ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανίχνευση επιθέσεων με την μέθοδο της εντροπίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μάριος Π. Γύφτος

Επιβλέπων : Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβρης 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανίχνευση επιθέσεων με την μέθοδο της εντροπίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μάριος Π. Γύφτος

Επιβλέπων : Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 18η Οκτώβρη 2016.

.....	.....	.....
Μιλτιάδης Αναγνώστου	Ευστάθιος Συκάς	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επίκουρη Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβρης 2016

.....
Μάριος Π. Γύφτος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΕΥΧΑΡΙΣΤΙΕΣ

Η ολοκλήρωση της διπλωματικής αυτής εργασίας αποτελεί το αποκορύφωμα όλων των προσπαθειών μου να αποκτήσω τις κατάλληλες γνώσεις και να διευρύνω τους επιστημονικούς μου ορίζοντες γενικά, αλλά κυρίως στον τομέα που μου κέντρισε περισσότερο το ενδιαφέρον κατά την φοίτησή μου στο Εθνικό Μετσόβιο Πολυτεχνείο. Η παρούσα διπλωματική εργασία αποτελεί ουσιαστικά την πρώτη μου ολοκληρωμένη και αυτόνομη προσπάθεια να εκθέσω τις γνώσεις μου στον τομέα της ασφάλειας δικτύων υπολογιστών και συγκεκριμένα στον κλάδο της ανίχνευσης επιθέσεων. Στο σημείο αυτό θεωρώ υποχρέωσή μου να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή Μιλτιάδη Αναγνώστου, που μου έδωσε την ευκαιρία να ασχοληθώ με τον τομέα αυτό, καθώς και για όλη τη συνεργασία και την εμπιστοσύνη που μου έδειξε. Παράλληλα θα ήθελα να ευχαριστήσω ιδιαιτέρως τον κύριο Βασίλη Ασθενόπουλο, διδακτορικό ερευνητή, που με ενθουσιασμό συνέβαλε καταλυτικά στην επιλογή και περαίωση της εργασίας αυτής. Είμαι ευγνώμων για τη διάθεση του χρόνου του και την προθυμία του κάθε φορά που ζήτησα τη βοήθειά του. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου και ιδιαίτερα του γονείς μου, για την υποστήριξή τους και τη συμπαράστασή τους, καθώς και την αρωγή τους όποτε χρειάστηκε, όχι μόνο κατά τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας, αλλά και όλων των χρόνων της φοιτητικής μου πορείας.

Περίληψη

Το βασικό πρόβλημα του πεδίου της ασφάλειας των δικτύων υπολογιστών είναι η έγκαιρη ανίχνευση και αντιμετώπιση επιθέσεων σε ένα δίκτυο. Στην σύγχρονη εποχή οι κυβερνοεπιθέσεις αποτελούν όλο και πιο συχνό φαινόμενο με αποτέλεσμα να θέτουν σε κίνδυνο την ασφάλεια της πληροφορίας. Η έγκαιρη ανίχνευση των επιθέσεων κρίνεται ιδιαίτερης σημασίας. Στα πλαίσια αυτής της εργασίας θα εξετάσουμε την ανίχνευση τέτοιων επιθέσεων και πιο συγκεκριμένα των κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDOS). Το ερώτημα που εξετάζει η παρούσα έρευνα είναι κατά πόσον είναι εφικτή η ανίχνευση επιθέσεων άρνησης υπηρεσίας με την στατιστικομαθηματική μέθοδο της εντροπίας. Πιο συγκεκριμένα, με ποια παραμετροποίηση της, δηλαδή με ποια από τα χαρακτηριστικά (features) πακέτων ή ροών, που συλλέγονται κατά την παρακολούθηση της κίνησης εντός ενός δικτύου, επιτυγχάνεται αποδοτικότερη ανίχνευση των επιθέσεων DDOS. Ως αποδοτική ανίχνευση θεωρείται η ανίχνευση που καταρχάς εντοπίζει επιτυχώς την επίθεση και εν συνεχεία παρουσιάζει όσο το δυνατόν λιγότερες λανθασμένες ενδείξεις (false positives, false negatives). Η εφαρμογή της μεθόδου της εντροπίας υλοποιείται σε δείγματα δεδομένων που περιέχουν «ομαλή» κίνηση και «ανώμαλη» κίνηση άρνησης υπηρεσίας. Τέλος, επιχειρείται ο προσδιορισμός ενός δείκτη διάκρισης της κίνησης (classifier) στις παραπάνω δύο κατηγορίες.

Λέξεις Κλειδιά:

ανίχνευση παρεισφρήσεων, κατανεμημένες επιθέσεις άρνησης υπηρεσίας, στατιστικές μέθοδοι, εντροπία, ασφάλεια

Abstract

A prominent problem in the field of computer network security is the early detection and response to attacks on a network. Nowadays cyberattacks have become common. Early detection is of particular importance. We investigate the detection of such attacks, and more specifically of distributed denial of service attacks (DDOS). The question addressed in this research is whether it is possible to detect denial of service attacks by an entropy-based detection method. More specifically, with which configuration, characteristics (features) of packets or flows collected during network traffic monitoring, we can achieve effective detection of DDOS attacks. A detection method is considered effective when, firstly, it successfully detects the attack and secondly presents the least possible errors (false positives, false negatives). The application of an entropy based method is implemented in datasets containing normal traffic and malicious denial of service traffic. Finally, we attempt to define a threshold based classifier, as a tool to distinguish between malicious and normal traffic.

Key Words:

Intrusion detection, distributed denial of service attacks, DDoS, traffic analysis, entropy, security.

Περιεχόμενα

Εικόνες

Πίνακες

Διαγράμματα

Έννοιες/ Ακρώνυμα

DOS (denial-of-service attack): Επίθεση άρνησης υπηρεσίας

DDOS (distributed denial-of-service): Κατανεμημένη επίθεση άρνησης υπηρεσίας

Malware: Κακόβουλο λογισμικό

Ευπάθεια (Vulnerability): Η ύπαρξη μιας αδυναμίας, ενός σχεδιαστικού ή προγραμματιστικού λάθους (implementation error) το οποίο μπορεί να οδηγήσει σε μη αναμενόμενη κατάσταση διακινδυνεύοντας την ασφάλεια του συστήματος.

Εκμετάλλευση (Exploit): Η μέθοδος μέσω της οποία επιτυγχάνεται η παραβίαση της ασφάλειας ενός συστήματος με την εκμετάλλευση ευπαθειών (vulnerabilities).

ICMP protocol: Το πρωτόκολλο Internet Control Message Protocol (ICMP) αποτελεί ένα από τα βασικά πρωτόκολλα του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους.

SNMP protocol: Το πρωτόκολλο SNMP (Simple Network Management Protocol) αποτελεί μέρος του συνόλου διαδικτυακών πρωτοκόλλων (Internet Protocol - IP) όπως αυτά έχουν οριστεί από την αρμόδια επιτροπή (Internet Engineering Task Force -IETF). Το συγκεκριμένο πρωτόκολλο εφαρμόζεται στα συστήματα διαχείρισης δικτυών και δικτυακών συσκευών επιτρέποντας, εφόσον χρειάζεται, την παρέμβαση του διαχειριστή. Αποτελείται από ομάδα προτύπων διαχείρισης δικτύου και περιλαμβάνει ένα πρωτόκολλο επιπέδου εφαρμογών (application layer), ένα σχήμα βάσης δεδομένων και μια ομάδα από σύνολα δεδομένων.

Ψευδώς θετικά (False Positives): Τα ψευδώς θετικά αποτελέσματα αποτελούν τις λανθασμένες επισημάνσεις που παράγει ένα σύστημα ανίχνευσης παρεισφρήσεων (Intrusion Detection System - IDS), όταν ανιχνεύσει κάποιο γεγονός ως περίπτωση πιθανής επίθεσης ενώ δεν είναι. Τα ψευδώς θετικά ενδέχεται να προκύψουν από κακή ρύθμιση του IDS ή από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν σαφώς από μία επίθεση.

Ψευδώς Αρνητικά (False Negatives): Τα ψευδώς αρνητικά αποτελούν τις περιπτώσεις επιθέσεων τις οποίες το IDS δεν κατάφερε να επισημάνει. Τα ψευδώς αρνητικά συνήθως προκύπτουν από κακή ρύθμιση του IDS ή από την εμφάνιση μίας νέας επίθεσης, για την οποία δεν υπάρχει προηγούμενη καταγραφή.

Επιθέσεις μηδενικής μέρας (zero day): Επιθέσεις που εκμεταλλεύονται μια ευπάθεια μηδενικής μέρας. Μια **ευπάθεια μηδενικής μέρας** είναι ένας όρος για μια νέα καινούρια ευπάθεια, που ο προμηθευτής κάποιας εφαρμογής δεν γνωρίζει ακόμα και επομένως δεν υπάρχει το αντίστοιχο patch.

Ωφέλιμο φορτίο (Payloads): ο όρος αναφέρεται στα επιβλαβή αποτελέσματα της εκτέλεσης λογισμικού.

SBA (Signature Based Approach): Προσέγγιση Υπογραφής

ABA (Anomaly Based Approach): Προσέγγιση Ανωμαλιών

Antivirus: Λογισμικό ανίχνευσης κακόβουλου λογισμικού

Bits: Δυαδικά ψηφία

MITM: man-in-the-middle attack, επίθεση ενδιάμεσου

C&C: Command and Control server

PCA: Principal Component Analysis, Ανάλυση σε Πρωτεύουσες Συνιστώσες

Botnet: Ένα botnet είναι ένα διασυνδεδεμένο δίκτυο υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό χωρίς τη γνώση του χρήστη και ελέγχονται από εγκληματίες του κυβερνοχώρου. Συνήθως χρησιμοποιούνται για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου spam, για την μετάδοση ιών και συμμετέχουν και σε άλλες εγκλήματικές πράξεις στον κυβερνοχώρο. Μερικές φορές είναι γνωστό ως στρατός ζόμπι.

Bot: 'Ενα ανεξάρτητο κακόβουλο λογισμικό, δηλαδή ένα αυτόνομο πρόγραμμα που μπορεί να προγραμματιστεί και να τρέξει από το λειτουργικό σύστημα. Συνήθως ως bot αναφέρεται ένας μολυσμένος υπολογιστής με το εν λόγω κακόβουλο λογισμικό.

Peer-to-peer (P2P): Ένα δίκτυο υπολογιστών **peer-to-peer** (ή **P2P**) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

Κεφάλαιο 1: Εισαγωγή

1.1 Εισαγωγή

Το κεφάλαιο αυτό έχει στόχο την εισαγωγή του αναγνώστη στο γνωστικό αντικείμενο που πραγματεύεται η παρούσα εργασία προσδιορίζοντας τόσο το πρόβλημα όσο και το ερώτημα, το οποίο θα προσπαθεί να απαντηθεί στην συνέχεια.

Η ταχύτατη εξέλιξη στον τομέα της τεχνολογία και συγκεκριμένα στον τομέα του διαδικτύου έχει αυξήσει σημαντικά το πλήθος των δεδομένων που ανταλλάσσονται, τόσο ανάμεσα στα επιμέρους ιδιωτικά δίκτυα όσο και μέσω του διαδικτύου. Πολλά από τα δεδομένα που ανταλλάσσονται χαρακτηρίζονται ως ευαίσθητα δεδομένα, οπότε τίθεται το θέμα της ασφάλειας της πληροφορίας που μεταδίδεται μέσω του διαδικτύου. Οι κακόβουλοι χρήστες του διαδικτύου (hackers) επιδιώκουν να υποκλέψουν τέτοιου είδους πληροφορίες (ευαίσθητα δεδομένα) Σε άλλες περιπτώσεις προσπαθούν απλώς να παρακωλύσουν την παροχή υπηρεσιών με σκοπό να βλάψουν τον πάροχο της υπηρεσίας για λογαριασμό ενός τρίτου ή με σκοπό να ζητήσουν λύτρα από το θύμα. Παρατηρείται λοιπόν μια διαρκής αύξηση των κυβερνοεπιθέσεων και ιδιαίτερα αυτών που είναι στοχευμένες και προηγμένες (Advanced Persistent Threats), οι οποίες θεωρούνται ως η σημαντικότερη απειλή για την ασφάλεια των πληροφοριών και των συστημάτων που τις υποστηρίζουν. Αν και στην σύγχρονη αγορά υπάρχει ένας σημαντικός αριθμός τεχνολογικών λύσεων για την ασφάλεια των συστημάτων, η συνεχώς αυξανόμενη ευφυΐα των επιτιθέμενων και η ταυτόχρονη αδυναμία των αμυνόμενων δημιουργεί μία κατάσταση ανασφάλειας και περιορισμένης αποτελεσματικότητας στον εντοπισμό των επιθέσεων. Καθώς όλο και περισσότερο η πληροφορία γίνεται διαθέσιμη σε ηλεκτρονική μορφή μέσω του διαδικτύου, η έννοια της ύπαρξης ενός προηγμένου εχθρού, ο οποίος συνεχώς στοχοποιεί την πληροφορία αυτή, με στόχο την απόκτηση δεδομένων είναι αναπόφευκτη.

Συνεπώς οι διαχειριστές των δικτύων αντιμετωπίζουν όλο και πιο συχνά ένα ευρύ φάσμα από ασυνήθιστα γεγονότα κάποια από τα οποία, άλλα όχι όλα, μπορεί να είναι κακόβουλα. Οι διαχειριστές πρέπει να ανιχνεύσουν αυτές τις ανωμαλίες όταν συμβαίνουν και στην συνέχεια να τις κατηγοριοποιήσουν ώστε να διαλέξουν την κατάλληλη μέθοδο αντιμετώπισης. Η πρωταρχική πρόκληση στην αυτοματοποιημένη ανίχνευση και στην κατηγοριοποίηση των ανωμαλιών είναι ότι οι ανωμαλίες αυτές αποτελούν ένα μεγάλο εύρος γεγονότων, από κατάχρηση ενός δικτύου (network scans, DOS, DDOS attacks) σε ασυνήθιστη συμπεριφορά των χρηστών του δικτύου ακόμη και σε νέα, άγνωστα γεγονότα.

Οι επιθέσεις άρνησης υπηρεσίας (DDoS) αποτελούν έναν συνήθη τύπο επίθεσης εξαιτίας της διαθεσιμότητας δωρεάν εργαλείων και φθηνών διαδικτυακών υπηρεσιών που επιτρέπουν σε οποιονδήποτε με πρόσβαση στο Internet να ξεκινήσει μια επίθεση. Αυτό έχει οδηγήσει σε έντονη αύξηση της συχνότητας, του μεγέθους και της πολυπλοκότητα των επιθέσεων τα τελευταία χρόνια. Χαρακτηριστική είναι η δημοσίευση της εταιρίας Arbor Networks η οποία δείχνει μια συνεχή κλιμάκωση τόσο στο μέγεθος όσο και στη συχνότητα των επιθέσεων [1]. Συνεπώς, ο προσδιορισμός μεθόδων ανίχνευσης τέτοιων επιθέσεων κρίνεται ιδιαίτερα σημαντικός για την ασφάλεια της μετάδοσης της πληροφορίας μέσω του διαδικτύου. Ακολουθεί μια ιστορική αναδρομή σχετικά με τις μεθόδους ανίχνευσης παρεισφρήσεων δίνοντας έμφαση στις σύγχρονες μεθόδους ανίχνευσης και πως η παρούσα έρευνα εξετάζει ένα ιδιαίτερα σημαντικό κομμάτι αυτών των μεθόδων.

1.2 Ιστορική Αναδρομή

Η πρώτη μέθοδος ανίχνευσης ανωμαλιών για την ανίχνευση παρεισφρήσεων προτάθηκε σχεδόν πριν από 40 χρόνια [2]. Σήμερα, παρόλο που ένα μεγάλο μέρος της επιστημονικής κοινότητας ασχολείται με το θέμα της ανίχνευσης ανωμαλιών δικτύου, το πρόβλημα της εύρεσης μιας γενικής μεθόδου για ένα ευρύ φάσμα ανωμαλιών δικτύου εξακολουθεί να είναι άλυτο. Τα ευρέως διαθέσιμα συστήματα που χρησιμοποιούνται για την ανίχνευση παρεισφρήσεων είναι αναποτελεσματικά ενάντια σε ένα σύγχρονο κακόβουλο λογισμικό (malware). Τέτοια συστήματα, ως επί το πλείστον, χρησιμοποιούν τεχνικές που βασίζονται στα χαρακτηριστικά των επιθέσεων ή αλλιώς στις υπογραφές τους (misuse-based techniques ή signature-based techniques). Αυτή η προσέγγιση παρουσιάζει ελλείψεις [3] [4]. Οι υπογραφές περιγράφουν μόνο παράνομα μοτίβα στην κίνηση δικτύου, οπότε απαιτείται γνώση των μοτίβων αυτών εκ των προτέρων [5]. Ως αποτέλεσμα, οι λύσεις που βασίζονται στις υπογραφές δεν μπορούν να αντιμετωπίσουν νέες τεχνικές επιθέσεων και επιθέσεις που δεν είναι ακόμη γνωστές, επιθέσεις μηδενικής ημέρας (0-day attacks) [3]. Επιπλέον, δεν είναι σε θέση να εντοπίσουν μία συγκεκριμένη επίθεση μέχρι ένας κανόνας για την αντίστοιχη ευπάθεια να έχει δημιουργηθεί, δοκιμαστεί, κυκλοφορήσει και αναπτυχθεί, το οποίο συνήθως απαιτεί ένα μεγάλο χρονικό διάστημα. Ως εκ τούτου, μια διαφορετική προσέγγιση των τεχνικών ανίχνευσης ανωμαλιών δικτύου κρίνεται απαραίτητη ως μία πιθανή λύση για τη συμπλήρωση των λύσεων που προσφέρουν τα συστήματα που βασίζονται στις υπογραφές. Οι μέθοδοι εντροπίας που βασίζονται στις κατανομές των χαρακτηριστικών δικτύου παρουσιάζουν ιδιαίτερο ενδιαφέρον ως μία τέτοια περίπτωση όπου αξίζει να διερευνηθεί εάν και κατά πόσον οι προσεγγίσεις αυτές, που βασίζονται στην εντροπία, είναι αποτελεσματικές στην ανίχνευση ανωμαλιών δικτύου, που προκαλούνται από σύγχρονα κακόβουλα λογισμικά όπως αυτά των botnet [6] [7]. Τα Botnet είναι ένα σύνολο μολυσμένων μηχανημάτων (bots) που ελέγχεται μέσω εξυπηρετητών (servers) Command and Control (C & C) από τους επιτιθέμενους. Η συχνότητα εμφάνισης του εν λόγω κακόβουλου λογισμικού, καθώς και το επίπεδο πολυπλοκότητας του αυξάνεται κάθε χρόνο [8]. Τα πλήγματα από αυτού του είδους κακόβουλου λογισμικού μπορούν να πάρουν πολλές σοβαρές μορφές συμπεριλαμβανομένης της απώλειας σημαντικών δεδομένων ή χρημάτων. Η προσέγγιση που βασίζεται στην εντροπία για την ανίχνευση ανωμαλιών, που προκαλούνται από botnet, σε ένα τοπικό δίκτυο δεν έχει διερευνηθεί. Οι μέθοδοι που βασίζονται στην εντροπία και έχουν προταθεί στο παρελθόν αφορούν μεγάλο εύρος διάφορων worms (που δεν εμφανίζουν την ίδια συμπεριφορά με τα botnets) ή διαφορετικά είδη κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) σε δίκτυα υψηλής ταχύτητας [7] [9] [10]. Σε αυτή την πτυχιακή προτείνουμε μια αποτελεσματική μέθοδο βασισμένη στην εντροπία για την ανίχνευση κατανεμημένων επιθέσεων άρνησης υπηρεσιών.

1.3 Βιβλιογραφική Ανασκόπηση

Αυτή η ενότητα αναφέρεται σε σχετικές έρευνες στον τομέα της ανίχνευσης ανωμαλιών δικτύου. Η ενότητα ξεκινά με μια γενική επισκόπηση των τελευταίων εξελίξεων σε αυτό το ευρύ θέμα. Στη συνέχεια, παρουσιάζεται πιο λεπτομερής περιγραφή των τεχνικών ανίχνευσης ανωμαλιών που συνδέονται στενά με την προσέγγιση που προτείνεται σε αυτό το άρθρο.

1.3.1 Γενική επισκόπηση τεχνικών ανίχνευσης ανωμαλιών

Το πρόβλημα της ανίχνευσης ανωμαλιών έχει μελετηθεί εκτενώς. Υπάρχουν πολλές έρευνες, άρθρα ανασκόπησης, καθώς και βιβλία σχετικά με αυτό το ευρύ θέμα. Ένα εκτενές εύρος ερευνών επί τεχνικών ανίχνευσης ανωμαλιών βρίσκεται σε πολλά βιβλία [11] [12] [13] [14]. Σε έρευνες, οι συγγραφείς προσεγγίζουν πιο γενικά και σφαιρικά το θέμα της ανίχνευσης ανωμαλιών [15] [16]. Σε αρκετά άρθρα ανασκόπησης περιγράφονται διάφορες μέθοδοι ανίχνευσης ανωμαλιών δικτύου. Από τις προαναφερθείσες έρευνες οι πιο αποτελεσματικές μέθοδοι ανίχνευσης ανωμαλιών δικτύου είναι οι PCA (Principle Component Analysis) [17] [18], ανάλυση Wavelet [19] [20], Μαρκοβιανά μοντέλα (Markovian models) [21], Ομαδοποίηση (Clustering) [22], ιστογράμματα [23], Σκίτσα (Sketches) [24] και η εντροπία [7] [10] [25].

Σε αυτό το σημείο θα δοθεί μεγαλύτερη έμφαση σε ερευνητικά έργα που σχετίζονται αυστηρά με την προσέγγιση που προτείνεται σε αυτό το άρθρο. Ακολουθεί μια ανάλυση των μεθόδων ανίχνευσης που βασίζονται στις κατανομές χαρακτηριστικών μέσω της εντροπίας, ιστογραμμάτων και σκίτσων. Ιδιαίτερη προσοχή δίδεται στις μεθόδους που χρησιμοποιούν την εντροπία. Η ενότητα ξεκινά με τη σύγκριση της προσέγγισης των κατανομών των χαρακτηριστικών της κίνησης(feature distributions) σε σχέση με την παλαιότερη, αλλά ακόμη πιο δημοφιλή ανίχνευση μέσω μετρητών(counters).

1.3.2 Ανίχνευση με μετρητές (counters)

Στο παρελθόν, οι ανωμαλίες αντιμετωπίζονταν ως αποκλίσεις του όγκου της κίνησης (traffic volume). Απλοί μετρητές όπως: ο αριθμός των ροών, των πακέτων (συνολικός αριθμός από πακέτα που προωθήθηκαν, κατακερματισμένα πακέτα, απορριφθέντα πακέτα) και των bytes (ανά πακέτο, ανά δευτερόλεπτο) χρησιμοποιήθηκαν. Αυτοί οι μετρητές μπορούν να προέλθουν από συσκευές δικτύου μέσω του Πρωτοκόλλου απλής διαχείρισης δικτύου (SNMP) [26] ή του NetFlow.

Ο Barford [27] παρουσίασε την ανάλυση wavelet για να διακρίνει μεταξύ προβλέψιμων και ανώμαλων μεταβολών του όγκου κίνησης, χρησιμοποιώντας ένα πολύ βασικό σύνολο μετρητών του NetFlow και των δεδομένων του SNMP. Χρησιμοποιώντας προηγμένες τεχνικές ανάλυσης σήματος σε συνδυασμό με πολύ απλές μετρήσεις, δηλαδή τον αριθμό των ροών, των πακέτων και των bytes είχε σαν αποτέλεσμα ορισμένα θετικά αποτελέσματα στην ανίχνευση υψηλής έντασης ανωμαλιών, όπως αποτυχία λειτουργίας του δικτύου.

Ο Kim [28] πρότεινε μια μέθοδο όπου πολλές διαφορετικές επιθέσεις DDoS [29] [30] περιγράφονται με βάση την συμπεριφορά της κίνησης ως προς τα χαρακτηριστικά των ροών. Πιο συγκεκριμένα, οι συγγραφείς επικεντρώθηκαν σε μετρητές όπως ο αριθμός των ροών, των πακέτων και των bytes, τα μεγέθη ροών και πακέτων, το μέσο μέγεθος ροών και του αριθμού των πακέτων ανά ροή. Στο παράδειγμα που παρουσιάστηκε στο άρθρο αυτό σχετικά με πλημμύρα TCP SYN εφαρμόστηκε το παρακάτω πρότυπο/μοτίβο: ένας μεγάλος αριθμός ροών, ωστόσο μικρός αριθμός μικρών πακέτων και κανένας περιορισμός στο εύρος ζώνης και στο συνολικό πλήθος πακέτων. Αυτό το πρότυπο διαφέρει σημαντικά από το αυτό που παράγεται από ICMP / UDP επιθέσεις πλημμύρας, όπου χαρακτηρίζεται από την κατανάλωση μεγάλου εύρους ζώνης και ένα μεγάλο αριθμό πακέτων. Αν και οι συγγραφείς ανέφεραν κάποια καλά αποτελέσματα, ανέφεραν επίσης ότι η κοινή νόμιμη peer-to-peer κίνηση (P2P) μπορεί να οδηγήσει σε μερικούς ψευδείς συναγερμούς στην προσέγγισή τους.

Πλέον, υπάρχουν αρκετές εμπορικές λύσεις, όπως π.χ. το Invea-Tech FlowMon [31] ή το AKMA Labs FlowMatrix [32], οι οποίες προσφέρουν ορισμένες προηγμένες μεθόδους ανίχνευσης ανωμαλιών, που βασίζονται κυρίως σε προκαθορισμένα σύνολα κανόνων για την ανίχνευση των

ανεπιθύμητων προτύπων συμπεριφοράς και σε μερικά απλά μακροπρόθεσμα προφίλ συμπεριφοράς του δικτύου όσον αφορά τις υπηρεσίες και τον όγκο της κίνησης.

Κλείνοντας αυτή την υποενότητα, πρέπει να σημειωθεί ότι παρόλο που υπάρχουν πολλές μέθοδοι που βασίζονται σε μετρητές, η χρήση τους είναι περιορισμένη. Το πρόβλημα εντοπίζεται στο γεγονός ότι η προσέγγιση βασισμένη σε μετρητές συνδέεται στενά με τον όγκο της κίνησης. Σήμερα πολλές ενέργειες ανώμαλης κίνησης δικτύου, όπως χαμηλό ποσοστό(low-rate) DDoS [33] [34] κρυφή σάρωση (stealth scanning) ή επικοινωνία μεταξύ botnet δεν μεταβάλουν σημαντικά τον όγκο της κίνησης.

1.3.3 Ανίχνευση με κατανομές χαρακτηριστικών (feature distributions)

Η ανίχνευση ανωμαλιών δικτύου μέσω των κατανομών των χαρακτηριστικών της κυκλοφορίας γίνεται όλο και πιο δημοφιλής. Αρκετές κατανομές χαρακτηριστικών, π.χ. με βάση την επικεφαλίδα (διευθύνσεις, θύρες), με βάση τον όγκο της κίνησης (ποσοστό ροών, πακέτων και bytes) και με βάση την συμπεριφορά (in / out συνδέσεις για το συγκεκριμένο host) έχουν προταθεί [7] [10] [35]. Ωστόσο, είναι ασαφές ποια χαρακτηριστικά κατανομών αποδίδουν καλύτερα. Ο Nychis [7] διερευνώντας τις εξαρτήσεις μεταξύ διευθύνσεων και θυρών και συνέστησε συστήνει τη χρήση χαρακτηριστικών κατανομής με βάση τον όγκο και την συμπεριφορά της κίνησης. Αντίθετα, ο Tellenbach [10] δεν βρήκε καμία συσχέτιση μεταξύ των χαρακτηριστικών επικεφαλίδας. Στην δική μας προσέγγιση έγινε χρήση χαρακτηριστικών επικεφαλίδας όπως θα περιγραφεί αναλυτικά στην συνέχεια.

1.3.3.1 Η εντροπία του Shannon

Η εντροπία, ως το μέτρο της αβεβαιότητας, μπορεί να χρησιμοποιηθεί για να συνοψίσει τα χαρακτηριστικά των κατανομών σε συμπαγή μορφή, δηλαδή, σε έναν μόνο αριθμό. Υπάρχουν πολλές μορφές της εντροπίας, αλλά μόνο λίγες έχουν εφαρμοστεί στην ανίχνευση ανωμαλιών δικτύου. Η πιο δημοφιλής είναι η γνωστή εντροπία του Shannon [36] [37]. Η εφαρμογή του μέτρου του Shannon σαν σχετική εντροπία και υπό συνθήκη εντροπία για την ανίχνευση ανώμαλης συμπεριφοράς εντός ενός δικτύου προτάθηκαν από τους Lee και Xiang [38]. Επίσης, ο Lakhina στο [35] έκανε χρήση της εντροπίας Shannon για να συνοψίσει μια κατανομή χαρακτηριστικών των ροών ενός δικτύου.

1.3.3.2 Άλλες τεχνικές

Εκτός από την εντροπία, κάποιες άλλες τεχνικές που βασίζονται στις κατανομές των χαρακτηριστικών χρησιμοποιούνται με επιτυχία στο πλαίσιο της ανίχνευσης ανωμαλιών [39], όπως σκίτσα και τα ιστογράμματα. Παραδείγματος χάριν, προτάθηκε μια μέθοδος ταξινόμησης ροών με βάση την μοντελοποίηση των ιστογραμμάτων των ροών δικτύου, χρησιμοποιώντας Dirichlet Mixture Processes για τυχαίες κατανομές [40]. Οι συγγραφείς επικύρωσαν το μοντέλο τους επί τριών συνθετικών περιπτώσεων και πέτυχαν σχεδόν 100% ακρίβεια ταξινόμησης. Στο [24] ο Stoecklin εισήγαγε δύο στρωμάτων (two layered) τεχνική ανίχνευσης ανωμαλιών με σκίτσα. Υποστηρίζει ότι η κύρια δύναμη της μεθόδου τους είναι η κατασκευή λεπτομερώς καθορισμένου μοντέλου, το οποίο καταγράφει τις λεπτομέρειες των χαρακτηριστικών των κατανομών, αντί να τις συνοψίζει σε μια τιμή της εντροπίας. Το κύριο πρόβλημα των τεχνικών που δεν βασίζονται στην εντροπία είναι η σωστή ρύθμιση τους [41]. Η απόδοση ανίχνευσης εξαρτάται σε μεγάλο βαθμό από την ακρίβεια του μεγέθους του παραθύρου ανίχνευσης. Αυτό μπορεί να είναι δύσκολο να διαχειριστεί όταν παρατηρούνται αλλαγές της κίνησης δικτύου.

1.4 Περιγραφή Επόμενων Κεφαλαίων

Ο κύριος στόχος της παρούσας πτυχιακής είναι να δείξει ότι η προσέγγιση της εντροπίας αποτελεί μία κατάλληλη τεχνική για την ανίχνευση σύγχρονων επιθέσεων botnet. Ο στόχος αυτός επιδιώχθηκε να επιτευχθεί με την υλοποίηση των ακόλουθων βημάτων: (i) την κατάλληλη επιλογή μεθόδου που βασίζεται στην εντροπία για την ανίχνευση επιθέσεων άρνησης υπηρεσίας, (ii) την εφαρμογή της μεθόδου, (iii) την επιλογή κατάλληλου συνόλου δεδομένων, (iv) την αξιολόγηση της μεθόδου. Πιο αναλυτικά ακολουθεί μια περιγραφή των επόμενων κεφαλαίων.

Το δεύτερο κεφάλαιο αποσκοπεί στην περιγραφή των επιθέσεων που θέτουν σε κίνδυνο την ασφάλεια της πληροφορίας και την περιγραφή των τρόπων ανίχνευσης τους. Προσδιορίζονται οι στόχοι των επιτιθέμενων και οι τεχνικές τις οποίες εφαρμόζουν για την υλοποίηση των επιθέσεων τους. Από το μεγάλο εύρος των επιθέσεων που πλήττουν τα πληροφοριακά συστήματα η παρούσα έρευνα θα εστιάσει στις επιθέσεις άρνησης υπηρεσίας και τους τρόπους με τους οποίους αυτές υλοποιούνται. Τέλος, πραγματοποιείται μία σύντομη αναφορά των σύγχρονων μεθόδων ανίχνευσης και πως η δική μας μέθοδος έρχεται να συμπληρώσει/επαληθεύσει τις ήδη υπάρχουσες μεθόδους.

Στο τρίτο κεφάλαιο παρουσιάζεται η προσέγγιση της παρούσας έρευνας. Στο κεφάλαιο αυτό γίνεται εκτενής αναφορά της μεθόδου ανίχνευσης που προτείνεται στην παρούσα διπλωματική ορίζοντας, το θεωρητικό υπόβαθρο για την υλοποίηση του πειράματος καθώς επίσης και της σημασίας της ανίχνευσης επιθέσεων, αξιοποιώντας στατιστικομαθηματικές μεθόδους και συγκεκριμένα της εντροπίας. Προσδιορίζεται η σύνδεση μεταξύ της θεωρίας της πληροφορίας με την ανίχνευση επιθέσεων/ ανωμαλιών. Πιο συγκεκριμένα, περιγράφεται ο τρόπος με τον οποίο η έννοια την εντροπίας συνδέεται με την ανίχνευση επιθέσεων, πώς ο μαθηματικοστατιστικός τύπος της εντροπίας, που εισάχθηκε από τον Shannon ως ένα μέτρο περιγραφής της αταξίας ενός συστήματος, με κατάλληλη παραμετροποίηση μπορεί να δημιουργήσει ένα μοντέλο/μία μέθοδο προς επιτυχή ανίχνευση επιθέσεων.

Στο τέταρτο κεφάλαιο προσδιορίζεται ο αλγόριθμος της εντροπίας που χρησιμοποιήθηκε, με χρήση κατάλληλων παραμέτρων από τις επικεφαλίδες των μεταδιδόμενων πακέτων σε ένα δίκτυο, ώστε να απαντήσει στα ερωτήματα που εξετάζει η έρευνα. Τα δεδομένα που χρησιμοποιήθηκαν στο πείραμα προσδιορίζονται, επισημαίνοντας ότι επειδή δεν είναι δυνατή η προσομοίωση μιας τέτοιας επίθεσης σε ένα υπαρκτό δίκτυο, χρησιμοποιήθηκαν δεδομένα από βάσεις δεδομένων που εξυπηρετούν αυτόν τον σκοπό. Εξετάζονται τρία σενάρια επιθέσεων υλοποιημένα από διαφορετικό πλήθος επιτιθέμενων bots και διαφορετικών μεθόδων επίθεσης. Ακολουθεί, πειραματικό μέρος στο οποίο περιγράφεται ο αλγόριθμος που χρησιμοποιήθηκε, τα δεδομένα που επιλέχτηκαν για να αποτελέσουν ένα αντιπροσωπευτικό δείγμα προς εξέταση, και παρουσιάζονται τα αποτελέσματα της μεθόδου.

Τέλος, στο πέμπτο κεφάλαιο πραγματοποιείται μια αξιολόγηση των αποτελεσμάτων με σκοπό τον προσδιορισμό του βαθμού αποδοτικότητας της κάθε προσέγγισης. Επιδιώχτηκε επίσης ο προσδιορισμός ενός κατηγοριοποιητή κίνησης (classifier), ενός μέτρου εκτίμησης των επιθέσεων, δηλαδή ένα μέτρο το οποίο θα προσδιορίζει πότε μια μεταβολή στις τιμές της εντροπίας μπορεί να θεωρηθεί ως ύποπτη. Τέλος, θα προταθεί για μελλοντική έρευνα μια παραμετροποίηση του αλγορίθμου, μια απλοποιημένη μέθοδος, έτσι ώστε να εξεταστεί το ενδεχόμενο την ανίχνευσης των επιθέσεων με μικρότερη απαιτούμενη υπολογιστική ισχύ.

Κεφάλαιο 2: Βασικές Έννοιες

2.1 Η έννοια της ασφάλειας

Σε αυτό το κεφάλαιο θα επιχειρηθεί μια προσέγγιση της ασφάλειας με την έννοια του όρου όσον αφορά τα δίκτυα υπολογιστών. Ξεκινώντας από βασικές ιδιότητες της ασφάλειας θα ακολουθήσει επισκόπηση των σύγχρονων επιθέσεων και απειλών και των μεθόδων αντιμετώπισης των προαναφερθέντων επιθέσεων, σκοπεύοντας έτσι στην παράθεση μίας τυπολογίας των πιο βασικών όρων που θα χρησιμοποιηθούν σε αυτή την πτυχιακή.

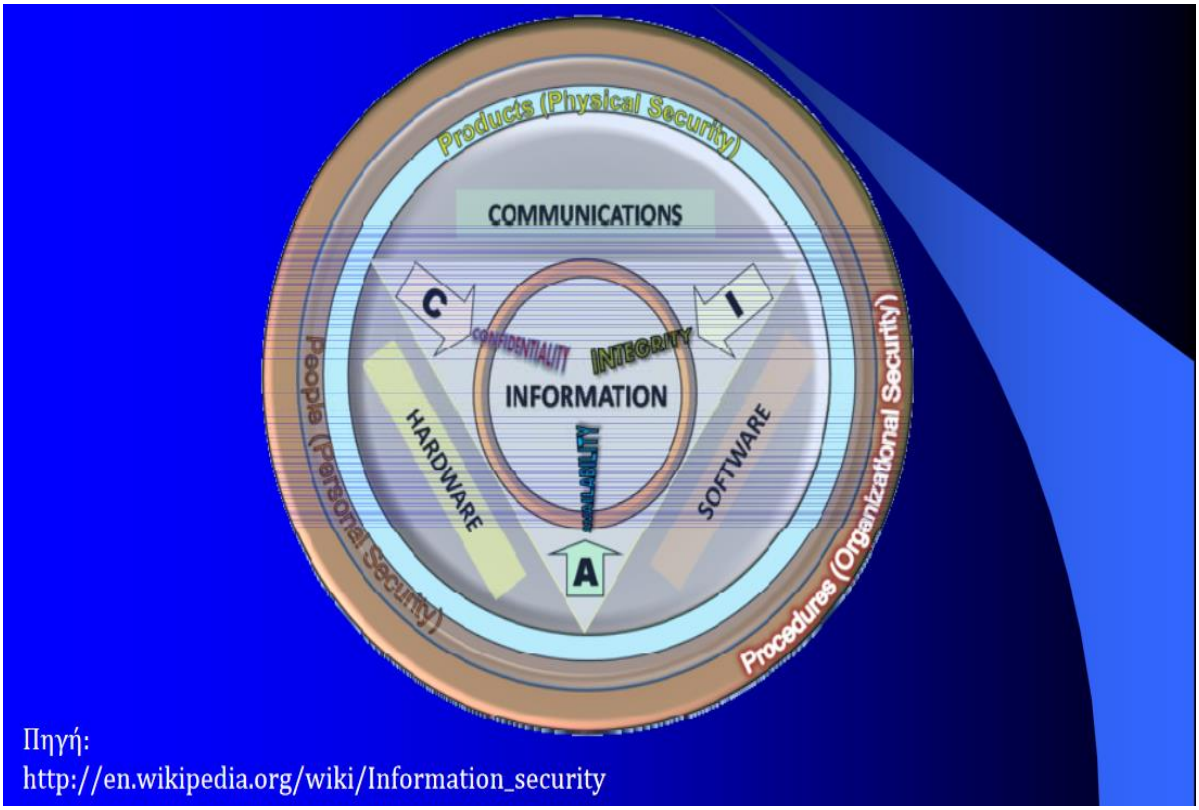
Η έννοια της ασφάλειας σχετίζεται με την ικανότητα μίας οντότητας να προστατεύει τις πληροφορίες της από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων της (λογισμικό, υποδομές). Επιπλέον, αφορά την δυνατότητα ενός δικτύου υπολογιστών ή πληροφοριακού συστήματος να διατηρήσει εκ των προτέρων ένα επίπεδο αξιοπιστίας. Στο σημείο αυτό θα πρέπει να γίνει μια προσπάθεια να οριστεί τι θεωρείται αξιόπιστο σύστημα. Στα πλαίσια της παρούσας ερευνητικής εργασίας θα θεωρηθεί αξιόπιστο το σύστημα το οποίο σε τυχαία συμβάντα ή κακόβουλες ενέργειες διασφαλίζει την διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και των συναφών υπηρεσιών που παρέχονται.

Τίθεται, συνεπώς, το ζήτημα της διασφάλισης τριών θεμελιωδών ιδιοτήτων της ασφάλειας: της Διαθεσιμότητας (Availability), της Εμπιστευτικότητας (Confidentiality) και της Ακεραιότητας (Integrity).

Η Διαθεσιμότητα αφορά την ιδιότητα της προσπελασιμότητας πληροφοριών και υπηρεσιών ενός δικτύου υπολογιστών από εξουσιοδοτημένες οντότητες χωρίς αδικαιολόγητη καθυστέρηση. Οι επιθέσεις άρνησης υπηρεσίας (denial of service) αποσκοπούν στην παρεμπόδιση εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων, καθώς επίσης και στην καθυστέρηση κρίσιμων από πλευράς χρόνου (time-critical) λειτουργιών.

Η Εμπιστευτικότητα αφορά την πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Υπό την ιδιότητα της εμπιστευτικότητας, ένα ασφαλές δίκτυο αποσκοπεί στην διακίνηση των δεδομένων και των πληροφοριών μεταξύ των υπολογιστών του, ώστε να αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Άλλες εκφάνσεις της ιδιότητας της εμπιστευτικότητας αποτελεί η ιδιωτικότητα, δηλαδή η προστασία των δεδομένων προσωπικού χαρακτήρα.

Η Ακεραιότητα αφορά την πρόληψη μη εξουσιοδοτημένης μεταβολής ή αλλοίωσης πληροφοριών, δηλαδή, την πρόληψη μη εξουσιοδοτημένης εγγραφής ή διαγραφής πληροφοριών, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων (Εικόνα 1. Ασφάλεια της πληροφορίας).



Εικόνα 1. Ασφάλεια της πληροφορίας

Η αυξανόμενη εξάρτηση από τα πληροφοριακά συστήματα, τόσο σε προσωπικό όσο και σε κοινωνικό επίπεδο, καθορίζει τον σύγχρονο τρόπο ζωής. Ακόμη, πρέπει να ληφθεί υπόψιν ότι πλέον οι επικοινωνίες, οι μεταφορές, οι τραπεζικές συναλλαγές και η εθνική ασφάλεια στηρίζονται στα πληροφοριακά συστήματα. Συνεπώς, η ασφάλεια των πληροφοριακών συστημάτων αποτελεί πλέον θέμα τεράστιας σημασίας με οικονομικές, πολιτικές ακόμη και στρατιωτικές προεκτάσεις. Στο σημείο αυτό, είναι ιδιαίτερης σημασίας να επισημανθεί ότι παρόλη την αυξανόμενη προσπάθεια για επαγρύπνηση και πληροφόρηση των χρηστών των πληροφοριακών συστημάτων, πρωταρχικός στόχος των επιτιθέμενων σε ένα σύστημα είναι η εκμετάλλευση του ανθρώπινου παράγοντα.

2.2 Απειλές ασφάλειας

Η ασφάλεια ενός συστήματος διακυβεύεται όταν βρίσκεται σε κίνδυνο μία εκ των τριών θεμελιωδών ιδιοτήτων της. Οι απειλές διαχωρίζονται σε ακούσιες, όπως οι αστοχίες υλικού/λογισμικού και σε εκούσιες που οφείλονται σε κακόβουλους χρήστες. Τα πληροφοριακά συστήματα παρουσιάζουν ευάλωτα σημεία, τα οποία χαρακτηρίζονται ως ευπάθειες. Οι ευπάθειες κατηγοριοποιούνται σε φυσικές (κλοπές, καταστροφές data centre), εκ φύσεως (φυσικές καταστροφές), software/hardware (δυσλειτουργίες, ανεπαρκής έλεγχος), υποκλοπές εκπεμπόμενων σημάτων (emanations), επικοινωνιών (υποκλοπές/ αλλοιώσεις μηνυμάτων), ανθρώπινες (κοινωνική μηχανική-social engineering). Η αξιοποίηση των ευπαθειών αυτών οδηγεί στην υλοποίηση επιθέσεων διακινδυνεύοντας την ασφάλεια των πληροφοριακών συστημάτων.

2.3 Επιτιθέμενοι

Σε αυτό το υποκεφάλαιο επιχειρείται μία διάκριση των επιτιθέμενων βασισμένη στα κίνητρα τους και τον τρόπο με τον οποίο επιλέγουν να χρησιμοποιήσουν τις δεξιότητες τους. Στο σημείο αυτό να σημειωθεί ότι οι επιτιθέμενοι είναι γνωστοί ως hackers. Ακολουθεί διαχωρισμός που διακρίνει τα κίνητρα και την στοχοθεσία των δρώντων αυτών.

- Black Hat Hackers (Crackers) : Αυτοί οι hackers προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ιδιωτικά αρχεία και πληροφορίες, μέσω επιθέσεων στα πληροφοριακά συστήματα για προσωπικό όφελος.

- Gray Hat Hackers : Αποτελούν το πλήθος «γκρίζας ζώνης» . Δεδομένων των συνθηκών κάτω από τις οποίες ενεργούν επιλέγουν είτε να υπερασπιστούν ένα σύστημα πληροφοριών ή δίκτυο, είτε να λειτουργούν σαν Black Hats για να επιτύχουν τους στόχους τους.

- White Hat Hackers (Ethikal Hackers): Αυτοί οι hackers έχουν γνώσεις προκειμένου να υπερασπιστούν τα συστήματα πληροφοριών. Χρησιμοποιούν τις δεξιότητες τους για να αυξήσουν, αντί να μειώσουν ,την ασφάλεια των δικτύων.

- Hacktivists: Είναι οι hackers που χρησιμοποιούν τις δεξιότητες τους για να προβάλουν ένα κοινωνικό, ιδεολογικό, θρησκευτικό ή πολιτικό μήνυμα.

- State-Sponsored Hackers: Ομάδες hacker που δραστηριοποιούνται από τις κυβερνήσεις σε κατασκοπεία. Είναι γνωστοί ως APTs (Advanced Persistent Threats) λόγω της συγκεκαλυμένης φύσης τους και της επιμονής τους σε συγκεκριμένες μακροχρόνιες επιθέσεις.

2.4 Επιθέσεις

2.4.1 Στόχοι επιθέσεων

Οι στόχοι των επιθέσεων ποικίλουν ανάλογα με τους σκοπούς και τις ικανότητες του επιτιθέμενου καθώς επίσης και τα αποτρεπτικά μετρά ασφαλείας. Ενδεικτικά, στόχοι μπορεί να είναι μικρά τοπικά δίκτυα(LAN's), Πανεπιστήμια, κυβερνητικές ιστοσελίδες ή μεγάλοι οργανισμοί. Σε κάθε περίπτωση, στόχος επίθεσης μπορεί να αποτελέσει κάθε ηλεκτρονικός υπολογιστής ή δίκτυο που είναι διασυνδεδεμένο με τον παγκόσμιο ιστό. Στην συνέχεια, θα αναφερθούν ορισμένοι πιθανοί στόχοι επιθέσεων, καθώς επίσης και λόγοι για τους οποίους οι στόχοι «προσελκύουν» τους επιτιθέμενους. Τα μικρά τοπικά δίκτυα συνήθως χαρακτηρίζονται από ανεπαρκή μέτρα ασφαλείας, με αποτέλεσμα να αποτελούν «εύκολο» στόχο για τον επιτιθέμενο. Τα πανεπιστήμια φιλοξενούν ένα μεγάλο αριθμό χρηστών πολλοί εκ των οποίων δεν διαθέτουν επαρκή γνώση για τους κινδύνους που προκύπτουν από λανθασμένη χρήση των συστημάτων. Ως αποτέλεσμα, δημιουργούνται τρύπες ασφαλείας που ενδεχομένως να εκμεταλλευτεί ο επιτιθέμενος με σκοπό την απόκτηση παράνομης πρόσβασης σε συστήματα του πανεπιστημίου που ενδεχομένως να αποτελέσουν για τον επιτιθέμενο ένα εργαλείο αυξημένης επεξεργαστικής ισχύος. Πιο δύσκολοι στόχοι μπορούν να θεωρηθούν κυβερνητικές ιστοσελίδες ή μεγάλοι

οργανισμοί καθώς διαθέτουν πιο ισχυρά μέτρα ασφαλείας και είναι αρκετά πιο δύσκολο να παραβιαστούν. Παρόλα αυτά, μπορούν να επιφέρουν μεγάλο κέρδος προς τους επιτιθέμενους, καθώς μία τέτοια επιτυχής επίθεση θα μπορούσε να δώσει πρόσβαση σε ευαίσθητα και απόρρητα δεδομένα και πληροφορίες, όπως απόρρητα έγγραφα κυβερνητικών οργανισμών, αριθμούς πιστωτικών καρτών τραπεζών ή μεγάλα χρηματικά ποσά μέσω της κρυπτογράφησης «ευαίσθητων» αρχείων. Στο σημείο αυτό, για την καλύτερη κατανόηση των επιθέσεων και συνεπώς την ανεύρεση των βέλτιστων τρόπων για την αντιμετώπιση τους, επιδιώκεται η κατηγοριοποίηση τους.

2.4.2 Κατηγοριοποίηση Επιθέσεων

Σε αυτό το υποκεφάλαιο θα γίνει μια προσπάθεια κατηγοριοποίησης των διάφορων ειδών επιθέσεων, καθώς επίσης θα περιγράφουν ορισμένες τεχνικές που εφαρμόζονται για την υλοποίηση επιθέσεων.

2.4.2.1 Τοπικές – Απομακρυσμένες επιθέσεις:

Ο συγκεκριμένος διαχωρισμός εξετάζει το ενδεχόμενο ο επιτιθέμενος να έχει φυσική πρόσβαση στο σύστημα στόχος.

Στην περίπτωση που ο επιτιθέμενος έχει φυσική πρόσβαση γίνεται αναφορά σε τοπική επίθεση. Οι τοπικές επιθέσεις αφορούν μη εξουσιοδοτημένους χρήστες, που επιδιώκουν είτε την απόκτηση δικαιωμάτων πρόσβασης στο σύστημα είτε την απόκτηση περισσότερων δικαιωμάτων από αυτά που ήδη έχουν (privilege escalation) είτε την χρήση των δικαιωμάτων τους με κακόβουλες προθέσεις.

Στην αντίθετη περίπτωση οπού ο επιτιθέμενος δεν έχει φυσική πρόσβαση στον στόχο, γίνεται αναφορά για απομακρυσμένες επιθέσεις. Οι απομακρυσμένες επιθέσεις μπορούν να υλοποιηθούν σε δικτυωμένα συστήματα, δηλαδή είτε ο επιτιθέμενος και ο στόχος βρίσκονται εντός του ίδιου τοπικού δικτύου(εσωτερικές επιθέσεις) είτε ο επιτιθέμενος υλοποιεί την επίθεση μέσω διαδικτύου σε ένα απομακρυσμένο σύστημα(εξωτερικές επιθέσεις). Στόχος είναι η απόκτηση πρόσβασης στο μηχάνημα αυτό μέσω της εκμετάλλευσης κάποιας ευπάθειας στο σύστημα.

2.4.2.2 Παθητικές – Ενεργητικές επιθέσεις:

Σε αυτή την μορφή διαχωρισμού εξετάζεται ο βαθμός αλληλεπίδρασης του επιτιθέμενου με το μηχάνημα-στόχος.

Παθητικές επιθέσεις:

Οι παθητικές επιθέσεις αποσκοπούν στην απόκτηση ή παρακολούθηση πληροφορίων ή δεδομένων που εντοπίζονται σε δίκτυα υπολογιστών χωρίς την τροποποίηση ή την άμεση παρεμβολή του επιτιθέμενου. Γνωστές τεχνικές παθητικών επιθέσεων είναι οι Wiretapping, Mimicry, Port scan, Idle scan [42].

- Με την τεχνική wiretapping(ή Telephone tapping) ο επιτιθέμενος μπορεί να παρακολουθήσει όλες τις επικοινωνίες και να αποκτήσει ευαίσθητες πληροφορίες. Εκτός από την περίπτωση που η πληροφορία είναι κρυπτογραφημένη μπορεί εύκολα να

διαβαστεί από τον επιτιθέμενο, θέτοντας σε κίνδυνο τους κωδικούς πρόσβασης, τα σήματα ελέγχου ή άλλες ευαίσθητες πληροφορίες.

- Με την τεχνική Mimicry ο επιτιθέμενος λειτουργεί ένα εξυπηρετητή(server) που «ακούει» στο ίδιο κανάλι ή πλαστογραφεί (spoof) την ταυτότητα (ID) ενός νόμιμου εξυπηρετητή, προκαλώντας στους χρήστες με το πρόγραμμα-πελάτη(client program) να στείλουν τα στοιχεία τους τόσο στο νόμιμο εξυπηρετητή όσο και στον επιτιθέμενο, ο οποίος αποκτά πληροφορίες των χρηστών.

- Ο ανιχνευτής θυρών (Port scanner) είναι μία εφαρμογή που σχεδιάστηκε για να εξετάσει ένα server ή υπολογιστή (host) για ανοιχτές θύρες. Καθώς αποτελεί ένα βασικό εργαλείο κατά τα πρώτα στάδια της υλοποίησης των επιθέσεων, θα αναλυθεί ο τρόπος λειτουργίας αυτής της εφαρμογής. Η ανίχνευση θυρών αποτελεί διαδικασία αποστολής αιτημάτων πελατών(client requests) ενός φάσματος διευθύνσεων θυρών του εξυπηρετητή (server port addresses) σε έναν υπολογιστή με στόχο την εξεύρεση ενεργών θυρών. Η πλειονότητα των χρήσεων της διαδικασίας ανίχνευσης θυρών δεν είναι επιθέσεις, αλλά ενδεχομένως ανιχνεύσεις για τον καθορισμό των διαθέσιμων υπηρεσιών σε έναν απομακρυσμένο υπολογιστή. Για τον λόγο αυτό, η συγκεκριμένη διαδικασία δεν μπορεί να χαρακτηριστεί ως κακόβουλη, δίνοντας την δυνατότητα στους επιτιθέμενους να χρησιμοποιούν το εργαλείο χωρίς να ενεργοποιήσουν κάποιο σύστημα ασφαλείας του ενδεχόμενου στόχου.

  Σε αυτό το σημείο, θα πρέπει να γίνει αναφορά στον τρόπο λειτουργίας του TCP/IP για να αναλυθούν περαιτέρω οι διάφοροι τύποι ανίχνευσης. Ο σχεδιασμός και η λειτουργία του διαδικτύου βασίζεται στο μοντέλο Internet Protocol Suite, γνωστό ως TCP/IP. Σε αυτό το σύστημα επικοινωνίας, οι αναφορές στα μηχανήματα (hosts) και στις υπηρεσίες τους (host services) πραγματοποιούνται με την χρήση δύο συνιστωσών: μια διεύθυνση και ενός αριθμού θύρας. Υπάρχουν 65536 διακριτές θύρες διαθέσιμες προς χρήση. Οι περισσότερες υπηρεσίες χρησιμοποιούν ένα περιορισμένο εύρος αριθμών. Κάποιοι ανιχνευτές θυρών σαρώνουν μόνο τους πιο κοινούς αριθμούς θύρας, ή τις θύρες που συνδέονται πιο συχνά με ευάλωτες υπηρεσίες, σε ένα δεδομένο μηχάνημα.

  Το αποτέλεσμα της σάρωσης σε μια θύρα είναι συνήθως γενικευμένη σε μία από τις τρεις κατηγορίες:

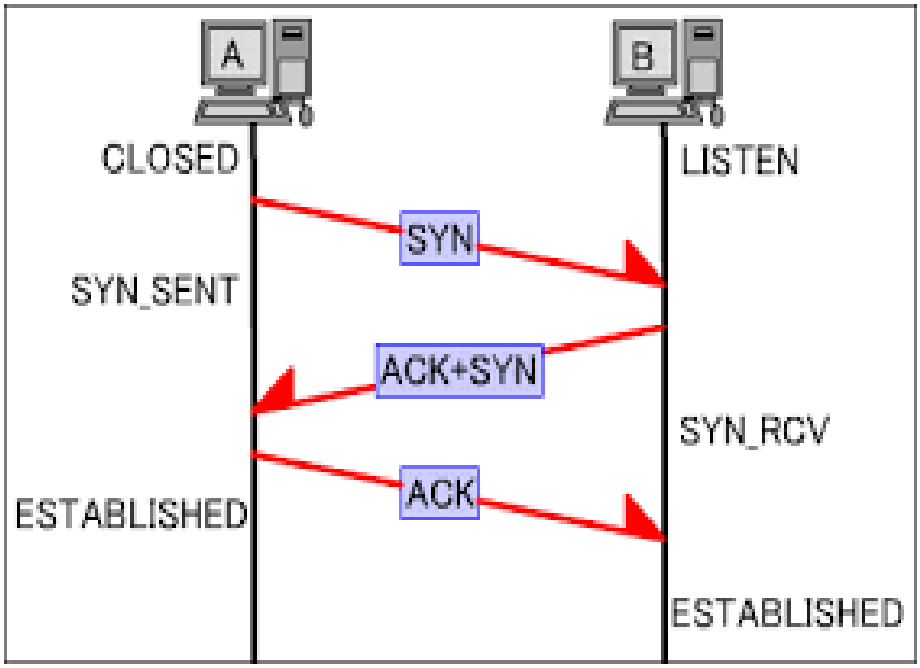
  1. Open or Accepted: Ο host απέστειλε απάντηση που δείχνει ότι μια υπηρεσία ακούει στη θύρα.

  2. Closed or Denied or Not Listening: Ο host απέστειλε απάντηση που δείχνει ότι οι συνδέσεις δεν θα μπορούν να δημιουργηθούν στην θύρα.

  3. Filtered, Dropped or Blocked: Δεν υπήρξε καμία απάντηση από τον host.

  Όλες οι μορφές ανίχνευσης θυρών βασίζονται στην υπόθεση ότι το μηχάνημα-στόχος είναι συμβατό με το RFC 793 - Πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol - TCP). Για την επίτευξη μίας επικοινωνίας ενός εξυπηρετητή με έναν πελάτη εφαρμόζεται το πρωτόκολλο TCP/IP, απαιτώντας μία διαδικασία τριών βημάτων (3-way handshake). Η τεχνική χειραψίας τριών βημάτων TCP συχνά αναφέρεται ως « SYN - SYN-ACK» (ή ακριβέστερα SYN, SYN- ACK, ACK) επειδή υπάρχουν τρία μηνύματα που μεταδίδονται από το πρωτόκολλο TCP για να διαπραγματευτεί και να ξεκινήσει μια

συνεδρία TCP μεταξύ δύο υπολογιστών. Ο μηχανισμός χειραψίας TCP έχει σχεδιαστεί με τρόπο που επιτρέπει την διαπραγμάτευση των παραμέτρων της σύνδεσης TCP πριν από τη διαβίβαση των δεδομένων. Ακολουθεί (Εικόνα 2. Τριμερής Χειραψία TCP) η απεικόνιση της τριμερούς χειραψίας TCP [43].



Εικόνα 2. Τριμερής Χειραψία TCP

Αφού αναλύθηκε ο τρόπος λειτουργίας του TCP/IP θα ακολουθήσουν οι διάφορες τεχνικές ανίχνευσης θυρών που εφαρμόζονται:

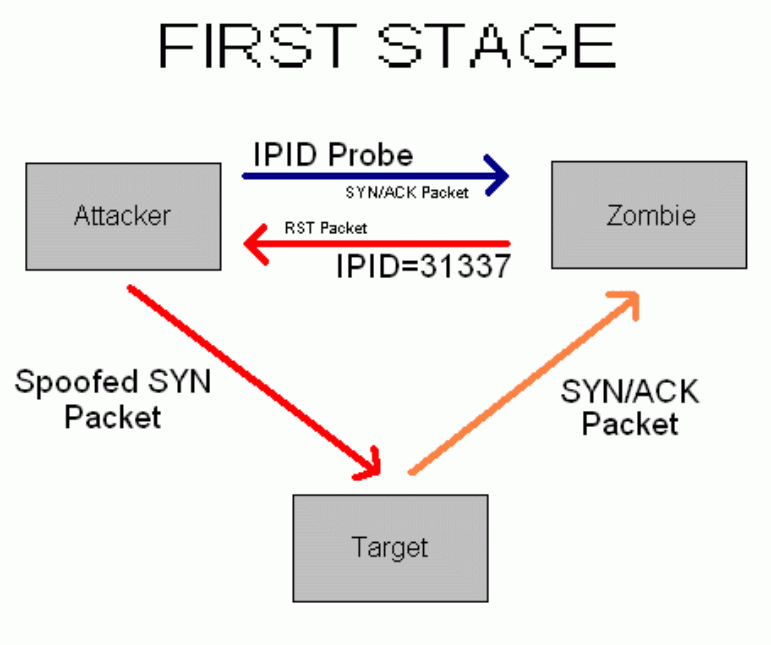
I. ***TCP scanning*:** Οι απλούστεροι ανιχνευτές θυρών χρησιμοποιούν τις λειτουργίες του δικτύου του λειτουργικού. Αυτή η λειτουργία σάρωσης έχει το πλεονέκτημα ότι ο χρήστης δεν χρειάζεται ειδικά προνόμια. Ωστόσο, η χρήση των λειτουργιών δικτύου του λειτουργικού συστήματος αποτρέπει τον έλεγχο χαμηλού επιπέδου με αποτέλεσμα τέτοιου τύπου σάρωση να είναι λιγότερο συχνή. Επιπρόσθετα, αυτή η μέθοδος δημιουργεί αυξημένη κίνηση στο δίκτυο του στόχου, καθιστώντας την εισβολή ανιχνεύσιμη από το σύστημα ανίχνευσης παρεισφρήσεων.

II. ***SYN scanning*:** Αποτελεί μια άλλη μορφή σάρωσης TCP. Σε αυτή όμως την περίπτωση, αντί να χρησιμοποιηθούν οι λειτουργίες δικτύου του λειτουργικού συστήματος, ο ανιχνευτής θυρών παράγει ο ίδιος πακέτα IP προς μετάδοση παρακολουθώντας το δίκτυο για απαντήσεις. Αυτός ο τύπος σάρωσης είναι επίσης γνωστός ως «half-open scanning», διότι ποτέ δεν εγκαθιδρύει μια πλήρη σύνδεση TCP. Η χρήση των παραγόμενων εκ του ανιχνευτή IP πακέτων ονομάζεται raw networking και έχει πολλά πλεονεκτήματα, δίνοντας στο σαρωτή πλήρη έλεγχο των πακέτων που αποστέλλονται και το χρονικό όριο(timeout) αναμονής για τις απαντήσεις, επιτρέποντας λεπτομερείς αναφορές των απαντήσεων.

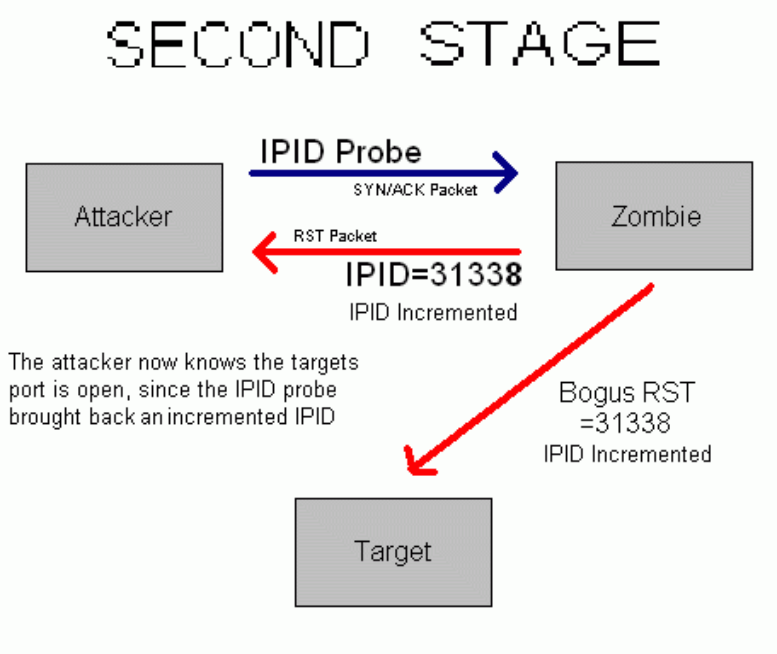
III. ***UDP scanning*:** Η UDP σάρωση είναι επίσης εφικτή, αν και υπάρχουν τεχνικές προκλήσεις. Το UDP πρωτόκολλο χρησιμοποιείται για την μεταφορά δεδομένων στο διαδίκτυο και δεν χρησιμοποιείται για την δημιουργία συνδέσεων. Ωστόσο, αν ένα πακέτο UDP στέλνεται σε μια θύρα που δεν είναι ανοιχτή, το σύστημα θα απαντήσει με μήνυμα ICMP μη προσβάσιμης θύρας (ICMP port unreachable message). Οι περισσότεροι ανιχνευτές θυρών UDP χρησιμοποιούν αυτή τη μέθοδο σάρωσης, εκμεταλλευόμενοι την απουσία απόκρισης για να συμπεράνουν εάν μια θύρα είναι ανοιχτή. Ωστόσο, εάν μια θύρα είναι αποκλεισμένη από ένα τείχος προστασίας, η μέθοδος αυτή θα αναφέρει ψευδώς ότι η θύρα είναι ανοιχτή.

IV. ***ACK scanning*:** Η σάρωση ACK είναι ένα από τα πιο ασυνήθιστα είδη σάρωσης, καθώς δεν προσδιορίζεται επακριβώς εάν η θύρα είναι ανοικτή ή κλειστή, αλλά αν στην θύρα εφαρμόζεται κάποιο φίλτρο προστασίας. Η μέθοδος αυτή προσφέρει στον επιτιθέμενο πληροφορίες για την ύπαρξη τοίχους προστασίας (firewall) και του συνόλου κανόνων του.

- Τέλος, μια ακόμα μορφή παθητικής επίθεσης αποτελεί η αδρανής σάρωση (idle scanning),μια μέθοδος σάρωσης θυρών TCP που αποστέλλει πλαστογραφημένα πακέτα (spoofed packets) σε έναν υπολογιστή για να εντοπίσει ποιες υπηρεσίες είναι διαθέσιμες στο μηχάνημα αυτό. Ο σκοπός αυτός επιτυγχάνεται με την απομίμηση του επιτιθέμενου ως άλλου υπολογιστή που ονομάζεται "ζόμπι" (που δεν μεταδίδει ή λαμβάνει πληροφορίες). Ο επιτιθέμενος παρατηρώντας τη συμπεριφορά του συστήματος '' ζόμπι '' συλλέγει πληροφορίες για το σύστημα-στόχος. Οι Idle scans εκμεταλλεύονται την προβλέψιμη τιμή του πεδίου αναγνώρισης της κεφαλίδας IP: κάθε πακέτο IP από μια δεδομένη πηγή έχει ένα αναγνωριστικό που προσδιορίζει μοναδικά τα κομμάτια(fragments) ενός αρχικού datagram.



Εικόνα 3. Πρώτο Στάδιο επίθεσης spoofing



Εικόνα 4. Δεύτερο Στάδιο επίθεσης spoofing

Όπως περιγράφεται στην παραπάνω αναπαράσταση ο επιτιθέμενος σαρώνει αρχικά έναν υπολογιστή με ένα διαδοχικό και προβλέψιμο αριθμό ακολουθίας (IPID). Μόλις βρεθεί ένα κατάλληλο ζόμπι το επόμενο βήμα θα είναι να προσπαθήσει να δημιουργήσει μια σύνδεση TCP με δεδομένη υπηρεσία (θύρα) του συστήματος στόχου, πλαστοπροσωποποιώντας το ζόμπι. Αυτό γίνεται με την αποστολή ενός πακέτου SYN στον υπολογιστή στόχο, πλαστογραφώντας την διεύθυνση IP από το ζόμπι, δηλαδή θέτοντας την διεύθυνση πηγής να ισούται με την διεύθυνση IP του ζόμπι. Εάν η θύρα του υπολογιστή προορισμού είναι ανοιχτή θα δεχθεί τη σύνδεση για την υπηρεσία, απαντώντας με ένα πακέτο SYN / ACK πίσω στο ζόμπι. Ο υπολογιστής ζόμπι τότε θα στείλει ένα πακέτο RST στον υπολογιστή-στόχο (για να επαναφέρετε τη σύνδεση), διότι δεν έστειλε πραγματικά το πακέτο SYN την πρώτη φορά. Εφόσον το ζόμπι έπρεπε να στείλει το RST πακέτο θα αυξήσει το IPID του. Με αυτό τον τρόπο, ο επιτιθέμενος θα μάθει αν η θύρα στόχος είναι ανοιχτή. Ο επιτιθέμενος θα στείλει ένα άλλο πακέτο στο ζόμπι. Εάν το IPID αυξάνεται μόνο κατά ένα βήμα, τότε ο επιτιθέμενος θα γνωρίζει ότι η συγκεκριμένη θύρα είναι κλειστή. Η μέθοδος υποθέτει ότι το μηχάνημα «ζόμπι» δεν έχει άλλες αλληλεπιδράσεις. Αν υπάρχει μήνυμα που αποστέλλεται για άλλους λόγους μεταξύ της πρώτης αλληλεπίδρασης του επιτιθέμενου με το ζόμπι και της δεύτερης αλληλεπίδρασης εκτός από το RST μήνυμα τότε θα υπάρξει false positive (ψευδώς θετικά).

Ενεργητικές επιθέσεις:

Ενεργητικές είναι οι επιθέσεις στις οποίες ο επιτιθέμενος έχει αυξημένη αλληλεπίδραση με τον στόχο του. Στην ουσία όλες οι επιθέσεις που δεν ανήκουν στις παθητικές είναι ενεργητικές. Ο επιτιθέμενος στέλνει διάφορα πακέτα στον στόχο, μέσω των οποίων μπορεί να συλλέξει πληροφορίες για αυτόν ή και να υλοποιήσει ένα exploit. Τέτοιου είδους επιθέσεις στοχεύουν είτε ένα ολόκληρο υποδίκτυο είτε μεμονωμένους στόχους είτε πρόκειται για επιθέσεις άρνησης υπηρεσιών.

Επιθέσεις σε Δίκτυο:

- ***Man in the middle:*** Μία επίθεση man-in-the-middle είναι μια επίθεση όπου ο επιτιθέμενος μεταδίδει κρυφά και, ενδεχομένως, αλλάζει την επικοινωνία μεταξύ δύο μερών που πιστεύουν πως συνδέονται άμεσα μεταξύ τους. Ως μια επίθεση που στοχεύει στην παράκαμψη της αμοιβαίας επαλήθευσης ταυτότητας, μία man-in-the-middle επίθεση μπορεί να επιτύχει μόνο όταν ο επιτιθέμενος μπορεί να μιμηθεί κάθε ένα από τα άκρα επικοινωνίας όπως αναμένει το κάθε νόμιμο άκρο. Τα περισσότερα πρωτόκολλα κρυπτογράφισης περιλαμβάνουν κάποιας μορφής ελέγχου ταυτότητας στο τελικό σημείο (endpoint authentication), ειδικά για να αποτρέψουν τις επιθέσεις MITM. Για παράδειγμα, το TLS (*Transport Layer Security*) είναι ένα πρωτόκολλο που διασφαλίζει την επικοινωνία εξυπηρετητή - πελάτη (server -client) μέσω του διαδικτύου, αποτρέποντας την μεσολάβηση κάποιου τρίτου που θα "υποκλέψει" το περιεχόμενο της επικοινωνίας [44].

- **ARP spoofing:** Το ARP spoofing, ARP cache poisoning ή ARP poison routing είναι μια τεχνική με την οποία ο επιτιθέμενος στέλνει πλαστογραφημένα (spoofed) Address Resolution Protocol (ARP) μηνύματα σε ένα τοπικό δίκτυο. Εν συντομία, ο στόχος είναι να συσχετίσει τη διεύθυνση MAC του επιτιθέμενου με τη διεύθυνση IP ενός άλλου υπολογιστή, προκαλώντας οποιαδήποτε κίνηση που προορίζονταν για τη συγκεκριμένη διεύθυνση IP να αποστέλλεται στον εισβολέα. Το ARP spoofing μπορεί να επιτρέψει σε έναν επιτιθέμενο να υποκλέψει τα πλαίσια δεδομένων (data frames) σε ένα δίκτυο, να τροποποιήσει την κυκλοφορία, ακόμη και να σταματήσει όλη την κυκλοφορία. Συχνά, η επίθεση χρησιμοποιείται ως μία πρώτη επίθεση για την επίτευξη επόμενων επιθέσεων, όπως η άρνηση παροχής υπηρεσιών(denial of service), man-in-the-middle. Η επίθεση μπορεί να χρησιμοποιηθεί μόνο σε δίκτυα που χρησιμοποιούν το Address Resolution Protocol, και περιορίζεται σε τοπικά τμήματα του δικτύου [45].

Επιθέσεις σε μεμονωμένους στόχους:

Οι επιθέσεις αυτού του τύπου στοχεύουν στην εκμετάλλευση ευπαθειών στο μηχάνημα-στόχος, εκμεταλλευόμενες γνωστές ευπάθειες στα συστήματα όπως buffer overflow, υπερχείλιση σωρού(heap overflow), υπερχείλιση στοίβας (stack overflow), SQLinjection.

Τα πιο εξελιγμένα είδη απειλών σε συστήματα πληροφορικής παρουσιάζονται από προγράμματα που εκμεταλλεύονται τα τρωτά σημεία των συστημάτων πληροφορικής. Τέτοιες απειλές αναφέρονται ως κακόβουλο λογισμικό ή malware.

Πολλές από αυτές τις επιθέσεις που βασίζονται σε αυτά τα προγράμματα είναι αυτοματοποιημένες, δηλαδή υπάρχουν προγράμματα που υλοποιούν μέρος ή ολόκληρη την επίθεση. Το κακόβουλο λογισμικό διαχωρίζεται σε δύο κατηγορίες: τα προγράμματα που χρειάζονται ένα πρόγραμμα ξενιστή (host program) και τα ανεξάρτητα προγράμματα. Η πρώτη κατηγορία που αναφέρεται ως παρασιτικό κακόβουλο λογισμικό, είναι ουσιαστικά τμήματα προγραμμάτων που δεν μπορούν να υπάρξουν ανεξάρτητα χωρίς κάποιο πρόγραμμα εφαρμογής, βοηθητικό πρόγραμμα, ή πρόγραμμα συστήματος. Οι ιοί, λογικές βόμβες, και κερκόπορτες αποτελούν παραδείγματα. Το ανεξάρτητο κακόβουλο λογισμικό είναι ένα αυτόνομο πρόγραμμα που μπορεί να προγραμματιστεί και να τρέξει από το λειτουργικό σύστημα. Παραδείγματα αυτής της κατηγορίας είναι τα σκουλήκια και τα προγράμματα bot.

Ακολουθεί μια σύντομη περιγραφή των εν λόγω κακόβουλων λογισμικών [46].

- **Ιοί (viruses):** Κακόβουλο λογισμικό που προσαρτά τον εαυτό του σε ένα πρόγραμμα και μεταδίδει αντίγραφα του εαυτού του σε άλλα προγράμματα
- **Σκουλήκια (worms):** Ένα πρόγραμμα υπολογιστή που μπορεί να τρέξει ανεξάρτητα και μπορεί να διαδώσει μια λειτουργική έκδοση του εαυτού του σε άλλους υπολογιστές σε ένα δίκτυο.
- **Λογική Βόμβα (Logic bomb):** Ένα πρόγραμμα που εισάγεται στο λογισμικό από έναν επιτιθέμενο. Μια λογική βόμβα βρίσκεται αδρανής μέχρι να συναντήσει μια προκαθορισμένη κατάσταση. Το πρόγραμμα στη συνέχεια ενεργοποιεί μια μη εγκεκριμένη πράξη.
- **Δούρειοι Ίπποι (Trojans):** Ένα πρόγραμμα υπολογιστή που φαίνεται να έχει μια χρήσιμη λειτουργία, αλλά έχει επίσης μία κρυφή και δυνητικά κακόβουλη λειτουργία που αποφεύγει τους μηχανισμούς ασφάλειας, μερικές φορές με την αξιοποίηση νόμιμων αδειών από ένα φορέα συστήματος που επικαλείται το πρόγραμμα Δούρειος ίππος.
- **Κερκόπορτα (backdoor):** Κάθε μηχανισμός που παρακάμπτει ένα κανονικό έλεγχο ασφαλείας. Μπορεί να επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε λειτουργίες.
- **Προγράμματα μεταφόρτωσης (Downloaders):** Πρόγραμμα που εγκαθιστά άλλα αντικείμενα σε ένα μηχάνημα το οποίο βρίσκεται υπό επίθεση. Συνήθως, ένα πρόγραμμα μεταφόρτωσης αποστέλλεται μέσω e-mail.
- **Auto-router:** Κακόβουλα εργαλεία των hacker, που χρησιμοποιούνται για να παρεισφρήσουν εξ αποστάσεως σε μηχανήματα.
- **Γεννήτρια ιών (kit):** Σύνολο εργαλείων για την αυτόματη δημιουργία ιών.
- **Προγράμματα αποστολής ανεπιθύμητης αλληλογραφίας (Spammer):** Χρησιμοποιείται για την αποστολή μεγάλων όγκων ανεπιθύμητα e-mail.
- **Προγράμματα πλημμύρας (Flooders):** Χρησιμοποιούνται για επίθεση σε δικτυωμένα υπολογιστικά συστήματα που διακινούν μεγάλο όγκο πληροφορίας, προκειμένου να εκτελέσουν επίθεση άρνησης υπηρεσίας(DoS).
- **Προγράμματα καταγραφής πληκτρολόγησης (Keyloggers):** Καταγράφουν σε ένα σύστημα που έχει παραβιαστεί, τα πλήκτρα που πατά ο χρήστης.
- **Rootkit:** Σύνολο εργαλείων των hacker που χρησιμοποιείται εφόσον ο επιτιθέμενος έχει διεισδύσει σε ένα υπολογιστικό σύστημα και έχει αποκτήσει πρόσβαση ως διαχειριστής (root).
- **Zombie:** Πρόγραμμα που ενεργοποιείται σε ένα ήδη μολυσμένο μηχάνημα ώστε να εξαπολύει επιθέσεις σε άλλα μηχανήματα.

2.4.3 Επίθεση Άρνησης Υπηρεσιών

Στο σημείο αυτό θα γίνει μια εκτενής αναφορά σε ένα συγκεκριμένο είδος επίθεσης γνωστή ως επίθεση Άρνησης Υπηρεσιών, το οποίο σύμφωνα με πρόσφατες έρευνες αυξάνεται δραματικά τα τελευταία χρόνια [47]**.**

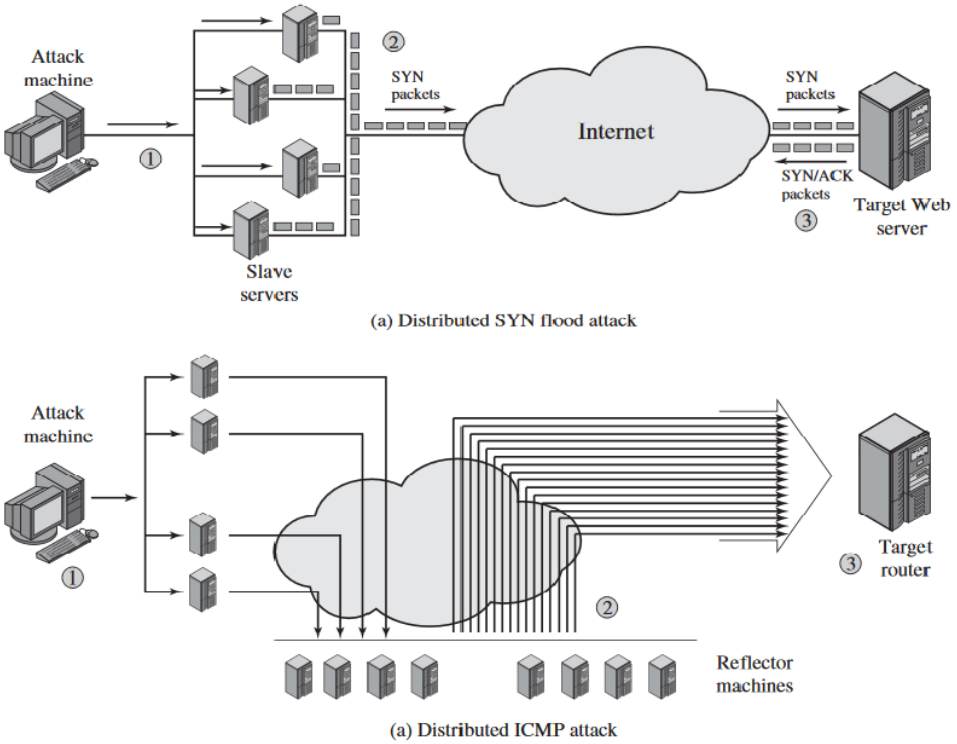
Αυτές οι επιθέσεις έχουν σαν στόχο να προκαλέσουν δυσλειτουργία του συστήματος ή του δικτύου που πλήττουν ώστε να το εμποδίσουν να προσφέρει τις υπηρεσίες για τις οποίες είναι

προορισμένο στους νόμιμους χρήστες του. Τέτοιου είδους ενδεικτικές δυσλειτουργίες αποτελούν η επανεκκίνηση, η παύση, η κατάρρευση ενός συστήματος ή η δημιουργία αυξημένης κίνησης (traffic) και συμφόρησης ενός δικτύου. Οι επιθέσεις αυτές ονομάζονται (D)DoS - (Distributed) Denial Of Service επιθέσεις. Οι DDoS επιθέσεις καθιστούν τα υπολογιστικά συστήματα μη προσβάσιμα, «πλημμυρίζοντας» servers, δίκτυα, ή ακόμα και τα συστήματα των χρηστών με άχρηστη κίνηση, έτσι ώστε οι νόμιμοι χρήστες να μην έχουν πρόσβαση στους πόρους αυτούς. Σε μια τυπική περίπτωση DDoS επίθεσης, ένας μεγάλος αριθμός παραβιασμένων υπολογιστών χρησιμοποιείται για να αποστείλει άχρηστα πακέτα. Τα τελευταία χρόνια, οι μέθοδοι επίθεσης καθώς και τα αντίστοιχα εργαλεία έχουν γίνει πιο εξειδικευμένα και αποτελεσματικά, είναι πιο δύσκολο να εντοπιστούν οι πραγματικοί επιτιθέμενοι, ενώ οι τεχνικές άμυνας δεν μπορούν να αντισταθούν σε επιθέσεις ευρείας κλίμακας.

2.4.3.1 Περιγραφή Επίθεσης DDOS

Μια επίθεση DDoS επιχειρεί να καταναλώσει τους πόρους του συστήματος-στόχου συντελώντας στην μη ικανότητα παροχής υπηρεσίας. Μία μέθοδος κατηγοριοποίησης των επιθέσεων DDoS είναι λαμβάνοντας υπόψιν το είδος των πόρων, του συστήματος-στόχος, που καταναλώνουν. Σε γενικές γραμμές, ο πόρος που καταναλώνεται είναι είτε ο εσωτερικός πόρος του υπολογιστή στο σύστημα στόχο είτε η χωρητικότητα μετάδοσης δεδομένων στο τοπικό δίκτυο που βρίσκεται ο στόχος. Ένα απλό παράδειγμα επίθεσης εσωτερικού πόρου είναι η επίθεση πλημμύρας SYN (SYN flood)όπως φαίνεται στο ακόλουθο σχήμα (a). Ακολουθούν τα βήματα της επίθεσης:

1. Ο επιτιθέμενος αποκτά τον έλεγχο πολλαπλών υπολογιστών(κόμβων) του Διαδικτύου, αναθέτοντας τους να επικοινωνήσουν με το σύστημα-στόχος, που είναι κάποιος εξυπηρετητής διαδικτύου.
2. Οι κόμβοι αυτοί ξεκινούν να στέλνουν πακέτα SYN (synchronize/initialization) του πρωτοκόλλου TCP/IP, με εσφαλμένες πληροφορίες ως προς την διεύθυνση IP επιστροφής, στον στόχο.
3. Κάθε πακέτο SYN αποστέλλει ένα αίτημα για να ανοίξει μια σύνδεση TCP. Για κάθε τέτοιο πακέτο, ο εξυπηρετητής διαδικτύου (Web server) απαντά με ένα SYN / ACK (synchronize/ initialization), προσπαθώντας να δημιουργήσει μια σύνδεση TCP με μια οντότητα TCP στην ψευδή διεύθυνση IP. Ο εξυπηρετητής διαδικτύου διατηρεί μια δομή δεδομένων για κάθε αίτηση SYN, περιμένοντας να λάβει μία απάντηση με αποτέλεσμα να υπερφορτώνεται και να τελματώνει καθώς δέχεται όλο και περισσότερη κίνηση. Τελικά, το αποτέλεσμα είναι ότι οι νόμιμες συνδέσεις δεν μπορούν να αποκαθίστανται, καθώς το μηχάνημα του θύματος περιμένει να ολοκληρώσει τις ψεύτικες "μισάνοιχτες" συνδέσεις.



Εικόνα 5. Κατανεμημένες επιθέσεις SYN(a)/ICMP(b)

Η δομή δεδομένων κατάστασης TCP συνδέσεων είναι ένας ιδιαίτερα δημοφιλής στόχος επιθέσεων DDOS αλλά οπωσδήποτε όχι ο μοναδικός. Ένας επιτιθέμενος μπορεί να προσπαθήσει να καταναλώσει χώρο του δίσκου με τρόπους όπως:

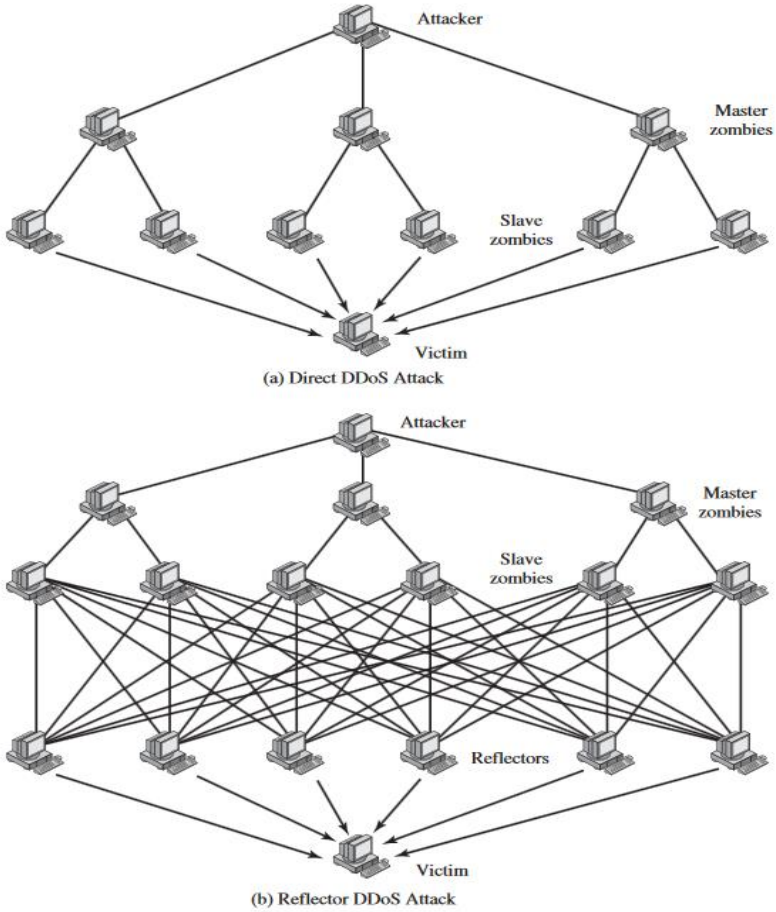
- δημιουργώντας υπερβολικό πλήθος μηνυμάτων ηλεκτρονικού ταχυδρομείου
- παράγοντας σκόπιμα σφάλματα που πρέπει να τηρούνται σε ημερολόγιο του συστήματος
- την τοποθέτηση αρχείων σε ανώνυμες περιοχές FTP ή σε περιοχές κοινόχρηστου δικτύου

Στο σχήμα (b) της προηγούμενης εικόνας αναπαρίσταται μία επίθεση που καταναλώνει πόρους μετάδοσης δεδομένων. Η επίθεση αυτή υλοποιείται από τα ακόλουθα βήματα:

1. Ο επιτιθέμενος παίρνει τον έλεγχο πολλαπλών κόμβων του Διαδικτύου, αναθέτοντας τους να στείλουν πακέτα ICMP ECHO με πλαστογραφημένες διεύθυνσεις IP του στόχου σε ένα σύνολο άλλων κόμβων που ενεργούν ως ανακλαστήρες.
2. Οι κόμβοι-ανακλαστήρες λαμβάνουν πολλαπλά πλαστογραφημένα αιτήματα και απαντούν, στέλνοντας πακέτα echo στον υπολογιστή που θεωρούν ως αποστολέα των πακέτων, δηλαδή στο σύστημα-στόχος.
3. Ο δρομολογητής-στόχος πλημμυρίζει με πακέτα, χωρίς να αφήνει χωρητικότητα μετάδοσης δεδομένων για την νόμιμη κίνηση του διαδικτύου.

Οι επιθέσεις DDOS μπορούν επίσης να διακριθούν σε άμεσες και σε ανακλαστικές, εξαρτώμενες από την αρχιτεκτονική των μηχανημάτων που χρησιμοποιούνται στις επιθέσεις, όπως αυτή θα περιγραφεί στην συνέχεια. Σε μία άμεση επίθεση DDOS, ο επιτιθέμενος επιδιώκει να εμφυτεύσει λογισμικό zombie σε ένα πλήθος κόμβων σε διάφορα σημεία του διαδικτύου. Συνήθως, σε τέτοιου είδους επίθεση χρησιμοποιούνται δύο ειδών μηχανήματα, τα κύρια (master)και τα δευτερεύοντα (slave). Μία ανακλαστική επίθεση DDOS προσθέτει ένα ακόμα είδος

μηχανημάτων. Σε αυτό τον τύπο επίθεσης τα zombie κατασκευάζουν πακέτα, απαιτώντας απόκριση που να περιέχει την διεύθυνση IP του στόχου φερόμενη ως IP προέλευσης. Εν συνεχεία, τα πακέτα αυτά αποστέλλονται σε μη μολυσμένα μηχανήματα που ονομάζονται ανακλαστήρες. Τα μη μολυσμένα μηχανήματα με την σειρά τους απαντούν με πακέτα που στέλνονται στο μηχάνημα-στόχος. Οι δύο τύποι επιθέσεων DDOS αναπαρίστανται στο ακόλουθο σχήμα.



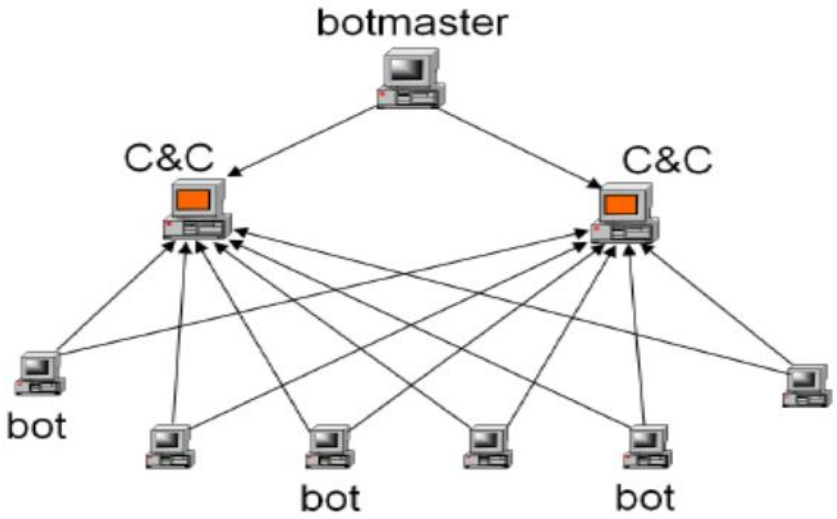
Εικόνα 6. Είδη επιθέσεων DDOS

2.4.4 Botnets

Οι DDoS επιθέσεις, χωρίς αμφιβολία αποτελούν την πιο επικίνδυνη μορφή επιθέσεων που υλοποιούνται από botnets. Πρωτού γίνει αναφορά στα botnets, πρέπει να ορισθεί τι είναι ένα bot. Στην απλούστερη μορφή του, ένα bot είναι ένα κομμάτι κώδικα υπολογιστή που εκτελεί μια εργασία αυτόματα. Μπορεί να παίξει πόκερ για λογαριασμό κάποιου (Dance, 2011),να πραγματοποιεί αναζητήσεις για μεγάλους πρώτους αριθμούς (GIMPS, 2011), ή να ψάχνει για εξωγήινη νοημοσύνη (SETI, 2011). Σύμφωνα με τους Provos & Holz (2007), ένα botnet ορίζεται ως «δίκτυο μολυσμένων υπολογιστών που μπορούν να ελέγχονται απομακρυσμένα από έναν επιτιθέμενο». Με λίγα λόγια, ένα botnet είναι ένα σύνολο από bots που χρησιμοποιείται με κακόβουλη πρόθεση. Μόλις ένα μηχάνημα μολυνθεί με ένα bot και ρυθμιστεί από τον επιτιθέμενο, μπορεί να αποκτήσει τον πλήρη έλεγχο του μολυσμένου υπολογιστή. Ο επιτιθέμενος είναι επίσης γνωστός ως botmaster.

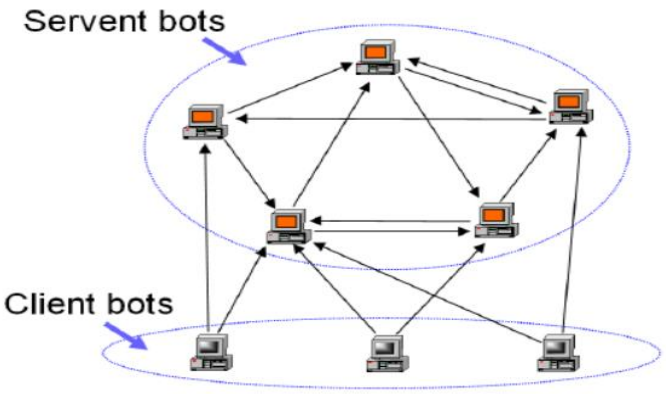
2.4.4.1 Οργάνωση και αρχιτεκτονική ενός botnet

Τα πρώτα botnets οργανώθηκαν σε κεντρικό επίπεδο ή με δομημένο τρόπο, με κάθε bot να επικοινωνεί απευθείας με τον κόμβο διοίκησης και ελέγχου (Command and Control server). Τα Botnets λαμβάνουν εντολές από τον κόμβο διοίκησης και ελέγχου και στην συνέχεια στέλνουν τα αποτελέσματα πίσω στον κόμβο διοίκησης και ελέγχου. Τα πιο πρόσφατα botnets, που είναι πιο εξελιγμένα, δημιουργούν μια ιεραρχία εξυπηρετητών διοίκησης και ελέγχου ώστε να καθιστούν πιο δύσκολη την διαδικασία εντοπισμού του κύριου εξυπηρετητή διοίκησης και ελέγχου. Υποδεέστεροι εξυπηρετητές διοίκησης και ελέγχου, που συχνά αποκαλούνται ελεγκτές bot, είναι συχνά και οι ίδιοι μολυσμένοι υπολογιστές. Η πολυεπίπεδη (multi-tier) αρχιτεκτονική διοίκησης και ελέγχου των botnets παρέχει ανωνυμία για το botmaster. Η χρήση διαμεσολαβητών(proxying) είναι μία ακόμα προσέγγιση που εφαρμόζεται για την απόκρυψη της ταυτότητας του botmaster. Μια απεικόνιση ενός κεντρικοποιημένου (centralized) botnet φαίνεται παρακάτω.



Εικόνα 7. Centralized Botnet

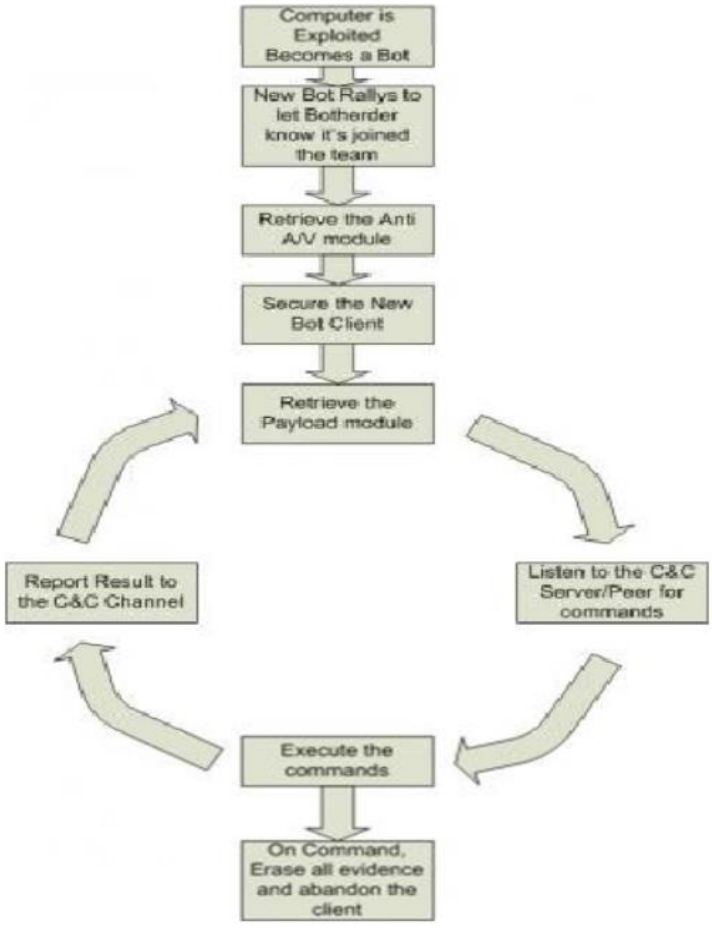
Το παραπάνω σχήμα δείχνει την κεντρικοποιημένου (centralized) αρχιτεκτονική διοίκησης και ελέγχου που χρησιμοποιείται στην πλειοψηφία των πρωταρχικών botnets. Πιο πρόσφατα, τα αποκεντρωμένα (decentralized) botnets έχουν προκύψει. Οι αποκεντρωμένες αρχιτεκτονικές botnet έχουν γενικευτεί ως peer-to-peer (P2P) αρχιτεκτονικές. Δεν υπάρχει κεντρικός εξυπηρετητής διοίκησης και ελέγχου σε ένα P2P botnet. Οι εξυπηρετητές μπορούν να λειτουργήσουν εντελώς ανεξάρτητα μεταξύ τους, έτσι ώστε ακόμη και αν ένας από τους εξυπηρετητές ανιχνευτεί και κλείσει να υπάρξει πολύ μικρή επίδραση στη συνολική λειτουργικότητα του botnet. Σε αυτή την αρχιτεκτονική οι εξυπηρετητές δεν γνωρίζουν όλους τους υπολογιστές του botnet, κάθε εξυπηρετητής γνωρίζει μόνο ένα υποσύνολο του συνολικού αριθμού των μολυσμένων υπολογιστών, με αποτέλεσμα να καθιστά πολύ πιο δύσκολο τον εντοπισμό και τον τερματισμό ολόκληρου του δικτύου του botnet. Μια απεικόνιση ενός αποκεντρωμένου δικτύου (decentralized) φαίνεται παρακάτω.



Εικόνα 8. Decentralized Botnet

2.4.4.2 Κύκλος Ζωής ενός botnet

Ο κύκλος ζωής ενός botnet είναι προκαθορισμένος, ανεξάρτητα από την αρχιτεκτονική ελέγχου και επικοινωνίας που χρησιμοποιήθηκε κατά την αρχική μέθοδο διάδοσης του κακόβουλου κώδικα στα μηχανήματα-στόχος. Ακολουθούν τα βήματα της ζωής ενός botnet:



Εικόνα 9. Κύκλος ζωής botnet

1. Μέσω της εκμετάλλευσης μίας ευπάθειας στο μηχάνημα-στόχος το κακόβουλο λογισμικό αποκτά πρόσβαση στο σύστημα-στόχος και το μετατρέπει σε bot.
2. Το πρόσφατα μολυσμένο μηχάνημα στέλνει ένα μήνυμα προς τον botmaster πληροφορώντας τον ότι έχει ενταχθεί στην ομάδα. Αυτή η διαδικασία είναι γνωστή ως συσπείρωση (rallying).
3. Στο επόμενο βήμα το bot, χρησιμοποιώντας τον εξυπηρετητή διοίκησης και ελέγχου του, προσπαθεί να κατεβάσει και να εγκαταστήσει ένα anti-antivirus λογισμικό το οποίο θα καταστήσει οποιοδήποτε λογισμικό προστασίας από ιούς στο μηχάνημα μη αποτελεσματικό.
4. 'Ενα από τα επόμενα βήματα που πραγματοποίει ένα bot είναι να διορθώσει τρωτά σημεία του συστήματος στο οποίο φιλοξενείται με την εφαρμογή patches. Η διαδικασία αυτή θα αποτρέψει άλλα κακόβουλα προγράμματα να εισχωρήσουν στο σύστημα και να πάρουν τον έλεγχο του συστήματος.
5. Ένα από τα κύρια χαρακτηριστικά του botnet είναι ότι η λειτουργικότητά του μπορεί να αλλάξει καθ' υπόδειξη του επιτιθέμενου. Η σχεδίαση των botnet επιτρέπει στον botmaster να εγκαθιστά payloads τα οποία θα υλοποιήσουν τη λειτουργικότητα που απαιτείται σε κάθε περίπτωση.
6. Στην συνέχεια κατά τη διάρκεια της φάσης διοίκησης και ελέγχου, ο botmaster στέλνει εντολές προς εκτέλεση στο botnet χρησιμοποιώντας μια κατάλληλη αρχιτεκτονική, όπως η κεντρική ή αποκεντρωμένη, και το κατάλληλο πρωτόκολλο επικοινωνίας συμπεριλαμβανομένων των IRC, HTTP, ή P2P.
7. Το bot στη συνέχεια εκτελεί την εντολή και αναφέρει τα αποτελέσματα της πίσω στον εξυπηρετητή διοίκησης και ελέγχου σε καθορισμένο από τον επιτιθέμενο χρόνο.
8. Σε αυτό το βήμα το bot και πάλι πηγαίνει πίσω στο στάδιο 5, σύμφωνα με το οποίο περιμένει εκ νέου οδηγίες ή νέα payload που πρέπει να παραδοθούν.
9. Τέλος, με τη λήψη μιας προκαθορισμένης εντολής από τον botmaster το bot μπορεί να σβήσει όλα τα ίχνη του από τον υπολογιστή και να τον εγκαταλείψει. Το bot συχνά αφήνει το σύστημα σε μία κατάσταση όπου υπάρχουν ευπάθειες στο σύστημα ώστε να διασφαλίσει ότι μελλοντικές επιθέσεις μπορεί να υλοποιηθούν.

2.4.4.3 Πρωτόκολλο επικοινωνίας των botnet

Τα πρώτα botnets χρησιμοποιούσαν το πρωτόκολλο IRC (Internet Relay Chat) για να επικοινωνήσουν. Στην συνέχεια χρησιμοποιήθηκε το πρωτόκολλο HTTP (Hypertext Transfer Protocol), κυρίως επειδή σχεδόν σε κάθε κόμβο στο διαδίκτυο αναμένεται να έχει πρόσβαση στο διαδίκτυο μέσω του HTTP. Επιπλέον, η επικοινωνία μέσω ενός κοινού πρωτόκολλου καθιστά την ανίχνευση της δραστηριότητας ενός botnet πιο δύσκολη [48] [49] [50].

2.5 Μέθοδος υλοποίησης επιθέσεων

Στο σημείο αυτό αφού πραγματοποιήθηκε μια αναφορά στα είδη των επιθέσεων που θέτουν σε κίνδυνο την ασφάλεια των πληροφοριακών συστημάτων. Θα εξεταστεί η διαδικασία μέσω της οποίας οργανώνεται και υλοποιείται μια επίθεση σε ένα σύστημα το οποίο είναι συνδεδεμένο στο διαδίκτυο. Μια τυπική προσέγγιση ακολουθεί τα εξής βήματα:

1. Απαρίθμηση δικτύου (Network enumeration)
2. Ανάλυση ευπαθειών (Vulnerability analysis)
3. Εκμετάλλευση (Exploitation)

2.5.1 Απαρίθμηση δικτύου:

Η απαρίθμηση του δικτύου είναι μια υπολογιστική δραστηριότητα κατά την οποία ανακτώνται πληροφορίες σχετικά με τις ομάδες και τις υπηρεσίες ενός δικτύου υπολογιστών. Είναι η διαδικασία ανακάλυψης και εντοπισμού υπολογιστών/συσκευών ενός δικτύου. Για την υλοποίηση της απαρίθμησης του δικτύου χρησιμοποιούνται κυρίως πρωτόκολλα όπως ICMP και SNMP για την συλλογή πληροφοριών. Ο επιτιθέμενος σε αυτό το στάδιο της επίθεσης επιδιώκει να ελέγξει ένα εύρος θυρών σε απομακρυσμένους υπολογιστές αναζητώντας ευρέως γνωστές υπηρεσίες, σε μια προσπάθεια να προσδιορίσει περαιτέρω τη λειτουργία ενός απομακρυσμένου υπολογιστή.

2.5.2 Ανάλυση ευπαθειών:

Οι ευπάθειες (vulnerabilities) προκύπτουν από ελαττώματα που εντοπίζονται σε λογισμικά και η εκμετάλλευση τους μπορεί να οδηγήσει σε μια επιτυχής επίθεση. Μερικά από τα πλέον χαρακτηριστικά παραδείγματα ευπαθειών λογισμικού είναι τα Buffer Overflows και SQL injections.

2.5.3 Εκμετάλλευση:

Η διαδικασία κατά την οποία γίνεται κατάλληλη εκμετάλλευση των ευπαθειών ονομάζεται exploit. Στο σημείο αυτό παρουσιάζεται η δυσκολία της ακριβούς μετάφρασης του όρου exploit στην ελληνική γλώσσα συνεπώς θα διατηρηθεί η αγγλική ορολογία. Το exploit αποτελεί τμήμα λογισμικού, ένα μεγάλο κομμάτι δεδομένων ή μια ακολουθία εντολών, το οποίο εκμεταλλεύεται σφάλματα ή ευπάθειες, προκαλώντας μη αναμενόμενες συμπεριφορές στο λογισμικό ή στο υλικό των ηλεκτρονικών υπολογιστών.

2.6 Μέθοδοι αντιμετώπισης επιθέσεων

Έχοντας παραθέσει τους στόχους που παρακινούν τους επιτιθέμενους καθώς επίσης και τις μεθόδους υλοποίησης των επιθέσεων τους, στο σημείο αυτό θα γίνει μια ανασκόπηση των μεθόδων και των τεχνικών που εφαρμόζονται για την επίλυση των προβλημάτων των επιθέσεων αυτών. Η ανίχνευση παρεισφρήσεων αποτελεί βασική τεχνική στην ασφάλεια πληροφοριών διαδραματίζοντας σημαντικό ρόλο στην ανίχνευση διάφορων τύπων επιθέσεων και εξασφαλίζοντας την ασφάλεια ενός δικτύου. Πριν συνεχιστεί η ανάλυση των μεθόδων ανίχνευσης παρεισφρήσεων πρέπει να οριστεί η συγκεκριμένη έννοια. Στα πλαίσια της παρούσας έρευνας, ως ανίχνευση παρεισφρήσεων θα θεωρηθεί η διαδικασία παρακολούθησης και ανάλυσης γεγονότων που προκύπτουν σε έναν υπολογιστή ή ένα δίκτυο υπολογιστών εντοπίζοντας όλα τα προβλήματα ασφαλείας. Συνεπώς, ένα σύστημα ανίχνευσης παρεισφρήσεων (Intrusion Detection System - IDS) είναι μία εφαρμογή ή συσκευή παρακολούθησης ανωμαλιών ή κακόβουλων δραστηριοτήτων του

δικτύου. Τα IDS χρησιμοποιούνται για την ανίχνευση διάφορων επιθέσεων οι οποίες μπορούν να κατηγοριοποιηθούν [51] [52]ως εξής:

- ***Άρνησης Υπηρεσιών:*** Όπως έχει αναφερθεί προηγουμένως αναλυτικά μια επίθεση DoS είναι μια επίθεση στην οποία ο επιτιθέμενος πλημμυρίζει έναν υπολογιστική ή τους πόρους μνήμης με ψευδείς αιτήσεις, έτσι ώστε να αδυνατεί να εξυπηρετήσει τα νόμιμα αιτήματα συνεπώς στερώντας στους χρήστες πρόσβαση στην υπηρεσία.
- ***Probing:*** Το probing αποτελεί επίθεση που αποσκοπεί στην απόκτηση πρόσβασης στις ρυθμίσεις (configuration) του μηχανήματος στόχος ή ολόκληρου του δικτύου.
- **User-to-Root (U2R):** Οι επιθέσεις αυτές έχουν ως στόχο την απόκτηση δικαιωμάτων διαχειριστή σε ένα μηχάνημα στο οποίο ο εισβολέας έχει πρόσβαση στο επίπεδο χρήστη. Η διαδικασία αυτή ονομάζεται επίσης κλιμάκωση δικαιωμάτων χρήστη (privilege escalation).
- ***Remote-to-Local (R2L):*** Κατά την διάρκεια της συγκεκριμένης κατηγορίας επιθέσεων ο επιτιθέμενος στέλνει πακέτα σε ένα μηχάνημα, στο οποίο δεν έχει πρόσβαση, μέσω διαδικτύου προκειμένου να αναγνωρίσει τα ευπαθή σημεία του συστήματος και να εκμεταλλευτεί τα προνόμια που θα είχε ένας τοπικός χρήστης στον υπολογιστή.

Αφού αναφέρθηκαν οι τύποι επιθέσεων που αντιμετωπίζουν τα IDS στην συνέχεια θα ακολουθήσει μία προσπάθεια κατηγοριοποίηση τους βασισμένη στους ακόλουθους παράγοντες:

1. Τοποθεσία
2. Λειτουργικότητα
3. Προσέγγιση ανάπτυξης τους (deployment approach)
4. Μηχανισμών ανίχνευσης

2.6.1 Τοποθεσία

Host Based Intrusion Detection (HIDS)

Το HIDS αποτελεί σύστημα ανίχνευσης παρεισφρήσεων σε ένα συγκεκριμένο μηχάνημα παρακολουθώντας την ασφάλεια του εν λόγω συστήματος ή υπολογιστή από εσωτερικές και εξωτερικές επιθέσεις. Οι εσωτερικές επιθέσεις αφορούν την κατάσταση ανίχνευσης των προσβάσιμων πόρων από κάποιο πρόγραμμα και αν αυτό δημιουργεί ενδεχόμενες παραβιάσεις ασφάλειας του συστήματος. Οι εξωτερικές επιθέσεις αφορούν την ανάλυση πακέτων, από το HIDS, προς και από τις διεπαφές του συστήματος (υπολογιστή). Το HIDS καταγράφει τις δραστηριότητες (logging) και ενημερώνει τις αρμόδιες αρχές (π.χ. του διαχειριστή του συστήματος). Τέτοια προγράμματα ανίχνευσης παρεισφρήσεων αποτελούν τα τείχη προστασίας(firewalls) και τα antivirus. Ωστόσο, ένα HIDS έχει περιορισμένη «εικόνα» ολόκληρης της τοπολογίας του δικτύου καθιστώντας έτσι αδύνατη την ανίχνευση επιθέσεων που στοχεύουν ένα μηχάνημα του δικτύου που δεν έχει εγκατεστημένο το HIDS.

Network Based Intrusion Detection (NIDS)

Το σύστημα ανίχνευσης παρεισφρήσεων δικτύου (NIDS) παρακολουθεί την κίνηση του δικτύου και αναλύει την διερχόμενη κίνηση για πιθανές επιθέσεις. Κατά τον εντοπισμό επίθεσης ή μη φυσιολογικής συμπεριφοράς αποστέλλεται στον διαχειριστή του δικτύου ανάλογη ειδοποίηση.

2.6.2 Λειτουργικότητα

Σύστημα ανίχνευσης παρείσφρησης (intrusion detection system, IDS)

Όπως αναφέρθηκε, η ανίχνευση εισβολής αποτελεί την διαδικασία εντοπισμού κακόβουλης δραστηριότητας που στοχεύει υπολογιστικούς και δικτυακούς πόρους. Υπάρχουν δύο τύποι συστημάτων ανίχνευσης εισβολής: HIDS και NIDS. Τα συστήματα ανίχνευσης παρείσφρησης ανιχνεύουν πιθανές εισβολές και αναφέρουν τα σχετικά ευρήματα στον διαχειριστή. Υπάρχουν δύο τύποι τεχνικών ανίχνευσης παρείσφρησης: 1) ανίχνευσης Ανωμαλιών (Anomaly detection) 2) ανίχνευση Καταχρήσεων (Misuse detection). Η τεχνική της ανίχνευσης ανωμαλιών αναλύει τις συλλεγόμενες πληροφορίες συγκρίνοντας τες με αναφορικές τιμές που υποδηλώνουν κανονική/φυσιολογική συμπεριφορά υπηρεσίας. Η τεχνική της ανίχνευσης καταχρήσεων βασίζεται στις υπογραφές γνωστών επιθέσεων. Και στις δύο περιπτώσεις τα IDS ανιχνεύουν τις επιθέσεις χωρίς να επιχειρούν να τις σταματήσουν.

Σύστημα αποτροπής παρείσφρησης (intrusion prevention system, IPS)

Τα IDS έχουν μόνο ικανότητες ανίχνευσης εισβολών χωρίς αποτρεπτικές λειτουργίες. Το σύστημα αποτροπής παρείσφρησης αποτελεί προληπτική τεχνική, η οποία αποτρέπει την επίθεση πριν εισέλθει στο δίκτυο εξετάζοντας τα πακέτα και το μοτίβο τους (pattern) και αν κριθούν κακόβουλα εμποδίζονται. Το IPS αποτελεί ένα σύστημα που παρέχει πρώιμη ανίχνευση των επιθέσεων.

2.6.3 Προσέγγιση ανάπτυξης συστημάτων ανίχνευσης παρείσφρησης (deployment)

Single host

Στην εγκατάσταση single host ενός συστήματος ανίχνευσης εισβολής δικτύου (NIDS), το σύστημα είναι εγκατεστημένο σε ένα μηχάνημα του δίκτυο που μπορεί να είναι ένας δρομολογητής, ένας εξυπηρετητής ή switch δικτύου. Όλη η κίνηση εισέρχεται και εξέρχεται από το δίκτυο μέσω του εν λόγω κόμβου, όπου ελέγχεται, από το NIDS, για επιθέσεις και κανονικής/φυσιολογικής κίνησης πακέτα. Τα πλεονεκτήματα της συγκεκριμένης προσέγγισης έχουν να κάνουν με το γεγονός ότι ένα μόνο NIDS μπορεί να παρακολουθεί ένα ευρύ υποδίκτυο, χωρίς να δημιουργεί επιβάρυνση στο σύστημα του δικτύου. Παρόλα αυτά, αν πρόκειται για δίκτυο με «μεγάλη» κίνηση η επεξεργασία και η εξέταση όλων των πακέτων αποτελεί μια σύνθετη διαδικασία.

Multiple hosts (Distributed agents)

Στην κατανεμημένη προσέγγιση του NIDS, το σύστημα έχει εγκατασταθεί σε όλους (ή σε μερικούς) κόμβους του δικτύου. Τα μηχανήματα αυτά παρακολουθούν την κίνηση που δρομολογείται μέσω των συγκεκριμένων κόμβων και παράγουν τα ανάλογα αποτελέσματα. Τα αποτελέσματα αυτά, στη συνέχεια, αποστέλλονται στον κεντρικό ελεγκτή του NIDS (σύστημα διαχείρισης του NIDS). Αυτό το σύστημα διαχείρισης συντονίζεται με τους υπεύθυνους κόμβους και παράγει συναγερμούς(alarms) για συγκεκριμένα πακέτα και τους μεταδίδει στο δίκτυο. Η προσέγγιση αυτή επιλύει το πρόβλημα της επεξεργασίας και εξέτασης μεγάλου όγκου πακέτων,

που αντιμετωπίζει η προηγούμενη προσέγγιση, ωστόσο είναι δυσχερέστερη η διαχείριση και ρύθμιση κάθε μεμονωμένου κόμβου.

2.6.4 Μηχανισμοί ανίχνευσης

Στο πλαίσιο των μηχανισμών ανίχνευσης μπορούν να γίνουν περισσότεροι του ενός είδους κατηγοριοποιήσεις όπως αυτές περιγράφονται στην συνέχεια.

Κατηγοριοποίηση συναρτήσει του τρόπου ανίχνευσης των επιθέσεων

Μηχανισμός ανίχνευσης υπογραφής (Signature based)

Στον μηχανισμό ανίχνευσης υπογραφής τα χαρακτηριστικά (μοτίβα) των επιθέσεων αποθηκεύονται σε βάση δεδομένων. Κάθε πακέτο της κίνησης του δικτύου συγκρίνεται με τα μοτίβα επιθέσεων για την ανίχνευση μη φυσιολογικής συμπεριφοράς. Τα σύστηματα που βασίζονται στην ανίχνευση επιθέσεων με υπογραφή ανιχνεύουν μόνο γνωστές επιθέσεις, δηλαδή επιθέσεις των οποίων τα χαρακτηριστικά έχουν καταγραφεί στο παρελθόν και έχουν καταχωρηθεί στην βάση δεδομένων των επιθέσεων.

Μηχανισμός ανίχνευσης ανωμαλιών (Anomaly based intrusion detection system)

Η λειτουργία μηχανισμού ανίχνευσης ανωμαλιών στηρίζεται στην συμπεριφορά του δικτύου. Πιο συγκεκριμένα, είναι αναγκαίο να οριστεί η φυσιολογική συμπεριφορά του δικτύου από το διαχειριστή. Καθορίζονται δηλαδή κανόνες φυσιολογικής και μη φυσιολογικής συμπεριφοράς. Η διαδικασία αυτή είναι ιδιαίτερα δύσκολη δεδομένου ότι η δραστηριότητα ενός δικτύου ή ενός συστήματος παρουσιάζει πολλές διακυμάνσεις και δεν είναι εύκολο να μοντελοποιηθεί. Ακόμη κακή ρύθμιση της φυσιολογικής για το δίκτυο συμπεριφοράς μπορεί να οδηγήσει σε έντονη εμφάνιση false positives.

Κατηγοριοποίηση συναρτήσει του χρόνου ανίχνευσης των επιθέσεων

Μηχανισμός ανίχνευσης σε πραγματικό χρόνο (Real Time detection)

Αυτά τα συστήματα ανίχνευσης παρείσφρησης λειτουργούν σε πραγματικό χρόνο δηλαδή συλλέγουν πακέτα από το δίκτυο (live) για την ανίχνευση μη φυσιολογικών δραστηριοτήτων. Η αποδοτικότητα των συστημάτων ανίχνευσης παρείσφρησης σε πραγματικό χρόνο εξαρτάται σε μεγάλο βαθμό από τον αριθμό των επιλεγμένων χαρακτηριστικών (features), δεδομένου ότι το σύστημα πρέπει να συγκρίνει αυτά τα χαρακτηριστικά με τα χαρακτηριστικά των εισερχόμενων πακέτων σε πολύ υψηλούς ρυθμούς. Επίσης, ο αριθμός των χαρακτηριστικών επίσης επηρεάζει την κατανάλωση των πόρων του συστήματος.

Μηχανισμός ανίχνευσης σε μεταγενέστερο χρόνο (Offline detection)

Τα συστήματα ανίχνευσης παρείσφρησης σε μεταγενέστερο χρόνο(offline συστήματα) λειτουργούν χωρίς να είναι συνδεδεμένα στο διαδίκτυο, δηλαδή αυτά τα συστήματα ανίχνευσης επεξεργάζονται αποθηκευμένα σύνολα δεδομένων(data sets) από επιθέσεις. Τα Offline συστήματα ανίχνευσης παρέχουν πληροφορίες σχετικά με την επίθεση και βοηθούν στην αποκατάσταση των ζημιών που προκλήθηκαν από την επίθεση. Αυτά τα συστήματα ανίχνευσης βοηθούν στην κατανόηση του μηχανισμού των επιθέσεων και αποσκοπούν στην μείωση των πιθανοτήτων για μελλοντικές επιθέσεις του ίδιου τύπου.

Κεφάλαιο 3: Προσέγγιση αντιμετώπισης επιθέσεων άρνησης υπηρεσίας

3.1 Εισαγωγή

Το κεφάλαιο αποτελεί το υπόβαθρο, πάνω στο οποίο θα στηριχθεί η επιλογή της μεθόδου της εντροπίας για την ανίχνευση επιθέσεων άρνησης υπηρεσίας. Στόχος είναι κατ' αρχήν η εξοικείωση του αναγνώστη με την έννοια της θεωρίας της πληροφορίας (Information Theory) και της ευρείας έννοιας της εντροπίας. Κατά δεύτερον λόγο, επιχειρείται η κατανόηση της εντροπίας όπως αυτή ορίζεται στα πληροφοριακά συστήματα και πώς αυτή η έννοια μπορεί να οδηγήσει σε επιτυχή ανίχνευση επιθέσεων άρνησης υπηρεσίας σε ένα δίκτυο.

Όπως έχει αναλυθεί στο προηγούμενο κεφάλαιο η ανίχνευσης DDoS επιθέσεων δέχεται κυρίως δύο προσεγγίσεις: Προσέγγιση Υπογραφής (Signature Based Approach -SBA), Προσέγγιση Ανωμαλιών (Anomaly Based Approach - ABA).

Στα συστήματα Προσέγγιση Υπογραφής (SBA), τα χαρακτηριστικά των επιθέσεων συγκρίνονται με μία βάση δεδομένων υπογραφών ή με χαρακτηριστικά από γνωστές κακόβουλες απειλές. Αυτός ο τρόπος είναι παρόμοιος με τον τρόπο ανίχνευσης κακόβουλου λογισμικού των περισσότερων antivirus. Το μειονέκτημα αυτής της μεθόδου είναι η καθυστέρηση μεταξύ μιας νέας απειλής που ανακαλύπτεται και της ενημέρωσης της αντίστοιχης βάσης δεδομένων για την υπογραφή της απειλής αυτής. Κατά τη διάρκεια αυτής της περιόδου, οι νέες απειλές θα είναι μη ανιχνεύσιμες. Η προσέγγιση SBA είναι αποτελεσματική, επειδή είναι εύκολο να εφαρμοστεί. Σύμφωνα με τους Ditcheva και Fowler [53], έχει αποδειχθεί ότι τα IDS που βασίζονται στην υπογραφή εντοπίζουν γνωστές επιθέσεις με χαμηλά ψευδώς αρνητικά (false negatives) αποτελέσματα. Αλλά η SBA περιορίζεται από το γεγονός της ενημέρωσης των βάσεων δεδομένων για νέες επιθέσεις με αποτέλεσμα να είναι αδύνατον να ανιχνευθούν επιθέσεις μηδενικής μέρας (zero day).

Η προσέγγιση που βασίζεται στην ανίχνευση ανωμαλιών (ABA) έχει προταθεί για να ξεπεραστούν οι περιορισμοί της SBA. Η μέθοδος αυτή χρησιμοποιεί προσεγγίσεις ανάλυσης της κατανομής (distribution analysis approaches), εξόρυξης δεδομένων (data mining) και στατιστικές προσεγγίσεις. Η ABA παρακολουθεί την κίνηση του δικτύου συγκρίνοντας την με κίνηση που θεωρείται «φυσιολογική» με τη βοήθεια επιλεγμένων δεικτών**.** Τα κριτήρια έχουν να κάνουν με το εύρος ζώνης που χρησιμοποιείται, τα πρωτόκολλα που χρησιμοποιούνται, τις θύρες και τις συσκευές που συνδέονται μεταξύ τους κ.α. Στόχος είναι να ειδοποιεί τον διαχειριστή δικτύου όταν η κυκλοφορία εντοπίζεται ως «ανώμαλη», δηλαδή σημαντικά διαφορετική από την «φυσιολογική» κρίνοντας στη βάση των επιλεγμένων δεικτών και κριτηρίων. Το μειονέκτημα της συγκεκριμένης μεθόδου είναι η αύξηση των ψευδών συναγερμών για «θετικά» αποτελέσματα.

Η προσέγγιση της παρούσας διπλωματικής εργασίας στην ανίχνευση επιθέσεων άρνησης υπηρεσιών στηρίζεται στην μέθοδο εφαρμογής της στατιστικομαθηματικής προσέγγισης της *εντροπίας*, όπως αυτή ορίστηκε από τον Shannon. Η θεμελιώδης υπόθεση εργασίας στην παρούσα διπλωματική είναι ότι η χρήση στατιστικών μεθόδων επιτρέπει την διάκριση μεταξύ της DDoS κίνησης και της νόμιμης κίνησης, όπου νόμιμη κίνηση ή φυσιολογική κίνηση θεωρείται κίνηση που δεν θέτει σε κίνδυνο την ασφάλεια ενός πληροφοριακού συστήματος. Η συγκεκριμένη προσέγγιση ανίχνευσης επιθέσεων με βάση την εντροπία αποφέρει σημαντικά οφέλη στην ανίχνευση επιθέσεων DDoS. Η εντροπία είναι μέτρο της αταξίας του υπό εξέταση συστήματος. Σε αυτή την βάση στηρίχθηκε η ανάπτυξη της μεθόδου που χρησιμοποιεί έναν αλγόριθμο της εντροπίας για τον προσδιορισμό αυτής της αταξίας σε ένα δίκτυο υπολογιστών. Στο σημείο αυτό

πρέπει να σημειωθεί σε μεθόδους ανίχνευσης που στηρίζονται στην εντροπία πρέπει να έχει οριστεί εκ των προτέρων ποια κίνηση θεωρείται «φυσιολογική» για το εν λόγο δίκτυο. Αυτό επιτυγχάνεται με την συνεχή παρακολούθηση του δικτύου. Ως αποτέλεσμα, προσδιορίζεται ένα εύρος τιμών της εντροπίας του συστήματος που χαρακτηρίζεται ως «φυσιολογικό» ή «ομαλό». Όταν το υπό παρακολούθηση δίκτυο λειτουργεί με «φυσιολογικό» τρόπο, οι τιμές της εντροπίας είναι σχετικά ομαλές, δηλαδή κυμαίνονται στο προηγουμένως ορισμένο εύρος τιμών. Σε αντίθετη περίπτωση, δηλαδή σε περίπτωση επίθεσης άρνησης υπηρεσίας, η τιμή εντροπίας ενός ή περισσότερων χαρακτηριστικών (features) θα μεταβληθεί σημαντικά. Η χρήση του μέτρου της εντροπίας μπορεί να αυξήσει την ευαισθησία της ανίχνευσης για ανίχνευση ανώμαλων περιστατικών. Παρόλο που η εφαρμογή της εντροπίας έχει αρκετά πλεονεκτήματα, ο υπολογισμός της σε πραγματικό χρόνο σε ένα δίκτυο υψηλής ταχύτητας είναι απαιτητικός σε επεξεργασία και μνήμη.

Προτού γίνει περαιτέρω αναφορά στις στατιστικές μεθόδους που θα εφαρμοστούν, θα γίνει μια αναφορά στην θεωρία πίσω από τις μεθόδους αυτές, δηλαδή την θεωρία πληροφορίας.

3.2 Η θεωρία πληροφορίας στην ανίχνευση ανωμαλιών

Η χρήση της θεωρίας πληροφορίας για ανίχνευση ανωμαλιών περιγράφεται στο έργο των Lee και Xiang [38]**,** όπου διερεύνησε τη χρήση των διαφόρων μέτρων της θεωρίας της πληροφορίας όπως η εντροπία, η υπό συνθήκη εντροπία, η σχετικής υπό συνθήκη εντροπία, το κέρδος πληροφορίας και το πληροφοριακό κόστος ανίχνευσης ανωμαλιών. Οι Lee και Xiang καθόρισαν το πώς αυτά τα μεγέθη μπορούν να χρησιμοποιηθούν στην ανίχνευση ανωμαλιών και στη συνέχεια να εφαρμοστούν σε διαφορετικά σύνολα δεδομένων (datasets). Κάθε ένα από αυτά τα μεγέθη, εκτός από το πληροφοριακό κόστος, αναλύεται σε αυτό το κεφάλαιο.. Αυτό αφορά την ταχύτητα του μοντέλου όταν απαιτείται ανάλυση σε πραγματικό χρόνο και είναι εκτός του πεδίου εφαρμογής της παρούσας έρευνας.

Η πρώτη μέθοδος ανίχνευσης ανωμαλίας βασισμένη στην θεωρία της πληροφορίας που περιεγράφηκε είναι η εντροπία. Η εντροπία μπορεί να χρησιμοποιηθεί ως μέτρο κανονικότητας των εξεταζόμενων δεδομένων. Ο τύπος υπολογισμού της είναι:

$$H = -\sum_{x \in X} p(x) \log \mathrm{p}(x) \qquad (1)$$

όπου *log* είναι ο λογάριθμος με βάση το 2 και $p(x)$ είναι η πιθανότητα εμφάνισης του ενδεχομένου x, το οποίο στην περίπτωση της εφαρμογής της εντροπίας στην ανίχνευση επιθέσεων δικτύου αντιστοιχεί σε κάποιο από τα πεδία της επικεφαλίδας των πακέτων όπως διεύθυνση πηγής, διεύθυνση προορισμού. Μια άλλη μέθοδος είναι η χρήση της υπό συνθήκης εντροπίας. Η υπό συνθήκη εντροπία περιγράφει το ποσοστό της αβεβαιότητας που απομένει όταν έχει παρατηρηθεί ένα γεγονός, όπως ένα υποσύνολο των εξεταζόμενων γεγονότων. Οι Lee και Xiang δηλώνουν ότι υπό συνθήκη εντροπία είναι χρήσιμη «ως μέτρο της κανονικότητας διαδοχικών εξαρτήσεων ... [και] όσο μικρότερη είναι η υπό συνθήκη εντροπία, τόσο το καλύτερο. Ωστόσο, συστήματα με υψηλότερη υπό συνθήκη εντροπία είναι πιο δύσκολο να μοντελοποιηθούν.

Ακόμη, αναφέρθηκαν στο πώς η σχετική εντροπία μπορεί να χρησιμοποιηθεί στην σύγκριση δύο κατανομών από την ίδια λίστα γεγονότων. Όταν η υπό συνθήκη εντροπία

χρησιμοποιείται σε ένα σύνολο δεδομένων, η σχετική υπό συνθήκη εντροπία υπολογίζει την απόσταση μεταξύ δύο συνόλων δεδομένων. Συνεπώς, ανωμαλίες είναι εφικτό να ανιχνευθούν εάν η εντροπία του συστήματος συγκρίνεται ανά μικρά χρονικά διαστήματα όπως μέρα με τη μέρα (ή άλλη χρονική περίοδο) με βάση την εντροπία της προηγούμενης ημέρας. Αυτό αποτελεί έναν τρόπο ανίχνευσης ενδεχόμενων αλλαγών στο σύστημα λόγω μιας επίθεσης (ή άλλη ανώμαλη εκδήλωση). Ο αλγόριθμος που υλοποιήθηκε αξιοποιεί αυτή την παρατήρηση με την διαφορά ότι συγκρίνει τις τιμές της εντροπίας με την άφιξη κάθε νέου πακέτου και όχι με βάση διαφορετικές χρονικές περιόδους.

3.3 Η εντροπία στην ανίχνευση ανωμαλιών

Έρευνες δείχνουν ότι στατιστικές μετρήσεις και επεξεργασία των αποτελεσμάτων τους οδηγούν σε αποτελεσματικές προσεγγίσεις αντιμετώπισης επιθέσεων DDOS. Μία από αυτές τις τεχνικές είναι η εντροπία του Shannon, η οποία έχει χρησιμοποιηθεί για την ανίχνευση παρεισφρήσεων. Οι Nychis, Sekar, Andersen, Kim και Zhang [7] ανέλυσαν διαφορετικές τεχνικές που χρησιμοποιούν δείκτες από τη θεωρία της πληροφορίας για την ανίχνευση ανωμαλιών στην κίνηση δικτύου υπολογιστών. Δήλωσαν οτι: «Οι βασισμένες στην εντροπία προσεγγίσεις για την ανίχνευση ανωμαλιών παρουσιάζουν ιδιαίτερο ενδιαφέρον, δεδομένου ότι παρέχουν πιο λεπτομερή στοιχεία από την παραδοσιακή ανάλυση του όγκου της κίνησης» (Nychis, Sekar, Andersen, Kim, & Zhang, 2008).

Η εντροπία συγκεκριμένα προσφέρει το πλεονέκτημα ότι συλλαμβάνει σε μία μόνο τιμή τις αλλαγές στα χαρακτηριστικά της κίνησης δικτύου, και παρατηρώντας τις τιμές της σε πολλαπλά χαρακτηριστικά (features) αποκαλύπτει πιθανή κίνηση ασυνήθιστης συμπεριφοράς. Έχει αποδειχτεί ότι εξετάζοντας χαρακτηριστικά κίνησης, όπως αυτά συλλαμβάνονται από την εντροπία, είναι ένας αποτελεσματικός τρόπος για την ανίχνευση ενός ευρύ φάσματος σημαντικών ανωμαλιών καθώς και επιθέσεων DDOS. Σε αυτή την παρατήρηση στηρίζεται η προσέγγιση της παρούσας έρευνας για την ανίχνευση επιθέσεων DDOS με την εντροπία.

Η εντροπία είναι ένα μέγεθος που επηρεάζεται από διάφορους παράγοντες. Ο προσδιορισμών μερικών από αυτούς είναι καθοριστικής σημασίας για την έρευνα που πραγματοποιήθηκε. Πιο συγκεκριμένα, έστω ένα δείγμα πακέτων κίνησης ενός δικτύου, το εύρος τιμών που παίρνει η εντροπία εξαρτάται από το N, που είναι ο αριθμός των διακριτών τιμών που παρατηρείται στο δείγμα των πακέτων της κίνησης. Στην πράξη, αυτό σημαίνει ότι τιμή της εντροπίας τείνει να αυξηθεί όταν το δείγμα αυξάνεται, δηλαδή, όταν ο όγκος της κίνησης αυξάνεται [35]. Αυτό έχει μια σειρά από συνέπειες για την προσέγγισή μας. Κατά τη διαδικασία ανίχνευσης, αυτό σημαίνει ότι ανωμαλίες που τυχόν υπάρχουν σε μεγάλο όγκο κίνησης, θα εμφανίσουν ασυνήθιστες τιμές για την εντροπία [54]. Έτσι ορισμένες ανωμαλίες ανιχνεύονται με βάση τις αλλαγές της τιμής της εντροπίας.

Η μέθοδος εντοπισμού ανωμαλιών στην παρούσα εργασία αξιοποιεί αυτές τις παρατηρήσεις σχετικά με την εντροπία για την ανίχνευση των επιθέσεων DDOS.

Ακόμη, οι Laura Feinstein και Dan Schnackenberg [54] παρατήρησαν μέσα από πειράματα ότι όσο ένα δίκτυο δεν δέχεται επίθεση οι τιμές της εντροπίας για διάφορα πεδία της κεφαλίδας των πακέτων περιορίζονται σε ένα περιορισμένο εύρος τιμών μικρής διακύμανσης. Αντίθετα, όταν το δίκτυο δέχεται επίθεση, οι τιμές αυτές της εντροπίας υπερβαίνουν αυτό το εύρος με ανιχνεύσιμο τρόπο.

Το κεφάλαιο αυτό περιέγραψε πώς εφαρμόζονται έννοιες της θεωρίας πληροφορίας στην ανίχνευση ανωμαλιών. Στο κεφάλαιο 4 περιγράφεται η μέθοδος υλοποίησης της συγκεκριμένης προσέγγισης.

Κεφάλαιο 4: Πείραμα / Αποτελέσματα

4.1 Εισαγωγή

Στο κεφάλαιο αυτό προσδιορίζεται ο αλγόριθμος της εντροπίας που θα χρησιμοποιηθεί, με την χρήση κατάλληλων παραμέτρων από τις επικεφαλίδες των μεταδιδόμενων πακέτων σε ένα δίκτυο, ώστε να απαντήσει στα ερωτήματα που εξετάζει η έρευνα. Τα δεδομένα που χρησιμοποιούνται στο πείραμα αντλήθηκαν, επισημαίνοντας ότι επειδή δεν είναι δυνατή η προσομοίωση μιας τέτοιας επίθεσης σε ένα υπαρκτό δίκτυο, από διαδικτυακές βάσεις δεδομένων, οι οποίες εξυπηρετούν αυτόν τον σκοπό. Εξετάζονται τρία σενάρια επιθέσεων υλοποιημένα από διαφορετικό πλήθος επιτιθέμενων bots και διαφορετικών μεθόδων επίθεσης. Το ερώτημα το οποίο εξετάζει η συγκεκριμένη έρευνα είναι σε πρώτο στάδιο εάν η εντροπία με το μοντέλο το οποίο θα εφαρμόσουμε μπορεί να ανιχνεύσει τις επιθέσεις άρνησης υπηρεσιών και εν συνεχεία με ποιους τρόπους μπορεί να επιτευχθεί πιο ακριβής ανίχνευση. Ακολουθεί αναλυτική περιγραφή του τρόπου λειτουργίας του αλγορίθμου που χρησιμοποιήθηκε και παρουσίαση των αποτελεσμάτων του για τις διάφορες μεθόδους και τα διάφορα δεδομένα που χρησιμοποιήθηκαν.

4.2 Αλγόριθμος Εντροπίας

Ο αλγόριθμος της εντροπίας που χρησιμοποιήθηκε στα πλαίσια της διπλωματικής αυτής εργασίας χρησιμοποιεί στατιστικά στοιχεία, από συγκεκριμένα πεδία στις επικεφαλίδες των πακέτων που εξετάζει, για να μοντελοποιήσει την κατανομή των πακέτων αυτών, όπως διεύθυνση πηγής (source IP),διεύθυνση προορισμού (destination IP) και τέλος την κατανομή μεγέθους ροών(FSD-flow size distribution).

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, έστω n ανεξάρτητα σύμβολα το καθένα με πιθανότητα επιλογής p_i. Τότε η εντροπία H ορίζεται ως:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \qquad (2)$$

Από τον τύπο αυτό συνεπώς συμπεραίνουμε ότι η εντροπία μπορεί να υπολογιστεί σε ένα δείγμα συνεχόμενων πακέτων. Συγκρίνοντας την τιμή της εντροπίας για ένα δείγμα με την τιμή της για ένα άλλο δείγμα της ίδιας καταγραφής έχουμε έναν μηχανισμό ανίχνευσης αλλαγών στην ομοιομορφία της κατανομής. Όταν ένα δίκτυο δεν δέχεται κάποια επίθεση δηλαδή όταν καταγράφεται μόνο ομαλή κίνηση οι τιμές της εντροπίας για διάφορα πεδία των επικεφαλίδων των πακέτων εμφανίζουν ένα περιορισμένο εύρος διακύμανσης. Ωστόσο όταν ένα δίκτυο δέχεται επίθεση οι τιμές αυτές ξεπερνούν αυτό το εύρος σε βαθμό που κάνει αυτές τις μεταβολές ανιχνεύσιμες [54]. Στο πρώτο μέρος του πειράματος επιδιώχθηκε να επαληθευτεί αυτή η υπόθεση.

Στα πλαίσια της εφαρμογής του αλγορίθμου αυτού, η εντροπία θα υπολογιστεί για την διεύθυνση πηγής με την χρήση ενός κυλιόμενου παραθύρου σταθερού εύρους πακέτων W. Η πιθανότητα p_i στον αλγόριθμο είναι η συχνότητα εμφάνισης κάθε μοναδικού συμβόλου διαιρεμένο με το συνολικό αριθμό συμβόλων του δείγματος. Η διαδικασία υπολογισμού της εντροπίας είναι η εξής:

1. Υπολογισμός της εντροπίας των *W* πρώτων πακέτων σχετικά με μια συγκεκριμένη παράμετρο της επικεφαλίδας των πακέτων, στην περίπτωση μας της διεύθυνσης πηγής.
2. Απομόνωση του όρου του αθροίσματος που αναφέρεται στην πιθανότητα του πρώτου συμβόλου του παραθύρου (αυτό το σύμβολο είναι το *i=1*) καθώς επίσης και την τιμή της αντίστοιχης πιθανότητας p_{i-1}.
3. Μετακίνηση του παραθύρου ώστε ο νέος πρώτος όρος να είναι ο προηγουμένως δεύτερος όρος και οι επόμενοι *W-1* διαδοχικοί όροι να περιέχονται στο παράθυρο.
4. Απομόνωση του όρου του αθροίσματος που αναφέρεται στην πιθανότητα του συμβόλου που εισήχθη από την μετακίνηση του παραθύρου.
5. Αφαίρεση των όρων που απομονώθηκαν στα βήματα 2 και 4 από την τιμή που υπολογίστηκε στο βήμα 1.
6. Επανυπολογισμός των πιθανοτήτων που επηρεάστηκαν στο τωρινό παράθυρο δεδομένων. Δηλαδή, επανυπολογισμός του και της πιθανότητας του συμβόλου που προστέθηκε από την μετακίνηση του παραθύρου.
7. Χρησιμοποιώντας τις τιμές που υπολογίστηκαν στο βήμα 6 προστίθενται οι δύο όροι που λείπουν από το άθροισμα της εντροπίας και συγκρίνεται η τιμή της νέας εντροπίας με την εντροπία που είχε υπολογιστεί προηγουμένως.
8. Επαναλαμβάνονται τα βήματα 2-7 για τον υπολογισμό διαδοχικών τιμών της εντροπίας.

Το μέγεθος του παραθύρου *W* είναι μια μεταβλητή που ελέγχει την εξομάλυνση των βραχυπρόθεσμων διακυμάνσεων της ανίχνευσης. Αύξηση του μεγέθους παραθύρου μειώνει τις μεταβολές στην εντροπίας και μπορεί να αυξήσει την πιθανότητα των false-positives που οφείλονται σε σύντομες και πιθανά ασήμαντες ανωμαλίες. Ωστόσο, το παράθυρο θα πρέπει να είναι αρκετά μικρό ώστε οι επιθέσεις να εντοπίζονται γρήγορα. Τίθεται λοιπόν το θέμα του μεγέθους του συγκεκριμένου παραθύρου. Σύμφωνα με σχετικές έρευνες [54], για δεδομένα πλήθους 1.000.000 επιλέγεται παράθυρο 10.000 πακέτων.

Στο πρώτο μέρος του πειράματος, εφαρμόζεται το μοντέλο της εντροπίας σε καταγεγραμμένη κίνηση δικτύου με διαφορετικές παραμετροποιήσεις. Στην συνέχεια, γίνεται μια προσπάθεια προσδιορισμού ενός κατωφλίου το οποίο θα διαχωρίζει την ομαλή από την ανώμαλη κίνηση και τέλος μια σύγκριση των εφαρμοσμένων παραμετροποιήσεων για τον προσδιορισμό τις βέλτιστης εκ αυτών. Ακολουθεί λεπτομερής αναφορά στα δεδομένα που χρησιμοποιήθηκαν (datasets), ο κώδικας και η διαδικασία που ακολουθήθηκε για να υλοποιηθεί η επεξεργασία των datasets καθώς και το λογισμικό το οποίο χρησιμοποιήθηκε για την υλοποίηση του πειράματος.

4.3 Δεδομένα (datasets)

Στα πλαίσια της συγκεκριμένης διπλωματικής δεν ήταν δυνατή η αναπαραγωγή/ προσομοίωση δεδομένων κίνησης που να περιέχουν μολυσμένη και φυσιολογική κίνηση. Ως εναλλακτικός τρόπος υλοποίησης των πειραμάτων χρησιμοποιήθηκαν δεδομένα κίνησης από διαθέσιμες βάσεις δεδομένων που περιείχαν τα επιθυμητά είδη κίνησης, δηλαδή διάφορα είδη κίνησης DDOS.

Η βάση δεδομένων που χρησιμοποιήθηκε για την μολυσμένη κίνηση του πρώτου μέρους του πειράματος είναι από το Malware Capture Facility Project που δημιουργήθηκε στο CTU University το 2013 από το διδακτορικό φοιτητή Sebastián García και τον μεταπτυχιακό φοιτητή Vojtech Uhlir. Από την συγκεκριμένη βάση δεδομένων χρησιμοποιήθηκαν τρία διαφορετικά σενάρια για να εξακριβωθεί η σωστή λειτουργία ανίχνευσης του αλγορίθμου της εντροπίας. Τα τρία αυτά σενάρια αποτελούνται από UDP και ICMP επιθέσεις διαφορετικού μεγέθους botnet σε κάθε περίπτωση. Κάθε ένα από τα σενάρια ήταν καταγεγραμμένα σε pcap αρχεία που περιείχαν την μολυσμένη κίνηση. Η σχέση μεταξύ της διάρκειας, του πλήθους των πακέτων, το πλήθος των ροών πακέτων και το μέγεθος των αρχείων των αρχικών σεναρίων φαίνονται στον ακόλουθο πίνακα

Id	Διάρκεια(ώρες)	#Πακέτα	#Ροές πακέτων	#Μέγεθος	Είδος DDOS επίθεσης	Bot	#Bots
1	4.21	62.089.135	1.121.077	53GB	UDP και ICMP	Rbot	1
2	0.21	6.337.202	107.252	5.2GB	ICMP	Rbot	3
3	4.75	90.389.782	1.309.792	73GB	UDP	Rbot	10

Πίνακας 1. Σενάρια Επιθέσεων

4.3.1 Επεξεργασία δεδομένων

Τα δεδομένα αυτά περιείχαν ολόκληρα πακέτα Ethernet. Για την υλοποίηση των πειραμάτων χρειάστηκε να εξάγουμε κάποια πεδία από την επικεφαλίδα των πακέτων: timestamp, source IP address, destination IP address, source port number, destination port number και το πλήθος των bytes στο εκάστοτε πακέτο.

Λόγω του μεγάλου όγκου των δεδομένων, από το πρώτο dataset χρησιμοποιήθηκαν 40.000 πακέτα ενώ από τα υπόλοιπα δύο από 300.000 πακέτα μολυσμένης κίνησης. Η επιλογή έγινε με έναν αλγόριθμο τυχαίας επιλογής. Τα δεδομένα που προέκυψαν χρησιμοποιήθηκαν στα σενάρια που θα περιγράφουν στην συνέχεια.

Έχοντας συλλέξει τα δείγματα, τόσο της ομαλής όσο και της ανώμαλης κίνησης ξεχωριστά, το επόμενο βήμα ήταν η συγχώνευση της ομαλής με την ανώμαλη κίνηση σε κλίμακα 7:3 αντίστοιχα. Τα δεδομένα αυτά αποθηκεύτηκαν σε ένα txt αρχείο με χρήση του προγράμματος παρακολούθησης κίνησης δικτύου Wireshark και στην συνέχεια με την χρήση ενός αλγορίθμου υλοποιημένου στην γλώσσα προγραμματισμού C# αποθηκεύτηκαν σε μια βάση δεδομένων (Microsoft SQL Server 2014) για ευκολότερη πρόσβαση και καλύτερη επεξεργασία.

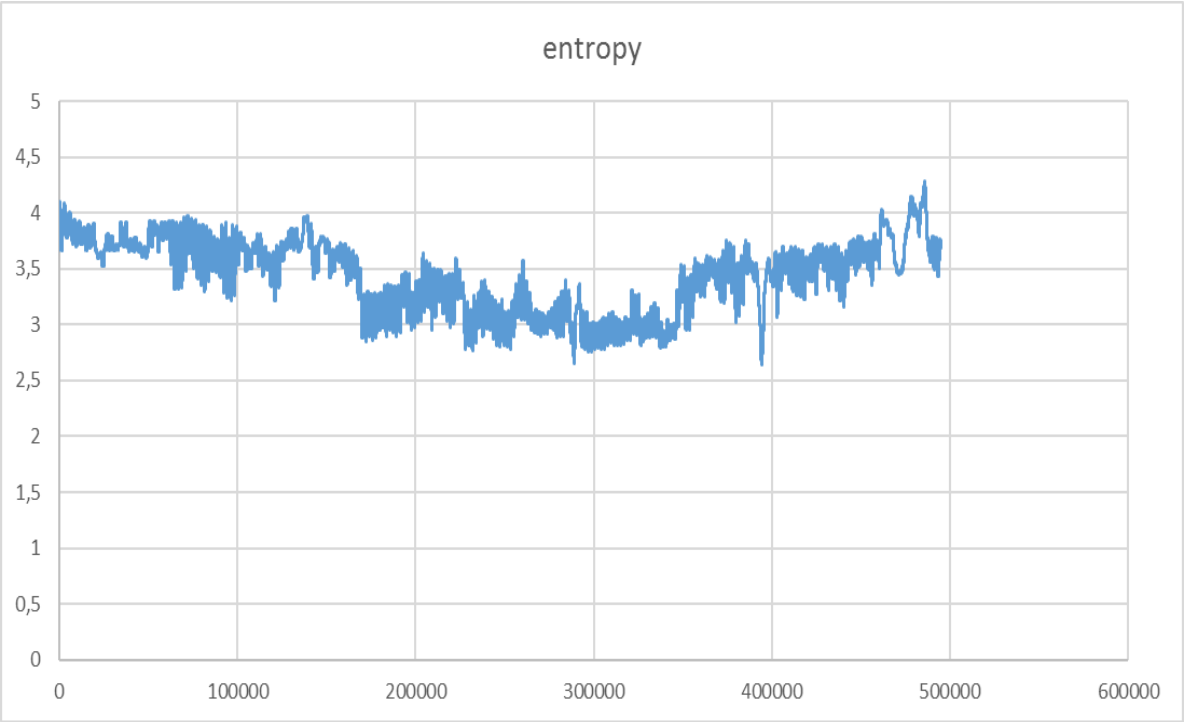
4.4 Πρώτο μέρος πειράματος-Εκτέλεση των σεναρίων

Στα πλαίσια του πρώτου μέρους του πειράματος, χρησιμοποιήσαμε έτοιμη καταγραφή ομαλής και ανώμαλης κίνησης (DDOS attack), από την επιστημονική κοινότητα, τις οποίες συγχωνεύσαμε. Υλοποιήθηκαν τρία διαφορετικά σενάρια όπως αυτά φαίνονται στον προηγούμενο Πίνακας 1. Σενάρια Επιθέσεων. Η ομαλή κίνηση αποτελούταν από καταγραφή 1.000.000 πακέτων. Η ανώμαλη κίνηση προερχόταν από Rbot, το rbot είναι ένα ισχυρό bot IRC γραμμένο σε Ruby, με πακέτα UDP και ICMP καταγεγραμμένης κίνησης εκ των οποίων για το πείραμα μας χρησιμοποιήθηκε ένα τυχαίο δείγμα 200.000-300.000 πακέτων. Συνεπώς, το αρχείο που εξετάσαμε στα πλαίσια αυτού του σταδίου του πειράματος αποτελούταν από περίπου 1.300.000 πακέτα. Η συγχώνευση των κινήσεων πραγματοποιήθηκε με το εργαλείο Wireshark τοποθετώντας την μολυσμένη κίνηση σε ένα συγκεκριμένο εύρος περίπου στις 800.000-1.000.000.

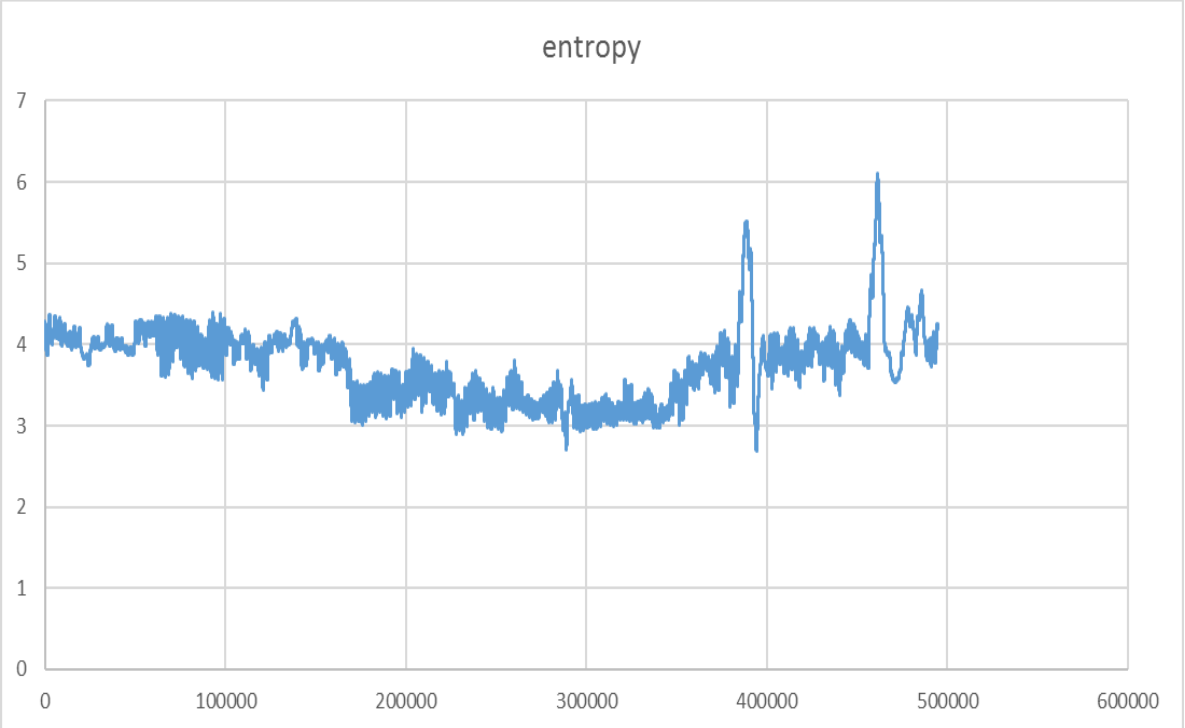
Η μέθοδος της εντροπίας εφαρμόστηκε τόσο στα δείγματα που είχαν μονο ομαλή κίνηση όσο και στα δείγματα που είχαν συγχωνευμένη ομαλή με ανώμαλη κίνηση. Ο λόγος εφαρμογής της μεθόδου στο δείγμα ομαλής κίνησης είναι ο προσδιορισμός ενός εύρους τιμών της εντροπίας για τις οποίες έχουμε «φυσιολογική» κίνηση. Για την ανίχνευση της «ανώμαλης» κίνησης είναι απαραίτητος ο προσδιορισμός του τι δεχόμαστε ως φυσιολογικό. Στην συνέχεια αφού έχει προσδιοριστεί το φυσιολογικό είναι δυνατός ο προσδιορισμός της μη φυσιολογικής ή «ανώμαλης» κίνησης. Στην συνέχεια εφαρμόστηκε η μέθοδος στα διάφορα dataset που δημιουργήθηκαν για την παρούσα έρευνα.

4.4.1.Διαγράμματα Ομαλής Κίνησης

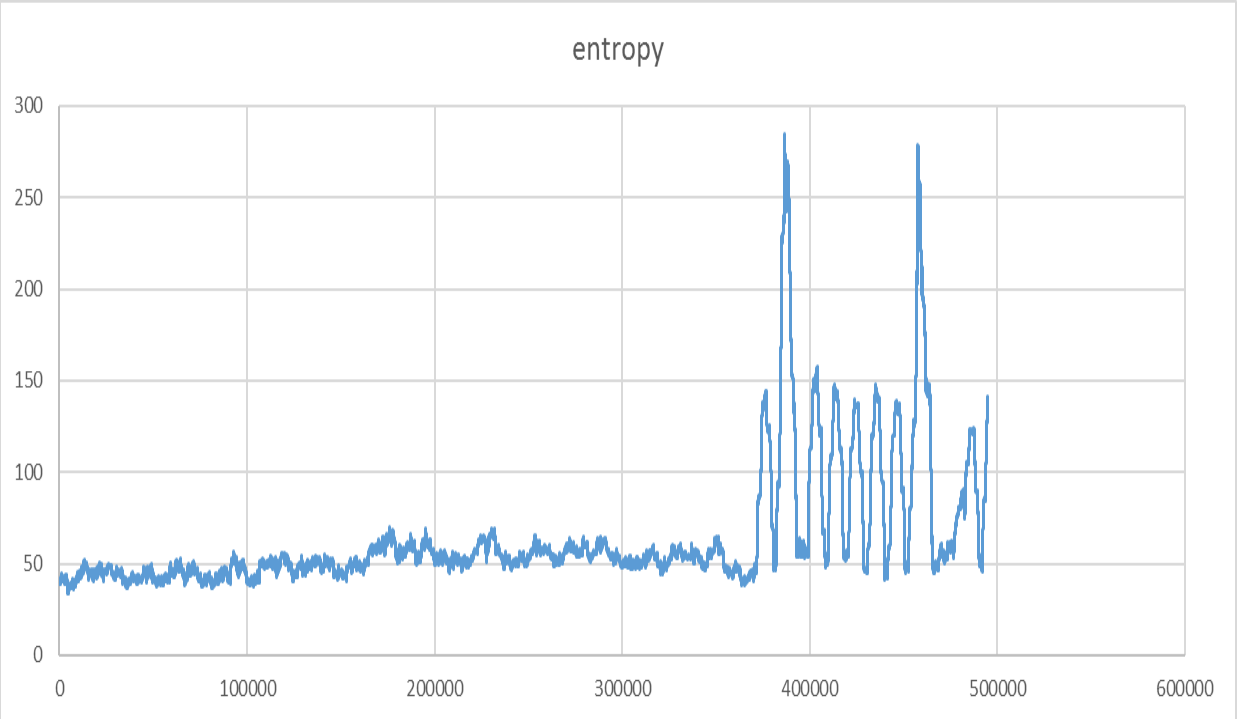
Στις περιπτώσεις των διευθύνσεων πηγής και προορισμού η εντροπία υπολογίζεται με τον παραπάνω αλγόριθμο. Το κάθε σύμβολο *p(x)* αντιστοιχεί στην πιθανότητα εμφάνισης της διεύθυνσης *x* στο υπό εξέταση παράθυρο. Στην περίπτωση του FSD, δηλαδή της κατανομής μεγέθους ροών, το σύμβολο *p(x)* αντιπροσωπεύει την πιθανότητα εμφάνισης του x, όπου x είναι το πλήθος εμφάνισης του ίδιου μεγέθους ροών. Ακολουθούν τα διαγράμματα εντροπίας για την καταγραφή ομαλής κίνησης με βάση τις κατανομές ως προς source IP, destination IP και FSD. Στον άξονα των x είναι οι χρονικές στιγμές, όπου σαν χρονική στιγμή δεχόμαστε την παραδοχή ότι είναι η άφιξη κάθε πακέτου και στον άξονα των y οι τιμές της εντροπίας. Για να γίνει πιο εύκολη η επεξεργασία των δεδομένων και ο σχεδιασμός των διαγραμμάτων χρησιμοποιήθηκε κλίμακα 2:1 για τα διαγράμματα που θα ακολουθήσουν



Διάγραμμα 1.Normal Traffic Source IP Entropy



Διάγραμμα 2. Normal Traffic Destination IP Entropy



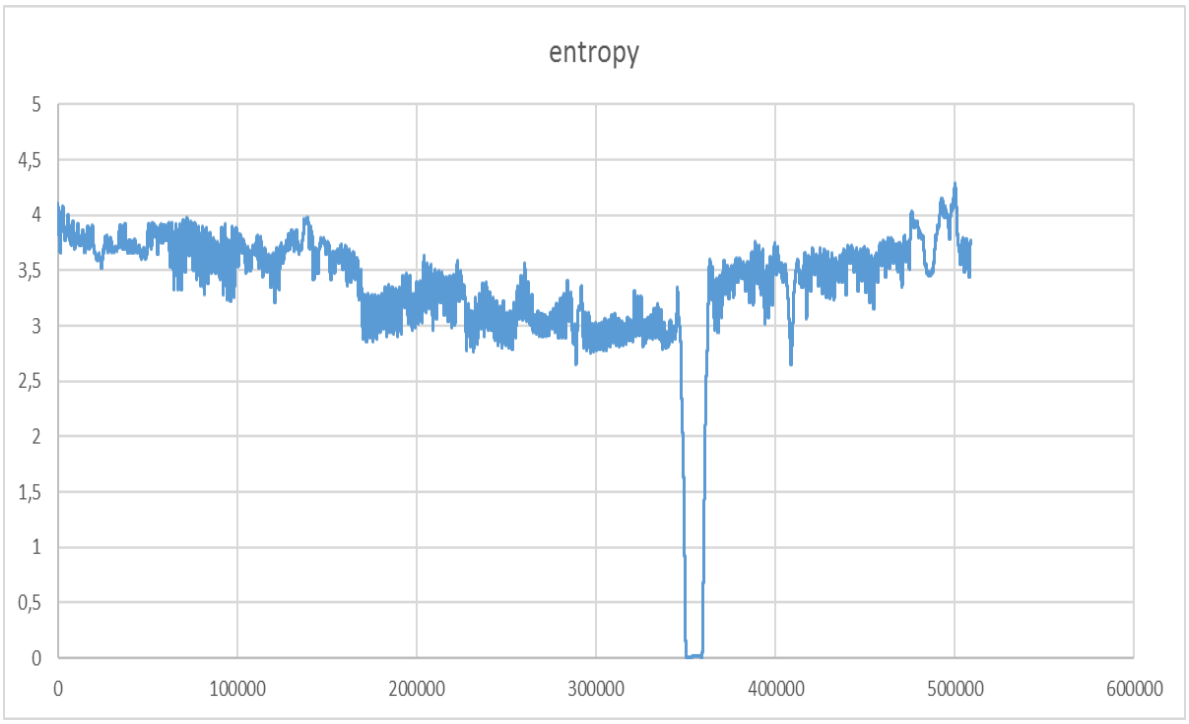
Διάγραμμα 3. Normal Traffic FSD Entropy

Τα διαγράμματα 1-3 αποτελούν τα αποτελέσματα της εφαρμογής της εντροπίας στο dataset ομαλής κίνησης για διαφορετικές παραμέτρους, διεύθυνση πηγής, διεύθυνση προορισμού και κατανομής μεγέθους ροής (FSD) αντίστοιχα. Στο διάγραμμα της διεύθυνσης πηγής δεν παρουσιάζεται έντονη διακύμανση των τιμών της εντροπίας οπότε την θεωρούμε σαν βάση για τον προσδιορισμό της ανώμαλης κίνησης. Ομοίως και για τα αλλά δύο διαγράμματα. Στο σημείο αυτό πρέπει να δοθούν περαιτέρω διευκρινήσεις ως προς τις διακυμάνσεις που εντοπίζονται στα άλλα δύο διαγράμματα. Στο διάγραμμα της εντροπίας με βάση την διεύθυνση προορισμού παρατηρούμε μερικές έντονες διακυμάνσεις στις τιμές της εντροπίας όπως και στο διάγραμμα FSD, στο οποίο είναι αρκετές περισσότερες. Οι διακυμάνσεις στο διάγραμμα της διεύθυνσης προορισμού οφείλονται στο γεγονός ότι σε εκείνο το παράθυρο (διάστημα) που εμφανίζεται η αύξηση της τιμής της εντροπίας υπάρχει μεγάλο πλήθος πακέτων που αποτελούνται από διακριτές/διαφορετικές διευθύνσεις προορισμού. Αυτό σημαίνει δηλαδή ότι όσο πιο μεγάλή είναι η εντροπία, τόσο πιο τυχαία/μη προβλέψιμη είναι η μεταβλητή, όπου ως μεταβλητή στην συγκεκριμένη περίπτωση έχουν την πιθανότητα εμφάνισης μίας διεύθυνσης προορισμού. Πρέπει επίσης να αναφερθεί ότι οι επιθέσεις που εξετάζουμε, δηλαδή οι επιθέσεις άρνησης υπηρεσίας, λειτουργούν με τον ακόλουθο τρόπο: πολλά bots επιτίθονται σε έναν ή μερικούς στόχους. Οπότε αν επρόκειτο για επίθεση η διεύθυνση προορισμού του στόχου θα εμφανιζόταν συχνά μέσα στο υπό εξέταση παράθυρο και συνεπώς η τιμή της εν λόγω εντροπίας δεν θα αυξανόταν αλλά θα μειωνόταν. Ομοίως και για την περίπτωση του FSD. Στην συνέχεια ακολουθούν τα διαγράμματα για κάθε ένα από τα τρία σενάρια.

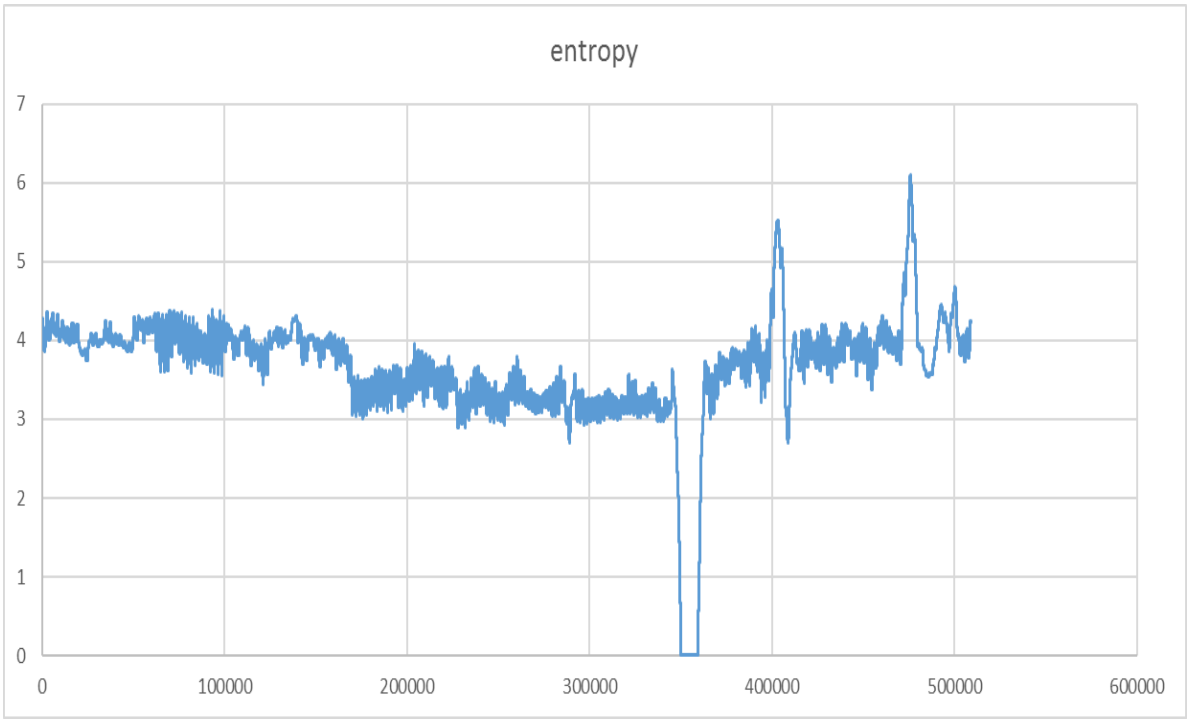
4.4.2.Διαγράμματα Κίνησης Σενάριο 1(Κίνηση από 1 bot)

Στα datasets που χρησιμοποιήθηκαν για τα σενάρια που θα ακολουθήσουν, η ανώμαλη εισάχθηκε μετά τα πρώτα 700.000 πακέτα ομαλής κίνησης. Όπως φαίνεται στα ακόλουθα διαγράμματα οι τιμές της εντροπίας άρχισαν να μειώνονται σημαντικά μέχρι που μηδενίστηκαν

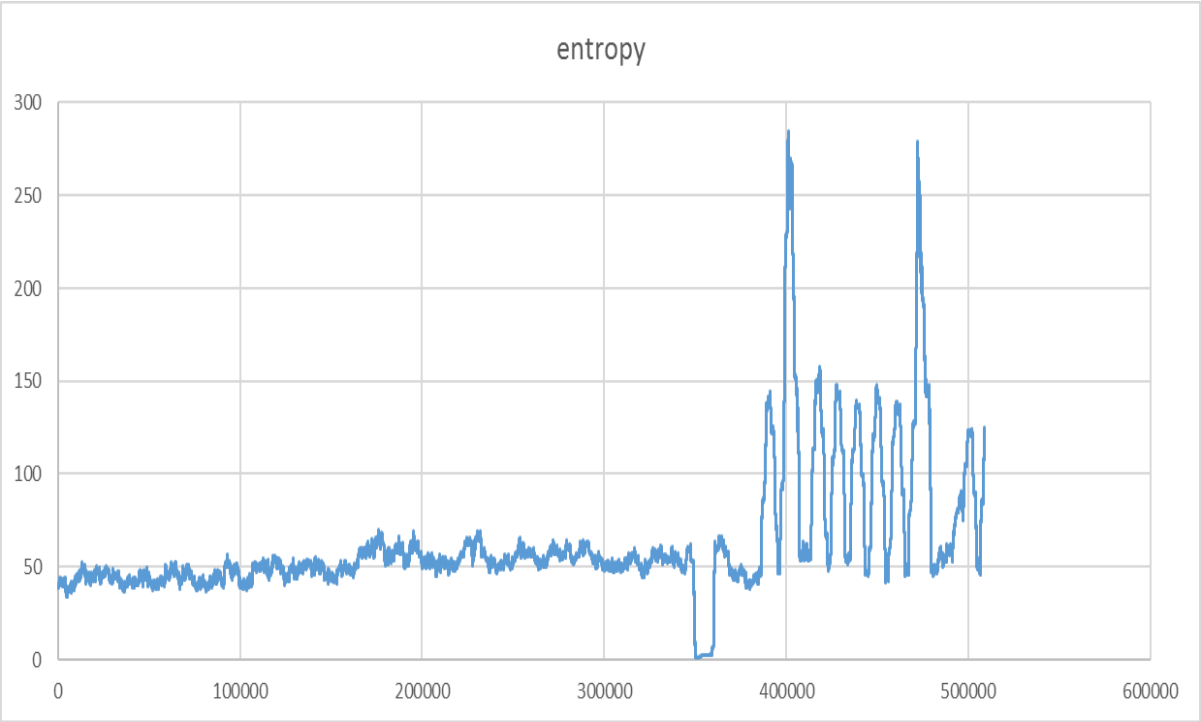
κατά την διάρκεια της επίθεσης. Στην συνέχεια, αφού ολοκληρώθηκε η επίθεση οι τιμές της εντροπίας αυξήθηκαν και έφτασαν σε ένα εύρος τιμών που μπορεί να θεωρηθεί φυσιολογικό.



Διάγραμμα 4. Senario 1-Source IP Entropy



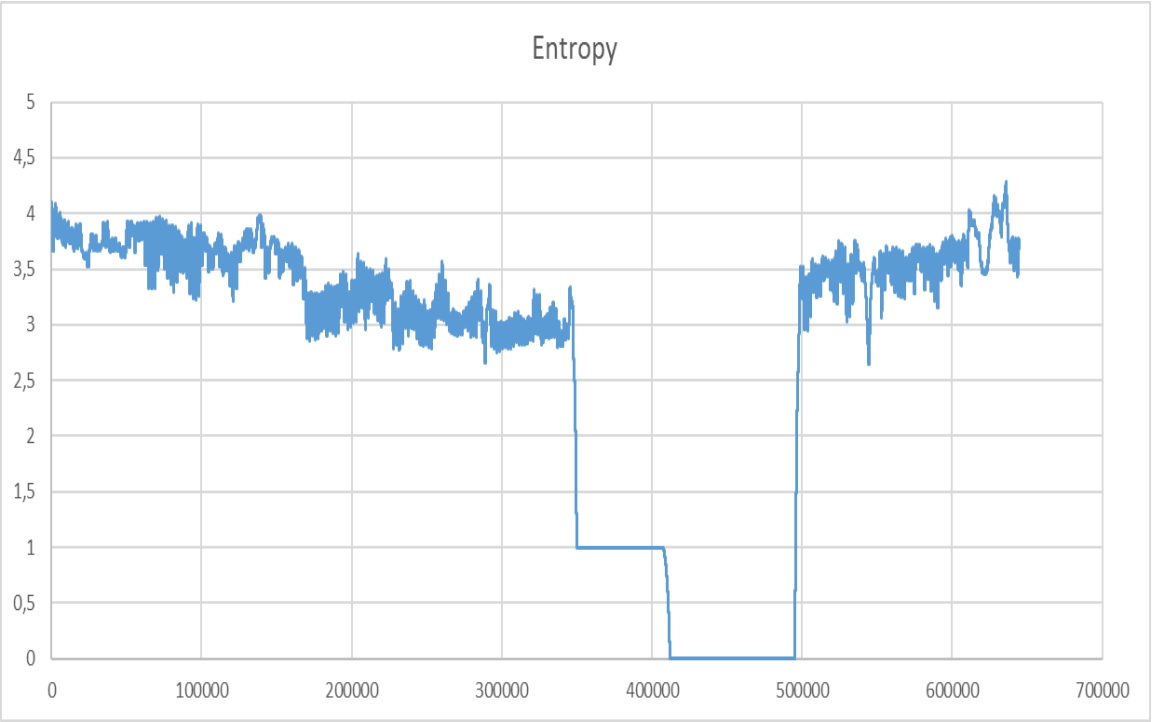
Διάγραμμα 5. Senario 1-Destination IP Entropy



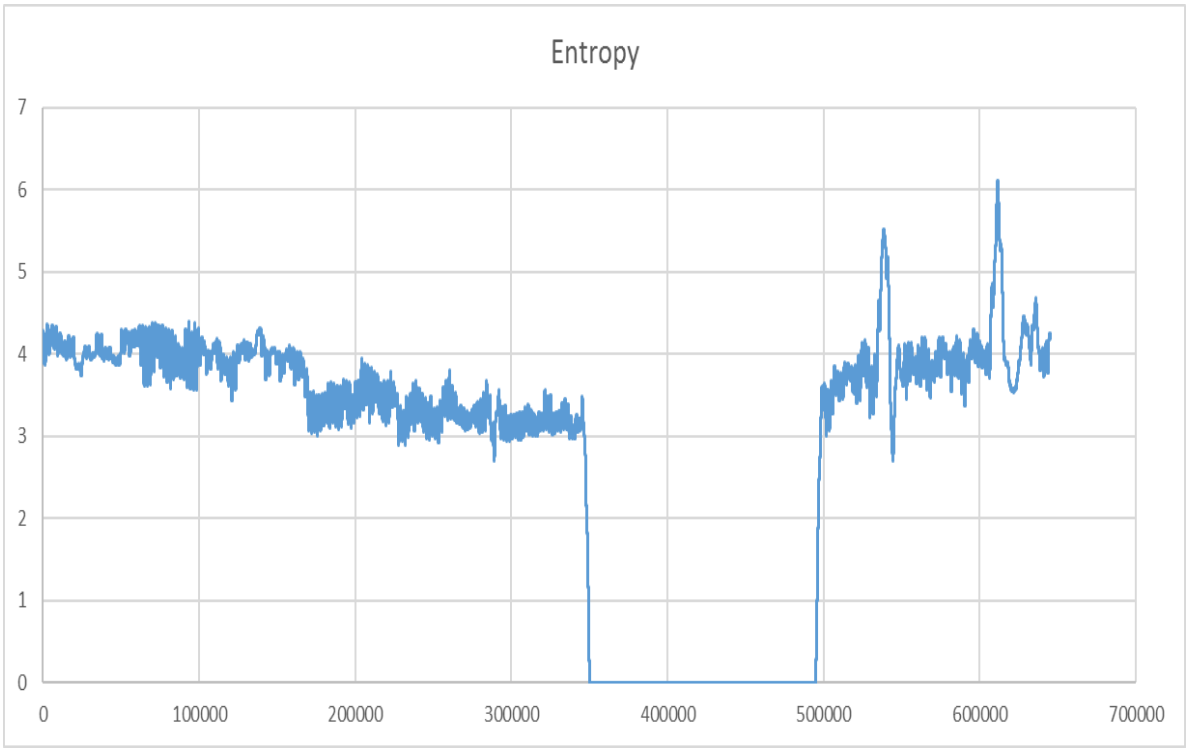
Διάγραμμα 6. Senario 1-FSD Entropy

Όπως φαίνεται από τα διαγράμματα και οι τρείς παραμετροποιήσεις ανιχνεύουν τις επιθέσεις του πρώτου σεναρίου καθώς παρατηρείται σημαντική αλλαγή στις τιμές της εντροπίας.

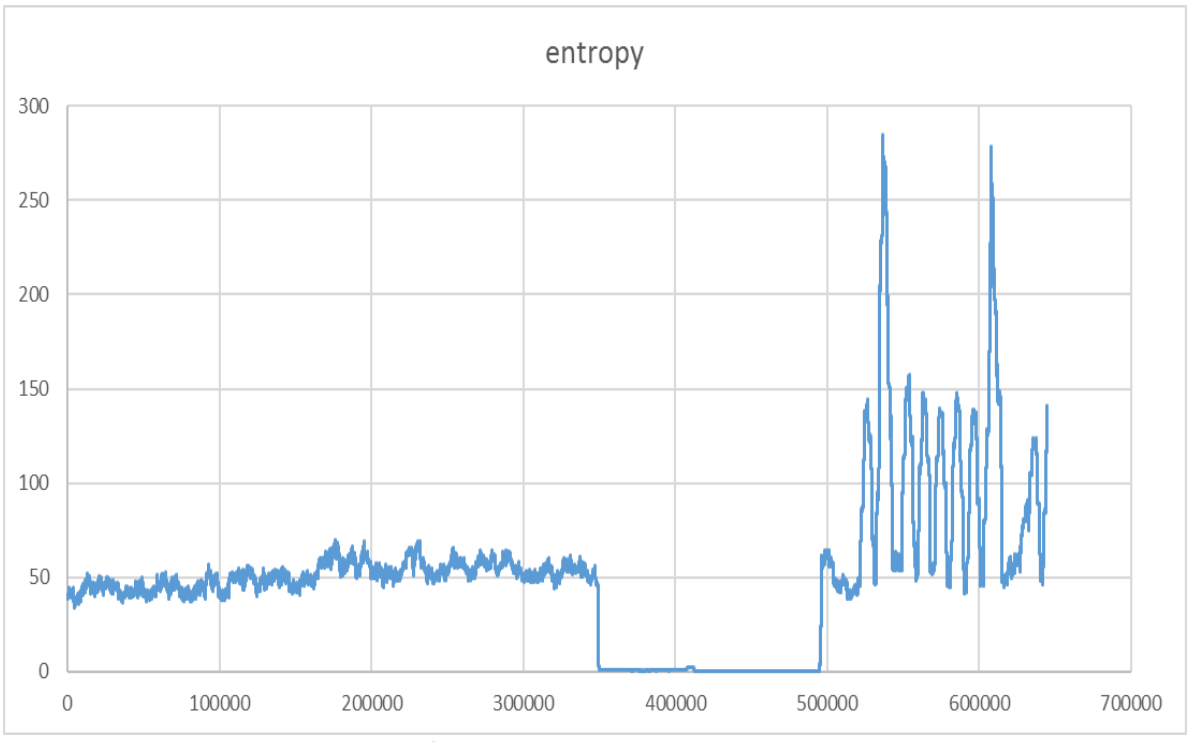
4.4.3. Διαγράμματα Κίνησης Σενάριο 2(Κίνηση από 3 bot)



Διάγραμμα 7. Senario 2-Source IP Entropy

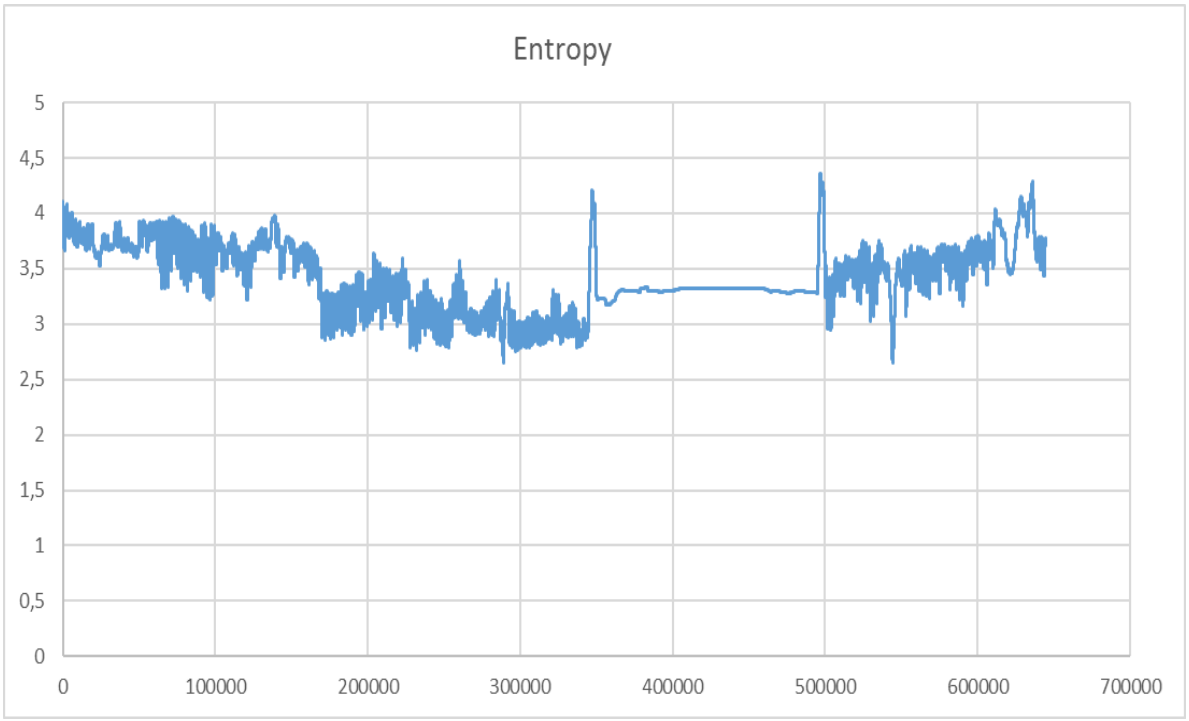


Διάγραμμα 8. Senario 2-Destination IP Entropy

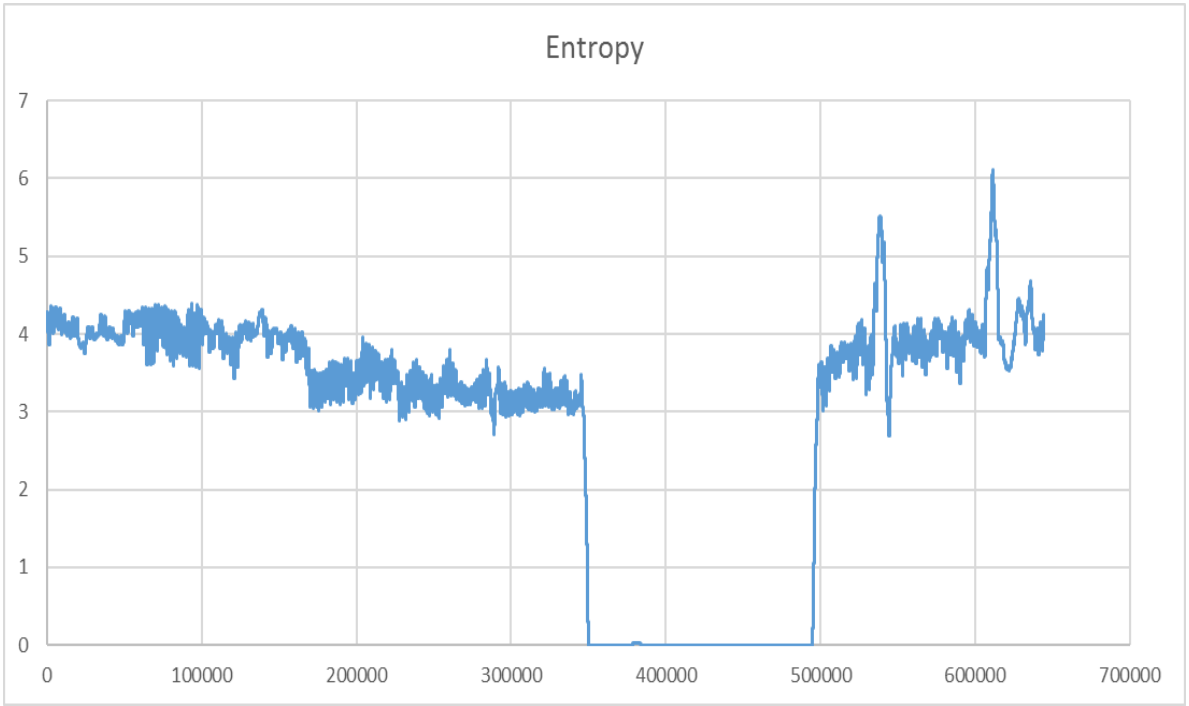


Διάγραμμα 9. Senario 2-FSD Entropy

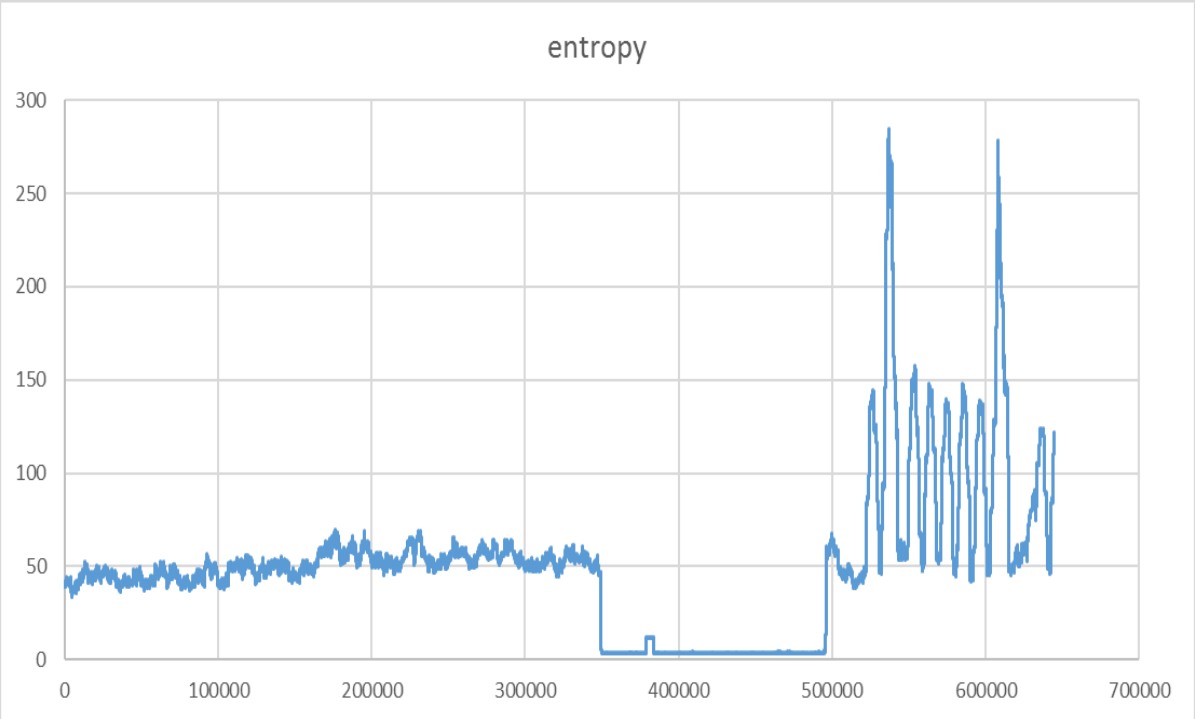
4.4.4.Διαγράμματα Κίνησης Σενάριο 3(Κίνηση από 10 bot)



Διάγραμμα 10. Senario 3-Source IP Entropy



Διάγραμμα 11. Senario 3-Destination IP Entropy



Διάγραμμα 12. Senario3 FSD Entropy

Στο τρίτο σενάριο στο οποίο η επίθεση πραγματοποιείται από δέκα bots η ανίχνευση με την διεύθυνση πηγής αποτυγχάνει να ανιχνεύσει την επίθεση.

4.5 Δεύτερο μέρος πειράματος-Προσδιορισμός Classifier

Στο δεύτερο μέρος του πειράματος επιδιώχτηκε ο προσδιορισμός ενός classifier, δηλαδή ενός κατηγοριοποιητή κίνησης με βάση την εντροπία. Ως κατηγοριοποιητής κίνησης επιλέχτηκε η σύγκριση, των τιμών της εντροπίας, με ένα όριο διαχωρισμού της ομαλής με την ανώμαλη κίνηση, δηλαδή ενός κατωφλίου. Ο συγκεκριμένος προσδιορισμός ήταν ιδιαίτερα δύσκολος, διότι ακολουθώντας την βιβλιογραφία για την ανίχνευση επιθέσεων η τιμή κατωφλίου (threshold) προσδιοριζόταν αυθαίρετα βασισμένη στα εκάστοτε datasets.
Αυτό οφείλεται στο γεγονός ότι είναι δύσκολο να τεθούν τα κατάλληλα κατώτατα όρια τα οποία βοηθούν στην εξισορρόπηση των ψευδώς θετικών και ψευδώς αρνητικών αποτελεσμάτων. Όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο τα ψευδώς θετικά αποτελέσματα είναι αυτά τα οποία εντοπίζουν λανθασμένα επιθέσεις ενώ τα ψευδώς αρνητικά αποτυγχάνουν να εντοπίσουν τις επιθέσεις σε συγκεκριμένα σημεία των datasets. Ακόμη, είναι πολύ δύσκολο να εξαχθούν τα χαρακτηριστικά κανονικής και ανώμαλης συμπεριφοράς του δικτύου με ακρίβεια. Τα μεγέθη ανίχνευσης ανωμαλιών ,όπως είναι στην προκειμένη περίπτωση η εντροπία, χρησιμοποιούν ένα προκαθορισμένο συγκεκριμένο όριο, όπως για παράδειγμα μια ανώμαλη απόκλιση ορισμένων στατιστικών χαρακτηριστικών από την κανονική κίνηση του δικτύου για τον εντοπισμό μη φυσιολογικής κίνησης από την κανονική. Ως εκ τούτου, η χρήση και η επιλογή των στατιστικών μεθόδων και εργαλείων είναι ζωτικής σημασίας [55].
Εφόσον η εντροπία της ανώμαλης κίνησης είναι σημαντικά διαφορετική από την εντροπία της κανονικής, ιδανική λύση του προσδιορισμού του κατωφλίου θα ήταν η επιλογή της ελάχιστης

τιμής της εντροπίας όταν το εξεταζόμενο δίκτυο λειτουργεί υπό φυσιολογικές συνθήκες. Κάτι τέτοιο δεν είναι εφικτό καθώς η ελάχιστη τιμή δεν είναι σταθερή ούτε στην διάρκεια του χρόνου(ώρες, μέρες) ούτε από ένα σημείο του δικτύου σε ένα άλλο. Αυτό σημαίνει ότι σε ένα πραγματικό δίκτυο με καταγραφή σε πραγματικό χρόνο δεν είναι δυνατόν να είναι γνωστή εκ των προτέρων η ελάχιστη φυσιολογική τιμή της εντροπίας. Για τον λόγο αυτό ο προσδιορισμός ενός στατιστικού τύπου για τον προσδιορισμό αυτού του ορίου είναι ιδιαίτερα σημαντικός. Στα πλαίσια της διπλωματικής αυτή εργασίας, έγινε προσπάθεια ενός πιο λεπτομερούς προσδιορισμού της τιμής κατωφλίου. Πιο συγκεκριμένα, σύμφωνα με πρόσφατη δημοσίευση [57], η τιμή κατωφλίου σε στατιστικές προσεγγίσεις ανίχνευσης επιθέσεων άρνησης υπηρεσίας μπορεί να προσδιοριστεί ως εξής:

Threshold = average entropy + standard deviation

Όπου threshold είναι η τιμή κατωφλίου, average entropy ο μέσος όρος των τιμών εντροπίας για την ομαλή κίνηση και standard deviation η τυπική απόκλιση των τιμών της εντροπίας στην ομαλή κίνηση. Η τυπική απόκλιση συνηθίζεται να συμβολίζεται με το σύμβολο σ και υπολογίζεται ως εξής:

$$\sigma = \sqrt{\frac{1}{N} * \sum_{i=1}^{N} (\bar{x} - x_i)^2} \qquad (3)$$

Στην περίπτωση μας $\bar{x}$ είναι η μέση τιμή της εντροπίας ομαλής κίνησης του δείγματος x_i η κάθε τιμή της εντροπίας και *N* είναι το πλήθος των τιμών της εντροπίας στο dataset. Όσον αφορά το πείραμα μας και επειδή όπως είδαμε στο πρώτο μέρος του πειράματος οι τιμές της εντροπίας όταν ανιχνεύσει επίθεση άρνησης υπηρεσίας μειώνονται θέλουμε να προσδιορίσουμε ένα κάτω όριο των φυσιολογικών τιμών της εντροπίας. Συνεπώς ο τύπος γίνεται:

Threshold = average entropy - standard deviation

Έχοντας προσδιορίσει την τιμή κατωφλίου την εφαρμόσαμε στο dataset ομαλής κίνησης για τον προσδιορισμό των ψευδώς θετικών αποτελεσμάτων. Η εφαρμογή έγινε στο dataset ομαλής κίνησης διεύθυνσης προορισμού καθώς όπως συμπεράναμε στο πρώτο μέρος του πειράματος η ανίχνευση με βάση την διεύθυνση πηγής αποτυγχάνει να εντοπίσει όλα τα σενάρια επιθέσεων. Το αποτέλεσμα αυτής της δοκιμής ήταν ο εντοπισμός 21,98% ψευδώς θετικών, αποτέλεσμα το οποίο είναι μη αποδεκτό επειδή είναι πολύ υψηλό. Συνεπώς επιχειρήθηκε μια παραμετροποίηση του τύπου εισάγοντας μία επιπλέον παράμετρο a ως εξής:

Threshold = average entropy - a**standard deviation*

Στην συνέχεια με συνεχής πειραματισμούς της τιμής του a επιδιώχτηκε η ελαχιστοποίηση των ψευδώς θετικών σε ποσοστό μικρότερου ή ίσου του 0,1. Ο ακόλουθος πίνακας παρουσιάζει τα αποτελέσματα των πειραμάτων αυτών. Τα αποτελέσματα δείχνουν ότι όσο μειώνεται η τιμή του a τόσο μειώνεται το ποσοστό των ψευδώς θετικών. Οι επιθυμητές τιμές του a είναι αυτές του a = 1,95 και a = 2.

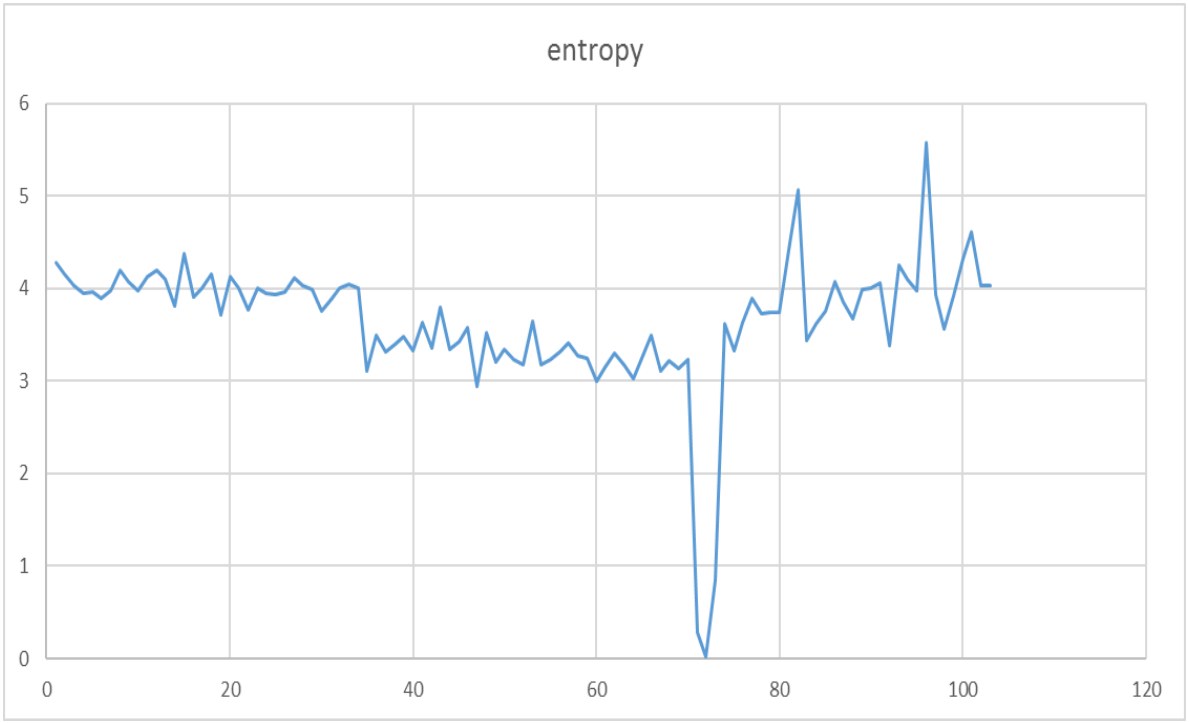
a	*False positives(%)*
1	21,98209901
1,2	16,23513512
1,25	14,67352053
1,3	13,26867347
1,35	11,8405941
1,4	10,49655505
1,45	9,432111685
1,5	8,287466376
1,55	7,303325956
1,6	6,218276547
1,65	5,315449176
1,7	4,332924916
1,75	3,419289475
1,8	2,769088112
1,85	2,220098768
1,9	1,620806444
1,95	1,071009019
2	0,633029664

Πίνακας 2. Τιμές παραμέτρου α- Ποσοστά false positives

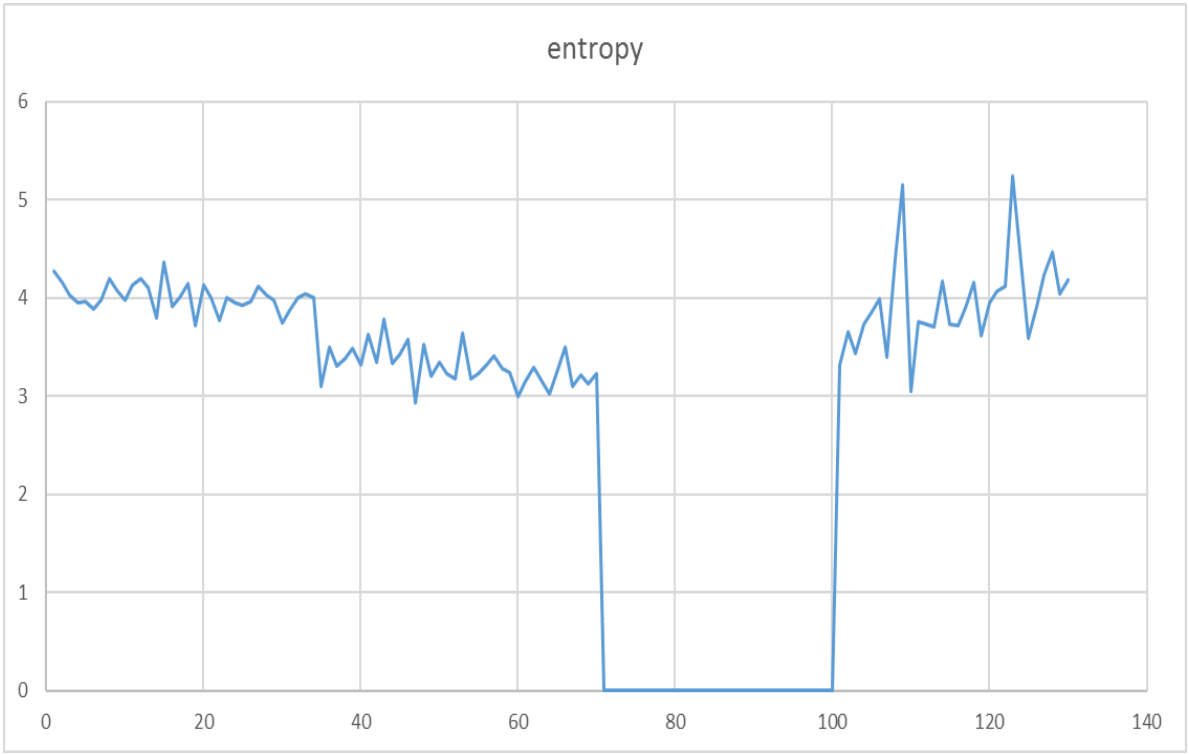
Θα μπορούσε να επιδιωχτεί ακόμη μεγαλύτερη μείωση του ποσοστού ψευδώς θετικών κάτι τέτοιο όμως δεν είναι επιθυμητό διότι το όριο κατωφλίου δεν θα μπορούσε να εντοπίσει μέρος της επίθεσης. Αν παρατηρήσουμε την διάρκεια της επίθεσης από το πρώτο μέρος του πειράματος και ορίζοντας σε αυτό το σημείο το όριο κατωφλίου συμπεραίνουμε ότι όσο πιο μικρή η τιμή κατωφλίου τόσο λιγότερο μέρος της επίθεσης ανιχνεύει η μέθοδος. Συνεπώς, επιδιώκεται ο προσδιορισμός του ορίου κατωφλίου με τέτοιο τρόπο ώστε να μπορεί να εφαρμοστεί γενικότερα, και όχι ειδικά μόνο για το συγκεκριμένο dataset, δηλαδή για ένα ευρύτερο σύνολο datasets.
Ως προς την ανίχνευση με βάση την FSD, λόγω της μεγάλης διακύμανσης των τιμών στην ομαλή κίνηση, η μέση τιμή της εντροπίας και η τυπική απόκλιση έχουν πολύ υψηλές τιμές με αποτέλεσμα να μην είναι δυνατή η ανίχνευση των επιθέσεων με a=1,95 ή a=2. Συνεπώς, δεδομένου ότι οι διακυμάνσεις στην φυσιολογική κίνηση αποτρέπουν τον προσδιορισμό ενός γενικότερου κατωφλίου, που ήταν η αρχική επιδίωξη αυτού του πειραματικού μέρους, η μέθοδος ανίχνευσης με βάση την FSD απορρίπτεται. Οδηγούμαστε λοιπόν στο συμπέρασμα ότι η βέλτιστη μέθοδος ανίχνευσης επιθέσεων με την εντροπία είναι βάση της διεύθυνσης προορισμού.
Τέλος, στο τρίτο μέρος του πειράματος επιχειρήθηκε η εφαρμογή μίας αρκετά απλοποιημένης προσέγγισης, ως προς την απαιτούμενη υπολογιστική ισχύ, με βάση την εντροπία για την ανίχνευση των επιθέσεων.

4.6 Τρίτο μέρος πειράματος-Προσδιορισμός απλοποιημένης μεθόδου ανίχνευσης επιθέσεων

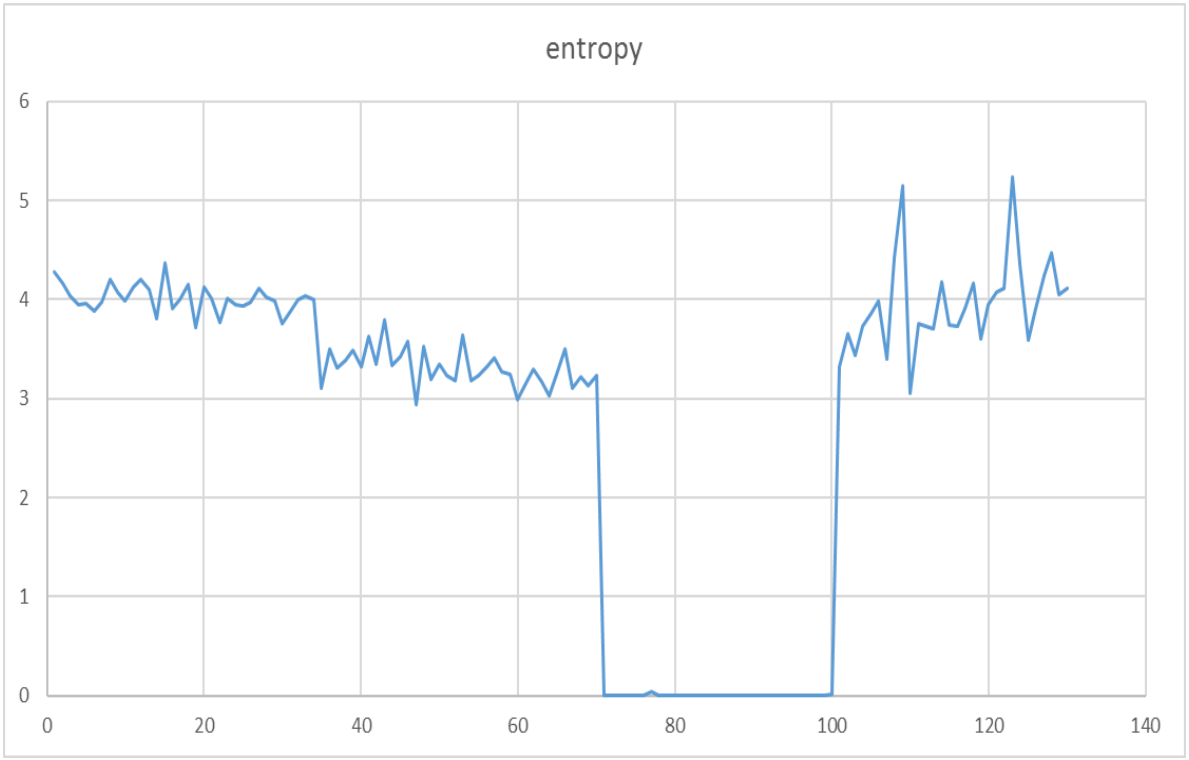
Λόγω του μεγάλου όγκου δεδομένων προς επεξεργασία και της απαιτούμενης υπολογιστικής ισχύς της μεθόδου που εφαρμόστηκε επιδιώχθηκε μία παραλλαγή της υλοποίησης της μεθόδου της εντροπίας. Στην παραλλαγή αυτή ο υπολογισμός της εντροπίας δεν γίνεται σε κυλιόμενα παράθυρα αλλά σε διακριτά παράθυρα εύρους W πακέτων το οποίο είναι υπολογιστικά απλούστερο. Σκοπός του τρίτου μέρους είναι ο προσδιορισμός του εάν μια απλούστερη μέθοδος εντροπίας μπορεί να παράγει σωστά αποτελέσματα ανίχνευσης των επιθέσεων μειώνοντας σημαντικά την απαιτούμενη υπολογιστική ισχύ. Τα dataset στα οποία εφαρμόστηκε η μέθοδος αυτή είναι τα ίδια με αυτά από τα προηγούμενα πειραματικά μέρη. Δεδομένου ότι καταλήξαμε στο ότι η ανίχνευση επιθέσεων με βάση την διεύθυνση προορισμού είναι η βέλτιστη, η απλοποιημένη μέθοδος εφαρμόστηκε μόνο για αυτή την παραμετροποίηση της εντροπίας. Ακολουθούν τα αποτελέσματα της ανίχνευσης. Για να προκύψουν τα ακόλουθα αποτελέσματα χρησιμοποιήθηκε παράθυρο W= 10.000.



Διάγραμμα 13. Simplified Method Senario1



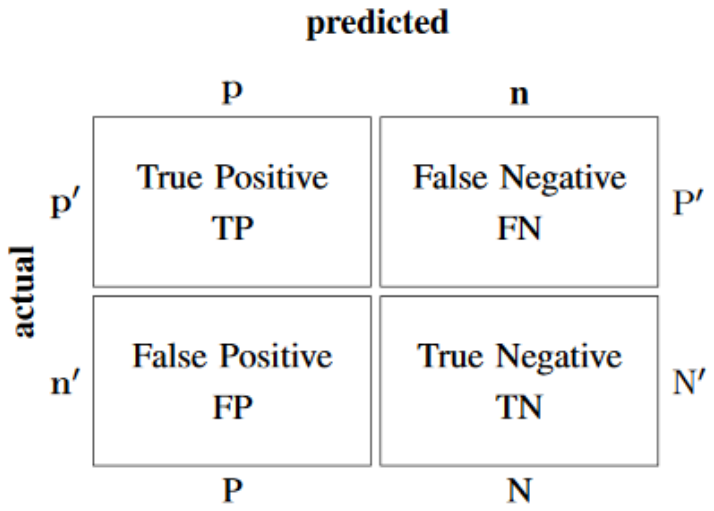
Διάγραμμα 14. Simplified Method Senario2



Διάγραμμα 15. Simplified Method Senario3

Από τα διαγράμματα συμπεραίνομαι ότι η απλοποιημένη μέθοδος μπορεί να ανιχνεύσει τις επιθέσεις όλων των σεναρίων. Το ερώτημα όμως που τίθεται είναι κατά πόσο μπορεί να αυξηθεί το παράθυρο W ώστε η μέθοδος αυτή να εξακολουθεί να ανιχνεύει την επίθεση.

Για να μπορέσουμε να συγκρίνουμε την απόδοση της αρχικής μεθόδου σε σχέση με την απόδοση της απλοποιημένης θα θεωρήσουμε ότι κάθε απόπειρα κατηγοριοποίησης μπορεί να οδηγήσει σε ένα από τα τέσσερα ακόλουθα αποτελέσματα:



Εικόνα 10. Πιθανά αποτελέσματα κατηγοριοποίησης

Ένας ιδανικός κατηγοριοποιητής κίνησης δεν θα πρέπει να παράγει ψευδώς θετικά (False Positives - FP) και ψευδώς αρνητικά (False Negatives - FN) στατιστικά λάθη/αποτελέσματα. Για την αξιολόγηση ενός μη ιδανικού κατηγοριοποιητή κίνησης θα μπορούσε κανείς να μετρήσει το ποσοστό των σωστών εκτιμήσεων προς το σύνολο των εκτιμήσεων (ACC), το ποσοστό «ομαλής» κίνησης που αναγνωρίζεται ως «ανώμαλη» (False Positive Rate - FPR) και το ποσοστό των ανωμαλιών που απέτυχε να εντοπίσει ο ανιχνευτής(False Negative Rate - FNR). Οι τύποι υπολογισμού των προαναφερθέντων μονάδων μέτρησης καθώς επίσης και κάποιες επιπλέον μετρήσεις που χρησιμοποιούνται για την αξιολόγηση της απόδοσης ενός κατηγοριοποιητή παρουσιάζονται στον ακόλουθο πίνακα:

Name	Formula
True Positive Rate (TPR) eqv. with Recall, Sensitivity	$TPR = \frac{TP}{TP+FN}$
True Negative Rate (TNR) eqv. with Specificity	$TNR = \frac{TN}{FP+TN}$
Positive Predictive Value (PPV) eqv. with Precision	$PPV = \frac{TP}{TP+FP}$
Negative Predictive Value (NPV)	$NPV = \frac{TN}{TN+FN}$
False Positive Rate (FPR) eqv. with Fall-out	$FPR = \frac{FP}{FP+TN} = 1 - TNR$
False Discovery Rate (FDR)	$FDR = \frac{FP}{FP+TP} = 1 - PPV$
False Negative Rate (FNR)	$FNR = \frac{FN}{FN+TP}$
Accuracy (ACC)	$ACC = \frac{TP+TN}{TP+FN+FP+TN}$
F1 score – harmonic mean of Precision and Recall	$F1 = \frac{2TP}{2TP+FP+FN}$

Πίνακας 2. Μονάδες αξιολόγησης κατηγοριοποιητή

Στην προσέγγιση μας, έχοντας πλέον ορίσει τους τρόπους αξιολόγησης ενός κατηγοριοποιητή εφαρμόσαμε ορισμένους από τους τύπους αυτούς στην αρχική μέθοδο υπολογισμού της εντροπίας (ως προς την διεύθυνση προορισμού) και της απλοποιημένης μεθόδου για τις δύο τιμές του a που μας εξασφαλίζουν το επιθυμητό ποσοστό FP όπως αυτό προσδιορίστηκε στο δεύτερο μέρος του πειράματος.

a = 1,95	Σενάριο 1				Σενάριο 2				Σενάριο 3			
	ACC	FPR	FNR	TPR	ACC	FPR	FNR	TPR	ACC	FPR	FNR	TPR
Αρχική μέθοδος	0,996	0,003	0,027	0,972	0,996	0,003	0,004	0,995	0,996	0,003	0,007	0,992
Απλοποιημένη μέθοδος W=10.000	1	0	0	1	1	0	0	1	1	0	0	1
Απλοποιημένη μέθοδος W=5.000	1	0,025	0	1	1	0,025	0	1	1	0,025	0	1
Απλοποιημένη μέθοδος W=2.500	1	0,002	0	0	1	0,002	0	1	1	0,002	0	1
Απλοποιημένη μέθοδος W=1.000	0,999	0	0,035	0,964	1	0	0	1	1	0,0009	0	1

Πίνακας 3. Λεπτομερής απόδοση των εφαρμοσμένων μεθόδων για a =1,95

a = 2	Σενάριο 1				Σενάριο 2				Σενάριο 3			
	ACC	FPR	FNR	TPR	ACC	FPR	FNR	TPR	ACC	FPR	FNR	TPR
Αρχική μέθοδος	0,996	0,002	0,027	0,977	0,996	0,002	0,004	0,996	0,996	0,002	0,007	0,993
Απλοποιημένη μέθοδος W=10.000	1	0	0	1	1	0	0	1	1	0	0	1
Απλοποιημένη μέθοδος W=5.000	1	0,025	0	1	1	0,025	0	1	1	0,025	0	1
Απλοποιημένη μέθοδος W=2.500	1	0,002	0	0	1	0,002	0	1	1	0,002	0	1
Απλοποιημένη μέθοδος W=1.000	0,999	0	0,035	0,964	1	0	0	1	1	0,0009	0	1

Πίνακας 4. Λεπτομερής απόδοση των εφαρμοσμένων μεθόδων για a =2

Αρχικά, υπολογίστηκαν οι τιμές για την αρχική μέθοδο και για την απλοποιημένη μέθοδο με παράθυρο W= 10.000. Όπως φαίνεται από τους πίνακες για a=1,95 και a=2 οι τιμές της απλοποιημένης μεθόδου περιγράφουν έναν ιδανικό κατηγοριοποιητή κίνησης. Όμως, επειδή στην απλοποιημένη μέθοδο πρέπει να έχει οριστεί εκ των προτέρων το παράθυρο W πακέτων το σενάριο αυτό δεν είναι ρεαλιστικό, δηλαδή δεν αποδίδει αν επιχειρηθεί να εφαρμοστεί σε πραγματικό χρόνο σε κάποιο δίκτυο. Αρχικά, εάν έχει οριστεί μεγάλο παράθυρο W και η επίθεση είναι αρκετά μικρότερη από το μέγεθος του παραθύρου τότε είναι πολύ πιθανό η επίθεση να μην ανιχνευτεί καθόλου. Συνεπώς είναι κρίσιμη η επιλογή του μεγέθους του παραθύρου. Για τον λόγο αυτό θεωρούμε ότι η αρχική μέθοδος, παρόλο που απαιτεί μεγαλύτερη υπολογιστική ισχύ και εξετάζει με την σειρά όλα τα πακέτα, είναι καταλληλότερη. Επιπλέον, επιχειρήθηκε ο υπολογισμός των ποσοστών αξιολόγησης του κατηγοριοποιητή για τρείς ακόμα περιπτώσεις της απλοποιημένης μεθόδου για να αποδείξουμε ότι και αυτή η μέθοδος εμπίπτει σε σφάλματα. Όπως φαίνεται από τους παραπάνω δύο πίνακες όταν το παράθυρο W έφτασε στην τιμή 1.000, δηλαδή υπολογισμός της εντροπίας ανά παράθυρα 1.000 πακέτων η απλοποιημένη μέθοδος άρχισε να εμφανίζει σφάλματα. Ο λόγος που δεν εντόπισε σφάλματα αυτή η μέθοδος για τα προηγούμενα μεγάλα παράθυρα W, δηλαδή για W =10.000 , 5.000 και 2.500 αντίστοιχα, είναι επειδή το πλήθος των τιμών της εντροπίας των εξεταζόμενων datasets ήταν πολύ μικρό. Ως αποτέλεσμα οι αλλαγές στις τιμές της εντροπίας να είναι πολύ απότομες, όπως φαίνεται και στα διαγράμματα 13,14 και 15 και οι επιθέσεις εντοπίζονταν από τον κατηγοριοποιητή χωρίς σφάλματα. Στην περίπτωση όμως που το παράθυρο μειώθηκε σημαντικά (W=1.000) και συνεπώς το πλήθος των τιμών της εντροπίας αυξήθηκε άρχισαν να εμφανίζονται σφάλματα.

Το συμπέρασμα που προκύπτει από αυτές τις μετρήσεις είναι ότι παρόλο που η απλοποιημένη μέθοδος δείχνει να είναι ελάχιστα ποιο αποδοτική (στην περίπτωση W=1.000 διαφέρει από την αρχική μας μέθοδο μόλις 0,003), η αρχική προσέγγιση προσφέρει έναν αρκετά αξιόπιστο τρόπο ανίχνευσης με υψηλά ποσοστά επιτυχούς ανίχνευσης επιθέσεων και πολύ χαμηλά ποσοστά σφαλμάτων.

Κεφάλαιο 5: Συμπεράσματα – Μελλοντικές Προτάσεις

Στόχος της παρούσας έρευνας υπήρξε η ανάπτυξη ενός υποδείγματος για την ανίχνευση επιθέσεων DDOS με την στατιστικομαθηματική μέθοδο της εντροπίας. Το ερώτημα που απάντησε η παρούσα έρευνα είναι ότι μπορεί να επιτευχθεί αποδοτική ανίχνευση των επιθέσεων αυτών με την μέθοδο της εντροπίας. Στην συνέχεια παρατίθεται η συμβολή του κάθε κεφαλαίου στην απάντηση του αρχικού ερωτήματος καθώς επίσης και τα σημαντικότερα συμπεράσματα της εργασίας.

Στο πρώτο-εισαγωγικό κεφάλαιο έγινε αναφορά στα ερεθίσματα που έδωσαν το έναυσμα για προβληματισμό πάνω στο αντικείμενο, στο στόχο και στην μεθοδολογία που ακολουθήθηκε στην συγγραφή της εργασίας. Στην συνέχεια γίνεται μία προσπάθεια εισαγωγής του αναγνώστη στο αντικείμενο το οποίο πραγματεύεται η έρευνα.

Το δεύτερο κεφάλαιο επιχείρησε να παρουσιάσει το σύνολο των επιθέσεων καθώς επίσης να προσδιορίσει από ποιους υλοποιούνται και ποιους στόχους έχουν οι επιθέσεις αυτές, δίνοντας έμφαση στις επιθέσεις DDOS. Εν συνεχεία περιεγράφηκαν οι σύγχρονοι μέθοδοι ανίχνευσης των επιθέσεων αυτών.

Στο τρίτο κεφάλαιο προσδιορίστηκε η μεθοδολογία που ακολουθήθηκε στο πειραματικό μέρος της εργασίας και οι λόγοι για τους οποίους κατευθυνθήκαμε προς την εφαρμογή της συγκεκριμένης μεθόδου

Στο τέταρτο κεφάλαιο περιεγράφηκε η μέθοδος της εντροπίας που εφαρμόστηκε, ποιες παράμετροι χρησιμοποιήθηκαν και προσδιορίστηκαν τα δεδομένα που χρησιμοποιήθηκαν για την υλοποίηση των πειραμάτων. Πιο αναλυτικά, αρχικά προσδιορίστηκαν τα τρία μέρη του πειράματος, η αρχική μέθοδος της εντροπίας, ο προσδιορισμός ενός classifier και τέλος παρουσιάστηκε μια απλοποιημένη μέθοδος ανίχνευσης με στόχο να αποτελέσει βάση για μελλοντική έρευνα. Στο πρώτο μέρος, περιγράφονται αναλυτικά τα δεδομένα που χρησιμοποιήθηκαν για το κάθε ένα εκ των τριών σεναρίων και ποιες παραμετροποιήσεις δέχτηκε η μέθοδος μας, διεύθυνση πηγής, διεύθυνση προορισμού και FSD. Ενώ παραδεχόμαστε ότι τα πειράματά μας περιορίστηκαν σε μικρό αριθμό περιπτώσεων, πιστεύουμε ότι οι περιπτώσεις αυτές ήταν αντιπροσωπευτικές.

Στην συνέχεια, παρουσιάστηκαν τα αποτελέσματα της μεθόδου.

- Συγκρίνοντας τα διαγράμματα παρατηρούμε ότι η μέθοδος της εντροπίας με βάση την διεύθυνση πηγής στο διάγραμμα 10 για το σενάριο 3 αποτυγχάνει να εντοπίσει την επίθεση οπότε θεωρούμε την συγκεκριμένη μέθοδο μη αποτελεσματική.

- Στο δεύτερο μέρος κατά τον προσδιορισμό του classifier επιλέχτηκε ως εργαλείο η τιμή κατωφλίου. Λόγω του απαγορευτικού ποσοστού λάθους του αρχικού τύπου εφαρμόστηκε κατάλληλη παραμετροποίηση του κατωφλίου και υπολογίστηκε ότι οι τιμές a=1,95 και a=2 αποδίδουν με αποδεκτά ποσοστά λάθους, δηλαδή περίπου 1%.

- Στην συνέχεια παρατηρήθηκε ότι εξ αιτίας της μεγάλης διακύμανσης που εμφανίζουν οι τιμές της εντροπίας στην περίπτωση του FSD,όπως φαίνεται στο διάγραμμα 3, δεν μπορεί να προσδιοριστεί μια τιμή κατωφλίου που να ανιχνεύει την επίθεση, διότι η μέση τιμή και η τυπική απόκλιση λαμβάνουν υψηλές τιμές με αποτέλεσμα και το μεγαλύτερο μέρος της «ομαλής» κίνησης να ανιχνεύεται ως ανώμαλη. Για τον λόγο αυτό, επειδή ο classifier δεν μπορεί να διαχωρίσει την ομαλή από την «ανώμαλη» κίνηση, για την συγκεκριμένη

προσέγγιση η μέθοδος υπολογισμού της εντροπίας με την FSD θεωρείται μη αποτελεσματική.

- Συνεπώς η βέλτιστη μέθοδος ανίχνευσης των επιθέσεων στα συγκεκριμένα dataset που εφαρμόστηκε είναι η μέθοδος της εντροπίας με βάση την διεύθυνση προορισμού.

- Στο τρίτο μέρος του πειράματος, η υλοποίηση της απλοποιημένης μεθόδου έδειξε ότι με λιγότερους υπολογισμούς γίνονται ανιχνεύσιμες οι επιθέσεις, δεδομένου ότι στην πρώτη περίπτωση υπολογιζόταν η εντροπία για κάθε πακέτο δηλαδή για τις συγκεκριμένες υλοποιήσεις περίπου 990.000 υπολογισμοί εντροπίας ενώ στην απλοποιημένη μέθοδο οι υπολογισμοί ήταν ,για παράθυρο W=10.000, περίπου 100.

- Το μειονέκτημα της απλοποιημένης μεθόδου είναι ότι η αποτελεσματικότητα ανίχνευσης της εξαρτάται σε μεγάλο βαθμό από το μέγεθος του παραθύρου W, το οποίο πρέπει να έχει ορισθεί εκ των προτέρων αυθαίρετα, παραδείγματος χάριν αν η μέθοδος αυτή εφαρμοστεί σε πραγματικό χρόνο η επιλογή του παραθύρου θα πρέπει να γίνει τυχαία γεγονός που θα επηρεάσει καθοριστικά την αποτελεσματικότητα της μεθόδου. Δηλαδή εάν ολόκληρο το εύρος μίας επίθεσης εμπίπτει σε ένα μόνο μέρος του παραθύρου υπολογισμού τότε είναι πολύ πιθανό να μην εντοπιστεί η επίθεση.

- Συγκρίνοντας την απλοποιημένη μέθοδο με την αρχική παρατηρήθηκε από τους πίνακες 3, 4 ότι και οι δύο μέθοδοι παρέχουν εξίσου υψηλή ακρίβεια (αρχική μέθοδος περίπου 0,996 και απλοποιημένη μέθοδος 0,999).

- Τέλος, δεδομένου ότι η αρχική μέθοδος εξετάζει όλα τα πακέτα ένα προς ένα ενώ η δεύτερη απλοποιημένη μέθοδος εξαρτάται σε σημαντικό βαθμό από τον αυθαίρετο προσδιορισμό του παραθύρου, λαμβάνοντας υπόψιν ότι οι δύο μέθοδοι προσφέρουν τον ίδιο υψηλό βαθμό ακρίβειας στην ανίχνευση επιθέσεων, για να διασφαλίσουμε την αποφυγή αυτού του αυθαίρετου παραθύρου που μπορεί να οδηγήσει σε αποτυχία ανίχνευσης μικρού εύρους επιθέσεων, οδηγούμαστε στο συμπέρασμα ότι η αρχική μέθοδος αποτελεί πιο αποτελεσματική προσέγγιση.

Στο τελευταίο μέρος της διπλωματικής εργασίας αναφέρονται τα αποτελέσματα και πως αυτά συνέβαλαν στην απάντηση του αρχικού ερωτήματος που εξέταζε η εργασία αυτή και αναφέρονται κάποιες προτάσεις για πιθανή μελλοντική έρευνα και ανάλυση της ανίχνευσης επιθέσεων με την μέθοδο της εντροπίας, οι οποίες μπορεί να αποδειχθούν αρκετά ενδιαφέρουσες και πολύ χρήσιμες για την κατανόηση και μελέτη των επιθέσεων DDOS και των μεθόδων ανίχνευσης τους.

Αρχικά θα ήταν ενδιαφέρον να εφαρμοστεί η μέθοδος που επιγράφθηκε και σε άλλα dataset για να επαληθευτούν τα αποτελέσματα που προέκυψαν.

Σαν μια περαιτέρω ανάλυση, προτείνεται η εφαρμογή της μεθόδου της εντροπίας που εφαρμόστηκε στην παρούσα έρευνα σε πραγματικό χρόνο. Για να πραγματοποιηθεί αυτή η προσέγγιση θα ήταν ιδιαίτερα ενδιαφέρουσα η προσομοίωση ενός δικτύου προς παρακολούθηση

καθώς επίσης και η προσομοίωση του δικτύου των επιτιθέμενων bots για να παρατηρηθούν τα αποτελέσματα της μεθόδου μας σε καταγραφές πραγματικού χρόνου.

Μεγάλο ενδιαφέρον θα παρουσίαζε επίσης το ενδεχόμενο να μελετηθεί η αποτελεσματικότητα του επιλεγμένου ορίου κατωφλίου σε διαφορετικά δείγματα δεδομένων ή ακόμα και στο προαναφερθέν προσομοιωμένο δίκτυο, τόσο για την επαλήθευση του όσο και για την παρατήρηση των αποτελεσμάτων του classifier σε πραγματικό χρόνο.

Τέλος, δεδομένου ότι τα τελευταία χρόνια οι επιθέσεις DDOS αυξάνονται τόσο σε αριθμό όσο και σε ισχύ, η μελέτη για τον προσδιορισμό ενός ευρέως αποδεκτού παραθύρου πακέτων, που θα ανιχνεύει αποτελεσματικά τις συγκεκριμένες επιθέσεις, της απλοποιημένης μεθόδου, δεδομένου ότι απαιτεί μικρότερη υπολογιστική ισχύ από την αρχική προσέγγιση, θα οδηγήσει σε πολύ σημαντικά αποτελέσματα.

Βιβλιογραφικές Αναφορές

1. «helpnetsecurity,» 19 July 2016. [Ηλεκτρονικό]. Available: https://www.helpnetsecurity.com/2016/07/19/ddos-attacks-escalate/

2. D. Denning, «An intrusion-detection model,» *IEEE Transactions on Software Engineering,* τόμ. 13, p. 17, 1987.

3. T. Cheng, Y. Lin, Y. Lai και P. Lin, «Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems,» *IEEE Communications Surveys & Tutorials,* τόμ. 14, 2012.

4. P. Berezi, B. Jasiul και M. Szpyrka, «An Entropy-Based Network Anomaly Detection Method,» *Entropy,* τόμ. 17, 2015.

5. Z. Li, A. Das και J. Zhou, «USAID: Unifying Signature-Based and Anomaly-Based Intrusion,» σε *Advances in Knowledge Discovery and Data Mining*, Springer Berlin Heidelberg, 2005, pp. 702-712.

6. F. L, S. D, B. R και K. D, «Statistical approaches to DDoS attack detection and response,» *DARPA Information Survivability Conference and Exposition,* τόμ. 2, 2003.

7. G. Nychis, V. Sekar, D. Andersen, H. Kim και H. Zhang, «An Empirical Evaluation of Entropy-based Traffic Anomaly Detection,» *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement,* p. 151–156, 2008.

8. «Sophos Security Threat Report 2014» 2014.

9. Y. Xiang, K. Li και W. Zhou, «Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,» *IEEE Transactions on Information Forensics and Security,* τόμ. XI, αρ. 2, pp. 426-437, 2011.

10. B. Tellenbach, M. Burkhart, D. Sornette και T. Maillart, «Beyond Shannon: Characterizing Internet Traffic with Generalized Entropy Metrics,» σε *Passive and Active Measurement Conference*, Seoul, 2009.

11. I. Witten, E. Frank και M. Hall, Data Mining: Practical Machine Learning Tools and Techniques, San Francisco: Morgan Kaufmann Publishers Inc., 2011.

12. D. Bhattacharyya και J. Kalita, Network Anomaly Detection: A Machine Learning Perspective, Boca Raton: Chapman & Hall/CRC, 2013.

13. C. Aggarwal, Outlier Analysis, New York: Springer, 2013.

14. T. Hastie, R. Tibshirani και J. Friedman, The Elements of Statistical Learning: Data Mining, New York: Springe, 2009.

15. V. Chandola, A. Banerjee και V. Kumar, « Anomaly Detection: A Survey,» ACM ComputingSurveys, 2009.

16. V. Hodge και J. Austin, «A Survey of Outlier Detection Methodologies,» Artificial Intelligence Review, 2004.

17. L. Huang, X. Nguyen, M. Garofalakis, M. Jordan, A. Joseph και N. Taft, «In-Network PCA and Anomaly Detection,» EECS Department, University of California, Berkeley, 2007.

18. M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn και L. Chang, «A novel anomaly detection scheme based on principal component classifier,» σε *Third IEEE International Conference on Data Mining*, Melbourne, 2003.

19. W. Lu και A. Ghorbani, «Network Anomaly Detection Based on Wavelet Analysis,» *EURASIP Journal on Advances in Signal Processing,* 2009.

20. W. Lu, M. Tavallaee και A. Ghorbani, «Detecting Network Anomalies Using Different Wavelet Basis Functions,» σε *Sixth Annual Conference on Communication Networks and Services Research*, Halifax, 2008.

21. N. Ye, Y. Zhang και C. Borror, «Robustness of the Markov-chain model for cyber-attack detection,» *IEEE Transactions on Reliability,* p. 116–123, 2004.

22. I. Syarif, A. Prugel-Bennett και G. Wills, «Unsupervised Clustering Approach for Network Anomaly Detection,» σε *Networked Digital Technologies*, Berlin/Heidelberg, Springer, 2012, p. 135–145.

23. A. Kind, M. Stoecklin και X. Dimitropoulos, «Histogram-based Traffic Anomaly Detection,» *IEEE Transactions on Network and Service Management,* p. 110–121, 2009.

24. M. Stoecklin, J. L. Boudec και A. Kind, « Two-layered Anomaly Detection Technique Based on Multi-modal Flow Behavior Models.,» σε *9th International Conference on Passive and Active Network Measuremen*, Cleveland, 2008.

25. F. Iglesias και T. Zseby, «Entropy-Based Characterization of Internet Background Radiation,» *Entropy,* p. 74–101, 2014.

26. D. Harrington, R. Presuhn και B. Wijnen, «An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks,» [Ηλεκτρονικό]. Available: http://www.ietf.org/rfc/rfc3411.txt. [Πρόσβαση 16 April 2015].

27. P. Barford, J. Kline, D. Plonka και A. Ron, « A Signal Analysis of Network Traffic Anomalies,» σε *2nd ACM SIGCOMM Workshop on Internet Measuremen*, Marseille, 2002.

28. M. Kim, H. Kong, S. Hong, S. Chung και J. Hong, «A flow-based method for abnormal network traffic detection.,» σε *IEEE/IFIP Network Operations and Management Symposium* , Seoul, 2004.

29. G. Kambourakis, C. Kolias, S. Gritzalis και J. Park, «DoS attacks exploiting signaling in {UMTS} and {IMS}.,» *Comput. Commun.,* pp. 226-235, 2011.

30. K. Choi, X. Chen, S. Li, M. Kim, K. Chae και J. Na, «ntrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid.,» *Energies,* τόμ. V, p. 4091–4109, 2012.

31. Invea-Tech FlowMon, [Ηλεκτρονικό]. Available: https://www.invea.com.

32. AKMA Labs FlowMatrix, [Ηλεκτρονικό]. Available: http://www.akmalabs.com.

33. I. Jingle και E. Rajsingh, «ColShield: An effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks.,» *Human-centric Comput. Inf. Sci.,* τόμ. IV, 2014.

34. W. Zhou, W. Jia, S. Wen, Y. Xiang και W. Zhou, « Detection and defense of application-layer {DDoS} attacks in backbone web traffic.,» *Future Gener. Comput. Syst.,* p. 36–46, 2014.

35. A. Lakhina, M. Crovella και C. Diot, «Mining Anomalies Using Traffic Feature Distributions.,» σε *2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Philadelphia, 2005.

36. C. Shannon, «A Mathematical Theory of Communication.,» *Bell Syst. Tech. J.,* p. 379–423, 1948.

37. J. Baez, T. Fritz και T. Leinster, «A Characterization of Entropy in Terms of Information Loss.,» *Entropy,* p. 1945–1957, 2011.

38. W. Lee και D. Xiang, «Information-theoretic measures for anomaly detection.,» σε *2001 IEEE Symposium on Security and Privacy*, Oakland, 2001.

39. J. Zhang, X. Chen, Y. Xiang, W. Zhou και J. Wu, «Robust Network Traffic Classification.,» *EEE/ACM Trans. Netw.,* 2014.

40. A. Soule, K. Salamatia, N. Taft, R. Emilion και K. Papagiannaki, «Flow Classification by Histograms: Or How to Go on Safari in the Internet.,» σε *Joint International Conference on Measurement and Modeling of Computer Systems*, New York, 2004.

41. B. Tellenbach, «Detection, Classification and Visualization of Anomalies using Generalized Entropy Metrics.».

42. «http://www.computercraft.info/wiki/Network_Attacks,» [Ηλεκτρονικό].

43. «http://www.inetdaemon.com/,» 1 Septermber 2013. [Ηλεκτρονικό]. Available: http://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml.

44. «https://en.wikipedia.org/,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Man-in-the-middle_attack.

45. «https://en.wikipedia.org/,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/ARP_spoofing.

46. W. Stallings, Cryptography and Network Security: Principles and Practice.

47. «ZDNet,» 8 June 2016. [Ηλεκτρονικό]. Available: http://www.zdnet.com/article/ddos-attacks-increase-over-125-percent-year-over-year/.

48. P. Anilkumar, «Botnets and Distributed Denial of Service Attacks».

49. G. P. M, «Botnet Tracking Tools,» 8 August 2014. [Ηλεκτρονικό]. Available: https://www.sans.org/reading-room/whitepapers/detection/botnet-tracking-tools-35347.

50. F. Bégin, «SANS,» 27 July 2011. [Ηλεκτρονικό]. Available: https://www.sans.org/reading-room/whitepapers/malicious/byob-build-botnet-33729.

51. «Academia.edu,» [Ηλεκτρονικό]. Available: https://www.academia.edu/11395235/CLASSIFICATION_OF_INTRUSION_DETECTION_SYSTEMS.

52. V. Jaiganesh, S. Mangayarkarasi και D. Sumathi, «Intrusion Detection Systems: A Survey and Analysis of Classification Techniques,» *International Journal of Advanced Research in Computer and Communication Engineering,* τόμ. II, αρ. 4, 2013.

53. B. Ditcheva και L. Fowler, «Signature-based Intrusion Detection,» Chapel Hill, 2005.

54. L. Feinstein και D. Schnackenberg, «Statistical Approaches to DDoS Attack Detection and,» 2003.

55. G. Carlet, «Denial-of-service attack-detection techniques,» *IEEE Internet Comput.,* τόμ. X, p. 82–89, 2006.

56. Y. Liu, N. Xiong, J. Park, C. Yang και K. Xu, «Fair incentive mechanism with pyramidal structure for peer-to-peer networks.,» *IET Commun.,* τόμ. IV, pp. 1-12, 2010.

57. M. Mathew, «A Statistical Approach to Detect Denial of Service Attacker,» *Journal for Research,* τόμ. II, αρ. 1, 2016.