DDoS σύμφωνα με την ενέργεια που εφαρμόζεται. Έτσι έχουμε τις ακόλουθες κατηγορίες:

- Παρεμπόδιση Εισβολών.
- Ανίχνευση Εισβολών.
- Ανεκτικότητα και Μετριασμός Εισβολών, και
- Απόκριση σε Εισβολές.

Η δεύτερη κατηγοριοποίηση διαχωρίζει τους μηχανισμούς αντιμετώπισης των επιθέσεων DDoS με βάση την τοποθεσία εφαρμογής του μηχανισμού

αντιμετώπισης με αποτέλεσμα τις τρεις ακόλουθες κατηγορίες αντιμετώπισης επιθέσεων DDoS:

- Δίκτυο του θύματος
- Ενδιάμεσο δίκτυο, και
- Δίκτυο πηγής.

Η κατηγοριοποίηση των μηχανισμών αντιμετώπισης των επιθέσεων DDoS που έχουμε προτείνει απεικονίζεται στο Σχήμα 2.4. Στη συνέχεια συζητάμε εκτεταμένα κάθε μία από τις κατηγορίες της πρώτης ταξινόμησης και απλά αναφερόμαστε στους μηχανισμούς αντιμετώπισης των επιθέσεων DDoS και τον τρόπο με τον οποίο ταξινομούνται στην τελευταία κατηγοριοποίηση.

5. Κατηγοριοποίηση με Βάση τη Δραστηριότητα

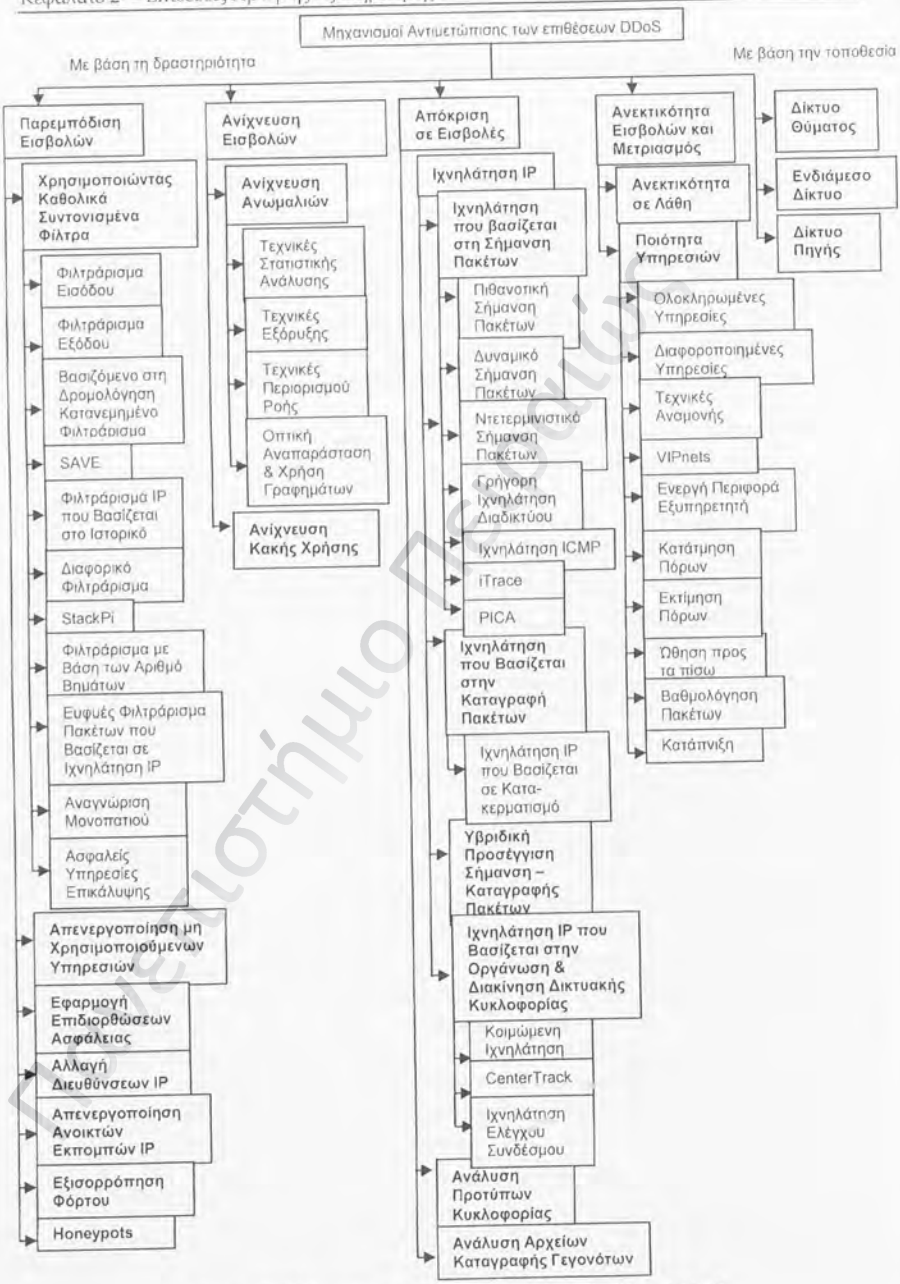
5.1 Παρεμπόδιση Εισβολών

Η καλύτερη στρατηγική μετριασμού μίας επίθεσης είναι η πλήρης παρεμπόδιση της επίθεσης. Σε αυτό το στάδιο προσπαθούμε να σταματήσουμε τις επιθέσεις DDoS από το να πραγματοποιηθούν σε πρώτη φάση. Υπάρχουν πολλοί μηχανισμοί αντιμετώπισης των επιθέσεων DDoS που προσπαθούν να προστατέψουν τα συστήματα από επιθέσεις:

Χρησιμοποιώντας καθολικά συντονισμένα φίλτρα μπορούμε να σταματήσουμε τα πακέτα επίθεσης πριν να έχουν καταστροφικές επιδράσεις. Οι μηχανισμοί φιλτραρίσματος μπορούν να διαχωριστούν στις ακόλουθες κατηγορίες:

Το *φιλτράρισμα εισόδου (ingress filtering)* είναι μία προσέγγιση σύμφωνα με την οποία ένας δρομολογητής ρυθμίζεται έτσι ώστε να μην επιτρέπει να περάσουν στο δίκτυο εισερχόμενα πακέτα με μη-νόμιμες διευθύνσεις πηγής. Η τεχνική *φιλτραρίσματος εισόδου*, η οποία είχε προταθεί από τους Ferguson και Senie [Ferguson, 2000], είναι ένας μηχανισμός περιορισμού προκειμένου να σταματήσει η κυκλοφορία με διευθύνσεις IP που δεν ταιριάζουν στο πρόθεμα δικτυακής περιοχής (domain) που είναι συνδεδεμένες με τον δρομολογητή εισόδου. Αυτός ο μηχανισμός μπορεί δραστικά να μειώσει τις επιθέσεις DoS που χρησιμοποιούν παραποιημένες διευθύνσεις IP εάν τον χρησιμοποιούν όλες οι δικτυακές περιοχές. Μερικές φορές η νόμιμη κυκλοφορία μπορεί να απορριφθεί μέσω της τεχνικής του *φιλτραρίσματος εισόδου* όταν χρησιμοποιείται το πρωτόκολλο Mobile IP [Perkins, 2002] για να συνδεθεί ένας κινητός κόμβος σε ένα "ξένο" δίκτυο.

Το *φιλτράρισμα εξόδου* [Brenton, 2006] είναι ένα εξωτερικό φίλτρο, το οποίο εξασφαλίζει ότι πακέτα με μόνο παραχωρημένα ή δεσμευμένα διαστήματα διευθύνσεων IP αφήνουν το δίκτυο. Τα φίλτρα εξόδου δεν βοηθούν να αποφευχθεί η απώλεια πόρων της δικτυακής περιοχής (domain) από όπου προέρχεται το πακέτο αλλά προστατεύουν άλλες δικτυακές περιοχές (domains)



Σχήμα 2. 4 Μηχανισμοί Προστασίας από τις Επιθέσεις DDoS

από πιθανές επιθέσεις. Εκτός από το θέμα της ακριβούς τοποθέτησης, τόσο τα φίλτρα εισόδου όσο και τα φίλτρα εξόδου έχουν παρόμοια συμπεριφορά.

Το *βασιζόμενο στη δρομολόγηση κατανεμημένο φιλτράρισμα* πακέτων προτάθηκε από τους Park και Lee [Park, 2001a]. Αυτή η προσέγγιση έχει τη δυνατότητα να φιλτράρει ένα μεγάλο ποσοστό παραποιημένων πακέτων IP και να παρεμποδίζει πακέτα επιθέσεων από το να φτάσουν το στόχο τους καθώς και να βοηθήσει στον εντοπισμό της προέλευσης της επίθεσης (ιχνηλάτηση IP). Τα φίλτρα που βασίζονται σε δρομολόγηση χρησιμοποιούν πληροφορίες δρομολόγησης για να φιλτράρουν πλαστά πακέτα IP, κάτι που τα διαφοροποιεί από το φιλτράρισμα εισόδου. Καθώς οι δρομολογήσεις στο Διαδίκτυο αλλάζουν με το πέρασμα του χρόνου [Paxson, 1999] είναι σημαντική πρόκληση για τα φίλτρα που βασίζονται σε δρομολόγηση να ανανεώνονται σε πραγματικό χρόνο. Το κύριο μειονέκτημα αυτής της προσέγγισης είναι ότι απαιτεί καθολική γνώση της τοπολογίας του δικτύου, γεγονός το οποίο οδηγεί σε θέματα κλιμάκωσης αλλά και καθολική εφαρμογή.

Η απαίτηση της καθολικής εφαρμογής είναι επίσης απαραίτητη στο πρωτόκολλο *Ενδυνάμωσης Εγκυρότητας Διεύθυνσης Πηγής (Source Address Validity Enforcement (SAVE))* [Li, 2002] το οποίο παρέχει στους δρομολογητές Διαδικτύου πληροφορίες για την κατασκευή πίνακα που αντιστοιχίζουν διαστήματα διευθύνσεων πηγής σε διεπαφές δρομολογητών. Το πρωτόκολλο SAVE [Li, 2002] παρουσιάζει επίσης πολλές αδυναμίες μεταξύ των οποίων περιλαμβάνεται η πιθανή τροποποίηση του πίνακα εισόδου, καθώς ο επιτιθέμενος έχει την ικανότητα να εισάγει λανθασμένα μηνύματα ανανέωσης και η ασυνέπεια του πίνακα εισόδου εξαιτίας συχνών αλλαγών δρομολόγησης, οδηγούν σε λανθασμένο φιλτράρισμα πακέτων.

Το *φιλτράρισμα IP που βασίζεται στο ιστορικό (History-based IP filtering (HIP))* είναι άλλος ένας μηχανισμός φιλτραρίσματος που προτάθηκε από τους Peng και άλλους [Peng, 2003], προκειμένου να παρεμποδιστούν οι επιθέσεις DDoS. Σύμφωνα με αυτή την προσέγγιση, ο ακραίος δρομολογητής δέχεται τα εισερχόμενα πακέτα σύμφωνα με μία προκαθορισμένη βάση δεδομένων διευθύνσεων IP. Η βάση δεδομένων των διευθύνσεων IP βασίζεται στο ιστορικό των προηγούμενων συνδέσεων του ακραίου δρομολογητή (edge router). Αυτή η προσέγγιση είναι αυτοδύναμη, δεν χρειάζεται τη συνεργασία ολόκληρης της διαδικτυακής κοινότητας, είναι εφαρμόσιμη σε μία πλούσια ποικιλία τύπων κυκλοφορίας και απαιτεί μικρή ρύθμιση. Από την άλλη πλευρά, εάν οι επιτιθέμενοι γνωρίζουν ότι το φιλτράρισμα των πακέτων IP πραγματοποιείται με βάση τις προηγούμενες συνδέσεις, μπορούν να εξαπατήσουν τον εξυπηρετητή ώστε να περιληφθούν στη βάση δεδομένων των διευθύνσεων IP. Αυτό μπορεί να παρεμποδιστεί αυξάνοντας την περίοδο κατά την οποία οι διευθύνσεις IP πρέπει να εμφανίζονται ώστε να θεωρηθούν αυτές οι διευθύνσεις συχνές.

Οι Tanachaiwiwat και άλλοι [Tanachaiwiwat, 2003] πρότειναν ένα *διαφορικό μηχανισμό φιλτραρίσματος πακέτων (differential packet filtering)* ενάντια των επιθέσεων πλημμύρας DDoS. Σύμφωνα με αυτή την προσέγγιση, σε κανονικές συνθήκες κυκλοφορίας δικτύου κάθε εισερχόμενο πακέτο θεωρείται ασφαλές, "φυσιολογικό" ή επικίνδυνο σύμφωνα με ένα συνεχώς ανανεούμενο πίνακα ιστορικού έμπιστων πηγών IP. Όταν ανιχνεύεται μία επίθεση, απορρίπτονται κάποια "ύποπτα" πακέτα IP απορρίπτονται ενώ κάποιες ασφαλείς και υποβαθμίζονται φυσιολογικές διευθύνσεις IP. Η μέθοδος που προτείνουν οι Tanachaiwiwat και άλλοι βασίζεται σε πιθανοτικά μέσα προκειμένου να προσδιορίσουν τα επικίνδυνα πακέτα, κάτι που πιθανώς να οδηγήσει σε απόρριψη νόμιμης κυκλοφορίας, αλλά η μέθοδος αυτή είναι προσαρμόσιμη στις αλλαγές κυκλοφορίας και στις προσπάθειες διατήρησης της ποιότητας υπηρεσιών.

Σε αντίθεση με τις άλλες μεθόδους προστασίας από επιθέσεις DDoS που χρησιμοποιούν μία πιθανοτική προσέγγιση προκειμένου να ανιχνεύσουν τη μη-νόμιμη κυκλοφορία, το *StackPi* [Perrig, 2003] είναι μία μέθοδος που στοχεύει στον περιορισμό της κακόβουλης κυκλοφορίας σημειώνοντας τα πακέτα ντετερμινιστικά ανιχνεύοντας τις παραποιημένες διευθύνσεις IP. Το StackPi αποτελείται από δύο τμήματα: τη σημείωση και το φιλτράρισμα πακέτων. Η σημείωση πακέτων περιλαμβάνει τη συνένωση της συνάρτησης κατακερματισμού MD5 της διεύθυνσης IP του επόμενου κόμβου με τη διεύθυνση IP του τρέχοντος κόμβου. Το αποτέλεσμα υπολογίζεται σε κάθε δρομολογητή και τοποθετείται στο πεδίο αναγνώρισης IP της επικεφαλίδας IP, όπου οι νέες τιμές αντικαθιστούν τις παλιές όταν χρησιμοποιούνται πλήρως τα 16 bit του δικτύου χρησιμοποιούνται πλήρως. Κατά αυτόν τον τρόπο, επιτυγχάνεται μία μοναδική σημείωση για κάθε ζευγάρι <πηγής, προορισμού>, το οποίο αποθηκεύεται σε ένα πίνακα στον ακραίο κόμβο (endhost). Συγχρόνως, η μέθοδος φιλτραρίσματος είναι υπεύθυνη για την ανίχνευση κακόβουλης κυκλοφορίας χρησιμοποιώντας τη μέθοδο σημείωσης. Με άλλα λόγια, η πρόσβαση επιτρέπεται εάν η σημείωση ταιριάζει με μία εγγραφή στη βάση δεδομένων που έχει δημιουργηθεί, διαφορετικά δεν επιτρέπεται.

Οι Jin και άλλοι [Jin, 2003] πρότειναν την προσέγγιση *φιλτραρίσματος με βάση τον αριθμό βημάτων (hop-count filtering)*. Πρόκειται για μία μέθοδο που βασίζεται στο γεγονός ότι ο αριθμός των βημάτων από την πηγή έως τον προορισμό υποδηλώνεται έμμεσα από το πεδίο χρόνου ζωής (Time To Live (TTL)) σε ένα πακέτο IP. Συνδέοντας την διεύθυνση πηγής IP με το στατιστικό αριθμό των βημάτων που απαιτούνται προκειμένου ένα πακέτο να φτάσει στον προορισμό του μπορεί να εκτιμηθεί η αυθεντικότητα της ισχυριζόμενης διεύθυνσης πηγής IP. Σε κανονική λειτουργία, ο αριθμός βημάτων υπολογίζεται από την τιμή TTL στην επικεφαλίδα IP και αποθηκεύεται σε έναν πίνακα με την αντίστοιχη διεύθυνση IP. Όταν ανιχνεύεται μία επίθεση, ένα λαμβανόμενο πακέτο IP απορρίπτεται εάν υπάρχει σημαντική ασυμφωνία

ανάμεσα στον αριθμό βημάτων και την τιμή που έχει προηγουμένως αποθηκευθεί στον υπάρχοντα πίνακα. Αυτή η διαδικασία εξαρτάται σημαντικά από υποθέσεις και πιθανοτικές μεθόδους, που καθιστούν τη μέθοδο ανακριβή. Επιπλέον, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν διευθύνσεις με συναφή αριθμό βημάτων, καθιστώντας αυτή τη στρατηγική προστασίας μη αποτελεσματική.

Το *ευφυές φιλτράρισμα πακέτων που βασίζεται σε ιχνηλάτηση IP (IP traceback-based intelligent packet filtering)* [Sung, 2002] προτείνει ένα προνομιακό φιλτράρισμα προκειμένου να φιλτραριστούν πακέτα που πιθανόν να ανήκουν σε κακόβουλη κίνηση. Η μέθοδος αυτή βασίζεται στο γεγονός ότι πακέτα επίθεσης που προέρχονται από την ίδια πηγή είναι πιο πιθανό να διασχίσουν το ίδιο μονοπάτι (υποθέτοντας ότι έχουμε σταθερότητα στη δρομολόγηση). Επομένως, αναγνωρίζοντας ένα πακέτο επίθεσης, είναι δυνατόν να φιλτράρουμε όλα τα ακόλουθα πακέτα που διασχίζουν το ίδιο μονοπάτι.

Οι Yaar και άλλοι [Yaar, 2003] πρότειναν μία μέθοδο που ονομάζεται *Αναγνώριση Μονοπατιού (Path Identification (PI))* σύμφωνα με την οποία το φιλτράρισμα πραγματοποιείται σε ακραίους υπολογιστές με ένα καθορισμένο όριο εάν τα πακέτα έχουν σημείωση που υποδηλώνει ότι προέρχονται από πηγές επίθεσης. Καθώς η σημείωση σε αυτή τη μέθοδο δεν είναι μοναδική σε κάθε μονοπάτι, το όριο φιλτραρίσματος επιτρέπει στο θύμα να περιορίσει τους λανθασμένους θετικούς συναγερμούς αυξάνοντας όμως τους λανθασμένους αρνητικούς συναγερμούς. Τόσο το *ευφυές φιλτράρισμα πακέτων που βασίζεται σε ιχνηλάτηση IP* όσο και το *PI* απαιτούν καθολική εφαρμογή προκειμένου να είναι αποτελεσματικά. Επιπλέον, επιτρέπουν στα θύματα μίας επίθεσης να κατηγοριοποιούν τα δικτυακά πακέτα βασιζόμενα στη σήμανση των πακέτων αλλά οι μέθοδοι αυτές πρέπει να συνδυαστούν με άλλες μεθόδους προκειμένου να επιτευχθεί η αναγνώριση των σημάνσεων που αναπαριστούν κυκλοφορία επίθεσης.

Η αρχιτεκτονική *Ασφαλών Υπηρεσιών Επικάλυψης (Secure Overlay Services (SOS))* [Keromytis, 2002] είναι βασικά ένα δίκτυο επικάλυψης (overlay) που αποτελείται από κόμβους οι οποίοι επικοινωνούν μεταξύ τους πάνω από το υποκείμενο δικτυακό υπόστρωμα. Αυτή η αρχιτεκτονική εφαρμόζει επαλήθευση πρόσβασης σε διάφορους κόμβους που είναι κατανεμημένοι στο Διαδίκτυο, και στη συνέχεια η αυθεντικοποιημένη κυκλοφορία προωθείται μέσω του δικτύου επικάλυψης (overlay) σε ένα μυστικό κόμβο. Επιτρέπεται η εισερχόμενη κυκλοφορία από το μυστικό κόμβο σε μία περίμετρο που περιβάλλει τον προστατευόμενο στόχο, ενώ φιλτράρεται οποιαδήποτε άλλη κυκλοφορία. Η αρχιτεκτονική SOS απαιτεί την υποστήριξη ενός δικτύου επικάλυψης. Αν και η αρχιτεκτονική SOS μπορεί θεωρητικά να φιλτράρει όλη την κακόβουλη κυκλοφορία, δημιουργεί μία σημαντική αύξηση στην καθυστέρηση κατά μήκος του μονοπατιού επικοινωνίας που εκτιμάται να είναι δέκα φορές μεγαλύτερη από την περίπτωση της άμεσης επικοινωνίας. Είναι σημαντικό να τονίσουμε ότι η αρχιτεκτονική SOS μπορεί να εφαρμοστεί μόνο

σε συστήματα κρίσιμων αποστολών, όπου η πιστοποίηση είναι προϋπόθεση για τη χρήση αυτών των συστημάτων, και τα συστήματα αυτά δεν στοχεύουν στον μετριασμό των επιθέσεων DDoS ενάντια των δημόσιων συστημάτων όπως είναι οι εξυπηρετητές ιστού.

Το κύριο μειονέκτημα που αντιμετωπίζουν οι παραπάνω προσεγγίσεις είναι ότι προκειμένου να είναι αποτελεσματικές θα πρέπει να εφαρμοστούν στο ευρύ Διαδίκτυο. Η ευρεία εφαρμογή τους είναι δύσκολο να επιτευχθεί λόγω οικονομικών, πολιτικών και διαχειριστικών λόγων ή άλλων τεχνολογικών προτιμήσεων.

Απενεργοποιώντας μη χρησιμοποιούμενες υπηρεσίες [Geng, 2000] είναι μία άλλη μέθοδος προκειμένου να παρεμποδίσουμε τις επιθέσεις DDoS. Εάν κάποιες δικτυακές υπηρεσίες δεν χρειάζονται ή δεν χρησιμοποιούνται, οι υπηρεσίες αυτές πρέπει να απενεργοποιούνται για να παρεμποδιστούν οι επιθέσεις. Για παράδειγμα, εάν η υπηρεσία ηχούς UDP δεν χρειάζεται, απενεργοποιώντας την, το σύστημα θα γίνει πιο ασφαλές απέναντι σε τέτοιες επιθέσεις.

Εφαρμόζοντας επιδιορθώσεις ασφάλειας [Geng, 2000], μπορεί να θωρακιστούν οι κόμβοι ενάντια των επιθέσεων DDoS. Οι κόμβοι πρέπει να ανανεώνονται με βάση τις τελευταίες ενημερώσεις ασφάλειας που είναι διαθέσιμες προκειμένου να περιορίσουν τις συνέπειες των επιθέσεων DDoS.

Η *αλλαγή διευθύνσεων IP* [Geng, 2000], είναι άλλη μία απλή λύση σε μία επίθεση DDoS προκειμένου να ακυρώσουν την διεύθυνση IP του υπολογιστή του θύματος αλλάζοντάς τη με μία νέα. Αυτή η τεχνική ονομάζεται *προστασία κινούμενου στόχου*. Μόλις η αλλαγή της διεύθυνσης IP ολοκληρωθεί θα ενημερωθούν όλοι οι δικτυακοί δρομολογητές και οι ακραίοι δρομολογητές θα απορρίψουν τα πακέτα επίθεσης. Παρόλα αυτά, και αυτές οι ενέργειες αφήνουν τον υπολογιστή ευπαθή καθώς ο επιτιθέμενος μπορεί να πραγματοποιήσει την επίθεση στη νέα διεύθυνση IP. Αυτή η επιλογή είναι πρακτική για τοπικές επιθέσεις DDoS, οι οποίες βασίζονται σε διευθύνσεις IP. Από την άλλη πλευρά, οι επιτιθέμενοι μπορούν να καταστήσουν αυτή την τεχνική σε μία ασήμαντη διαδικασία προσθέτοντας μία λειτουργία ανίχνευσης υπηρεσίας ονομάτων δικτυακών περιοχών (domain) στα εργαλεία επιθέσεων DDoS.

Απενεργοποιώντας τις ανοικτές εκπομπές IP [Geng, 2000], οι κόμβοι δεν μπορούν πια να χρησιμοποιηθούν σαν ανακλαστήρες σε επιθέσεις *πλημμύρας ICMP* και *Smurf*. Παρόλα αυτά, η αντιμετώπιση τέτοιων επιθέσεων μπορεί να είναι επιτυχής μόνο εάν όλα τα γειτονικά δίκτυα απενεργοποιήσουν τη δυνατότητα ανοικτής εκπομπής IP.

Η *εξισορρόπηση του φόρτου (load balancing)* [Lee, 2003] είναι μία απλή μέθοδος που ενεργοποιεί τους παρόχους δικτύου να αυξήσουν το παρεχόμενο εύρος ζώνης στις κρίσιμες συνδέσεις και να παρεμποδίσουν το ενδεχόμενο να τεθούν εκτός λειτουργίας κατά τη διάρκεια μίας επίθεσης DDoS. Επιπλέον, σε μία αρχιτεκτονική πολλαπλών εξυπηρετητών η εξισορρόπηση του φόρτου είναι

απαραίτητη έτσι ώστε τόσο η βελτίωση της κανονικής λειτουργίας όπως και η παρεμπόδιση ή ο μετριασμός του αποτελέσματος μίας επίθεσης DDoS να μπορεί να επιτευχθεί.

Τα *honeypots* [Weiler, 2002] μπορούν επίσης να χρησιμοποιηθούν προκειμένου να παρεμποδίσουν τις επιθέσεις DDoS. Τα *honeypots* είναι συστήματα τα οποία ρυθμίζονται με περιορισμένη ασφάλεια και τα οποία μπορούν να χρησιμοποιηθούν προκειμένου να παραπλανήσουν τον επιτιθέμενο να επιτεθεί στο *honeypot* και όχι στο πραγματικό σύστημα. Τα *honeypots* τυπικά μπορούν να χρησιμοποιηθούν όχι μόνο στην προστασία συστημάτων αλλά επιπλέον στην συγκέντρωση πληροφοριών για τους επιτιθέμενους αποθηκεύοντας μία εγγραφή της δραστηριότητάς τους και μαθαίνοντας τους τύπους επιθέσεων και τα εργαλεία λογισμικού που χρησιμοποιεί ο επιτιθέμενος. Η τρέχουσα έρευνα συζητά τη χρήση *honeypots* που μιμείται όλες τις πλευρές ενός νόμιμου δικτύου (όπως είναι οι εξυπηρετητές ιστού, οι εξυπηρετητές και πελάτες ηλεκτρονικού ταχυδρομείου, κ.τ.λ.) προκειμένου να προσελκύσουν τους πιθανούς επιτιθέμενους DDoS. Η ιδέα είναι να δελεάσουν τον επιτιθέμενο να πιστέψει ότι έχει καταλάβει το σύστημα (δηλαδή το *honeypot*) για επίθεση σαν υποτελή κόμβο του και να τον προσελκύσει για να εγκαταστήσει κώδικα είτε για χειριστή είτε για πράκτορα μέσα στο *honeypot*. Κάτι τέτοιο προστατεύει τα νόμιμα συστήματα από το να καταληφθούν, ανιχνεύει τη συμπεριφορά του χειριστή ή του πράκτορα και επιτρέπει στο σύστημα να κατανοήσει καλύτερα πώς να προστατευθεί ενάντια των μελλοντικών επιθέσεων DDoS. Παρόλα αυτά αυτό το σχήμα έχει πολλαπλά μειονεκτήματα. Πρώτα από όλα, η μέθοδος υποθέτει ότι η επίθεση πρέπει να είναι ανιχνεύσιμη χρησιμοποιώντας εργαλεία ανίχνευσης που βασίζονται σε υπογραφές. Εάν όχι, το πακέτο προωθείται στον προορισμό σε δίκτυα που είναι σε λειτουργία.

Αν και οι μέθοδοι προστασίας προσφέρουν μία πρώτη γραμμή προστασίας από τις επιθέσεις DDoS, χρειαζόμαστε ένα δεύτερο τείχος προστασίας, καθώς η απειλή των επιθέσεων DDoS δεν μπορεί να αντιμετωπιστεί μόνο με μηχανισμούς πρόληψης.

5.2. Ανίχνευση Εισβολών

Η ανίχνευση εισβολών είναι μία πολύ ενεργός ερευνητική περιοχή. Εφαρμόζοντας την ανίχνευση εισβολών, ένας κόμβος και ένα δίκτυο μπορούν να προστατευτούν από το να αποτελέσουν πηγή μίας δικτυακής επίθεσης καθώς και να πέσουν θύμα μίας επίθεσης DDoS. Τα συστήματα ανίχνευσης εισβολών ανιχνεύουν επιθέσεις DDoS είτε χρησιμοποιώντας "εκ των προτέρων" γνώση για τους τύπους των γνωστών επιθέσεων (υπογραφές (signatures)) είτε αναγνωρίζοντας αποκλίσεις από τις "φυσιολογικές" συμπεριφορές συστημάτων.

Η *ανίχνευση ανωμαλιών (anomaly detection)* βασίζεται στην ανίχνευση συμπεριφορών που είναι "μη-φυσιολογικές" με βάση κάποια "φυσιολογικά"

πρότυπα. Έχουν αναπτυχθεί πολλά συστήματα και προσεγγίσεις ανίχνευσης ανωμαλιών που στόχο έχουν την ανίχνευση των επιθέσεων DDoS.

Το *NOMAD* είναι ένα κλιμακωτό σύστημα παρακολούθησης που σχεδιάστηκε από τους Talpade και άλλους [Talpade, 1998]. Αυτό το σύστημα έχει τη δυνατότητα να ανιχνεύει ανωμαλίες στο δίκτυο κάνοντας στατιστική ανάλυση των πληροφοριών επικεφαλίδας των πακέτων IP. Μπορεί να χρησιμοποιηθεί για την ανίχνευση ανωμαλιών στο τοπικό δίκτυο κυκλοφορίας.

Μία άλλη μέθοδος ανίχνευσης των επιθέσεων DDoS χρησιμοποιεί τη *Πληροφοριακή Βάση Διαχείρισης (Management Information Base (MIB))* δεδομένων από δρομολογητές. Τα δεδομένα MIB από ένα δρομολογητή περιλαμβάνουν παραμέτρους που υποδηλώνουν διαφορετικά στατιστικά στοιχεία που αφορούν τα πακέτα και τη δρομολόγηση. Οι Cabrera και άλλοι [Cabrera, 2001] επικεντρώθηκαν στην αναγνώριση στατιστικών προτύπων με διαφορετικές παραμέτρους, προκειμένου να επιτύχουν την ανίχνευση επιθέσεων DDoS σε αρχικό στάδιο. Φαίνεται αρκετά υποσχόμενη η πιθανή αντιστοίχιση στατιστικών ανωμαλιών πακέτων ICMP, UDP και TCP σε συγκεκριμένες επιθέσεις DDoS. Αν και αυτή η προσέγγιση μπορεί να είναι αποτελεσματική για ελεγχόμενο φόρτο κυκλοφορίας, χρειάζεται επιπλέον να αξιολογηθεί σε ένα πραγματικό δικτυακό περιβάλλον. Αυτή η ερευνητική περιοχή μπορεί να παρέχει σημαντικές πληροφορίες και μεθόδους που μπορεί να χρησιμοποιηθούν στην αναγνώριση και το φιλτράρισμα των επιθέσεων DDoS.

Ένας μηχανισμός που ονομάζεται *δειγματοληψία και φιλτράρισμα πακέτων που ενεργοποιείται από πιθανή συμφόρηση (congestion triggered packet sampling and filtering)* προτάθηκε από τους Huang και Pullen [Huang, 2001]. Σύμφωνα με αυτή την προσέγγιση, ένα υποσύνολο απορριπτόμενων πακέτων εξαιτίας της συμφόρησης, συλλέγεται για στατιστική ανάλυση. Εάν υποδηλώνεται από τα στατιστικά αποτελέσματα μία ανωμαλία, ένα σήμα στέλνεται στον δρομολογητή για να φιλτράρει τα κακόβουλα πακέτα.

Οι Lee και Stolfo [Lee, 1998] χρησιμοποιούν *τεχνικές εξόρυξης δεδομένων* για να ανακαλύψουν πρότυπα χαρακτηριστικών του συστήματος που περιγράφουν τη συμπεριφορά προγράμματος και χρήστη και υπολογίζουν έναν ταξινομητή που μπορεί να αναγνωρίσει ανωμαλίες και εισβολές. Αυτή η μέθοδος επικεντρώνεται σε ανίχνευση εισβολών που βασίζεται σε κόμβους. Μία βελτίωση αυτής της προσέγγισης είναι ένα μοντέλο *μετα-ανίχνευσης (meta-detection)* [Lee, 1999], το οποίο χρησιμοποιεί τα αποτελέσματα από πολλαπλά μοντέλα προκειμένου να παράσχει πιο ακριβή ανίχνευση.

Οι Mirkovic και άλλοι [Mirkovic, 2002b] πρότειναν ένα σύστημα που ονομάζεται D-WARD το οποίο πραγματοποιεί ανίχνευση της προέλευσης επιθέσεων DDoS βασιζόμενοι στην ιδέα ότι οι επιθέσεις DDoS πρέπει να

σταματήσουν όσο το δυνατόν πιο κοντά στην πηγή. Το D-WARD εγκαθίσταται στους ακραίους δρομολογητές ενός δικτύου και παρακολουθεί την κυκλοφορία που στέλνεται από και προς τους εσωτερικούς κόμβους. Εάν παρατηρηθεί κάποια ασυμμετρία στους ρυθμούς με τους οποίους παράγονται τα πακέτα, από έναν εσωτερικό κόμβο, το D-WARD περιορίζει το ρυθμό των πακέτων. Το μειονέκτημα αυτής της προσέγγισης είναι ότι υπάρχει μία πιθανότητα πολλαπλών λανθασμένων θετικών συναγερμών κατά την ανίχνευση συνθηκών επίθεσης DDoS κοντά στην πηγή, λόγω της ασυμμετρίας που μπορεί να υπάρχει στον ρυθμό των πακέτων για μικρή διάρκεια, όπως για παράδειγμα για κάποιες νόμιμες ροές όπως οι ροές UDP πραγματικού χρόνου, οι οποίες παρουσιάζουν ασυμμετρία. Παρόλα αυτά, η μέθοδος D-WARD δεν μπορεί να ανιχνεύσει επιθέσεις στις οποίες οι επιτιθέμενοι συνεργάζονται μεταξύ τους και παράγουν κυκλοφορία και προς τις δύο κατευθύνσεις (δηλ. εισερχόμενη και εξερχόμενη).

Οι Gil και Poletto [Gil, 2001] προτείνουν μία ευριστική (heuristic) δομή δεδομένων (MULTOPS). Η προτεινόμενη μέθοδος θεωρώντας δεδομένη την ανίχνευση των διευθύνσεων IP που συμμετέχουν σε μία επίθεση DDoS, χρησιμοποιεί μηνύματα για να παρεμποδίσει μόνο αυτές τις συγκεκριμένες διευθύνσεις. Κάθε συσκευή Διαδικτύου διατηρεί ένα δέντρο πολλαπλών επιπέδων που περιέχει στατιστικά στοιχεία για το ρυθμό των πακέτων και για προθέματα υποδικτύων σε διαφορετικά συγκεντρωτικά επίπεδα. Το MULTOPS χρησιμοποιεί δυσανάλογους ρυθμούς από και προς κόμβους και υποδίκτυα για να ανιχνεύσει επιθέσεις. Όταν αποθηκεύει τα στατιστικά στοιχεία που βασίζονται σε διευθύνσεις πηγής θεωρείται ότι λειτουργεί με μέθοδο κατευθυνόμενη προς την επίθεση, διαφορετικά με μέθοδο κατευθυνόμενη προς το θύμα. Μπορεί επομένως να χρησιμοποιηθεί μία δομή δεδομένων MULTOPS για να κρατά τα ίχνη των επιτιθέμενων κόμβων ή των κόμβων που δέχονται επίθεση. Όταν ο ρυθμός πακέτων από και προς ένα υποδίκτυο φτάνει ένα συγκεκριμένο όριο, δημιουργείται ένας νέος υποκόμβος για να κρατά τα ίχνη ρυθμών πακέτων με μεγαλύτερη ευκρίνεια. Αυτή η διαδικασία μπορεί να συνεχιστεί εφόσον διατηρούνται οι ρυθμοί πακέτων για κάθε διεύθυνση IP. Επομένως, ξεκινώντας κάποιος από μικρά δείγματα μπορεί να ανιχνεύσει με αυξανόμενη ακρίβεια, τις ακριβείς διευθύνσεις πηγής ή προορισμού της επίθεσης. Οι διευθύνσεις πηγής IP που λαμβάνονται μπορεί να είναι παραποιημένες διευθύνσεις αλλά είναι ακόμα πολύτιμες προκειμένου να εφαρμοστεί ένα όριο στο ρυθμό των πακέτων. Μεταξύ των μειονεκτημάτων αυτής της προσέγγισης, περιλαμβάνεται η απαίτηση για επαναρρύθμιση του δρομολογητή και νέων σχημάτων διαχείρισης μνήμης. Επιπλέον, δεν μπορεί να παρεμποδίσει κλιμακωτές επιθέσεις ούτε μπορεί να ανιχνεύσει παραποιημένες διευθύνσεις IP που έχουν δημιουργηθεί με τυχαίο τρόπο και προέρχονται από μία μηχανή ή από επιθέσεις DDoS οι οποίες χρησιμοποιούν πολλούς πράκτορες.

Οι Onut και άλλοι [Onut, 2007] πρότειναν μία προσέγγιση δικτυακής απεικόνισης, που συνδυάζει την ανίχνευση ανωμαλιών με τους *αλγόριθμους γραφημάτων* προκειμένου να επιτευχθεί *οπτική ανίχνευση εισβολών*. Η προτεινόμενη μέθοδος *(SVision)* δημιουργεί μία οπτική αναπαράσταση των κόμβων του δικτύου, οι οποίοι ομαδοποιούνται γραφικά ανάλογα με τις υπηρεσίες που χρησιμοποιούν. Κατά αυτό τον τρόπο, οι κόμβοι μπορούν να ταξινομηθούν σε ομάδες "φυσιολογικών" και "μη-φυσιολογικών" κόμβων ανάλογα με τις υπηρεσίες που χρησιμοποιούν, δίνοντας έμφαση στις ομάδες κόμβων που μπορούν να αποτελούν απειλή για το Διαδίκτυο. Το σύνολο των υπηρεσιών μπορεί να επιλεχθεί από το διαχειριστή του δικτύου και μπορεί να ποικίλει από δίκτυο σε δίκτυο.

Η *ανίχνευση κακής χρήσης (misuse detection)* χρησιμοποιεί εκ των προτέρων γνώση για τις εισβολές προσπαθώντας να ανιχνεύσει επιθέσεις με βάση συγκεκριμένα πρότυπα ή υπογραφές γνωστών επιθέσεων. Αυτά τα πρότυπα έχουν οριστεί σαν υπογραφές εισβολών. Τα πρότυπα εισβολών μπορεί να είναι οποιοδήποτε χαρακτηριστικό πακέτο, συνθήκες, διάταξη και σχέσεις μεταξύ των γεγονότων που οδηγούν σε εισβολή ή άλλη κακή χρήση. Αν και τα συστήματα ανίχνευσης κακής χρήσης είναι πιο ακριβή στην ανίχνευση γνωστών επιθέσεων, το βασικό τους μειονέκτημα είναι ότι οι επιθέσεις είναι σε συνεχή εξέλιξη και αυτό οδηγεί στην ανάγκη για μία ενημερωμένη βάση γνώσης των επιθέσεων. Πολλά γνωστά συστήματα παρακολούθησης δικτύων πραγματοποιούν ανίχνευση εισβολών βασιζόμενη σε υπογραφές, όπως είναι το NetRanger της Cisco [Computing, 2002], το NID [CIAC, 1997b], το SecureNet PRO [SecureNet, 2007], το RealSecure [ISS, 2007], το NFR-NID [NSS, 2007] και το Snort [Snort, 2007].

5.3 Απόκριση στις Εισβολές

Μόλις αναγνωριστεί μία επίθεση, το επόμενο βήμα είναι να αναγνωριστεί η πηγή της επίθεσης και να παρεμποδιστεί ανάλογα η κυκλοφορία. Το τμήμα της παρεμπόδισης πραγματοποιείται με χειρωνακτικό έλεγχο (π.χ. επικοινωνώντας με τους διαχειριστές των δρομολογητών στην κατεύθυνση της πηγής και ενεργοποιώντας λίστες ελέγχου πρόσβασης) καθώς ένα αυτοματοποιημένο σύστημα απόκρισης μπορεί να προκαλέσει επιπλέον μείωση της συνολικής απόδοσης σαν απόκριση σε ένα λανθασμένο συναγερμό. Υπάρχουν και τα αυτοματοποιημένα συστήματα απόκρισης σε εισβολές, αλλά εφαρμόζονται μόνο μετά από μία περίοδο αυτό-εκπαίδευσης (για αυτούς που εφαρμόζουν νευρωνικούς υπολογισμούς προκειμένου να ανακαλύψουν την τεχνική DDoS) ή δοκιμής (για αυτούς που λειτουργούν με στατικούς κανόνες). Υπάρχουν πολλές μέθοδοι που στοχεύουν στην ανίχνευση και την αναγνώριση της πραγματικής πηγής της επίθεσης.

Η *ιχνηλάτηση IP (IP traceback)* ιχνηλατεί τις επιθέσεις στην προέλευσή τους, έτσι ώστε να είναι δυνατή η εύρεση της ταυτότητας του επιτιθέμενου επιτυγχάνοντας

την ανίχνευση ασύμμετρων δρόμων, καθώς και τον χαρακτηρισμό μονοπατιών. Κάποιοι παράγοντες που καθιστούν την τεχνική της *ιχνηλασίας IP* δύσκολη είναι η μη σταθερή φύση της δρομολόγησης του Διαδικτύου και η έλλειψη απόδοσης ευθύνης στην πηγή για το πρωτόκολλο TCP/IP. Προκειμένου να είναι αποτελεσματική η *ιχνηλάτηση IP* είναι απαραίτητο να υπολογιστεί και να κατασκευαστεί το μονοπάτι της επίθεσης. Σε πολύ βασικό επίπεδο, η *ιχνηλάτηση IP* μπορεί να θεωρηθεί σαν τη χειρωνακτική διαδικασία κατά την οποία οι διαχειριστές του δικτύου που δέχεται επίθεση τηλεφωνούν στον Πάροχο Υπηρεσιών Διαδικτύου (Internet Service Provider (ISP)) ζητώντας την κατεύθυνση από την οποία έρχονται τα πακέτα. Καθώς η χειρωνακτική εύρεση της πηγής είναι πολύ κουραστική έχουν προταθεί διάφορες μέθοδοι που προσπαθούν να κάνουν αυτή τη διαδικασία αυτοματοποιημένη και ευκολότερη.

Οι μέθοδοι *ιχνηλάτησης IP* για την απόκριση σε επιθέσεις DDoS μπορούν διακριθούν σε τέσσερις κύριες κατηγορίες την *ιχνηλάτηση IP που βασίζεται στη σημείωση πακέτων (Packet Marking-based)* [Al-Duwairi, 2005], την *ιχνηλάτηση IP που βασίζεται στην καταγραφή πακέτων (Packet Logging-based)* [Al-Duwairi, 2005], τις *υβριδικές προσεγγίσεις* που συνδυάζουν τη σημείωση και την καταγραφή πακέτων προκειμένου να πραγματοποιηθεί *ιχνηλάτηση IP* και τέλος την *ιχνηλάτηση IP που βασίζεται στην οργάνωση και διακίνηση δικτυακής κυκλοφορίας (Traffic Engineering-based)* [Al-Duwairi, 2005].

Η βασική ιδέα της *σήμανσης πακέτων (packet marking)* είναι ότι οι δρομολογητές στο μονοπάτι από τις πηγές επίθεσης έως τα θύματα προσθέτουν σημάδια (marks) στο πεδίο αναγνώρισης IP του κινούμενου πακέτου. Τα θύματα διακρίνουν τα πακέτα επίθεσης από τα νόμιμα πακέτα βασιζόμενα στα σημάδια (marks) των πακέτων. Το πρόβλημα είναι ότι το πεδίο αναγνώρισης IP είναι μόνο 16 bit, μέγεθος που δεν είναι αρκετό για την αποθήκευση ολόκληρου του μονοπατιού (το μέσο μήκος του μονοπατιού είναι κατά προσέγγιση 15) [Yaar, 2003]. Συγκεκριμένα σχήματα κωδικοποίησης πρέπει να εφαρμοστούν προκειμένου να μειωθεί το μήκος των σημαδιών. Αφού τα τρέχοντα σχήματα κωδικοποίησης δεν έχουν την ικανότητα να αντιστοιχήσουν κάθε σημάδι σε ένα μοναδικό μονοπάτι, νόμιμα πακέτα θα αντιμετωπίζονται σαν πακέτα επίθεσης αν έχουν διασχίσει το μονοπάτι κωδικοποιημένα με το ίδιο σημάδι όπως το μονοπάτι που διέσχισαν τα πακέτα επίθεσης.

Η *πιθανοτική σήμανση πακέτων (probabilistic packet marking (PPM))* περιγράφει αποτελεσματικούς τρόπους για την κωδικοποίηση πληροφοριών τμημάτων μονοπατιών δρομολόγησης, περιλαμβάνοντας δεδομένα ιχνηλάτησης σε πακέτα IP. Είναι μία προσέγγιση που μπορεί να εφαρμοστεί κατά τη διάρκεια ή μετά από μία επίθεση και δεν απαιτεί επιπλέον κυκλοφορία δικτύου, αποθήκευση δρομολογητή ή αύξηση του μεγέθους του πακέτου. Αν και δεν είναι αδύνατο να επανα-κατασκευάσουμε ένα διατεταγμένο μονοπάτι δικτύου χρησιμοποιώντας μία μη διατεταγμένη συλλογή από δείγματα δρομολογητών, απαιτείται από το θύμα η λήψη ενός μεγάλου αριθμού πακέτων. Το

πλεονέκτημα αυτής της προσέγγισης είναι ότι δεν παράγεται επιπλέον κυκλοφορία, αφού υπάρχει περιορισμός στα πακέτα. Επιπλέον, δεν υπάρχει αλληλεπίδραση με τους παρόχους υπηρεσιών Διαδικτύου και αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί για να ακολουθήσει τα ίχνη μίας επίθεσης αφού αυτή έχει πραγματοποιηθεί.

Σύμφωνα με αυτή τη μέθοδο, οι δρομολογητές πραγματοποιούν *πιθανοτική σήμανση* στα προωθούμενα πακέτα. Για αυτό το σκοπό, φυλάσσονται τρία πεδία σήμανσης σε κάθε πακέτο: η αρχή, το τέλος και η απόσταση. Το σχήμα αυτό σχεδιάστηκε έτσι ώστε σε κάθε κόμβο κατά μήκος του μονοπατιού του πακέτου, το πεδίο απόστασης να αναπαριστά τον αριθμό των βημάτων ανάμεσα στον προορισμό όπως ορίζεται στο ζεύγος (αρχή, τέλος) και το συγκεκριμένο κόμβο. Με άλλα λόγια, εάν ένα πακέτο φτάσει στον προορισμό του με τα πεδία σήμανσης (αρχή, τέλος, απόσταση) να έχουν τεθεί ως (x,y,d) αντίστοιχα υποδηλώνεται ότι το πακέτο προωθήθηκε μεταξύ των άκρων (x,y) που είναι d βήματα μακριά. Η διαδικασία σημείωσης πραγματοποιείται στους δρομολογητές του Διαδικτύου ως εξής: εάν ένας δρομολογητής αποφασίσει να σημειώσει ένα πακέτο σύμφωνα με μία συγκεκριμένη πιθανότητα, q, χρησιμοποιεί την διεύθυνση του IP στο πεδίο αρχής και αρχικοποιεί το πεδίο απόστασης θέτοντας το ίσο με μηδέν. Διαφορετικά, εάν το πεδίο απόστασης είναι ίσο με μηδέν γράφει την διεύθυνση IP του στο πεδίο τέλους και αυξάνει το πεδίο απόστασης.

Μόλις ανιχνευθεί μία επίθεση από το θύμα, πρέπει να συλλέξει ένα σημαντικό αριθμό πακέτων επίθεσης και να εξάγει πληροφορίες σημείωσης (π.χ. τα ακραία σημεία και την απόστασή τους) από αυτά. Στη συνέχεια συνδυάζει τις πληροφορίες αυτές ώστε να ανακατασκευάσει το μονοπάτι επίθεσης (ή το δέντρο επίθεσης εάν συμμετέχουν πολλαπλοί επιτιθέμενοι). Αυτή η προσέγγιση απαιτεί 64 bit για τα πεδία αρχής και τέλους και 8 bit για το πεδίο απόστασης. Επομένως, συνολικά 72 bit πρέπει να δεσμευτούν σε κάθε πακέτο προκειμένου να χρησιμοποιηθούν στη διαδικασία σήμανσης. Με στόχο την αντιμετώπιση αυτού του μη-πρακτικού περιορισμού, οι Savage και άλλοι [Savage, 2001] πρότειναν ένα σχήμα κωδικοποίησης που μειώνει τις απαιτήσεις σήμανσης σε 16 bit. Εκτός από το γεγονός ότι η μέθοδος PPM δεν είναι απρόσβλητη από την παραποίηση των πεδίων σήμανσης [Park, 2001b], υπάρχουν πολλά προβλήματα που σχετίζονται με την κωδικοποίηση των πληροφοριών σήμανσης μεταξύ, των οποίων περιλαμβάνονται η απαίτηση τεράστιου αριθμού πακέτων επίθεσης προκειμένου να πραγματοποιηθεί η διαδικασία ανακατασκευής μονοπατιών (ή δέντρου), η μεγάλη επιβάρυνση που δημιουργείται προκειμένου να αριθμήσει και να συνδυάσει ένα σημαντικό αριθμό τμημάτων διευθύνσεων IP καθώς και το υψηλό ποσοστό λανθασμένων συναγερμών στην περίπτωση πολλαπλών επιτιθέμενων.

Επιπλέον, υπάρχει ένα μειονέκτημα ασυμβατότητας καθώς η σήμανση IP στο πεδίο ταυτότητας (ID) έρχεται σε σύγκρουση με το IPsec [Kent, 1998] στο οποίο η Επικεφαλίδα Πιστοποίησης (Authentication Header) κρυπτογραφεί

την επικεφαλίδα αναγνώρισης. Επιπλέον, η *πιθανοτική σήμανση πακέτων* απαιτεί τροποποιήσεις στις συσκευές δρομολόγησης προκειμένου να παράγει τέτοια σημάδια σε πραγματικό χρόνο. Αυτή η προσέγγιση δεν είναι αποτελεσματική ενάντια ενός κατειλημμένου δρομολογητή. Οι Ioannidis και Bellovin [Ioannidis, 2002] διαφωνούν στο ότι ακόμα και εάν αναγνωριστεί το μονοπάτι επίθεσης, δεν είναι ξεκάθαρο ποια είναι τα επόμενα βήματα που πρέπει να ακολουθηθούν.

Πολλές άλλες μέθοδοι (π.χ., [Song, 2001], [Dean, 2001], [Goodrich, 2002]) προτάθηκαν προκειμένου να αυξήσουν την απόδοση και τη λειτουργικότητα του *PPM*. Οι Song και Perrig [Song, 2001] βελτίωσαν την απόδοση του *PPM* και πρότειναν τη χρήση των αλυσίδων κατακερματισμού προκειμένου να πιστοποιούνται οι δρομολογητές. Χρησιμοποιούν ένα πεδίο απόστασης με 5 bit, αλλά δεν τεμαχίζουν τα μηνύματα του δρομολογητή. Αυτή η μέθοδος είναι αποτελεσματική και ακριβής ακόμα και όταν πραγματοποιούνται πολλές επιθέσεις DDoS και χρησιμοποιεί ένα έξυπνο σχήμα κωδικοποίησης προκειμένου να μειωθούν οι απαιτήσεις αποθήκευσης. Από την άλλη πλευρά, αυτός ο μηχανισμός υποθέτει ότι το θύμα έχει ένα χάρτη των δρομολογητών στην κατεύθυνση της πηγής προς όλους τους επιτιθέμενους και η αυξανόμενη εφαρμογή του δεν υποστηρίζεται.

Οι Dean και άλλοι [Dean, 2002] εισήγαγαν μία ενδιαφέρουσα αλγεβραϊκή προσέγγιση στη μέθοδο του *PPM*. Αυτό το σχήμα δεν απαιτεί ένα χάρτη για το δρομολογητή στην κατεύθυνση της πηγής προκειμένου να κατασκευάσουν ένα μονοπάτι επίθεσης. Αλλά όπως και η προσέγγιση *PPM* [Savage, 2001], αυτή η μέθοδος μοιράζεται παρόμοια προβλήματα ασυμβατότητας με προηγούμενες εκδόσεις και είναι λιγότερο αποτελεσματική υπό την παρουσία πολλαπλών επιτιθέμενων.

Οι Goodrich και άλλοι [Goodrich, 2002] πρότειναν μία μέθοδο σήμανσης που σημειώνει κόμβους και όχι συνδέσμους μέσα στα πακέτα. Καθώς αυτή η προσέγγιση δεν χρησιμοποιεί το πεδίο απόστασης, παρουσιάζει προβλήματα στην ανακατασκευή του γραφήματος και δεν μπορεί να επεκταθεί σε περιπτώσεις με μεγάλο αριθμό επιτιθέμενων.

Επιπρόσθετα, στον παραπάνω αλγόριθμο σήμανσης πακέτων, οι Adler και άλλοι [Adler, 2002] και Park και Lee [Park, 2001b] μελέτησαν παραλλαγές για διάφορες παραμέτρους του *PPM*. Οι Adler και άλλοι [Adler, 2002] παρουσιάζουν μία θεωρητική ανάλυση της ιχνηλάτησης, παρουσιάζοντας μία μέθοδο σήμανσης ενός bit. Αυτή η προσέγγιση είναι κυρίως θεωρητικού ενδιαφέροντος και δεν μπορεί να επεκταθεί σε μεγάλο αριθμό επιτιθέμενων. Οι Park και Lee [Park, 2001b] πρότειναν να χρησιμοποιήσουν κατανεμημένα φίλτρα στους δρομολογητές και να φιλτράρουν τα πακέτα σύμφωνα με την τοπολογία του δικτύου. Αυτό το σχήμα μπορεί να σταματήσει την πλαστή κυκλοφορία σε πρώτο στάδιο. Παρόλα αυτά, προκειμένου να είναι αποτελεσματικό, είναι απαραίτητο να γνωρίζουμε την τοπολογία του Διαδικτύου και την πολιτική δρομολόγησης ανάμεσα στα Αυτόνομα

Συστήματα, κάτι το οποίο είναι δύσκολο να επιτευχθεί στο επεκτεινόμενο Διαδίκτυο.

Οι Liu και άλλοι [Liu, 2007] πρότειναν μία προσέγγιση που ονομάζεται *δυναμική πιθανοτική σήμανση πακέτων (Dynamic Probabilistic Packet Marking (DPPM))*, προκειμένου να βελτιώσει την αποτελεσματικότητα της μεθόδου PPM. Η διαφορά τους εστιάζεται στο γεγονός ότι οι Liu και άλλοι δεν χρησιμοποιούν μία καθορισμένη πιθανότητα σήμανσης, αλλά προτείνουν να εκτιμήσουν την απόσταση που θα διασχίσει ένα πακέτο και στη συνέχεια να επιλέξουν την κατάλληλη πιθανότητα σήμανσης. Η μέθοδος DPPM μπορεί να επιτρέψει την εύρεση της πηγής της επίθεσης με ακρίβεια ακόμα και στην περίπτωση που ο επιτιθέμενος χρησιμοποιεί παραποιημένες διευθύνσεις IP.

Αν και πραγματοποιήθηκαν πολλές βελτιώσεις, αυτές οι μέθοδοι παρουσιάζουν ακόμα πολλά από τα προβλήματα που κληρονομήθηκαν από την αρχική μέθοδο PPM, όπως η απαίτηση ύπαρξης μεγάλου αριθμού πακέτων και το πρόβλημα της παραποίησης των πεδίων σήμανσης.

Μία άλλη προσέγγιση σήμανσης πακέτων είναι η προσέγγιση η οποία υιοθετήθηκε από τη μέθοδο *ντετερμινιστικής σήμανσης πακέτων (Deterministic Packet Marking (DPM))* ([Belenky, 2003a], [Belenky, 2003b]). Σύμφωνα με αυτή την προσέγγιση, η σήμανση πακέτων πραγματοποιείται μόνο σε ένα ακραίο δρομολογητή εισερχόμενης κυκλοφορίας που βρίσκεται κοντά στην πηγή. Η μέθοδος αυτή όμως συνοδεύεται με κάποιες αδυναμίες που παρουσιάζει το *φιλτράρισμα εισόδου* ειδικά όσον αφορά στην εφαρμογή του.

Αυτοί οι μηχανισμοί ιχνηλάτησης απαιτούν από τα θύματα των επιθέσεων τη συλλογή χιλιάδων πακέτων για να ανακατασκευάσουν ένα μονοπάτι επίθεσης και δεν μπορούν να επεκταθούν σε μεγάλες επιθέσεις DDoS. Προκειμένου να αντιμετωπιστούν αυτά τα μειονεκτήματα οι Yaar και άλλοι [Yaar, 2005] πρότειναν μία νέα μέθοδο σημείωσης πακέτων που ονομάζεται *γρήγορη ιχνηλάτηση Διαδικτύου (Fast Internet Traceback (FIT))* η οποία βελτιώνει σημαντικά την ιχνηλάτηση IP σε πολλαπλές διαστάσεις. Πρώτα από όλα τα θύματα μπορούν να αναγνωρίσουν τα μονοπάτια επίθεσης με μεγάλη πιθανότητα αφού λάβουν μόνο δεκάδες πακέτων. Επιτυγχάνεται λοιπόν μία μείωση 1-3 φορές στον αριθμό των απαιτούμενων πακέτων που απαιτούνται για την αναγνώριση μονοπατιών επίθεσης, σε σύγκριση με τις προηγούμενες μεθόδους σημείωσης πακέτων. Επιπλέον, η μέθοδος *FIT* μπορεί να επεκταθεί σε μεγάλες κατανεμημένες επιθέσεις με χιλιάδες επιτιθέμενους. Τα κύρια πλεονεκτήματα της μεθόδου *FIT* είναι η μέθοδος στην οποία στηρίζεται προκειμένου να ανακατασκευάσει το χάρτη του δρομολογητή και ο γρήγορος μηχανισμός που χρησιμοποιεί για την αναγνώριση του δρομολογητή σήμανσης.

Οι Chen [Chen, 2006] και άλλοι πρότειναν μία νέα μέθοδο ιχνηλάτησης IP που ονομάζεται *Σήμανση Διεπαφής Δρομολογητή (Router Interface Marking (RIM))*. Η μέθοδος αυτή σε αντίθεση με τις άλλες μεθόδους *PPM* που θεωρούν

τον ίδιο τον δρομολογητή σαν ατομική μονάδα ιχνηλάτησης, χρησιμοποιεί τη διεπαφή του δρομολογητή σαν ατομική μονάδα ιχνηλάτησης. Αυτό το βασικό χαρακτηριστικό διαφοροποίησης της μεθόδου *RIM* από τις άλλες μεθόδους *PPM* συνοδεύεται και από άλλα πλεονεκτήματα μεταξύ των οποίων περιλαμβάνονται (1) η συλλογή ενός σχετικά μικρού αριθμού σημειωμένων πακέτων προκειμένου να εκτελεστεί ιχνηλάτηση, (2) η υποστήριξη της ιχνηλάτησης τελευταίου βήματος, (3) ο μικρός αριθμός λανθασμένων αρνητικών συναγερμών και (4) η δυνατότητα εισαγωγής στη μέθοδο *RIM* νέων μηχανισμών για την αντιμετώπιση πλαστογράφησης πεδίων σημείωσης.

Σαν μία εναλλακτική λύση της εγγραφής πληροφοριών σημείωσης μέσα στα πακέτα IP, ο Bellovin [Bellovin, 2000] πρότεινε την εγγραφή των πληροφοριών σημείωσης σε ξεχωριστά πακέτα ιχνηλάτησης ICMP με τη μέθοδο *ιχνηλάτησης ICMP (ICMP traceback)*. Σε αυτή τη μέθοδο, κάθε δρομολογητής αποφασίζει με μία πιθανότητα q, να στείλει ένα επιπρόσθετο μήνυμα ICMP για ένα προωθημένο πακέτο προς τον προορισμό παρά να συμπεριλάβει πληροφορίες σημείωσης μέσα στο ίδιο το πακέτο. Εάν συγκεντρωθούν αρκετά μηνύματα ιχνηλάτησης συγκεντρωθούν στο θύμα, μπορεί να εντοπιστεί η πηγή της κυκλοφορίας δημιουργώντας μία αλυσίδα μηνυμάτων ιχνηλάτησης. Ένα σημαντικό θέμα αυτής της μεθόδου είναι η επικύρωση των μηνυμάτων ιχνηλάτησης. Αν και η απαίτηση της *Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure (PKI))* παρεμποδίζει τους επιτιθέμενους από την παραγωγή λανθασμένων μηνυμάτων *ιχνηλάτησης ICMP*, είναι απίθανο ότι κάθε δρομολογητής θα υλοποιήσει ένα σχήμα που βασίζεται σε πιστοποιητικά. Επιπλέον, η κυκλοφορία ICMP παράγει επιπλέον δικτυακή κυκλοφορία ακόμα και όταν δεν πραγματοποιείται επίθεση DoS.

Προκειμένου να αντιμετωπιστεί το θέμα της αυξημένης δικτυακής κυκλοφορίας που δημιουργεί η ιχνηλάτηση ICMP προτάθηκε η *ιχνηλάτηση ICMP που καθορίζεται από την πρόθεση (intention driven ICMP traceback (iTrace))* [Mankin, 2001], σύμφωνα με την οποία τα μηνύματα ιχνηλάτησης ICMP εκπέμπονται μόνο προς προορισμούς που έχουν εκδηλώσει ενδιαφέρον λήψης τέτοιων μηνυμάτων. Προκειμένου να επιτευχθεί αυτή η λειτουργία, η μέθοδος *iTrace* προτείνει την ανταλλαγή πληροφοριών δρομολόγησης BGP (Border Gateway Protocol) σαν μέσο για τη διανομή του ενδιαφέροντος του συστήματος για τη λήψη μηνυμάτων *ιχνηλάτησης ICMP*.

Μία παρόμοια μέθοδος που ονομάζεται *προσωρινή αποθήκευση και συνάθροιση πληροφοριών μονοπατιού (Path Information Caching and Aggregation (PICA))* προτάθηκε από τους Hsu και άλλους [Hsu, 2003]. Η κύρια διαφοροποίηση αυτής της μεθόδου βασίζεται στο γεγονός ότι η δημιουργία πακέτων καθορίζεται από τον δρομολογητή και όχι από τον προορισμό. Η μέθοδος αυτή έχει το πλεονέκτημα ενεργοποίησης μηνυμάτων ιχνηλάτησης μόνο όταν το άθροισμα των πακέτων που προορίζονται στο ίδιο υποδίκτυο ξεπερνά ένα συγκεκριμένο όριο κατά τη διάρκεια ενός καθορισμένου χρονικού διαστήματος. Το κύριο πρόβλημα που παρουσιάζει η μέθοδος *PICA* είναι ότι

σε επιθέσεις DDoS μεγάλης κλίμακας, μπορεί να μην ξεπεραστεί ποτέ το καθορισμένο όριο, ειδικά σε δρομολογητές απομακρυσμένους από το θύμα.

Προκειμένου να αντιμετωπιστούν οι επιθέσεις DDoS που προκαλούνται από ανακλαστήρες, ο Barros [Barros, 2000] πρότεινε μία τροποποίηση των μηνυμάτων *ιχνηλάτησης ICMP*. Σε αυτή την προσέγγιση, δρομολογητές στέλνουν μηνύματα ICMP στην πηγή του πακέτου που είναι υπό επεξεργασία και όχι στον προορισμό του. Αυτή η αντίστροφη ιχνηλάτηση δίνει στο θύμα τη δυνατότητα να αναγνωρίσει τον(ους) επιτιθέμενο(ους) πράκτορα(ες) από αυτά τα πακέτα.

Η μέθοδος *καταγραφής πακέτων (packet logging)* είναι ανάλογη με αυτή της σημείωσης πακέτων με τη διαφορά ότι αντί να γράφονται πληροφορίες δρομολογητών μέσα σε πακέτα IP, οι πληροφορίες πακέτων (υπογραφές ή ακόμα και το ίδιο το πακέτο) εγγράφονται στη μνήμη του δρομολογητή. Μόλις ανιχνευθεί μία επίθεση, οι δρομολογητές καναλιού ανόδου (upstream) του θύματος ελέγχονται προκειμένου να διαπιστωθεί αν στη μνήμη τους περιλαμβάνονται πληροφορίες πακέτων ή όχι. Εάν βρεθούν πληροφορίες πακέτων σε ένα δρομολογητή, τότε ο δρομολογητής θεωρείται τμήμα του μονοπατιού επίθεσης. Προφανώς, οι κύριες προκλήσεις που παρουσιάζει η μέθοδος καταγραφής πακέτων είναι οι απαιτήσεις αποθήκευσης σε ενδιάμεσους δρομολογητές, η διατήρηση της εμπιστευτικότητας και η συλλογή πληροφοριών πακέτων από δρομολογητές Διαδικτύου.

Αυτή η προσέγγιση υιοθετήθηκε από τους Baba και άλλους [Baba, 2002], σύμφωνα με τους οποίους οι δρομολογητές καταγράφουν πληροφορίες για τα μετακινούμενα πακέτα και στη συνέχεια χρησιμοποιούν τα καταγεγραμμένα δεδομένα προκειμένου να ιχνηλατήσουν κάθε πακέτο από τον τελικό προορισμό του πίσω στην πηγή προέλευσης βήμα-βήμα. Τα κύρια προβλήματα αυτής της μεθόδου ιχνηλάτησης είναι οι υψηλές απαιτήσεις αποθήκευσης, ειδικά σε υψηλές ταχύτητες Διαδικτύου και το μεγάλο ποσοστό λανθασμένων συναγερμών.

Οι Snoeren και άλλοι [Snoeren, 2001] πρότειναν μία καινοτόμα προσέγγιση που ονομάζεται *ιχνηλάτηση που βασίζεται σε κατακερματισμό (Hash-based IP Traceback)* προκειμένου να αντιμετωπιστεί το πρόβλημα μεγάλων απαιτήσεων αποθηκευτικών πόρων. Η βασική τους ιδέα ήταν η αποθήκευση περιλήψεων (digests) πακέτων σε ένα δρομολογητή χρησιμοποιώντας μία αποτελεσματική δομή αποθήκευσης δεδομένων που είναι γνωστή σαν Bloom Filter [Bloom, 1970]. Αυτή η προσέγγιση παρέχει σημαντική μείωση στις απαιτήσεις αποθήκευσης σε κάθε δρομολογητή. Επιπλέον, διατηρεί την εμπιστευτικότητα καθώς οι περιλήψεις (digests) των πακέτων που αποθηκεύονται σε ένα δρομολογητή δεν αποκαλύπτουν το περιεχόμενό τους. Ένας σχεδιασμός υλικού προτάθηκε στο [Sanchez, 2001] προκειμένου να υποστηριχθεί η υλοποίηση αυτού του σχήματος σε μεγάλες Διαδικτυακές ταχύτητες. Τα βασικά μειονεκτήματα της *ιχνηλάτησης που βασίζεται σε κατακερματισμό* είναι ότι παρουσιάζει υψηλό φόρτο αποθήκευσης και επεξεργασίας λόγω της

ντετερμινιστικής του φύσης. Επιπλέον, η μέθοδος δεν μπορεί να εφαρμοστεί για τη λήψη και αποθήκευση πακέτων πληροφοριών από δικτυακούς δρομολογητές καθώς απαιτεί ειδικούς πόρους. Το σημαντικό μειονέκτημα, που παρουσιάζει η ιχνηλάτηση που βασίζεται σε κατακερματισμό είναι το μικρό παράθυρο χρόνου μέσω του οποίου τα πακέτα μπορούν να ιχνηλατηθούν.

Οι *υβριδικές προσεγγίσεις* χρησιμοποιούν τόσο τη *σημείωση πακέτων (packet marking)* όσο και την *καταγραφή πακέτων (packet logging)*. Καθώς χρησιμοποιούνται και οι δύο τεχνικές, η συλλογή των σημειωμένων πακέτων μπορεί να συγκλίνει (converge) γρηγορότερα σε σχέση με τις απλές μεθόδους PPM, και η επιβάρυνση υπολογισμού και αποθήκευσης μπορεί να μειωθεί σε σύγκριση με απλές μεθόδους *καταγραφής πακέτων*. Παρόλα αυτά, ακόμα και οι υβριδικές μέθοδοι παρουσιάζουν μειονεκτήματα. Για παράδειγμα, η μέθοδος που προτάθηκε από τους Basheer και άλλους [Basheer, 2006] απαιτεί πρόσθετα 34 bit σε ένα πακέτο IP για τη σημείωση πακέτων (κάτι που δεν είναι πρακτικό).

Η ιχνηλάτηση IP που βασίζεται *στην οργάνωση και διακίνηση δικτυακής κυκλοφορίας* περιλαμβάνει μεθόδους οι οποίες αλλάζουν την δικτυακή κυκλοφορία με ένα ελεγχόμενο τρόπο κατά τη διάρκεια της επίθεσης.

Οι Wang και άλλοι [Wang, 2001] πρότειναν μία προσέγγιση που ονομάζεται <κοιμώμενη ιχνηλάτηση (Sleepy Traceback)> (δηλ. εφαρμογή υδατογραφήσης και ανίχνευση πακέτων στη διεύθυνση πηγής IP του επιτιθέμενου μόνο εάν το υποσύστημα IDS καθορίσει ότι μία επίθεση είναι σε εξέλιξη). Αυτό το σύστημα είναι διαφορετικό από αυτά που προαναφέρθηκαν, καθώς χρησιμοποιεί τη δυνατότητα προγραμματισμού των ενεργών κόμβων, προκειμένου να πραγματοποιήσουν απόκριση σε εισβολές. Οι κόμβοι σε ένα Ενεργό Δίκτυο (Active Network) επικοινωνούν μεταξύ τους χρησιμοποιώντας ειδικά τροποποιημένα πακέτα, τα οποία ονομάζονται "κάψουλες" και τα οποία περιέχουν κώδικα. Αυτός ο κώδικας εισάγει αποτελεσματικά μία νέα υπηρεσία (ή τροποποιεί μία υπάρχουσα) στον κόμβο που το εξετάζει. Όσο μία επίθεση είναι σε εξέλιξη, οι Ενεργοί Κόμβοι ανταλλάσσουν πληροφορίες και επαναπρογραμματίζουν τις δικτυακές συσκευές, προκειμένου να περιοριστεί η κυκλοφορία DDoS όσο το δυνατόν πιο κοντά στην πηγή. Τα Ενεργά Δίκτυα έχουν χρησιμοποιηθεί και σε άλλες προσεγγίσεις προκειμένου να προστατέψουν τα δίκτυα ενάντια των επιθέσεων DDoS. Το AEGIS [Chen, 2001] είναι ένας άλλος μηχανισμός που βασίζεται σε ενεργά δίκτυα. Η κύρια τεχνολογία σε αυτή τη προσέγγιση είναι τα Ενεργά Δίκτυα, τα οποία, όπως προαναφέρθηκε ενσωματώνουν προγραμματιστική δυνατότητα στους κόμβους του ενδιάμεσου δικτύου και επιτρέπουν στους τελικούς χρήστες να τροποποιήσουν τον τρόπο που οι δικτυακοί κόμβοι επεξεργάζονται την κυκλοφορία των δεδομένων.

Το *CenterTrack* [Stone, 2000] είναι μία αρχιτεκτονική σύμφωνα με την οποία δημιουργείται ένα δίκτυο επικάλυψης από ενθυλακώσεις IP, το οποίο συνδέει

όλους τους ακραίους δρομολογητές με τους κεντρικούς δρομολογητές ανίχνευσης. Όταν ανιχνεύεται μία επίθεση DoS, οι δρομολογητές στα ακραία σημεία του σκελετού του δικτύου καθοδηγούνται ώστε να επαναδρομολογήσουν πακέτα που κατευθύνονται στο θύμα-στόχο. Οι δρομολογητές ανίχνευσης μπορούν να αναγνωρίσουν τα σημεία εισόδου των κύριων ροών κυκλοφορίας επίθεσης. Οι ακραίοι δρομολογητές δεν χρειάζεται να υποστηρίζουν την ανίχνευση λαθών εισόδου. Από την άλλη πλευρά, υπάρχει υψηλή επιβάρυνση αποθήκευσης και επεξεργασίας λόγω της απαίτησης των ακραίων δρομολογητών να καταγράφουν πακέτα προκειμένου να αναγνωρίσουν την κυκλοφορία επίθεσης. Η τεχνική αυτή είναι εφαρμόσιμη μόνο σε επιθέσεις μεγάλης ροής.

Η *τεχνική ιχνηλάτισης ελέγχου συνδέσμου (link-testing traceback)* προτάθηκε από τους Burch και Cheswick [Burch, 2000]. Σε αυτό το σχήμα το θύμα δοκιμάζει κάθε έναν από τους εισερχόμενους συνδέσμους σαν πιθανούς συνδέσμους εισόδου για την κυκλοφορία DDoS. Με την τεχνική αυτή αποκαλύπτεται το μονοπάτι της επίθεσης, πλημμυρίζοντας τους συνδέσμους με μεγάλες ποσότητες κυκλοφορίας και εξετάζοντας εάν αυτό προκαλεί αναστάτωση στο δίκτυο. Εάν αυτό πράγματι συμβαίνει, αυτός ο σύνδεσμος είναι πιθανότατα τμήμα του μονοπατιού της επίθεσης. Αυτό το σχήμα απαιτεί σημαντική γνώση της τοπολογίας του δικτύου και δεν μπορεί να αντιμετωπίσει πολλαπλούς επιτιθέμενους. Υπάρχει επίσης μια διαφωνία ως προς το πόσο είναι δύσκολο για το θύμα να παράγει τα πακέτα για την πλημμύρα καθώς δέχεται επίθεση DDoS. Μερικοί θεωρούν ότι η ελεγχόμενη πλημμύρα σε διάφορους συνδέσμους μπορεί να αποτελεί μία επίθεση DDoS. Οι μηχανισμοί *ελέγχου συνδέσμου* λειτουργούν καλύτερα όταν υπάρχει μόνο μία επιτιθέμενη πηγή και δίνει άσχημα αποτελέσματα όταν πραγματοποιείται μία κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS) [Snort, 2007].

Το κύριο πρόβλημα αυτής της μεθόδου είναι ότι δεν είναι αποτελεσματική για πολλαπλούς επιτιθέμενους ή για επιθέσεις με ρυθμό που διακυμαίνεται. Επιπλέον, περιλαμβάνει πολλά σημεία διακλάδωσης (branch points) και δημιουργεί επιβάρυνση επικοινωνίας εξαιτίας της ανταλλαγής μηνυμάτων. Η θετική πλευρά είναι ότι αυτά τα σχήματα είναι σχήματα αντί-δρασης (reactive) με την έννοια ότι ενεργοποιούνται μόνο όταν υπάρχει μία επίθεση, κατά συνέπεια η επιβάρυνση που προκαλούν περιορίζεται στην περίοδο της επίθεσης και όχι συνεχώς. Επιπλέον, είναι συνήθως ευκολότερο να εφαρμοστούν σε σχέση με τις προσεγγίσεις σήμανσης πακέτων και καταγραφής πακέτων. Από την άλλη πλευρά, καθώς όλη η διαδικασία ιχνηλάτησης πρέπει να πραγματοποιηθεί όσο η επίθεση είναι σε εξέλιξη, δημιουργούνται μεγάλοι χρονικοί περιορισμοί στους διαχειριστές δικτύου. Από νομική πλευρά, αυτές οι προσεγγίσεις δεν μπορούν να θέσουν τους επιτιθέμενους υπόλογους, καθώς δεν συλλέγουν αποδείξεις για τα πακέτα επίθεσης και τις πηγές τους.

Η *ανάλυση των προτύπων κυκλοφορίας (Traffic Pattern Analysis)* [Lee, 2003] είναι μία άλλη μέθοδος προκειμένου να αποκριθούμε σε επιθέσεις DDoS. Κατά τη διάρκεια μίας επίθεσης DDoS, τα δεδομένα προτύπων κυκλοφορίας μπορεί να αποθηκευτούν και στη συνέχεια να αναλυθούν μετά την επίθεση προκειμένου να βρεθούν συγκεκριμένα χαρακτηριστικά που μπορεί να υποδεικνύουν την ύπαρξη μίας επίθεσης. Τα αποτελέσματα από αυτή την ανάλυση δεδομένων μπορεί να χρησιμοποιηθούν προκειμένου να ανανεώσουν την εξισορρόπηση φόρτου καθώς και στην εύρεση νέων μηχανισμών φιλτραρίσματος προκειμένου να επιτευχθεί η προστασία από επιθέσεις DDoS.

Η *ανάλυση των αρχείων καταγραφής γεγονότων (event logs)* [Lee, 2003] είναι άλλη μία καλή προσέγγιση που στόχο έχει την απόκριση στις επιθέσεις DDoS. Τα επιλεγμένα καταγεγραμμένα στοιχεία τα οποία πραγματοποιούνται κατά τη διάρκεια της έναρξης και της εκτέλεσης της επίθεσης μπορεί να χρησιμοποιηθούν, προκειμένου να ανακαλυφθεί ο τύπος των επιθέσεων DDoS που πραγματοποιήθηκε και να εφαρμοστεί μία ανάλυση σήμανσης και ψηφιακών πειστηρίων. Δικτυακός εξοπλισμός όπως τα αντι-πυρικά τείχη, οι ελεγκτές δικτυακής κίνησης (sniffers), τα καταγεγραμμένα στοιχεία των εξυπηρετητών και τα honeypot [Weiler, 2002] μπορεί να χρησιμοποιηθούν στην επιλογή των καταγεγραμμένων στοιχείων.

5.4 Ανεκτικότητα Εισβολών και Μετριασμός

Η έρευνα όσον αφορά στην ανεκτικότητα εισβολών δέχεται ότι είναι αδύνατο να παρεμποδιστεί ή να σταματήσει εντελώς μία επίθεση DDoS και, για το λόγο αυτό, επικεντρώνεται στην ελαχιστοποίηση της επίδρασης της επίθεσης και στη μεγιστοποίηση της ποιότητας των υπηρεσιών. Η ανεκτικότητα στις εισβολές μπορεί να διαχωριστεί σε δύο κατηγορίες: στην *ανεκτικότητα σε λάθη* και στην *ποιότητα υπηρεσιών (Quality of Service (QoS))*.

Η *ανεκτικότητα στα λάθη* είναι μία ερευνητική περιοχή που έχει αναπτυχθεί πολύ και της οποίας σχέδια ενσωματώνονται σε πιο κρίσιμες υποδομές εφαρμοζόμενα σε τρία επίπεδα: υλικό, λογισμικό και σύστημα [NIST, 1995]. Η ιδέα της ανεκτικότητας των λαθών είναι ότι έχοντας διπλές υπηρεσίες Διαδικτύου και διαφοροποιώντας τα σημεία πρόσβασης, το δίκτυο μπορεί να συνεχίσει να προσφέρει τις υπηρεσίες του όταν η κυκλοφορία πλημμύρας προκαλέσει συμφόρηση σε μία δικτυακή ζεύξη.

Η *ποιότητα υπηρεσίας (Quality of Service (QoS))* περιγράφει την επιβεβαίωση της ικανότητας του δικτύου να παρέχει προβλέψιμα αποτελέσματα για συγκεκριμένους τύπους εφαρμογών ή κυκλοφορίας. Έχουν αναπτυχθεί πολλές τεχνικές *ποιότητας υπηρεσιών (QoS)* και ανεκτικότητας σε εισβολές προκειμένου να μετριαστούν οι επιθέσεις DDoS.

Ανάμεσα στις *τεχνικές ποιότητας υπηρεσιών (QoS)* και ανεκτικότητας σε εισβολές οι *ολοκληρωμένες υπηρεσίες ((Integrated Services (IntServ))* και οι

διαφοροποιημένες υπηρεσίες (Differentiated (DiffServ) Services) έχουν εμφανιστεί σαν κύριες αρχιτεκτονικές [Zhao, 2000]. Οι *ολοκληρωμένες υπηρεσίες (IntServ)* χρησιμοποιούν το πρωτόκολλο εξασφάλισης πόρων (Resource Reservation Protocol (RSVP)) προκειμένου να προσδιορίσουν την τοποθεσία των πόρων κατά μήκος του μονοπατιού από το οποίο θα περάσει μία συγκεκριμένη ροή κυκλοφορίας επίθεσης. Το εύρος ζώνης της ζεύξης και ο χώρος προσωρινής μνήμης διασφαλίζονται για τη συγκεκριμένη ροή κυκλοφορίας. Η *διαφοροποίηση υπηρεσιών (Diffserv)* ([Blake, 1998], [Geoffrey, 2002]) είναι ένα πλαίσιο εργασίας διαφοροποίησης που βασίζεται σε διαχωρισμό της κίνησης σε ομαδοποιημένες κλάσεις (per-aggregate-class). Η διαφοροποίηση υπηρεσιών χρησιμοποιεί το byte τύπου υπηρεσίας (type-of-service (TOS)) στην επικεφαλίδα IP και δεσμεύει πόρους που βασίζονται στο TOS κάθε πακέτου.

Οι *τεχνικές αναμονής (queuing)* εφαρμόζονται εκτεταμένα προκειμένου να αντιμετωπίσουν τις επιθέσεις DDoS. Η πιο παλιά και ευρέως εφαρμόσιμη τεχνική ουράς αναμονής είναι η *ουρά αναμονής που βασίζεται στις κλάσεις (Class-based queuing (CBQ))*. Η *ουρά αναμονής που βασίζεται στις κλάσεις* δημιουργεί διαφορετικές ουρές κυκλοφορίας για διαφορετικούς τύπους πακέτων και για πακέτα διαφορετικών TOS. Σε κάθε μία από αυτές τις ουρές μπορεί να παραχωρηθεί ένα συγκεκριμένο ποσοστό εξερχόμενου εύρους ζώνης. Οι ουρές αναμονής που βασίζονται σε κλάσεις έχουν τη δυνατότητα να διατηρούν την ποιότητα υπηρεσιών κατά τη διάρκεια μίας επίθεσης DDoS σε ομάδες εξυπηρετητών ιστού [Karg, 2001].

Μία αρχιτεκτονική που βασίζεται στην εξασφάλιση μηχανισμών ποιότητας υπηρεσιών στους ενδιάμεσους δρομολογητές είναι τα VIPnet που προτάθηκαν από τον Brustoloni [Brustoloni, 2002]. Στα VIPnet νόμιμη κυκλοφορία θεωρείται ότι είναι η κυκλοφορία που προέρχεται από δίκτυα τα οποία υλοποιούν την υπηρεσία VIPnet. Όλη η άλλη κυκλοφορία θεωρείται χαμηλής προτεραιότητας και μπορεί να απορριφθεί στην περίπτωση μίας επίθεσης.

Μία παρόμοια προσέγγιση με τα VIPnet υιοθετήθηκε από τους Khattab και άλλους [Khattab, 2003] οι οποίοι πρότειναν μία προσέγγιση που ονομάζεται *προληπτική περιφορά εξυπηρετητή (proactive server roaming)* προκειμένου να μετριάσουν τις επιθέσεις DoS. Σύμφωνα με αυτή την προσέγγιση ο ενεργός εξυπηρετητής προληπτικά αλλάζει την τοποθεσία του μέσα σε ένα σύνολο εξυπηρετητών προκειμένου να προστατευθεί από μη προβλέψιμες και μη ανιχνεύσιμες επιθέσεις. Μόνο οι νόμιμοι πελάτες μπορούν να ανιχνεύουν τον κινούμενο εξυπηρετητή. Αυτό το περιφερόμενο σχήμα έχει ασήμαντη επιβάρυνση σε καταστάσεις που δεν υπάρχουν επιθέσεις και μπορεί να παρέχει καλή απόκριση σε περιπτώσεις επιθέσεων.

Χρησιμοποιώντας τεχνικές που εφαρμόζονται στη ρύθμιση της ποιότητας υπηρεσιών οι Garg και Reddy [Gang, 2002] πρότειναν μία προσέγγιση προστασίας από τις επιθέσεις DDoS η οποία ρυθμίζει την κατανάλωση πόρων.

Η μέθοδος αυτή ανήκει στην κατηγορία *κατάτμησης πόρων (resource accounting)*. Προτείνουν ότι η ρύθμιση πόρων μπορεί να πραγματοποιηθεί σε επίπεδο ροής, όπου κάθε ροή λαμβάνει ένα δίκαιο μερίδιο με τον ίδιο τρόπο που πραγματοποιείται ο χρονοπρογραμματισμός μέσω της εκ περιτροπής ανάθεσης (round robin) στην Κεντρική Μονάδα Επεξεργασίας (CPU). Παρόλα αυτά, είναι ακόμα δυνατό να πραγματοποιηθεί μία επίθεση DoS όταν υπάρχει ένας μεγάλος αριθμός κόμβων που συνδέονται στον εξυπηρετητή, οι οποίοι απαιτούν το μερίδιο τους στους πόρους, προκαλώντας κατά αυτό τον τρόπο έλλειψη πόρων.

Στην ίδια κατηγορία με την *κατάτμηση πόρων (resource accounting)* ανήκει μία προσέγγιση που ονομάζεται *δημιουργία εμποδίων σε πελάτες (creating client bottlenecks)*. Αυτή η μέθοδος προστασίας προσπαθεί να δημιουργήσει μία διαδικασία εμποδίων στους υπολογιστές-πράκτορες και να περιορίσει την επιθετική τους ικανότητα. Ο αλγόριθμος των RSA προβλημάτων-παιχνιδιών πελάτη (Client Puzzles) και των δοκιμών Turing απαιτούν ο πελάτης να πραγματοποιήσει κάποιους επιπλέον υπολογισμούς ή να απαντήσουν σε μία ερώτηση πριν ξεκινήσουν την πραγματοποίηση μίας σύνδεσης. Αυτό έχει σαν αποτέλεσμα να δίνεται η δυνατότητα στα συστήματα-πρακτόρων να ανιχνεύσουν τη μείωση της απόδοσης, και μπορούν πιθανότατα να σταματήσουν τη συμμετοχή τους στην αποστολή επιθετικής DDoS κυκλοφορίας. Οι Juels και Brainard [Juels, 1999] πρότειναν μία προσέγγιση με βάση την οποία ο πελάτης καλείται να επιλύσει ένα κρυπτογραφικό πρόβλημα με ποικίλη πολυπλοκότητα πριν ο εξυπηρετητής δεσμεύσει πόρους για τις αιτήσεις που δέχεται και αρχίσει να τις εξυπηρετεί. Τα κρυπτογραφικά προβλήματα που καλείται να λύσει ο πελάτης επιτρέπουν τη "σταδιακή μείωση υπηρεσιών". Όταν πραγματοποιείται μία επίθεση ο εξυπηρετητής μπορεί να αυξήσει την πολυπλοκότητα των κρυπτογραφικών προβλημάτων που καλείται να λύσει ο πελάτης πριν ο εξυπηρετητής δεχτεί την αίτηση του πελάτη και δεσμεύσει κάποιους από τους πόρους του. Το κύριο μειονέκτημα της χρήσης κρυπτογραφικών προβλημάτων είναι ότι προκειμένου ο πελάτης να λύσει τα αντίστοιχα κρυπτογραφικά προβλήματα, απαιτείται ειδικό λογισμικό. Οι Aura και άλλοι [Aura, 2000], πρότειναν μία μικρή παραλλαγή στη μέθοδο που προτάθηκε από τους Juels και Bernard. Πρότειναν βελτιώσεις στην αποτελεσματικότητα της μεθόδου μειώνοντας το μέγεθος των κρυπτογραφικών προβλημάτων και τον αριθμό των συναρτήσεων κατακερματισμού που απαιτούνται για την επιβεβαίωση των λύσεων με αποτέλεσμα την κατά προσέγγιση επίλυση των προβλημάτων.

Η *εκτίμηση πόρων* (resource pricing) είναι άλλη μία προσέγγιση που προτάθηκε από τους Maknins και άλλους, προκειμένου να μετριαστούν οι επιθέσεις DDoS. Οι Mankins και άλλοι [Mankins, 2003] σημειώνουν ότι η αποτελεσματικότητα των επιθέσεων DDoS οφείλεται σε κάποιο βαθμό στο γεγονός ότι το κόστος πέφτει σημαντικά στον εξυπηρετητή, κατά τη διάρκεια

μίας επίθεσης, με αποτέλεσμα η κυκλοφορία επίθεσης να είναι ουσιαστικά αδύνατο να διαχωριστεί από τη νόμιμη κυκλοφορία. Πρότειναν μία κατανεμημένη αρχιτεκτονική πύλης και ένα πρωτόκολλο πληρωμής που θέτει δυναμικά μεταβλητές τιμές τόσο στο δίκτυο, όσο και στον εξυπηρετητή και τους πληροφοριακούς πόρους προκειμένου να θέσει κάποιο κόστος στην έναρξη εξυπηρέτησης αιτήσεων – σε όρους νομισματικών πληρωμών ή/και υπολογιστικών βαρών – στους πελάτες που έχουν κάνει αίτηση. Εφαρμόζοντας διαφορετικές συναρτήσεις εκτίμησης και συναλλαγής, η αρχιτεκτονική αυτή μπορεί να παρέχει διαφοροποίηση στην ποιότητα υπηρεσιών και διαχωρισμό όσον αφορά στην επιθετική συμπεριφορά. Αναγνωρίζεται ένας μηχανισμός καταμερισμού προτεραιότητας στους μελλοντικούς πελάτες σαν κλειδί και τιμωρούνται οι πελάτες που προκαλούν φόρτο στον εξυπηρετητή. Το μειονέκτημα αυτής της μεθόδου είναι ότι ο κακόβουλος χρήστης μπορεί να εισβάλει στο σύστημα με παραποιημένη αίτηση σε χαμηλή τιμή, αυξάνοντας κατά αυτό τον τρόπο την τιμή για τους νόμιμους χρήστες. Προκειμένου να λυθεί αυτό το πρόβλημα, οι Mankin και άλλοι πρότειναν να διαχωρίσουν τους πόρους σε κλάσεις και να χρησιμοποιούν διαφορετικές συναρτήσεις εκτίμησης για κάθε κλάση.

Η μέθοδος *βαθμολογίας πακέτων (Packetscore)* ([Kim, 2004], [Chuah, 2004]) ενεργοποιεί κάθε ακραίο δρομολογητή ενός δικτύου ISP να υπολογίσει ένα "βαθμό" για κάθε υποπτο πακέτο και ύστερα να κατατάξει την πιθανότητα ενός πακέτου να είναι πακέτο επίθεσης, δεδομένων των τιμών των πεδίων που μεταφέρει, χρησιμοποιώντας μία προσέγγιση που βασίζεται σε Μπαϋεζιανή θεωρία. Παρόλα αυτά οι μέθοδοι μετριασμού των επιθέσεων DDoS που βασίζονται στη στατιστική έχουν πολλά μειονεκτήματα. Για παράδειγμα, τα προφίλ δικτυακής κυκλοφορίας, που διατηρούνται στο θύμα ή στους ακραίους δρομολογητές, μπορεί να τροποποιηθούν κακόβουλα πριν την έναρξη της επίθεσης και οι επιτιθέμενοι μπορούν να παράγουν πακέτα με χαρακτηριστικά που ταιριάζουν σε αυτά τα προφίλ δικτυακής κυκλοφορίας.

Διάφορες αυτόνομες αρχιτεκτονικές έχουν προταθεί για να επιδείξουν ανεκτικότητα σε εισβολές κατά τη διάρκεια επιθέσεων DDoS που επικεντρώνονται στην κατανάλωση εύρους ζώνης. Η XenoService [Yan, 2000] είναι μία υποδομή ενός κατανεμημένου δικτύου με κόμβους ιστού που ανταποκρίνονται σε μία επίθεση σε οποιαδήποτε ιστοσελίδα κατασκευάζοντας πανομοιότυπες ιστοσελίδες γρήγορα και ευρέως ανάμεσα στους εξυπηρετητές XenoService, επιτρέποντας κατά αυτόν τον τρόπο στην επιτιθέμενη ιστοσελίδα να λάμβάνει περισσότερη δικτυακή συνδεσιμότητα ώστε να απορροφηθεί η πλημμύρα. Αν και μία τέτοια αρχιτεκτονική μπορεί να επιβεβαιώσει την ποιότητα υπηρεσίας (Quality of service (QoS)) κατά τη διάρκεια των επιθέσεων DDoS, είναι αμφίβολο ότι πολλοί πάροχοι θα υιοθετήσουν μία τέτοια υποδομή γρήγορα.

Η μέθοδος *ώθησης προς τα πίσω (Pushback)* [Ioannidis, 2002], προσπαθεί να λύσει το πρόβλημα των επιθέσεων DDoS μέσα από το δίκτυο χρησιμοποιώντας το επίπεδο συμφόρησης ανάμεσα σε διαφορετικούς δρομολογητές. Όταν το επίπεδο συμφόρησης ενός συνδέσμου φτάσει ένα συγκεκριμένο όριο, ο δρομολογητής αποστολής ξεκινά την απόρριψη πακέτων και προσπαθεί να αναγνωρίσει παράνομη κυκλοφορία μετρώντας πόσες φορές απορρίπτονται τα πακέτα που έχουν μία συγκεκριμένη διεύθυνση IP προορισμού, καθώς ο επιτιθέμενος αλλάζει συνεχώς την διεύθυνση IP της πηγής. Ο δρομολογητής στη συνέχεια στέλνει ένα μήνυμα "pushback" στους δρομολογητές που τον συνδέουν με άλλους συνδέσμους που έχουν υποστεί συμφόρηση, ζητώντας τους να περιορίσουν την δικτυακή κυκλοφορία που φτάνει σε αυτόν τον προορισμό. Η μέθοδος *ώθησης προς τα πίσω* απαιτεί μία εφαρμογή μεγάλου εύρους προκειμένου να είναι αποτελεσματική. Επιπλέον, υπάρχει μεγάλη απαίτηση αποθήκευσης, έτσι ώστε να μπορούν να αναλυθούν τα απορριπτόμενα πακέτα από τον ρυθμιστή ροής και την εξωτερική ουρά.

Η *κατάπνιξη (throttling)* [Yau, 2005] είναι μία προσέγγιση μετριασμού των επιθέσεων DDoS, η οποία παρεμποδίζει τους δρομολογητές (ειδικότερα τους εξυπηρετητές ιστού) από το να διακόψουν τη λειτουργία τους. Η μέθοδος αυτή ακολουθεί την ίδια προσέγγιση με τη μέθοδο *ώθησης προς τα πίσω (pushback)*, με στόχο τη ρύθμιση των ροών επίθεσης, έτσι ώστε η ροή νόμιμης κυκλοφορίας να λάβει δίκαιο μερίδιο από τους διαθέσιμους πόρους. Αυτός ο στόχος μπορεί να επιτευχθεί εφαρμόζοντας επιλεκτικό περιορισμό του ρυθμού των εισερχόμενων ροών. Στην προσέγγιση *ρύθμισης δρομολογητών μεγίστων-ελαχίστων βασισμένων στους εξυπηρετητές (max-min fair server-centric router throttles)* εγκαθίστανται ρυθμιστικές βαλβίδες (rate throttles) σε ένα υποσύνολο των δρομολογητών ανοδικού καναλιού. Εγκαθιστώντας τέτοιου είδους βαλβίδες όλη η κυκλοφορία που περνά μέσω του δρομολογητή στην πηγή περιορίζει το ρυθμό της με βάση το ρυθμό της βαλβίδας. Αυτό το σχήμα μπορεί να διανείμει τη συνολική χωρητικότητα του εξυπηρετητή με ένα τρόπο δικαιοσύνης μέγιστου-ελάχιστου ανάμεσα στους δρομολογητές που τον εξυπηρετούν. Αυτό σημαίνει ότι μόνο οι επιθετικές ροές οι οποίες δεν σέβονται τα μερίδια ροής τιμωρούνται και όχι οι άλλες ροές. Η δυσκολία στην υλοποίηση της κατάπνιξης είναι ότι είναι ακόμα δύσκολο να διαχωρίσουμε τη νόμιμη κυκλοφορία από την κυκλοφορία επίθεσης. Στη διαδικασία κατάπνιξης, μπορεί μερικές φορές να απορριφθεί ή να καθυστερήσει νόμιμη κυκλοφορία και η κακόβουλη κυκλοφορία μπορεί να καταφέρει να περάσει από τους εξυπηρετητές.

5.5 Κατηγοριοποίηση με Βάση την Τοποθεσία Εφαρμογής

Βασιζόμενοι στην τοποθεσία της εφαρμογής διαχωρίζουμε τους μηχανισμούς προστασίας από επιθέσεις DDoS σε αυτούς που εφαρμόζονται στο θύμα, στο ενδιάμεσο δίκτυο και στο δίκτυο πηγής.

Μηχανισμοί Δικτύου Θύματος: Τα περισσότερα από τα συστήματα που δημιουργήθηκαν για την αντιμετώπιση των επιθέσεων DDoS σχεδιάστηκαν έτσι ώστε να λειτουργούν στην πλευρά του θύματος, καθώς αυτή η πλευρά δέχεται την μεγαλύτερη επίδραση της επίθεσης. Το θύμα έχει μεγαλύτερο κίνητρο να εφαρμόσει ένα σύστημα προστασίας από επιθέσεις DDoS, και ίσως θυσιάσει λίγη από την απόδοσή του και τους πόρους του προκειμένου να αυξήσει την ασφάλειά του. Παραδείγματα αυτών των συστημάτων είναι το EMERALD [Porras, 1997], η αποτίμηση πόρων (resource accounting) ([Gang, 2002], [Juels, 1999], [Zheng, 1997], [Spatscheck, 1999], [Lau, 2000]) και μηχανισμοί ασφάλειας πρωτοκόλλων ([Sterne, 2001], [Leiwo, 2000], [Meadows, 1999], [Schuba, 1997]). Όλοι αυτοί οι μηχανισμοί αυξάνουν την ικανότητα του θύματος να αναγνωρίζει ότι είναι ο στόχος της επίθεσης, και να κερδίζει περισσότερο χρόνο για να ανταποκριθεί.

Μηχανισμοί Ενδιάμεσου Δικτύου: Οι μηχανισμοί αντιμετώπισης των επιθέσεων DDoS που εφαρμόζονται στο ενδιάμεσο δίκτυο είναι πιο αποτελεσματικοί από αυτούς οι οποίοι εφαρμόζονται στο δίκτυο του θύματος καθώς η επίθεση μπορεί να αντιμετωπιστεί εύκολα και να βρεθεί η πηγή της επίθεσης. Χαρακτηριστικά παραδείγματα αυτών των μηχανισμών είναι το WATCHERS [Bradley, 1998], η ιχνηλάτηση (traceback) [Savage, 2001], [Ioannidis, 2002], [Dean, 2002], [Snoeren, 2001], [Wang, 2001]) και η ώθηση προς τα πίσω (pushback) [Ioannidis, 2002]. Παρόλα αυτά αυτοί οι μηχανισμοί προστασίας παρουσιάζουν διάφορα μειονεκτήματα τα οποία παρεμποδίζουν την ευρεία εφαρμογή τους, όπως είναι η αύξηση της απόδοσης του ενδιάμεσου δικτύου και η μεγαλύτερη δυσκολία να ανιχνευθούν επιθέσεις αφού το ενδιάμεσο δίκτυο συνήθως δεν αισθάνεται επίδραση από την επίθεση.

Μηχανισμοί Δικτύου Πηγής: Οι μηχανισμοί προστασίας DDoS που εφαρμόζονται στο δίκτυο της πηγής μπορούν να σταματήσουν τις ροές επίθεσης πριν μπουν στον πυρήνα του Διαδικτύου και πριν αθροιστούν με άλλες επιτιθέμενες. Αν οι μηχανισμοί αντιμετώπισης εφαρμόζονται κοντά στην πηγή, μπορεί να διευκολυνθεί η ιχνηλάτηση και η διερεύνηση της επίθεσης. Παραδείγματα αυτών των μηχανισμών έχουν προταθεί στα ([Gil, 2001],[Cs3, 2007],[Mirkovic, 2002b]). Ένας μηχανισμός δικτύου πηγής έχει τα ίδια μειονεκτήματα με τους μηχανισμούς ενδιάμεσου δικτύου για την ανίχνευση της ύπαρξης μίας επίθεσης. Αυτό το μειονέκτημα μπορεί να εξισορροπηθεί από την ικανότητά του να θυσιάσει μερικούς από τους πόρους του και μέρος της απόδοσής του για καλύτερη ανίχνευση της επίθεσης. Παρόλα αυτά ένα τέτοιο σύστημα μπορεί να περιορίσει τη νόμιμη κυκλοφορία στο δίκτυο σε περίπτωση που πραγματοποιηθεί μία αναξιόπιστη ανίχνευση επίθεσης.

6. Επίλογος

Αναμφισβήτητα, οι επιθέσεις DoS πρέπει να αντιμετωπιστούν σαν ένα σοβαρό πρόβλημα στο Διαδίκτυο καθώς ο μεγάλος ρυθμός ανάπτυξής τους και η ευρεία

υποδοχή τους προκαλεί το γενικό κοινό, τις δύσπιστες κυβερνήσεις και τις επιχειρήσεις. Είναι προφανές ότι το κύμα των επιθέσεων DoS θα συνεχίσει να υποτελεί μία σημαντική απειλή, καθώς όσο ανακαλύπτονται νέα μέτρα αντιμετώπισης οι επιθέσεις DoS εξελίσσονται. Αφού οι επιθέσεις DoS είναι πολύπλοκες και δύσκολο να αντιμετωπιστούν, δεν υπάρχει μοναδική λύση, όλοι είναι αδύναμοι απέναντι σε αυτή την επίθεση και όλων η ασφάλεια είναι αλληλένδετη. Μία δικτυακή υποδομή πρέπει να είναι αρκετά ισχυρή ώστε να μπορέσει να υιοθετήσει και να αγκαλιάσει νέες μεθόδους προστασίας ενάντια των εξελιγμένων και μη-προβλέψιμων μεθόδων επίθεσης.

Οι επιθέσεις DDoS είναι μία σοβαρή απειλή όχι μόνο για τα ενσύρματα δίκτυα αλλά και για τις ασύρματες υποδομές. Έχει γίνει κάποια πρόοδος προκειμένου να προστατευθούν τα ασύρματα δίκτυα από τις επιθέσεις DDoS. Οι Geng και άλλοι [Geng, 2002] πρότειναν ένα εννοιολογικό μοντέλο για την προστασία του ασύρματου Διαδικτύου από τις DDoS επιθέσεις, το οποίο ενσωματώνει τόσο συνεργάσιμες τεχνολογικές λύσεις και μηχανισμούς με οικονομικό κίνητρο, που βασίζονται σε αμοιβές με βάση τη χρήση. Επιπλέον, απαιτείται περαιτέρω ανάλυση προκειμένου να συνδυαστούν τα μειονεκτήματα όσον αφορά στην ασφάλεια των ασύρματων πρωτοκόλλων με τους μηχανισμούς προστασίας που είναι ώριμοι σε ένα ασύρματο περιβάλλον.

Βιβλιογραφία

[Adams, 1999] C. Adams, J. Gilchrist, *"The CAST-256 Encryption Algorithm, RFC 2612"*, June 1999, Available from < http://www.ietf.org/rfc/rfc2612.txt>.

[Adler, 2002] M. Adler, *"Tradeoffs in Probabilistic Packet Marking for IP Traceback"*, In Proceedings of the 34th ACM Symposium Theory of Computing (STOC), Montreal, Quebec, Canada, May 19–21, 2002, pp. 407–418.

[Al-Duwairi, 2005] B. N. Al-Duwairi, *"Mitigation and Traceback Countermeasures for DDoS attacks"*, Doctoral Dissertation, Iowa State University Ames, Iowa, 2005.

[Aura, 2000] T. Aura, P. Nikander, J. Leiwo, *"DoS-Resistant Authentication with Client Puzzles"*, In Proceedings of the 8th International Workshop on Security Protocols, Springer, New York, 2000, pp. 170–177.

[Baba, 2002] T. Baba and S. Matsuda, *"Tracing Network Attacks to their Sources"*, In Proceedings of IEEE Internet Computing, vol. 6, no. 2, pp. 20-26, 2002.

[Barlow, 2000] J. Barlow, W. Thrower, *"TFN2K—An Analysis"*, 2000, Available from <http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt>.

[Barros, 2000] C. Barros, *"A Proposal for ICMP Traceback Messages"*, Internet Draft, Available from < http://sandbox.mc.edu/~bennet/cs6523/readings.html >, Sept. 18, 2000.

[Basheer, 2006] D. Basheer and G. Manimaran, *"Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback,"* IEEE Transactions on Parallel and Distributed Systems, Vol. 17 No. 5 , May 2006, pp. 403– 418.

[Belenky, 2003a] A. Belenky and N. Ansari *"IP Traceback With Deterministic Packet Marking"*, In Proceedings of IEEE COMMUNICATIONS LETTERS, Vol. 7, No. 4, pp. 162-164, April 2003.

[Belenky, 2003b] A. Belenky and N. Ansari, *"Accommodating Fragmentation in Deterministic Packet Marking for IP Traceback"*, In Proceedings of IEEE GLOBECOM 2003, San Francisco, CA, December 2003.

[Bellovin, 1989] S. Bellovin, *"Security Problems in the TCP/IP Protocol Suite"*, Computer Communications Review 19 (2) (1989) 32–48.

[Bellovin, 2000] S. Bellovin, *"The ICMP Traceback Message"*, Network Working Group, Internet Draft, March 2000, Available from < http://tools.ietf.org/html/draft-ietf-itrace-00 >.

[Blake, 1998] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, *"An Architecture for Differentiated Services"*, In IETF, RFC 2475, 1998.

[Bloom, 1970] B. H. Bloom, *"Space/time Trade-offs in Hash Coding with Allowable Errors"*, In Proceedings of Communications of ACM, Vol. 13, No. 7, July 1970, pp. 422-426.

[Bradley, 1998] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, R.A. Olsson, *"Detecting Disruptive Routers: a Distributed Network Monitoring Approach"*, In Proceedings of the 1998 IEEE Symposium on Security and Privacy, Oakland, CA, IEEE Press, New York, 1998, pp. 115–124.

[Brenton, 2006] C. Brenton, Sans Institute, *"Egress Filtering FAQ"*, 19 April 2006, Available from <http://www.sans.org/y2k/egress.htm>.

[Brustoloni, 2002] J. Brustoloni, *"Protecting Electronic Commerce from Distributed Denial of Service Attacks"*, In Proceedings of the 11th International World Wide WebConference, ACM, Honolulu, HI, 2002, pp. 553–561.

[Bysin, 2001] Bysin, *"Knight.c Sourcecode"*, PacketStormSecurity.nl July 11, 2001, Available from <http://packetstormsecurity.nl/distributed/knight.c>.

[Burch, 2000] H. Burch, H. Cheswick, *"Tracing Anonymous Packets to their Approximate Source"*, In Proceedings of USENIX LISA (New Orleans) Conference, 2000, pp. 319–327.

[Cabrera, 2001] J.B.D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, R.K. Mehra, *"Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables—a Feasibility Study"*, In Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management, Seattle, WA, May 14–18, 2001.

[CERT, 1997] CERT Coordination Center, *"Denial of Service Attacks"*, Available from <http://www.cert.org/tech_tips/denial_of_service.html>, 1997.

[CERT, 1999] CERT Coordination Center, *"CERT Advisory CA-1999-17 Denial of Service Tools"*, Available from <http://www.cert.org/advisories/CA-1999-17.html>.

[CERT, 2001a] CERT Coordination Center, *"Trends in Denial of Service Attack Technology"*, October 2001, Available from <http://www.cert.org/archive/pdf/DoS_trends.pdf>.

[CERT, 2001b] CERT Coordination Center, *"CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL"*, Available from <http://www.cert.org/advisories/CA-2001-19.html>.

[CERT, 2001c] CERT Coordination Center, Carnegie Mellon Software Engineering Institute, *"CERT Advisory CA-2001-20 Continuing Threats to Home Users"*, 23, 2001, Available from <http://www.cert.org/advisories/CA-2001-20.html>.

[Chang, 2002] R.K.C. Chang, *"Defending Against Flooding-based, Distributed Denial of Service Attacks: a Tutorial"*, IEEE Communications Magazine 40 (10) (2002) 42–51.

[Chen, 2001] E.Y. Chen, *"AEGIS: an Active-network-powered Defense Mechanism Against DDoS Attacks"*, In Proceedings of the Third International Working Conference on Active Networks (IWAN 2001), Lecture Notes in Computer Science, Vol. 2207, Springer, Berlin, 2001, pp. 1–15.

[Chen, 2006] R. Chen, J.M. Park, R. Marchany *"RIM: Router Interface Marking for IP Traceback"*, In Proceedings of Global Telecommunications Conference 2006, Globecom 2006, 27 Nov. – 1 Dec. 2006, San Francisco, pp. 1-5.

[Chuah, 2004] M. Chuah, W. Lau, Y. Kim, J. Chao, *"Transient Performance of PacketScore for Blocking DDoS attacks"*, In Proceedings. IEEE ICC 2004, Paris, France, June 2004.

[CIAC, 1997a] CIAC, Information Bulletin, *"I-020: Cisco 7xx Password Buffer Overflow"*, Available from <http://ciac.llnl.gov/ciac/bulletins/i-020.shtml>, 1997.

[CIAC, 1997b] Computer Incident Advisory Capability, J. Donetti, S. Elko, *"Network Intrusion Detector Overview"*, Computer Security Technology Center, Lawrence Livermore National Laboratory, LLNL CSTC 97-055, Available from <http://www.ciac.org/ciac/ConferenceProceedings/DOECompSec97/nid.pdf>.

[CIAC, 2001] CIAC Information Bulletin, *"I-040: The Ramen Worm"*, 2001, Available from <http://www.ciac.org/ciac/bulletins/l-040.shtml>.

[Cisco, 1999] Cisco Systems, Inc., *"Defining Strategies to Protect Against TCP SYN Denial of Service attacks"*, 1999, Available from <http://www.cisco.com/warp/public/707/4.html>.

[Computing, 2002] Computing, D. Ludlow, Network IT Week, *"Cisco Netranger Sensor"*, 27 Mar 2002, Available from <http://www.computing.co.uk/networkitweek/software/2058440/cisco-netranger-sensor>.

[Criscuolo, 2000] P.J. Criscuolo, *"Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319"*, Department of Energy Computer Incident Advisory (CIAC), UCRL-ID-136939, Rev. 1, Lawrence Livermore National Laboratory, February 14, 2000, Available from <http://ftp.se.kde.org/pub/security/csir/ciac/ciacdocs/ciac2319.txt>.

[CSI/FBI, 2001] Computer Security Institute and Federal Bureau of Investigation, *"CSI/FBI Computer Crime and Security Survey 2001"*, CSI, March 2001, Available from <http://www.gocsi.com>.

[CS3, 2007] Creative Suite 3, *"MANAnet Reverse Firewall: Fighting DDoS Attacks at Their Origins"*, Checked June 2007, Available from < http://www.cs3-inc.com/ps_rfw.html >.

[Daemon9, 1996] Daemon9, Route, Infinity, *"IP-spoofing Demystified: Trustrelationship Exploitation"*, Phrack Magazine, Guild Productions, kid, June 1996.

[Davidowicz, 1999] D. Davidowicz, *"Domain Name System (DNS) Security"*, 1999, Available from <http://compsec101.antibozo.net/papers/dnssec/dnssec.html>.

[Dean, 2002] D. Dean, M. Franklin, A. Stubblefield, *"An Algebraic Approach to IP Traceback"*, ACM Transactions on Information and System Security 5 (2) (2002) 119–137.

[Dittrich, 1999a] D. Dittrich, *"The DoS Project's "Trinoo" Distributed Denial of Service Attack Tool"*, University of Washington, October 21, 1999, Available from <http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt>.

[Dittrich, 1999b] D. Dittrich, *"The "Stacheldraht" Distributed Denial of Service Attack Tool"*, University of Washington, December 1999, Available from <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>.

[Dittrich, 2000a] D. Dittrich, *"The Tribe Flood Network Distributed Denial of Service Attack Tool"*, University of Washington, October 21, 1999, Available from <http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt>.

[Dittrich, 2000b] D. Dittrich, G. Weaver, S. Dietrich, N. Long, *"The "mstream" Distributed Denial of Service Attack Tool"*, May 2000, Available from < http://staff.washington.edu/dittrich/misc/mstream.analysis.txt >.

[Dietrich, 2000] S. Dietrich, N. Long, D. Dittrich, *"Analyzing Distributed Denial of Service Tools: the Shaft Case"*, In Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA, December 3–8, 2000, pp. 329–339.

[Ferguson, 2000] P. Ferguson, D. Senie, *"Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing"*, RFC 2827, May 2000.

[Gang, 2002] A. Garg, A.L.N. Reddy, *"Mitigating Denial of Service Attacks Using QoS Regulation"*, In Proceedings of the Tenth IEEE International Workshop on Quality of Service, 2002, pp. 45–53.

[Geng, 2000] X. Geng, A.B. Whinston, *"Defeating Distributed Denial of Service Attacks"*, IEEE IT Professional Vol. 2 , No. 4, (2000) pp. 36–42.

[Geng, 2002] X. Geng, Y. Huang, A.B. Whinston, *"Defending Wireless Infrastructure against the Challenge of DDoS Attacks"*, Mobile Networks and Applications, Vol. 7, No. 3, (2002) pp. 213–223.

[Geoffrey, 2002] M.B. Geoffrey, G. Xie, *"A Feeedback Mechanism for Mitigating Denial of Service Attacks Against Differentiated Services Clients"*, In Proceedings of the 10th International Conference on Telecommunications systems, Monterey, CA, October 2002, pp. 204–213.

[Gil, 2001] T.M. Gil, M. Poleto, *"MULTOPS: a Data-Structure for Bandwidth Attack Detection"*, In Proceedings of 10th Usenix Security Symposium, Washington, DC, August 13–17, 2001, pp. 23–38.

[Goodrich, 2002] M. T. Goodrich, *"Efficient Packet Marking for Large-Scale IP Traceback"*, In Proceedings of ACM CCS 2002, Washington, DC, November 2002.

[Hancock, 2000] B. Hancock, *"Trinity v3, a DDoS Tool, Hits the Streets"*, Computers Security 19 (7) (2000) 574.

[Houle, 2001] K.J. Houle, G.M. Weaver, *"Trends in Denial of Service Attack Technology"*, CERT and CERT coordination center, Carnegie Mellon University, October 2001, Available from <http://www.cert.org/archive/pdf/DoS_trends.

pdf>.

[Hsu, 2003] F. Hsu and T. Chiueh, *"A Path Information Cashing and Aggregation Approach to Traffic Source Identification"*, In Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), Providence, RI, May 2003.

[Huang, 2001] Y. Huang, J.M. Pullen, *"Countering Denial of Service Attacks Using Congestion Triggered Packet Sampling and Filtering"*, In Proceedings of the 10th International Conference on Computer Communiations and Networks, 2001.

[Ioannidis, 2002] J. Ioannidis, S.M. Bellovin, *"Implementing Pushback: Router-Based Defense against DDoS Attacks"*, In Proceedings of Network and Distributed System Security Symposium, NDSS '02, San Diego, CA, 2002, pp. 6–8.

[ISS, 2007] Internet Security Systems, *"Intrusion Detection Solutions"*, Last Checked 2007, Available from <http://www.iss.net/products/product_sections /Intrusion_Detection_.html>.

[Jin, 2003] G. Jin, H. Wang, and K. G. Shin, *"Hop-count Filtering: an Effective Defense against Spoofed DDoS Traffic"*, In Proceedings of the 10th ACM conference on Computer and communication security, Washington D.C., USA, 2003.

[Juels, 1999] A. Juels, J. Brainard, *"Client Puzzles: a Cryptographic Countermeasure against Connection Depletion Attacks"*, In Proceedings of NDSS '99 (Networks and Distributed Security Systems), San Diego, CA, USA, February 1999, Internet Society, pp. 151–165.

[Kargl, 2001] F. Kargl, J. Maier, M. Weber, *"Protecting Web Servers from Distributed Denial of Service Attacks"*, In Proceedings of the Tenth International Conference on World Wide Web, Hong Kong, May 1–5, 2001, pp. 514–524.

[Karig, 2001] D. Karig, R. Lee, *"Remote Denial of Service Attacks and Countermeasures"*, Department of Electrical Engineering, Princeton University, Technical Report CE-L2001-002, October 2001.

[Kenney, 1997] Kenney, Malachi, *"Ping of Death"*, January 1997, Available from <http://www.insecure.org/sploits/ping-o-death.html>.

[Kent, 1998] S. Kent, R. Atkinson, *"Security Architecture for the Internet Protocol"*, IETF RFC2401, 1998.

[Keromytis, 2002] A. Keromytis, V. Misra, D. Rubenstein, *"SoS: Secure Overlay Services"*, In Proceedings of the ACM SIGCOMM_02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2002, pp. 61–72.

[Khattab, 2003] S.M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, T. Znati, *"Proactive Server Roaming for Mitigating Denial of Service Attacks"*, In Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE 03), Newark, NJ, August 2003, pp. 500–504.

[Kim, 2004] Y. Kim, W. Lau, M. Chuah, J. Chao, *"PacketScore: A statistical-based Overload Control against DDoS Attacks"*, In Proceedings of IEEE INFOCOM 2004, Hong Kong, China, March 2004.

[Lau, 2000] F. Lau, S.H. Rubin, M.H. Smith, Lj. Trajkovic, *"Distributed Denial of Service Attacks"*, In Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, Nashville, TN, 2000, pp. 2275–2280.

[Lee, 1998] W. Lee, S.J. Stolfo, *"Data Mining Approaches for Intrusion Detection"*, In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, January 1998, pp. 79–93.

[Lee, 1999] W. Lee, S.J. Stolfo, K.W. Mok, *"A Data Mining Framework for Building Intrusion Detection Models"*, In Proceedings of the1999 IEEE Symposium on Security and Privacy, Oakland, CA, May 9–12, 1999, pp. 120–132.

[Lee, 2003] R.B. Lee, *"Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures"*, Princeton University, Department of Electrical Engineering Princeton Architecture Laboratory for Multimedia and Security, Technical Report CE-L2003-03, May 16, 2003, Available from <http://palms.ee.princeton.edu/PALMSopen/DDoS%20Survey%20Paper_20030516_Final.pdf>

[Leiwo, 2000] J. Leiwo, P. Nikander, T. Aura, *"Towards Network Denial of Service Resistant Protocols"*, In Proceedings of the 15th International Information Security Conference (IFIP/SEC 2000), Beijing, China, Kluwer, Dordrecht, 2000.

[Li, 2002]J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, *"SAVE: Source Address Validity Enforcement Protocol"*, In Proceedings of 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOMM 2002), New York, 23-17 June 2002, Vol. 3, pp. 1557-1566.

[Liu, 2007] J. Liu, Z.-J. Lee, Y.C. Chung, *"Dynamic Probabilistic Packet Marking for Efficient IP Traceback"*, Computer Networks Vol.51, 2007, pp. 866-882.

[Lo, 1998] J. Lo et al., *"An IRC Tutorial"*, 1998, Available from <http://www.irchelp.org/irchelp/irctutorial.html#part1>.

[Mankin, 2001] A. Mankin, D. Massey, C.L. Wu, S.F. Wu, L. Zhang, *"On Design and Evaluation of "Intention-Driven ICMP Traceback""*, In Proceedings of the 10th International Conference on Computer Communications and Networks (IC3N_2001), Arizona, 2001.

[Mankins, 2003] S.M. Mankins, C. Sangpachatanaruk, T. Znati, R. Melhem, D. Moss, *"Proactive Server Roaming for Mitigating Denial of Service Attacks"*, In Proceedings of 1st International Conference on Information Technology Research and Education (ITRE), Newark, NJ, USA, August 10–13, 2003.

[Meadows, 1999] C. Meadows, *"A Formal Framework and Evaluation Method for Network Denial of Service"*, In Proceedings of the 12th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, Silver Spring, MD, 1999, pp. 4–13.

[Mirkovic, 2002a] J. Mirkovic, J. Martin, P. Reiher, *"A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms"*, UCLA CSD Technical Report no. 020018, 2002.

[Mirkovic, 2002b] J. Mirkovic, G. Prier, P. Reiher, *"Attacking DDoS at the Source"*, In Proceedings of ICNP 2002, Paris, France, 2002, pp. 312–321.

[Mirkovic, 2004] J. Mirkovic, P. Reiher, *"A Taxonomy of DDoS Attacks and Defense Mechanisms"*, ACM SIGCOMM Computer Communication Review, 34 (2) April 2004, 39-53.

[Moore, 2001] D. Moore, G. Voelker, S. Savage, *"Inferring Internet Denial of Service Activity"*, In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 2001, pp. 9–22.

[NIST, 1995] National Institute of Standards and Technology, *"A Conceptual Framework for System Fault Tolerance"*, 1995, Available from <http://hissa.nist.gov/chissa/SEI_Framework/framework_1.html>.

[NSS, 2007] NSS, *"NFR NID-310 V3.2.1"*, Available from <http://www.nss.co.uk/grouptests/ids/edition4/nfr/nfr.htm>.

[Onut, 2007] V. Onut, A. A. Ghobani, *"SVision: A Novel Visual Network-anomaly Identification Technique"*, Computers and Security Vol. 26, 2007, pp.201-212.

[Park, 2001a] K. Park, H. Lee, *"On the Effectiveness of Route-based Packet Filtering for Distributed DoS attack Prevention in Power Law Internets"*, In Proceedings of the ACM SIGCOMM'01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2001, pp. 15–26.

[Park, 2001b] K. Park, H. Lee, *"On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack"*, In Proceedings of IEEE INFOCOMM, Anchorage, AK, USA, 2001, pp. 338–347.

[Paxson, 1999] V. Paxson, *"End-to-end Internet Packet Dynamics"*, IEEE/ ACM Transactions on Networking Vol. 7, No. 3, (1999) pp. 277–292.

[Paxson, 2001] V. Paxson, *"An Analysis of using Reflectors for Distributed Denial of Service Attacks"*, ACM Computer Communication Review Vol. 31, No. 3, (2001), pp. 38–47.

[Peng, 2003] T. Peng, C. Leckie, K. Ramamohanarao, *"Protection from Distributed Denial of Service Attack using History-based IP Filtering"*, In Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, USA, 2003.

[Perkins, 2002] C. Perkins, *"IP Mobility Support for IPv4"*, IETF RFC 3344, 2002.

[Perrig, 2003] A. Perrig, D. Song, A. Yaar, *"StackPi: a New Defense Mechanism against IP Spoofing and DDoS Attacks"*, CMU technical report, December 2002, Updated February 2003.

[Porras, 1997] P.A. Porras, P.G. Neumann, *"EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances"*, In Proceedings of the Nineteenth National Computer Security Conference, Baltimore, MD, October 22–25, 1997, pp. 353–365.

[Sanchez, 2001] L. A. Sanchez, W. C. Milliken, A. C. Snoeren, F. Tchakountio, C. E. Jones, S. T. Kent, C. Partridge, and W. Timothy Strayer, *"Hardware Support for a Hash-Based IP Traceback"*, In Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEX-II), Anaheim, CA, June 2001.

[Savage, 2001] S. Savage, D. Wetherall, A. Karlin, T. Anderson, *"Network Support for IP Traceback"*, IEEE/ACM Transaction on Networking Vol. 9, No. 3, (2001) , pp. 226–237.

[Schuba, 1997] C. Schuba, I. Krsul, M. Kuhn, G. Spafford, A. Sundaram, D. Zamboni, *"Analysis of a Denial of Service Attack on TCP"*, In Proceedings of IEEE Security and Privacy Symposium, Oakland, CA, USA, May 4–7, 1997, IEEE Computer Society, Silver Spring, MD, 1997, pp. 208–223.

[SecureNet, 2007] *"SecureNet Pro"*, Last Checked 2007, Available from < http://securenet-pro.secutrain-inc.qarchive.org>.

[Snoeren, 2001] A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, S.T. Kent, W.T. Strayer, *"Hash-based IP Traceback"*, In Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, ACM Press, New York, 2001, pp. 3–14.

[Snort, 2007] *"The Open Source Network Intrusion Detection System: Snort"*, Available from <http://www.snort.org>.

[Song, 2001] D.X. Song, A. Perrig, *"Advanced and Authenticated Marking Schemes for IP Traceback"*, In Proceedings of IEEE INFOCOMM, Anchorage, AK, USA, 2001, pp. 878–886.

[Spatscheck, 1999] O. Spatscheck, L. Peterson, *"Defending against Denial of Service Requests in Scout"*, In Proceedings of the 3rd USENIX/ACM Symposium on Operating System Design and Implementation, New Orleans, LA, 1999, pp. 59–72.

[Stein, 2002] L.D. Stein, J.N. Stewart, *"The World Wide WebSecurity FAQ"*, version 3.1.2, February 4, 2002, Available from <http://www.w3.org/Security/

Faq>.

[Sterne, 2001] D. Sterne, K. Djahandari, B. Wilson, B. Babson, D. Schnackenberg, H. Holliday, T. Reid, *"Autonomic Response to Distributed Denial of Service Attacks"*, In Proceedings of Recent Advances in Intrusion Detection, 4th International Symposium, RAID 2001 Davis, CA, USA, October 10–12, 2001, pp. 134–149.

[Stone, 2000] R. Stone, *"CenterTrack: An IP Overlay Network for Tracking DoS Floods"*, In Proceedings of the 9th USENIX Security Symposium, Denver, CO, August 14–17, 2000, pp. 199–212.

[Sung, 2002] M. Sung, J. Xu, *"IP Traceback-based Intelligent Packet Filtering: a Novel Technique for Detecting against Internet DDoS Attacks"*, IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No 9, pp. 861--872, September 2003.

[Talpade, 1998] R.R. Talpade, G. Kim, S. Khurana, *"NOMAD: Traffic-based Network Monitoring Framework for Anomaly Detection"*, In Proceedings of the Fourth IEEE Symposium on Computers and Communications, 1998.

[Tanachaiwiwat, 2003] S. Tanachaiwiwat, and K. Hwang, *"Differential Packet Filtering against DDoS Flood Attacks"*, ACM Conference on Computer and Communications Security (CCS), Washington, DC, October 2003.

[Wang, 2001] X. Wang, D.S. Reeves, S.F. Wu, J. Yuill, *"Sleepy Watermark Tracing: an Active Network-based Intrusion Response Framework"*, In Proceedings of the 16th International Conference of Information Security (IFIP/SEC_01), Paris, France.

[Weiler, 2002] N. Weiler, *"Honeypots for Distributed Denial of Service"*, In Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109–114.

[Xforce, 2006] *"Finger Bomb Recursive Request"*, Available from <http://xforce.iss.net/static/47.php>.

[Xuan, 2001] D. Xuan, R. Bettati, W, Zhao, *"A Gateway-based Defense System for Distributed DoS Attacks in High-Speed Networks"*, In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security W1A2 0900 United States Military Academy, West Point, NY, 5-6 June 2001.

[Yaar, 2003] A. Yaar, A. Perrig, and D. Song, *"Pi: A Path Identification Mechanism to Defend against DDoS Attacks"*, In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA , 1-14 May 2003, pp. 93- 107.

[Yaar, 2005] A. Yaar, A. Perrig, D. Song, *"FIT: Fast Internet Traceback"*, In Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), 13-17 March 2005, Miami, FL, USA, pp. 1395-1406.

[Yan, 2000] J. Yan, S. Early, R. Anderson, *"The XenoService—a Distributed Defeat for Distributed Denial of Service"*, In Proceedings of ISW 2000, IEEE Computer Society, Boston USA, 2000.

[Yau, 2005] D. K. Yau, John C. S. Lui, and F. Liang, *"Defending Against Distributed Denial of Service Attacks with Max-min Fair Server-centric Router Throttles"*, IEEE/ACM Transactions on Networking, Vol. 13, No. 1, February 2005.

[Zaroo, 2002] P. Zaroo, *"A Survey of DDoS Attacks and Some DDoS Defense Mechanisms"*, Advanced Information Assurance (CS 626), 2002.

[Zhao, 2000] W. Zhao, D. Olshefski, H. Schulzrinne, *"Internet Quality of Service: an Overview"*, Columbia Technical Report CUCS-003-00, 2000.

[Zheng, 1997] Y.L. Zheng, J. Leiwo, *"A Method to Implement a Denial of Service Protection Base"*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 1270, Springer, Berlin, 1997, pp. 90–101.

Κεφάλαιο 3ο

Επιθέσεις Άρνησης Εξυπηρέτησης και Ηλεκτρονική Διακυβέρνηση

1. Εισαγωγή

Έχοντας λοιπόν κατανοήσει το πρόβλημα των επιθέσεων άρνησης εξυπηρέτησης (DoS) από τη γενική επισκόπηση του προηγούμενου κεφαλαίου, σε αυτό το κεφάλαιο σημειώνουμε τη σοβαρότητα των επιθέσεων DoS για τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, έναν τομέα υψίστης σημασίας. Η χρήση των ηλεκτρονικών τεχνολογιών στις κυβερνητικές υπηρεσίες έχει παίξει πολύ σημαντικό ρόλο στην διαμόρφωση πιο άνετου βίου για τους πολίτες. Ακόμα και αν η μετάβαση στην ψηφιακή διακυβέρνηση έχει πολλά πλεονεκτήματα για την ποιότητα των κυβερνητικών υπηρεσιών συνοδεύεται από πολλές απειλές ασφάλειας. Μία από τις πιο σημαντικές απειλές και ένα από τα δυσκολότερα προβλήματα ασφάλειας που αντιμετωπίζει η ηλεκτρονική διακυβέρνηση είναι οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service (DoS)).

Σε αυτό το κεφάλαιο παρουσιάζονται σημαντικά στατιστικά στοιχεία, χαρακτηριστικά περιστατικά των επιθέσεων DoS και αποτελέσματα από έρευνες που καταδεικνύουν τη σοβαρότητα του προβλήματος. Επιπλέον, προτείνουμε μία λίστα με τις καλύτερες πρακτικές που μπορεί να υιοθετήσει ένας οργανισμός

προκειμένου να ενδυναμώσει την άμυνά του ενάντια στις επιθέσεις DoS και τις κατανεμημένες επιθέσεις DoS (Distributed DoS (DDoS)).

Καθώς ζούμε σε έναν κόσμο όπου οι ηλεκτρονικές και διαδικτυακές τεχνολογίες παίζουν ένα πολύ σημαντικό ρόλο προκειμένου να μας βοηθήσουν να ζήσουμε πιο άνετα, οι τοπικές και κρατικές κυβερνήσεις απαιτείται να υιοθετήσουν και να συμμετάσχουν στην τεχνολογική επανάσταση. Οι τεχνολογίες ψηφιακής ή ηλεκτρονικής διακυβέρνησης επιτρέπουν σε τοπικές και εθνικές κυβερνήσεις να διανείμουν πληροφορίες και να παράσχουν υπηρεσίες στους πολίτες τους με ένα αποτελεσματικό και εύκολο τρόπο ελαχιστοποιώντας το χρόνο λήψης και επιστροφής αιτήσεων, επεξεργασίας και λήψης πληροφοριών. Αυτός ο εκσυγχρονισμός της διακυβέρνησης διευκολύνει τη σύνδεση και τη συνεργασία αρχών σε διάφορα επίπεδα διακυβέρνησης, κεντρικής, περιφερειακής και τοπικής, επιτρέποντας μία εύκολη ανταλλαγή προϊόντων και πρόσβαση σε βάσεις δεδομένων και πόρους που θα ήταν αδύνατο με άλλο τρόπο.

Η ηλεκτρονική διακυβέρνηση αναμφισβήτητα κάνει τη ζωή και την επικοινωνία των πολιτών ευκολότερη αποφεύγοντας πολύωρη ταλαιπωρία και γραφειοκρατία. Επίσης, παρέχει τις ίδιες ευκαιρίες για επικοινωνία με την κυβέρνηση όχι μόνο σε ανθρώπους στις πόλεις αλλά και σε ανθρώπους σε επαρχιακές περιοχές. Η ηλεκτρονική διακυβέρνηση επιτρέπει μεγαλύτερη πρόσβαση σε πληροφορίες, βελτιώνει τις δημόσιες υπηρεσίες και προωθεί δημοκρατικές διαδικασίες.

Αυτή η στροφή προς την τεχνολογική χρήση και τη μετατροπή σε μία "κυβέρνηση χωρίς γραφειοκρατία" αυξάνεται συνεχώς. Σύμφωνα με το [Holden, 2003] το 1995 το 8.7% των τοπικών κυβερνήσεων είχαν ιστοσελίδες, ενώ το 2003 αυτός ο αριθμός παρουσίασε σημαντική αύξηση που έφτασε το 83%. Σύμφωνα με το [West, 2006] το ποσοστό των κυβερνητικών ιστοσελίδων που παρέχουν κυβερνητικές υπηρεσίες μέσω Διαδικτύου η Βόρεια Αμερική (περιλαμβανομένων των Ηνωμένων Εθνών, του Καναδά και του Μεξικού) παρέχει το υψηλότερο ποσοστό κυβερνητικών υπηρεσιών μέσω Διαδικτύου, 71% για το 2006, μία σημαντική αύξηση από 54% που ήταν το 2005 και 28% για το 2001 αντίστοιχα. Ακολουθούν για το 2006, τα νησιά του Ειρηνικού Ωκεανού με ποσοστό 48% (σημαντική αύξηση από το 2005 με ποσοστό 24%), η Ασία με ποσοστό 42% (από 38% για το 2005), η δυτική Ευρώπη με ποσοστό 34% (από 20% για το 2005) και η Μέση Ανατολή με ποσοστό 31% (από 13% για το 2005).

Παρά αυτά τα ενθαρρυντικά στατιστικά στοιχεία η υιοθέτηση της ηλεκτρονικής διακυβέρνησης προχωρά με αργό ρυθμό όσον αφορά στα θέματα ασφάλειας, όπως η εμπιστευτικότητα και η αξιοπιστία που επηρεάζουν τη γρήγορη πρόοδο της ηλεκτρονικής διακυβέρνησης. Αναμφισβήτητα η ασφάλεια της ηλεκτρονικής διακυβέρνησης αποτελεί ένα σημαντικό κίνητρο που θα παροτρύνει τους πολίτες στη χρήση των ηλεκτρονικών κυβερνητικών υπηρεσιών.

Συγκεκριμένα σύμφωνα με το [West, 2006] σε έρευνα που πραγματοποιήθηκε για το 2006 μόνο το 26% (αύξηση από 18% για το 2005) των κυβερνητικών ιστοσελίδων που εξετάστηκαν διέθεταν κάποια μορφή πολιτικής εμπιστευτικότητας και μόνο το 14% διέθετε πολιτική ασφάλειας (μία αύξηση από 10%).

Καθώς η ηλεκτρονική διακυβέρνηση βασίζεται σε τεχνολογίες Διαδικτύου αντιμετωπίζει τον κίνδυνο της διασυνδεσιμότητας και των πολύ γνωστών αδυναμιών των δικτυακών υποδομών. Οι επιθέσεις DoS έχουν ήδη θέσει τις πιο διάσημες ιστοσελίδες ηλεκτρονικής διακυβέρνησης εκτός δικτύου για αρκετές ώρες προκαλώντας μεγάλες απώλειες και μεγάλο κόστος επιδιόρθωσης. Σύμφωνα με το Ινστιτούτο για την αποδοτικότητα της ηλεκτρονικής διακυβέρνησης [IFG.CC, 2002], το 2002, 36 κυβερνητικές ιστοσελίδες ήταν θύματα εισβολών. Οι περισσότερες από τις επιθέσεις στην ηλεκτρονική διακυβέρνηση έλαβαν μέρος στην Ασία (25%) και πιο συγκεκριμένα στην Κίνα και την Σιγκαπούρη (19%) καθώς και στις Η.Π.Α. (19%).

Σύμφωνα με την Αμερικάνικη υπό-επιτροπή Εποπτείας και Ερευνών [SOI, 2001] οι εγγραφές FedCIRC περιστατικών δηλώνουν ότι το 1998 ο αριθμός των περιστατικών που αναφέρθηκαν ήταν 376 και επηρέασαν 2.732 Αμερικανικά Κυβερνητικά συστήματα. Το 1999 σημειώθηκαν 580 περιστατικά που προκάλεσαν ζημιές σε 1.306.271 Αμερικάνικα κυβερνητικά συστήματα. Η Symantec [Symantec, 2004] (Τόμος VI, που εκδόθηκε τον Σεπτέμβριο του 2004, δραστηριότητα μεταξύ Ιανουαρίου 2004 και Ιουνίου του 2004) δίνει πληροφορίες που αφορούν συγκεκριμένα δεδομένα επίθεσης. Από αυτή την έρευνα προκύπτει ότι η τρίτη πιο σημαντική επίθεση που αντιμετώπισε η ηλεκτρονική διακυβέρνηση, εκτός από αυτές που σχετίζονται με επιθέσεις σκουλήκια (worm-related), είναι η επίθεση πλημμύρας TCP SYN.

Επομένως προκειμένου να είναι αποτελεσματικές οι υπηρεσίες ηλεκτρονικής διακυβέρνησης χωρίς διακοπές στην πρόσβαση ιστού όπως και στο ηλεκτρονικό ταχυδρομείο και τις υπηρεσίες βάσεων δεδομένων, υπάρχει μία ανάγκη για προστασία από επιθέσεις DoS. Μόνο με αξιόπιστες υπηρεσίες ηλεκτρονικής διακυβέρνησης που δεν απειλούνται από επιθέσεις DoS οι κυβερνήσεις μπορούν να κερδίσουν την εμπιστοσύνη των πολιτών.

Το αποτέλεσμα αυτών των επιθέσεων στους κυβερνητικούς οργανισμούς μεταξύ άλλων περιλαμβάνει μείωση ή καθολική απώλεια δικτυακής συνδεσιμότητας και συνεπώς μείωση της ικανότητας των οργανισμών να πραγματοποιήσουν νόμιμες επιχειρησιακές διαδικασίες στο δίκτυο για μία εκτεταμένη χρονική περίοδο. Η διάρκεια της επίδρασης της επίθεσης εξαρτάται από τον αριθμό των δυνατών δικτυακών επιθέσεων. Είναι επίσης σημαντικό να σημειώσουμε ότι ακόμα και αν ένας οργανισμός δεν είναι στόχος μίας επίθεσης, μπορεί να παρουσιάσει αυξημένη δικτυακή καθυστέρηση και απώλεια πακέτων,

ή πιθανόν και καθολική απώλεια λειτουργίας, καθώς μπορεί να χρησιμοποιείται από κάποιον επιτιθέμενο προκειμένου να πραγματοποιήσει μία επίθεση DDoS.

Σε αυτό το κεφάλαιο, σημειώνουμε τη σοβαρότητα που έχει μία επίθεση DoS για τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης. Για αυτό το σκοπό παρουσιάζονται χαρακτηριστικά περιστατικά των επιθέσεων DoS στις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Επιπλέον, παρουσιάζουμε μία λίστα με τις καλύτερες πρακτικές που μπορούν να χρησιμοποιηθούν από τους κυβερνητικούς οργανισμούς προκειμένου να ενδυναμώσουν περισσότερο την ασφάλεια στα συστήματά τους και να τους βοηθήσουμε να προστατέψουν τα συστήματά τους από το ενδεχόμενο να συμμετάσχουν σε μία κατανεμημένη επίθεση ή να γίνουν θύμα μίας επίθεσης DoS/DDoS. Μακροχρόνια μέτρα αντιμετώπισης προτείνονται επίσης που πρέπει να υιοθετηθούν για πιο αποτελεσματικές λύσεις στο πρόβλημα.

Μετά από αυτή την εισαγωγή, αυτό το κεφάλαιο οργανώνεται ως εξής. Η ενότητα 2 παρουσιάζει περιστατικά επιθέσεων DoS και αποτελέσματα από έρευνες που σχετίζονται με τις επιθέσεις DoS. Η ενότητα 3 παρουσιάζει τις καλύτερες πρακτικές για την αντιμετώπιση των επιθέσεων DoS που μπορούν να χρησιμοποιηθούν από τις κυβερνητικές οργανώσεις. Η ενότητα 4 παρουσιάζει μακροχρόνια μέτρα αντιμετώπισης των επιθέσεων DoS, ενώ η ενότητα 5 κλείνει το κεφάλαιο.

2. Περιστατικά Επιθέσεων Άρνησης Εξυπηρέτησης

Αναμφίβολα, οι επιθέσεις DoS είναι ένα απειλητικό πρόβλημα για το Διαδίκτυο, που προκαλεί καταστρεπτικές οικονομικές απώλειες θέτοντας τις ιστοσελίδες οργανισμών εκτός δικτύου για ένα σημαντικό χρονικό διάστημα. Η σοβαρότητα της επίδρασης των DoS μπορεί εύκολα να επιβεβαιωθεί από πρόσφατες αναφορές εφημερίδων που ονομάζουν γνωστούς και μεγάλους οργανισμούς με σημαντική έκθεση στην ηλεκτρονική οικονομία σαν θύματα επιθέσεων DoS.

Ο Howard [Howard, 1998] αναφέρει στατιστικές επιθέσεων άρνησης εξυπηρέτησης από τις οποίες είναι προφανής η δραματική αύξηση αυτών των επιθέσεων από τα πέντε πρώτα χρόνια του ιστού. Το Σκουλήκι του Διαδικτύου (Internet Worm [Spafford, 1998]) ήταν μία χαρακτηριστική ιστορία της επικαιρότητας καθώς προκάλεσε επίθεση DoS σε εκατοντάδες μηχανές. Αλλά ήταν το 1999, όταν οι Κατανεμημένες επιθέσεις DoS (DDoS) χτύπησαν ένα μεγάλο αριθμό γνωστών ιστοσελίδων.

Ο Criscuolo [Criscuolo, 2000] αναφέρει ότι η πρώτη επίθεση DDoS πραγματοποιήθηκε στο Πανεπιστήμιο της Μινεσότα τον Αύγουστο του 1999. Η επίθεση πλημμύρισε τον εξυπηρετητή Relay chat, διήρκεσε για δύο ημέρες και εκτιμήθηκε ότι τουλάχιστον 214 συστήματα συμμετείχαν στην πραγματοποίηση της επίθεσης. Τον Φεβρουάριο του 2000 μία σειρά από μαζικές επιθέσεις DoS

κατέστησαν εκτός λειτουργίας διάφορες ιστοσελίδες ηλεκτρονικού εμπορίου στο Διαδίκτυο περιλαμβανομένου του Yahoo.com. Αυτή η επίθεση κράτησε το Yahoo εκτός Διαδικτύου για δύο ώρες και οδήγησε σε μία σημαντική διαφημιστική απώλεια. Τον Οκτώβριο του 2002 [Fox News, 2002], 13 δρομολογητές που παρείχαν υπηρεσία DNS στους χρήστες του Διαδικτύου έπεσαν θύματα επίθεσης DDoS. Αν και η επίθεση διήρκεσε μόνο μία ώρα, 7 από τους 13 εξυπηρετητές root τέθηκαν εκτός λειτουργίας κάτι που υποδεικνύει την πιθανή ευπάθεια του Διαδικτύου στις επιθέσεις DDoS. Τον Ιανουάριο του 2001, στις ιστοσελίδες της Microsoft [WindowsITPro, 2001] που φιλοξενούν το Hotmail, MSN, Expedia και άλλες σημαντικές υπηρεσίες ήταν αδύνατη η πρόσβαση για περίπου 22 ώρες εξαιτίας μίας επίθεσης DDoS. Εκτός από τις επιθέσεις σε ιστοσελίδες υψηλού προφίλ, η πλειοψηφία των επιθέσεων δεν δημοσιοποιούνται για προφανείς λόγους.

Το CERT (Computer Emergency Response Team) [CERT, 2001] αναφέρει ότι τον Ιούλιο του 2001 ο δικτυακός τόπος του Λευκού Οίκου έπεσε θύμα του σκουληκιού Code Red. Η επίθεση στον Λευκό Οίκο διήρκεσε από τις 8 π.μ. μέχρι τις 11.15 μ.μ. Μεταξύ 1 μ.μ. και 2 μ.μ. οι αιτήσεις στην ιστοσελίδα συνέχισαν να αποτυγχάνουν, ενώ μετά τις 2 μ.μ. ο δικτυακός τόπος ήταν περιοδικά μη προσβάσιμος. Προκειμένου να καταπραΰνουν τα αποτελέσματα της επίθεσης, ο Λευκός Οίκος στιγμιαία άλλαξε την διεύθυνση IP του δικτυακού τόπου Whitehouse.gov.

Το Sophos.com [Sophos, 2002] αναφέρει, ότι τον Ιούνιο του 2002, ο δικτυακός τόπος της Πακιστανικής κυβέρνησης δέχτηκε μία επίθεση DoS που πραγματοποιήθηκε από Ινδούς υποστηρικτές. Η επίθεση πραγματοποιήθηκε μέσω ενός ευρέως διαδεδομένου σκουληκιού του Διαδικτύου που είναι γνωστό ως W32/Yaha-E, το οποίο ενθάρρυνε Ινδούς και συγγραφείς ιών να πραγματοποιήσουν επιθέσεις εναντίον των ιστοσελίδων της Πακιστανικής Κυβέρνησης. Το σκουλήκι έφτανε σαν ένα προσάρτημα σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου με θέμα που σχετίζεται με την αγάπη και τη φιλία. Το σκουλήκι τόνισε τις πολιτικές εντάσεις ανάμεσα στην Ινδία και το Πακιστάν και κατάφερε να καταστήσει απρόσιτη την ιστοσελίδα www.pak.gov.pk.

Το ITworld.com [ITworld.com, 2001] αναφέρει ότι ακόμα και ο δικτυακός τόπος του CERT έπεσε θύμα επίθεσης DDoS στις 28 Μαΐου του 2001. Αν και το κέντρο συντονισμού CERT είναι το πρώτο μέρος στο οποίο μπορεί κάποιος να βρει αξιόλογες πληροφορίες προκειμένου να προστατευθεί από κακόβουλες επιθέσεις του κυβερνοχώρου έπεσε θύμα μίας επίθεσης DDoS και έμεινε εκτός λειτουργίας για δύο ημέρες καθώς δεχόταν πληροφορίες με ρυθμούς πολλές εκατοντάδες φορές υψηλότερους από το συνηθισμένο.

Το Cs3.Inc [Cs3.Inc, 2005] αναφέρει ότι μία επίθεση DDoS πραγματοποιήθηκε στην Αμερικανική Στρατιωτική Διοίκηση του Ειρηνικού τον Απρίλιο του 2001. Η πηγή της επίθεσης ήταν άνθρωποι της Δημοκρατίας της Κίνας, αν και η ακριβής

προέλευση της επίθεσης δεν έχει ακόμα αναγνωριστεί. Παρά το γεγονός ότι τα εσωτερικά δίκτυα της Στρατιωτικής Διοίκησης δεν επηρεάσθηκαν, σε μακροχρόνιο επίπεδο κανείς δεν μπορεί να αρνηθεί το γεγονός ότι οι κρίσιμες κυβερνητικές λειτουργίες μπορούν εύκολα να διακοπούν από τους επιτιθέμενους. Μετά από αυτό το περιστατικό η πολιτική ένταση ανάμεσα στις δύο χώρες αυξήθηκε σημαντικά. Η αμερικάνικη κυβέρνηση ανησυχεί ότι κρίσιμα δικτυακά στοιχεία μπορεί να είναι στόχος μίας επίθεσης DDoS σαν ψηφιακή συνέχεια των τρομοκρατικών επιθέσεων ενάντια της Νέας Υόρκης τον Σεπτέμβριο του 2001. Αλλά τα κυβερνητικά συστήματα δεν είναι μόνο θύματα των επιθέσεων DoS αλλά μπορούν άθελά τους να χρησιμοποιηθούν για την πραγματοποίηση μίας επίθεσης DDoS φιλοξενώντας άθελα τους πράκτορες της επίθεσης DDoS.

Οι Moore και άλλοι [Moore, 2001] αναφέρουν ότι το Φεβρουάριο του 2001 δικτυακοί ερευνητές του UCSD από το κέντρο υπερυπολογιστών του San Diego (San Diego Supercomputer center (SDSC)) και την Πολυτεχνική Σχολή Jacobs ανέλυσαν το παγκόσμια διαδεδομένο πρότυπο των κακόβουλων επιθέσεων DoS ενάντια των υπολογιστών συλλόγων, πανεπιστημίων και ιδιωτών. Πρότειναν μία νέα τεχνική, που ονομάζεται ανάλυση "backscatter" που δίνει την εκτίμηση για την παγκόσμια δραστηριότητας των επιθέσεων DoS. Αυτή η έρευνα παρείχε τα μόνα δημόσια διαθέσιμα δεδομένα που μετρούν ποσοτικά τη δραστηριότητα των επιθέσεων DoS στο Διαδίκτυο και ενεργοποίησε τους ερευνητές να κατανοήσουν τη φύση των επιθέσεων αυτών.

Οι ερευνητές χρησιμοποίησαν σύνολα δεδομένων που συλλέχθηκαν και αναλύθηκαν σε μία χρονική περίοδο τριών εβδομάδων. Εκτίμησαν τον αριθμό, τη διάρκεια και το επίκεντρο των επιθέσεων, προκειμένου να χαρακτηρίσουν τη συμπεριφορά τους και παρατήρησαν περισσότερες από 12,000 επιθέσεις εναντίον 5,000 διαφορετικών στόχων, που ποικίλουν από γνωστές εταιρείες ηλεκτρονικού εμπορίου έως μικρούς ξένους παρόχους υπηρεσιών Διαδικτύου ακόμα και ανεξάρτητους προσωπικούς υπολογιστές με συνδέσεις dial-up. Κάποιες από τις επιθέσεις πλημμύρησαν τους στόχους τους με περισσότερα από 600,000 μηνύματα ανά πακέτο το δευτερόλεπτο.

Επιπλέον, ανέφεραν ότι το 50% των επιθέσεων διήρκεσαν λιγότερο από 10 λεπτά, το 80% λιγότερο από τριάντα λεπτά και το 90% λιγότερο από μία ώρα. Το 2% των επιθέσεων διήρκεσαν λιγότερο από πέντε ώρες, το 1% περισσότερο από δέκα ώρες και αρκετές δεκάδες κάλυψαν χρονική περίοδο πολλαπλών ημερών. Επιπλέον, σύμφωνα με αυτή την έρευνα το 90% ήταν επιθέσεις που βασίζονται στο TCP και περίπου το 40% ρυθμούς τόσο υψηλούς όσο 500 πακέτα ανά δευτερόλεπτο (pps) ή μεγαλύτερο. Τα πακέτα που αναλύθηκαν έφτασαν περίπου στα 500,000 πακέτα ανά δευτερόλεπτο, ενώ άλλες ανέκδοτες πηγές αναφέρουν μεγαλύτερες επιθέσεις που καταναλώνουν 35 Mbps για περιόδους περίπου 72 ωρών και επιθέσεις μεγάλης έντασης που φτάνουν τα 800 Mbps.

Το Ινστιτούτο Ασφάλειας Υπολογιστών (Computer Security Institute) [CSI, 2003] στην έρευνα του 2003 CSI/FBI αναφέρει ότι οι επιθέσεις DoS αναλογούν περισσότερο από το ένα τρίτο ανάμεσα στα περιστατικά σε ιστοσελίδες του παγκόσμιου ιστού, όπου πραγματοποιείται η μη εξουσιοδοτημένη πρόσβαση ή η κακή χρήση. Το 42% των ερωτηθέντων στην έρευνα του 2003 ανέφεραν ότι δέχτηκαν επιθέσεις DoS, ενώ το 2000, το 27% ανέφεραν ότι δέχτηκαν τέτοιες επιθέσεις. Φαίνεται ότι υπάρχει μία σημαντική ανοδική τάση στις επιθέσεις DoS. Το Ινστιτούτο Ασφάλειας Υπολογιστών [CSI, 2004] στην έρευνα του 2004 CSI/FBI αναφέρει ότι οι πιο υψηλές οικονομικές απώλειες που έχουν αναφερθεί εξαιτίας μίας μόνο επίθεσης DoS αυξήθηκε από $1 εκατομμύριο το 1998 σε $26 εκατομμύρια το 2004 και για πρώτη φορά προκύπτει ότι είναι ο τύπος περιστατικών που προκάλεσε τη μεγαλύτερη καθολική ζημιά.

Κατά τη διάρκεια των έξι πρώτων μηνών του 2006, η Symantec [PCPro, 2006] παρατήρησε κατά μέσο όρο 6,110 επιθέσεις DoS ανά ημέρα. Ενώ για όλο το έτος 2006 σύμφωνα με το Ινστιτούτο Ασφάλειας Υπολογιστών [CSI, 2006] μεταξύ των επιθέσεων που ανιχνεύτηκαν το 25% ανήκαν στην κατηγορία των επιθέσεων DoS. Επιπλέον, για το έτος 2006 [CSI, 2006] οι οικονομικές απώλειες που οφείλονται σε επιθέσεις DoS κυμαίνονται από $20,872 σε $56,672.

Τον Σεπτέμβριο του 2004 [Infosec, 2004] διάφορες ιστοσελίδες της Ολλανδικής κυβέρνησης τέθηκαν εκτός λειτουργίας σαν αποτέλεσμα μίας επίθεσης που πραγματοποίησαν κάποιοι χάκερς. Η επίθεση πραγματοποιήθηκε σαν ένδειξη διαμαρτυρίας ενάντια σε πολιτικές του δεξιού υπουργικού συμβουλίου. Με μία επίθεση DDoS, οι επιτιθέμενοι έστελναν συνεχώς πλαστές αιτήσεις για πληροφορίες στις ιστοσελίδες της ολλανδικής κυβέρνησης, με αποτέλεσμα τον αποκλεισμό των νόμιμων χρηστών. Από την επίθεση επηρεάστηκαν δύο ιστοσελίδες που παρείχαν πληροφορίες για κυβερνητικά ιδρύματα και τις δραστηριότητες, οι overheid.nl και regering.nl. Οι ιστοσελίδες αυτές τέθηκαν εκτός λειτουργίας για πέντε ημέρες. Μία ομάδα 15 επιτιθέμενων που ονομάζει των εαυτό της "Hacking Crew 10pht" ανέλαβε την ευθύνη για τις επιθέσεις σε μία ολλανδική ιστοσελίδα συζήτησης [Register, 2005]. Πέντε από την ομάδα των νεαρών επιτιθέμενων καταδικάστηκαν σε ποινές που κυμαίνονται από υποχρεωτική εργασία (work orders) έως προφυλάκιση. Αξίζει να σημειωθεί ότι, ο κύριος ύποπτος για την επίθεση ήταν ένας 18-χρονος ο οποίος έλαβε ποινή φυλάκισης 38 ημερών. Ήταν η πρώτη φορά στην Ολλανδία που κάποιος καταδικάστηκε για τέτοιου τύπου επίθεση.

Το Φεβρουάριο του 2005 [TheRegister, 2005], οι ιστοσελίδες του Ιάπωνα Πρωθυπουργού και του Υπουργικού Συμβουλίου τέθηκαν εκτός λειτουργίας εξαιτίας μία επίθεσης DoS. Η πηγή και τα κίνητρα της επίθεσης – που δεν προκάλεσαν μόνιμες ζημιές- παραμένουν αδιευκρίνιστα. Η λειτουργία των ιστοσελίδων αποκαταστάθηκαν αλλά η επίθεση αυτή και άλλες παρόμοιες που πραγματοποιήθηκαν τον Ιανουάριο και τον Αύγουστο του 2004 και προκάλεσαν μικρή ζημιά, αυξάνουν τις ανησυχίες και για μελλοντικές επιθέσεις DoS στις ιαπωνικές κυβερνητικές ιστοσελίδες.

Το καλοκαίρι του 2006 ιστοσελίδες της Σουηδικής Αστυνομίας και κυβέρνησης απενεργοποιήθηκαν από μία επίθεση DoS [HeiseSecurity, 2007]. Η αστυνομία δεν κατάφερε να προσδιορίσει την πηγή της επίθεσης. Το περιστατικό αυτό έδωσε ώθηση στην Σουηδική κυβέρνηση να θεσμοθετήσει κάθε επίθεση DoS ενάντια ιστοσελίδων να θεωρείται ποινικό αδίκημα, με μέγιστη ποινή τη φυλάκιση για δύο χρόνια.

- Κάποιες από τις κεντρικές κυβερνητικές ιστοσελίδες του Ντουμπάι [Headstar.com, 2007] δέχτηκαν επίθεση τον Φεβρουάριο του 2007. Η επίθεση πραγματοποιήθηκε από μία ομάδα Τούρκων εξτρεμιστών και αντιμετωπίστηκε μέσα σε δύο ώρες. Οι επιτιθέμενοι κατέστρεψαν κάποια δεδομένα στην ιστοσελίδα του τμήματος Ισλαμικών υποθέσεων, το οποίο είναι υπεύθυνο για κάποιες Ισλαμικές πρακτικές όπως η διάδοση του Ισλαμισμού. Οι επιτιθέμενοι δημιούργησαν κακή λειτουργία σε κάποιες από τις παρεχόμενες υπηρεσίες της ιστοσελίδας και απώλεια δεδομένων.

Πριν λίγο καιρό, η Εσθονία ήταν γνωστή σαν η πρώτη χώρα που πραγματοποιεί τις εθνικές εκλογές της μέσω Διαδικτύου, καθώς ήταν μία από τις πιο προηγμένες χώρες στην Ευρώπη, στη χρήση Διαδικτύου και υπηρεσιών ηλεκτρονικής διακυβέρνησης. Πρόσφατα όμως, αυτή η πρωτιά της αμαυρώθηκε. Συγκεκριμένα, καθώς η Εσθονία απέκτησε την ανεξαρτησία της από την Σοβιετική Ένωση το 1991, το τέλος του Απριλίου του 2007 απέσυρε ένα άγαλμα ενός στρατιώτη του κόκκινου στρατού από το κέντρο της πρωτεύουσας της. Αυτή η κίνηση προκάλεσε μεγάλη αντίδραση από τη Ρωσία που είχε σαν αποτέλεσμα μεταξύ άλλων την έναρξη ενός κυβερνο-πολέμου (cyberwar) [CBW, 2007] που διήρκεσε δύο εβδομάδες. Αυτός ο κυβερνό-πόλεμος είχε σαν αποτέλεσμα την απενεργοποίηση ιστοσελίδων κυβερνητικών οργανισμών, πολιτικών παρατάξεων, εφημερίδων, τραπεζών και εταιρειών της Εσθονίας. Η ζημιά που προκλήθηκε από την απενεργοποίηση αυτών των ιστοσελίδων δεν έχει υπολογιστεί ακόμα. Οι επιτιθέμενοι απενεργοποίησαν τις Εσθονικές ιστοσελίδες χρησιμοποιώντας επιθέσεις DDoS, οι οποίες πλημμύρισαν τις ιστοσελίδες με δεκάδες χιλιάδες επισκέψεις. Ο μεγάλος αριθμός των επισκέψεων ξεπέρασε τη χωρητικότητα των εξυπηρετητών και απενεργοποίησε τις ιστοσελίδες. Αυτές οι επιθέσεις είναι το πρώτο γνωστό περιστατικό κυβερνο-πολέμου τόσο μεγάλης κλίμακας και προκάλεσε μεγάλη ανησυχία στις χώρες του NATO.

Πρέπει να λάβουμε υπόψη μας το γεγονός ότι πολλοί κυβερνητικοί οργανισμοί ερμηνεύουν τις επιθέσεις DDoS σαν απλά μη επαρκή εξυπηρέτηση από τους παρόχους υπηρεσιών εξυπηρέτησης και δεν γνωρίζουν ότι δέχονται επίθεση. Αυτό έχει σαν αποτέλεσμα εννέα από τις δέκα επιθέσεις DDoS να μην αναφέρονται. Συγκεκριμένα, σύμφωνα με το Ινστιτούτο Ασφάλειας Υπολογιστών [CSI, 2006], το 2003 50% των επιθέσεων που πραγματοποιήθηκαν περιλαμβανομένων των επιθέσεων DoS δεν αναφέρθηκαν. Ενώ για το 2006, αν και έχουμε μία μείωση των επιθέσεων που δεν αναφέρθηκαν σε 30%, το ποσοστό εξακολουθεί να είναι πολύ μεγάλο. Παρά την ύπαρξη τέτοιων στοιχείων, οι

περισσότεροι κυβερνητικοί οργανισμοί δεν λαμβάνουν υπόψη τους την ανάγκη ύπαρξης προστατευτικών μηχανισμών για την αντιμετώπιση των επιθέσεων DoS.

Αν και δεν υπάρχει λύση-πανάκεια για όλους τους τύπους των επιθέσεων DoS, υπάρχουν πολλοί μηχανισμοί προστασίας που μπορούν να χρησιμοποιηθούν προκειμένου να γίνει πιο δύσκολη η πραγματοποίηση μίας επίθεσης και να παράσχουν τρόπους για την αποκάλυψη της ταυτότητας του επιτιθέμενου.

3. Οι Καλύτερες Πρακτικές για την Αντιμετώπιση των Επιθέσεων Άρνησης Εξυπηρέτησης

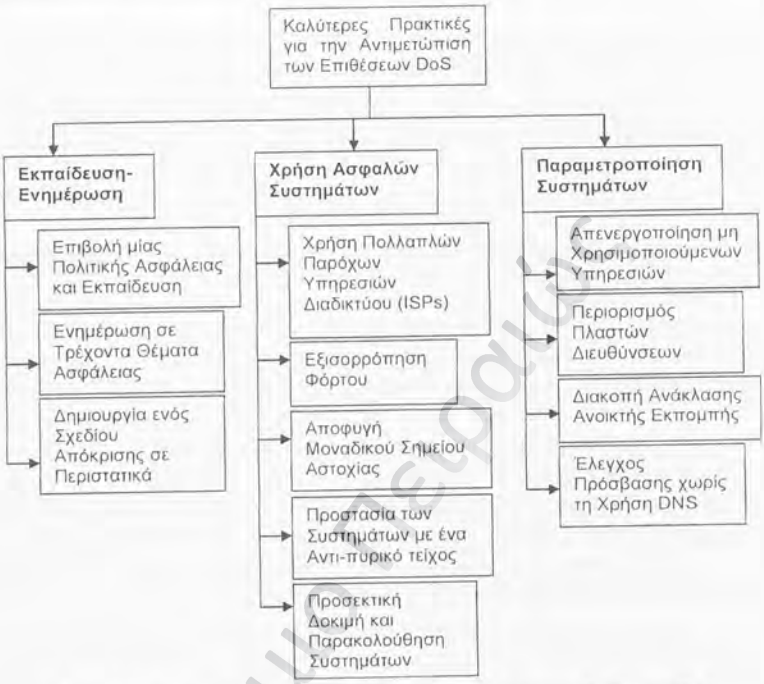
Οι επιθέσεις DoS μπορούν να οδηγήσουν σε μία ολοκληρωτική ακινητοποίηση όλων των κυβερνητικών οργανισμών, προκαλώντας την απώλεια εσόδων ή/και την παραγωγικότητα εκατομμυρίων απομακρύνοντας τους πολίτες από τις ηλεκτρονικές υπηρεσίες. Μερικές από τις κυβερνήσεις δεν κατανοούν τη σοβαρότητα του προβλήματος, με αποτέλεσμα να είναι ευπαθή τα συστήματά τους και να παραβιάζονται εύκολα. Αυτά τα συστήματα αποτελούν μεγάλη απειλή όχι μόνο για τους οργανισμούς αυτούς αλλά και για οποιονδήποτε άλλο που δέχεται επίθεση μέσω αυτών των συστημάτων. Αυτό σημαίνει ότι είναι σημαντικό οι κυβερνήσεις να λάβουν προληπτικά μέτρα προκειμένου να μειώσουν την πιθανότητα τέτοιων επιθέσεων και την επίδρασή τους.

Καθώς οι επιθέσεις DoS είναι ιδιαίτερα πολύπλοκες πρέπει να σημειώσουμε ότι δεν υπάρχει μία μοναδική λύση και κανένα σύστημα δεν είναι απόλυτα ασφαλές. Κανένας όμως, δεν μπορεί να αρνηθεί ότι οι αποτελεσματικά προσχεδιασμένες κυβερνητικές υπηρεσίες θα μπορούσαν να ανταποκριθούν αποτελεσματικά και γρήγορα σε απειλές ασφάλειας όπως είναι οι επιθέσεις Άρνησης Εξυπηρέτησης. Στη συνέχεια αναφέρουμε μία λίστα από κάποιες πρακτικές που μπορούν να χρησιμοποιηθούν προκειμένου να μειωθούν αυτές οι επιθέσεις και να περιοριστεί η επίδρασή τους. Οι προτεινόμενες πρακτικές έχουν κατηγοριοποιηθεί σε τρεις κύριες κατηγορίες (Σχήμα 3.1):

- την εκπαίδευση – ενημέρωση,
- την παραμετροποίηση συστημάτων και
- την χρήση ασφαλών συστημάτων.

Αν και οι παραπάνω κατηγορίες παρουσιάζουν πολλά κοινά σημεία και στοιχεία αλληλο-κάλυψης, η προτεινόμενη προσέγγιση κατηγοριοποίησης μας βοηθά στην καλύτερη κατανόηση και δόμηση των προτεινόμενων πρακτικών.

Εκπαίδευση – ενημέρωση: Είναι υψίστης σημασίας προκειμένου οι οργανισμοί να διασφαλίσουν τα συστήματά τους να ενημερωθούν και να εκπαιδευτούν για όλα τα τρέχοντα θέματα ασφάλειας, να εφαρμόσουν μία αποτελεσματική πολιτική ασφάλειας και να δημιουργήσουν ένα αξιόπιστο σχέδιο απόκρισης σε κρίσιμα περιστατικά.



Σχήμα 3. 1 Καλύτερες Πρακτικές για την Αντιμετώπιση των Επιθέσεων DoS

- ***Επιβολή μίας Πολιτικής Ασφάλειας και Εκπαίδευση:*** Όπως σημειώνεται από τους Walters [Walters, 2001] είναι μεγάλης σημασίας η επιβολή και η διατήρηση μίας πολιτικής ασφάλειας. Επιπρόσθετα των βασικών ανανεώσεων σε αντιβιοτικά, στην ελεγχόμενη πρόσβαση των χρηστών και στα ασφαλή λογισμικά, σε καμία περίπτωση δεν πρέπει να παραβλέπουμε να περιλαμβάνονται σε αυτή την πολιτική τρόπους για την αντιμετώπιση επιθέσεων DoS/DDoS. Επιπλέον, μία πολιτική ασφάλειας πρέπει να έχει γνωστοποιηθεί κατάλληλα σε όλους τους υπαλλήλους. Είναι σημαντικό να επιβεβαιώσουμε ότι καθώς η γνωστική εξειδίκευση των διαχειριστών συστημάτων και των ελεγκτών ακολουθεί τις τρέχουσες εξελίξεις, υπάρχει ανάγκη για συχνές πιστοποιήσεις. Ιδιαίτερης σημασίας είναι η συνεχής εκπαίδευση του προσωπικού του οργανισμού σε νέες τεχνικές σήμανσης και ψηφιακών πειστηρίων.
- ***Ενημέρωση στα Τρέχοντα Θέματα Ασφάλειας:*** Όπως είναι ευρέως γνωστό προκειμένου να αντιμετωπιστούν οι επιθέσεις DoS ο καλύτερος τρόπος είναι να προσπαθούμε να είμαστε πάντα προστατευμένοι και ενημερωμένοι στα θέματα ασφάλειας [Householder, 2001]. Είναι σημαντικό να ενημερωνόμαστε για τις τρέχουσες βελτιώσεις, ανανεώσεις,

δελτία και ανακοινώσεις ασφάλειας, προκειμένου να προστατευθούμε από επιθέσεις DoS.

- *Δημιουργία ενός Σχεδίου Απόκρισης σε Περιστατικά:* Είναι σημαντικό να είμαστε προετοιμασμένοι και έτοιμοι για κάθε πιθανό σενάριο επίθεσης. Οι κυβερνητικοί οργανισμοί θα πρέπει να ορίσουν ένα σύνολο ξεκάθαρων διαδικασιών που πρέπει να ακολουθηθούν σε επείγουσες καταστάσεις και να εκπαιδεύουν ομάδες προσωπικού με ξεκάθαρα καθορισμένες ευθύνες έτσι ώστε να είναι έτοιμοι να αποκριθούν σε επείγουσες περιπτώσεις [Householder, 2001]. Οποιαδήποτε επίθεση ή ύποπτα ελαττώματα ενός συστήματος θα πρέπει να αναφέρονται στις κατάλληλες αρχές (όπως είναι το FBI και το CERT) έτσι ώστε οι πληροφορίες να μπορούν να χρησιμοποιηθούν για την προστασία και άλλων χρηστών.

Χρήση Ασφαλών Συστημάτων: Κρίνεται απαραίτητο τα συστήματα που χρησιμοποιούν οι οργανισμοί να είναι ασφαλή. Σημαντικό βήμα για την επίτευξη αυτού του σκοπού αποτελεί η χρήση πολλαπλών παρόχων υπηρεσιών Διαδικτύου, η εξισορρόπηση φόρτου και η αποφυγή μοναδικού σημείου αστοχίας. Επιπλέον, ιδιαίτερα σημαντική κρίνεται η προστασία των συστημάτων με αντι-πυρικά τείχη προστασίας και η προσεκτική δοκιμή και παρακολούθηση συστημάτων.

- *Χρήση Πολλαπλών Παρόχων Υπηρεσιών Διαδικτύου:* Οι κυβερνητικοί οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο χρήσης περισσότερων από έναν ISP, προκειμένου να κάνουν ακόμα πιο δύσκολη την πραγματοποίηση μίας επίθεσης DoS/DDoS εναντίον τους. Στην επιλογή των παρόχων, είναι σημαντικό να λάβουμε υπόψη μας ότι οι πάροχοι θα πρέπει να χρησιμοποιούν διαφορετικά μονοπάτια πρόσβασης προκειμένου να αποφύγουν την πλήρη απώλεια πρόσβασης στην περίπτωση που ένα από τα μονοπάτια ή τις ζεύξεις τεθεί εκτός λειτουργίας [Walters, 2001]. Έχει προταθεί επίσης η εισαγωγή νομοθεσίας για τους παρόχους προκειμένου να εφαρμόζουν φιλτράρισμα εξόδου.

- *Εξισορρόπηση Φόρτου:* Οι Specht και άλλοι [Specht, 2003] υποστηρίζουν ότι μία καλή προσέγγιση προκειμένου να αποφύγουμε το ενδεχόμενο να πέσει ένας οργανισμός θύμα επιθέσεων DoS είναι να κατανείμει τον φόρτο των συστημάτων του οργανισμού σε πολλαπλούς εξυπηρετητές. Προκειμένου να επιτευχθεί αυτό, μπορούν να χρησιμοποιηθούν ένα DNS με εκ περιτροπή ανάθεση (round robin DNS) ή δρομολογητές υλικού για την αποστολή εισερχόμενων αιτήσεων σε έναν ή περισσότερους εξυπηρετητές.

- *Αποφυγή Μοναδικού Σημείου Αστοχίας:* Προκειμένου να αποφύγουμε την αστοχία μοναδικού σημείου η καλύτερη λύση είναι η ύπαρξη πλεοναζόντων μηχανών που μπορούν να χρησιμοποιηθούν σε περίπτωση

που κάποια παρόμοια μηχανή απενεργοποιηθεί [Householder, 2001]. Επιπλέον, οι οργανισμοί θα πρέπει να αναπτύξουν σχέδια ανάκτησης που θα τους επιτρέψουν να καλύψουν κάθε πιθανό σημείο αποτυχίας του συστήματός τους. Επιπλέον, οι οργανισμοί θα πρέπει να χρησιμοποιούν πολλαπλά λειτουργικά συστήματα προκειμένου να δημιουργήσουν "βιοδιαφοροποίηση" και να αποφύγουν εργαλεία επιθέσεων DoS που στοχεύουν σε συγκεκριμένα Λειτουργικά Συστήματα.

- *Προστασία των Συστημάτων με ένα Αντι-πυρικό Τείχος (firewall):* Ο Walters [Walters, 2001] δηλώνει ότι καθώς η έκθεση σε πιθανούς εισβολείς αυξάνεται, είναι απαραίτητη η εγκατάσταση τειχών προστασίας που περιορίζουν σημαντικά τις συναλλαγές στην περιφέρεια των συστημάτων των κυβερνητικών οργανισμών προκειμένου να παρέχουν αποτελεσματική προστασία. Τα αντι-πυρικά τείχη θα πρέπει να ρυθμίζονται κατάλληλα ώστε να αφήνονται ανοιχτές μόνο οι απαραίτητες θύρες (ports). Επιπλέον, τα αντι-πυρικά τείχη έχουν τη δυνατότητα να ελέγχουν προσεκτικά, να αναγνωρίζουν και να επεξεργάζονται προσπάθειες εισβολών. Το φιλτράρισμα εισόδου θα πρέπει να εγκαθίσταται στους κυβερνητικούς εξυπηρετητές ιστού έτσι ώστε να μην μπορούν να χρησιμοποιηθούν σαν πράκτορες για την πραγματοποίηση επιθέσεων σε άλλους εξυπηρετητές. Οι κυβερνητικές υπηρεσίες θα πρέπει επίσης να καθορίσουν ένα σύνολο διευθύνσεων IP που μπορούν να χρησιμοποιηθούν μόνο από κυβερνητικούς εξυπηρετητές.
- *Προσεκτική Δοκιμή και Παρακολούθηση Συστημάτων:* Το πρώτο βήμα προκειμένου να ανιχνευθεί η ανώμαλη συμπεριφορά είναι ο "χαρακτηρισμός" της "φυσιολογικής" συμπεριφοράς στα πλαίσια του δικτύου της κυβερνητικής υπηρεσίας. Το επόμενο βήμα θα πρέπει να είναι ο έλεγχος των προνομίων πρόσβασης, των δραστηριοτήτων και των εφαρμογών. Οι διαχειριστές πρέπει να πραγματοποιούν εικοσιτετράωρη παρακολούθηση προκειμένου να μειώσουν τα εξαντλητικά αποτελέσματα των επιθέσεων DoS που πιθανόν να υποστεί ένας κυβερνητικός εξυπηρετητής. Μέσω αυτής της διαδικασίας, οι οργανισμοί μπορούν να ανιχνεύσουν ασυνήθιστα επίπεδα δικτυακής κυκλοφορίας ή χρήση της Κεντρικής Μονάδας Επεξεργασίας (ΚΜΕ) [Householder, 2001]. Υπάρχει μία μεγάλη ποικιλία εργαλείων που έχουν τη δυνατότητα να ανιχνεύσουν, να περιορίσουν και να αναλύσουν τις επιθέσεις άρνησης εξυπηρέτησης.

Παραμετροποίηση Συστημάτων: Προκειμένου να διασφαλίσουν τα συστήματά τους οι οργανισμοί καλούνται να κάνουν σωστή παραμετροποίηση των συστημάτων τους. Βασικές πρακτικές όπως η απενεργοποίηση μη-χρησιμοποιούμενων υπηρεσιών, ο περιορισμός των παραποιημένων διευθύνσεων, η διακοπή ανάκλασης ανοικτής εκπομπής και ο έλεγχος

πρόσβασης χωρίς τη χρήση DNS μπορούν να έχουν θεαματικά αποτελέσματα στη διασφάλιση των συστημάτων.

- *Απενεργοποίηση μη Χρησιμοποιούμενων Υπηρεσιών:* Είναι σημαντικό, όπως σημειώνεται από τους Leng και άλλοι [Leng, 2000], τα συστήματα των οργανισμών να παραμένουν απλά ελαχιστοποιώντας τον αριθμό των υπηρεσιών που "τρέχουν" σε αυτά. Αυτό μπορεί να επιτευχθεί κλείνοντας όλες τις υπηρεσίες που δεν απαιτούνται. Είναι σημαντικό να κλείσουν ή να περιορίστουν σημαντικές υπηρεσίες που διαφορετικά μπορεί να παραβιαστούν ή να ανατραπούν προκειμένου να πραγματοποιηθούν επιθέσεις DoS. Για παράδειγμα, εάν δεν απαιτούνται οι υπηρεσίες ηχούς UDP ή παραγωγής χαρακτήρων, η απενεργοποίηση τους θα βοηθήσει στην προστασία τους από επιθέσεις που εκμεταλλεύονται αυτές τις υπηρεσίες.
- *Περιορισμός Παραποιημένων Διευθύνσεων:* Μία προσέγγιση που οι εισβολείς χρησιμοποιούν συχνά προκειμένου να αποκρύψουν την ταυτότητα τους όταν πραγματοποιούν επιθέσεις DoS είναι η χρήση παραποιημένων διευθύνσεων πηγής. Όπως υποστηρίζουν και οι Singer και άλλοι [Singer, 2000] είναι σημαντικό να περιορίσουμε τη χρήση παραποιημένων διευθύνσεων. Αν και δεν είναι δυνατόν να αντιμετωπιστεί πλήρως η χρήση παραποιημένων διευθύνσεων IP, υπάρχουν κάποιες προσεγγίσεις που μπορεί να χρησιμοποιηθούν προκειμένου να γίνει πιο δύσκολη η απόκρυψη της πηγής των επιθέσεων και να συντομεύσει την ιχνηλάτηση μίας επίθεσης έως την πηγή της. Οι διαχειριστές συστημάτων μπορούν αποτελεσματικά να μειώσουν το ρίσκο των παραποιημένων διευθύνσεων IP χρησιμοποιώντας φιλτράρισμα πακέτων στην είσοδο και την έξοδο μέσω αντι-πύρικων τειχών ή /και δρομολογητών.
- *Διακοπή Ανάκλασης Ανοικτής Εκπομπής:* Είναι σημαντικό να απενεργοποιήσουμε την κατευθυνόμενη εισερχόμενη ανοικτή εκπομπή προκειμένου να παρεμποδίσουμε ένα δίκτυο από το ενδεχόμενο να χρησιμοποιηθεί σαν ανακλαστήρας σε επιθέσεις όπως η πλημμύρα ICMP και η Smurf [Leng, 2000]. Κλείνοντας την ρύθμιση της κατευθυνόμενης ανοικτής εκπομπής πακέτων IP στους δρομολογητές και κάνοντας αυτή την ρύθμιση προκαθορισμένη είναι η καλύτερη ενέργεια που μπορεί να πραγματοποιηθεί από τους πωλητές δικτυακού υλικού.
- *Έλεγχος Πρόσβασης χωρίς τη Χρήση DNS:* Χρησιμοποιώντας ονόματα κόμβων στη λίστα πρόσβασης και όχι διευθύνσεων IP κάνει τα συστήματα ευπαθή σε παραποιημένα ονόματα [Leng, 2000]. Τα συστήματα δεν πρέπει να βασίζονται σε δικτυακές περιοχές (domain) ή ονόματα κόμβων προκείμενου να καθορίσουν εάν η πρόσβαση είναι εξουσιοδοτημένη ή όχι.

Διαφορετικά, οι εισβολείς μπορούν να υποκριθούν ένα σύστημα, απλά τροποποιώντας τους πίνακες αντίστροφης αναζήτησης.

4. Μακροπρόθεσμα Μέτρα Αντιμετώπισης

Η ποικιλία και πολυπλοκότητα των επιθέσεων DoS είναι πολύ πιθανό να αυξηθεί, επομένως ανεξάρτητα από τα μέτρα προστασίας που μπορούν να χρησιμοποιηθούν τώρα, χρειάζεται να αντιμετωπίσουμε τις επιθέσεις DoS σαν ένα πρόβλημα που απαιτεί μακροχρόνια προσπάθεια προκειμένου να ορίσουμε και να υλοποιήσουμε αποτελεσματικές λύσεις. Είναι σημαντικό να σημειώσουμε εδώ ότι οι κυβερνήσεις πρέπει να υιοθετήσουν μία μη-διεισδυτική και όχι ακραία προσέγγιση για την προστασία από επιθέσεις DoS, καθώς υπάρχει μία λεπτή γραμμή ανάμεσα στον περιορισμό της εγκληματικής δραστηριότητας και τον περιορισμό της οικονομίας, της εκπαίδευσης, της ελεύθερης διακίνησης πληροφοριών και της προσωπικής ελευθερίας.

Το Sans Institute [Sans, 2000] αναγνωρίζει κάποιες ενέργειες που θα μπορούσαν να βοηθήσουν στην προστασία από επιθέσεις DoS πιο αποτελεσματικά στο μακρινό μέλλον. Μεταξύ αυτών περιλαμβάνεται η γρήγορη υιοθέτηση των στοιχείων του IPsec του IPv6 και του ασφαλούς DNS (Secure DNS). Είναι σημαντικό η διαδικασία ανανέωσης της ασφάλειας να είναι αυτοματοποιημένη. Οι πωλητές θα πρέπει να ενθαρρύνονται να την υλοποιούν εκ μέρους των πελατών τους προκειμένου να κάνουν ευκολότερη την ανανέωση των προϊόντων τους και να παρέχουν πληροφορίες για θέματα ασφάλειας. Επιπλέον, είναι απαραίτητη η έρευνα και ανάπτυξη ασφαλέστερων λειτουργικών συστημάτων. Μεταξύ των θεμάτων που πρέπει να διευθετηθούν περιλαμβάνεται η ανίχνευση ανωμαλιών αλλά και άλλες μορφές ανίχνευσης εισβολών. Επιπλέον, οι κυβερνήσεις θα πρέπει να σκεφτούν την πραγματοποίηση κάποιων αλλαγών στις κυβερνητικές πολιτικές προμήθειας με τέτοιο τρόπο ώστε να δοθεί έμφαση στην ασφάλεια και την προστασία.

Σημαντικό ρόλο στον αγώνα ενάντια των επιθέσεων άρνησης εξυπηρέτησης είναι η ίδρυση οργανισμών που θα είναι υπεύθυνοι για την παρακολούθηση της δικτυακής ασφάλειας και την επεξεργασία περιστατικών. Αυτοί οι οργανισμοί θα πρέπει να ενθαρρύνουν τη δημόσια ενημέρωση για θέματα ασφάλειας και να πληροφορούν τους ιδιοκτήτες κρίσιμων υποδομών και τα κυβερνητικά τμήματα σχετικά με τις απειλές. Επιπλέον, σημαντικό κρίνεται να προωθούν την υιοθέτηση και την παραγωγή προτύπων ασφαλείας, να διατηρούν βάσεις δεδομένων με στατιστικά στοιχεία και περιστατικά αλλά και να συνεργάζονται με παρόμοιους οργανισμούς (π.χ. το CERT).

Οι κυβερνήσεις θα πρέπει να επιβεβαιώσουν ότι οι κυβερνητικές υπηρεσίες θα κάνουν όλα τα απαραίτητα βήματα προκειμένου να επιβεβαιώσουν την ασφάλεια των πληροφοριακών τους συστημάτων. Οι κυβερνητικές υπηρεσίες θα πρέπει να ενθαρρύνουν μία καλύτερη έρευνα των πληροφοριακών επιθέσεων με σεβασμό στην εμπιστευτικότητα και τα προσωπικά δικαιώματα των χρηστών του

Διαδικτύου. Απαραίτητη είναι η επιπρόσθετη χρηματοδότηση για την εκπαίδευση ειδικού προσωπικού σε Πληροφοριακές Τεχνολογίες ασφάλειας και για την εκπαίδευση πολιτών προκειμένου να προστατευθούν από το κυβερνοέγκλημα. Είναι επίσης απαραίτητο να προωθήσουμε και να ενθαρρύνουμε τις αστυνομικές αρχές προκειμένου να διωχθούν ποινικά οι εισβολείς σε διεθνές επίπεδο και να εξεταστεί το νομικό πλαίσιο έτσι ώστε να διευκολυνθεί αυτή η συνεργασία.

5. Επίλογος

Αναμφισβήτητα, οι επιθέσεις DoS πρέπει να αντιμετωπιστούν σαν ένα σοβαρό πρόβλημα στο Διαδίκτυο. Ο ρυθμός ανάπτυξής τους και η ευρεία αποδοχή τους προκαλούν ανασφάλεια στους πολίτες για τις ηλεκτρονικές συναλλαγές και δημιουργούν αμφιβολίες σε κυβερνήσεις και επιχειρήσεις. Κανείς δεν μπορεί να αρνηθεί ότι οι επιθέσεις DoS θα συνεχίσουν να αποτελούν σημαντική απειλή για όλους τους οργανισμούς περιλαμβανομένων των κυβερνητικών οργανισμών. Είναι προφανές ότι θα ακολουθήσουν νέοι μηχανισμοί προστασίας οι οποίοι αντίστοιχα θα ακολουθηθούν από την εξέλιξη των νέων μεθόδων επιθέσεων DoS. Η υποδομή ενός δικτύου πρέπει να είναι αρκετά ισχυρή ώστε να αντιμετωπίσει άμεσες επιθέσεις DoS και αρκετά επεκτάσιμη ώστε να μπορεί να υιοθετήσει και να αγκαλιάσει νέες μεθόδους προστασίας ενάντια των εξελισσόμενων και μη προβλέψιμων μεθόδων επίθεσης. Προκειμένου να επιβεβαιώσουμε την υψηλή ανθεκτικότητα και απόδοση των δημόσιων και ιδιωτικών δικτύων πρέπει να συντονιστούν οι προσπάθειες των διαχειριστών, των παρόχων υπηρεσιών και των κατασκευαστών εξοπλισμού. Μεγάλης σημασίας είναι η επικοινωνία των πολιτών με τις κυβερνητικές αρχές μέσω δικτύου. Κανείς δεν πρέπει να έχει το δικαίωμα να θέσει εκτός λειτουργίας πολύτιμες υπηρεσίες ηλεκτρονικής διακυβέρνησης. Μία περισσότερο αποτελεσματική προσέγγιση θα ήταν να ζητήσουμε από όλους τους πολίτες να αναλάβουν την ασφάλεια του Διαδικτύου για ότι τους αφορά. Η ενημέρωση του κοινού είναι το κλειδί προκειμένου η ηλεκτρονική διακυβέρνηση να είναι ασφαλής και επιτυχημένη.

Βιβλιογραφία

[Fox News, 2002] Fox News (2002), *"Powerful Attack Cripples Internet"*, Available from <http://www.linuxsecurity.com/content/view/112716/65/>.

[CERT, 2001b] CERT Coordination Center Advisory CA-2001-19, *"Code Red Worm Exploiting Buffer Overflow in IIS Indexing Service DLL"*, Carnegie Mellon Software Engineering Institute, 2001, Available from <http://www.cert.org/advisories/CA-2001-19.html>.

[CBW, 2007] Czech Business Weekly, Pavla Kozáková, *"Cyberwar is Breaking out of Sci-fi Genre"*, 11 June 2007, Available from <http://www.cbw.cz/phprs/2007061112.html>

[CSI, 2003] CSI Inc., *"2003 CSI/FBI Computer Crime and Security Survey"*, USA 2003.

[CSI, 2004] CSI Inc., *"2004 CSI/FBI Computer Crime and Security Survey"*, USA 2004.

[CSI, 2006] CSI Inc., *"2006 CSI/FBI Computer Crime and Security Survey"*, USA 2006.

[Criscuolo, 2000] P.J. Criscuolo, *"Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319"*, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, 2000 Available from <http://ftp.se.kde.org/pub/security/csir/ciac/ciacdocs/ciac2319.txt>.

[Cs3.Inc, 2005] Cs3 Inc., *"Defending Government Network Infrastructure Against Distributed Denial of Service Attacks"*, CS3-inc.com. Available from <http://www.cs3-inc.com/government-ddos-threat-and-solutions.pdf>.

[Headstar.com, 2007] Headstar.com, E-Government Bulletin Live Home, *"Dubai Central Government Websites Hacked"*, 1 March 2007, Available from < http://www.headstar.com/egblive/?p=22>

[HeiseSecurity, 2007] Heise Security, *"Sweden Criminalises DoS Attacks"*, 20 February 2007, Available from < http://www.heise-security.co.uk/news/85570 >.

[Holden, 2003] S. Holden, D. Norris, and P. Fletcher, *"Electronic Government at the Local Level: Progress to Date and Future Issues"*, Public Performance and Management Review, Vol. 26, Issue 4, 2003, pp. 325-344.

[Householder, 2001] A. Householder, A. Manion, L. Pesante, G.M. Weaver and R. Thomas, *"Trends in Denial of Service Attack Technology"*, CERT Coordination Center, Carnegie Mellon University, v10.0, 2001, Available from <http://www.cert.org/archive/pdf/DoS_trends.pdf >

[Howard, 1998] J. Howard, *"An Analysis of Security Incidents on the Internet 1989-1995"*, PhD thesis, Carnegie Mellon University, 1998, Available from <http://www.cert.org/research/ JHThesis/Start.html>.

[IfG.CC, 2002] Institute for eGovernment Competence Center (IfG.CC), *"E-GOVERNMENT: First Fight the Hackers"*, 2002, Available from <http://64.233.179.104/search?q=cache:R_LWlkZ8wKsJ:www.uni-potsdam.de/db/elogo/html/modules.php%3Fname%3DNews%26file%3Darticle%26sid%3D1450+EGovernment+First+fight+the+Hackers+ifg.cc&hl=el&gl=gr&ct=clnk&cd=1>.

[Infosec, 2004] InfoSec News, *"Dutch Government Sites Attacked"*, 6 October 2004, Available from < http://archive.cert.unistuttgart.de/isn/2004/10/msg000

13.html>

[ITworld.com, 2001], ITworld, *"CERT Hit by DDoS Attack for a Third Day"*, Available from <http://www.itworld.com/Sec/3834/IDG010524CERT2/>.

[Leng, 2000] X. Leng and A.B. Whinston, *"Defeating Distributed Denial of Service Attacks"*, IEEE IT Professional 2 (4) , 2000, pp. 36-42.

[Moore, 2001] D. Moore, G. Voelker, and S. Savage, *"Inferring Internet Denial of Service Activity"*, Proceedings of the USENIX Security Symposium, Washington, DC, USA, 2001, pp. 9–22.

[PCPro, 2006] PCPro, *"Analysis: Websites Struggling for Legal Recourse for DoS Attacks"*, 23rd November 2006, Available from <http://www.pcpro.co.uk/news

/98598/analysis-websites-struggling-for-legal-recourse-for-dos-attacks.html>.

[Sans, 2000] SANS Institute, *"Consensus Roadmap for Defeating Distributed Denial of Service Attacks"*, Version 1.10. Sans Portal, 2000, Available from < http://www.sans.org/dosstep/roadmap.php>.

[Singer, 2000] Singer, A. , *"Eight Things That ISP's and Network Managers Can Do to Help Mitigate Distributed Denial of Service Attacks"*, San Diego Supercomputer Center (SDSC), (NPACI), 2000, Available from <http://security.sdsc.edu/publications/ddos.shtml>.

[SOI, 2001] US Subcommittee on Oversight and Investigations Hearing, *"Protecting America's Critical Infrastructures: How Secure are Government Computer Systems?"*, Energycommerce.house.gov, 2001, Available from <http://energycommerce.house.gov/107/hearings/04052001Hearing153/McDonald229.htm>.

[Sophos.com, 2002] Sophos.com, *"Indian Sympathisers Launch Denial of Service Attack on Pakistani Government"*, Available from <http://www.sophos.com/virusinfo/articles/yahae3.html>.

[Spafford, 1998] Spafford, E.H., *"The Internet Worm Program: An Analysis"*, Purdue Technical Report SD-TR-823, Department of Computer Science Purdue University, West Lafayette, IN, 1998.

[Specht, 2003] S. Specht, & R. Lee, *"Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures"*, Princeton University Technical Report CE-L2003-03, 2003.

[TheRegister, 2005] The Register, John Leyden, "Japan.gov weathers DDoS attack", 24th February 2005, Available from <http://www.theregister.com/2005

/02/24/japan_ddos_attack/>.

[Walters, 2001] R. Walters, *"Top 10 Ways to Prevent Denial-of-Service Attacks"*, Information Systems Security. (10) 3, 2001.

[West, 2006] D.M. West, *"Global E-Govenrment, 2006"*, Center for Public Policy, Brown University, Providence, Rhode Island, www.InsidePolitics.org, August 2006.

[WindowsITPro, 2001] WindowsITPro, *"Microsoft Suffers Another DoS Attack"*, WindowsITPro Instant Doc 19770, 2001, Available from <http://www.windows itpro.com/Articles/Index.cfm?ArticleID=19770&DisplayTab=Article>.

Κεφαλαίο 4ο

Ανίχνευση Επιθέσεων Χρησιμοποιώντας eSOM

1. Εισαγωγή

Μετά από τη γενική επισκόπηση στο πρόβλημα των επιθέσεων *Άρνησης Εξυπηρέτησης (DoS)* που παρουσιάσαμε εκτεταμένα στο δεύτερο κεφάλαιο και έχοντας πλέον κατανοήσει τη σοβαρότητα του προβλήματος που καταδεικνύεται από συχνά και μεγάλου βεληνεκούς περιστατικά (Κεφάλαιο 3ο) καλούμαστε να βρούμε αποτελεσματικούς τρόπους αντιμετώπισης των επιθέσεων αυτών. Στο Κεφάλαιο 3 προτείναμε μία σειρά από αποτελεσματικές πρακτικές που μπορούν να υιοθετηθούν από τους οργανισμούς, προκειμένου να διασφαλίσουν σε κάποιο βαθμό τα συστήματά τους. Οι πρακτικές αυτές μπορούν να χρησιμοποιηθούν σαν μία πρώτη γραμμή προστασίας προκειμένου να περιοριστούν οι εισβολές αλλά σίγουρα δεν αποτελούν λύση-πανάκεια. Μία δεύτερη γραμμή προστασίας η *ανίχνευση εισβολών (Intrusion Detection)* είναι απαραίτητη προκειμένου να ανιχνευθούν οι επιθέσεις και να περιοριστούν οι καταστρεπτικές τους συνέπειες.

Σε αυτό το κεφάλαιο προτείνουμε μία μέθοδο ανίχνευσης δικτυακών εισβολών περιλαμβανομένων των επιθέσεων DoS. Το προτεινόμενο σύστημα στοχεύει στην ακριβή και αξιόπιστη διάκριση μεταξύ της παράνομης ("μη-φυσιολογικής") συμπεριφοράς και της νόμιμης ("φυσιολογικής") συμπεριφοράς. Η προτεινόμενη προσέγγιση βασίζεται στην κατάλληλη επεξεργασία αρχείων καταγραφής δικτυακής κυκλοφορίας χρησιμοποιήσαμε μία κατηγορία νευρωνικών δικτύων που είναι γνωστά σαν *αναδυόμενοι Αυτό-Οργανούμενοι Χάρτες (emergent Self-Organizing Maps (eSOM)).*

Τα αρχεία καταγραφής της δικτυακής κίνησης είναι αναμφισβήτητα ένα ισχυρό όπλο προκειμένου να διασφαλίσουμε τα συστήματά μας αλλά και να ανιχνεύσουμε πιθανές εισβολές. Συγκεκριμένα, τα αρχεία καταγραφής δικτυακής κίνησης μας βοηθούν να κατανοήσουμε το λόγο μίας απρόβλεπτης αποτυχίας του συστήματός μας, την έκταση της ζημιάς που προκλήθηκε από μία επίθεση ή ακόμα και την ανίχνευση μίας επίθεσης σε πραγματικό χρόνο.

Από την άλλη πλευρά, οι χάρτες πάντα μας παρείχαν έναν πρακτικό τρόπο πλοήγησης και επέκτασης. Αν και σχεδόν τα πάντα σήμερα έχουν χαρτογραφηθεί, εξακολουθούμε να παρατηρούμε τις δραστηριότητες στον κυβερνοχώρο από την κλειδαρότρυπα [Girardin, 1998]. Οι χάρτες που αναπαριστούν τη δικτυακή κυκλοφορία μπορούν να μας βοηθήσουν σημαντικά προκειμένου να αποκτήσουμε μία καθολική εικόνα για το τι συμβαίνει σε ένα υπολογιστικό δίκτυο και συγκεκριμένα να ανιχνεύουμε με αποτελεσματικότητα πιθανές εισβολές.

Προκειμένου να απαλλάξουμε τους διαχειριστές δικτύων από την ιδιαίτερα δύσκολη και χρονοβόρα εργασία εξέτασης της δικτυακής κυκλοφορίας και να αποφύγουμε μεγάλη επιβάρυνση επεξεργασίας, προτείνουμε μία προσέγγιση ανίχνευσης ανωμαλιών που χρησιμοποιεί τα eSOM για την αναπαράσταση της δικτυακής κυκλοφορίας. Η προσέγγισή μας εκμεταλλεύεται την ανθρώπινη ικανότητα να διαχειρίζεται με αποτελεσματικότητα την πολυπλοκότητα. Η παρακολούθηση της δικτυακής κυκλοφορίας γίνεται φιλική προς το χρήστη και η απεικόνιση της δικτυακής πληροφορίας δίνει νέες δυνατότητες ανίχνευσης και ανάλυσης πιθανών εισβολών.

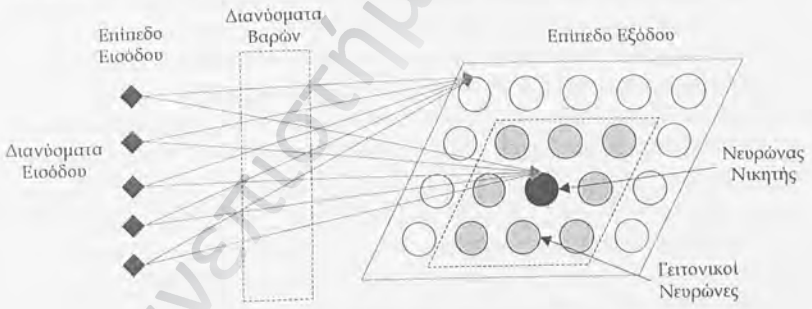
Τα νευρωνικά δίκτυα έχουν το σημαντικό πλεονέκτημα ανοχής σε ανακριβή δεδομένα. Τα eSOM βασίζονται στα απλά Kohonen's SOM (KSOM) αλλά παρουσιάζουν κάποια πλεονεκτήματα που μπορούμε να τα εκμεταλλευτούμε προκειμένου να επιτύχουμε καλύτερα αποτελέσματα στην ανίχνευση εισβολών. Συνδυάζοντας τις τεχνικές μηχανικής μάθησης και της απεικόνισης πληροφοριών έχουμε τη δυνατότητα να έχουμε μία πιο ξεκάθαρη εικόνα της δικτυακής δραστηριότητας. Η προτεινόμενη μέθοδος παράγει υποσχόμενα αποτελέσματα ως προς την ικανότητά της να ταξινομεί τη "φυσιολογική" απέναντι στη "μη-φυσιολογική" συμπεριφορά.

Η προτεινόμενη μέθοδος μπορεί να χρησιμοποιηθεί είτε για την ανάλυση δεδομένων πραγματικού χρόνου είτε για παλαιότερη δικτυακή κυκλοφορία. Για την αξιολόγηση της προσέγγισης χρησιμοποιήθηκε το σύνολο δεδομένων KDD-99 (Knowledge Discovery in Databases) [Kdd, 1999] και όχι αυθαίρετα δημιουργημένα δεδομένα προκειμένου να επιβεβαιωθεί η αξιοπιστία των αποτελεσμάτων.

Ακολουθώντας αυτή την εισαγωγή, το κεφάλαιο αυτό έχει διαμορφωθεί ως εξής. Η ενότητα 2 περιγράφει τον αλγόριθμο KSOM. Η ενότητα 3 παρουσιάζει σχετικές εργασίες προτεινόμενων μεθόδων ανίχνευσης εισβολών που βασίζονται στα KSOM, ενώ η ενότητα 4 περιγράφει τα eSOM και τις διαφορές τους από τα απλά KSOM. Στην ενότητα 5 παρουσιάζουμε την προσέγγισή μας που βασίζεται στα eSOM για την ανίχνευση των επιθέσεων DoS, Probe, R2L (Remote to Local), U2R (User to Root). Παρουσιάζουμε επίσης την αξιολόγηση της προσέγγισής μας καθώς και πειραματικά αποτελέσματα ενώ η ενότητα 6 ολοκληρώνει το κεφάλαιο.

2. Αυτό-Οργανούμενοι Χάρτες

Τα KSOM [Haykin, 1999] έχουν τη βάση τους στη βιολογία. Ανήκουν στην κατηγορία μη-επιτηρούμενης (unsupervised) ή ανταγωνιστικής μάθησης και παράγουν διδιάστατους (2D) τοπολογικούς χάρτες (Σχήμα 4.1 [Kohonen, 2001]), οι οποίοι απεικονίζουν τα δεδομένα εισόδου με βάση την ομοιότητά τους.



Σχήμα 4.1 Η Αρχιτεκτονική του Δικτύου KSOM

Είναι μη-επιτηρούμενα, καθώς δεν υπάρχουν διανύσματα στόχοι όπως στην περίπτωση των δικτύων διανυσματικής οπισθοδιάδοσης (back propagation vector). Τα KSOM εκπαιδεύονται χρησιμοποιώντας μόνο τα χαρακτηριστικά των δεδομένων εκπαίδευσης. Είναι ανταγωνιστικά, γιατί υπάρχει μόνο ένας νευρώνας νικητής στο εξωτερικό επίπεδο. Τα εκπαιδευμένα KSOM δημιουργούν ομάδες δεδομένων, όπου παρόμοια διανύσματα τοποθετούνται σε μία συγκεκριμένη περιοχή στον χώρο εξόδου. Αυτό είναι ιδιαίτερα χρήσιμο για την

ανακάλυψη ομάδων και σχέσεων στα δεδομένα. Η παραγόμενη απεικόνιση είναι τοπολογικά διατηρήσιμη (topology preserving). Τα KSOM χρησιμοποιούνται εκτεταμένα για ανάλυση και απεικόνιση δεδομένων [Oja, 2003].

Η διαδικασία μάθησης στα KSOM αποτελείται από τα ακόλουθα βήματα:

1. Τα τυχαία βάρη w_{ij} αρχικοποιούνται με μικρές τυχαίες τιμές.
2. Χρησιμοποιείται ένα πρότυπο εισόδου x.
3. Υπολογίζεται η Ευκλείδεια απόσταση (εξίσωση 1 [Haykin, 1999]) ανάμεσα στο δείγμα δεδομένων εισόδου x, και στο κάθε βάρος νευρώνα w_{ij}. Ο νικητής (η πιο ταιριαστή μονάδα (Best Matching Unit)) επιλέγεται σαν o(x):

$$o(x) = \arg\min_j \|x - w_{ij}\|, \text{ j=1,2,...} l \tag{4.1}$$

4. Προκειμένου να επιτύχουμε τοπολογική απεικόνιση, προσαρμόζονται όλα τα βάρη στη γειτονιά, ανάλογα με την απόσταση τους από τον νικητή νευρώνα σύμφωνα με την ακόλουθη εξίσωση [Haykin, 1999]:

$$\forall j : w_{ij}(t) = w_{ij}(t-1) + a(t)\eta(t') \cdot \left(x_i(t) - w_{ij}(t-1)\right) \tag{4.2}$$

Όπου a είναι ο ρυθμός εκμάθησης, η η συνάρτηση γειτνίασης και t', ο χρόνος που ξοδεύτηκε στο τρέχον απόσπασμα (context). Η συνάρτηση γειτνίασης η μειώνεται καθώς το t' αυξάνει.

5. Επανάληψη των βημάτων 2, 3, 4 μέχρι να επιτευχθεί σύγκλιση.

Τα KSOM εκπαιδεύονται μέχρι να επιτευχθεί σύγκλιση, κάτι το οποίο εξαρτάται από το πόσο πολύπλοκα είναι τα δεδομένα εισόδου. Τα KSOM επιτρέπουν μία καλύτερη γενική επισκόπηση των δεδομένων που αναπαριστούν την δικτυακή κυκλοφορία. Επιπλέον, είναι μία τεχνική που παρουσιάζει το πλεονέκτημα να βρίσκει κρυμμένες σχέσεις δεδομένων καθώς τα διαιρεί οπτικά σε τμήματα, κάτι που οδηγεί σε μία πολύ ευκολότερη απεικόνιση των δεδομένων.

Τα KSOM απαιτούν ελάχιστες ειδικές γνώσεις και επιτυγχάνουν ρυθμούς μεγάλης ταχύτητας και μετατροπής σε σχέση με άλλες τεχνικές εκμάθησης. Από την άλλη πλευρά, τα KSOM παρουσιάζουν πολλούς περιορισμούς που έχουν σαν αποτέλεσμα ένας απλός χάρτης να μην είναι ικανός να χαρακτηρίσει αξιόπιστα πληροφορίες όπως η δικτυακή κυκλοφορία. Τα eSOM μας βοηθούν να παράγουμε πιο αξιόπιστα αποτελέσματα.

3. Αυτό-Οργανούμενοι Χάρτες και Ανίχνευση Εισβολών

Τα KSOM χρησιμοποιήθηκαν εκτεταμένα στην περιοχή της ανίχνευσης εισβολών. Οι Girardin και άλλοι [Girardin, 1998] πρότειναν ένα πειραματικό σύστημα, το οποίο βασίζεται σε ελατηριακές επικαλύψεις (spring layouts) και μη επιτηρούμενα νευρωνικά δίκτυα που μπορούν να χρησιμοποιηθούν για την ταξινόμηση των καταγεγραμμένων γεγονότων, την εκτίμηση χρήσης, την ανάλυση τάσεων σε πραγματικό χρόνο, την ανίχνευση ανωμαλιών και την

ανίχνευση προσπαθειών εισβολής. Ο Nguyen [Nguyen, 2002] περιγράφει ένα πακέτο λογισμικού που ονομάζεται iSOM, και αποτελεί μία μονάδα του συστήματος ανίχνευσης εισβολών INBOUNDS. Αυτό το λογισμικό πακέτο χρησιμοποιεί KSOM προκειμένου να ανιχνεύσει ανωμαλίες στην κυκλοφορία του υπολογιστικού δικτύου.

Οι Hoglund και άλλοι [Hoglund, 2000] πρότειναν ένα πρωτότυπο σύστημα ανίχνευσης ανωμαλιών σε περιβάλλον UNIX, το οποίο βασίζεται σε ένα κόμβο και παρακολουθεί τους χρήστες των κόμβων του δίκτυου. Το σύστημα αυτό βασίζεται στα KSOM για να εξετάσει αν η συμπεριφορά ενός χρήστη είναι "μη-φυσιολογική". Οι Lichodzijewski και άλλοι [Lichodzijewski, 2002] χρησιμοποιούν ιεραρχικά KSOM προκειμένου να επιτύχουν ανίχνευση εισβολών βασιζόμενη σε ένα κόμβο. Η αρχιτεκτονική του ιεραρχικού KSOM που χρησιμοποιείται αποτελείται από δύο επίπεδα. Το πρώτο επίπεδο αποτελείται από τρεις χάρτες. Κάθε χάρτης απεικονίζει ένα πεδίο των διανυσμάτων δεδομένων και του χρόνου. Ο χάρτης του δεύτερου επιπέδου συνδυάζει τα αποτελέσματα από κάθε χάρτη πρώτου επιπέδου προκειμένου να παρέχει μία ολοκληρωμένη εικόνα της κατάστασης του δικτύου.

Οι Labib και άλλοι [Labib, 2002] προτείνουν ένα σύστημα ανίχνευσης ανωμαλιών που ονομάζεται NSOM (Network-based Self-Organising Map), και το οποίο προσπαθεί να κατηγοριοποιήσει πραγματικά δεδομένα Ethernet χρησιμοποιώντας KSOM. Το KSOM εκπαιδεύεται με κανονικά δεδομένα και στη συνέχεια το σύστημα δοκιμάζεται με πραγματικά δεδομένα Ethernet. Μία επίθεση ανιχνεύεται αν ο νικητής νευρώνας δεν είναι ένας από τους σημειωμένους νευρώνες. Οι Rhodes και άλλοι [Rhodes, 2000] πρότειναν μία προσέγγιση για την ανίχνευση εισβολών χρησιμοποιώντας πολλαπλά KSOM. Η προσέγγισή τους δεν βασίζεται σε ένα μόνο KSOM προκειμένου να ανιχνεύσει εισβολές αλλά κατασκευάζεται μία αρχιτεκτονική στοίβας παρακολούθησης με πολλαπλά KSOM, το κάθε ένα από τα οποία είναι ειδικό στην αναγνώριση "μη-φυσιολογικής" συμπεριφοράς σε ένα συγκεκριμένο πρωτόκολλο.

Οι Jirapummin και άλλοι [Jirapummin, 2002] πρότειναν μία προσέγγιση που βασίζεται στα KSOM και το νευρωνικό δίκτυο ανθεκτικής διάδοσης (Resilient Propagation (RPROP)) προκειμένου να επιτύχουν ανίχνευση εισβολών συνδυάζοντας απεικόνιση (με KSOM) και ταξινόμηση (με RPROP) σε κανονική κυκλοφορία και εισβολές. Οι Gonzalez και Dasgupta [Gonzalez, 2002] χρησιμοποιούν KSOM προκειμένου να συγκρίνουν τα αποτελέσματα μίας Νευρο-απρόσβλητης (Neuro-Immune) προσέγγισης για την ανίχνευση ανωμαλιών με μία μη επιτηρούμενη τεχνική (KSOM). Αυτή η σύγκριση δεν οδηγεί ξεκάθαρα σε ένα νικητή.

Οι Kayacik και άλλοι [Kayacik, 2003] πρότειναν μία προσέγγιση για ανίχνευση εισβολών που βασίζεται σε μία ιεραρχία των KSOM. Προσπάθησαν να ορίσουν κατά πόσο είναι αποτελεσματική μία προσέγγιση ανίχνευσης

εισβολών που βασίζεται σε μία ακολουθία ιεραρχικών KSOM χρησιμοποιώντας μόνο 6 από τα 41 πεδία του συνόλου δεδομένων KDD [KDD, 1999].

Όλες οι παραπάνω προσεγγίσεις ανίχνευσης εισβολών βασίζονται σε απλά KSOM που μπορούν να βελτιωθούν σημαντικά εάν χρησιμοποιηθούν τα eSOM.

4. Αναδυόμενοι Αυτο-Οργανούμενοι Χάρτες

Αν και όπως περιγράφηκε στην προηγούμενη ενότητα τα KSOM παρουσιάζουν πολλά πλεονεκτήματα και έχουν χρησιμοποιηθεί εκτενώς στην ερευνητική περιοχή της ανίχνευσης εισβολών μία ειδική κατηγορία των Αυτο-Οργανούμενων Χάρτων (Self-Organizing Maps) που ονομάζονται *αναδυόμενοι Αυτό-Οργανούμενοι Χάρτες (emergent Self-Organizing Maps (eSOM))* φαίνεται πως παρέχει καλύτερα αποτελέσματα σε σύγκριση με τα KSOM που μπορούμε να τα εκμεταλλευτούμε προκειμένου να επιτύχουμε καλύτερα αποτελέσματα στη διαδικασία ανίχνευσης εισβολών.

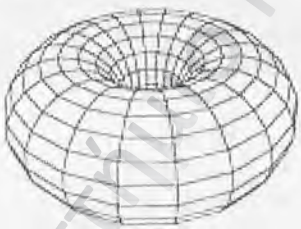
Κάτι που συχνά παραβλέπεται στα KSOM είναι ότι η αυτο-οργάνωση επιτρέπει την ανάδειξη δομής στα δεδομένα. Σύμφωνα με το [Ultsch, 1999] "Ανάδειξη είναι η ικανότητα ενός συστήματος να παράγει ένα φαινόμενο σε ένα νέο, υψηλότερο επίπεδο". Προκειμένου να επιτύχουμε ανάδειξη, είναι απαραίτητη η ύπαρξη και συνεργασία ενός μεγάλου αριθμού στοιχειωδών διαδικασιών. Οι αναδυόμενες δομές έχουν την ικανότητα να περιγράφουν καλύτερα πολύπλοκα συστήματα που αποτελούνται από μονάδες χαμηλού επιπέδου. Η ανάδειξη μπορεί να παρουσιαστεί όχι μόνο σε φυσικά αλλά και σε τεχνητά συστήματα. Τα eSOM έχουν εφαρμοστεί σε έναν ευρύ αριθμό περιοχών περιλαμβανομένων της ιατρικής διάγνωσης [Ultsch, 2004] και της περιβαλλοντικής επιστήμης [Ultsch, 2002].

Ένα από τα βασικά μειονεκτήματα των KSOM είναι ότι οι ικανότητές τους περιορίζονται σε λίγους νευρώνες. Ο μικρός αριθμός νευρώνων (μερικές δεκάδες) των KSOM δεν τους επιτρέπει να παρουσιάσουν ανάδειξη. Πιο συγκεκριμένα σε ένα KSOM σε κάθε νευρώνα αντιστοιχούν τα καλύτερα ταίρια (best matches) ενός μεγάλου αριθμού δεδομένων εισόδου. Έτσι κατά κάποιον τρόπο κάθε νευρώνας αναπαριστά μία ομάδα. Ο περιορισμός των λίγων νευρώνων περιορίζει την τοπολογική διατήρηση των KSOM σε μικρούς χάρτες. Η ομαδοποίηση που βασίζεται σε ένα KSOM έχει πολλά παρόμοια σημεία με τον αλγόριθμο ομαδοποίησης k-Means. Πιο συγκεκριμένα ένα KSOM με λίγους νευρώνες είναι σχεδόν το ίδιο με τον αλγόριθμο ομαδοποίησης k-Means [Ultsch, 2003] όπου k είναι ο αριθμός των νευρώνων του KSOM.

Από την άλλη πλευρά, τα eSOM μπορούν να επεκταθούν από μερικές χιλιάδες σε δεκάδες χιλιάδες νευρώνες. Πιο συγκεκριμένα, ο αριθμός των νευρώνων σε ορισμένες περιπτώσεις μπορεί να είναι μεγαλύτερος από τον αριθμό των δεδομένων. Αυτό έχει σαν αποτέλεσμα μόνο ένα μικρό μέρος των δεδομένων να μπορεί να αναπαρασταθεί από κάθε νευρώνα.

Ο μεγάλος αριθμός νευρώνων στα eSOM είναι απαραίτητος προκείμενου να επιτύχουμε ανάδειξη. Η συνεργασία ενός τέτοιου μεγάλου αριθμού νευρώνων οδηγεί σε δομές ενός υψηλότερου επιπέδου. Αυτή η συνεργασία επιτρέπει την παρατήρηση συστημάτων σε ένα ανώτερο επίπεδο παρατηρώντας τις συνολικές δομές, χωρίς να λαμβάνουμε υπόψη τις τμηματικές δομές και επιτρέποντας μας να παρατηρήσουμε δομές που διαφορετικά θα ήταν αόρατες. Η διαδικασία τμηματοποίησης στα eSOM πραγματοποιείται παρατηρώντας ολόκληρο τον χάρτη που παράγεται από τα eSOM και όχι εστιάζοντας στους νευρώνες του.

Επιπλέον, τα eSOM παρουσιάζουν την έννοια των χαρτών χωρίς σύνορα προκειμένου να αποφευχθούν επιδράσεις ορίων, κάτι που δεν χρησιμοποιείται στα απλά KSOM. Ένα σημαντικό μειονέκτημα που παρουσιάζουν τα KSOM είναι ότι τα σημεία που βρίσκονται στα άκρα του χάρτη περιέχουν πολύ λιγότερους νευρώνες σε σχέση με τα κεντρικά σημεία του χάρτη με αποτέλεσμα να χάνεται πολύτιμη πληροφορία. Η λύση που εφαρμόζουν τα eSOM προκειμένου να αντιμετωπίσουν αυτό το πρόβλημα είναι η συνένωση των άκρων του χάρτη ώστε να δημιουργηθεί ένα σπειροειδές πλέγμα χωρίς όρια όπως απεικονίζεται στο Σχήμα 4.2.

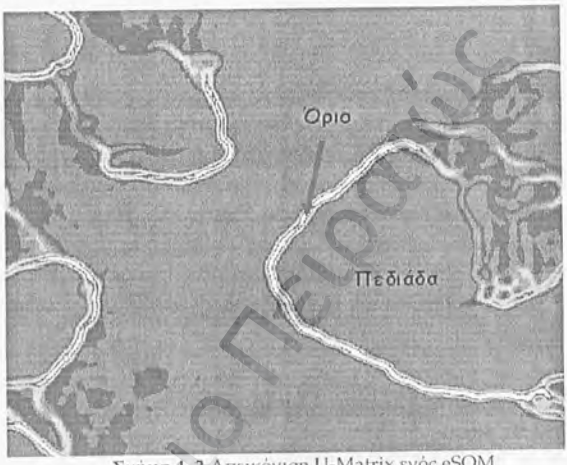


Σχήμα 4. 2 Σπειροειδές Πλέγμα Χάρτη eSOM χωρίς Όρια.

Υπάρχουν πολλές μέθοδοι που μπορούν να χρησιμοποιηθούν προκειμένου να απεικονίσουμε τις δομές που δημιουργούνται από τα eSOM περιλαμβανομένων των βασιζόμενων σε απόσταση (U-Matrix), των βασιζόμενων σε πυκνότητα (P-Matrix) και των βασιζόμενων στην απόσταση και την πυκνότητα (U*-Matrix). Με δοκιμές που πραγματοποιήθηκαν δεν παρατηρήθηκαν σημαντικές διαφορές οι οποίες να επιφέρουν αλλαγές στα πειραματικά μας αποτελέσματα ανάμεσα στις διάφορες μεθόδους απεικόνισης. Για το λόγο αυτό επιλέχθηκε η μέθοδος απεικόνισης που βασίζεται στην απόσταση U-Matrix καθώς είναι η πιο απλή και δημιουργεί τη μικρότερη υπολογιστική επιβάρυνση.

Σύμφωνα με αυτή τη μέθοδο [Ultsch, 1999] το άθροισμα (ύψος) των αποστάσεων ανάμεσα στα βάρη των νευρώνων και των γειτόνων τους κανονικοποιούνται από το μεγαλύτερο ύψος. Το αποτέλεσμα του αθροίσματος των αποστάσεων αναπαρίσταται σαν ανύψωση του κάθε νευρώνα. Με αυτό τον τρόπο, τα δεδομένα εισόδου αναπαριστώνται και απεικονίζονται σαν

τρισδιάστατη εικόνα. Το ύψος θα έχει μεγάλη τιμή σε περιοχές του χάρτη όπου ανήκουν λίγα σημεία δεδομένων και μικρή τιμή σε περιοχές που αναπαριστά ομάδες. Επομένως θα δημιουργηθούν λόφοι (όρια) και πεδιάδες αντίστοιχα όπως φαίνονται στο Σχήμα 4.3.



Σχήμα 4. 3 Απεικόνιση U-Matrix ενός eSOM

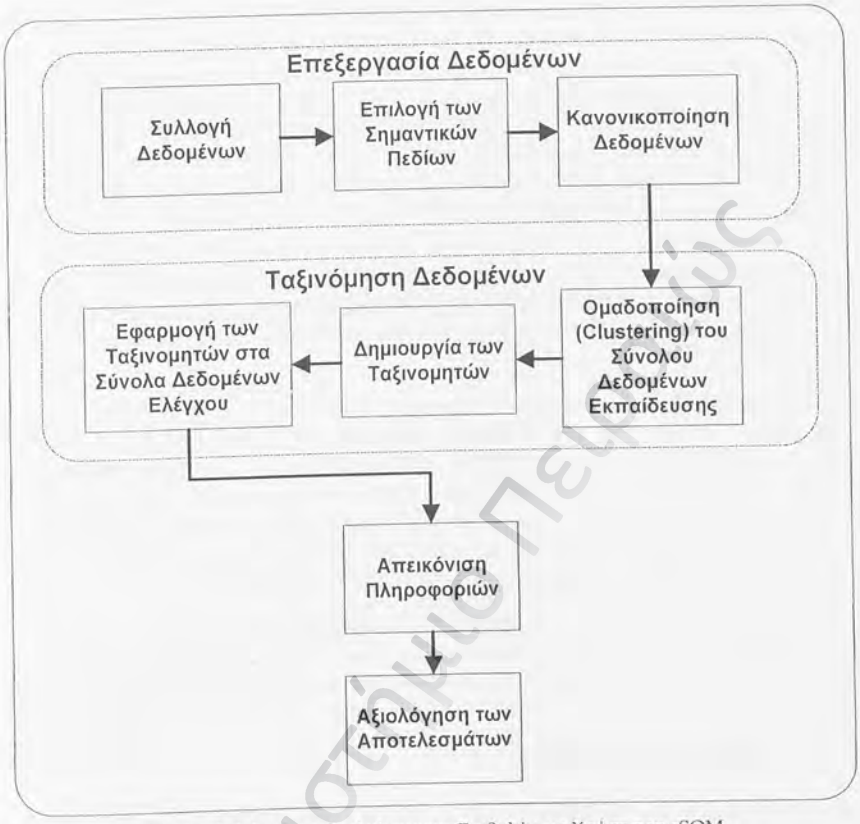
Εάν n είναι ένας νευρώνας στο χάρτη, $NN(n)$ είναι το σύνολο των άμεσων γειτόνων στο χάρτη και $w(n)$ είναι το διάνυσμα βαρών (weight vector) που αντιστοιχεί στον νευρώνα n, τότε το ύψος *U-height* κάθε νευρώνα n δίνεται από την ακόλουθη εξίσωση [Ultsch, 2003]:

$$U\text{-}height(n) = \sum_{m \in NN(n)} d(w(n) - w(m)), \tag{4.3}$$

όπου $d(x,y)$ είναι η απόσταση που χρησιμοποιείται στον αλγόριθμο SOM προκειμένου να κατασκευαστεί ο χάρτης.

5. Ανίχνευση Εισβολών με το eSOM

Η διαδικασία που ακολουθήσαμε προκειμένου να πραγματοποιήσουμε ανίχνευση εισβολών με τη χρήση eSOM, παρουσιάζεται αναλυτικά στο Σχήμα 4.4. Το πρώτο στάδιο περιλαμβάνει την επεξεργασία των δεδομένων που θα χρησιμοποιηθούν για την ταξινόμηση της δικτυακής κίνησης. Αφού λοιπόν συλλέξουμε τα δεδομένα που περιγράφουν τη δικτυακή κυκλοφορία, επιλέγουμε τα σημαντικότερα πεδία των δεδομένων (Παράγραφος 5.2) και στη συνέχεια τα κανονικοποιούμε.



Σχήμα 4. 4 Διαδικασία Ανίχνευσης Εισβολών με Χρήση του eSOM

Προκειμένου, να αποφύγουμε να έχουμε μεγάλη επίδραση των πεδίων των διανυσμάτων εισόδου είναι απαραίτητο να κανονικοποιήσουμε τα δεδομένα εισόδου. Έχουν χρησιμοποιηθεί πολλές μέθοδοι για την κανονικοποίηση των δεδομένων. Κανονικοποιήσαμε τα δεδομένα με μέσο μηδέν και διακύμανση ένα, μία τεχνική που παράγει πολύ καλά αποτελέσματα στις περισσότερες περιπτώσεις όπως αναφέρεται στην βιβλιογραφία [Duda, 2001].

Το επόμενο στάδιο της προσέγγισης ανίχνευσης εισβολών είναι η ταξινόμηση των δεδομένων. Προκειμένου να ταξινομήσουμε τα δεδομένα πραγματοποιούμε ομαδοποίηση (clustering) του συνόλου δεδομένων εκπαίδευσης χρησιμοποιώντας το eSOM.

Εκπαιδεύουμε τα eSOM με υπάρχοντα αρχεία καταγραφής (logs) της δικτυακής κυκλοφορίας και εκμεταλλευόμαστε τα κύρια πλεονεκτήματα των eSOM, δηλαδή το μεγάλο αριθμό των νευρώνων και τη δυνατότητα λήψης

χαρτών χωρίς σύνορα (borderless) ώστε να αποφευχθεί η απώλεια πληροφοριών. Προκειμένου να απεικονίσουμε αυτές τις δομές χρησιμοποιείται η μέθοδος U-Matrix. Η μέθοδος U-Matrix μας επιτρέπει να επιτύχουμε μία καλή απεικόνιση της δικτυακής κυκλοφορίας δίνοντας και τη δυνατότητα να παρατηρήσουμε τη ύπαρξη πιθανών εισβολών. Στην περίπτωση μας, κάθε καταγραφή (log) της δικτυακής κυκλοφορίας αναπαρίσταται με ένα διάνυσμα και κάποια καθορισμένα πεδία. Κάθε διάνυσμα έχει μία μοναδική θέση στο U-Matrix και η απόσταση ανάμεσα στα δύο σημεία είναι η ανομοιότητα των δύο καταγεγραμμένων γεγονότων (logs) της δικτυακής κυκλοφορίας. Το U-Matrix του εκπαιδευμένου συνόλου δεδομένων διαιρείται σε πεδιάδες που αναπαριστούν ομάδες δεδομένων "φυσιολογικής" δικτυακής κίνησης και δεδομένων επίθεσης και λόφους που αναπαριστούν τα όρια ανάμεσα στις ομάδες.

Ανάλογα με τη θέση του καλύτερου ταιριάσματος ενός σημείου εισόδου που χαρακτηρίζει μία σύνδεση, αυτό το σημείο μπορεί να ανήκει σε μία πεδιάδα (ομάδα ("φυσιολογική" ή επιτιθέμενη συμπεριφορά)) ή αυτό το σημείο δεδομένων μπορεί να μην ταξινομηθεί εάν το καλύτερο ταίριασμά του ανήκει σε ένα λόφο (όριο). Επομένως ένα σημείο εισόδου μπορεί να ταξινομηθεί ανάλογα με τη θέση του καλύτερου ταιριάσματός του. Ο χάρτης που θα δημιουργηθεί μετά την εκπαίδευση του eSOM, αναπαριστά τη δικτυακή κυκλοφορία.

Μετά την εκπαίδευση του συνόλου δεδομένων εκπαίδευσης έχει δημιουργηθεί ένας χάρτης στον οποίο είναι ξεκάθαρη η δημιουργία κλάσεων "φυσιολογικής" δικτυακής κίνησης και επιθέσεων (δημιουργία ταξινομητών). Κάθε μία από αυτές τις ομάδες (κλάσεις) χρησιμοποιείται στη συνέχεια για την ταξινόμηση νέων συνόλων δεδομένων (εφαρμογή των ταξινομητών στα σύνολα δεδομένων ελέγχου).

Εφαρμόζοντας τους ταξινομητές στα νέα σύνολα δεδομένων δικτυακής κίνησης λαμβάνουμε μία νέα οπτική απεικόνιση η οποία παρουσιάζει πως ταξινομούνται τα δεδομένα ελέγχου στις υπάρχουσες κλάσεις.

5.1 Το Σύνολο Δεδομένων KDD

Το σύνολο δεδομένων KDD-99 (Knowledge Discovery in Databases) [Kdd, 1999] είναι ένα πρότυπο σύνολο δεδομένων που μπορεί να χρησιμοποιηθεί προκειμένου να αξιολογήσουμε προτεινόμενες προσεγγίσεις στην περιοχή της ανίχνευσης εισβολών και χρησιμοποιείται ευρέως σαν ένα σύνολο δεδομένων σημείο αναφοράς στην ανίχνευση εισβολών. Οι επιθέσεις που περιλαμβάνονται σε αυτό το σύνολο δεδομένων ανήκουν σε μία από τις ακόλουθες κατηγορίες: DoS, R2L (Remote to Local), U2R (User to Root) και Probe. Σε αυτό το σύνολο δεδομένων, κάθε σύνδεση χαρακτηρίζεται από 41 πεδία (αναλυτική περιγραφή των πεδίων παρουσιάζεται στο Παράρτημα Α). Από το 10% του KDD συνόλου δεδομένων με χαρακτηρισμό (labeled) χρησιμοποιήσαμε σύνολα δεδομένων πολύ μικρότερου μεγέθους προκειμένου να εξετάσουμε τα αποτελέσματα της

προσέγγισής μας σε όλους τους τύπους επιθέσεων περιλαμβανομένων της Probe, R2L και U2R των οποίων η αναλογία ενάντια των επιθέσεων DoS είναι πολύ μικρότερη όπως φαίνεται στον Πίνακα 4.1.

Επιθέσεις Άρνησης Εξυπηρέτησης (DoS): Όπως έχουμε αναφέρει στο Κεφάλαιο 2, ο κύριος στόχος μίας επίθεσης DoS είναι η διακοπή των υπηρεσιών προσπαθώντας να περιορίσει την πρόσβαση σε μία μηχανή ή υπηρεσία. Παραδείγματα επιθέσεων DoS είναι οι επιθέσεις back, land, pod, teardrop, smurf και neptune.

Πίνακας 4. 1. Χαρακτηριστικά του Συνόλου Δεδομένων KDD

Σύνολο Δεδομένων 10% KDD											
DoS	back	2203	R2L	ftp write	8	Probe	ipsweep	1247	U2R	Buffer overflow	8
	land	21		Guess passwd	53		nmap	231		Load module	53
	pod	264		imap	12		portsweep	1040		Perl	3
	teardrop	979		multihop	7		satan	1589		Rootkit	10
	smurf	280790		phf	4						
	neptune	107201		spy	2						
				warezclient	1020						
				Warezmaster	20						
	Συνολικές DoS	**391458**		**Συνολικές R2L**	**1126**		**Συνολικές Probe**	**4107**		**Συνολικές U2R**	**52**
Συνολικές επιθέσεις		**396743**									
Συνολικά "φυσιολογικά' δεδομένα		**97278**									

Remote to Local (R2L): Σε μία επίθεση Remote to Local ο επιτιθέμενος κερδίζει μη εξουσιοδοτημένη τοπική πρόσβαση από μία απομακρυσμένη μηχανή και εκμεταλλεύεται αυτή την πρόσβαση προκειμένου να στείλει πακέτα στο δίκτυο. Παραδείγματα επιθέσεων R2L είναι οι επιθέσεις ftp_write, guess passwd, imap, warezclient, warezmaster, phf, spy και multihop.

User to Root (U2R): Σε μία επίθεση U2R ο επιτιθέμενος κερδίζει μη εξουσιοδοτημένη πρόσβαση σε τοπικά δικαιώματα υπερ-χρήστη (root). Παραδείγματα είναι οι επιθέσεις loadmodule, perl, rookit και buffer overflow[1].

Probe: Ο επιτιθέμενος εξετάζει ένα δίκτυο προκειμένου να βρει αδυναμίες που απαιτούν λιγότερη τεχνική εξειδίκευση. Παραδείγματα επιθέσεων Probe είναι οι επιθέσεις ipsweep, nmap, portsweep και satan.

[1] Η υπερχείλιση προσωρινής μνήμης (buffer overflow) αποτελεί μία επίθεση User to Root (U2R) παρόλα αυτά όπως αναφέρθηκε στο Κεφάλαιο 2 μπορεί να χρησιμοποιηθεί σαν πρώτο βήμα ώστε στη συνέχεια να επιτευχθεί επίθεση Άρνησης Εξυπηρέτησης.

Αναλυτική περιγραφή όλων των επιθέσεων που περιλαμβάνονται στο σύνολο δεδομένων KDD παρουσιάζονται στο Παράρτημα Β.

5.2 Επιλογή Πεδίων

Μία πολύ σημαντική απόφαση είναι η επιλογή των πεδίων των διανυσμάτων που θα χρησιμοποιηθούν στην ταξινόμηση με τα eSOM. Τα πεδία της δικτυακής κυκλοφορίας θα πρέπει να είναι σε κατάλληλη μορφή προκειμένου να τα επεξεργαστεί το eSOM και αντιπροσωπευτικά της δικτυακής δραστηριότητας προκειμένου να μπορέσουμε να διακρίνουμε τη "φυσιολογική" από τη "μη-φυσιολογική" συμπεριφορά. Είναι σημαντικό τα επιλεγμένα πεδία των διανυσμάτων να αυξάνουν την αντίθεση ανάμεσα στη "φυσιολογική" και στη "μη- φυσιολογική" συμπεριφορά όσον αφορά στις δικτυακές επιθέσεις.

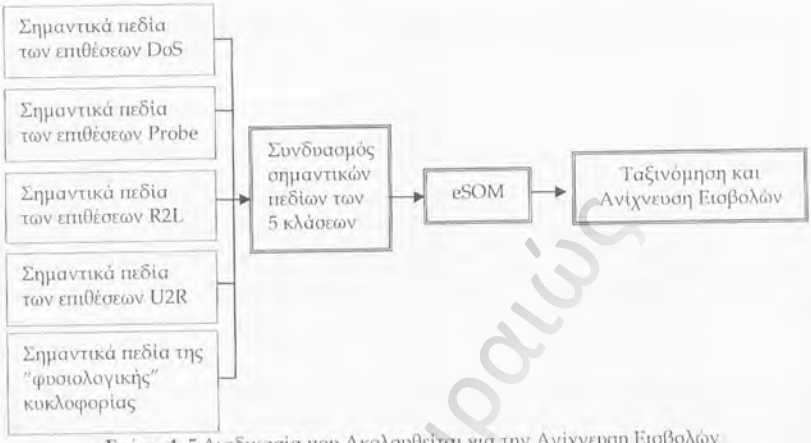
Οι Mukkamala και άλλοι [Mukkamala, 2003] αναγνώρισαν τα πιο σημαντικά χαρακτηριστικά από το σύνολο δεδομένων KDD-99 χρησιμοποιώντας δύο μεθόδους ταξινόμησης τις Μηχανές Διανυσμάτων Υποστήριξης (SVMs (Support Vector Machines)) και τα Τεχνητά Νευρωνικά Δίκτυα (ANNs (Artificial Neural Networks)). Τα πιο σημαντικά πεδία για τις πέντε κλάσεις του συνόλου δεδομένων KDD (DoS, Probe, R2L, U2R και "φυσιολογική" δικτυακή κίνηση) από τα 41 πεδία του συνόλου δεδομένων KDD αναπαριστώνται στον Πίνακα 4.2 [Gonzalez, 2002].

Πραγματοποιήσαμε μία δυαδική ταξινόμηση χρησιμοποιώντας τα σημαντικά πεδία κάθε τύπου επιθέσεων και πολυ-ταξική ταξινόμηση συνδυάζοντας τα πιο σημαντικά πεδία για τους τέσσερις τύπους επιθέσεων (DoS, Probe, R2L, U2R) (13 πεδία) και τα πιο σημαντικά πεδία κάθε τύπου επίθεσης και φυσιολογικών δεδομένων (18 πεδία) (Σχήμα 4.5).

Πρέπει να σημειώσουμε εδώ για τα πεδία των οποίων οι τιμές είναι αλφαριθμητικές, προκειμένου να πραγματοποιήσουμε τα πειράματα μας αντιστοιχίζουμε κάθε στιγμιότυπο της αλφαριθμητικής τιμής σε αυξανόμενες ακέραιες τιμές. Για παράδειγμα για το πεδίο Υπηρεσίας ("Service") η αντιστοιχία που εφαρμόσαμε είναι της μορφής http→1, ftp→2, smtp→3 κ.ο.κ.

Πίνακας 4. 2 Σημαντικά Πεδία για τις Πέντε Κλάσεις του Συνόλου Δεδομένων KDD

"Φυσιολογική" κίνηση	DoS
Duration	Duration
Service	Source Bytes
Source bytes	Destination bytes
Destination bytes	Count
Hot indicators	Same Service Rate
File creations	Connections with SYN errors
Count	Connections –Same Service –SYN errors
REG error rate	Destination-Host Count
Same service-REG error rate	Destination-Host-Same source- port rate
Same service rate	Destination-Host-SYN error rate
Destination-Host-Service-Count	Destination-Host-Same-Service error rate
Destination-Host-Same source- port rate	
Destination-Host-Service source- SYN error rate	
Probe	**R2L**
Service	Service
Source bytes	Source bytes
Destination bytes	Destination bytes
Count	Destination-Host Count
Same service rate	Destination-Host-Service Count
Destination-Host Count	Same service rate
Destination-Host-Same Service Count	
U2R	
Source bytes	
Destination bytes	
Destination-Host Count	
Destination-Host-Service Count	



Σχήμα 4. 5 Διαδικασία που Ακολουθείται για την Ανίχνευση Εισβολών

5.3 Πειραματικά Αποτελέσματα

Πραγματοποιήσαμε μία σειρά πειραμάτων προκειμένου να εξετάσουμε την αποτελεσματικότητα της προτεινόμενης προσέγγισης. Για την αξιολόγηση χρησιμοποιήσαμε το εργαλείο Databionics eSOM ([Ultsch, 2005], [Databionic, 2007]).

Προκειμένου να πραγματοποιήσουμε ομαδοποίηση με eSOM U-Matrices ακολουθήσαμε την διαδικασία που περιγράφεται αναλυτικά στην προηγούμενη ενότητα. Τα καλύτερα ταιριάσματα (best matches) των εκπαιδευμένων δεδομένων και επομένως το αντίστοιχο σύνολο δεδομένων χωρίζονται (χειρωνακτικά) σε ομάδες που αναπαριστούν "φυσιολογική" συμπεριφορά και συμπεριφορά επίθεσης. Επομένως, αναγνωρίζουμε τις περιοχές του χάρτη που αναπαριστούν μία ομάδα η οποία ακολούθως μπορεί να χρησιμοποιηθεί για την ταξινόμηση νέων συνόλων δεδομένων.

Οι Πίνακες 4.3 και 4.4 παρουσιάζουν τα σύνολα δεδομένων (ΣΔ) που χρησιμοποιήθηκαν προκειμένου να εκπαιδεύσουμε και να δοκιμάσουμε την προσέγγισή μας. Στον Πίνακα 4.3 περιγράφονται σύνολα δεδομένων (ΣΔ) που περιλαμβάνουν μόνο επιθέσεις DoS ενώ στον Πίνακα 4.4 περιγράφονται σύνολα δεδομένων (ΣΔ) που περιλαμβάνουν όλους τους τύπους επιθέσεων. Όλα τα σύνολα δεδομένων είναι τμήματα διαφόρων μεγεθών, του διαθέσιμου συνόλου δεδομένων του 10% KDD, τα οποία περιλαμβάνουν "φυσιολογικά" δεδομένα και επιθέσεις DoS, Probe, R2L και U2R.

Πίνακας 4. 3 Σύνολα Δεδομένων που Χρησιμοποιήθηκαν για Αξιολόγηση

Σύνολα Δεδομένων	Δεδομένα "Φυσιολογικής" Κίνησης	Συνολικές DoS	Επιθέσεις DoS	
ΣΔ_1	29126	10697	3695 smurf	2002 back
			5000 neptune	
ΣΔ_2	10517	3000	1000 smurf	1000 back
			1000 neptune	
ΣΔ_3	30180	9816	3695 smurf	2002 back
			4000 neptune	20 pod
			99 teardrop	
ΣΔ_4	39238	19938	7001 smurf	2002 back
			397 teardrop	17 land
ΣΔ_5	39298	13939	5001 smurf	2002 back
			6419 neptune	119 pod
			397 teardrop	1 land
ΣΔ_6	39238	10339	4001 neptune	2002 back
			4001 smurf	119 pod
				17 land
ΣΔ_7	32768	30763	18992 neptune	102 pod
			11258 smurf	17 land
			394 teardrop	
ΣΔ_8	10505	9000	5000 neptune	4000 neptune
ΣΔ_9	10505	10000	8000 smurf	2000 neptune
ΣΔ_10	39320	11950	11950 neptune	
ΣΔ_11	10517	4000	4000 neptune	
ΣΔ_12	39299	11278	11278 smurf	
ΣΔ_13	10518	7563	7563 smurf	
ΣΔ_14	15005	15000	15000 neptune	
ΣΔ_15	10000	20000	20000 smurf	

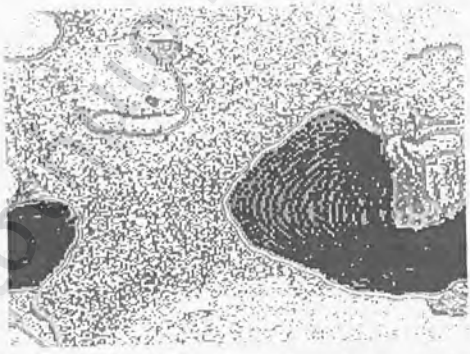
Πίνακας 4. 4 Σύνολα Δεδομένων που Χρησιμοποιήθηκαν για Αξιολόγηση

Σύνολο Δεδομένων	Επιθέσεις	"Φυσιολογική" δικτυακή κίνηση
ΣΔ_16	3732 DoS	5065
ΣΔ_17	3737 DoS	5064
ΣΔ_18	2052 Probe	3905
ΣΔ_19	2055 Probe	3503
ΣΔ_20	562 R2L	1001
ΣΔ_21	564 R2L	1001
ΣΔ_22	3732 DoS	10072
	2052 Probe	
	562 R2L	
	26 U2R	
	6372 Συνολικές επιθέσεις	
ΣΔ_23	3737 DoS	9669
	2055 Probe	
	564 R2L	
	27 U2R	
	6383 Συνολικές επιθέσεις	

Πρέπει να σημειώσουμε εδώ ότι, καθώς η διαδικασία εκπαίδευσης παρουσιάζει μεγάλη υπολογιστική επιβάρυνση ειδικά εάν ο αριθμός των δεδομένων εισόδου ξεπερνά τις 10,000, τα πειράματα αξιολόγησης περιορίζονται σε σύνολα δεδομένων των οποίων το μέγεθος κυμαίνεται από 20,000 έως 60,000 εγγραφές. Φυσικά αυτό το μειονέκτημα μπορεί να εξισορροπηθεί εάν λάβουμε υπόψη μας το γεγονός ότι η εκπαίδευση πραγματοποιείται μόνο μία φορά και η ακρίβεια των αποτελεσμάτων για δεδομένα ελέγχου είναι πολύ υψηλή.

Πραγματοποιήσαμε δυαδική ταξινόμηση (δηλ. "φυσιολογικά" δεδομένα /δεδομένα επίθεσης) για να ταξινομήσουμε κάθε κλάση επιθέσεων (DoS, Probe, R2L, U2R) ενάντια της "φυσιολογικής" κυκλοφορίας.

Ο χάρτης eSOM ενός εκπαιδευμένου συνόλου δεδομένων ("φυσιολογικά" δεδομένα - δεδομένα επίθεσης DoS) απεικονίζεται στο Σχήμα 4.6. Όπως φαίνεται ξεκάθαρα τα δεδομένα εκπαίδευσης μπορούν να διαχωριστούν σε δύο κλάσεις που είναι πολύ ευδιάκριτες, κλάση κανονικών δεδομένων (σκούρο χρώμα) και κλάση δεδομένων επίθεσης (ανοιχτό χρώμα). Στο Σχήμα 4.7 απεικονίζεται η μορφή που λαμβάνει ο χάρτης εκπαίδευσης όταν σε αυτόν εφαρμοστούν τα δεδομένα ελέγχου.

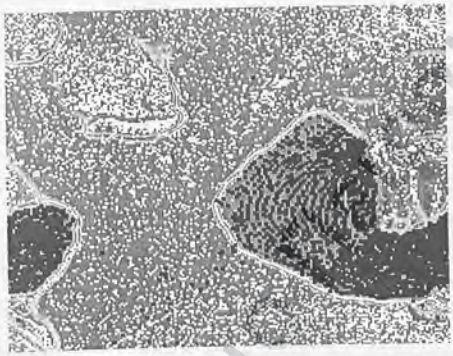


Σχήμα 4. 6. eSOM U-Matrix του Συνόλου Δεδομένων Εκπαίδευσης

Προκειμένου να αξιολογήσουμε την αποτελεσματικότητα της προτεινόμενης προσέγγισης χρησιμοποιήσαμε δύο μέτρα: το *ρυθμό ανίχνευσης (Detection Rate (DR))* και το *ρυθμό λανθασμένων συναγερμών (False alarm Rate (FR))* που ορίζονται στο [Rhodes, 2000], ως εξής:

$$\mathrm{DR} = \frac{TP}{TP + FN}, \mathrm{FR} = \frac{FP}{TN + FP}, \tag{4.4}$$

όπου TP είναι ο αριθμός των πραγματικών (T) θετικών (True Positives (TP)) (καταγεγραμμένα αρχεία επιθέσεων που ταξινομούνται σαν επιθέσεις), TN ο αριθμός των πραγματικών (T) αρνητικών (True Negatives (TN)) (καταγεγραμμένα αρχεία φυσιολογικής συμπεριφοράς που ταξινομούνται σαν φυσιολογικά), FP ο αριθμός των λανθασμένων θετικών (False Positives (FP)) (καταγεγραμμένα αρχεία φυσιολογικής συμπεριφοράς που ταξινομούνται σαν επιθέσεις) και FN ο αριθμός των λανθασμένων αρνητικών (False Negatives (FN)) (καταγεγραμμένα αρχεία επιθέσεων που ταξινομούνται σαν φυσιολογική συμπεριφορά).



Σχήμα 4. 7.eSOM U-Matrix του Συνόλου Δεδομένων Ελέγχου

Η πιο αποτελεσματική προσέγγιση πρέπει να μειώνει όσο το δυνατόν περισσότερο το *ρυθμό των λανθασμένων συναγερμών (False Alarm rate (FA))* και την ίδια στιγμή να αυξάνει το *ρυθμό ανίχνευσης (Detection Rate (DR))*.

Οι Πίνακες 4.5 και 4.6 παρουσιάζουν τα αποτελέσματα της αξιολόγησης των διάφορων πειραμάτων που πραγματοποιήσαμε. Στους πίνακες αυτούς παρουσιάζονται ο *ρυθμός ανίχνευσης (Detection Rate (DR))* και ο *ρυθμός λανθασμένων συναγερμών (False Alarm rate (FA))* για κάθε πείραμα καθώς και οι παράμετροι που χρησιμοποιήθηκαν για την εκπαίδευση του eSOM. Σύμφωνα με το [Ultsch, 2005] προκειμένου να αποφύγουμε τοπολογικά λάθη η ιδανική αρχιτεκτονική πρέπει να έχει τουλάχιστον 4000 νευρώνες και ο λόγος των γραμμών και των στηλών πρέπει να είναι διαφορετικός από τη μονάδα. Στον Πίνακα 4.6 απεικονίζονται τα αποτελέσματα πειραμάτων που πραγματοποιήθηκαν με σχετικά μικρά αρχεία (αναλογικά με τα αρχεία του Πίνακα 4.4). Για το λόγο αυτό τα πειράματα του Πίνακα 4.6 πραγματοποιήθηκαν με 50x82 νευρώνες και 20 επαναλήψεις εκπαίδευσης ενώ τα πειράματα του Πίνακα 4.6 πραγματοποιήθηκαν με 160x180 ή 180x200 νευρώνες και οι επαναλήψεις εκπαίδευσης κυμαίνονται μεταξύ 50 και 60. Η Γκαουσιανή (Gaussian) συνάρτηση:

Πίνακας 4. 5 Αποτελέσματα Αξιολόγησης

Πειράματα Αξιολόγησης	Σύνολα Δεδομένων Εκπαίδευσης	Σύνολα Δεδομένων Δοκιμής	Παράμετροι Εκπαίδευσης	DR	FA
Πείραμα 1	ΣΔ_1	ΣΔ_2	160x180 νευρώνες 50 εποχές	98.9%	0.9%
Πείραμα 2	ΣΔ_3	ΣΔ_2	160x180 νευρώνες 50 εποχές	99.46%	1.1%
Πείραμα 3	ΣΔ_4	ΣΔ_8	160x180 νευρώνες 50 εποχές	98.3%	2.9%
Πείραμα 4	ΣΔ_5	ΣΔ_9	160x180 νευρώνες 50 εποχές	99.4%	0.21%
Πείραμα 5	ΣΔ_6	ΣΔ_8	180x200 νευρώνες 60 εποχές	99.17%	0.3%
Πείραμα 6	ΣΔ_6	ΣΔ_9	180x200 νευρώνες 60 εποχές	99.24%	0.32%
Πείραμα 7	ΣΔ_7	ΣΔ_8	180x200 νευρώνες 60 εποχές	98.3%	2.9%
Πείραμα 8	ΣΔ_10	ΣΔ_11	180x200 νευρώνες 60 εποχές	98.8%	1.61%
Πείραμα 9	ΣΔ_10	ΣΔ_14	180x200 νευρώνες 60 εποχές	99.43%	0.39%
Πείραμα 10	ΣΔ_12	ΣΔ_13	160x180 νευρώνες 50 εποχές	99.81%	0.1%
Πείραμα 11	ΣΔ_12	ΣΔ_15	160x180 νευρώνες 50 εποχές	99.89%	0.05%
Πείραμα 12	ΣΔ_6	ΣΔ_15	180x200 60 εποχές	99.78%	0.34%

Πίνακας 4. 6 Αποτελέσματα Αξιολόγησης

Πειράματα	Αριθμός Πεδίων	Σύνολα Δεδομένων Εκπαίδευσης	Σύνολα Δεδομένων Ελέγχου	DR	FA
Πείραμα 13	11	ΣΔ_16	ΣΔ_17	93,55%	0,21%
Πείραμα 14	7	ΣΔ_18	ΣΔ_19	91,33%	0,25%
Πείραμα 15	5	ΣΔ_20	ΣΔ_21	95,92%	2,6%
Πείραμα 16	13	ΣΔ_22	ΣΔ_23	93% DoS 96,29% U2R 98,97% Probe 92,3% R2L 96,29% U2R 95,17% **Συνολικό**	6,39%
Πείραμα 17	18	ΣΔ_22	ΣΔ_23	99,49% DoS 99,75% probe 99,46% R2L 100% R2L 99,59% **Συνολικό**	3.4%

$$f(x_i, x_j) = exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right)$$

για ένα σύνολο δεδομένων $D = \{x_i, y_i\}_{i=1}^{n}$, χρησιμοποιήθηκε σαν συνάρτηση πυρήνα γειτνίασης και μέθοδο αρχικοποίηση βαρών ενώ σαν συνάρτηση απόστασης η ευκλείδεια. Ο αρχικός και τελικός ρυθμός εκμάθησης ήταν 0.5 και 0.1 αντίστοιχα και η αρχική τιμή για την ακτίνα (radius) ήταν 79 (για 160x180 νευρώνες), 89 (για 180x200), 24 (για 50x82) ενώ η τελική ακτίνα 1. Επιπλέον προκειμένου να αποφύγουμε τοπολογικά λάθη που προκαλούνται από την επίδραση των ορίων χρησιμοποιήσαμε σπειροειδές πλέγμα χωρίς όρια.

5.3.1 Σχολιασμός και Σύγκριση Αποτελεσμάτων

Η πιο πρόσφατη ερευνητική εργασία σε αυτή την περιοχή που χρησιμοποιεί SOM [Kayacik, 2003] που ξεπερνά όλες τις προηγούμενες προτάσεις αναφέρει ρυθμούς ανίχνευσης για όλες τις επιθέσεις που περιλαμβάνονται στο KDD σύνολο δεδομένων, κυμαίνονται μεταξύ 89% και 99.7% ανάλογα με το τμήμα δεδομένων που χρησιμοποιήθηκε για τη δοκιμή στο σύνολο δεδομένων KDD-99 και ρυθμό λανθασμένων θετικών συναγερμών (false alarm) να κυμαίνεται μεταξύ 4.6% και 1.7% αντίστοιχα.

Όπως φαίνεται στους Πίνακες 4.5 και 4.6 (πειράματα 13, 14, 15) όπου εμφανίζονται τα αποτελέσματα αξιολόγησης για *δυαδική ταξινόμηση*, ο ρυθμός ανίχνευσης κυμαίνεται από 89% έως 99.7% όταν στα σύνολα δεδομένων εκπαίδευσης και δοκιμής περιλαμβάνεται μόνο ένα είδος επίθεσης (είτε DoS, είτε R2L, είτε U2R, είτε Probe) και ο αντίστοιχος ρυθμός λανθασμένων συναγερμών κυμαίνεται από 0.1% έως 2.6%. Ο υψηλότερος ρυθμός ανίχνευσης και ο χαμηλότερος ρυθμός συναγερμών επιτυγχάνονται για τις επιθέσεις DoS ενώ στις επιθέσεις R2L παρουσιάζεται ο υψηλότερος ρυθμός λανθασμένων συναγερμών ίσος με 2.6%. Στο πείραμα 16 (Πίνακας 4.6) χρησιμοποιήσαμε τα 13 πιο σημαντικά πεδία που προέρχονται από τον συνδυασμό των σημαντικών πεδίων για κάθε τύπο επίθεσης (DoS, R2L, U2R, probe). Ο ρυθμός ανίχνευσης, σε αυτό το πείραμα, για κάθε τύπο επίθεσης κυμαίνεται από 93% έως 98.97% για κάθε τύπο επίθεσης ενώ ο συνολικός ρυθμός ανίχνευσης είναι ίσος με 95.17%. Ο υψηλότερος ρυθμός ανίχνευσης επιτυγχάνεται για τις επιθέσεις Probe. Ο αντίστοιχος ρυθμός λανθασμένου συναγερμού είναι πολύ υψηλός και ίσος με 6.7%. Στο πείραμα 17 (Πίνακας 4.6) χρησιμοποιήσαμε τα σημαντικά πεδία που προέρχονται από κάθε τύπο επίθεσης και τα σημαντικά πεδία για την κανονική κυκλοφορία (18 πεδία). Ο ρυθμός ανίχνευσης χρησιμοποιώντας 18 πεδία κυμαίνεται από 99.46% έως 100% για κάθε τύπο επίθεσης και ο αντίστοιχος ρυθμός λανθασμένων συναγερμών παρουσιάζει μία σημαντική μείωση όσον αφορά στο ρυθμό των λανθασμένων συναγερμών φτάνοντας το 3.4%.

Η προσέγγιση ανίχνευσης εισβολών χρησιμοποιώντας eSOM παρουσιάζει πολύ καλά αποτελέσματα με πολύ χαμηλούς ρυθμούς λανθασμένων συναγερμών όταν στα σύνολα δεδομένων εκπαίδευσης και δοκιμής περιλαμβάνεται μόνο μία επίθεση. Όταν τα σύνολα δεδομένων εκπαίδευσης και δοκιμής περιλαμβάνουν περισσότερες επιθέσεις τα αποτελέσματα είναι πιο υποσχόμενα όταν χρησιμοποιούμε 18 πεδία που προέρχονται από το συνδυασμό των σημαντικών πεδίων κάθε τύπου επίθεσης και "φυσιολογικής" δικτυακής κυκλοφορίας.

Για την αξιολόγηση της προσέγγισής μας χρησιμοποιήσαμε το σύνολο δεδομένων KDD [KDD, 1999] που χρησιμοποιείται ευρέως προκειμένου να συγκρίνουμε τις προσεγγίσεις ανίχνευσης εισβολών σαν ένα βασικό σύνολο δεδομένων σύγκρισης. Αν και τα υποσύνολα που χρησιμοποιήσαμε επιλέχθηκαν τυχαία και είναι διαφορετικά από τα υποσύνολα που χρησιμοποιήθηκαν σε προηγούμενες προσεγγίσεις τα αποτελέσματα είναι πολύ ενθαρρυντικά.

Από τα παραπάνω αποτελέσματα, αποδεικνύεται ότι η προτεινόμενη μέθοδος είναι ικανή να κάνει ακριβείς ταξινομήσεις επιθέσεων και δεδομένων "φυσιολογικής" δικτυακής κυκλοφορίας και έχει μικρότερη απόκλιση από άλλες προτεινόμενες μεθόδους. Επιπλέον, πρέπει να σημειωθεί ότι προκειμένου να είμαστε σίγουροι ότι η προσέγγισή μας θα παρέχει πάντα αξιόπιστα και ακριβή αποτελέσματα πρέπει να ανανεώνουμε το εκπαιδευμένο χάρτη eSOM σύμφωνα με νέα πρότυπα δικτυακών επιθέσεων.

6. Επίλογος

Εκμεταλλευόμενοι την απεικόνιση της δικτυακής κυκλοφορίας η προσέγγισή μας ανιχνεύει τις δικτυακές επιθέσεις ταξινομώντας κακόβουλη και "φυσιολογική" δικτυακή δραστηριότητα. Η προτεινόμενη μέθοδος είναι ιδιαιτέρα ισχυρή στην παραγωγή αποδοτικών αποτελεσμάτων. Το κύριο πλεονέκτημά της επικεντρώνεται στο γεγονός ότι τα eSOM επεκτείνουν τις ικανότητες των απλών KSOM αναπτύσσοντας δομές υψηλού επιπέδου που δεν θα ήταν ορατές με απλά KSOM στα οποία χρησιμοποιούνται μόνο λίγοι νευρώνες.

Το κύριο μειονέκτημα είναι η υψηλή υπολογιστική επιβάρυνση που δημιουργείται κατά τη διάρκεια της εκπαίδευσης των συνόλων δεδομένων τα οποία έχουν μέγεθος μεγαλύτερο από 10,000 εγγραφές. Αλλά σίγουρα η υπολογιστική επιβάρυνση του eSOM δεν απαγορεύει τη χρήση του, καθώς πραγματοποιείται μόνο κατά τη διάρκεια της εκπαίδευσης, η οποία δεν πραγματοποιείται τόσο συχνά όσο ο ελεγχος με νέα δεδομένα δικτυακής κίνησης. Επιπλέον, κατά τη διαδικασία ταξινόμησης οι κλάσεις των ταξινομημένων δεδομένων πρέπει να οριστούν χειρωνακτικά μέσω της παρατήρησης του χάρτη κάτι που μπορεί να εισάγει ένα διαδικαστικό λάθος.

Βιβλιογραφία

[Databionic, 2007] *Databionic eSOM Tools*, Available from <http://databionic-esom.sourceforge.net/devel.html>.

[Douligeris, 2004] C. Douligeris, A. Mitrokotsa, *"DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art"*, Computer Networks, Vol. 44, (5), April 2004, pp.643-666.

[Duda, 2001] R.O. Duda, P.E. Hart, D.G. Stork, *"Pattern Classification"*, A Wiley-Interscience Publication, John Wiley & Sons, Inc. 2001, Second Edition.

[Gonzalez, 2002] F. Gonzalez, D. Dasgupta, *"Neuro-Immune and Self-Organizing Map Approaches to Anomaly Detection"*, In Proc. of 1st ICAIS, pp. 203-211, UK, 9-11 September 2002.

[Girardin, 1998] L. Girardin, D. Brodbeck, *"A Visual Approach for Monitoring for Logs"*, In Proceedings of the 12th Systems Administration Conference (LISA – 98), Boston, Massachusetts, December 1998, pp. 299 - 308

[Haykin, 1999] S. Haykin, *"Neural Networks: A Comprehensive Foundation"*, Prentice-Hall, New Jersey, USA, 2nd edition, 1999.

[Hoglund, 2000] A. J. Hoglund, K. Hatonen, A. S. Sorvari, *"A Computer Host-based User Anomaly Detection System Using the SOM"*, In Proceedings of IEEE IJCNN 2000, Vol. 5, pp. 411-416.

[Kayacik, 2003] G.H. Kayacik, A.N. Zincir-Heywood, M.I. Heywood, *"On the Capability of SOM based Intrusion Detection Systems"*, In Proceedings of IEEE IJCNN, Portland, USA, July 2003.

[Kdd, 1999] The UCI KDD Archive Information and Computer Science University of California, Irvine, *"Kdd Cup 1999 Data"*, October 1999, Available from http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html.

[Kohonen, 2001] T. Kohonen, *"Self-Organizing Maps"*, 3rd Edition, Springer, New York, NY, 2001.

[Labib, 2002] K. Labib, V. Rao Vemuri, *"NSOM: A Real-time Network-Based Intrusion Detection System Using Self-Organizing Maps"*, 2002, Networks security.

[Lichodzijewski, 2002] P. Lichodzijewski, A.N. Zincir-Heywood, M. I. Heywood, *"Host-Based Intrusion Detection Using Self-Organizing Maps"*, In Proceedings of IJCNN '02.

[Mukkamala, 2003] S. Mukkamala, A. H. Sung, *"Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques"*, International Journal of Digital Evidence, Winter 2003, Vol. 1, Issue 4.

[Nguyen, 2002] B.V. Nguyen, *"SOM for Anomaly Detection"*, CS680 report, Spring 2002.

[Oja, 2003] M. Oja, S. Kaski, and T. Kohonen, *"Bibliography of Self-Organizing Map (SOM) Papers: 1998-2001 Addendum"*, Neural Computing Surveys, Vol. 3, 2003, pp. 1--156

[Rhodes, 2000] B. Rhodes, J. Mahaffey, J. Cannady, *"Multiple SOMs for Intrusion Detection"*, In Proceedings of the NISSC 2000 Conference.

[Ultsch, 1999] A. Ultsch, *"Data Mining and Knowledge Discovery with Emergent SOFMs for Multivariate Time Series"*, In Kohonen Maps, (1999), pp. 33-46.

[Ultsch, 2002] A. Ultsch, F. Roske, *"Self-Organizing Feature Maps Predicting Sea Levels"*, Information Sciences 144/1-4, Elsevier, Amsterdam, 2002, pp.91-125.

[Ultsch, 2003]A. Ultsch, *"Maps for Visualization of High-Dimensional Data Spaces"*, In Proceedings of WSOM, Kyushu, Japan, (2003), pp. 225-230.

[Ultsch, 2004] A. Ultsch, D. Kaempf, *"Knowledge Discovery in DNA Microarray Data of Cancer Patients with Emergent Self Organizing Maps"*, In Proceedings of the European Symposium on Artificial Neural Networks (ESANN 2004), Bruges, Belgium, April 28-30, 2004, pp.495-500.

[Ultsch, 2005] A. Ultsch, F. Moerchen *"ESOM-Maps: Tools for Clustering, Visualization, and Classification with Emergent SOM"*, Technical Report Department of Mathematics and Computer Science, University of Marburg, Germany, (46), 2005.

Κεφάλαιο 5ο

Ανίχνευση Εισβολών και Απόκριση σε Ασύρματα Δίκτυα κατά Περίσταση

1. Εισαγωγή

Στα προηγούμενα κεφάλαια ασχοληθήκαμε με προβλήματα ασφάλειας που αφορούν τα ενσύρματα δίκτυα. Τα *ασύρματα δίκτυα κατά περίσταση (ad hoc)* έχουν ερευνηθεί εκτενέστατα τα τελευταία χρόνια, κυρίως λόγω των σημαντικών πλεονεκτημάτων που παρουσιάζουν και λόγω της αυξανόμενης ζήτησής τους. Παρόλα αυτά, παρουσιάζουν πολλές έμφυτες αδυναμίες και απαιτούν αποτελεσματικούς μηχανισμούς ασφαλείας προκειμένου να διασφαλιστούν.

Καλούμαστε λοιπόν να ερευνήσουμε τα προβλήματα ασφάλειας που παρουσιάζουν τα *ασύρματα δίκτυα κατά περίσταση* και να προτείνουμε αποτελεσματικούς τρόπους διασφάλισής τους. Στο προηγούμενο κεφάλαιο προτείναμε μία προσέγγιση ανίχνευσης εισβολών στα ενσύρματα δίκτυα που βασίζεται στα νευρωνικά δίκτυα eSOM και αποδείξαμε ότι παράγει αξιόπιστα και ικανοποιητικά αποτελέσματα. Σε αυτό το κεφάλαιο εξετάζουμε τη δυνατότητα επέκτασης της προτεινόμενης προσέγγισης στα ασύρματα δίκτυα κατά περίσταση.

Συγκεκριμένα, προτείνουμε μία μηχανή ανίχνευσης εισβολών που βασίζεται στα eSOM και μία πιστοποιημένη μηχανή απόκρισης σε εισβολές που βασίζεται σε ένα καινοτόμο πρωτόκολλο συμφωνίας κλειδιών. Εκμεταλλευόμαστε τεχνικές απεικόνισης πληροφοριών και μηχανικής μάθησης προκειμένου να επιτύχουμε αποτελεσματική ανίχνευση εισβολών στα ασύρματα δίκτυα κατά περίσταση και βασιζόμαστε σε αρχές ασφαλούς επικοινωνίας προκειμένου να περιορίσουμε τις επιδράσεις πιθανών επιθέσεων. Η αξιοπιστία και η αποφυγή τροποποίησεων των χαρτών eSOM επιτυγχάνεται με τη χρήση μίας προτεινόμενης μεθόδου υδατογράφησης η οποία περιγράφεται αναλυτικά στο επόμενο κεφάλαιο. Η απόδοση του προτεινόμενου μοντέλου αξιολογείται κάτω από διαφορετικές συνθήκες κυκλοφορίας και πρότυπα κίνησης.

1.1 Ορισμός των Ασύρματων Δικτύων κατά Περίσταση

Τα ασύρματα δίκτυα κατά περίσταση (ad hoc) έχουν υιοθετηθεί από ένα μεγάλο εύρος περιβαλλόντων κάνοντας επικείμενη τη γρήγορη εξάπλωσή τους. Τα δίκτυα κατά περίσταση μπορούν να οριστούν σαν δυναμικά δίκτυα ομοτίμων (peer-to-peer) κόμβων (Σχήμα 5.1), οι οποίοι χρησιμοποιούν τη μεταφορά πληροφοριών πολλαπλών βημάτων, με ένα τρόπο αυτο-οργάνωσης χωρίς να βασίζονται σε προϋπάρχουσα υποδομή. Σε αυτά τα δίκτυα κάθε κόμβος μπορεί να λειτουργήσει σαν πηγή ή σαν δρομολογητής. Όλοι οι κόμβοι συνεργάζονται μεταξύ τους προκειμένου να παρέχουν βασικές δικτυακές υπηρεσίες. Οι κόμβοι που δεν μπορούν να επικοινωνήσουν άμεσα εξαρτώνται από τους γείτονές τους προκειμένου να προωθήσουν τα μηνύματά τους στον κατάλληλο προορισμό, ενώ η έλλειψη συνεργασίας μπορεί να έχει μοιραίες συνέπειες στην απόδοση του δικτύου.

Σχήμα 5. 1 Ένα ασύρματο δίκτυο κατά περίσταση

Η ασφάλεια σε τέτοια δίκτυα που δεν έχουν συγκεκριμένη υποδομή αποδείχτηκε πως είναι ένας τομέας-πρόκληση. Στα δίκτυα κατά περίσταση όλοι

οι κόμβοι μπορούν να εμφανίζονται και να εξαφανίζονται από το δίκτυο οποιαδήποτε στιγμή. Λόγω των σημαντικών πλεονεκτημάτων τους, οι εφαρμογές τους ποικίλουν σε ένα μεγάλο εύρος περιοχών όπου η ίδρυση υποδομής, όπως οι σταθμοί βάσης, είναι είτε αδύνατη είτε όχι αποτελεσματική όσον αφορά στο κόστος. Για παράδειγμα, τα δίκτυα κατά περίσταση χρησιμοποιούνται σε πολλές κρίσιμες εφαρμογές, περιλαμβανομένων των εφαρμογών ανάκαμψης από καταστροφές ή ακόμα και σε τακτικά περιβάλλοντα μάχης.

Υπάρχουν πολλά είδη δικτύων κατά περίσταση. Σε αυτό το κεφάλαιο, αναφερόμαστε σε ένα ανοιχτό δίκτυο κατά περίσταση που αποτελείται από ένα σύνολο από κόμβους, οι οποίοι χαρακτηρίζονται από μικρή διάρκεια συμμετοχής, αφού υπάρχει μεγάλος αριθμός γεγονότων άφιξης και αναχώρησης. Οι κόμβοι δικτύου κατά περίσταση έχουν μικρό εύρος επικοινωνίας και χαμηλή δυνατότητα μετάδοσης. Θα πρέπει να τονίσουμε ότι ο τύπος του μέσου επικοινωνίας στα δίκτυα κατά περίσταση δεν είναι τόσο σημαντικό στοιχείο όσο ο τύπος του δικτύου και η έλλειψη υποδομής. Το μέσο επικοινωνίας μπορεί να ποικίλει από υπέρυθρες, λέιζερ, ηλεκτρομαγνητικά κύματα (radio) έως και καλώδια και ζεύξεις οπτικών ινών.

1.2 Προβλήματα Ασφάλειας στα Ασύρματα Δίκτυα κατά Περίσταση

Δεδομένου του τρέχοντος ρυθμού επέκτασης της χρήσης των δικτύων κατά περίσταση υπάρχει μία μεγάλη ώθηση να γίνει η επικοινωνία σε αυτά τα δίκτυα ασφαλής. Δυστυχώς όμως, η ασφάλεια στα δίκτυα κατά περίσταση έχει πολλά ανοιχτά θέματα. Τα χαρακτηριστικά τους οδηγούν σε νέες αδυναμίες και νέες επιθέσεις, άγνωστες στα ενσύρματα δίκτυα ή τα δίκτυα που βασίζονται σε υποδομή. Από την άλλη πλευρά, τα περισσότερα από αυτά τα χαρακτηριστικά συμβάλλουν στο γεγονός ότι τα δίκτυα κατά περίσταση είναι ιδιαίτερα χρήσιμα. Το έργο της προστασίας τους είναι πολύ ενδιαφέρον και προκλητικό, αφού απαιτεί αποτελεσματικά και αποδοτικά πρωτόκολλα και μηχανισμούς.

Αν και τα δίκτυα αυτά χαρακτηρίζονται από μεγάλη προσαρμοστικότητα, παρουσιάζουν επίσης πολλούς έμφυτους περιορισμούς περιλαμβανομένων της έλλειψης κεντρικών οντοτήτων ελέγχου και της δυναμικά εναλλασσόμενης τοπολογίας, οδηγώντας σε ένα όχι τόσο καλά καθορισμένο όριο όπου μπορούν να εφαρμοστούν οι μηχανισμοί ελέγχου πρόσβασης και τα αντι-πυρικά τείχη (firewalls). Η δυναμικά εναλλασσόμενη τοπολογία σε συνδυασμό με την έλλειψη κεντρικού ελέγχου, την έλλειψη έμπιστων τρίτων οντοτήτων, την επανεκκίνηση των συνδέσεων για διάφορους λόγους, την ευκολία υποκλοπής μηνυμάτων και τους περιορισμένους πόρους είναι μερικά από τα θέματα ασφάλειας που καλούμαστε να αντιμετωπίσουμε. Προκειμένου να επιτύχουμε ασφάλεια στα δίκτυα κατά περίσταση εκτός από τις τεχνικές προστασίας η χρήση μηχανισμών ανίχνευσης και απόκρισης σε εισβολές, είναι απαραίτητη σαν ένα δεύτερο τείχος προστασίας, προκειμένου να επιτύχουμε αξιόπιστη επικοινωνία.

1.3 Η Προσέγγισή μας

Η ανίχνευση εισβολών είναι ένα ανεκτίμητο ώριμο "οπλοστάσιο" με μεγάλη ιστορία έρευνας για την προστασία των ενσύρματων δικτύων όπως περιγράψαμε αναλυτικά στο πρώτο κεφάλαιο. Δυστυχώς όμως, η ανίχνευση εισβολών αν και είναι ενεργός ερευνητική περιοχή στα ασύρματα δίκτυα κατά περίσταση, είναι ακόμα στα πρώτα στάδια ανάπτυξής της.

Σχήμα 5.2 Προτεινόμενη Προσέγγιση

Παρουσιάζουμε μία μέθοδο διασφάλισης των ασύρματων δικτύων κατά περίσταση που βασίζεται στην ανίχνευση εισβολών. Στο Σχήμα 5.2 απεικονίζεται συνοπτικά η προσέγγισή μας για τη διασφάλιση των ασύρματων δικτύων κατά περίσταση. Το πρώτο βήμα της προσέγγισής μας περιλαμβάνει τη συλλογή και την προεπεξεργασία των δεδομένων που αναπαριστούν την ασύρματη δικτυακή κυκλοφορία. Στη συνέχεια πραγματοποιήσαμε ανίχνευση εισβολών χρησιμοποιώντας τα eSOM, μία τεχνική που εφαρμόσαμε ήδη στα ενσύρματα δίκτυα με επιτυχία (Κεφάλαιο 4).

Αφού δημιουργηθούν οι χάρτες eSOM για τους κόμβους του ασύρματου δικτύου κατά περίσταση αναπτύσσουμε μία τεχνική *Απόκρισης σε Εισβολές* που βασίζεται στην ασφαλή μεταφορά των χαρτών ανάμεσα στους κόμβους του δικτύου. Επιπλέον προτείνουμε μία μέθοδο υδατογράφησης των χαρτών eSOM η οποία περιγράφεται αναλυτικά στο επόμενο κεφάλαιο.

Το επίκεντρο αυτού του κεφαλαίου είναι η μηχανή *Ανίχνευσης Εισβολών* που βασίζεται στα eSOM και ο σχεδιασμός της μηχανής *Απόκρισης σε Εισβολές*. Εκμεταλλευόμαστε το σημαντικό πλεονέκτημα των νευρωνικών δικτύων, δηλαδή την ανεκτικότητα τους σε ανακριβή δεδομένα προκειμένου να ταξινομήσουμε τη "φυσιολογική" συμπεριφορά ενάντια της "μη-φυσιολογικής". Συνδυάζοντας τεχνικές μηχανικής μάθησης, απεικόνισης πληροφοριών και συμφωνίας κλειδιών έχουμε τη δυνατότητα να έχουμε μία ξεκάθαρη εικόνα για το πόσο ασφαλές είναι ένα δίκτυο κατά περίσταση ενάντια επιθέσεων.

Τα Νευρωνικά Δίκτυα είναι μία ερευνητική περιοχή με πολλά πλεονεκτήματα που δεν έχουν ακόμα χρησιμοποιηθεί στην περιοχή των δικτύων κατά περίσταση. Εκμεταλλευόμαστε τα κύρια πλεονεκτήματα τους στο σχεδιασμό μίας μηχανής ανίχνευσης εισβολών, που είναι τμήμα ενός τοπικού πράκτορα IDS. Χρησιμοποιώντας τα eSOM, έχουμε μία οπτική αναπαράσταση της κατάστασης

"φυσιολογικής" συμπεριφοράς – επίθεσης σε κάθε κόμβο ενός δικτύου κατά περίσταση.

Επιπλέον προτείνουμε ένα πιστοποιημένο πρωτόκολλο συμφωνίας κλειδιών. Βασιζόμενοι σε αυτό το πρωτόκολλο προτείνουμε μία αποτελεσματική μηχανή Απόκρισης σε εισβολές με την οποία επιτυγχάνουμε την ασφαλή διακίνηση των χαρτών eSOM ανάμεσα στους κόμβους του δικτύου. Κατά αυτό τον τρόπο επιτυγχάνουμε την ασφαλή ενημέρωση των κόμβων για την ύπαρξη πιθανής εισβολής. Επομένως, κάθε κόμβος μπορεί να καθορίσει αν ένας γειτονικός του κόμβος είναι υπό επίθεση και να επιλέξει κάποιον άλλο προκειμένου να προωθηθούν τα μηνύματα του αλλά και να περιοριστεί η επίδραση της επίθεσης.

Ακολουθώντας αυτή την εισαγωγή, το κεφάλαιο αυτό οργανώνεται ως εξής. Στη συνέχεια αυτής της ενότητας ορίζουμε και περιγράφουμε τον τρόπο λειτουργίας των ασύρματων δικτύων κατά περίσταση αλλά και τα προβλήματα ασφάλειας που παρουσιάζουν. Περιγράφουμε την προσέγγισή μας για τη διαφύλαξη των ασύρματων δικτύων η οποία βασίζεται στην ανίχνευση και απόκριση σε εισβολές. Στην ενότητα 2 παρουσιάζεται σχετική εργασία για την ανίχνευση εισβολών στα ασύρματα δίκτυα κατά περίσταση, ενώ στην ενότητα 3 παρουσιάζεται σχετική εργασία για την ανίχνευση εισβολών με τη χρήση συμφωνίας κλειδιού. Στην ενότητα 4 παρουσιάζεται το προτεινόμενο μοντέλο ανίχνευσης εισβολών στα ασύρματα δίκτυα κατά περίσταση. Στην ενότητα 5 παρουσιάζεται η προτεινόμενη μηχανή ανίχνευσης εισβολών και συγκεκριμένα το προτεινόμενο πρωτόκολλο συμφωνίας κλειδιού στο οποίο βασίζεται η *Μονάδα Απόκρισης σε Εισβολές*. Στην ενότητα 6 παρουσιάζεται αξιολόγηση της προτεινόμενης προσέγγισης. Συγκεκριμένα, περιγράφεται το περιβάλλον προσομοίωσης, οι προσομοιωμένες επιθέσεις, τα χαρακτηριστικά (πεδία) της δικτυακής κίνησης που χρησιμοποιήθηκαν, τα αποτελέσματα της προσομοίωσης και τέλος η σύγκρισή τους με αποτελέσματα άλλων προσεγγίσεων. Η ενότητα 7 ολοκληρώνει το κεφάλαιο.

2. Ανίχνευση Εισβολών στα Ασύρματα Δίκτυα κατά Περίσταση

Οι τεχνικές ανίχνευσης εισβολών που εφαρμόζονται στα ενσύρματα δίκτυα δεν μπορούν να εφαρμοστούν εύκολα στα ασύρματα δίκτυα κατά περίσταση λόγω των μεγάλων διαφορών ανάμεσα στους δύο τύπους δικτύων. Σε σύγκριση με τα ενσύρματα δίκτυα όπου η παρακολούθηση των δικτύων πραγματοποιείται σε δικτυακές πύλες, δρομολογητές και μεταγωγείς, τα ασύρματα δίκτυα κατά περίσταση παρουσιάζουν έλλειψη σημείων συγκέντρωσης δικτυακής κυκλοφορίας στα οποία θα μπορούσε να πραγματοποιηθεί παρακολούθηση της δικτυακής κυκλοφορίας. Ακόμα και αν ήταν δυνατή η ύπαρξη τέτοιων σημείων συγκέντρωσης, η τοποθεσία τους θα άλλαζε συνεχώς λόγω κινητικότητας. Για το λόγο αυτό, στα ασύρματα δίκτυα κατά περίσταση είναι αναγκαία η ανάπτυξη

κατανεμημένων συστημάτων ανίχνευσης εισβολών τα οποία βασίζονται σε τοπικά καταγεγραμμένα (audit) δεδομένα.

Στα ασύρματα δίκτυα κατά περίσταση, κακόβουλοι κόμβοι μπορεί να εισέρχονται και να εξαφανίζονται από το δίκτυο σε τυχαίες χρονικές στιγμές, να αναστατώνουν τη δικτυακή δραστηριότητα και να αποφεύγουν την ανίχνευση. Οι κακόβουλοι κόμβοι μπορούν να συμπεριφέρονται κακόβουλα σε μη συνεχή χρονικά διαστήματα, κάνοντας ακόμα πιο δύσκολη την ανίχνευση τους [Patwardhan, 2005]. Η περιορισμένη φυσική ασφάλεια των κόμβων καθιστά δυνατή την κλοπή νόμιμων πιστοποιητικών και την πραγματοποίηση ακόμα πιο σοβαρών επιθέσεων. Οι δυναμικές τοπολογίες καθιστούν πολύ δύσκολη τη λήψη μίας καθολικής άποψης του δικτύου και οποιαδήποτε προσέγγιση μπορεί πολύ γρήγορα να μην ανταποκρίνεται πια στην πραγματικότητα.

Επιπλέον, θα πρέπει να επικεντρωθούμε σε μηχανισμούς ασφάλειας λαμβάνοντας υπόψη την ευκολία παρακολούθησης των ασύρματων συναλλαγών, την έλλειψη σταθερής υποδομής και τους περιορισμένους πόρους που παρουσιάζουν τα ασύρματα δίκτυα κατά περίσταση. Αυτό σημαίνει ότι είναι καλύτερα να χρησιμοποιούμε ένα περιοδικό *Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System (IDS))* παρά ένα συνεχώς ενεργοποιημένο μηχανισμό παρεμπόδισης εισβολών. Οι περιορισμοί πόρων που τα δίκτυα κατά περίσταση αντιμετωπίζουν περιλαμβανόμενων της περιορισμένης μπαταρίας, εύρους ζώνης και συχνής προβληματικής επικοινωνίας κάνουν ακόμα πιο δύσκολο το διαχωρισμό ανάμεσα σε μία νέα νόμιμη λειτουργία μετά από μία αποσύνδεση, και μία εισβολή· με αποτέλεσμα τη δύσκολη ταξινόμηση "φυσιολογικής" και "μη-φυσιολογικής" συμπεριφοράς ([Makki, 2004], [Komninos, 2007]). Για παράδειγμα, ένας κόμβος που στέλνει λανθασμένες πληροφορίες δρομολόγησης δεν είναι απαραίτητα κατειλημμένος αλλά μπορεί να μην είναι συγχρονισμένος λόγω κινητικότητας.

Οι Zhang και Lee [Zhang, 2003] πρότειναν το πρώτο (υψηλού επιπέδου) κατανεμημένο και συνεργατικό σύστημα ανίχνευσης εισβολών (IDS) που βασίζεται στην ανίχνευση ανωμαλιών, το οποίο παρέχει έναν αποτελεσματικό οδηγό για το σχεδιασμό συστημάτων ανίχνευσης εισβολών (IDS) σε ασύρματα δίκτυα κατά περίσταση. Η κύρια μέθοδος ανίχνευσης εισβολών που προτείνεται είναι η ανίχνευση ανωμαλιών με βάση τις ανανεώσεις δρομολόγησης στο επίπεδο ελέγχου πρόσβασης στο μέσο (Medium Access Control (MAC)) και στο επίπεδο εφαρμογής.

Οι Huang και Lee [Huang, 2003a] επέκτειναν την προηγούμενη εργασία τους προτείνοντας ένα σύστημα ανίχνευσης εισβολών (IDS) που βασίζεται σε ομάδες κόμβων, προκειμένου να αντιμετωπιστούν οι περιορισμένοι πόροι που αντιμετωπίζουν τα κινητά δίκτυα κατά περίσταση. Χρησιμοποιούν ένα σύνολο στατιστικών χαρακτηριστικών που προέρχονται από τους πίνακες δρομολόγησης και εφαρμόζουν τον επαγωγικό αλγόριθμο ταξινόμησης δένδρου αποφάσεων (decision tree induction algorithm C4.5) προκειμένου να ανιχνεύσουν τη "φυσιολογική" ενάντια της "μη-φυσιολογικής" συμπεριφοράς·

Το προτεινόμενο σύστημα έχει την ικανότητα να αναγνωρίσει την πηγή της επίθεσης, εάν ο επιτιθέμενος είναι άμεσος (ενός-βήματος) γείτονας.

Οι Deng και άλλοι [Deng, 2003] πρότειναν μία ιεραρχικά κατανεμημένη και μία εντελώς κατανεμημένη προσέγγιση ανίχνευσης εισβολών. Η προσέγγιση που χρησιμοποιήθηκε και στις δύο αρχιτεκτονικές βασίζεται στον αλγόριθμο ταξινόμησης Μηχανών Υποστήριξης Διανυσμάτων (Support Vector Machines (SVM)). Χρησιμοποιούν ένα σύνολο παραμέτρων που προέρχονται από το επίπεδο δικτύου. Υποστηρίζουν ότι μία ιεραρχικά κατανεμημένη προσέγγιση μπορεί να είναι μία πιο υποσχόμενη λύση σε σύγκριση με μία πλήρως κατανεμημένη προσέγγιση ανίχνευσης εισβολών.

Οι Kachirski και Guha [Kachirski, 2002] πρότειναν ένα σύστημα ανίχνευσης εισβολών που βασίζεται σε ομάδες και χρησιμοποιεί τεχνολογίες κινητών πρακτόρων. Το προτεινόμενο σύστημα χρησιμοποιεί κινητούς πράκτορες, κάθε ένας από τους οποίους έχει ένα συγκεκριμένο ρόλο. Τα αποτελέσματα κάθε κόμβου συγκεντρώνονται σε σημεία σύμπλεξης (cluster) προκειμένου να περιοριστεί το έργο παρακολούθησης των πακέτων σε λίγους κόμβους και να ελαχιστοποιηθεί ο χρόνος επεξεργασίας που σχετίζεται με το σύστημα ανίχνευσης εισβολών (IDS) για κάθε κόμβο.

Οι Liu και άλλοι [Liu, 2005] πρότειναν μία πλήρως κατανεμημένη προσέγγιση ανίχνευσης ανωμαλιών που βασίζεται στο επίπεδο MAC. Η προτεινόμενη προσέγγιση επιλέγει χαρακτηριστικά από το επίπεδο MAC για να δημιουργήσει προφίλ φυσιολογικής συμπεριφοράς των κινητών κόμβων και στη συνέχεια εφαρμόζει ανάλυση συνδυασμού πεδίων [Huang, 2003b] στα διανύσματα πεδίων που κατασκευάζονται από τα δεδομένα εκπαίδευσης.

Οι Tseng και άλλοι [Tseng, 2003] πρότειναν μία προσέγγιση ανίχνευσης εισβολών που βασίζεται σε προδιαγραφές (specification) προκειμένου να ανιχνεύσουν επιθέσεις στο πρωτόκολλο δρομολόγησης AODV (Ad hoc on Demand Distance Vector) [Perkins, 2003]. Η σωστή συμπεριφορά δρομολόγησης AODV καθορίζεται χρησιμοποιώντας μηχανές τερματικών καταστάσεων και η τρέχουσα συμπεριφορά των ροών AODV συγκρίνεται με αυτή των προδιαγραφών. Το μειονέκτημα των τεχνικών που βασίζονται σε προδιαγραφές είναι η ανάγκη πραγματοποίησης ενός συμβιβασμού μεταξύ της πολυπλοκότητας και της ακρίβειας.

Οι Anjum και άλλοι [Anjum, 2003] προτείνουν μία προσέγγιση ανίχνευσης εισβολών που βασίζεται σε υπογραφές βασιζόμενη στην υπόθεση ότι οι υπογραφές επιθέσεων είναι απόλυτα γνωστές σε ένα δίκτυο κατά περίσταση. Επιπλέον, αυτή η προσέγγιση ερευνά την ικανότητα διάφορων πρωτοκόλλων δρομολόγησης να διευκολύνουν τη διαδικασία ανίχνευσης εισβολών. Οι συγγραφείς συμπεραίνουν ότι η επιλογή του πρωτοκόλλου δρομολόγησης εξαρτάται από τον τύπο της ανίχνευσης που θέλουμε να πραγματοποιήσουμε. Η ανίχνευση που θέλουμε να κάνουμε μπορεί να είναι ένας κύριος παράγοντας που πρέπει να λάβουμε υπόψη μας στην περίπτωση ανίχνευσης κακής χρήσης (misuse detection). Οι συγγραφείς δείχνουν ότι τα αντιδραστικά (reactive)

πρωτόκολλα δρομολόγησης για δίκτυα κατά περίσταση είναι λιγότερο αποτελεσματικά σε σχέση με τα προληπτικά (proactive) πρωτόκολλα δρομολόγησης στην ανίχνευση εισβολών ακόμα και στην περίπτωση που δεν υπάρχει κινητικότητα.

Οι Chen και άλλοι [Chen, 2005] πρότειναν μία κατανεμημένη προσέγγιση ανίχνευσης εισβολών που βασίζεται στην θεωρία Dempster-Shafer. Εκμεταλλεύονται τα κύρια πλεονεκτήματα αυτής της θεωρίας και την ικανότητα της να απεικονίσει την αβεβαιότητα ή την έλλειψη ολοκληρωμένων πληροφοριών και την κατάλληλη αριθμητική διαδικασία για τη συγχώνευση πολλαπλών τμημάτων δεδομένων.

Σε αυτό το κεφάλαιο, προτείνουμε μία πλήρως κατανεμημένη προσέγγιση ανίχνευσης εισβολών που ταιριάζει περισσότερο στα ενυπάθη χαρακτηριστικά των ασύρματων δικτύων κατά περίσταση. Η προσέγγιση ανίχνευσης εισβολών πραγματοποιείται χρησιμοποιώντας τους *αναδυόμενους Αυτό-Οργανούμενους Χάρτες (emergent Self-Organizing Maps (eSOM))*.

3. Ανίχνευση Εισβολών με Χρήση Πρωτοκόλλων Συμφωνίας Κλειδιού

Η αποτελεσματική ανίχνευση εισβολών θα πρέπει να συνδυάζεται με μία αποτελεσματική και ασφαλή απόκριση εισβολών. Η απόκριση σε εισβολές προκειμένου να είναι αποτελεσματική και ασφαλής θα πρέπει να βασίζεται σε μηχανισμούς ασφάλειας όπως η διαχείριση και συμφωνία κλειδιών ομάδας. Έχουν προταθεί πολλά πρωτόκολλα διαχείρισης κλειδιών ομάδας ([Burmester, 1995], [Becker, 1998)], [Kim, 2004], [Steiner, 1998]) για ασύρματα δίκτυα, περιλαμβανομένου ενός μεγάλου αριθμού που βασίζεται σε δομή δέντρων ([Kim, 2004], [Bartia, 2003], [Dutta, 2004], [Dutta, 2005], [Nalla, 2002]). Παρόλα αυτά, τα περισσότερα από αυτά τα πρωτόκολλα δεν μπορούν να εφαρμοστούν σε ένα περιβάλλον χωρίς υποδομή ή σε ένα περιβάλλον το οποίο είναι ευαίσθητο στη διαχείριση πόρων, όπως είναι τα δίκτυα κατά περίσταση.

Για παράδειγμα, στο πρωτόκολλο Octopus [Becker, 1998], τέσσερις κόμβοι δημιουργούν ένα 2^2 –κύβο και τα υπόλοιπα μέλη του δικτύου είναι "ακμές" που συνδέονται με έναν από τους κεντρικούς κόμβους. Σε ένα δυναμικό δίκτυο κατά περίσταση, δεν είναι εύκολο να διατηρήσουμε μία τέτοια τοπολογία. Το πρωτόκολλο Tree-Group Diffie-Hellman (TGDH) που προτάθηκε στο [Kim, 2004], βασίζεται σε μία δομή δυαδικού δένδρου και βελτιώνει την απόδοσή του πρωτοκόλλου IKA1/2 (Internet Key Agreement) [Steiner, 1998]. Παρόλα αυτά βασίζεται σε εκθετική ύψωση modulo (modular exponentiation) που είναι η υπολογιστικά πιο δαπανηρή πράξη καθώς, μπορεί να απαιτεί $O(n)$ εκθετικές υψώσεις, προκειμένου να υπολογιστεί το ομαδικό κλειδί συνεδρίας.

Οι Hwang και Chang [Hwang, 2003] πρότειναν ένα πρωτόκολλο συμφωνίας κλειδιών που βασίζεται σε ένα ομαδικό διαμοιραζόμενο συνθηματικό, την πράξη αποκλειστικό-Ή (exclusive-OR (XOR)) και μία δομή δυαδικού δένδρου. Αν και αυτή η προσέγγιση είναι πραγματικά αποτελεσματική για δίκτυα κατά

περίσταση είναι ευαίσθητη στον υπολογισμό συνθηματικών και στις επιθέσεις επανάληψης. Οι Lo και άλλοι [Lo, 2005] βελτίωσαν την προηγούμενη προσέγγιση [Hwang, 2003] προσθέτοντας αμοιβαία πιστοποίηση και μία διαδικασία περιοδικής ανανέωσης κλειδιών. Παρόλα αυτά, η προσέγγισή τους παραμένει ευαίσθητη σε επιθέσεις λεξικού (dictionary) και στη βίαιη επίθεση "brute force" αφού βασίζεται σε συνθηματικά.

Σε αυτό το κεφάλαιο, χρησιμοποιούμε ένα *Πρωτόκολλο Συμφωνίας Κλειδιού* σε συνδυασμό με eSOM προκειμένου να επιβεβαιώσουμε ότι η απεικόνιση πληροφοριών που παρέχει το eSOM, δεν θα τροποποιηθεί από κακόβουλους επιτιθέμενους.

4. Μοντέλο Ανίχνευσης Εισβολών

Οι κακόβουλοι κόμβοι σε ένα κινητό δίκτυο κατά περίσταση στοχεύουν στην εκμετάλλευση του φυσικού επιπέδου, του επιπέδου δικτύου ή του επιπέδου MAC. Η πλειοψηφία των μηχανισμών ασφάλειας σε τέτοια δίκτυα επικεντρώνονται στο επίπεδο δικτύου. Λίγη έρευνα έχει πραγματοποιηθεί στο επίπεδο MAC. Ο ρόλος του επιπέδου MAC στα ασύρματα δίκτυα κατά περίσταση είναι πολύ σημαντικός, καθώς είναι υπεύθυνο για τη διατήρηση της επικοινωνίας ανάμεσα στους κόμβους και τον προγραμματισμό της πρόσβασης σε ένα διαμοιραζόμενο ασύρματο ραδιοδίαυλο (radio channel). Το επίπεδο MAC επηρεάζεται άμεσα σχεδόν από όλες τις ανωμαλίες, καθώς βρίσκεται στα πρώτα επίπεδα της στοίβας πρωτοκόλλων. Πράγματι, ο ρυθμός παράδοσης ή η διαπερατότητα μπορεί να επηρεάζεται από κακόβουλη συμπεριφορά ή κακή χρήση του διαμοιραζόμενου μέσου (π.χ. εγωισμός) λόγω του αυξημένου φόρτου δρομολόγησης. Ο έλεγχος επιβάρυνσης για κάθε πακέτο δεδομένων που παραδόθηκε μπορεί επίσης να αυξηθεί. Επομένως, οι μηχανισμοί ανίχνευσης εισβολών που βασίζονται σε χαρακτηριστικά που επιλέγονται από το επίπεδο MAC είναι γρηγορότεροι όσον αφορά στις καθυστερήσεις ανίχνευσης και στο χρόνο απόκρισης. Επιπλέον, αυτά τα χαρακτηριστικά κάνουν ευκολότερο το διαχωρισμό ανάμεσα στη "φυσιολογική" και στη "μη-φυσιολογική" συμπεριφορά.

Η αρχιτεκτονική του συστήματος ανίχνευσης εισβολών (IDS) που εφαρμόζεται σε δίκτυα κατά περίσταση μπορεί να είναι είτε κατανεμημένη και να βασίζεται στη συνεργασία ή κατανεμημένη και ιεραρχική. Η έλλειψη των κεντρικών κόμβων παρακολούθησης και η έλλειψη παρακολούθησης ανάμεσα στους ομότιμους κόμβους σε ένα ασύρματο δίκτυο κατά περίσταση καθιστά ένα κεντρικό σύστημα ανίχνευσης εισβολών ανεπαρκές. Αν και τα συστήματα ανίχνευσης εισβολών (IDS) που βασίζονται σε συμπλέγματα (clusters) έχουν το πλεονέκτημα χαμηλότερου φόρτου ανίχνευσης, η διαδικασία δημιουργίας συμπλεγμάτων (clusters) και εκλογής των αρχηγών ομάδας μπορεί να δημιουργήσει μεγάλο φόρτο. Επιπλέον, η ύπαρξη αρχηγών ομάδας και η προφανής πιθανότητα εκμετάλλευσής τους από κακόβουλους επιτιθέμενους καθιστούν αδύνατη την αναμενόμενη ασφάλεια. Επιπλέον, τα κατανεμημένα και ιεραρχικά συστήματα ανίχνευσης εισβολών (IDS) είναι πιο αποτελεσματικά για

τα δίκτυα κατά περίσταση με χαμηλή κινητικότητα. Επομένως, η δυναμική και συνεργάσιμη φύση των δικτύων κατά περίσταση συνεπάγεται ότι το σύστημα ανίχνευσης εισβολών θα πρέπει να βασίζεται στη συνεργασία και να είναι κατανεμημένο.

Κάθε κόμβος ενός δικτύου κατά περίσταση πρέπει να πραγματοποιεί τοπική ανίχνευση εισβολών χρησιμοποιώντας τοπικά δεδομένα παρακολούθησης (audit). Όταν είναι απαραίτητη η επιβεβαίωση άλλων κόμβων προκειμένου να ανιχνευθεί μία επίθεση, πρέπει να συνεργάζονται οι τοπικοί ανιχνευτές εισβολών. Επιπλέον, αυτή η επικοινωνία ανάμεσα στους τοπικούς πράκτορες IDS θα πρέπει να πραγματοποιείται μέσω ασφαλών καναλιών επικοινωνίας.

Η αρχιτεκτονική IDS που υιοθετούμε είναι αυτή που προτείνεται στο [Zhang, 2003] και αποτελείται από πολλαπλούς τοπικούς πράκτορες IDS, όπως απεικονίζεται στο Σχήμα 5.3, που είναι υπεύθυνοι για την ανίχνευση πιθανών εισβολών τοπικά. Η συλλογή όλων των ανεξάρτητων πρακτόρων IDS δημιουργεί το σύστημα IDS για το δίκτυο κατά περίσταση. Κάθε τοπικός πράκτορας IDS αποτελείται από τα ακόλουθα στοιχεία:

Μονάδα Συλλογής Δεδομένων: είναι υπεύθυνη για τη συλλογή τοπικών καταγεγραμμένων δεδομένων και καταγεγραμμένης δραστηριότητας.

Μηχανή Ανίχνευσης Εισβολών: είναι υπεύθυνη για την ανίχνευση τοπικών ανωμαλιών χρησιμοποιώντας τοπικά καταγεγραμμένα δεδομένα. Η τοπική ανίχνευση εισβολών πραγματοποιείται χρησιμοποιώντας τον αλγόριθμο ταξινόμησης eSOM.

Η διαδικασία που ακολουθείται στην τοπική μηχανή ανίχνευσης είναι αυτή που περιγράφεται ακολούθως:

- Επιλογή χαρακτηρισμένων (labeled) καταγεγραμμένων δεδομένων και πραγματοποίηση των κατάλληλων μετασχηματισμών.
- Υπολογισμός του ταξινομητή χρησιμοποιώντας τα δεδομένα εκπαίδευσης και τον αλγόριθμο eSOM.
- Εφαρμογή του ταξινομητή για την δοκιμή των τοπικών καταγεγραμμένων δεδομένων προκειμένου να ταξινομηθούν σαν "φυσιολογικά" ή "μη-φυσιολογικά".

Πρέπει να σημειώσουμε εδώ, ότι είναι σημαντικό να διαφυλάσσεται η ακεραιότητα του παραγόμενου χάρτη eSOM από πιθανές τροποποιήσεις και παραβιάσεις. Προκειμένου να επιτευχθεί αυτό προτείνουμε μία μέθοδο υδατογράφησης η οποία περιγράφεται αναλυτικά στο Κεφάλαιο 6.

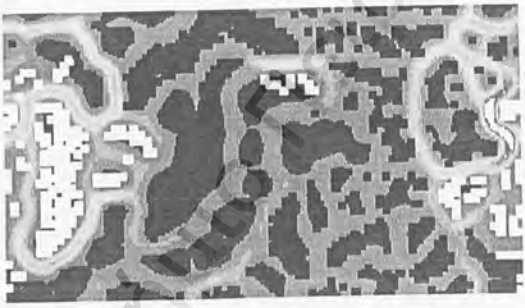
Μηχανή Απόκρισης σε Εισβολές: Στα δίκτυα κατά περίσταση η απόκριση σε πιθανές επιθέσεις θα πρέπει να είναι γρήγορη, καθώς η επίδραση μίας επίθεσης λόγω των προαναφερθέντων περιορισμένων πόρων μπορεί να είναι πιο σοβαρή. Η απεικόνιση πληροφοριών μπορεί να μας βοηθήσει προκειμένου να έχουμε άμεση απόκριση σε πιθανές εισβολές. Εκμεταλλευόμαστε την απεικόνιση πληροφοριών προτείνοντας μία μηχανή *Ανίχνευσης Εισβολών* και μία μηχανή *Απόκρισης σε Εισβολές* που συνεργάζονται αποτελεσματικά για την καταπολέμηση πιθανών εισβολών.

Σχήμα 5. 3 Αρχιτεκτονική Ανίχνευσης Εισβολών

Η προτεινόμενη μηχανή *Απόκρισης σε Εισβολές* βασίζεται σε ένα πρωτόκολλο συμφωνίας κλειδιών. Το προτεινόμενο *πιστοποιημένο πρωτόκολλο συμφωνίας κλειδιού ομάδας (authenticated group key agreement protocol)* έχει κάποια μοναδικά χαρακτηριστικά μεταξύ των οποίων περιλαμβάνεται η χρήση ενός διαμοιραζόμενου κύριου (master) κλειδιού και η δομή ενός δένδρου που εξαρτάται από την απόσταση ανάμεσα στους κόμβους του δικτύου κατά περίσταση. Χρησιμοποιώντας αυτό το πρωτόκολλο συμφωνίας κλειδιών μπορούμε να δημιουργήσουμε τα *Τοπικά Κλειδιά (Local Keys (LK))* και ένα *Καθολικό Κλειδί (Global Key (GK))* προκειμένου να διασφαλιστεί η ασφαλής επικοινωνία της προτεινόμενης μηχανής *Απόκρισης σε Εισβολές*.

Εάν η *Μηχανή Ανίχνευσης Εισβολών* ανιχνεύσει μία εισβολή τότε ενεργοποιείται η *Μηχανή Απόκρισης σε Εισβολές*. Κάθε κόμβος στο δίκτυο κατά περίσταση μπορεί να συμμετέχει στη *Μηχανή Απόκρισης σε Εισβολές*. Η *Μηχανή Απόκρισης σε Εισβολές* είναι υπεύθυνη για την αποστολή τοπικών και καθολικών συναγερμών προκειμένου να γνωστοποιήσει στους κόμβους του δικτύου κατά περίσταση το περιστατικό της επίθεσης.

Η προτεινόμενη *Μηχανή Απόκρισης σε Εισβολές* αποτελείται από τρεις κύριες μονάδες: τη *Μονάδας Επικοινωνίας*, τη *Μονάδα Τοπικής Απόκρισης* και τη *Μονάδα Καθολικής Απόκρισης*. Η *Μονάδα Τοπικής Απόκρισης* ενεργοποιείται κάθε φορά που μία εισβολή ανιχνεύεται από τη *Μηχανή Ανίχνευσης Εισβολών*, ενώ η *Μονάδα Καθολικής Απόκρισης* ενεργοποιείται μόνο σε σοβαρές περιπτώσεις επιθέσεων, π.χ. όταν ο χάρτης eSOM ενός κόμβου (Σχημα 5.4) καλύπτεται στο μεγαλύτερο κομμάτι του (πάνω απο τα (2/3)) με σημάδια επίθεσης (ανοιχτό χρώμα). Μεγάλη προσοχή πρέπει να δοθεί στον τρόπο λειτουργίας της *Μηχανής Απόκρισης Εισβολών* προκειμένου να αποφευχθεί πιθανή πλημμύρα ή επιθέσεις άρνησης εξυπηρέτησης που έχουν προκληθεί από μηνύματα κοινοποίησης για πιθανές εισβολές. Επομένως, κάθε μήνυμα ειδοποίησης που παράγεται από τη *Μηχανή Απόκρισης σε Εισβολές* στέλνεται μόνο μία φορά, ενώ η *Μονάδα Καθολικής Απόκρισης* ενεργοποιείται μόνο σε σοβαρές περιπτώσεις επιθέσεων.

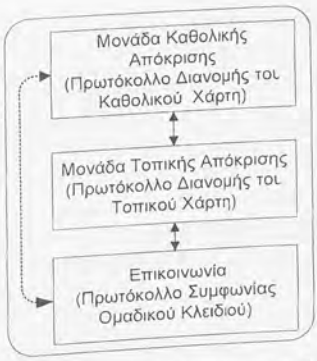


Σχήμα 5. 4 Χάρτης eSOM ενός Κόμβου ενός Δικτύου κατά Περίσταση

5. Προτεινόμενη Μηχανή Απόκρισης σε Εισβολές

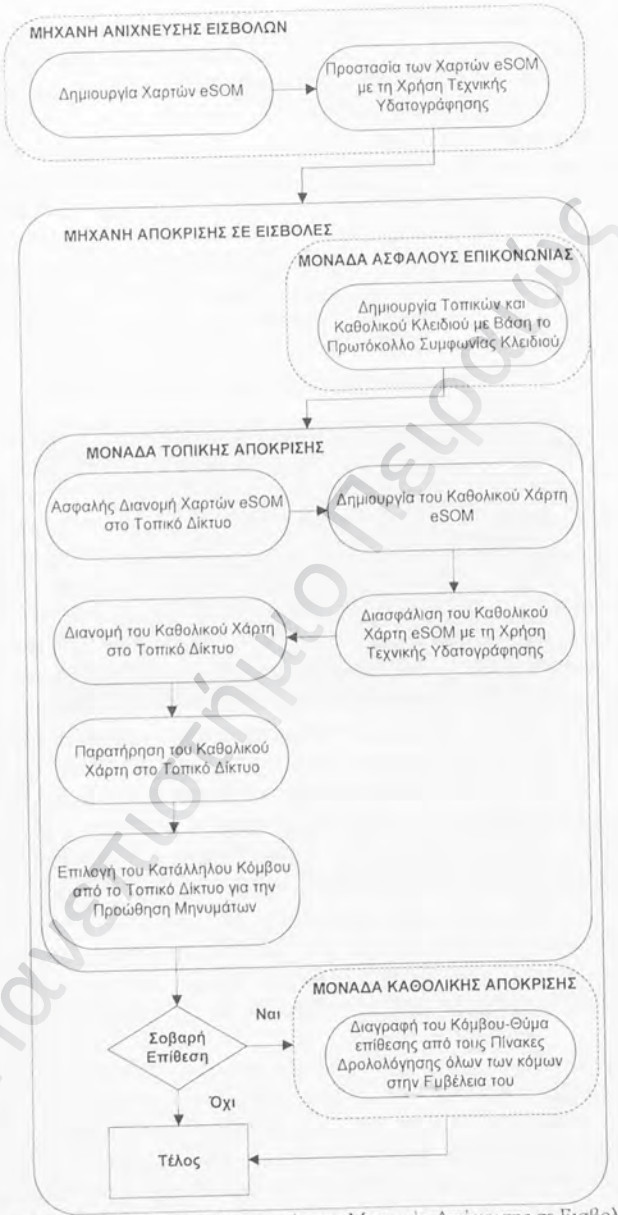
Η *Μηχανή Απόκρισης σε Εισβολές* και τα συστατικά της απεικονίζονται στο Σχήμα 5.5. Η *Μονάδα Επικοινωνίας* είναι υπεύθυνη για τη συμφωνία των *τοπικών κλειδιών (LK)* και ενός *καθολικού κλειδιού (GK)* με βάση ένα *Πρωτόκολλο Συμφωνίας Ομαδικού Κλειδιού*, τα οποία θα χρησιμοποιηθούν στις μονάδες *Τοπικής* και *Καθολικής Απόκρισης* αντίστοιχα. Η *Μονάδα Τοπικής Απόκρισης* είναι υπεύθυνη για τη δημιουργία του *Πρωτοκόλλου Διανομής των Τοπικών Χαρτών* eSOM ενώ η *Μονάδα Καθολικής Απόκρισης* είναι υπεύθυνη για το *Πρωτόκολλο Διανομής του Καθολικού Χάρτη*.

Αναλυτικότερα η λειτουργία της *Μηχανής Απόκρισης σε Εισβολές* και ο τρόπος αλληλεπίδρασής της με τη *Μηχανή Ανίχνευσης Εισβολών* παρουσιάζεται στο Σχήμα 5.6. Η *Μηχανή Απόκρισης σε Εισβολές* δέχεται σαν είσοδο τους χάρτες eSOM που έχουν δημιουργηθεί από τη *Μηχανή Ανίχνευσης Εισβολών*. Οι χάρτες αυτοί δημιουργούνται τοπικά σε κάθε κόμβο του ασύρματου δικτύου κατά περίσταση και προστατεύονται από πιθανές τροποποιήσεις με την προτεινόμενη τεχνική υδατογράφησης που περιγράφεται αναλυτικά στο Κεφάλαιο 6.



Σχήμα 5. 5 Μηχανή Απόκρισης σε Εισβολές

Η *Μονάδα Τοπικής Απόκρισης* χρησιμοποιώντας τα *Τοπικά* και το *Καθολικό Κλειδί* που παράγονται από τη *Μονάδα Ασφαλούς Επικοινωνίας*, επιτυγχάνει την ασφαλή διανομή των *Τοπικών Χαρτών* eSOM στο τοπικό δίκτυο. Στη συνέχεια περιλαμβάνει τη δημιουργία ενός *Καθολικού Χάρτη* eSOM, ο οποίος αποτελείται από τους *Τοπικούς Χάρτες* eSOM όλων των άμεσων (ενός-βήματος) γειτόνων ενός κόμβου. Προκειμένου να επιβεβαιώσουμε την αυθεντικότητα και την ακεραιότητα του *Καθολικού Χάρτη* eSOM εφαρμόζουμε ένα *Πρωτόκολλο Διανομής του Καθολικού Χάρτη*. Ο παραγόμενος *Καθολικός Χάρτης* eSOM χρησιμοποιείται κυρίως για την απεικόνιση της κατάστασης ασφαλείας του τοπικού δικτύου κατά περίσταση που αποτελείται από τους άμεσους γείτονες (ενός-βήματος) ενός κόμβου. Ο *Καθολικός Χάρτης* eSOM προστατεύεται επίσης χρησιμοποιώντας την προτεινόμενη τεχνική υδατογράφησης. Ανάλογα με το μέγεθος της πιθανής επίθεσης, γεγονός που συμπεραίνεται από την παρατήρηση του *Καθολικού Χάρτη*, καθορίζεται το επόμενο βήμα της *Μηχανής Απόκρισης*. Αυτός ο χάρτης βοηθά επίσης τους κόμβους να επιλέξουν τον πιο κατάλληλο και ασφαλή γειτονικό κόμβο για την προώθηση των μηνυμάτων. Η *Μονάδα Καθολικής Απόκρισης* είναι



Σχήμα 5. 6 Αναλυτική Λειτουργία της Μηχανής Απόκρισης σε Εισβολές

υπεύθυνη για την ενημέρωση όλων των γειτόνων στην εμβέλεια επικοινωνίας του κόμβου που δέχτηκε επίθεση. Όταν η επίθεση δεν είναι πολύ σοβαρή επιλέγεται από το τοπικό δίκτυο ο κατάλληλος κόμβος για την προώθηση μηνυμάτων-πακέτων. Σε περίπτωση που η επίθεση είναι ιδιαίτερα σοβαρή γεγονός που καθορίζεται από την έκταση του χάρτη eSOM ενός κόμβου (Σχήμα 5.4) που καλύπτεται (πάνω από τα (2/3)) με σημάδια επίθεσης (ανοιχτό χρώμα). Στην περίπτωση αυτή ενεργοποιείται η *Μονάδα Καθολικής Απόκρισης* η οποία είναι υπεύθυνη για την ενημέρωση όλων των κόμβων στην εμβέλεια του κόμβου θύματος-επίθεσης για την ενδεχόμενη επίθεση και την εκκίνηση διαγραφής του κόμβου–θύματος από τους αντίστοιχους πίνακες δρομολόγησης.

5.1 Μονάδα Επικοινωνίας

Το έργο της διασφάλισης των δικτύων κατά περίσταση είναι πολύπλοκο και απαιτητικό, εάν λάβουμε υπόψη μας τα έμφυτα χαρακτηριστικά αδυναμίας που παρουσιάζουν θέτοντάς τα εκτεθειμένα σε ένα μεγάλο εύρος επιθέσεων. Επιπλέον, η εφαρμογή μηχανισμών ασφαλείας, που έχουν αναπτυχθεί για δίκτυα που βασίζονται σε μία συγκεκριμένη υποδομή, είναι πολύ δύσκολο να επιτευχθεί στα ασύρματα δίκτυα κατά περίσταση.

Η *εγκαθίδρυση κλειδιών* είναι ένας μηχανισμός ασφαλείας ζωτικής σημασίας που έχει ερευνηθεί εκτεταμένα για τη διασφάλιση των δομημένων δικτύων. Ο σκοπός ενός *πρωτοκόλλου εγκαθίδρυσης κλειδιού ομάδας* είναι η εγκαθίδρυση ενός ομαδικού κλειδιού συνεδρίας που θα μπορούσε να χρησιμοποιηθεί στις διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης προκειμένου να επιβεβαιώσει την αυθεντικότητα των μεταδιδόμενων μηνυμάτων πάνω από ένα ανοιχτό κανάλι. Τα πρωτόκολλα εγκαθίδρυσης ομαδικών κλειδιών διαχωρίζονται σε δύο βασικές κατηγορίες: τα πρωτόκολλα *διανομής κλειδιού ομάδας* και τα *πρωτόκολλα συμφωνίας κλειδιού ομάδας* [Menezes, 1996].

Στα *πρωτόκολλα διανομής κλειδιού ομάδας*, ένα συμμετέχον μέλος της ομάδας επιλέγει το ομαδικό κλειδί συνεδρίας για την ασφαλή διανομή του κλειδιού στα άλλα μέλη της ομάδας χρησιμοποιώντας εκ των προτέρων συμμετρικά ή ασύμμετρα διαμοιραζόμενα μυστικά. Αυτό το σενάριο δεν είναι ρεαλιστικό και δεν μπορεί να εφαρμοστεί σε δίκτυα κατά περίσταση αφού απαιτείται η ύπαρξη μίας Τρίτης Εμπιστευτικής Οντότητας (Trusted Third Party (TTP)) για τη διανομή του κλειδιού συνεδρίας. Στα *πρωτόκολλα συμφωνίας κλειδιού ομάδας* (*group key agreement protocols (GKA)*) τα μέλη της ομάδας συμφωνούν σε ένα κοινό μυστικό κλειδί, το οποίο προκύπτει από την δημόσια συνεισφορά κάθε συμμετέχοντος. Τα *πρωτόκολλα διανομής κλειδιού ομάδας* ταιριάζουν καλύτερα σε δίκτυα κατά περίσταση με μέτρια μεγέθη και χωρίς την ύπαρξη κεντρικής αρχής για τη διανομή κλειδιών.

Ένα *πιστοποιημένο πρωτόκολλο κλειδιού ομάδας* παρέχει την επιπρόσθετη ιδιότητα πιστοποίησης των κλειδιών, η οποία επιβεβαιώνει κάθε μέλος της ομάδας ότι το συμφωνημένο κλειδί δεν θα αποκαλυφθεί σε κάποιο άλλο μέλος. Αυτή η ιδιότητα πιστοποίησης ονομάζεται επίσης *πλήρης πιστοποίηση κλειδιού* (*implicit key*

authentication). Το προτεινόμενο *πιστοποιημένο πρωτόκολλο συμφωνίας κλειδιού ομάδας* βασίζεται στο *πρωτόκολλο συμφωνίας κλειδιού ομάδας* που προτείνεται από τους Lo και άλλους [Lo, 2005] και Hwang και Chang [Hwang, 2003]. Το πρωτόκολλό μας υιοθετεί την πράξη αποκλειστικό-Ή (exclusive-OR (XOR)) που προτείνεται στα [Hwang, 2003] και [Lo, 2005] και όχι στους modular ή εκθετικούς υπολογισμούς που έχουν υψηλό υπολογιστικό κόστος. Επιπλέον, έχει κάποια μοναδικά χαρακτηριστικά που το κάνει ακόμα πιο ασφαλές. Χρησιμοποιεί ένα διαμοιραζόμενο κύριο (master) μυστικό κλειδί (K_M) και βασίζεται στη δομή ενός δένδρου το οποίο εξαρτάται από την απόσταση ανάμεσά στους κόμβους του δικτύου κατά περίσταση.

Μέσω του προτεινόμενου πρωτοκόλλου GKA επιτυγχάνονται οι ακόλουθοι στόχοι ασφάλειας: *μυστικότητα κλειδιού, ανεξαρτησία κλειδιού, πρόσθια μυστικότητα (forward secrecy), οπισθόδρομη μυστικότητα (backward secrecy)* [Lo, 2005]. Η *μυστικότητα κλειδιού* επιτυγχάνεται αφού το κλειδί μπορεί να υπολογιστεί μόνο από μέλη ομάδας. Επιπλέον, καθώς η αποκάλυψη οποιωνδήποτε συνόλων ή ομάδων κλειδιών, δεν οδηγεί στην αποκάλυψη κάποιου άλλου ομαδικού κλειδιού, επιτυγχάνεται επίσης η *ανεξαρτησία κλειδιών*. Επιπλέον, η αποκάλυψη κάποιου μακροπρόθεσμου μυστικού δεν οδηγεί στην αποκάλυψη παλιών ομαδικών κλειδιών. Επομένως, η παραβίαση των τρέχοντων κλειδιών συνεδρίας δεν συνεπάγεται την αποκάλυψη μελλοντικών μυστικών συνεδρίας. Κατά συνέπεια, ένα μέλος που αποχωρεί από την ομάδα παρεμποδίζεται από την πρόσβαση σε ομαδικές επικοινωνίες και επιτυγχάνεται η *πρόσθια μυστικότητα (forward secrecy)*. Επιπλέον, η αποκάλυψη των τρέχοντων μυστικών συνεδρίας δεν συνεπάγεται την αποκάλυψη παλαιότερων κλειδιών συνεδρίας, επομένως επιτυγχάνεται η *οπισθόδρομη μυστικότητα (backward secrecy)*. Μέσω της *οπισθόδρομης μυστικότητας (backward secrecy)* ένα νέο μέλος παρεμποδίζεται από την αποκρυπτογράφηση μηνυμάτων που ανταλλάσσονται ακόμα και αν έχουν καταγραφεί παλαιότερα μηνύματα που έχουν κρυπτογραφηθεί με παλαιότερο κλειδί πριν συμμετάσχει το νέο αυτό μέλος στην ομάδα.

Στις ακόλουθες παραγράφους δίνουμε μία σύντομη περιγραφή του τρόπου με τον οποίο λειτουργεί το πρωτόκολλο GKA. Στον Πίνακα 5.1 παρέχεται η περιγραφή όλων των συμβολισμών που χρησιμοποιούνται στο πρωτόκολλο GKA και στις μονάδες *Τοπικής και Καθολικής Απόκρισης*.

Το πιστοποιημένο πρωτόκολλο συμφωνίας κλειδιών δεν βασίζεται σε συνθηματικά όπως οι μέθοδοι που προτείνονται στα [Lo, 2005] και [Hwang, 2003], αφού τέτοιου είδους πρωτόκολλα είναι ευπαθή σε επιθέσεις λεξικού (dictionary) και βίαιες επιθέσεις "brute force". Στο δικό μας σενάριο, υπάρχουν n μέλη που διαμοιράζονται ένα μυστικό κύριο (master) κλειδί K_M. Το K_M είναι ενσωματωμένο στη συσκευή κάθε κόμβου-μέλους και χρησιμοποιείται για την αρχική επικοινωνία. Αν και το K_M μπορεί να χρησιμοποιηθεί σαν το πρώτο βήμα προκειμένου να αρχικοποιηθεί μία ασφαλής επικοινωνία, δεν είναι ούτε αποτελεσματικό ούτε αρκετό για να χρησιμοποιηθεί σε ασφαλή επικοινωνία συνεδρίας. Επιπλέον, το προτεινόμενο πρωτόκολλο συμφωνίας κλειδιών δε

βασίζεται σε ένα πλήρες δυαδικό δένδρο όπως στο [Lo, 2005] αλλά σε ένα απλό δένδρο με ρίζα (rooted tree).

Υποθέτουμε ότι υπάρχουν n μέλη $M_1, \ldots, M_n$, σε ένα δίκτυο κατά περίσταση που επιθυμούν να έχουν ασφαλή επικοινωνία. Κάθε μέλος αυτής της ομάδας έχει έναν *μοναδικό αριθμό ταυτότητας* (Identity Number (*ID*)). Αυτά τα μέλη συνεργάζονται βασιζόμενα στη δομή ενός δένδρου.

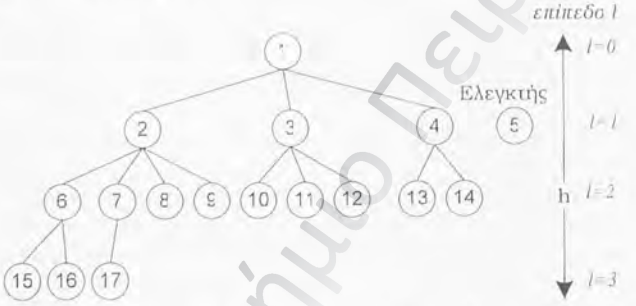
Πίνακας 5. 1 Περιγραφή συμβολισμών του αλγόριθμου GKA

Συμβολισμός	Περιγραφή
M_i	Μέλος i
M_d	Το μέλος είναι ένας κόμβος απόγονος (descendant node)
M_a	Το μέλος είναι ένας κόμβος πρόγονος (ascendant node)
M_{ai}	Το μέλος του δικτύου κατά περίσταση που είναι θύμα μίας επίθεσης
MC_j	Το μέλος του δικτύου κατά περίσταση που είναι το $j^{ο\sigma τό}$ παιδί του κόμβου γονιού στη δομή δένδρου
M_L	Το μέλος του δικτύου κατά περίσταση που αφήνει το δίκτυο (πρωτόκολλο αποχώρησης)
ID_i	Ταυτότητα του μέλους i
K_M	Master κλειδί
$H(\,)$	Μονόδρομη (one – way) συνάρτηση κατακερματισμού (hash) f
S_i	Συμβαλλόμενο (contributory) κλειδί του μέλους i
z	Υπο-κλειδί (subkey) που έχει παραχθεί από τα $M_1, \ldots, M_{n-1}$
K_i', K_i	K_i' είναι το ενδιάμεσο κλειδί και K_i είναι το κλειδί συνεδρίας που κρατείται από το M_i
$nonce_i$	Ο τυχαίος αριθμός που παράγεται από το μέλος M_i
T_i	Το μονοπάτι δένδρου του μέλους κόμβου M_i μέσω του κόμβου γονιού του μέχρι τον κόμβο ρίζα (π.χ. στο Σχήμα 5.6 το μονοπάτι κλειδιών T_5 του κόμβου M_5 είναι $M_5 \rightarrow M_2 \rightarrow M_1$)
$\oplus$	Πράξη XOR
$\|$	Αλυσιδωτή σύνδεση
E_x	Κρυπτογράφηση δεδομένων με κλειδί x μέσω ενός συμμετρικού αλγορίθμου
map_i	Ο eSOM χάρτης του κόμβου μέλους i
LK	Τοπικό μυστικό κλειδί (Local secret Key)
GK	Καθολικό μυστικό κλειδί (Global secret Key)

Σε αυτή τη δομή του δένδρου, κάθε κόμβος είναι είτε φύλλο είτε γονιός ενός ή περισσότερων παιδιών. Αυτοί οι κόμβοι συμβολίζονται με τον μοναδικό αριθμό κάθε μέλους. Σε αυτή την ομάδα, ορίζουμε το μέλος MCh να είναι "ελεγκτής". Ο "ελεγκτής" είναι ένα μέλος της ομάδας που επιλέγεται τυχαία από τον κόμβο ρίζα και τους άμεσους (ενός-βήματος) γείτονές του, όταν δημιουργείται η δομή του δένδρου. Σε περίπτωση που ο τυχαία επιλεγμένος ελεγκτής MCh αποχωρήσει από την ομάδα των κόμβων λόγω κινητικότητας, ο κόμβος-ρίζα έχει τη δυνατότητα να ανιχνεύσει αυτή την κινητικότητα και να επιλέξει κάποιον άλλο

άμεσο (ενός-βήματος) γείτονα για "ελεγκτή". Ο ελεγκτής δεν συμμετέχει στη δομή του δένδρου, αλλά έχει σαν επιπρόσθετο ρόλο την επιβεβαίωση της ορθότητας του κλειδιού συνεδρίας. Επιπλέον, προκειμένου να επιλέξουμε τον "ελεγκτή", δεν απαιτείται η γνώση της καθολικής στατικής τοπολογίας αλλά απλά των άμεσων (ενός-βήματος) γειτόνων του κόμβου-ρίζας, κάτι που αναγνωρίζεται εύκολα από τον κόμβο-ρίζα.

Το δένδρο κατασκευάζεται με βάση την απόσταση ανάμεσα στους κόμβους και τους μοναδικούς τους αριθμούς. Εάν υποθέσουμε ότι το επίπεδο 0 είναι η ρίζα του δένδρου και ότι βρίσκεται στον κόμβο M_1 με αριθμό ταυτότητας ID_1, τότε στο επίπεδο ένα θα βρίσκονται οι άμεσοι (ενός-βήματος) γείτονές του, στο επίπεδο δύο οι γείτονες που βρίσκονται δύο βήματα μακριά, μέχρι το τελευταίο επίπεδο όπου τοποθετούνται οι πιο απομακρυσμένοι κόμβοι μέσα στην εμβέλεια μετάδοσης του κόμβου ρίζας.



Σχήμα 5. 7. Δομή Κλειδιού που Απεικονίζει την Ιδιότητα Μέλους

Το Σχήμα 5.7 απεικονίζει ένα παράδειγμα ενός δένδρου κλειδιού με 17 μέλη. Στο δένδρο κλειδιού, η ρίζα του τοποθετείται στο επίπεδο $l=0$ και το ύψος του είναι h, όπου $h=4$. Όλοι οι κόμβοι στο επίπεδο ένα είναι άμεσοι (ενός-βήματος) γείτονες του κόμβου ρίζας M_1, όλοι οι κόμβοι στο επίπεδο δύο είναι γείτονες δύο βημάτων του κόμβου M_1 (ρίζα) και άμεσοι (ενός βήματος) γείτονες των κόμβων γονιών του επιπέδου ένα (M_2, M_3, M_4 αντίστοιχα). Επιπλέον όλοι οι κόμβοι στο επίπεδο τρία είναι γείτονες τρία βήματα μακριά του κόμβου-ρίζα M_1 (οι τελευταίοι κόμβοι στην εμβέλεια επικοινωνίας του κόμβου M_1). Ο κόμβος μέλος M_5 είναι ο "ελεγκτής". Ο στόχος μας είναι όλοι οι κόμβοι στο δίκτυο κατά περίσταση να συμφωνούν στο κλειδί συνεδρίας K:

$$K = S_1 \oplus S_2 \oplus .... \oplus S_n, \tag{5.1}$$

όπου το S_i συνεισφέρεται από το M_i και επιλέγεται τυχαία.

Το πρωτόκολλο διαχωρίζεται σε δύο φάσεις:

- τη *φάση αρχικοποίησης κλειδιού*, και
- τη φάση *δημιουργίας του κλειδιού συνεδρίας*.

Στη *φάση αρχικοποίησης κλειδιού*, οι κόμβοι M_1, M_2, …, M_n συνεργάζονται έτσι ώστε μυστικά να κατασκευάσουν ένα υποκλειδί z:

$$z = S_1 \oplus S_2 \oplus \ldots \oplus S_n \quad (5.2)$$

Σημειώνουμε εδώ ότι στην εξίσωση 5.2 ο κόμβος ελεγκτής M_{Ch} δεν συνεισφέρει στην κατασκευή του υποκλειδιού.

Στην φάση *παραγωγής του κλειδιού συνεδρίας*, κάθε M_i (i= 1, 2, …, n και $i \neq Ch$) συμμετέχει σε διαφορετικές ανταλλαγές με τον κόμβο M_{Ch}. Μετά από αυτή την ανταλλαγή όλα τα μέλη έχουν αρκετές πληροφορίες προκειμένου να υπολογίσουν το κλειδί συνεδρίας K. Ο κόμβος μέλος M_{Ch}, επιπλέον επιβεβαιώνει ότι τα άλλα μέλη δημιούργησαν το ίδιο κλειδί συνεδρίας K. Περιγράφουμε τη μέθοδό μας με λεπτομέρεια στις ακόλουθες υπο-ενότητες.

Επιπλέον, στη συνέχεια αυτής της ενότητας θα εξετάσουμε τι συμβαίνει όταν κάποιος κόμβος αποχωρεί ή εισέρχεται στην ομάδα κόμβων αφού δημιουργηθεί το αντίστοιχο κλειδί ομάδας-συνεδρίας. Περιγράφουμε λοιπόν τον τρόπο λειτουργίας των πρωτοκόλλων:

- *Συμμετοχής Μέλους* και
- *Αποχώρησης Μέλους*.

Σε περίπτωση που δεν πραγματοποιηθεί καμία συμμετοχή ή αποχώρηση από την ομάδα για ένα συγκεκριμένο χρονικό διάστημα, προκειμένου να προστατεύουμε το κλειδί συνεδρίας προτείνουμε τη δημιουργία ενός *πρωτοκόλλου περιοδικής ανανέωσης* το οποίο περιγράφεται σε επόμενη υπο-ενότητα.

5.1.1 Φάση Αρχικοποίησης Κλειδιού

Αρχικά, όλοι οι κόμβοι μέλη θεωρούνται κακόβουλοι μέχρι να αποδειχτεί το αντίθετο. Ένας κόμβος που ξεκινά την κανονική διαδικασία επικοινωνίας (*Φάση Αρχικοποίησης Κλειδιού*) θεωρείται ότι είναι έγκυρος. Κατά την προτεινόμενη *Φάση Αρχικοποίησης Κλειδιού*, αντίστοιχα με το [19], για $i \neq Ch$, όλοι οι κόμβοι μέλη εκτελούν τρία βήματα προκειμένου να επιτύχουν αμοιβαία πιστοποίηση.

Στο *πρώτο βήμα*, κάθε κόμβος απόγονος (M_d) στέλνει στον πρόγονο του (M_a) ένα μήνυμα που περιλαμβάνει την ταυτότητά του (ID_d), την ταυτότητα του προγόνου του (ID_a) και ένα κρυπτογραφημένο μήνυμα με το κύριο (master) κλειδί (K_M) που προέρχεται από τη συνένωση της ταυτότητας του απόγονου (ID_d), την ταυτότητα του προγόνου του (ID_a) και κάποια τυχαία ποσότητα $nonce_d$ που παράγεται από το M_d (δηλ. $E_{K_M}(ID_d \| ID_a \| nonce_d)$).

Στο *δεύτερο βήμα* ο κόμβος πρόγονος (M_a) στέλνει στον κόμβο απόγονο (M_d) ένα μήνυμα που περιλαμβάνει την ταυτότητά του ID (ID_a), την ταυτότητα του προγόνου (ID_d) και ένα κρυπτογραφημένο μήνυμα με το κύριο (master) κλειδί (K_M) που προέρχεται από τη συνένωση της ταυτότητας του κόμβου απόγονου (ID_d), την ταυτότητα του κόμβου προγόνου (ID_a), την τυχαία ποσότητα ($nonce_d$) που παράχθηκε από τον απόγονο αυξημένο κατά ένα ($nonce_d+1$), και την τυχαία τιμή $nonce_a$ που δημιουργήθηκε από τον πρόγονο (π.χ. $E_{K_M}(ID_a \| ID_d \| nonce_d + 1 \| nonce_a)$).

Στο *τρίτο βήμα* ο κόμβος απόγονος (M_d) στέλνει στον κόμβο πρόγονο (M_a) ένα μήνυμα που περιλαμβάνει την ταυτότητά του (ID_d), την ταυτότητα του προγόνου του (ID_a) και ένα κρυπτογραφημένο μήνυμα με το κύριο (master) κλειδί (K_M) που προέρχεται από τη συνένωση της ταυτότητας του απόγονου (ID_d), την ταυτότητα του προγόνου (ID_a), την τυχαία τιμή που παράγεται από τον πρόγονο αυξημένη κατά ένα ($nonce_a+1$), και το ενδιάμεσο κλειδί K_i' (δηλ. $E_{K_M}(ID_a \| ID_d \| nonce_a+1 \| K_i'))$.

Η τιμή που έχει το K_i' εξαρτάται από τη θέση του κόμβου i στο δένδρο.

- Εάν ο M_i είναι ένας κόμβος φύλλο τότε $K_i' = S_i$. (5.3)
- Εάν ο M_i είναι ένας κόμβος γονιός τότε $K_i' = S_i \oplus K'_{C_1} \oplus ... \oplus K'_{C_j}$, (5.4)

  όπου K'_{C_j} είναι το ενδιάμεσο κλειδί του j παιδιού (C_j) του M_i κόμβου.
- Εάν i=1, ο M_i είναι ο κόμβος ρίζα και υπολογίζει τις τιμές του z, όπου $z = S_1 \oplus K'_{C_1} \oplus K'_{C_2} \oplus ... \oplus K'_{C_j} = S_1 \oplus S_2 \oplus ... \oplus S_{n-1}$. (5.5)

Ο αλγόριθμος της *Φάσης Αρχικοποίησης Κλειδιού* απεικονίζεται στο Σχήμα 5.8.

Για ($i \neq Ch$): Χρησιμοποιούνται τα Βήματα 1 έως 3 προκειμένου να επιτευχθεί αμοιβαία πιστοποίηση

Βήμα 1

$M_d \xrightarrow{ID_d, ID_a, E_{K_M}(ID_d \| ID_a \| nonce_d)} M_a$

Βήμα 2

$M_d \xleftarrow{ID_a, ID_d, E_{K_M}(ID_a \| ID_d \| nonce_d + 1 \| nonce_a)} M_a$

Βήμα 3

$M_d \xrightarrow{ID_a, ID_d, E_{K_M}(ID_a \| ID_d \| nonce_a + 1 \| K_i')} M_a$

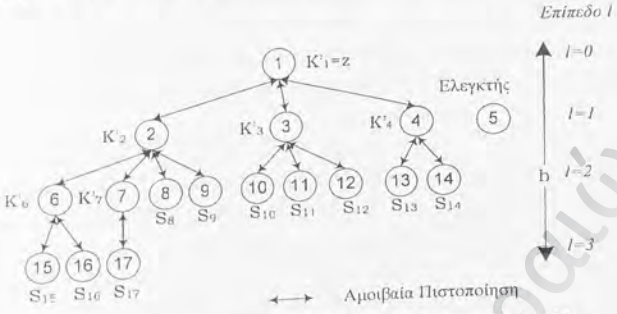
- Εάν ο M_i είναι ένας κόμβος φύλλο, τότε $K_i' = S_i$. (5.6)
- Εάν ο M_i είναι ένας κόμβος γονιός, έχει ένα ή περισσότερα παιδιά και αναπαρίσταται σαν C_j (j= 1,…,l), τότε:

  $K_i' = S_i \oplus K'_{C_1} \oplus ... \oplus K'_{C_j}$. (5.7)
- Εάν ο M_i είναι κόμβος ρίζα (i=1) τότε ο M_1 υπολογίζει το υποκλειδί z

  $z = S_1 \oplus K'_{C_1} \oplus K'_{C_2} \oplus ... \oplus K'_{C_j} = S_1 \oplus S_2 \oplus ... \oplus S_{n-1}$. (5.8)

Σχήμα 5. 8 Αλγόριθμος Φάσης Αρχικοποίησης Κλειδιού

Ένα παράδειγμα του μηχανισμού δημιουργίας του υποκλειδιού z για τους κόμβους M_i για $i=1, 2, \ldots, 17$ is απεικονίζεται στο Σχήμα 5.9.



Σχήμα 5. 9 Δημιουργία του Υποκλειδιού z από τους M_1 έως M_{17}

Στο τέλος αυτής της φάσης τα *Τοπικά Κλειδιά (LK)* των άμεσων γειτόνων (ενός-βήματος) του κόμβου-ρίζα υπολογίζονται και μετέπειτα, χρησιμοποιούνται στη μονάδα *Τοπικής Απόκρισης*:

$$LK = LK_j = z \oplus S_j \quad (5.9)$$

όπου j είναι όλοι οι άμεσοι (ενός-βήματος) γείτονες του κόμβου ρίζα και συνεπώς ανήκουν στο πρώτο επίπεδο του δένδρου.

5.1.2 Φάση Συμφωνίας Κλειδιού Συνεδρίας

Η προτεινόμενη φάση συμφωνίας κλειδιού συνεδρίας χρησιμοποιεί ένα διαμοιραζόμενο κύριο (master) κλειδί και όχι ένα συνθηματικό. Το υποκλειδί $z(=S_1 \oplus S_2 \oplus \ldots \oplus S_n)$ που υπολογίστηκε από τον κόμβο M_1 στο τέλος της *Φάσης Αρχικοποίησης Κλειδιού* χρησιμοποιείται στη *Φάση Συμφωνίας Κλειδιού Συνεδρίας*. Αντίστοιχα με το [Lo, 2003], ο αλγόριθμος της *Φάσης Συμφωνίας Κλειδιού Συνεδρίας* απεικονίζεται στο Σχήμα 5.10:

Βήμα 1

M_1 *ανοικτή εκπομπή* $ID_1, E_{K_M}(ID_1 \| z \| nonce_1)$ → M_i, *για* $i=2,3,\ldots,n$

Βήμα 2

M_{Ch} *ανοικτή εκπομπή* $ID_{Ch}, E_{K_M}(ID_{Ch} \| S_{Ch} \| nonce_1 + 1 \| nonce_{Ch})$ → M_i *για* $i = 1, 2, \ldots, n$ *και* $i \neq Ch$

Βήμα 3

M_{Ch} ← $ID_i, ID_{Ch}, H(ID_{Ch} \| nonce_{Ch} + 1 \| K_i)$ M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$ και $K_i = z \oplus S_{Ch}$ (5.10)

Βήμα 4

M_{Ch} ελέγχει το κλειδί συνεδρίας K.

Σχήμα 5. 10 Αλγόριθμος Φάσης Συμφωνίας Κλειδιού Συνεδρίας

Στο *πρώτο βήμα* της *Φάσης Συμφωνίας Κλειδιού Συνεδρίας*, η ρίζα M_1 του δένδρου στέλνει με ανοικτή εκπομπή το υποκλειδί z σε όλα τα μέλη M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$. Συγκεκριμένα, ο M_1 εκπέμπει με ανοικτή εκπομπή ένα μήνυμα το οποίο περιλαμβάνει την ταυτότητά του (ID_1) και ένα κρυπτογραφημένο μήνυμα με το κύριο κλειδί K_M, το οποίο περιλαμβάνει την ένωση της ταυτότητας του κόμβου M_1 (ID_1), το υποκλειδί z, και την τυχαία ποσότητα $nonce_1$ που δημιουργείται από τον κόμβο M_1 (δηλ. $E_{K_M}(ID_1 \| z \| nonce_1)$).

Στο *δεύτερο βήμα*, ο ελεγκτής M_{Ch}, αφού λάβει το υποκλειδί z από τον κόμβο M_1, παράγει μία τυχαία ποσότητα S_{Ch}, η οποία θα χρησιμοποιηθεί στη φάση συμφωνίας κλειδιού συνεδρίας και μία τυχαία ποσότητα $nonce_{Ch}$ για αμοιβαία πιστοποίηση. Τότε, ο κόμβος M_{Ch} στέλνει με ανοικτή εκπομπή σε όλους τους κόμβους M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$, την ταυτότητά του (ID_{Ch}) και ένα κρυπτογραφημένο μήνυμα με κύριο κλειδί K_M το οποίο περιλαμβάνει τη συνένωση της ταυτότητας του (ID_{Ch}), την παραγόμενη τυχαία ποσότητα S_{Ch}, την τυχαία ποσότητα που παράχθηκε από τον κόμβο M_1 αυξημένη κατά ένα ($nonce_1 + 1$) και το $nonce_{Ch}$ που παράγεται από το M_{Ch} (δηλ. $E_{K_M}(ID_n \| S_n \| nonce_1 + 1 \| nonce_n)$).

Στο *τρίτο βήμα* τα μέλη M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$, αναλύουν (unbind) την ποσότητα που έλαβαν από το M_{Ch} και κατασκευάζουν ένα κλειδί συνεδρίας $K_i = z \oplus S_{Ch}$. Τότε, ο κόμβος-μέλος M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$, στέλνει ένα μήνυμα που περιλαμβάνει την ταυτότητά του (ID_i), την ταυτότητα του μέλους κόμβου M_{Ch} (ID_{Ch}) και το αποτέλεσμα της συνάρτησης κατακερματισμού H ενός μηνύματος που προέρχεται από τη συνένωση του ID_{Ch}, την τυχαία ποσότητα $nonce_{Ch}$ αυξημένη κατά ένα και το K_i (δηλ. $H(ID_n \| nonce_n + 1 \| K_i)$).

Στο *τέταρτο βήμα*, ο κόμβος μέλος M_{Ch} επιβεβαιώνει ότι κάθε μέλος παρήγαγε (δημιούργησε) το ίδιο κλειδί συνεδρίας $K = (K_1 = K_2 = \ldots = K_n)$ και ενημερώνει όλους τους κόμβους μέλη M_i, για $i = 1, 2, \ldots, n$ και $i \neq Ch$, ότι το κλειδί συνεδρίας δημιουργήθηκε επιτυχώς. Το *κλειδί συνεδρίας* K που συμφωνήθηκε σε αυτή τη φάση είναι το *Καθολικό Κλειδί (Global Key (GK))* που θα χρησιμοποιηθεί στη μονάδα *Καθολικής Απόκρισης (Global Response)*:

$$GK = K = z \oplus S_{Ch} \tag{5.11}$$

5.1.3 Γεγονότα Συμμετοχής

Σε ένα δυναμικό δίκτυο κατά περίσταση, οι κόμβοι μέλη μπορεί να έχουν μικρή διάρκεια συμμετοχής. Νέα μέλη μπορεί να συμμετάσχουν ή να αποχωρήσουν από την ομάδα μελών, αφού δημιουργηθεί το κλειδί συνεδρίας. Τα νέα μέλη δεν είναι εξουσιοδοτημένα ώστε να γνωρίζουν το κλειδί συνεδρίας που έχει συμφωνηθεί πριν τη συμμετοχή τους στο δίκτυο κατά περίσταση. Επομένως, τα μέλη κόμβοι του δικτύου κατά περίσταση θα πρέπει να αλλάξουν το συμφωνημένο κλειδί συνεδρίας καθώς και το μυστικό διαμοιραζόμενο κλειδί (K_M). Με τον ίδιο τρόπο, στην περίπτωση που ένας κόμβος αποχωρήσει από το

δίκτυο κατά περίσταση, το κλειδί συνεδρίας θα πρέπει να αλλάξει προκειμένου να επιβεβαιωθεί η ασφαλής επικοινωνία των κόμβων που έχουν μείνει στην ομάδα. Αυτή η ενότητα περιγράφει δύο πρωτόκολλα που επιτυγχάνουν τα παραπάνω, συγκεκριμένα:

- το *Πρωτόκολλο Συμμετοχής Μέλους*, και
- το *Πρωτόκολλο Αποχώρησης Μέλους*.

Α. Πρωτόκολλο Συμμετοχής Μέλους

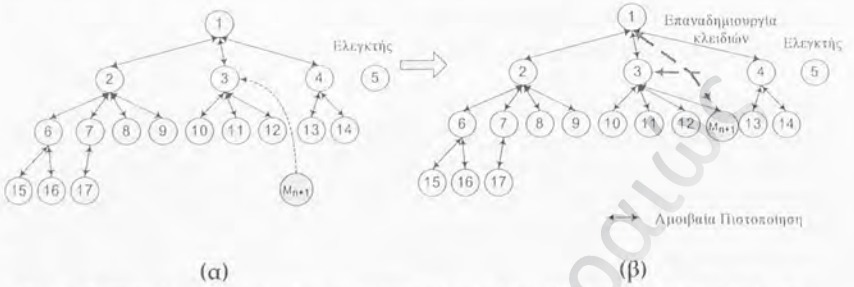
Το προτεινόμενο *Πρωτόκολλο Συμμετοχής Μέλους* ακολουθεί τη ροή πρωτοκόλλου που υποδηλώνεται από τη δομή του δένδρου. Ας υποθέσουμε ότι μία ομάδα κόμβων έχει n μέλη: $M_1, M_2, \ldots, M_n$ και ότι ένα νέο μέλος M_{n+1} θέλει να συμμετάσχει στην ομάδα των κόμβων. Το νέο μέλος στέλνει ένα μήνυμα αίτησης συμμετοχής το οποίο περιλαμβάνει την ταυτότητά του (ID_{n+1}). Το νέο μέλος επιτρέπεται να συμμετάσχει στην ομάδα όταν τα υπάρχοντα μέλη της ομάδας λαμβάνουν το μήνυμά του και το δέχονται. Επιπλέον, τα μέλη της ομάδας πρέπει να αλλάξουν το κύριο κλειδί από K_M σε K'_M και να ανακατασκευάσουν το κλειδί συνεδρίας.

Η διαδικασία που θα ακολουθηθεί εξαρτάται από το πόσο κοντά στον κόμβο μέλος ρίζα M_1 θα είναι το νέο μέλος κόμβος M_{n+1}. Επομένως, εάν το νέο μέλος κόμβος M_{n+1} είναι ένας άμεσος (ενός-βήματος) γείτονας του κόμβου ρίζας M_1 τότε θα τοποθετηθεί στο επίπεδο ένα, εάν είναι γείτονας δύο βημάτων του κόμβου ρίζας M_1, και επομένως άμεσος γείτονας (ενός-βήματος) του κόμβου γονιού στο επίπεδο ένα, θα τοποθετηθεί στο επίπεδο δύο. Εάν υποθέσουμε ότι το νέο μέλος M_{n+1} είναι l-βήματα μακριά από τον κόμβο ρίζα M_1, τότε η θέση του στο δένδρο θα είναι στο $l^{\text{οστό}}$ επίπεδο και θα είναι παιδί του κόμβου του οποίου είναι άμεσος γείτονας ενός βήματος. Τότε το μονοπάτι κλειδιού $M_{n+1} \rightarrow M_{l-1} \rightarrow M_l$

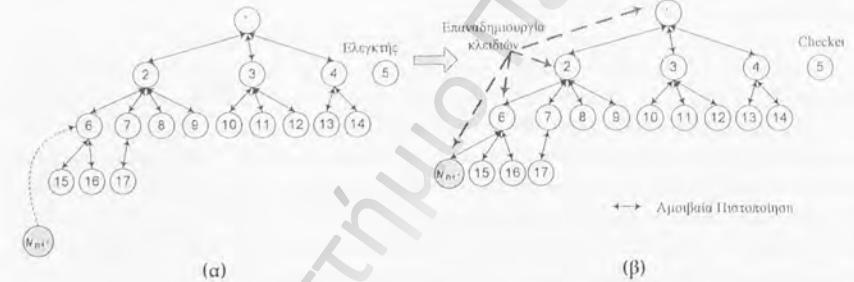
Η διαδικασία που θα ακολουθηθεί εξαρτάται από το πόσο κοντά στον κόμβο μέλος ρίζα M_1 θα είναι ο νέος κόμβος-μέλος M_{n+1}. Επομένως, εάν το νέο μέλος κόμβος M_{n+1} είναι ένας άμεσος (ενός-βήματος) γείτονας του κόμβου-ρίζας M_1 τότε θα τοποθετηθεί στο επίπεδο ένα, εάν είναι γείτονας δύο βημάτων του κόμβου-ρίζας M_1, και επομένως άμεσος γείτονας (ενός-βήματος) του κόμβου γονιού στο επίπεδο ένα, θα τοποθετηθεί στο επίπεδο δύο. Εάν υποθέσουμε ότι το νέο μέλος M_{n+1} είναι l-βήματα μακριά από τον κόμβο ρίζα M_1, τότε η θέση του στο δένδρο θα είναι στο $l^{\text{οστό}}$ επίπεδο και θα είναι παιδί του κόμβου του οποίου είναι άμεσος γείτονας (ενός-βήματος). Τότε το μονοπάτι κλειδιού $M_{n+1} \rightarrow M_{l-1} \rightarrow M_{l-2} \rightarrow \ldots \rightarrow M_1$ όπου M_{l-1} (M_{l-2}) αναπαριστά τον κόμβο μέλος που βρίσκεται στο $l\text{-}1^{\text{οστό}}$($l\text{-}2^{\text{οστό}}$) επίπεδο και είναι κόμβος μέλος γείτονας ενός (δύο)-βημάτων του νέου κόμβου μέλους κόμβου (αντίστοιχα).

Δύο παραδείγματα όπου ένας νέος κόμβος-μέλος M_{n+1} συμμετέχει σε μία ομάδα n μελών $M_1, M_2, \ldots, M_n$ απεικονίζονται στα σχήματα 5.11 και 5.12 όπου το νέο μέλος θα γίνει εσωτερικός κόμβος ή κόμβος-φύλλο αντίστοιχα. Ο νέος κόμβος-μέλος M_{n+1} είναι ένα γείτονας τριών βημάτων του κόμβου ρίζας M_1, ένας γείτονας δύο βημάτων του μέλους κόμβου M_2 και άμεσος γείτονας (ενός

βήματος) του κόμβου-μέλους M_5. Κάθε ένα από τα μέλη M_i, εκτός από τον κόμβο ρίζα M_1 του μονοπατιού κλειδιού T_{n+1}, $M_{n+1} \rightarrow M_5 \rightarrow M_2 \rightarrow M_1$ πραγματοποιεί τη *Φάση Αρχικοποίησης Κλειδιού*.



Σχήμα 5. 11 Το Δέντρο Κλειδιού με τη Συμμετοχή ενός Νέου Κόμβου στο Δεύτερο Επίπεδο.



Σχήμα 5. 12 Το Δένδρο Κλειδιού με τη Συμμετοχή ενός Νέου Κόμβου στο Τρίτο Επίπεδο.

Συγκεκριμένα, εάν ο M_d είναι ένας κόμβος απόγονος και ο M_a είναι ένας κόμβος πρόγονος στο μονοπάτι κλειδιού τότε πραγματοποιείται το πρωτόκολλο της *Φάσης Εκκίνησης του Μονοπατιού Δένδρου Κλειδιού* που απεικονίζεται *στο* Σχήμα 5.13.

Τέλος, ο κόμβος-ρίζα M_1 πραγματοποιεί τον αλγόριθμο της *Φάσης Συμφωνίας Κλειδιού* (ενότητα 5.1.2) για να ανακατασκευάσει και να επαληθεύσει το νέο κλειδί συνεδρίας.

Βήμα α

$M_d \xrightarrow{ID_d, ID_a, E_{K'_M}(ID_d \| ID_a \| nonce''_d)} M_a$

Βήμα β

$M_d \xleftarrow{ID_a, ID_d, E_{K'_M}(ID_a \| ID_d \| nonce''_d + 1 \| nonce''_a)} M_a$

Βήμα γ

$M_d \xrightarrow{ID_a, ID_d, E_{K'_M}(ID_a \| ID_d \| nonce''_a + 1 \| K_i'')} M_a$

- Εάν ο M_i είναι ένας κόμβος φύλλο τότε $K_i'' = S_i''$. (5.12)
- Εάν ο M_i είναι ένας κόμβος-γονιός και έχει ένα ή περισσότερα παιδιά που αναπαριστώνται σαν C_j ($j= 1,\ldots,l$), τότε:
  $K_i'' = S_i'' \oplus K_{C_1}'' \oplus \ldots \oplus K_{C_l}''$. (5.13)
- Εάν το παιδί M_{C_j} του M_i δεν είναι στο μονοπάτι κλειδιού, τότε:
  $K_{C_j}'' = K_{C_j}'$, (5.14)
- Εάν ο κόμβος M_i είναι ο κόμβος ρίζα ($i=1$), τότε ο M_1 υπολογίζει το υποκλειδί z' χρησιμοποιώντας το K_i'' των μελών στο μονοπάτι του κλειδιού και το K_i των άλλων μελών του δέντρου και υπολογίζει το νέο υποκλειδί:
  $z' = S_1 \oplus K'_{C_1} \oplus K'_{C_2} \oplus \ldots \oplus K'_{C_j}$ (5.15)

Σχήμα 5. 13 Πρωτόκολλο Φάσης Έκκίνησης Μονοπατιού Δένδρου Κλειδιού

Β. Πρωτόκολλο Αποχώρησης Μέλους

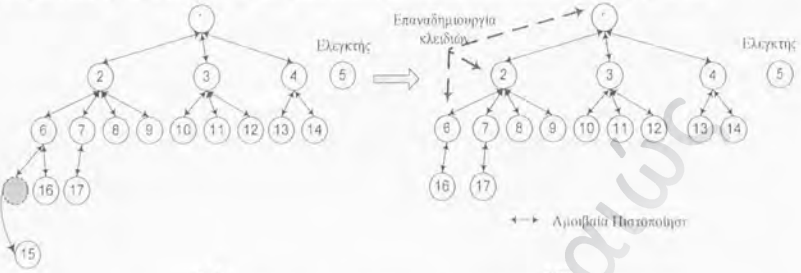
Ας υποθέσουμε ότι υπάρχουν n μέλη στην ομάδα του δικτύου κατά περίσταση και ότι το μέλος M_L θέλει να αποχωρήσει. Σε αυτή την περίπτωση, το κλειδί συνεδρίας που έχει συμφωνηθεί πρέπει να αλλάξει και η δομή του κλειδιού πρέπει να τροποποιηθεί. Προκειμένου να διατηρηθεί η ασφάλεια της ομάδας των κόμβων του δικτύου κατά περίσταση, το διαμοιραζόμενο κύριο (master) κλειδί (K_M) πρέπει επίσης να αλλάξει σε K'_M το οποίο προέρχεται από την πράξη XOR ανάμεσα στο K_M και το παλιό κλειδί συνεδρίας K_{old} :

$K'_M = K_M \oplus K_{old}$. (5.16)

Το μέλος αποχώρησης M_L ξεκινά το *Πρωτόκολλο Αποχώρησης Μέλους* στέλνοντας ένα μήνυμα αποχώρησης σε όλα τα μέλη της ομάδας. Το *Πρωτόκολλο Αποχώρησης Μέλους* χρησιμοποιεί το διαμοιραζόμενο κύριο κλειδί K'_M και εξαρτάται από τη θέση του M_L' στο δένδρο του κλειδιού. Επομένως, διαχωρίζουμε δύο περιπτώσεις ανάλογα με το αν ο κόμβος M_L είναι κόμβος-φύλλο ή εσωτερικός κόμβος.

Περίπτωση 1: Ο M_L είναι κόμβος φύλλο

Το Σχήμα 5.14 (α) απεικονίζει ένα παράδειγμα αυτής της περίπτωσης. Σε αυτή την περίπτωση, πρέπει να πραγματοποιηθούν τα ακόλουθα δύο βήματα:



(α) (β)

Σχήμα 5. 14 Το Δένδρο Κλειδιού μετά την Αποχώρηση του Μέλους M_2

Βήμα 1

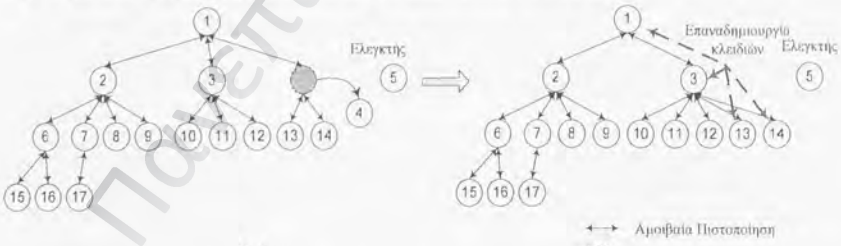
Εάν ο κόμβος M_{15} αποχωρήσει από την ομάδα, η νέα δομή δένδρου κλειδιού απεικονίζεται στο Σχήμα 5.14 (β).

Βήμα 2

Κάθε ένα από τα μέλη M_i εκτός από τον κόμβο ρίζα M_1, στο μονοπάτι του κλειδιού $M_6 \rightarrow M_2 \rightarrow M_1$ πραγματοποιεί τη *Φάση Αρχικοποίησης Κλειδιού* όπως περιγράφεται στην ενότητα 5.1.1. Τέλος, ο κόμβος M_1 πραγματοποιεί τον αλγόριθμο της *Φάσης Συμφωνίας Κλειδιού Συνεδρίας* (ενότητα 5.1.2) για να ανακατασκευάσει και να επαληθευθεί το νέο κλειδί συνεδρίας.

Περίπτωση 2: ο M_L είναι ένας εσωτερικός κόμβος.

Το Σχήμα 5.15 (α) απεικονίζει ένα παράδειγμα αυτής της περίπτωσης. Σε αυτή την περίπτωση πραγματοποιούνται τα ακόλουθα δύο βήματα:



(α) (β)

Σχήμα 5. 15 Το Δένδρο Κλειδιού μετά την Αποχώρηση του Μέλους M_{14}

Βήμα 1

Εάν ο κόμβος M_4 αποχωρήσει από την ομάδα, τότε ο άμεσος γείτονας (ενός-βήματος) που είναι πιο κοντά στα παιδιά του κόμβου που αποχώρησε θα γίνει ο κόμβος γονιός τους. Στο παράδειγμά μας στο Σχήμα 5.15 όταν ο κόμβος μέλος

M_4 αποχωρεί, τότε ο κόμβος που θα τον αντικαταστήσει είναι είτε ο κόμβος M_2 είτε ο κόμβος M_3. Εάν υποθέσουμε ότι ο κόμβος M_3 βρίσκεται πιο κοντά στα παιδιά του M_4 τότε ο κόμβος M_3 θα γίνει ο νέος κόμβος γονιός και η δομή δένδρου θα αναδιοργανωθεί. Η νέα δομή δένδρου απεικονίζεται στο Σχήμα 5.15 (β).

Βήμα 2

Κάθε ένα από τα μέλη M_i, εκτός από τον κόμβο ρίζα M_1 στο μονοπάτι κλειδιού $M_3 \rightarrow M_1$ και τα δύο παιδιά M_{13}, M_{14} του κόμβου M_3, πραγματοποιούν τη φάση εκκίνησης του κλειδιού. Πιο συγκεκριμένα, για τους κόμβους M_3, M_{13}, M_{14} το πρωτόκολλο της *Φάσης Εκκίνησης Μονοπατιού Δένδρου Κλειδιού* πραγματοποιείται (όπως περιγράφεται στην ενότητα 5.1.3Α) προκειμένου να υπολογιστεί το νέο υποκλειδί z'. Τέλος, το M_1 πραγματοποιεί τον αλγόριθμο της ενότητας 5.1.2 για να ανακατασκευάσει το νέο κλειδί συνεδρίας.

5.1.4 Περιοδική Ανανέωση του Κλειδιού Συνεδρίας

Εάν κανένα μέλος δεν εισέλθει ή δεν αποχωρήσει από την ομάδα των κόμβων του δικτύου κατά περίσταση για μία μεγάλη χρονική περίοδο, το κλειδί συνεδρίας K, πρέπει να αλλαχθεί προκειμένου να προστατευθεί από πιθανή έκθεση και να επαληθευθεί η δύναμή του ως προς την ασφάλεια. Παρόμοια με το [Lo, 2005], τα βήματα που πρέπει να πραγματοποιηθούν είναι τα ακόλουθα.

Στο *πρώτο βήμα*, ο κόμβος μέλος M_{Ch} στέλνει με ανοιχτή εκπομπή ένα μήνυμα στους κόμβους μέλη M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$. Το εκπεμπόμενο μήνυμα περιλαμβάνει την ταυτότητα του κόμβου μέλους M_{Ch} (ID_{Ch}) και ένα κρυπτογραφημένο μήνυμα μόνο με το παλαιό κλειδί (K_{old}) το οποίο περιλαμβάνει τη συνένωση της ταυτότητας του μέλους-κόμβου (ID_{Ch}), μία νέα τυχαία ποσότητα (S''_{Ch}) που παράγεται από το M_{Ch}, και το $nonce_{Ch}$ που παράγεται από τον κόμβο M_{Ch} (δηλ. $(E_{K_{old}}(ID_{Ch} \| S''_{Ch} \| nonce_{Ch}))$).

Στο *δεύτερο βήμα*, οι κόμβοι μέλη M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$, αποκρυπτογραφούν το μήνυμα που στάλθηκε από τον M_{Ch} και υπολογίζουν ένα νέο κλειδί συνεδρίας:

$$K_{new} = K_{old} \oplus S''_{Ch}. \quad (5.17)$$

Στο *τρίτο βήμα*, οι κόμβοι μέλη M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$, στέλνουν ένα μήνυμα στον κόμβο μέλος M_{Ch} το οποίο περιλαμβάνει την ταυτότητα (ID_i) του κάθε κόμβου μέλους M_i, την ταυτότητα (ID_{Ch}) του κόμβου μέλους M_{Ch} και το αποτέλεσμα της συνάρτησης κατακερματισμού της συνένωσης που περιλαμβάνει την ταυτότητα (ID_{Ch}) του κόμβου μέλους M_{Ch}, το $nonce_{Ch}$ που παράγεται από τον κόμβο M_{Ch} αυξημένο κατά ένα και το νέο κλειδί συνεδρίας K_{new}.

Στο *τέταρτο βήμα*, ο κόμβος μέλος M_{Ch} επιβεβαιώνει ότι κάθε μέλος δημιούργησε το ίδιο κλειδί συνεδρίας K_{new} ($=K_1=K_2=\ldots=K_n$) , και ενημερώνει όλα τα μέλη M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$, ότι το κλειδί συνεδρίας δημιουργήθηκε επιτυχώς.

Σημειώνουμε εδώ ότι το νέο κλειδί συνεδρίας K_{new} είναι το νέο Καθολικό Κλειδί (GK_{new}) που θα χρησιμοποιηθεί στη μονάδα *Καθολικής Απόκρισης*:

$$GK_{new} = K_{new} = K_{old} \oplus S''_{Ch} \quad (5.18)$$

Το πρωτόκολλο *Περιοδικής Ανανέωσης του Καθολικού Κλειδιού Συνεδρίας* [Lo, 2005] παρουσιάζεται στο Σχήμα 5.16.

Βήμα 1

M_{Ch} *ανοικτή εκπομπή* $ID_{Ch}, E_{K_{old}}(ID_{Ch} \| S''_{Ch} \| nonce_{Ch})$ → M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$

Βήμα 2

M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$, υπολογίζει το νέο κλειδί συνεδρίας:

$$K_i = K_{old} \oplus S''_{Ch} \quad (5.19)$$

Βήμα 3

M_{Ch} ← $ID_i, ID_{Ch}, H(ID_{Ch} \| nonce_{Ch}+1 \| K_i)$ M_i, για $i=1, 2, 3, \ldots, n$ και $i \neq Ch$

Βήμα 4

M_{Ch} ελέγχει το νέο κλειδί συνεδρίας $K_{new} = K_i$.

Σχήμα 5. 16 Πρωτόκολλο Περιοδικής Ανανέωσης Καθολικού Κλειδιού Συνεδρίας

Εκτός από την περιοδική ανανέωση του *Καθολικού Κλειδιού (Global Key (GK))*, τα *Τοπικά Κλειδιά (Local Keys (LK))* που χρησιμοποιούνται από τη *Μονάδα Τοπικής Απόκρισης* πρέπει επίσης να ανανεώνονται μετά από μία μεγάλη χρονική περίοδο.

Τα βήματα που πραγματοποιούνται για την περιοδική ανανέωση των *Τοπικών Κλειδιών (Local Keys(LK))* είναι τα ακόλουθα:

Στο *πρώτο βήμα*, οι κόμβοι μέλη M_j που βρίσκονται στο πρώτο επίπεδο του δένδρου και είναι άμεσοι γείτονες (ενός-βήματος) του κόμβου M_1 στέλνουν στον κόμβο-ρίζα M_1 ένα μήνυμα που περιλαμβάνει την ταυτότητά τους (ID_j) και ένα κρυπτογραφημένο μήνυμα με τα παλαιά *Τοπικά Κλειδιά* ($LK_{old}=LK_j$) το οποίο περιλαμβάνει τη συνένωση των ταυτοτήτων τους (ID_j), μία νέα τυχαία ποσότητα (S''_j) που παράγεται από το M_j, και το $nonce_j$ που δημιουργήθηκε από τον κόμβο M_j, (δηλ. $(E_{LK_{old}}(ID_j \| S''_j \| nonce_j))$).

Στο *δεύτερο βήμα*, οι κόμβοι μέλη M_j υπολογίζουν τα νέα *Τοπικά Κλειδιά*

$$LK_{new} = LK'_j = LK_{old} \oplus S''_j \quad . \quad (5.20)$$

Στο *τρίτο βήμα*, οι κόμβοι μέλη M_j στέλνουν στον κόμβο ρίζα M_1 ένα μήνυμα που περιλαμβάνει την ταυτότητά τους (ID_j) και το αποτέλεσμα της συνάρτησης κατακερματισμού (H) της συνένωσης, η οποία περιλαμβάνει την ταυτότητα (ID_j) των κόμβων μελών M_j, το $nonce_j$ που δημιουργείται από το M_j αυξημένο κατά ένα και τα νέα *Τοπικά Κλειδιά (Locals Keys(LK))* $LK_{new} = LK'_j$.

Στο *τέταρτο βήμα*, ο κόμβος ρίζας M_1 ελέγχει τα νέα τοπικά κλειδιά. Το πρωτόκολλο *Περιοδικής Ανανέωσης των Τοπικών Κλειδιών* παρουσιάζεται στο Σχήμα 5.17.

Βήμα 1

$M_j \xrightarrow{ID_j, E_{LK_{old}}(ID_j \| S_j'' \| nonce_j)} M_1$

όπου j είναι όλοι οι κόμβοι στο επίπεδο 1 του δέντρου.

Βήμα 2

M_j, υπολογίζει τα νέα *Τοπικά Κλειδιά*, $LK_{new} = LK'_j = LK_{old} \oplus S''_j$

Βήμα 3

$M_j \xrightarrow{ID_j, H(ID_j \| nonce_j + 1 \| LK'_j)} M_1$

Βήμα 4

M_1 ελέγχει τα νέα *Τοπικά Κλειδιά* $LK_{new} = LK'_j$.

Σχήμα 5. 17 Πρωτόκολλο Περιοδικής Ανανέωσης Τοπικών Κλειδιών

5.2 Μονάδα Τοπικής Απόκρισης

Η *Μονάδα Τοπικής Απόκρισης* είναι υπεύθυνη για την παραγωγή του χάρτη eSOM του δικτύου των άμεσων γειτόνων (ενός-βήματος) ενός κόμβου. Πιο συγκεκριμένα, σε ένα τοπικό δίκτυο κατά περίσταση κάθε κόμβος δημιουργεί τον τοπικό του χάρτη eSOM μέσω της *Μηχανής Ανίχνευσης Εισβολών*. Κάθε κόμβος μεταφέρει τον τοπικό του χάρτη eSOM, μέσω του *Πρωτοκόλλου Διανομής Τοπικού Χάρτη*, σε όλους τους άμεσους γείτονές του.

Εάν υποθέσουμε ότι έχουμε ένα σύνολο από κόμβους του δικτύου κατά περίσταση $M_1, M_2, \ldots, M_n$ και M_i, για $i=2, 3, \ldots, n$, που είναι άμεσοι (ενός βήματος) γείτονες του κόμβου M_1, τότε στο *πρώτο βήμα*, ο κόμβος M_1 στέλνει με ανοιχτή εκπομπή ένα μήνυμα σε όλους τους κόμβους M_i, για $i=2, 3, \ldots, n$. Το εκπεμπόμενο μήνυμα περιλαμβάνει την ταυτότητα (ID_1) του κόμβου μέλους M_1, τον χάρτη του (map_1) και το αποτέλεσμα της συνάρτησης κατακερματισμού (H) ενός μηνύματος που έχει δημιουργηθεί από την ένωση της ταυτότητάς του (ID_1), του χάρτη του (map_1) και μίας τυχαίας ποσότητας $nonce_1$ που παράγεται από το M_1 (δηλ. $H_{LK}(ID_1 \| map_1 \| nonce_1)$). Η συνάρτηση κατακερματισμού χρησιμοποιεί το *Τοπικό Κλειδί* (LK) που παράγεται από τη *Μονάδα Επικοινωνίας*:

$$LK = LK_i = z \oplus S_i \,. \tag{5.21}$$

Στο *δεύτερο βήμα* όλοι οι κόμβοι M_i, για $i=2, 3, \ldots, n$, στέλνουν στον κόμβο-μέλος M_1 ένα μήνυμα το οποίο περιλαμβάνει την ταυτότητά τους (ID_i), τους χάρτες τους (map_i) και το αποτέλεσμα της συνάρτησης κατακερματισμού ενός μηνύματος που παράγεται από τη συνένωση των ταυτοτήτων τους (ID_i), την τυχαία ποσότητα $nonce_1$ που παράγεται από τον κόμβο M_1 αυξημένη κατά ένα ($nonce_1+1$) και τους χάρτες (map_i) (δηλ. $H_{LK}(ID_i \| nonce_1 + 1 \| map_i)$).

Στο *τρίτο βήμα*, ο κόμβος μέλος M_1 μπορεί να υπολογίσει τον καθολικό χάρτη χρησιμοποιώντας τους χάρτες (map_i) που στέλνονται από τα άλλα μέλη του δικτύου άμεσης συνδεσιμότητας (ενός-βήματος) M_i, για $i=2, 3, \ldots, n$.

Στο *τέταρτο βήμα*, ο κόμβος-μέλος M_1 εκπέμπει ένα μήνυμα σε όλους τους κόμβους M_i, για $i=2, 3, \ldots, n$. Το μήνυμα περιλαμβάνει την ταυτότητά του (ID_1), τον *Καθολικό Χάρτη (GlobalMap)* που παράγεται και το αποτέλεσμα της συνάρτησης κατακερματισμού ενός μηνύματος το οποίο περιλαμβάνει τη συνένωση της ταυτότητάς του (ID_1), τον *Καθολικό Χάρτη (GlobalMap)* και την τυχαία ποσότητα $nonce_1$ που παράγεται από τον κόμβο-ρίζα M_1 (δηλ. $H_{LK}(ID_1 || GlobalMap || nonce_1)$). Το *Πρωτόκολλο Διανομής Τοπικού Χάρτη* απεικονίζεται στο Σχήμα 5.18.

Βήμα 1

M_1 *ανοικτή εκπομπή* $ID_1, map_1, H_{LK}(ID_1 \| map_1 \| nonce_1)$ $\rightarrow$ M_i, για $i=2, 3, \ldots, n$

Βήμα 2

M_1 $\leftarrow$ $ID_i, map_i, H_{LK}(ID_i \| nonce_1 + 1 \| map_i)$ M_i, για $i=2, 3, \ldots, n$

Βήμα 3

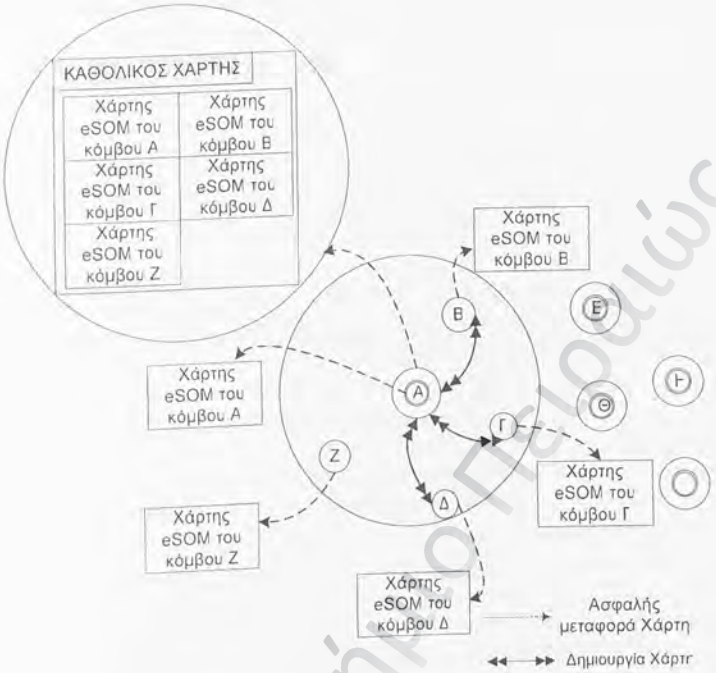
M_1 δημιουργεί τον τοπικό καθολικό χάρτη των άμεσων (ενός βήματος) γειτόνων του.

Βήμα 4

M_1 *ανοικτή εκπομπή* $ID_1, GlobalMap, H_{LK}(ID_1 \| GlobalMap \| nonce_1)$ $\rightarrow$ M_i, για $i=2, 3, \ldots, n$

Σχήμα 5. 18 Πρωτόκολλο Διανομής Τοπικού Χάρτη

Στο Σχήμα 5.19, οι κόμβοι Γ, Β, Δ και Ζ είναι άμεσοι (ενός-βήματος) γείτονες του κόμβου Α. Οι κόμβοι Β, Γ, Δ και Ζ δημιουργούν τον δικό τους χάρτη eSOM και χρησιμοποιούν το πρωτόκολλο *Διανομής Τοπικού Χάρτη* προκειμένου να μεταφέρουν ασφαλώς το χάρτη τους στο κόμβο Α. Ο κόμβος Α επιλέγει τους τοπικούς πιστοποιημένους χάρτες eSOM από τους γείτονές του, δημιουργεί το δικό του χάρτη και στη συνέχεια δημιουργεί τον *Καθολικό Χάρτη* του τοπικού δικτύου. Παρατηρώντας τον *Καθολικό Χάρτη* του τοπικού δικτύου, ο κόμβος Α μπορεί να έχει μία εικόνα για την κατάσταση ασφάλειας των γειτονικών κόμβων. Βασιζόμενος σε αυτή την πληροφορία ο κόμβος Α επιλέγει τον κατάλληλο κόμβο προκειμένου να προωθήσει τα μηνύματά του. Παρατηρώντας τους *Τοπικούς Χάρτες* όλων των γειτονικών κόμβων και θεωρώντας ασφαλείς τους κόμβους που δεν είναι θύματα της επίθεσης, ο κόμβος Α επιλέγει έναν κατάλληλο κόμβο για την προώθηση μηνυμάτων. Στην περίπτωση που όλοι οι κόμβοι είναι θύματα της επίθεσης, ο κόμβος που θεωρείται ότι έχει τη δυνατότητα να προωθεί πληροφορίες είναι αυτός που θα προωθήσει τα μηνύματα.



Σχήμα 5. 19. Λειτουργία της Μονάδας Τοπικής Απόκρισης

5.3 Μονάδα Καθολικής Απόκρισης

Η *Μονάδα Καθολικής Απόκρισης* είναι υπεύθυνη για την ενημέρωση όλων των γειτόνων του κόμβου που έχει δεχτεί επίθεση M_{at}, όχι μόνο αυτών που είναι άμεσοι (ενός-βήματος) γείτονες αλλά όλων των κόμβων στην εμβέλεια επικοινωνίας του (M_i, για $i=1, 2, \ldots, r$ και $i \neq at$), ότι υπάρχει μία πιθανή εισβολή σε αυτό τον κόμβο. Η ενημέρωση όλων των κόμβων στην εμβέλεια επικοινωνίας του κόμβου που δέχεται την επίθεση πραγματοποιείται χρησιμοποιώντας το *Πρωτόκολλο Διανομής Χάρτη - Καθολικής Απόκρισης*.

Εάν υποθέσουμε ότι έχουμε μία ομάδα από κόμβους ενός δικτύου κατά περίσταση, M_i, για $i=1, 2, 3, \ldots, r$, που είναι όλοι οι κόμβοι στην εμβέλεια επικοινωνίας του κόμβου μέλους M_{at} στο πρώτο βήμα του *Πρωτόκολλου Διανομής Χάρτη - Καθολικής Απόκρισης* ο κόμβος-μέλος M_{at} που είναι ένα πιθανό θύμα της επίθεσης, στέλνει με ανοιχτή εκπομπή ένα μήνυμα σε όλους τους κόμβους M_i, για $i=1, 2, 3, \ldots, r$ και $i \neq at$, στην εμβέλεια επικοινωνίας του κόμβου M_{at}. Το εκπεμπόμενο μήνυμα περιλαμβάνει την ταυτότητα του κόμβου που δέχτηκε την επίθεση (ID_{at}) και το αποτέλεσμα της συνάρτησης κατακερματισμού (H) ενός μηνύματος που δημιουργήθηκε από τη συνένωση της ταυτότητάς του (ID_{at}), του

χάρτη του (map_{at}) και της τυχαίας ποσότητας ($nonce_{at}$) που δημιουργήθηκε από τον κόμβο M_{at} (δηλ. $H_{GK}(ID_{at} \| map_{at} \| nonce_{at})$). Η συνάρτηση κατακερματισμού χρησιμοποιεί το *Καθολικό Κλειδί (Global Key (GK))* που δημιουργείται από τη μονάδα επικοινωνίας:

$$GK = K = z \oplus S_{Ch} \,. \tag{5.22}$$

Στο *δεύτερο βήμα*, όλοι οι κόμβοι M_i, για $i=1, 2, 3, \ldots, r$ και $i \neq at$, αποβάλλουν το M_{at} από τους πίνακες δρομολόγησής τους. Το *Πρωτόκολλο Διανομής Χάρτη - Καθολικής Απόκρισης* παρουσιάζεται στο Σχήμα 5.20.

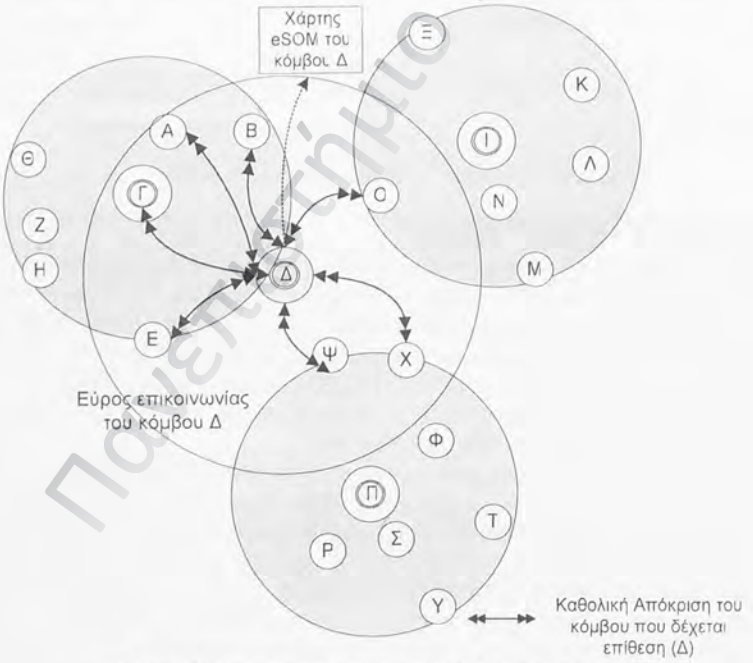
Βήμα 1

M_{at} —*ανοικτή εκπομπή*, $ID_{at}, H_{GK}(ID_{at} \| map_{at} \| nonce_{at})$→ M_i, για $i=1, 2, \ldots, r$ και $i \neq at$

Βήμα 2

Ο κόμβος M_i, για $i=1, 2, \ldots, r$ και $i \neq at$, αποβάλλει το M_{at} από τους πίνακες δρομολόγησης.

Σχήμα 5. 20 Πρωτόκολλο Διανομής Χάρτη – Καθολικής Απόκρισης



Σχήμα 5. 21 Λειτουργία της Μηχανής Καθολικής Απόκρισης

Στο Σχήμα 5.21 απεικονίζεται η λειτουργία της *Μονάδας Καθολικής Απόκρισης*. Σε αυτό το σχήμα απεικονίζονται τρία τοπικά δίκτυα κατά περίσταση. Το πρώτο τοπικό δίκτυο περιλαμβάνει τους άμεσους (ενός-βήματος) γείτονες του κόμβου Γ (περιλαμβάνει τους κόμβους Α, Β, Δ, Ε, Ζ, Η, Θ). Το δεύτερο τοπικό δίκτυο περιλαμβάνει τους άμεσους (ενός-βήματος) γείτονες του κόμβου Ι (περιλαμβάνει τους κόμβους Κ, Λ, Μ, Ν, Ξ, Ο), και το τρίτο τοπικό δίκτυο περιλαμβάνει τους άμεσους (ενός-βήματος) γείτονες του κόμβου Π (περιλαμβάνει τους κόμβους Ρ, Σ, Τ, Υ, Φ, Χ, Ψ). Υποθέτουμε ότι η *Μηχανή Ανίχνευσης Εισβολών* ανίχνευσε τον κόμβο Δ σαν θύμα μίας σοβαρής επίθεσης. Στη συνέχεια ενεργοποιείται η *Μονάδα Καθολικής Απόκρισης* και ο τοπικός χάρτης eSOM του κόμβου Δ διανέμεται χρησιμοποιώντας το πρωτόκολλο καθολικής διανομής προκειμένου να ενημερώσει όλους τους γείτονες στην εμβέλεια επικοινωνίας του κόμβου Δ για την επίθεση έτσι ώστε όλοι οι γείτονες να αποβάλλουν τον κόμβο που δέχεται επίθεση από τους πίνακες δρομολόγησης και να ανανεώσουν τα μονοπάτια που χρησιμοποιούν για τη μεταφορά μηνυμάτων.

Πρέπει να σημειώσουμε εδώ ότι η *Μονάδα Καθολικής Απόκρισης* στην προτεινόμενη προσέγγιση δεν μπορεί να διαβληθεί. Μπορούμε να διαχωρίσουμε δύο περιπτώσεις πιθανής διαβολής της *Μονάδας Καθολικής Απόκρισης* οι οποίες όμως και οι δύο καλύπτονται ώστε να διαφυλαχθεί η ασφάλεια της Μονάδας. Στην πρώτη περίπτωση, ένας κακόβουλος κόμβος προκαλεί την πλαστή ενεργοποίηση της *Μονάδας Καθολικής Απόκρισης* διαδίδοντας τη φήμη ότι είναι θύμα μιας σοβαρής επίθεσης. Σε αυτή την περίπτωση ο κακόβουλος κόμβος δεν θα λάβει προνόμια για τον εαυτό του, αφού με αυτή του την ενέργεια θα προκαλέσει την απομόνωση του και την αποβολή του από τους πίνακες δρομολόγησης των γειτόνων του. Στη δεύτερη περίπτωση, ένας κακόβουλος κόμβος προσπαθεί να διαδώσει ψευδείς φήμες ότι κάποιος άλλος νόμιμος κόμβος είναι θύμα μίας επίθεσης. Αλλά αυτό το γεγονός μπορεί να αποφευχθεί αφού η ακεραιότητα των χαρτών eSOM των κόμβων μελών επιβεβαιώνεται μέσω μηχανισμών ακεραιότητας όπως είναι η προτεινόμενη μέθοδος υδατογράφησης που περιγράφεται αναλυτικά στο επόμενο κεφάλαιο.

6. Αξιολόγηση Απόδοσης

6.1. Περιβάλλον Προσομοίωσης

Προκειμένου να αξιολογήσουμε την αποτελεσματικότητα και τη δυνατότητα εφαρμογής της προσέγγισής μας έχουμε πραγματοποιήσει μία σειρά πειραμάτων σε ένα ασύρματο κινητό δίκτυο κατά περίσταση. Για τα πειράματά μας πραγματοποιήσαμε κάποιες υποθέσεις. Πρώτα από όλα, υποθέτουμε ότι το κινητό δίκτυο υλοποιεί το πρωτόκολλο 802.11 στο επίπεδο MAC [Liu, 2005(7)], με μία χειραψία ανταλλαγής τεσσάρων τρόπων RTS (ReadyToSend)/CTS (ClearToSend)/DATA/ACK. Κανένας άλλος μηχανισμός ασφαλούς και δίκαιας πρόσβασης δεν χρησιμοποιείται. Το δίκτυο δεν έχει προϋπάρχουσα υποδομή

και το πρωτόκολλο δρομολόγησης δικτύων κατά περίσταση που χρησιμοποιήθηκε είναι το AODV.

Η υλοποίηση του προσομοιωτή πραγματοποιήθηκε με τη βιβλιοθήκη ns-2 [NS-2, 2007]. Η προσομοίωση μοντελοποιεί ένα δίκτυο 50 κόμβων που τοποθετούνται τυχαία σε μία περιοχή 1800 x 1000 m^2. Κάθε κόμβος έχει εύρος διάδοσης 250 μέτρα και η χωρητικότητα του δικτύου είναι 2 Mbps. Οι κόμβοι στην προσομοίωση κινούνται σύμφωνα με το μοντέλο "κατεύθυνσης τυχαίας οδού" (random way point). Στην αρχή της προσομοίωσης, κάθε κόμβος περιμένει για ένα διάστημα παύσης, στη συνέχεια τυχαία επιλέγει και κινείται προς αυτή την κατεύθυνση με μία ταχύτητα που λαμβάνει τιμές ομοιόμορφα μεταξύ μηδέν και της μέγιστης ταχύτητας. Όταν φτάσει τον προορισμό του σταματά και πάλι και επαναλαμβάνει την παραπάνω διαδικασία μέχρι το τέλος της προσομοίωσης. Η μέγιστη και ελάχιστη ταχύτητα έχει τεθεί να είναι μεταξύ 0 και 10 m/s, αντίστοιχα, και τα διαστήματα παύσης να είναι 0, 20, 50, 70 και 200 sec. Ένα διάστημα παύσης ίσο με 0 sec αντιστοιχεί στη συνεχή κίνηση του κόμβου και ένα διάστημα παύσης ίσο με 200 sec αντιστοιχεί στο χρόνο που ο κόμβος παραμένει σταθερός. Αξιολογήσαμε την απόδοση του προτεινόμενου σχήματος ανίχνευσης εισβολών για 5, 10, 15 και 20 κακόβουλους κόμβους. Σε κάθε περίπτωση ο αριθμός όλων των κόμβων στο δίκτυο έχει τεθεί ίσος με 50. Η κακόβουλη συμπεριφορά εκδηλώνεται κατά το χρονικό διάστημα μεταξύ των 50 και 200 sec. Οι κόμβοι λειτουργούν φυσιολογικά κατά το χρονικό διάστημα μεταξύ 0 και 50 sec.

Αυτές οι παράμετροι έχουν σαν αποτέλεσμα ένα δίκτυο με μάλλον υψηλή κινητικότητα και υψηλή δραστηριότητα δικτυακής κίνησης. Αναπτύχθηκαν κατά μέσον όρο είκοσι γεννήτορες κίνησης και προσομοίωσαν το ρυθμό δεδομένων TCP (Transport Control Protocol) σε δέκα κόμβους προορισμού. Αυτό το πρότυπο κυκλοφορίας έχει σαν αποτέλεσμα είκοσι συνδέσεις ανάμεσα στους κόμβους πηγής και προορισμού. Τα πακέτα αποστολής έχουν τυχαία μεγέθη και εκθετικούς χρόνους ενδο-αφίξεων. Οι πηγές και οι προορισμοί επιλέγονται τυχαία με σταθερή πιθανότητα. Το μέσο μέγεθος του ωφέλιμου φορτίου δεδομένων ήταν 512 bytes. Κάθε εκτέλεση της προσομοίωσης διήρκεσε 200 sec με διάστημα λήψης δειγμάτων των χαρακτηριστικών 1 sec. Χρησιμοποιήσαμε την Συνάρτηση Κατανεμημένου Συντονισμού (Distributed Coordination Function (DCF)) IEEE 802.11 σαν πρωτόκολλο ελέγχου πρόσβασης στο μέσο. Η κινητικότητα των κόμβων καθορίζεται τυχαία από αρχεία σεναρίου που παράγονται από τον γεννήτορα σεναρίων του ns-2.

6.2. Προσομοιωμένες Επιθέσεις

Οι επιθέσεις στα κινητά δίκτυα κατά περίσταση ακολουθούν τον ίδιο διαχωρισμό, όπως και στα ασύρματα τοπικά δίκτυα (Wireless Local Area Network (WLAN)) και ενσύρματα δίκτυα, χωρίζονται δηλαδή σε *παθητικές* και *ενεργητικές* επιθέσεις. Οι *παθητικές επιθέσεις* βασίζονται στην παρακολούθηση της δικτυακής κυκλοφορίας και την προσπάθεια να κερδίσουν ή/και να

χρησιμοποιήσουν πληροφορίες χωρίς να τις τροποποιήσουν ή να μεταβάλουν τους πόρους του συστήματος. Αυτός ο τύπος επιθέσεων είναι πολύ δύσκολος να ανιχνευθεί από τη φύση του. Από την άλλη πλευρά, οι *ενεργές επιθέσεις* προσπαθούν να τροποποιήσουν πληροφορίες ή/και πόρους του συστήματος και να χρησιμοποιήσουν ασυνείδητα τη λειτουργικότητά τους.

Ένα παράδειγμα ενεργών επιθέσεων είναι η επίθεση *απόρριψης πακέτων*. Σε μία επίθεση απόρριψης πακέτων ένας κακώς συμπεριφερόμενος κόμβος απλά καταστρέφει ή απορρίπτει δεδομένα ή πακέτα δρομολόγησης χωρίς να αναλαμβάνει την ευθύνη. Η επίθεση απόρριψης πακέτων είναι επίσης γνωστή σαν επίθεση περιφρόνησης και έχει τις ακόλουθες παραλλαγές ανάλογα με τη συχνότητα και την επιλεκτικότητα. Εξαρτάται δηλαδή από το αν η απόρριψη των πακέτων είναι τυχαία ή συνεχής όσον αφορά στο χρονικό διάστημα που ο κακόβουλος κόμβος απορρίπτει πακέτα. Στην *επιλεκτική απόρριψη*, τα πακέτα απορρίπτονται σύμφωνα με κάποια συγκεκριμένα κριτήρια. Η επιλεκτική απόρριψη είναι επίσης γνωστή σαν επίθεση *"γκρίζας οπής"*.

Στα πειράματά μας έχουμε προσομοιώσει μία σταθερή επίθεση *επιλεκτικής απόρριψης* όπου ο επιτιθέμενος απλά απορρίπτει όλα τα πακέτα δεδομένων ενώ λειτουργεί νόμιμα όσον αφορά στη δρομολόγηση και στα πακέτα του επιπέδου MAC. Αυτός ο τύπος επίθεσης είναι ιδιαίτερα δύσκολο να ανιχνευθεί εάν λάβουμε υπόψη μας ότι η απόρριψη πακέτων μπορεί να οφείλεται σε κακόβουλη συμπεριφορά ή στην κινητικότητα. Επιπρόσθετα στο πρόβλημα ο κακόβουλος κόμβος μπορεί να παρουσιάσει κακόβουλη συμπεριφορά όταν είναι περισσότερο ωφέλιμο για αυτόν και όχι από την αρχή της επίθεσης.

6.3 Πεδία

Τα διανύσματα πεδίων που χρησιμοποιούνται στην ταξινόμησή μας από το eSOM είναι ένα κρίσιμο βήμα στη διαμόρφωση της προτεινόμενης προσέγγισης ανίχνευσης εισβολών. Τα χαρακτηριστικά της δικτυακής κυκλοφορίας θα πρέπει να είναι σε κατάλληλη μορφή προκειμένου να μπορούν εύκολα να επεξεργαστούν από το eSOM και αντιπροσωπευτικά προκειμένου να αυξήσουν την αντίθεση ανάμεσα στη "φυσιολογική" και τη "μη-φυσιολογική" δραστηριότητα. Επιπλέον, τα πεδία θα πρέπει να μας παρέχουν υψηλό κέρδος πληροφοριών έτσι ώστε να μπορούμε να διακρίνουμε χωρίς αμφιβολία αν ένα γεγονός είναι "φυσιολογικό" ή "μη-φυσιολογικό".

Τα στατιστικά πεδία που χρησιμοποιήσαμε είχαν εισαχθεί από τους Liu και άλλους [Liu, 2005] στην προτεινόμενη προσέγγισή τους για την πραγματοποίηση ανίχνευσης εισβολών στο επίπεδο MAC. Αυτά τα χαρακτηριστικά είναι τα ακόλουθα:

Διάνυσμα ανάθεσης του δικτύου (Network allocation vector (NAV)): είναι ένα ειδικό χαρακτηριστικό ενός κόμβου το οποίο απεικονίζει το χρονικό διάστημα κατά το οποίο ο κόμβος θα απασχολεί το μέσο για την αποστολή των μηνυμάτων του.

Ρυθμός μετάδοσης κυκλοφορίας: υποδηλώνει το ρυθμό των μεταφερόμενων πακέτων.
Ρυθμός λήψης κυκλοφορίας: υποδηλώνει το ρυθμό των λαμβανόμενων πακέτων.
Ρυθμός επανα-μετάδοσης των πακέτων RTS (ΕτοιμοΝαΣτείλει (ReadyTo Send)): υποδηλώνει το ρυθμό των πακέτων ReadyToSend (RTS) που επαναμεταφέρονται από τον κόμβο που παρακολουθείται. Μία υψηλή τιμή αυτού του χαρακτηριστικού υποδηλώνει πιθανή επίθεση απόρριψης.
Ρυθμός επανα-μετάδοσης των πακέτων δεδομένων (DATA): υποδηλώνει τον ρυθμό των πακέτων δεδομένων που επανα-μεταδίδονται από τον κόμβο που παρακολουθείται. Μία υψηλή τιμή αυτού του χαρακτηριστικού υποδηλώνει μία πιθανή επίθεση πακέτων απόρριψης.
Αριθμός των ενεργών γειτονικών κόμβων: αναπαριστά τον αριθμό των γειτονικών κόμβων που πραγματοποιούν μεταδόσεις δεδομένων.
Αριθμός των κόμβων προώθησης: αναπαριστά τον αριθμό των γειτονικών κόμβων που επικοινωνούν άμεσα με τον κόμβο που παρακολουθείται.

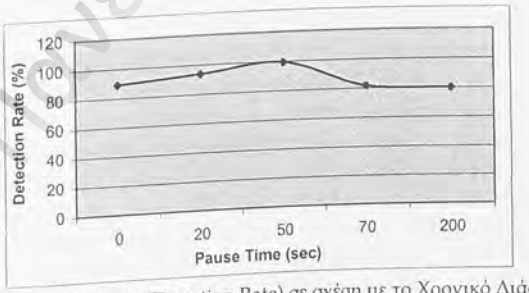
Προκειμένου να αποφύγουμε το ενδεχόμενο μεγάλης επιρροής των χαρακτηριστικών κάποιων διανυσμάτων εισόδου είναι απαραίτητο να κανονικοποιήσουμε τα δεδομένα εισόδου. Πολλές μέθοδοι έχουν χρησιμοποιηθεί για την κανονικοποίηση δεδομένων. Κανονικοποιήσαμε τα δεδομένα με μέσο μηδέν και διακύμανση ένα, μία τεχνική που παράγει πολύ καλά αποτελέσματα στις περισσότερες περιπτώσεις όπως αναφέρεται στη βιβλιογραφία [Duda, 2001]. Για την αξιολόγηση χρησιμοποιήσαμε το εργαλείο Databionics ESOM ([Ultsch, 2005],[Databionic, 2007]).

6.4. Αποτελέσματα Προσομοίωσης

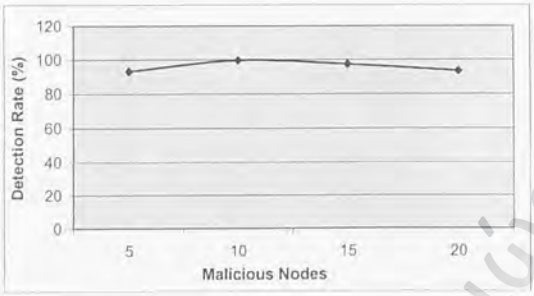
Τα αποτελέσματα της αξιολόγησης που παρουσιάζονται αποδεικνύουν ότι μπορούμε να επιτύχουμε μία διαφοροποίηση ανάμεσα σε "φυσιολογικές" και "μη-φυσιολογικές" συμπεριφορές όσον αφορά στις επιθέσεις *απόρριψης πακέτων*. Προκειμένου να πραγματοποιήσουμε ομαδοποίηση με τα eSOM ακολουθήσαμε την εξής διαδικασία. Τα καλύτερα ταίρια (best matches) των συνόλων δεδομένων εκπαίδευσης και επομένως τα αντίστοιχα σύνολα δεδομένων ομαδοποιούνται χειρωνακτικά σε ομάδες αναπαριστώντας τη φυσιολογική συμπεριφορά και τη συμπεριφορά επίθεσης. Επομένως, αναγνωρίζουμε τις περιοχές του χάρτη που αναπαριστούν μία ομάδα και μπορούν να χρησιμοποιηθούν για την ταξινόμηση νέων συνόλων δεδομένων. Ο χάρτης eSOM ενός συνόλου εκπαίδευσης αναπαριστάται στο Σχήμα 5.22. Όπως είναι πολύ ευδιάκριτο το σύνολο δεδομένων εκπαίδευσης μπορεί να διαχωριστεί σε δύο κλάσεις, την κλάση των δεδομένων "φυσιολογικής" δικτυακής κίνησης (σκούρο χρώμα) και την κλάση των δεδομένων απόρριψης πακέτων (ανοιχτό χρώμα). Προκειμένου να είμαστε σίγουροι ότι η προσέγγισή μας θα παράγει πάντα αποτελεσματικά και ακριβή αποτελέσματα πρέπει να ανανεώνουμε το εκπαιδευμένο χάρτη eSOM σύμφωνα με τις νέες συνθήκες όσον αφορά στην κινητικότητα.

Σχήμα 5. 22 Χάρτης eSOM ενός Κόμβου ενός Δικτύου κατά Περίσταση

Το Σχήμα 5.23 παρουσιάζει το μέσο *ρυθμό ανίχνευσης (Detection Rate (DR))* όλων των κόμβων πηγής που αναπαριστούν τη δραστηριότητα κυκλοφορίας και αναγνωρίζονται σαν "φυσιολογική" συμπεριφορά ή επίθεση από το eSOM όσον αφορά στα χρησιμοποιούμενα διαστήματα παύσης. Ο ρυθμός ανίχνευσης φαίνεται πως δεν επηρεάζεται από την κινητικότητα και σε όλες τις περιπτώσεις είναι πάνω από 80%. Για μεγάλα διαστήματα παύσης ο ρυθμός μειώνεται ελαφρά λόγω της κυκλοφορίας TCP και της μείωσης της κινητικότητας. Πράγματι, ένας πράκτορας TCP σταματά την αποστολή πακέτων όταν δεν λαμβάνει επιβεβαίωση. Ακόμα και αφού το πρωτόκολλο AODV ανακαλύψει ένα νέο μονοπάτι σε αυτό τον προορισμό, ο πράκτορας συνεχίζει να στέλνει πακέτα δεδομένων μέσω του κακόβουλου κόμβου, καθώς αυτός ανταποκρίνεται φυσιολογικά στα πακέτα ελέγχου. Καθώς το δίκτυο παρουσιάζει μία μάλλον χαμηλή κινητικότητα, η κυκλοφορία του δικτύου απορρίπτεται πάντα από τον κακόβουλο κόμβο και σύντομα θα σταματήσει από τον πράκτορα TCP, γεγονός που έχει σαν αποτέλεσμα να μειώνονται τα δεδομένα παρακολούθησης που εισάγονται στο eSOM.



Σχήμα 5. 23 Ρυθμός ανίχνευσης (Detection Rate) σε σχέση με το Χρονικό Διάστημα Παύσης (Pause Time)



Σχήμα 5. 24 Ρυθμός Ανίχνευσης (Detection Rate) σε σχέση με τον Αριθμό των Κακόβουλων Κόμβων

Ο ρυθμός ανίχνευσης σαν συνάρτηση του αριθμού των κακόβουλων κόμβων αναπαρίσταται στο Σχήμα 5.24. Ο ρυθμός είναι υψηλός, όπως και στο προηγούμενο σχήμα, πάντα πάνω από 80%. Όταν λίγοι κακόβουλοι κόμβοι υπάρχουν στο δίκτυο, οι συνδέσεις που επηρεάζονται από αυτούς είναι επίσης λίγες καθώς οι κόμβοι πηγής κινούνται τυχαία στο δίκτυο. Αυτό έχει σαν αποτέλεσμα σε διπλές γραμμές στα δεδομένα παρακολούθησης που εισάγονται στο eSOM με αποτέλεσμα τη μείωση του ποσοστού ανίχνευσης. Όταν ο αριθμός των κακόβουλων κόμβων είναι υψηλός σε σύγκριση με τον αριθμό των κόμβων πηγής, οι συνδέσεις TCP που παράγονται αυτόματα από τον προσομοιωτή ns είναι λίγες, κάτι το οποίο οδηγεί σε πολλαπλές διπλές γραμμές στα δεδομένα παρακολούθησης που εισάγονται στο eSOM, με αποτέλεσμα τη μείωση του ρυθμού ανίχνευσης. Η κυκλοφορία TCP χρησιμοποιείται σαν πιο ρεαλιστική.

Οι Πίνακες 5.2 και 5.3 παρουσιάζουν το μέσο ρυθμό λανθασμένων συναγερμών σαν συνάρτηση των διαστημάτων παύσης που χρησιμοποιούνται και τον αριθμό των κακόβουλων κόμβων, αντίστοιχα. Όταν ένας κόμβος πηγής παράγει κυκλοφορία σε διαφορετικούς προορισμούς και μία από αυτές τις συνδέσεις επηρεάζεται από κακόβουλους κόμβους, τότε το eSOM δυσκολεύεται να διαχωρίσει τη "φυσιολογική" από τη "μη-φυσιολογική" κυκλοφορία. Εάν αυτό συνδυαστεί με πολλαπλές διπλές γραμμές στα δεδομένα παρακολούθησης λόγω κινητικότητας, ο υψηλός αριθμός κακόβουλων κόμβων παράγει υψηλό ρυθμό λανθασμένων συναγερμών. Οι υψηλοί λανθασμένοι συναγερμοί προκαλούνται κυρίως λόγω της δυσκολίας που αντιμετωπίζει ο ταξινομητής (eSOM) προκειμένου να διαχωρίσει την αλλαγή στη συμπεριφορά ενός κόμβου (όπως αναπαρίσταται από τα επιλεγμένα πεδία) που προκαλείται είτε λόγω κίνησης είτε λόγω κακόβουλης συμπεριφοράς.

Πίνακας 5. 2 Λανθασμένοι Συναγερμοί σε Σχέση με το Χρονικό Διάστημα Παύσης

Χρονικό Διάστημα παύσης (sec)	Λανθασμένοι Συναγερμοί (%)
0	21
20	20
50	22
70	20

Πίνακας 5. 3 Λανθασμένοι Συναγερμοί σε Σχέση με τον Αριθμό των Κακόβουλων Κόμβων

Κακόβουλοι Κόμβοι	Λανθασμένοι Συναγερμοί (%)
5	26
10	22
15	17
20	21

6.4.1 Σύγκριση Αποτελεσμάτων

Δύο αντιπροσωπευτικές εργασίες στην περιοχή της ανίχνευσης ανωμαλιών είναι των Deng και άλλοι [Deng, 2003] και Liu και άλλοι [Liu, 2005]. Οι Deng και άλλοι [Deng, 2003] προτείνουν την ανίχνευση ανωμαλιών στα κινητά δίκτυα κατά περίσταση (Mobile Ad hoc Networks (MANET)) χρησιμοποιώντας SVM (Support Vector Machines) με μία εντελώς κατανεμημένη αρχιτεκτονική. Το ποσοστό λανθασμένων συναγερμών κυμαίνονται από 3.5±5.8% έως 20.85±8.03% για την επίθεση "μαύρης τρύπας" (Black hole) και την επίθεση Συχνών Πλαστών Αιτήσεων Δρομολόγησης (Frequent False Routing Requesting (FFRR)).

Επιπλέον, οι Liu και άλλοι [Liu, 2005] στην προσέγγισή τους για την επίθεση απόρριψης πακέτων χρησιμοποιούν την ανάλυση διασταύρωσης πεδίων (cross feature analysis) και αν και το ποσοστό των λανθασμένων συναγερμών είναι χαμηλό 0.29%, η ανίχνευση εισβολών είναι επίσης χαμηλή 72%. Καθώς η επίθεση απόρριψης πακέτων είναι δύσκολο να αντιμετωπιστεί, το χαμηλό ποσοστό λανθασμένων συναγερμών συνοδεύεται από χαμηλό ποσοστό ανίχνευσης.

Η μηχανή ανίχνευσης εισβολών που προτείνουμε παρουσιάζει ένα αρκετά μεγάλο ποσοστό ανίχνευσης για τη συγκεκριμένη επίθεση που μελετήσαμε. Το βασικό πλεονέκτημα της προτεινόμενης μεθόδου είναι η οπτική αναπαράσταση της "φυσιολογικής" και "μη-φυσιολογικής" κατάστασης σε ένα κινητό δίκτυο κατά περίσταση. Επιπλέον, η προτεινόμενη μηχανή ανίχνευσης εισβολών έχει

την ικανότητα άμεσης απόκρισης στην περίπτωση μίας πιθανής εισβολής επιλέγοντας τον πιο ασφαλή κόμβο όπως υποδηλώνεται από το χάρτη eSOM για την προώθηση μηνυμάτων. Προκειμένου να επιβεβαιωθεί η αξιοπιστία και να αποφευχθούν πιθανές τροποποιήσεις του χαρτών eSOM πρέπει να χρησιμοποιηθεί το προτεινόμενο πρωτόκολλο συμφωνίας κλειδιού κατά τις συναλλαγές των κόμβων.

7. Επίλογος

Η περιοχή των δικτύων κατά περίσταση έχει κερδίσει μεγάλη προσοχή από τους ερευνητές τα πρόσφατα χρόνια, καθώς η εξέλιξη των ασύρματων δικτύων και το υλικό των κινητών συσκευών έχουν κάνει δυνατή την εξυπηρέτηση πολλών εφαρμογών από αυτό τον τύπο δικτύων. Η ασφάλεια σε αυτά τα περιβάλλοντα είναι ένα κρίσιμο θέμα. Η ανίχνευση εισβολών μπορεί να συμπληρώσει την παρεμπόδιση εισβολών. Σε αυτό το κεφάλαιο, παρουσιάσαμε μία μηχανή *Ανίχνευσης Εισβολών* που είναι τμήμα ενός τοπικού πράκτορα IDS που υπάρχει σε κάθε κόμβο του δικτύου κατά περίσταση. Η συνεργασία όλων των τοπικών πρακτόρων IDS αποτελεί το σύστημα *Ανίχνευσης Εισβολών* για το δίκτυο κατά περίσταση. Η προτεινόμενη μηχανή ανίχνευσης εισβολών βασίζεται στα eSOM, μία ειδική και αποτελεσματική κλάση νευρωνικών δικτύων που παράγει σαν έξοδο ένα χάρτη και παρέχει οπτική αναπαράσταση της ταξινόμησης που πραγματοποιείται. Εξετάσαμε την απόδοση των eSOM στην ταξινόμηση "φυσιολογικής" και "μη-φυσιολογικής" συμπεριφοράς στα δίκτυα κατά περίσταση και εκμεταλλευτήκαμε το πλεονέκτημα οπτικοποίησης της δικτυακής κυκλοφορίας. Χρησιμοποιώντας το eSOM, κάθε κόμβος του δικτύου κατά περίσταση δημιουργεί τον τοπικό του χάρτη eSOM, καθώς και τον καθολικό χάρτη του τοπικού δικτύου κατά περίσταση. Ο καθολικός και οι τοπικοί χάρτες eSOM μας δίνουν το σημαντικό πλεονέκτημα να μπορούμε να έχουμε οπτική αναπαράσταση της κατάστασης ασφαλείας κάθε κόμβου κατά περίσταση, καθώς και του τοπικού δικτύου κατά περίσταση. Επομένως, κάθε κόμβος έχει τη δυνατότητα να επιλέξει ένα ασφαλές μονοπάτι δρομολόγησης για την προώθηση πακέτων αποφεύγοντας τους κατειλημμένους γείτονες.

Επιπλέον, προτείναμε μία μηχανή *Απόκρισης σε Εισβολές* που αποτελείται από τρεις μονάδες: τη μονάδα *Επικοινωνίας*, τη μονάδα *Τοπικής Απόκρισης* και τη μονάδα *Καθολικής Απόκρισης*. Η *Απόκριση στις Εισβολές* θα πρέπει να είναι όσο το δυνατόν πιο γρήγορη και αξιόπιστη στην μεταφορά μηνυμάτων ενημέρωσης. Για το λόγο αυτό, προτείνουμε ένα *πιστοποιημένο Πρωτόκολλο Συμφωνίας Κλειδιού*. Η μονάδα *Τοπικής Απόκρισης* δημιουργεί έναν καθολικό χάρτη μέσω του πιστοποιημένου πρωτοκόλλου, για τους άμεσους (ενός-βήματος) γείτονες κάθε κόμβου του δικτύου κατά περίσταση. Η μονάδα *Καθολικής Απόκρισης* ενημερώνει κάθε κόμβο στην εμβέλεια επικοινωνίας του επιτιθέμενου κόμβου για το στιγμιότυπο της επίθεσης και ξεκινά την απομάκρυνση του κόμβου που δέχτηκε την επίθεση από τους πίνακες δρομολόγησης.

Ένα άλλο θέμα που πρέπει να εξετάσουμε προκειμένου να διασφαλίσουμε την ασφαλή λειτουργία του συστήματος Ανίχνευσης και Απόκρισης σε Εισβολές είναι η προστασία των χαρτών eSOM από πιθανές τροποποιήσεις και παραβιάσεις. Προκειμένου λοιπόν να επιτύχουμε την αξιοπιστία των χαρτών eSOM προτείνουμε μία καινοτόμο μέθοδο υδατογραφήσης, η οποία περιγράφεται αναλυτικά στο επόμενο κεφάλαιο.

Βιβλιογραφία

[Anjum, 2003] F. Anjum, D. Subhadrabandhu, S. Sarkar, *"Signature-based Intrusion Detection for Wireless Ad-Hose Networks"*, In Proceedings of Vehicular Technology Conference (VTC'03), Wireless Security Symposium, October (2003), Orlando, Florida.

[Barua, 2003] R. Barua, R. Dutta, P. Sarkar, *"Extending Joux Protocol to Multi Party Key Agreement"*, In Proceedings of Indocrypt 2003, LNCS 2904, pp. 205-217, Springer-Verlag, 2003.

[Becker, 1998] K. Becker and U.Wille, *"Communication Complexity of Group Key Distribution"*, In Proceedings of 5th ACM Conference on Computer and Communications Security, ACM Press, 1998, pp. 1–6.

[Burmester, 1995] M. V. D. Burmester and Y. Desmedt, *"A Secure and Efficient Conference Key Distribution System"*, In A. D. Santis, editor, Advances in Cryptology -- EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 275—286.

[Chen, 2005] T. M. Chen and V. Venkataramanan, *"Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks"*, IEEE Internet Computing, Vol. 9, No. 6, November (2005), pp. 35-41.

[Databionic, 2007] *Databionic eSOM Tools*, Available from <http://databionic-esom.sourceforge.net/devel.html>

[Deng, 2003] H. Deng, Q. Zeng, and D. P. Agrawal, *"SVM-based Intrusion Detection System for Wireless Ad Hoc Networks"*, In Proceedings of the IEEE Vehicular Technology Conference (VTC'03), October (2003), Orlando, Florida, USA, pp. 2147-2151.

[Duda, 2001] R.O. Duda, P.E. Hart, D.G. Stork, *"Pattern Classification"*, A Wiley-Interscience Publication, John Wiley & Sons, Inc. 2001, Second Edition.

[Dutta, 2004] R. Dutta, R. Barua and P. Sarkar, *"Provably Secure Authenticated Tree Based Group Key Agreement"*, In Proceedings of ICICS 2004, LNCS 3269, pp. 92-104, Springer-Verlag, 2004.

[Dutta, 2005] R. Dutta and R. Barua, *"Dynamic Group Key Agreement in Tree-based Setting"*, In Proceedings of ACISP 2005, LNCS 3574, pp. 101-112, Springer-Verlag, 2005.

[Haykin, 1999] S. Haykin, *"Neural Networks: A Comprehensive Foundation"*, Prentice-Hall, New Jersey, USA, 2nd edition (1999).

[Huang, 2003a] Y. Huang, and W. Lee, *"A Cooperative Intrusion Detection System for Ad Hoc Networks"*, in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03), October (2003), Fairfax, VA, USA, pp. 135-147.

[Huang, 2003b] Y. Huang, W. Fan, W. Lee and P. Yu, *"Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies"*, In Proceedings of the 23rd International Conference on Distributed Computing Systems, May (2003), Rhode Island, USA, pp. 478.

[Hwang, 2003] R. J. Hwang and R. C. Chang, *"Key Agreement in Ad Hoc Networks"*, Lecture Notes in Computer Science Volume 2745/2003 Parallel and Distributed Processing and Applications, pp.382-390.

[Kachirski, 2002] O. Kachirski, and R. Guha, *"Intrusion Detection Using Mobile Agents in Wireless Ad hoc Networks"*, in Proceedings of the IEEE Workshop on Knowledge Media Networking, July (2002), Kyoto Japan, pp.153-158.

[Kim, 2004] Y. Kim, A. Perrig, and G. Tsudik, *"Tree-based Group Key Agreement"*, ACM Transactions on Information and System Security, Vol.7, No.1, February (2004), pp.60–96.

[Komninos, 2007] N. Komninos, D. Vergados, and C. Douligeris, *"Detecting Unauthorized and Compromised Nodes in Mobile Ad-Hoc Networks"*, Journal in Ad Hoc Networks, Elsevier, Volume 5, Issue 3, April 2007, pp. 289-298.

[Liu, 2005] Y. Liu, Y. Li and H. Man, *"MAC Layer Anomaly Detection in Ad Hoc Networks"*, In Proceedings of 6th IEEE Information Assurance Workshop, June (2005), West Point, New York, USA.

[Lo, 2005] C. Lo, C. Huang and Y. Huang, *"A Key Agreement Protocol Using Mutual Authentication for Ad-Hoc Networks"*, In Proceedings of International Conference on Services Systems and Services Management 2005 (ICSSSM'05), Vol. 2, June (2005), pp. 814-818.

[Makki, 2004] S. Makki, N. Pissinou, H. Huang, *"The Security Issues in the Ad-Hoc on Demand Distance Vector Routing Protocol (AODV)"*, In Proceedings of the 2004 International Conference on Security and Management (SAM'04), pp. 427-432.

[Menezes, 1996] A.J Menezes, S. A. Vanstone, P.C. Van Oorschot, *"Handbook of Applied Cryptography"*, 1st Edition, 1996, CRC Press, Inc., Florida, USA.

[Nalla, 2002] D. Nalla and K. C. Reddy, *"Identity Based Authenticated Group Key Agreement Protocol"*, In Proceedings of Indocrypt 2002, LNCS 2551, pp. 215-233, Springer-Verlag, 2002.

[NS-2, 2007] *The Network Simulator*, Last Check August 2007, Available from < http://www.isi.edu/nsnam/ns/>.

[Patwardhan, 2005] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga, *"Secure Routing and Intrusion Detection in Ad Hoc Networks"*, Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 8-12, 2005.

[Perkins, 2003] C.E. Perkins, E.M. Belding-Royer, and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing", July 2003, IETF RFC 3561.

[Steiner, 1998] M. Steiner, G. Tsudik and M. Waidner, *"CLIQUES: a new approach to group key agreement"*, In Proceeding of the 18th international conference on distributed computing systems (ICDS'98), May (1998), pp.380-387.

[Tseng, 2003] C.Y. Tseng, P. Balasubramanyan, R. Limprasittiporn, J. Rowe, and K. Levitt, *"A Specification-based Intrusion Detection System for AODV"*, In Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'03), October (2003), Fairfax, Virginia, USA, pp. 125-134.

[Ultsch, 1999] A. Ultsch, *"Data Mining and Knowledge Discovery with Emergent SOFMs for Multivariate Time Series"*, In Kohonen Maps, Elsevier Science,(1999) pp. 33-46.

[Ultsch, 2003] A. Ultsch, *"Maps for Visualization of High-dimensional Data Spaces"*, In Proceedings of Workshop on Self-Organizing Maps (WSOM '03), September (2003), Kyushu, Japan, pp. 225-230.

[Ultsch, 2005] A. Ultsch, F. Moerchen *"eSOM-Maps: Tools for Clustering, Visualization, and Classification with emergent SOM"*, Tech. Report Dept. of Mathematics and Computer Science, University of Marburg, Germany, No. 46 (2005).

[Zhang, 2003] Y. Zhang, W. Lee, Y. Huang, *"Intrusion Detection Techniques for Mobile Wireless Networks"*, Wireless Networks Vol. 9, No. 5, (September 2003), pp. 545-556.

Κεφαλαίο 6ο

Προστασία των Χαρτών eSOM με Χρήση Τεχνικών Υδατογράφησης

1. Εισαγωγή

Στο προηγούμενο κεφάλαιο προτείναμε μία προσέγγιση ανίχνευσης και απόκρισης σε εισβολές στα ασύρματα δίκτυα κατά περίσταση. Προκειμένου όμως, η προτεινόμενη προσέγγιση να είναι αποτελεσματική είναι απαραίτητο *Τοπικοί Χάρτες* eSOM που δημιουργούνται σε κάθε κόμβο του δικτύου, αλλά και ο *Καθολικός Χάρτης* τοπικού δικτύου, να προστατεύονται από πιθανές τροποποιήσεις ή παραβιάσεις. Για το σκοπό αυτό προτείνουμε μία καινοτόμα τεχνική υδατογράφησης η οποία μας βοηθά να διασφαλίσουμε την ακεραιότητα των χαρτών eSOM και να ανιχνεύσουμε πιθανές τροποποιήσεις σε αυτούς. Η προτεινόμενη τεχνική υδατογράφησης προέρχεται από τον αποτελεσματικό συνδυασμό των μεθόδων ενσωμάτωσης Lattice και Block-Wise ([[Seitz, 2005], [Zhang, 2006], [Furon, 2005]).

Η υδατογράφηση έχει χρησιμοποιηθεί εκτεταμένα στην ερευνητική περιοχή της ασφάλειας πληροφοριών. Πιο συγκεκριμένα, στην περιοχή της ανίχνευσης εισβολών οι Wang και άλλοι [Wang, 2001] πρότειναν ένα πλαίσιο εργασίας για

την ανίχνευση εισβολών σε ενσύρματα δίκτυα όπου ενεργοποιείται η υδατογράφηση και η ιχνηλάτηση των πακέτων στην διεύθυνση IP πηγής του επιτιθέμενου, μόνο εάν το υποσύστημα ανίχνευσης εισβολών διαπιστώσει ότι υπάρχει μία επίθεση σε εξέλιξη.

Οι Páez και άλλοι [Páez, 2006] πρότειναν ένα σχήμα ασφάλειας για Συστήματα Ανίχνευσης Εισβολών βασιζόμενα σε Περιοδεύοντες Συνεργάσιμους Πράκτορες (Cooperative Itinerant Agents (CIA)). Πρότειναν ένα νέο σχήμα ασφάλειας προκειμένου να επιβεβαιώσουν την ακεραιότητα των οντοτήτων ενός Συστήματος Ανίχνευσης Εισβολών που βασίζεται σε κινητούς συνεργάσιμους πράκτορες χρησιμοποιώντας τεχνικές υδατογράφησης λογισμικού. Πιο συγκεκριμένα, πρότειναν τη χρήση λογισμικού δακτυλικών αποτυπωμάτων προκειμένου να διακρίνουν πράκτορες του ίδιου τύπου και να ανιχνεύσουν πιο πολύπλοκες επιθέσεις.

Παρά τα σημαντικά πλεονεκτήματα που παρουσιάζουν οι τεχνικές υδατογράφησης δεν έχει προταθεί καμία εφαρμογή τεχνικών υδατογράφησης στην περιοχή ασφάλειας των ασύρματων δικτύων κατά περίσταση. Λαμβάνοντας υπόψη μας το γεγονός ότι οι χάρτες εικόνας εκτίθενται στην πιθανότητα παραποίησης, τεχνικές υδατογράφησης μπορούν να εφαρμοστούν στους χάρτες eSOM ([Ultsch, 1999], [Ultsch, 2002], [Ultsch, 2005]) προκειμένου να επιβεβαιώσουμε την αυθεντικότητά τους και να ανιχνεύσουμε πιθανές τροποποιήσεις των χαρτών. Χρησιμοποιώντας τις τεχνικές υδατογράφησης μπορούν να προσδιοριστούν τα τμήματα εικόνων που είναι ύποπτα για παράνομες τροποποιήσεις και μετατροπές. Στο κεφάλαιο αυτό περιγράφεται αναλυτικά η προτεινόμενη μέθοδος υδατογράφησης και ο τρόπος εφαρμογής της στη διασφάλιση των ασύρματων δικτύων κατά περίσταση.

Ακολουθώντας αυτή την εισαγωγή το κεφάλαιο αυτό οργανώνεται ως εξής. Στην ενότητα 2 περιγράφεται η εφαρμογή της μεθόδου υδατογράφησης στην προτεινόμενη προσέγγισης ανίχνευσης και απόκρισης σε εισβολές με χρήση των eSOM. Στην ενότητα 3 περιγράφεται η προτεινόμενη μέθοδος υδατογράφησης. Συγκεκριμένα, περιγράφονται οι μέθοδοι ενσωμάτωσης Lattice και Block-Wise και ο συνδυασμός τους προκειμένου να προκύψει η προτεινόμενη μέθοδος υδατογράφησης. Η ενότητα 4 παρουσιάζει τα αποτελέσματα αξιολόγησης της προτεινόμενης μεθόδου υδατογράφησης και η ενότητα 5 ολοκληρώνει το κεφάλαιο.

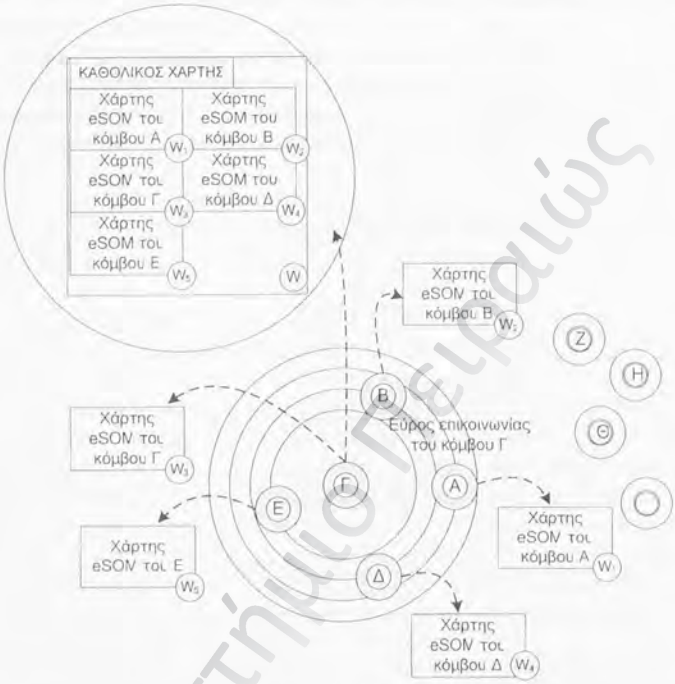
2. Η Προσέγγιση Υδατογράφησης για την Προστασία των Χαρτών eSOM

Οι τεχνικές υδατογράφησης προσπαθούν να προστατέψουν τα πνευματικά δικαιώματα οποιουδήποτε ψηφιακού μέσου ενσωματώνοντας ένα μοναδικό μήνυμα στις πρωτότυπες πληροφορίες [Seitz, 2005]. Οι μέθοδοι ενσωμάτωσης περιλαμβάνουν τη χρήση ενός αριθμού διαφορετικών αλγορίθμων πιστοποίησης, κρυπτογράφησης και συνάρτησης κατακερματισμού προκειμένου να προστατευθεί η ακεραιότητα και δημιουργία αντιγράφων του συγκεκριμένου μηνύματος. Στην διατριβή αυτή, χρησιμοποιούμε τεχνικές υδατογράφησης για τους χάρτες eSOM, που είναι στη μορφή μη συμπιεσμένων εικόνων (Bmp).

Σχήμα 6. 1 Διαδικασία Επιλογής του Κόμβου Προώθησης Μηνυμάτων

Πιο συγκεκριμένα, προκειμένου να διαφυλάξουμε την αξιοπιστία των χαρτών eSOM που παράγονται από την προτεινόμενη μηχανή *Ανίχνευσης Εισβολών* στα ασύρματα δίκτυα κατά περίσταση (Κεφάλαιο 5, Παράγραφος 4) προτείνουμε μία κατωτόμα και αποτελεσματική μέθοδο υδατογράφησης. Η διαδικασία που ακολουθείται απεικονίζεται στο Σχήμα 6.1. Μετά από την εφαρμογή του αλγόριθμου ταξινόμησης eSOM και μετά από τη δημιουργία των *Τοπικών Χαρτών* eSOM από κάθε κόμβο του δικτύου κατά περίσταση εφαρμόζεται η τεχνική υδατογράφησης στους χάρτες eSOM. Στη συνέχεια, κάθε κόμβος συλλέγει τους υδατογραφημένους χάρτες eSOM των άμεσων γειτόνων του και δημιουργεί τον *Καθολικό Χάρτη* του τοπικού δικτύου των άμεσων (ενός-βήματος) γειτόνων του. Ο *Καθολικός Χάρτης* του τοπικού δικτύου προέρχεται από τη συνένωση των υδατογραφημένων *Τοπικών Χαρτών* των άμεσων (ενός-βήματος) γειτόνων κάθε κόμβου του δικτύου. Στον *Καθολικό Χάρτη* εφαρμόζεται και πάλι η τεχνική υδατογράφησης προκειμένου να αποφευχθεί κάθε πιθανή τροποποίησή του και να διασφαλιστεί η ακεραιότητά του. Κατά αυτόν τον τρόπο κάθε κόμβος έχει τη δυνατότητα να γνωρίζει την κατάσταση ασφαλείας του τοπικού δικτύου με σιγουριά αφού η αξιοπιστία των χαρτών eSOM διαφυλάσσεται μέσω της

υδατογραφήσης. Επομένως επιλέγει τον κατάλληλο κόμβο για να προωθηθούν τα μηνύματά του.



Σχήμα 6. 2 Υδατογραφημένοι Χάρτες eSOM ενός Δικτύου κατά Περίσταση

Ένα παράδειγμα της προτεινόμενης προσέγγισης εφαρμογής της υδατογράφησης στην ανίχνευση και απόκριση εισβολών στα ασύρματα δίκτυα κατά περίσταση απεικονίζεται στο Σχήμα 6.2. Οι κόμβοι Α, Β, Γ, Δ και Ε είναι στο εύρος επικοινωνίας του κόμβου Γ. Κάθε κόμβος Α, Β, Γ, Δ, Ε δημιουργεί το δικό του *Τοπικό Χάρτη* eSOM και εφαρμόζει υδατογράφηση σε αυτό (απεικονίζονται σαν W_1, W_2, W_3, W_4, W_5 αντίστοιχα). Ο κόμβος Γ επιλέγει τους *Τοπικούς Υδατογραφημένους Χάρτες* eSOM από τους άμεσους (ενός-βήματος) γείτονές του και δημιουργεί τον *Καθολικό Χάρτη* του τοπικού (άμεσων (ενός-βήματος) γειτόνων) δικτύου του. Παρατηρώντας τον *Καθολικό Χάρτη* του τοπικού του δικτύου, ο κόμβος Γ έχει τη δυνατότητα να παρατηρήσει οπτικά την κατάσταση ασφάλειας των άμεσων (ενός-βήματος) γειτόνων του. Βασιζόμενος σε αυτές τις πληροφορίες ο κόμβος Γ επιλέγει τον κατάλληλο κόμβο προκειμένου να προωθήσει τα μηνύματά του. Ο κόμβος Γ, προκειμένου να επιβεβαιώσει την αυθεντικότητα του *Καθολικού Χάρτη*, εφαρμόζει υδατογράφηση και στον *Καθολικό Χάρτη* (απεικονίζεται σαν W). Παρατηρώντας τον *Καθολικό Χάρτη* ο οποίος

περιλαμβάνει τους *Τοπικούς Χάρτες* όλων των γειτονικών του (ενός-βήματος) κόμβων και θεωρώντας σαν ασφαλείς τους κόμβους που δεν είναι θύματα επιθέσεων πραγματοποιεί την επιλογή του κατάλληλου κόμβου για την προώθηση των μηνυμάτων του.

3. Η Προτεινόμενη Μέθοδος Υδατογράφησης

Η προτεινόμενη μέθοδος ενσωμάτωσης προέρχεται από τον αποτελεσματικό συνδυασμό δύο μεθόδων ενσωμάτωσης της μεθόδου Lattice και Block-Wise. Η μέθοδος Lattice έχει δύο παραμέτρους, την *άλφα0* (αραίωση δικτυωτού πλέγματος (lattice spacing)) και τη *βήτα* (δύναμη ενσωμάτωσης), ενώ η μέθοδος Block-Wise έχει μόνο μία παράμετρο την *άλφα* (παράγοντας κβαντοποίησης). Συνδυάσαμε αυτές τις δύο τεχνικές υδατογράφησης προκειμένου να υλοποιήσουμε έναν κρυπτογραφικό κωδικοποιητή - αποκωδικοποιητή που μπορεί να χρησιμοποιηθεί προκειμένου να πιστοποιήσουμε τους κόμβους σε ένα δίκτυο κατά περίσταση.

Μία από τις πιο σημαντικές απαιτήσεις της υδατογράφησης είναι η αντιληπτή διαφάνεια ανάμεσα στην αυθεντική δουλειά και την υδατογραφημένη. Συγκεκριμένα για τις εικόνες υπάρχουν κάποια αντικειμενικά μέτρα που χρησιμοποιούνται ευρέως. Το υδατογραφημένο μήνυμα μπορεί να έχει ένα υψηλότερο ή χαμηλότερο επίπεδο αντιληπτής διαφοράς, εννοώντας ότι υπάρχει μία μεγαλύτερη ή μικρότερη πιθανότητα ότι ένας παρατηρητής θα αντιληφθεί τη διαφορά ανάμεσα στην υδατογραφημένη και τη μη-υδατογραφημένη εικόνα, στην περίπτωσή μας, του χάρτη eSOM.

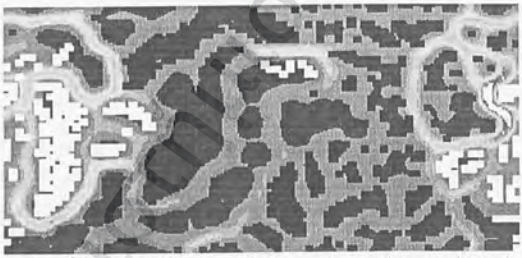
Για μία δίκαια σύγκριση ανάμεσα στην αυθεντική και την υδατογραφημένη εικόνα υπάρχουν αποτελεσματικά μέτρα ελέγχου παραποίησης [Furon, 2005] που είναι αξιόπιστα και χρησιμοποιούνται ευρέως σε ερευνητικά και αναπτυξιακά περιβάλλοντα. Αυτά τα μέτρα ελέγχου παραποίησης δεν εκμεταλλεύονται τις ικανότητες του Ανθρώπινου Οπτικού Συστήματος (Human Visual System (HVS)) αλλά παρέχουν αξιόπιστα αποτελέσματα. Επιπλέον υπάρχει ένα αντικειμενικό κριτήριο που βασίζεται στην ευαισθησία του ματιού και ονομάζεται *αντιληπτή απόσταση Watson*. Είναι επίσης γνωστή σαν *Απλή Αντιληπτή Διαφορά (Just Noticeable Difference (JND))* και αποτελείται από μία συνάρτηση ευαισθησίας, δύο στοιχεία κάλυψης (masking components) που βασίζονται στην φωτεινότητα, την κάλυψη φωτεινότητας (luminance masking) και ένα στοιχείο συγκέντρωσης (pooling). Ο Πίνακας 6.1 δίνει τα μέτρα ποιότητας που χρησιμοποιούνται πιο συχνά για τη σύγκριση υδατογραφημένων και μη υδατογραφημένων μηνυμάτων.

Η εικόνα δοκιμής που χρησιμοποιήσαμε για το έλεγχο της προτεινόμενης προσέγγισης υδατογράφησης είναι σε μορφή bitmap, ασπρόμαυρη (grayscale) και έχει ανάλυση 256x400. Είναι ο χάρτης eSOM ενός κόμβου δικτύου κατά περίσταση και απεικονίζεται στο Σχήμα 6.3. Προκειμένου να χρησιμοποιήσουμε τα μέτρα του Πίνακα 6.1 και να έχουμε μία άποψη για τη διαφορά ανάμεσα στην αυθεντική και την υδατογραφημένη εικόνα ήταν απαραίτητο να

αξιολογήσουμε τις ιδανικές τιμές. Αν υποθέσουμε ότι η αυθεντική και η υδατογραφημένη εικόνα είναι εντελώς πανομοιότυπες οι παραγόμενες τιμές φαίνονται στον Πίνακα 6.2.

Πίνακας 6. 1 Μέτρα Ποιότητας

Μέσο Τετραγωνικό Λάθος (Mean Square Error (MSE))	Η αναμενόμενη τιμή του τετραγωνικού λάθους.
Ποσοστό Σήματος προς Θόρυβο (Signal to Noise Ratio (SNR))	Το ποσοστό της δύναμης σήματος προς τη δύναμη του θορύβου που φθείρει το σήμα.
Κορυφή Ποσοστού Σήματος προς Θόρυβο (Peak Signal to Noise Ratio (PSNR))	Το μέγιστο Ποσοστό Σήματος προς τον Θόρυβο.
Ακρίβεια Εικόνας (Image Fidelity (IF))	Η διαδικασία τεμαχισμού (rending) μίας εικόνας με ακρίβεια χωρίς καμία ορατή παραμόρφωση απώλειας πληροφοριών.
Κανονικοποιημένος Διασταυρούμενος Συσχετισμός (Normalized Cross Correlation (NCC))	Μέτρο ομοιότητας δύο σημάτων.
Ποιότητα Συσχετισμού (Correlation Quality (CQ))	Η απόκλιση δύο μηνυμάτων.
Απόσταση Watson (Watson Distance (WD))	Η απόσταση δύο σημείων ή pixel μεταξύ δύο εικόνων.



Σχήμα 6. 3 Χάρτης eSOM ενός Κόμβου ενός Δικτύου κατά Περίσταση

Πίνακας 6. 2 Ιδανικές Τιμές της Εικόνας Δοκιμής

Μέτρα Ποιότητας	Ιδανικές Τιμές
MSE	0
SNR (dB)	94
PSNR (dB)	110
IF	100
NC	1
CQ	138.178
Απόσταση Watson	0

Στις ακόλουθες παραγράφους περιγράφονται οι μέθοδοι ενσωμάτωσης Lattice και Block-Wise και πώς εφαρμόζεται ο συνδυασμός τους για την υδατογράφησης των χαρτών eSOM.

3.1 Μέθοδος Ενσωμάτωσης Lattice

Σε ένα κώδικα δικτυωτού πλέγματος (lattice code), κάθε λέξη κώδικα (codeword) είναι ένα σημείο σε ένα κανονικό δικτυωτό πλέγματος. Οι παράμετροι της διαδικασίας ενσωμάτωσης είναι: αλφα0 (a_0) η οποία αναπαριστά τη δύναμη ενσωμάτωσης και βήτα (β) η οποία αναπαριστά το διάστημα (spacing) του δικτυωτού πλέγματος. Τα σημεία σε ένα απλό N-διάστατο δικτυωτό πλέγματος μπορούν να κατασκευαστούν προσθέτοντας ακέραια πολλαπλάσια N ξεχωριστών διανυσμάτων. Επομένως κάθε σημάδι (mark) μηνύματος w_m, είναι ένα σημείο σε ένα δικτυωτό πλέγματος ορισμένο ως το άθροισμα ενός ή περισσότερων σημείων αναφοράς (reference marks) w_r.

Τα σημεία αναφοράς (reference marks) είναι ορθογώνια το ένα στο άλλο. Ο ακέραιος που περιγράφει την πιο κοντινή λέξη κώδικα σε οποιοδήποτε διάνυσμα μηνύματος υπολογίζεται βρίσκοντας πρώτα το μήκος του διανύσματος του μηνύματος προβαλλόμενο στο σημείο αναφοράς, και στη συνέχεια διαιρώντας το με το μήκος και κβαντοποιώντας το στο πλησιέστερο διάνυσμα. Το σύστημα υδατογράφησης Lattice ενσωματώνει μόνο ένα bit ανά 256 pixel σε μία εικόνα. Κάθε bit κωδικοποιείται χρησιμοποιώντας τον κώδικα trellis και παράγει μία ακολουθία τεσσάρων bit. Η κωδικοποίηση trellis είναι ένας κώδικας συσπείρωσης (convolutional code) με αριθμό καταστάσεων 2^3=8 και πιθανές εξόδους 2^4=16. Επομένως μετά τη διαδικασία κωδικοποίησης τα bit πρέπει να ενσωματώνονται σε 256 pixel. Αυτό σημαίνει ότι κάθε ένα από τα τέσσερα bit ενσωματώνεται σε 256/4=64 pixel. Η εικόνα χωρίζεται σε τμήματα (block) των 8x8 pixel προκειμένου να φιλοξενήσει τα bit. Το πρότυπο αναφοράς κατασκευάζεται αποτελούμενο από 8x8 τυχαία pixel και οι τιμές των pixel κανονικοποιούνται ώστε να έχουν μέσο μηδέν και διακύμανση ένα. Κάθε bit ενσωματώνεται συσχετίζοντας ένα τμήμα (block) με το πρότυπο αναφοράς (reference pattern) μεγέθους 8x8, και κβαντοποιώντας το αποτέλεσμα σε έναν περιττό ή ζυγό ακέραιο. Το πρότυπο που προστίθεται στο τμήμα (block) μεγέθους 8x8 σύμφωνα με το ευρετήριο του πλησιέστερου σημείου στο δικτυωτό υποπλέγμα ($z_m[i]$) υπολογίζεται με τους ακόλουθους τύπους:

$$z_m[i] = 2\left\lfloor \frac{l[i]/(\beta|w_r|) - m_c[i]}{2} + 0.5 \right\rfloor + m_c[i] \qquad (6.1)$$

όπου w_r είναι το πρότυπο αναφοράς, $m_c[i]$ είναι το αντίστοιχο μήνυμα και $l[i]$ είναι το μήκος του c_i (i-οστό τμήμα της εικόνας) προβαλλόμενο στο w_r. Το $l[i]$ δίνεται από την ακόλουθη εξίσωση:

$$l[i] = \frac{c_i * w_r}{|w_r|}, \qquad (6.2)$$

Το προστιθέμενο πρότυπο $w_{a_0 i}$ δίνεται από την εξίσωση (6.3)

$$w_{a_0 i} = a(\beta z_m[i] w_r - c_i). \tag{6.3}$$

Στην πλευρά του αποκωδικοποιητή το $z[i]$ υπολογίζεται από την εξίσωση (6.4):

$$z[i] = \left\lfloor \frac{c_i * w_r}{\beta w_r * w_r} + 0.5 \right\rfloor, \tag{6.4}$$

και στη συνέχεια ανιχνεύεται το λιγότερο σημαντικό ψηφίο του. Το κωδικοποιημένο μήνυμα στη συνέχεια αποκωδικοποιείται με τον αποκωδικοποιητή trellis.

3.2 Μέθοδος Ενσωμάτωσης Block-Wise

Η μέθοδος Block-Wise περιλαμβάνει τις βασικές ιδιότητες της συμπίεσης JPEG όπου πραγματοποιείται η Μετατροπή Διακριτού Συνημίτονου (Discrete Cosine Transform (DCT)). Τόσο ο κωδικοποιητής όσο και ο αποκωδικοποιητής χρησιμοποιούν αυτές τις ιδιότητες προκειμένου να επιτύχουν τη διαδικασία ενσωμάτωσης και εξαγωγής αντίστοιχα. Η προκαθορισμένη παράμετρος είναι μία παράμετρος δύναμης (strength parameter) άλφα *(a)*, η οποία χρησιμοποιείται σαν παράγοντας κλιμάκωσης του πίνακα κβαντοποίησης φωτεινότητας (luminance quantization matrix).

Τέσσερα bit ενσωματώνονται σε κάθε τμήμα (block) της εικόνας, τα οποία έχουν μέγεθος 8x8 (64 pixel) και παρουσιάζουν υψηλή συχνότητα Μετατροπής Διακριτού Συνημιτόνου (DCT). Στη μέθοδο Lattice ενσωματώνεται ένα bit ανά 256 pixel. Χρησιμοποιώντας τη μέθοδο Block-Wise η εικόνα μπορεί να φιλοξενήσει 16 φορές περισσότερη πληροφορία. Η ενσωμάτωση πραγματοποιείται στους συντελεστές DCT υψηλής συχνότητας και όχι σε αυτούς της χαμηλής συχνότητας προκειμένου να αποφευχθούν οπτικές διαφορές που μπορεί να οδηγήσουν σε μη αποδεκτή χαμηλή ακρίβεια. Ειδικότερα χρησιμοποιούνται 28 συντελεστές που σημαίνει ότι κάθε bit ενσωματώνεται σε επτά συντελεστές.

Οι επτά συντελεστές που πρόκειται να φιλοξενήσουν ένα bit επιλέγονται τυχαία σύμφωνα με έναν αριθμό seed. Το επόμενο βήμα είναι να διαιρέσουμε κάθε συντελεστή *(C[i])* με τον αντίστοιχο παράγοντα κβαντοποίησης *(aq[i])* και να το στρογγυλοποιήσουμε στον κοντινότερο ακέραιο, δηλ.:

$$C_I[i] = \left\lfloor \frac{C[i]}{aq[i]} + 0.5 \right\rfloor, \tag{6.5}$$

όπου q[i] είναι η αντίστοιχη τιμή του πίνακα φωτεινότητας.

Στη συνέχεια ο αλγόριθμος λαμβάνει το λιγότερο σημαντικό ψηφίο (b_e) από τους επτά προκύπτοντες $C_{I[i]}$ ακέραιους και εφαρμόζει αποκλειστικό-ή για να λάβει μία τιμή bit *b*. Η τιμή bit, που πρέπει να ενσωματωθεί, είναι η b. Στην περίπτωση που το $b_e \neq b$ επιλέγεται ένας από τους επτά ακέραιους $C_{I[i]}$, ανάλογα

με το ποιος θα προκαλέσει τη μικρότερη επίδραση ακρίβειας. Έστω ότι το $C_{wl[i]}$ υποδηλώνει το αποτέλεσμα. Αυτό σημαίνει ότι $C_{wl}[i]=C_l[i]$ για όλα τα i στην περίπτωση που ισχύει $b_e=b$. Αν είναι $b_e \neq b$, κάθε μέλος $C_{wl[i]}$ πολλαπλασιάζεται με τους αντίστοιχους παράγοντες κβαντοποίησης προκειμένου να λάβουμε τις υδατογραφημένες εκδόσεις των συντελεστών DCT. Δηλαδή ισχύει:

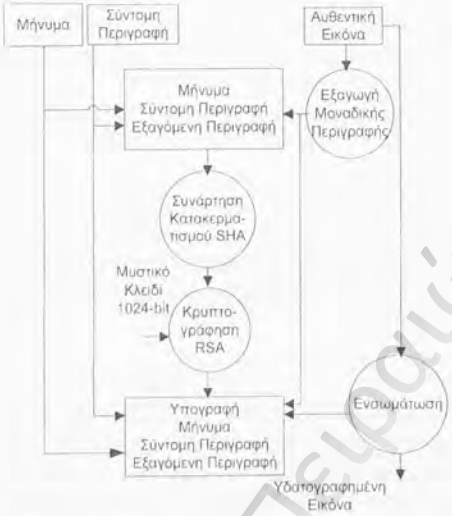
$$C_w[i] = aq[i]C_{wI}[i] \tag{6.6}$$

Στον αποκωδικοποιητή η διαδικασία είναι ακριβώς η ίδια. Από κάθε τμήμα με μεγέθος 8x8 (64 pixel) εξάγεται το λιγότερο σημαντικό bit b_e από κάθε έναν από τους επτά συντελεστές και συγκρίνεται με το ενσωματωμένο b. Εάν τα δύο bit είναι διαφορετικά, το αντίστοιχο τμήμα δεν πιστοποιείται αλλά σημειώνεται σαν αλλοιωμένο (corrupted).

3.3 Μέθοδος Συνδυασμού

Ο αλγόριθμος Lattice χρησιμοποιεί κωδικοποίηση ελέγχου λαθών. Η λειτουργικότητά του βασίζεται στη δημιουργία ορθογώνιων σημείων αναφοράς προκειμένου να χρησιμοποιηθούν στη διαδικασία ενσωμάτωσης. Αλλά στην περίπτωση που κάποιος τροποποιήσει έναν αριθμό τμημάτων, ο αποκωδικοποιητής δεν θα το ανιχνεύσει αφού χρησιμοποιεί κωδικοποίηση trellis. Φυσικά, εάν αλλάξει ένας συνεχής αριθμός τμημάτων, ο αποκωδικοποιητής δεν θα έχει την ικανότητα να εξάγει τη σωστή ακολουθία των bit. Η μέθοδος Lattice ενσωματώνει ένα bit ανά 256 pixel παρέχοντας μία υδατογραφημένη εικόνα πολύ χαμηλής ποιότητας. Από την άλλη πλευρά, η μέθοδος Block-Wise ενσωματώνει τέσσερα bit ανά 64 pixel. Το ωφέλιμο φορτίο που μπορεί να φιλοξενηθεί είναι μεγαλύτερο, σε σύγκριση με αυτό της μεθόδου Lattice, κάτι που είναι ιδιαίτερα χρήσιμο σε εικόνες χαμηλής ανάλυσης. Αλλά η ποιότητα της παραγόμενης εικόνας δεν είναι τόσο καλή, καθώς ο χρήστης μπορεί να εκμεταλλευθεί την απουσία ελέγχου λαθών. Οποιαδήποτε τροποποίηση της υδατογραφημένης εικόνας μπορεί να εντοπιστεί συγκρίνοντας το εξαγόμενο μήνυμα με το αυθεντικό. Ερωτήσεις όπως ποιος και γιατί τροποποίησε την εικόνα μπορούν να απαντηθούν εύκολα. Επομένως σε περιπτώσεις όπου τόσο η ποιότητα όσο και ικανότητα εντοπισμού των τροποποιημένων τμημάτων των εικόνων έχουν την ίδια σημασία, είναι απαραίτητο να συνδυάσουμε τις δύο μεθόδους ενσωμάτωσης [Kominos, 2005].

Ο συνδυασμός των δύο μεθόδων ενσωμάτωσης υλοποιείται χρησιμοποιώντας έναν κρυπτογραφικό κωδικοποιητή-αποκωδικοποιητή. Ένας κόμβος μπορεί να δώσει ένα μικρό μήνυμα όπως είναι η ταυτότητά του (ID) και μία σύντομη περιγραφή (π.χ. ο αριθμός των άμεσων γειτόνων του). Στη συνέχεια μπορεί να χρησιμοποιηθεί, μία μοναδική περιγραφή της εικόνας (π.χ. το άθροισμα των τιμών pixel των τεσσάρων τμημάτων της εικόνας στις γωνίες). Αυτά τα τρία μηνύματα εισάγονται σε μία συνάρτηση κατακερματισμού και στη συνέχεια η τιμή κρυπτογραφείται με ένα μυστικό κλειδί 1024-bit. Η υπογραφή με τη μικρή και την εκτεταμένη περιγραφή ενσωματώνονται με τον αλγόριθμο Block-Wise. Ο κωδικοποιητής απεικονίζεται στο Σχήμα 6.4.



Σχήμα 6. 4 Κρυπτογραφικός Κωδικοποιητής

Από την υδατογραφημένη έκδοση της εικόνας, από την πλευρά του αποκωδικοποιητή, η υπογραφή, η σύντομη και η μοναδική περιγραφή εξάγονται με τη μέθοδο Lattice ενώ το μήνυμα εξάγεται με τη μέθοδο Block-Wise. Η μοναδική περιγραφή αξιολογείται και πάλι αλλά αυτή τη φορά από την υδατογραφημένη έκδοση της εικόνας, και συγκρίνεται με την εξαγόμενη από την αυθεντική εικόνα. Έτσι το πρώτο βήμα είναι να επιβεβαιώσουμε αν ταιριάζουν οι μοναδικές περιγραφές. Στην περίπτωση που ένα υδατογράφημα αντιγράφεται και ενσωματώνεται σε μία άλλη εικόνα, η εξαγόμενη περιγραφή δεν θα είναι η ίδια. Καθώς οι τιμές pixel της εικόνας αλλάζουν ελάχιστα προκειμένου να φιλοξενήσουν το υδατογράφημα, η εξαγόμενη περιγραφή δεν μπορεί να είναι ακριβώς η ίδια, αλλά μόνο πολύ κοντινή. Επομένως, έχουν καθοριστεί κάποια ανώτατα και κατώτατα όρια για αυτό το βήμα επιβεβαίωσης με βάση τις ιδανικές τιμές (Πίνακας 6.2) της εικόνας ελέγχου (Σχήμα 6.3). Το επόμενο βήμα είναι να αποκρυπτογραφηθεί η υπογραφή χρησιμοποιώντας το δημόσιο κλειδί των 1024-bit. Λαμβάνεται επίσης το αποτελέσματα της συνάρτησης κατακερματισμού που είχε εφαρμοστεί στη συνένωση του μηνύματος, της σύντομης και της μοναδικής περιγραφής. Το δεύτερο βήμα του αποκωδικοποιητή είναι να επιβεβαιώσει εάν η αποκρυπτογραφημένη υπογραφή ταιριάζει απόλυτα με το εξαγόμενο αποτέλεσμα της συνάρτησης κατακερματισμού. Εάν τόσο τα αποτελέσματα των συναρτήσεων κατακερματισμού όσο και οι μοναδικές περιγραφές είναι έγκυρες, η διαδικασία πιστοποίησης είναι επιτυχής. Ο σχεδιασμός του αποκωδικοποιητή απεικονίζεται στο Σχήμα 6.5.

Σχήμα 6. 5 Κρυπτογραφικός Αποκωδικοποιητής

4. Αποτελέσματα Υδατογράφησης

Προκειμένου να αξιολογήσουμε την απόδοση και την αποτελεσματικότητα των μεθόδων ενσωμάτωσης, πραγματοποιήσαμε πολλές δοκιμές. Έχει εξεταστεί ένας μεγάλος αριθμός περιπτώσεων με διάφορες τιμές παραμέτρων. Αρχικά παρουσιάζεται η επίδραση της μεθόδου ενσωμάτωσης Lattice. Στη συνέχεια παρουσιάζονται τα αποτελέσματα της μεθόδου Block-Wise και τέλος παρουσιάζονται τα αποτελέσματα από το συνδυασμό των δύο μεθόδων.

4.1 Αποτελέσματα Μεθόδου Ενσωμάτωσης Lattice

Στην περίπτωση της μεθόδου Lattice ο μέγιστος αριθμός των ενσωματωμένων bit μπορεί να είναι 400 (ένα bit ανά 256 pixel). Τα μέτρα που χρησιμοποιούνται για την αξιολόγηση των διαφορών ανάμεσα σε δύο εικόνες παρουσιάστηκαν στον Πίνακα 6.1. Οι δοκιμές πραγματοποιήθηκαν για ένα εύρος των τιμών των παραμέτρων προκειμένου να καταλήξουμε στις πιο αποτελεσματικές τιμές. Οι παράμετροι είναι η *δύναμη ενσωμάτωσης β (embedding strength (β))* και το *διάστημα δικτυωτού πλέγματος αλφα0 (lattice spacing (a_0))*. Το εύρος της τιμής a_0 κυμαίνεται από 0.35 έως 5.33 και το εύρος του β από 0.7 έως 1.1. Το βήμα αύξησης για το a_0 είναι 0.02 και για το β 0.1. Οι τιμές μέτρησης για τη μέθοδο Lattice είναι πολύ κοντά στις ιδανικές. Πιο συγκεκριμένα, η κατεύθυνση προς το μηδέν επιτυγχάνεται χρησιμοποιώντας χαμηλές τιμές του a_0 στην περίπτωση του MSE (Πίνακας 6.3). Εάν την ίδια χρονική η τιμή του β είναι επίσης χαμηλή, το MSE

μειώνεται ακόμα περισσότερο. Όσον αφορά στα SNR και PSNR, οι τιμές τους είναι υψηλότερες όταν οι παράμετροι a_0 και β είναι χαμηλές. Η πιστότητα της εικόνας (IF) ορίζεται σαν το ποσοστό ομοιότητας των δύο εικόνων. Επομένως η τιμή 100% θεωρείται ότι είναι η ιδανική. Χρησιμοποιώντας τα μέτρα ποιότητας NC και CQ, παρατηρούμε ότι οι μετρήσεις τους είναι πιο κοντά στις ιδανικές, καθώς οι τιμές των a_0 και β μειώνονται. Τέλος, όλες οι παραπάνω παρατηρήσεις δικαιολογούνται και από τη μέτρηση Watson η οποία βασίζεται στη φωτεινότητα, την αντίθεση και την κάλυψη συγκέντρωσης (pooling masking).

Πίνακας 6. 3 Αποτελέσματα της Μεθόδου Lattice

Lattice	MSE	SNR	PSNR	IF	NC	CQ	Watson	Σωστά Bit
a_0=0.35, β=1.0	0.019	64.49	70.21	100	1	137.04	8.144	370
a_0=1.01, β=0.9	0.27	51.84	56.72	99.996	1	136.97	21.178	400
a_0=1.85, β=0.8	0.97	49.97	53.12	99.993	1	136.97	51.687	400

Επομένως, οι ιδανικές τιμές των παραμέτρων είναι αυτές που δίνουν τα καλύτερα αποτελέσματα. Μπορούν να είναι ακόμα και οι μηδενικές τιμές. Αλλά στην πλευρά του αποκωδικοποιητή δεν εξάγονται όλα τα bit σωστά. Ειδικότερα, χρησιμοποιώντας χαμηλές τιμές για τα a_0 και β ο αποκωδικοποιητής δεν μπορεί να λάβει τα σωστά ενσωματωμένα bit. Επομένως, μπορούμε να πούμε ότι είναι απαραίτητο να κάνουμε ένα συμβιβασμό μεταξύ των αποτελεσμάτων ποιότητας και των αποτελεσμάτων του αποκωδικοποιητή, προκειμένου να καθορίσουμε τις ιδανικές τιμές. Από τα πειράματα που πραγματοποιήσαμε καταλήξαμε στις προτεινόμενες τιμές $a \approx 0.8$ και $\beta = 0.9$. Στον Πίνακα 6.3 δίνονται ορισμένες τιμές αξιολόγησης των πειραμάτων μας προκειμένου να δικαιολογήσουμε τα παραπάνω συμπεράσματα. Η υδατογραφημένη έκδοση της εικόνας δοκιμής δεν παρουσιάζει σημαντική διαφορά από την αυθεντική εικόνα δοκιμής.

4.2 Αποτελέσματα Μεθόδου Ενσωμάτωσης Block-Wise

Στην περίπτωση της μεθόδου Block-Wise, οι δοκιμές πραγματοποιήθηκαν για την ίδια εικόνα (Σχήμα 6.3) προκειμένου τα αποτελέσματα να είναι συγκρίσιμα με αυτά της μεθόδου Lattice. Μία βασική διαφορά είναι ο αριθμός των bit που ενσωματώνονται. Αφού η μέθοδος ενσωματώνει τέσσερα bit κάθε 64 pixel και η εικόνα έχει 102,400 pixel συνολικά, ο αριθμός των bit που μπορούν να φιλοξενηθούν είναι 6,406. Το μέγεθος της πληροφορίας που μπορεί να υδατογραφηθεί είναι σημαντικά υψηλότερο και συγκεκριμένα είναι 16 φορές μεγαλύτερο από το αντίστοιχο μέγεθος της μεθόδου Lattice. Επομένως πριν καν πραγματοποιήσουμε τη δοκιμή αναμένεται ότι τα αποτελέσματα δεν θα είναι το ίδιο καλά. Οι πληροφορίες σε αυτή την περίπτωση είναι πολύ περισσότερες, το οποίο σημαίνει ότι οι τροποποιήσεις στην εικόνα θα παράγουν χειρότερες τιμές

στα μέτρα ποιότητας. Η μόνη παράμετρος της μεθόδου Block-Wise είναι αυτή που είναι υπεύθυνη για την κβαντοποίηση του πίνακα φωτεινότητας και ονομάζεται *άλφα* (*α*).

Η παρατήρηση των αποτελεσμάτων αποδεικνύει αυτό που σημειώθηκε εξαρχής. Οι τιμές των μέτρων ποιότητας δεν είναι το ίδιο καλές σε σύγκριση με αυτές της μεθόδου Lattice. Η μέτρηση του MSE είναι υψηλότερη από τη μηδενική τιμή, που είναι η ιδανική. Οι τιμές των SNR και PSNR, που χρησιμοποιούνται εκτενώς, δείχνουν ότι όταν η τιμή της παραμέτρου *άλφα* (*α*) αυξάνεται το αποτέλεσμα χειροτερεύει. Όσον αφορά στα IF, NC, CQ, οι μετρήσεις φαίνεται να απέχουν σημαντικά από τις ιδανικές τιμές καθώς το *άλφα* παίρνει υψηλότερες τιμές. Το ίδιο ισχύει και για την αντιληπτή απόσταση από το μοντέλο Watson, καθώς τα αποτελέσματα είναι χειρότερα όταν το *άλφα* (*α*) αυξάνεται. Κάποιες τιμές των μέτρων ποιότητας δίνονται στον Πίνακα 6.4.

Πίνακας 6. 4 Αποτελέσματα της Μεθόδου Ενσωμάτωσης Block-Wise

Block-Wise	MSE	SNR	PSNR	IF	NC	CQ	Watson	Σωστά Bit
α=0.03	0.312	44.11	62.18	99.9981	0.99997	138.9	12.144	6012
α=0.16	4.324	36.22	52.32	99.9701	0.99988	137.902	108.972	6406
α=0.33	11.321	31.45	44.29	99.8926	0.99978	137.123	309.456	6406

Σύμφωνα με τα παραπάνω προκύπτει ότι καθώς η τιμή του *άλφα* (*α*) αυξάνεται, η υδατογραφημένη εικόνα παρουσιάζει χαμηλότερη πιστότητα. Επομένως η ιδανική τιμή της παραμέτρου θα ήταν μία μικρή τιμή, π.χ. 0.01. Αλλά όπως φαίνεται τιμές μικρότερες από 0.05 δεν επιτρέπουν στον αποκωδικοποιητή να λάβει το σωστό μήνυμα. Η τιμή του *άλφα* που θα επιλεγεί εξαρτάται από το πόσο ευαίσθητη επιθυμεί ο χρήστης να είναι η μέθοδος προκειμένου να προσδιορίσει τα τροποποιημένα bit και να σημειώσει τα αντίστοιχα τμήματα. Υψηλότερες τιμές του *άλφα* (*α*) αυξάνουν την ευαισθησία της μεθόδου, αλλά ταυτόχρονα μειώνεται η ποιότητα της εικόνας. Επομένως είναι και πάλι απαραίτητο να έχουμε ένα συμβιβασμό ανάμεσα στην ποιότητα της εικόνας και την ευαισθησία εντοπισμού τροποποίησης. Μία πιθανή προτεινόμενη τιμή θα μπορούσε να είναι *α*≈0.2. Η υδατογραφημένη έκδοση της πρωτότυπης εικόνας που δημιουργήθηκε με τη μέθοδο Block-Wise δεν παρουσιάζει οπτικά αντιληπτές διαφορές από την εικόνα ελέγχου, η οποία απεικονίζεται στο Σχήμα 6.3.

4.3 Αποτελέσματα Μεθόδου Συνδυασμού

Προκειμένου να πραγματοποιήσουμε υδατογράφηση στους χάρτες eSOM εκμεταλλευόμαστε τα πλεονεκτήματα των δύο μεθόδων υδατογράφησης, της μεθόδου Lattice και Block-Wise. Όπως προαναφέρθηκε η μέθοδος Lattice παρέχει υδατογραφημένες εικόνες υψηλής ποιότητας αλλά ο αριθμός των bit που ενσωματώνονται είναι μόνο ένα bit ανά 256 pixel. Από την άλλη πλευρά, η μέθοδος Block-Wise ενσωματώνει τέσσερα bit ανά 64 pixel αλλά με το κόστος

χαμηλής ποιότητας της παραγόμενης εικόνας. Επιπλέον, η απουσία του ελέγχου λαθών στη μέθοδο Block-Wise μας δίνει το πλεονέκτημα να μπορούμε εύκολα να εντοπίσουμε όποιες τροποποιήσεις της υδατογραφημένης εικόνας.

Στους χάρτες eSOM το τμήμα που είναι πιο πιθανό να τροποποιηθεί παράνομα υδατογραφείται με τη μέθοδο Block-Wise, ενώ η υπόλοιπη εικόνα υδατογραφείται με τη μέθοδο Lattice. Αυτό σημαίνει ότι οι περιοχές στο χάρτη eSOM που απεικονίζονται στο Σχήμα 6.3 με το ανοιχτό χρώμα και αναπαριστούν την κλάση δεδομένων επίθεσης θα υδατογραφηθούν με τη μέθοδο Block-Wise ενώ ο υπόλοιπος χάρτης eSOM (η κλάση δεδομένων "φυσιολογικής" δικτυακής κίνησης (σκούρο χρώμα)) με τη μέθοδο Lattice. Με αυτό τον τρόπο, έχουμε τη δυνατότητα να έχουμε μία εικόνα υψηλότερης ποιότητας αλλά ταυτόχρονα αν ένας επιτιθέμενος αλλάξει για παράδειγμα την περιοχή της κλάσης επίθεσης ο αλγόριθμος που συνδυάζει τις δύο μεθόδους ενσωμάτωσης έχει τη δυνατότητα να προσδιορίσει τα τροποποιημένα pixel. Αυτό επιτυγχάνεται συγκρίνοντας το εξαγόμενο μήνυμα με το αυθεντικό.

Πίνακας 6. 5 Τιμές Αποτελεσμάτων της Μεθόδου Υδατογράφησης Συνδυασμού

άλφα0=0.93, βήτα=1.0, άλφα=0.1	Lattice άλφα0, βήτα	Block-Wise άλφα	Συνδυασμός μεθόδων άλφα0,βήτα,άλφα
MSE	0.385	1.785	0.394
SNR	44.2	40.45	45.74
PSNR	53.14	47.25	51.98
IF	99.9972	99.9978	99.9975
NC	0.99999	0.99902	0.99998
CQ	139.457	139.578	139.457
Απόσταση Watson	31.415	59.788	31.499

άλφα0=1.53, βήτα=0.8, άλφα=0.2	Lattice άλφα0, βήτα	Block-Wise άλφα	Συνδυασμός μεθόδων άλφα0,βήτα,άλφα
MSE	0.557	4.121	0.74
SNR	44.08	32.97	42.41
PSNR	51.14	40.54	49.75
IF	99.9968	99.9482	99.9836
NC	0.99998	0.99989	0.99997
CQ	139.784	139.78	139.785
Απόσταση Watson	49.145	155.518	50.002

Το μήνυμα ενσωματώνεται στο τμήμα της εικόνας που υδατογραφείται με τη μέθοδο Block-Wise, ενώ η υπογραφή, η μικρή και η εξαγόμενη περιγραφή στο μεγάλο τμήμα της εικόνας. Πραγματοποιήσαμε και πάλι μετρήσεις των μέτρων ποιότητας προκειμένου να ερευνήσουμε τα αποτελέσματα. Αφού η μέθοδος Lattice δίνει καλύτερα αποτελέσματα από τη μέθοδο Block-Wise, αναμένεται ότι οι παραγόμενες τιμές αποτελεσμάτων θα βρίσκονται ανάμεσα στις αντίστοιχες

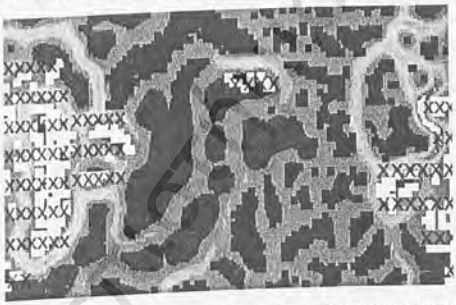
τιμές που παράγονται από τις δύο μεθόδους. Σίγουρα τα αποτελέσματα δεν είναι τόσο καλά όσο αυτά που παράγονται από τη μέθοδο Lattice αλλά ταυτόχρονα είναι καλύτερα από αυτά που παράγονται με τη μέθοδο Block-Wise. Στον Πίνακα 6.5 παρουσιάζονται μερικά αποτελέσματα από το συνδυασμό των δύο μεθόδων προκειμένου να τα συγκρίνουμε με αυτά των δύο μεθόδων όταν χρησιμοποιούνται ξεχωριστά. Ο πίνακας δικαιολογεί ότι ο συνδυασμός των δύο μεθόδων παράγει αποτελέσματα ανάμεσα σε αυτά που παράγονται με τη χρήση των δύο μεθόδων ξεχωριστά.

Στον Πίνακα 6.6 παρουσιάζεται ο μέγιστος αριθμός bit που μπορούν να φιλοξενηθούν στην εικόνα ελέγχου (Σχήμα 6.3) χρησιμοποιώντας τις δύο μεθόδους ενσωμάτωσης ξεχωριστά και τον συνδυασμό τους.

Πίνακας 6. 6 Μέγιστος Αριθμός Ενσωματωμένων bit

	Lattice	Block-Wise	Συνδυασμός Μεθόδων
Μέγιστος Αριθμός Ενσωματωμένων Bit	400	6406	>= 4100

4.3.1 Έλεγχος Τροποποίησης Υδατογραφημένης Εικόνας



Σχήμα 6. 6 Υδατογραφημένη Εικόνα για τη Δοκιμή του Κρυπτογραφικού Κωδικοποιητή – Αποκωδικοποιητή

Πραγματοποιήσαμε ένα τελευταίο έλεγχο προκειμένου να επιβεβαιώσουμε το γεγονός ότι σε περίπτωση που κάποιος τροποποιήσει το τμήμα του χάρτη eSOM (Σχήμα 6.3) που έχει υδατογραφηθεί με τη μέθοδο Block-Wise, ο αποκωδικοποιητής έχει την ικανότητα να αναγνωρίσει την τροποποίηση, να ενημερώνει το χρήστη ότι η πιστοποίηση απέτυχε και να παράγει σαν έξοδο ένα αρχείο στο οποίο τα τροποποιημένα τμήματα (block) σημειώνονται. Το τμήμα της εικόνας που είναι πιο πιθανό να τροποποιηθεί παράνομα είναι η περιοχή με το ανοιχτό χρώμα, η οποία απεικονίζει την κλάση της επίθεσης. Στην υδατογραφημένη έκδοση της εικόνας, η περιοχή με το ανοιχτό χρώμα, που αναπαριστά την ύπαρξη μίας επίθεσης σε έναν κόμβο του δικτύου κατά περίσταση, άλλαξε και αυτή η εικόνα μπήκε σαν είσοδος στον αποκωδικοποιητή

προκειμένου να εξετάσουμε την αυθεντικότητα της. Η διαδικασία πιστοποίησης απέτυχε και παράχθηκε μία σημειωμένη εικόνα (Σχήμα 6.6). Παρατηρώντας αυτή τη σημειωμένη εικόνα είναι προφανές ότι ο αποκωδικοποιητής έχει επιτυχώς εντοπίσει τα τροποποιημένα τμήματα. Επομένως, η όλη υλοποίηση του κρυπτογραφικού κωδικοποιητή – αποκωδικοποιητή είναι σωστή.

5. Επίλογος

Στο κεφάλαιο αυτό παρουσιάσαμε μία καινοτόμα και αποτελεσματική μέθοδο υδατογράφησης προκειμένου να διασφαλίσουμε την ακεραιότητα των *Τοπικών* και *Καθολικών Χαρτών* που παράγονται από τη μηχανή Ανίχνευσης και Απόκρισης σε Εισβολές στα ασύρματα δίκτυα κατά περίσταση που περιγράφηκε στο προηγούμενο κεφάλαιο. Η προτεινόμενη μέθοδος υδατογράφησης είναι αποτέλεσμα του αποτελεσματικού συνδυασμού δύο μεθόδων ενσωμάτωσης της Lattice και της Block-Wise. Η προτεινόμενη μέθοδος υδατογράφησης εκμεταλλεύεται τα πλεονεκτήματα των μεθόδων Lattice και Block-Wise προκειμένου να παράγει αξιόπιστα και ακριβή αποτελέσματα. Το πιο ευαίσθητο τμήμα του χάρτη eSOM, το οποίο αναπαριστά την ύπαρξη επίθεσης στον κόμβο του δικτύου υδατογραφείται με τη μέθοδο Block-Wise ενώ το υπόλοιπο τμήμα του χάρτη υδατογραφείται με τη μέθοδο Lattice. Εκμεταλλευόμαστε τα σημαντικά πλεονεκτήματα της οπτικής απεικόνισης και της υδατογράφησης στα ασύρματα δίκτυα κατά περίσταση, δύο ερευνητικές περιοχές που δεν είχαν χρησιμοποιηθεί προηγουμένως στην ερευνητική περιοχή των ασυρμάτων δικτύων κατά περίσταση.

Πρέπει να σημειώσουμε εδώ ότι προκειμένου να επιβεβαιώσουμε την εφαρμογή της προτεινόμενης μεθόδου υδατογράφησης σε πραγματικά περιβάλλοντα ασύρματων δικτύων κατά περίσταση που αντιμετωπίζουν περιορισμούς πόρων, υπολογίζονται εκ των προτέρων όλοι οι απαραίτητοι υπολογισμοί της τεχνικής υδατογράφησης. Με αυτό τον τρόπο, η μόνη υπολογιστική πολυπλοκότητα προκύπτει από την δημιουργία και την επιβεβαίωση της ψηφιακής υπογραφής. Επιπλέον, η υπολογιστική επιβάρυνση της προτεινόμενης μεθόδου υδατογράφησης είναι η ίδια με το μήκος του κλειδιού που χρησιμοποιούμε στους αλγόριθμους υπογραφής, π.χ. 1024-bit.

Βιβλιογραφία

[Furon, 2005] T. Furon, *"A Survey of Watermarking Security"*, In Proceedings of Digital Watermarking: 4h International Workshop (IWDW), LNCS Proceedings, Italy, (2005), pp. 201-215.

[Komninos, 2005] N. Komninos, *"Combined Image Watermarking Techniques using a Cryptographic Encoder"*, Algorithms & Security Group, Technical Report TR-033.

[Páez, 2006] R., C. Satizábal, J. Forné, *"Cooperative Itinerant Agents (CIA): Security Scheme for Intrusion Detection Systems"*, In Proceedings of the International Conference on Internet Surveillance & Protection (ICISP '06), (2006) p. 26.

[Seitz, 2005] J. Seitz, *"Digital Watermarking for Digital Media"*, Information Science Publishing, ISBN: 1591405181, 2005.

[Wang, 2001] X. Wang, D.S. Reeves, S.F. Wu, J. Yuill, "Sleepy watermark tracing: an active network-based intrusion response framework", In Proceedings of the 16th International Conference of Information Security (IFIP/SEC'01), Paris, France.

[Zhang, 2006] Q. Zhang, *"New techniques for Digital Watermarking"*, ProQuest / UMI, ISBN: 0542283778, 2006-12-13.

[Ultsch, 1999] A. Ultsch, *"Data Mining and Knowledge Discovery with Emergent SOFMs for Multivariate Time Series"*, In Kohonen Maps, Elsevier Science,(1999) pp. 33-46.

[Ultsch, 2003] A. Ultsch, *"Maps for Visualization of High-dimensional Data Spaces"*, In Proceedings of Workshop on Self-Organizing Maps (WSOM '03), September (2003), Kyushu, Japan, pp. 225-230.

[Ultsch, 2005] A. Ultsch, F. Moerchen *"eSOM-Maps: Tools for Clustering, Visualization, and Classification with emergent SOM"*, Tech. Report Dept. of Mathematics and Computer Science, University of Marburg, Germany, No. 46 (2005).

Κεφάλαιο 7ο

Ανίχνευση Εισβολών Χρησιμοποιώντας Αλγόριθμους Ταξινόμησης με Ευαισθησία στο Κόστος

1. Εισαγωγή

Στα προηγούμενα κεφάλαια εξετάσαμε και προτείναμε μηχανισμούς διασφάλισης των υπολογιστικών επικοινωνιών σε ενσύρματα και ασύρματα δίκτυα κατά περίσταση. Επίκεντρο των προτεινόμενων μηχανισμών είναι η ανίχνευση εισβολών καθώς όπως ήδη αναφέραμε αποτελεί ένα πολύτιμο όπλο για τη διασφάλιση των υπολογιστικών συστημάτων. Προκειμένου να πραγματοποιήσουμε την ανίχνευση εισβολών υιοθετήσαμε μηχανισμούς ταξινόμησης της δικτυακής κυκλοφορίας.

Τα συνήθη προβλήματα ταξινόμησης απαιτούν τη λήψη της απόφασης ταξινόμησης που ελαχιστοποιεί την πιθανότητα λάθους. Παρόλα αυτά, για πολλά πεδία προβλημάτων όπως η ανίχνευση εισβολών, η απαίτηση δεν είναι

απλά να προβλέψουμε την πιο πιθανή κατηγορία (κλάση) στην οποία ανήκουν τα δεδομένα, αφού διαφορετικοί τύποι λαθών επιφέρουν διαφορετικό κόστος. Στην ανίχνευση εισβολών, η εμφάνιση λανθασμένων θετικών συναγερμών έχει σημαντικά μικρότερο κόστος από την αποτυχημένη ανίχνευση επιθέσεων. Σε τέτοιες περιπτώσεις, είναι προτιμότερο να λάβουμε την απόφαση ταξινόμησης που δημιουργεί το μικρότερο αναμενόμενο κόστος, παρά εκείνη με τη μικρότερη πιθανότητα λάθους. Για το σκοπό αυτό σε αυτό το κεφάλαιο επικεντρωνόμαστε σε μεθόδους ανίχνευσης εισβολών που παρουσιάζουν ευαισθησία ως προς το κόστος.

Αν και έχει πραγματοποιηθεί εκτεταμένη έρευνα στο χώρο της ταξινόμησης με ευαισθησία στο κόστος, ειδικότερα στο πεδίο των βέλτιστων στατιστικών αποφάσεων [DeGroot, 2004], έχει αγνοηθεί σε μεγάλο βαθμό στο χώρο της ανίχνευσης εισβολών. Υπάρχουν δύο άλλες εργασίες ([Fan, 2000] , [Pietraszek, 2004]) που μελετούν την ανίχνευσης εισβολών με ευαισθησία στο κόστος. Και οι δύο μέθοδοι χρησιμοποιούν έναν αλγόριθμο κάλυψης (wrapper) (τον αλγόριθμο MetaCost [Domingos, 1999] και τον αλγόριθμο Weighting [Ting, 1998] αντίστοιχα σε συνδυασμό με τον αλγόριθμο ταξινόμησης RIPPER [Cohen, 1995]. Αν και οι δύο εργασίες παρουσιάζουν αποτελέσματα για το σύνολο δεδομένων KDD [KDD, 1999], καμμία δεν χρησιμοποιεί τον πίνακα κόστους που αντιστοιχεί στο σύνολο δεδομένων KDD με αποτέλεσμα να μην υπάρχει η δυνατότητα πραγματοποίησης συγκρίσεων.

Σε αυτό το κεφάλαιο, προτείνουμε τη χρήση μεθόδων ταξινόμησης που μπορούν εύκολα να ενσωματωθούν στο πλαίσιο εργασίας βέλτιστων στατιστικών αποφάσεων προκειμένου να δημιουργήσουμε συστήματα ανίχνευσης εισβολών που θα είναι αποτελεσματικά στην ελαχιστοποίηση του αναμενόμενου κόστους της λειτουργίας τους. Εφαρμόζουμε την προτεινόμενη προσέγγιση ανίχνευσης εισβολών με ευαισθησία στο κόστος τόσο σε ενσύρματα όσο και ασύρματα δίκτυα κατά περίσταση και εξετάζουμε την αποτελεσματικότητά της σε τέσσερις πολύ αποτελεσματικούς αλγόριθμους ταξινόμησης, το πολυ-επίπεδο perceptron (MultiLayer Perceptron (MLP)), το γραμμικό (Linear) ταξινομητή, το Μοντέλο Γκαουσσιανών Μειγμάτων (Gaussian Mixture Model (GMM)) και τον ταξινομητή απλοϊκού μοντέλου (Naïve Bayes). Δυστυχώς, δεν μπορούν όλοι οι αλγόριθμοι ταξινόμησης να χρησιμοποιηθούν σε αυτή τη προσέγγιση ελαχιστοποίησης αναμενόμενου κόστους. Για παράδειγμα, η ερώτηση για το πώς μπορούμε να επεκτείνουμε την ταξινόμηση με ευαισθησία στο κόστος για τις Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machines) παραμένει ένα ανοιχτό ερευνητικό θέμα ([Lin, 2002], [Fumera, 2002]) στο χώρο των βέλτιστων στατιστικών αποφάσεων και για αυτό δεν θα συμπεριληφθεί στην έρευνά μας.

Συμπεριλαμβάνουμε όμως τον αλγόριθμο των Μηχανών Υποστήριξης Αποφάσεων (SVM) σε μία σύγκριση που πραγματοποιούμε ανάμεσα στους πέντε αλγόριθμους (MLP, Linear, GMM, Naïve Bayes, SVM) προκειμένου να εντοπίσουμε τον πιο αποτελεσματικό στην ανίχνευση εισβολών χωρίς οι αλγόριθμοι να παρουσιάζουν ευαισθησία ως προς το κόστος.

Σε αυτό το κεφάλαιο εξετάζουμε την ανίχνευση εισβολών που βασίζεται σε ταξινόμηση με και χωρίς ευαισθησία ως προς το κόστος και προσπαθούμε να απαντήσουμε σε ορισμένα βασικά ερωτήματα.

- Αρχικά σε ποιο βαθμό πρέπει να ταιριάζει η κατανομή του συνόλου δεδομένων ελέγχου με το σύνολο δεδομένων εκπαίδευσης.
- Δεύτερον, για την ανίχνευση εισβολών με ή χωρίς ευαισθησία στο κόστος αν υπάρχουν κάποιοι αλγόριθμοι ταξινόμησης που είναι καλύτεροι από κάποιους άλλους ή υπάρχει μία ποικιλία ως προς την αποτελεσματικότητα.
- Τέλος, σε ποιο βαθμό ο ρυθμός *λανθασμένων συναγερμών* αυξάνεται όταν το κόστος των επιθέσεων που δεν ανιχνεύτηκαν αυξάνεται σε σχέση με το κόστος των λανθασμένων συναγερμών.

Προκειμένου να απαντήσουμε στα παραπάνω ερωτήματα πραγματοποιούμε αξιολόγηση της προσέγγισής μας σε ενσύρματα και ασύρματα δίκτυα κάτω από διαφορετικές πειραματικές συνθήκες, πίνακες κόστους και διαφορετικά μοντέλα ταξινόμησης, όσον αφορά στο αναμενόμενο κόστος αλλά και στους ρυθμούς *ανίχνευσης εισβολών* και *λανθασμένων συναγερμών*. Διαπιστώνουμε ότι ακόμα και κάτω από μη ευνοϊκές συνθήκες, η ταξινόμηση με ευαισθησία στο κόστος μπορεί να βελτιώσει σημαντικά, αν όχι ελαφρά, την απόδοση των αλγόριθμων ταξινόμησης στην ανίχνευση εισβολών.

Ακολουθώντας την εισαγωγή αυτή το κεφάλαιο αυτό οργανώνεται ως εξής. Η επόμενη ενότητα παρουσιάζει τη μέθοδο που ακολουθούμε προκειμένου οι αλγόριθμοι ταξινόμησης να μπορούν άμεσα να ενσωματωθούν στο πλαίσιο εργασίας των βέλτιστων στατιστικών αποφάσεων προκειμένου να δημιουργήσουμε *Συστήματα Ανίχνευσης Εισβολών* (Intrusion Detection Systems (IDS)) με ευαισθησία στο κόστος. Τα συστήματα αυτά θα έχουν τη δυνατότητα να ελαχιστοποιούν το αναμενόμενο κόστος της λειτουργίας τους αναλύοντας τη σχέση ανάμεσα στους πίνακες κόστους και τον επιθυμητό συμβιβασμό των ρυθμών *ανίχνευσης εισβολών* και *λανθασμένων συναγερμών*. Επιπλέον στην ενότητα αυτή περιγράφονται τα μοντέλα ταξινόμησης που χρησιμοποιήθηκαν. Η ενότητα 3 περιγράφει αναλυτικά τα πειράματα αξιολόγησης που πραγματοποιήθηκαν. Η ενότητα των πειραμάτων αξιολόγησης χωρίζεται σε δύο βασικές κατηγορίες τα πειράματα που πραγματοποιήθηκαν για ενσύρματα και ασύρματα δίκτυα κατά περίσταση. Κάθε μία από αυτές τις κατηγορίες χωρίζεται με τη σειρά της στα πειράματα που πραγματοποιήθηκαν στους αλγόριθμους ταξινόμησης με και χωρίς ευαισθησία στο κόστος αντίστοιχα. Η ενότητα 4 ολοκληρώνει το κεφάλαιο με συμπεράσματα και σχολιασμό των αποτελεσμάτων.

2. Ταξινόμηση με Ευαισθησία στο Κόστος

Έχοντας ένα προσδιορισμένο κόστος για σωστές και λανθασμένες προβλέψεις, η βέλτιστη απόφαση μπορεί να υπολογιστεί χρησιμοποιώντας τη δεσμευμένη πιθανότητα κάθε κλάσης δεδομένου του παραδείγματος σύμφωνα με το μοντέλο

μας.[2] Πιο συγκεκριμένα, για ένα σύνολο Ω από k κλάσεις, έστω ότι ένας kxk πίνακας C τέτοιος ώστε $C(i,j)$ να είναι το αναμενόμενο κόστος για την πρόβλεψη της κλάσης i όταν η πραγματική κλάση είναι j. Εάν $i=j$ τότε η απόφαση είναι σωστή, ενώ αν $i \neq j$ η απόφαση είναι λανθασμένη. Επιπλέον, έστω ότι οι Y και H είναι τυχαίες μεταβλητές που υποδηλώνουν την πραγματική και την υποτιθέμενη ετικέτα κλάσης αντίστοιχα. Για κάθε παρατήρηση $x \in X$ η βέλτιστη απόφαση θα είναι η κλάση i που ελαχιστοποιεί μία συνάρτηση απώλειας ίση με το αναμενόμενο κόστος:

$$L(x,i) = E[C \mid X = x, H = i] \equiv \sum_{j \in \Omega} P(Y = j \mid X = x) \cdot C(i,j) \tag{7.1}$$

όπου το $P(Y \mid X)$ υποδηλώνει τη δεσμευμένη κατανομή των ετικετών κλάσης δεδομένης μίας παρατήρησης, σύμφωνα με το μοντέλο μας. Σε αυτό το πλαίσιο εργασίας, αυτό που απαιτείται είναι ένα μοντέλο που μπορεί να εκτιμήσει αυτή την πιθανότητα. Η συνάρτηση λήψης αποφάσεων με ευαισθησία ως προς το κόστος $f: S \to \Omega$ θα επιλέξει απλά την απόφαση i που ελαχιστοποιεί το αναμενόμενο κόστος δεδομένης της απόφασης και του παραδείγματος[3]. Πιο συγκεκριμένα:

$$f(x) = \arg\min_{i \in \Omega} L(x,i) \tag{7.2}$$

Η μορφή του πίνακα κόστους C εξαρτάται από τη συγκεκριμένη εφαρμογή. Γενικά, είναι λογικό να επιλέγουμε τα διαγώνια στοιχεία του πίνακα να είναι ίσα με μηδέν, π.χ. $C(i,j)=0$, για $i=j$, καθώς η σωστή ταξινόμηση δεν συνοδεύεται από κόστος. Τα άλλα στοιχεία του πίνακα καθορίζουν το κόστος της λανθασμένης ταξινόμησης ενός παραδείγματος j ως κλάσης i. Θα πρέπει να είναι μη αρνητικά εάν τα στοιχεία της διαγωνίου είναι ίσα με μηδέν, δηλ. $C(i,j) \geq 0$ για $i \neq j$. Σημειώνουμε ότι όταν όλα τα μη διαγώνια κόστη είναι ίσα με 1, το μέτρο αναμενόμενου κόστους συμπίπτει με το μέτρο του αναμενόμενου λάθους ταξινόμησης.

2.1 Επιλογή του Πίνακα Κόστους

Σαν παράδειγμα, ας θεωρήσουμε έναν πίνακα κόστους C για δύο κλάσεις, θετική και αρνητική. Το κόστος ενός λανθασμένου θετικού συναγερμού είναι $C(2, 1)$, ενώ το κόστος ενός λανθασμένου αρνητικού συναγερμού είναι $C(1, 2)$ και μπορούμε να θέσουμε $C(1, 1) = C(2, 2) = 0$, δηλ., μία σωστή ταξινόμηση δεν θα

[2] Η υποδηλωμένη εξάρτηση από κάποιο μοντέλο m μπορεί να γραφεί σαφώς δεσμεύοντας τα πάντα στο μοντέλο. Στη συνέχεια η αναμενόμενη τιμή θα γράφεται $E[C \mid x,f,m]$ και η δεσμευμένη πιθανότητα των κλάσεων $P(y \mid x,m)$.

[3] Το οποίο φυσικά δεν είναι απαραίτητα το ίδιο με την απόφαση με την πιθανότητα ελάχιστου λάθους. Επιπλέον, αυτό το πλαίσιο εργασίας μπορεί να επεκταθεί εύκολα στην περίπτωση όπου το σύνολο αποφάσεων διαφέρουν από το σύνολο των ετικετών κλάσης.

έχει κόστος. Για τις εφαρμογές ανίχνευσης εισβολών, είναι συνηθισμένο να αναφερόμαστε στις επιθέσεις σαν θετικό γεγονός και στην κανονική δικτυακή συμπεριφορά σαν αρνητικό γεγονός. Επιπλέον, η εμφάνιση *λανθασμένων αρνητικών συναγερμών (False Negatives (FN))* θεωρείται σοβαρότερο λάθος από αυτό ενός *λανθασμένου θετικού συναγερμού (False Positives (FP))*, επομένως ο πίνακας C θα πρέπει να αναπαριστά αυτή τη σοβαρότητα λάθους κάτι που επιτυγχάνεται αν ισχύει $C(1, 2) \geq C(2, 1)$. Σε ορισμένες περιπτώσεις, όπως σε βάσεις δεδομένων που θεωρούνται σημεία αναφοράς για την ανίχνευση εισβολών, ο πίνακας κόστους είναι διαθέσιμος, ενώ σε άλλες περιπτώσεις πρέπει να επιλεγχθεί από το χρήστη.

2.2 Αλγοριθμικές Συγκρίσεις και Μέτρα Σύγκρισης

Όταν πραγματοποιούμε συγκρίσεις ανάμεσα σε αλγόριθμους, είναι σημαντικό να χρησιμοποιούμε το ίδιο μέτρο ποιότητας για όλους τους αλγόριθμους. Ένα κοινό μέτρο ποιότητας είναι η εμπειρική τιμή της αναμενόμενης τιμής του κόστους C όταν μετράται σε ένα ανεξάρτητο δοκιμαστικό σύνολο *D*:

$$\hat{E}(C \mid D) = \frac{1}{|D|} \sum_{d \in D} C\left(f(x_d), y_d\right), \tag{7.3}$$

όπου $d = (x_d, y_d)$

Όταν ένας πίνακας κόστους αυτού του τύπου ορίζεται σαν μέτρο εκτίμησης σε μία βάση δεδομένων που θεωρείται σημείο αναφοράς, τότε είναι προτιμότερο να χρησιμοποιούμε αυτόν τον πίνακα. Παρόλα αυτά, είναι σημαντικό να σημειώσουμε ότι γενικά στη βιβλιογραφία ο *ρυθμός ανίχνευσης εισβολών (DR)* και ο *ρυθμός λανθασμένων συναγερμών (FA)* είναι τα μέτρα εκτίμησης που χρησιμοποιούνται συνήθως:

$$\mathrm{DR} = \frac{TP}{TP + FN}, \quad \mathrm{FA} = \frac{FP}{TN + FP}, \tag{7.4}$$

όπου TP, TN, FP, FN, υποδηλώνουν τον αριθμό των πραγματικών (T) και λανθασμένων (F) θετικών (P) και αρνητικών (N) συναγερμών αντίστοιχα. Στόχος είναι να μειώσουμε το *ρυθμό λανθασμένων συναγερμών (FA)*, αυξάνοντας ταυτόχρονα το *ρυθμό ανίχνευσης εισβολών (DR)*. Αφού αυτό συνήθως δεν είναι δυνατό, είναι επιθυμητό να επιτευχθεί ένας συμβιβασμός ανάμεσα στα δύο μέτρα. Αυτός ο συμβιβασμός μπορεί να επιτευχθεί αυτόματα μέσω της χρήσης του κατάλληλου πίνακα κόστους.

Συγκεκριμένα, η εξίσωση (7.3) χρησιμοποιώντας τα μέτρα της εξίσωσης (7.4) μπορεί να γραφεί:

$$\hat{E}(C \mid D) = \frac{FN * C(2,1) + FP * C(1,2)}{|D|}, \tag{7.5}$$

οπότε απομένει να ορίσουμε έναν κατάλληλο πίνακα κόστους.
Μπορούμε να γράψουμε το αναμενόμενο κόστος με την μορφή:

$$E[C] = q \cdot P(H = 1 \mid C = 2) \cdot P(C = 2) + r \cdot P(H = 2 \mid C = 1) \cdot P(C = 1)$$
$$= q(1 - DR)P(C = 2) + r \cdot FA \cdot P(C = 1),$$

όπου το 2 υποδηλώνει ένα θετικό παράδειγμα.

Τέλος, θέτοντας $r = \frac{1}{P(C=1)}$ και $q = \frac{k}{P(C=2)}$, λαμβάνουμε μία συνάρτηση κόστους που ελαχιστοποιεί το *FA-kDR*, όπου το *k* είναι μία ελεύθερη παράμετρος που καθορίζει το συμβιβασμό που θέλουμε να επιτύχουμε μεταξύ λανθασμένων συναγερμών και επιτυχών ανιχνεύσεων επιθέσεων.

Σε αυτό το κεφάλαιο θα χρησιμοποιήσουμε τη μέθοδο που περιγράψαμε και θα αξιολογήσουμε τα αποτελέσματα χρησιμοποιώντας αυτές τις ποσότητες *(DR, FA)* σαν δευτερεύοντα εναλλακτικά μέτρα σύγκρισης.

2.3 Μοντέλα

Όπως αναφέρθηκε στην αρχή της ενότητας 2, ο υπολογισμός των πιθανοτήτων κλάσεων εξαρτάται από το μοντέλο που υιοθετείται. Ιδανικά κάποιος θα μπορούσε να υιοθετήσει την υποκειμενική ερμηνεία των πιθανοτήτων (subjective Bayesian) και να θεωρήσει μία κατανομή σε όλο το χώρο των μοντέλων, δηλ. ένα και μοναδικό διάνυσμα παραμέτρων όλων των πιθανών μοντέλων. Αν και αυτό μπορεί να δημιουργήσει προβλήματα υπερπροσαρμογής (overfitting), θα χρησιμοποιήσουμε εμπειρικές μεθόδους επιλογής μοντέλου προκειμένου να αποφύγουμε αυτή την πιθανή παγίδα. Η διαδικασία που ακολουθήθηκε περιγράφεται αναλυτικά στην ενότητα 3.1. Στη συνέχεια αυτή της ενότητας θα δώσουμε μία σύντομη περιγραφή των τριών τύπων μοντέλων που χρησιμοποιήθηκαν κατά τη διάρκεια αυτής της έρευνας, το *πολυ-επίπεδο perceptron (Multilayer Perceptron (MLP))*, το μοντέλο Γκαουσσιανών μειγμάτων (Gaussian Mixture Model (GMM)) και το μοντέλο Μηχανών Υποστήριξης Διανυσμάτων (Support Vector Machines (SVM)).

Ένα συγκεκριμένο MLP μπορεί να θεωρηθεί απλά σαν μία συνάρτηση $g: S \to \Omega$, όπου το g μπορεί επίσης να οριστεί σαν σύνθεση άλλων συναρτήσεων $z_i: S \to Z$. Στις περισσότερες περιπτώσεις, αυτή η ανάλυση μπορεί να γραφεί σαν $g(x) = K(w'z(x))$, όπου το $x \in S$, το w είναι ένα διάνυσμα παραμέτρων, το K είναι ένας συγκεκριμένος *πυρήνας (kernel)* και η συνάρτηση $z(x) = [z_1(x), z_2(x), \ldots]$ είναι γνωστή σαν *κρυφό επίπεδο (hidden layer)*. Για κάθε μία από αυτές τις παραμέτρους έχουμε $z_i(x) = K_i(v_i'x)$, όπου κάθε v_i είναι ένα διάνυσμα παραμέτρων, $V = [v_1, v_2, \ldots]$ είναι ο πίνακας παραμέτρων του κρυφού επιπέδου και τέλος K_i είναι ένας αυθαίρετος *πυρήνας (kernel)*. Για τη συγκεκριμένη εφαρμογή θέλουμε να χρησιμοποιήσουμε ένα MLP m σαν μοντέλο για τη δεσμευμένη πιθανότητα κλάσης δεδομένων των παρατηρήσεων δηλ.

$$P(Y = y \mid X = x, M = m), \qquad y = g(x), \tag{7.6}$$

Για το λόγο αυτό χρησιμοποιούμε ένα σιγμοειδή (sigmoid) πυρήνα για το K. Στα πειράματα θα υλοποιήσουμε τη συνάρτηση υπερβολικής εφαπτομένης

(hyperbolic tangent) σαν πυρήνα για το κρυμμένο επίπεδο, όταν υπάρχει. Στην περίπτωση που δεν υπάρχει κρυμμένο επίπεδο, θα έχουμε $z(x)=x$, οπότε και $z_i = x_i$.

Το GMM, το δεύτερο μοντέλο που χρησιμοποιήσαμε, χρησιμοποιήθηκε για να μοντελοποιήσουμε τη δεσμευμένη πυκνότητα των παρατηρήσεων για κάθε κλάση, δηλ. την:

$P(X = x \mid Y = y, M = m)$.

Αυτό μπορεί να επιτευχθεί απλά χρησιμοποιώντας για κάθε κλάση y, ένα μείγμα αποτελούμενο από ένα σύνολο μελών U_y για τη μοντελοποίηση της πυκνότητας παρατήρησης κάθε κλάσης y. Στη συνέχεια, για μία δεδομένη κλάση y η πυκνότητα σε κάθε σημείο x υπολογίζεται περιθωριοποιώντας τα μέλη του μείγματος $u \in U_y$, για την κλάση:

$$P(X = x \mid Y = y) = \sum_u P(X = x \mid U = u) P(U = u \mid Y = y),$$

όπου αφαιρέσαμε την εξάρτηση από το m για απλότητα.

Σημειώνουμε ότι η συνάρτηση πιθανότητας $p(X = x \mid U = u)$ ακολουθεί την Γκαουσσιανή (Gaussian) κατανομή, με παράμετρο Σ_u τον πίνακα συνδιακύμανσης (covariance) Σ_u, το διάνυσμα του μέσου μ_u, ενώ το $P(U = u \mid Y = y)$ είναι μία άλλη παράμετρος το *βάρος συνισταμένης (the component weight)*[4].

Τέλος, πρέπει να εκτιμήσουμε ξεχωριστά από τα δεδομένα το $P(Y = y)$, οπότε λαμβάνουμε τη δεσμευμένη πιθανότητα κλάσης δεδομένων των παρατηρήσεων

$$P(Y = y \mid X = x) = \frac{1}{Z} P(X = x \mid Y = y) P(Y = y) \tag{7.7}$$

όπου το $Z = \sum_{j \in \Omega} P(X = x \mid Y = y) P(Y = j)$ δεν εξαρτάται από το y και έχουμε και πάλι αφαιρέσει την εννοούμενη εξάρτηση από το m.

Οι δεσμευμένες πιθανότητες κλάσεις είτε από την εξίσωση (7.7) είτε από την εξίσωση (7.6), ανάλογα με το μοντέλο, μπορούν στη συνέχεια να χρησιμοποιηθούν στην εξίσωση (7.1), προκειμένου να υπολογιστεί η συνάρτηση απόφασης (7.2).

Ο αλγόριθμος SVM ([Burges, 1998], [Vapnik, 1995]), δεδομένου ενός συνόλου δεδομένων $D = \{x_i, y_i\}_{i=1}^n$, $x_i \in X, y_i \in \{-1, 1\}$, κάποια σταθερά C>0 και μία συνάρτηση $\Phi : X \to H$, απαιτεί την ελαχιστοποίηση του:

$$J(w, b, \xi) = \frac{1}{2}\|w\|^2 + C \sum_{i=1}^{n} \xi_i \tag{7.8}$$

με τους περιορισμούς:

---

[4] Αφού χρησιμοποιούμε ξεχωριστές συνισταμένες μειγμάτων για κάθε κλάση, $P(U = u \mid Y = y) = 0$, όταν $u \notin U_y$, το οποίο επίσης μας επιτρέπει να απαλλαχθούμε από την εξάρτηση από το y στη συνάρτηση πιθανότητας.

$$y_i\left(w'\Phi(x_i+b)\right)\geq 1-\xi_i \tag{7.9}$$

$$\xi_i\geq 0, \qquad \forall i\in[1,n]. \tag{7.10}$$

Τα διανύσματα x_i αντιστοιχίζονται σε ένα υψηλότερο (πιθανόν αόριστο) διάστημα διαστάσεων (dimensional space) από τη συνάρτηση Φ. Ο αλγόριθμος SVM βρίσκει ένα γραμμικό διαχωρισμό υπερεπιπέδου με ένα μέγιστο περιθώριο (marginal) σε αυτό το υψηλό διάστημα διαστάσεων. Τα σημεία που αναπαριστώνται σε αυτό το περιθώριο ονομάζονται διανύσματα υποστήριξης (support vectors).

Η παράμετρος C αναπαριστά το συμβιβασμό ανάμεσα στο μέγεθος του περιθωρίου και τον αριθμό των παραβιασμένων περιορισμών. Το πρόβλημα αυτό μπορεί να γραφεί ως εξής:

Μεγιστοποίηση του

$$L(a)=\sum_i a_i-\frac{1}{2}\sum_{i,j}a_i a_j y_i y_j \Phi(x_i)\Phi(x_j), \tag{7.11}$$

με τους περιορισμούς,

$$0\leq a_i\leq C, \qquad \forall i\in[1,n] \tag{7.12}$$

όπου a_i είναι οι πολλαπλασιαστές Lagrange που αντιστοιχούν σε κάθε περιορισμό. Πρέπει να κάνουμε δύο σημαντικές σημειώσεις. Αρχικά, ότι το a_i θα είναι μη μηδενικό μόνο για αυτά τα i που είναι διανύσματα υποστήριξης (support vectors). Ας τα αναπαραστήσουμε αυτά $s_1, s_2, \ldots, s_N$. Δεύτερον, η γνώση του Φ δεν απαιτείται, αλλά μόνο η γνώση του $\Phi(x_i)\Phi(x_j)$ για $x_i, x_j \in X$. Είναι δυνατό να γραφεί ο αλγόριθμος με τη βοήθεια της συνάρτησης πυρήνα

$$K(x_i,x_j)=\Phi(x_i)\Phi(x_j). \tag{7.13}$$

Επομένως, το τελικό μοντέλο SVM μπορεί να γραφεί σαν,

$$f'(x)=\sum_{i=1}^{N}a_i y_i K(s_i,x)+b. \tag{7.14}$$

Καθώς η ερώτηση για το πώς μπορούμε να επεκτείνουμε την ταξινόμηση με ευαισθησία στο κόστος για τις Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machines) παραμένει ένα ανοιχτό ερευνητικό θέμα [Lin, 2002] στο χώρο των βέλτιστων στατιστικών αποφάσεων, για το λόγο αυτό δεν περιλαμβάνεται ο αλγόριθμος SVM στην έρευνά μας για την ανίχνευση εισβολών με ευαισθησία στο κόστος. Χρησιμοποιούμε όμως τον αλγόριθμο SVM στη σύγκριση που πραγματοποιούμε όσον αφορά στην απόδοση των αλγόριθμων ταξινόμησης χωρίς τη χρήση κόστους στην ανίχνευση εισβολών.

3. Πειράματα Αξιολόγησης

Πραγματοποιήσαμε μία σειρά πειραμάτων αξιολόγησης τόσο για ενσύρματη όσο και ασύρματη δικτυακή κυκλοφορία. Για κάθε κατηγορία δικτυακής κυκλοφορίας εξετάσαμε την απόδοση που παρουσιάζουν τέσσερις διαφορετικοί αλγόριθμοι ταξινόμησης: το MLP, ο Γραμμικός (Linear) ταξινομητής, ο

ταξινομητής GMM με διαγώνιους πίνακες συνδιακύμανσης και το μοντέλο απλοϊκού ταξινομητή (Naïve Bayes) (GMM με ένα Γκαουσιανό μείγμα). Επιπλέον, εξετάσαμε την απόδοση του αλγόριθμου SVM στην ανίχνευση εισβολών χωρίς τη χρήση κόστους.

Για την προτεινόμενη προσέγγιση ανίχνευσης εισβολών με ευαισθησία στο κόστος αναμενόταν ότι η χρήση των πινάκων κόστους στη λήψη αποφάσεων θα είχε σαν αποτέλεσμα χαμηλότερο κόστος από το να μη χρησιμοποιούνται. Μία ιδιαίτερα ενδιαφέρουσα ερώτηση που ερευνούμε είναι πως η απόκλιση των κατανομών στα σύνολα δεδομένων εκπαίδευσης και ελέγχου επηρεάζει το αναμενόμενο κόστος για ένα συγκεκριμένο πίνακα κόστους. Επιπλέον, εξετάζουμε πως οι ρυθμοί λανθασμένων συναγερμών και ανίχνευσης εισβολών αλλάζουν όταν αλλάζουμε το σχετικό κόστος των λανθασμένων συναγερμών και των λανθασμένων αρνητικών συναγερμών. Για την πραγματοποίηση των πειραμάτων χρησιμοποιήσαμε τη βιβλιοθήκη Torch [Torch, 2004].

3.1 Ρύθμιση Παραμέτρων

Προκειμένου να πραγματοποιήσουμε την καλύτερη τυφλή επιλογή παραμέτρων για κάθε μοντέλο ακολουθήσαμε τη διαδικασία δεκαπλής διασταυρωμένης επικύρωσης (10 fold cross – validation). Για το μοντέλο MLP ρυθμίσαμε τρεις παραμέτρους τον ρυθμό εκμάθησης (learning rate (η)), τις επαναλήψεις (iterations (T)) και τον αριθμό των κρυφών επιπέδων (hidden layers (n_h)). Κρατώντας σταθερό το n_h (αρχικά ίσο με 0) επιλέξαμε το κατάλληλο η με τιμές που κυμαίνονταν από 0.0001 έως 0.1 με βήμα 0.1 και το κατάλληλο T επιλέγοντας ανάμεσα σε 10, 100, 500 και 1000. Για την επιλογή του κατάλληλου n_h, έχοντας επιλέξει το κατάλληλο η και το κατάλληλο T, εξετάσαμε διάφορες τιμές για το n_h και επιλέξαμε την καλύτερη από τις 10, 20, 40, 60, 80, 100, 120, 140, 160, 320. Επιπλέον, χρησιμοποιήσαμε το μοντέλο χωρίς κρυφά επίπεδα (n_h) για το *Γραμμικό (Linear)* μοντέλο.

Για το μοντέλο GMM ρυθμίσαμε επίσης τρεις παραμέτρους το *κατώφλι (threshold (θ))*, τον αριθμό των επαναλήψεων (T) και τον αριθμό των Γκαουσσιανών μειγμάτων (n_g). Κρατώντας σταθερό το n_g (ίσο με 20) επιλέξαμε το κατάλληλο θ με τιμές που κυμαίνονταν από 0.1 έως 0.0001 με βήμα 0.1 και το κατάλληλο T με τιμές 25, 100, 500 και 1000. Για την επιλογή του κατάλληλου n_g, έχοντας επιλέξει το κατάλληλο θ και το κατάλληλο T, εξετάσαμε διάφορες τιμές για το n_g και επιλέξαμε την καλύτερη από τις 10, 20, 40, 60, 80, 100, 120, 140, 160 και 320. Επιπλέον, χρησιμοποιήσαμε το μοντέλο GMM με ένα Γκαουσσιανό μείγμα (n_g) σαν μοντέλο Naïve Bayes.

Για το μοντέλο SVM χρησιμοποιήσαμε την τετραγωνική εκθετική συνάρτηση πυρήνα: $k(x_i, x_j) = exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right)$

για ένα σύνολο δεδομένων $D = \{x_i, y_i\}_{i=1}^{n}$, $x_i \in X, y_i \in \{-1,1\}$.
Ρυθμίσαμε δύο παραμέτρους το std που καθορίζει το διάστημα της διακύμανσης σ και τη σταθερά C.
Εξετάσαμε για το std και το C τις τιμές 0.1, 1, 10, 100 και 1000 και επιλέξαμε τον ιδανικό συνδυασμό τους που ελαχιστοποιεί το αναμενόμενο κόστος.

3.2 Δεδομένα Ενσύρματης Δικτυακής Κίνησης

3.2.1 Σύνολα Δεδομένων

Για την εκπαίδευση των ταξινομητών και την εφαρμογή τους σε ενσύρματα δίκτυα χρησιμοποιήσαμε το σύνολο δεδομένων 10% KDD, το οποίο περιγράφεται αναλυτικά στην παράγραφο 5.1 του Κεφαλαίου 4. Στη συνέχεια πραγματοποιήσαμε έλεγχο του εκπαιδευμένου μοντέλου με σύνολα δεδομένων ελέγχου. Σκοπός ήταν να προβλέψουμε την κλάση ("φυσιολογικά" δεδομένα ή κάποια από τις επιθέσεις για κάθε εγγραφή-σύνδεση του συνόλου δεδομένων ελέγχου). Συγκεκριμένα, για τον έλεγχο του εκπαιδευμένου μοντέλου χρησιμοποιήσαμε δύο σύνολα δεδομένων. Το πρώτο σύνολο ελέγχου δοκιμής είναι το σύνολο δεδομένων ελέγχου της βάσης δεδομένων KDD το οποίο περιέχει 311,029 συνδέσεις. Είναι σημαντικό να σημειώσουμε εδώ ότι τα δεδομένα δοκιμής δεν παρουσιάζουν την ίδια κατανομή πιθανότητας με αυτά των δεδομένων εκπαίδευσης. Επίσης, το σύνολο αυτό των δεδομένων ελέγχου περιλαμβάνει κάποιους συγκεκριμένους τύπους επιθέσεων που δεν περιλαμβάνονται στα δεδομένα εκπαίδευσης. Συγκεκριμένα, υπάρχουν 17 νέοι τύποι επιθέσεων που δεν παρουσιάζονται στο σύνολο δεδομένων εκπαίδευσης. Οι υπόλοιποι τύποι επιθέσεων υπάρχουν στο σύνολο δεδομένων ελέγχου με διαφορετικά ποσοστά σε σχέση με τις αντίστοιχες κατηγορίες στα δεδομένα εκπαίδευσης. Υπάρχουν τέσσερις νέοι τύποι επιθέσεων U2R που αντιστοιχούν στο 92.90% (189/228) της κλάσης U2R στο σύνολο δεδομένων ελέγχου. Επιπλέον υπάρχουν επτά νέοι τύποι επιθέσεων R2L που αντιστοιχούν στο 63% (10196/16189) της κλάσης R2L στο σύνολο δεδομένων ελέγχου. Υπάρχουν τέσσερις νέοι τύποι επιθέσεων DoS στο σύνολο δεδομένων ελέγχου που αντιστοιχούν στο 2.85% (6555/229853) της κλάσης DoS και δύο νέες επιθέσεις Probe που αντιστοιχούν στο 42.94% (1789/4166) της κλάσης Probe στο σύνολο δεδομένων ελέγχου.

Στον Πίνακα 7.1 φαίνεται η αναλογία εγγραφών επίθεσης και φυσιολογικής συμπεριφοράς του πρώτου συνόλου δεδομένων ελέγχου. Το δεύτερο σύνολο δεδομένων ελέγχου που χρησιμοποιήσαμε προκύπτει από το αντίστοιχο πρώτο αφαιρώντας όλους τους νέους τύπους επιθέσεων (που δεν περιλαμβάνονται στο σύνολο δεδομένων εκπαίδευσης). Στον Πίνακα 7.2 φαίνεται η αναλογία εγγραφών επίθεσης και φυσιολογικής συμπεριφοράς του δεύτερου συνόλου δεδομένων ελέγχου. Ενώ στον Πίνακα 7.3 φαίνονται οι αναλογίες των εγγραφών επίθεσης των νέων τύπων επιθέσεων που περιλαμβάνονται μόνο στο πρώτο σύνολο δεδομένων ελέγχου.

Πίνακας 7. 1 Σύνολο Δεδομένων Ελέγχου 1 που Περιλαμβάνει Νέες Επιθέσεις

Σύνολο Δεδομένων Δοκιμής 1												
DOS	apache2	794	R2L	ftp write	3	PROBE	ipsweep	306	U2R	buffer overflow	22
	neptune	58001		guess passwd	4367		mscan	1053		httptunnel	158
	land	9		imap	1		nmap	84		loadmodule	2
	mailbomb	5000		multihop	18		portsweep	354		perl	2
	back	1098		named	17		saint	736		ps	16
	pod	87		spy	2		satan	1633		rootkit	13
	processtable	759		phf	2					sqlattack	2
	teardrop	12		sendmail	17					xterm	13
	smurf	164091		snmpgetattack	7741						
	udpstorm	2		snmpguess	2406						
				warezmater	1602						
				worm	2						
				xlock	9						
				xsnoop	4						
	Συνολικές DoS	**229853**		**Συνολικές R2L**	**16189**		**Συνολικές Probe**	**4166**		**Συνολικές U2R**	**228**
Σύνολο Εγγραφών Επίθεσης		250436										
Συνολικές Εγγραφές Φυσιολογικής Συμπεριφοράς		60593										

Πίνακας 7. 2 Σύνολο Δεδομένων 2 Ελέγχου Δεν Περιλαμβάνει Άγνωστες Επιθέσεις)

Σύνολο Δεδομένων Δοκιμής 2 (χωρίς)												
DOS	neptune	58001	R2L	ftp write	3	PROBE	ipsweep	306	U2R	buffer overflow	22
	land	9		guess passwd	4367		nmap	84		loadmodule	2
	back	1098		imap	1		portweep	354		perl	2
	pod	87		multihop	18		satan	1633		rootkit	13
	teardrop	12		phf	2						
	smurf	164091		warezmaster	1602						
	Συνολικές DoS	**223298**		**Συνολικές R2L**	**5993**		**Συνολικές Probe**	**2377**		**Συνολικές U2R**	**39**
Σύνολο Εγγραφών Επίθεσης		231707										
Συνολικές Εγγραφές Φυσιολογικής Συμπεριφοράς		60593										

Πίνακας 7. 3 Σύνολο Νέων Τύπων Επιθέσεων

Νέες επιθέσεις												
DoS	apache2	794	R2L	Named	17	Probe	mscan	1053	U2R	httptunnel	158
	Mailbomb	5000		sendmail	17		saint	736		ps	16
	Process table	759		snmpgetattack	7741					sqlattack	2
	Udpstorm	2		snmpguess	2046					xterm	13
				worm	2						
				xlock	9						
				xsnoop	4						
	Συνολικές DoS	6555		Συνολικές R2L	10196		Συνολικές Probe	1789		Συνολικές U2R	189
Συνολικές επιθέσεις			18729									

3.2.2 Προ-επεξεργασία Δεδομένων

Χρησιμοποιήθηκαν και τα 41 πεδία του συνόλου δεδομένων KDD [KDD, 1999] (αναλυτική περιγραφή των πεδίων στο Παράρτημα Α). Τα πεδία των συνόλων δεδομένων KDD έχουν διάφορους τύπους –συνεχείς, και διακριτούς με σημαντικά κυμαινόμενο εύρος τιμών. Οι περισσότεροι αλγόριθμοι ταξινόμησης δεν μπορούν να επεξεργαστούν δεδομένα σε αυτή τη μορφή. Για το λόγο αυτό οι διακριτές τιμές των αντίστοιχων πεδίων μετατράπηκαν σε συνεχείς τιμές ακολουθώντας της διαδικασία της κωδικοποίησης one-hot *(one-hot encoding)* [Hastie, 2003] που χρησιμοποιείται ευρέως στη βιβλιογραφία. Σύμφωνα με αυτή την κωδικοποίηση εάν έχουμε μία διακριτή μεταβλητή, με τιμές $x_1, x_2 \ldots, x_n$, τότε μπορούμε να αντιστοιχήσουμε αυτές τις τιμές σε ένα n-διάστατο διάνυσμα της μορφής $[0, 0, \ldots, 0, 1, 0, \ldots, 0]$, δηλ. αντιστοιχεί κάθε τιμή i σε ένα διάνυσμα x έτσι ώστε $y_i=1$ και $y_j=0$ για όλα τα $j \neq i$.

Τα ονόματα των επιθέσεων αντιστοιχήθηκαν ως εξής 0 για "φυσιολογικά" δεδομένα, 1 για δεδομένα Probe, 2 για δεδομένα DoS, 3 για δεδομένα U2R, και 4 για δεδομένα R2L. Επιπλέον, προκειμένου να αποφύγουμε μεγάλη επίδραση κάποιων τιμών πεδίων είναι απαραίτητο να κανονικοποιήσουμε τα δεδομένα εισόδου στους αλγόριθμους ταξινόμησης. Τα κανονικοποιήσαμε με μέσο μηδέν και διακύμανση ένα μία τεχνική που παράγει πολύ καλά αποτελέσματα στις περισσότερες περιπτώσεις όπως αναφέρεται στην βιβλιογραφία.

3.2.3 Πίνακες Κόστους

Δημιουργήσαμε για κάθε αλγόριθμο ταξινόμησης δύο μοντέλα. Ένα μοντέλο στο οποίο χρησιμοποιούμε τον Πίνακα κόστους 7.4 όπως έχει καθοριστεί για το σύνολο δεδομένων KDD 1999 [Elkan, 1999] ως ακολούθως και ένα μοντέλο στο οποίο δεν υπάρχει διαφορετικό κόστος για τις λανθασμένες ταξινόμησης επιθέσεων σαν "φυσιολογική" συμπεριφορά ή σαν διαφορετικός τύπος επίθεσης (Πίνακας κόστους 7.5).

Πίνακας 7. 4 Πίνακας Κόστους για το Σύνολο Δεδομένων KDD 99

Πραγματική / Πρόβλεψη	Φυσιολογική	Probe	DoS	U2R	R2L
Φυσιολογική	0	1	2	2	2
Probe	1	0	2	2	2
DoS	2	1	0	2	2
U2R	3	2	2	0	2
R2L	4	2	2	2	0

Πίνακας 7. 5 Πίνακας Κόστους για το Σύνολο Δεδομένων KDD 99

Πραγματική / Πρόβλεψη	Φυσιολογική	Probe	DoS	U2R	R2L
Φυσιολογική	0	1	1	1	1
Probe	1	0	1	1	1
DoS	1	1	0	1	1
U2R	1	1	1	0	1
R2L	1	1	1	1	0

Επιπλέον, ορίσαμε έναν αυθαίρετο πίνακα κόστους προκειμένου να εξετάσουμε πως αλλάζει το αναμενόμενο κόστος όταν αυξάνεται το σχετικό κόστος για κάθε λάθος ταξινόμηση μίας επίθεσης σαν "φυσιολογική" δικτυακή κίνηση (Πίνακας 7.6). Ορίσαμε λοιπόν στον πίνακα κόστους, το κόστος ταξινόμησης αν μία εγγραφή "φυσιολογικής" δικτυακής κυκλοφορίας ταξινομηθεί σαν επίθεση να είναι ίσο με *a* ενώ το κόστος αν μία επίθεση ταξινομηθεί σαν φυσιολογική συμπεριφορά να είναι ίσο με 1. Πραγματοποιήσαμε μία σειρά πειραμάτων με το *a* να παίρνει τιμές από 1 έως 10. Τα πειράματα πραγματοποιήθηκαν για τον αλγόριθμο MLP με ταξινόμηση πολλαπλών κλάσεων (multi-class) δηλαδή θεωρώντας ότι έχουμε τέσσερις κλάσεις επιθέσεων και μία κλάση "φυσιολογικής" συμπεριφοράς. Επιλέξαμε το συγκεκριμένο αλγόριθμο καθώς παρουσιάζει το μικρότερο λάθος ταξινόμησης.

Πίνακας 7. 6 Πίνακας Κόστους για το Σύνολο Δεδομένων KDD 99

Πραγματική / Πρόβλεψη	Φυσιολογική	Probe	DoS	U2R	R2L
Φυσιολογική	0	1	1	1	1
Probe	a	0	0	0	0
DoS	a	0	0	0	0
U2R	a	0	0	0	0
R2L	a	0	0	0	0

Αν υποθέσουμε ότι έχουμε N επιθέσεις και $p(y_i)$ είναι η πιθανότητα της επίθεσης i ενώ $p(y_0)$ είναι η πιθανότητα για τη "φυσιολογική" δικτυακή κυκλοφορία, τότε με χρήση του παραπάνω πίνακα κόστους το αναμενόμενο κόστος για μία λανθασμένη ταξινόμηση μίας επίθεσης i σαν "φυσιολογική" δικτυακή κίνηση είναι:

$$ap(y_1) + ap(y_2) + ... + ap(y_N) = a\sum_{i=1}^{N} p(y_i),$$

Στην προκειμένη περίπτωση που έχουμε τέσσερις επιθέσεις τότε το αναμενόμενο κόστος για μία λανθασμένη ταξινόμηση μίας επίθεσης i σαν "φυσιολογική" δικτυακή κίνηση είναι:

$$ap(y_1) + ap(y_2) + ap(y_3) + ap(y_4) = a\sum_{i=1}^{4} p(y_i).$$

Ενώ εάν αποφασίσουμε ότι μία εγγραφή που αντιστοιχεί σε φυσιολογική δικτυακή κυκλοφορία είναι επίθεση, τότε το αναμενόμενο κόστος είναι:

$$1 * p(y_0) + 0 * \sum_{i=1}^{N} p(y_i) = p(y_0).$$

Επομένως όταν ο ταξινομητής προβλέπει μία κλάση επίθεσης τότε το αναμενόμενο κόστος θα είναι το ίδιο ανεξάρτητα από την επίθεση που προβλέπει.

3.2.4 Παράμετροι Αλγόριθμων Ταξινόμησης

Για την επιλογή των καλύτερων παραμέτρων σαν μέτρο σύγκρισης χρησιμοποιήθηκε το κόστος που δίνεται από την εξίσωση 7.3. Ακολουθώντας τη διαδικασία ρύθμισης παραμέτρων που περιγράφεται στην ενότητα 3.1 για το σύνολο δεδομένων 10% KDD (ενότητα 5.1 Κεφάλαιο 4) καταλήξαμε στις παραμέτρους που φαίνονται στον Πίνακα 7.7.

Πίνακας 7. 7 Παράμετροι Συνόλου Δεδομένων Εκπαίδευσης για Μοντέλα Ταξινόμησης με Κόστος.

	Χωρίς κόστος	Με κόστος
MLP	η=0.001	η=0.001
	T=100	T=500
	n_h=160	n_h=140
Linear	η=0.001	η=0.001
	T=100	T=500
	n_h=160	n_h=140
GMM	θ=0.0001	θ=0.1
	T=1000	T=1000
	n_g=120	n_g=320
Naïve Bayes	θ=0.0001	θ=0.1
	T=1000	T=1000
	n_g=1	n_g=1

3.2.5 Αποτελέσματα Πειραμάτων Αξιολόγησης

Α. Αποτελέσματα Ταξινόμησης με τη Χρήση Κόστους

Αξιολογήσαμε κάθε αλγόριθμο τόσο με χρήση πίνακα κόστους όσο και χωρίς τη χρήση πίνακα κόστους για τη λήψη αποφάσεων. Στον Πίνακα 7.8 παρουσιάζονται τα αποτελέσματα για το Σύνολο Δεδομένων Ελέγχου 1, ενώ στον Πίνακα 7.9 παρουσιάζονται τα αποτελέσματα για το Σύνολο Δεδομένων Ελέγχου 2. Και στις δύο περιπτώσεις, μ είναι το εμπειρικό κόστος, ενώ χαμηλό και υψηλό είναι οι τιμές ορίων του διαστήματος εμπιστοσύνης 99%. Το διάστημα εμπιστοσύνης εκτιμήθηκε χρησιμοποιώντας 1000 δείγματα bootstrap [Efron, 1994] (βλ. Παράρτημα Γ) των Συνόλων Δεδομένων Ελέγχου.

Είναι ξεκάθαρο ότι το μέσο εμπειρικό κόστος για το Σύνολο Δεδομένων Ελέγχου 1 είναι πολύ υψηλότερο από το αντίστοιχο κόστος για το Σύνολο Δεδομένων Ελέγχου 2. Αυτό είναι αναμενόμενο, αφού το Σύνολο Δεδομένων Ελέγχου 1 περιλαμβάνει τύπους επιθέσεων που δεν περιλαμβάνονται στο σύνολο δεδομένων εκπαίδευσης. Είναι επίσης προφανές ότι οι ταξινομητές Γραμμικός (Linear) και GMM και οι δύο επιτυγχάνουν καλύτερα αποτελέσματα όταν χρησιμοποιούμε τον πίνακα κόστους για να λάβουμε αποφάσεις. Παρόλα αυτά, αυτό δεν ισχύει για τους ταξινομητές MLP και απλοϊκού μοντέλου (Naive Bayes). Αυτή η αδυναμία του ταξινομητή Naïve Bayes μπορεί να δικαιολογηθεί από το γεγονός ότι ο ταξινομητής Naïve Bayes υποθέτει ότι όλα τα πεδία του συνόλου δεδομένων εκπαίδευσης είναι ανεξάρτητα. Ο λόγος για τη συμπεριφορά του ταξινομητή MLP δεν είναι απόλυτα ξεκάθαρος. Μία πιθανή περίπτωση είναι ότι οι πιθανότητες που το μοντέλο παράγει σαν έξοδο δεν αναπαριστούν με ακρίβεια την αβεβαιότητα της ταξινόμησης, π.χ. ο ταξινομητής είναι "πολύ βέβαιος" λόγω της εκπαίδευσης μέγιστης πιθανότητας. Παρόλα αυτά, παρατηρούμε ότι η απόδοση του μοντέλου MLP είναι πολύ κοντά με την

απόδοση του μοντέλου GMM με κόστος. Αυτή η υπόθεση είναι συνεπής με το γεγονός ότι η απόδοση του ταξινομητή MLP είναι μεν πολύ κοντά στην απόδοση του μοντέλου GMM με κόστος για το Σύνολο Δεδομένων Ελέγχου 1, αλλά σημαντικά χειρότερη από το Σύνολο Δεδομένων Ελέγχου 2.

Πίνακας 7. 8 Αποτελέσματα για το Σύνολο Δεδομένων Ελέγχου 1

	Χωρίς Κόστος			Με Κόστος		
	χαμηλό	μ	υψηλό	χαμηλό	μ	υψηλό
MLP	0.2384	**0.2427**	0.2472	0.2390	**0.2431**	0.2476
Linear	0.2425	**0.2467**	0.2511	0.2414	**0.2452**	0.2489
GMM	0.2497	**0.2538**	0.2578	0.2378	**0.2420**	0.2457
Naïve Bayes	0.3786	**0.3829**	0.3871	0.5304	**0.5400**	0.5353

Πίνακας 7. 9 Αποτελέσματα για το Σύνολο Δεδομένων Ελέγχου 2

	Χωρίς Κόστος			Με Κόστος		
	χαμηλό	μ	υψηλό	χαμηλό	μ	υψηλό
MLP	0.0711	**0.0736**	0.0759	0.0713	**0.0739**	0.0765
Linear	0.0735	**0.0761**	0.0784	0.0716	**0.074**	0.0763
GMM	0.0821	**0.0845**	0.0869	0.0686	**0.071**	0.0734
Naïve Bayes	0.2173	**0.2204**	0.2231	0.3733	**0.3775**	0.3817

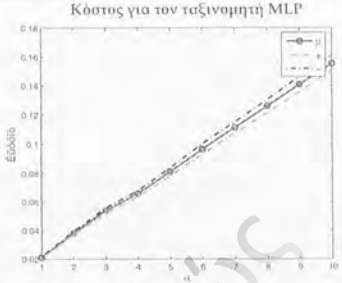
Επιπλέον, πραγματοποιήσαμε μία σειρά πειραμάτων για τον ταξινομητή MLP, αφού αυτός παρουσιάζει το χαμηλότερο λάθος ταξινόμησης, για τον αυθαίρετο πίνακα κόστους 7.6 που περιγράφεται στην ενότητα 3.2.3. Εξετάσαμε πώς αλλάζει η απόδοση του ταξινομητή MLP όταν αυξάνουμε το κόστος των λανθασμένων θετικών συναγερμών σε σχέση με τους λανθασμένους αρνητικούς συναγερμούς. Χρησιμοποιήσαμε και πάλι τη μεθοδολογία bootstrap [Efron, 1994] προκειμένου να λάβουμε διαστήματα εμπιστοσύνης για τα αποτελέσματα.

Στο Σχήμα 1 (α) και (β) η μεσαία γραμμή αναπαριστά το αναμενόμενο κόστος όπως εκτιμήθηκε για τα Σύνολα Δεδομένων Ελέγχου 1 και 2 αντίστοιχα. Οι περιβάλλουσες γραμμές υποδηλώνουν το διάστημα εμπιστοσύνης 99% του αναμενόμενου κόστους όπως αυτό εκτιμήθηκε από τα δείγματα bootstrap [Efron, 1994] (βλ. Παράρτημα Γ). Από το Σχήμα 1 (α) και το Σχήμα 1 (β), είναι ξεκάθαρο ότι το αναμενόμενο κόστος για τα Σύνολα Δεδομένων Ελέγχου 1 και 2 αντίστοιχα, αυξάνεται γραμμικά με το άλφα (α), το οποίο υποδηλώνει την καλή συμπεριφορά του ταξινομητή MLP. Στο Σχήμα 1 (γ) και το Σχήμα 1 (δ) παρατηρούμε το ρυθμό ανίχνευσης (DR) για κάθε τύπο επίθεσης για τα Σύνολα Δεδομένων Ελέγχου 1 και 2 αντίστοιχα. Ο ρυθμός ανίχνευσης (DR) για όλες τις επιθέσεις είναι καλύτερος για το Σύνολο Δεδομένων Ελέγχου 2, ενώ υπάρχει μία αύξηση του DR για όλους τους τύπους επιθέσεων και για τα δύο Σύνολα Δεδομένων Ελέγχου. Επιπλέον, παρατηρούμε μία σημαντική αύξηση του ρυθμού ανίχνευσης για τις επιθέσεις που περιλαμβάνονται στο Σύνολο Δεδομένων εκπαίδευσης, αυτό δεν ισχύει για τις νέες επιθέσεις, ειδικά για τις επιθέσεις R2L. Το DR για τις επιθέσεις DoS και Probe παρουσιάζει μία μικρή αύξηση. Ενώ για τις επιθέσεις U2R και το σύνολο Δεδομένων Ελέγχου 1 το DR κυμαίνεται από

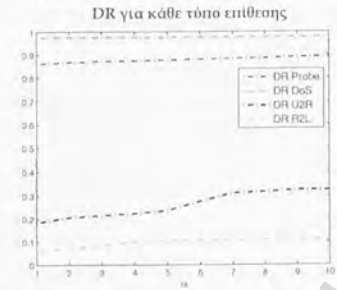
0.184 σε 0.325 μία αύξηση της τάξης του 14.1%. Για τις επιθέσεις U2R και το Σύνολο Δεδομένων Ελέγχου 2 παρατηρούμε επίσης μία σημαντική αύξηση του DR από 0.615 σε 0.82, μία αύξηση της τάξης του 20%. Για τις επιθέσεις R2L και το Σύνολο Δεδομένων Ελέγχου 1 υπάρχει μία αύξηση του DR από 0.06 σε 0.108, μία αύξηση της τάξης του 10.2%. Για τις επιθέσεις R2L και το Σύνολο Δεδομένων Ελέγχου 2, το DR κυμαίνεται από 0.163 σε 0.297, μία αύξηση της τάξης του 13.4%.

Στο Σχήμα 1 (ε) παρατηρούμε ότι ο μέσος ρυθμός ανίχνευσης (DR) παρουσιάζει μία μικρή αύξηση από 0.913 σε 0.919 για το Σύνολο Δεδομένων Ελέγχου 1 και από 0.977 σε 0.98 για το Σύνολο Δεδομένων Ελέγχου 2. Στο Σχήμα 1 (ζ) απεικονίζεται πως επηρεάζεται ο ρυθμός λανθασμένων συναγερμών από την αύξηση του κόστους *(a)* των λανθασμένων θετικών συναγερμών σε σχέση με αυτό των λανθασμένων αρνητικών συναγερμών. Παρατηρούμε μία μικρή αύξηση από 0.016 σε 0.018, δηλαδή μία αύξηση της τάξης του 0.2%. Ο ρυθμός των λανθασμένων συναγερμών (FA) είναι ο ίδιος και για τα δύο Σύνολα Δεδομένων αφού ο αριθμός των "φυσιολογικών" συνδέσεων είναι ο ίδιος και για τα δύο Σύνολα Δεδομένων. Σαν συμπέρασμα, παρατηρούμε ότι ο ρυθμός ανίχνευσης (DR) αυξήθηκε σημαντικά για τις επιθέσεις U2R (20%) και R2L (13.4%) για το Σύνολο Δεδομένων Ελέγχου 2, αλλά *όχι* για νέες επιθέσεις σε αυτές τις κατηγορίες. Σε κάθε περίπτωση, η αύξηση του ρυθμού λανθασμένων συναγερμών (FA) είναι της τάξης μόνο 0.2%

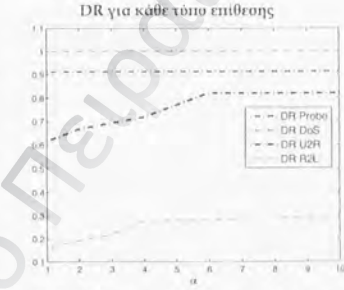
(α) Το αναμενόμενο κόστος για το Σύνολο Δεδομένων Ελέγχου 1.



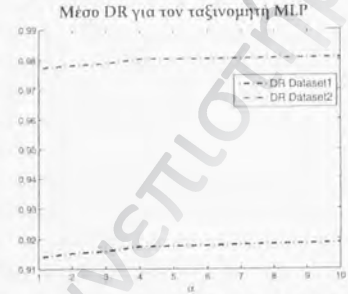
(β) Το αναμενόμενο κόστος για το Σύνολο Δεδομένων Ελέγχου 2.



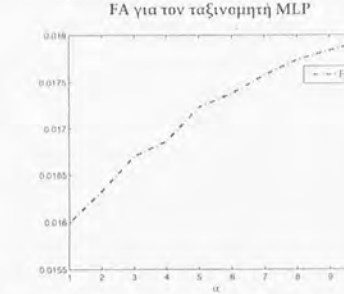
(γ) Το DR για κάθε τύπο επίθεσης για το Σύνολο Δεδομένων Ελέγχου 1.



(δ) Το DR για κάθε τύπο επίθεσης για το για το Σύνολο Δεδομένων Ελέγχου 2.



(ε) Το μεσο DR για κάθε Σύνολο Δεδομένων Ελέγχου



(ζ) Το FA για τα Σύνολα Δεδομένων Ελέγχου

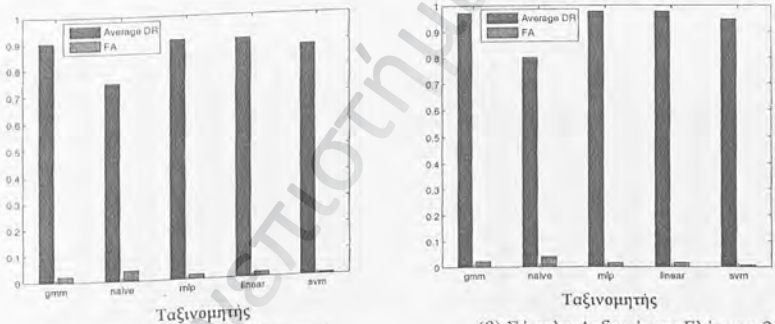
Σχήμα 7. 1 Η Επίδραση του *a* στην Απόδοση του Μοντέλου MLP.

Β. Αποτελέσματα Ταξινόμησης χωρίς τη Χρήση Κόστους

Στη συνέχεια εξετάζουμε την απόδοση του κάθε αλγορίθμου όσον αφορά στο ρυθμό ανίχνευσης εισβολών (DR) και στο ρυθμό λανθασμένων συναγερμών (FA) χωρίς τη χρήση κόστους. Αυτή τη φορά η ταξινόμηση έγινε με πίνακα κόστους τον Πίνακα 7.5 ενώ οι παράμετροι που χρησιμοποιήθηκαν οι ακόλουθες (Πίνακας 7.10)

Πίνακας 7. 10 Παράμετροι Συνόλου Δεδομένων Εκπαίδευσης για τα Μοντέλα Ταξινόμησης Χωρίς Κόστος

	Χωρίς κόστος
MLP (5 class)	η=0.001
	T=100
	n_h=160
Linear (5 class)	η=0.001
	T=100
	n_h=160
GMM (5 class)	θ=0.0001
	T=1000
	n_g=120
Naïve Bayes (5 class)	θ=0.0001
	T=1000
	n_g=1
SVM (5 class)	std=100
	c=1000



(α) Σύνολο Δεδομένων Ελέγχου 1 (με νέες επιθέσεις)

(β) Σύνολο Δεδομένων Ελέγχου 2 (χωρίς νέες επιθέσεις)

Σχήμα 7. 2 Μέσος Ρυθμός Ανίχνευσης Εισβολών (DR) και Ρυθμός Λανθασμένων Συναγερμών για Κάθε Ταξινομητή.

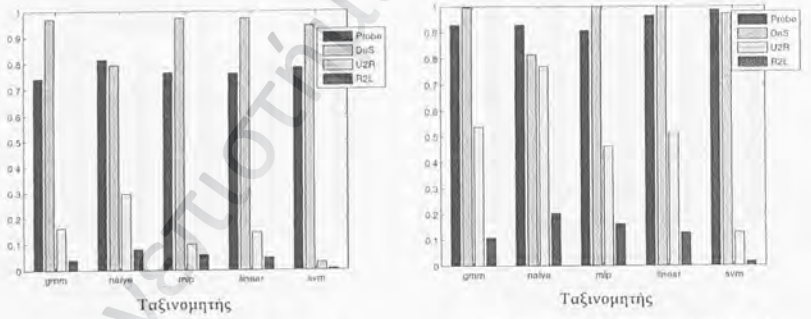
Στο σχήμα 7.2 παρουσιάζεται ο μέσος ρυθμός ανίχνευσης εισβολών (DR) και ο ρυθμός λανθασμένων συναγερμών (FA) για κάθε ταξινομητή (MLP, Linear, GMM, Naïve Bayes, SVM) για το Σύνολο Δεδομένων Δοκιμής 1 (που περιλαμβάνει νέες επιθέσεις) (Σχήμα 7.2 (α)) και το Σύνολο Δοκιμής 2 (που δεν περιλαμβάνει νέες επιθέσεις) (Σχήμα 7.2 (β)). Από τα σχήματα 7.2 (α) και (β) είναι προφανές ότι ο ρυθμός ανίχνευσης (DR) είναι καλύτερος για το σύνολο δεδομένων Δοκιμής 2 (που δεν περιλαμβάνει νέες επιθέσεις οι οποίες δεν

περιλαμβάνονται στο σύνολο δεδομένων εκπαίδευσης). Αντίστοιχα και ο ρυθμός λανθασμένων συναγερμών (FA) είναι χαμηλότερος.

Για το Σύνολο Δεδομένων Δοκιμής 1 (Σχήμα 7.2 (α)) ο υψηλότερος μέσος ρυθμός ανίχνευσης εισβολών (DR) επιτυγχάνεται με τον ταξινομητή MLP και είναι ίσος με 0.91 (91%) ενώ ο χαμηλότερος μέσος ρυθμός ανίχνευσης εισβολών (DR) είναι ίσος με 0.75 (75%) και παρουσιάζεται με τον αλγόριθμο Naïve Bayes.

Αντίστοιχα, για το Σύνολο Δεδομένων Δοκιμής 2 (Σχήμα 7.2 (β)) ο υψηλότερος μέσος ρυθμός ανίχνευσης εισβολών (DR) επιτυγχάνεται με τον ταξινομητή MLP και είναι ίσος με 0.98 (98%) ενώ ο χαμηλότερος ρυθμός ανίχνευσης εισβολών (DR) είναι ίσος με 0.80 (80%) και παρουσιάζεται με τον αλγόριθμο Naïve Bayes. Αντίστοιχα ο χαμηλότερος ρυθμός λανθασμένων συναγερμών (FA) είναι ίσος με 0.006 (0.6%) και επιτυγχάνεται με τον ταξινομητή MLP, ενώ ο υψηλότερος ρυθμός λανθασμένων συναγερμών (FA) που παρουσιάζεται με τη χρήση του ταξινομητή Naïve Bayes είναι ίσος με 0.039 (3.9%) και για τα δύο σύνολα δεδομένων ελέγχου αφού οι εγγραφές φυσιολογικής συμπεριφοράς είναι οι ίδιες και για τα δύο σύνολα.

Κρίνεται λοιπόν ο αλγόριθμος MLP πιο αποτελεσματικός για την ανίχνευση των τεσσάρων επιθέσεων κατά μέσο όρο, ενώ ο αλγόριθμος SVM επιτυγχάνει ιδιαίτερα χαμηλό αριθμό λανθασμένων συναγερμών και αρκετά ικανοποιητικό ρυθμό ανίχνευσης εισβολών και ίσο με 0.946 (94.6%).



(α) Σύνολο Δεδομένων Δοκιμής 1 (με νέες επιθέσεις)

(β) Σύνολο Δεδομένων Δοκιμής 2 (χωρίς νέες επιθέσεις)

Σχήμα 7. 3 Ρυθμός Ανίχνευσης Εισβολών (DR) για Κάθε Τύπο Επίθεσης και για Κάθε Ταξινομητή.

Στο Σχήμα 7.3 παρουσιάζεται ο ρυθμός ανίχνευσης εισβολών (DR) για κάθε τύπο επίθεσης (Probe, DoS, R2L, U2R) και για κάθε ταξινομητή (MLP, Linear, GMM, Naïve Bayes και SVM) για το Σύνολο Δεδομένων Δοκιμής 1 (που περιλαμβάνει νέες επιθέσεις) (Σχήμα 7.3 (α)) και το Σύνολο Δοκιμής 2 (που δεν περιλαμβάνει νέες επιθέσεις) (Σχήμα 7.3 (β)).

Για το Σύνολο Δεδομένων Δοκιμής 1 (Σχήμα 7.3 (α)) ο υψηλότερος ρυθμός ανίχνευσης εισβολών (DR) για την επίθεση Probe επιτυγχάνεται με τον ταξινομητή Naïve Bayes και είναι ίσος με 0.813 (81.3%), για την επίθεση DoS επιτυγχάνεται με τον ταξινομητή GMM και είναι ίσος με 0.97 (97%), για την επίθεση U2R επιτυγχάνεται με τον ταξινομητή Naïve Bayes και είναι ίσος με 0.293 (29.3%) και για την επίθεση R2L επιτυγχάνεται και πάλι με τον ταξινομητή Naïve Bayes και είναι ίσος με 0.079 (7.9%). Για το Σύνολο Δεδομένων Δοκιμής 2 (Σχήμα 7.3 (β)) ο υψηλότερος ρυθμός ανίχνευσης εισβολών (DR) για την επίθεση Probe επιτυγχάνεται με τον ταξινομητή Linear και είναι ίσος με 0.965, για την επίθεση DoS επιτυγχάνεται με τον ταξινομητή MLP και είναι ίσος με 0.999 και για τις επιθέσεις U2R και R2L επιτυγχάνεται με τον ταξινομητή Naïve Bayes και είναι ίσος με 0.769 (76.9%) και 0.202 (20.2%) αντίστοιχα.

Παρατηρούμε λοιπόν ότι και για τα δύο σύνολα δεδομένων δοκιμής ο καλύτερος ρυθμός ανίχνευσης επιτυγχάνεται για τις επιθέσεις R2L και U2R χρησιμοποιώντας τον ταξινομητή Naïve Bayes. Επιπλέον παρατηρούμε ότι οι ταξινομητές παρουσιάζουν μεγάλη δυσκολία να ανιχνεύσουν νέες επιθέσεις U2R και R2L που δεν περιλαμβάνονται στο σύνολο δεδομένων εκπαίδευσης. Ενώ οι ταξινομητές SVM και MLP κρίνονται καλύτεροι στην ταξινόμηση νέων επιθέσεων Probe και DoS αντίστοιχα.

3.3 Δεδομένα Ασύρματης Δικτυακής Κίνησης

3.3.1 Περιβάλλον Προσομοίωσης

Προκειμένου να αξιολογήσουμε την αποτελεσματικότητα και τη δυνατότητα εφαρμογής της προσέγγισής μας σε κινητά ασύρματα δίκτυα κατά περίσταση πραγματοποιήσαμε μία σειρά πειραμάτων. Για τα πειράματά μας πραγματοποιήσαμε κάποιες υποθέσεις. Πρώτα από όλα, υποθέτουμε ότι το δίκτυο υλοποιεί το πρωτόκολλο IEEE 802.11 στο επίπεδο MAC. Κανένας άλλος μηχανισμός ασφαλούς και δίκαιας πρόσβασης δεν χρησιμοποιείται. Το δίκτυο δεν έχει προϋπάρχουσα υποδομή και το πρωτόκολλο δρομολόγησης κατά περίσταση (ad hoc) που εφαρμόστηκε είναι το AODV (Ad hoc On demand Distance Vector) [Perkins, 2003].

Η υλοποίηση του προσομοιωτή πραγματοποιήθηκε με το εργαλείο GloMoSim [GloMoSim, 2000]. Η προσομοίωση μοντελοποιεί ένα δίκτυο 50 κόμβων που τοποθετούνται τυχαία σε μία περιοχή 850 x 850 m^2. Κάθε κόμβος έχει εύρος διάδοσης 250 μέτρα και η χωρητικότητα του δικτύου είναι 2 Mbps. Οι κόμβοι στην προσομοίωση κινούνται σύμφωνα με το μοντέλο "κατεύθυνσης τυχαίας οδού" (random way point). Στην αρχή της προσομοίωσης, κάθε κόμβος περιμένει για ένα διάστημα παύσης, στη συνέχεια επιλέγει και κινείται προς αυτή την κατεύθυνση με μία ταχύτητα που λαμβάνει τιμές ομοιόμορφα μεταξύ μηδέν και της μέγιστης ταχύτητας. Όταν φτάσει στον προορισμό του σταματά και πάλι και επαναλαμβάνει την παραπάνω διαδικασία μέχρι το τέλος της προσομοίωσης. Η ελάχιστη ταχύτητα ισούται με 0 m/s ενώ η μέγιστη 20 m/s. Τα διαστήματα

παύσης που χρησιμοποιήσαμε προκειμένου να εξετάσουμε την συμπεριφορά των αλγόριθμων ταξινόμησης για ασύρματα δίκτυα ποικίλης κινητικότητας είναι 0, 200, 400 και 700 sec. Σημειώνεται ότι η διάρκεια κάθε προσομοίωσης είναι 700 sec, οπότε ένα διάστημα παύσης ίσο με 0 sec αντιστοιχεί σε συνεχή κίνηση του κόμβου και ένα διάστημα παύσης ίσο με 700 sec αντιστοιχεί σε ένα σταθερό δίκτυο. Επιπλέον αξιολογήσαμε την απόδοση των αλγόριθμων ταξινόμησης για τις περιπτώσεις που υπάρχουν 5, 15 και 20 κακόβουλοι κόμβοι στο ασύρματο κινητό δίκτυο κατά περίσταση.

Κάθε κόμβος στέλνει δικτυακή κυκλοφορία CBR (Constant Bit Rate). Το μέγεθος των πακέτων που στέλνει κυμαίνεται από 128 έως 1024 bytes. Μελετήσαμε επίσης την απόδοση των αλγόριθμων ταξινόμησης για διάφορες τιμές της περιόδου δειγματοληψίας (5, 10, 15, 30 sec) προκειμένου να εξετάσουμε την ταχύτητα με την οποία μπορεί να πραγματοποιηθεί η ανίχνευση των επιθέσεων. Προκειμένου να εξετάσουμε την απόδοση των αλγόριθμων ταξινόμησης για διαφορετικές περιόδους δειγματοληψίας δημιουργήσαμε τέσσερα σύνολα των δεδομένων εκπαίδευσης και αντίστοιχα τέσσερα σύνολα δεδομένων δοκιμής ένα για κάθε περίοδο δειγματοληψίας (5, 10, 15 και 30 sec).

Ένα σημαντικό θέμα που είχαμε να αντιμετωπίσουμε είναι ο χαρακτηρισμός της "φυσιολογικής" και "μη-φυσιολογικής" συμπεριφοράς για το ασύρματο δίκτυο κατά περίσταση στα σύνολα δεδομένων εκπαίδευσης. Προκειμένου να λάβουμε μόνο "φυσιολογική" δικτυακή κίνηση πραγματοποιήσαμε μία προσομοίωση χωρίς να περιλαμβάνονται κακόβουλοι κόμβοι στο δίκτυο με χρονικό διάστημα παύσης 0 και διάρκεια προσομοίωσης 700 sec. Όλη η δικτυακή κυκλοφορία που δημιουργήθηκε θεωρήθηκε "φυσιολογική". Προκειμένου να επιτύχουμε το χαρακτηρισμό κακόβουλης κυκλοφορίας πραγματοποιήσαμε μία ακόμα προσομοίωση με 25 κακόβουλους κόμβους να περιλαμβάνονται στο δίκτυο οι οποίοι πραγματοποιούσαν τέσσερα είδη προσομοιωμένων επιθέσεων. Όλη η δικτυακή κίνηση που δημιουργήθηκε θεωρήσαμε ότι είναι κακόβουλη.

Δημιουργήσαμε επίσης σύνολα δεδομένων δοκιμής για διαφορετικά διαστήματα παύσης (0, 200, 400, 700 sec) και διαφορετικό αριθμό κακόβουλων κόμβων (5, 15, 25).

3.3.2 Προσομοιωμένες Επιθέσεις

Οι επιθέσεις που προσομοιώσαμε είναι οι ακόλουθες:

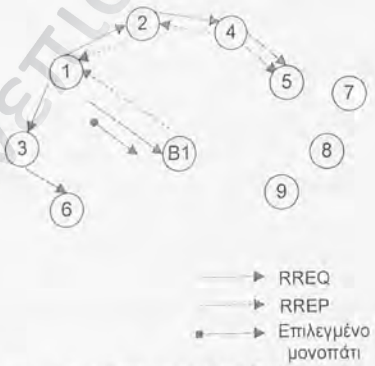
Επίθεση Πλημμύρας (Flooding): Προσομοιώσαμε μία επίθεση πλημμύρας πολλαπλών μονοπατιών στο επίπεδο δικτύου όπου ένας κακόβουλος κόμβος στέλνει πλαστά πακέτα RREQ σε τυχαίους προορισμούς σε όλους τους κόμβους δικτύου κάθε 100 msec.

Πλαστά πακέτα RERR (Forging RERR (Route ERRors)): Προσομοιώσαμε μία επίθεση δημιουργίας πλαστών πακέτων όπου ένας κακόβουλος κόμβος παραποιεί και στέλνει με ανοικτή εκπομπή ένα μήνυμα RERR σε ένα επιλεγμένο θύμα κάθε 100 sec με αποτέλεσμα τις επαναλαμβανόμενες αποτυχίες σύνδεσης (link failures).

Απόρριψη πακέτων (Packet Dropping): Προσομοιώσαμε μία επίθεση επιλεκτικής απόρριψης πακέτων. Ο κακόβουλος κόμβος απορρίπτει όλα τα πακέτα RRER, αυτό έχει σαν αποτέλεσμα οι νόμιμοι κόμβοι να προωθούν πακέτα σε σπασμένους συνδέσμους ενώ θα έπρεπε να χρησιμοποιήσουν ένα άλλο μονοπάτι για την προώθηση των πακέτων τους.

Μαύρη Τρύπα (Black Hole): Προσομοιώσαμε μία επίθεση "μαύρης τρύπας". Ένας κακόβουλος κόμβος που είναι "μαύρη τρύπα" διαφημίζει μία καινούρια διαδρομή προς τον προορισμό χωρίς να ελέγχει τον πίνακα δρομολόγησής του, λαμβάνει τα πακέτα δεδομένων από την πηγή και τα κρατά χωρίς να τα προωθεί. Πιο συγκεκριμένα ένας κακόβουλος κόμβος εκμεταλλεύεται ένα συγκεκριμένο χαρακτηριστικό του AODV [Perkins, 2003] και στέλνει με ανοικτή εκπομπή ένα πακέτο RREP (Route REPly) στην πηγή χωρίς να ελέγχει εάν έχει ένα νέο μονοπάτι προς τον επιλεγμένο προορισμό, επομένως είναι πάντα ο πρώτος που απαντά. Επιπλέον, λόγω της έλλειψης επιβεβαίωσης στο πρωτόκολλο AODV ο κακόβουλος κόμβος μπορεί να απορρίψει τα πακέτα που έχει λάβει οδηγώντας σε απώλεια κρίσιμων πληροφοριών. Μία απεικόνιση αυτής της επίθεσης φαίνεται στο Σχήμα 7.4.

Στο Σχήμα 7.4, ο κόμβος πηγή 1 θέλει να επικοινωνήσει με το προορισμό 5. Για τον σκοπό αυτό στέλνει με ανοικτή εκπομπή ένα μήνυμα RREQ (Route REQuest) στους γειτονικούς κόμβους 2, 3 και B1. Ο B1 που είναι κακόβουλος κόμβος στέλνει ένα μήνυμα RREP (Route REPly)στον κόμβο 1 χωρίς να ελέγξει εάν όντως έχει μονοπάτι προς τον κόμβο 5. Επομένως ο κόμβος 1 πιστεύοντας ότι ο κόμβος B1 έχει μονοπάτι προς τον επιθυμητό προορισμό μεταφέρει όλα τα πακέτα δεδομένων στον B1 ο οποίος τα απορρίπτει.



Σχήμα 7. 4 Επίθεση Μαύρης Τρύπας

Σημειώνουμε ότι, δεν λαμβάνονται υπόψη οι μετρήσεις όλων των κόμβων του δικτύου, αλλά μόνο αυτών που υπήρξαν γείτονες κάποιου κακόβουλου κόμβου κατά την διάρκεια της δειγματοληψίας αφού αυτοί είναι υπεύθυνοι στην

προκειμένη περίπτωση να ανιχνεύσουν τις επιθέσεις. Θεωρούμε δηλαδή ότι εφόσον το IDS είναι εγκατεστημένο σε όλους τους κόμβους του δικτύου και κάθε ένας κόμβος χωριστά εκτελεί αυτόνομες μετρήσεις, τότε το πιθανότερο είναι να εντοπιστεί η επίθεση των κακόβουλων κόμβων από τους γείτονές τους. Άρα, για να μελετήσουμε την απόδοση των αλγορίθμων ταξινόμησης χρησιμοποιούμε μόνο τις μετρήσεις των γειτονικών κόμβων των κακόβουλων κόμβων και όχι όλων των κόμβων του δικτύου.

Επιπλέον, προκειμένου να εξετάσουμε την απόδοση κάθε αλγόριθμου ταξινόμησης διακρίναμε δύο περιπτώσεις: την περίπτωση στην οποία πραγματοποιούμε δυαδική ταξινόμηση (2 κλάσεις ("φυσιολογική" συμπεριφορά – επίθεση)) και την περίπτωση στην οποία πραγματοποιούμε ταξινόμηση πολλαπλών κλάσεων (5 κλάσεις ("φυσιολογική" συμπεριφορά – κάθε τύπος επίθεσης)).

3.3.3 Πεδία

Τα διανύσματα πεδίων που χρησιμοποιούνται στους αλγόριθμους ταξινόμησης μας είναι ένα κρίσιμο βήμα στη διαμόρφωση της προτεινόμενης προσέγγισης ανίχνευσης εισβολών. Τα χαρακτηριστικά της δικτυακής κυκλοφορίας θα πρέπει να είναι σε κατάλληλη μορφή προκειμένου να μπορούν εύκολα να επεξεργαστούν από τους αλγόριθμους ταξινόμησης και αντιπροσωπευτικά προκειμένου να αυξήσουν την αντίθεση ανάμεσα στη "φυσιολογική" και τη "μη-φυσιολογική" δραστηριότητα έτσι ώστε να μπορούμε να πούμε χωρίς αμφιβολία αν ένα γεγονός είναι "φυσιολογικό" ή "μη-φυσιολογικό".

Τα πεδία που χρησιμοποιήσαμε για την πραγματοποίηση ανίχνευσης εισβολών στο επίπεδο δικτύου είναι τα ακόλουθα:

RREQ Sent: αντιστοιχεί στον αριθμό των πακέτων RREQ που στέλνει κάθε κόμβος.

RREQ Received: αντιστοιχεί στον αριθμό των πακέτων RREQ που λαμβάνει κάθε κόμβος.

RREP Sent: αντιστοιχεί στον αριθμό των πακέτων RREP που στέλνει κάθε κόμβος.

RREP Received: αντιστοιχεί στον αριθμό των πακέτων RREP που λαμβάνει κάθε κόμβος.

RError Sent: αντιστοιχεί στον αριθμό των πακέτων RError που στέλνει κάθε κόμβος.

RError Received: αντιστοιχεί στον αριθμό των πακέτων RError που λαμβάνει κάθε κόμβος.

Data Sent: αντιστοιχεί στον αριθμό των πακέτων δεδομένων (data) που στέλνει κάθε κόμβος.

Data Received: αντιστοιχεί στον αριθμό των πακέτων δεδομένων (data) που λαμβάνει κάθε κόμβος.

Αριθμός Γειτόνων: αντιστοιχεί στον αριθμό των άμεσων γειτόνων κάθε κόμβου.

PCR (Percentage of the Change in Route entries): αντιστοιχεί στο ποσοστό των αλλαγών στις εγγραφές δρομολόγησης. Το *PCR* [Sun, 2004] υπολογίζεται από τον τύπο $(|S2 - S1| + |S1 - S2|)/|S1|$, όπου το $|S|$ υποδηλώνει των αριθμό των στοιχείων του S.

Η ποσότητα $(S2 - S1)$ αντιστοιχεί στην αύξηση των νέων εγγραφών του πίνακα δρομολόγησης κατά τη διάρκεια του διαστήματος $(t2 - t1)$, και το $(S1 - S2)$ αντιστοιχεί στις διαγραμμένες εγγραφές του πίνακα δρομολόγησης κατά τη διάρκεια $(t2 - t1)$. Μαζί αναπαριστούν τις αλλαγές των εγγραφών στον πίνακα δρομολόγησης $(t2 - t1)$.

PCH (Percentage of the Change in number of Hops): αντιστοιχεί στο ποσοστό αλλαγών των αριθμών των βημάτων. Το PCH [Sun, 2004] υπολογίζεται σαν $(H2 - H1)/H1$. Το $(H2 - H1)$ υποδηλώνει τις αλλαγές του αθροίσματος των βημάτων όλων των εγγραφών δρομολόγησης κατά το χρονικό διάστημα $(t2 - t1)$.

3.3.4 Πίνακες Κόστους

Για τα δεδομένα που αφορούν την ασύρματη δικτυακή κίνηση οι πίνακες κόστους έχουν καθοριστεί από εμάς. Όταν έχουμε να κάνουμε με δυαδική ταξινόμηση χρησιμοποιήσαμε τον Πίνακας 7.11. Θέτουμε λοιπόν κόστος 10 για κάθε ταξινόμηση επίθεσης σαν "φυσιολογική" συμπεριφορά, ενώ το κόστος για την ταξινόμησης "φυσιολογικής" συμπεριφοράς σαν επίθεση είναι 1.

Πινακας 7. 11 Πίνακας Κόστους για το Σύνολο Δεδομένων Ασύρματης Κίνησης για Δυαδική Ταξινόμηση

Πραγματική / Πρόβλεψη	Φυσιολογική κίνηση	επίθεση
Φυσιολογική Κίνηση	0	1
Επίθεση	10	0

Ανάλογα για ταξινόμηση πολλαπλών κλάσεων, συγκεκριμένα 4 κλάσεις επιθέσεων ασύρματης δικτυακής κίνησης και μία κλάση "φυσιολογικής" συμπεριφοράς χρησιμοποιήσαμε τον Πίνακα 7.12.

Πίνακας 7. 12 Πίνακας Κόστους για το Σύνολο Δεδομένων Ασύρματης Κίνησης για Ταξινόμηση Πολλαπλών Κλάσεων

Πραγματική / Πρόβλεψη	Φυσιολογική	BlackHole	Packet Dropping RERR	Forging RERR	Flooding RREQ
Φυσιολογική	0	1	1	1	1
BlackHole	10	0	1	1	1
Packet Dropping RERR	10	1	0	1	1
Forging RERR	10	1	1	0	1
Flooding RREQ	10	1	1	1	0

3.3.5 Παράμετροι Αλγορίθμων Ταξινόμησης

Στον Πίνακα 7.12 φαίνονται οι παράμετροι που χρησιμοποιήθηκαν για κάθε σύνολο δεδομένων εκπαίδευσης με και χωρίς τη χρήση κόστους. Για την επιλογή των καλύτερων παραμέτρων σαν μέτρο σύγκρισης χρησιμοποιήθηκε το κόστος που δίνεται από την εξίσωση 7.3. Καταλήξαμε σε αυτές τις παραμέτρους αφού ακολουθήσαμε τη διαδικασία που περιγράφεται στην παράγραφο 3.1.

Πίνακας 7. 13 Παράμετροι για τα Σύνολα Δεδομένων Εκπαίδευσης Ασύρματης ΔικτυακήςΚίνησης

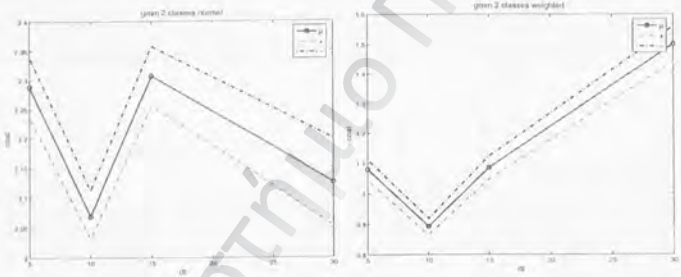
	dt 5		dt 10		dt 15		dt 30	
	Χωρίς κόστος	Με κόστος	Χωρίς κόστος	Με κόστος	Χωρίς κόστος	Με κόστος	Χωρίς κόστος	Με κόστος
mlp_2class	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.01
	T=10	T=1000	T=10	T=10	T=10	T=10	T=10	T=500
	n_h=320	n_h=320	n_h=100	n_h=20	n_h=320	n_h=320	n_h=10	n_h=20
linear_2class	η=η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.0001	η=0.01
	T=10	T=1000	T=10	T=10	T=10	T=10	T=10	T=500
	n_h=0	n_h=0	n_h=1	n_h=1	n_h=0	n_h=0	n_h=0	n_h=0
mlp_5class	η=0.001	η=0.001	η=0.1	η=0.001	η=0.01	η=0.01	η=0.0001	η=0.001
	T=500	T=1000	T=1000	T=500	T=1000	T=500	T=10	T=1000
	n_h=320	n_h=100	n_h=80	n_h=40	n_h=40	n_h=20	n_h=120	n_h=20
linear_5class	η=0.001	η=0.001	η=0.1	η=0.001	η=0.01	η=0.01	η=0.0001	η=0.001
	T=500	T=1000	T=1000	T=500	T=1000	T=500	T=10	T=1000
	n_h=0	n_h=0	n_h=1	n_h=1	n_h=0	n_h=0	n_h=0	n_h=0
gmm_2class	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.01	θ=0.1
	T=1000	T=100	T=100	T=1000	T=500	T=100	T=25	T=25
	n_g=320	n_g=320	n_g=320	n_g=320	n_g=320	n_g=320	n_g=320	n_g=320
naive_2class	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.1	θ=0.01	θ=0.1
	T=1000	T=100	T=100	T=1000	T=500	T=100	T=25	T=25
	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1
gmm_5class	θ=0.01	θ=0.01	θ=0.01	θ=0.01	θ=0.001	θ=0.01	θ=0.001	θ=0.0001
	T=500	T=500	T=1000	T=100	T=1000	T=25	T=1000	T=25
	n_g=80	n_g=160	n_g=40	n_g=160	n_g=40	n_g=80	n_g=20	n_g=40
naive_5class	θ=0.01	θ=0.01	θ=0.01	θ=0.01	θ=0.001	θ=0.01	θ=0.001	θ=0.0001
	T=500	T=500	T=1000	T=100	T=1000	T=25	T=1000	T=25
	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1	n_g=1

3.3.6 Αποτελέσματα Πειραμάτων Αξιολόγησης

Α. Αποτελέσματα Ταξινόμησης με τη Χρήση Κόστους

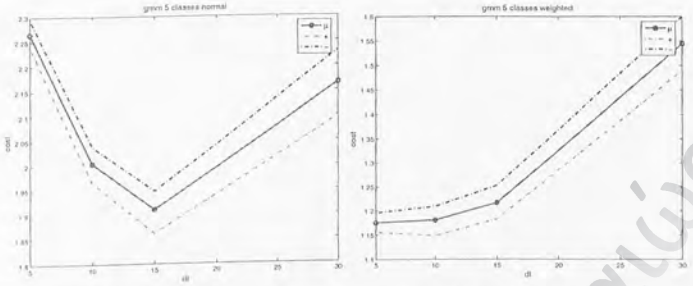
Προκειμένου να εξετάσουμε την απόδοση των αλγορίθμων ταξινόμησης για διαφορετικά χρονικά διαστήματα λήψης δεδομένων χρησιμοποιήσαμε τη μεθοδολογία bootstrapping [Efron, 1994]. Στη συνέχεια παρουσιάζεται το κόστος κάθε αλγόριθμου ταξινόμησης (Gaussian Mixture Model, Naïve Bayes, MLP, Linear) πραγματοποιώντας δυαδική (2-class) ή πολλαπλών κλάσεων (5-class) ταξινόμηση, σε συνάρτηση με το χρονικό διάστημα λήψης δεδομένων (5, 10, 15, 30 sec). Για κάθε περίπτωση παρουσιάζονται τα αποτελέσματα όταν η διαδικασία λήψης αποφάσεων είτε χρησιμοποιεί τον πίνακα κόστους είτε όχι.

Σε κάθε γραφική παράσταση (Σχήματα 7.5 έως 7.12) η μεσαία γραμμή αναπαριστά το αναμενόμενο κόστος όπως εκτιμήθηκε με βάση τα δεδομένα ελέγχου. Οι περιβάλλουσες γραμμές περικλείουν το διάστημα εμπιστοσύνης (99%) του αναμενόμενου κόστους όπως αυτό εκτιμήθηκε από τα δείγματα bootstrap.



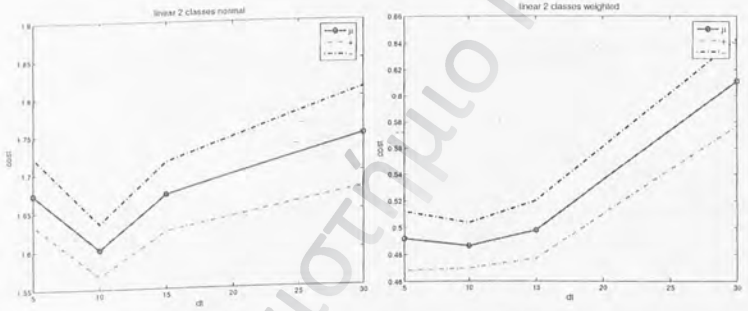
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 5 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο GMM (Δυαδική Ταξινόμηση) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



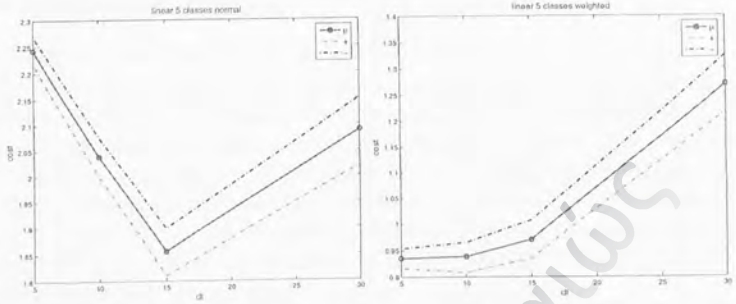
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 6 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο GMM (Ταξινόμηση Πολλαπλών Κλάσεων) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



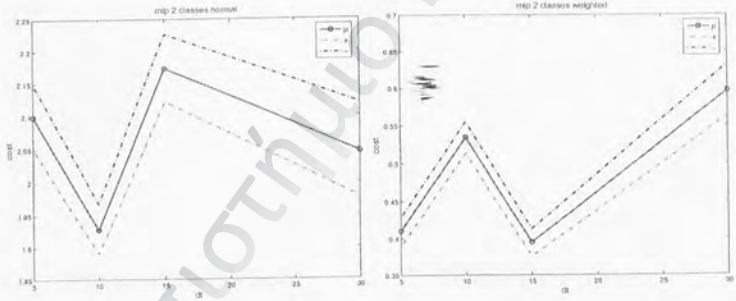
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 7 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο Linear (Δυαδική Ταξινόμηση) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



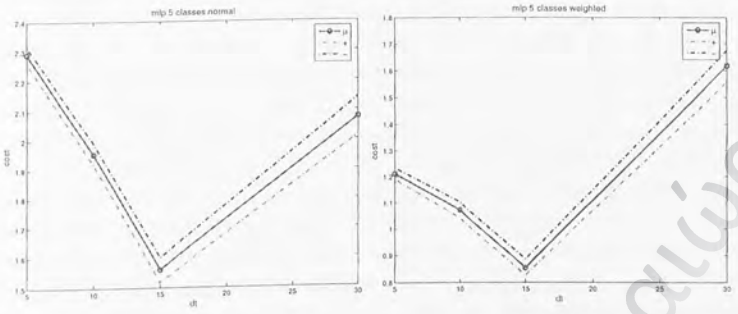
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 8 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο Linear (Ταξινόμηση Πολλαπλών Κλάσεων) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



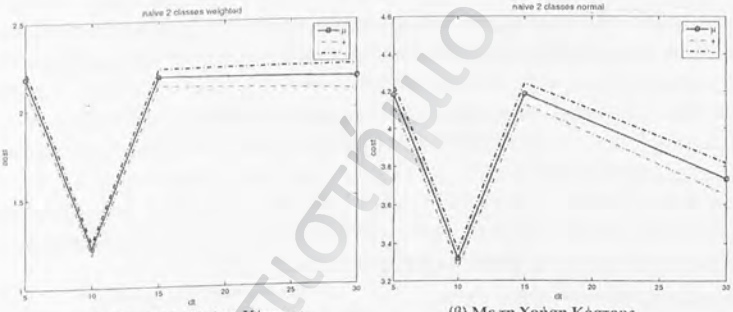
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 9 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο MLP (Δυαδική Ταξινόμηση) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



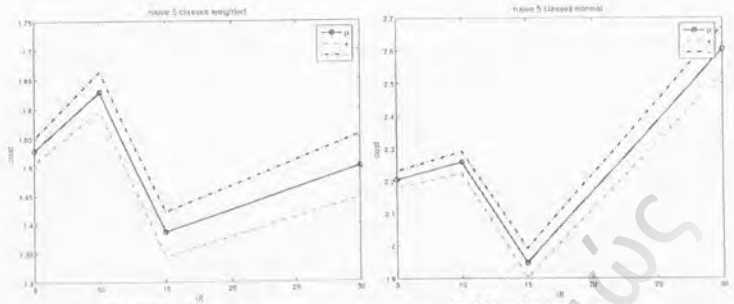
(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 10 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο MLP (Ταξινόμηση Πολλαπλών Κλάσεων) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

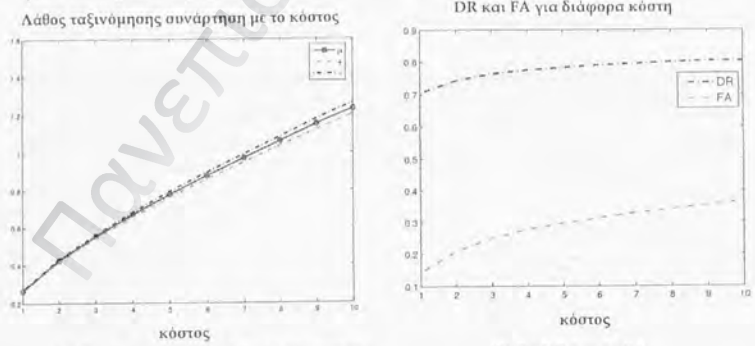
Σχήμα 7. 11 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο Naïve-Bayes (Δυαδική Ταξινόμηση) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.



(α) Χωρίς τη Χρήση Κόστους (β) Με τη Χρήση Κόστους

Σχήμα 7. 12 Αναμενόμενο Κόστος Ταξινόμησης για τον Αλγόριθμο Naïve-Bayes (Ταξινόμηση Πολλαπλών Κλάσεων) σε Συνάρτηση με την Περίοδο Δειγματοληψίας.

Από τις παραπάνω γραφικές παραστάσεις φαίνεται ότι το αναμενόμενο κόστος ταξινόμησης παρουσιάζει σημαντική μείωση όταν το κόστος λαμβάνεται υπόψη κατά την ταξινόμηση. Άρα η ταξινόμηση με ευαισθησία ως προς το κόστος μας βοηθά σημαντικά στη βελτίωση της ταξινόμησης και τη διάκριση μεταξύ "φυσιολογικής" και "μη-φυσιολογικής" συμπεριφοράς. Επιπλέον παρατηρούμε ότι το αναμενόμενο κόστος παρουσιάζει τις χαμηλότερες τιμές του για περιόδους δειγματοληψίας dt=10 ή dt=15 sec για όλους τους αλγόριθμους ταξινόμησης με την περίοδο δειγματοληψίας dt=10 sec να υπερτερεί. Κάτι που μπορεί να δικαιολογηθεί αν σκεφτούμε ότι η περίοδος δειγματοληψίας dt=5 sec είναι πολύ μικρή ώστε τα διανύσματα χαρακτηριστικών (πεδίων) να μπορούν με σαφήνεια να περιγράψουν τις συνθήκες δικτυακής κυκλοφορίας σε ένα ασύρματο δίκτυο κατά περίσταση. Αντίστοιχα και η περίοδος δειγματοληψίας dt=30 sec είναι πολύ μεγάλη και χάνεται σημαντική πληροφορία που υποδηλώνει τις αλλαγές τις δικτυακής κυκλοφορίας.

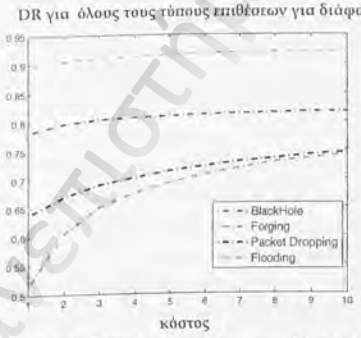


(α) Το αναμενόμενο κόστος ταξινόμησης (β) Το DR και το FA

Σχήμα 7. 13 Μέτρα Εκτίμησης Απόδοσης για τον Αλγόριθμο MLP (Ταξινόμηση Πολλαπλών Κλάσεων) για Διάφορα Κόστη και Περίοδο Δειγματοληψίας dt=10.

Στο Σχήμα 7.13 φαίνεται το αναμενόμενο λάθος ταξινόμησης με χρήση κόστους σε συνάρτηση με το κόστος για τον αλγόριθμο MLP πολλαπλών τάξεων. Προκειμένου να εξετάσουμε την απόδοση του αλγορίθμου ταξινόμησης MLP (πολλαπλών τάξεων) για διαφορετικά κόστη χρησιμοποιήσαμε και πάλι τη μεθοδολογία bootstrapping (βλ. Παράρτημα Γ). Στη γραφική παράσταση που απεικονίζεται στο Σχήμα 7.13 (α) η μεσαία γραμμή αναπαριστά το αναμενόμενο κόστος όπως εκτιμήθηκε με βάση τα δεδομένα ελέγχου. Οι περιβάλλουσες γραμμές περικλείουν το διάστημα εμπιστοσύνης (99%) του αναμενόμενου κόστους όπως αυτό εκτιμήθηκε από τα δείγματα bootstrap.

Στο Σχήμα 7.13 (β) φαίνεται πώς επηρεάζεται ο μέσος ρυθμός ανίχνευσης εισβολών (DR) και ο ρυθμός λανθασμένων συναγερμών (FA) σε συνάρτηση με το κόστος. Παρατηρούμε λοιπόν ότι ο ρυθμός ανίχνευσης εισβολών (DR) κυμαίνεται μεταξύ 0.705 (70.5%0 και 0.803 (80.3%) ενώ ο ρυθμός λανθασμένων συναγερμών (FA) κυμαίνεται μεταξύ 0.142 (14.2%) και 0.365 (36.5%). Παρατηρούμε λοιπόν ότι έχουμε μία σημαντική αύξηση του ρυθμού ανίχνευσης εισβολών (DR) της τάξης του 9.8% που συνοδεύεται όμως από μία αντίστοιχη αύξηση του ρυθμού των λανθασμένων συναγερμών (FA). Επομένως, πρέπει να βρούμε ένα συμβιβασμό ανάμεσα στις δύο αυξήσεις για μία ενδιάμεση τιμή κόστους. Για παράδειγμα για κόστος ίσο με 3 ο ρυθμός ανίχνευσης εισβολών (DR) είναι ίσος με 0.763, ενώ ο ρυθμός λανθασμένων συναγερμών (FA) είναι ίσος με 0.249.



Σχήμα 7.14 Το DR για Κάθε Τύπο Επίθεσης για τον Αλγόριθμο MLP (Ταξινόμηση Πολλαπλών Κλάσεων) για Διάφορα Κόστη και Περίοδο Δειγματοληψίας dt=10.

Στο Σχήμα 7.14 φαίνεται πώς επηρεάζεται ο ρυθμός ανίχνευσης (DR) κάθε τύπου επίθεσης σε συνάρτηση με το κόστος. Φαίνεται λοιπόν ότι ο ρυθμός ανίχνευσης (DR) για την επίθεση Μαύρης Τρύπας (Black Hole) κυμαίνεται από 0.782 έως 0.817. Ο ρυθμός ανίχνευσης (DR) για τις επιθέσεις Πλαστών Πακέτων (Forging) κυμαίνεται από 0.514 έως 0.743 δηλαδή παρουσιάζει μία αξιοσημείωτη βελτίωση της τάξης του 22.9%. Παρατηρούμε ότι σημαντική βελτίωση του ρυθμού ανίχνευσης εισβολών (DR) για την επίθεση Πλαστών Πακέτων (Forging) της τάξης του 13.6% παρουσιάζεται ακόμα και όταν το κόστος δεν έχει αυξηθεί

σημαντικά και είναι ίσο με 3. Ο ρυθμός ανίχνευσης (DR) για την επίθεση Απόρριψης Πακέτων (Packet Dropping) παρουσιάζει επίσης σημαντική βελτίωση της τάξης του 10.9% και κυμαίνεται από 0.637 έως 0.746. Τέλος ο ρυθμός ανίχνευσης (DR) για τις επιθέσεις (R2L) κυμαίνεται από 0.896 έως 0.921 μία επίσης σημαντική βελτίωση.

Β. Αποτελέσματα Ταξινόμησης Χωρίς τη Χρήση Κόστους

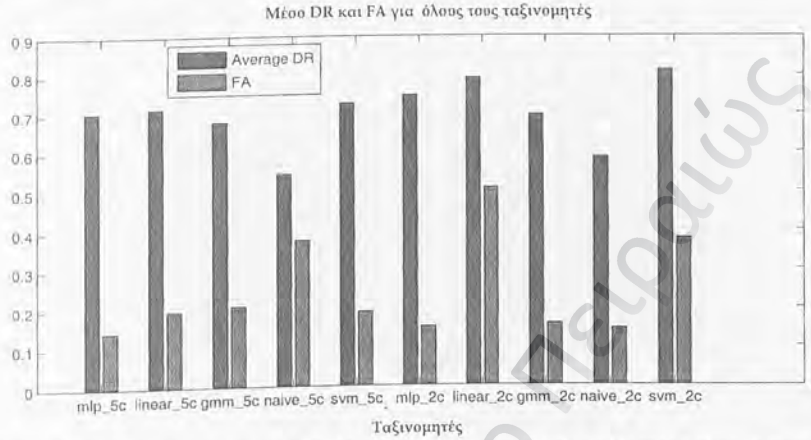
Στη συνέχεια εξετάζουμε την απόδοση του κάθε αλγόριθμου ταξινόμησης όσον αφορά στο ρυθμό ανίχνευσης εισβολών (DR) και τον ρυθμό λανθασμένων συναγερμών (FA) χωρίς τη χρήση κόστους.

Πίνακας 7. 14 Παράμετροι για τα Σύνολα Δεδομένων Εκπαίδευσης

	dt 5	dt 10	dt 15	dt 30
mlp_2class	η=0.0001	η=0.001	η=0.001	η=0.01
	T=1000	T=500	T=100	T=500
	n_h=140	n_h=80	n_h=140	n_h=20
linear_2class	η=0.0001	η=0.001	η=0.001	η=0.01
	T=1000	T=500	T=100	T=500
	n_h=0	n_h=0	n_h=0	n_h=0
mlp_5class	η=0.001	η=0.001	η=0.01	η=0.01
	T=1000	T=1000	T=500	T=500
	n_h=140	n_h=80	n_h=40	n_h=10
linear_5class	η=0.001	η=0.001	η=0.01	η=0.01
	T=1000	T=1000	T=500	T=500
	n_h=0	n_h=0	n_h=0	n_h=0
gmm_2class	θ=0.1	θ=0.001	θ=0.001	θ=0.01
	T=500	T=500	T=100	T=500
	ngaus=140	n_g=160	n_g=140	n_g=120
naive_2class	θ=0.1	θ=0.001	θ=0.001	θ=0.01
	T=500	T=500	T=100	T=500
	n_g=1	n_g=1	n_g=1	n_g=1
gmm_5class	θ=0.001	θ=0.001	θ=0.001	θ=0.0001
	T=500	T=25	T=500	T=500
	n_g=100	n_g=160	n_g=160	n_g=80
naive_5class	θ=0.001	θ=0.001	θ=0.001	θ=0.0001
	T=500	T=25	T=500	T=500
	n_g=1	n_g=1	n_g=1	n_g=1
svm_2class	std=100	std=100	std=100	std=1000
	c=1	c=1	c=1	c=1000
svm_5class	std=100	std=100	std=100	std=1000
	c=100	c=10	c=10	c=1000

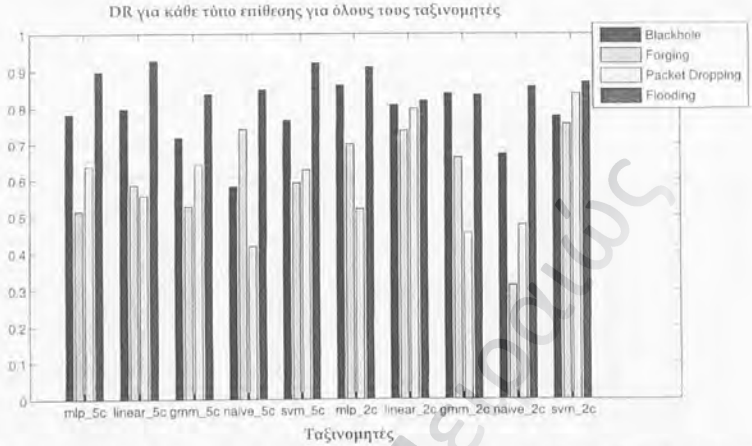
Προκειμένου να πραγματοποιήσουμε αυτό τον έλεγχο αυτή τη φορά η ρύθμιση των παραμέτρων που χρησιμοποιήθηκαν για την εκπαίδευση των

συνόλων δεδομένων πραγματοποιήθηκε με κριτήριο το λάθος ταξινόμησης και όχι το αναμενόμενο κόστος. Οι παράμετροι που επιλέχθηκαν τελικά φαίνονται στον Πίνακα 7.14.



Σχήμα 7. 15 Μέσο DR και FA για κάθε Αλγόριθμο Ταξινόμησης Χωρίς Κόστος Ταξινόμησης και με Περίοδο Δειγματοληψίας dt=10 sec.

Στο Σχήμα 7.15 παρουσιάζεται ο μέσος ρυθμός ανίχνευσης εισβολών (DR) και ο ρυθμός λανθασμένων συναγερμών (FA) κάθε ταξινομητή (MLP, Linear, GMM, Naïve Bayes, SVM) τόσο για δυαδική ταξινόμηση όσο και για ταξινόμηση πολλαπλών κλάσεων (5-class) για το Σύνολο Δεδομένων εκπαίδευσης που αντιστοιχούν σε περίοδο δειγματοληψίας dt=10 καθώς αυτή η περίοδος δειγματοληψίας αποδείχτηκε ως η πιο αποτελεσματική (Παράγραφος 3.3.6 Α). Όπως φαίνεται από το Σχήμα 7.15 ο υψηλότερος μέσος ρυθμός ανίχνευσης εισβολών (DR) επιτυγχάνεται με τη χρήση του ταξινομητή SVM για δυαδική ταξινόμηση (2-class) και είναι ίσος με 0.812. Παρόλα αυτά ο συγκεκριμένος ταξινομητής παρουσιάζει αρκετά υψηλό ρυθμό λανθασμένων συναγερμών (FA) ίσο με 0.379. Ο χαμηλότερος ρυθμός λανθασμένων συναγερμών (FA) επιτυγχάνεται με τον ταξινομητή MLP πολλαπλών κλάσεων (5-class) και είναι ίσος με 0.142, ενώ ο αντίστοιχος ρυθμός ανίχνευσης εισβολών (DR) είναι επίσης αρκετά υψηλός και ίσος με 0.705. Ο χαμηλότερος ρυθμός ανίχνευσης εισβολών (DR) είναι ίσος με 0.544 και παρουσιάζεται για τον ταξινομητή Naïve Bayes όταν πραγματοποιείται πολλαπλών κλάσεων (5-class) ταξινόμηση. Σαν πιο αποτελεσματικός ταξινομητής με αρκετά υψηλό ποσοστό ανίχνευσης (DR) ίσο με 0.746 και αρκετά χαμηλό ποσοστό λανθασμένων συναγερμών (FA) ίσο με 0.15 κρίνεται ότι είναι ο ταξινομητής MLP όταν πραγματοποιεί δυαδική ταξινόμηση (2-class).



Σχήμα 7. 16 DR για Κάθε Τύπο Επίθεσης για Κάθε Ταξινομητή χωρίς Κόστος Ταξινόμησης και με Περίοδο Δειγματοληψίας dt=10 sec.

Στο Σχήμα 7.16 παρουσιάζεται ο ρυθμός ανίχνευσης εισβολών (DR) για κάθε τύπο επίθεσης (BlackHole, Forging, Packet Dropping και Flooding). Για την επίθεση Μαύρης Τρύπας (BlackHole) το υψηλότερο ποσοστό ανίχνευσης εισβολών (DR) επιτυγχάνεται με τον ταξινομητή MLP όταν πραγματοποιεί δυαδική ταξινόμηση και είναι ίσο με 0.86. Για την επίθεση Forging το υψηλότερο ποσοστό ανίχνευσης (DR) επιτυγχάνεται με τον ταξινομητή SVM όταν πραγματοποιεί δυαδική ταξινόμηση (2-class) και είναι ίσο με 0.755. Για την επίθεση Απόρριψης Πακέτων (Packet Dropping) το υψηλότερο ποσοστό ανίχνευσης εισβολών (DR) επιτυγχάνεται και πάλι με τον ταξινομητή SVM για δυαδική ταξινόμηση (2-class) και είναι ίσος με 0.838. Τέλος, για την επίθεση Πλημμύρας (Flooding) ο υψηλότερος ρυθμός ανίχνευσης εισβολών (DR) επιτυγχάνεται με τον Γραμμικό (Linear) ταξινομητή όταν πραγματοποιείται ταξινόμηση πολλαπλών κλάσεων (5-class) και είναι ίσος με 0.927.

Επιπλέον μελετήσαμε την αποτελεσματικότητα των αλγόριθμων ταξινόμησης σε συνάρτηση με την κινητικότητα του ασύρματου δικτύου κατά περίσταση αλλά και τον αριθμό των κακόβουλων κόμβων που περιλαμβάνονται στο δίκτυο. Στον Πίνακα 7.15 παρουσιάζεται το λάθος ταξινόμησης για κάθε αλγόριθμο ταξινόμησης για κάθε περίοδο δειγματοληψίας (5, 10, 15, 30 sec) για τέσσερα διαστήματα παύσης 0, 200, 400, 700 sec. Για διάστημα παύσης ίσο με 0 sec δηλαδή όταν το δίκτυο βρίσκεται σε συνεχή κίνηση σαν πιο αποτελεσματικός κρίνεται ο αλγόριθμος SVM όταν πραγματοποιείται ταξινόμηση πολλαπλών κλάσεων και καλύτερη περίοδος δειγματοληψίας τα 15 sec, ενώ το αντίστοιχο λάθος ταξινόμησης είναι ίσο με 0.169. Για το διάστημα παύσης ίσο με 200 sec

δηλαδή ένα ασύρματο δίκτυο κατά περίσταση με μέτρια κινητικότητα σαν πιο αποτελεσματικός αλγόριθμος ταξινόμησης κρίνεται και πάλι ο SVM όταν πραγματοποιείται ταξινόμηση πολλαπλών κλάσεων (5-class), καλύτερη περίοδος δειγματοληψίας τα 15 sec και αντίστοιχο λάθος ταξινόμησης ίσο με 0.151. Για διάστημα παύσης ίσο με 400 sec ιδιαίτερα αποτελεσματικοί είναι οι αλγόριθμοι MLP δυαδικής ταξινόμησης και ο SVM πολλαπλής ταξινόμησης. Νικητής όμως είναι και πάλι ο αλγόριθμος SVM πολλαπλής ταξινόμησης με καλύτερη περίοδο δειγματοληψίας τα 15 sec και αντίστοιχο λάθος ταξινόμησης ίσο με 0.138. Τέλος για διάστημα παύσης ίσο με 700 sec δηλαδή μιλάμε για ένα ασύρματο δίκτυο κατά περίσταση το οποίο είναι σταθερό καλύτερος αλγόριθμος ταξινόμησης κρίνεται το MLP όταν πραγματοποιείται ταξινόμηση πολλαπλών κλάσεων με καλύτερη περίοδο δειγματοληψίας τα 30 sec και το αντίστοιχο κόστος ταξινόμησης είναι ίσο με 0.142.

Γενικά λοιπόν σαν συμπέρασμα μπορούμε να πούμε ότι οι αλγόριθμοι ταξινόμησης SVM και MLP είναι οι πιο αποτελεσματικοί για όλα είδη κινητικότητας δικτύων με πιο αποτελεσματική περίοδο δειγματοληψίας τα 15 sec και μέσο λάθος ταξινόμησης 0.15.

Πίνακας 7. 15 Λάθος Ταξινόμησης για Δίκτυα κατά Περίσταση Διαφορετικής Κινητικότητας για όλους τους Αλγόριθμους Ταξινόμησης.

	pause_0				pause 200				pause 400				pause 700			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
gmm_2class	0.301	0.190	**0.179**	0.188	0.272	**0.190**	0.181	0.232	0.214	**0.185**	0.206	0.221	0.326	0.243	0.247	**0.194**
	0.214				0.219				**0.207**				0.252			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
gmm_5class	0.303	0.223	**0.186**	0.348	0.218	0.264	**0.174**	0.225	0.229	0.262	**0.161**	0.196	0.252	0.236	0.239	**0.177**
	0.265				0.220				**0.212**				0.226			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
naïve_2class	0.456	0.447	**0.370**	0.382	0.431	**0.299**	0.398	0.350	0.342	**0.252**	0.333	0.352	0.485	**0.318**	0.474	0.361
	0.414				0.370				**0.320**				0.410			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
naïve_5class	0.372	0.326	**0.255**	0.427	0.327	0.430	**0.216**	0.330	0.354	0.483	**0.199**	0.298	0.341	0.362	0.298	**0.243**
	0.345				0.325				**0.333**				0.311			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
mlp_2class	0.276	0.229	**0.154**	0.191	0.246	0.168	**0.153**	0.203	0.187	**0.166**	0.175	0.185	0.275	0.220	0.192	**0.179**
	0.213				0.193				**0.178**				0.217			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
mlp_5class	0.291	0.188	**0.179**	0.300	0.198	0.234	**0.148**	0.185	0.204	0.241	**0.124**	0.160	0.216	0.212	0.202	**0.142**
	0.240				0.191				**0.182**				0.193			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
linear_2class	0.405	0.355	**0.242**	0.320	0.387	**0.245**	0.284	0.315	0.261	**0.237**	0.285	0.342	0.432	**0.274**	0.415	0.293
	0.331				0.308				**0.281**				0.354			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
linear_5class	0.381	0.335	**0.312**	0.565	0.396	0.362	**0.362**	0.507	0.401	0.405	**0.334**	0.513	0.414	0.350	**0.350**	0.438
	0.398				0.407				0.414				**0.388**			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
svm_2class	0.341	0.375	**0.220**	0.591	0.353	0.267	**0.206**	0.573	**0.243**	0.246	0.255	0.576	0.370	**0.281**	0.333	0.602
	0.382				0.349				**0.330**				0.396			
	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
svm_5class	0.299	0.201	**0.169**	0.142	0.196	0.244	**0.151**	0.162	0.202	0.243	**0.138**	0.187	0.216	0.206	**0.219**	0.313
	0.203				**0.188**				0.193				0.239			

Στον Πίνακα 7.16 παρουσιάζεται το λάθος ταξινόμησης για κάθε αλγόριθμο ταξινόμησης για κάθε περίοδο δειγματοληψίας (5, 10, 15, 30 sec) για τρεις περιπτώσεις όσον αφορά στον αριθμό των κακόβουλων κόμβων που περιλαμβάνεται στο δίκτυο 5, 10 και 15. Όταν στο δίκτυο περιλαμβάνονται λίγοι κακόβουλοι κόμβοι δηλ. 5 τότε η ανίχνευση της κακόβουλης συμπεριφοράς και ο διαχωρισμός της από τη "φυσιολογική" είναι ιδιαίτερα δύσκολος. Ο αλγόριθμος ταξινόμησης που παρουσιάζει το μικρότερο λάθος ταξινόμησης είναι ο SVM όταν πραγματοποιεί ταξινόμηση πολλαπλών κλάσεων (5 κλάσεις), η καλύτερη περίοδος δειγματοληψίας τα 15 sec και το αντίστοιχο λάθος ταξινόμησης 0.088. Όταν στο δίκτυο περιλαμβάνεται ένας μεσαίος αριθμός κακόβουλων κόμβων δηλ. 15 τότε η ανίχνευση της κακόβουλης συμπεριφοράς είναι λίγο πιο εύκολη. Ο αλγόριθμος ταξινόμησης που παρουσιάζει το μικρότερο λάθος ταξινόμησης είναι και πάλι το MLP όταν πραγματοποιεί ταξινόμηση πολλαπλών κλάσεων (5 κλάσεις), η καλύτερη περίοδος δειγματοληψίας τα 15 sec το αντίστοιχο λάθος ταξινόμησης 0.148. Τέλος όταν στο δίκτυο υπάρχει ένας αρκετά μεγάλος αριθμός κακόβουλων κόμβων δηλ. 25 τότε η ανίχνευση των επιθέσεων είναι ακόμα πιο εύκολη. Ο αλγόριθμος ταξινόμησης που παρουσιάζει την καλύτερη απόδοση είναι και πάλι το MLP όταν πραγματοποιεί ταξινόμηση πολλαπλών κλάσεων, με καλύτερη περίοδος δειγματοληψίας τα 30 sec και το αντίστοιχο λάθος ταξινόμησης 0.053.

Συμπεραίνουμε λοιπόν, ότι είναι πιο εύκολη η ανίχνευση των εισβολών σε δίκτυα κατά περίσταση μικρής ή μέτριας κινητικότητας καθώς όταν η κίνηση των κόμβων είναι πολύ γρήγορη τα δεδομένα που συλλέγονται δεν μπορούν να παράσχουν διακριτή διαφοροποίηση "φυσιολογικής" και "μη-φυσιολογικής" συμπεριφοράς. Επιπλέον η ανίχνευση εισβολών είναι πιο αποτελεσματική σε δίκτυα όπου υπάρχουν πολλοί κακόβουλοι κόμβοι καθώς τα δεδομένα που παράγονται και αναπαριστούν την κακόβουλη συμπεριφορά είναι περισσότερα. Ενώ πιο αποδοτικές περίοδοι δειγματοληψίας κρίνονται τα 10 ή 15 sec καθώς τα 5 sec είναι πολύ λίγα για να συλλέξουμε πληροφορίες για την τρέχουσα δικτυακή κατάσταση ενώ τα 30 sec είναι πολλά καθώς πολύτιμη πληροφορία που αναπαριστά τη δικτυακή κυκλοφορία χάνεται. Τέλος πιο αποδοτικοί αλγόριθμοι ταξινόμησης στην ανίχνευση εισβολών κρίνονται οι MLP και SVM.

Πίνακας 7. 16 Λάθος ταξινόμησης για δίκτυα κατά περίσταση για όλους τους αλγόριθμους ταξινόμησης σε σχέση με τον αριθμό των κακόβουλων κόμβων που υπάρχουν στο δίκτυο.

	malicious 5				malicious 15				malicious 25			
gmm_2class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.559	0.524	0.446	**0.418**	0.272	**0.190**	0.181	0.232	0.137	0.121	**0.113**	0.111
	0.487				0.219				**0.120**			
gmm_5class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.613	0.585	**0.466**	0.547	0.218	0.263	**0.173**	0.225	0.137	0.161	0.099	**0.084**
	0.553				0.220				**0.120**			
naïve_2class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.531	**0.504**	0.536	0.511	0.431	**0.299**	0.398	0.350	0.241	**0.178**	0.201	0.203
	0.520				0.370				**0.206**			
naïve_5class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.655	0.714	**0.476**	0.560	0.327	0.430	**0.216**	0.330	0.261	0.394	0.150	**0.125**
	0.601				0.325				**0.232**			
mlp_2class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.539	0.452	**0.416**	0.424	0.246	0.168	**0.153**	0.203	0.111	0.080	**0.059**	0.075
	0.457				0.193				**0.081**			
mlp_5class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.565	0.529	**0.392**	0.427	0.198	0.234	**0.148**	0.185	0.111	0.129	0.063	**0.053**
	0.478				0.191				**0.089**			
linear_2class	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.569	0.461	**0.449**	0.480	0.387	**0.245**	0.284	0.315	0.009	0.200	0.154	**0.166**
	0.490				0.308				**0.132**			
linear_5class	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	d30	dt 5	dt10	dt15	d30
	0.600	0.556	**0.441**	0.521	0.396	0.362	**0.362**	0.507	0.311	0.300	**0.243**	0.367
	0.530				0.407				**0.305**			
svm_2class	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
	0.462	0.424	**0.407**	0.507	0.353	**0.267**	0.272	0.573	**0.290**	**0.279**	**0.208**	0.611
	0.450				0.366				**0.347**			
svm_5class	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30	dt 5	dt10	dt15	dt30
	0.74	0.509	**0.088**	0.475	0.23	0.244	**0.150**	0.187	0.092	0.134	**0.073**	0.047
	0.453				**0.203**				**0.086**			

4. Επίλογος

Σε αυτό το κεφάλαιο ασχοληθήκαμε με την δημιουργία συστημάτων ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος. Προτείναμε μία μέθοδο που στόχο έχει να μεγιστοποιήσει την ανίχνευση των εισβολών και να ελαχιστοποιήσει το κόστος. Η προσέγγιση βασίζεται στη χρήση αλγόριθμων ταξινόμησης που πραγματοποιούν τις αποφάσεις ταξινόμησης λαμβάνοντας υπόψη το κόστος αν μία επίθεση ταξινομηθεί σαν "φυσιολογική" συμπεριφορά. Εξετάσαμε την απόδοση της προτεινόμενης προσέγγισης τόσο σε δεδομένα που προέρχονται από ενσύρματα δίκτυα όσο και σε δεδομένα που προέρχονται από ασύρματα δίκτυα κατά περίσταση. Για τα ενσύρματα δίκτυα χρησιμοποιήσαμε τη βάση δεδομένων KDD και πραγματοποιήσαμε αξιολόγηση της προσέγγισης τόσο για δεδομένα που περιέχουν νέους τύπους επιθέσεων (που δεν περιλαμβάνονται στα σύνολα δεδομένων εκπαίδευσης) όσο και για δεδομένα χωρίς νέους τύπους επιθέσεων. Οδηγηθήκαμε στο συμπέρασμα ότι η προτεινόμενη προσέγγιση δεν βοηθά στην ανίχνευση νέων επιθέσεων που δεν υπάρχουν στο σύνολο δεδομένων εκπαίδευσης. Επιπλέον, για τα ενσύρματα δίκτυα καταλήξαμε στο συμπέρασμα ότι η χρήση της μεθόδου ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος οδηγεί σε σημαντική αύξηση του ρυθμού ανίχνευσης εισβολών (DR) ιδιαίτερα για τις επιθέσεις U2R και R2L χωρίς να συνοδεύεται από σημαντική αύξηση του ρυθμού λανθασμένων συναγερμών (FA). Επιπλέον, εξετάσαμε την απόδοση των αλγόριθμων χωρίς τη χρήση κόστους. Για τις επιθέσεις R2L και U2R σαν πιο αποτελεσματικός κρίνεται ο αλγόριθμος Naïve Bayes ενώ για τις επιθέσεις Probe και DoS οι ταξινομητές MLP και SVM.

Για τα ασύρματα δίκτυα παρατηρήσαμε ότι και πάλι με τη χρήση της μεθόδου ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος επιτυγχάνεται και πάλι σημαντική βελτίωση του ρυθμού ανίχνευσης εισβολών (DR) η οποία συνοδεύεται με μία αρκετά μεγάλη αύξηση του ρυθμού λανθασμένων συναγερμών. Εύκολα όμως μπορούμε να επιτύχουμε ένα συμβιβασμό με μία ικανοποιητική βελτίωση του ρυθμού ανίχνευσης εισβολών (DR) χωρίς να οδηγηθούμε σε σημαντική αύξηση του ρυθμού λανθασμένων συναγερμών. Παρατηρήσαμε ότι η καλύτερη βελτίωση της ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος πραγματοποιείται για την επίθεση Forging. Επιπλέον συμπεράναμε ότι σαν καλύτερη περίοδος δειγματοληψίας είναι τα 10 ή 15 sec. Χωρίς τη χρήση κόστους οι πιο αποτελεσματικοί ταξινομητές για τις επιθέσεις *"Μαύρης Τρύπας"*, Πλαστών πακέτων (Forging) και Απόρριψης πακέτων (Packet Dropping) είναι ο ταξινομητής SVM ενώ για την επίθεση πλημμύρας (Flooding) ο Γραμμικός (Linear) ταξινομητής. Οι αλγόριθμοι ταξινόμησης παρουσιάζουν καλύτερη απόδοση για ασύρματα δίκτυα κατά περίσταση μέτριας ή μικρής κινητικότητας και η ανίχνευση εισβολών είναι πιο αποτελεσματική όταν περιλαμβάνεται στο δίκτυο μεγάλος αριθμός κακόβουλων κόμβων.

Βιβλιογραφία

[Burges, 1998] C. J. C. Burges, *"A Tutorial on Support Vector Machines for Pattern Recognition"*, In Knowledge Discovery and Data Mining, Vol. 2, Springer-Verlag, London, UK, 1998 pp. 121–167.

[Cohen, 1995] W.W. Cohen, *"Fast Effective Rule Induction"*, In Proceedings of the Twelfth International Conference on Machine Learning, Lake Taho, Ca, 1995, Morgan Kaufmann, pp. 115-123.

[DeGroot, 2004] M. H. DeGroot, *"Optimal Statistical Decisions"*, John Wiley & Sons, 1970, Republished in 2004.

[Domingos, 1999] P. Domingos, *"MetaCost: A general Method for Making Classifiers Cost-Sensitive"*, In Proceedings of the Fifth ACM SIGKDD Int'l conf. On Knowledge Discovery and Data Mining, pp. 155-164, San Diego, CA, 1999, CA.

[Efron, 1994] B. Efron, R. J. Tibshirani, *"An Introduction to the Bootstrap"*, Monographs on Statistics & Applied Probability, Vol. 57, Chapmann & Hall, Nov, Pub. Date: May 1994.

[Elkan, 1999] C. Elkan, *"Results of the KDD'99 Classifier Learning Contest"*, September 1999, Available from < http://www-cse.ucsd.edu/users/elkan/clresults.html>

[Fan, 2000] W. Fan, W. Lee, S. J. Stolfo, and M. Miller, *"A Multiple Model Cost-Sensitive Approach for Intrusion Detection"*, In Proceedings of the 11th European conference on Machine Learning 2000 (ECML'00), Barcelona, Catalonia, Spain, May 31- June 2, 2000, Lecture Notes in Computer Science, Vol. 1810, pp. 142-153.

[Fumera, 2002] G. Fumera, F. Roli, *"Cost-sensitive Learning in Support Vector Machines"*, in Proceedings of Workshop on Macnine Learning, Methods and applications, oth Meeting of the Italian Association of artificial Intelligence (AIIA), Siena, Italy, 2002.

[GloMoSim, 2000] *GloMoSim, Global Mobile Information Systems Simulation Library*, Version 2.0, December 2000, Available from <http://pcl.cs.ucla.edu/projects/glomosim/>.

[Hastie, 2003] T. Hastie, R. Tibshirani, J. Friedman, *"The Elements of Statistical Learning: Data Mining, Inference, and Prediction"*, Springer Series in Statistics, Springer-Verlag, New York, 2003.

[Kdd, 1999] The UCI KDD Archive Information and Computer Science University of California, Irvine, *"Kdd Cup 1999 Data"*, October 1999, Available from http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html.

[Lin, 2002] Y. Lin, Y. Lee, G. Wahba, *"Support Vector Machines for Classification in Nonstandard Situations"*, Machine Learning, Vol. 46, 2002 Kluwer academic Publishers, pp.191-202.

[Perkins, 2003] C.E. Perkins, E.M. Belding-Royer, and S. Das, *"Ad Hoc On Demand Distance Vector (AODV) Routing"*, July 2003, IETF RFC 3561.

[Pietraszek, 2004] T. Pietraszek, *"Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection"*, In Proceedings of Recent Advances in Intrusion Detection 7th International Symposium (RAID'04), Sophia, Antipolis,

France, September, 15-17, 2004, Lecture Notes in Computer Science 3224, Springer 2004, pp.102-124.

[Sun, 2004] B. Sun, *"Intrusion Detection in Mobile Ad Hoc Networks"*, Doctor of Philosophy, Computer Science, Texas A& M University, May 2004.

[Ting, 1998] K. Ting, *"Inducing Cost-sensitive Trees via Instance Weighting"*, In Proceedings of the Second European Symposium on Principles of Data Mining and Knowledge Discovery. Volume 1510 of Lecture Notes in AI., Springer-Verlag (1998), pp. 137-147.

[Torch, 2004] *Torch Library*, Release 3.1, 11 August 2004, Available from <http://www.torch.ch>.

[Vapnik, 1995] V. N. Vapnik, *"The Nature of Statistical Learning Theory"*, Springer, New York, 1995.

Κεφαλαίο 8ο

Συμπεράσματα και Μελλοντική Έρευνα

1. Συμπεράσματα

Στη διατριβή αυτή έγινε μία προσπάθεια προσέγγισης του προβλήματος ασφάλειας των υπολογιστικών συστημάτων και δικτύων, έτσι ώστε να δοθούν αποτελεσματικές και αξιόπιστες απαντήσεις στο πρόβλημα. Ακολουθήσαμε μία προσέγγιση πολλαπλών κατευθύνσεων ώστε να καλύψουμε όλες τις διαστάσεις του προβλήματος.

- Αρχικά ερευνήσαμε το πρόβλημα των επιθέσεων άρνησης εξυπηρέτησης (Denial of Service (DoS)), μία από τις κύριες απειλές και μεταξύ των δυσκολότερων προβλημάτων ασφάλειας στο σημερινό Διαδίκτυο. Παρουσιάσαμε μία πλήρη επισκόπηση των επιθέσεων DoS, τους τρόπους λειτουργίας τους, κατηγοριοποιώντας τόσο γνωστούς όσο πιθανούς μηχανισμούς επίθεσης. Περιγράψαμε τα σημαντικά χαρακτηριστικά κάθε τύπου επίθεσης DoS και προτείναμε μία κατηγοριοποίηση των υπαρχόντων μηχανισμών αντιμετώπισης. Επιπλέον αναλύσαμε τα πλεονεκτήματα και μειονεκτήματα για τους μηχανισμούς αντιμετώπισης που έχουν προταθεί. Στόχος ήταν η περιγραφή του προβλήματος με μία ολοκληρωμένη και δομημένη εικόνα στο πεδίο των επιθέσεων DoS ώστε να επιτύχουμε καλύτερη

κατανόηση αυτών των επιθέσεων και να σχεδιάσουμε πιο αποτελεσματικούς μηχανισμούς αντιμετώπισης.

- Σημειώσαμε τη σοβαρότητα και την επικινδυνότητα που παρουσιάζουν οι επιθέσεις DoS όπως καταδεικνύεται από στατιστικά στοιχεία και χαρακτηριστικά περιστατικά επιθέσεων DoS σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, έναν ιδιαίτερο κρίσιμο και σημαντικό τομέα. Προτείναμε επίσης μία λίστα με τις καλύτερες πρακτικές που μπορούν να υιοθετηθούν από τους κυβερνητικούς οργανισμούς προκειμένου να ενδυναμώσουν περισσότερο την ασφάλεια των συστημάτων τους από το ενδεχόμενο να συμμετάσχουν σε μία επίθεση DDoS ή να γίνουν θύμα μίας επίθεσης DoS/DDoS. Καθώς όμως το πρόβλημα των επιθέσεων DoS είναι ιδιαίτερα πολύπλοκο και σοβαρό χρειάζεται να αντιμετωπιστεί μέσω μίας μακροχρόνιας προσπάθειας. Προτείναμε λοιπόν, μακροπρόθεσμα μέτρα αντιμετώπισης που μπορούν να υιοθετηθούν προκειμένου να επιτευχθεί το καλύτερο αποτέλεσμα.
- Προτείναμε μία μέθοδο ανίχνευσης των δικτυακών εισβολών περιλαμβανομένων των επιθέσεων DoS η οποία βασίζεται στην ακριβή και αποτελεσματική διάκριση μεταξύ της παράνομης ("μη-φυσιολογικής") και της νόμιμης ("φυσιολογικής") δικτυακής κυκλοφορίας. Η προτεινόμενη προσέγγιση βασίζεται στην κατάλληλη επεξεργασία αρχείων καταγραφής δικτυακής κυκλοφορίας χρησιμοποιώντας μία κατηγορία νευρωνικών δικτύων που είναι γνωστά σαν *αναδυόμενοι Αυτό-Οργανούμενοι Χάρτες (emergent Self-Organizing Maps (eSOM))*.
- Προκειμένου να απαλλάξουμε τους διαχειριστές δικτύων από την ιδιαίτερα δύσκολη και χρονοβόρα εργασία εξέτασης της δικτυακής κυκλοφορίας και προκειμένου να αποφύγουμε μεγάλη επιβάρυνση επεξεργασίας, συνδυάζουμε τις τεχνικές μηχανικής μάθησης και της απεικόνισης πληροφοριών ώστε να έχουμε μία πιο ξεκάθαρη εικόνα της δικτυακής δραστηριότητας.
- Εκμεταλλευτήκαμε το πλεονεκτήματα των νευρωνικών δικτύων ανοχής σε ανακριβή δεδομένα αλλά και την ανθρώπινη ικανότητα να διαχειρίζεται με αποτελεσματικότητα την πολυπλοκότητα. Επιτύχαμε η παρακολούθηση της δικτυακής κυκλοφορίας να είναι φιλική προς το χρήστη καθώς η απεικόνιση της δικτυακής πληροφορίας δίνει νέες δυνατότητες ανίχνευσης και ανάλυσης πιθανών εισβολών.
- Η προτεινόμενη μέθοδος μπορεί να χρησιμοποιηθεί είτε για την ανάλυση δεδομένων πραγματικού χρόνου είτε για παλαιότερη δικτυακή κυκλοφορία. Για την αξιολόγηση της προσέγγισης χρησιμοποιήθηκε το σύνολο δεδομένων KDD-99 [KDD, 1999] που χρησιμοποιείται ευρέως προκειμένου να συγκρίνουμε τις προσεγγίσεις

ανίχνευσης εισβολών σαν ένα βασικό σύνολο δεδομένων σύγκρισης και όχι αυθαίρετα δημιουργημένα δεδομένα προκειμένου να επιβεβαιωθεί η αξιοπιστία των αποτελεσμάτων. Εξετάσαμε την απόδοση της προτεινόμενης προσέγγισης στις επιθέσεις DoS, Probe, R2L και U2R.

- Η προσέγγιση ανίχνευσης εισβολών χρησιμοποιώντας eSOM παρουσιάζει πολύ καλά αποτελέσματα με πολύ χαμηλούς ρυθμούς λανθασμένων συναγερμών. Όταν τα σύνολα δεδομένων εκπαίδευσης και δοκιμής περιλαμβάνουν περισσότερες επιθέσεις τα αποτελέσματα είναι πιο υποσχόμενα όταν χρησιμοποιούμε 18 πεδία που προέρχονται από το συνδυασμό των σημαντικών πεδίων κάθε τύπου επίθεσης και "φυσιολογικής" δικτυακής κυκλοφορίας.
- Η προτεινόμενη προσέγγιση αναλύει και αποκωδικοποιεί δικτυακά γεγονότα που δεν είναι αναγνώσιμα από τον άνθρωπο και τα παρέχει σε μορφή αναγνώσιμη.
- Τα αποτελέσματα που παράγει η προτεινόμενη μέθοδος ανίχνευσης εισβολών μέσω της απεικόνισης πληροφοριών είναι εύκολα αντιληπτά και διευκολύνουν το έργο του διαχειριστή δικτύου στον εντοπισμό των επιθέσεων.
- Επιπλέον, πρέπει να σημειωθεί ότι προκειμένου να είμαστε σίγουροι ότι η προσέγγισή μας θα παρέχει πάντα αξιόπιστα και ακριβή αποτελέσματα πρέπει να αγανεώνουμε τους εκπαιδευμένους χάρτες eSOM σύμφωνα με νέα πρότυπα δικτυακών επιθέσεων αλλά και σε νέες δικτυακές συνθήκες.
- Η προτεινόμενη μέθοδος ανίχνευσης εισβολών είναι απλή στην εφαρμογή της και μπορεί εύκολα να μεταφερθεί σε διαφορετικές αρχιτεκτονικές.
- Το κύριο μειονέκτημα της προτεινόμενης προσέγγισης είναι η υψηλή υπολογιστική επιβάρυνση που δημιουργείται κατά τη διάρκεια της εκπαίδευσης των συνόλων δεδομένων τα οποία έχουν μέγεθος μεγαλύτερο από 10,000 εγγραφές. Αλλά σίγουρα η υπολογιστική επιβάρυνση του eSOM δεν απαγορεύει τη χρήση του, καθώς πραγματοποιείται μόνο κατά τη διάρκεια της εκπαίδευσης, η οποία δεν πραγματοποιείται τόσο συχνά όσο ο έλεγχος με νέα δεδομένα δικτυακής κίνησης. Επιπλέον, κατά τη διαδικασία ταξινόμησης οι κλάσεις των ταξινομημένων δεδομένων πρέπει να οριστούν χειρωνακτικά μέσω της παρατήρησης του χάρτη κάτι που μπορεί να εισάγει ένα διαδικαστικό λάθος.
- Εξετάσαμε τα προβλήματα ασφάλειας στα *ασύρματα δίκτυα κατά περίσταση (ad hoc)* και τις έμφυτες αδυναμίες που παρουσιάζουν. Επιπλέον, εξετάσαμε τη δυνατότητα επέκτασης της προτεινόμενης προσέγγισης

ανίχνευσης εισβολών με βάση τα eSOM στα ασύρματα δίκτυα κατά περίσταση.

- Συγκεκριμένα προτείναμε ένα κατανεμημένο σύστημα ανίχνευσης εισβολών για τα ασύρματα δίκτυα κατά περίσταση που βασίζεται στα eSOM. Χρησιμοποιώντας το eSOM, κάθε κόμβος του δικτύου κατά περίσταση δημιουργεί τον τοπικό του χάρτη eSOM, καθώς και τον καθολικό χάρτη του τοπικού δικτύου κατά περίσταση. Ο καθολικός και οι τοπικοί χάρτες eSOM μας δίνουν το σημαντικό πλεονέκτημα να μπορούμε να έχουμε οπτική αναπαράσταση της κατάστασης ασφαλείας κάθε κόμβου κατά περίσταση, καθώς και του τοπικού δικτύου κατά περίσταση. Επομένως, κάθε κόμβος έχει τη δυνατότητα να επιλέξει ένα ασφαλές μονοπάτι δρομολόγησης για την προώθηση πακέτων αποφεύγοντας τους κατειλημμένους γείτονες.
- Προτείναμε μία μηχανή *Απόκρισης σε Εισβολές* για τη διασφάλιση των ασύρματων δικτύων κατά περίσταση καθώς κρίνεται απαραίτητη για το μετριασμό των επιθέσεων και τον περιορισμό των επιδράσεων τους. Η προτεινόμενη μηχανή *Απόκρισης σε Εισβολές* κρίνεται απαραίτητη ειδικά στα ασύρματα δίκτυα που παρουσιάζουν πολλά έμφυτα προβλήματα και αδυναμίες συμπεριλαμβανομένων των περιορισμένων πόρων.
- Η μηχανή *Απόκρισης σε Εισβολές* αποτελείται από τρεις μονάδες: τη μονάδα *Επικοινωνίας*, τη μονάδα *Τοπικής Απόκρισης* και τη μονάδα *Καθολικής Απόκρισης*. Η *Απόκριση στις Εισβολές* θα πρέπει να είναι όσο το δυνατόν πιο γρήγορη και αξιόπιστη στην μεταφορά μηνυμάτων ενημέρωσης. Για το λόγο αυτό, η Μονάδα Επικοινωνίας βασίζεται σε ένα προτεινόμενο *πιστοποιημένο Πρωτόκολλο Συμφωνίας Κλειδιού*.
- Λαμβάνουμε υπόψη μας το γεγονός ότι στα δυναμικά δίκτυα όπως τα ασύρματα δίκτυα κατά περίσταση, οι κόμβοι μέλη μπορεί να έχουν μικρή διάρκεια συμμετοχής καθώς νέα μέλη μπορεί να συμμετάσχουν ή να αποχωρήσουν από την ομάδα μελών, αφού δημιουργηθεί το κλειδί συνεδρίας. Για το σκοπό αυτό προτείνουμε ένα *Πρωτόκολλο Συμμετοχής Μέλους* και ένα *Πρωτόκολλο Αποχώρησης Μέλους*. Επιπλέον, προκειμένου να διασφαλίσουμε το κλειδί συνεδρίας από πιθανή έκθεση εάν κανένα μέλος δεν εισέλθει ή δεν αποχωρήσει από την ομάδα των κόμβων του δικτύου κατά περίσταση για μία μεγάλη χρονική περίοδο, προτείνουμε ένα *Πρωτόκολλο Περιοδικής Ανανέωσης Κλειδιού*.
- Μέσω του προτεινόμενου *Πρωτοκόλλου Συμφωνίας Κλειδιού Ομάδας* επιτυγχάνονται οι ακόλουθοι στόχοι ασφάλειας: *μυστικότητα κλειδιού*, *ανεξαρτησία κλειδιού*, *πρόσθια μυστικότητα (forward secrecy)* και *οπισθόδρομη μυστικότητα (backward secrecy)*.
- Η μονάδα *Τοπικής Απόκρισης* δημιουργεί έναν καθολικό χάρτη μέσω του πιστοποιημένου πρωτοκόλλου, για τους άμεσους (ενός-βήματος) γείτονες κάθε κόμβου του δικτύου κατά περίσταση. Η μονάδα *Καθολικής*

Απόκρισης ενημερώνει κάθε κόμβο στην εμβέλεια επικοινωνίας του επιτιθέμενου κόμβου για το στιγμιότυπο της επίθεσης και ξεκινά την απομάκρυνση του κόμβου που δέχτηκε την επίθεση από τους πίνακες δρομολόγησης.

- Η προτεινόμενη μηχανή *Ανίχνευσης Εισβολών* στα ασύρματα δίκτυα κατά περίσταση παρουσιάζει ένα αρκετά μεγάλο ποσοστό ανίχνευσης για τις επιθέσεις επιλεκτικής απόρριψης πακέτων. Το βασικό πλεονέκτημά της είναι η οπτική αναπαράσταση της "φυσιολογικής" και "μη-φυσιολογικής" κατάστασης σε ένα κινητό δίκτυο κατά περίσταση. Αν και παρουσιάζει μεγάλο αριθμό λανθασμένων συναγερμών, έχει την ικανότητα άμεσης απόκρισης στην περίπτωση μίας πιθανής εισβολής επιλέγοντας τον πιο ασφαλή κόμβο όπως υποδηλώνεται από το χάρτη eSOM για την προώθηση μηνυμάτων.
- Προκειμένου όμως, η προτεινόμενη προσέγγιση ανίχνευσης εισβολών στα ασύρματα δίκτυα κατά προσέγγιση να παρέχει αξιόπιστα αποτελέσματα τα οποία δεν μπορούν να τροποποιούν κακόβουλοι επιτιθέμενοι, είναι απαραίτητο να συνδυαστεί με μεθόδους παρεμπόδισης εισβολών. Είναι απαραίτητο λοιπόν, οι *Τοπικοί Χάρτες* eSOM που δημιουργούνται σε κάθε κόμβο του δικτύου, αλλά και ο *Καθολικός Χάρτης* τοπικού δικτύου, να προστατεύονται από πιθανές τροποποιήσεις ή παραβιάσεις. Για το σκοπό αυτό προτείνουμε μία καινοτόμα τεχνική υδατογράφησης, η οποία μας βοηθά να διασφαλίσουμε την ακεραιότητα των χαρτών eSOM και να ανιχνεύσουμε πιθανές τροποποιήσεις σε αυτούς. Η προτεινόμενη τεχνική υδατογράφησης προέρχεται από τον αποτελεσματικό συνδυασμό των μεθόδων ενσωμάτωσης Lattice και Block-Wise.
- Η προτεινόμενη μέθοδος υδατογράφησης εκμεταλλεύεται τα πλεονεκτήματα των μεθόδων Lattice και Block-Wise προκειμένου να παράγει αξιόπιστα και ακριβή αποτελέσματα. Η μέθοδος Lattice παρέχει υδατογραφημένες εικόνες υψηλής ποιότητας αλλά ο αριθμός των bit που ενσωματώνονται είναι μόνο ένα bit ανά 256 pixel. Από την άλλη πλευρά, η μέθοδος Block-Wise ενσωματώνει τέσσερα bit ανά 64 pixel αλλά με το κόστος χαμηλής ποιότητας της παραγόμενης εικόνας. Επιπλέον, η απουσία του ελέγχου λαθών στη μέθοδο Block-Wise μας δίνει το πλεονέκτημα να μπορούμε εύκολα να εντοπίσουμε όποιες τροποποιήσεις της υδατογραφημένης εικόνας. Για το λόγο αυτό συνδυάζουμε με αποτελεσματικό τρόπο της δύο μεθόδους υδατογράφησης προκειμένου να επιτύχουμε τη διασφάλιση της ακεραιότητας των χαρτών eSOM.
- Το πιο ευαίσθητο τμήμα του χάρτη eSOM, το οποίο αναπαριστά την ύπαρξη επίθεσης στον κόμβο του δικτύου υδατογραφείται με τη μέθοδο Block-Wise ενώ το υπόλοιπο τμήμα του χάρτη υδατογραφείται με τη μέθοδο Lattice.

- Εκμεταλλευόμαστε τα σημαντικά πλεονεκτήματα της οπτικής απεικόνισης και της υδατογράφησης στα ασύρματα δίκτυα κατά περίσταση, δύο ερευνητικές περιοχές που δεν είχαν χρησιμοποιηθεί προηγουμένως στην ερευνητική περιοχή των ασυρμάτων δικτύων κατά περίσταση.
- Προκειμένου να επιβεβαιώσουμε την εφαρμογή της προτεινόμενης μεθόδου υδατογράφησης σε πραγματικά περιβάλλοντα ασύρματων δικτύων κατά περίσταση που αντιμετωπίζουν περιορισμούς πόρων, υπολογίζονται εκ των προτέρων όλοι οι απαραίτητοι υπολογισμοί της τεχνικής υδατογράφησης. Με αυτό τον τρόπο, η μόνη υπολογιστική πολυπλοκότητα προκύπτει από τη δημιουργία και την επιβεβαίωση της ψηφιακής υπογραφής. Επιπλέον, η υπολογιστική επιβάρυνση της προτεινόμενης μεθόδου υδατογράφησης είναι η ίδια με το μήκος του κλειδιού που χρησιμοποιούμε στους αλγόριθμους υπογραφής, π.χ. 1024-bit.
- Ένα άλλο σημαντικό πρόβλημα που εξετάσαμε είναι ο περιορισμός του αναμενόμενου κόστους ενός συστήματος ανίχνευσης εισβολών. Επιθυμητό είναι το σύστημα ανίχνευσης εισβολών να λειτουργεί λαμβάνοντας υπόψη ότι κάθε απόφαση που λαμβάνει έχει και το αντίστοιχο κόστος για το σκοπό αυτό προτείναμε μία προσέγγιση ανίχνευσης εισβολών με ευαισθησία στο κόστος.
- Προτείναμε μία μέθοδο που στόχο έχει να μεγιστοποιήσει την ανίχνευση των εισβολών και να ελαχιστοποιήσει το κόστος. Η προσέγγιση βασίζεται στη χρήση αλγόριθμων ταξινόμησης που πραγματοποιούν τις αποφάσεις ταξινόμησης λαμβάνοντας υπόψη το κόστος αν μία επίθεση ταξινομηθεί σαν "φυσιολογική" συμπεριφορά. Εξετάσαμε την απόδοση της προτεινόμενης προσέγγισης τόσο σε δεδομένα που προέρχονται από ενσύρματα δίκτυα όσο και σε δεδομένα που προέρχονται από ασύρματα δίκτυα κατά περίσταση κάτω από διαφορετικές πειραματικές συνθήκες, πίνακες κόστους και διαφορετικά μοντέλα ταξινόμησης, όσον αφορά στο αναμενόμενο κόστος αλλά και στους ρυθμούς *ανίχνευσης εισβολών* και *λανθασμένων συναγερμών*.
- Για τα ενσύρματα δίκτυα χρησιμοποιήσαμε τη βάση δεδομένων KDD και πραγματοποιήσαμε αξιολόγηση της προσέγγισης τόσο για δεδομένα που περιέχουν νέους τύπους επιθέσεων (που δεν περιλαμβάνονται στα σύνολα δεδομένων εκπαίδευσης) όσο και για δεδομένα χωρίς νέους τύπους επιθέσεων. Οδηγηθήκαμε στο συμπέρασμα ότι η προτεινόμενη προσέγγιση δεν βοηθά στην ανίχνευση νέων επιθέσεων που δεν υπάρχουν στο σύνολο δεδομένων εκπαίδευσης.
- Επιπλέον, για τα ενσύρματα δίκτυα καταλήξαμε στο συμπέρασμα ότι η χρήση της μεθόδου ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος οδηγεί σε σημαντική αύξηση του ρυθμού ανίχνευσης εισβολών

(DR) ιδιαίτερα για τις επιθέσεις U2R και R2L χωρίς να συνοδεύεται από σημαντική αύξηση του ρυθμού λανθασμένων συναγερμών (FA).

- Εξετάσαμε την απόδοση των αλγόριθμων χωρίς τη χρήση κόστους. Για τις επιθέσεις R2L και U2R σαν πιο αποτελεσματικός κρίνεται ο αλγόριθμος Naïve Bayes ενώ για τις επιθέσεις Probe και DoS οι ταξινομητές MLP και SVM.
- Για τα ασύρματα δίκτυα παρατηρήσαμε ότι και πάλι με τη χρήση της μεθόδου ανίχνευσης εισβολών με ευαισθησία ως προς το κόστος επιτυγχάνεται και σημαντική βελτίωση του ρυθμού ανίχνευσης εισβολών (DR) η οποία συνοδεύεται με μία αύξηση του ρυθμού λανθασμένων συναγερμών. Εύκολα όμως μπορούμε να επιτύχουμε ένα συμβιβασμό με μία ικανοποιητική βελτίωση του ρυθμού ανίχνευσης εισβολών (DR) χωρίς να οδηγηθούμε σε σημαντική αύξηση του ρυθμού λανθασμένων συναγερμών.
- Παρατηρήσαμε ότι η καλύτερη βελτίωση της ανίχνευσης εισβολών στα ασύρματα δίκτυα κατά περίσταση με ευαισθησία ως προς το κόστος πραγματοποιείται για την επίθεση πλαστών πακέτων (Forging). Επιπλέον, συμπεράναμε ότι σαν καλύτερη περίοδος δειγματοληψίας είναι τα 10 ή 15 sec.
- Χωρίς τη χρήση κόστους ο πιο αποτελεσματικός ταξινομητής για τις επιθέσεις *"Μαύρης Τρύπας", Πλαστών πακέτων (Forging)* και *Απόρριψης πακέτων (Packet Dropping)* είναι ο ταξινομητής SVM ενώ για την επίθεση πλημμύρας (Flooding) ο Γραμμικός (Linear) ταξινομητής.
- Οι αλγόριθμοι ταξινόμησης παρουσιάζουν καλύτερη απόδοση για ασύρματα δίκτυα κατά περίσταση μέτριας ή μικρής κινητικότητας και η ανίχνευση εισβολών είναι πιο αποτελεσματική όταν περιλαμβάνεται στο δίκτυο μεγάλος αριθμός κακόβουλων κόμβων.

2. Μελλοντική Έρευνα

Στη διατριβή αυτή ερευνήσαμε το πρόβλημα της διασφάλισης υπολογιστικών και δικτυακών συστημάτων επικεντρώνοντας την έρευνά μας στην ανίχνευση εισβολών προτείνοντας αποτελεσματικές προσεγγίσεις. Οι προτεινόμενες προσεγγίσεις επιτυγχάνονται χρησιμοποιώντας πολλαπλές μονάδες και αλγόριθμους, οι οποίοι συνεργάζονται για την επίτευξη της αποτελεσματικής διασφάλισης των υπολογιστικών συστημάτων. Υπάρχουν όμως δυνατότητες να βελτιωθούν οι προτεινόμενες προσεγγίσεις μέσα από προγραμματιστικές-αλγοριθμικές τροποποιήσεις αλλά και νέους δρόμους εξερεύνησης και χρήσης διαφορετικών μεθοδολογιών:

- Η ποικιλία και πολυπλοκότητα των δικτυακών επιθέσεων περιλαμβανομένων των επιθέσεων *άρνησης εξυπηρέτησης (Denial of Service (DoS))* είναι πολύ πιθανό να αυξηθεί. Ανεξάρτητα από τα μέτρα προστασίας που μπορούν να χρησιμοποιηθούν τώρα, χρειάζεται να αντιμετωπίσουμε τις δικτυακές επιθέσεις σαν ένα πρόβλημα που απαιτεί

μακροχρόνια προσπάθεια προκειμένου να ορίσουμε και να υλοποιήσουμε αποτελεσματικές λύσεις.

- Είναι σημαντικό να ερευνήσουμε την εξέλιξη των δικτυακών επιθέσεων περιλαμβανομένων των επιθέσεων DoS. Καθώς οι επιτιθέμενοι συνεχώς αλλάζουν τα εργαλεία τους και τις στρατηγικές τους προκειμένου να ξεπεράσουν τα συστήματα ασφάλειας που αναπτύσσονται από τους διαχειριστές συστημάτων και τους ερευνητές. Είναι απαραίτητο λοιπόν, να είμαστε σε συνεχή εγρήγορση προκειμένου να κατανοήσουμε τα νέα προβλήματα που θα δημιουργηθούν και να τροποποιήσουμε τις προσεγγίσεις μας προκειμένου να αντιμετωπιστούν οι νέες επιθέσεις.
- Είναι απαραίτητη η ενημέρωση των κατηγοριοποιήσεων των τύπων επιθέσεων DoS και των αντίστοιχων κατηγοριοποιήσεων των μηχανισμών προστασίας ενάντια των επιθέσεων DoS με νέα στοιχεία ώστε να υπάρχει δομημένη γενική, εικόνα και πλήρης επισκόπηση στο πρόβλημα των επιθέσεων DoS σύμφωνα με τις εξελίξεις.
- Ιδιαίτερα σημαντικό είναι να προτείνουμε νέες πρακτικές, πολιτικές και μακροπρόθεσμα μέτρα προκειμένου να υιοθετηθούν από τους οργανισμούς ώστε να διασφαλίσουν τα συστήματά τους από πιθανές εισβολές.
- Οι προτεινόμενες προσεγγίσεις ανίχνευσης εισβολών τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα είναι σημαντικό να επεκταθούν στην ανίχνευση και άλλων δικτυακών επιθέσεων. Ειδικότερα για τα ασύρματα δίκτυα κατά περίσταση οι προτεινόμενοι μέθοδοι ανίχνευσης εισβολών να επεκταθούν στη χρήση και άλλων πρωτοκόλλων δρομολόγησης.
- Δεδομένου του γεγονότος ότι η επιλογή των κατάλληλων πεδίων βοηθά στο διαχωρισμό των κλάσεων και κατά επέκταση στην περίπτωση μας, στη βελτίωση της αποτελεσματικότητας της ανίχνευσης εισβολών, είναι σημαντικό να ερευνηθεί η χρήση νέων πεδίων αλλά και αλγόριθμοι επιλογή χαρακτηριστικών (πεδίων) των συνόλων δεδομένων από τα αρχεία καταγραφής.
- Οι αλγόριθμοι ταξινόμησης MLP, Γραμμικός (Linear) ταξινομητής, ο αλγόριθμος Γκαουσσιανών Μειγμάτων (GMM), ο αλγόριθμος απλοϊκού μοντέλου Naïve Bayes και ο αλγόριθμος SVM χρησιμοποίησαν και τα 41 πεδία του συνόλου δεδομένων KDD-99 [KDD, 1999]. Σημαντικό είναι να εξεταστεί η απόδοση των αλγορίθμων αυτών με λιγότερα πεδία, όπως τα πιο σημαντικά πεδία για κάθε τύπο επίθεσης (DoS, Probe, R2L, U2R) που έχουν προταθεί από τους Mukkamala και άλλοι [Mukkamala, 2003].
- Όπως ήδη αναφέραμε προκειμένου να είναι αποτελεσματική η μέθοδος ανίχνευσης εισβολών με τη χρήση του eSOM και να παρέχει αξιόπιστα αποτελέσματα είναι σημαντικό να πραγματοποιείται ανανέωση στους εκπαιδευμένους χάρτες eSOM, σύμφωνα με νέα πρότυπα δικτυακών επιθέσεων. Είναι σημαντικό να ερευνηθεί πόσο συχνά πρέπει να

πραγματοποιείται αυτή η ανανέωση τόσο στα ενσύρματα όσο και στα ασύρματα δίκτυα.

- Είναι μεγάλης σημασίας να ερευνηθεί η δυνατότητα περιορισμού της υπερφόρτωσης στα υπολογιστικά συστήματα κατά τη διάρκεια της εκπαίδευσης συνόλου δεδομένων μεγάλου μεγέθους, που δημιουργείται με τον αλγόριθμο ταξινόμησης eSOM.
- Σημαντικό κρίνεται επίσης να εξεταστεί η εφαρμογή της μεθόδου υδατογράφησης των χαρτών eSOM και η ανάπτυξη κατάλληλης μηχανής απόκρισης και για τα ενσύρματα δίκτυα προκειμένου να περιοριστούν οι επιδράσεις πιθανών εισβολών.
- Εκτός από την προτεινόμενη τεχνική υδατογράφησης να ερευνηθούν άλλοι πιθανοί μηχανισμοί διασφάλισης της ακεραιότητας και παρεμπόδισης τροποποίησης των χαρτών eSOM .
- Να μελετήσουμε την πιθανή επέκταση της μηχανής ανίχνευσης εισβολών στα ασύρματα δίκτυα κατά περίσταση και σε άλλες πιθανές αρχιτεκτονικές πέραν της πλήρους κατανεμημένης αρχιτεκτονικής. Πιθανή συνεργασία ανάμεσα στους κόμβους του δικτύου κατά περίσταση μπορεί να βοηθήσει σημαντικά στη βελτίωση της απόδοσης της μηχανής ανίχνευσης εισβολών και τον περιορισμό των λανθασμένων συναγερμών.
- Επιπλέον σημαντική είναι πιθανή επέκταση της προσέγγισης ανίχνευσης εισβολών με ευαισθησία στο κόστος, η εφαρμογή της και σε άλλους αλγόριθμους ταξινόμησης και η διερεύνηση της αποτελεσματικότητάς της σε αυτούς. Σε αυτό το πλαίσιο εργασίας η μέθοδος ανίχνευσης εισβολών με ευαισθησία στο κόστος είναι σημαντικό να εφαρμοστεί και στον αλγόριθμο ταξινόμησης eSOM και να συγκριθεί η αποτελεσματικότητά του σε σχέση με άλλους αλγόριθμους ταξινόμησης.
- Σαν μελλοντική εργασία στην προτεινόμενη προσέγγιση ανίχνευσης εισβολών με ευαισθησία στο κόστος, σημαντικό είναι να εξετάσουμε τη σχέση ανάμεσα στην απόκλιση κατανομής των συνόλων δεδομένων και των πινάκων κόστους που χρησιμοποιούνται. Μία ενδιαφέρουσα προσέγγιση θα είναι η χρήση αποκλειστικά Μπαϋεζιανών Μεθόδων.
- Ένα άλλο σημαντικό σημείο επέκτασης στην ανίχνευση εισβολών με ευαισθησία στο κόστος είναι η πρόταση λήψης κάποιων αποφάσεων για ενέργειες που θα πραγματοποιούνται σε μία πιθανή ανίχνευση εισβολής και στόχο θα έχουν να ελαχιστοποιούν το αναμενόμενο κόστος κάθε απόφασης. Παραδείγματα τέτοιων αποφάσεων θα μπορούσαν να είναι "Καμία ενέργεια", "Κλήση του Διαχειριστή Δικτύου", "Αποκλεισμό Διευθύνσεων IP".
- Επιπλέον μπορούμε να αντιμετωπίσουμε την ανίχνευση εισβολών σαν ένα πρόβλημα ακολουθιακής λήψης αποφάσεων [DeGroot, 2004] όπου κάθε απόφαση δεν θα εξαρτάται μόνο από την τρέχουσα παρατήρηση, αλλά και από το ιστορικό των παρατηρήσεων και τις παλαιότερες αποφάσεις. Κατά αυτό τον τρόπο όχι μόνο μπορούμε να συμβάλουμε στην

προσαρμοστικότητα τέτοιων συστημάτων, αλλά επίσης μπορούμε να ελαττώσουμε τη διαδικασία επιλογής του κατάλληλου διαστήματος δειγματοληψίας για τη συλλογή στατιστικών στοιχείων για τα πακέτα της δικτυακής κυκλοφορίας.

Βιβλιογραφία

[DeGroot, 2004] M.H. DeGroot MH, *"Optimal Statistical Decisions"*, John Wiley & Sons, 1970. Republished in 2004

[Kdd, 1999] The UCI KDD Archive Information and Computer Science University of California, Irvine, *"Kdd Cup 1999 Data"*, October 1999, Available from http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html.

[Mukkamala, 2003] S. Mukkamala, A. H. Sung, *"Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques"*, International Journal of Digital Evidence, Winter 2003, Vol. 1, Issue 4.

Παράρτημα Α -Πεδία του συνόλου δεδομένων KDD-99

Τα πεδία του συνόλου δεδομένων KDD-99 [KDD, 1999] μπορούν να χωριστούν στις ακόλουθες βασικές κατηγορίες [Stolfo, 2000].

Βασικά Πεδία: Τα βασικά πεδία μπορούν να ληφθούν από τις επικεφαλίδες πακέτων χωρίς να επιθεωρείται το περιεχόμενο των πακέτων.

Πεδία Περιεχόμενου: η γνώση της δικτυακής περιοχής (domain) χρησιμοποιείται προκειμένου να εκτιμήσουμε το ωφέλιμο φορτίο (payload) των πακέτων TCP.

Πεδία που βασίζονται στο χρόνο: Λόγω της προσωρινής φύσης των δικτυακών επιθέσεων είναι σημαντικό να επιθεωρήσουμε τα πακέτα μέσα σε ένα συγκεκριμένο χρονικό διάστημα. Αυτά τα πεδία σχεδιάζονται ώστε να συλλέγουν ιδιότητες μετά από ένα χρονικό διάστημα δύο δευτερολέπτων. Τα πεδία που βασίζονται στο χρόνο διακρίνονται σε δύο κατηγορίες, στα πεδία "ίδιου κόμβου" και στα πεδία "ίδιας υπηρεσίας". Τα πεδία "ίδιου κόμβου" εξετάζουν μόνο τις συνδέσεις των δύο προηγούμενων δευτερολέπτων που έχουν το ίδιο κόμβο προορισμού με την τρέχουσα σύνδεση, και υπολογίζουν στατιστικά στοιχεία που σχετίζονται με τη συμπεριφορά του πρωτοκόλλου, την υπηρεσία, κ.τ.λ. Τα παρόμοια χαρακτηριστικά "ίδιας υπηρεσίας" εξετάζουν μόνο τις συνδέσεις τα δύο τελευταία δευτερόλεπτα που έχουν την ίδια υπηρεσία με την τρέχουσα υπηρεσία.

Πεδία που βασίζονται σε κόμβο: Με βάση τον κόμβο προορισμού δημιουργήθηκαν πεδία χρησιμοποιώντας ένα ιστορικό αριθμού συνδέσεων– σε αυτή την περίπτωση 100- στον ίδιο κόμβο. Τα πεδία που βασίζονται σε κόμβο χρησιμοποιούνται για την εκτίμηση επιθέσεων που διαρκούν για διαστήματα που ξεπερνούν τα δύο δευτερόλεπτα.

Μία πλήρης λίστα του συνόλου πεδίων που ορίζονται για τις εγγραφές συνδέσεων παρουσιάζεται ακολούθως:

Πίνακας Α. 1 Πεδία των διανυσμάτων εγγραφών (συνδέσεων) του συνόλου Δεδομένων KDD-99

Όνομα Πεδίου	Περιγραφή	Τύπος
Βασικά Χαρακτηριστικά ανεξάρτητων συνδέσεων TCP.		
1. duration	Διάρκεια (αριθμός δευτερολέπτων) της σύνδεσης.	Συνεχής
2. protocol_type	Τύπος πρωτοκόλλου, π.χ. tcp, udp, κ.τ.λ.	Διακριτή
3. service	Δικτυακή υπηρεσία στον προορισμό, π.χ., http, telnet, κ.τ.λ.	Διακριτή
4. src_bytes	Αριθμός από byte δεδομένων που μεταφέρονται από την πηγή στον προορισμό.	Συνεχής
5. dst_bytes	Αριθμός από byte δεδομένων που μεταφέρονται από τον προορισμό στην πηγή.	Συνεχής
6. flag	Κατάσταση σύνδεσης κανονική ή λάθους.	Διακριτή
7. land	1 εάν η σύνδεση είναι από/προς τον ίδιο κόμβο/θύρα, 0 διαφορετικά.	Διακριτή
8. wrong_fragment	Αριθμός "λανθασμένων" τμημάτων (fragments).	Συνεχής
9. urgent	Αριθμός επειγόντων πακέτων.	Συνεχής
Πεδία περιεχομένου κατά τη διάρκεια μίας σύνδεσης με βάση τη γνώση domain (suggested by domain knowledge).		
10. hot	Αριθμός ``hot'' ενδείξεων.	Συνεχής
11. num_failed_logins	Αριθμός αποτυχημένων προσπαθειών σύνδεσης (login).	Συνεχής
12. logged_in	1 εάν συνδέθηκε (login) στο σύστημα επιτυχώς, 0 διαφορετικά.	Διακριτή
13. num_compromised	Αριθμός "παραβιασμένων" συνθηκών.	Συνεχής
14. root_shell	1 εάν λαμβάνεται root shell, 0 διαφορετικά.	Διακριτή
15. su_attempted	1 γίνει προσπάθεια χρήσης της εντολής ``su-root'', 0 διαφορετικά.	Διακριτή
16. num_root	Αριθμός προσβάσεων σαν "root".	Συνεχής
17. num_file_creations	Αριθμός δημιουργίας αρχείων.	Συνεχής

18. num_shells	Αριθμός των shell prompts.	Συνεχής
19. num_access_files	Αριθμός προσβάσεων σε αρχεία.	Συνεχής
20. num_outbound_cmds	Αριθμός εξερχόμενων εντολών σε μία συνεδρία ftp.	Συνεχής
21. is_hot_login	1 εάν η σύνδεση ανήκει στη λίστα «hot», 0 διαφορετικά.	Διακριτή
22. is_guest_login	1 εάν η σύνδεση είναι σαν "guest", 0 διαφορετικά.	Διακριτή
23. count	Αριθμός συνδέσεων στον ίδιο κόμβο όπως η τρέχουσα σύνδεση τα τελευταία δύο δευτερόλεπτα.	Συνεχής
Τα ακόλουθα πεδία αναφέρονται σε συνδέσεις ίδιου κόμβου.		
24. serror_rate	Ποσοστό των συνδέσεων που έχουν λάθη "SYN".	Συνεχής
25. rerror_rate	Ποσοστό των συνδέσεων που έχουν λάθη "REJ".	Συνεχής
26. same_srv_rate	Ποσοστό των συνδέσεων που χρησιμοποιούν την ίδια υπηρεσία όπως η τρέχουσα.	Συνεχής
27. diff_srv_rate	Ποσοστό των συνδέσεων που χρησιμοποιούν διαφορετικές υπηρεσίες.	Συνεχής
28. srv_count	Αριθμός των συνδέσεων που χρησιμοποιούν την ίδια υπηρεσία, όπως η τρέχουσα σύνδεση τα τελευταία δύο δευτερόλεπτα.	Συνεχής
Τα ακόλουθα πεδία αναφέρονται σε συνδέσεις στην«ίδια υπηρεσία».		
29. srv_serror_rate	Ποσοστό των συνδέσεων που έχουν λάθη "SYN" στην ίδια υπηρεσία όπως η τρέχουσα.	Συνεχής
30. srv_rerror_rate	Ποσοστό των συνδέσεων που έχουν λάθη "REJ" στην ίδια υπηρεσία όπως η τρέχουσα.	Συνεχής
31. srv_diff_host_rate	Ποσοστό των συνδέσεων στις οποίες διαφορετικοί κόμβοι χρησιμοποιούν την τρέχουσα υπηρεσία.	Συνεχής

Τα ακόλουθα πεδία βασίζονται σε μετρήσεις που πραγματοποιήθηκαν στον ίδιο κόμβο χρησιμοποιώντας ένα ιστορικό αριθμού συνδέσεων (100

	συνδέσεις).	
32. dst_host_count	Αριθμός συνδέσεων στον τρέχοντα κόμβο που έχουν τον ίδιο κόμβο προορισμού κατά τη διάρκεια μίας καθορισμένης χρονικής περιόδου.	Συνεχής
33. dst_host_srv_count	Αριθμός συνδέσεων στον τρέχοντα κόμβο που έχουν τον ίδιο κόμβο προορισμού και χρησιμοποιούν την ίδια υπηρεσία.	Συνεχής
34. dst_host_same_srv_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο που έχουν τον ίδιο κόμβο προορισμού και χρησιμοποιούν την ίδια υπηρεσία.	Συνεχής
35. dst_host_diff_srv_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο που χρησιμοποιούν διαφορετική υπηρεσία.	Συνεχής
36. dst_host_same_src_port_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο που έχουν την ίδια θύρα πηγής (src port).	Συνεχής
37. dst_host_srv_diff_host_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο που χρησιμοποιούν την ίδια υπηρεσία και προέρχονται από διαφορετικούς κόμβους.	Συνεχής
38. dst_host_srv_serror_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο και καθορισμένη υπηρεσία που παρουσιάζουν ένα λάθος "SYN".	Συνεχής
39. dst_host_serror_rate	Ποσοστό των συνδέσεων στον τρέχοντα κόμβο και καθορισμένη υπηρεσία που έχουν λάθος "SYN".	Συνεχής
40. dst_host_rerror_rate	% ποσοστό συνδέσεων στον τρέχοντα κόμβο που έχουν λάθος "REJ".	Συνεχής
41. dst_host_srv_rerror_rate	% των συνδέσεων στον τρέχοντα κόμβο και καθορισμένη υπηρεσία που έχουν ένα λάθος "REJ".	Συνεχής

Παράρτημα Β – Επιθέσεις του Συνόλου Δεδομένων KDD-99

Επιθέσεις Άρνησης Εξυπηρέτησης (Denial of Service (DoS))

Apache2	Η επίθεση Apache2 είναι μία επίθεση άρνησης εξυπηρέτησης ενάντια σε έναν εξυπηρετητή ιστού Apache στον οποίο ένας πελάτης στέλνει μία αίτηση με πολλές επικεφαλίδες http. Εάν ο εξυπηρετητής λάβει πολλές από αυτές τις αιτήσεις η λειτουργία του θα επιβραδυνθεί και μπορεί να τεθεί και ολοκληρωτικά εκτός λειτουργίας (crash).
Back	Πρόκειται για μία επίθεση άρνησης εξυπηρέτησης ενάντια σε έναν εξυπηρετητή ιστού Apache, κατά την οποία ο επιτιθέμενος στέλνει πολλές αιτήσεις για URL το οποίο περιέχει πολλούς χαρακτήρες "/". Καθώς ο εξυπηρετητής προσπαθεί να επεξεργαστεί αυτές τις αιτήσεις η λειτουργία του επιβραδύνεται και δεν επεξεργάζεται άλλες αιτήσεις.
Land	Η επίθεση Land είναι μία επίθεση άρνησης εξυπηρέτησης η οποία είναι αποτελεσματική ενάντια κάποιων παλιότερων υλοποιήσεων TCP/IP. Η επίθεση Land πραγματοποιείται όταν ο επιτιθέμενος στέλνει ένα πακέτο SYN με παραποιημένη διεύθυνση πηγής στο οποίο η διεύθυνση πηγής είναι η ίδια με τη διεύθυνση προορισμού.
Mailbomb	Η επίθεση Mailbomb είναι μία επίθεση κατά την οποία ο επιτιθέμενος στέλνει πολλά μηνύματα σε έναν εξυπηρετητή, προκαλώντας υπερχείλιση στην ουρά ταχυδρομείου του εξυπηρετητή και κατ' επέκταση αποτυχία του συστήματος.
Neptune (SYN Flood)	Η επίθεση πλημμύρας SYN είναι μία επίθεση άρνησης εξυπηρέτησης στην οποία κάθε υλοποίηση TCP/IP είναι σε κάποιο βαθμό τρωτή. Κάθε μη – ολοκληρωμένη (half-open) σύνδεση TCP που πραγματοποιείται σε μία μηχανή έχει σαν αποτέλεσμα ο εξυπηρετητής 'tcpd' να προσθέτει μία εγγραφή στη δομή δεδομένων που αποθηκεύει πληροφορίες οι οποίες περιγράφουν όλες τις συνδέσεις που εκκρεμούν. Αυτή η δομή δεδομένων έχει καθορισμένο μέγεθος, και μπορεί να υπερχειλίσει αν σκοπίμως δημιουργηθούν πολλές μη-ολοκληρωμένες (partially-open) συνδέσεις.
Pod (Ping of Death)	Η Ping of Death είναι μία επίθεση άρνησης εξυπηρέτησης που επηρεάζει πολλά παλιότερα λειτουργικά συστήματα. Έχει εκτεταμένα αναφερθεί ότι μερικά συστήματα θα αντιδράσουν με μη προβλέψιμο τρόπο όταν λάβουν υπερμεγέθη πακέτα IP. Πιθανές αντιδράσεις περιλαμβάνουν την κατάρρευση (crashing), το "πάγωμα" (freezing) και την επανεκκίνηση.
ProcessTable	Η επίθεση Process Table είναι μία σχετικά καινούρια επίθεση

	άρνησης εξυπηρέτησης που μπορεί να πραγματοποιηθεί εναντίον πολλαπλών δικτυακών υπηρεσιών και σε μία ποικιλία διαφορετικών συστημάτων UNIX. Η επίθεση πραγματοποιείται εναντίον δικτυακών υπηρεσιών οι οποίες χρησιμοποιούν τη διαδικασία fork() ή διαφορετικά δεσμεύουν μία νέα διαδικασία για κάθε νέα εισερχόμενη σύνδεση TCP/IP.
Smurf	Στην επίθεση "smurf", οι επιτιθέμενοι χρησιμοποιούν πακέτα αιτήσεων ηχούς ICMP κατευθυνόμενα σε διευθύνσεις IP ανοικτής εκπομπής από απομακρυσμένες τοποθεσίες προκειμένου να δημιουργήσουν διεύθυνση άρνησης εξυπηρέτησης πολλών υποδικτύων (denial-of-service attack address of many subnets), δημιουργώντας μία μεγάλη, συνεχόμενη ροή από απαντήσεις ηχούς που πλημμυρίζουν το θύμα.
Teardrop	Η επίθεση teardrop είναι μία επίθεση άρνησης εξυπηρέτησης που εκμεταλλεύεται ένα ελάττωμα στην υλοποίηση παλαιότερων υλοποιήσεων TCP/IP. Μερικές υλοποιήσεις της τμηματοποίησης IP που επανασυνθέτουν κώδικα σε αυτές τις πλατφόρμες δεν χειρίζονται κατάλληλα τα επικαλυπτόμενα τμήματα IP.
Udpstorm	Η επίθεση Udpstorm είναι μία επίθεση άρνησης εξυπηρέτησης που προκαλεί δικτυακή συμφόρηση και καθυστέρηση (slowdown). Όταν πραγματοποιείται σύνδεση ανάμεσα σε δύο υπηρεσίες UDP, κάθε μία από τις οποίες παράγει έξοδο, αυτές οι δύο υπηρεσίες μπορούν να παράγουν ένα πολύ μεγάλο αριθμό πακέτων που μπορεί να οδηγήσει σε άρνηση εξυπηρέτησης στη μηχανή στην οποία προσφέρονται οι υπηρεσίες.

Επιθέσεις Remote to Local (R2L)

ftp_write	Η επίθεση Ftp-write είναι μία επίθεση Remote to Local User που εκμεταλλεύεται μία συνηθισμένη κακή ρύθμιση ανώνυμου ftp. Η επίθεση αυτή πραγματοποιείται όταν ένας απομακρυσμένος χρήστης ftp δημιουργεί ένα αρχείο .rhost σε ένα κατάλογο ανώνυμου FTP χωρίς προστασία εγγραφής και αποκτά τοπική πρόσβαση.
Guess_ passwd	Υπολογισμός συνθηματικών ενός έγκυρου χρήστη χρησιμοποιώντας απλές παραλλαγές του ονόματος λογαριασμού σε μία σύνδεση telnet.
Imap	Η επίθεση imap εκμεταλλεύεται μία υπερχείλιση προσωρινής μνήμης (buffer overflow) σε έναν εξυπηρετητή imap του Redhat Linux 4.2 η οποία επιτρέπει στους απομακρυσμένους επιτιθέμενους να εκτελέσουν αυθαίρετες εντολές με δικαιώματα root. Ο εξυπηρετητής imap πρέπει να τρέχει με δικαιώματα root έτσι ώστε ο επιτιθέμενος να μπορεί να έχει πρόσβαση στους φακέλους ταχυδρομείου και να πραγματοποιήσει κακή διαχείριση αρχείων εκ μέρους του χρήστη που έχει συνδεθεί.
Multihop	Σενάριο πολλαπλών ημερών στο οποίο ο χρήστης αρχικά εισβάλει σε ένα μηχάνημα.
Named	Η επίθεση named εκμεταλλεύεται μία υπερχείλιση προσωρινής μνήμης (buffer overflow) στην έκδοση BIND 4.9, σε εκδόσεις προηγούμενες από την BIND 4.9.7 και στην έκδοση BIND 8 σε εκδόσεις προηγούμενες από την 8.1.2. Μία ακατάλληλα ή κακόβουλα μορφοποιημένη αντίστροφη ερώτηση σε μία ροή TCP με προορισμό την υπηρεσία named μπορεί να προκαλέσει κατάρρευση στον εξυπηρετητή named ή να επιτρέψει σε έναν επιτιθέμενο να αποκτήσει δικαιώματα root.
Phf	Η επίθεση Phf εκμεταλλεύεται ένα "κακογραμμένο" πρόγραμμα CGI που επιτρέπει την εκτέλεση αυθαίρετων εντολών σε μία μηχανή με έναν λανθασμένα ρυθμισμένο εξυπηρετητή ιστού.
Sendmail	Η επίθεση sendmail εκμεταλλεύεται μία υπερχείλιση προσωρινής μνήμης στην έκδοση 8.8.3 του sendmail και επιτρέπει σε έναν απομακρυσμένο επιτιθέμενο να εκτελέσει εντολές με δικαιώματα υπερ-χρήστη. Στέλνοντας ένα κατάλληλα τροποποιημένο μήνυμα ηλεκτρονικού ταχυδρομείου σε ένα σύστημα στο οποίο εκτελείται μία έκδοση του sendmail με αδυναμίες, οι εισβολείς μπορούν να επιβάλουν στο πρόγραμμα sendmail την εκτέλεση αυθαίρετων εντολών με δικαιώματα root.
Snmpget-attack	Περιλαμβάνει την παρακολούθηση των πληροφοριών σε έναν δρομολογητή SNMP.

Snmpguess	Περιλαμβάνει τον υπολογισμό των συνθηματικών σε δρομολογητές SNMP.
Spy	Ένα σενάριο πολλαπλών ημερών στο οποίο ένα χρήστης εισβάλει σε μία μηχανή με σκοπό την εύρεση σημαντικών πληροφοριών και προσπαθεί να αποφύγει την ανίχνευση χρησιμοποιώντας διάφορες μεθόδους προκειμένου να αποκτήσει πρόσβαση.
Warezclient	Περιλαμβάνει τη λήψη παράνομου λογισμικού το οποίο προηγουμένως στάλθηκε μέσω ανώνυμου FTP κατά την επίθεση warezmaster.
Warezmaster	Περιλαμβάνει την αποστολή Warez (συνήθως παράνομων αντιγράφων λογισμικού) σε έναν εξυπηρετητή έχοντας δικαιώματα εγγραφής σε λογαριασμούς επισκεπτών.
xlock	Σε μία επίθεση xlock, ένας απομακρυσμένος επιτιθέμενος αποκτά τοπική πρόσβαση εξαπατώντας ένα νόμιμο χρήστη, που άφησε χωρίς επιτήρηση την κονσόλα του X, με στόχο να αποκαλυφθεί το συνθηματικό του. Ένας επιτιθέμενος μπορεί να παρουσιάσει μία τροποποιημένη έκδοση του προγράμματος xlock στην κονσόλα ενός χρήστη (η οποία έχει αφεθεί χωρίς επιτήρηση) ελπίζοντας ότι ο χρήστης θα πληκτρολογήσει το συνθηματικό του.

Επιθέσεις Probe

Ipsweep	Η επίθεση ipsweep είναι ένα τρόπος παρακολούθησης (sweep) για να καθοριστούν ποιοι κόμβοι είναι ενεργοί (listening) στο δίκτυο. Αυτό το είδος πληροφορίας είναι χρήσιμο σε έναν επιτιθέμενο που αναζητά μηχανές με αδυναμίες για την προετοιμασία επιθέσεων.
Mscan	Το mscan είναι ένα εργαλείο probing που χρησιμοποιεί τόσο μεταφορές ζώνης DNS ή/και εξαντλητικούς ελέγχους διευθύνσεων IP για να εντοπίσουν μηχανές με πιθανές αδυναμίες.
Nmap	Το nmap είναι ένα εργαλείο γενικού σκοπού για την πραγματοποίηση δικτυακού ελέγχου (scans). Το nmap υποστηρίζει πολλούς διαφορετικούς τύπους ελέγχων θυτών με επιλογές που περιλαμβάνουν έλεγχο SYN, FIN και ACK, για TCP και UDP, όπως και έλεγχο ICMP (Ping). Το πρόγραμμα nmap επιτρέπει επίσης στο χρήστη να καθορίσει τις θύρες που θα ελεγχθούν, το χρονικό διάστημα αναμονής μεταξύ των ελέγχων θυρών, και αν οι θύρες πρέπει να ελεγχθούν σειριακά ή με τυχαία σειρά.
Portsweep	Παρακολούθηση πολλών θυρών προκειμένου να καθοριστούν ποιες υπηρεσίες υποστηρίζονται σε κάθε κόμβο.
Saint	Το SAINT είναι το ολοκληρωμένο δικτυακό εργαλείο διαχειριστή (Security Administrator's Integrated Network Tool). Στην πιο απλή του μορφή, συλλέγει όσο περισσότερες πληροφορίες μπορεί για τους απομακρυσμένους κόμβους και δίκτυα εξετάζοντας δικτυακές υπηρεσίες όπως οι finger, NFS, NIS, ftp and tftp, rexd, statd, και άλλες υπηρεσίες.
Satan	Το Satan είναι ένας προκάτοχος του προγράμματος ελέγχου (scanning) SAINT. Ενώ το SAINT και το SATAN μοιάζουν πολύ στον στόχο και τον σχεδιασμό τους, οι συγκεκριμένες αδυναμίες που κάθε εργαλείο ελέγχει είναι λίγο διαφορετικές.

Παράρτημα Γ - Μεθοδολογία Bootstrap

Η μεθοδολογία bootstrap [Efron, 1994] είναι μία χρήσιμη μέθοδος για την προσομοίωση του υπολογισμού των εκτιμητών $\{f_k\}$ από πολλαπλά δείγματα $\{D_k\}$ που λαμβάνονται από μία κατανομή Ω. Καθώς κανονικά έχουμε ένα δείγμα D καθορισμένου μεγέθους, τα δείγματα D_k λαμβάνονται με επανάθεση από το D, την εμπειρική κατανομή, και όχι από το Ω, την πραγματική κατανομή.

Πιο συγκεκριμένα, για να υπολογίσουμε την απόδοση ενός αλγορίθμου, λαμβάνουμε δείγματα D_k με $n = |D_k| = |D|$. Για κάθε $i \in D_k$, έχουμε το κόστος c_i. Το οποίο χρησιμοποιούμε για να υπολογίσουμε το μέσο κόστος του δείγματος D_k:

$$C_k = \frac{\sum_{i \in D_k} c_i}{n}$$

Κατά αυτόν τον τρόπο λαμβάνουμε ένα δείγμα $S = \{C_k\}_{k=1}^{K}$ από K bootstrap εκτιμήσεις του αναμενόμενου κόστους. Είναι δυνατόν να χρησιμοποιήσουμε αυτό το δείγμα σαν μία εμπειρική κατανομή και να εκτιμήσουμε τις ποσότητες που μας ενδιαφέρουν. Στην περίπτωση μας εάν μας ενδιαφέρει η πιθανότητα το κόστος να έχει μία τιμή πάνω από ένα όριο θ μπορούμε να την υπολογίσουμε ως εξής:

$$P(C > \theta) = \int_{\theta}^{\infty} p(C)dC \approx \frac{1}{K} \sum_{k=1}^{K} u(C_k),$$

όπου $u(x)=0$ εάν $x \le \theta$ και 1 διαφορετικά.

Βιβλιογραφία

[Efron, 1994] B. Efron, R. J. Tibshirani, *"An Introduction to the Bootstrap"*, *Monographs on Statistics & Applied Probability"*, Vol. 57, Chapmann & Hall, Nov, Pub. Date: May 1994.

[Kdd, 1999] The UCI KDD Archive Information and Computer Science University of California, Irvine, *"Kdd Cup 1999 Data"*, October 1999, Available from <http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html>.

[Pickering, 2002] K.J. Pickering,*"Evaluating the Viability of Intrusion Detection System Benchmarking"*, Thesis TCC 402, Computer Engineering, University of Virginia, March 2002.

[Stolfo, 2000] S.J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, *"Cost-based Modeling and Evaluation for Data Mining With Application to Fraud and Intrusion Detection: Results from the JAM Project"*, In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX '00), 2000.

Γλωσσάριο

A program runs - Ένα πρόγραμμα "τρέχει"
Active network - Ενεργό δίκτυο
Ad hoc networks - Δίκτυα κατά περίσταση
Adaptive Learner for Alert Classification (ALAC) - Προσαρμοσμένη εκμάθηση για την ταξινόμηση συναγερμών
Agent - Πράκτορας
Amplification attack - Επίθεση ενίσχυσης
Anomaly Detection - Ανίχνευση Ανωμαλιών
Association Rules Analysis - Ανάλυση Κανόνων Συσχέτισης
Attached - Προσαρτημένου
Authentication - Αυθεντικοποιήση
Authentication Header - Επικεφαλίδα πιστοποίησης
Autonomous System - Αυτόνομο Σύστημα
Availability - Διαθεσιμότητα
Back propagation networks - Δίκτυα διανυσματικής οπισθοδιάδοσης
Backward secrecy - Οπισθόδρομη μυστικότητα
Bandwidth - Εύρος ζώνης
Bayesian - Μπαϋεζιανός (see also subjective)
Benchmark databases - Βάση δεδομένων που θεωρείται σημείο αναφοράς
Binomial - Διωνυμική
Biodiversity - Βιοδιαφοροποίηση
Block - Τμήμα
Bottleneck - Εμπόδιο
Branch points - Σημεία διακλάδωσης
Broadcast - Ανοικτή Εκπομπή
Browser - Πρόγραμμα Πλοήγησης
Buffer - Προσωρινή μνήμη
Buffer overflow - Υπερχείλιση προσωρινής μνήμης
Buffer overrun - Υπερφόρτωση προσωρινής μνήμης
Categories - Κατηγορίες
Central Processing Unit (CPU) - Κεντρική Μονάδα Επεξεργασίας
Chat room - Δωμάτιο συζητήσεων
Clandestine attacker - Κρυφός επιτιθέμενος
Class label - Ετικέτα κλάσης
Client - Πελάτης
Cluster - Σύμπλεγμα
Codeword - Λέξη κώδικα
Component weight - Βάρος συνισταμένης
Compromise - Παραβιάζω

Conditional - Υπό συνθήκη / Δεσμευμένη
Conditional class probability - Δεσμευμένη Πιθανότητα Κλάσεων
Conditional distribution - Δεσμευμένη κατανομή
Conditional observation density - Δεσμευμένη πυκνότητα παρατηρήσεων
Confidentiality - Εμπιστευτικότητα
Congestion triggered packet sampling and filtering - Δειγματοληψία και φιλτράρισμα πακέτων που ενεργοποιείται από πιθανή συμφόρηση
Consensus Roadmap for Defeating Distributed Denial of Service Attacks – Κοινός οδικός χάρτης για την αντιμετώπιση των Κατανεμημένων επιθέσεων Άρνησης Εξυπηρέτησης
Consequential costs - Επακόλουθα κόστη
Continuous - Συνεχής
Convolutional code - Κώδικας συσπείρωσης
Correlation Quality (CQ) - Ποιότητα Συσχετισμού
Corrupted - Αλλοιωμένο
Cost - sensitive - Με ευαισθησία ως προς το κόστος
Cost matrix - Πίνακας κόστους
Covariance - Συνδιακύμανση
Crashing -Κατάρρευση
Cross - validation - Διασταυρωμένη επικύρωση
Data - Δεδομένα
Data mining - Εξόρυξη δεδομένων
Decision making function - Συνάρτηση λήψης αποφάσεων
Degrading attack - Επίθεση υποβιβασμού
Denial of Service attacks (DoS) - Επιθέσεις άρνησης εξυπηρέτησης
Deterministic Packet Marking (DPM) - Ντετερμινιστικής σημείωση πακέτων
Differential packet filtering - Διαφορικό φιλτράρισμα πακέτων
Directed attack - Κατευθυνόμενη επίθεση
Discrete - Διακριτός
Discrete Cosine Transform (DCT) - Μετατροπή Διακριτού Συνημιτόνου
Disruptive attack - Καταστρεπτική επίθεση
Distributed Denial of Service attacks (DDoS) - Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης
Distribution - Κατανομή
Domain - Δικτυακή περιοχή
Domain Name Service (DNS) - Υπηρεσία διάθεσης ονομάτων και διευθύνσεων που χρησιμοποιούνται στο Διαδίκτυο
Downloading - Κατέβασμα, λήψη
Dynamic Probabilistic Packet Marking (DPPM) - Δυναμική πιθανοτική σήμανση πακέτων
Echo request - Αίτηση ηχούς

Edge router - Ακραίος δρομολογητής
E-government - Ηλεκτρονική διακυβέρνηση
Embedding strength - Δύναμη ενσωμάττωσης
Emergence - Ανάδειξη
Emergent Self-Organising Maps (eSOMs) - Αναδυούμενοι Αυτο-Οργανούμενοι Χάρτες
Empirical - Εμπειρικός
Empirical value - Εμπειρική τιμή
Endhost - Ακραίος κόμβος
Epoch - Εποχή
Estimator - Εκτιμητής
Event logs - Αρχεία γεγονότων καταγραφής
Expectation - Αναμενόμενη τιμή
Expected cost - Αναμενόμενο κόστος
Expert System - Έμπειρο Σύστημα
Exponentiation - Εκθετικές υψώσεις
External attackers - Εξωτερικούς επιτιθέμενους
False negatives - Λανθασμένοι αρνητικοί συναγερμοί
False positives - Λανθασμένοι θετικοί συναγερμοί
Fast Internet Traceback (FIT) - Γρήγορη ιχνηλάτηση Διαδικτύου
Filtering - Φιλτράρισμα
Fine-grained - Με μεγαλύτερη ευκρίνεια
Finite Automata - Πεπερασμένα Αυτόματα
Finite State Machines - Μηχανές Πεπερασμένων Καταστάσεων
Firewall - Αντι-πυρικό τείχος
Flag - Σημαία
Flood attack - Επίθεση πλημμύρας
Forensic analysis - Ανάλυση σήμανσης και ψηφιακών πειστηρίων
Forge - Παραποιώ
Forward secrecy - Πρόσθια μυστικότητα
Free parameter - Ελεύθερη παράμετρος
Freezing - Πάγωμα
Frequentist - Συχνοτικός, Κλασσικός (see Empirical)
Frequentist model selection - Εμπειρικές μεθόδους επιλογής μοντέλου
Gaussian - Γκαουσσιανή
Guest account - Λογαριασμός επισκέπτη
Handler - Χειριστής
Hash function - Συνάρτηση κατακερματισμού
Heuristic - Ευριστική
Hidden layer - Κρυφό επίπεδο
Hidden Markov Models - Κρυφά Μαρκοβιανά Μοντέλα

Host - Κόμβος
Hyperbolic tangent - Υπερβολική εφαπτομένη
ICMP echo request - Αίτηση ηχούς ICMP
Image Fidelity (IF) - Ακρίβεια Εικόνας
Implicit key authentication - Πλήρης πιστοποίηση κλειδιού
Infected - Μολυσμένος
Inference - Συμπερασματολογία
Integrity - Ακεραιότητα
Intention driven ICMP traceback (iTrace)- Ιχνηλάτηση ICMP που καθορίζεται από την πρόθεση
Internal attackers - Εσωτερικούς επιτιθέμενους
Internet - Διαδίκτυο
Internet Service Provider (ISP) - Πάροχος Υπηρεσιών Διαδικτύου
Intrusion Detection System - Σύστημα Ανίχνευσης Εισβολών
IP source address - Διεύθυνση πηγής IP
Iteration - Επανάληψη
Just Noticeable Difference (JND) - Απλή Αντιληπτή Διαφορά
Kernel - Πυρήνας
Key independence - Ανεξαρτησία κλειδιού
Key secrecy - Μυστικότητα κλειδιού
Labeled - Χαρακτηρισμένο
Lattice code - Κώδικας δικτυωτού πλέγματος
Learning rate - Ρυθμός εκμάθησης
Legitimate packets - Νόμιμα πακέτα
Likelihood - Πιθανοφάνεια
Likelihood ratio test - Έλεγχος πηλίκου πιθανοφανειών
Linear classifier - Γραμμικός ταξινομητής
Link - Δικτυακή ζεύξη
Link-testing - ελέγχου συνδέσμου
Link-testing traceback - Ιχνηλάτιση ελέγχου συνδέσμου
Logistic regression - Λογιστική παλινδρόμηση
Loss function - Συνάρτηση απώλειας
Luminance masking - Κάλυψη φωτεινότητας
Machine Learning - Μηχανική εκμάθηση
Malformed packet - Τροποποιημένο πακέτο
Malicious - Κακόβουλος
Management Information Base (MIB) - Πληροφοριακή Βάση Διαχείρισης
Mannually - Χειρωνακτικά
Marginal - Περιθωριο
Marginalizing - Περιθωριοποιώντας
Mark - Σημάδι

Masking components - Στοιχεία επικάλυψης
Masquerader - Μεταμφιεσμένος
Master - Επιτελής
Master - Κύριο
Maximum likelihood - Μεγιστη αληθοφάνεια
Max-min fair server-centric router throttles - Ρύθμιση δρομολογητών μεγίστων-ελαχίστων βασισμένων στους εξυπηρετητές
Mean Square Error (MSE)) - Μέσο Τετραγωνικό Λάθος
Measurable - Μετρήσιμος
Measure - Μέτρο
Meta-detection - Μετα-ανίχνευση
Misconfiguration - Κακή ρύθμιση
Misuse detection - Ανίχνευση κακής χρήσης
Multicast - Πολλαπλής εκπομπής
Multilayer Perceptron (MLP) - Πολυ-επίπεδου perceptron
Multinomial - Πολυωνυμική
Naïve Bayes classifier - Ταξινομητή απλοϊκού μοντέλου
Nested - Εγκλωβισμένος
Network Allocation Vector (NAV) - Διάνυσμα ανάθεσης του δικτύου
Network Device Level - Επίπεδο Δικτυακής Συσκευής
Neuro-Immune - Νευρό-απρόσβλητης
Neuron - Νευρώνας
Node - Κόμβος
Non-repudiation - Καταλογισμός ευθύνης
Normalized Cross Correlation (NCC) - Κανονικοποιημένος Διασταυρούμενος Συσχετισμός
Off-line - Εκτός δικτύου
Operating System - Λειτουργικό Σύστημα
Operational costs - Κόστη λειτουργίας
Outlier Detection - Ανίχνευση εκτοπών
Overfitting - Υπερπροσαρμογή
Overlay network - Δίκτυο επικάλυψης
Packet digests - Περιλήψεις πακέτων
Packet logging - Καταγραφή πακέτων
Packet marking - Σήμανση πακέτου
Packetscore - Βαθμολογία πακέτων
Parameter - Παράμετρος
Partially open connections - Μη-ολοκληρωμένες συνδέσεις
Password - Συνθηματικό
Path Information Caching and Aggregation (PICA) - Προσωρινή αποθήκευση και συνάθροιση πληροφοριών μονοπατιού

Pattern Matching - Ταίριασμα Προτύπου
Payload - Ωφέλιμο φορτίο
Peak Signal to Noise Ratio (PSNR) - Κορυφή Ποσοστού Σήματος προς Θόρυβο
Peer-to-peer network - Δίκτυο ομοτίμων
Penetration - Εισβολή
Per-aggregate-class - Διαχωρισμός της κίνησης σε ομαδοποιημένες κλάσεις
Point-to-point - Σημείο-προς-σημείο
Pooling - Συγκέντρωση
Port - Θύρα
Principal Component Analysis (PCA) - Ανάλυση κύριων στοιχείων
Proactive - Προληπτικό
Proactive server roaming - Προληπτική περιφορά εξυπηρετητή
Probabilistic - Πιθανοτικός
Probabilistic Packet Marking (PPM) - Πιθανοτική σήμανση πακέτων
Public Key Infrastructure (PKI) - Υποδομή Δημόσιου Κλειδιού
Pushback - Ώθηση προς τα πίσω
Quality of Service - Ποιότητα υπηρεσίας
Quantize - Κβαντοποιώ
Radio channel - Ασύρματο ραδιοδίαυλο
Random way point - Κατεύθυνσης τυχαίας οδού
Rate throttles - Ρυθμιστική βαλβίδα
Reactive - Αντίδρασης
Reference Marks - Σημείο Αναφοράς
Reference Pattern - Πρότυπο Αναφοράς
Remote - Απομακρυσμένος
Replacement - Επανάθεση
Resample - Επαναδειγματολειπτώ
Resilient Propagation - Ανθεκτικής Διάδοσης
Resource accounting - Κατάτμηση πόρων
Resource pricing - Εκτίμηση πόρων
Risk - Κίνδυνος
Rooted tree- Δένδρο με ρίζα
Round robin - Εκ περιτροπής ανάθεση
Router - Δρομολογητής
Router Interface Marking (RIM) - Σήμανση Διεπαφής Δρομολογητή
Sampling - Δειγματοληψία
Scan - Δικτυακός έλεγχος
Script - Πρόγραμμα
Server - Εξυπηρετητή
Set - Σύνολο
Shared - Διαμοιραζόμενο

Sigmoid - Σιγμοειδή
Signal to Noise Ratio (SNR) - Ποσοστό Σήματος προς Θόρυβο
Signature - Υπογραφή
Simulation - Προσομοίωση
Slave - Υποτελής
Slowdown - Καθυστέρηση
Sniffer - Ελεγκτής δικτυακής κίνησης
Space - Χώρος
Spacing - Διάστημα
Specifications - Προδιαγραφές
Spoofing - Παραποίηση
Spring Layous -Ελατηριακές επικαλύψεις
Stream of packets - Ροή πακέτων
Strength Parameter - Παράμετρος Δύναμης
Subjective - Υποκειμενικός
Subjective Bayesian - Υποκειμενική ερμηνεία των πιθανοτήτων
Support Vector Machines (SVM) - Μηχανές Διανυσμάτων Υποστήριξης
Survivabilty - Επιβιωσιμότητα
Sweep - Παρακολούθηση
Switch - Μεταγωγέας
Test - Έλεγχος
Three-way handshake - Χειραψία τριών τρόπων
Threshold - Κατώφλι
Throttling - Κατάπνιξη
Topology preserving - Τοπολογικά διατηρήσιμη
Traceback - Ιχνηλάτηση
Trade-off - Συμβιβασμός
Traffic Engineering - Οργάνωση και διακίνηση δικτυακής κυκλοφορίας
Transit State Analysis - Ανάλυση Μετάβασης Καταστάσεων
Trojan horse - Δούρειος Ίππος
Tune - Ρυθμίζω
Tunnel - Ενθυλάκωση
Unauthorized - Μη εξουσιοδοτημένος
Unsupervised - Μη επιτηρούμενης
Uploading - Ανέβασμα, αποστολή
Upstream - Κανάλι ανόδου
Variance - Διακύμανση
Vulnerability - Ευπάθεια
Watermarking - Υδατογράφηση
Watson Distance (WD) - Απόσταση Watson
Weight initialization method - Μέθοδος αρχικοποίησης βαρών

Weighted class error - Κόστος ταξινόμησης με βάρη
Wireless Local Area Network (WLAN) - Ασύρματα τοπικά δίκτυα
Worm - Σκουλήκι
Wrapper algorithm - Αλγόριθμος κάλυψης

Ακρώνυμα

2D- 2-Dimensional
ACK - Acknowledge
AH - Authentication Header
ALAC - Adaptive Learner for Alert Classification
ANN - Artificial Neural Networks
AODV - Ad hoc On demand Distance Vector
BGP - Border Gateway Protocol
CBQ - Class Based Queuing
CBR - Constant Bit Rate
CERT - Computer Emergency Response Team
CIA - Cooperative Itinerant Agents
CIAC - Computer Incident Advisory Capability
CPU - Central Processing Unit
CQ - Correlation Quality
CQ - Correlation Quality
CSI - Computer Security Institute
CTS - Clear To Send
DCT - Discrete Cosin Transform
DDoS - Distributed Denial of Service
DiffServ - Differentiated Services
DNS - Domain Name Service
DoS - Denial of Service
DPM - Deterministic Packet Marking
DPPM - Dynamic Probabilistic Packet Marking
DR - Detection Rate
eSOM - emergent Self Organizing Maps
FAQ - Frequently Asked Questions
FBI -Federal Bureau of Investigation
FIT - Fast Internet Traceback
FN - False Negatives
FP - False Positives
FR - False alarm Rate
GK - Global Key
GKA - Group Key Agreement
GMM - Gaussian Mixture Model
HIP - History based IP
HMM - Hidden Markov Models
HVS - Human Visual System
ICMP - Internet Control Message Protocols

IDS - Intrusion Detection System
IF - Image Fidelity
IF - Image Fidelity
IGMP - Internet Group Message Protocol
IIS - Internet Information Server
IKA - Internet Key Agreement
IntServ - Integrated Services
IP - Internet Protocol
IRC - Internet Relay Chat
ISP - Internet Service Provider
iTrace - ICMP Traceback
JND - Just Noticeable Difference
KDD - Knowledge Discovery in Databases
KSOM - Kohonen Self Organizing Maps
LK - Local Keys
MAC - Media Access Control
MAC - Message Authentication Code
MANET - Mobile Ad hoc Network
MLP - Multilayer Perceptron
MSE - Mean Square Error
MSE - Mean Square Error
NAV - Network Allocation Vector
NCC - Normalise Cross Correlation
NCC - Normalized Cross Correlation
NSOM - Network-based Self-Organising Map
OS - Operating System
PCA - Principal Component Analysis
PCH - Percentage of the Change in the number of Hops
PCR - Percentage of the Change in Route errors
PI - Path Identification
PICA - Path Identification Caching and Aggregation
PKI - Public Key Infrastructure
PPM - Probabilistic Packet Marking
PSNR - Peak Signal to Noise Ratio
PSNR - Peak Signal to Noise Ratio
QoS - Quality of Service
R2L - Remote to Local
RERR -Route Error
RIM - Router Interface Marking
RPROP - Resilient Propagation
RREP - Route Reply

RREQ - Route Request
RSVP - Resource Reservation Protocol
RTS - Ready To Send
SAVE - Source Address Validity Enforcement
SDSC - San Diego Supercomputer Service
SNR - Signal to Noise Ratio
SNR - Signal to Noise Ratio
SOS - Secure Overlay Services
SSh - Secure Shell
SVM - Support Vector Machine
TCP SYN
TFN - Tribe Flood Network
TGDH - Tree Group Diffie Hellman
TN - True Negatives
TOS - Type Of Service
TP - True Positives
TTL - Time To Live
TTP - Trusted Third Party
U2R - User to Root
UCSD – University of California San Diego
UDP – User Datagram Protocol
VIPnets - Virtual IP networks
WD - Watson Distance
WLAN - Wireless Local Area Network
WP - Watson Distance
WWW - World Wide Web
XOR - exclusive OR