Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων Και Μηχανικων Υπολογιστων

Τομεας Επικοινωνιων, Ηλεκτρονικης Και Συστηματων Πληροφορικης

Συνδυαστικές Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών σε Υβριδικά Δίκτυα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ ΑΓΓΕΛΑΚΟΠΟΥΛΟΥ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Αθηνα, Ιούλιος 2018

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

Συνδυαστικές Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών σε Υβριδικά Δίκτυα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ιωάννη Αγγελακόπουλου

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 16 Ιουλίου 2018.

.....	.....	.....
Συμεών Παπαβασιλείου	Θεοδώρα Βαρβαρίγου	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Επίκουρος Καθηγήτρια Ε.Μ.Π.

Αθηνα, Ιούλιος 2018.

.....
ΙΩΑΝΝΗΣ ΑΓΓΕΛΑΚΟΠΟΥΛΟΣ
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών

Περίληψη

Ο σκοπός της παρούσας διπλωματικής είναι ο σχεδιασμός και η υλοποίηση μιας προηγμένης κατανεμημένης επίθεσης άρνησης εξυπηρέτησης (Distributed Denial of Service - DDoS) σε συστήματα, που κάνουν χρήση ασύρματης σύνδεσης στο Διαδίκτυο, μέσω πολλαπλών διεπαφων. Επίσης εστιάζουμε και στην αντιμετώπισή της, συνεισφέροντας σημαντικά στην πρόληψη και ταυτόχρονα στην άμυνα απέναντι σε παρόμοιες επιθέσεις που πιθανόν να προκύψουν μελλοντικά.

Συγκεκριμένα, στην παρούσα διπλωματική εργασία σχεδιάστηκε και υλοποιήθηκε μία επίθεση DDoS βασισμένη σε δύο τεχνικές, την Crossfire και την Pulsating επίθεση, που ανήκουν στην οικογένεια των DDoS επιθέσεων, αλλά είναι πιο εξελιγμένες και καταστροφικές από την κλασική και απλή περίπτωση. Ταυτόχρονα, πραγματοποιήθηκε αξιολόγηση της επίθεσης, όσον αφορά την αποδοτικότητά της και την εφαρμογή της σε σενάρια τα οποία περιλαμβάνουν πραγματικά φυσικά συστήματα.

Είναι γεγονός ότι στη σημερινή εποχή πολλές διαδικτυακές εφαρμογές και ιστότοποι γίνονται ολοένα θύματα επιθέσεων DDoS χαρακτήρα, από κακόβουλους χρήστες του Διαδικτύου με σκοπο, την παρεμπόδιση της σωστής λειτουργίας τους και παροχής υπηρεσιών στους υπόλοιπους χρήστες. Παρόλο που έχουν προταθεί πολλές αποδοτικές λύσεις για την αντιμετώπιση επιθέσεων αυτού του τύπου, οι κακόβουλοι χρήστες συνεχώς προσαρμόζονται και εξαπολύουν περισσότερο προηγμένες και καταστροφικές επιθέσεις, με αποτέλεσμα η αντιμετώπισή τους να γίνεται ακόμα πιο δύσκολη. Η επίθεση που παρουσιάζεται στην παρούσα εργασία έρχεται να προτείνει ένα νέο τρόπο σκέψης όσον αφορά την υλοποίηση τέτοιων επιθέσεων και να συμβάλλει στην αποτελεσματική πρόληψη και αντιμετώπισή τους. Παράλληλα, ανοίγει το δρόμο για περαιτέρω έρευνα όσον αφορά την διαχείριση παρόμοιων επιθέσεων.

Λέξεις-Κλειδιά: DDoS επιθέσεις, Crossfire επίθεση, Pulsating επίθεση, ασύρματα δίκτυα, bottleneck σύνδεσμος, χωρητικότητα, διαθέσιμο εύρος ζώνης

Abstract

The purpose of this diploma thesis was the of an advanced DDoS (Distributed Denial of Service) attack on systems, which have wireless connectivity to the Internet through multiple interfaces and its mitigation, thus contributing considerably to the prevention and defence against similar attacks which might unveil in the future.

Specifically, in the current diploma thesis a DDoS attack was designed and conducted, based on two other techniques, the Crossfire and the Pulsating attacks. These attacks belong to the DDoS attack family, however they are more advanced and destructive than the classic and simple case. Concurrently, an evaluation of the attack was conducted, based on its efficiency and applicability on scenarios with real world systems.

It is a fact that nowadays many online applications and websites become victims of DDoS attacks launched by malicious internet users aiming to disrupt their regular functioning and service providing to other users. Despite the fact that many considerable solutions for the mitigation of such attacks have been proposed, the malicious users constantly adapt and unleash more complexed and noisome attacks, thus their mitigation becomes even harder. The attack presented in this thesis proposed a new way of thinking regarding the implementation of such attacks and contributes to their efficient prevention and mitigation. In addition, it opens up the way for further research regarding the management of similar attacks.

Keywords: DDoS attacks, Crossfire attack, Pulsating attack, wireless networks, bottleneck link, capacity, available bandwidth

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον Καθηγητή κ. Συμεών Παπαβασιλείου, ο οποίος μέσα από το μάθημα των ”Δικτύων Υπολογιστών”, μου ”άνοιξε” τον δρόμο προς την σύγχρονη επιστήμη των Δικτύων Υπολογιστών και Επικοινωνιών. Ακόμα θα ήθελα να τον ευχαριστήσω για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου ένα επίκαιρο θέμα, με ουσιαστική πρακτική εφαρμογή και σημασία για τον τομέα της Ασφάλειας Δικτύων και Υπολογιστών. Το θέμα αυτό μου έδωσε το έναυσμα όχι μόνο να αποκτήσω περισσότερες γνώσεις αλλά και να ”κυνηγήσω” ένα λαμπρό μέλλον στον τομέα της Ασφάλειας Δικτύων και Υπολογιστών.

Επιπλέον, οφείλω και ένα μεγάλο ευχαριστώ στον μεταδιδακτορικό ερευνητή κ. Βασίλειο Καρυώτη, ο οποίος μου παρείχε πολύτιμη βοήθεια καθ΄ όλη τη διάρκεια της εκπόνησης της διπλωματικής. Οι συμβουλές, οι ιδέες και η καθοδήγηση του ήταν καίριες για την επιτυχή έκβαση αυτής της εργασίας.

Περιεχόμενα

Κατάλογος σχημάτων

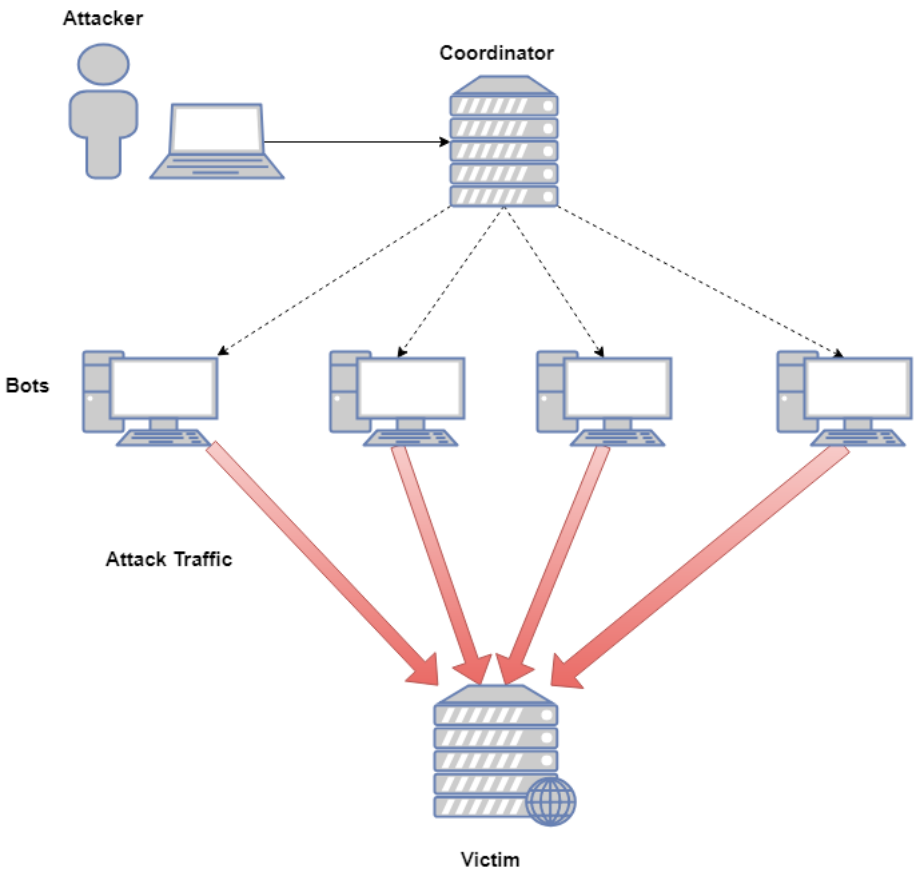
Κατάλογος πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Επιθέσεις DoS/DDoS

Με τον όρο DDoS (Distributed Denial of Service) επιθέσεις, αναφερόμαστε σε επιθέσεις που αποσκοπούν στην διακοπή της ομαλής λειτουργίας και παροχής υπηρεσιών μιας ιστοσελίδας, συστημάτων συνδεδεμένων στο διαδίκτυο κ.τ.λ προς νόμιμους χρήστες. [10] Οι DDoS επιθέσεις αποτελούν εξέλιξη της επίθεσης DoS, η οποία έχει το χαρακτηριστικό ότι προέρχεται μόνο από ένα σύστημα συνδεδεμένο στο Διαδίκτυο. Αντίθετα στην επίθεση DDoS γίνεται χρήση πολλαπλών συστημάτων με σύνδεση στο Διαδίκτυο, των οποίων η συνεισφορά στην επίθεση είναι προσθετική με αποτέλεσμα να είναι πολύ πιο καταστροφική από την απλή περίπτωση του DoS (βλ. σχήμα 1.1).



Σχήμα 1.1: Επιθέσεις DDoS

Συγκεκριμένα και οι δύο επιθέσεις έχουν ως κοινό χαρακτηριστικό είτε την δημιουργία ενός τεράστιου αριθμού ψεύτικων αιτήσεων προς ένα server η ομάδα από servers με σκοπό την παρεμπόδιση παροχής υπηρεσιών σε χρήστες, οι οποίοι τις χρειάζονται πραγματικά, είτε την αποστολή ενός τεράστιου όγκου δεδομένων σε ένα σύστημα με αποτέλεσμα την κατάρρευση και κατά συνέπεια την επανεκκίνησή του. Όπως προαναφέρθηκε όμως στην DoS επίθεση ο επιτεθέμενος χρησιμοποιεί ένα μόνο σύστημα για την δημιουργία αυτού του τεράστιου αριθμού ψεύτικων συνδέσεων ή όγκου δεδομένων με αποτέλεσμα η πρώτη να μην είναι αποδοτική απέναντι στα σημερινά συστήματα τα οποία είναι ικάνα να εξυπηρετούν εκατοντάδες χρήστες ταυτόχρονα. Ακόμα είναι εύκολη η ανίχνευση της συγκεκριμένης επίθεσης, ακριβώς γιατί βασί-

ζεται σε ένα μόνο σύστημα (είναι εύκολο να βρεθεί ποιό είναι). Για το λόγο αυτό σήμερα κυριαρχούν οι επιθέσεις DDoS, κατά τις οποίες γίνεται ταυτόχρονη χρήση εκατομμυρίων συσκευών που είναι συνδεμένες στο Διαδίκτυο, ικανές να παράγουν την συσσωρευμένη κίνηση που απαιτείται για να πλήξει τα σύγχρονα συστήματα και ακόμα περισσότερη.

Την τελευταία δεκαετία μόνο έχουν παρατηρηθεί μερικές από τις περισσότερο καταστροφικές επιθέσεις DDoS στην ανθρώπινη ιστορία. Επιγραμματικά μερικές από αυτές είναι: Spamhaus (2013) [11], against Cloudfare (2014) [12], Hong Kong (2014) [13] and Github (2018) [14], η οποία έφτασε τα 1,3 petabit/sec και αποτελεί την μεγαλύτερη καταγρεγραμμένη επίθεση στην ιστορία την περίοδο της συγγραφής της διπλωματικής εργασίας. Προφανώς, έχουν εξαπολυθεί και πολλές άλλες επιθέσεις DDoS, οι οποίες έχουν πλήξει σε μεγάλο βαθμό δημοφιλείς ιστοσελίδες και παρόχους διαδικτυακών υπηρεσιών και χαρακτηρίζονται από τη χρήση όλο και πιο πολύπλοκων τεχνικών.

1.2 Αντικείμενο Διπλωματικής Εργασίας

Όπως αναφέρθηκε και προηγουμένως οι επιθέσεις DDoS γίνοται όλο και εξυπνότερες με αποτέλεσμα να καθιστούν τους υπάρχοντες μηχανισμούς άμυνας αναποτελεσματικούς σε μεγάλο βαθμό απέναντί τους. Συγκεκριμένα οι επιτιθέμενοι φροντίζουν η κίνηση που παράγεται από κάθε σύστημα που μετέχει στην επίθεση να είναι τόση σε μέγεθος ώστε να θυμίζει πραγματική κίνηση που δημιουργείται από νόμιμους χρήστες (Crossfire attack). Η ύπαρξη όμως ένος τεράστιου αριθμού τέτοιων συστημάτων και ο συνδυασμός της κίνησης που παράγουν σε μια ενιαία έχει ως αποτέλεσμα να δημιουργούνται ροές της τάξεως των Gbit/sec και παραπάνω, οι οποίες είναι δύσκολο να ανιχνευτούν. Σε άλλες περιπτώσεις γίνεται εκμετάλλευση των φυσικών περιορισμών που επιβάλλουν τα μέσα δικτύωσης των συστημάτων, όπως το μέγιστο εύρος ζώνης

(bandwidth) των καλωδίων ή αδυναμιών πολλών μηχανισμών που χρησιμοποιούν πολλά πρωτόκολλα απαραίτητων για την ομαλή και αποδοτική λειτουργία του Διαδικτύου, όπως ο μηχανισμός ελέγχου συμφόρησης (congestion control/avoidance algorithm) του TCP (Pulsating attack). Οι επιθέσεις αυτές θα επεξηγηθούν αναλυτικά στη συνέχεια.

Στην παρούσα διπλωματική εργασία γίνεται ένας συνδυασμός των στοιχείων των δύο παραπάνω επιθέσεων, τα οποία σε συνεργασία με τη χρήση ασύρματων δικτύων ή κινητών (mobile) δικτύων, όπου οι συσκευές έχουν πολλάπλά interfaces, προσφέροντας στην επίθεσή μας τόσο μυστικότητα όσο και αποδοτικότητα. Παράλληλα, εξετάζεται η λειτουργία ενός τέτοιου συστήματος και μελετώνται τρόποι αντιμετώπισης της επίθεσης.

1.3 Συνεισφορά

Η συνεισφορά της διπλωματικής συνοψίζεται ως εξής:

- Έγινε σχεδιασμός και υλοποίηση μίας επίθεσης DDoS πάνω σε δίκτυα, που προσφέρουν ασύρματη συνδεσιμότητα στο Διαδίκτυο. Η ύπαρξη των ασύρματων δικτύων και η δυνατότητα εκτέλεσης μίας αποδοτικής DDoS επίθεσης μέσω αυτών προσφέρει μεγάλη ευελεξία στον επιτιθέμενο (κινητικότητα στο χώρο και χρήση μεγαλύτερου εύρους συσκευών). Ταυτόχρονα, θεωρούμε ότι κάθε συσκευή υπό τον έλεγχο του επιτιθέμενου διαθέτει τρεις διαφορετικές διεπαφές συνδεδεμένες σε διαφορετικά ασύρματα δίκτυα, συνεισφέροντας ακόμα περισσότερο στην επιτυχία της επίθεσης.
- Σχεδιάστηκαν συντονιστές, οι οποίοι εκτός από την δυνατότητα εύρεσης των μονοπατιών προς τον στόχο/θύμα είναι ικανοί να πραγματοποιήσουν αρκετά ακριβείς μετρήσεις του διαθέσιμου εύρους ζώνης (available bandwidth) του συνδέσμου στο μονοπάτι

με την μικρότερη χωρητικότητα (bottleneck σύνδεσμος), παρά την ύπαρξη ασύρματων δικτύων. Επίσης είναι σε θέση να χειρίζονται άλλες απλές συσκευές (bots), ως εξής: Όταν το διαθέσιμο εύρος ζώνης πέσει κάτω από ένα κατώφλι, λόγω της υπάρχουσας κίνησης στο μονοπάτι (Cross traffic), τότε δίνει εντολή στα bots να ξεκινήσουν την επίθεση. Αντίστοιχα, όταν το διαθέσιμο εύρος ζώνης στο bottleneck σύνδεσμο ξεπεράσει το κατώφλι, τότε δίνουν εντολές στα bots να σταματήσουν την επίθεση και η διαδικασία επαναλαμβάνεται. Οι συντονιστές αντιλαμβάνονται, την αλλαγή στις τιμές του διαθέσιμου εύρους ζώνης μέσω διαδοχικών δειγματοληψιών του μονοπατιού για τυχόν αλλαγές του διαθέσιμου ευρους ζώνης (direct probing).

- Επίσης σχεδιάστηκαν απλές συσκευές (bots), οι οποίες στέλνουν την κακόβουλη κίνηση προς τον στόχο. Συγκεκριμένα, όταν λάβουν εντολή από κάποιον συντονιστή για να ξεκινήσει η επίθεση, αποστέλλουν κίνηση με τη μορφή τετραγωνικού παλμού, η οποία εκμεταλλεύεται το μηχανισμό ελέγχου συμφόρησης του πρωτοκόλλου TCP. Με τον τρόπο αυτό, η επίθεση στοχεύει να προκαλέσει όσο το δυνατό μεγαλύτερη ζημιά με την περισσότερη δυνατή μυστικότητα. Ακόμα έχουν την δυνατότητα, εφόσον ξεκινήσει καινούριος κύκλος της επίθεσης να ανελιχθούν σε συντονιστές, όπως θα αναφερθεί σε επόμενο κεφάλαιο.

- Τέλος, αξιολογήθηκε, η αποδοτικότητα της επίθεσης για δύο σενάρια με διαφορετικές παραμέτρους. Τα αποτελέσματα για κάθε σενάριο παρουσιάστηκαν με τη χρήση γραφημάτων, ταυτόχρονα με τα συμπεράσματα που προέκυψαν σχετικά με την επίδοση της επίθεσης για κάθε ένα από αυτά. Μέσα από τα πειράματα που πραγματοποιήθηκαν έγινε εμφανές το εύρος της ζημιάς που μπορεί να προκαλέσει μία παρόμοια επίθεση σε ένα δίκτυο.

1.4 Οργάνωση Κειμένου

Η οργάνωση του υπόλοιπου μέρους της παρούσας διπλωματικής εργασίας διεκπεραιώνεται ως εξής. Στο Κεφάλαιο 2 παρουσίαζονται αναλυτικά ορισμένες από τις κυριότερες επιθέσεις που ανήκουν στην οικογένεια των DDoS επιθέσεων. Στο Κεφάλαιο 3 παρουσιάζεται το θεωρητικό υπόβαθρο πάνω στο οποίο στηρίζεται η εργασία. Στο Κεφάλαιο 4 γίνεται ανάλυση της επίθεσης με παράθεση καθενός από τα στάδιά της, καθώς και των κύριων στοιχείων που την απαρτίζουν. Στο Κεφάλαιο 5 παρουσιάζονται οι παράμετροι αξιολόγησης και τα αποτελέσματα της επίθεσης. Στο Κεφάλαιο 6 παρατίθενται τρόποι αντιμετώπισής της καθώς και πιθανές μελλοντικές επεκτάσεις πάνω στο συγκεκριμένο αντικείμενο.

Κεφάλαιο 2

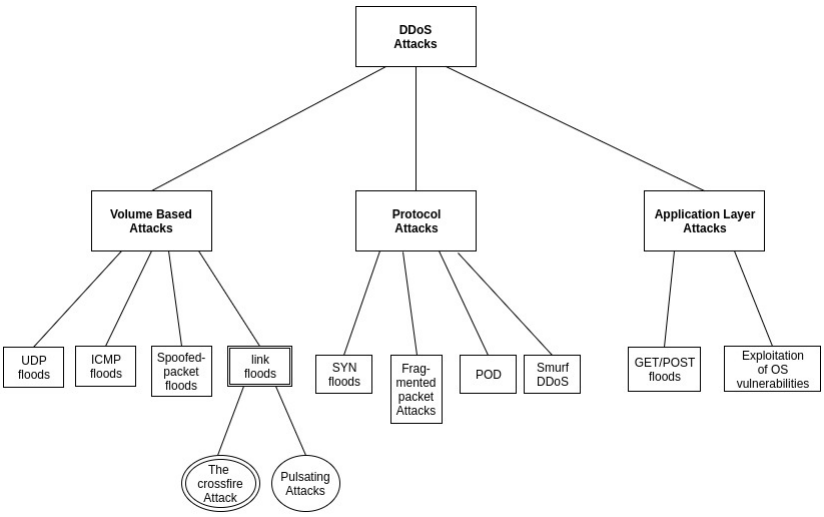
Κατανεμημένες Επιθέσεις τύπου Άρνησης - DDoS

2.1 Τύποι των Επιθέσεων

Οι επιθέσεις DDoS μπορούν να χωριστούν ανάλογα με τον τρόπο υλοποίησής τους σε τρεις διαφορετικές κατηγορίες, όπως στο σχήμα 2.1 [15]:

- **Volume based Attacks (Επιθέσεις βασισμένες στον όγκο δεδομένων)**:
  Όπως προδίδει και το όνομα τους, αυτές οι επιθέσεις έχουν ως στόχο να κορεστεί το bandwidth μίας ιστοσελίδας ή δικτυακού τόπου και το σκέλος τους μετράται σε bits per second (bps). Σε αυτή την κατηγορία περιλαμβάνονται τα UDP floods (πλημμύρες UDP), τα ICMP floods (πλημμύρες ICMP) και άλλα spoofed-packet floods (επιθέσεων "ψεύτικων"-πακέτων).

- **Protocol Attacks (Επιθέσεις Πρωτοκόλλων)**:
  Οι επιθέσεις αυτές καταλαμβάνουν πόρους από κάποιον server



Σχήμα 2.1: Οικογένεια των επιθέσεων DDoS

ή ενδιάμεσων μέσων επικοινωνίας, όπως εξισσοροπητές φορτίων (load balancers), τειχών προστασίας (firewalls), κ.τ.λ. Το σκέλος τους μετράται σε πακέτα ανά δευτερόλεπτο (packets per second). Στις επιθέσεις αυτές περιλαμβάνονται οι πλημμύρες SYN (SYN floods), οι επιθέσεις κατακερματισμένων πακέτων (fragmented packet attacks), το ”Ping του θανάτου” (Ping of Death) και άλλες πολλές.

- **Application Layer Attacks (Επιθέσεις Επιπέδου Εφαρμογής)**: Οι επιθέσεις αυτές έχουν το χαρακτηριστικό ότι κάνουν χρήση ”νόμιμων” και ”απλών” αιτημάτων με σκοπό να καταστείλουν κάποιον web server. Το σκέλος τους μετράται σε αιτήματα ανά δευτερόλεπτο (requests per second). Σε αυτές περιλαμβάνονται οι GET/POST πλημμύρες (GET/POST floods), καθώς και επιθέσεις που εκμεταλλεύονται αδυναμίες των λειτουργικών συστημάτων (Windows, OpenBSD, κ.τ.λ), καθώς και τα low-and-slow attacks.

2.2 Γνωστές DDoS Επιθέσεις

Ενδεικτικά ορισμένες από τις πιο γνωστές επιθέσεις DDoS που έχουν πραγματοποιηθεί είναι οι εξής [15]:

UDP flood: Η συγκεκριμένη επίθεση εκμεταλλεύεται το γεγονός ότι το User Datagram Protocol (UDP) δεν χρησιμοποιεί συνόδους (sessions), όπως το TCP. Συγκεκριμένα στο πλαίσιο της επίθεσης αυτής "πλημμυρίζονται" τυχαίες πορτες ενός απομακρισμένου συστήματος με ένα μεγάλο αριθμό από UDP πακέτα, με αποτέλεσμα το πρώτο να αναζητά συνεχώς την εφαρμογή η οποία αναμένει σε εκείνες τις πόρτες. Όταν αυτή η εφαρμογή δεν βρεθεί τότε το σύστημα απαντά με πακέτα ICMP Destination Unreachable, καταναλώνοντας σημαντικούς πόρους με κίνδυνο να μην μπορεί να εξυπηρετήσει περαιτέρω χρήστες [16, 15].

SYN flood: Σε αυτή την περίπτωση γίνεται εκμετάλλευση μίας αδυναμίας κατά τη διάρκεια της "τριμερούς χειραψίας" ("three-way handshake") του TCP. Συγκεκριμένα, ένα αίτημα SYN το οποίο ξεκινά μία TCP σύνδεση με ένα απομακρισμένο σύστημα πρέπει να απαντηθεί με ένα SYN-ACK πακέτο, από το σύστημα αυτό και τέλος να επιβεβαιωθεί με ένα ACK πακέτο από το σύστημα που έκανε πρώτο το αίτημα. Ο επιτιθέμενος εκμεταλλεύεται αυτή τη διαδικασία, αποστέλλοντας πολλαπλά SYN πακέτα στο απομακρισμένο σύστημα, με αποτέλεσμα τη δημιουργία πολλών απαντήσεων SYN-ACK. Όμως ο επιτεθέμενος είτε δεν αποκρίνεται στα SYN-ACK πακέτα, είτε χρησιμοποιεί ψεύτικες IP διευθύνσεις (spoofed IP) και κατά συνέπεια το απομακρισμένο σύστημα περιμένει από των αιτώντα να ανταποκριθεί μέσω των ACK πακέτων, για κάθε μία από τις αιτήσεις, καταλαμβάνοντας πόρους σε σημείο που δεν μπορούν να πραγματοποιηθούν άλλες συνδέσεις (άρνηση υπηρεσιών). Την τεχνική αυτή χρησιμοποιεί σε κάποιο βαθμό και η επίθεση που έχουμε σχεδιάσει και αναλύσει στο πλαίσιο αυτής της διπλωματικής, η οποία θα εξηγηθεί αργότερα [17, 15].

Ping of Death (POD): Η επίθεση αυτή περιλαμβάνει την αποστολή πολλαπλών παραμορφωμένων ή κακόβουλων ping σε ένα σύστημα. Ένα πακέτο IPv4 ping μπορεί να έχει και ως 65535 bytes σε μέγεθος και πολλά συστήματα TCP/IP δεν μπορούν να διαχειριστούν πακέτα με μεγαλύτερα μεγέθη. Επίσης το επίπεδο Ζεύξης Δεδομένων (Data Link Layer) επιβάλλει περιορισμούς στο μέγιστο μέγεθος ενός πακέτου (συνήθως 1500 Bytes για τα δίκτυα Ethernet). Στην περίπτωση που ένα πακέτο IP ξεπερνά σε μέγεθος την υποστηριζόμενη MTU (Maximum Transmission Unit), τότε αυτό κατακερματίζεται σε μικρότερα πακέτα IP (θραύσματα - fragments) και ο αποδέκτης τα επανασυνδέει στο αρχικό ολοκληρωμένο πακέτο. Κατά την επίθεση Ping of Death, πραγματοποιείται αποστολή παραποιημένων πακέτων/θραυσμάτων, με αποτέλεσμα ο αποδέκτης να καταλήγει να έχει ένα πακέτο που ξεπερνά τα 65535 bytes όταν επανασυναρμολογηθεί. Κατά συνέπεια είναι δυνατό να προκληθεί υπερχείλιση των buffer της μνήμης που έχει κατανεμηθεί για το πακέτο, δημιουργώντας άρνηση υπηρεσιών στο σύστημα [18, 15].

HTTP flood: Κατά τη διάρκεια της επίθεσης αυτής ο επιτιθέμενος χρησιμοποιεί αιτήματα HTTP GET ή POST εναντίον ενός διαδικτυακού ιστότοπου/server ή εφαρμογής. Σε αντίθεση με προηγούμενες επιθέσεις που αναφέρθηκαν οι πλημμύρες HTTP δεν κάνουν χρήση παραμορφωμένων πακέτων ή τεχνικών που κάνουν χρήση ψεύτικων (spoofed) διευθύνσεων IP, ενώ ταυτόχρονα χρειάζονται λιγότερους πόρους (όπως το bandwidth) για να καταστήσουν την ιστοσελίδα ή τον server μη λειτουργικούς. Η επίθεση είναι πολύ αποτελεσματική, καθώς η κακόβουλη κίνηση δεν είναι εύκολο να διακριθεί από την νόμιμη, ενώ το σύστημα αναγκάζεται να χρησιμοποιήσει όσο το δυνατό περισσότερους πόρους γίνεται για την εξυπηρέτηση ενός αιτήματος [19, 15].

2.3 Επιθέσεις Βασισμένες στην Κρυφή Μνήμη

Προχωρώντας σε πιο εξελιγμένες μορφές DDoS επιθέσεων δεν θα μπορούσαμε να παραλείψουμε τις επιθέσεις που βασίζονται στην Κρυφή Μνήμη (Memcached Attacks) που εκμεταλλεύονται τους
Memcached web servers [20].

Ως Memcached web servers εννοούμε συστήματα κατανεμημένης κρυφής μνήμης, τα οποία χρησιμοποιούνται συνήθως για να επιταχύνουν ιστοσελίδες που υλοποιούν δυναμικές βάσεις δεδομένων, αποθηκεύοντας δεδομένα και αντικείμενα στη Μνήμη Τυχαίας Προσπέλασης τους (Random Access Memory - RAM) έτσι ώστε να ελαχιστοποιηθούν οι φορές που θα πρέπει να προσπελαθεί μία εξωτερική πηγή με δεδομένα (π.χ., μία Βάση Δεδομένων). Οι Memcached servers είναι ευρέως διαδεδομένοι στη σημερινή εποχή, εφόσον χρησιμοποιούνται από μεγάλους παρόχους διαδικτυακών υπηρεσιών όπως το Youtube, το Facebook, το Pinterest, το Twitter, τα Amazon Web Services (AWS), κ.τ.λ.

Εξαιτίας της δυνατότητάς τους να προσπελαύνουν δεδομένα ταχύτερα, οι servers αυτοί έχουν γίνει την περίοδο της συγγραφής αυτής της διπλωματικής στόχος πολλών κακόβουλων χρηστών οι οποίοι τους χρησιμοποιούν ως ένα μέσο ενίσχυσης επιθέσεων DDoS έως και 50000 φορές περισσότερο από μία απλή περίπτωση [14].

Συγκεκριμένα, ο/η επιτιθέμενος/η στέλνει ένα μικρό αίτημα από μία ψεύτικη/"κλεμμένη" (spoofed) IP στον Memcached server και αυτό απαντά πίσω στο πραγματικό μηχάνημα με την ίδια IP με μία "μεγαλύτερη" απάντηση. Πολλά τέτοια αιτήματα έχουν ως αποτέλεσμα το τελευταίο να δέχεται ένα τεράστιο όγκο δεδομένων προερχόμενων από τον Memcached server, με αποτέλεσμα να καταλώνονται όλοι οι πόροι του. Ταυτόχρονα, καταναλώνονται και σημαντικοί πόροι του Διαδικτύου, με αποτέλεσμα να μην είναι δυνατό να εξυπηρετηθούν νέα αιτήματα από νόμιμους χρήστες, οπότε έχουμε άρνηση υπηρεσιών.

Το αξιοσημείωτο της επίθεσης αυτής είναι ότι ένα αίτημα μερικών Byte μπορεί να προκαλέσει μία απάντηση εκατοντάδων KByte, φανερώντας την τεράστια κλιμάκωση μίας τέτοιας επίθεσης χρησιμοποιώντας ελάχιστα κακόβουλα συστήματα. Προς το παρόν οι πιο αποτελεσματικοί τρόποι αντιμετώπισης των επιθέσεων αυτών είναι η εφαρμογή ειδικών κανόνων firewall ώστε να εμποδιστεί η λειτουργία ορισμένων θυρών UDP που χρησιμοποιούν οι Memcached servers και η απαγόρευση της υποκλοπής διευθύνσεων IP στο Διαδίκτυο από τους ISPs (Internet Service Providers), κάτι το οποίο είναι αρκετά δύσκολο να επιτευχθεί.

2.4 Επιθέσεις Διασταυρούμενων Πυρών

Οι επιθέσεις Διασταυρούμενων Πυρών (Crossfire Attacks) ανήκουν σε μία ειδική κατηγορία DDoS επιθέσεων, τις link flooding επιθέσεις. Η κυριότερη διαφορά των επιθέσεων αυτών σε σχέση με μία απλή DDoS επίθεση είναι ότι δεν στοχοποιούν έναν συγκεκριμένο server ή ιστοσελίδα. Αντίθετα, κύριος σκοπός τους είναι η διακοπή ή η παρεμπόδιση της συνδεσιμότητας των συστημάτων Διαδικτύου, καθώς και η πρόκληση ασταθειών στην δρομολόγηση των πακέτων. Παρόλα αυτά οι συγκεκριμένες επιθέσεις είναι δύσκολο να υλοποιηθούν σε πραγματικά σενάρια, κυρίως λόγω της δυσκολίας επιλογής των συνδέσμων-στόχων.

Όπως και οι περισσότερες επιθέσεις τύπου DDoS, έτσι και τα Crossfire attacks υλοποιούνται με την χρήση ενός ή περισσότερων botnets. Με τον όρο botnet εννοούμε ένα πλήθος από συσκευές συνδεδεμένες στο Διαδίκτυο (συνήθως υπό την ιδιοκτησία απλών χρηστών) τις οποίες έχει καταλάβει ο επιτιθέμενος αθέμιτα με σκοπό να τις χρησιμοποιήσει για την διεξαγωγή της επίθεσης. Οι συσκευές αυτές, επονομαζόμενες και bots, τρέχουν κάποιου είδους κακόβουλο λογισμικό (malicious software - malware-), υπεύθυνο για την διεξαγωγή της επίθεσης, και την πιθανή επικοινωνία κάθε bot με έναν διαχειριστή (coordinator), ο οποίος ελέγχει τις δραστηριότητες του κάθε bot [21].

Το κυριότερο πλεονέκτημα των Crossfire επιθέσεων σε σχέση με άλλες επιθέσεις DDoS που κάνουν χρήση ενός botnet, αποτελεί το γεγονός ότι οι πρώτες δεν είναι εύκολα ανιχνεύσιμες από τους ήδη υπάρχοντες μηχανισμούς προστασίας του διαδικτύου [3, 22]. Συγκεκριμένα, στις επιθέσεις αυτές μπορεί να γίνει χρήση πραγματικών διευθύνσεων IP, καθιστώντας αυτόματα όποιους μηχανισμούς ανίχνευσης και παρεμπόδισης της χρήσης spoofed διευθύνσεων IP, μάταιες (όπως το "φιλτραρισμά τους"). Επιπρόσθετα, τα bots μπορούν να "πνίξουν" κάποιο link δημιουργώντας νόμιμη κίνηση και όχι ανεπιθύμητη (π.χ., αποστέλλοντας πακέτα τα οποία διέρχονται από συγκεκριμένους δρομολογητές). Τέλος η κίνηση που δημιουργεί το κάθε bot μπορεί να είναι χαμηλής έντασης/μηδαμινή. Παρόλαυτά, όταν όλη η κίνηση του botnet περάσει συγκεντρωτικά από ένα link την ίδια χρονική στιγμή αυτό έχει σαν αποτέλεσμα τον "πνιγμό" του. Ο διαχειριστής-coordinator μπορεί να βρει ένα σύνολο από servers με διευθύνσεις IP εμφανείς στο Διαδίκτυο και με όλη την κίνηση που προορίζεται προς εκείνους να διέρχεται από κοινούς συνδέσμους. Ύστερα μπορεί να προγραμματίσει τα bot να στείλουν μηδαμινή κίνηση προς αυτές τις διευθύνσεις IP.

Συγκεκριμένα οι επιθέσεις Crossfire έχουν ως σκοπό να παρεμποδίσουν την συνδεσιμότητα μιας ομάδας συστημάτων/servers στο Διαδίκτυο, παρακάμπτοντας την αποστολή κακόβουλης κίνησης απευθείας σε εκείνα ως εξής [3, 22, 23]:

(α΄) Ο επιτιθέμενος κατασκευάζει έναν χάρτη από συνδέσμους γύρω από την ομάδα/στόχο, κάνοντας πολλά traceroutes σε διάφορους κόμβους στο δίκτυο.

(β΄) Διακρίνει τους μόνιμους συνδέσμους (persistent links), οι οποίοι συνδέουν τον στόχο με το Διαδίκτυο.

(γ΄) Βρίσκει servers δολώματα ή ομάδες από server (decoy servers) οι οποίες δεν ανήκουν στον στόχο, αλλά η κίνηση σε αυτά δρομολογείται μέσω των μόνιμων συνδέσμων του προηγούμενου βήματος.

(δ΄) Καταναλώνει το bandwidth των μόνιμων συνδέσμων στέλνοντας πολλαπλές ροές με μηδαμινό bandwidth (π.χ., HTTP Requests) από τα bots που ελέγχει προς τους decoy servers.

Παρακάτω παρουσίαζονται τα βήματα όπως αναφέρονται στο [3], αλλά με λιγότερες λεπτομέρειες:

(Α΄) *Σχεδίαση του χάρτη συνδέσμων*

Ο επιτιθέμενος για να πνίξει τον στόχο πρέπει πρωτίστως να κατασκευάσει έναν χάρτη με συνδέσμους του Διαδικτύου που περικλύει την περιοχή στόχο. Για να κατασκευάσει τον χάρτη συνδέσμων ο επιτιθέμενος, αρχικά ορίζει στα bots να τρέξουν traceroutes προς τους δημόσιους servers στην περιοχή στόχο και στους servers δολώματα. Το αποτέλεσμα του traceroute είναι η επιστροφή μίας λίστας από διευθύνσεις IP διαφόρων routers (με συνδέσμους/links να θεωρούμε τις διευθύνσεις IP των γειτόνων ενός router). Η λίστα αυτή δηλαδή δηλώνει το μονοπάτι από IPs που θα ακολουθήσει η κίνηση της επίθεσης. Επίσης αξίζει να σημειωθεί ότι συνήθως πραγματοποιούνται πολλάπλά traceroutes προς τους servers, έτσι ώστε να διαπιστωθεί η μονιμότητα και η πολυπλοκότητα της διαδρομής, χαρακτηριστικά απαραίτητα για την κατασκευή του χάρτη συνδέσμων.

Συνήθως όμως ο επιτιθέμενος δεν είναι δυνατό να επιλέξει απευθείας τους συνδέσμους στόχους από τον χάρτη συνδέσμων καθώς πολλές από τις διαδρομές αυτές μεταβάλλονται με το χρόνο. Αυτό συμβαίνει λόγω των λειτουργιών *διαχείρισης της κίνησης* (traffic engineering) που χρησιμοποιούν οι ISP's (π.χ., εξισσορόπιση φορτίου - load balancing). Το αποτέλεσμα είναι τα διάφορα traceroutes προς τον ίδιο server να περιλαμβάνουν αρκετούς διαφορετικούς συνδέσμους κάθε φορά. Συνεπώς η επιλογή ενός τέτοιου συνδέσμου θα οδηγούσε τον επιτιθέμενο να προσπαθεί να ''πνίξει'' έναν ασταθή στόχο, γεγονός που θα καθιστούσε την επίθεση ανεπιτυχή.

Τους συνδέσμους αυτούς τους ονομάζουμε *μεταβλητούς* (transient) σε αντίθεση με τους συνδέσμους, οι οποίοι εμφανίζονται πάντοτε σε μία διαδρομή τους οποίους ονομάζουμε *μόνιμους* (persistent). Ο επιτιθέμενος ενδιαφέρεται μόνο για τους μόνιμους συνδέσμους, οπότε τους διαχωρίζει από τους μεταβλητούς.

(Β΄) *Προετοιμασία της επίθεσης*

Σε αυτό το στάδιο ο επιτιθέμενος εξακριβώνει τους κρίσιμους συνδέσμους (critical links), από το χάρτη συνδέσμων. Με τον όρο κρίσιμοι σύνδεσμοι εννοούμε τους μόνιμους συνδέσμους, οι οποίοι αν αποκοπούν αποκλείουν ταυτόχρονα το μεγαλύτερο όγκο της κίνησης προς την περιοχή-στόχο.

Συγκεκριμένα, ο επιτιθέμενος χρησιμοποιεί το χάρτη συνδέσμων και υπολογίζει την πυκνότητα ροής για κάθε σύνδεσμο του δικτύου στον χάρτη. Ως πυκνότητα ροής ενός μόνιμου συνδέσμου ορίζουμε των αριθμό των ροών μεταξύ των bots και των servers της περιοχής-στόχου που μπορούν να δημιουργηθούν, εν μέσω του συνδέσμου αυτού.

Μία μεγάλη πυκνότητα ροής σε έναν σύνδεσμο συνεπάγεται ότι ο σύνδεσμος μπορεί να μεταφέρει ένα υψηλό ποσό κίνησης προς μία περιοχή-στόχο (κακόβουλη και νόμιμη). Οπότε είναι προς το συμφέρον του επιτιθέμενου να επιλέξει αυτό το σύνδεσμο ως πιθανό στόχο. Έχει αποδειχθεί ότι η πυκνότητα ροής ακολουθεί μία κατανομή *power-law* σε ένα χάρτη συνδέσμων, καθιστώντας εύκολη την εύρεση των ροών με τη μεγαλύτερη πυκνότητα ροής προς την περιοχή στόχο από τον επιτιθέμενο [3].

Έχοντας όλα τα παραπάνω δεδομένα, ο επιτιθέμενος επιλέγει στη συνέχεια διάφορα μη επικαλυπτόμενα σύνολα από συνδέσμους στόχους για να αποκόψει. Στόχος του επιτιθέμενου είναι να επιλέξει βέλτιστα δύο ή περισσότερα τέτοια σύνολα έτσι ώστε να καταφέρει να εμποδίσει την εισροή όσο περισσότερης κίνησης είναι εφικτό προς την περιοχή-στόχο. Για την επιλογή των συνόλων αυτών γίνε-

ται χρήση του χαρτη συνδέσμων και της πυκνότητας ροής.

(Γ΄) *Συντονισμός των bots*

Με το πέρας των παραπάνω βημάτων ο επιτιθέμενος συντονίζει τα bots, ώστε να ξεκινήσουν την επίθεση. Για κάθε σύνολο συνδέσμων που θα βρίσκεται υπό επίθεση, ανατίθενται σε κάθε bot μία λίστα από servers δολώματα (decoy servers), αλλά και ο ρυθμός αποστολής της κίνησης προς καθέναν από αυτούς, αντίστοιχα. Ο ρυθμός αποστολής επιλέγεται προσεκτικά έτσι ώστε και η κίνηση που δημιουργεί το κάθε bot να μην ενεργοποιεί ''συναγερμούς'' των ISPs (είναι δηλαδή μηδαμινή) και η συσσωρευμένη κίνηση από όλα τα bots, ταυτόχρονα, να επαρκεί, ώστε να ''πνίξει'' όλους τους συνδέσμους-στόχους (target links).

Όπως αναφέρθηκε προηγουμένως η συσσωρευμένη κακόβουλη κίνηση προς κάθε σύνδεσμο-στόχο πρέπει να είναι αρκετά μεγάλη, έτσι ώστε να ξεπερνά την υπολοιπόμενη χωρητικότητα (capacity) ή bandwidth του εν λόγω συνδέσμου και άρα οι νόμιμες ροές που περνούν από τους συνδέσμους αυτούς να περιοριστούν σε σημαντικό βαθμό. Ο επιτιθέμενος πρέπει όμως να ικανοποιήσει δύο περιορισμούς. Ο πρώτος είναι η κάθε μεμονωμένη κίνηση από κάθε bot να είναι αρκετά μικρή έτσι ώστε να μην ενεργοποιηθούν οι μηχανισμοί ασφάλειας δικτύου. Συνήθως, τέτοιοι μηχανισμοί αφορούν τα *Δίκτυα Καθοριζόμενα από το Λογισμικό* (Software Defined Networks - SDN), όπου ο ''χειριστής'' (SDN Controller) παρακολουθώντας το δίκτυο μπορεί να καταλάβει αν η κίνηση είναι κακόβουλη. Επίσης την ίδια λειτουργία επιτελούν πιο στοχευμένα τα *Συστήματα Εύρεσης Διεισδύσεων* (Intrusion Detection Systems - IDS). Ο δεύτερος περιορισμός είναι η συσσωρευμένη κακόβουλη κίνηση που επαρκεί για να ''πνίξει'' τους συνδέσμους-στόχους να ανατίθεται ομοιόμορφα στα διάφορα bots και στους servers δολώματα. Το αποτέλεσμα είναι να επιτυγχάνεται πανομοιοτυπία των κακόβουλων ροών με τις νόμιμες καθώς και την μη αναγνωρισιμότητα από τους servers στην περιοχή στόχο και τους servers δολώ-

ματα.

Ο επιτιθέμενος αναθέτει στα bots να ξεκινήσουν να στέλνουν τις κακόβουλες ροές. Σε κάθε bot έχουν ανατεθεί πολλές διαφορετικές ροές, κάθε μία από τις οποίες έχει ως στόχο και έναν διαφορετικό server δόλωμα ή bot. Τα bots έχουν επίσης την δυνατότητα να ρυθμίζουν δυναμικά κι τον ρυθμό με τον οποίο στέλνουν πακέτα στους στόχους τους. Συγκεκριμένα, ξεκινούν με χαμηλούς ρυθμούς και τους αυξάνουν σταδιακά μέχρι ο αντίστοιχος στόχος σύνδεσμος να ''πνιγεί''.

(Δ΄) Κινούμενες Επιθέσεις

Ο επιτιθέμενος είναι δυνατό να αλλάξει το σύνολο των συνδέσμων στόχων κατά τη διάρκεια της επίθεσης, μέσα από τα διαφορετικά τέτοια σύνολα που έχουν αναφερθεί σε προηγούμενο βήμα. Η δυνατότητα αυτή συμβάλλει στην επέκταση του χρόνου εκτέλεσης της Crossfire επίθεσης, αφού όπως είναι λογικό αν το σύνολο ήταν πάντοτε σταθερό, τότε σε κάποια χρονική στιγμή θα ενεργοποιούνταν οι μηχανισμοί προστασίας του Διαδικτύου.

2.5 Παλμοδικές Επιθέσεις

Οι Παλμοδικές επιθέσεις (Pulsating Attacks) ανήκουν και αυτές στην οικογένεια των DDoS και συγκεκριμένα των link flooding επιθέσεων, άλλα είναι ακόμη περισσότερο καταστροφικές. Συγκεκριμένα, στις παλμοδικές επιθέσεις τα bots συντονίζονται, έτσι ώστε να δημιουργούν κατά διαστήματα παλμούς προς τους συνδέσμους-στόχους με σκοπό να μειώσουν σημαντικά το throughput των συνδέσεων TCP που διασχίζουν τους συνδέσμους αυτούς. Δυό από τις πιο γνωστές παλμοδικές επιθέσεις είναι οι εξής:

The Shrew attack: Η επίθεση Shrew [25] έχει ως στόχο το πρωτόκολλο TCP και εκμεταλλεύεται την ιδιαιτερότητα του minimum Retransmission

Time Out (minRTO) του TCP πρωτοκόλλου, ότι οι ροές που υφίστανται ταυτόχρονη απόρριψη πακέτων πιθανότατα θα ξαναμεταδώσουν τα πακέτα τους την ίδια χρονική στιγμή. Αναλυτικότερα, στόχος της επίθεσης αυτής είναι να δημιουργήσει βραχείς συμφορήσεις όταν νόμιμες ροές TCP αναμεταδίδουν τα πακέτα τους. Το αποτέλεσμα είναι το πρωτόκολλο TCP να θεωρεί ότι υπάρχει συμφόρηση για μεγάλο διάστημα, μειώνοντας έτσι το ρυθμό αναμετάδοσής του σχεδόν στο μηδέν. Για να το πετύχει αυτό ο επιτιθέμενος στέλνει ειδικά κατασκευασμένους ορθογωνικούς παλμούς σε μορφή ροής με περίοδο που πλησιάζει το minRTO και διάρκεια κοντά στο maximum Round-Trip Time των νόμιμων ροών.

The RoQ attack: Η επίθεση RoQ (Reduce of Quality) [26] σε αντίθεση με τις περισσότερες επιθέσεις DoS προσπαθεί να μειώσει την αποδοτικότητα του στόχου παρά να αποκόψει εντελώς τις υπηρεσίες που προσφέρει. Η λειτουργία της επίθεσης RoQ είναι αρκετά παρόμοια με της επίθεσης Shrew, με την έννοια ότι και πάλι χρησιμοποιούνται ειδικά κατασκευασμένοι ορθογωνικοί παλμοί με σκοπο να οδηγήσουν τον στόχοθύμα σε μία κατάσταση στην οποία δεν είναι δυνατό να βρεί ισορροπία μεγιστοποιώντας την απόδοσή του. Η κύρια διαφορά των επιθέσεων αυτών είναι ότι ενώ η επίθεση Shrew εκμεταλλεύεται τις ιδιαιτερότητες του πρωτοκόλλου TCP, η επίθεση RoQ δεν χρησιμοποιεί κάποιο συγκεκριμένο μηχανισμό, απλώς επιδεινώνει την απόδοση του στόχου.

2.6 Προκαλώντας Συμφόρηση στο Διαδίκτυο μέσω Συντονισμένων και Αποκεντρωμένων Παλμοδικών Επιθέσεων

Το κυριότερο μειονέκτημα των παραπάνω επιθέσεων είναι ότι χρησιμοποιούν έναν κύριο συντονιστή ο οποίος είναι υπεύθυνος για να αναθέτει στα bots τις παραμέτρους για την επίθεση, καθώς και για τον

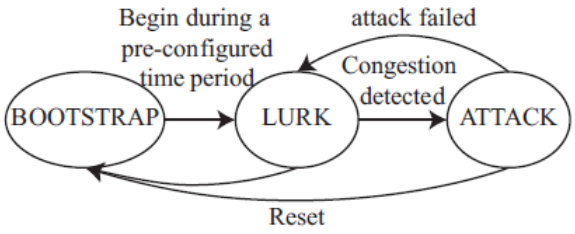
συγχρονισμό τους. Ως συνέπεια, είναι ευκολότερο για τους μηχανισμούς άμυνας του Διαδικτύου να ανακαλύψουν τις επιθέσεις αυτές και να τις διακόψουν. Το εμπόδιο αυτό ξεπεράστηκε μέσω ενός πιο εξελιγμένου είδους παλμοδικής επίθεσης, το οποίο υλοποιεί τον αποκεντρωμένο συντονισμό και συγχρονισμό των bots, επιτυγχάνοτας συγχρόνως και την μέγιστη δυνατή καταστροφικότητα και μη εντοπισημότητα. Η επίθεση αυτή με ονομάσια, Προκαλώντας Συμφόρηση στο Διαδίκτυο μέσω Συντονισμένων και Αποκεντρωμένων Παλμοδικών Επιθέσεων (Congesting the Internet with Coordinated And Decentralized Pulsating Attacks - CICADAS) [3] παρουσιάζεται αναλυτικότερα παρακάτω:

Ο κυριότερος στόχος της επίθεσης CICADAS είναι να συντονίσει τα bots χωρίς να γίνει χρήση κάποιου συντονιστή και διαθέτοντας ελάχιστες γνώσεις για την κατάσταση του Διαδικτύου. Ως καταλύτης για την ενεργοποίηση των bots και κατά συνέπεια της επίθεσης, μπορεί να χρησιμοποιηθεί συμφόρηση σε έναν σύνδεσμο στόχο. Τα bots μπορούν να ''παρατηρούν'' τον σύνδεσμο-στόχο για τυχόν συμφορήσεις (λειτουργούν ως σήμα συγχρονισμού) εξετάζοντας διάφορες μετρικές, όπως η απώλεια πακέτων ή η καθυστέρησή τους και να συγχρονίζονται με εκείνες. Συγκεκριμένα, κάθε bot υποθέτει το εύρος της συμφόρησης μέσω των αλλαγών στην καθυστέρηση μεταφοράς στο σύνδεσμο-στόχο.

Τα δύο κυριότερα συστατικά της επίθεσης αποτελούν [3]: 1) Ο Εκτιμητής Συμφορήσεων (Congestion Detector), ο οποίος διαπιστώνει τις διάφορες περιπτώσεις συμφορήσεων στο σύνδεσμο-στόχο, μέσω των παρατηρούμενων RTTs και 2) Η γεννήτρια της επίθεσης, η οποία χρησιμοποιώντας τις παραπάνω εκτιμήσεις ρυθμίζει την ροή της επίθεσης, έτσι ώστε οι αποκεντρωμένες κακόβουλες ροές όταν προστίθενται να δημιουργούν περιοδικούς παλμούς στο σύνδεσμο-στόχο, χωρίς τη μεσολάβηση κάποιου κεντρικού συντονιστή.

2.6.1 Στάδια της Επίθεσης

Η επίθεση CICADAS χωρίζεται σε τρία στάδια [3]: το στάδιο εκκίνησης (Bootstrap Phase), το στάδιο παραμονής (Lurk Phase) και το στάδιο επίθεσης (Attack Phase). Τα στάδια αυτά και οι μεταβάσεις μεταξύ τους φαίνονται καλύτερα στο σχήμα 2.2.



Σχήμα 2.2: Στάδια της επίθεσης CICADAS

Αναλυτικότερα, στο στάδιο εκκίνησης τα bots λαμβάνουν τις παραμέτρους απαραίτητες για την υλοποίηση της επίθεσης (π.χ., την περίοδο της επίθεσης, το μήκος ξεσπάσματος, το πλάτος ξεσπάσματος και τον στόχο-σύνδεσμο). Οι πρώτες τρεις παράμετροι συμβάλλουν στην κατασκευή του τετραγωνικού παλμού που θα ''πνίξει'' τον σύνδεσμο στόχο. Τα bots ύστερα μπορούν να μεταβούν στο επόμενο στάδιο (Lurk Phase), χωρίς να υπάρχει χρονικός συγχρονισμός μεταξύ τους.

Στο στάδιο παραμονής τα bots παρακολουθούν τον σύνδεσμο στόχο για τυχόν συμφόρηση (παρατηρούν υψηλά RTTs στα πακέτα εξερεύνησης/probes που στέλνουν μεταξύ τους). Όταν αποφανθούν ότι όντως υπάρχει συμφόρηση τότε μεταβαίνουν στο στάδιο επίθεσης.

Στο τελευταίο στάδιο, το στάδιο επίθεσης, κάθε bot αποστέλλει τετραγωνικούς παλμούς προς τον στόχο-σύνδεσμο, με σκοπό να προκληθεί μακρά συμφόρηση σε αυτό. Ο αριθμός των bots που θα ενεργοποιηθούν παίζει σημαντικό ρόλο εφόσον όσο περισσότερα είναι τόσο μεγαλύτερη συμφόρηση αναμένεται στο σύνδεσμο-στόχο εξαιτίας της κακόβουλης κίνησης, ενώ η νόμιμη θα περιορίζεται. Αν ο συντονισμός των bots αποτύχει τότε αυτά επιστρέφουν στο στάδιο παραμονής.

2.6.2 Εκτιμητής Συμφορήσεων

Όπως αναφέρθηκε και προηγουμένως η επίθεση CICADAS στηρίζεται αρκετά στον εκτιμητή συμφορήσεων για τον επιτυχή συντονισμό των bots και την έναρξη της επίθεσης. Συγκεκριμένα ο εκτιμητής επιτελεί δύο λειτουργίες. Στέλνει πακέτα εξερεύνησης/probes στο σύνδεσμο στόχο και εκτιμά πότε συμβαίνει συμφόρηση στον σύνδεσμο αυτόν.

Κατά την πρώτη λειτουργία ειδικά πακέτα probes με μικρό μέγεθος αποστέλλονται μεταξύ των bots, με την προϋπόθεση ότι εκείνα διέρχονται από τον σύνδεσμο στόχο. Ύστερα τα bots παρατηρούν τα RTTs των πακέτων αυτών τα οποία χρειάζονται για τη δεύτερη λειτουργία του εκτιμητή.

Κατά την δεύτερη λειτουργία του εκτιμητή, χρησιμοποιούνται οι μετρήσεις των RTTs έτσι ώστε να βρεθεί αν στο σύνδεσμο στόχο ξεκινά συμφόρηση, βρίσκεται σε εξέλιξη ή υποχωρεί. Ταυτόχρονα και προηγούμενες εκτιμήσεις συμφορήσεων λαμβάνονται υπόψην, έτσι ώστε κάθε νέα εκτίμηση να είναι πιο ακριβής. Σε αυτό το κομμάτι συμβάλλει και η χρήση του φίλτρου Kalman (Kalman filter), ώστε να αποβάλλονται

οποιεσδηποτε παρεμβολές λόγω της φύσης και της πολυπλοκότητας του Διαδικτύου, όπως θόρυβοι και η τελική εκτίμηση να είναι όσο περισσότερο κοντά γίνεται στην πραγματικότητα.

2.6.3 Γεννήτρια Επιθέσεων

Σκοπός του επιτιθέμενου είναι να συνδυαστούν όλες οι μεμονωμένες ροές των bots σε έναν τετραγωνικό παλμό στο σύνδεσμο στόχο, ο οποίος θα προκαλέσει μεγάλη συμφόρηση. Για την δημιουργία των μεμονωμένων αυτών ροών η επίθεση CICADAS χρησιμοποιεί την τεχνική TCP embedding [3]. Η τεχνική αυτή εκμεταλλεύται τις ιδιαιτερότητες του πρωτοκόλλου TCP και συγκεκριμένα τον αλγόριθμο ελέγχου συμφορήσεων που υλοποιεί (θα αναφερθεί και αργότερα). Αυτό επιτρέπει στην επίθεση CICADAS να παραμένει δυσεύρετη από τους μηχανισμούς προστασίας του διαδικτύου, αλλά και να διατηρεί τη συμφόρηση για μεγαλύτερα χρονικά διαστήματα προκαλώντας μεγαλύτερη ζημιά για την περιοχή-στόχο.

Κεφάλαιο 3

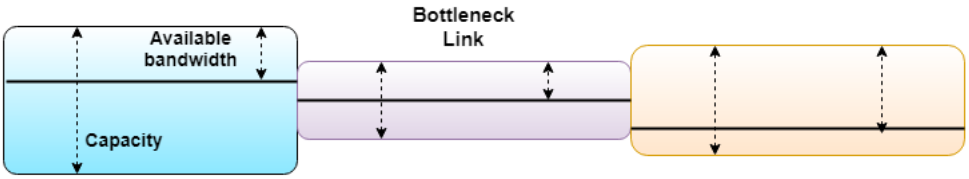
Θεωρητικό υπόβαθρο

Σε αυτό το κεφάλαιο παρουσιάζονται βασικοί ορισμοί και έννοιες [6, 8] απαραίτητες για την κατανόηση του τρόπου λειτουργίας της επίθεσης που αναπτύχθηκε στο πλαίσιο αυτής της διπλωματικής. Ξεκινάμε με γενικούς ορισμούς που αφορούν χαρακτηριστικά του διαδικτύου και καταλήγουμε σε ειδικότερες έννοιες σχετικές με την επίθεση

3.1 Βασικοί ορισμοί

Εύρος ζώνης (Bandwidth): Το bandwidth ενός συνδέσμου ή ενός μονοπατιού ενός δικτύου ορίζεται ως ο ρυθμός με τον οποίο μπορούν αυτά να μεταφέρουν δεδομένα. Ειδικότερα, συσχετίζεται με το μέγεθος των δεδομένων που μπορεί να μεταφέρει ένας σύνδεσμος ή ένα μονοπάτι ανά μονάδα χρόνου.

Segments και Hops: Δύο μετρικές που έχουν σχέση με το bandwidth είναι τα segments και τα hops. Ως segment ορίζουμε ένα φυσικό σύνδεσμο σημείου προς σημείο (*point-to-point* link), ένα εικονικό κύκλωμα (virtual circuit) ή ένα τοπικό δίκτυο κοινής πρόσβασης (shared access



Σχήμα 3.1: Χωρητικότητα, Διαθέσιμο Εύρος Ζώνης και Bottleneck Σύνδεσμος

local area network). Αντιθέτως, το hop μπορεί να αποτελείται από ένα ή περισσότερα segments συνδεδεμένα μεταξύ τους μέσω διακοπτών (switches), γεφυρών (bridges), κ.τ.λ. Ένα μονοπάτι από άκρο-σε-άκρο (*end-to-end* path) από ένα σύστημα/πηγή (source) σε ένα άλλο σύστημα/προορισμό (sink) ορίζεται ως η ακολουθία των hops που τα συνδέει μεταξύ τους.

Ρυθμός μετάδοσης (Transmission rate): Ο σταθερός ρυθμός με τον οποίο ένα segment ή ένας σύνδεσμος μπορούν να μεταφέρουν δεδομένα, ονομάζεται *transmission rate* του συνδέσμου ή του segment εκείνου. Το κυριότερο χαρακτηριστικό του transmission rate είναι ότι περιορίζεται από τα φυσικά χαρακτηριστικά του μέσου πάνω στο οποίο γίνεται η μεταφορά των δεδομένων.

Maximum Transmission unit (MTU): Ως MTU θεωρούμε τον μέγιστο αριθμό από bytes που μπορεί να μεταφέρει το φυσικό μέσο ανά πακέτο. Συνήθως, ορίζεται στα 1500 Bytes/πακέτο.

Χωρητικότητα (Capacity)): Ορίζουμε τη *χωρητικότητα* ενός hop ως το bit rate με το οποίο το hop αυτό μπορεί να μεταφέρει IP πακέτα με μέγεθος ίσο με το MTU. Επεκτείνοντας αυτόν τον ορισμό, η χωρητικότητα C ενός end-to-end μονοπατιού είναι ο μέγιστος ρυθμός με τον οποίο το μονοπάτι μπορεί να μεταφέρει δεδομένα από την πηγή στο τέλμα (βλ. σχήμα 3.1). Η μικρότερη χωρητικότητα σε ένα μονοπάτι ορίζει και το capacity C ολόκληρου του end-to-end μονοπατιού ως εξής:

$$C = \min_{i=1,\ldots,H} C_i \tag{3.1}$$

όπου το C_i αποτελεί τη χωρητικότητα του i-οστού hop και το H τον συνολικό αριθμό των hops στο μονοπάτι.

Στενός Σύνδεσμος (Narrow Link): Στενός σύνδεσμος ορίζεται ως το hop με τη μικρότερη χωρητικότητα σε ένα μονοπάτι. Ο ορισμός αυτός είναι αρκετά συνυφασμένος με τον όρο bottleneck σύνδεσμο τον οποίο θα χρησιμοποιήσουμε αρκετά παρακάτω (βλ. σχήμα 3.1).

Διαθέσιμο Εύρος Ζώνης (Available Bandwidth): Ως διαθέσιμο εύρος ζώνης ενός συνδέσμου θεωρούμε την αχρησιμοποίητη ή περίσσια χωρητικότητα του συνδέσμου σε μια συγκεκριμένη χρονική στιγμή (βλ. σχήμα 3.1. Αμέσως διακρίνεται η διαφορά με τη χωρητικότητα που παρουσιάστηκε παραπάνω η οποία εξαρτάται από τις φυσικές ιδιότητες και περιορισμούς του μέσου μετοφοράς των δεδομένων. Αντίθετα, το διαθέσιμο εύρος ζώνης εξαρτάται και από την κίνηση που διατρέχει τον σύνδεσμο σε μία δεδομένη χρονική περίοδο, αποτελώντας έτσι μία χρονικά μεταβαλλόμενη μετρική. Έστω $\bar{u}(t-\tau, t)$ η μέση χρησιμοποίηση (average utilization) για μια χρονική περίοδο $(t-\tau, t)$, που δίνεται από τον τύπο:

$$\bar{u}(t-\tau, t) = \frac{1}{\tau} \int_{t-\tau}^{t} u(x)dx \tag{3.2}$$

όπου το $u(x)$ είναι το στιγμιαίο διαθέσμιο εύρος ζώνης του συνδέσμου τη χρονική στιγμή x και το τ, ο *μέσος χρονικός ορίζοντας* του διαθέσιμου εύρους ζώνης. Μαθηματικά το διαθέσιμο εύρος ζώνης A_i του i-οστού hop ορίζεται από τον τύπο:

$$A_i = (1 - u_i)C_i \tag{3.3}$$

όπου το C_i είναι η χωρητικότητα του i-οστού hop και το u_i, είναι η μέση χρησιμοποίηση στο hop αυτό στο συγκεκριμένο χρονικό διάστημα. Ο ορισμός επεκτείνεται και για ένα μονοπάτι με H hops ως εξής:

$$A = min_{i=1,\ldots,H} A_i \tag{3.4}$$

Σφικτός σύνδεσμος (Tight Link): Το hop με το μικρότερο διαθέσιμο εύρος ζώνης σε ένα από άκρο-σε-άκρο μονοπάτι ονομάζεται σφικτός σύνδεσμος του μονοπατιού. Στο πλαίσιο αυτής της διπλωματικής ταυτίζεται με το στενό σύνδεσμο.

3.2 Τεχνικές Εκτίμησης του Bandwidth

Σε αυτό το κομμάτι του κεφαλαίου θα αναφερθούν ορισμένες βασικές τεχνικές εκτίμησης του bandwidth σε ένα δίκτυο, οι οποίες αποτελούν ένα σημαντικό συστατικό της επίθεσης που σχεδιάσαμε. Εκείνες που θα μας απασχολήσουν στο πλαίσιο αυτής της διπλωματικής είναι η τεχνική *packet pair/train dispersion* (PPTD) και η τεχνική trains of packet pairs (TOPP). Η τεχνική TOPP είναι εκείνη πάνω στην οποία βασίζεται και το εργαλείο εκτίμησης του bandwidth, το οποίο χρησιμοποιείται στο πλαίσιο αυτής της διπλωματικής. Θα γίνει αναφορά σε αυτό αναλυτικότερα παρακάτω.

3.2.1 Packet Pair/Train Dispersion

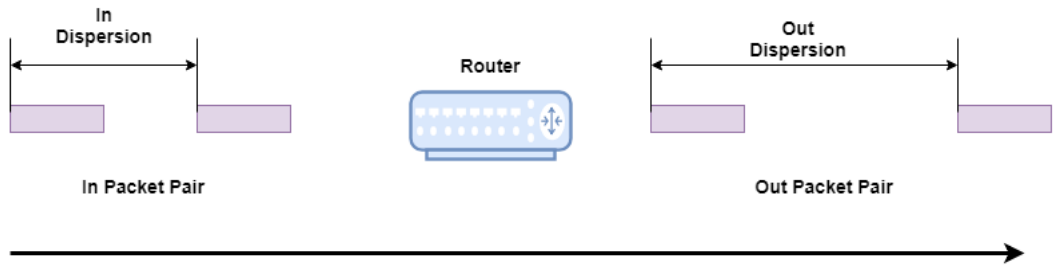
Η τεχνική αυτή όπως και η τεχνική TOPP χρησιμοποιείται για την εκτίμηση του εύρους ζώνης σε ένα από άκρο-σε-άκρο μονοπάτι [4, 6, 8]. Συγκεκριμένα στην τεχνική packet pair probing, μια πηγή στέλνει πολλαπλά *πακέτα δυάδες* (packet pairs) σε έναν αποδέκτη. Κάθε δύαδα

αποτελείται από δύο πακέτα του ίδιου μεγέθους απεσταλμένα το ένα πίσω από το άλλο. Η διασπορά (dispersion) μίας δυάδας πακέτων σε έναν συγκεκριμένο σύνδεσμο είναι η χρονική διαφορά μεταξύ του πρώτου και του τελευταίου bit κάθε πακέτου. Έχοντας υπολογίσει την διασπορά είναι δυνατό ύστερα να εκτιμηθεί εύκολα και η χωρητικότητα C ενός από άκρο-σε-άκρο μονοπατιού από τον τύπο:

$$C = \frac{L}{\Delta_R} \tag{3.5}$$

όπου L είναι το μέγεθος των πακέτων και Δ_R η διασπορά που θα μετρήσει ο αποδέκτης.

Η τεχνική packet train probing αποτελεί μία επέκταση της τεχνικής packet pair probing, χρησιμοποιώντας πολλαπλά διαδοχικά πακέτα. Η διασπορά ενός "τραίνου" από πακέτα σε έναν σύνδεσμο ορίζεται ως ο χρόνος μεταξύ των τελευταίων bit του πρώτου και του τελευταίου πακέτου (βλ. σχήμα 3.2).



Σχήμα 3.2: Διασπορά της δυάδας πακέτων

3.2.2 Trains of Packet Pairs

Στην τεχνική TOPP αποστέλλονται πολλαπλές δυάδες πακέτων με σταδιακά αυξανόμενο ρυθμό από την πηγή στον αποδέκτη [4, 6, 8]. Έστω ότι μία δυάδα πακέτων μεγέθους L αποστέλλεται από την πηγή με αρχική διασπορά Δ_S. Ο ρυθμός αποστολής των πακέτων θα είναι

τότε ίσος με $R_o = \frac{L}{\Delta_S}$. Αν το R_o είναι μεγαλύτερο από το από άκρο-σε-άκρο εύρος ζώνης A τότε η δεύτερη δυάδα πακέτων θα "φρακάρει" πίσω από την πρώτη και άρα ο ρυθμός αποστολής R_m που θα μετρήσει ο αποδέκτης θα είναι μικρότερος από του αποστολέα. Αντίθετα αν $R_o < A$ τότε οι δυάδες πακέτων θα φτάσουν στον αποδέκτη με τον ίδιο ρυθμό με τον οποίο αποστάλθηκαν από την πηγή. Ο υπολογισμός των παραπάνω ρυθμών είναι σημαντικός καθώς εκτός από το *διαθέσιμο εύρος ζώνης* A είναι δυνατό να υπολογιστεί και η *χωρητικότητα* C του από άκρο-σε-άκρο μονοπατιού.

Συγκεκριμένα, έστω ένα μονοπάτι αποτελούμενο από έναν μόνο σύνδεσμο με χωρητικότητα C, διαθέσιμο εύρος ζώνης A και μέσο ρυθμό αποστολής cross traffic $R_c = C - A$. Όπως προαναφέρθηκε το R_o αυξάνεται σταδιακώς. Όταν ξεπεράσει το A, τότε ο ρυθμός αποστολής της δυάδας πακέτων που υπολογίζει ο αποδέκτης είναι ίσος με

$$R_m = \frac{R_o}{R_o + R_c} C \tag{3.6}$$

ή

$$\frac{R_o}{R_m} = \frac{R_o + R_c}{C} \tag{3.7}$$

Η τεχνική TOPP υπολογίζει το διαθέσιμο εύρος ζώνης A ώς τον μέγιστο δυνατό ρυθμό αποστολής δεδομένων ώστε $R_o \approx R_m$. Από την παραπάνω εξίσωση είναι δυνατό να υπολογιστεί και η χωρητικότητα C.

Κεφάλαιο 4

Ανάλυση και Περιγραφή της Επίθεσης

Σε αυτό το κεφάλαιο γίνεται ανάλυση του σχεδιασμού της επίθεσης, που αποτελεί τον πυρήνα της παρούσας διπλωματικής, των κύριων στοιχείων της, καθώς και της λειτουργίας της. Πριν περιγράψουμε αναλυτικά τα χαρακτηριστικά της επίθεσης κάνουμε πρώτα μία αναφορά σε ορισμένα βασικά εργαλεία, που χρησιμοποιήθηκαν. Ύστερα συνεχίζουμε με την παρουσίαση του μοντέλου της επίθεσης, η οποία περιλαμβάνει την τοπολογία και διάφορα τεχνικά χαρακτηριστικά, που την αφορούν και ολοκληρώνουμε με την αναλυτική περιγραφή των διαφόρων σταδίων της.

4.1 C.O.R.E

Το **Common Open Research Emulator** (C.O.R.E) αποτελεί ένα εργαλείο ικανό να εξομοιώσει με ακρίβεια ενσύρματα και ασύρματα δίκτυα [9]. Παρέχει τη δυνατότητα σχεδιασμού τοπολογιών δικτύων πολύ κοντά στα πραγματικά δίκτυα. Το κυριότερο χαρακτηριστικό του είναι

ότι επιτρέπει την δημιουργία εικονικών μηχανών (virtual machines), οι οποίες δεν επιβαρύνουν το πραγματικό/φυσικό σύστημα, που εκτελεί το εργαλείο.

Οι εικονικές μηχανές συμπεριφέρονται όπως ακριβώς μία πραγματική συσκευή, με την έννοια ότι χρησιμοποιούν λειτουργικό σύστημα (ίδιο με το φυσικό σύστημα) και επιτελούν όλες τις βασικές λειτουργίες του. Για τα πειραματά μας κάθε συσκευή χρησιμοποιεί το λειτουργικό σύστημα Linux, όπως θα αναφερθεί και παρακάτω. Η σημαντικότερη δυνατότητα, που προσφέρει το εργαλείο αυτό είναι το γεγονός ότι οι εικονικές μηχανές έχουν τη δυνατότητα της εύκολης χρήσης ορισμένων εργαλείων, όπως το iperf και το wireshark. Ταυτόχρονα ο χρήστης είναι σε θέση να εγκαταστήσει στο σύστημα καινούρια εργαλεία, τα οποία γίνονται αυτόματα ορατά από τις εικονικές μηχανές και να τα χρησιμοποιήσει μέσω δικών του προσωπικών *scripts*, γραμμένα στη γλώσσα *python*. Οι παραπάνω δυνατότητες μας ώθησαν στην επιλογή του C.O.R.E για την εξομοίωση και τη μελέτη της επίθεσής μας.

4.2 RT-WABest

Το *Round-Trip Wireless Available Bandwidth estimation tool* (RT-WABest) αποτελεί ένα εργαλείο εκτίμησης του *διαθέσιμου εύρους ζώνης* και της *χωρητικότητας* του bottleneck συνδέσμου σε ένα από άκρο-σε-άκρο μονοπάτι χωρίς να χρειάζεται ο χρήστης να έχει τον έλεγχο και των δύο άκρων του μονοπατιού [4]. Σε συνδυασμό με τη δυνατότητα του να εκτιμά το διαθέσιμο εύρος ζώνης σε δίκτυα, στα οποία παρεμβάλλονται και ασύρματα δίκτυα, το καθιστά ως μία από τις καλύτερες και αποδοτικότερες επιλογές για την εύρεση συμφορήσεων στο δίκτυό μας. Τα περισσότερα εργαλεία που κυκλοφορούν στο Διαδίκτυο (Pathchar, IGI, Pchar, Cprobe, Pathload, LinkWidth) [5, 6, 7, 8] μπορούν να εκτιμήσουν το διαθέσιμο εύρος ζώνης μόνο σε ενσύρματα δίκτυα, γεγονός που τα καθιστά περιττά στην περιπτωσή μας, που επικεντρώνουμε σε

ασύρματα δίκτυα.

Το RT-WABest λειτουργεί σε δύο σκέλη. Στο πρώτο σκέλος γίνεται εκτίμηση της χωρητικότητας του bottleneck συνδέσμου στο μονοπάτι μας. Στο δεύτερο σκέλος γίνεται υπολογισμός του διαθέσιμου εύρους ζώνης του μονοπατιού. Τα δύο σκέλη παρουσιάζονται αναλυτικότερα παρακάτω.

4.2.1 Εκτίμηση της Χωρητικότητας

Η εκτίμηση της χωρητικότητας (capacity) του bottleneck συνδέσμου στο απο άκρο-σε-άκρο μονοπάτι, στο οποίο εκτελείται το RT-WABest, γίνεται μέσω της αποστολής από την πηγή προς τον αποδέκτη N δυάδων πακέτων με μέγεθος L. Η χωρητικότητα C του bottleneck συνδέσμου υπολογίζεται από τον τύπο:

$$C = median \frac{L}{RTT_2^i - RTT_1^i} \quad (i = 1, 2, ...N) \tag{4.1}$$

όπου το RTT_1^i είναι το Round-Trip Time του πρώτου πακέτου της i-οστής δυάδας πακέτων και το RTT_2^i είναι το Round-Trip Time του δεύτερου πακέτου της δυάδας πακέτων. Η διαφορά τους $RTT_2^i - RTT_1^i$ αποτελεί τη διασπορά με την οποία καταφθάνουν τα πακέτα απάντησης της συγκεκριμένης δυάδας πίσω στην πηγή (βλ. τεχνική TOPP). Στην ουσία όμως χρειαζόμαστε τη διαφορά μεταξύ των χρόνων που απαιτούν τα πακέτα για να φτάσουν μόνο από την πηγή στον αποδέκτη και το ανάποδο. Παρακάτω θα δούμε ότι τα *RTTs* εκφυλίζονται στους χρόνους αυτούς, λόγω της ιδιαιτερότητας των TCP RST πακέτων.

Συγκεκριμένα ο υπολογισμός των RTTs των πακέτων γίνεται μέσω της αποστολής TCP SYN πακέτων μεγέθους ίσο με την MTU (όπως και

στην επίθεσή μας) σε μία πόρτα του αποδέκτη, η οποία ειναι ''κλειστή''. Αυτό εχει ως συνέπεια να αποστέλλονται πακέτα TCP RST ως απάντηση στα TCP SYN πακέτα, με την ιδιαιτερότητα όμως ότι το μικρό μεγεθός τους συμβάλλει στο να μην συναντούν σχεδόν καμία καθυστέρηση στην επιστροφή.

Όπως έχει προαναφερθεί οι περισσότερες τεχνικές και εργαλεία εκτίμησης του διαθέσιμου εύρους ζώνης λειτουργούν μόνο σε ενσύρματα δίκτυα, καθώς σε αυτά δεν υπάρχει περίπτωση η απάντηση ενός πακέτου παλαιότερου σε σειρά να συναγωνιστεί την απάντηση ενός νεότερου. Το RT-WABest καταφέρνει να ξεπεράσει αυτό το εμπόδιο αποστέλλοντας μία συνεχόμενη (back-to-back) δυάδα πακέτων. Ειδικότερα, το πρώτο πακέτο είναι TCP RST πακέτο μεγέθους ίσο με την MTU και το δεύτερο ένα TCP SYN πακέτο, και μεγέθους ίσο με την MTU. Το TCP RST πακέτο όμως δεν προκαλεί την δημιουργία απάντησης στο δίκτυο, οπότε δεν υπάρχει κάποια απάντηση, η οποία να συναγωνιστεί την απάντηση του δεύτερου TCP SYN πακέτου.

4.2.2 Εκτίμηση του Διαθέσιμου Εύρους Ζώνης

Εφόσον έχει υπολογιστεί η χωρητικότητα C του bottleneck συνδέσμου στο από άκρο-σε-άκρο μονοπάτι, είναι δυνατό να υπολογιστεί τώρα το διαθέσιμο εύρος ζώνης A ολόκληρου του μονοπατιού μέσω του τύπου:

$$A = \begin{cases} 2C - \frac{C^2}{R} & \text{R} \geq \frac{C}{2} \\ 0 & \text{R} < \frac{C}{2} \end{cases} \tag{4.2}$$

όπου το R είναι ο μέσος ρυθμός διασποράς στον αποδέκτη.

Για τον υπολογισμό του μέσου ρυθμού διασποράς R το RT-WABest αποστέλλει από την πηγή στον αποδέκτη ένα τραίνο πακέτων αποτε-

λούμενο από K TCP SYN διαδοχικά πακέτα, σε μία ανενεργή πόρτα. Τα πακέτα αυτά δημιουργούν ως απαντήσεις πακέτα TCP RST. Όπως προαναφέρθηκε τα πακέτα αυτά δεν συναντούν μεγάλη καθυστέρηση στο μονοπάτι της επιστροφής λόγω του μικρού μεγέθους τους. Ο μέσος ρυθμός διασποράς υπολογίζεται τότε από τον τύπο:

$$R = \frac{L}{mean(T_i)} \quad (i = 1, 2, ..., K-1) \tag{4.3}$$

όπου το T_i αποτελεί τη διασπορά των πακέτων TCP RST πακέτων (όπως στην εξίσωση 4.1), που αποτελούν απάντηση στη δυάδα των TCP SYN πακέτων με αριθμούς *i+1* και *i*, αντίστοιχα.

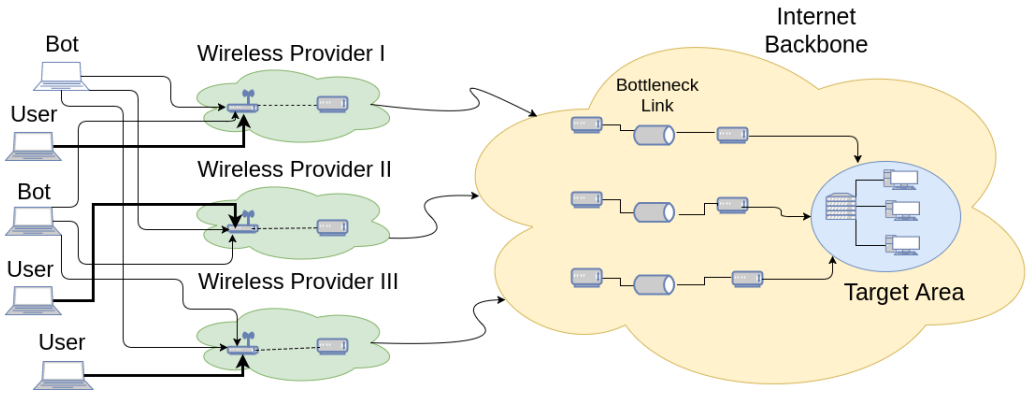
Ύστερα, μέσω της εξίσωσης (4.2) υπολογίζεται εύκολα το διαθέσιμο εύρος ζώνης του από άκρο-σε-άκρο μονοπατιού. Επίσης αξίζει να επισημανθεί ότι το RT-WABest φροντίζει, ώστε να μην έχουμε ανταγωνισμό μεταξύ ενός TCP SYN πακέτου και ενός TCP RST, ενός προηγούμενου TCP RST πακέτου. Συγκεκριμένα, περιμένει κάποιο χρονικό διάστημα (timeout) μέχρι να φτάσει η απάντηση TCP RST ενός προηγούμενου TCP SYN πακέτου στην πηγή πριν στείλει το επόμενο TCP SYN πακέτο. Αν περάσει ο timeout χρόνος τότε το TCP RST πακέτο θεωρείται ως ”χαμένο” και προβαίνει στην αποστολή του επόμενου TCP SYN πακέτου.

4.3 Nping

Το *Nping* αποτελεί ένα εργαλείο για τη δημιουργία δικτυακών πακέτων και εντάσσεται στη σουίτα εργαλείων *Nmap* [27]. Το Nping παρέχει δυνατότητα δημιουργίας πακέτων που ανήκουν σε διαφορετικά πρωτόκολλα (όπως το TCP, το UDP, το ICMP και το ARP), παραχωρώντας ταυτόχρονα τον πλήρη έλεγχο της κατασκευής τους στο χρήστη. Το Nping έχει ποικίλους τρόπους χρήσης, όμως ένας από αυτούς είναι και η πρόκληση επιθέσεων τύπου DDoS. Για αυτούς τους λόγους χρη-

σιμοποιήθηκε και στα πειράματά μας ως η γεννήτρια των πακέτων της επίθεσής μας.

4.4 Μοντέλο Συστήματος



Σχήμα 4.1: Γενική Τοπολογία Δικτύου.

4.4.1 Τοπολογία Δικτύου

Στο πλαίσιο αυτής της διπλωματικής υποθέτουμε μια υβριδική τοπολογία αποτελούμενη από ενσύρματα και ασύρματα δίκτυα (wired-wireless networks), όπως φαίνεται στο σχήμα 4.1. Αναλυτικότερα:

- **Απλοί χρήστες και bots**: Το πρώτο κομμάτι της τοπολογίας μας αποτελείται από συσκευές/τερματικά, τα οποία είτε ανήκουν σε νόμιμους χρήστες είτε είναι bots (υπό τον έλεγχο του επιτιθέμενου). Τα τερματικά που ανήκουν σε νόμιμους χρήστες διαθέτουν μόνο μία διεπαφή συνδεδεμένη σε έναν πάροχο ασύρματου δικτύου. Ο μοναδικός σκοπός τους είναι να δημιουργούν νόμιμη κίνηση (Cross traffic), στην οποία παρεμβάλλεται η κακόβουλη κίνηση κατά την ώρα της επίθεσης. Τα bots από την άλλη πλευρά

αποτελούν περισσότερο πολύπλοκα τερματικά, με την έννοια ότι διαθέτουν τρεις ξεχωριστές διεπαφές συνδεδεμένες η κάθε μία με έναν διαφορετικό πάροχο ασύρματου δικτύου. Κάθε διεπαφή χρησιμεύει ώστε να στέλνει κακόβουλη κίνηση από διαφορετικό πάροχο προς την περιοχή-στόχο.

- **Πάροχοι Ασύρματου Δικτύου (Wireless Internet Providers)**: Όπως φαίνεται και από το σχήμα η τοπολογία μας διαθέτει τρεις παρόχους ασύρματου δικτύου. Σε κάθε έναν από εκείνους αντιστοιχεί και ένα ξεχωριστό δίκτυο αποτελούμενο από δρομολογητές διασυνδεδεμένους ενσύρματα μεταξύ τους. Επιπροσθέτως, διαθέτουν και ένα σημείο ασύρματης πρόσβασης (Wireless Access Point), το οποίο συνδέεται και αυτό ενσύρματα με το υπόλοιπο δίκτυό τους. Η χρησιμότητα του σημείου ασύρματης πρόσβασης είναι να προσφέρει στα τερματικά που ανήκουν στους νόμιμους χρήστες και τα bots ασύρματη σύνδεση με το δίκτυο του παρόχου και κατ' επέκταση με το Διαδίκτυο.

- **Κύριο Δίκτυο/Διαδίκτυο (Internet Backbone)**: Το κύριο δίκτυο ή Διαδίκτυο προσομοιώνει το πραγματικό Διαδίκτυο. Συγκεκριμένα, αποτελείται από πολλούς διαφορετικούς δρομολογητές, οι οποίοι είναι συνδεδεμένοι ενσύρματα μεταξύ τους και παρέχουν πρόσβαση στην περιοχή στόχο σε κάθε πάροχο ασύρματου δικτύου και άρα σε νόμιμα τερματικά και bots. Επίσης μέσω του διαδικτύου είναι δυνατή η συνδεσιμότητα μεταξύ των διαφόρων παρόχων ασύρματου δικτύου, ώστε να υπάρχουν εναλλακτικές διαδρομές προς την περιοχή στόχο σε περίπτωση που "πέσουν" κάποιοι σύνδεσμοι. Τέλος το Διαδίκτυο περιέχει και τα *bottleneck links*, καθώς και τους servers δολώματα, τα οποία είναι υψίστης σημασίας για την επίθεση. Θα γίνει αναφορά σε αυτά αναλυτικότερα παρακάτω.

- **Περιοχή-Στοχος (Target Area)**: Η περιοχή στόχος αποτελείται από έναν δρομολογητή/server και τερματικά που ανήκουν σε απλούς

χρήστες. Ο δρομολογητής/server παρεμβάλλεται μεταξύ του κύριου δικτύου/Διαδικτύου και των απλών τερματικών παρέχοντάς τους πρόσβαση στο πρώτο. Η κύρια χρησιμότητα των τερματικών της περιοχής-στόχου είναι να δέχονται κίνηση από τα τερματικά που ανήκουν στους νόμιμους χρήστες εκτός της περιοχής αυτής.

4.4.2 Τεχνικά Χαρακτηριστικά

Παρακάτω θα αναφερθούν ορισμένα τεχνικά χαρακτηριστικά που σχετίζονται με τις συσκευές που απαρτίζουν το δίκτυό μας και είναι βασικά για την κατανόηση της λειτουργίας τους.

Bots

Όπως προαναφέρθηκε κάθε bot θεωρείται ότι διαθέτει τρεις ασύρματες διεπαφές, κάθε μία συνδεδεμένη σε έναν διαφορετικό πάροχο. Στο πλαίσιο αυτής της διπλωματικής κάθε διεπαφή έχει αντικατασταθεί με ένα διαφορετικό τερματικό, που διαθέτει μια μόνο διεπαφή συνδεδεμένη σε έναν από τους παρόχους ασύρματου δικτύου. Η αλλαγή αυτή πραγματοποιήθηκε έτσι ώστε να μελετηθεί η συμπεριφορά συσκευών/τερματικών, που έχουν την δυνατότητα να αποστέλλουν ταυτόχρονα κίνηση μέσω διαφορετικών διεπαφών. Οι πολλαπλές διεπαφές υλοποιήθηκαν με τον συγκεκριμένο τρόπο καθώς δεν υπήρχε δυνατότητα πραγματικής υλοποίησής τους.

Συγκεκριμένα, κάθε τερματικό χρησιμοποιεί το λειτουργικό σύστημα Linux (Ubuntu 16.04 - Kernel 3.13). Ο πυρήνας του Linux δεν επιτρέπει την ταυτόχρονη αποστολή δεδομένων από περισσότερες της μίας διεπαφές, παρά μόνο σειριακά και με λειτουργία κάθε φορά μόνο μίας διεπαφής. Το γεγονός αυτό μας οδήγησε να αντικαταστήσουμε ένα τερματικό που διαθέτει τρεις διεπαφές με τρία τερματικά που διαθέτουν

μία διεπαφή, θεωρώντας ότι αποτελούν τμήμα της ίδιας συσκευής. Όπως θα αναφερθεί και στο επόμενο κεφάλαιο η συγκεκριμένη αλλαγή έχει ορισμένες αρνητικές επιπτώσεις για την αποδοτικότητα της επίθεσης, οι οποίες όμως μπορούν να θεωρηθούν αμελητέες.

Επιπροσθέτως, κάθε συσκευή λειτουργεί σε περιβάλλον superuser/root, ώστε να είναι δυνατές οι λειτουργίες κατασκευής πακέτων και της αποστολής τους ύστερα στο δίκτυο, μέσω του εργαλείου *nping*, που αναφέρθηκε νωρίτερα. Παράλληλα, σε κάθε συσκευή είναι εγκατεστημένη η γλώσσα προγραμματισμού Python (2.7 και 3.4), στην οποία είναι υλοποιημένες ορισμένες λειτουργίες της επίθεσης που θα αναλυθούν παρακάτω.

Απλές συσκευές/τερματικά

Όπως και τα bots έτσι και οι απλές συσκευές/τερματικά χρησιμοποιούν το λειτουργικό σύστημα Linux (Ubuntu 16.04 - Kernel 3.13). Οι συσκευές που ανήκουν σε απλούς χρήστες, οι οποίοι βρίσκονται εκτός της περιοχής-στόχου χρησιμοποιούν το εργαλείο iPerf, μέσω του οποίου έχουν την δυνατότητα να αποστέλλουν κίνηση TCP ή UDP με μεταβαλλόμενους ρυθμούς αποστολής προς έναν αποδέκτη. Το εργαλείο αυτό εμπεριέχεται στον emulator C.O.R.E, που χρησιμοποιούμε, αλλά αποτελεί και αυτόνομο εργαλείο. Η κίνηση που δημιουργούν μέσω του iPerf αποτελεί το Cross traffic που θα μας απασχολήσει παρακάτω. Οι συσκευές που ανήκουν στην περιοχή-στόχο κάνουν επίσης χρήση του εργαλείου *netcat*, το οποίο επιτρέπει σε μία συσκευή να ''ανοίξει'' μία άλλοτε κλειστή δικτυακή πόρτα και να ''ακούσει'' ή να στείλει δεδομένα από εκείνη. Στην περιπτωσή μας χρησιμοποιείται για να ''ανοίξει'' η πόρτα 6000, στην οποία κατευθύνεται η κίνηση TCP που στέλνουν οι απλές συσκευές εκτός της περιοχής στόχου μέσω του iPerf. Η ''ανοιχτή'' πόρτα είναι προαπαιτούμενο ώστε να εγκαθιδρυθεί μία σύνδεση TCP μεταξύ δύο συσκευών, που θέλουν να επικοινωνήσουν. Αντίθετα, το πρωτόκολλο

UDP δεν απαιτεί την εγκαθίδρυση μίας σύνδεσης μεταξύ των συσκευών, ώστε να γίνει η αποστολή δεδομένων μεταξύ τους. Συνεπώς σε αυτή την περίπτωση δεν είναι αναγκαίο το ''άνοιγμα'' μιας δικτυακής πόρτας.

4.4.3 Δρομολογητές (Routers)

Οι δρομολογητές αποτελούν τις πολυπλοκότερες συσκευές στην τοπολογία μας. Όπως και οι απλές συσκευές και τα bots έτσι και οι δρομολογητές χρησιμοποιούν το λειτουργικό σύστημα Linux με την μόνη διαφορά ότι έχουν επιπλέον εγκατεστημένο το εργαλείο *quagga* [28], το οποίο καθιστά δυνατή τη μετατροπή μιας απλής συσκευής σε δρομολογητή

Το *quagga* αποτελεί σουίτα διαδικτύακής δρομολόγησης (Network Routing Software Suite), η οποία παρέχει τη δυνατότητα χρήσης διαφόρων πρωτοκόλλων δρομολόγησης, όπως τα Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP) και το IS-IS [24]. Για τα δικά μας πειράματα χρησιμοποιήθηκαν τα πρωτόκολλα δρομολόγησης OSPF και BGP, τα οποία είναι και τα πιο δημοφιλή.

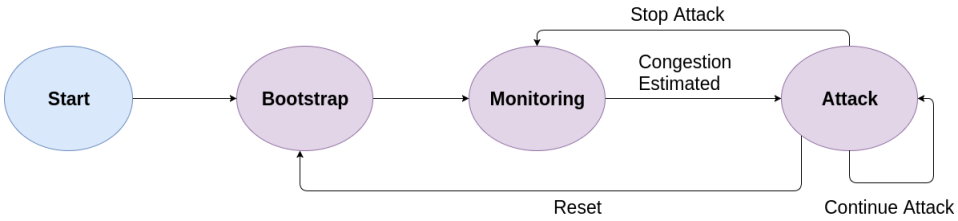
Το OSPF αποτελεί το κύριο πρωτόκολλο δρομολόγησης στα δίκτυα εντός των παρόχων ασύρματου δικτύου που έχουμε υλοποιήσει. Το OSPF αποτελεί το ιδανικό πρωτόκολλο για τη δρομολόγηση εντός μικρών σε μέγεθος δικτύων, καθώς βασίζεται στον αλγόριθμο του Dikjstra, ο οποίος έχει μεγάλο βαθμό σύγκλισης. Συνεπώς χρησιμοποιήθηκε για τα δίκτυα τα οποία αποτελούνται από λιγότερες συσκευές δρομολόγησης, όπως θα γινόταν και σε πραγματικά σενάρια.

Αντίθετα, για τη δρομολόγηση μεταξύ των δρομολογητών του κύριου κορμού του δικτύου ή αλλιώς του Διαδικτύου, χρησιμοποιείται το πρωτόκολλο δρομολόγησης BGP. Το BGP βασίζεται στον αλγόριθμο δρομολόγησης του Bellman-Ford, γεγονός που το καθιστά πιο αργό από το

πρωτόκολλο OSPF. Παρ' όλα αυτά αποτελεί ιδανικό αλγόριθμο δρομολόγησης για δίκτυα, τα οποία έχουν πολύ μεγάλο μέγεθος. Συγκεκριμένα, το BGP λειτουργεί μέσω της χρήσης των ASs (Autonomous Systems), τα οποία μπορεί να είναι και πολλά υποδίκτυα, τα οποία έχουν συνδεσιμότητα μεταξύ τους. Το κάθε AS θεωρείται ως μία απλή συσκευή για το BGP και κάθε πληροφορία που ανταλλάσσεται μεταξύ των ASs αφορά μόνο τα υπόλοιπα ASs και όχι τα περιεχόμενά τους. Επίσης σε αντίθεση με το OSPF το BGP μπορεί να πραγματοποιεί τοπικές ενημερώσεις όταν συμβεί κάποια αλλαγή στην τοπολογία, ενώ το OSPF θα πρέπει να "ξανατρέξει" από την αρχή, γεγονός που το καθιστά μη αποδοτικό για πολύ μεγάλες τοπολογίες (π.χ., Διαδίκτυο). Όπως θα δούμε όμως και στο επόμενο κεφάλαιο, το BGP καθυστερεί να συγκλίνει αρκετά σε σχέση με το OSPF.

4.5 Στάδια της Επίθεσης

Η επίθεσή μας χωρίζεται σε τρία στάδια, όπως και η επίθεση CICADAS [2], το *Στάδιο Εκκίνησης* (Bootstrap Phase), το *Στάδιο Παρακολούθησης* (Monitoring Phase) και το *Στάδιο Επίθεσης* (Attack Phase). Οι μεταβάσεις μεταξύ των σταδίων φαίνονται καλύτερα στο σχήμα 4.2.



Σχήμα 4.2: Στάδια της Επίθεσης

Στα παρακάτω υποκεφάλαια γίνεται ανάλυση καθενός από τα στάδια της επίθεσής μας.

4.6 Σταδιο Εκκίνησης

Μόλις ξεκινήσουν την λειτουργία τους για πρώτη φορά, τα bots εισέρχονται στο *Bootstrap Phase*. Σε αυτό το στάδιο τα bots αρχικοποιούν ορισμένες βασικές πληροφορίες, όπως την διεύθυνση IP τους και την διεύθυνση IP του στόχου τους. Στην περίπτωσή μας η περιοχή-στοχος περιέχει μόνο έναν server, οπότε και ορίζεται ως στόχος η συγκεκριμένη διεύθυνση IP. Στην περίπτωση που είχαμε παραπάνω από έναν servers στην περιοχή στόχο τότε θα πραγματοποιούταν ανάθεση για κάθε μία από τις διευθύνσεις IP των servers αυτών. Η διεύθυνση IP του κάθε bot είναι σημαντική για την πρώτη φορά που εισέρχονται σε αυτό το στάδιο καθώς με βάση αυτή ορίζεται ο συντονιστής (coordinator). Αρχικά ως συντονιστής ορίζεται το bot με τον αριθμό 1, (συγκεκριμένα κάθε μία από τις τρεις συσκευές που συνδέονται στους παρόχους ασύρματου δικτύου και ανήκουν στο bot με αριθμό 1). Στη συνέχεια κάθε bot δημιουργεί ένα δικό του socket, το οποίο θα χρησιμοποιηθεί για την αποστολή και τη λήψη πληροφοριών αργότερα. Από εκεί και πέρα η διαδικασία που ακολουθείται είναι διαφορετική για τα απλά bots και τον κάθε συντονιστή αντίστοιχα.

Ο κάθε συντονιστής συνεχίζει πραγματοποιώντας traceroutes προς την περιοχή στόχο για να ανακαλύψει τη διαδρομή που θα χρησιμοποιήσουν οι συσκευές στο ίδιο δίκτυο με εκείνον, όταν θα υλοποιήσουν την επίθεση. Όταν διαπιστωθεί η διαδρομή μέσω του traceroute, αποστέλλεται σε κάθε ένα από τα bots του ίδιου δικτύου, που θα πραγματοποιήσουν την επίθεση, μέσω των προαναφερθέντων sockets. Ύστερα ο συντονιστής μεταβαίνει στο επόμενο στάδιο, το *Monitoring Phase*.

Τα απλά bots, αντίστοιχα, μπαίνουν σε μία παθητική κατάσταση στην οποία περιμένουν να ''ακούσουν'' την πληροφορία της διαδρομής από τους συντονιστές τους. Συνεπώς καθόλη τη διαδικασία της εύρεσης της διαδρομής προς την περιοχή-στόχο από τους συντονιστές τα απλά bots παραμένουν αδρανή. Όταν λάβουν την παραπάνω πληροφο-

ρία μέσω του socket που έχουν δημιουργήσει προηγουμένως, την αρχικοποιούν και μεταβαίνουν με την σειρά τους στο επόμενο στάδιο το *Monitoring Phase*, το οποίο είναι τυπικό στάδιο για εκείνα.

4.7 Στάδιο Παρακολούθησης

Το στάδιο παρακολούθησης (Monitoring Phase) αποτελεί το σημαντικότερο εκ των τριών σταδίων, καθώς σε αυτό βασίζεται σε μεγάλο βαθμό η επιτυχία ολόκληρης της επίθεσης. Μόλις ολοκληρωθούν τα βήματα του προηγηγούμενου σταδίου, όλες οι κακόβουλες συσκευές μεταβαίνουν στο στάδιο αυτό. Όπως και προηγουμένως το στάδιο αυτό είναι διαφορετικό για τα απλά bots και για κάθε συντονιστή αντίστοιχα.

Κάθε συντονιστής εφόσον έχει υπολογίσει τη διαδρομή προς την περιοχή στόχο, ξεκινά τη διαδικασία εύρεσης του bottleneck συνδέσμου, καθώς και του διαθέσιμου εύρους ζώνης του. Οι δύο αυτές πληροφορίες είναι καίριες για την έναρξη και την διατήρηση της επίθεσης, όπως θα διαπιστωθεί παρακάτω. Συγκεκριμένα, κάθε συντονιστής εκτελεί μια ειδική συνάρτηση, η οποία δέχεται ως είσοδο τη διαδρομή που βρέθηκε μέσω των traceroutes και ξεκινά το εργαλείο *RT-WABest* μέσω του οποίου θα βρεθούν ο bottleneck σύνδεσμος και το διαθέσιμο εύρος ζώνης του. Για λόγους διευκόλυνσης και ταχύτητας των πειραμάτων θεωρούμε γνωστή τη συνολική χωρητικότητα του bottleneck συνδέσμου (είναι όμως δυνατό να βρεθεί εύκολα μέσω του RT-WABest). Κάθε φορά που τρέχει το εργαλείο και επιστρέφει μια τιμή σε Mbps για το διαθέσιμο εύρος ζώνης, αυτή διαιρείται με την τιμή της χωρητικότητας την οποία θεωρούμε σταθερή και λαμβάνουμε ένα ποσοστό. Το ποσοστό αυτό, το οποίο το ονομάζουμε αλλιώς και *κατώφλι* (threshold), αντικατοπτρίζει το πόσο μεγάλο είναι το διαθέσιμο ευρος ζώνης σε σχέση με τη σταθερή χωρητικότητα, τη χρονική στιγμή που εκτελέσθηκε το εργαλείο. Όταν το ποσοστό αυτό πέσει κάτω από μία τιμή, που εξαρτάται από τη χωρητικότητα του bottleneck συνδέσμου, τότε θεωρούμε

ότι υπάρχει συμφόρηση (Congestion) στο bottleneck σύνδεσμο, οπότε πρέπει να ξεκινήσει η επίθεση. Η συμφόρηση στο bottleneck σύνδεσμο οφείλεται στη νόμιμη κίνηση (Cross traffic) που διατρέχει τον σύνδεσμο τη συγκεκριμένη χρονική περίοδο.

Η συγκεκριμένη συνάρτηση δεν αρκείται όμως στο να εκτελεί απλώς το εργαλείο RT-WABest. Εφόσον, όπως έχει προαναφερθεί, το εργαλείο χρειάζεται μία διεύθυνση IP, έτσι ώστε να βρει το διαθέσιμο εύρος ζώνης του bottleneck συνδέσμου της διαδρομής προς εκείνη, χρησιμοποιούνται διευθύνσεις IP από το μονοπάτι που έχει βρεθεί στο προηγούμενο στάδιο. Το εργαλείο ξεκινά με μία διεύθυνση IP σχετικά κοντά στην περιοχή στόχο. Αν το κατώφλι υπολογιστεί μεγαλύτερο από το ζητούμενο τότε συμπεραίνουμε ότι δεν υπάρχει συμφόρηση στο bottleneck σύνδεσμο και άρα η συνάρτηση επιστρέφει με το συντονιστή να ενημερώνει τα bots ότι η επίθεση δεν θα ξεκινήσει και η συνάρτηση επανεκκινεί. Αν το κατώφλι έχει πέσει κάτω από την τιμή που θέλουμε, τότε η εκτέλεση μεταβαίνει σε μία δυαδική αναζήτηση για την εύρεση ενός συνδέσμου ο οποίος είναι κοντά στο bottleneck σύνδεσμο, αν όχι ο ίδιος. Μέσω της δυαδικής αναζήτησης εξετάζεται αρχικά το *διαθέσιμο εύρος ζώνης* του συνδέσμου, ο οποίος είναι ο μεσαίος κατά σειρά στο μονοπάτι προς την περιοχή-στόχο. Αν το νέο ποσοστό που θα υπολογιστεί από τη νέα εκτέλεση του εργαλείου βρεθεί μεγαλύτερο από την τιμή του κατωφλίου, τότε συμπεραίνουμε ότι εξετάζουμε έναν σύνδεσμο όπισθεν του bottleneck συνδέσμου και άρα η δυαδική αναζήτηση τρέχει εκ νέου για τους εναπομείναντες συνδέσμους έμπροσθεν του εξετάζοντος. Στην περίπτωση όμως που το ποσοστό συμφωνεί με το όριο που επιβάλλει το κατώφλι, τότε έχουμε βρει έναν σύνδεσμο ο οποίος είναι κοντά στο bottleneck σύνδεσμο ή ακόμη και τον ίδιο, οπότε και η συνάρτηση επιστρέφει τη συγκεκριμένη διεύθυνση IP του server/δρομολογητή (άκρο του συνδέσμου) καθώς και το διαθέσιμο εύρος ζώνης που υπολογίστηκε. Η δυαδική αναζήτηση είναι απαραίτητη έτσι ώστε να βρεθεί ένας σύνδεσμος (ειδικότερα μία διεύθυνση IP), ο οποίος είναι αρκετά κοντά στο bottleneck σύνδεσμο και αρκετά μακριά από την περιοχή-στόχο, ώστε

να μειωθεί η ανιχνευσιμότητα της επίθεσης. Ο server/δρομολογητής με την παραπάνω IP ονομάζεται server δόλωμα (decoy server), καθώς η κακόβουλη κίνηση περνά από τον bottleneck σύνδεσμο κατευθυνόμενη προς εκείνον (προκαλώντας έμμεσα ζημιά), αλλά ταυτόχρονα βρίσκεται μακρία απο την περιοχή-στόχο συμβάλλοντας στην μη αναγνωρισιμότητά της

Αξίζει επίσης να αναφερθεί ότι η συγκεκριμένη συνάρτηση έχει ανατεθεί σε ένα νήμα, το οποίο τρέχει παράλληλα με το κύριο πρόγραμμα του συντονιστή για τη μεγιστοποιήση της αποδοτικότητας και την παραλληλοποίηση των διεργασιών του συντονιστή. Όταν το νήμα επιστρέψει τις δύο πληροφορίες που βρέθηκαν (την διεύθυνση IP και το available bandwidth) πίσω στον συντονιστή, τότε εκείνος τις εντάσσει ταυτόχρονα με ορισμένες παραμέτρους απαραίτητες για την λειτουργία της επίθεσης σε μία ειδική δομή δεδομένων. Τις παραμέτρους αυτές αποτελούν 1) η περίοδος της επίθεσης, 2) το μήκος ξεσπάσματος (burst length), 3) το πλάτος του ξεσπάσματος (burst magnitude), 4) μία λίστα από διευθύνσεις IP bots (θα αναλυθεί αργότερα) και 5) το σήμα ότι πρέπει να ξεκινήσει η επίθεση. Όπως έχει προαναφερθεί η επίθεσή μας είναι παλμοδική, οπότε στο διάστημα μίας περιόδου αποστέλλεται ένας παλμός με χρονικό μήκος το μήκος ξεσπάσματος και ύψος το πλάτος ξεσπάσματος. Οι τιμές των παραμέτρων αυτών είναι σταθερές στα πειραματά μας. Αναλυτικότερα η περίοδος ορίζεται ίση με $= 1sec$, το μήκος ξεσπάσματος ίσο με $b\_len = 0.2sec$ και το πλάτος ξεσπάσματος εξαρτάται από το σενάριο το οποίο εξετάζουμε. Ο λόγος για τον οποίο οι τιμές αυτές επιλέχθηκαν ως έχουν σχετίζεται με τον ελάχιστο χρόνο αναμετάδοσης του TCP και θα εξηγηθεί στο επόμενο κεφάλαιο, στο οποίο παρουσιάζονται τα αποτελέσματα της επίθεσης για κάθε σενάριο. Στη συνέχεια η δομή αυτή αποστέλλεται κωδικοποιημένη από κάθε συντονιστή στα bots που ανήκουν στο ίδιο δίκτυο με εκείνον μέσω του socket που έχει δημιουργηθεί στην αρχή για κάθε συσκευή. Ύστερα κάθε συντονιστής μεταβαίνει στο τρίτο στάδιο, το στάδιο επίθεσης (Attack Phase), το οποίο είναι τυπικό για εκείνον.

Από την άλλη πλευρά τα bots παραμένουν αδρανή περιμένοντας μόνο την πληροφορία για την εκκίνηση της επίθεσης από τον συντονιστή τους ή για την εκλογή νέου συντονιστή (θα αναφερθεί αργότερα). Όταν λάβουν την ειδική δομή δεδομένων μέσω του socket τους, την αποκωδικοποιούν και αποθηκεύουν τα στοιχεία της επίθεσης. Ύστερα με την σειρά τους τα bots μεταβαίνουν και εκείνα στο στάδιο της επίθεσης.

4.8 Στάδιο Επίθεσης

Το στάδιο της επίθεσης (Attack Phase), αποτελεί το τελευταίο στάδιο της επίθεσής μας. Όπως προαναφέρθηκε το στάδιο αυτό διαφέρει μεταξύ των bots και των συντονιστών. Αναλυτικότερα οι διεργασίες που επιτελούνται εδώ αναφέρονται παρακάτω:

Όταν μεταβαίνουν σε αυτό το στάδιο οι συντονιστές, στην ουσία δεν επιτελούν καμία επιπλέον διεργασία εκτός από το να παρακολουθούν το δίκτυο για τυχόν διακοπή της συμφόρησης στο bottleneck σύνδεσμο. Συγκεκριμένα, εισέρχονται σε έναν ατέρμονα βρόχο, στον οποίο αδρανοποιούνται για ορισμένα δευτερόλεπτα (επιλέγεται τυχαία η τιμή τους από το διάστημα 3 έως 7 sec, ώστε να προλάβει να υποχωρήσει η συμφόρηση). Στη συνέχεια μόλις ''ξυπνήσουν'' αναθέτουν στο νήμα να ''τρέξει'' πάλι το εργαλείο RT-WABest και περιμένουν μέσω ενός διαύλου να λάβουν τα αποτελέσματα. Η συνάρτηση που έχει αναφερθεί στο προηγούμενο στάδιο έχει κατασκευαστεί με τέτοιο τρόπο έτσι ώστε να λειτουργεί και στην περίπτωση που διακοπεί η συμφόρηση στο bottleneck σύνδεσμο. Ειδικότερα, αν η συμφόρηση συνεχίζει να υφίσταται, τότε το ποσοστό που θα λάβουμε θα παραμένει μικρότερο από την τιμή του κατωφλίου που έχουμε ορίσει και η τιμή αυτή θα επιστραφεί στον συντονιστή. Σε αυτή την περίπτωση ο βρόχος τρέχει από την αρχή. Αν η συμφόρηση πάψει να υπάρχει η μειωθεί σε βαθμό που το ποσοστό είναι μεγαλύτερο από το κατώφλι, τότε υφίστανται δύο περιπτώσεις, είτε να έχει εκτιμηθεί λάθος τιμή (αδυναμία του εργαλείου όταν ένας

σύνδεσμος έχει "πνιγεί") και η συμφόρηση να συνεχίζει να υπάρχει στο σύνδεσμο, είτε όντως να έχει πάψει να υπάρχει η συμφόρηση. Για να αποφευχθεί αυτό το λάθος χρησιμοποιούμε την την παρακάτω συνθήκη:

$$(av\_bw - cong\_av\_bw)/cong\_av\_bw > 1 \; and \; av\_bw < 1.2 * cap \qquad (4.4)$$

όπου το *av_bw* αποτελεί την τιμή του διαθέσιμου εύρους ζώνης (available bandwidth) που υπολογίστηκε σε αυτή την εκτέλεση του εργαλείου, το *cong_av_bw* την τιμή του διαθέσιμου εύρους ζώνης, όταν είχε εκτιμηθεί ότι υπάρχει συμφόρηση και ξεκίνησε η επίθεση και το *cap* την χωρητικότητα (capacity) του bottleneck συνδέσμου.

Στην ουσία η συνθήκη αυτή μας εξασφαλίζει ότι η καινούρια τιμή του διαθέσιμου εύρους ζώνης που υπολογίσαμε πρέπει είναι μεγαλύτερη από εκείνη που υπολογίσαμε όταν πρωτοανακαλύφθηκε η συμφόρηση, καθώς και κοντά στη χωρητικότητα του bottleneck συνδέσμου, όταν η συμφόρηση σταμάτησε. Η δεύτερη ανισότητα στη συνθήκη μας λαμβάνει υπόψη τις περιπτώσεις που μπορεί να εισαχθεί κάποια μικρή υπερεκτίμιση από το RT-WABest, η οποία θεωρείται ως ελάχιστο σφάλμα.

Όταν η παραπάνω συνθήκη ικανοποιείται, οι συντονιστές εξέρχονται από τον ατέρμονα βρόχο. Στη συνέχεια αποστέλλουν σήμα σε κάθε bot στην ομάδα τους να διακόψει την επίθεση και μεταβαίνουν στην διαδικασία τυχαίας εκλογής ενός νέου συντονιστή, από τις συσκευές της ομάδας τους. Το βήμα αυτό έχει συμπεριληφθεί έτσι ώστε να συμβάλλει στην μη ανιχνευσιμότητα της επίθεσης και της ομαλής συνέχειας της, εφόσον δεν είναι εύκολο να βρεθεί εύκολα ο συντονιστής από τους μηχανισμούς άμυνας του διαδικτύου (ειδικά αν ο αριθμός των bot είναι μεγάλος). Στην συνέχεια ο κάθε πρώην συντονιστής επιστρέφει στο στάδιο παρακολούθησης, στο οποίο εισέρχεται τώρα ως απλό bot.

Από την άλλη πλευρά όταν τα bots έχουν λάβει επιτυχώς τα δεδομένα της επίθεσης από τους συντονιστές τους, ''τρέχουν'' μία ειδική συνάρτηση υπεύθυνη για την εξαπόλυση της κακόβουλης κίνησης στο Διαδίκτυο. Η συνάρτηση αυτή λαμβάνει ως ορίσματα τα παραπάνω δεδομένα. Συγκεκριμένα, η συνάρτηση αυτή κάνει χρήση της γεννήτριας κακόβουλης κίνησης ως εξής:

- Υπολογίζει τα συνολικά bits που πρέπει να σταλλούν ως ένα πλάτος ξεσπάσματος, μέσω της εξίσωσης $magn = burst\_magn * 1024000$.
- Υπολογίζει τα πακέτα που πρέπει να αποσταλούν, ώστε να εξισωθούν με ένα πλάτος ξεσπάσματος μέσω της εξίσωσης $packets = magn/(MTU * 8) + 1$, όπου το MTU είναι ίσο με 1500 Bytes.
- Υπολογίζει το ρυθμό σε πακέτα/δευτερόλεπτο με τον οποίο πρέπει να αποσταλούν τα πακέτα της επίθεσης. Όμως ο ρυθμός υπολογίζεται έτσι ώστε όλα τα πακέτα που πρέπει να αποσταλλούν σε μία περίοδο του παλμού να χωράνε σε ένα μήκος ξεσπάσματος, μέσω της εξίσωσης $pps = packets/burst\_len + 1$.
- Επιλέγεται μία τυχαία πόρτα-στόχος (destination port) στην οποία θα αποσταλλούν τα κακόβουλα πακέτα προς τον στόχο.
- Αν το συγκεκριμένο bot έχει διεύθυνση IP, η οποία ταιριάζει με μία από τις διευθύνσεις IP που περιέχονται στην λίστα που έχει λάβει από τον συντονιστή του τότε θα αποστείλει την κακόβουλη κίνηση προς ένα άλλο bot που ανήκει σε άλλη ομάδα. Ειδικότερα, αν το bot ανήκει στην πρώτη ομάδα τότε θα στείλει την κίνηση του προς ένα bot της δεύτερης ομάδας. Αντίστοιχα, αν ανήκει στην δεύτερη ομάδα θα στείλει την κίνηση προς ένα bot της τρίτης ομάδας. Αν ανήκει στην τρίτη ομάδα θα στείλει την κίνηση προς ένα bot της πρώτης ομάδας. Ως ομάδες θεωρούμε τα δίκτυα των παρόχων ασύρματου δικτύου. Στην περίπτωση που η διεύθυνση IP του bot δεν βρίσκεται μέσα στη λίστα, τότε η κακόβουλη κίνηση θα κατευθυνθεί προς τον server δόλωμα (decoy server), του οποίου

την διεύθυνση IP έχει λάβει επίσης από τον συντονιστή του. Η κακόβουλη κίνηση έχει μοιραστεί έτσι ώστε η μισή να κατευθύνεται προς τον server δόλωμα και η μισή προς τα bots, περνώντας πάντα από τους bottleneck συνδέσμους. Το αποτέλεσμα είναι να αποκρύπτεται η κακόβουλη φύση της και να θεωρείται ως νόμιμη κίνηση προς άλλες συσκευές και servers.

- Τέλος καλείται το εργαλείο *nping* (γεννήτρια της κακόβουλης κίνησης) το οποίο στέλνει πακέτα μεγέθους ίσο με τη MTU (1500 Bytes), με τις αντίστοιχες προαναφερθείσες παραμέτρους προς τους κατάλληλους στόχους. Τα πακέτα που αποστέλλονται ως κομμάτι της επίθεσης είναι TCP SYN πακέτα, για λόγους που θα αναφερθούν παρακάτω.

Η αποστολή της κακόβουλης κίνησης συνεχίζεται περιοδικά και ατέρμονα μέχρι το bot να δεχθεί μήνυμα από τον συντονιστή του να σταματήσει την επίθεση, οπότε και επιστρέφει στο στάδιο παρακολούθησης. Τα πακέτα που αποστέλλονται ως μέρος της επίθεσης έχουν ενεργοποιημένη την σημαία SYN. Το πρωτόκολλο που χρησιμοποείται είναι προφανώς το TCP καθώς η συγκεκριμένη σημαία αποτελεί κομμάτι της τριμερούς χειραψίας του TCP, η οποία δεν υφίσταται στο πρωτόκολλο UDP. Σκοπός μας είναι με την αποστολή αυτών των πακέτων να εκμεταλλευτούμε την ομογένεια του ελάχιστου χρόνου αναμετάδοσης (minimum Retransmission Time - minRTO) του TCP. Το μηχανισμό εκμεταλλεύονται και οι επιθέσεις Shrew και η CICADAS. Όπως έχει προαναφερθεί σύμφωνα με το μηχανισμό αυτό TCP ροές, οι οποίες υφίστανται ταυτόχρονη απώλεια πακέτων θα προσπαθήσουν να αναμεταδόσουν στον ίδιο χρόνο. Άρα οι προσεκτικά κατασκευασμένοι TCP παλμοί που κατασκευάσαμε με περίοδο ίση με το minRTO (1 sec περίπου) και μήκος ξεσπάσματος ίσο με το μέγιστο Round-Trip χρόνο (0.2 sec περίπου) και πλάτος ξεσπάσματος τέτοιο ώστε η συνολική κίνηση να ξεπερνά το συνολικό capcacity του bottleneck συνδέσμου, θα αναγκάσουν τις νόμιμες ροές να υποχωρίσουν προσπαθώντας να ανα-

μεταδώσουν, ενώ η κακόβουλη κίνηση θα καταλαμβάνει το μεγαλύτερο μέρος του bandwidth του bottleneck συνδέσμου. Το φαινόμενο αυτό θα γίνει εμφανέστερο στο επόμενο κεφάλαιο στο οποίο θα αναλυθούν τα αποτελέσματα της επίθεσης. Επίσης τα TCP SYN πακέτα που χρησιμοποιούμε λειτουργούν ως μάσκα για τα επίσης πακέτα TCP SYN που στέλνει το εργαλείο RT-WABest για τις μετρήσεις του. Σαφώς θα μπορούσαν να χρησιμοποιηθούν και πακέτα TCP με διαφορετικά δεδομένα. Αφού σταματήσει η επίθεση τα bots εισέρχονται και πάλι στο στάδιο παρακολούθησης.

Πέραν των δεδομένων της επίθεσης τα απλά bots μπορούν να δεχθούν μήνυμα από τους συντονιστές τους (εφόσον εισέλθουν στο στάδιο παρακολούθησης) ότι ανακηρύσσονται ως οι νέοι συντονιστές, πάλι μέσω του socket τους. Μετά το συγκεκριμένο μήνυμα εισέρχονται εκ νέου στο στάδιο παρακολούθησης αυτή τη φορά όμως ως συντονιστές.

Κεφάλαιο 5

Παράμετροι Αξιολόγησης της Επίθεσης και Αποτελέσματα

Σε αυτό το κεφάλαιο γίνεται παρουσίαση των σεναρίων που εξετάσθηκαν στο πλαίσιο αυτής της διπλωματικής και των αποτελεσμάτων που προέκυψαν. Συγκεκριμένα, πρώτα γίνεται αναφορά στις μετρικές που χρησιμοποιήθηκαν για την αξιολόγηση της επίθεσης και ύστερα παρουσίαζονται τα αποτελέσματα για κάθε σενάριο που εκτελέσαμε ξεχωριστά.

5.1 Παράμετροι Αξιολόγησης

Για την αξιολόγηση της επίθεσής μας χρησιμοποιήθηκαν δύο μετρικές: 1) Το μέγεθος της κακόβουλης κίνησης που καταφέρνει να διέρχεται από τον bottleneck σύνδεσμο κατά τη διάρκεια διεξαγωγής της επίθεσης και 2) το ποσοστό της χωρητικότητας του bottleneck συνδέσμου που αναλογεί στην κακόβουλη κίνηση, πάλι κατά τη διάρκεια της επίθεσης.

Μέγεθος της κίνησης: Το μέγεθος της κακόβουλης κίνησης μετράται

σε bits ανά δευτερόλεπτο. Μέσω αυτής της μετρικής αποφαινόμαστε αν η κακόβουλη κίνηση καταφέρνει να περάσει ολόκληρη μέσα από τον bottleneck σύνδεσμο ή μόνο ένα μέρος της γιατί ανταγωνίζεται την νόμιμη κίνηση.

Ποσοστό της χωρητικότητας του bottleneck συνδέσμου: Μέσω της συγκεκριμένης μετρικής γίνεται εμφανέστερη η επικράτηση της κακόβουλης κίνησης έναντι της νόμιμης κίνησης (Cross traffic), όταν και οι δύο διέρχονται από τον bottleneck σύνδεσμο.

5.2 Σενάρια

Στο πλαίσιο αυτής της διπλωματικής εξετάστηκαν δύο σενάρια: 1) Για χωρητικότητα του bottleneck συνδέσμου 10Mbps και 2) Για χωρητικότητα του bottleneck συνδέσμου 40Mbps.

Ο λόγος που επιλέχθηκαν αυτές οι δύο τιμές και όχι μεγαλύτερες οφείλεται σε περιορισμούς που επιβάλλει το εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης που χρησιμοποιούμε (RT-WABest). Συγκεκριμένα, οι μετρήσεις για μεγαλύτερες χωρητικότητες bottleneck συνδέσμων επέφεραν ασταθή αποτελέσματα. Επίσης, επιχειρήσαμε οι τιμές αυτές να είναι όσο πιο κοντά γίνεται στις δυνατότητες της κινητής τηλεφωνίας (LTE/4G), όπου η μεταφορά δεδομένων κυμένεται κοντά σε αυτές τις ταχύτητες. Οι χωρητικότητες προσεγγίζουν τις παρακάτω τιμές, ώστε να μπορεί μελλοντικά η επίθεση να επεκταθεί και να προσαρμοστεί για τα δίκτυα κινητής τηλεφωνίας, προσφέροντας μεγάλη ευελιξία στον επιτιθέμενο. Οι ταχύτητες που προσφέρει το 4G δίκτυο παρουσιάζονται αναλυτικότερα στον πίνακα 5.1.

Πίνακας 5.1: LTE Speeds

	LTE
Peak download	100 Mbps
Peak upload	50 Mbps

Για κάθε ένα από τα σενάρια μας εκτελέσθηκαν 60 πειράματα, εξετάζοντας την αποτελεσματικότητα και την απόδοση της επίθεσής μας για νόμιμες κινήσεις (Cross traffic) με πρωτόκολλα μεταφοράς TCP, UDP και TCP/UDP, αντίστοιχα. Συγκεκριμένα, 20 προσομοιώσεις εκτελέσθηκαν για κάθε μία από αυτές τις τρεις περιπτώσεις και κάθε προσομοίωση διήρκησε 450 δευτερόλεπτα. Αναλυτικότερα, λεπτομέρειες για κάθε προσομοίωση παρουσιάζονται στους πίνακες 5.3, 5.4 . Σε κάθε ένα από τα σενάριά μας θεωρούμε 3 bottleneck συνδέσμους στην τοπολογία μας με την ανάλογη χωρητικότητα, ενώ οι χωρητικότητες όλων των υπόλοιπων συνδέσμων έχουν τεθεί στα 100 Mbps. Και στα δύο σενάρια τα ασύρματα δίκτυα των τριών παρόχων ασύρματου δικτύου έχουν δυνατότητες για εύρος ζώνης κοντά στα 50 Mbps. Για την διεξαγωγή των επιθέσεων χρησιμοποιήθηκαν 10 bots (1 συντονιστής και 9 απλά bots). Κάθε διεπαφή που διαθέτουν τα bots συνδέεται σε ένα από τα τρία ασύρματα δίκτυα, αντίστοιχα (με τον τρόπο που έχει αναφερθεί στο προηγούμενο κεφάλαιο). Επιπρόσθετα 5 νόμιμες συσκευές/τερματικά συνδεδεμένες στα ίδια ασύρματα δίκτυα με τα bots χρησιμοποιήθηκαν για τη δημιουργία της νόμιμης κίνησης (δύο ροές για τα ασύρματα δίκτυα 1 και 2 και μία ροή για το δίκτυο 3). Για κάθε ένα από τα πειράματά μας περιμένουμε περίπου 150 δευτερόλεπτα μετά την εκκίνηση της προσομοίωσης έτσι ώστε το πρωτόκολλο δρομολόγησης να συγκλίνει και ύστερα τα bots ξεκινούν την επίθεση. Οι ροές που ανήκουν στην νόμιμη κίνηση (Cross traffic) ξεκινούν για κάθε ασύρματο δίκτυο σε διαφορετικούς χρόνους, όπως φαίνεται στον πίνακα 5.2. Τέλος οι τιμές κατωφλίου που έχουν οριστεί σε κάθε σενάριο για την εκκίνηση της επίθεσης παρουσιάζονται στον πίνακα 5.5.

Πίνακας 5.2: Χρόνοι αρχής και τέλους για τις νόμιμες ροές

Flows	**Start Times (sec)**	**End Time (sec)**	**Wireless Network**
1	240	350	Wireless 1
2	230	350	Wireless 1
3	200	320	Wireless 2
4	230	300	Wireless 2
5	200	350	Wireless 3

Πίνακας 5.3: Παράμετροι του σεναρίου των 10 Mbps

Cross Traffic	**Wireless 1** 50Mbps	**Wireless 2** 50Mbps	**Wireless 3** 50Mbps
TCP	6.48Mbps	7.2Mbps	7.3Mbps
UDP	6.48Mbps	7.2Mbps	7.3Mbps
TCP/UDP	3.72/2.76Mbps	3.6/3.6Mbps	7.3/0Mbps

Πίνακας 5.4: Παράμετροι του σεναρίου των 40 Mbps

Cross Traffic	**Wireless 1** 150Mbps	**Wireless 2** 150Mbps	**Wireless 3** 150Mbps
TCP	31.2Mbps	30Mbps	32.4Mbps
UDP	31.2Mbps	30Mbps	32.4Mbps
TCP/UDP	16.8/14.4Mbps	15/15Mbps	32.4/0Mbps

Πίνακας 5.5: Οι τιμές κατωφλίου για τα δύο σενάρια ως ποσοστά της συνολικής χωρητικότητας των bottleneck συνδέσμων

Σενάρια	**Τιμές κατωφλίου**
10 Mbps	40%
40 Mbps	30%

Επισημαίνεται ότι κατά τη διάρκεια της επίθεσης, οι τελικοί παλμοί που δημιουργούνται από την συνένωση των επιμέρους ροών των bots (που δημιουργεί το Nping) έχουν πλάτος μικρότερο από την συνολική χωρητικότητα των bottleneck συνδέσμων και όχι λίγο μεγαλύτερο, όπως συμβαίνει στις παλμοδικές επιθέσεις. Επιλογή μικρότερων πλατών για τους παλμούς οφείλεται στην αστάθεια που παρατηρείται στο εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης. Παρ' όλα αυτά όπως παρατηρείται παρακάτω η επίθεση παραμένει επιτυχής για τα δύο σενάριά μας.

5.3 Αποτελεσματα

Παρακάτω ακολουθούν τα αποτελέσματα για τα δύο σενάρια που εξετάσαμε στη μορφή γραφικών παραστάσεων:

5.3.1 10 Mbps Χωρητικότητα του Bottleneck Συνδέσμου

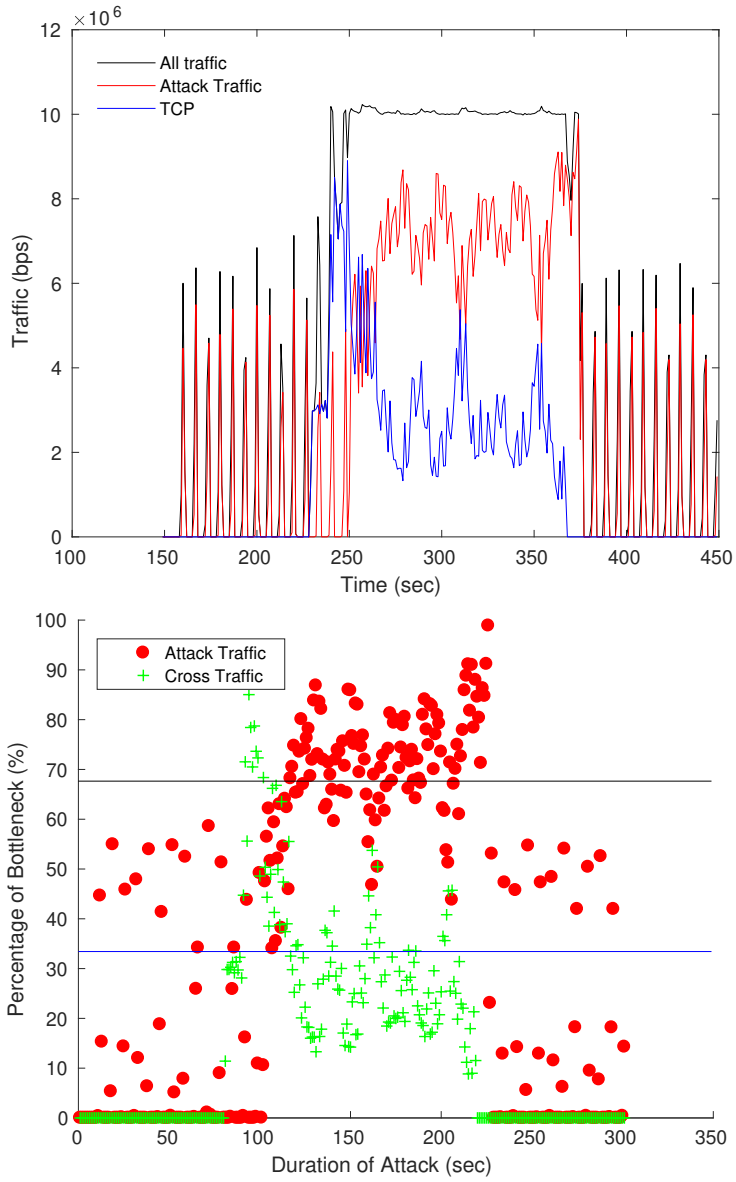
Πρέπει να σημειωθεί ότι σε αυτό το σενάριο έχει οριστεί ο τελικός παλμός που προέρχεται από την συνένωση των επιμέρους παλμών των bots και διέρχεται από τον bottleneck σύνδεσμο να έχει συνολικό πλάτος κοντά στα 6-7 Mbps. Επίσης στα γραφήματα που απεικονίζουν τα ποσοστά της χωρητικότητας του bottleneck συνδέσμου, που καταλαμβάνουν η κακόβουλη και η νόμιμη κίνηση, η μαύρη και η μπλε οριζόντιες γραμμές εκφράζουν το μέσο όρο των ποσοστών για τις δύο κινήσεις, αντίστοιχα. Τέλος πρέπει να τονιστεί ότι με τους διαφορετικούς χρόνους εκκίνησης των νόμιμων ροών για κάθε ασύρματο δίκτυο και bottleneck σύνδεσμο αντίστοιχα (βλ. πίνακα 5.2), σε συνδυασμό με το διαφορετικό αριθμό ροών που αντιστοιχούν σε κάθε bottleneck σύνδεσμο (βλ. πίνακες 5.3, 5.4), εξετάζουμε πως συμπεριφέρεται η επίθεση σε διαφορετικές συνθήκες παρόλο που η χωρητικότητα και των τριών παραμένει σταθερή

και στα δύο σενάρια.

TCP Νόμιμη Κίνηση

Όπως παρατηρούμε από το διάγραμμα 5.1 η επίθεση είναι επιτυχής στον πρώτο bottleneck σύνδεσμο. Βλέπουμε ότι ο συντονιστής (coordinator) για το πρώτο μονοπάτι ξεκινά να εκτιμά το διαθέσιμο εύρος ζώνης του (δηλαδή του bottleneck συνδέσμου), εφόσον περάσουν τα πρώτα 150 δευτερόλεπτα και άρα το πρωτόκολλο δρομολόγησης BGP έχει συγκλίνει (το OSPF έχει συγκλίνει απευθείας). Τις χρονικές στιγμές 230 και 240 sec ξεκινούν οι νόμιμες ροές προς την περιοχή-στόχο φτάνοντας τα 7 Mbps περίπου, την χρονική στιγμή 245 sec, όπως έχει οριστεί. Ο συντονιστής αντιλαμβάνεται ότι το διαθέσιμο εύρος ζώνης στο bottleneck σύνδεσμο έχει πέσει κάτω από το κατώφλι που έχει οριστεί και στέλνει σήμα στα bots να ξεκινήσουν την επίθεση. Η συντονισμένη επίθεση όπως φαίνεται στο διάγραμμα ξεκινά την χρονική στιγμή 250 sec, οπότε και αρχίζει να υποχωρεί η νόμιμη κίνηση έναντι της κακόβουλης. Συγκεκριμένα, η κακόβουλη κίνηση καταφέρνει να περάσει ολόκληρη μέσα από το bottleneck σύνδεσμο φτάνοντας τα 7 Mbps περίπου (όσο και το πλάτος των τελικών παλμών) καταλαμβάνοντας περίπου το 70% της συνολικής χωρητικότητάς του (βλ. μαύρη γραμμή στο διάγραμμα με τα ποσοστά). Αντίθετα, η νόμιμη κίνηση υποχωρεί αρκετά σε σχέση με την αρχική της τιμή, κοντά στα 3 Mbps, καταλαμβάνοντας μόνο το 30% περίπου της συνολικής χωρητικότητας του bottleneck συνδέσμου (βλ. μπλε γραμμή στο διάγραμμα με τα ποσοστά), όπως περιμέναμε και ο bottleneck σύνδεσμος έχει πνιγεί εντελώς (δεν μπορεί να τον διασχίσει περαιτέρω κίνηση). Παρ΄ όλα αυτά εδώ γίνεται εμφανής η απουσία των παλμών της κακόβουλης κίνησης με πλάτος λίγο μεγαλύτερο από τη χωρητικότητα του bottleneck συνδέσμου, καθώς σε αυτή την περίπτωση η κακόβουλη κίνηση θα είχε καταλάβει ολόκληρη την χωρητικότητα του συνδέσμου και η νόμιμη κίνηση θα είχε υποχωρήσει σχεδόν στο μηδέν. Το ζήτημα αυτό θα εξεταστεί αναλυ-

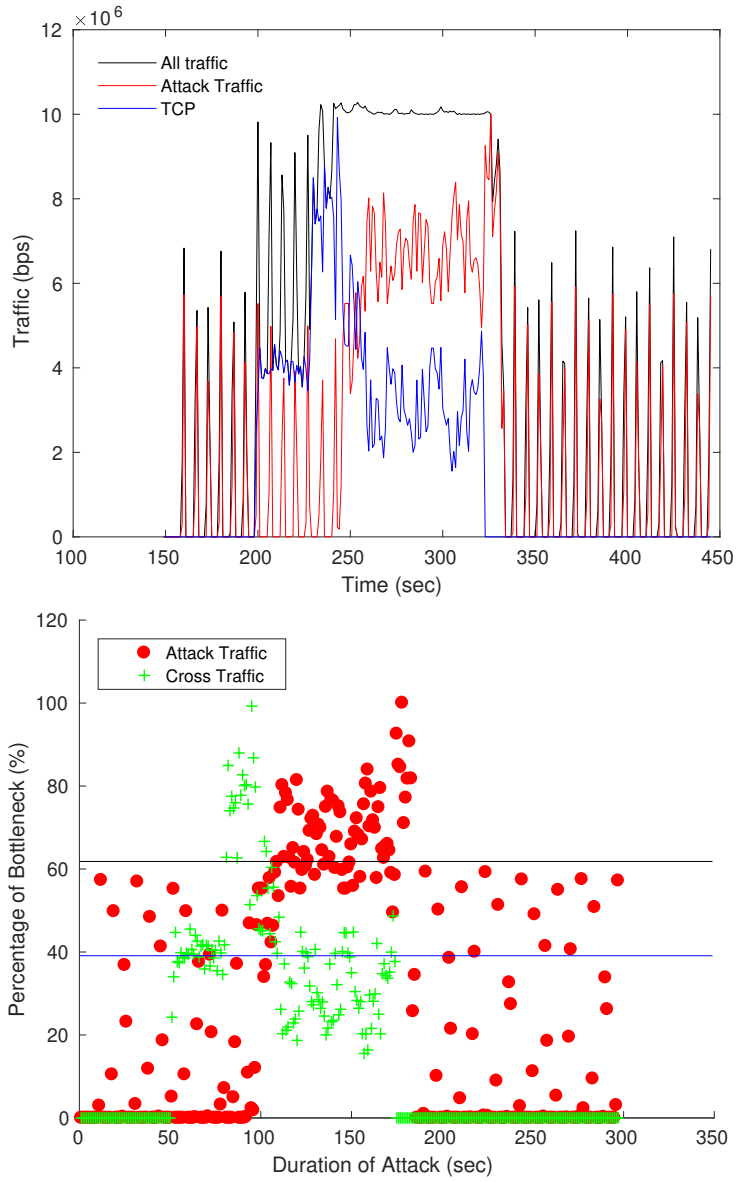
τικότερα στο επόμενο κεφάλαιο. Επίσης για τον ίδιο λόγο βλέπουμε κάποιες ραγδαίες μεταβολές στις δύο κινήσεις (η νόμιμη κίνηση καταφέρνει να καταναλώσει λίγο περισσότερο εύρος ζώνης, ενώ κανονικά δεν θα έπρεπε να συμβαίνει αυτό). Πρέπει ακόμα να σημειωθεί ότι για το συγκεκριμένο σενάριο γίνεται εμφανέστερη η κίνηση που δημιουργεί το εργαλείο εκτίμησης που χρησιμοποιούμε (RT-WABest), στις περιόδους που η επίθεση δεν υφίσταται. Το φαινόμενο αυτό είναι απόλυτα λογικό, εφόσον έχει να κάνει με την λειτουργία του εργαλείου, εισχωρεί δηλαδή κίνηση στο δίκτυο για να πραγματοποιήσει τις μετρήσεις του (το ίδιο πραγματοποιούν σε μεγαλύτερο βαθμό και τα υπόλοιπα εργαλεία εκτίμησης του διαθέσιμου εύρους ζώνης). Το αποτέλεσμα είναι όμως να συμβάλλει αρνητικά στην αναγνωρισιμότητα της επίθεσης από τους μηχανισμούς προστασίας του Διαδικτύου. Στο επόμενο κεφάλαιο θα αναφερθούν ορισμένες λύσεις στο συγκεκριμένο πρόβλημα ως πλαίσιο μελλοντικής επέκτασης της επίθεσης.



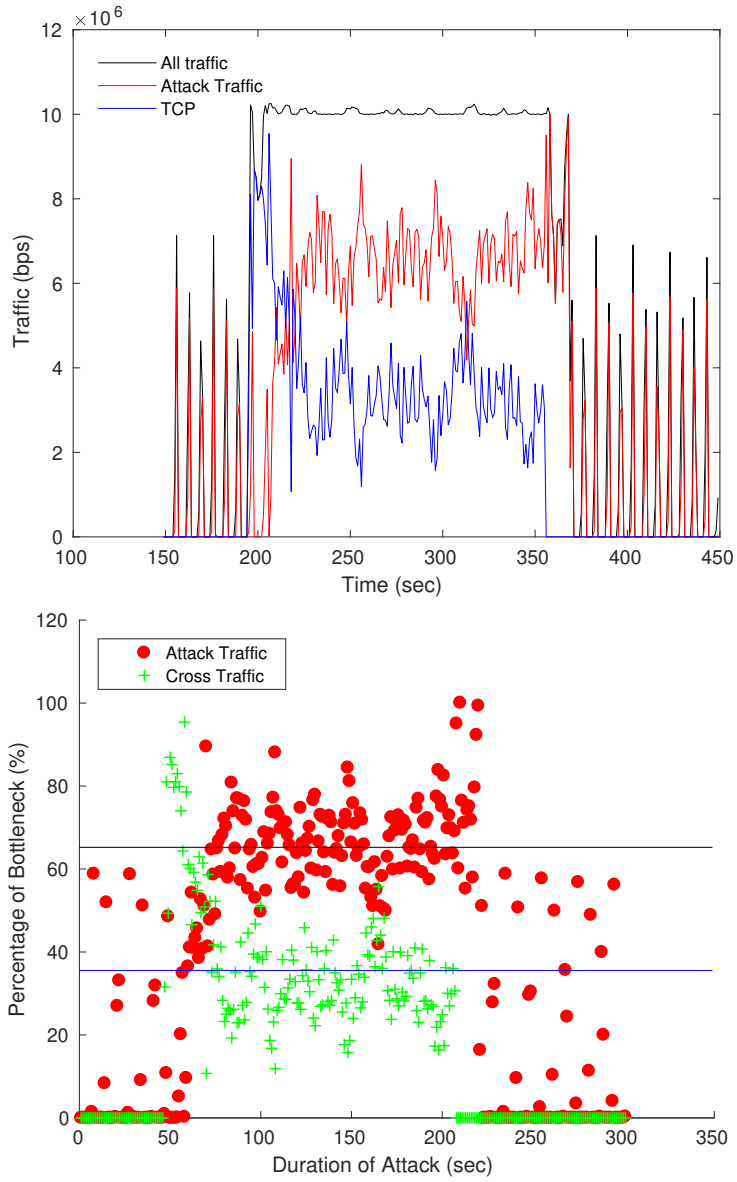
Σχήμα 5.1: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

Παρακάτω παρατίθενται και τα αποτελέσματα για τους δύο άλλους bottleneck συνδέσμους. Όπως παρατηρούμε η επίθεση είναι επιτυχής και για τους άλλους συνδέσμους, με την μόνη διαφορά ότι η κακόβουλη κίνηση καταλαμβάνει ελάχιστα μικρότερο ποσοστό της χωρητικότητας

του bottleneck συνδέσμου σε σχέση με τον πρώτο σύνδεσμο. Η μικρή αυτή πτώση ίσως οφείλεται στους διαφορετικούς χρόνους εκκίνησης των νόμιμων ροών για τον δεύτερο bottleneck σύνδεσμο και της ύπαρξης μίας μόνο νόμιμης κίνησης για τον τρίτο bottleneck σύνδεσμο. Ακόμα, είναι πιθανό στις συγκεκριμένες περιπτώσεις να μην συγχρονίζονται σωστά οι μεμονωμένοι παλμοί των κακόβουλων ροών και άρα οι τελικοί μας παλμοί να μην έχουν το επιθυμητό πλάτος και μήκος.



Σχήμα 5.2: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

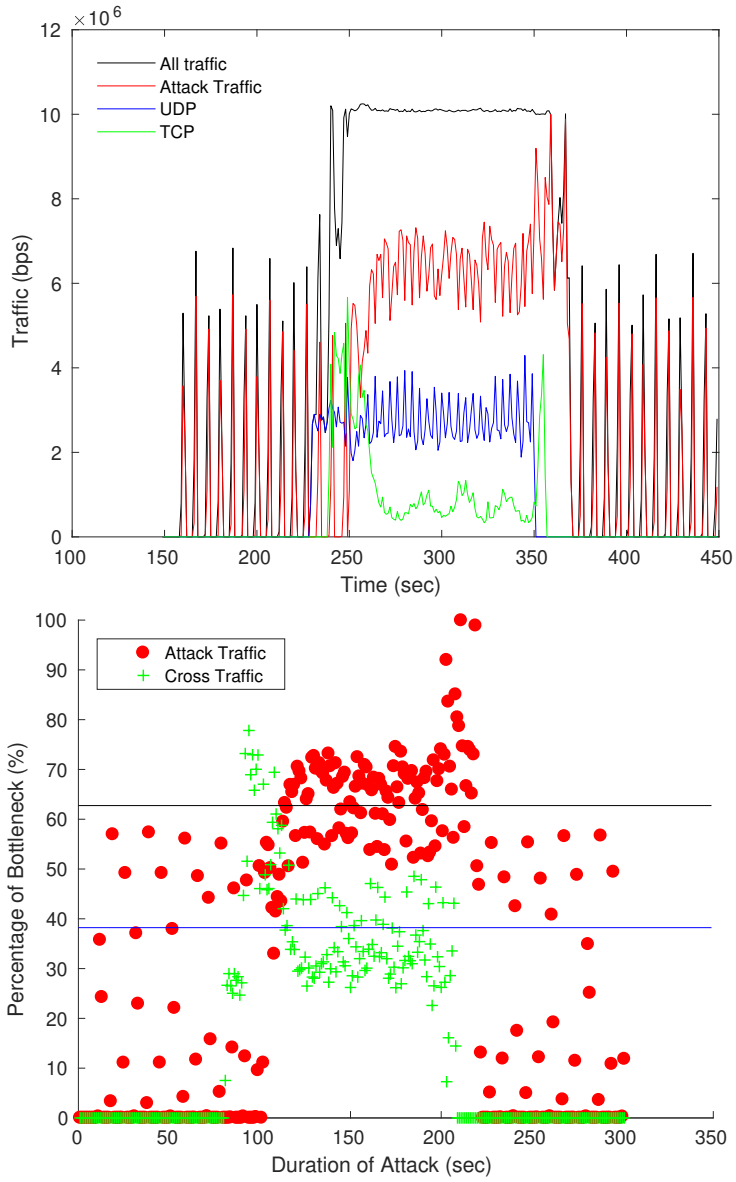


Σχήμα 5.3: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

TCP/UDP Νόμιμη Κίνηση

Σε αυτή την περίπτωση έχουμε TCP και UDP νόμιμη κίνηση προς την περιοχή-στόχο, ταυτόχρονα. Όπως παρατηρούμε από το διάγραμμα

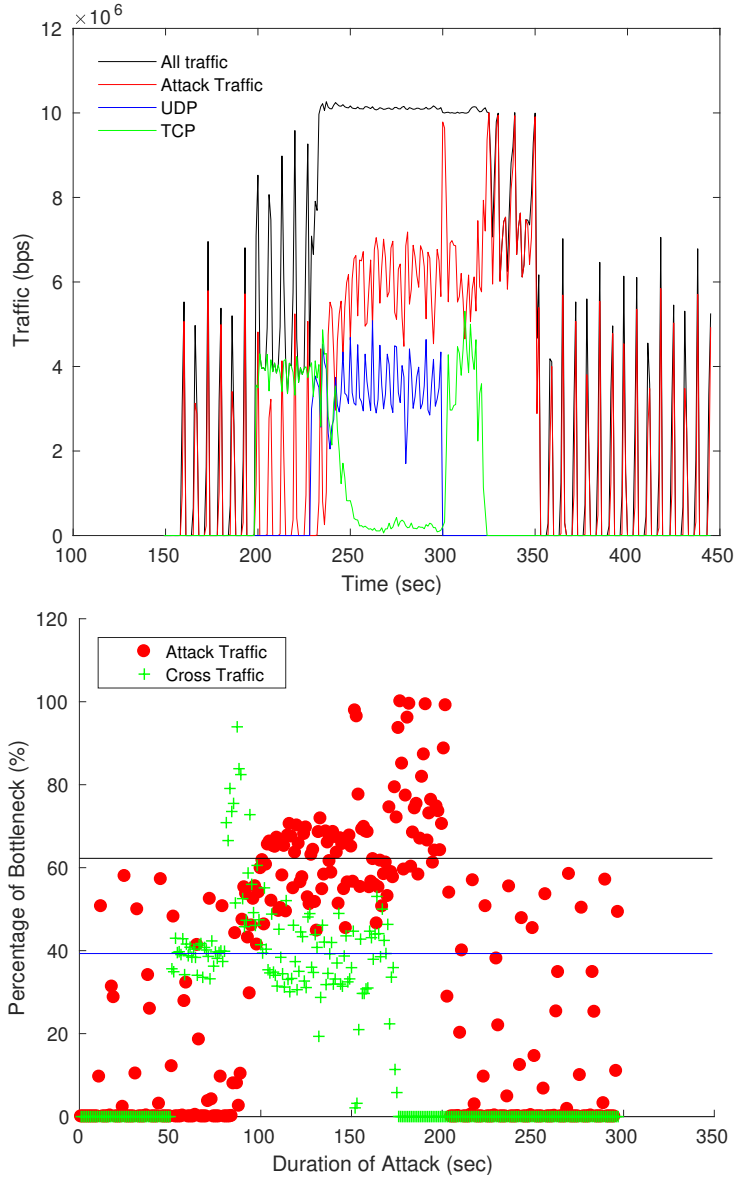
5.4, πάλι βλεπουμε να υπερτερεί η κακόβουλη κίνηση έναντι της νόμιμης μετά την χρονική στιγμή 250 sec που ξεκινά η επίθεση. Συγκεκριμένα, η κακόβουλη κίνηση και πάλι περνά ολόκληρη από το bottleneck σύνδεσμο φτάνοντας τα 7 Mbps περίπου και καταλαμβάνοντας το 65% της συνολικής του χωρητικότητας (βλ. μαύρη γραμμή). Η κύρια διαφορά όμως με την με την προηγούμενη περίπτωση που υπήρχε μόνο TCP νόμιμη κίνηση είναι ότι η UDP νόμιμη κίνηση προς την περιοχή-στόχο δεν υποχωρεί στο ελάχιστο, ενώ η TCP νόμιμη κίνηση υποχωρεί ραγδαία. Το φαινόμενο αυτό είναι απόλυτα λογικό, εφόσον το TCP πρωτόκολλο ανταποκρίνεται σε αλλαγές στο δίκτυο (π.χ., μηχανισμός ελέγχου συμφόρησης), ενώ το πρωτόκολλο UDP δεν ανταποκρίνεται σε καμία αλλαγή. Επίσης η επίθεσή μας έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να εκμεταλλεύεται τη λειτουργία του μηχανισμού ελέγχου συμφόρησης του TCP, ο οποίος οδηγεί τις TCP ροές στη μείωση του ρυθμού αναμετάδοσης τους όταν υπάρχει συμφόρηση. Αντίθετα το πρωτόκολλο UDP δεν διαθέτει κανέναν τέτοιο μηχανισμό. Όλα τα πακέτα αποστέλλονται μία φορά χωρίς αναμεταδόσεις και υποχωρήσεις. Για αυτό το λόγο παρατηρούμε ότι η UDP κίνηση στο πείραμά μας δεν έχει επηρεαστεί στο ελάχιστο από την κακόβουλη TCP κίνηση, την οποία ανταγωνίζεται.



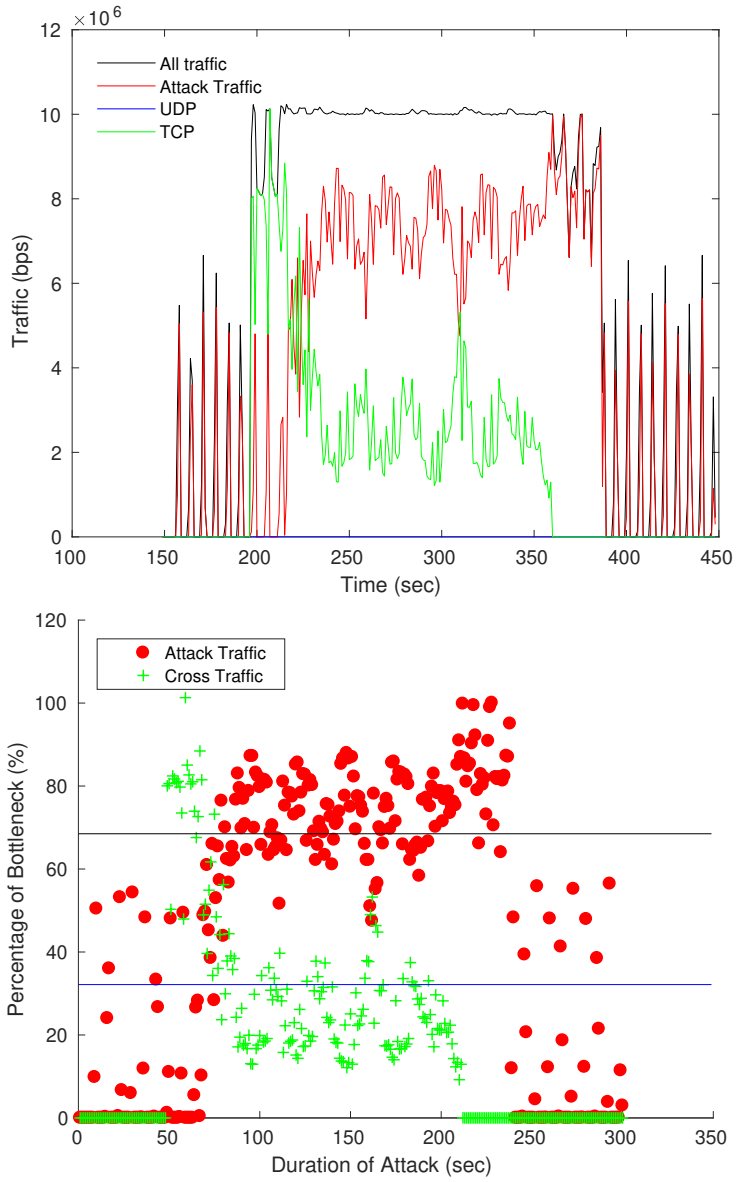
Σχήμα 5.4: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

Παρακάτω παρουσίαζονται και τα διαγράμματα για τους άλλους δύο bottleneck συνδέσμους. Η εικόνα που λαμβάνουμε είναι παρόμοια με εκείνη για τον πρώτο bottleneck σύνδεσμο. Επισημαίνουμε ότι για τον τρίτο bottleneck σύνδεσμο δεν υπάρχει UDP νόμιμη κίνηση παρά μόνο

TCP, οπότε και τα αποτελέσματα εκφυλίζονται σε εκείνα της προηγούμενης περίπτωσης. Για αυτό το λόγο βλέπουμε και μία αύξηση του ποσοστού της χωρητικότητας που καταλαμβάνει η κακόβουλη κίνηση στον συγκεκριμένο σύνδεσμο, σε σχέση με τους άλλου συνδέσμους (βλ. μάυρη γραμμή).



Σχήμα 5.5: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

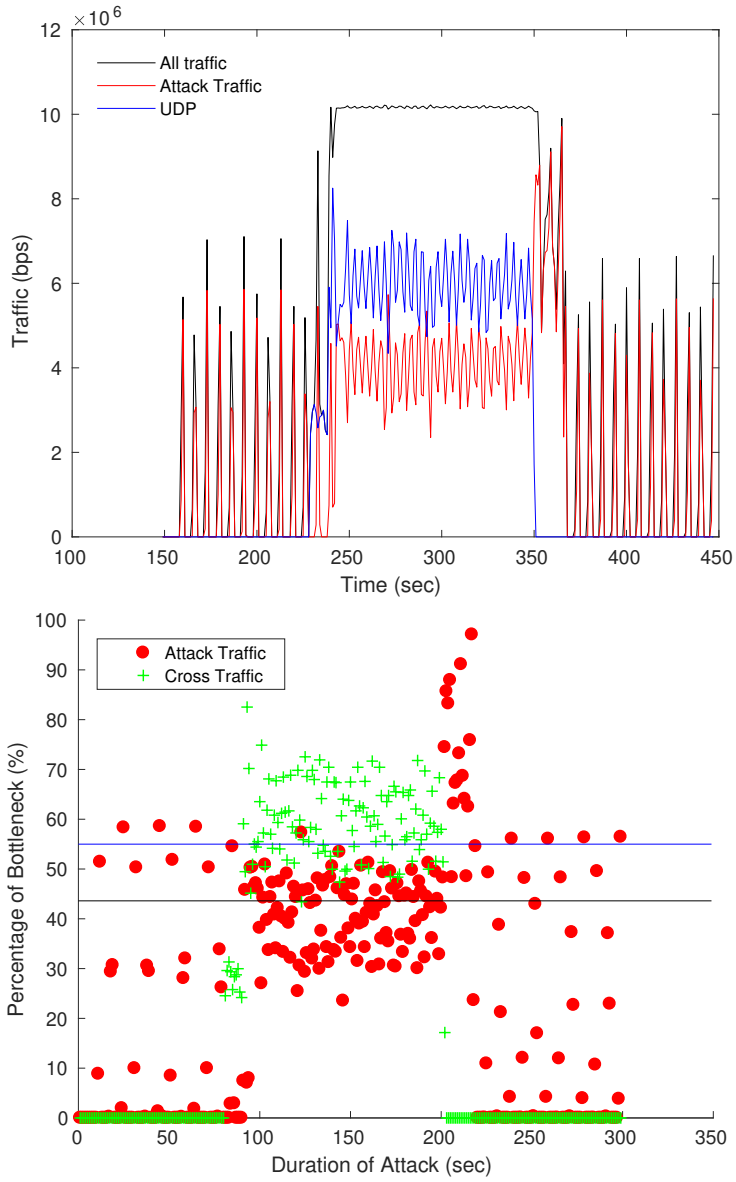


Σχήμα 5.6: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

UDP Νόμιμη Κίνηση

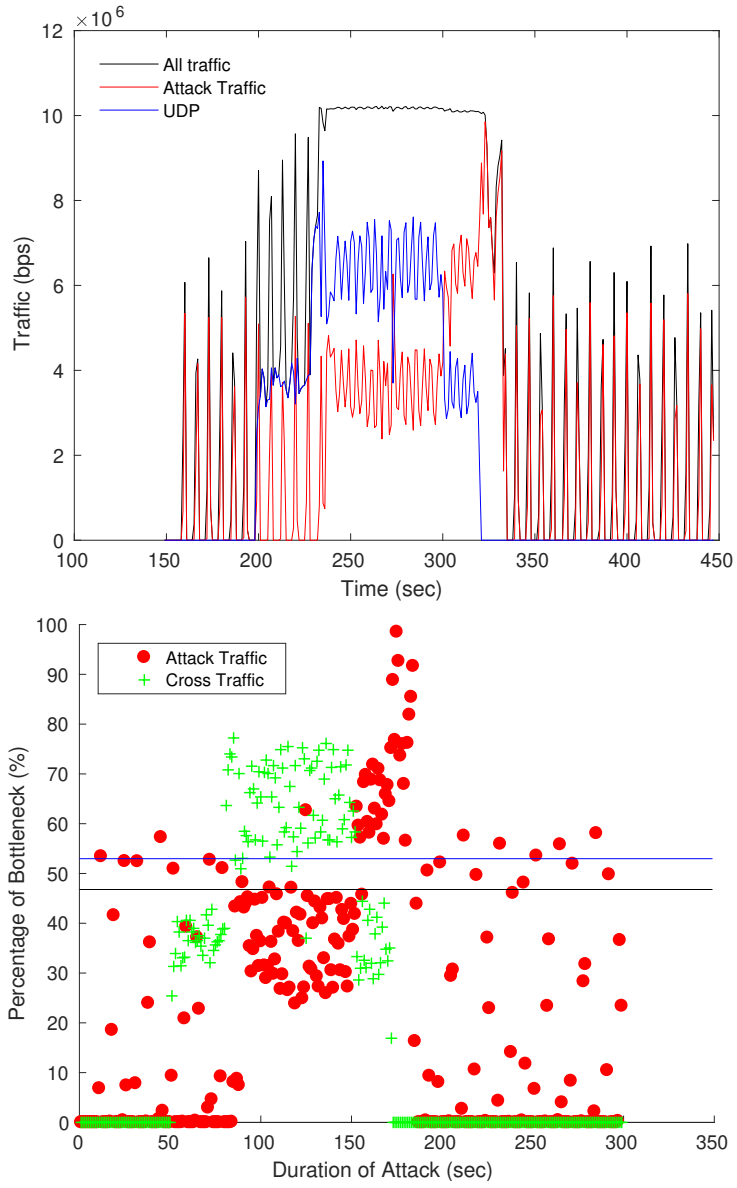
Όπως φαίνεται από το διάγραμμα 5.7 η περίπτωση που η νόμιμη κίνηση αποτελείται μόνο από UDP πακέτα είναι η μοναδική στην οποία

η επίθεσή μας είναι εντελώς αναποτελεσματική. Συγκεκριμένα, παρατηρούμε ότι ενώ το εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης έχει προβλέψει σωστά ότι υπάρχει συμφόρηση στο bottleneck σύνδεσμο και η επίθεση ξεκίνησε την χρονική στιγμή 250 sec, η νόμιμη UDP κίνηση (Cross traffic) που διέρχεται από εκείνον έχει υποχωρήσει ελάχιστα, καταλαμβάνοντας το 55% περίπου της συνολικής χωρητικότητάς του. Όπως εξηγήθηκε και στην προηγούμενη περίπτωση, το πρωτόκολλο UDP δεν ανταποκρίνεται σε καμία αλλαγή στο δίκτυο. Όλα τα πακέτα θα αποσταλούν από την πηγή με τον αρχικό ρυθμό μετάδοσης που έχει οριστεί και όσα χαθούν στην πορεία δεν θα αναμεταδωθούν. Το αποτέλεσμα είναι η νόμιμη UDP κίνηση να ανταγωνίζεται σε μεγάλο βαθμό την κακόβουλη κίνηση, η οποία είναι τώρα εκείνη που υποχωρεί, γιατί υπόκειται στο πρωτόκολλο TCP. Άρα στην περίπτωση που η νόμιμη κίνηση είναι μόνο τύπου UDP η επίθεση μας δεν έχει καμία απολύτως επίδραση σε εκείνη, παρά μόνο φροντίζει ώστε να καταλειφθεί το υπόλοιπο εύρος ζώνης του bottleneck συνδέσμου και αυτός να πνιγεί εντελώς. Παρ' όλο που η επίθεση δεν είναι αποτελεσματική σε αυτή την περίπτωση, η περιοχή-στόχος και παλί θα δεχθεί ζημία εφόσον θα ελαχιστοποιηθεί αρκετά η ποιότητα των υπηρεσιών που προσφέρει στους νόμιμους χρήστες (βέβαια σε μικρότερο βαθμό από τις προηγούμενες περιπτώσεις).

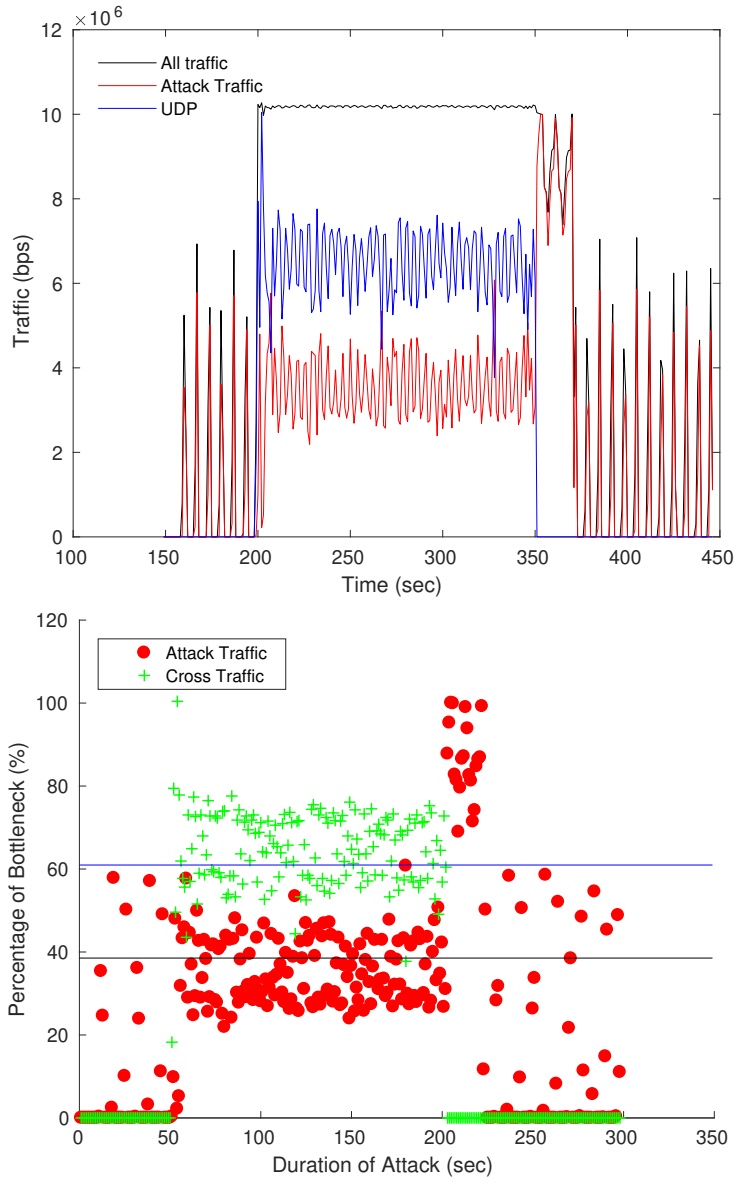


Σχήμα 5.7: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση

Και για τους άλλους δύο bottleneck συνδέσμους έχουμε την ίδια εικόνα με τον πρώτο. Τα διαγράμματά τους παρατίθενται παρακάτω.



Σχήμα 5.8: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση



Σχήμα 5.9: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 10Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση

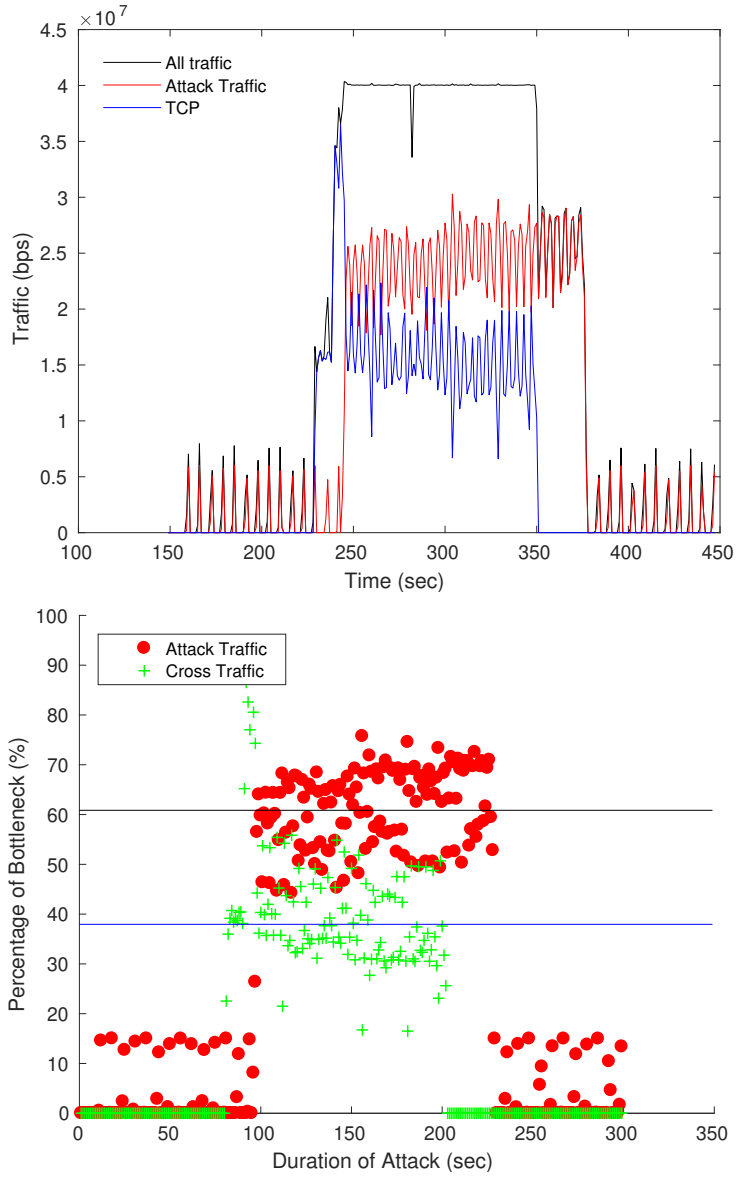
5.3.2 40 Mbps Χωρητικότητα του Bottleneck Συνδέσμου

Η μόνη διαφορά αυτού του σεναρίου σε σχέση με το προηγούμενο είναι ότι αυξάνεται η χωρητικότητα των bottleneck συνδέσμων σε 40 Mbps, καθώς και η νόμιμη κίνηση που αποστέλλουν οι απλοί χρήστες προς την περιοχή-στόχο. Σκοπός μας είναι να εξετάσουμε πως συμπεριφέρεται η επίθεσή μας, όταν τα bots πρέπει να στείλουν μεγαλύτερο μέγεθος κίνησης για να "πνίξουν" τους στόχους τους. Παρακάτω παρουσιάζονται οι περιπτώσεις για κινήσεις TCP, TCP/UDP και UDP.

TCP Νόμιμη Κίνηση

Όπως συμπεραίνουμε από το διάγραμμα 5.10 η επίθεση μας είναι αποτελεσματική και για την περίπτωση που έχει αυξηθεί η χωρητικότητα των συνδέσμων. Παρ' όλα αυτά δεν είναι τόσο αποδοτική όσο στην περίπτωση με τα 10 Mbps χωρητικότητας των bottleneck συνδέσμων. Αναλυτικότερα, παρατηρούμε ότι η επίθεση ξεκινά σωστά όταν η συσσωρευμένη νόμιμη TCP κίνηση έχει φτάσει τα 32 Mbps περίπου (τη χρονική στιγμή 250 sec). Το εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης που χρησιμοποιούμε (RT-WABest) αποκρίνεται ταχύτερα στην περίπτωση αυτή, όμως δεν συμβαίνει το ίδιο με την επίθεση γενικότερα. Ενώ έχει οριστεί οι τελικοί κακόβουλοι παλμοί που θα διέρχονται από τον bottleneck σύνδεσμο να έχουν πλάτος κοντά στα 30 Mbps, παρατηρούμε ότι το μέσο πλάτος τους εδώ είναι κοντά στα 25 Mbps καταλαμβάνοντας το 60% περίπου της συνολικής χωρητικότητας του συνδέσμου (βλ. μαύρη γραμμή στο διάγραμμα των ποσοστών). Αυτό σημαίνει ότι υπάρχει μεγαλύτερος ανταγωνισμός με την νόμιμη κίνηση. Όμως και πάλι βλεπουμε πως η είσοδος της κακόβουλης κίνησης στον bottleneck σύνδεσμο έχει ως συνέπεια να καταπιεστεί η νόμιμη κίνηση από τα 32 Mbps στα 17 Mbps περίπου, καταλαμβάνοντας το 40% περίπου της συνολικής χωρητικότητας του bottleneck συνδέσμου (βλ. μπλε γραμμή), επιβεβαιώντας την επιτυχία της επίθεσης. Και πάλι πρέπει

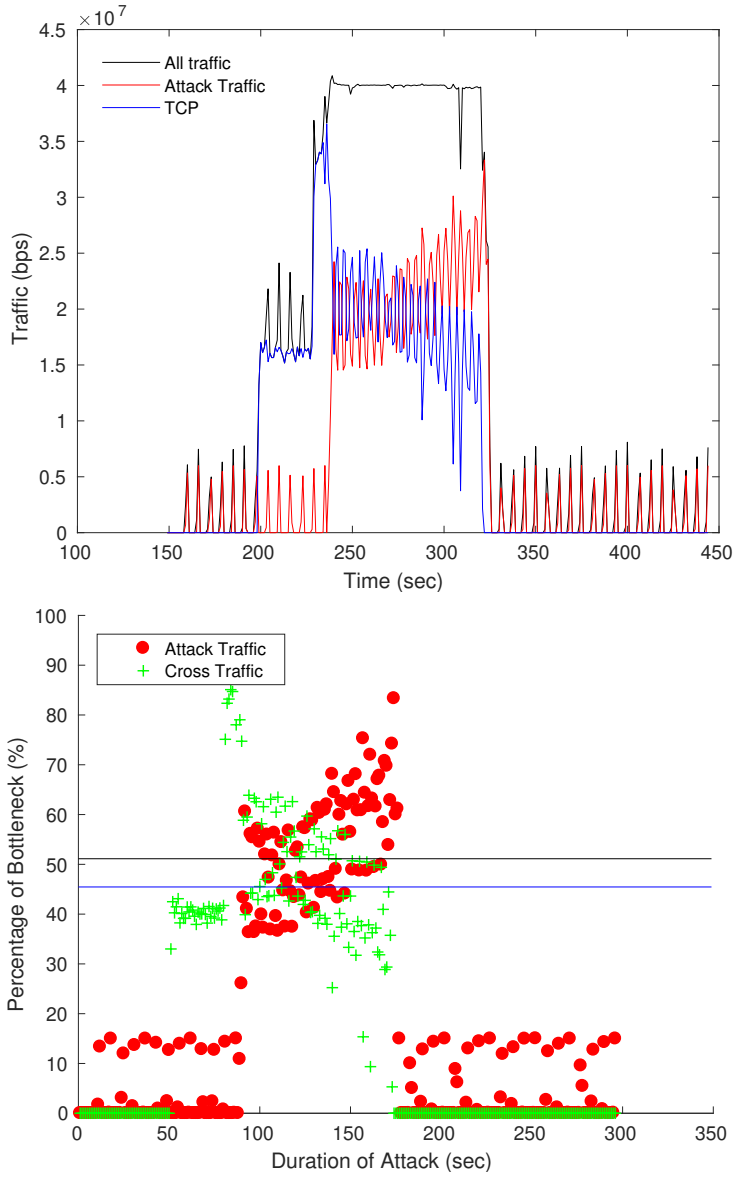
να τονιστεί πως το πλάτος των τελικών κακόβουλων παλμών επηρεάζει σημαντικά την απόδοση της επίθεσης. Αν εκείνο ξεπερνούσε την χωρητικότητα του bottleneck συνδέσμου θα αναμέναμε σαφώς καλύτερα αποτελέσματα. Επίσης και σε αυτό το σενάριο γίνεται εμφανής η κίνηση που εισάγει το εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης που χρησιμοποιούμε. Το γεγονός αυτό συμβάλλει όπως και προηγουμένως στην αναγνωρισιμότητα της επίθεσης (τρόποι επίλυσης τους συγκεκριμένου προβλήματος θα αναφερθούν στο επόμενο κεφάλαιο).



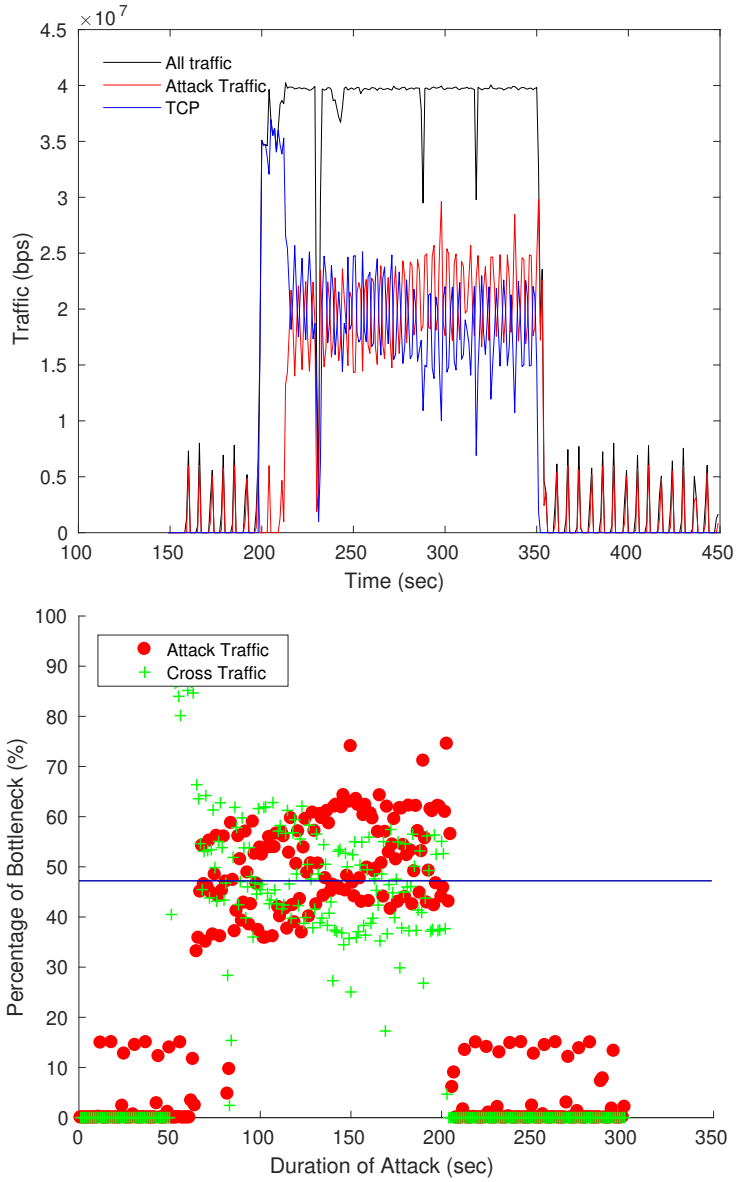
Σχήμα 5.10: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

Παρακάτω παρουσίαζονται τα αποτελέσματα για τους άλλους δύο bottleneck συνδέσμους. Παρατηρούμε μία σαφή πτώση του ποσοστού που καταλαμβάνει η κακόβουλη κίνηση και για τους δύο συνδέσμους. Συγκεκριμένα, στον δεύτερο bottleneck σύνδεσμο το ποσοστό κυμένε-

ται κοντά στο 50%. Η πτώση αυτή οφείλεται στο γεγονός ότι η επίθεση δεν προλαβαίνει στον λιγοστό χρόνο που υφίσταται συμφόρηση να οδηγήσει την νόμιμη κίνηση σε υποχώρηση. Στον τρίτο bottleneck σύνδεσμο παρατηρούμε ότι σε κάποια σημεία έχουμε απότομη πτώση της κίνησης που διέρχεται από τον σύνδεσμο (π.χ., χρονική στιγμή 230 sec). Αυτές οι πτώσεις πιθανότατα οφείλονται στην αδυναμία του εξομοιωτή να υποστηρίξει την ταυτόχρονη ύπαρξη ενός μεγάλου αριθμού συσκευών που διαθέτει η τοπολογία μας, συναρτήσει των μεγάλων σε μέγεθος ροών που δημιουργούνται. Επίσης η συνολική κακόβουλη κίνηση που περνά από τον σύνδεσμο φτάνει τα 20 - 22 Mbps, καταλαμβάνοντας μόνο το 48% της συνολικής χωρητικότητας του συνδέσμου. Αντίθετα η νόμιμη κίνηση σημειώνει μία μικρότερη πτώση από τα 32 Mbps στα 20 Mbps καταλαμβάνοντας τα ίδια ποσοστά χωρητικότητας με την κακόβουλη κίνηση. Η μόνη εξήγηση που μπορεί να δωθεί για αυτό το φαινόμενο είναι ότι δεν πραγματοποιήθηκε σωστός συντονισμός των bots της τρίτης ομάδας, σε συνδυασμό με την αδυναμία του εξομοιωτή να υποστηρίξει τις ροές.



Σχήμα 5.11: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

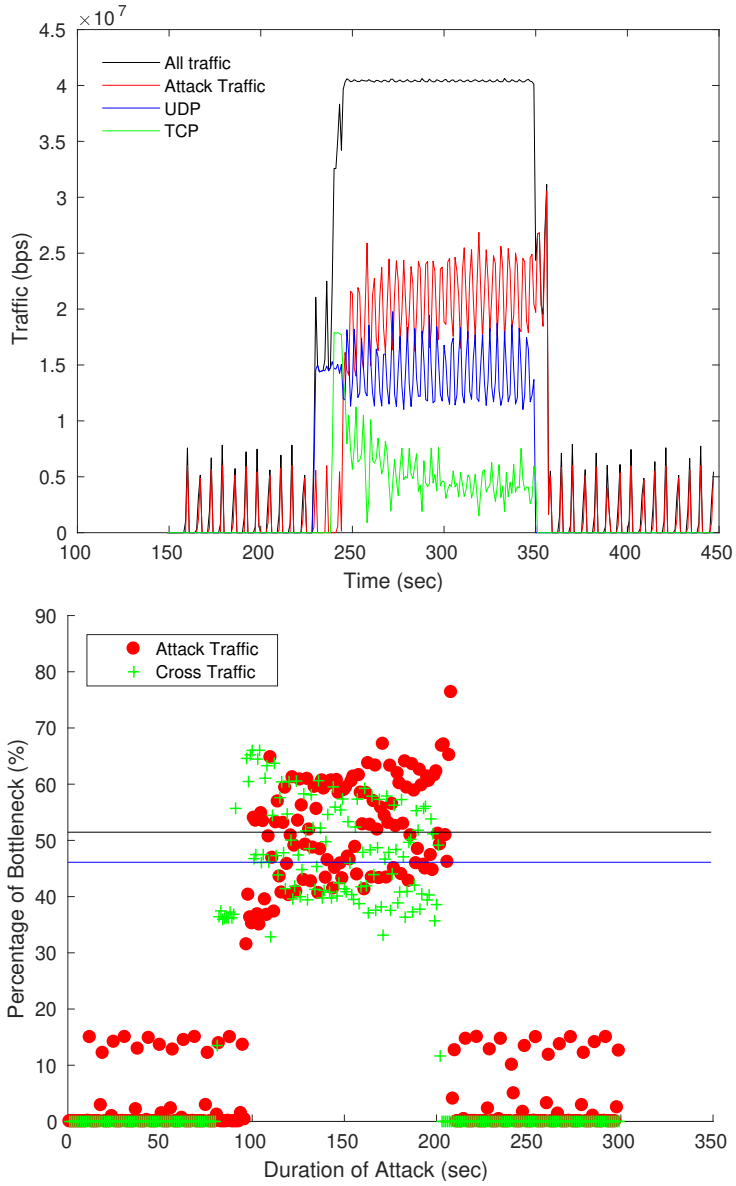


Σχήμα 5.12: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP Νόμιμη Κίνηση

TCP/UDP Νόμιμη Κίνηση

Τα αποτελέσματα που λάβαμε για την περίπτωση αυτή πλησιάζουν αρκετά τα αποτελέσματα του σεναρίου για τα 10 Mbps χωρητικότη-

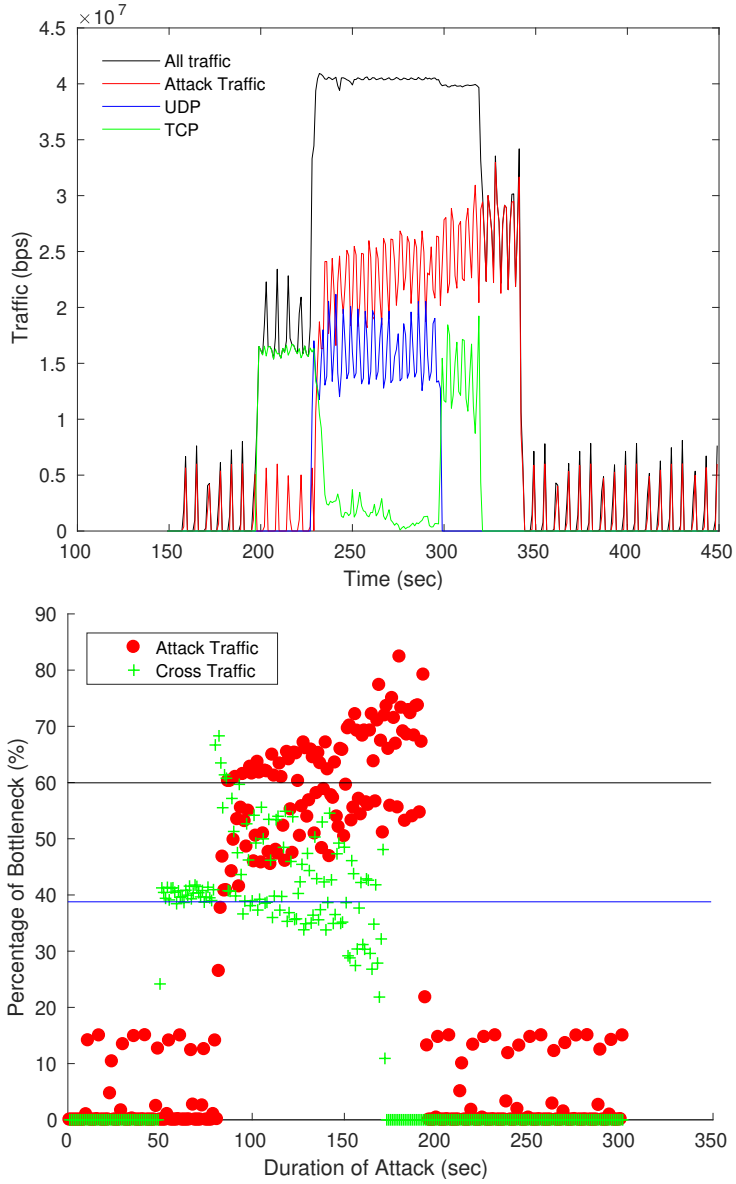
τας του bottleneck συνδέσμου. Συγκεκριμένα, για τον πρώτο σύνδεσμο παρατηρούμε ότι ο εκτιμητής του διαθέσιμου εύρους ζώνης αντιλήφθηκε σχετικά γρήγορα τη συμφόρηση στο bottleneck σύνδεσμο (χρονική στιγμή 250 sec) και αμέσως ξεκίνησε η επίθεση. Η κακόβουλη κίνηση βλέπουμε πως φτάνει τα 21 Mbps καταλαμβάνοντας περίπου το 53% της συνολικής χωρητικότητας του συνδέσμου (βλ. μαύρη γραμμή στο διάγραμμα με τα ποσοστά 5.13). Αντίθετα, η νόμιμη κίνηση η οποία αποτελείται τώρα και από UDP αλλά και TCP κίνηση έχει διαφορετική συμπεριφορά. Όπως ήταν το αναμενόμενο η κακόβουλη κίνηση προκαλεί την υποχώρηση της νόμιμης TCP κίνησης. Ειδικότερα, βλέπουμε ότι από τα 17 Mbps που καταλάμβανε αρχικά, έπεσε κοντά στα 4 Mbps (3 φορές μικρότερη). Αντίθετα, η UDP νόμιμη κίνηση δεν σημείωσε καμία πτώση, παραμένοντας στα 15 Mbps, όπως ήταν αναμενόμενο εφόσον δεν αποκρίνεται σε καμία αλλαγή. Η UDP κίνηση είναι εκείνη που δικαιολογεί την κατάληψη του 48% περίπου της συνολικής χωρητικότητας του bottleneck συνδέσμου από τη συνολική νόμιμη κίνηση (βλ. μπλε γραμμή στο διάγραμμα με τα ποσοστά 5.13).



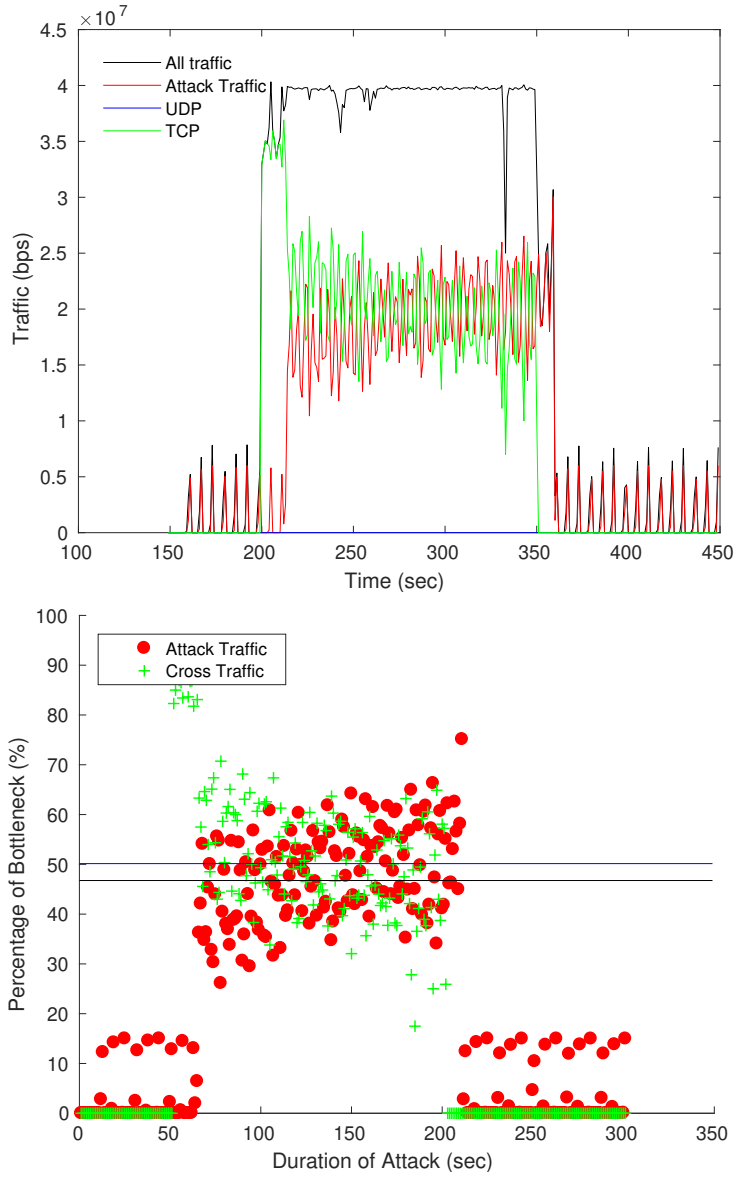
Σχήμα 5.13: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

Παρακάτω παρουσίαζονται και τα αποτελέσματα για τους άλλους δύο συνδέσμους, τα οποία συνάδουν με εκείνα για τον πρώτο σύνδεσμο. Πρέπει να σημειωθεί ότι και πάλι για τον τρίτο bottleneck σύνδεσμο δεν υπάρχει UDP νόμιμη κίνηση παρά μόνο TCP, οπότε και τα αποτελέ-

σματα που λάβαμε πλησιάζουν εκείνα της προηγούμενης περίπτωσης.



Σχήμα 5.14: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

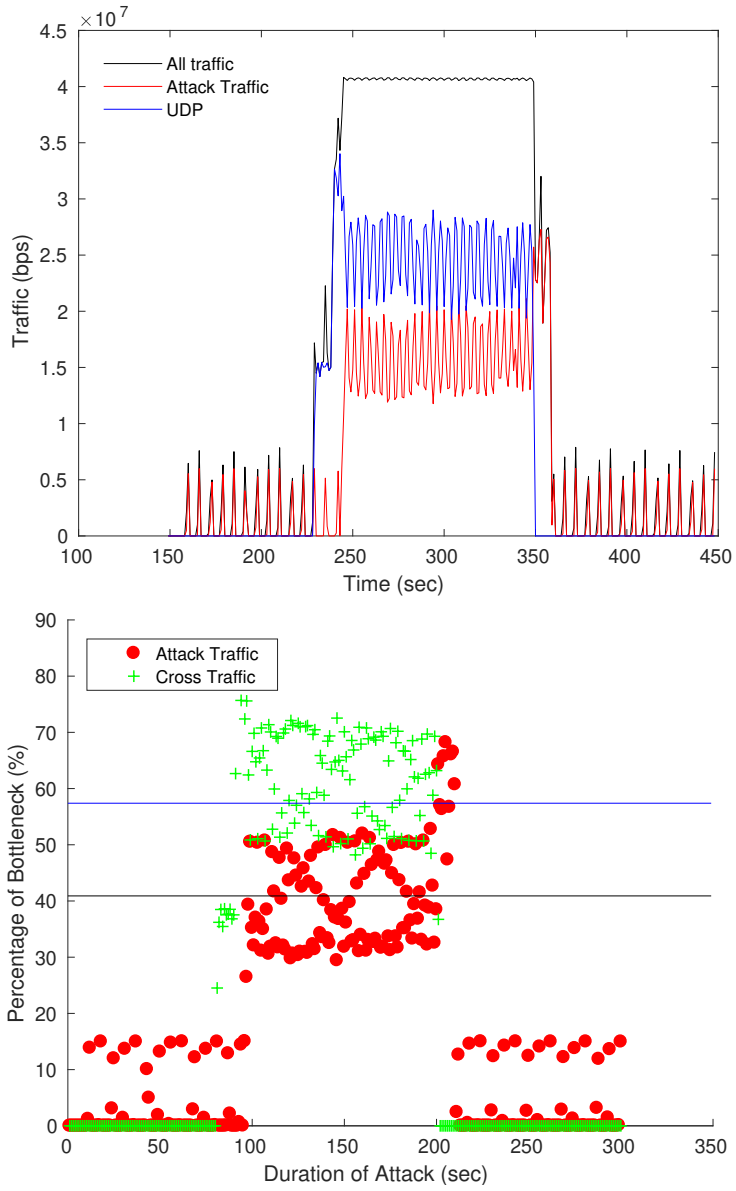


Σχήμα 5.15: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και TCP/UDP Νόμιμη Κίνηση

UDP Νόμιμη Κίνηση

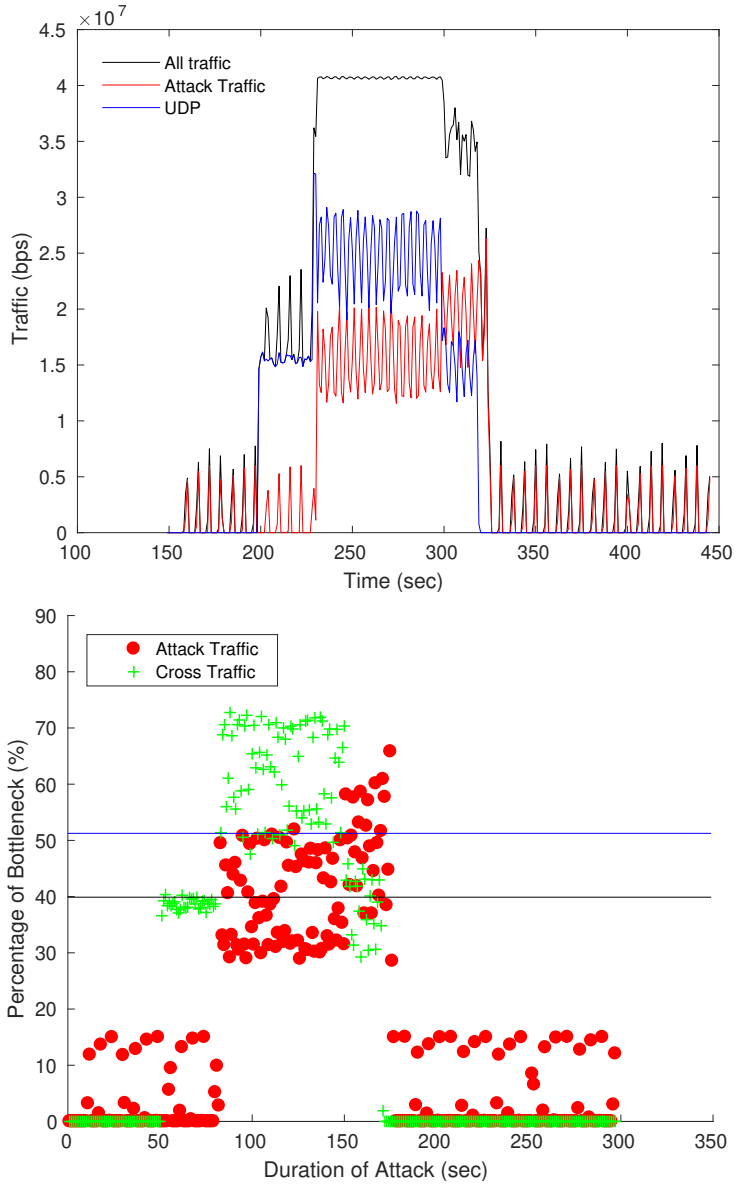
Στη συγκεκριμένη περίπτωση που έχουμε μόνο UDP νόμιμη κίνηση, περιμένουμε η επίθεση μας να μην είναι αποτελεσματική. Πράγματι,

όπως φαίνεται και από τα αποτελέσματα για τον πρώτο σύνδεσμο (διάγραμμα 5.16) η επίθεσή μας είναι αναποτελεσματική για αυτού του είδους κίνηση. Παρατηρούμε ότι η επίθεση ξεκινά λίγο μετά την υπάρξη της συμφόρησης στον bottleneck σύνδεσμο (χρονική στιγμή 250 sec). Η UDP κίνηση παρότι σημειώνει μία σημαντική πτώση από τα 32 Mbps στα 25 Mbps παραμένει κυρίαρχη καθόλη τη διάρκεια της επίθεσης, καταλαμβάνοντας το 60% της συνολικής χωρητικότητας του bottleneck συνδέσμου (βλ. μπλε γραμμή στο διάγραμμα με τα ποσοστά). Αντίθετα, η κακόβουλη κίνηση φτάνει μόνο τα 15 Mbps, καταλαμβάνοτας το 40% της συνολικής χωρητικότητας του bottleneck συνδέσμου (βλ. μαύρη γραμμή στο διάγραμμα με τα ποσοστά), σηματοδοτώντας την αποτυχία της επίθεσης στη συγκεκριμένη περίπτωση.

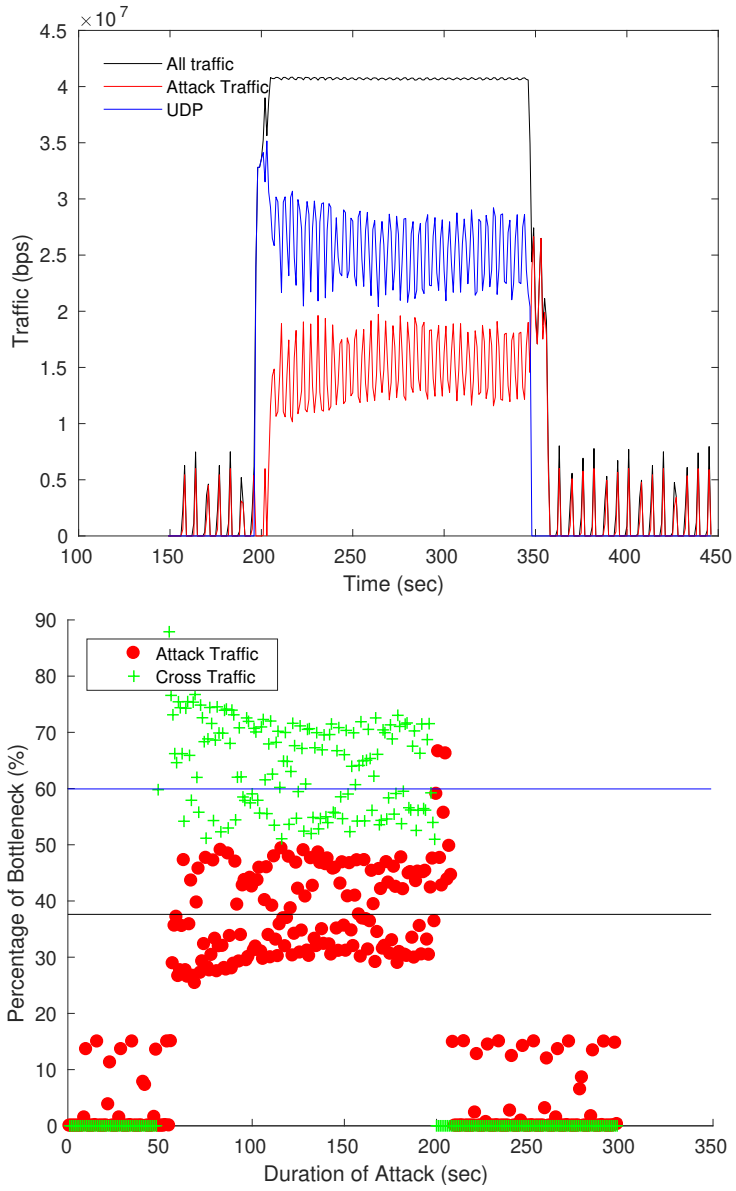


Σχήμα 5.16: Μεγέθη και Ποσοστά των Κινήσεων για τον 1ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση

Παρακάτω παρουσιάζονται τα αποτελέσματα για τους άλλους δύο συνδέσμους. Όπως περιμένουμε η αποτυχία της επίθεσης γίνεται εμφανής και σε αυτούς τους συνδέσμους.



Σχήμα 5.17: Μεγέθη και Ποσοστά των Κινήσεων για τον 2ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση



Σχήμα 5.18: Μεγέθη και Ποσοστά των Κινήσεων για τον 3ο Bottleneck Σύνδεσμο με 40Mbps Χωρητικότητα και UDP Νόμιμη Κίνηση

5.4 Γενικά Συμπεράσματα

Από τα αποτελέσματα που παρουσιάστηκαν παραπάνω γίνεται εμφανές ότι η επίθεσή μας είναι επιτυχής σε μεγάλο βαθμό. Η μόνη περίπτωση, στην οποία δεν υφίσταται αυτός ο ισχυρισμός είναι όταν η νόμιμη κίνηση (Cross traffic) αποτελείται μοναδικά από UDP πακέτα. Η επίθεση εκμεταλλεύεται τις ιδιαιτερότητες του πρωτοκόλλου TCP και συγκεκριμένα του μηχανισμου ελέγχου συμφορήσεων που διαθέτει για την επιτυχία της. Το πρωτόκολλο UDP δεν διαθέτει κάποιον τέτοιο μηχανισμό και γενικά δεν ανταποκρίνεται σε αλλαγές στο δίκτυο, οπότε και καθιστά αναποτελεσματική την επίθεσή μας. Επίσης πρέπει να αναφερθεί ότι ενώ χρησιμοποιήθηκαν μηχανισμοί για να είναι λιγότερο αναγνωρίσιμη η επίθεση, (π.χ., καταμοιρασμός της κακόβουλης κίνησης ανάμεσα σε bots και servers δολώματα, αλλαγή των συντονιστών, κ.τ.λ) η εισαγωγή μεγάλου μεγέθους κίνησης στο δίκτυο λόγω του εργαλείου εκτίμησης του διαθέσιμου εύρους ζώνης που χρησιμοποιούμε (RT-WABest), υποδηλωνει την ύπαρξή της.

Ταυτόχρονα, η χρησιμοποίηση ενός emulator, ο οποίος προσομοιώνει εκατοντάδες συσκευές, καταναλώνοντας τους περιορισμένους πόρους ενός μόνο φυσικού συστήματος δεν μας επέτρεψε να χρησιμοποιήσουμε έναν μεγάλο αριθμό από bots, ώστε κάθε μεμονωμένη κακόβουλη κίνηση να είναι ελάχιστη σε σχέση με την συνολική που διέρχεται από κάθε bottleneck σύνδεσμο. Το γεγονός αυτό πάλι συμβάλλει αρνητικά στην αναγνωρισιμότητα της επίθεσης, όμως σε πραγματικά σενάρια που ο επιτιθέμενος έχει στην διάθεση του εκατομμύρια συσκευές, η παραπάνω λεπτομέρεια δεν υφίσταται. Στο επόμενο κεφάλαιο θα παρουσιασοτύν ορισμένοι τρόποι αντιμετώπισης της επίθεσης καθώς και μελλοντικές επεκτάσεις της, οι οποίες την καθιστούν ακόμα πιο αποδοτική.

Κεφάλαιο 6

Τρόποι Αντιμετώπισης και Μελλοντικές Επεκτάσεις

Σε αυτό το κεφάλαιο θα παρουσιαστούν πιθανοί τρόποι αντιμετώπισης, καθώς και ορισμένες μελλοντικές επεκτάσεις της επίθεσης.

6.1 Πιθανοί Τρόποι Αντιμετώπισης της Επίθεσης

Ένας από τους περισσότερο διαδεδομένους αλλά και ευκολότερους στην υλοποίηση τρόπους αντιμετώπισης της επίθεσής μας είναι οι τεχνικές διαχείρισης της κίνησης (Traffic Engineering - TE). Σύμφωνα με τις τεχνικές αυτές, όταν σε ένα δίκτυο παρατηρηθούν περιπτώσεις συμφόρησης, αλλάζουν τα μονοπάτια που περιέχουν κορεσμένους συνδέσμους και χρησιμοποιούνται εναλλακτικές διαδρομές για την εξισορρόπιση του φορτίου της μεγάλης σε μέγεθος κινήσεως (load balancing). Παρ' όλα αυτά μία απλή αλλαγή των διαδρομών δεν θα είχε ως αποτέλεσμα να σταματήσει ή να μειωθεί η ζημία που προκαλεί η επίθεση, εφόσον νέα

σύνολα συνδέσμων-στόχων θα χρησιμοποιούνταν για την συνέχεια της επίθεσης [3]. Πρέπει οι τεχνικές διαχείρισης της κίνησης να είναι συνεπώς ''εξυπνότερες'', προσπαθώντας ταυτόχρονα να καταδείξουν τα bots που συμμετέχουν στην επίθεση και τον επιτιθέμενο. Μία τέτοια τεχνική προτείνεται στο [23], όπου κρατείται μνήμη για παλαιότερες αλλαγές στην δρομολόγηση με στόχο να βρεθεί η περιοχή-στόχος και ταυτόχρονα να περιοριστεί η συμφόρηση στους κορεσμένους συνδέσμους. Η τεχνική αυτή μπορεί να συνδυαστεί και με άλλους μηχανισμούς άμυνας, όπως χρήση TTL inspectors [29], Bot-Hunters, Phantom Nets και White Holes [30]. Παράλληλα έχει προταθεί και η χρήση Ορισμένων από το Λογισμικό Δικτύων (Software Defined Networks - SDN) σε συνδυασμό με το Traffic Engineering, ώστε να γίνεται απολεσματικότερη παρακολούθηση της κίνησης για περιπτώσεις DDoS επιθέσεων και αντιμετώπισής τους ύστερα [22]

Ίσως η αποτελεσματικότερη τεχνική για την αντιμετώπιση προηγμένων DDoS επιθέσεων είναι η χρήση Τεχνητών Νευρωνικών Δικτύων (Artificial Neural Networks). Τα Νευρωνικά Δίκτυα είναι πολλές συσκευές συνδεμένες μεταξύ τους, οι οποίες λειτουργούν συλλογικά, όπως ένας νευρώνας, για την επίλυση ενός προβλήματος. Η χρήση επαρκώς εκπαιδευμένων Νεωρωνικών Δικτύων είναι ικανή να διαπιστώσει την ύπαρξη προηγμένων επιθέσεων DDoS σε ελάχιστο χρόνο και να συμβάλλει ικανοποιητικά στην αντιμετώπισή τους. Στην ουσία η εύρεση των DDoS επιθέσεων γίνεται μέσω του φιλταρίσματος των επικεφαλίδων των πακέτων και του διαχωρισμού των νόμιμων (αυθεντικών) πακέτων από τα κατασκευσμένα πακέτα της επίθεσης. Συνεπώς η χρήση τέτοιων μηχανισμών θα ήταν εξαιρετικά αποτελεσματική απέναντι στην επίθεσή μας. Το κύριο μειονέκτημα του συγκεκριμένου μηχανισμού άμυνας είναι ότι θα πρέπει να χρησιμοποιηθεί ένας σχετικά μεγάλος αριθμός από συσκευές ως κομμάτι του Νευρωνικού Δικτύου, οι οποίες στην συνέχεια πρέπει να εκπαιδευτούν επαρκώς σε επίκαιρα δεδομένα (από πρόσφατες επιθέσεις DDoS), ώστε να μπορέσουν να ανιχνεύουν αποτελεσματικά παρόμοιες μελλοντικές επιθέσεις.

6.2 Μελλοντικές Επεκτάσεις

Η επίθεσή μας είναι δυνατό να εξελιχθεί και να γίνει περισσότερο καταστροφική και μη ανιχνεύσιμη από τους μηχανισμούς άμυνας του Διαδικτύου. Ένας από τους τρόπους με τους οποίους θα μπορούσαμε να το επιτύχουμε αυτό είναι η χρήση ενός περισσότερο εξελιγμένου εκτιμητή συμφορήσεων από εκείνον που χρησιμοποιήσαμε στο πλαίσιο αυτής της διπλωματικής (RT-WABest). Συγκεκριμένα, η υλοποίηση μιας ενεργούς εξερεύνησης (active probing), έναντι της άμεσης εξερεύνησης (direct probing) που χρησιμοποιούμε στην επίθεσή μας, σε συνδυασμό με τη χρήση ένος φίλτρου Kalman (Kalman Filter), μπορεί να προσφέρει περισσότερο ακριβείς εκτιμήσεις για την ύπαρξη συμφορήσεων χωρίς επιπλέον επιβάρυνση του δικτύου. Όπως και στην επίθεση CICADAS [2] η συνεχής αποστολή ειδικών probes με ελάχιστο μέγεθος και ύστερα η χρήση του φίλτρου Kalman για την εκτίμηση της επόμενης συμφόρησης στο bottleneck σύνδεσμο από τη διασπορά των πρώτων, συντελούν έναν απο τους αποτελεσματικότερους εκτιμητές συμφορήσεων. Επίσης με τη χρήση της παραπάνω τεχνικής είναι δυνατό να συντονίζονται τα bots χωρίς την ύπαρξη συντονιστών, συμβάλλοντας ακόμα περισσότερο στην μη ανιχνευσιμότητά της επίθεσης. Θα πρέπει όμως να λειφθούν υπόψη και οι περιορισμοί που επιβάλλουν τα ασύρματα δίκτυα, τα οποία χρησιμοποιούμε στο πλαίσιο της επίθεσής μας.

Μία ακόμα πιθανή βελτίωση του εκτιμητή συμφορήσεων θα αποτελούσε η χρήση Νευρωνικών Δικτύων [31] και Fuzzy Δικτύων [32] για την ταχύτερη και αποδοτικότερη εκτίμηση του διαθέσιμου εύρους ζώνης σε ένα από άκρο-σε-άκρο μονοπάτι και κατ' επέκταση την ύπαρξη συμφόρησης σε αυτό. Όπως και στους τρόπους αντιμετώπισης που αναφέρθηκαν προηγουμένως έτσι και σε αυτή την περίπτωση πρέπει να χρησιμοποιηθεί ένας σημαντικός αριθμός από συσκευές (τις οποίες όμως ήδη κατέχει ο επιτιθέμενος) και να γίνει πρώτα εκπαίδευση των δικτύων σε επαρκή δεδομένα πραγματικών σεναρίων. Σε αντίθεση όμως με τους τρόπους αντιμετώπισης, εδώ ο επιτιθέμενος κατέχει και τον χρόνο για

προετοιμασία αλλα και τους πόρους ώστε να υλοποιήσει τα προηγμένα αυτά δίκτυα, αποκτώντας το πλεονέκτημα επί των μηχανισμών άμυνας του Διαδικτύου.

Τέλος η πιθανή προσαρμογή της επίθεσης για τα δίκτυα κινητής τηλεφωνίας (Mobile Networks), είναι δυνατό να την καταστήσει καταστροφική σε βαθμό πολύ μεγαλύτερο από τις πιο σύγχρονες επιθέσεις DDoS που έχουμε συναντήσει μέχρι στιγμής. Η ταχεία ανάπτυξη των κινητών δικτύων, με την ραγδαία αύξηση των ταχυτήτων μεταφοράς δεδομένων (βλ. advanced LTE, 5G), σε συνδυασμό με τη μελλοντική αξιοποίηση πολλαπλών δικτύων, ταυτόχρονα, θα συμβάλλουν στην ανάπτυξη παρόμοιων και ακόμα πιο προηγμένων επιθέσεων DDoS.

Επίλογος

Στο πλαίσιο της παρούσας διπλωματικής σχεδιάστηκε και υλοποιήθηκε μία εξελιγμένη επίθεση κατανεμημένης άρνησης υπηρεσιών (Distributed Denial of Service), σε συστήματα, που συνδέονται ασύρματα στο Διαδίκτυο, μέσω πολλαπλών διεπαφων. Η επίθεση χωρίζεται σε τρία στάδια υλοποίησης, το στάδιο εκκίνησης (Bootstrap Phase), το στάδιο παρακολούθησης (Monitoring Phase) και το στάδιο επίθεσης (Attack Phase).

Ξεκινήσαμε με την περιγραφή της τοπολογίας της επίθεσης και των διαφόρων σταδίων της. Συνεχίσαμε, με την παρουσίαση των σεναρίων, στα οποία ελέγθηκε η επίθεσή μας. Συγκεκριμένα, εξετάσαμε δύο σενάρια 1) για 10 Mbps χωρητικότητα των bottleneck συνδέσμων και 2) για 40 Mbps χωρητικότητα των bottleneck συνδέσμων. Για κάθε ένα από τα σενάρια αυτά έγιναν πειράματα κάνοντας χρήση TCP, UDP και TCP/UDP κίνησης αντίστοιχα.

Τέλος ακολούθησε η αξιολόγηση των πειραμάτων μας. Αναλυτικότερα, παρατηρήσαμε ότι η επίθεση ήταν επιτυχής σε μεγάλο βαθμό για τις παραμέτρους των σεναρίων μας, παρά τους περιορισμούς που μας επέβαλε το περιβάλλον (emulator), στο οποίο εκτελέσθηκαν τα πειράματα. Τα θετικά μας συμπεράσματα ανοίγουν νέους δρόμους για την ανάπτυξη παρόμοιων επιθέσεων στα δίκτυα κινητής τηλεφωνίας.

Βιβλιογραφία

[1] T.S. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Commun. Surveys & Tutorials*, pp. 2046–2069, Vol. 15, No. 4, 4th Quarter, March 2013 .

[2] Y.M. Ke, C.-W. Chen, H.-C. Hsiao, A. Perig and V. Sekar, "CICADAS: Congesting the Internet with Coordinated And Decentralized Pulsating Attacks", *Proc. 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS)*, pp. 669-710, May-June 2016.

[3] M.S. Kang, S.B. Lee and V.D. Gligor, "The Crossfire Attack", *IEEE Symposium on Security and Privacy (SP)*, May 2013.

[4] T. Yang, Y. Jin, Y. Chen, and Y. Jin, "RT-WABest: A Novel End-to-end Bandwidth Estimation Tool in IEEE 802.11 Wireless Network", *Int'l Journal of Distributed Sensor Networks*, Vol. 13, No. 2, 2017.

[5] N. Hu and P. Steenkiste "Estimating Available Bandwidth Using Packet Pair Probing", September 9, 2002

[6] C. Dovrolis, R. Prasad, M. Murray, and k. claffy, "Bandwidth estimation: metrics, measurement techniques, and tools", *IEEE Network*, vol. 17, no. 6, pp. 27–35, Apr 2003.

[7] R.L.Carter and M.E.Crovella "Measuring Bottlenck Link Speed in Packet-Switched Networks", *Performance Evaluation*, vol. 27-28, pp 297–318, Oct. 1996

[8] Sambuddho Chakravarty, Angelos Stavrou, Angelos D. Keromytis, ”LinkWidth: A Method to Measure Link Capacity and Available Bandwidth using Single-End Probes”, *Columbia University Academic Commons*, 2008

[9] Comparison of CORE Network Emulation Platforms, *Proceedings of IEEE MILCOM Conference*, 2010, pp.864-869.

[10] What is a DDoS Attack?
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[11] The DDoS That Knocked Spamhaus Offline
https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

[12] Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

[13] CloudFlare: Hong Kong democracy movement hit by ‘one of largest DDoS attacks in internet history’
https://thenextweb.com/asia/2014/06/20/cloudflare-hong-kong-democracy-movement-battling-one-largest-ddos-attacks-history/

[14] Biggest-Ever DDoS Attack (1.35 Tbs) Hits Github Website
https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

[15] DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS) DEFINITION
https://www.incapsula.com/ddos/ddos-attacks.html

[16] UDP Flood Attacks
https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

[17] SYN Flood Attack
https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

[18] Ping of Death Attack
https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

[19] HTTP Flood Attack
https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

[20] Memcached DDoS Attack
https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/

[21] What is a DDoS Botnet?
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

[22] Gkounis, Dimitrios, Vasileios Kotronis and Xenofontas A. Dimitropoulos. "Towards Defeating the Crossfire Attack using SDN." *CoRR* abs/1412.2013 (2014): n. pag.

[23] Dimitrios Gkounis, Vasileios Kotronis, Christos Liaskos, and Xenofontas Dimitropoulos "On the Interplay of Link-Flooding Attacks and Traffic Engineering" *SIGCOMM Comput. Commun.* Rev. 46, 2, May 2016, 5-11.

[24] Bruce Mechtly and Jack Decker "Using ethereal and TCPportconnect in undergraduate networking labs." *J. Comput. Sci.* Coll. 19, 1, October 2003, 289-298.

[25] Kuzmanovic, Aleksandar and Edward W. Knightly. "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants."*SIGCOMM* (2003).

[26] Guirguis, Mina, Azer Bestavros and Ibrahim Matta. "Exploiting the transients of adaptation for RoQ attacks on Internet resources." *Proceedings of the 12th IEEE International Conference on Network Protocols, 2004.* ICNP 2004. (2004): 184-195.

[27] Nping https://nmap.org/nping/

[28] Quagga Routing Suite https://www.quagga.net/

[29] Farha, A. Ip spoofing. The Internet Protocol Jrn. 10, 4 (2007).

[30] Shin, Seungwon, Phillip A. Porras, Vinod Yegneswaran, Martin W. Fong, Guofei Gu and Mabry Tyson. "FRESCO: Modular Composable Security Services for Software-Defined Networks." *NDSS* (2013).

[31] Eswaradass, Alaknantha, Xian-He Sun and Ming Wu. "A neural network based predictive mechanism for available bandwidth." emph19th IEEE International Parallel and Distributed Processing Symposium (2005): 10 pp.-.

[32] Alzate, Marco A., Jose-Carlos Pagan, Néstor M. Peña and Miguel A. Labrador. "End-to-end bandwidth and available bandwidth estimation in multi-hop IEEE 802.11b ad hoc networks." *2008 42nd Annual Conference on Information Sciences and Systems* (2008): 659-664.