ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΞΙΟΛΟΓΗΣΗ ΑΛΓΟΡΙΘΜΩΝ ΕΝΤΟΠΙΣΜΟΥ ΕΠΙΘΕΣΕΩΝ ΑΡΝΗΣΗΣ ΥΠΗΡΕΣΙΑΣ ΑΠΟ ΤΗΝ ΚΙΝΗΣΗ ΤΟΥ ΔΙΚΤΥΟΥ

ΦΩΤΕΙΝΗ ΠΑΠΑΓΑΛΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΗΡΑΚΛΕΙΟ ΜΑΡΤΙΟΣ 2004

Αξιολόγηση Αλγορίθμων Εντοπισμού Επιθέσεων Άρνησης Υπηρεσίας από την Κίνηση του Δικτύου

Φωτεινή Παπαγάλου

Μεταπτυχιακή Εργασία

Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

Περίληψη

Τα τελευταία χρόνια, πολλοί δικτυακοί τόποι έχουν υποστεί Επίθεση Άρνησης Υπηρεσίας (Denial of Service – DoS), μεταξύ των οποίων, η πιο διαδεδομένη είναι η επίθεση TCP SYN flooding. Σκοπός των επιθέσεων άρνησης υπηρεσίας είναι η κατανάλωση όσο το δυνατόν περισσότερων πόρων, με τελικό αποτέλεσμα τη στέρηση της παροχής των προβλεπόμενων υπηρεσιών από τους νόμιμους χρήστες. Η επίθεση τύπου TCP SYN flooding εκμεταλλεύεται το μηχανισμό χειραψίας τριών σημείων (three way handshake) του πρωτοκόλλου TCP καθώς και τον περιορισμό του στη δυνατότητα διατήρησης ημι-ανοιχτών συνδέσεων. Κάθε σύστημα που είναι συνδεδεμένο στο Διαδίκτυο και παρέχει υπηρεσίες δικτύου οι οποίες βασίζονται στο πρωτόκολλο TCP, όπως για παράδειγμα ένας εξυπηρετητής παγκόσμιου ιστού (web server) ή ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου, είναι δυνατό να υποστεί μια επίθεση άρνησης υπηρεσίας.

Στην παρούσα εργασία παρουσιάζουμε και αξιολογούμε δυο αλγόριθμους εντοπισμού ανωμαλιών στην προσπάθειά μας να εντοπίσουμε έγκαιρα επιθέσεις τύπου TCP SYN flooding: έναν αλγόριθμο προσαρμοζόμενου κατωφλιού και μια συγκεκριμένη εφαρμογή του αθροιστικού αλγόριθμου ελέγχου (CUSUM) για τον εντοπισμό σημείου ανωμαλίας.

Σκοπός μας είναι να αναλύσουμε μέσω εκτενών πειραμάτων με πραγματικά ίχνη κίνησης, τα πλεονεκτήματα και τα μειονεκτήματα των αλγορίθμων αυτών όσον αφορά στην πιθανότητα εντοπισμού, στο ποσοστό των λανθασμένων σημάνσεων συναγερμού και στην καθυστέρηση εντοπισμού. Επίσης, μελετούμε τον τρόπο με τον οποίο τα παραπάνω χαρακτηριστικά επηρεάζονται από τις παραμέτρους του εκάστοτε αλγόριθμου αλλά και από το είδος των επιθέσεων. Ακόμη, η μελέτη αυτή στοχεύει

στο να συμβάλλει στην κατάλληλη ρύθμιση των παραμέτρων των αλγορίθμων, έτσι ώστε να ικανοποιούνται συγκεκριμένες απαιτήσεις επίδοσης.

Τα πειραματικά μας αποτελέσματα δείχνουν πως παρόλο που οι απλοί αλγόριθμοι, όπως ο αλγόριθμος προσαρμοζόμενου κατωφλιού, παρουσιάζουν πολύ ικανοποιητική επίδοση όσον αφορά σε επιθέσεις υψηλής έντασης, η απόδοσή τους ελαττώνεται όταν καλούνται να εντοπίσουν επιθέσεις χαμηλής έντασης. Αντίθετα, αλγόριθμοι οι οποίοι στηρίζονται σε ισχυρές θεωρητικές βάσεις, όπως ο αλγόριθμος CUSUM, επιδεικνύουν σταθερά καλή απόδοση ανεξάρτητα από το είδος των επιθέσεων που καλούνται να εντοπίσουν, χωρίς να είναι απαραίτητα δαπανηρή ή περίπλοκη η υλοποίησή τους.

Επόπτης:

Βασίλειος Α. Σύρης
Επίκουρος Καθηγητής
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

Evaluation of algorithms for Denial of Service (DoS) Attack Detection based on network traffic

Fotini Papagalou

Master of Science Thesis

Computer Science Department
University of Crete

Abstract

Over the past few years many sites on the Internet have been subjected to Denial of Service (DoS) attacks, among which TCP SYN flooding is the most prevalent. The aim of denial of service attacks is to consume all the available resources, with main purpose to prevent legitimate users from receiving service. TCP SYN flooding exploits the three-way handshake mechanism of the TCP protocol and its limitation in maintaining half-open connections. Any system connected to the Internet and providing TCP-based network services, such as a Web server or mail server, is potentially subject to this kind of attack.

In this study, we present and evaluate two anomaly detection algorithms for detecting early TCP SYN attacks: an adaptive threshold algorithm and a particular application of the cumulative sum (CUSUM) algorithm for change point detection.

We focus on investigating, through extended experiments with real traffic traces, the tradeoffs between the detection probability, the false alarm rate and the detection delay, and how these tradeoffs are affected by the parameters of the detection algorithm and the characteristics of the attacks. Such an investigation can assist in tuning the parameters of the detection algorithm to satisfy specific performance requirements.

Our experimental results indicate that although simple and straightforward algorithms, such as the adaptive threshold algorithm, have good performance for high intensity attacks, their performance deteriorates for low intensity attacks. On the other hand, algorithms based on a strong theoretical foundation, like the CUSUM algorithm, can exhibit robust performance over various attack types, without necessarily being complex or costly to implement.

Supervisor:

Vasilios A. Siris

Associate Professor

Computer Science Department

University of Crete

Ευχαριστίες

Ολοκληρώνοντας τη μεταπτυχιακή μου εργασία, θα ήθελα να ευχαριστήσω όλους όσοι με βοήθησαν σε όλα τα στάδια ανάπτυξής της.

Αρχικά, θα ήθελα να ευχαριστήσω τον επόπτη καθηγητή μου Βασίλειο Σύρη, ο οποίος μου έδωσε τη δυνατότητα να ασχοληθώ με το θέμα της εργασίας αυτής και με καθοδήγησε σε όλη τη διάρκειά της. Ιδιαίτερα τον ευχαριστώ για την εξαιρετική συνεργασία, την ενθάρρυνση που μου προσέφερε, καθώς και για τις εύστοχες πάντα παρατηρήσεις και υποδείξεις του. Ευχαριστώ επίσης θερμά τους καθηγητές Παναγιώτη Τσακαλίδη και Απόστολο Τραγανίτη για τη συμμετοχή τους στην επιτροπή εξέτασης της εργασίας μου, αλλά και για τις καίριες συμβουλές και τα εποικοδομητικά σχόλιά τους. Ευχαριστώ και τους καθηγητές Ευάγγελο Μαρκάτο και Γιάννη Στυλιανού για τις ενδιαφέρουσες και χρήσιμες παρατηρήσεις τους.

Ιδιαίτερα ευχαριστώ τον Παναγιώτη Καραγεωργάκη για τη σημαντική βοήθειά του σε θέματα προγραμματισμού αλλά και για την ηθική του υποστήριξη.

Ευχαριστώ ακόμη τους Χάρη Μαρινάκη, Βαγγέλη Αγγελάκη και Στέφανο Παπαδάκη για τη βοήθεια και συμπαράστασή τους καθώς και όλα τα μέλη των ομάδων Δικτύων και Αρχιτεκτονικής Υπολογιστών και Συστημάτων VLSI του Ινστιτούτου Πληροφορικής για τη συνεργασία τους.

Θα ήθελα επίσης να ευχαριστήσω όλους τους φίλους μου και ιδιαίτερα τη Χαρά Αθανασοπούλου και τη Ρόη Φλουρή για τη στήριξή τους σε όλη τη διάρκεια της εργασίας μου.

Περισσότερο θα ήθελα να ευχαριστήσω τους γονείς μου για τη συμπαράστασή τους και την εμπιστοσύνη που δείχνουν στις επιλογές μου.

Τέλος, θα ήθελα να ευχαριστήσω το Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου Κρήτης και το Ινστιτούτο Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας για την υλικοτεχνική και οικονομική υποστήριξη που μου παρείχαν κατά τη διάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

Κατάλογος Σχημάτων

Στους γονείς μου,
Μανόλη και Ιωάννα

1 Εισαγωγή

1.1 Εισαγωγή

Το Διαδίκτυο, όχι πολλά χρόνια πριν, αποτελούσε ένα κατά πολύ μικρότερο τμήμα της υπολογιστικής κοινότητας συγκριτικά με σήμερα. Οι κόμβοι του ήταν διεσπαρμένοι σε μερικά ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες. Οι χρήστες του περιλάμβαναν φοιτητές, ερευνητές και γενικότερα ανθρώπους που ασχολούνταν κατά τον έναν ή τον άλλο τρόπο με την τεχνολογία και τις επιστήμες. Η υποδομή του, το διάσημο ζεύγος πρωτοκόλλων TCP/IP, είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά, χωρίς να περιλαμβάνει ιδιαίτερους μηχανισμούς ή δικλίδες ασφαλείας.

Η ραγδαία ανάπτυξη των τηλεπικοινωνιών και η διαδεδομένη χρήση του Διαδικτύου έχουν δώσει τα τελευταία χρόνια νέα διάσταση στην έννοια της επικοινωνίας και στην διακίνηση της πληροφορίας. Τα τελευταία χρόνια το Διαδίκτυο αναπτύσσεται και επεκτείνεται με εκθετικούς ρυθμούς τόσο σε επίπεδο πλήθους χρηστών όσο και σε επίπεδο παρεχόμενων υπηρεσιών. Η ευρεία χρήση του έχει σαν αποτέλεσμα τεράστιος όγκος και μεγάλη ποικιλία πληροφοριών να διακινείται πλέον μέσω του Διαδικτύου καθιστώντας το ζωτικό παράγοντα σε κάθε μορφή ανθρώπινης δραστηριότητας: οικονομικής, πολιτικής, κοινωνικής.

Η φύση όμως αυτή του Διαδικτύου έχει καταστήσει διαρκώς αυξανόμενη την ανάγκη προστασίας των δεδομένων αλλά και των πόρων αυτού. Το πρόβλημα της ασφάλειας στο Διαδίκτυο, απασχολεί έντονα, και έχει κινητοποιήσει κρατικούς και μη φορείς ασφαλείας, την επιστημονική κοινότητα καθώς και εταιρίες ανάπτυξης λογισμικού και δικτυακών υποδομών προς την κατεύθυνση της πληρέστερης κατανόησης και επίλυσής του. Όσο μεγαλώνει η διάδοση του Διαδικτύου και πληθαίνουν τα υπολογιστικά συστήματα και οι εφαρμογές που είναι συνδεδεμένα με αυτό, τόσο σημαντικότερος γίνεται ο τομέας της ασφάλειας των εφαρμογών αλλά και των υπολογιστικών συστημάτων

Στα πλαίσια αυτής της θέσης και όσον αφορά στο πρόβλημα της ασφάλειας στο Διαδίκτυο έχουν πραγματοποιηθεί διάφορες απόπειρες καταγραφής, ταξινόμησης και ομαδοποίησης επιθέσεων καθώς και στρατηγικών αντιμετώπισής τους.

Ένα από τα σημαντικότερα και δημοφιλέστερα είδη επιθέσεων, είναι οι επιθέσεις Άρνησης Υπηρεσίας και ειδικότερα τύπου TCP SYN flooding. Σκοπός των

επιθέσεων άρνησης υπηρεσίας είναι η κατανάλωση όσο το δυνατόν περισσότερων πόρων, με τελικό αποτέλεσμα τη στέρηση της παροχής των προβλεπόμενων υπηρεσιών από τους νόμιμους χρήστες. Στην παρούσα εργασία παρουσιάζουμε και αξιολογούμε δυο αλγόριθμους εντοπισμού ανωμαλιών στην προσπάθειά μας να εντοπίσουμε έγκαιρα επιθέσεις τύπου TCP SYN flooding: έναν αλγόριθμο προσαρμοζόμενου κατωφλιού και μια συγκεκριμένη εφαρμογή του αθροιστικού αλγόριθμου ελέγχου (CUSUM) για τον εντοπισμό σημείου ανωμαλίας.

Σκοπός μας είναι να αναλύσουμε μέσω εκτενών πειραμάτων με πραγματικά ίχνη κίνησης, τα πλεονεκτήματα και τα μειονεκτήματα των αλγορίθμων αυτών όσον αφορά στην πιθανότητα εντοπισμού, στο ποσοστό των λανθασμένων σημάνσεων συναγερμού και στην καθυστέρηση εντοπισμού. Επίσης, μελετούμε τον τρόπο με τον οποίο τα παραπάνω χαρακτηριστικά επηρεάζονται από τις παραμέτρους του εκάστοτε αλγόριθμου αλλά και από το είδος των επιθέσεων. Ακόμη, η μελέτη αυτή στοχεύει στο να συμβάλλει στην κατάλληλη ρύθμιση των παραμέτρων των αλγορίθμων, έτσι ώστε να ικανοποιούνται συγκεκριμένες απαιτήσεις επίδοσης.

1.2 Περιγραφή του πρωτοκόλλου TCP / IP

Στον τομέα των δικτύων, με τον όρο πρωτόκολλο εννοείται ένα σύνολο από συμβάσεις που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει τον τρόπο με τον οποίο διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών, κλπ. Ειδικότερα στο Διαδίκτυο, το οποίο είναι στην ουσία πολλά μικρότερα δίκτυα τα οποία συνδέονται μεταξύ τους, χρειάζεται ένα σύνολο από συμβάσεις που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα.

Το αρχικό επικοινωνιακό πρωτόκολλο ήταν το NCP [1] (Network Control Protocol) το οποίο όμως αντικαταστάθηκε με το πέρασμα του χρόνου, διότι αποδείχθηκε αργό κι ανασφαλές. Αντικαταστάθηκε λοιπόν από δύο υψηλών προδιαγραφών και μεγαλύτερης πολυπλοκότητας πρωτόκολλα, τα γνωστά σήμερα ως TCP και IP ή συνηθέστερα TCP/IP (Transmission Control Protocol / Internet Protocol) [2].

Το TCP/IP προσφέρει στην ουσία το σύνολο αυτών των συμβάσεων που προαναφέραμε. Όλοι οι υπολογιστές που είναι συνδεδεμένοι στο Διαδίκτυο,

υλοποιούν το πρωτόκολλο TCP/IP κι έτσι μπορούν να επικοινωνούν παρά τη διαφορετικότητά τους. Είναι στην ουσία ένα σύνολο πρωτοκόλλων το οποίο αναπτύχθηκε από μια ομάδα ερευνητών με αφορμή το δίκτυο ARPAnet [3], το οποίο και αποτελεί το πιο γνωστό TCP/IP δίκτυο.

Είναι ανοιχτό, ελεύθερα διαθέσιμο, ανεξάρτητο από hardware ή λειτουργικό σύστημα, ή από τα φυσικά χαρακτηριστικά του δικτύου, ενώ χρησιμοποιεί έναν κοινό τρόπο διευθυνσιοδότησης για όλους τους υπολογιστές τους συνδεδεμένους στο δίκτυο.

Το Διαδίκτυο χρησιμοποιεί την τεχνολογία μεταγωγής πακέτων [4][5], για τη μεταφορά των δεδομένων: τα δεδομένα τεμαχίζονται σε κομμάτια (πακέτα) και σε κάθε πακέτο μπαίνει μια επικεφαλίδα με τις διευθύνσεις του υπολογιστή - αποστολέα και του υπολογιστή - παραλήπτη.

1.2.1 Το πρωτόκολλο IP

Το πρωτόκολλο IP [6], είναι το καθιερωμένο πρωτόκολλο του επιπέδου δικτύου στο Διαδίκτυο και παρέχει μια αναξιόπιστη, χωρίς σύνδεση (connection-less) και χωρίς εγγυήσεις (best effort) υπηρεσία διανομής πακέτων. Το πρωτόκολλο αυτό επίσης αναλαμβάνει τη διευθυνσιοδότηση και δρομολόγηση των μηνυμάτων από τον έναν κόμβο στον άλλο. Το IP καθορίζει ως βασική μονάδα μεταφοράς δεδομένων το datagram, ένα συγκεκριμένο είδος πακέτου, το οποίο χρησιμοποιείται σε κάθε IP δίκτυο. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ότι το πακέτο αυτό θα φτάσει στον προορισμό του, γι' αυτό άλλωστε και χαρακτηρίζεται ως αναξιόπιστη η υπηρεσία που παρέχει.

Το IP είναι πρωτόκολλο χωρίς σύνδεση, γιατί μεταχειρίζεται το κάθε πακέτο ανεξάρτητα από όλα τα υπόλοιπα, με αποτέλεσμα το καθένα να δρομολογείται μέσω διαφορετικών μονοπατιών, έτσι ώστε κάποια από τα πακέτα αυτά να χαθούν ενώ κάποια άλλα να παραδοθούν κανονικά. Δεν εγγυάται επίσης ούτε ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν ούτε ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Τέλος, το IP παρέχει χωρίς εγγυήσεις παράδοση των πακέτων, γιατί είναι δυνατό τα πακέτα να απορριφθούν στην περίπτωση που οι πόροι έχουν εξαντληθεί ή το υποκείμενο δίκτυο έχει καταρρεύσει. Τα πακέτα δρομολογούνται προς τους

προορισμούς τους, ενώ υπάρχει ένα σύνολο από κανόνες, οι οποίοι χαρακτηρίζουν πώς οι διάφοροι υπολογιστές και οι ενδιάμεσοι δρομολογητές θα πρέπει να επεξεργαστούν να πακέτα, πώς και πότε θα πρέπει να δημιουργηθούν μηνύματα λάθους (error messages) καθώς και πότε θα πρέπει να απορριφθούν πακέτα.

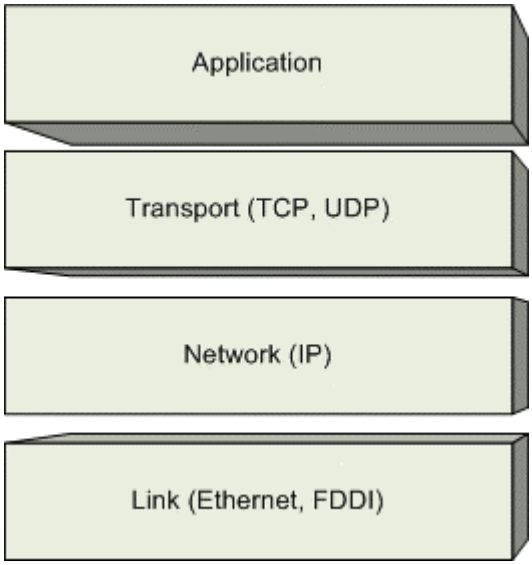
1.2.2 Το πρωτόκολλο TCP

Το TCP [7], προσφέρει ένα αξιόπιστο πρωτόκολλο πάνω από το IP, χρησιμοποιείται προκειμένου να εξασφαλίσει αξιόπιστη επικοινωνία στις εφαρμογές και τις υπηρεσίες που τη χρειάζονται. Βρίσκεται ανάμεσα στο επίπεδο του IP και στο επίπεδο εφαρμογής. Φροντίζει για την μετατροπή των μηνυμάτων σε πακέτα στον κόμβο αποστολής αλλά και εκτελεί την αντίθετη μετατροπή στον κόμβο προορισμού. Εγγυάται ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα. Εγγυάται επίσης τη μη ύπαρξη διπλότυπων πακέτων στον παραλήπτη. Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής - παραλήπτης και ο υπολογιστής - αποστολέας, αλλά όχι οι ενδιάμεσοι υπολογιστές, παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του. Ο παραλήπτης ελέγχει επίσης αν το περιεχόμενο των πακέτων φτάνει σωστά.

Η μέθοδος αυτή εξασφαλίζει αξιοπιστία και ταχύτητα διότι οι ενδιάμεσοι υπολογιστές δεν εκτελούν ελέγχους.

1.2.3 Επίπεδα του πρωτοκόλλου

Το πρωτόκολλο αυτό αποτελείται από τέσσερα επίπεδα: Το επίπεδο ζεύξης (Link layer), το επίπεδο δικτύου (IP), το επίπεδο μεταφοράς (TCP) και το επίπεδο εφαρμογής (application).



Σχήμα 1: Επίπεδα του TCP

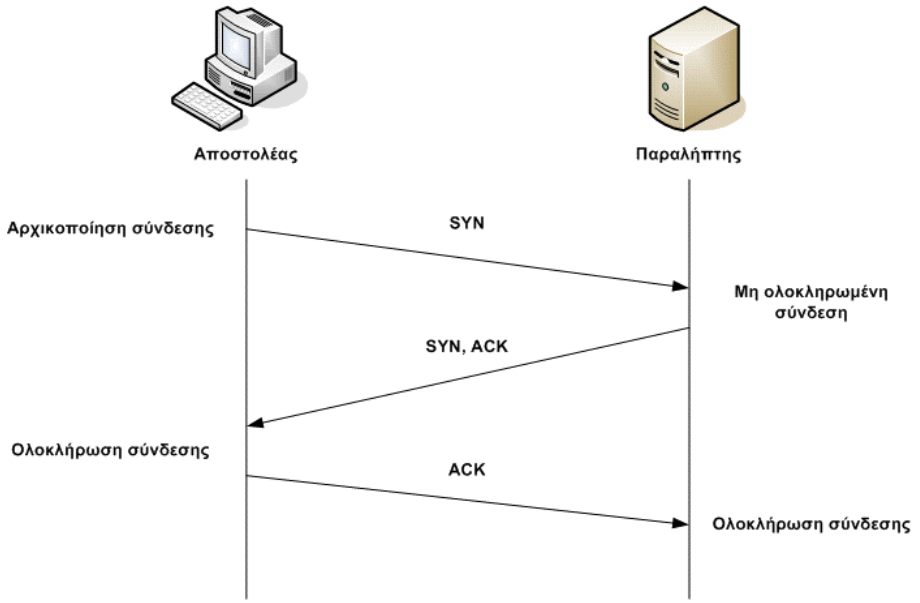
Τα δεδομένα δημιουργούνται στον υπολογιστή του αποστολέα για να μεταδοθούν προς τον παραλήπτη στο επίπεδο εφαρμογής, δηλαδή στο ανώτερο επίπεδο. Αυτό το επίπεδο συνιστούν τα προγράμματα που χειρίζεται και ο χρήστης και με τα οποία δημιουργεί τα δεδομένα, όπως για παράδειγμα ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Από το επίπεδο εφαρμογής τα δεδομένα οδηγούνται προς το επίπεδο TCP το οποίο όπως προαναφέραμε αναλαμβάνει να τα διαμορφώσει έτσι ώστε να μπορούν να μεταδοθούν με ασφάλεια και στη συνέχεια, όταν τα δεδομένα τεμαχιστούν, τα τμήματα αυτά οδηγούνται στο επίπεδο IP το οποίο αναλαμβάνει να τα κατευθύνει προς το σωστό προορισμό. Τέλος τα δεδομένα, τεμαχισμένα και με κατάλληλη σήμανση διευθυνσιοδότησης, μεταδίδονται μέσα από το φυσικό επίπεδο σαν απλά ηλεκτρικά σήματα μέσα από κατάλληλα μέσα μετάδοσης (π.χ. καλώδια, τηλεφωνικές συνδέσεις, δορυφορικές συνδέσεις κ.ο.κ.).

Στον παραλήπτη τα δεδομένα θα ακολουθήσουν την αντίστροφη πορεία: Τα ηλεκτρικά σήματα θα φτάσουν στον προορισμό τους, θα ανέβουν στο IP επίπεδο (σαν πακέτα πληροφοριών), το οποίο θα ελέγξει αν έπρεπε να φτάσουν εκεί και θα αφαιρέσει τις επικεφαλίδες του επιπέδου αυτού. Στη συνέχεια, το επόμενο TCP επίπεδο τα παραλαμβάνει και περιμένει να φτάσουν όλα τα πακέτα. Θα ελέγξει ότι έφτασαν όλα ορθά, θα τα βάλει στη σειρά, θα αφαιρέσει τις TCP επικεφαλίδες, θα τα ενώσει και θα τα προωθήσει στο ανώτερο επίπεδο. Αν κάποιο πακέτο είναι εσφαλμένο θα ζητήσει από τον αποστολέα την αναμετάδοσή του. Το τελευταίο επίπεδο αναλαμβάνει να εμφανίσει τα δεδομένα στον χρήστη.

1.2.4 Χειραψία Τριών Σημείων

Στο επίπεδο TCP λαμβάνει χώρα και η λεγόμενη χειραψία τριών σημείων [8], η οποία βοηθά στην εγκατάσταση μιας σύνδεσης ιδεατού κυκλώματος ανάμεσα στον αποστολέα και τον παραλήπτη. Όταν ένας υπολογιστής θελήσει να συνδεθεί με κάποιον άλλο στέλνει και λαμβάνει μια σειρά από μηνύματα προκειμένου να εγκαταστήσει μια σύνδεση TCP. Όλη αυτή η διαδικασία εγγυάται ότι και οι δυο πλευρές είναι έτοιμες να μεταδώσουν δεδομένα και επίσης ότι και οι δύο γνωρίζουν πως ο συνομιλητής τους είναι «έτοιμος» πριν στην ουσία αρχίσει η μετάδοση. Τα βασικά βήματα της χειραψίας αυτής είναι τα ακόλουθα:

- Ο αποστολέας στέλνει μια αίτηση σύνδεσης στον παραλήπτη
- Ο παραλήπτης απαντά με μια επιβεβαίωση
- Ο αποστολέας απαντά με μια δική του επιβεβαίωση και το κύκλωμα εγκαθίσταται. Στη συνέχεια, τα δεδομένα μπορούν να μεταδοθούν και προς τις δύο κατευθύνσεις.



Σχήμα 2: Χειραψία τριών σημείων

1.3 Οι Επιθέσεις στην Κίνηση του Δικτύου

Με τον όρο επίθεση σε κάποιο δικτυακό τόπο ή υπολογιστικό σύστημα, εννοούμε κάθε κακοπροαίρετη ενέργεια, η οποία σκοπό έχει τη μείωση της ασφάλειας, της διαθεσιμότητας, της αξιοπιστίας και της εμπιστευτικότητας των

υπολογιστικών και δικτυακών πόρων του συστήματος. Η διαδικασία αναγνώρισης της επίθεσης η οποία γίνεται με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα υπολογιστικό σύστημα/δίκτυο και στη συνέχεια την ανάλυσή τους για τυχόν εντοπισμό ενδείξεων επίθεσης, ονομάζεται Ανίχνευση Επίθεσης (Intrusion Detection). Ανάλογα, τα συστήματα τα οποία αυτοματοποιούν τη διαδικασία παρακολούθησης των γεγονότων που λαμβάνουν χώρα σε ένα υπολογιστικό σύστημα / δίκτυο και τα αναλύουν προκειμένου να εντοπιστούν πιθανές ενδείξεις προβλημάτων ασφάλειας, ονομάζονται Συστήματα Ανίχνευσης Επιθέσεων (IDS) [9].

Η μη φυσιολογική και προβλεπόμενη λειτουργία ενός συστήματος και κατά συνέπεια η άρνηση στους χρήστες των υπηρεσιών που αυτό προσφέρει, μπορεί είτε να οφείλεται σε κάποια αδυναμία του συστήματος όπως σχεδιαστικά λάθη αυτού ή λάθη κατά την υλοποίησή του, είτε σε καθαρά κακοπροαίρετη πρόθεση κάποιων χρηστών του συστήματος. Σε αυτή τη δεύτερη περίπτωση, το σύστημα υπολειτουργεί ή καταρρέει είτε επειδή δέχθηκε κάποιο είδος επίθεσης μέσω του Διαδικτύου, είτε γιατί εξουσιοδοτημένοι χρήστες του συστήματος αναζητούν περισσότερα δικαιώματα από αυτά που τους έχουν αποδοθεί και με δόλιους τρόπους προσπαθούν να τα αποκτήσουν, είτε τέλος επειδή πλήρως εξουσιοδοτημένοι χρήστες του συστήματος καταχρώνται των δικαιωμάτων τους.

Ο λόγος λοιπόν για τον οποίο η ασφάλεια είναι ένα πολύ μεγάλο και σημαντικό θέμα σε όλα τα υπολογιστικά συστήματα είναι γιατί υπάρχουν πολλά είδη επιθέσεων:

- *Γνωστοποίηση του περιεχομένου των μηνυμάτων (παθητική επίθεση):*

Αυτό συμβαίνει στην περίπτωση που ένα μήνυμα το οποίο αποστέλλεται από τον αποστολέα στον παραλήπτη, γίνεται γνωστό και σε τρίτους. Παραβιάζεται η εμπιστευτικότητα

- *Ανάλυση κίνησης (παθητική επίθεση):*

Πραγματοποιείται με την παρακολούθηση πληροφοριών οι οποίες εμπεριέχονται στα μηνύματα τα οποία αποστέλλονται σε ένα σύστημα, όπως διεύθυνση προορισμού, μέγεθος και συχνότητα αποστολής τους. Και σε αυτή την περίπτωση παραβιάζεται η εμπιστευτικότητα.

- *Πλαστοπροσωπία (ενεργητική επίθεση):*

Ο χρήστης αποστέλλει στο σύστημα ένα μήνυμα προσποιούμενος πως είναι κάποιος άλλος. Παραβιάζεται η πιστοποίηση της αυθεντικότητας του χρήστη.

- *Αναπαραγωγή (ενεργητική επίθεση):*

Ο χρήστης συλλαμβάνει ένα μήνυμα το οποίο αποστέλλεται μεταξύ δύο άλλων χρηστών και το αναπαράγει σε κάποια επόμενη χρονική στιγμή, είδος επίθεσης που παραβιάζει την αξιοπιστία της επικοινωνίας των χρηστών.

- *Τροποποίηση των μηνυμάτων (ενεργητική επίθεση):*

Ο χρήστης συλλαμβάνει ένα μήνυμα το οποίο αποστέλλεται μεταξύ δύο άλλων χρηστών, στη συνέχεια το μετατρέπει σε μορφή που αυτός επιθυμεί και το ξαναστέλνει στον παραλήπτη. Και αυτό το είδος επίθεσης παραβιάζει την αξιοπιστία της επικοινωνίας των χρηστών.

- *Άρνηση υπηρεσίας (ενεργητική επίθεση):*

Ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους πλαστών αιτήσεων που δέχεται από τον επιτιθέμενο. Επίθεση η οποία παραβιάζει τη διαθεσιμότητα του συστήματος.

1.3.1 Επιθέσεις Άρνησης Υπηρεσίας

Οι Επιθέσεις Άρνησης Υπηρεσίας (Denial of Service attacks) [10] αποτελούν μια ολοένα αυξανόμενη απειλή για την παγκόσμια Διαδικτυακή υποδομή. Μια Επίθεση Άρνησης Υπηρεσίας (DoS) είναι μία μέθοδος που χρησιμοποιούν κακόβουλοι χρήστες για να αποτρέψουν ή να αρνηθούν στους νόμιμους χρήστες τη χρήση υπηρεσιών του δικτύου. Είναι επιθέσεις οι οποίες καθιστούν το θύμα (δίκτυο ή σύστημα) ανήμπορο να εκπληρώσει τη λειτουργία για την οποία έχει σχεδιαστεί, ή να καταστήσουν τις συσκευές του συστήματος μη διαθέσιμες στους χρήστες– συνδρομητές του συστήματος αυτού.

Οι επιθέσεις αυτές μπορεί να στοχεύουν στη μεγάλη αύξηση του φόρτου της Κεντρικής Μονάδας Επεξεργασίας (CPU) του συστήματος, στην επανεκκίνηση του συστήματος ή στη γενικότερη κατάρρευση του δικτύου. Οι επιθέσεις αυτού του είδους είναι ιδιαίτερα διαδεδομένες στο Διαδίκτυο, με αποτέλεσμα τα τελευταία χρόνια πολλοί δικτυακοί τόποι να έχουν υποστεί Επίθεση Άρνησης Υπηρεσίας. Σκοπός τους είναι η κακοπροαίρετη κατανάλωση πόρων των υπολογιστικών συστημάτων, των δικτύων ή των τελικών χρηστών, οι οποίοι αλλιώς θα χρησιμοποιούνταν στην εξυπηρέτηση των χρηστών, έτσι ώστε να αποτραπεί, ή τουλάχιστον να υποβαθμιστεί σοβαρά η παροχή υπηρεσιών στους χρήστες αυτούς. Τα είδη των πόρων οι οποίοι καταναλώνονται ως επί το πλείστον σε τέτοιες επιθέσεις μπορεί να είναι δικτυακό εύρος ζώνης (network bandwidth), επεξεργαστική ισχύς,

μνήμη, χώρος στους δίσκους, αλλά και πόροι διαφόρων εφαρμογών, όπως για παράδειγμα διαθέσιμες συνδέσεις ενός δικτυακού τόπου.

Υπάρχουν δύο κατηγορίες DoS επιθέσεων: οι λογικές επιθέσεις και οι επιθέσεις «πλημμύρας» (flooding attacks). Οι επιθέσεις της πρώτης κατηγορίας σπαταλούν τους πόρους του συστήματος, κάνοντας χρήση κάποιου προγραμματιστικού λάθους στο λογισμικό του συστήματος. Οι επιθέσεις της δεύτερης κατηγορίας είναι συνηθέστερες και έχουν ως κοινό χαρακτηριστικό την αποστολή στο θύμα (τον εξυπηρετητή (server) που αποτελεί τον στόχο της επίθεσης) ενός τόσο μεγάλου αριθμού πλαστών αιτημάτων σύνδεσης ώστε δεν μπορεί πλέον να διαχειριστεί το παραμικρό και διακόπτει τη λειτουργία του. Με άλλα λόγια, το θύμα καταναλώνει τους πόρους του προκειμένου να επεξεργαστεί τις αιτήσεις του επιτιθέμενου με αποτέλεσμα να μην είναι σε θέση να εξυπηρετήσει τις αιτήσεις των νόμιμων χρηστών. Κάθε υπολογιστικό σύστημα που είναι συνδεδεμένο στο Διαδίκτυο και δεν έχει προφυλαχθεί σωστά, μπορεί να γίνει στόχος τέτοιων επιθέσεων. Η διάρκεια των επιθέσεων άρνησης υπηρεσίας, μπορεί σε γενικές γραμμές να ποικίλλει, από λίγα λεπτά της ώρας μέχρι και ολόκληρες ημέρες.

1.3.2 Είδη DoS επιθέσεων

1.3.2.1 Ping of Denial

Πρόκειται για την παλαιότερη και πιο διαδεδομένη μορφή επίθεσης. Για την επίθεση αυτή ο επιτιθέμενος αποστέλλει πάρα πολλά μηνύματα ping τα οποία ο server είναι υποχρεωμένος να απαντήσει, δαπανώντας φυσικά υπολογιστική ισχύ και bandwidth. Αν τα μηνύματα ping είναι πάρα πολλά τότε ο αποδέκτης τους καθυστερεί σημαντικά στην εκτέλεση άλλων εργασιών διότι είναι πολύ απασχολημένος στέλνοντας αποκρίσεις στα ping μηνύματα, ενώ αν ο φόρτος γίνει πολύ μεγάλος είναι πιθανό να διακόψει τελείως τη λειτουργία του.

1.3.2.2 Επιθέσεις που εκμεταλλεύονται αδυναμίες του πρωτοκόλλου ICMP

Το πρωτόκολλο ICMP [11] χρησιμοποιείται για την επικοινωνία μεταξύ υπολογιστών. Το ICMP μεταφέρει πληροφορίες οι οποίες ενημερώνουν κάθε υπολογιστή για την κατάσταση της σύνδεσής του με άλλα μηχανήματα και είναι απαραίτητο για τη σωστή λειτουργία των δικτύων. Ο επιτιθέμενος στέλνει στο θύμα

μέσω του ICMP ένα από τα ακόλουθα μηνύματα μέσω των οποίων δηλώνει στο θύμα πως υπάρχει κάποιο πρόβλημα ώστε αυτό να διακόψει στη συνέχεια τη σύνδεσή του:

- Destination Unreachable
- Time To Live Exceeded
- Parameter Problem
- Packet Too Big

Η διεύθυνση επιστροφής (return address) των πακέτων ICMP «πλαστογραφείται», ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου.

1.3.2.3 E-mail bombing

Επιτυγχάνεται αποστέλλοντας μεγάλο αριθμό μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), κυρίως μεγάλου μεγέθους, σε υπολογιστές οι οποίοι διαχειρίζονται το ηλεκτρονικό ταχυδρομείο. Εκ πρώτης όψεως δε δίνει την εντύπωση ότι μπορεί μια επίθεση αυτού του είδους να επιφέρει σοβαρά αποτελέσματα, η αλήθεια είναι όμως ότι μπορεί μια τέτοια επίθεση να είναι ιδιαίτερα αποτελεσματική. Αποτέλεσμα είναι ο φόρτος των εργασιών διαχείρισής τους αλλά να οδηγήσει το όλο σύστημα σε κατάρρευση.

1.3.2.4 UDP Flooding

Ο επιτιθέμενος αποστέλλει UDP πακέτα [12] σε τυχαία πόρτα του θύματος, το οποίο απαντά με ένα ICMP πακέτο «destination unreachable». Όσο αυξάνει ο αριθμός των πακέτων, τόσο μεγαλύτερος γίνεται και ο φόρτος για το μηχάνημα το οποίο επιβαρύνεται όλο και περισσότερο με τελικό αποτέλεσμα την κατάρρευση του συστήματος.

1.3.2.5 IP Smurf

Στην περίπτωση της επίθεσης IP Smurf, δύο είναι τα στοιχεία στα οποία αυτή η επίθεση βασίζεται: η χρήση των πλαστών ICMP echo αιτήσεων και η κατεύθυνση των πακέτων προς πολλαπλές IP διευθύνσεις (broadcasting).

Το Πρωτόκολλο Μηνυμάτων Ελέγχου του Διαδικτύου (Internet Control Message Protocol – ICMP), χρησιμοποιείται προκειμένου να διαχειρίζεται τα λάθη και για την ανταλλαγή μηνυμάτων ελέγχου. Το ICMP μπορεί να χρησιμοποιηθεί για να καθορίσει εάν ένα μηχάνημα που είναι συνδεδεμένο στο Διαδίκτυο μπορεί να

αποκρίνεται στις αιτήσεις. Προκειμένου να το κάνει αυτό, το ICMP στέλνει μια αίτηση (echo request) στο μηχάνημα αυτό. Εάν το μηχάνημα λάβει αυτό το πακέτο, θα επιστρέψει ένα ICMP echo πακέτο απάντησης. Μια πολύ συνηθισμένη υλοποίηση αυτής της διαδικασίας είναι η εντολή «ping», η οποία συμπεριλαμβάνεται σε πολλά λειτουργικά συστήματα και πακέτα δικτυακού λογισμικού. Το ICMP χρησιμοποιείται προκειμένου να μεταφέρει πληροφορίες κατάστασης και λαθών, συμπεριλαμβανομένων και ειδοποιήσεις για συμφόρηση στο δίκτυο ή άλλα προβλήματα μεταφοράς δεδομένων σε ένα δίκτυο.

Στα δίκτυα IP, ένα πακέτο μπορεί να κατευθύνεται προς ένα μόνο μηχάνημα ή να εκπέμπεται προς ένα ολόκληρο δίκτυο (broadcast). Όταν συμβαίνει η δεύτερη περίπτωση, το πακέτο παραδίδεται σε όλους τους υπολογιστές που είναι συνδεδεμένοι στο δίκτυο αυτό.

Σε μια επίθεση smurf, οι επιτιθέμενοι χρησιμοποιούν ICMP echo αιτήσεις οι οποίες κατευθύνονται προς πολλές IP διευθύνσεις. Συνήθως τρία μέρη εμπλέκονται σε αυτού του είδους τις επιθέσεις: ο επιτιθέμενος, ο ενδιάμεσος και το θύμα (πρέπει να σημειωθεί ότι και ο ενδιάμεσος μπορεί κάλλιστα να αποτελεί θύμα της επίθεσης).

Ο ενδιάμεσος λαμβάνει μια ICMP echo αίτηση η οποία προορίζεται σε πολλές IP διευθύνσεις, συνήθως ενός δικτύου. Εάν ο ενδιάμεσος δε φιλτράρει με κάποιο τρόπο την ICMP κίνηση που αποστέλλεται προς τους υπολογιστές ενός δικτύου, το αποτέλεσμα θα είναι πολλοί από τους υπολογιστές αυτούς να λάβουν το πακέτο αυτό και να απαντήσουν με ένα αντίστοιχο πακέτο. Στην περίπτωση που όλοι οι υπολογιστές ενός δικτύου απαντήσουν σε αυτή την αίτηση, το αποτέλεσμα μπορεί να είναι να προκληθεί σοβαρή συμφόρηση στο δίκτυο, ακόμη και διακοπή της λειτουργίας του.

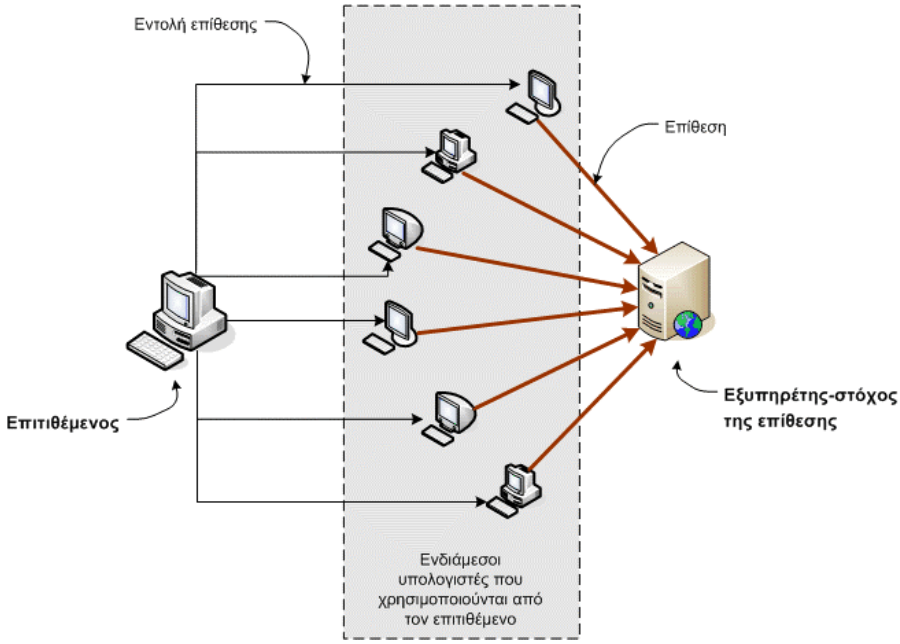
Όταν οι επιτιθέμενοι δημιουργούν τέτοια πακέτα, δε χρησιμοποιούν την IP διεύθυνση του δικού τους μηχανήματος ως διεύθυνση πηγής, αλλά αντίθετα. δημιουργούν πλαστά πακέτα τα οποία περιέχουν ως διεύθυνση πηγής την υποκλεμμένη διεύθυνση του υποψήφιου θύματος. Το αποτέλεσμα είναι ότι όταν όλοι όσοι λάβουν τις ICMP αιτήσεις απαντήσουν σε αυτές, απαντούν στην ουσία στο μηχάνημα του θύματος. Το θύμα υφίστανται δικτυακή συμφόρηση η οποία μπορεί να οδηγήσει σε κατάρρευση του δικτύου, ενώ ταυτόχρονα η επίδοση του υποβαθμίζεται, και τελικά να δε μπορεί να παρέχει στους χρήστες του τις απαιτούμενες υπηρεσίες.

1.3.2.6 Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας

Όταν σε μια επίθεση άρνησης υπηρεσίας συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις Άρνησης Υπηρεσίας (Distributed Denial of Service ή DDoS attacks). Στις επιθέσεις αυτού του είδους υπάρχει ένα πλήθος από επιτιθέμενους οι οποίοι συνεργάζονται (πολλές φορές και εν αγνοία τους) ώστε να δημιουργήσουν μια μεγάλης κλίμακας επίθεση άρνησης υπηρεσίας. Ο επιτιθέμενος αρχικά αποκτά πρόσβαση σε άλλους υπολογιστές, οι οποίοι ονομάζονται σκλάβοι (slaves) και τους οποίους χρησιμοποιεί ώστε να στέλνουν συντονισμένα με υψηλό ρυθμό κίνηση στο θύμα. Οι σκλάβοι αυτοί συμμετέχουν άθελά τους στην επίθεση αυτή, και η δράση τους καθορίζεται από τον αρχικό επιτιθέμενο.

Η επίθεση αυτή γίνεται ακόμα πιο έντονη στην περίπτωση που χρησιμοποιούνται τα λεγόμενα «κάτοπτρα» (reflectors). Οι reflectors, είναι μηχανήματα τα οποία συνήθως απαντάνε σε ερωτήσεις (queries), π.χ. DNS εξυπηρετητές [13] και στα οποία ο επιτιθέμενος στέλνει αιτήσεις με την IP διεύθυνση του θύματος την οποία έχει προηγουμένως υποκλέψει (spoofed). Το αποτέλεσμα είναι οι reflectors να απαντάνε στις αιτήσεις του θύματος, έτσι ώστε αυτό να κατακλυστεί από τις απαντήσεις αυτές και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών.

Πριν την εξαπόλυση μιας επίθεσης, οι επιτιθέμενοι όπως είπαμε παραβιάζουν κάποια μηχανήματα, συνήθως εξυπηρετητές με συνδέσεις υψηλού εύρους ζώνης με το Διαδίκτυο, και εγκαθιστούν σε κάθε έναν από αυτούς ειδικό λογισμικό το οποίο βοηθά στη δημιουργία της επίθεσης. Το λογισμικό αυτό λοιπόν, μετατρέπει σε σκλάβους τα συγκεκριμένα μηχανήματα, με αποτέλεσμα αυτά να περιμένουν τις εντολές του «αρχηγού» - επιτιθέμενου, προκειμένου να στέλνουν αιτήσεις σε ένα θύμα, το οποίο έχει προσδιοριστεί από τον «αρχηγό». Από τη στιγμή που το απαραίτητο λογισμικό έχει εγκατασταθεί στους σκλάβους, ο επιτιθέμενος έχει τη δυνατότητα να εξαπολύσει επιθέσεις εναντίον οποιουδήποτε θύματος.



Σχήμα 3: Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας

Οι επιτιθέμενοι όπως αναφέρθηκε μπορούν να χρησιμοποιήσουν πλαστές IP διευθύνσεις, προκειμένου προσδώσουν περισσότερο ύπουλο χαρακτήρα στην ενέργειά τους αυτή. Παράδειγμα μιας τέτοιας περίπτωσης, είναι το λογισμικό που έχει εγκατασταθεί σε ένα σκλάβο, να αντικαθιστά την πραγματική Διαδικτυακή διεύθυνσή του με μια πλαστή διεύθυνση, καθιστώντας εξαιρετικά δύσκολο το γεγονός να μπορέσει κάποιος να εντοπίσει το γεγονός ότι η συγκεκριμένη επίθεση ξεκίνησε από το συγκεκριμένο σκλάβο, πόσο μάλλον από τον αρχικό εισβολέα.

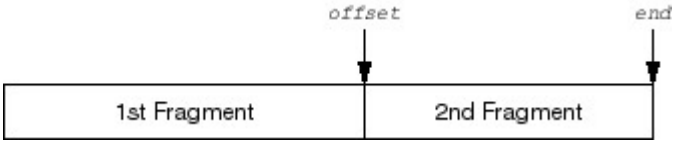
1.3.2.7 Επίθεση Teardrop

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν τα πακέτα τεμαχίζονται από το TCP/IP, προστίθεται σε αυτά κάποια πληροφορία ελέγχου έτσι ώστε ο παραλήπτης να επιβεβαιώσει πως αυτά έφτασαν δίχως σφάλματα. Σε περίπτωση που διαπιστωθεί κάποιο πρόβλημα, τότε ο παραλήπτης επικοινωνεί με τον αποστολέα και του ζητάει να ξαναστείλει τα πακέτα που αλλοιώθηκαν κατά τη μεταφορά.

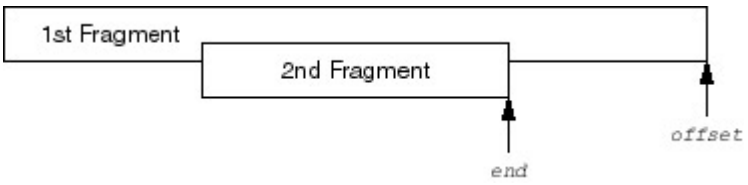
Εκμεταλλευόμενος αυτό το χαρακτηριστικό, ο επιτιθέμενος στέλνει συνεχώς πακέτα με λανθασμένα στοιχεία ελέγχου. Έτσι, υποχρεώνει τον παραλήπτη να σπαταλά υπολογιστική ισχύ και bandwidth, ζητώντας συνεχώς την επανάληψη της αποστολής τους.

Η διαδικασία επανασυναρμολόγησης των τεμαχισμένων πακέτων, θεωρεί ως φυσιολογική συμπεριφορά το γεγονός τα διάφορα τεμάχια ενός πακέτου να ευθυγραμμίζονται με τέτοιο τρόπο ώστε τα δεδομένα στην αρχή ενός τεμαχίου, να ακολουθούν τα δεδομένα που βρίσκονται στο τέλος του προηγούμενου τεμαχίου. Ενώ όμως αυτή είναι η περίπτωση όπου όλα βαίνουν φυσιολογικά, σε μια επίθεση τύπου Teardrop, τα τεμάχια, είναι σκοπίμως κατασκευασμένα με τέτοιο τρόπο ώστε να δημιουργούν προβλήματα κατά τη διαδικασία επανασυναρμολόγησής τους.

Η ρουτίνα αντιγραφής της μνήμης (memory copy routine) [14], υπολογίζει το μήκος των προς αντιγραφή δεδομένων, ως την τιμή η οποία προκύπτει αφαιρώντας από τον δείκτη τέλους (*end* pointer) την τιμή του δείκτη θέσης αρχής του δεύτερου τεμαχίου (*offset* pointer). Κάτω από φυσιολογικές συνθήκες το αποτέλεσμα θα είναι ένας θετικός ακέραιος αριθμός, όπως παραστατικά φαίνεται και στο επόμενο σχήμα.



Αντίθετα, στην περίπτωση της επίθεσης τύπου Teardrop, αποστέλλεται ένα τεμάχιο, το οποίο έχει ως σκοπό να είναι η τιμή του δείκτη τέλους μικρότερη από ότι η τιμή του δείκτη θέσης αρχής του δεύτερου τεμαχίου. Αυτό επιτυγχάνεται εξασφαλίζοντας ότι το δεύτερο τεμάχιο ορίζει μια θέση αρχής η οποία βρίσκεται μεταξύ των δεδομένων του πρώτου τεμαχίου και έχει τέτοιο μήκος ώστε το τέλος των δεδομένων του δεύτερου τεμαχίου να βρίσκεται μέσα στα δεδομένα του πρώτου, όπως φαίνεται και στο σχήμα:



Όταν κατά τη διαδικασία επανασυναρμολόγησης το IP επιχειρεί μια αντιγραφή μνήμης των τεμαχισμένων δεδομένων μέσα στον ενταμιευτή ο οποίος χρησιμοποιείται για να αποθηκεύσει ολόκληρο το πακέτο, το υπολογιζόμενο μήκος των δεδομένων προς αντιγραφή (δείκτης θέσης τέλους μείον τον δείκτη θέσης αρχής) παίρνει αρνητική τιμή. Η συνάρτηση αντιγραφής περιμένει μια τιμή τύπου ακέραιου χωρίς πρόσημο (unsigned integer), δέχεται όμως μία αρνητική τιμή, η μετατροπή της οποίας σε ακέραιο χωρίς πρόσημο αντιστοιχεί σε έναν πάρα πολύ μεγάλο θετικό

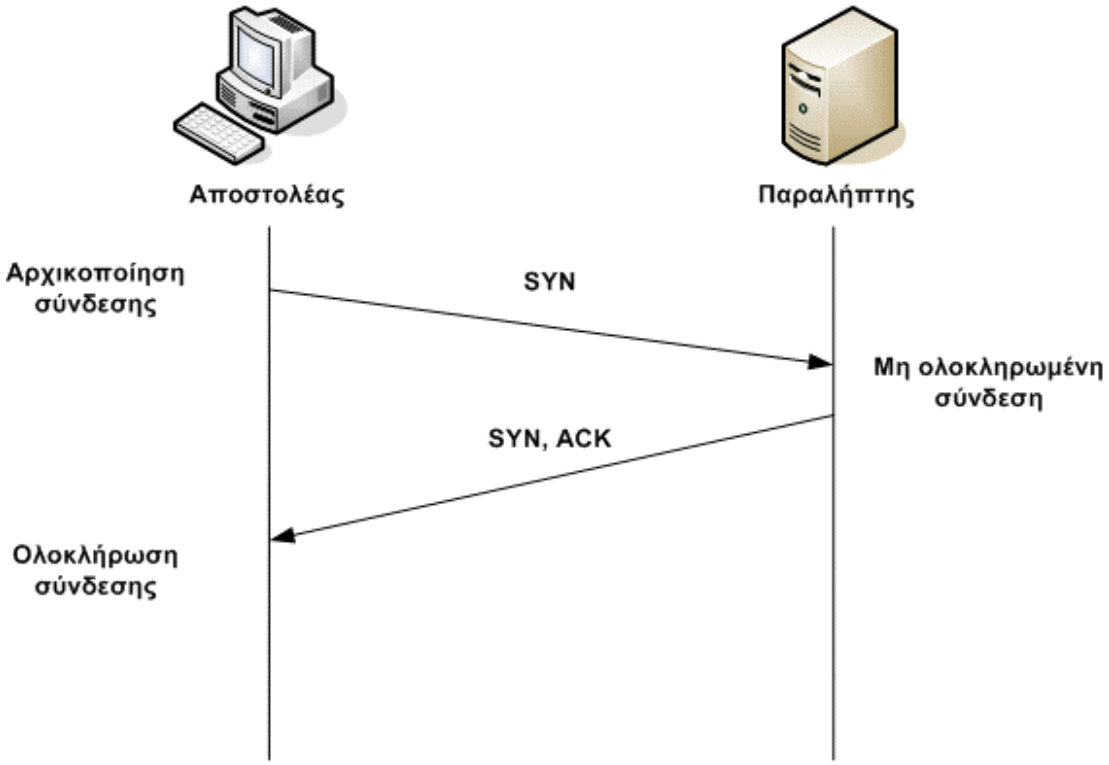
ακέραιο. Το αποτέλεσμα μιας τέτοιας ενέργειας, οδηγεί συνήθως σε δημιουργία προβλήματος στη στοίβα δεδομένων, αποτυχία του προγράμματος υλοποίησης του IP, ακόμα και σε κατάρρευση ολόκληρου του συστήματος.

1.3.2.8 SYN Flooding

Ένα από τα πιο δημοφιλή είδη flooding DoS επιθέσεων είναι η TCP SYN flooding [15] επίθεση.

Το πρωτόκολλο SYN-ACK όπως είπαμε αποτελεί τη βάση κάθε έναρξης σύνδεσης μέσα στο Internet. Θυμίζουμε ότι όταν ένας Η/Υ θέλει να συνδεθεί με έναν άλλο του αποστέλλει ένα πακέτο SYN στο οποίο ο server απαντάει με ένα πακέτο ACK (acknowledge - επιβεβαίωσης). Όταν ο Η/Υ που ζήτησε τη σύνδεση λάβει το ACK θεωρεί ότι η σύνδεση έχει ολοκληρωθεί και αρχίζει τη μετάδοση των δεδομένων.

Σε μια επίθεση SYN Flooding ο επιτιθέμενος στέλνει συνεχώς πακέτα SYN αλλά όχι ACK (επιβεβαίωσης). Έτσι, ο εξυπηρετητής που δέχεται την επίθεση είναι υποχρεωμένος για περιμένει για κάποιο χρονικό διάστημα την επιβεβαίωση, δεσμεύοντας φυσικά με την αναμονή αυτή ένα μέρος των διαθέσιμων πόρων του. Αν η επιβεβαίωση δεν έρθει ποτέ, το θύμα δεν αποδεσμεύει τους πόρους του. Γι' αυτό, ο επιτιθέμενος συνήθως στέλνει έναν συνεχώς αυξανόμενο αριθμό πακέτων SYN, δεσμεύοντας όλο και περισσότερους πόρους του θύματος στην αναμονή των επιβεβαιώσεών τους και οδηγώντας σιγά σιγά τον server του θύματος στην κατάρρευση. Αυτό συμβαίνει γιατί όλες αυτές οι ημι-ανοιχτές συνδέσεις συσσωρεύονται στον ενταμιευτή του θύματος, ο οποίος από κάποιο σημείο και μετά θα είναι πλήρης με αποτέλεσμα το σύστημα να μην είναι σε θέση να δεχτεί καμία καινούργια σύνδεση μέχρι ο ενταμιευτής να αδειάσει. Βέβαια, όπως έχει ήδη αναφερθεί, υπάρχει κάποιο χρονικό διάστημα για το οποίο ο εξυπηρετητής θα περιμένει να δεχτεί την επιβεβαίωση της σύνδεσης, μετά το πέρας του οποίου οι ημι-ανοιχτές συνδέσεις απορρίπτονται. Για το λόγο αυτό, ο επιτιθέμενος στέλνει συνεχώς νέες αιτήσεις σύνδεσης με ρυθμό ταχύτερο από τον ρυθμό με τον οποίο το σύστημα απορρίπτει τις αιτήσεις που βρίσκονται στην αναμονή. Αυτού του είδους οι επιθέσεις πραγματοποιούνται ως επί το πλείστον εναντίον διακομιστών παγκόσμιου ιστού (web servers).



Σχήμα 4: Ημιτελής χειραψία τριών σημείων – Επίθεση Άρνησης Υπηρεσίας

1.3.3 Σημαντικότητα των Επιθέσεων Άρνησης Υπηρεσίας

Γενικότερα, η προστασία των συστημάτων από DoS επιθέσεις θεωρείται ύψιστης σημασίας. Ένα στοιχείο που επιβεβαιώνει την παραπάνω πρόταση είναι το γεγονός ότι όταν λαμβάνει χώρα μια τέτοια επίθεση, σημαντικά και κρίσιμα στοιχεία ενός δικτύου, όπως για παράδειγμα, δρομολογητές, γέφυρες, βάσεις δεδομένων, firewalls, σταματούν τη λειτουργία τους, με άμεσο αποτέλεσμα οι απομακρυσμένοι χρήστες να μη μπορούν να συνδεθούν με τους υπολογιστές του ενδιαφέροντός τους. Παράλληλα, σε εταιρικό επίπεδο, οι εταιρείες δε μπορούν να προσφέρουν τις απαραίτητες πληροφορίες στους πελάτες τους, με αποτέλεσμα οι δεύτεροι να στραφούν σε άλλες λύσεις. Με άλλα λόγια, η πληροφορία δε μπορεί να μεταδοθεί.

Οι επιθέσεις αυτές θεωρούνται γενικότερα αρκετά εύκολο να πραγματοποιηθούν από κάποιον όχι ιδιαίτερα έμπειρο χρήστη, καταβάλλοντας σχετικά μικρή προσπάθεια, ενώ ταυτόχρονα είναι πολύ πιθανό η προσπάθεια αυτή των επιτιθέμενων να στεφθεί με επιτυχία και να δημιουργηθούν πολιτικά, οικονομικά και κοινωνικά προβλήματα. Πρόσφατες έρευνες [16], [17] έδειξαν πως το 40% των

επιθέσεων που λαμβάνουν χώρα είναι Επιθέσεις Άρνησης Υπηρεσίας, πράγμα που σημαίνει ότι το είδος αυτό των επιθέσεων είναι δημοφιλέστερο από οποιοδήποτε άλλο.

Παράλληλα, το κόστος που υφίστανται τα συστήματα όταν υπόκεινται σε επιθέσεις αυτού του είδους ανέρχεται σε πολλά εκατομμύρια, ακόμα και δισεκατομμύρια δολάρια. Σύμφωνα με έρευνα του έτους 2002 (CSI/FBI) [16] το μέσο κόστος για το θύμα το οποίο υφίσταται μια επίθεση άρνησης υπηρεσίας είναι μεγαλύτερο από ένα εκατομμύριο δολάρια, ενώ ταυτόχρονα αποκτά αρνητική δημοτικότητα και καταστρέφεται η φήμη του. Από το Σεπτέμβριο του έτους 1996, πολλές δεκάδες δικτυακών τόπων υπέστησαν επίθεση άρνησης υπηρεσίας, ενώ ειδικότερα την εβδόμη Φεβρουαρίου του 2000 πολλές μεγάλες και σημαντικές εταιρείες υπήρξαν θύματα μιας τέτοιας επίθεσης. Το Yahoo! δέχτηκε ένα κατακλυσμό από δεδομένα, που έφτασε σε ρυθμό ακόμα και το ένα gigabit το δευτερόλεπτο, γεγονός που οδήγησε στην κατάρρευση του συστήματος για τρεις ώρες. Την επόμενη μέρα, πολλές ηλεκτρονικές επιχειρήσεις (e-business) δέχτηκαν παρόμοιες επιθέσεις, μεταξύ των οποίων συμπεριλαμβάνονται τα Buy.com, Stamps.com, CNN.com, Amazon.com, ακόμα και το MSN. Οι επιθέσεις αυτές αιφνιδίασαν τους παραπάνω δικτυακούς τόπους (sites) κατακλύζοντάς τους με φαινομενικά νόμιμη κίνηση, δια μέσου της οποίας εμπόδιζαν ή καθυστερούσαν την πρόσβαση των χρηστών στους τόπους αυτούς.

Μετά από τα παραπάνω γεγονότα, η ενασχόληση των μέσων με το θέμα συνετέλεσε στο να αυξηθεί η δημόσια επαγρύπνηση επί του θέματος, αλλά ταυτόχρονα αύξησε το ενδεχόμενο για τη δημιουργία νέων επιθέσεων. Ιδιαίτερα δε ανησυχητικό είναι το γεγονός πως το είδος αυτό των επιθέσεων γίνεται όλο και πιο δημοφιλές, ενώ συνεχώς εμφανίζονται νέα είδη επιθέσεων άρνησης υπηρεσίας. Σήμερα, περισσότερο από ποτέ, οι εταιρείες οι οποίες δραστηριοποιούνται επιχειρηματικά μέσω εσωτερικών δικτύων ή του Διαδικτύου, πρέπει να είναι προετοιμασμένες για μια τέτοια επίθεση.

Αν και πολλοί πίστευαν πως με τη βοήθεια ενός firewall ή ενός συστήματος εντοπισμού επιθέσεων (IDS) θα είχαν καλύψει τις ανάγκες τους όσον αφορά στην ασφάλεια, η εμπειρία απέδειξε πως ένας τέτοιος ισχυρισμός δεν ισχύει, δεδομένου ότι ένα μόνο firewall δεν μπορεί να προσφέρει 100% προστασία από τις επιθέσεις. Ένας λόγος για τον οποίο δεν είναι εύκολο να εξαλειφθούν οι επιθέσεις άρνησης υπηρεσίας είναι το γεγονός ότι προκειμένου να γίνει κάτι τέτοιο απαιτούνται μετατροπές-

διορθώσεις στα πρωτόκολλα επικοινωνίας, κάτι που είναι πολύ δύσκολο να πραγματοποιηθεί, δεδομένου ότι οποιαδήποτε τροποποίηση στη στοίβα πρωτοκόλλων του TCP/IP θα έπρεπε να υιοθετηθεί από ολόκληρη την κοινότητα του Διαδικτύου. Αξιοσημείωτο είναι επίσης και το γεγονός ότι στις επιθέσεις αυτού του είδους είναι ιδιαίτερα δύσκολο να εντοπιστεί αυτός που πραγματικά εξαπολύει την επίθεση. Επιπλέον, ο ρυθμός με τον οποίο εμφανίζονται καινούργιες απειλές για την ασφάλεια των συστημάτων είναι εκπληκτικός με αποτέλεσμα να καθίστανται ανεπίκαιρες οι μέχρι τώρα γνωστές αρχιτεκτονικές ασφάλειας και τρόποι αντιμετώπισής τους. Για το λόγο αυτό, οι σημερινές πολιτικές ασφάλειας δικτύων και τα αντίστοιχα συστήματα, απαιτούν συνεχή έλεγχο και ενημέρωση προκειμένου να παραμένουν αποτελεσματικά. Από τη στιγμή που η πρόσβαση στο Διαδίκτυο εξακολουθεί να επεκτείνεται συνεχώς και η ποσότητα και ταχύτητα των δεδομένων που μεταφέρεται ολοένα και αυξάνεται, είναι αυτονόητο πως πρέπει να υιοθετηθούν νέα μέτρα ασφάλειας.

Στη συνέχεια της αναφοράς, παρουσιάζουμε και αξιολογούμε δύο αλγόριθμους εντοπισμού ανωμαλιών οι οποίοι χρησιμοποιούνται για τον εντοπισμό TCP SYN επιθέσεων: ένας αλγόριθμος προσαρμοζόμενου κατωφλιού (adaptive threshold) και μια συγκεκριμένη εφαρμογή του αθροιστικού αλγόριθμου ελέγχου (CUSUM) για τον εντοπισμό σημείου ανωμαλίας. Σκοπός μας είναι να αναλύσουμε τα πλεονεκτήματα και τα μειονεκτήματα των αλγορίθμων αυτών όσον αφορά στην πιθανότητα εντοπισμού, στο ποσοστό των λανθασμένων σημάνσεων συναγερμού και στην καθυστέρηση εντοπισμού. Επίσης, μελετούμε τον τρόπο με τον οποίο τα παραπάνω χαρακτηριστικά επηρεάζονται από τις παραμέτρους του εκάστοτε αλγόριθμου αλλά και από το είδος των επιθέσεων. Σκοπός αυτής της μελέτης είναι να βοηθήσει στην κατάλληλη ρύθμιση των παραμέτρων των αλγορίθμων, έτσι ώστε να ικανοποιούνται συγκεκριμένες απαιτήσεις επίδοσης (performance requirements).

2 Σχετικές Εργασίες

Στα πλαίσια της προσπάθειας αντιμετώπισης των Επιθέσεων Άρνησης Υπηρεσίας, πραγματοποιήθηκαν πολλές μελέτες και έγιναν πολλές προσπάθειες, πολλές από τις οποίες σκοπό έχουν τον εντοπισμό ανωμαλιών, κάτι που αποτελεί σοβαρή ένδειξη για την παρουσία επίθεσης σε ένα δίκτυο.

2.1 Το εργαλείο RRD (Round Robin Database)

Ένα εργαλείο το οποίο υλοποιήθηκε, χρησιμοποιήθηκε και προτάθηκε από τη WebTV είναι το RRD (Round Robin Database) tool [18], [19]. Το εργαλείο αυτό αποθηκεύει και εμφανίζει δεδομένα χρονοσειρών. Επιπλέον, εντοπίζει ανώμαλη συμπεριφορά στην εξερχόμενη κίνηση που υπάρχει μεταξύ δύο μεγάλων κέντρων δεδομένων, χρησιμοποιώντας τους αλγόριθμους Holt Winters και Exponential Smoothing. Στην ουσία υλοποιεί ένα μαθηματικό μοντέλο προκειμένου να επιτευχθεί αυτόματη αναγνώριση ανώμαλης συμπεριφοράς από το λογισμικό παρακολούθησης της κίνησης.

Το μοντέλο που προτείνεται αποτελείται από τρία τμήματα, καθένα από τα οποία βασίζεται στο προηγούμενό του.

- Έναν αλγόριθμο που να προβλέπει τις τιμές μιας χρονοσειράς για την επόμενη χρονική στιγμή στο μέλλον
- Ένα μέτρο της απόκλισης μεταξύ των προβλεπόμενων και των παρατηρούμενων τιμών
- Ένα μηχανισμό ο οποίος αποφασίζει εάν και πότε μια παρατηρούμενη τιμή ή ακολουθία από παρατηρούμενες τιμές έχει μεγάλη απόκλιση από τις προβλεπόμενες τιμές.

Το προτεινόμενο αυτό μοντέλο αποτελεί μια επέκταση της πρόβλεψης με τη βοήθεια του αλγόριθμου Holt Winters.

2.1.1 Exponential Smoothing

Είναι ένας απλός αλγόριθμος ο οποίος προβλέπει την επόμενη τιμή σε μια χρονοσειρά, δεδομένης της τωρινής τιμής και της τωρινής πρόβλεψης [20]. Έστω $\hat{y}_{t+1}$ ότι είναι η προβλεπόμενη τιμή για τη χρονική στιγμή t + 1. Τότε: $\hat{y}_{t+1} = ay_t + (1-a)\hat{y}_t$.

Η πρόβλεψη, είναι στην ουσία ένας σταθμισμένος μέσος όλων των προηγούμενων παρατηρήσεων της χρονοσειράς. Η βάση του συλλογισμού αυτού του αλγόριθμου είναι ότι η τωρινή τιμή είναι αυτή η οποία περιέχει τις περισσότερες πληροφορίες σχετικά με την πρόβλεψη της επόμενης τιμής, καθώς επίσης και το ότι η σημασία των

προηγούμενων παρατηρήσεων μειώνεται εκθετικά όσο παλιότερη είναι η παρατήρηση αυτή. Είναι ένας αυξητικός αλγόριθμος, με την έννοια ότι η επόμενη πρόβλεψη γίνεται ενημερώνοντας στην ουσία την τωρινή πρόβλεψη με την τωρινή παρατηρούμενη τιμή.

Η παράμετρος a $(0 < a < 1)$, καθορίζει το ρυθμό μείωσης $(1-a)$ καθώς και τη σημασία η οποία δίνεται στην τωρινή τιμή.

2.1.2 Holt Winters

Αποτελεί έναν πιο περίπλοκο αλγόριθμο ο οποίος βασίζεται στο Exponential Smoothing. Ο αλγόριθμος Holt Winters [20] βασίζεται στο συλλογισμό ότι η προς μελέτη χρονοσειρά μπορεί να αναλυθεί σε τρία μέρη: ένα βασικό σήμα, μια γραμμική τάση και μια εποχιακή επίδραση. Ο αλγόριθμος υποθέτει πως κάθε ένα από τα τμήματα αυτά εξελίσσεται μέσα στο χρόνο. Η τελική πρόβλεψη είναι το άθροισμα των τριών αυτών τμημάτων:

$\hat{y}_{t+1} = a_t + b_t + c_{t+1-m}$

Οι σχέσεις ενημέρωσης των τριών συστατικών είναι:

- Βασικό Σήμα:

$$a_t = \alpha(y_t - c_{t-m}) + (1-\alpha)(a_{t-1} + b_{t-1})$$

- Γραμμική Τάση:

$$b_t = \beta(a_t - a_{t-1}) + (1-\beta)b_{t-1}$$

- Εποχιακή Επίδραση:

$$c_t = \gamma(y_t - a_t) + (1-\gamma)c_{t-m}$$

Όπως και στο Exponential Smoothing, η ανανέωση των συντελεστών (τμημάτων) γίνεται χρησιμοποιώντας ένα μέσο όρο της πρόβλεψης και μιας εκτίμησης ο οποία αποκτάται αποκλειστικά και μόνο με βάση την παρατηρούμενη τιμή y_t και εξαρτάται από τους συντελεστές α, β, γ, $0 < \alpha, \beta, \gamma < 1$. Μεγάλες τιμές στις παραμέτρους αυτές σημαίνει ότι ο αλγόριθμος βασίζεται περισσότερο σε πρόσφατες παρατηρήσεις της χρονοσειράς προκειμένου να κάνει προβλέψεις, ενώ μικρότερες τιμές σημαίνουν πως ο αλγόριθμος δίνει μεγαλύτερη βαρύτητα σε παλαιότερες τιμές της χρονοσειράς. Η παράμετρος m αποτελεί την περίοδο της εποχιακής επίδρασης.

Στα πλαίσια της ίδιας εργασίας, περιγράφεται το Cricket [21], ένα front-end εργαλείο για το RRD, το οποίο διαχειρίζεται πολλαπλές χρονοσειρές μέσω του RRD. Χαρακτηριστικό του είναι η ομαδοποίηση χρονοσειρών με βάση κοινές μεταβλητές, χαρακτηριστικά γραφήματος ή άλλες ιδιότητες. Ο συλλέκτης δεδομένων του Cricket παρέχει μηχανισμούς για συλλογή δεδομένων και παροχή αυτών στο RRD. Το συλλέκτης αυτός διαχειρίζεται επίσης τα SNMP calls [22] και τα event logs. Ο δημιουργός γραφημάτων παράγει γραφήματα χρονοσειρών χρησιμοποιώντας τις δυνατότητες του RRD σε πραγματικό χρόνο και στη συνέχεια τα παρουσιάζει με τη μορφή ιστοσελίδων.

Τέλος, το Cricket παρέχει ένα μηχανισμό σημάνσεως συναγερμού, κάτι το οποίο δεν προσφέρει το RRD. Έτσι, παρέχει δυνατότητα παρακολούθησης χρονοσειρών και σήμανσης συναγερμού στην περίπτωση που κάποια τιμή υπερβαίνει ένα προκαθορισμένο κατώφλι.

2.1.3 Προσπάθεια Εντοπισμού Ανωμαλιών με τη Χρήση Χρονοσειρών- IBM

Στα πλαίσια της εργασίας αυτής [23], έγινε μελέτη της προληπτικού εντοπισμού ανωμαλιών για ένα διακομιστή παγκόσμιου ιστού, όπου έγινε ανάλυση χρονοσειρών των οποίων οι μετρήσεις ήταν το πλήθος των http εργασιών ανά δευτερόλεπτο. Χρησιμοποιήθηκε ένα στατιστικό μοντέλο το οποίο λάμβανε υπόψη του την περιοδικότητα και τη γενικότερη τάση που τυχόν παρουσίαζε το σήμα. Η μοντελοποίηση έγινε χρησιμοποιώντας τον αλγόριθμο Holt Winters, ενώ οι συσχετίσεις στο χρόνο μοντελοποιήθηκαν χρησιμοποιώντας ένα μοντέλο αυτοπαλινδρόμησης (autoregressive model) δεύτερης τάξης.

Τα δεδομένα συλλέχθηκαν από ένα web server μιας μεγάλης εταιρείας για περισσότερο από οχτώ μήνες (Ιούνιος 1996 – Ιανουάριος 1997). Κατασκευάστηκε ένα στατιστικό μοντέλο, το οποίο έκανε εκτίμηση των http εργασιών το δευτερόλεπτο βασισμένο σε πληροφορίες όπως η ώρα της ημέρας, η ημέρα της εβδομάδας και ο μήνας. Όπως προαναφέραμε, οι παραπάνω επιδράσεις αφαιρέθηκαν με τη χρήση μιας παραλλαγής του αλγόριθμου Holt Winters. Στη συνέχεια, εφάρμοσαν στα φιλτραρισμένα αυτά δεδομένα έναν αλγόριθμο εντοπισμού σημείου αλλαγής, προκειμένου να εντοπίσουν κάποια τυχόν ανωμαλία, όπως για παράδειγμα μια ξαφνική αύξηση στο μέσο ή τη διασπορά της χρονοσειράς.

Τα αποτελέσματα των πειραμάτων της ομάδας αυτής έδειξαν πως η προσέγγιση αυτή λειτούργησε πολύ καλά δίνοντας άκρως ικανοποιητικά

αποτελέσματα. Έτσι, αναφέρουν πως η μεθοδολογία τους μπόρεσε να «συλλάβει» και τα περιοδικά φαινόμενα (π.χ. επίδραση της ώρας της ημέρας, επίδραση της ημέρας της εβδομάδας) και τις γενικότερες «τάσεις» που τυχόν παρουσιάζει το σήμα (π.χ. σταδιακή αύξηση των http διεργασιών από μήνα σε μήνα). Αποτέλεσμα ήταν να εντοπιστούν όλα τα σημεία πραγματικών ανωμαλιών, χωρίς να παρατηρούνται λανθασμένοι συναγερμοί.

2.1.3.1 AR

Το μοντέλο αυτοπαλινδρόμησης ανήκει στην κατηγορία των μοντέλων γραμμικής πρόβλεψης και επιχειρεί να προβλέψει μια επόμενη τιμή μιας χρονοσειράς, δεδομένων παλαιότερα παρατηρούμενων τιμών αυτής. Η βασική ιδέα στην οποία στηρίζεται η λειτουργία του, είναι ότι η προϊστορία των τιμών της μετρούμενης μεταβλητής, μπορεί να χρησιμοποιηθεί για την πρόβλεψη επόμενων τιμών της μεταβλητής αυτής, δεδομένου του γεγονότος ότι οι επιδράσεις του παρελθόντος θα εξακολουθούν να υφίστανται και στο μέλλον. Με άλλα λόγια, η θεωρία του μοντέλου αυτοπαλινδρόμησης, βασίζεται στην υπόθεση ότι κάθε τιμή μιας χρονοσειράς, εξαρτάται μόνο από ένα σταθμισμένο άθροισμα των προηγούμενων τιμών της χρονοσειράς συν κάποιο είδος θορύβου.

Η μαθηματική έκφραση ενός τέτοιου μοντέλου δεύτερης τάξης είναι:

$$y_t = \theta_1 \cdot y_{t-1} + \theta_2 \cdot y_{t-2} + u_t$$

όπου y_t είναι η χρονοσειρά, θ_1 και θ_2 οι συντελεστές του μοντέλου και u_t ο θόρυβος που υπεισέρχεται.

2.1.3.2 Αλγόριθμοι Εντοπισμού Σημείου Αλλαγής

Ένα από τα βασικότερα προβλήματα στην ανάλυση χρονοσειρών είναι αυτό του εντοπισμού σημείου αλλαγής, δηλαδή του εντοπισμού του σημείου στο οποίο η χρονοσειρά σημειώνει αλλαγή στη συμπεριφορά της. Βασικό μέλημα των αλγορίθμων οι οποίοι χρησιμοποιούνται για την επίλυση τέτοιων προβλημάτων είναι να εντοπίσουν οποιαδήποτε «ύποπτη» αλλαγή στην κατανομή που ακολουθούν τα δεδομένα με τη μικρότερη δυνατή καθυστέρηση από τη στιγμή που αυτή η αλλαγή έλαβε χώρα, ενώ ταυτόχρονα το ποσοστό των λανθασμένων σημάνσεων συναγερμού θα πρέπει να παραμένει το ελάχιστο δυνατό.

Οι περισσότεροι αλγόριθμοι αυτού του είδους ασχολούνται ειδικότερα με τον εντοπισμό απότομων αλλαγών [24]. Με τον όρο αυτό εννοούμε αλλαγές στα χαρακτηριστικά των δεδομένων μας οι οποίες συμβαίνουν πολύ γρήγορα σε σχέση με το ρυθμό δειγματοληψίας, αν όχι ακαριαία. Οι αλλαγές αυτές συμβαίνουν στις ιδιότητες (χαρακτηριστικά) του μετρούμενου μεγέθους οι οποίες ιδιότητες παρουσιάζουν μια σταθερότητα πριν και μετά την αλλαγή. Επειδή οι περισσότεροι από τους αλγόριθμους των οποίων χαρακτηριστικό είναι η προσαρμογή στα δεδομένα μπορούν να εντοπίσουν μόνο αλλαγές οι οποίες πραγματοποιούνται σταδιακά, ο εντοπισμός των απότομων αλλαγών αποτελεί ένα πρόβλημα που παρουσιάζει ιδιαίτερο ενδιαφέρον σε πολλούς τομείς.

Για την επίλυση τέτοιου είδους προβλημάτων χρησιμοποιείται συνήθως ο έλεγχος δύο υποθέσεων τον οποίο υλοποιούν οι προαναφερθέντες αλγόριθμοι. Γίνεται λοιπόν ο έλεγχος ανάμεσα στη «μηδενική υπόθεση» (null hypothesis) ότι δηλαδή καμία αλλαγή στα χαρακτηριστικά του μετρούμενου μεγέθους δεν έχει συντελεστεί και όλα βαίνουν φυσιολογικά και στην «εναλλακτική υπόθεση» (alternative hypothesis), ότι κάποια αλλαγή έχει συμβεί.

Η προσέγγιση αυτή είναι κατά κάποιο τρόπο αναδρομική, αφού οι αλγόριθμοι αυτού του είδους σε κάθε βήμα παρατηρούν ένα δείγμα των στατιστικών δεδομένων και επιχειρούν να αποφανθούν εάν έχει συμβεί κάποια αλλαγή σε αυτό το δείγμα και σε ποιο σημείο ακριβώς. Το κυριότερο πλεονέκτημα αυτής της προσέγγισης είναι η ευκολία με την οποία οι αλγόριθμοι αυτοί μπορούν να εφαρμοστούν στα εκάστοτε δεδομένα.

2.1.4 SPA Expert System

Στο πανεπιστήμιο της Utah ανέπτυξαν το SPA Expert System [25], ένα σύστημα το οποίο είχε ως σκοπό να αξιολογήσει τη χρήση των μοντέλων χρονοσειρών στα προβλήματα εντοπισμού ανωμαλιών που τυχόν παρουσιάζονται στην απόδοση των υπολογιστικών συστημάτων.

Προκειμένου να επιτύχει το σκοπό του, το SPA εξετάζει το μέσο όρο του φόρτου ενός υπολογιστή (host) προκειμένου να αποφανθεί εάν ο συγκεκριμένος υπολογιστής έχει εμπλακεί σε κάποια κατάσταση η οποία ως αποτέλεσμα έχει επιφέρει τη μείωση της απόδοσής του. Ο αλγόριθμος που χρησιμοποιεί το SPA για τον εντοπισμό ανωμαλιών είναι ένα μοντέλο εκθετικά σταθμισμένου κινούμενου μέσου (exponentially weighted moving average).

Το σύστημα αυτό, θέτει αυτόματα κατώφλια και εντοπίζει και διαγιγνώσκει προβλήματα απόδοσης σε ένα δίκτυο στο οποίο είναι συνδεδεμένοι UNIX υπολογιστές [26]. Έμμεσος σκοπός είναι να μην εμπλέκεται η παρουσία ενός ανθρώπου – administrator ο οποίος να θέτει με χειροκίνητο τρόπο και δικούς του υπολογισμούς τα κατάλληλα κατώφλια, αλλά η όλη διαδικασία να γίνεται με αυτοματοποιημένο τρόπο.

Χρησιμοποιήθηκαν μοντέλα χρονοσειρών προκειμένου να μοντελοποιηθούν οι αποκλίσεις του φόρτου εργασίας του κάθε host. Επίσης, γίνεται εκτίμηση ενός διαστήματος εμπιστοσύνης και στη συνέχεια γίνεται σύγκριση των δεδομένων που συλλέχθηκαν από το SPA με μια αναμενόμενη τιμή, η οποία έχει καθοριστεί προηγουμένως από το ίδιο το μοντέλο. Οι τιμές των δεδομένων που δεν βρίσκονται στα όρια του διαστήματος εμπιστοσύνης, έχουν ως αποτέλεσμα τη σήμανση συναγερμού που ειδοποιεί τον διαχειριστή του συστήματος και ο οποίος είναι υπεύθυνος για την εγκυρότητα της ειδοποίησης αυτής.

Το αποτέλεσμα στο οποίο κατέληξαν ήταν ότι ένα μοντέλο χρονοσειράς είναι μια αποτελεσματική, πρακτική και εύκολα υλοποιήσιμη τεχνική για τον καθορισμό των κατάλληλων τιμών του κατωφλιού όσον αφορά τον έλεγχο της απόδοσης στα συστήματα υπολογιστών, καθώς και το γεγονός ότι το σύστημα SPA απέδωσε πολύ καλά αποτελέσματα, εφόσον εντόπισε σωστά τα περισσότερα των προβλημάτων τα οποία επηρέαζαν το μέσο φόρτο, ενώ ταυτόχρονα το ποσοστό λανθασμένων συναγερμών δεν υπερέβη το 6%.

2.1.5 Χρήση του Αλγόριθμου CUSUM για τον Εντοπισμό Σημείου Ανωμαλίας

Στο πανεπιστήμιο του Michigan, προτείνουν τη χρήση ενός αλγόριθμου τύπου CUSUM, προκειμένου να εντοπίσουν Επιθέσεις Άρνησης Υπηρεσίας τύπου SYN flooding [27]. Ο αλγόριθμος αυτός, εφαρμόζεται σε δεδομένα, τα οποία εκφράζουν τη διαφορά SYN-FIN πακέτων, κανονικοποιημένη ως προς μια εκτίμηση του μέσου αριθμού FIN πακέτων στη μονάδα του χρόνου.

Υποστηρίζουν πως ο μηχανισμός αυτός είναι απλός και ανθεκτικός στα λάθη και επίσης ότι είναι κατάλληλος για να εφαρμοστεί στους περιφερειακούς δρομολογητές. Πιο συγκεκριμένα, χρησιμοποιείται ο λόγος των SYN πακέτων ως

προς τα αντίστοιχα FIN στη μονάδα του χρόνου, έτσι ώστε η μετρική αυτή να είναι ανεξάρτητη από μοντέλα αφίξεων καθώς και από επιδράσεις τύπου «ώρα της ημέρας».

Ο όλος μηχανισμός ελέγχθηκε και αξιολογήθηκε με πειράματα εξομοίωσης. Τα δεδομένα που χρησιμοποιήθηκαν συγκεντρώθηκαν από τρεις διαφορετικές πηγές και προέρχονταν από διάφορες ώρες της ημέρας. Στη συνέχεια, προστέθηκαν επιθέσεις DDoS στα δεδομένα αυτά, θεωρώντας ως δεδομένο ότι ο ρυθμός της «πλημμύρας» από SYN πακέτα (της επίθεσης δηλαδή) είναι σταθερός, εφόσον η ευαισθησία στον εντοπισμό της επίθεσης εξαρτάται από το συνολικό όγκο της κίνησης.

Τα αποτελέσματα αυτών των πειραμάτων απέδειξαν πως η προσέγγιση αυτή έχει ιδιαίτερα καλά αποτελέσματα όσον αφορά στον εντοπισμό των επιθέσεων, με μειονέκτημα όμως την καθυστέρηση στον εντοπισμό της επίθεσης, η οποία είναι ιδιαίτερα υπολογίσιμη στις περιπτώσεις που η ένταση των επιθέσεων είναι μικρότερη από 50 SYN πακέτα το δευτερόλεπτο. Στη συνέχεια της αναφοράς αυτής, θα περιγράψουμε τη δική μας προσέγγιση πάνω στο θέμα του εντοπισμού Επιθέσεων Άρνησης Υπηρεσίας και συγκεκριμένα του τύπου SYN flooding. Όπως προαναφέραμε, οι επιθέσεις αυτού του είδους είναι ιδιαίτερα διαδεδομένες και επομένως είναι απαραίτητο να υπάρχουν μηχανισμοί για τον εντοπισμό των επιθέσεων αυτών. Παρουσιάζουμε δύο αλγόριθμους οι οποίοι βοηθούν στην επίτευξη του παραπάνω σκοπού: έναν αλγόριθμο προσαρμοζόμενου κατωφλιού (adaptive threshold) και μια συγκεκριμένη εφαρμογή του αθροιστικού αλγόριθμου ελέγχου (CUSUM) για τον εντοπισμό σημείου ανωμαλίας. Ο αλγόριθμος προσαρμοζόμενου κατωφλιού είναι ένας απλός και σαφής αλγόριθμος ο οποίος εντοπίζει τυχόν ανωμαλίες έχοντας ως κριτήριο την παραβίαση ενός κατωφλιού το οποίο τίθεται με βάση κάποιες πρόσφατες μετρήσεις της κίνησης. Ο δεύτερος αλγόριθμος, όπως προαναφέραμε είναι μια συγκεκριμένη εφαρμογή του αθροιστικού αλγόριθμου ελέγχου (CUSUM), ο οποίος είναι ένας ευρέως χρησιμοποιούμενος αλγόριθμος εντοπισμού ανωμαλιών και βασίζεται στη θεωρία εντοπισμού σημείου αλλαγής.

Η κυριότερη διαφοροποίηση της εργασίας μας από τις προαναφερθείσες προσεγγίσεις έγκειται στο ότι επικεντρωνόμαστε στη μελέτη της απόδοσης των αλγόριθμων εντοπισμού με σκοπό την αξιολόγησή τους ως προς τρεις κυρίως τομείς: την πιθανότητα εντοπισμού, το ποσοστό λανθασμένων συναγερμών και την καθυστέρηση στον εντοπισμό της επίθεσης που αυτοί παρουσιάζουν. Επίσης,

εξετάζονται και προσδιορίζονται η επίδραση των διαφόρων παραμέτρων των αλγορίθμων επί των παραπάνω θεμάτων (ταχύτητα εντοπισμού, πιθανότητα εντοπισμού, ποσοστό λανθασμένων συναγερμών), καθώς και ο βαθμός συσχέτισης των ανωτέρω σε σχέση με τις παραμέτρους που προαναφέρθηκαν. Μελετάται επίσης η επίδραση σε αυτά των διαφόρων τύπων επιθέσεων, όπως για παράδειγμα επιθέσεις μικρής έντασης ή επιθέσεις με αυξανόμενη ένταση. Κύριο στοιχείο της εργασίας αυτής είναι επίσης το γεγονός ότι κάνουμε χρήση κάποιων απλών αλγορίθμων, με στατιστικό ή όχι υπόβαθρο προκειμένου να εντοπίσουμε επιθέσεις άρνησης υπηρεσίας, χρησιμοποιούμε δηλαδή απλές στατιστικές μεθόδους σε ένα δικτυακό πρόβλημα.

Στο σημείο αυτό θα πρέπει να τονίσουμε και τη διαφορά που υπάρχει ανάμεσα στην προσέγγιση της εργασίας μας και σε αυτή που διεξήχθη στο πανεπιστήμιο του Michigan, όπου οι διακυμάνσεις κατά τη διάρκεια της ημέρας που τυχόν παρουσίαζαν τα γεγονότα αφαιρούνταν με τον υπολογισμό σε ένα χρονικό διάστημα των TCP SYN πακέτων σε σχέση με τα πακέτα FIN. Αυτό σημαίνει πως η όλη προσέγγιση βασίζονταν στον εντοπισμό της χρονικής στιγμής κατά την οποία ο αριθμός των SYN πακέτων υπερέβαινε κατά πολύ αυτόν των FIN πακέτων.

Αντίθετα, η μελέτη που διενεργήσαμε είναι περισσότερο γενική, υπό την έννοια ότι οι αλγόριθμοι που προτείνουμε είναι δυνατό να εφαρμοστούν και σε άλλου είδους επιθέσεις, όχι μόνο σε επιθέσεις τύπου TCP SYN flooding. Για παράδειγμα, μια άκρως ενδιαφέρουσα περίπτωση θα ήταν η εφαρμογή του αλγόριθμου για τον έγκαιρο εντοπισμό ανωμαλιών στην παραβίαση της ποιότητας υπηρεσίας (Quality of Service) [28]. Στην περίπτωση αυτή ο αλγόριθμος θα εφαρμόζονταν πάνω σε δεδομένα που θα εξέφραζαν την ποιότητα υπηρεσίας που απολαμβάνει ένας χρήστης, π.χ. τη μέση καθυστέρηση. Μια τέτοια εφαρμογή θα μπορούσε να αιτιολογηθεί από το γεγονός ότι ένα μεγάλο μέρος από τις παραβιάσεις που παρατηρούνται στις εγγυήσεις των συμβολαίων των χρηστών για ποιότητα υπηρεσίας οφείλονται σε ανωμαλίες (συμπεριλαμβανομένων σε αυτές τις ανωμαλίες και των επιθέσεων άρνησης υπηρεσίας), πράγμα που οδηγεί στο συμπέρασμα ότι οι τεχνικές εντοπισμού ανωμαλιών θα ήταν σε θέση να εντοπίσουν πιθανές παραβιάσεις των εγγυήσεων της ποιότητας υπηρεσίας πριν αυτές πραγματικά συμβούν.

Ο βασικός σκοπός αυτής της εργασίας είναι να αποδείξουμε, με βάση κάποια πειραματικά αποτελέσματα που θα περιγράψουμε στη συνέχεια, ότι ακόμη και ένας πολύ απλός αλγόριθμος μπορεί να έχει ιδιαίτερα ικανοποιητικά αποτελέσματα για

κάποιες μορφές επιθέσεων Άρνησης Υπηρεσίας τύπου SYN flooding, όπως για παράδειγμα επιθέσεις μεγάλης έντασης, ωστόσο όμως να έχει αρκετά άσχημη απόδοση για επιθέσεις οι οποίες για παράδειγμα έχουν χαμηλή ένταση. Επιπλέον δείχνουμε ότι οι αλγόριθμοι οι οποίοι έχουν ένα ισχυρά στατιστικό υπόβαθρο, επιδεικνύουν σταθερά ικανοποιητική απόδοση όταν καλούνται να εντοπίσουν πολλές διαφορετικές μορφές επιθέσεων, χωρίς να είναι πολύπλοκοι ή δαπανηροί στην υλοποίηση τους

3 Περιγραφή Διαδικασίας που ακολουθείται στην Προσπάθεια Εντοπισμού Ανωμαλιών στην Κίνηση Δικτύου

3.1 Αρχική Προσέγγιση

Η αρχική μας προσέγγιση για την αντιμετώπιση του προαναφερθέντος προβλήματος περιελάμβανε τρία βασικά βήματα, τα οποία σε γενικές γραμμές ακολουθούν όλες οι προσεγγίσεις οι οποίες βασίζονται στην φιλοσοφία της εκμάθησης φυσιολογικής συμπεριφοράς από το σύστημα εντοπισμού επιθέσεων. Στο σημείο αυτό, θα πρέπει να αναφέρουμε πως οι μηχανισμοί εντοπισμού ανωμαλιών – επιθέσεων, χωρίζονται σε δύο κυρίως κατηγορίες. Η μια από αυτές είναι η κατηγορία των μηχανισμών οι οποίοι καθορίζουν εκ των προτέρων ποια θεωρείται ότι είναι η φυσιολογική συμπεριφορά που θα πρέπει να εκδηλώνει η μεταβλητή την οποία μετράμε. Η δεύτερη κατηγορία είναι αυτή στην οποία το όλο σύστημα «μαθαίνει» με την πάροδο του χρόνου και με βάση την προϊστορία ποια θεωρείται «κανονική» συμπεριφορά του υπό εξέταση μεγέθους.

Στην πρώτη περίπτωση γίνεται ένας συνεχής έλεγχος εάν η μετρούμενη μεταβλητή υπερβαίνει ή όχι ένα προκαθορισμένο κατώφλι, η επιλογή του οποίου εξαρτάται από το τι έχουμε θεωρήσει εξ’αρχής ως φυσιολογική συμπεριφορά, και στη συνέχεια σήμανση συναγερμού κάθε φορά που το κατώφλι αυτό παραβιάζεται. Για παράδειγμα, εάν μετράμε τον υπολογιστικό φόρτο ενός μηχανήματος και καθορίσουμε ως φυσιολογική συμπεριφορά ο φόρτος αυτός να μην υπερβαίνει το 70% του μέγιστου φόρτου, θα πρέπει να γίνεται ένας συνεχής έλεγχος εάν ο φόρτος είναι μεγαλύτερος από 70% ή όχι.

Στη δεύτερη περίπτωση, θεωρούμε τη μεταβλητή την οποία μετράμε στο χρόνο. Αυτό έχει ως αποτέλεσμα να καταλήξουμε τελικά με μια χρονοσειρά την

οποία και αναλύουμε. Υπολογίζονται κάποια στατιστικά στοιχεία όπως για παράδειγμα την τυπική απόκλιση και τον μέσο όρο της χρονοσειράς και με βάση αυτά, γίνεται μια πρόβλεψη του ποια περιμένουμε να είναι η επόμενη στο χρόνο τιμή της μεταβλητής που μετράμε. Στην παρούσα εργασία ασχολούμαστε μόνο με την κατηγορία των αλγορίθμων οι οποίοι βασίζονται στη φιλοσοφία της εκμάθησης της φυσιολογικής συμπεριφοράς.

Όπως λοιπόν αναφέραμε και προηγουμένως, η αρχική μας προσέγγιση ακολουθεί τρία βασικά βήματα, τα οποία ακολουθούν γενικότερα οι προσεγγίσεις αυτής της κατηγορίας:

1. Αφαίρεση της εποχικότητας και της γενικότερης τάσης που τυχόν παρουσιάζει το σήμα
2. Αφαίρεση των σημαντικών συσχετίσεων στο χρόνο που μπορεί να παρουσιάζουν τα δεδομένα
3. Εφαρμογή του αλγόριθμου εντοπισμού ανωμαλιών

3.1.1 Αφαίρεση της εποχικότητας και της γενικότερης τάσης που τυχόν παρουσιάζει το σήμα

Είναι αρκετά πιθανό το σήμα το οποίο θέλουμε να αναλύσουμε να περιέχει επιδράσεις παραγόντων όπως η ώρα της ημέρας (για παράδειγμα μεγαλύτερος φόρτος σε ένα σύστημα το μεσημέρι από ότι το βράδυ), η μέρα της εβδομάδας (π.χ. μικρότερος ο φόρτος του συστήματος το Σαββατοκύριακο) ή ακόμα και ο μήνας του χρόνου (π.χ. μικρότερος ο φόρτος του συστήματος κατά τη διάρκεια του καλοκαιριού σε σχέση με τους υπόλοιπους μήνες του χρόνου). Προκειμένου να αφαιρεθούν επιδράσεις τέτοιου είδους από το σήμα, χρησιμοποιούμε αλγόριθμους όπως ο Holt Winters ή η Εκθετική Εξομάλυνση (Exponential Smoothing).

Στη συγκεκριμένη υλοποίησή μας, ο αλγόριθμος που χρησιμοποιήσαμε ήταν ο Holt Winters. Οι παράμετροι που υπεισέρχονται στον αλγόριθμο αυτό υπολογίστηκαν πειραματικά, δοκιμάστηκαν δηλαδή όλοι οι δυνατοί συνδυασμοί και επιλέχθηκε εκείνος ο οποίος έδωσε το μικρότερο τετραγωνικό λάθος. Έτσι, οι σχέσεις οι οποίες προκύπτουν μετά την επιλογή των παραμέτρων, αποτελούν την υλοποίηση του αλγόριθμου, τον οποίο εφαρμόζουμε στα δεδομένα μας. Το αποτέλεσμα που προκύπτει, το αφαιρούμε από το αρχικό μας σήμα και προκύπτει το σήμα το οποίο θα αποτελεί και το σήμα το οποίο θα επεξεργαζόμαστε στη συνέχεια.

3.1.2 Αφαίρεση των σημαντικών συσχετίσεων στο χρόνο που μπορεί να παρουσιάζουν τα δεδομένα

Στα υπολογιστικά και τα επικοινωνιακά συστήματα, παράγοντες όπως η φύση των διεργασιών του τελικού χρήστη, συχνά καταλήγουν στην παρουσία συσχετίσεων στο χρόνο μεταξύ των μετρήσεων. Ως αποτέλεσμα των παραπάνω, σε πολλές περιπτώσεις είναι δυνατό να ισχύει η ακόλουθη πρόταση: «Εάν μια μεταβλητή, η οποία είναι του ενδιαφέροντός μας, έχει μεγάλη (ή μικρή) τιμή τη χρονική στιγμή t, είναι ιδιαίτερα πιθανό ότι αυτή η μεταβλητή θα έχει επίσης μεγάλη (ή μικρή) τιμή τη χρονική στιγμή t+1». Προκειμένου λοιπόν να αφαιρέσουμε αυτού του είδους τις χρονικές συσχετίσεις, χρησιμοποιούμε ένα AR(2) μοντέλο αυτοπαλινδρόμησης [29].

$$y_t = \theta_1 \cdot y_{t-1} + \theta_2 \cdot y_{t-2} + u_t$$

Όπως είπαμε αυτό είναι ένα μοντέλο αυτοπαλινδρόμησης δεύτερης τάξης. Οι θ1 και θ2 είναι οι παράμετροι του μοντέλου, οι οποίες υπολογίζονται από τα δεδομένα, χρησιμοποιώντας κάποιες καθιερωμένες τεχνικές και το u_t είναι ανεξάρτητες και ομοιόμορφα κατανεμημένες τυχαίες μεταβλητές [30]. Εφαρμόζουμε το μοντέλο αυτό στο σήμα που προέκυψε από το προηγούμενο βήμα και το αποτέλεσμα το αφαιρούμε και πάλι από το σήμα που προέκυψε μετά την εφαρμογή του πρώτου βήματος. Έτσι, προκύπτει και το τελικό μας σήμα το οποίο θα χρησιμοποιήσουμε ως είσοδο στον αλγόριθμο εντοπισμού ανωμαλιών που θα συναντήσουμε στο τρίτο βήμα αυτής της προσέγγισης.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι έγινε έλεγχος της αποδοτικότητας του AR μοντέλου. Εκτελέστηκε σειρά πειραμάτων όπου καλύφθηκε μεγάλο μέρος του φάσματος της τάξης του μοντέλου αυτοπαλινδρόμησης, από την τάξη 2 έως και την
τάξη 16.

AR order	Mean	Std. Deviation	Variance
2	0,000017	2,645	6,996
3	0,000015	2,637	6,959
4	0,000013	2,633	6,937
5	0,000011	2,627	6,905
6	0,000009	2,623	6,879
7	0,000010	2,623	6,879
8	0,000007	2,615	6,836
9	0,000003	2,606	6,793
10	0,000000	2,602	6,769
11	-0,000001	2,601	6,766
12	-0,000003	2,599	6,753
13	-0,000004	2,598	6,749
14	-0,000004	2,598	6,749
15	-0,000005	2,597	6,746
16	-0,000005	2,597	6,746

Πίνακας 1: Επίδραση της τάξης του μοντέλου αυτοπαλινδρόμησης

Κατόπιν τούτου, και με βάση τα αποτελέσματα που παρουσιάζονται στον πίνακα 1, συνάγεται το συμπέρασμα ότι το υψηλότερης τάξης μοντέλο αυτοπαλινδρόμησης δεν παρουσιάζει ιδιαίτερα σημαντικά πλεονεκτήματα σε σχέση με τη χρήση του μοντέλου μικρότερης τάξης. Στον πίνακα 1 παρουσιάζονται οι τιμές του μέσου όρου και της διασποράς του τελικού σήματος που προκύπτει μετά την εφαρμογή των δυο προαναφερθέντων βημάτων για διάφορες τιμές της τάξης του AR μοντέλου. Σύμφωνα με τον πίνακα, το AR(10) παρουσιάζει τα καλύτερα αποτελέσματα, όμως η πολυπλοκότητα η οποία προστίθεται είναι πολύ πιο σημαντική από ότι το πραγματικό κέρδος που θα είχαμε στην περίπτωση που χρησιμοποιούσαμε το AR(10). Έτσι, καταλήγουμε στο αποτέλεσμα πως η καλύτερη επιλογή είναι η χρήση του μοντέλου AR(2).

3.1.2.1 Μοντέλο Εκθετικά Σταθμισμένου Κινούμενου Μέσου (Exponentially Weighted Moving Average – EWMA) – Δεύτερη Προσέγγιση

Μια άλλη προσέγγιση όσον αφορά στο θέμα της αφαίρεσης των χρονικών συσχετίσεων και της εποχικότητας, πολύ απλούστερη από την προηγούμενη, είναι η χρήση ενός μοντέλου Εκθετικά Σταθμισμένου Κινούμενου Μέσου – EWMA [31]. Σύμφωνα με την προσέγγιση αυτή, αφαιρούμε από το αρχικό μας σήμα (τα αρχικά δεδομένα, τα οποία δεν έχουν υποστεί την οποιαδήποτε επεξεργασία) ένα εκθετικά σταθμισμένο κινούμενο μέσο όλων των προηγούμενων δεδομένων,

συμπεριλαμβανομένης και της πιο πρόσφατης μέτρησης. Ο μέσος αυτός, υπολογίζεται από τη σχέση:

$$\overline{\mu}_n = \beta\overline{\mu}_{n-1} + (1-\beta)x_n$$

όπου

- β ($0 < \beta \leq 1$) είναι ο συντελεστής του μοντέλου, είναι σταθερά και καθορίζει το βάθος της μνήμης που θα έχει το EWMA
- x_n είναι η τρέχουσα παρατήρηση (η παρατήρηση τη χρονική στιγμή n)
- $\overline{\mu}_n$ είναι ο εκθετικά σταθμισμένος κινούμενος μέσος που ζητάμε να υπολογίσουμε

Η παράμετρος β καθορίζει το βαθμό με τον οποίο τα «παλαιότερα» δεδομένα επηρεάζουν τον υπολογισμό του Εκθετικά Σταθμισμένου Κινούμενου Μέσου. Μια μικρή τιμή της παραμέτρου αυτής υποδηλώνει ότι μόνο οι πιο πρόσφατες μετρήσεις επηρεάζουν τον υπολογισμό του μέσου αυτού. Έτσι, μια μικρή τιμή του β δίνει μεγαλύτερο βάρος στα πρόσφατα δεδομένα και μικρότερο βάρος στα παλαιότερα δεδομένα. Αντίθετα, μια μεγάλη τιμή της παραμέτρου β (π.χ. $\beta = 1$) δίνει περισσότερη σημασία και μεγαλύτερο βάρος στις παλαιότερες μετρήσεις. Συνήθως, η τιμή του β τίθεται μεταξύ 0.7 και 0.8 [32] αν και γενικότερα η επιλογή της παραμέτρου αυτής είναι αρκετά αυθαίρετη. Βέβαια, οι Lucas και Saccucci [33] παραθέτουν κάποιους πίνακες οι οποίοι βοηθούν στην επιλογή του β.

3.1.3 Εφαρμογή του αλγόριθμου εντοπισμού ανωμαλιών

Μετά την εφαρμογή των δύο προηγούμενων βημάτων, γίνεται εφαρμογή των κατάλληλων αλγορίθμων εντοπισμού ανωμαλιών στα δεδομένα που προέκυψαν. Τους αλγόριθμους που χρησιμοποιήθηκαν στην παρούσα εργασία, τους περιγράφουμε στη συνέχεια.

4 Περιγραφή Αλγορίθμων Εντοπισμού Ανωμαλιών της Κίνησης Δικτύου

4.1 Είδη Μετρικών

Όπως είπαμε, βασική επιδίωξη της εργασίας μας ήταν να χρησιμοποιήσουμε τεχνικές τις οποίες δανειστήκαμε από τον τομέα της στατιστικής, προκειμένου να τις

εφαρμόσουμε στον τομέα των δικτύων, έτσι ώστε να βοηθήσουμε στην προσπάθεια δημιουργίας μηχανισμών για τον εντοπισμό επιθέσεων άρνησης υπηρεσίας και συγκεκριμένα επιθέσεων τύπου SYN flooding. Με άλλα λόγια, προσπαθήσαμε να προσαρμόσουμε τους αλγόριθμους εντοπισμού ανωμαλιών έτσι ώστε να μπορούν να εφαρμοστούν στον τομέα των δικτύων και να μπορούν να εντοπίσουν ανωμαλίες που παρουσιάζονται στον τομέα αυτό, πιο απλά, στον εντοπισμό επιθέσεων.

Για τον λόγο αυτό, επειδή αυτό που προσπαθούμε να εντοπίσουμε είναι οι SYN flooding επιθέσεις, η μεταβλητή η οποία μας ενδιαφέρει και την οποία θα πρέπει να μετράμε είναι το πλήθος των TCP-SYN πακέτων που δέχεται το θύμα (ή στέλνει ο θύτης) στη μονάδα του χρόνου, γεγονός το οποίο συνεπάγεται και από την περιγραφή της επίθεσης.

Αυτό λοιπόν που προσπαθούμε να επιτύχουμε είναι να εντοπίσουμε τις περιπτώσεις εκείνες στις οποίες έχουμε ιδιαίτερα μεγάλη συγκέντρωση SYN πακέτων, είτε στην πλευρά του αποστολέα είτε του παραλήπτη. Έτσι, μελετούμε τη συμπεριφορά που παρουσιάζει η κατανομή της άφιξης των SYN πακέτων στην πλευρά κυρίως του θύματος. Το σήμα μας, δηλαδή η χρονοσειρά, είναι το πλήθος των πακέτων αυτού του είδους στη μονάδα του χρόνου. Στόχος μας είναι ο όσο το δυνατόν ταχύτερος εντοπισμός του σημείου ανωμαλίας, του σημείου δηλαδή εκείνου που η χρονοσειρά μας παρουσιάζει μια ασυνήθιστη με βάση το παρελθόν συμπεριφορά και ο αριθμός των SYN πακέτων είναι ασυνήθιστα μεγάλος, οπότε και έχουμε σοβαρό λόγο να θεωρήσουμε ότι μια επίθεση λαμβάνει χώρα και να προσπαθήσουμε να την αποτρέψουμε όσο είναι ακόμα νωρίς, πριν αυτή προλάβει να δημιουργήσει σοβαρό πρόβλημα στο θύμα.

Εκτός όμως από το να χρησιμοποιήσουμε το πλήθος των TCP-SYN πακέτων στη μονάδα του χρόνου ως μετρική, μπορούμε να χρησιμοποιήσουμε και άλλα μεγέθη ως μετρικές προκειμένου να εφαρμόσουμε στη συνέχεια τους αλγορίθμους εντοπισμού ανωμαλιών πάνω στα δεδομένα που θα έχουμε συλλέξει. Ένα τέτοιο παράδειγμα είναι η διαφορά των TCP-SYN από τα αντίστοιχα TCP-FIN πακέτα στη μονάδα του χρόνου. Σύμφωνα με το πρωτόκολλο TCP, υπό κανονικές συνθήκες απαιτείται μια αντιστοιχία ένα προς ένα μεταξύ των πακέτων TCP-SYN και των TCP-FIN τα οποία λαμβάνονται από τον παραλήπτη. Ωστόσο, στην πραγματικότητα, υπάρχει πάντοτε μια διαφορά μεταξύ του αριθμού των SYN πακέτων και αυτόν των FIN στη μονάδα του χρόνου. Αυτό, πολλές φορές οφείλεται στον αριθμό των TCP συνόδων (sessions) οι οποίες έχουν ιδιαίτερα μεγάλη διάρκεια.

Στις επιθέσεις τύπου SYN flooding, το θύμα κατακλύζεται από μια πληθώρα SYN πακέτων για κάποιο χρονικό διάστημα, έτσι ώστε να μην μπορεί τελικά να ανταποκριθεί στις αιτήσεις των νόμιμων χρηστών, αφού έχει υπόψη του πολλές ημι-ανοιχτές TCP συνδέσεις και δε μπορεί να συνάψει νέες. Στο ίδιο όμως χρονικό διάστημα, το πλήθος των FIN πακέτων που λαμβάνονται από το θύμα δεν μεταβάλλεται δραματικά. Για το λόγο αυτό, θα έχουν παρατηρηθεί πολύ περισσότερα SYN από ότι FIN πακέτα κατά τη διάρκεια της επίθεσης. Η διαφορά μεταξύ των SYN και των FIN πακέτων θα αυξάνεται συνεχώς δραματικά και θα παραμένει σε πολύ υψηλά επίπεδα, για όσο χρονικό διάστημα διαρκεί η επίθεση, κάτι που συνήθως είναι της τάξεως των αρκετών λεπτών. Επομένως, η παρουσία μιας μεγάλης διαφοράς ανάμεσα στα SYN και τα FIN πακέτα η οποία διαρκεί μάλιστα αρκετά μεγάλο χρονικό διάστημα (της τάξεως των λεπτών ή δεκάδων δευτερολέπτων) υποδηλώνει την ύπαρξη SYN flooding επίθεσης.

Βέβαια, όπως έχουμε προαναφέρει, υπάρχουν και άλλοι λόγοι για τους οποίους είναι δυνατόν να παρατηρούμε μια αύξηση στη διαφορά μεταξύ των SYN και των FIN πακέτων για κάποιο χρονικό διάστημα. Ένας από αυτούς θα μπορούσε να είναι το γεγονός ότι παρατηρείται μια σταθερή αύξηση στους χρήστες οι οποίοι χρησιμοποιούν το δίκτυο και παράλληλα, οι περισσότεροι από αυτούς συνάπτουν TCP συνόδους μεγάλης διάρκειας. Έτσι, το αποτέλεσμα είναι ο αριθμός των εγκατεστημένων TCP συνδέσεων μακράς διάρκειας να αυξάνεται συνεχώς. Επίσης, ένας ακόμη λόγος θα μπορούσε να είναι το γεγονός ότι κάποιοι δημοφιλείς εξυπηρετητές (servers) ή οι αντίστοιχοι σύνδεσμοι που είναι συνδεδεμένοι με αυτούς είναι εκτός λειτουργίας. Το αποτέλεσμα θα είναι οι SYN αιτήσεις να αναμεταδίδονται αυτόματα τρεις φορές, προτού η κάθε μια από αυτές τις αιτήσεις λήξει (times out).

Βέβαια, όλες αυτές οι περιπτώσεις θεωρούνται εξαιρετικές περιπτώσεις και παρατηρούνται σπάνια, δεν είναι δηλαδή αρκετά πιθανό να έχει συμβεί κάποια από αυτές όταν παρατηρείται μεγάλη αύξηση στη διαφορά μεταξύ του αριθμού των SYN και των FIN πακέτων.

Μια ακόμη μετρική η οποία θα μπορούσε να χρησιμοποιηθεί για τον εντοπισμό SYN flooding επιθέσεων είναι ο λόγος της διαφοράς SYN-FIN πακέτων ως προς μια εκτίμηση του μέσου αριθμού FIN πακέτων στη μονάδα του χρόνου. Στην ουσία δηλαδή, με τον τρόπο αυτό μελετούμε και πάλι τη σχέση των SYN και των FIN, βλέπουμε δηλαδή και σε αυτή την περίπτωση πόσο μεγαλύτερο είναι το πλήθος των SYN από τα FIN πακέτα στη μονάδα του χρόνου. Η κανονικοποίηση, βοηθάει

στην απομάκρυνση τυχόν συσχετίσεων στο χρόνο που παρουσιάζουν τα δεδομένα. Επειδή οι αφίξεις των αιτήσεων για TCP συνδέσεις χαρακτηρίζεται από εκρηκτική συμπεριφορά, είναι αρκετά δύσκολος ο εντοπισμός των επιθέσεων, αφού δεν υπάρχει κάποια συγκεκριμένη τιμή η οποία να θεωρείται φυσιολογική όσον αφορά στη διάρκεια μιας «έκρηξης» στις αιτήσεις TCP συνδέσεων. Υπάρχει ωστόσο ισχυρή συσχέτιση ανάμεσα στα TCP SYN και FIN πακέτα, γεγονός που όπως έχει προαναφερθεί αποτελεί σημαντική βοήθεια στον εντοπισμό SYN flooding επιθέσεων άρνησης υπηρεσίας. Σύμφωνα με την περιγραφή του πρωτοκόλλου TCP/IP, υπό φυσιολογικές συνθήκες, στο τέλος κάθε μετάδοσης δεδομένων, κάθε FIN πακέτο αντιστοιχεί σε ένα πακέτο SYN, ενώ αντίθετα, όταν λαμβάνει χώρα μια επίθεση SYN flooding, αυτή η αντιστοιχία παραβιάζεται.

4.2 Αλγόριθμος Προσαρμοζόμενου Κατωφλιού

Είναι ένας σαφής και απλός αλγόριθμος ο οποίος βασίζεται στον έλεγχο του εάν ο συνολικός όγκος κίνησης που μετράμε (στην περίπτωσή μας αριθμός των SYN πακέτων) κατά τη διάρκεια κάποιου χρονικού διαστήματος, υπερβαίνει ένα συγκεκριμένο κατώφλι. Επειδή οι μετρήσεις μας είναι πιθανό να παρουσιάζουν εποχιακές διακυμάνσεις ή διάφορες τάσεις, η τιμή του κατωφλιού τίθεται κάθε φορά με βάση μια εκτίμηση της μέσης τιμής των SYN πακέτων, η οποία υπολογίζεται από πρόσφατες μετρήσεις της κίνησης. Βασικό χαρακτηριστικό του αλγορίθμου αυτού είναι ότι τα δεδομένα που δέχεται ως είσοδο δεν έχουν υποστεί καμιά απολύτως επεξεργασία, με άλλα λόγια δεν έχουν ακολουθηθεί τα βήματα που περιγράφηκαν στο προηγούμενο κεφάλαιο πριν την εφαρμογή του αλγόριθμου αυτού.

Εάν x_n είναι η μετρική που χρησιμοποιούμε (SYN πακέτα) στο n-οστό χρονικό διάστημα, και $\overline{\mu}_{\text{n-1}}$ είναι ο μέσος ρυθμός ο οποίος υπολογίστηκε από προηγούμενες μετρήσεις, τότε η συνθήκη συναγερμού είναι η:

Εάν $x_n \geq (a+1)\overline{\mu}_{n-1}$ τότε σημαίνεται συναγερμός τη χρονική στιγμή n, όπου $\alpha > 0$ είναι μια παράμετρος που εκφράζει το επιπλέον ποσοστό από τη μέση τιμή και που αποτελεί ένδειξη ανώμαλης συμπεριφοράς. Η μέση τιμή μ_n υπολογίζεται σε ένα προηγούμενο χρονικό παράθυρο χρησιμοποιώντας ένα εκθετικά σταθμισμένο κινούμενο μέσο (EWMA) από προηγούμενες μετρήσεις

$$\overline{\mu}_n = \beta\overline{\mu}_{n-1} + (1-\beta)x_n$$

όπου β είναι ο συντελεστής του EWMA.

Ωστόσο, πειράματα έδειξαν ότι εάν εφαρμόσουμε αυτόν καθ' αυτόν τον παραπάνω αλγόριθμο, θα είχαμε πολλούς λάθος συναγερμούς (false alarms/positives) και γι' αυτό υλοποιήσαμε μια παραλλαγή του η οποία μπορεί να βελτιώσει την απόδοσή του. Σύμφωνα με την παραλλαγή αυτή, σημαίνεται συναγερμός αφού έχει παραβιαστεί το κατώφλι ένα συγκεκριμένο αριθμό συνεχόμενων φορών. Έτσι, η συνθήκη συναγερμού είναι πλέον:

Εάν $\sum_{i=n-k+1}^{n} 1_{\{x_i > (\alpha+1)\bar{\mu}_{i-1}\}} \geq k$ τότε σημαίνεται συναγερμός τη χρονική στιγμή n,

και k > 1 είναι η παράμετρος που εκφράζει τον αριθμό των συνεχόμενων παραβιάσεων του κατωφλιού που πρέπει να υπάρχουν προκειμένου να σημανθεί συναγερμός.

Οι παράμετροι που μεταβάλλονται στον αλγόριθμο αυτόν είναι ο συντελεστής μεγέθους α ο οποίος χρησιμοποιείται για τον υπολογισμό του κατωφλιού, ο αριθμός των συνεχόμενων παραβιάσεων του κατωφλιού πριν τη σήμανση συναγερμού k, ο συντελεστής β του EWMA και το μέγεθος του χρονικού διαστήματος στο οποίο παίρνουμε τις μετρήσεις μας.

4.3 Αλγόριθμος CUSUM

Ο αλγόριθμος αυτός ανήκει στην οικογένεια των αλγόριθμων εντοπισμού σημείου αλλαγής και βασίζεται στον έλεγχο υποθέσεων. Επιπλέον, έχει αναπτυχθεί για ανεξάρτητες και ομοιόμορφα κατανεμημένες μεταβλητές $\{y_i\}$. Σύμφωνα λοιπόν με αυτή την προσέγγιση, έχουμε δύο υποθέσεις, τη θ_0 και τη θ_1, από τις οποίες η πρώτη αντιστοιχεί στην στατιστική κατανομή που ακολουθούν τα δεδομένα μας πριν από μια αλλαγή και η δεύτερη στην κατανομή που ακολουθούν αυτά μετά από μια αλλαγή. Ο έλεγχος που γίνεται βασίζεται στον λογάριθμο του ρυθμού πιθανοφάνειας (log-likelihood ratio) S_n

$$S_n = \sum_{i=1}^{n} s_i ,$$

όπου

$$s_i = \ln \frac{p_{\theta_1}(y_i)}{p_{\theta_0}(y_i)}.$$

Η τυπική συμπεριφορά ενός log-likelihood ratio S_n είναι να παρουσιάζει μείωση πριν συμβεί κάποια αλλαγή και να αυξάνεται από τη στιγμή που έχουμε μια

αλλαγή και μετά. Για τον λόγο αυτό, ο έλεγχος για τον εντοπισμό σημείου αλλαγής βρίσκεται στη μέτρηση της διαφοράς μεταξύ του της τρέχουσας τιμής του Log-likelihood ratio και της μικρότερης τιμής που αυτό παρουσίασε στο παρελθόν. Επομένως, η συνθήκη συναγερμού για τον αλγόριθμο CUSUM είναι:

Εάν $g_n \geq h$ τότε σημαίνεται συναγερμός τη χρονική στιγμή *n,*

όπου

$$g_n = S_n - m_n$$

και

$$m_n = \min_{1 \leq j \leq n} S_j .$$

Η παράμετρος *h* εκφράζει ένα κατώφλι.

Υποθέτουμε πως οι $\{y_i\}$ είναι ανεξάρτητες και τυχαίες Gaussian μεταβλητές [34], με γνωστή διασπορά σ^2, την οποία θεωρούμε σταθερή μετά το σημείο αλλαγής και μ_0 και μ_1 η μέση τιμή πριν και μετά την αλλαγή αντίστοιχα. Έτσι, $\theta_0 = N(\mu_0, \sigma^2)$ και $\theta_1 = N(\mu_1, \sigma^2)$. Έτσι, προκύπτει:

$$g_n = [g_{n-1} + \frac{\mu_1 - \mu_0}{\sigma^2}(y_n - \frac{\mu_1 + \mu_0}{2})]^+ . \quad (1)$$

Όπως αναφέραμε, θεωρούμε πως οι $\{y_i\}$ είναι ανεξάρτητες και τυχαίες Gaussian μεταβλητές, κάτι το οποίο όμως δεν αληθεύει για μετρήσεις δικτυακής κίνησης. Αυτό οφείλεται στην εποχικότητα (εβδομαδιαίες και ημερήσιες διακυμάνσεις της κίνησης), σε γενικότερες τάσεις που επικρατούν και σε συσχετίσεις στο χρόνο. Επομένως, θα πρέπει να αφαιρέσουμε αυτή τη μη σταθερή συμπεριφορά που παρουσιάζουν τα δεδομένα μας, πριν εφαρμόσουμε σε αυτά τον αλγόριθμο CUSUM. Έτσι, αφαιρούμε την εποχικότητα και τις τάσεις που επικρατούν χρησιμοποιώντας τον αλγόριθμο Holt-Winters και τις χρονικές συσχετίσεις χρησιμοποιώντας το μοντέλο αυτοπαλινδρόμησης (autoregressive).

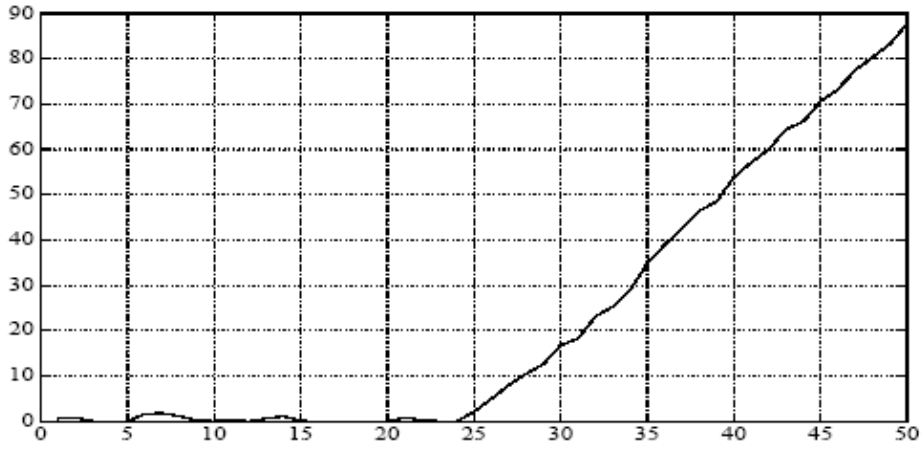
Πειράματα που έγιναν ωστόσο τα οποία θα περιγράψουμε και θα παρουσιάσουμε τα αποτελέσματά τους αναλυτικότερα στη συνέχεια, έδειξαν πως χρησιμοποιώντας την παραπάνω προσέγγιση, έχουμε πολύπλοκους και ιδιαίτερα χρονοβόρους υπολογισμούς, ενώ ταυτόχρονα το κέρδος που αποκομίζουμε είναι ελάχιστο συγκρίνοντας το αποτέλεσμα αυτής της προσέγγισης με αυτό που έχουμε αν κάνουμε χρήση απλούστερων μεθόδων. Για το λόγο αυτό χρησιμοποιούμε μια απλούστερη μέθοδο: Εφαρμόζουμε τον αλγόριθμο CUSUM στα δεδομένα $\tilde{x}_n$, όπου

$$\tilde{x}_n = x_n - \overline{\mu}_{n-1},$$

$\tilde{x}_n$ είναι η μετρική που χρησιμοποιούμε (πλήθος των SYN πακέτων) στο n-οστό χρονικό διάστημα και $\overline{\mu}_n$ είναι μια εκτίμηση του μέσου ρυθμού στη χρονική στιγμή *n*, η οποία υπολογίζεται χρησιμοποιώντας EWMA όπως και προηγουμένως. Η μέση τιμή της $\tilde{x}_n$ πριν από κάποια αλλαγή είναι μηδέν, γι' αυτό και η μέση τιμή της (1) είναι $\mu_0 = 0$. Τέλος, θα πρέπει να αναφερθούμε και στην τιμή του μ_1, δηλαδή της μέσης τιμής του ρυθμού της κίνησης μετά την αλλαγή. Επειδή αυτό δε μπορούμε να το γνωρίζουμε εκ των προτέρων, το προσεγγίζουμε με το μέγεθος $a\overline{\mu}_n$, όπου, όπως προαναφέραμε, η μέση τιμή $\overline{\mu}_n$ ανανεώνεται χρησιμοποιώντας EWMA και α είναι μια παράμετρος που εκφράζει το ποσοστό του πλάτους (amplitude) και που διαισθητικά αντιστοιχεί στο πιο πιθανό ποσοστό της αύξησης της μέσης τιμής μετά από μια επίθεση (σημείο αλλαγής). Έτσι, η (1) γίνεται:

$$g_n = [g_{n-1} + \frac{a\overline{\mu}_{n-1}}{\sigma^2}(x_n - \overline{\mu}_{n-1} - \frac{a\overline{\mu}_{n-1}}{2})]^+.$$

Οι παράμετροι οι οποίες μεταβάλλονται στον αλγόριθμο αυτόν είναι η παράμετρος α που εκφράζει το ποσοστό του εύρους (amplitude), το κατώφλι συναγερμού *h*, ο συντελεστής EWMA β και το μέγεθος του χρονικού διαστήματος στο οποίο παίρνουμε τις μετρήσεις μας. Οι παράμετροι αυτές είναι οι ίδιες με αυτές του προηγούμενου αλγόριθμου, εκτός από το *h*, το οποίο είναι το κατώφλι συναγερμού στον αλγόριθμο CUSUM, ενώ το κατώφλι συναγερμού στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού ήταν ο αριθμός των συνεχόμενων παραβιάσεων *k* του κατωφλιού.



Σχήμα 5: Μεταβολή της μεταβλητής g του αλγόριθμου CUSUM και απότομη αύξησή της στην περίπτωση που συναντάται ανώμαλη συμπεριφορά

4.4 Παραλλαγή του αλγόριθμου CUSUM

Στον αλγόριθμο CUSUM που μόλις περιγράψαμε, θεωρείται πως η λειτουργία του αλγορίθμου σταματάει όταν βρεθεί κάποιο σημείο αλλαγής – ανωμαλίας. Αυτό σημαίνει ότι σημαίνεται συναγερμός και στη συνέχεια οι μεταβλητές που χρησιμοποιούνται στην υλοποίηση του αλγορίθμου μηδενίζονται. Μηδενίζεται δηλαδή και η μεταβλητή g η οποία συγκρίνεται κάθε χρονική στιγμή με το αντίστοιχο κατώφλι. Έτσι ο αλγόριθμος λειτουργεί ξανά από την αρχή και προσπαθεί να εντοπίσει σημεία ανωμαλίας ξεχνώντας όλα όσα συνέβησαν μέχρι τη στιγμή εκείνη.
Μια παραλλαγή του αλγόριθμου αυτού είναι να μη θεωρεί ο αλγόριθμος ότι έφτασε σε επιτυχία, εντόπισε δηλαδή σημείο αλλαγής, όταν παραβιαστεί το κατώφλι από την τιμή της μεταβλητής g μία μόνο φορά αλλά k συνεχόμενες φορές.

Για να υλοποιηθεί αυτή η παραλλαγή του αλγορίθμου, όταν παραβιάζεται πρώτη φορά το κατώφλι, θεωρείται πως αυτό αποτελεί ένδειξη ανωμαλίας, η οποία όμως δε χρίζει άμεσης αντιμετώπισης. Για το λόγο αυτό, οι μεταβλητές δε μηδενίζονται, αλλά η συγκεκριμένη τιμή την οποία απέκτησε η μεταβλητή g και προκάλεσε την υπέρβαση του κατωφλιού αγνοείται και συνεχίζεται κανονικά η λειτουργία του αλγορίθμου. Με άλλα λόγια, σε αυτή την περίπτωση χρησιμοποιείται η συνθήκη

$$g_n = [g_{n-2} + \frac{a\overline{\mu}_{n-2}}{\sigma^2}(x_n - \overline{\mu}_{n-2} - \frac{a\overline{\mu}_{n-2}}{2})]^+$$

ή γενικότερα

$$g_n = [g_{n-k} + \frac{a\overline{\mu}_{n-k}}{\sigma^2}(x_n - \overline{\mu}_{n-k} - \frac{a\overline{\mu}_{n-k}}{2})]^+$$

όπου k είναι η χρονική στιγμή στην οποία είχαμε τελευταία φορά παρατηρήσει φυσιολογική συμπεριφορά στα προς μελέτη δεδομένα (τελευταία χρονική στιγμή όπου δεν υπήρξε παραβίαση του κατωφλιού). Συναγερμός τελικά σημαίνεται όταν παρατηρείται παραβίαση του κατωφλιού για πολλές συνεχόμενες φορές (k). Δηλαδή:

$$\sum_{i=n-k+1}^{n} 1_{\{g_n > h\}} \geq k$$

Αυτή η παραλλαγή του αλγορίθμου CUSUM θεωρήσαμε πως είναι άκρως ενδιαφέρουσα και πως θα έλυνε κάποια προβλήματα τα οποία τυχόν παρουσιάζονταν εάν χρησιμοποιούσαμε αποκλειστικά και μόνο την προηγούμενη εκδοχή του αλγορίθμου.

Η κίνηση σε ένα δίκτυο, και γενικότερα στο Διαδίκτυο, δε μπορεί να χαρακτηριστεί σε καμία περίπτωση «ομαλή», με σταθερό ρυθμό ή προβλέψιμη. Αντίθετα, τις περισσότερες των φορών παρατηρούνται εκρήξεις στην κίνηση οι οποίες συνήθως είναι φυσιολογικές, δεν προέρχονται από κακόβουλους χρήστες και δεν αποτελούν τμήματα κάποιας επίθεσης. Τις περισσότερες δε φορές, αυτές οι εκρήξεις είναι στιγμιαίες, ή χαρακτηρίζονται από την πολύ μικρή διάρκειά τους.

Χρησιμοποιώντας λοιπόν τον αλγόριθμο με την πρώτη του μορφή, θα μπορούσαμε να οδηγηθούμε σε ένα, αρκετά μεγάλο ίσως, αριθμό από λανθασμένους συναγερμούς στην περίπτωση που η κίνηση του συνδέσμου που μελετούμε παρουσίαζε εκρηκτική συμπεριφορά. Με τη νέα όμως αυτή προσέγγιση την οποία παρουσιάσαμε, τα φαινόμενα αυτά αποφεύγονται, εφόσον ο αλγόριθμος δε σημαίνει συναγερμό με την πρώτη ένδειξη που τυχόν αυτός έχει για ανωμαλία, αλλά μόνο αφού αυτός έχει «βεβαιωθεί» για την ύπαρξη ανωμαλίας, δεδομένου ότι ο συναγερμός σημαίνεται μετά από πολλές συνεχόμενες παραβιάσεις του κατωφλιού.

Εκτός όμως από την κίνηση η οποία παρατηρείται σε ένα δίκτυο, είναι πιθανό και οι επιθέσεις άρνησης υπηρεσίας και συγκεκριμένα τύπου TCP SYN flooding οι οποίες εξαπολύονται εναντίον του δικτύου αυτού να μην παρουσιάζουν μια σταθερότητα στη μορφή τους. Με άλλα λόγια, είναι δυνατό, κατά τη διάρκεια μιας επίθεσης, η ανωμαλία που παρουσιάζεται να μην έχει σταθερή ένταση, αλλά να αυξομειώνεται, με αποτέλεσμα να μην προκαλείται συνεχόμενη παραβίαση του κατωφλιού για πολλές συνεχόμενες χρονικές στιγμές.

Μια λύση στο πρόβλημα αυτό θα μπορούσε να δώσει μια ακόμη παραλλαγή του αλγορίθμου CUSUM, όμοια με την προηγούμενη, με μια μόνο διαφορά στη συνθήκη σήμανσης συναγερμού: Και σε αυτή την περίπτωση ο αλγόριθμος δε σταματά την πρώτη φορά που συναντάει παραβίαση του ορίου που έχει τεθεί, αλλά ελέγχει εάν σε χρονικό διάστημα k χρονικών στιγμών έχει παραβιαστεί το κατώφλι t φορές ($t \leq k$), όχι κατ' ανάγκη συνεχόμενες. Με άλλα λόγια:

$$\sum_{i=n-k+1}^{n} 1_{\{g_n > h\}} \geq t$$

Θεωρούμε πως οι παραλλαγές αυτές του αλγόριθμου CUSUM αποτελούν ιδιαίτερα αξιόλογες προτάσεις όσον αφορά στον εντοπισμό επιθέσεων άρνησης υπηρεσίας. Δεδομένου ότι οι επιθέσεις αυτού του είδους επιδεικνύουν μια αξιόλογη διάρκεια (ακόμα και όταν σε αυτή τη διάρκεια παρατηρούνται διαστήματα παύσης), πιστεύουμε πως είναι ασφαλέστερο να υλοποιηθεί ο προαναφερθείς αλγόριθμος με μια από τις παραπάνω μορφές του, έτσι ώστε να ελαχιστοποιηθεί η πιθανότητα της σήμανσης λανθασμένων συναγερμών, επιτυγχάνοντας παράλληλα τον εντοπισμό των περισσότερων δυνατόν πραγματικών επιθέσεων.

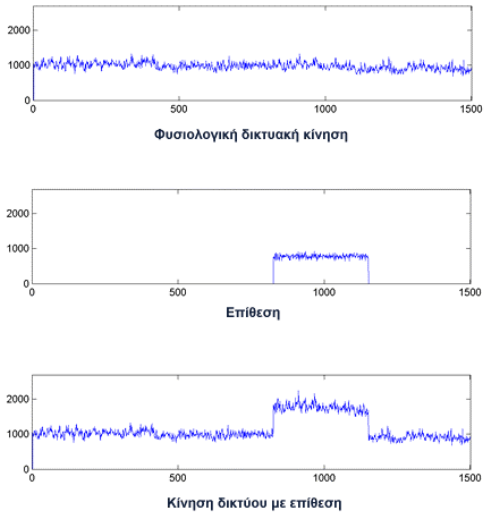
Μειονέκτημα βέβαια της προσέγγισης αυτής αποτελεί το γεγονός πως αυξάνεται η καθυστέρηση εντοπισμού, δεδομένου ότι υπάρχει ειδοποίηση για πιθανή επίθεση μετά από έναν προκαθορισμένο αριθμό παραβιάσεων του κατωφλιού, θεωρούμε όμως πως η καθυστέρηση αυτή, αν τεθούν οι κατάλληλες παράμετροι στον αλγόριθμο, μπορεί να ρυθμιστεί έτσι ώστε το μέγεθος της καθυστέρησης να κυμαίνεται μέσα σε αποδεκτά όρια, ώστε να είναι δυνατή η έγκαιρη αντιμετώπιση της επίθεσης από τους διαχειριστές του δικτύου πριν αυτή προκαλέσει ιδιαίτερο πρόβλημα.

5 Μορφές Επιθέσεων Άρνησης Υπηρεσίας τύπου SYN flooding

5.1 Επιθέσεις απότομες

Μια μορφή επίθεσης TCP SYN flooding, από τις πιο απλοϊκές, αλλά και από τις πιο συνηθισμένες παράλληλα, είναι η επίθεση κατά την οποία ο επιτιθέμενος στέλνει ξαφνικά μεγάλο πλήθος από SYN πακέτα προς το θύμα, συνεχόμενα, με σταθερό υψηλό ρυθμό, για κάποιο ικανό χρονικό διάστημα. Έτσι, το θύμα αιφνιδιάζεται,

κατακλύζεται από SYN πακέτα, με τελικό αποτέλεσμα σε σύντομο χρονικό διάστημα να μη μπορεί να αντιδράσει στο μεγάλο πλήθος πακέτων που δέχεται και τελικά να αδυνατεί να προσφέρει την απαιτούμενη ποιότητα υπηρεσίας στους χρήστες.



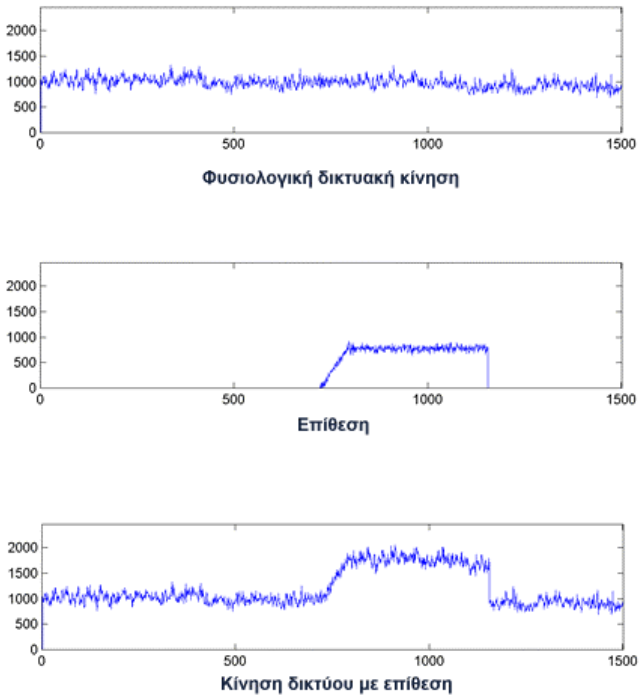
Σχήμα 6: Απλή Επίθεση

5.2 Επιθέσεις με κλίση

Οι επιθέσεις άρνησης υπηρεσίας δεν εμφανίζονται πάντοτε απότομα όπως στην προηγούμενη περίπτωση, αλλά πολλές φορές ξεκινούν από χαμηλούς ρυθμούς και αυξάνουν σταδιακά το ρυθμό τους. Βασικός σκοπός των επιθέσεων αυτών είναι να «ξεγελάσουν» κατά κάποιο τρόπο το σύστημα εντοπισμού των επιθέσεων, έτσι ώστε αυτές είτε να μη γίνουν καθόλου αντιληπτές από τους διαχειριστές του συστήματος-στόχου, είτε η καθυστέρηση στον εντοπισμό τους να είναι αξιόλογη, γεγονός που μπορεί να οδηγήσει στη μη έγκαιρη αντιμετώπισή τους.

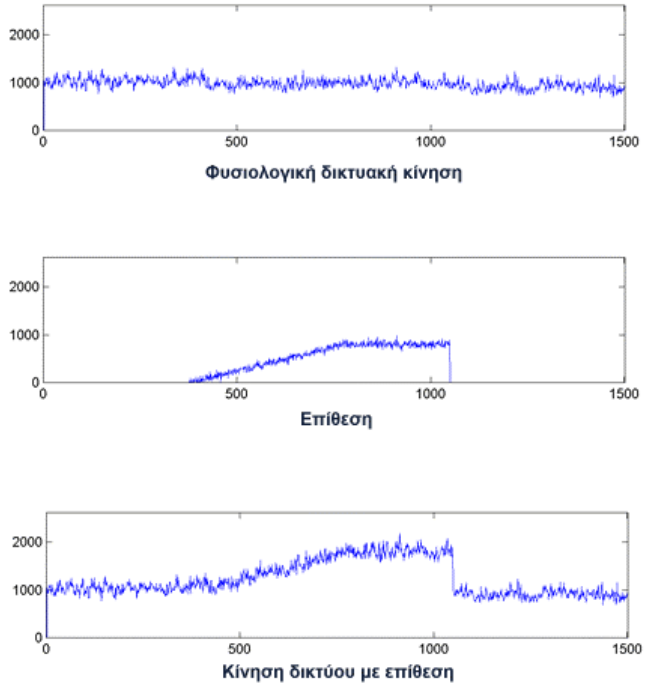
Στο σημείο αυτό θα πρέπει να αναφερθεί το γεγονός ότι και πάλι οι επιθέσεις άρνησης υπηρεσίας με κλίση, μπορούν να χωριστούν σε δύο γενικές υποκατηγορίες:

- Τις επιθέσεις στις οποίες η σταδιακή αύξηση του ρυθμού αποστολής δε διαρκεί πολύ και η επίθεση φτάνει στο ύψιστο σημείο της μέσα σε σύντομο χρονικό διάστημα από τη στιγμή εξαπόλυσής της.



Σχήμα 7: Επίθεση με κλίση μικρής διάρκειας

- Τις επιθέσεις στις οποίες η σταδιακή αυτή αύξηση του ρυθμού αποστολής έχει μεγάλη διάρκεια, δηλαδή η επίθεση φτάνει αρκετή ώρα μετά την έναρξή της στο μέγιστο ρυθμό αποστολής πακέτων προς το θύμα.



Σχήμα 8: Επίθεση με κλίση μεγάλη διάρκειας

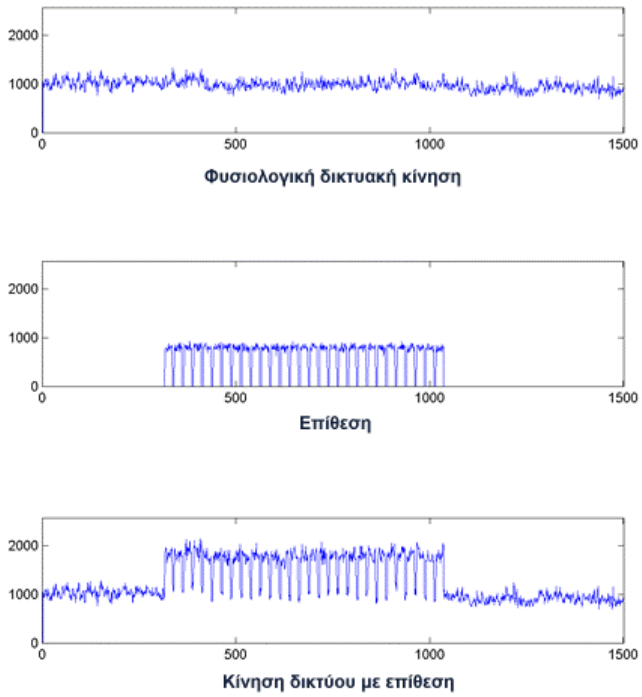
Οι επιθέσεις της μορφής αυτής πραγματοποιούνται κυρίως προκειμένου να αποφευχθεί ο εντοπισμός τους από συστήματα εντοπισμού επιθέσεων τα οποία χρησιμοποιούν αλγόριθμους εκμάθησης της φυσιολογικής συμπεριφοράς των δεδομένων με βάση το παρελθόν.

Έτσι, οι επιθέσεις αυτές προσπαθούν να εκμεταλλευτούν το προαναφερθέν χαρακτηριστικό των αλγορίθμων εντοπισμού και, ιδιαίτερα οι επιθέσεις της πρώτης υποκατηγορίας, να λειτουργήσουν με τέτοιο τρόπο ώστε να εκπαιδεύσουν τον αλγόριθμο εντοπισμού έτσι ώστε να θεωρεί φυσιολογική την κατάσταση της επίθεσης: Αυξάνοντας με αργό ρυθμό η επίθεση την έντασή της, ο αλγόριθμος εκπαιδεύεται και θεωρεί μια τέτοια μικρή αύξηση του ρυθμού άφιξης πακέτων φυσιολογική και αναμενόμενη. Από τη στιγμή λοιπόν που δεν παρατηρείται κάποια απότομη αύξηση στο πλήθος των πακέτων που καταλήγουν στο θύμα, αυτό δεν είναι σε θέση να αντιληφθεί την επίθεση η οποία υποκρύπτεται.

5.3 Επιθέσεις με διακοπές στην αποστολή πακέτων

Μια ακόμη μορφή επιθέσεων άρνησης υπηρεσίας η οποία στοχεύει στο να μη γίνει αντιληπτή από τα συστήματα εντοπισμού επιθέσεων είναι αυτή κατά την οποία ο επιτιθέμενος δε στέλνει για κάποιο χρονικό διάστημα συνεχώς TCP SYN πακέτα στο υποψήφιο θύμα, αλλά διακόπτει την αποστολή αυτή των κακόβουλων πακέτων για μικρά χρονικά διαστήματα.

Οι επιθέσεις αυτής της μορφής έχουν ως σκοπό να μη γίνουν αντιληπτές κυρίως από συστήματα τα οποία, προκειμένου να μειώσουν το ποσοστό λανθασμένων σημάνσεων συναγερμού, σημαίνουν συναγερμό αφού έχει παραβιαστεί η οποιαδήποτε συνθήκη έχουν θέσει ως συνθήκη συναγερμού, πολλές φορές συνεχόμενα. Έτσι, μια επίθεση η οποία ανα τακτά διαστήματα σταματά την αποστολή πακέτων προς το θύμα, δεν πληροί σε μεγάλα διαστήματα τη συνθήκη σήμανσης συναγερμού του συστήματος εντοπισμού επιθέσεων, ενώ ταυτόχρονα πλημμυρίζει το θύμα με κίνηση πολλαπλάσια της κανονικής, ικανής να δημιουργήσει προβλήματα στην κανονική λειτουργία του.



Σχήμα 9: Επιθέσεις με διακοπές στην αποστολή πακέτων

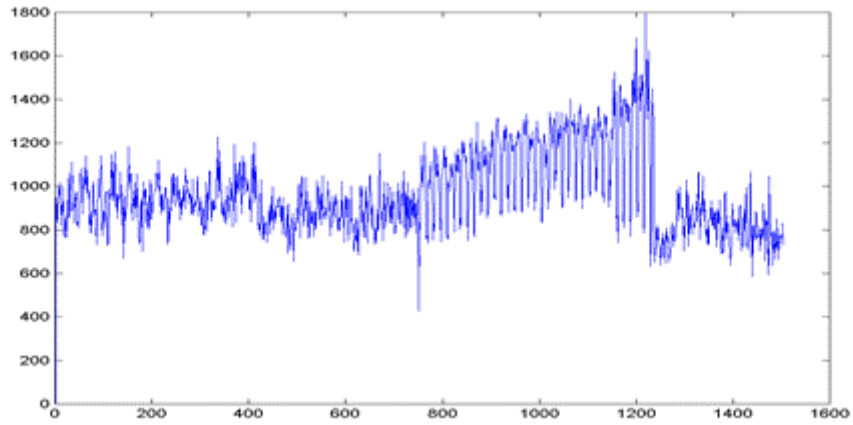
5.4 Επιθέσεις μικρής/μεγάλης έντασης

Στο σημείο αυτό θα πρέπει να αναφερθεί το γεγονός ότι ένας άλλος διαχωρισμός που γίνεται στις επιθέσεις άρνησης υπηρεσίας και ειδικότερα στις επιθέσεις τύπου SYN flooding, είναι το ότι υπάρχουν επιθέσεις πολύ υψηλής έντασης, αλλά και επιθέσεις χαμηλότερης έντασης. Οι επιθέσεις της πρώτης κατηγορίας κατακλύζουν το υποψήφιο θύμα με πακέτα που χαρακτηρίζονται από ιδιαίτερα υψηλό ρυθμό άφιξης ενώ οι επιθέσεις που ανήκουν στη δεύτερη κατηγορία διακρίνονται από ένταση η οποία δεν είναι αξιοσημείωτα μεγάλη, η αύξηση δηλαδή που παρατηρείται στο ρυθμό άφιξης των πακέτων στο θύμα δεν είναι πολύ μεγαλύτερη από το φυσιολογικό ρυθμό άφιξης πακέτων σε αυτό.

Όπως είναι προφανές οι επιθέσεις μεγάλης έντασης γίνονται ευκολότερα και γρηγορότερα αντιληπτές από τα συστήματα εντοπισμού επιθέσεων, καταφέρνουν όμως παρόλα αυτά πολλές φορές να δημιουργήσουν σοβαρό πρόβλημα, διότι ακριβώς επειδή η έντασή τους είναι αξιοσημείωτα μεγάλη, μπορούν και προξενούν προβλήματα μέσα σε πολύ μικρό χρονικό διάστημα, πολλές φορές μικρότερο από το χρονικό διάστημα που μεσολαβεί από τη στιγμή έναρξης της επίθεσης μέχρι τον εντοπισμό της και την αντιμετώπισή της από τους διαχειριστές του συστήματος.

Αντίθετα, οι επιθέσεις μικρότερης έντασης, είναι δυσκολότερες και πιο χρονοβόρες στον εντοπισμό τους από τα αντίστοιχα συστήματα. Η βασική τους ιδέα στηρίζεται στο γεγονός ότι μπορεί μεν να περάσει ένα αρκετά μεγάλο χρονικό διάστημα μέχρι να εντοπιστούν, στο μεταξύ όμως έχουν υπερφορτώσει για όλο αυτό το χρονικό διάστημα το υποψήφιο θύμα, το οποίο μπορεί να μην έχει καταρρεύσει εφόσον ο όγκος των δεδομένων που δέχεται δε θα είναι τόσο μεγάλος ώστε να το οδηγήσει σε κατάρρευση, είναι όμως ικανός να οδηγήσει το θύμα σε αύξηση του φόρτου του και πιθανότατα σε μείωση της ποιότητας υπηρεσίας που αυτό παρέχει στους χρήστες του.

Βέβαια, θα πρέπει να σημειωθεί ότι πολλές φορές στην πράξη παρατηρούνται μορφές επιθέσεων που δεν ανήκουν αμιγώς σε μια μόνο από τις προαναφερθείσες κατηγορίες, αλλά αποτελούν συνδυασμό αυτών. Για παράδειγμα, πολύ συχνό είναι το φαινόμενο να εξαπολύονται επιθέσεις με σταδιακή αύξηση που διαρκεί ένα μεγάλο χρονικό διάστημα και ταυτόχρονα ανήκουν στην κατηγορία των επιθέσεων μετριοπαθούς εντάσεως, ή ακόμα και στην κατηγορία των επιθέσεων που διακόπτουν τη λειτουργία τους.



Σχήμα 10: Επίθεση με κλίση αλλά και με διακοπές

6 Πειραματική Αξιολόγηση των Προτεινόμενων Αλγορίθμων

Στο κεφάλαιο αυτό αναλύεται και αξιολογείται η απόδοση των δύο αλγορίθμων που παρουσιάστηκαν στο προηγούμενο κεφάλαιο και οι οποίοι χρησιμοποιούνται στον εντοπισμό TCP SYN flooding επιθέσεων άρνησης υπηρεσίας.

Οι μετρικές απόδοσης με βάση τις οποίες αξιολογούμε τους αλγόριθμους αυτούς είναι η πιθανότητα εντοπισμού, το ποσοστό λαθών (λανθασμένων σημάνσεων συναγερμού) και η καθυστέρηση εντοπισμού. Εκτός όμως από τη μελέτη του βαθμού και είδους αλληλοεξάρτησης των μετρικών αυτών σε σχέση με την επιλογή των παραμέτρων των αλγορίθμων, γίνεται προσπάθεια, στην παρούσα μελέτη, να διερευνηθεί η επιρροή τόσο των παραμέτρων των αλγορίθμων εντοπισμού όσο και των χαρακτηριστικών της εκάστοτε επίθεσης πάνω στην απόδοση των αλγορίθμων αυτών.

Προκειμένου να μελετήσουμε πειραματικά την απόδοση των αλγορίθμων εντοπισμού, χρησιμοποιήσαμε πραγματική δικτυακή κίνηση.

Η κίνηση αυτή προέρχεται από δεδομένα που συλλέχθηκαν από το εργαστήριο MIT Lincoln (MIT Lincoln Laboratory) και από δεδομένα που συλλέχθηκαν από το κέντρο δικτύου του Πανεπιστημίου Κρήτης. Τα δεδομένα από το εργαστήριο του MIT ήταν δεδομένα δύο ημερών, κάθε μέρα από τις οποίες περιλάμβανε 11 ώρες κατά τις οποίες συλλέγονταν πακέτα (08:00-19:00). Η κίνηση που προέρχεται από δεδομένα του Πανεπιστημίου Κρήτης, αποτελείται από δεδομένα 14,5 ωρών (16:30-07:00). Η αρχική μας προσέγγιση ήταν να μελετηθεί η απόδοση των αλγορίθμων χρησιμοποιώντας ως μετρήσεις το πλήθος των TCP SYN πακέτων σε χρονικά διαστήματα των 10 δευτερολέπτων.

Οι επιθέσεις τις οποίες προσπαθούμε να εντοπίσουμε με τη βοήθεια των αλγορίθμων δημιουργήθηκαν με συνθετικό τρόπο και στη συνέχεια εισήχθησαν στα δεδομένα που προαναφέραμε. Αυτό συνέβη προκειμένου να είμαστε σε θέση να ελέγχουμε τα χαρακτηριστικά των εκάστοτε προς εντοπισμό επιθέσεων και επομένως να μπορέσουμε να διερευνήσουμε την απόδοση που παρουσιάζουν οι αλγόριθμοι εντοπισμού όταν αυτοί καλούνται να ανιχνεύσουν και να εντοπίσουν διαφορετικά είδη επιθέσεων. Η διάρκεια κάθε επίθεσης ακολουθούσε κανονική κατανομή με μέσο όρο 60 χρονικά διαστήματα (συνολική διάρκεια δηλαδή περίπου δέκα λεπτά της ώρας δεδομένου ότι χρησιμοποιήθηκαν χρονικά διαστήματα των δέκα δευτερολέπτων) και διασπορά 10 χρονικά διαστήματα.

Χρησιμοποιήθηκαν και μελετήθηκαν όχι μόνο επιθέσεις των οποίων η ένταση αυξάνεται απότομα, δηλαδή επιθέσεις οι οποίες φτάνουν στη μέγιστη έντασή τους μέσα σε ένα μόνο χρονικό διάστημα που αντιπροσωπεύει 10 δευτερόλεπτα, αλλά και επιθέσεις των οποίων η ένταση αυξάνεται σταδιακά. Ο χρόνος μεταξύ των αφίξεων των επιθέσεων ακολουθούσε την εκθετική κατανομή, με μέση τιμή τα 400 χρονικά

διαστήματα, περίπου δηλαδή 67 λεπτά της ώρας θεωρώντας πάντοτε ως δεδομένο το γεγονός ότι χρησιμοποιήθηκαν χρονικά διαστήματα των 10 δευτερολέπτων). Το αποτέλεσμα όλων των παραπάνω ήταν να δημιουργηθούν 8 περίπου επιθέσεις κατά τη διάρκεια μιας ημέρας όταν χρησιμοποιήθηκαν τα δεδομένα από το εργαστήριο του MIT [35], [36] και 11 περίπου επιθέσεις στην περίπτωση που χρησιμοποιήθηκαν τα δεδομένα από το κέντρο δικτύου του Πανεπιστημίου Κρήτης [37]. Τα αποτελέσματα προέκυψαν μετά την εκτέλεση των πειραμάτων (δημιουργία των επιθέσεων και εφαρμογή των αλγορίθμων) 50 συνεχόμενες φορές και λαμβάνοντας ένα διάστημα εμπιστοσύνης 95%.

Οι προαναφερθείσες τιμές, όσον αφορά στα χαρακτηριστικά των επιθέσεων οι οποίες δημιουργήθηκαν, προέκυψαν με βάση τις αντίστοιχες τιμές που παρατηρούνται σε πραγματικές επιθέσεις στο Διαδίκτυο [17]. Σύμφωνα λοιπόν με μελέτες, μια τυπική επίθεση άρνησης υπηρεσίας διαρκεί από 3 έως 20 λεπτά της ώρας, ενώ ταυτόχρονα ακολουθεί την κανονική κατανομή.

Όλα τα πειράματα έγιναν σε περιβάλλον Matlab [38] (MATrix LABoratory). Το Matlab είναι ένα μαθηματικό πακέτο αλλά και μια γλώσσα προγραμματισμού υψηλού επιπέδου για τη μελέτη κάθε είδους μαθηματικών συναρτήσεων. Αποτελεί επίσης ένα σύστημα επεξεργασίας πινάκων και συναρτήσεών τους για εφαρμογές αριθμητικής ανάλυσης και γραφικής παρουσίασης των αποτελεσμάτων. Δημιουργήθηκε από τον C. Moler, αρχικά σαν ένα εργαλείο διαχείρισης των βιβλιοθηκών Fortran [39]. Βασικό του αντικείμενο είναι οι πίνακες.

Εξελίχθηκε σε σύνθετο πακέτο (γραμμένο σε γλώσσα C, C++ [40]) για:

- Επίλυση αριθμητικών προβλημάτων μικρού και μεσαίου μεγέθους, χωρίς να απαιτείται προγραμματισμός σε συμβατικές γλώσσες προγραμματισμού (Fortran, C).
- Γρήγορα ανάπτυξη και δοκιμή αλγορίθμων, καθώς διαθέτει πλήθος έτοιμων συναρτήσεων και απλουστευμένη αλγοριθμική γλώσσα.
- Παρουσίαση των αποτελεσμάτων με γραφικό τρόπο.

Η μελέτη αυτή, έχει πραγματοποιηθεί λοιπόν σε περιβάλλον Matlab, όπου δημιουργήθηκαν διαφορετικά .m αρχεία, καθένα από τα οποία αποτελούσε υλοποίηση μιας μορφής των αλγορίθμων. Δημιουργήθηκε επίσης αρχείο το οποίο δημιουργεί τις συνθετικές επιθέσεις οι οποίες προστίθενται στη συνέχεια στα πραγματικά δεδομένα που έχουμε στην κατοχή μας, είτε από το εργαστήριο του MIT,

είτε από το Κέντρο Δικτύου του Πανεπιστημίου Κρήτης. Υλοποιήθηκαν επίσης μηχανισμοί, πάντα σε περιβάλλον Matlab, για τον αυτόματο υπολογισμό της Πιθανότητας Εντοπισμού μιας επίθεσης από τους αλγορίθμους, του Ποσοστού Εσφαλμένων Συναγερμών αλλά και της Καθυστέρησης στον Εντοπισμό μιας επίθεσης που τυχόν αυτοί παρουσιάζουν.

6.1 Επιθέσεις Μεγάλης Έντασης

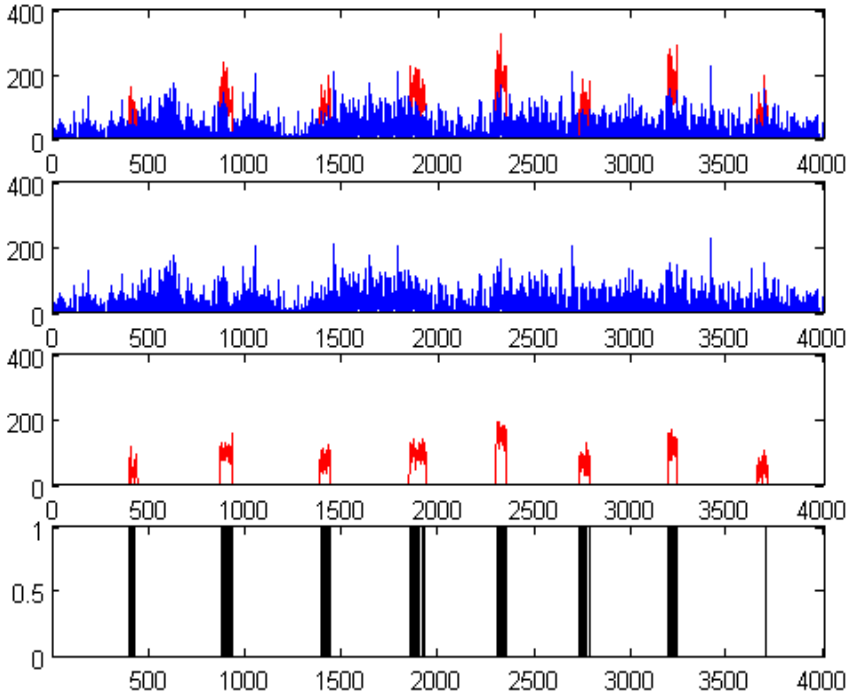
Κάποια πρώτα πειράματα που διεξήχθησαν, αφορούσαν σε επιθέσεις αξιοσημείωτα υψηλής έντασης, των οποίων ο μέσος ρυθμός αποστολής πακέτων ήταν 250% υψηλότερος από ότι ο μέσος ρυθμός της κίνησης, ο οποίος ήταν 31.64 SYN πακέτα σε μια μονάδα χρόνου. Ως μονάδα χρόνου ορίστηκαν τα δέκα δευτερόλεπτα.
Όσον αφορά στα δεδομένα του εργαστηρίου του MIT, οι παράμετροι οι οποίες επιλέχθηκαν μετά από δοκιμές και οι οποίες αποδείχθηκαν πως ήταν αυτές οι οποίες απέδιδαν τα βέλτιστα αποτελέσματα για τον αλγόριθμο προσαρμοζόμενου κατωφλιού ήταν $\alpha = 0.5$, $k = 4$, και $\beta = 0.98$. Οι αντίστοιχες παράμετροι για τον αλγόριθμο CUSUM ήταν $\alpha = 0.5$, $h = 5$, και $\beta = 0.98$.

Τα σχήματα 11 και 12 παρουσιάζουν τα αποτελέσματα μετά την εφαρμογή στα δεδομένα στα οποία προστέθηκαν οι επιθέσεις για τον αλγόριθμο προσαρμοζόμενου κατωφλιού και για τον αλγόριθμο CUSUM αντίστοιχα. Στα πειράματα αυτά, χρησιμοποιήθηκε η μορφή του CUSUM κατά την οποία η μεταβλητή g μηδενίζεται κάθε φορά που αυτή ξεπερνάει το προκαθορισμένο κατώφλι και σημαίνεται συναγερμός. Ο οριζόντιος άξονας στα σχήματα αυτά εκφράζει τον αριθμό των μονάδων χρόνου, επομένως η μονάδα χρόνου 0 και η 4000 αντιστοιχούν περίπου στην ώρα 08:00 και 19:00 αντίστοιχα.

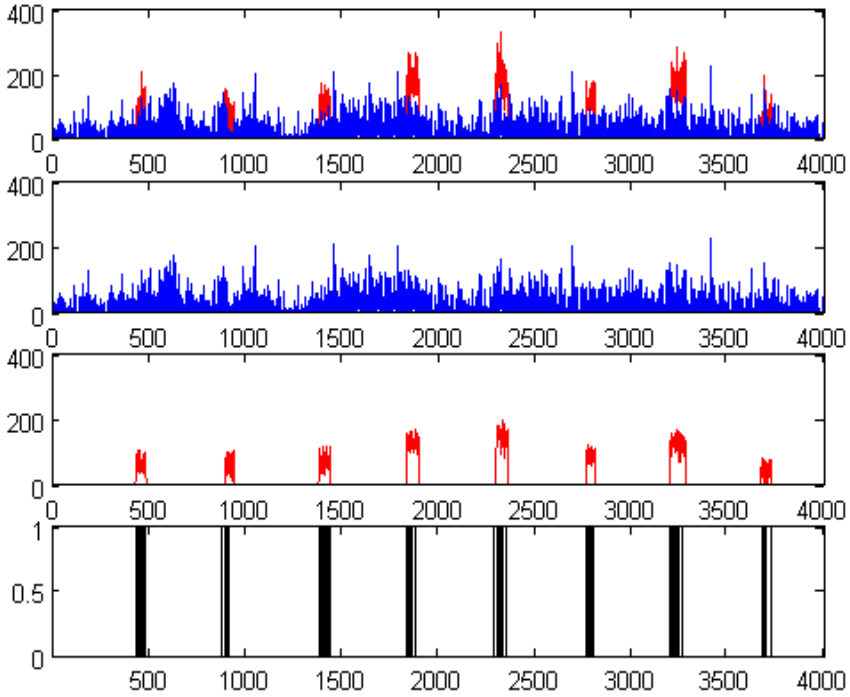
Σε κάθε γράφημα, και ακολουθώντας φορά από πάνω προς τα κάτω, παρουσιάζονται η αρχική κίνηση (τα αρχικά μας δεδομένα μαζί με τις επιθέσεις), η αρχική κίνηση, οι επιθέσεις μεμονωμένα, και τελικά, το τελευταίο γράφημα παρουσιάζει τα χρονικά διαστήματα στα οποία ο εκάστοτε αλγόριθμος συνάντησε σημείο ανωμαλίας και σημάνθηκε συναγερμός.

Τα παρακάτω σχήματα φανερώνουν ότι τόσο ο αλγόριθμος προσαρμοζόμενου κατωφλιού όσο και ο αλγόριθμος CUSUM επιδεικνύουν άριστη απόδοση στην περίπτωση που έχουμε επιθέσεις υψηλής έντασης, εφόσον και οι δύο αλγόριθμοι είχαν σαν αποτέλεσμα 100% πιθανότητα εντοπισμού και μηδενικό ποσοστό

λανθασμένων συναγερμών. Η καθυστέρηση στον εντοπισμό επίσης των δυο ήταν εντελώς παρόμοια, 3.01 και 2.75 μονάδες χρόνου αντίστοιχα.



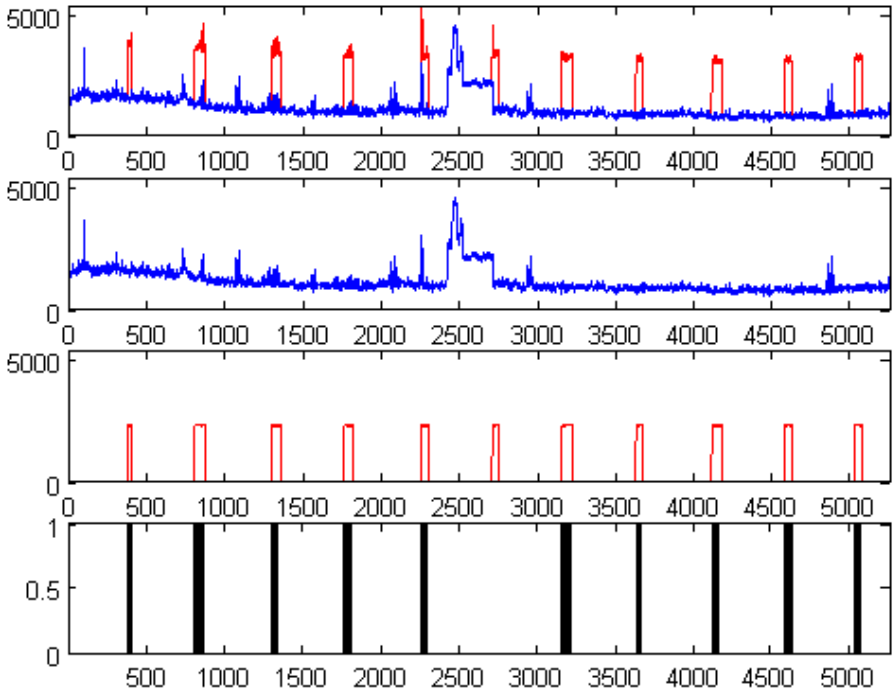
Σχήμα 11: Αλγόριθμος Προσαρμοζόμενου Κατωφλιού - Επιθέσεις μεγάλης κλίμακας



Σχήμα 12: Αλγόριθμος CUSUM - Επιθέσεις μεγάλης κλίμακας

Όσον αφορά στα δεδομένα του Πανεπιστημίου Κρήτης, οι δύο αλγόριθμοι επιδεικνύουν και πάλι την ίδια συμπεριφορά, καθώς εντοπίζουν την ολότητα των επιθέσεων, παρουσιάζοντας ταυτόχρονα σχεδόν μηδενικό ποσοστό λαθών. Οι τιμές των παραμέτρων οι οποίες χρησιμοποιήθηκαν ήταν $\alpha = 0.5$, $h = 40$, και $\beta = 0.98$ για τον αλγόριθμο CUSUM και $\alpha = 0.5$, $k = 4$, και $\beta = 0.98$ για τον αλγόριθμο προσαρμοζόμενου κατωφλιού. Στην περίπτωση βέβαια αυτή, αξίζει να σημειωθεί ότι παρατηρείται μια αύξηση στην καθυστέρηση εντοπισμού όσον αφορά και στους δύο αλγορίθμους (4 και 4,5 μονάδες χρόνου για τον αλγόριθμο προσαρμοζόμενου κατωφλιού και τον αλγόριθμο CUSUM αντίστοιχα).

Στο σημείο αυτό θα πρέπει να κάνουμε την εξής επισήμανση: στα αρχικά δεδομένα του Πανεπιστημίου Κρήτης, πριν προσθέσουμε σε αυτά τις συνθετικές επιθέσεις, παρατηρούμε μία μεγάλη αύξηση στον όγκο των δεδομένων για ένα συγκεκριμένο χρονικό διάστημα, το οποίο διαρκεί μερικές μονάδες χρόνου. Θεωρούμε το γεγονός αυτό μια ανωμαλία που παρουσιάζουν τα δεδομένα μας, και γι' αυτό την αγνοούμε, και για τον λόγο αυτό αγνοούμε οποιαδήποτε σήμανση συναγερμού υπάρχει από οποιονδήποτε αλγόριθμο στην περιοχή αυτή και δεν την προσμετρούμε στον υπολογισμό ούτε της πιθανότητας εντοπισμού επίθεσης, αλλά ούτε και στον υπολογισμό των λανθασμένων συναγερμών οι οποίοι τυχόν σημαίνονται.



Σχήμα 13: Δεδομένα του Πανεπιστημίου Κρήτης - Εφαρμογή του αλγόριθμου CUSUM σε επιθέσεις μεγάλης κλίμακας

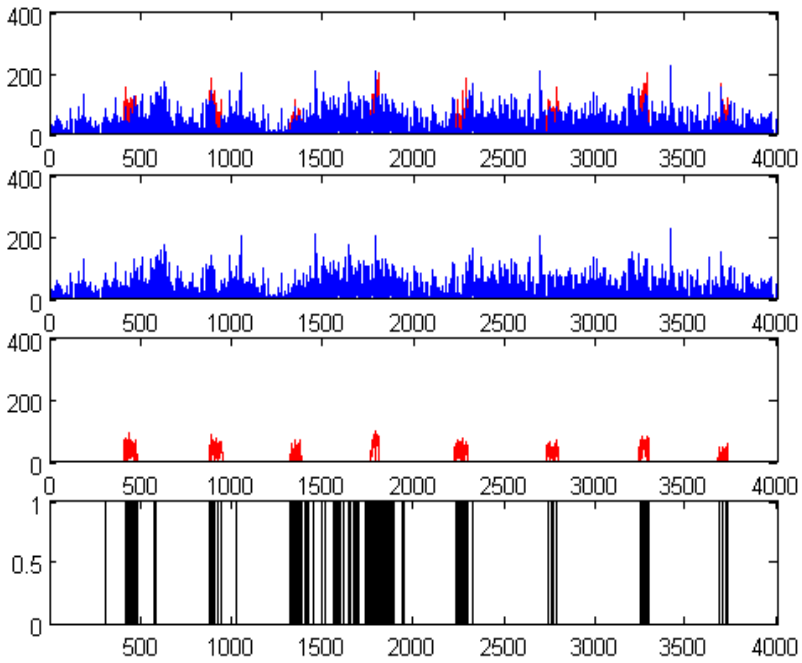
6.2 Επιθέσεις χαμηλής έντασης

Στη συνέχεια διερευνούμε την απόδοση τον αλγορίθμων όσον αφορά στην πιθανότητα εντοπισμού των επιθέσεων χαμηλής έντασης. Οι επιθέσεις αυτές χαρακτηρίζονται από μέσο ρυθμό αποστολής πακέτων 50% υψηλότερο από το μέσο ρυθμό της πραγματικής κίνησης.

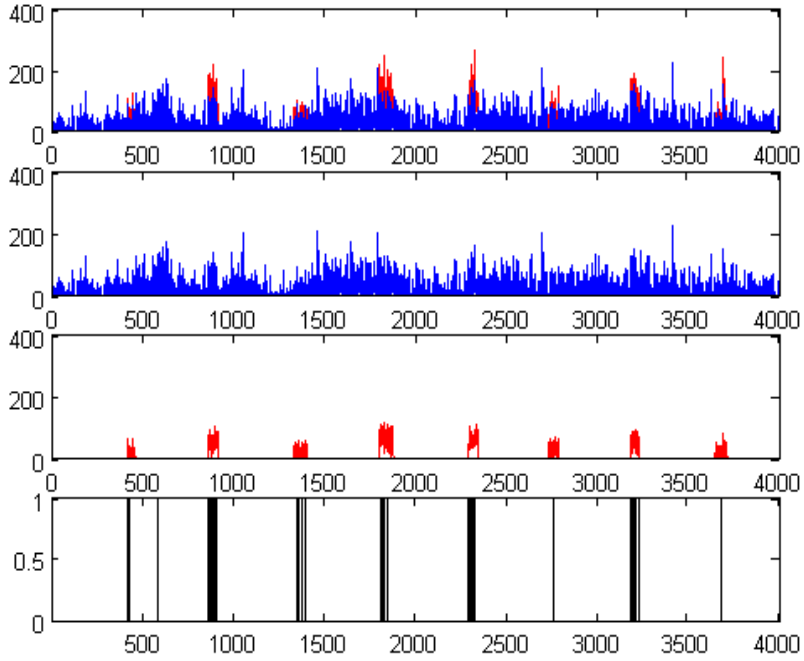
Ο εντοπισμός επιθέσεων χαμηλής κλίμακας είναι σημαντικός για δυο λόγους: Ο πρώτος είναι ότι οι επιθέσεις άρνησης υπηρεσίας συνήθως ξεκινούν από χαμηλούς ρυθμούς και αυξάνονται σταδιακά στη συνέχεια. Για το λόγο αυτό, ο έγκαιρος εντοπισμός τους θα βοηθούσε σημαντικά στο να αντιμετωπιστούν έγκαιρα και αποτελεσματικά από τους διαχειριστές του συστήματος. Ο δεύτερος λόγος είναι ότι ο εντοπισμός επιθέσεων χαμηλής κλίμακας θα βοηθούσε στον εντοπισμό των επιθέσεων στην πλευρά των επιτιθέμενων, όπου, ιδιαίτερα στην περίπτωση των κατανεμημένων επιθέσεων άρνησης υπηρεσίας ο ρυθμός αποστολής των πακέτων δεν αυξάνεται εντυπωσιακά κοντά στους σταθμούς που στέλνουν την κίνηση. Έτσι, ο έλεγχος που διεξάγεται από τους αλγορίθμους πραγματοποιείται στο σημείο που

μόλις περιγράψαμε, θα μπορούσε να διευκολύνει την αναγνώριση και εντοπισμό των συγκεκριμένων μηχανημάτων τα οποία λαμβάνουν μέρος σε μια κατανεμημένη επίθεση άρνησης υπηρεσίας.

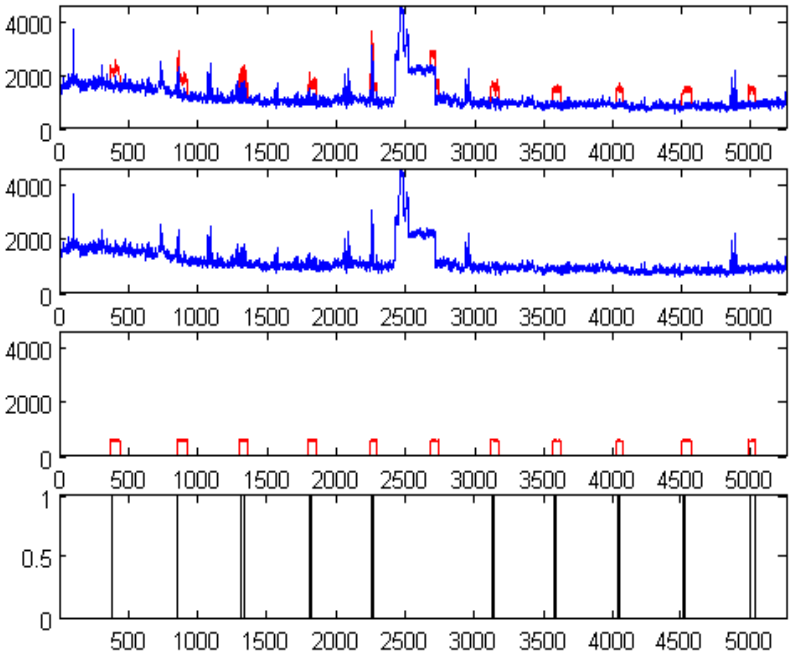
Το σχήμα 14 δείχνει πως για επιθέσεις χαμηλής κλίμακας, η απόδοση του αλγόριθμου προσαρμοζόμενου κατωφλιού έχει να επιδείξει σημαντική επιδείνωση, καθώς παρουσιάζει πολύ υψηλό ποσοστό σφαλμάτων, ίσο με 32%. Αντίθετα, στο σχήμα 15 φαίνεται ότι η απόδοση του αλγόριθμου CUSUM παραμένει στα ίδια σχεδόν επίπεδα με την περίπτωση των επιθέσεων υψηλής κλίμακας, εφόσον παρουσιάζει ποσοστό λαθών μικρότερο από 9%. Παρόλα αυτά βέβαια, θα πρέπει να αναφερθεί το γεγονός ότι η καθυστέρηση εντοπισμού του αλγόριθμου CUSUM έχει αυξηθεί αισθητά και είναι πλέον 10.25 μονάδες χρόνου, ενώ στην προηγούμενη περίπτωση, των επιθέσεων μεγάλης έντασης ήταν μόλις 2.75 μονάδες χρόνου. Τα αποτελέσματα που μόλις παρουσιάστηκαν, αφορούσαν σε πειράματα όπου ως δεδομένα χρησιμοποιήθηκαν τα δεδομένα από εργαστήριο του MIT.



Σχήμα 14: Αλγόριθμος Προσαρμοζόμενου Κατωφλιού - Επιθέσεις μικρής κλίμακας



Σχήμα 15: Αλγόριθμος CUSUM - Επιθέσεις μικρής κλίμακας. Δεδομένα του εργαστηρίου MIT



Σχήμα 16: Αλγόριθμος CUSUM – Επιθέσεις μικρής κλίμακας. Δεδομένα του Πανεπιστημίου Κρήτης

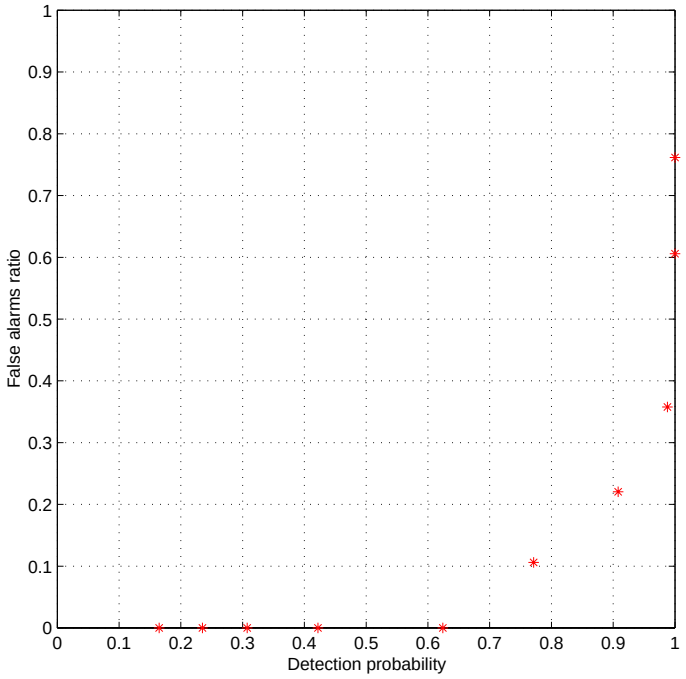
Και στην περίπτωση που χρησιμοποιούμε τα δεδομένα του Πανεπιστημίου Κρήτης στην προσπάθειά μας να μελετήσουμε την απόδοση των αλγορίθμων, βλέπουμε ότι οι προηγούμενες παρατηρήσεις επιβεβαιώνονται, καθώς ο αλγόριθμος CUSUM (σχήμα 16) παρουσιάζει σε αυτόν την περίπτωση σαφώς καλύτερη συμπεριφορά από ότι ο αλγόριθμος προσαρμοζόμενου κατωφλιού. Έτσι, όσον αφορά στην περίπτωση που χρησιμοποιείται ο αλγόριθμος CUSUM, παρατηρούμε πως επιδεικνύει άριστη συμπεριφορά, καθώς παρουσιάζει 100% πιθανότητα εντοπισμού και μηδενικό ποσοστό εσφαλμένων συναγερμών. Η καθυστέρηση στον εντοπισμό είναι 6.9 μονάδες χρόνου. Αντίστοιχα ο αλγόριθμος προσαρμοζόμενου κατωφλιού παρουσιάζει μείωση στην πιθανότητα εντοπισμού των επιθέσεων (83%) και παράλληλη αύξηση του ποσοστού λανθασμένων συναγερμών (40%).

Η διαφορά στην απόδοση μεταξύ του αλγόριθμου προσαρμοζόμενου κατωφλιού και του αλγόριθμου CUSUM, έγκειται κυρίως στον τρόπο με τον οποίο καθένας από αυτούς διατηρεί μνήμη του παρελθόντος. Ο αλγόριθμος προσαρμοζόμενου κατωφλιού διατηρεί μνήμη μόνο όσον αφορά στο εάν παραβιάστηκε ή όχι το κατώφλι τα προηγούμενα $k - 1$ χρονικά διαστήματα. Αντίθετα, ο αλγόριθμος CUSUM διατηρεί περισσότερη πληροφορία σχετικά με τον όγκο των δεδομένων ο οποίος υπερέβη τον αναμενόμενο με βάση το μέσο ρυθμό όγκο δεδομένων.

Στο σημείο αυτό θα πρέπει να επισημάνουμε την εξής παρατήρηση: όπως έχει ήδη προαναφερθεί, η αρχική μας προσέγγιση ήταν η αφαίρεση της εποχικότητας που παρουσιάζουν τα δεδομένα με τον αλγόριθμο Holt-Winters και στη συνέχεια αφαίρεση των χρονικών συσχετίσεων με το μοντέλο αυτοπαλινδρόμησης AR δεύτερης τάξης. Τα αποτελέσματα που εξήχθησαν μετά την εφαρμογή αυτής της μεθόδου, ήταν πανομοιότυπα με τα αποτελέσματα μετά την εφαρμογή της μεθόδου, σύμφωνα με την οποία αφαιρούμε τις χρονικές συσχετίσεις των δεδομένων με τη βοήθεια ενός μοντέλου εκθετικά σταθμισμένου κινούμενου μέσου, οδηγώντας μας στο συμπέρασμα πως είναι ιδιαίτερα συμφέρουσα η δεύτερη προσέγγιση, εφόσον αποδίδει τα ίδια αποτελέσματα με την πρώτη, αλλά ταυτόχρονα είναι σαφώς απλούστερη και λιγότερο χρονοβόρα.

6.2.1 Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών

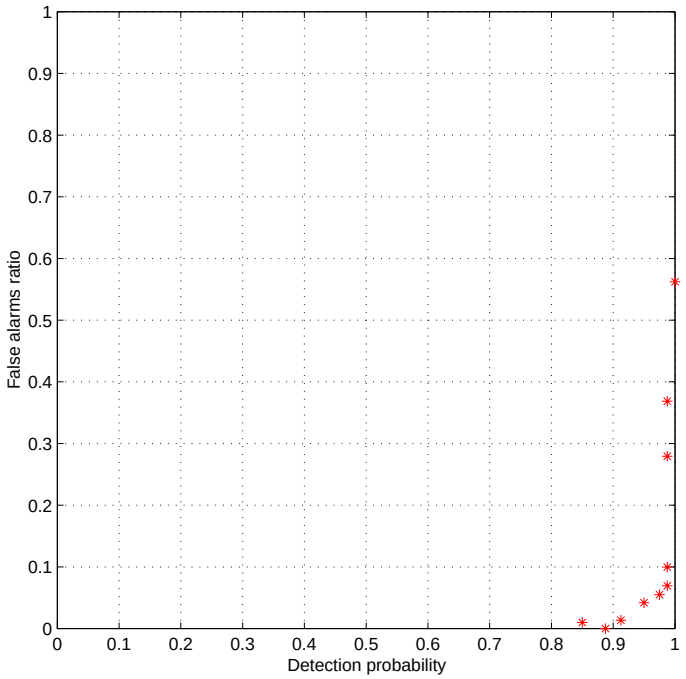
Τα αποτελέσματα τα οποία παρουσιάσαμε προηγουμένως αντιστοιχούσαν σε συγκεκριμένες τιμές των παραμέτρων των δύο αλγορίθμων εντοπισμού ανωμαλιών – επιθέσεων. Στη συνέχεια, σκοπεύουμε να διερευνήσουμε τη σχέση που υπάρχει μεταξύ της πιθανότητας εντοπισμού και του ποσοστού λανθασμένων σημάνσεων συναγερμού για διαφορετικές τιμές της παραμέτρου k του αλγορίθμου προσαρμοζόμενου κατωφλιού και της παραμέτρου h, η οποία αφορά στον αλγόριθμο CUSUM.



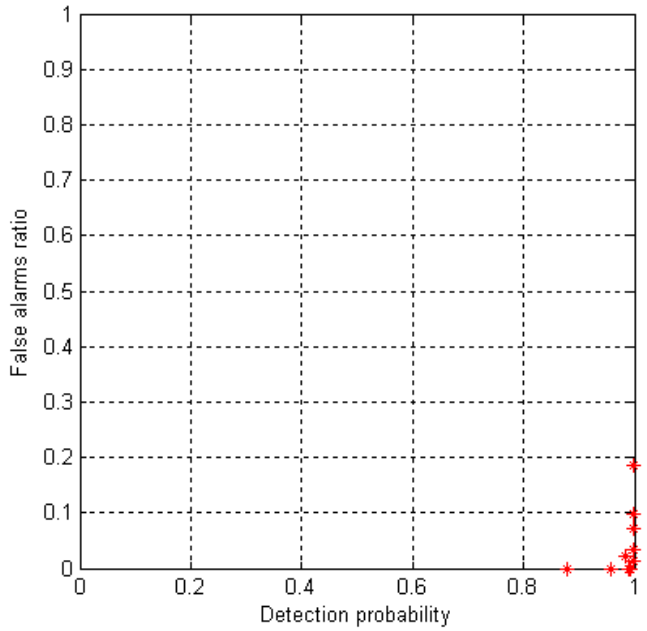
Σχήμα 17: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού για επιθέσεις χαμηλής έντασης – Δεδομένα του εργαστηρίου MIT

Τα σχήματα 17 και 18 δείχνουν τα αποτελέσματα που πήραμε στην περίπτωση που είχαμε επιθέσεις μικρής κλίμακας, μετά την εφαρμογή των αλγορίθμων προσαρμοζόμενου κατωφλιού και του αλγόριθμου CUSUM αντίστοιχα στα δεδομένα του εργαστηρίου του MIT. Κάθε κουκκίδα στο γράφημα αυτό αντιστοιχεί σε μια διαφορετική τιμή της παραμέτρου η οποία μεταβάλλεται (k ή h ανάλογα με τον χρησιμοποιούμενο αλγόριθμο). Η τιμή της κάθε κουκκίδας ισούται με το μέσο όρο των αποτελεσμάτων, μετά από 50 φορές εφαρμογής των αλγορίθμων. Ένας αλγόριθμος έχει βέλτιστη απόδοση όταν οι κουκκίδες που αντιστοιχούν στο

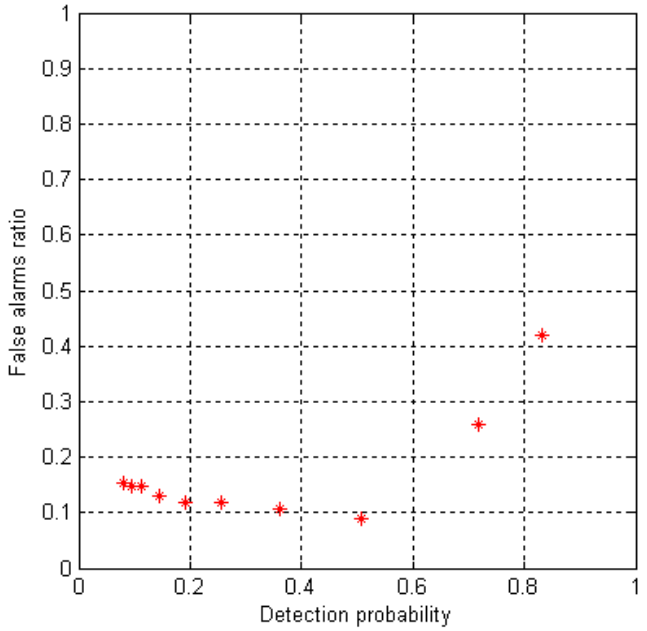
ζευγάρι Πιθανότητα Εντοπισμού – Ποσοστό Εσφαλμένων Συναγερμών είναι συγκεντρωμένες στην κάτω και δεξιά γωνία του γραφήματος. Παρατηρούμε λοιπόν, ότι ο αλγόριθμος CUSUM επιδεικνύει καλύτερη απόδοση, υποστηρίζοντας την προηγούμενη παρατήρησή μας. Ανάλογα είναι και τα συμπεράσματα που εξάγουμε μετά την εφαρμογή των αλγορίθμων στα δεδομένα τα οποία συλλέχθηκαν από το Πανεπιστήμιο Κρήτης (σχήματα 19 και 20). Όπως είναι φανερό, σε αυτήν την περίπτωση, ο αλγόριθμος προσαρμοζόμενου κατωφλιού παρουσιάζει αρκετά άσχημη απόδοση, καθώς εμφανίζει χαμηλό ποσοστό εντοπισμού επιθέσεων, ενώ παράλληλα το ποσοστό σφαλμάτων είναι υψηλό. Αντίθετα ο αλγόριθμος CUSUM επιδεικνύει άριστη σχεδόν συμπεριφορά, με σχεδόν απόλυτο εντοπισμό των επιθέσεων και μικρό ποσοστό σφαλμάτων.



Σχήμα 18: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου CUSUM για επιθέσεις χαμηλής έντασης - Δεδομένα του εργαστηρίου MIT



Σχήμα 19: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου CUSUM για επιθέσεις χαμηλής έντασης – Δεδομένα του Πανεπιστημίου Κρήτης

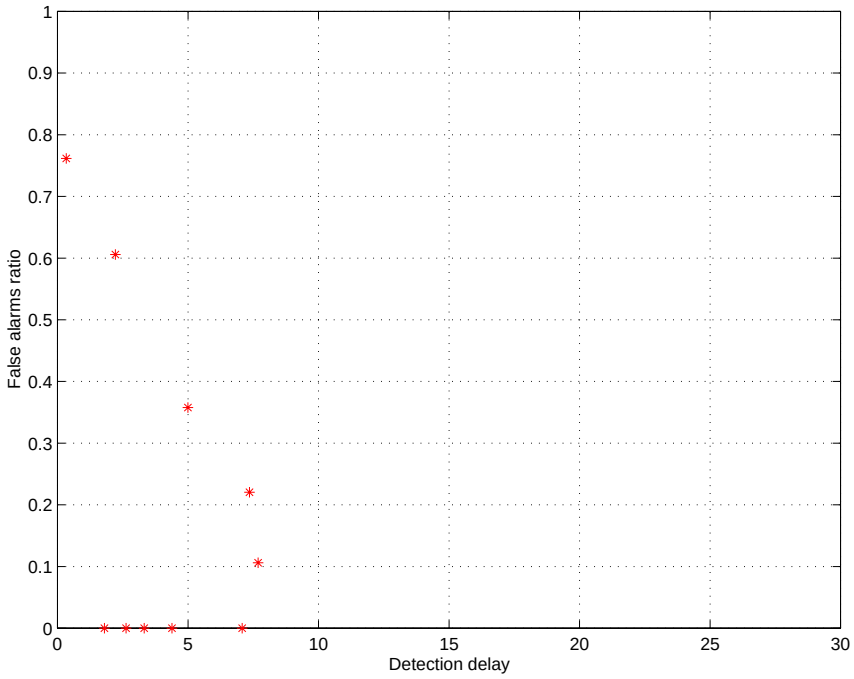


Σχήμα 20: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού για επιθέσεις χαμηλής έντασης – Δεδομένα από το Πανεπιστήμιο Κρήτης

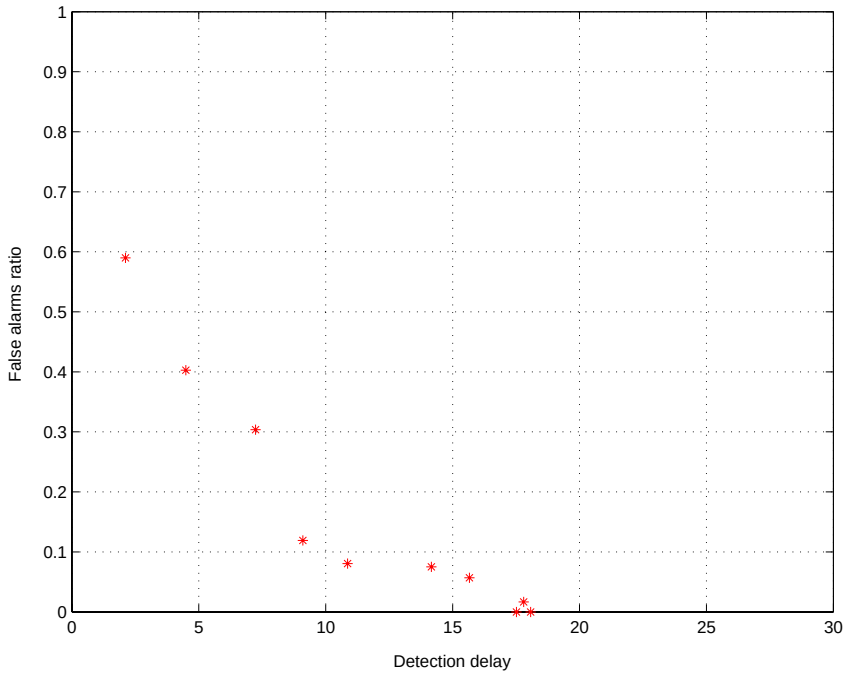
6.2.2 Συσχέτιση μεταξύ του ποσοστού εσφαλμένων συναγερμών και της καθυστέρησης εντοπισμού

Στη συνέχεια, μελετούμε τη σχέση που υπάρχει ανάμεσα στο ποσοστό εσφαλμένων συναγερμών και στην καθυστέρηση εντοπισμού. Τα σχήματα 21 και 22 φανερώνουν τα αποτελέσματα στην περίπτωση που έχουμε δημιουργήσει επιθέσεις χαμηλής κλίμακας στα δεδομένα από το εργαστήριο του MIT και έχουμε στη συνέχεια εφαρμόσει τους αλγόριθμους προσαρμοζόμενου κατωφλιού και τον αλγόριθμο CUSUM αντίστοιχα. Κάθε κουκκίδα στα γραφήματα αυτά αντιστοιχεί και πάλι σε μια διαφορετική τιμή της παραμέτρου k ή h, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο.

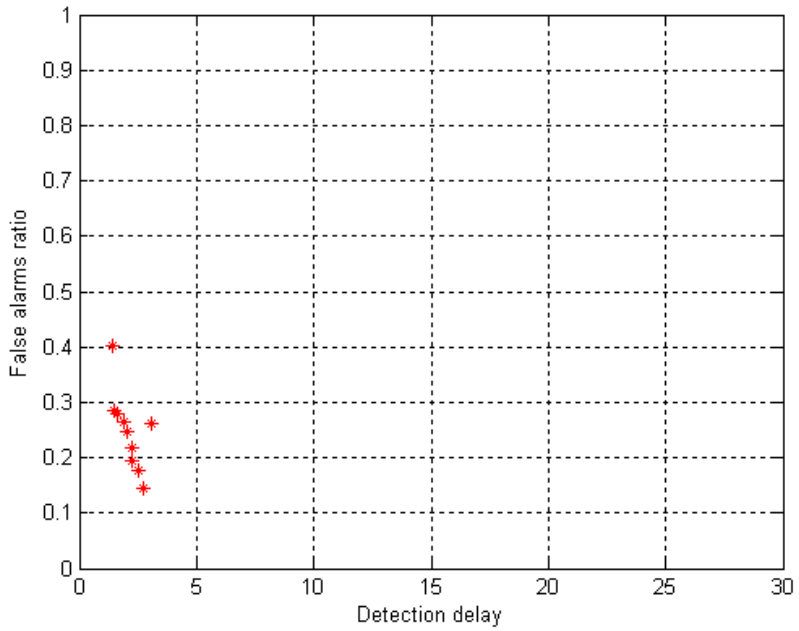
Ένας αλγόριθμος, επιδεικνύει άριστη συμπεριφορά στην περίπτωση που οι προαναφερθείσες κουκκίδες, οι οποίες αντιστοιχούν στο ζευγάρι Καθυστέρηση Εντοπισμού – Ποσοστό Εσφαλμένων Συναγερμών, βρίσκονται συγκεντρωμένες στην κάτω και αριστερή γωνία του γραφήματος. Παρατηρούμε ότι η συμπεριφορά των δύο αυτών μεγεθών ως προς τη μεταβαλλόμενη παράμετρο, είναι αντιστρόφως ανάλογη. Αξιοσημείωτο επίσης είναι το γεγονός ότι, όπως είναι φανερό και από το σχήμα 21, το οποίο αντιστοιχεί στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού, οι κουκκίδες που βρίσκονται στην κάτω και αριστερή γωνία του διαγράμματος, εκφράζουν μικρή καθυστέρηση εντοπισμού, ταυτόχρονα όμως παρουσιάζουν και μικρή πιθανότητα εντοπισμού.



Σχήμα 21: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού για επιθέσεις χαμηλής έντασης – Δεδομένα εργαστηρίου MIT

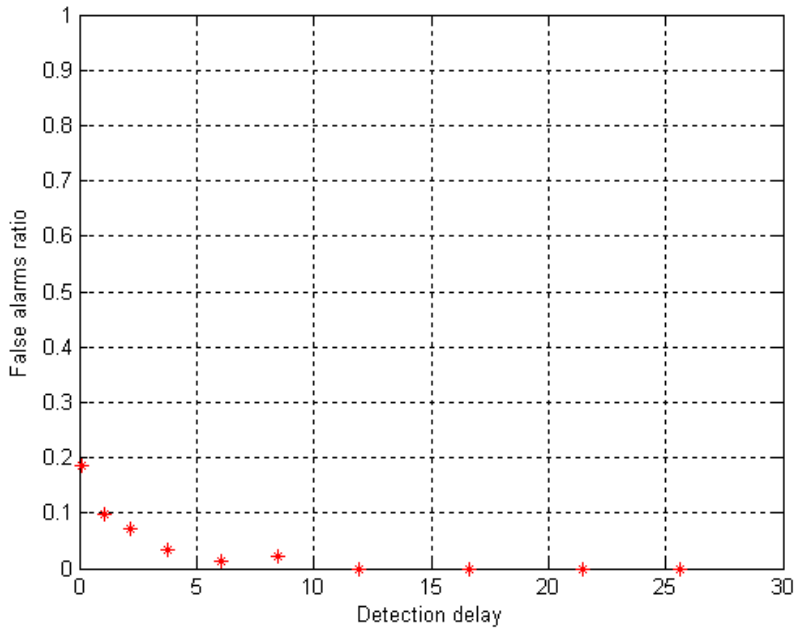


Σχήμα 22: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου CUSUM για επιθέσεις χαμηλής έντασης – Δεδομένα εργαστηρίου MIT



Σχήμα 23: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου προσαρμοζόμενου κατωφλιού για επιθέσεις χαμηλής έντασης – Δεδομένα Πανεπιστημίου Κρήτης

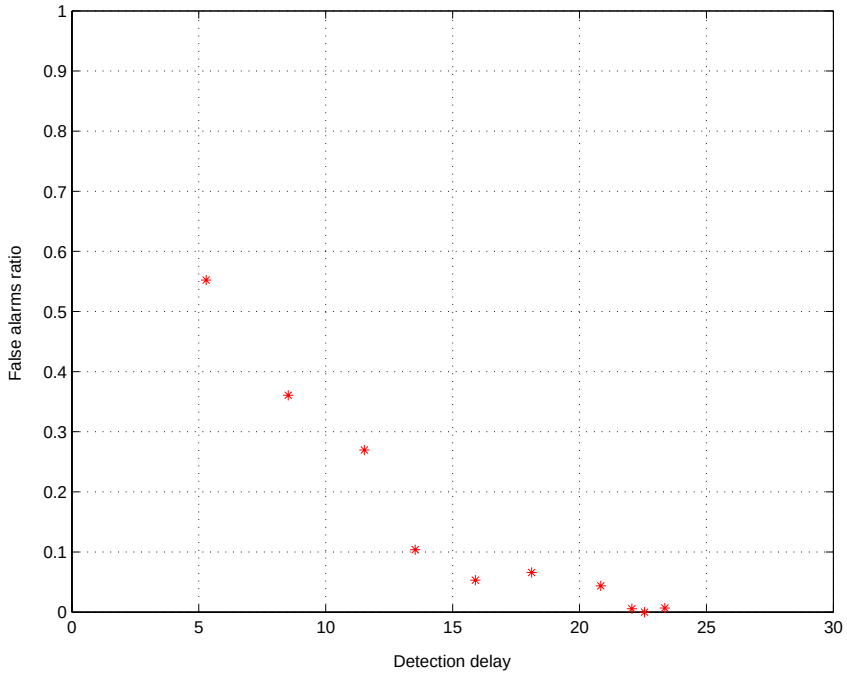
Στην περίπτωση που χρησιμοποιήθηκαν τα δεδομένα από το Πανεπιστήμιο Κρήτης, οι αλγόριθμοι παρουσιάζουν συμπεριφορά που διαφαίνεται στα σχήματα 23 και 24. Και σε αυτή την περίπτωση, είναι προφανής η καλύτερη συμπεριφορά του αλγόριθμου CUSUM, ο οποίος παρουσιάζει βέβαια μεγαλύτερη καθυστέρηση εντοπισμού από ότι ο αλγόριθμος προσαρμοζόμενου κατωφλιού, εμφανίζει όμως πολύ μικρότερο ποσοστό λαθών.



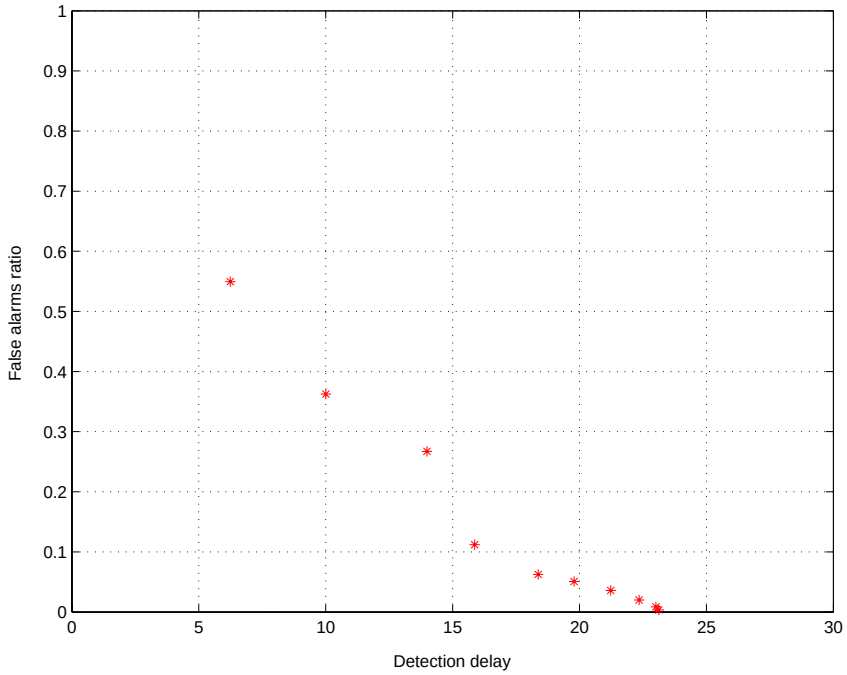
Σχήμα 24: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών στην περίπτωση του αλγόριθμου CUSUM για επιθέσεις χαμηλής έντασης – Δεδομένα του Πανεπιστημίου Κρήτης

6.2.3 Επιθέσεις με αυξανόμενη ένταση

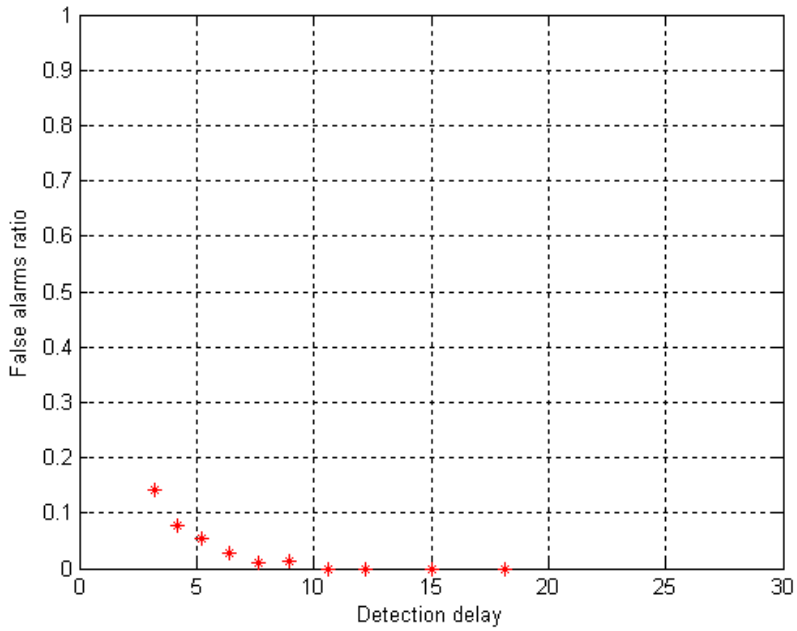
Στη συνέχεια διερευνούμε την απόδοση του αλγόριθμου CUSUM στην περίπτωση που υπάρχουν επιθέσεις στις οποίες ο ρυθμός αποστολής πακέτων δεν αυξάνεται απότομα, αλλά αυξάνεται σταδιακά μέχρι να φτάσει στο μέγιστο ρυθμό. Τα σχήματα 25 και 26 δείχνουν τη σχέση ανάμεσα στο ρυθμό λανθασμένων συναγερμών και στην καθυστέρηση εντοπισμού όταν η διάρκεια της σταδιακής αύξησης είναι 9 μονάδες χρόνου (δηλαδή 90 δευτερόλεπτα δεδομένου ότι μια μονάδα χρόνου αντιστοιχεί σε 10 δευτερόλεπτα) και 15 μονάδες χρόνου αντίστοιχα. Συγκρίνοντας τα γραφήματα αυτά με το γράφημα 20, παρατηρούμε ότι, όπως άλλωστε ήταν αναμενόμενο, η καθυστέρηση εντοπισμού αυξάνεται όταν αυξάνεται η διάρκεια της περιόδου κατά την οποία η επίθεση αυξάνεται σταδιακά μέχρι τελικά να φτάσει στο μέγιστο ρυθμό της. Εντελώς αντίστοιχα είναι και τα αποτελέσματα των ίδιων πειραμάτων που διεξήχθησαν με βάση τα δεδομένα του Πανεπιστημίου Κρήτης (σχήματα 27 και 28).



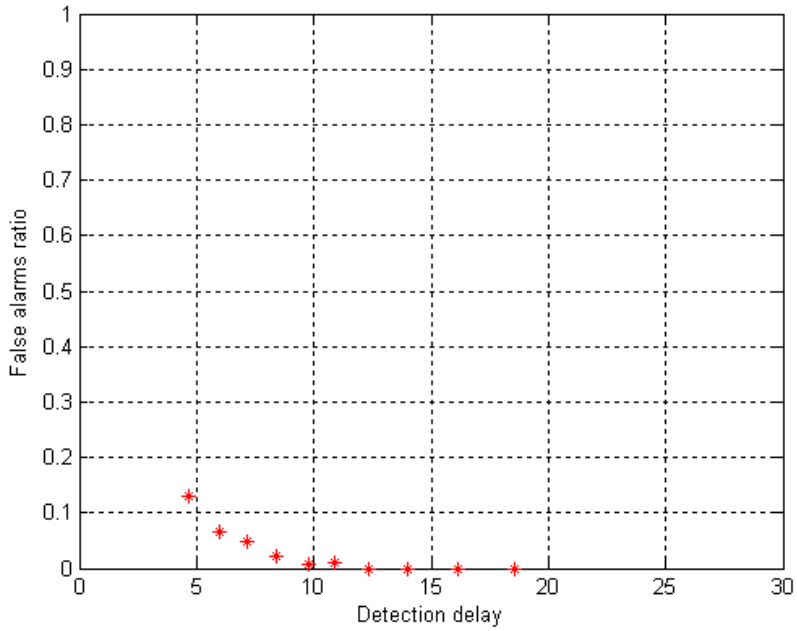
Σχήμα 25: Διάρκεια σταδιακής αύξησης 9 μονάδες χρόνου – Δεδομένα εργαστηρίου MIT



Σχήμα 26: Διάρκεια σταδιακής αύξησης 15 μονάδες χρόνου – Δεδομένα εργαστηρίου MIT



Σχήμα 27: Διάρκεια σταδιακής αύξησης 9 μονάδες χρόνου – Δεδομένα Πανεπιστημίου Κρήτης

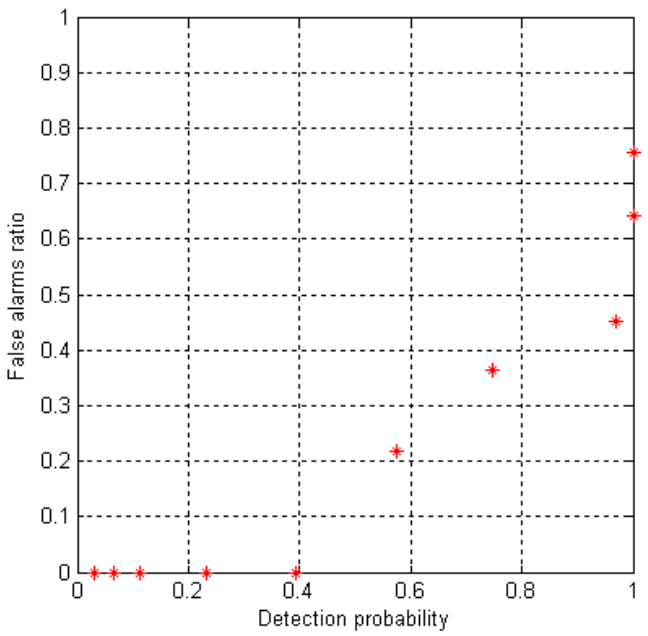


Σχήμα 28: Διάρκεια σταδιακής αύξησης 15 μονάδες χρόνου – Δεδομένα Πανεπιστημίου Κρήτης

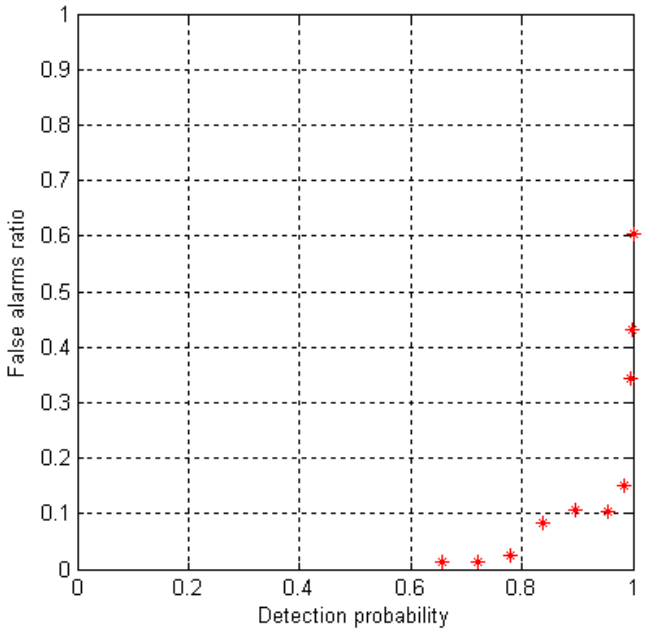
6.2.4 Επιθέσεις με διακοπές

Μια ακόμη κατηγορία επιθέσεων η οποία είναι δυνατό να παρατηρηθεί, είναι οι επιθέσεις στις οποίες η αποστολή πακέτων δεν είναι συνεχής, αλλά διακόπτεται για κάποιες μονάδες χρόνου. Στην περίπτωση αυτή, όπως παρατηρούμε και στα σχήματα,

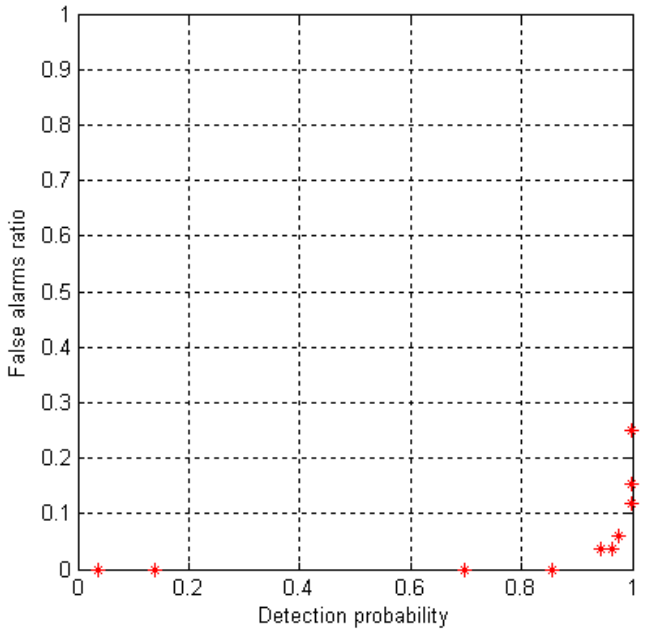
η απόδοση των αλγορίθμων μειώνεται, εφόσον οι επιθέσεις πλέον είναι δύσκολο να εντοπιστούν, παρόλα αυτά όμως ο αλγόριθμος CUSUM, παρουσιάζει μικρή μείωση στην απόδοσή του, πράγμα που σημαίνει ότι εντοπίζει αρκετά ικανοποιητικά ακόμα και αυτές, τις σχετικά «έξυπνες» μορφές επίθεσης άρνησης υπηρεσίας. Η καθυστέρηση εντοπισμού, όπως άλλωστε θα ήταν αναμενόμενο, παρουσιάζει αξιοσημείωτη αύξηση. Όσον αφορά στα συγκεκριμένα αποτελέσματα που παρουσιάζονται στα σχήματα 29 έως 34, οι επιθέσεις έχουν το χαρακτηριστικό ότι αποστέλλουν κίνηση για 3 μονάδες χρόνου συνεχόμενα και διακόπτουν στη συνέχεια την αποστολή για 1 μονάδα χρόνου, επαναλαμβάνοντας αυτό το μοτίβο μέχρι την ολοκλήρωση της επίθεσης. Πειράματα έγιναν επίσης και με βάση το σενάριο σύμφωνα με το οποίο ο επιτιθέμενος αποστέλλει κίνηση για 3 μονάδες χρόνου συνεχόμενα και σταματά στη συνέχεια για 2 μονάδες χρόνου. Στην περίπτωση αυτή οι αλγόριθμοι παρουσιάζουν ελαφρώς χειρότερη συμπεριφορά, καθώς αυξάνεται το ποσοστό των λαθών που παρατηρούνται.



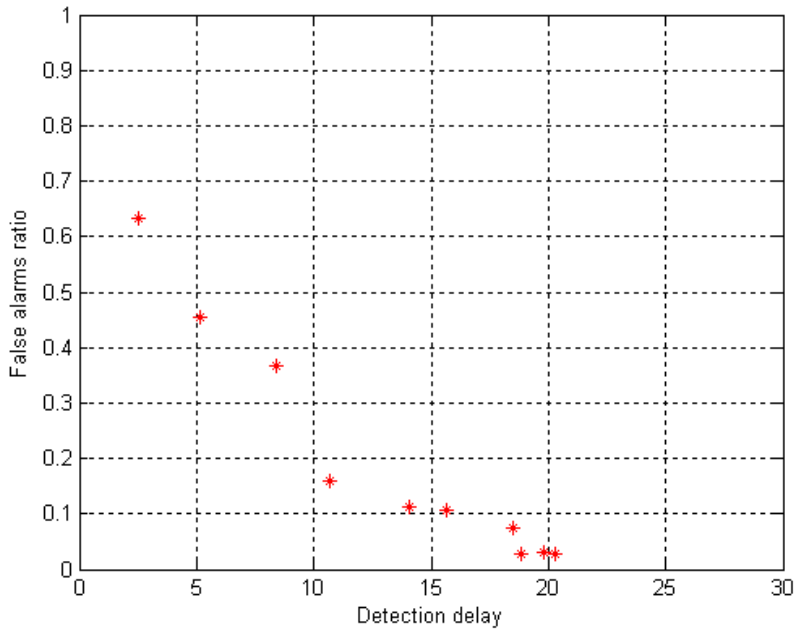
Σχήμα 29: Επιθέσεις με διακοπές - Αλγόριθμος Προσαρμοζόμενου Κατωφλιού
Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα εργαστηρίου MIT



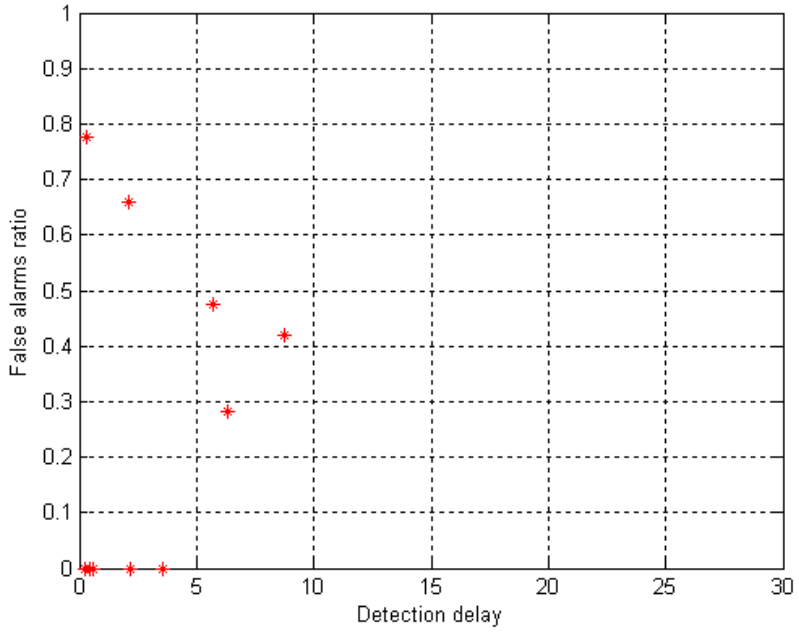
Σχήμα 30: Επιθέσεις με διακοπές - Αλγόριθμος CUSUM
Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα εργαστηρίου MIT



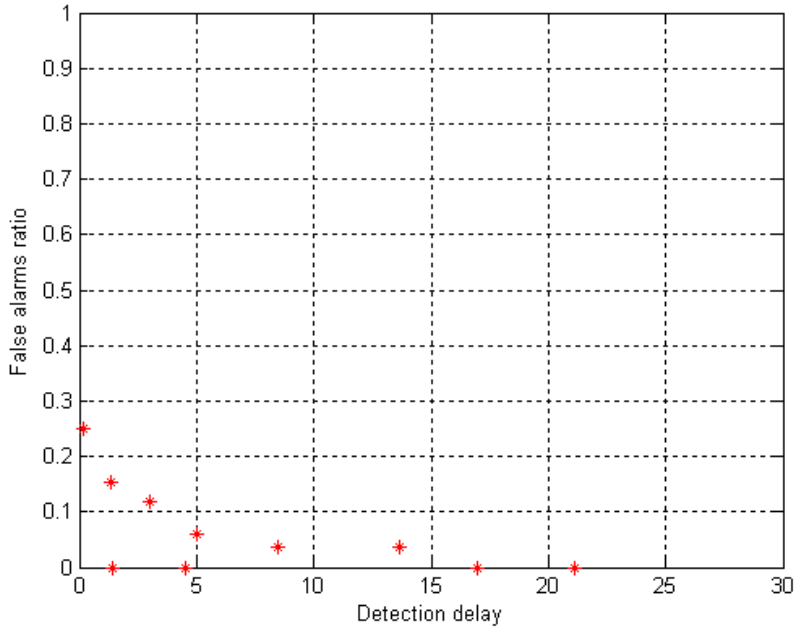
Σχήμα 31: Επιθέσεις με διακοπές - Αλγόριθμος CUSUM
Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα Πανεπιστημίου Κρήτης



Σχήμα 32: Επιθέσεις με διακοπές - Αλγόριθμος CUSUM
Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα εργαστηρίου MIT



Σχήμα 33: Επιθέσεις με διακοπές - Αλγόριθμος Προσαρμοζόμενου Κατωφλιού
Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα εργαστηρίου MIT



Σχήμα 34: Επιθέσεις με διακοπές - Αλγόριθμος CUSUM
Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών
Δεδομένα Πανεπιστημίου Κρήτης

	Επιθέσεις Χαμηλής Έντασης	**Επιθέσεις Υψηλής Έντασης**	**Επιθέσεις με διακοπές**	**Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, επιθέσεις χαμηλής έντασης**
Πιθανότητα Εντοπισμού	**100%**	**100%**	**97.5%**	**100%**
Ποσοστό Λαθών	**1%**	**0%**	**5%**	**0.2%**
Καθυστέρηση Εντοπισμού	**6.9**	**4.5**	**9**	**7.8**

Πίνακας 2: Αλγόριθμος CUSUM – Δεδομένα Πανεπιστημίου Κρήτης

	Επιθέσεις Χαμηλής Έντασης	**Επιθέσεις Υψηλής Έντασης**	**Επιθέσεις με διακοπές**	**Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, επιθέσεις χαμηλής έντασης**
Πιθανότητα Εντοπισμού	**100%**	**100%**	**98%**	**100%**
Ποσοστό Λαθών	**8%**	**0%**	**10%**	**0.3%**
Καθυστέρηση Εντοπισμού	**10.25**	**2.75**	**14**	**21**

Πίνακας 3: Αλγόριθμος CUSUM – Δεδομένα Εργαστηρίου MIT

	Επιθέσεις Χαμηλής Έντασης	Επιθέσεις Υψηλής Έντασης
Πιθανότητα Εντοπισμού	**100%**	**100%**
Ποσοστό Λαθών	**32%**	**0%**
Καθυστέρηση Εντοπισμού	**7**	**3.01**

Πίνακας 4: Αλγόριθμος Προσαρμοζόμενου Κατωφλιού – Δεδομένα Εργαστηρίου MIT

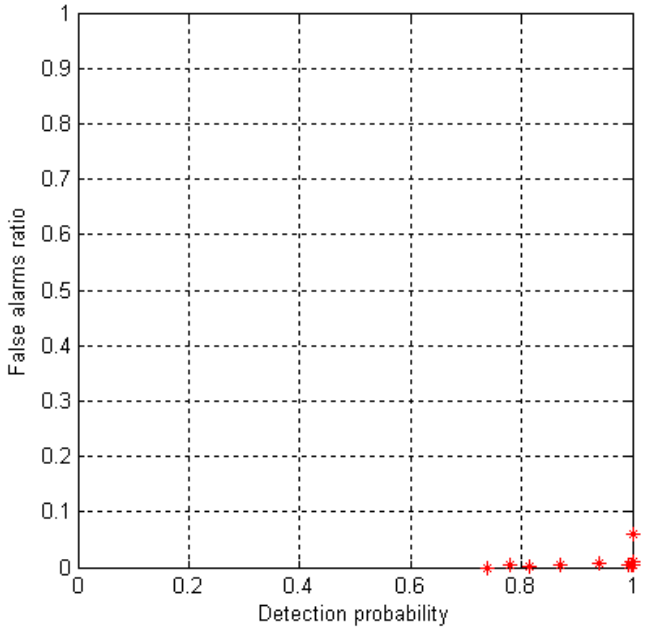
	Επιθέσεις Χαμηλής Έντασης	Επιθέσεις Υψηλής Έντασης
Πιθανότητα Εντοπισμού	**83%**	**100%**
Ποσοστό Λαθών	**41%**	**0%**
Καθυστέρηση Εντοπισμού	**3**	**4**

Πίνακας 5: Αλγόριθμος Προσαρμοζόμενου Κατωφλιού – Δεδομένα Πανεπιστημίου Κρήτης

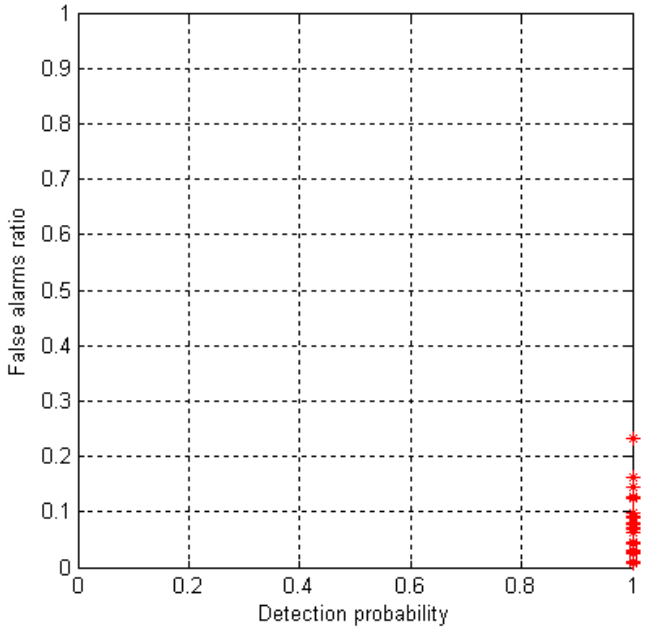
6.3 Χρήση διαφορετικής μετρικής

Ιδιαίτερα καλά αποτελέσματα είχαμε και στην περίπτωση που ως μετρική χρησιμοποιήθηκε ο λόγος της διαφοράς των SYN από τα FIN πακέτα ως προς μια εκτίμηση του μέσου αριθμού των FIN πακέτων. Η εκτίμηση αυτή έγινε για μια ακόμα φορά με τη βοήθεια του μοντέλου εκθετικά σταθμισμένου κινούμενου μέσου. Η χρήση της μετρικής αυτής, συμπίπτει με τη μετρική που χρησιμοποιήθηκε στο πανεπιστήμιο του Michigan, προκειμένου να εντοπιστούν επιθέσεις άρνησης υπηρεσίας τύπου SYN flooding. Τα αποτελέσματα ήταν ιδιαίτερα ικανοποιητικά, εφόσον και στην περίπτωση που ο αλγόριθμος εφαρμόστηκε στα δεδομένα του εργαστηρίου του MIT και στην περίπτωση που εφαρμόστηκε στα δεδομένα του Πανεπιστημίου Κρήτης, εντόπισε το σύνολο των επιθέσεων, παρουσιάζοντας ταυτόχρονα χαμηλό ποσοστό λαθών, όπως φαίνεται και από τα γραφήματα. Τέλος, θα πρέπει να σημειωθεί το γεγονός ότι η καθυστέρηση εντοπισμού παρουσιάζει σημαντική αύξηση στην περίπτωση που χρησιμοποιούνται τα δεδομένα από το εργαστήριο του MIT σε σχέση με την καθυστέρηση που παρατηρήθηκε όταν ως μετρική χρησιμοποιήθηκε μόνο το πλήθος των SYN πακέτων στη μονάδα του χρόνου, ενώ όταν ο αλγόριθμος εφαρμόζεται στα δεδομένα του Πανεπιστημίου

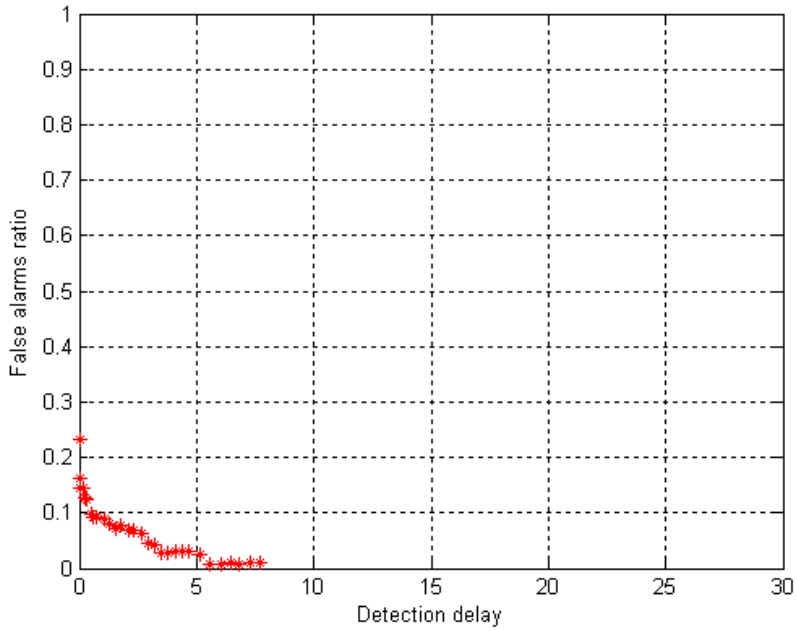
Κρήτης, η καθυστέρηση είναι της ίδιας τάξης μεγέθους, είτε χρησιμοποιούμε την παρούσα μετρική είτε το πλήθος των SYN πακέτων. Επιβεβαιώνεται λοιπόν η άποψη ότι ο αλγόριθμος CUSUM είναι κατάλληλος για τον έγκαιρο εντοπισμό επιθέσεων SYN flooding.



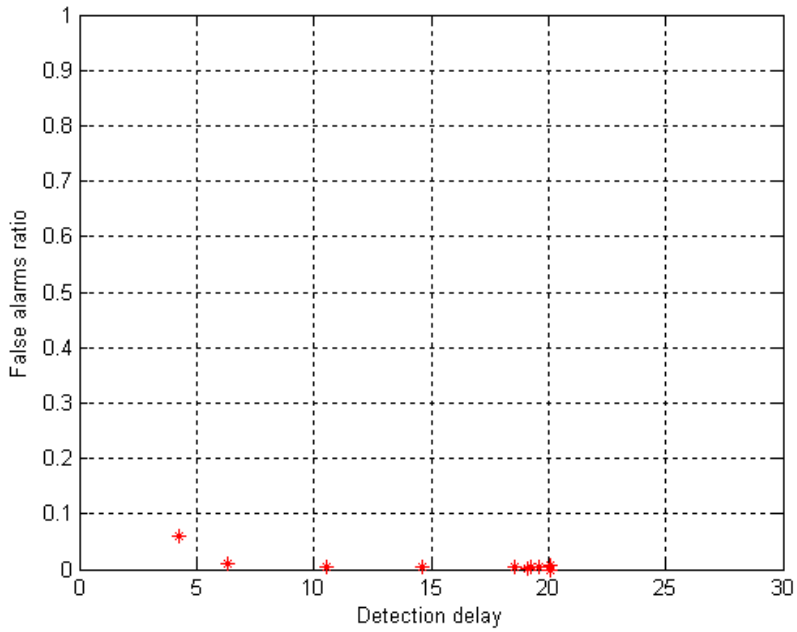
Σχήμα 35: Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, δεδομένα εργαστηρίου MIT, αλγόριθμος CUSUM



Σχήμα 36: Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, δεδομένα Πανεπιστημίου Κρήτης, αλγόριθμος CUSUM



Σχήμα 37: Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, δεδομένα Πανεπιστημίου Κρήτης, αλγόριθμος CUSUM



Σχήμα 38: Χρήση της μετρικής $\frac{SYN-FIN}{\overline{FIN}}$, δεδομένα εργαστηρίου MIT, αλγόριθμος CUSUM

6.4 Εφαρμογή του αλγορίθμου που προτείνεται από το Πανεπιστήμιο του Michigan

Στη συνέχεια, προκειμένου να ελέγξουμε εάν και κατά πόσο οι αλγόριθμοι που προτείνουμε βελτιστοποιούν τις ήδη υπάρχουσες τεχνικές εντοπισμού επιθέσεων άρνησης υπηρεσίας, εφαρμόζουμε στα δεδομένα που χρησιμοποιήσαμε στα μέχρι τώρα πειράματά μας, τον αλγόριθμο ο οποίος προτείνεται από το πανεπιστήμιο του Michigan. Ο αλγόριθμος αυτός αποτελεί μια διαφορετική υλοποίηση – μορφή του αθροιστικού αλγόριθμου ελέγχου CUSUM. Όπως έχει ήδη προαναφερθεί, η μετρική η οποία χρησιμοποιείται είναι ο λόγος $\frac{SYN-FIN}{\overline{FIN}}$, τον για τον οποίο, για χάρη συντομίας, θα χρησιμοποιούμε στο εξής το συμβολισμό X_n. Ο προτεινόμενος από το πανεπιστήμιο Michigan αλγόριθμος λειτουργεί ως εξής:

Έστω $E(X_n) = c$. Επιλέγεται στη συνέχεια μια σταθερά α, η οποία θεωρείται ως το άνω όριο της σταθεράς c, δηλαδή $\alpha > c$. Ορίζεται επίσης η διαφορά $\tilde{X}_n = X_n - a$, της οποίας ο μέσος όρος είναι αρνητικός υπό φυσιολογικές συνθήκες. Όταν μια επίθεση λάβει χώρα, τότε η μεταβλητή $\tilde{X}_n$ αποκτά απότομα υψηλή θετική τιμή.

Έστω

$$y_n = (y_{n-1} + \tilde{X}_n)^+,$$
$$y_0 = 0,$$

όπου το x^+ είναι ίσο με x εάν $x > 0$ και ίσο με 0 σε κάθε άλλη περίπτωση. Με άλλα λόγια, εάν ορίσουμε

$$S_k = \sum_{i=1}^{k} \tilde{X}_i$$

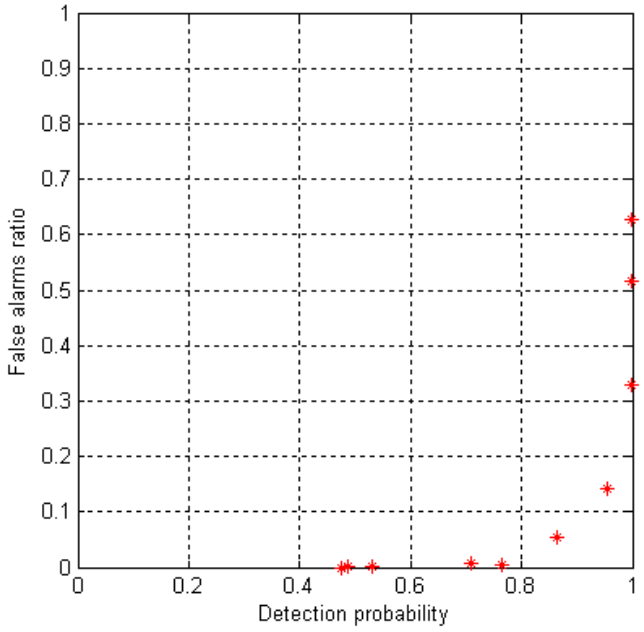
με $S_0 = 0$, τότε είναι φανερό πως

$$y_n = S_n - \min_{1 \le k \le n} S_k,$$

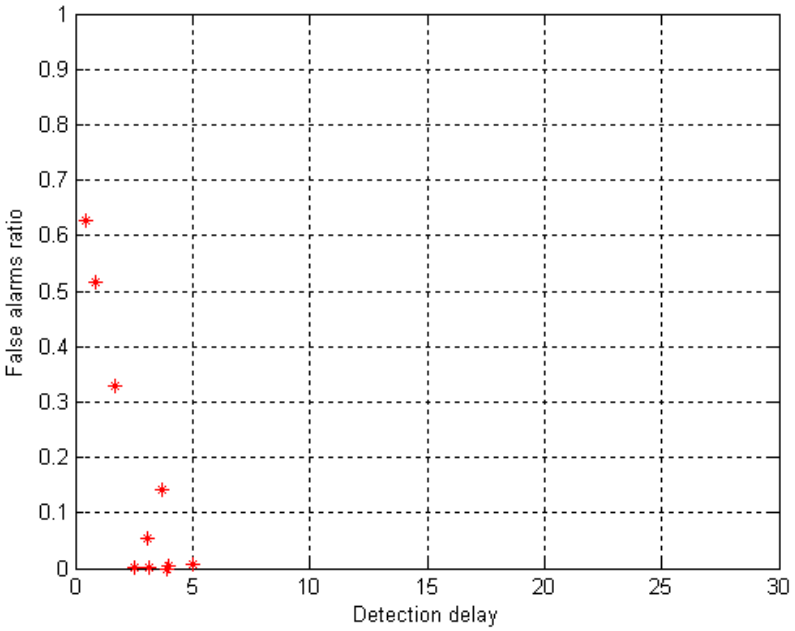
που εκφράζει τη μέγιστη συνεχόμενη αύξηση μέχρι τη χρονική στιγμή n. Ο έλεγχος που γίνεται είναι εάν η τιμή της μεταβλητής y_n υπερβαίνει ή όχι ένα κατώφλι N, οπότε και σημαίνεται συναγερμός.

Εφαρμόσαμε λοιπόν τον παραπάνω αλγόριθμο τόσο στα δεδομένα που συλλέχθηκαν από το εργαστήριο του MIT, όσο και στα δεδομένα του Πανεπιστημίου Κρήτης, με σκοπό να αξιολογήσουμε την απόδοσή του ως προς την πιθανότητα εντοπισμού, το ποσοστό εσφαλμένων συναγερμών και την καθυστέρηση εντοπισμού.

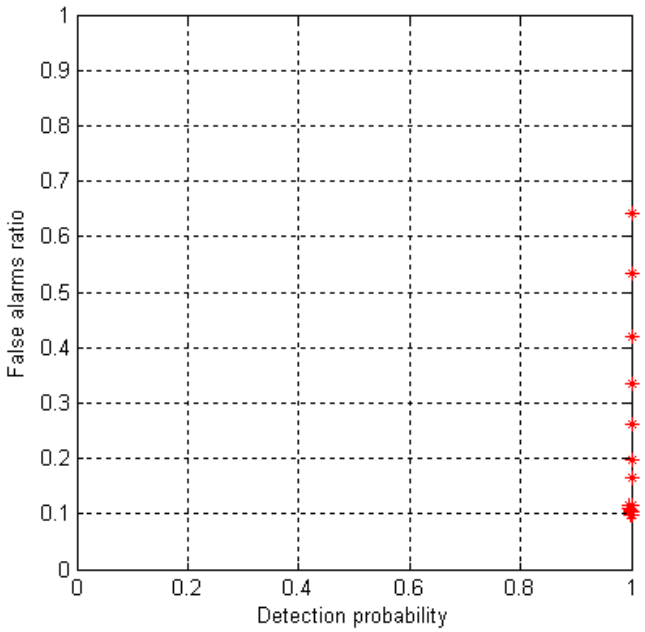
Τα αποτελέσματα, τα οποία φαίνονται στα σχήματα 39-42, δείχνουν ότι ο αλγόριθμος αυτός επιδεικνύει σαφώς πιο άσχημη συμπεριφορά από ότι η μορφή του αλγόριθμου CUSUM που εμείς προτείνουμε. Έτσι, παρατηρούμε πως αν και στην περίπτωση που εφαρμόζεται ο αλγόριθμος στα δεδομένα του Πανεπιστημίου Κρήτης η απόδοσή του είναι μικρότερη από ότι η απόδοση του CUSUM αλγόριθμου που προτείνουμε όταν αυτός εφαρμόζεται στα ίδια δεδομένα αλλά παρόλα αυτά θα μπορούσε να θεωρηθεί ανεκτή, η απόδοσή του στην περίπτωση που εφαρμόζεται στα δεδομένα του εργαστηρίου του MIT μειώνεται δραματικά, παρουσιάζοντας αρκετά υψηλό ποσοστό σφαλμάτων.



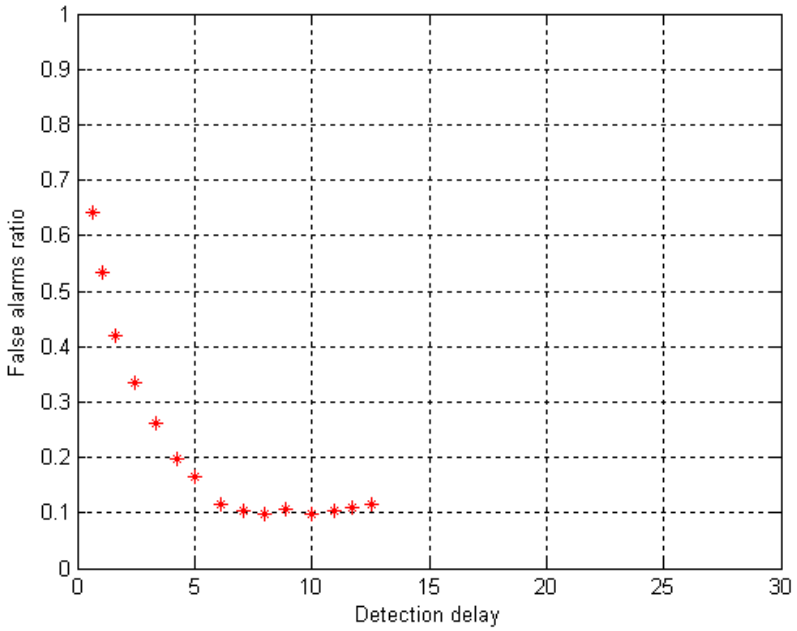
Σχήμα 39: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών – Δεδομένα Πανεπιστημίου Κρήτης



Σχήμα 40: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών – Δεδομένα Πανεπιστημίου Κρήτης



Σχήμα 41: Συσχέτιση μεταξύ της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών – Δεδομένα εργαστηρίου MIT



Σχήμα 42: Συσχέτιση μεταξύ της καθυστέρησης εντοπισμού και του ποσοστού εσφαλμένων συναγερμών – Δεδομένα εργαστηρίου MIT

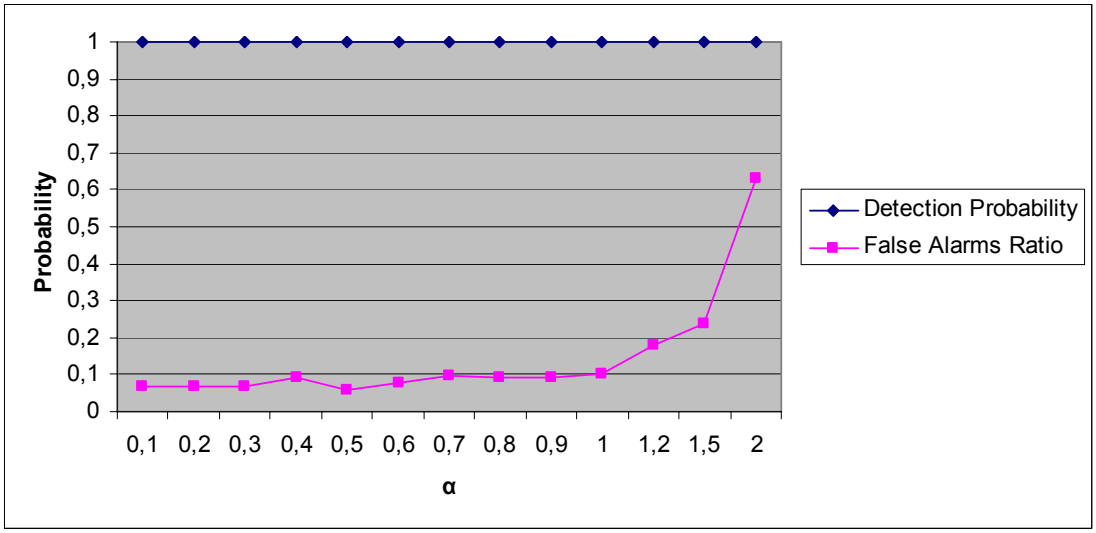
Είναι φανερό επομένως πως ο αλγόριθμος ο οποίος προτείνεται στην παρούσα εργασία βελτιώνει σημαντικά τον αλγόριθμο που προτείνεται από το πανεπιστήμιο του Michigan στα πλαίσια της πιθανότητας εντοπισμού και του ποσοστού εσφαλμένων συναγερμών. Μοναδικό πλεονέκτημα του αλγόριθμου αυτού είναι ο ιδιαίτερα μικρός χρόνος εκτέλεσής του.

Η διαφορά που παρατηρείται στην απόδοση των δυο αυτών διαφορετικών υλοποιήσεων του αλγόριθμου CUSUM, έγκειται στο γεγονός ότι η μορφή του αλγορίθμου που παρουσιάζεται στην εργασία αυτή λαμβάνει υπόψη της, κατά υπολογισμό της μεταβλητής g της οποίας η τιμή ελέγχεται με το κατώφλι h, πολλή περισσότερη πληροφορία σχετικά με τη χρονοσειρά και τα χαρακτηριστικά της, σε σχέση με τη μορφή του αλγορίθμου που παρουσιάστηκε απο το πανεπιστήμιο του Michigan. Έτσι, η προτεινόμενη από την εργασία αυτή μορφή του αλγορίθμου, λαμβάνει υπόψη της μεγέθη όπως η τυπική απόκλιση των δεδομένων αλλά και μια εκτίμηση της μέσης τιμής αυτών την τρέχουσα χρονική στιγμή (υπενθυμίζουμε πως ο τύπος ελέγχου της κρίσιμης μεταβλητής με το κατώφλι είναι $g_n = [g_{n-1} + \frac{a\overline{\mu}_{n-1}}{\sigma^2}(x_n - \overline{\mu}_{n-1} - \frac{a\overline{\mu}_{n-1}}{2})]^+$. Αντίθετα ο αλγόριθμος που παρουσιάστηκε από το πανεπιστήμιο του Michigan, δε λαμβάνει υπόψη του στατιστικά μεγέθη των

δεδομένων όπως τα προαναφερθέντα, με αποτέλεσμα να οδηγείται πολλές φορές σε λανθασμένες αποφάσεις.

6.5 Επίδραση του συντελεστή πλάτους *α*

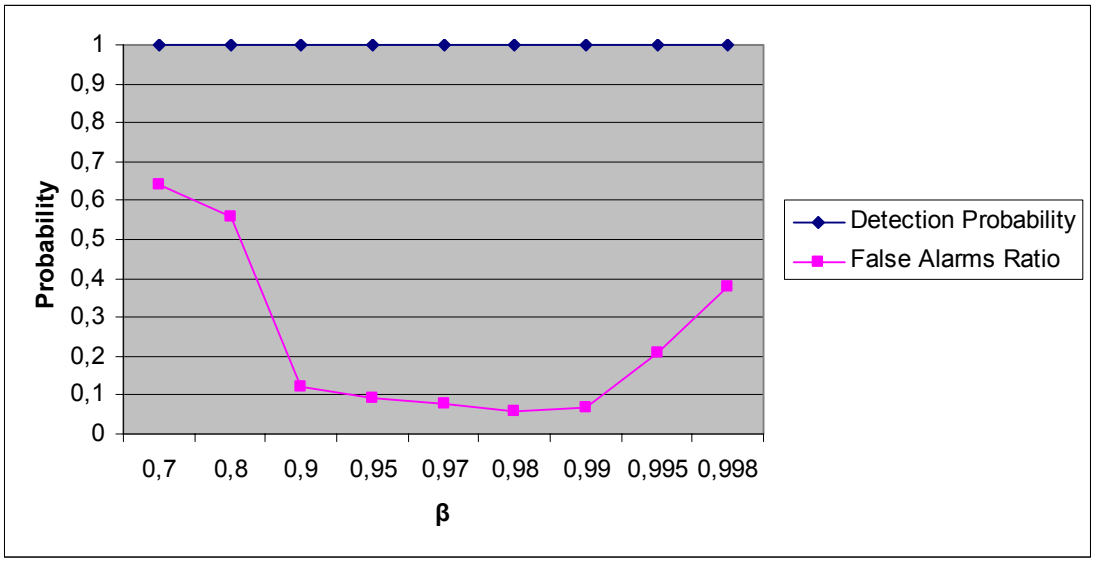
Το σχήμα 43 δείχνει την επίδραση του συντελεστή πλάτους *α* του αλγόριθμου CUSUM, στην περίπτωση που η παράμετρος *h* του αλγορίθμου έχει ρυθμιστεί με τέτοιο τρόπο ώστε να επιτυγχάνεται σε κάθε περίπτωση 100% πιθανότητα εντοπισμού. Τα αποτελέσματα που παρουσιάζονται στο σχήμα προέκυψαν μετά την εκτέλεση για κάθε σημείο του αντίστοιχου πειράματος για 10 φορές και τον υπολογισμό στη συνέχεια του μέσου όρου αυτών. Ο υπολογισμός του μέσου έγινε με βάση ένα διάστημα εμπιστοσύνης της τάξης του + / - 0.045. Με τη βοήθεια του σχήματος διαπιστώνουμε ότι η απόδοση του αλγόριθμου CUSUM δεν εξαρτάται από την τιμή του συντελεστή πλάτους *α*, όσον αφορά σε ένα ευρύ φάσμα τιμών του συντελεστή αυτού, σε γενικές γραμμές δηλαδή στο διάστημα (0.1, 1).



Σχήμα 43: Επίδραση του συντελεστή πλάτους *α*

6.6 Επίδραση του συντελεστή *β* του Εκθετικά Σταθμισμένου Κινούμενου Μέσου μοντέλου (EWMA)

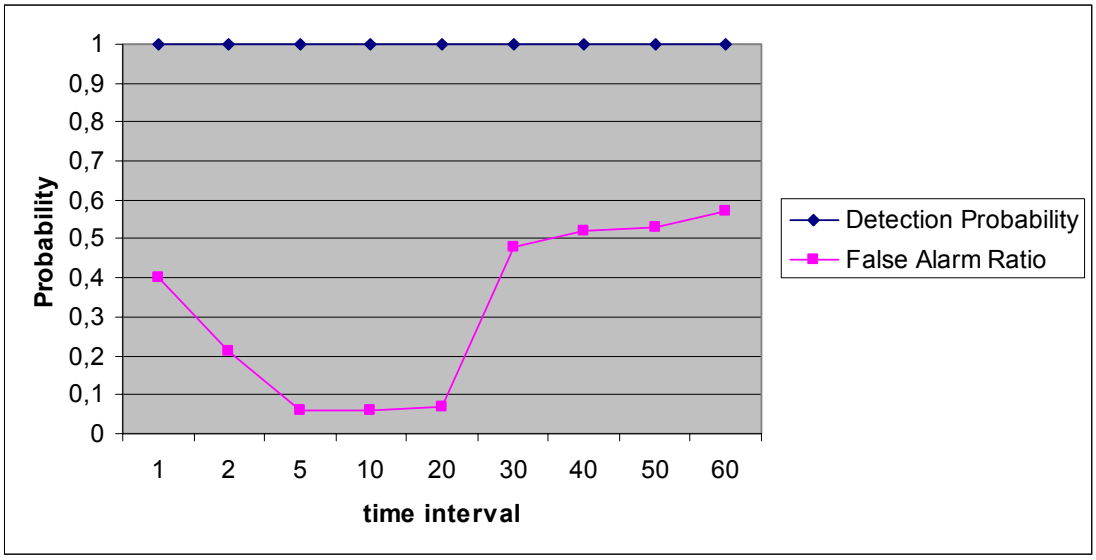
Το σχήμα 44 δείχνει την επίδραση του συντελεστή *β* του Εκθετικά Σταθμισμένου Κινούμενου Μέσου μοντέλου (EWMA) στην περίπτωση που η παράμετρος *h* του αλγορίθμου CUSUM έχει ρυθμιστεί με τέτοιο τρόπο ώστε να επιτυγχάνεται σε κάθε περίπτωση 100% πιθανότητα εντοπισμού. Όπως και στην προηγούμενη περίπτωση, το γράφημα που παρουσιάζεται προέκυψε μετά την εκτέλεση για κάθε σημείο του αντίστοιχου πειράματος για 10 φορές και τον υπολογισμό στη συνέχεια του μέσου όρου αυτών. Ο υπολογισμός του μέσου έγινε με βάση ένα διάστημα εμπιστοσύνης της τάξης του + / - 0.045. Από το γράφημα αυτό, εξάγεται το συμπέρασμα ότι ο αλγόριθμος CUSUM αποδίδει τα μέγιστα όταν ο συντελεστής *β* παίρνει τιμές από το διάστημα (0.95, 0.99). Μια πιθανή εξήγηση για το γεγονός αυτό θα μπορούσε να είναι ότι όταν ο συντελεστής του μοντέλου παίρνει τιμές πολύ κοντά στη μονάδα (>0.99), το μοντέλο δίνει περισσότερο βάρος σε παλαιότερες τιμές της μεταβλητής που μετράται (SYN πακέτα), με αποτέλεσμα οι τιμές αυτές να είναι εντελώς ασυσχέτιστες με την τρέχουσα χρονική στιγμή και ο αλγόριθμος να οδηγείται σε λανθασμένες αποφάσεις. Αντίθετα, όταν ο υπό μελέτη συντελεστής παίρνει χαμηλές τιμές, το μοντέλο εναποθέτει ιδιαίτερο βάρος σε πολύ πρόσφατες μετρήσεις με αποτέλεσμα να υπάρχουν ισχυρές χρονικές συσχετίσεις μεταξύ των δεδομένων. Αυτό οδηγεί στη μη κανονική κατανομή των δεδομένων με αποτέλεσμα το αλγόριθμος να επιδεικνύει απογοητευτική συμπεριφορά.



Σχήμα 44: Επίδραση του συντελεστή *β* του μοντέλου Εκθετικά Σταθμισμένου Κινούμενου Μέσου

6.7 Επίδραση του μεγέθους του χρονικού διαστήματος

Το σχήμα 45 δείχνει την επίδραση του μεγέθους του χρονικού διαστήματος το οποίο αντιστοιχεί σε μια μονάδα χρόνου, του χρονικού διαστήματος δηλαδή για το οποίο λαμβάνονται οι μετρήσεις, όσον αφορά στον αλγόριθμο CUSUM και για την περίπτωση που η παράμετρος *h* του αλγορίθμου έχει ρυθμιστεί με τέτοιο τρόπο ώστε να επιτυγχάνεται σε κάθε περίπτωση 100% πιθανότητα εντοπισμού. . Όπως και στην προηγούμενη περίπτωση, το γράφημα που παρουσιάζεται προέκυψε μετά την εκτέλεση για κάθε σημείο του αντίστοιχου πειράματος για 10 φορές και τον υπολογισμό στη συνέχεια του μέσου όρου αυτών. Ο υπολογισμός του μέσου έγινε με βάση ένα διάστημα εμπιστοσύνης της τάξης του + / - 0.045. Το γράφημα φανερώνει ότι ο αλγόριθμός CUSUM παρουσιάζει καλύτερη απόδοση για τιμές του χρονικού διαστήματος το οποίο αντιστοιχεί σε μια χρονική μονάδα που κυμαίνονται στο διάστημα από 5 έως 20 δευτερόλεπτα.



Σχήμα 45: Επίδραση του μεγέθους του χρονικού διαστήματος

7 Συμπεράσματα

Η αναγνώριση και ο εντοπισμός των ανωμαλιών γρήγορα και με ακρίβεια είναι γεγονός ύψιστης σημασίας για την αποδοτική και σωστή λειτουργία των υπολογιστικών συστημάτων και δικτύων. Ωστόσο, το γεγονός ότι πολλές επιθέσεις και ιδιαίτερα επιθέσεις άρνησης υπηρεσίας εξαπολύονται με «έξυπνα»

χαρακτηριστικά, τέτοια ώστε να είναι δυσκολότερος ο εντοπισμός τους, δυσχεραίνει, όπως είναι ευνόητο, και την προαναφερθείσα διαδικασία.

Στην παρούσα εργασία αναλύθηκαν, διερευνήθηκαν και αξιολογήθηκαν δύο αλγόριθμοι εντοπισμού επιθέσεων άρνησης υπηρεσίας και συγκεκριμένα τύπου TCP SYN flooding. Οι αλγόριθμοι αυτοί είναι ο αλγόριθμος προσαρμοζόμενου κατωφλιού και ένας ακόμη αλγόριθμος ο οποίος βασίζεται πάνω στον αλγόριθμο εντοπισμού σημείου ανωμαλίας CUSUM. Η εργασία είχε ως αντικείμενο τη μελέτη της συσχέτισης μεταξύ της πιθανότητας εντοπισμού μιας επίθεσης, το ποσοστό εσφαλμένων σημάνσεων συναγερμού και της καθυστέρησης εντοπισμού, καθώς και το ποσοστό στο οποίο τα παραπάνω μεγέθη επηρεάζονται από τη μεταβολή των παραμέτρων οι οποίες υπεισέρχονται στην υλοποίηση των αλγορίθμων εντοπισμού ανωμαλιών, αλλά επίσης και τον τρόπο, εκτός από το ποσοστό, με τον οποίο οι παράμετροι των αλγόριθμων επηρεάζουν τα μεγέθη αυτά.

Επιπλέον, μελετήθηκε η απόδοση των αλγορίθμων σε διαφορετικές περιπτώσεις κατά τις οποίες οι δημιουργούμενες επιθέσεις επιδείκνυαν κάθε φορά διαφορετική μορφή και είχαν διαφορετικά χαρακτηριστικά όσον αφορά στην έντασή τους αλλά και στο χρονικό διάστημα και ρυθμό κατά τα οποία αποστέλλουν κίνηση.

Το γενικότερο συμπέρασμα που προέκυψε από τη μελέτη των αλγορίθμων, είναι ότι αν και ένας απλός και σαφής αλγόριθμος όπως ο αλγόριθμος προσαρμοζόμενου κατωφλιού μπορεί να παρουσιάζει ικανοποιητική απόδοση, όσον αφορά στις περιπτώσεις όπου οι εμφανιζόμενες επιθέσεις χαρακτηρίζονται από τον ιδιαίτερα υψηλό ρυθμό αποστολής πακέτων, στις περιπτώσεις όμως στις οποίες οι παρατηρούμενες επιθέσεις χαρακτηρίζονται από σχετικά χαμηλό ρυθμό αποστολής κίνησης, η απόδοσή του μειώνεται αισθητά.

Αντίθετα, στην περίπτωση που ο αλγόριθμος που χρησιμοποιείται προκειμένου να επιτύχουμε τον εντοπισμό των επιθέσεων άρνησης υπηρεσίας είναι ο CUSUM, παρατηρούμε ότι επιδεικνύει σταθερά καλή απόδοση και επιθυμητή συμπεριφορά, όσον αφορά στα μεγέθη πιθανότητα εντοπισμού επιθέσεων, ποσοστό λαθών και καθυστέρηση εντοπισμού επιθέσεων, τόσο στις περιπτώσεις επιθέσεων υψηλής κλίμακας, όσο και στην περίπτωση των χαμηλότερης κλίμακας επιθέσεων. Έτσι, η επίδοσή του είναι πολύ ικανοποιητική όταν καλείται να εντοπίσει ένα φάσμα από διαφορετικά είδη επιθέσεων, χωρίς ταυτόχρονα να αυξάνεται η πολυπλοκότητά του.

Επίσης εφαρμόστηκε η μορφή του αλγόριθμου CUSUM η οποία παρουσιάστηκε σε εργασία του πανεπιστήμιου του Michigan στα δεδομένα τα οποία χρησιμοποιήθηκαν σε όλα τα προαναφερθέντα πειράματα με τους αλγόριθμους που παρουσιάστηκαν στην εργασία αυτή. Τα αποτελέσματα έδειξαν πως ο αλγόριθμος αυτός επιδεικνύει χειρότερη συμπεριφορά όσον αφορά στην πιθανότητα εντοπισμού και στο ποσοστό εσφαλμένων συναγερμών σε σχέση με τη συμπεριφορά της μορφής του αλγόριθμου CUSUM που περιγράφεται στην παρούσα εργασία.

Τέλος, στα πλαίσια της εργασίας αυτής, έγινε μελέτη της απόδοσης των αλγορίθμων όταν χρησιμοποιούνται διαφορετικές μετρικές όσον αφορά στα δεδομένα στα οποία εφαρμόζονται οι αλγόριθμοι αυτοί. Έτσι, μελετήθηκαν δύο μετρικές, η μια από τις οποίες είναι το πλήθος των TCP SYN πακέτων στη μονάδα του χρόνου και η άλλη ο λόγος της διαφοράς των SYN από τα FIN πακέτα ως προς μια εκτίμηση του μέσου αριθμού των FIN πακέτων. Πειραματικά αποτελέσματα απέδειξαν πως για την περίπτωση όπου επιθυμούμε να εντοπίσουμε επιθέσεις άρνησης υπηρεσίας τύπου TCP SYN flooding, η μετρική της οποίας η χρήση αποδίδει τα καλύτερα αποτελέσματα είναι ο λόγος $\frac{SYN - FIN}{\overline{FIN}}$.

8 Μελλοντική Εργασία

Επόμενο στάδιο της μελέτης όλων παρουσιάστηκαν στην εργασία αυτή, είναι η υλοποίηση και εφαρμογή των αλγορίθμων που μελετήθηκαν στην πράξη, σε πραγματικά υπολογιστικά συστήματα και δίκτυα. Η υλοποίηση αυτή, απαιτεί ένα μηχανισμό για εφαρμογή των αλγορίθμων σε πραγματικό χρόνο, αντίθετα με τη προσέγγιση που παρουσιάστηκε και η οποία επεξεργάζονταν τα δεδομένα εκ των υστέρων, μετά τη συλλογή τους, για το λόγο βέβαια ότι ή όλη εργασία αποτελούσε μια μελέτη – εξέταση κυρίως, της καταλληλότητας ή μη των υπό ανάλυση αλγορίθμων.

Ένα επίσης ιδιαίτερα σημαντικό θέμα το οποίο θα πρέπει να επιλυθεί προκειμένου να εφαρμοστούν οι αλγόριθμοι σε πραγματικά συστήματα είναι η κατάλληλη ρύθμιση των παραμέτρων των αλγορίθμων, η οποία προτιμότερο θα ήταν να γίνεται με τρόπο αυτοματοποιημένο, χωρίς την ανθρώπινη παρέμβαση. Η υλοποίηση της πρότασης αυτής εξάλλου θα βοηθούσε σημαντικά στον ταχύτερο και ακριβέστερο εντοπισμό των τυχόν επιθέσεων. Όπως έχει ήδη αναφερθεί, η επιλογή

των βέλτιστων παραμέτρων στα πειράματα τα οποία διεξήχθησαν, έγινε μετά από σειρά δοκιμών και σύγκριση των αποτελεσμάτων τους. Έτσι, επιλέχθηκαν οι παράμετροι εκείνες οι οποίες απέδιδαν τα πιο ικανοποιητικά αποτελέσματα.

Τελειώνοντας, θα πρέπει να αναφερθεί το γεγονός ότι αξιόλογη μελέτη για το μέλλον θα ήταν η μελέτη της εφαρμογής των αλγορίθμων εντοπισμού άρνησης υπηρεσίας στην προσπάθεια έγκαιρου εντοπισμού μείωσης της ποιότητας υπηρεσίας (Quality of Service – QoS) η οποία προσφέρεται στους χρήστες.

Οι διαφορές οι οποίες υπάρχουν μεταξύ μιας τέτοιας προσέγγισης και της προσέγγισης η οποία παρουσιάστηκε στην εργασία αυτή, είναι αρχικά το είδος της μεταβλητής την οποία μελετάμε στο χρόνο. Στην περίπτωση των TCP SYN flooding επιθέσεων άρνησης υπηρεσίας, ήταν ευκόλως εννοούμενο το γεγονός ότι τη μεταβλητή αυτή θα την αποτελούσαν τα SYN πακέτα ή κάποια έκφραση η οποία θα περιείχε το μέγεθος αυτό (π.χ. άλλη πιθανή μετρική θα ήταν η διαφορά TCP SYN και TCP FIN πακέτων στη μονάδα του χρόνου). Στην περίπτωση που ο αλγόριθμος όμως προσπαθεί να εντοπίσει έγκαιρα μείωση στην παρεχόμενη στους χρήστες ποιότητα υπηρεσίας, η μετρική που είναι ιδιαίτερα ενδιαφέρουσα είναι η καθυστέρηση την οποία αντιλαμβάνεται ο χρήστης στις υπηρεσίες που του προσφέρονται. Προκύπτει λοιπόν από τα παραπάνω ότι η καταλληλότερη μετρική για την περίπτωση εντοπισμού των παραβιάσεων των εγγυήσεων που παρέχονται στο χρήστη, είναι η μέτρηση της μέγιστης καθυστέρησης η οποία είναι αποδεκτή από αυτόν.

Τέλος, μια ακόμη αξιοσημείωτη διαφορά είναι η περίοδος των μετρήσεων. Δεδομένου ότι μια τέτοια προσέγγιση επικεντρώνεται όπως αναφέραμε στη μέτρηση της μέγιστης καθυστέρησης, οι μετρήσεις θα πρέπει να είναι της τάξης των χιλιοστών ή ακόμη και εκατομμυριοστών σε ορισμένες περιπτώσεις του δευτερολέπτου (msec και μsec αντίστοιχα), έτσι ώστε να υπάρχει η δυνατότητα για έγκαιρη και αποτελεσματική αντιμετώπιση του τυχόν προβλήματος.

9 Αναφορές και Βιβλιογραφία

[1] Internet History – Network Control Program, http://livinginternet.com/i/ii_ncp.htm

[2] TCP/IP Reference Page, http://www.protocols.com/pbook/tcpip1.htm

[3] History of Arpanet, www.dei.isep.ipp.pt/docs/arpa.html

[4] Packet Switching, http://en.wikipedia.org/wiki/Packet_switching

[5] Packet Switching, http://www.webopedia.com/TERM/P/packet_switching.html

[6] Internet Protocol, DARPA Internet Program Protocol Specification, RFC-971, http://www.ietf.org/rfc/rfc0791.txt

[7] J. Postel, Transmission Control Protocol, RFC793, http://rfc.sunsite.dk/rfc/rfc793.html

[8] TCP 3-way handshake, http://www.inetdaemon.com/tutorials/internet/tcp/connections.html

[9] A. Sundaram, An Introduction to Intrusion Detection, http://www.acm.org/crossroads/xrds2-4/intrus.html

[10] Denial of Service (DoS) Attack Resource Page, http://www.denialinfo.com/

[11] J. Postel, Internet Control Message Protocol, RFC792, http://www.faqs.org/rfcs/rfc792.html

[12] J. Postel, User Datagram Protocol, RFC768, http://www.faqs.org/rfcs/rfc768.html

[13] P. Mockapetris, Domain Names – Implementation and Specification, RFC-1035, ftp://ftp.is.co.za/rfc/rfc1035.txt

[14] C++ Reference, Memory Copy (memcpy), http://www.cplusplus.com/ref/cstring/memcpy.html

[15] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, http://www.cert.org/advisories/CA-1996-21.html

[16] Computer Security Institute – Computer Crime and Security Survey, http://gocsi.com/press/20020407.jhtml?_requestid=512256

[17] D. Moore, G. Voelker, and S. Savage. Inferring Internet denial of service activity. In Proceedings of USENIX Security Symposium, 2001.

[18] J. Brutlag. Aberrant behavior detection in time series for network monitoring. In Proceedings of LISA XIV, December 2000

[19] RRD Tool – A System to store and display Time Series data, http://www.gnu.org/directory/sysadmin/Monitor/rrdtool.html

[20] P. Brockwell and R. Davis, Introduction to Time Series and Forecasting, Springer, New York, 1996.

[21] J. Brutlag, Notes on rrdtool implementation of aberrant behavior detection, http://cricket.sourceforge.net/aberrant/rrd_hw.htm

[22] SNMP RFC - Standard MIBs and Informative Links, http://www.wtcs.org/snmp4tpc/snmp_rfc.htm

[23] J. Hellerstein, F. Zhang, and P. Shahabuddin. A statistical approach to predictive detection. Computer Networks, 35:77-95, 2001.

[24] M. Basseville and I. V. Nikiforov. Detection of Abrupt Changes: Theory and Applications. Prentice Hall, 1993.

[25] P. Hoogenboom, J. Lepreau, Computer System Performance Problem Detection Using Time Series Models, In Proceedings of the USENIX Summer 1993 Technical Conference, Cincinnati, Ohio June 21-25, 1993.

[26] The UNIX System, http://www.unix-systems.org

[27] H. Wang, D. Zhang, and K. G. Shin. Detecting SYN flooding attacks. In Proceedings of IEEE INFOCOM'02, 2002.

[28] Quality of Service (QoS), http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm

[29] Autoregressive Modelling, http://www.spss-science.co.uk/science/autosignal/help/Autoregressive_Modeling.htm

[30] Economic Statistics, http://www.fandm.edu/departments/economics/ahearn/210/fall00lct15.pdf

[31] Exponentially Weighted Moving Average Charts, http://www.qualityamerica.com/knowledgecente/knowctrEXPONENTIALLY_WEIGHTED_MOVING_AV.htm

[32] J. Stuart Hunter (1986). The Exponentially Weighted Moving Average, J Quality Technology, Vol. 18, No. 4, pp. 203-207.

[33] J. M. Lucas and M. S. Saccucci, (1990). Exponentially weighted moving average control schemes: Properties and enhancements, Technometrics 32, 1-29.

[34] Normal (Gaussian) Distribution, http://mathworld.wolfram.com/NormalDistribution.html

[35] MIT Lincoln Laboratory, http://www.ll.mit.edu/

[36] MIT Lincoln Laboratory - 1999 DARPA Intrusion Detection Evaluation Data Set, http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html

[37] UCnet: Κέντρο Επικοινωνιών και Δικτύων, Πανεπιστήμιο Κρήτης, http://www.ucnet.uoc.gr/

[38] The Mathworks – MATLAB, www.mathworks.com/products/matlab

[39] The FORTRAN Programming Language, http://www.engin.umd.umich.edu/CIS/course.des/cis400/fortran/fortran.html

[40] The Development of the C Language, http://cm.bell-labs.com/cm/cs/who/dmr/chist.html