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

Εικονικές Δικτυακές Υπηρεσίες για την Παρακολούθηση και Ασφάλεια Δικτύων Οριζόμενων από Λογισμικό

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Κωνσταντίνος Μ. Γιώτης

Αθήνα, Απρίλιος 2016

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

Εικονικές Δικτυακές Υπηρεσίες για την Παρακολούθηση και Ασφάλεια Δικτύων Οριζόμενων από Λογισμικό

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Κωνσταντίνος Μ. Γιώτης

Συμβουλευτική Επιτροπή : Βασίλειος Μάγκλαρης, Καθηγητής ΕΜΠ
Συμεών Παπαβασιλείου, Καθηγητής ΕΜΠ
Δημήτριος Καλογεράς, Ερευνητής ΕΠΙΣΕΥ 'Β

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την:

.....	.....	.....
Βασίλειος Μάγκλαρης	Συμεών Παπαβασιλείου	Δημήτριος Καλογεράς
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Ερευνητής ΕΠΙΣΕΥ 'Β
.....	.....	.....
Ευστάθιος Συκάς	Νεκτάριος Κοζύρης	Εμμανουήλ Βαρβαρίγος
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ
	.....	
	Ιωάννης Ιωαννίδης	
	Καθηγητής ΕΚΠΑ	

Αθήνα, Απρίλιος 2016

.....
Κωνσταντίνος Μ. Γιώτης

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

Περίληψη

Στα πλαίσια της διδακτορικής διατριβής γίνεται μελέτη και αξιολόγηση των δυνατοτήτων για προγραμματισμό του Επιπέδου Ελέγχου δικτύων μέσω του πρωτοκόλλου OpenFlow (OF), με στόχο την ανίχνευση και αντιμετώπιση κακόβουλων δικτυακών επιθέσεων, όπως οι Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (Distributed Denial of Service – DDoS). Η υπηρεσία αυτή προσφέρεται ως Εικονικοποιημένη Δικτυακή Λειτουργία (Virtualised Network Function – VNF), αποσυνδέοντας την υπηρεσία από τα χαρακτηριστικά της δικτυακής υποδομής.

Στην παρούσα διατριβή, επεκτείνονται διαχειριστικές δικτυακές λειτουργίες, προσφέροντας αποτελεσματικούς και κλιμακώσιμους μηχανισμούς για την ανίχνευση και αντιμετώπιση ανωμαλιών δικτύου. Συγκεκριμένα, αποδεικνύεται πειραματικά ότι η συλλογή και επεξεργασία OF στατιστικών δεδομένων μπορεί να υπερφορτώσει το Επίπεδο Ελέγχου, εισάγοντας έτσι προβλήματα στην διάθεση υπηρεσιών υπό κλίμακα. Έτσι, προτείνεται μία αρχιτεκτονική για την αποσύνδεση της συλλογής στατιστικών δεδομένων από το Επίπεδο Ελέγχου OF μέσω του πρωτοκόλλου sFlow, και την ανάληψη της σχετικής ευθύνης με παραδοσιακούς μηχανισμούς μετρήσεων, συγκεκριμένα με το πρωτόκολλο δειγματοληψίας sFlow, μειώνοντας την κατανάλωση πόρων του Επιπέδου Ελέγχου.

Επιπλέον, διερευνάται η χρήση μεταγωγέων OF ως ενδιάμεσων συσκευών για την αντιμετώπιση επιθέσεων DDoS σε παραδοσιακά δίκτυα. Ως εκ τούτου, προτείνεται μία αρθρωτή αρχιτεκτονική, βασισμένη σε ένα πολυεπίπεδο μηχανισμό ανίχνευσης και αναγνώρισης ανωμαλιών, ικανό να εγκαθιδρύει VNFs για τη χειραγώγηση και απόρριψη της κακόβουλης κίνησης. Ένας συνοριακός δρομολογητής καθοδηγείται ώστε να προωθήσει την κίνηση του θύματος προς έναν μεταγωγέα OF, όπου μπορούν να επιλεχθούν και να αποκοπούν οι κακόβουλες ροές τις οποίες θα αναγνωρίσει ένας Ελεγκτής OF, ενώ η καλοήθης κίνηση επιστρέφει προς το θύμα.

Ακόμη, διερευνείται η δημιουργία συνεργατικών σχημάτων μεταξύ περιοχών Software-Defined Networks (SDN) για την από κοινού αντιμετώπιση κατανεμημένων επιθέσεων. Συγκεκριμένα κατανέμεται η ίδια η διαδικασία αντιμετώπισης επιθέσεων, εκκινώντας από την δικτυακή περιοχή-θύμα και εμπλέκοντας όλες τις ενδιάμεσες περιοχές στο μονοπάτι της επίθεσης. Για την υλοποίηση της συνεργατικής λειτουργίας περιοχών ανεξάρτητων Αυτόνομων Συστημάτων, προτείνεται ένας μηχανισμός φήμης (reputation) μέσω του οποίου οι περιοχές SDN αξιολογούν τους γείτονες, αποτρέποντας τη συνεργασία εάν η περιοχή-θύμα έχει επιδείξει έλλειψη συνεργασίας.

Η αξιολόγηση των μηχανισμών βασίστηκε σε διαφορετικές τεχνικές ανίχνευσης ανωμαλιών, ενώ χρησιμοποιήθηκαν πραγματικά δεδομένα δικτύου που παρείχε το Center for Applied Internet Data Analysis (CAIDA) και το Τοπικό Δίκτυο του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ).

Λέξεις Κλειδιά

Δίκτυα Οριζόμενα από Λογισμικό (SDN), OpenFlow, Ανίχνευση Ανωμαλιών Δικτύου, Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (DDoS), Παρακολούθηση Δικτύου, sFlow, Εικονικοποίηση Δικτυακών Λειτουργιών (NFV)

Abstract

In this work we study and evaluate the Control Plane programmability offered by the OpenFlow protocol (OF), in order to detect and mitigate malicious network anomalies such as Distributed Denial of Service (DDoS) attacks. This service is offered as a Virtualized Network Function (VNF), thus decoupling the function itself from the capabilities of the hardware substrate.

In the present thesis, traffic management functionalities are extended, thus delivering efficient and scalable mechanisms for anomaly detection and mitigation. Specifically, we demonstrate that OF statistics collection and processing overloads the centralized OF Controller, introducing scalability issues. Hence, we propose an approach for the separation of the data collection process from the SDN Control Plane with the employment of sFlow monitoring data, thus relaxing the overhead imposed on usage of system resources.

Furthermore, we investigate the applicability of inserting an OpenFlow middlebox to mitigate DDoS attacks in legacy networks. We propose a modular architecture, based on a multilevel anomaly detection and identification mechanism, capable of deploying a VNF to manipulate and filter malicious traffic. The edge router is instructed to forward all traffic destined to the victim to an OpenFlow switch that is able to filter only malicious traffic identified by an OpenFlow Controller on a per-flow level, while benign flows are preserved.

Moreover, we investigate collaborative schemes to mitigate DDoS attacks in multi-domain Software-Defined Networks (SDNs). The mitigation process itself is distributed, initiated by the domain of the victim, and involving all domains in the path of an attack. In order to motivate close cooperation of SDN domains governed by diverse authorities, we implemented and evaluated a reputation mechanism, whereby domains assess the historical behavior of their neighbors, discouraging assistance in case the domain of the victim has a poor cooperation track-record.

The evaluation of the proposed mechanisms is achieved through the use of different anomaly detection techniques and real network data provided by the Center for applied Internet Data Analysis (CAIDA), and by the National Technical University of Athens (NTUA).

Keywords

Software-Defined Networks (SDN), OpenFlow, Network Anomaly Detection, DDoS Attacks, Network Monitoring, sFlow, Network Function Virtualisation (NFV)

Ευχαριστίες

Ολοκληρώνοντας το τελευταίο αυτό στάδιο των διδακτορικών μου σπουδών, είναι ανάγκη να ευχαριστήσω τους ανθρώπους που με βοήθησαν και μου συμπαραστάθηκαν όλα αυτά τα χρόνια. Τόσο ανθρώπους του συγγενικού και φιλικού μου περιβάλλοντος, όσο και ανθρώπους από τον ακαδημαϊκό χώρο, με τους οποίους συνεργαστήκαμε, και περάσαμε ημέρες μόχθου και κούρασης, αλλά και ημέρες χαράς και δημιουργικότητας.

Θα ήθελα να ευχαριστήσω μέσα από την καρδιά μου τον επιβλέποντα καθηγητή μου κ. Βασίλη Μάγκλαρη για την ουσιαστική και παραγωγική υποστήριξη που μου προσέφερε, από το διάστημα που ήμουν ακόμη προπτυχιακός φοιτητής του Εθνικού Μετσόβιου Πολυτεχνείου, μέχρι και σήμερα. Ως επιβλέπων καθηγητής της διπλωματικής μου εργασίας, παρείχε κατευθύνσεις και με οδήγησε σε ερευνητικές περιοχές οι οποίες αποτέλεσαν τα θεμέλια για τη μετέπειτα ερευνητική μου πορεία. Κυρίως όμως, του οφείλω ένα μεγάλο ευχαριστώ, αφενός για την εμπιστοσύνη που μου έδειξε όταν με δέχθηκε ως υποψήφιο διδάκτορα στο εργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων (NETMODE), και αφετέρου για τον προσωπικό κόπο και χρόνο που προσέφερε, όποτε αυτό χρειάστηκε στη διάρκεια της διδακτορικής μου διατριβής.

Επίσης, ευχαριστώ τον καθηγητή κ. Συμεών Παπαβασιλείου και τον Δρα Δημήτρη Καλογερά για την άψογη συνεργασία και τις εποικοδομητικές συζητήσεις που είχαμε όλα αυτά τα χρόνια· συζητήσεις οι οποίες άλλες φορές αποτέλεσαν τον σπόρο μιας νέας ερευνητικής εργασίας, και άλλες φορές τροφή για σκέψη, προβληματισμό, και ουσιαστική εξέλιξη.

Βέβαια, η πορεία της διδακτορικής μου διατριβής θα ήταν πιο δύσβατη, εάν δεν υπήρχε η άψογη συνεργασία και με τα υπόλοιπα μέλη του εργαστηρίου NETMODE. Ανάμεσά τους πρέπει να ξεχωρίσω τον Δρα Γιώργο Ανδρουλιδάκη και τον Δρα Χρήστο Αργυρόπουλο, των οποίων οι οδηγίες και κατευθύνσεις ήταν καταλυτικής σημασίας στο ταξίδι αυτό. Σημαντική ακόμη ήταν η υποστήριξη που δέχθηκα από τη Δρ. Μαίρη Γραμματικού, όπως και η συνεργασία που είχα με άλλα μέλη του εργαστηρίου όπως η Δρ Χρύσα Παπαγιάννη, ο Θανάσης Δουίτσης, ο Γιάννος Κρύφτης και ο Αδάμ Παυλίδης.

Για το τέλος, οφείλω ένα θερμό ευχαριστώ στους γονείς μου, την αδερφή, τους φίλους μου, και βεβαίως τη σύντροφο και συνοδοιπόρο μου, για την ανεκτίμητη υποστήριξη και φροντίδα που μου έχουν προσφέρει. Τους αγαπώ και τους ευχαριστώ μέσα από την καρδιά μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Εισαγωγή 11
2 Δίκτυα Νέας Γενιάς (Future Internet Networks) 18
2.1 Δίκτυα Επικάλυψης μέσω Νέων Πρωτοκόλλων Ενθυλάκωσης Πλαισίων 20
2.2 Δίκτυα Οριζόμενα από Λογισμικό (Software-Defined Networks) 21
2.2.1 Πρωτόκολλο OpenFlow (OpenFlow Protocol) 23
2.3 Εικονικοποίηση Δικτυακών Λειτουργιών 28
3 Παρακολούθηση Δικτυακής Κίνησης 30
3.1 Μέθοδοι και Πρωτόκολλα Παρακολούθησης Δικτυακής Κίνησης 30
3.1.1 Το πρωτόκολλο SNMP 30
3.1.2 Έλεγχος του εσωτερικού των πακέτων (Deep Packet Inspection) 31
3.1.3 Το πρωτόκολλο NetFlow 31
3.1.4 Το πρωτόκολλο sFlow 32
3.2 Παρακολούθηση δικτυακής κίνησης σε Δίκτυα Οριζόμενα από Λογισμικό 33
4 Ανίχνευση και Αντιμετώπιση Ανωμαλιών Δικτύου 36
4.1 Εμπορικές Υπηρεσίες Αντιμετώπισης Δικτυακών Επιθέσεων DDoS 36
4.2 Μέθοδοι Ανίχνευσης Ανωμαλιών Δικτύου 38
4.3 Ανίχνευση Ανωμαλιών Δικτύου σε Δίκτυα Οριζόμενα από Λογισμικό 39
4.4 Αντιμετώπιση Ανωμαλιών Δικτύου 40
4.5 Συνεργασία Αυτόνομων Συστημάτων για Αντιμετώπιση Ανωμαλιών Δικτύου 42
5 Ανίχνευση και Αντιμετώπιση Ανωμαλιών σε Περιβάλλοντα SDN 44
5.1 Εισαγωγή 44
5.2 Σχεδιαστικές Αρχές και Περιγραφή Αρχιτεκτονικής 45
5.2.1 Σχεδιαστικές αρχές 45
5.2.2 Αρχιτεκτονικά στοιχεία 47
5.3 Συλλογή Δεδομένων για Ανίχνευση και Αντιμετώπιση Ανωμαλιών σε SDNs 50
5.3.1 Συλλογή στατιστικών δεδομένων για ροές πακέτων σε SDN 50
5.3.2 Ανίχνευση και χαρακτηρισμός δικτυακών ανωμαλιών μέσω Εντροπίας 53
5.3.3 Αναγνώριση θύματος/θύτη και αντιμετώπιση δικτυακών επιθέσεων 56
5.4 Μεθοδολογία – Αποτελέσματα 57
5.4.1 Πειραματική τοπολογία και λεπτομέρειες υλοποίησης 58
5.4.2 Καταγραφή και αναπαραγωγή πραγματικής δικτυακής κίνησης 60
5.4.3 Πειράματα ανίχνευσης ανωμαλιών μέσω προσομοίωσης 61
5.4.4 Αντιμετώπιση ανωμαλιών σε δίκτυα SDN 71
6 Κλιμακώσιμη Αντιμετώπιση Ανωμαλιών σε Παραδοσιακά Δικτυακά Περιβάλλοντα μέσω πρωτοκόλλου OpenFlow 74
6.1 Εισαγωγή 74
6.2 Σχεδιαστικές Αρχές και Περιγραφή Αρχιτεκτονικής 75
6.2.1 Σχεδιαστικές αρχές 75
6.2.2 Αρχιτεκτονικά στοιχεία 78
6.3 Αναλυτική Περιγραφή Κύριων Δομικών Στοιχείων 81
6.3.1 Αλγόριθμοι ανίχνευσης και αναγνώρισης ανωμαλιών 81
6.3.2 Μέθοδος RTBH για την αναδρομολόγηση ύποπτης δικτυακής κίνησης 86
6.3.3 Αντιμετώπιση επιθέσεων DDoS 89
6.3.4 Κλιμακώσιμη αντιμετώπιση ανωμαλιών με συνάθροιση κακόβουλων ροών 91
6.4 Αξιολόγηση και Πειραματικά Αποτελέσματα 95

6.4.1 Πειραματική διάταξη ... 96
6.4.2 Αξιολόγηση πολυεπίπεδης προσέγγισης ανίχνευσης επιθέσεων DDoS ... 98
7 Αντιμετώπιση Κατανεμημένων Επιθέσεων σε Ευφυή Προγραμματιζόμενα Δίκτυα μέσω Συνεργατικών Σχημάτων Βασισμένων στη Φήμη ... 106
7.1 Εισαγωγή ... 106
7.2 Γενική Αρχιτεκτονική ... 107
7.2.1 Περιγραφή προτεινόμενης προσέγγισης ... 107
7.2.2 Δομικά στοιχεία εφαρμογής για το Επίπεδο Ελέγχου ... 110
7.3 Συνεργατικά Σχήματα Φήμης για Αντιμετώπιση Κατανεμημένων Επιθέσεων ... 112
7.3.1 Μηχανισμός φήμης μεταξύ ευφυών δικτυακών περιοχών ... 112
7.3.2 Διάδοση και ανάλυση αναφορών κατανεμημένων επιθέσεων ... 115
7.3.3 Συνδυασμός BGP και SDNi για την διάδοση αναφορών επιθέσεων DDoS ... 116
7.4 Αξιολόγηση Προτεινόμενης Προσέγγισης ... 117
7.4.1 Αξιολόγηση σε περιβάλλον περιορισμένης κλίμακας ... 119
7.4.2 Υλοποίηση περιβάλλοντος προσομοίωσης και πειράματα μεγάλης κλίμακας ... 121
8 Συμπεράσματα - Μελλοντική Έρευνα ... 125
8.1 Συμπεράσματα ... 125
8.2 Θέματα Μελλοντικής Έρευνας ... 128
9 Δημοσιεύσεις ... 130
9.1 Διεθνή Επιστημονικά Περιοδικά με Κρίση ... 130
9.2 Πρακτικά Διεθνών Επιστημονικών Συνεδρίων με Κρίση ... 130
10 Βιβλιογραφία ... 132

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1: Αναλογία Εικονικοποίησης Υπολογιστικών και Δικτυακών Πόρων **19**
Σχήμα 2: Ένας OpenFlow μεταγωγέας επικοινωνεί με έναν OF Controller μέσω ασφαλούς σύνδεσης (secure channel) χρησιμοποιώντας το πρωτόκολλο OpenFlow. **24**
Σχήμα 3: Επισκόπηση των κύριων δομικών στοιχείων μίας αρχιτεκτονικής NFV **29**
Σχήμα 4: Ενδεικτική αρχιτεκτονική του sFlow: sFlow Agents και Collector. **33**
Σχήμα 5: Αρχιτεκτονική άποψη του προτεινόμενου συστήματος για περιβάλλοντα SDN. **45**
Σχήμα 6: Μεταβολή της εντροπίας των πεδίων srcIP, dstIP, srcPort, dstPort των επικεφαλίδων των πακέτων, κατά τη διάρκεια μίας επίθεσης τύπου DDoS. 55
Σχήμα 7: Κύρια δομικά στοιχεία της προτεινόμενης αρχιτεκτονικής για ανίχνευση και αντιμετώπιση δικτυακών ανωμαλιών για τις περιπτώσεις: (α) Εγγενούς OF μεθόδου συλλογής δεδομένων, και (β) μεθόδου συλλογής δεδομένων βασισμένη στο πρωτόκολλο sFlow. **60**
Σχήμα 8: Υπολογισμός της μεταβολής της εντροπίας μέσω (α) της εγγενούς OpenFlow μεθόδου, και (β) κάνοντας χρήση του πρωτοκόλλου sFlow **63**
Σχήμα 9: Καμπύλες ROC για την ανίχνευση επιθέσεων DDoS, Worm Propagation και Port Scanning μέσω μεταβολής της εντροπίας, κάνοντας χρήση στατιστικών δεδομένων που συλλέχθηκαν (α) μέσω της εγγενούς OF μεθόδου, και (β) μέσω του πρωτοκόλλου sFlow. **64**
Σχήμα 10: (α) Καμπύλες ROC για τα πειράματα που πραγματοποιήθηκαν σε κίνηση 100 Mbps, (β) Καμπύλες ROC για τα πειράματα που πραγματοποιήθηκαν σε κίνηση 500 Mbps. **65**
Σχήμα 11: Καμπύλες ROC για την απόδοση του αλγορίθμου TRW-CB χρησιμοποιώντας δεδομένα από την εγγενή OF μέθοδο συλλογής και μέσω του πρωτοκόλλου sFlow, υπό συνθήκες: (a) Επιθέσεων Port Scanning, και (b) Επιθέσεων Worm Propagation. **68**
Σχήμα 12: Απεικόνιση της μεταβολής της εντροπίας χαρακτηριστικών μεγεθών κατά τη διάρκεια επιθέσεων: (a) DDoS, (b) Worm Propagation, και (c) Port Scanning, με χρήση (κόκκινο) και χωρίς χρήση (μπλε) του μηχανισμού Ανίχνευσης Ανωμαλιών. **72**
Σχήμα 13: Προτεινόμενη αρχιτεκτονική αντιμετώπισης δικτυακών επιθέσεων σε παραδοσιακά περιβάλλοντα, με χρήση μεταγωγέα OpenFlow ως ενδιάμεσο **75**
Σχήμα 14: Γενική επισκόπηση των κύριων στοιχείων που αποτελούν την προτεινόμενη αρχιτεκτονική προσέγγιση. **78**
Σχήμα 15: Γραφική απεικόνιση της BCS δομής δεδομένων, βασισμένη στις δομές τύπου *K*-ary Sketch. **83**
Σχήμα 16: Ενδεικτικό παράδειγμα χρήσης Φίλτρου Bloom με $m=50$ και $k=3$. **85**
Σχήμα 17: Παραδοσιακή μέθοδος Remotely Triggered Black Hole (RTBH) **87**
Σχήμα 18: Προτεινόμενη προσέγγιση για τη βελτίωση της μεθόδου RTBH **88**
Σχήμα 19: Κύρια δομικά στοιχεία της προτεινόμενης αρχιτεκτονικής προσέγγισης για την προστασία εξυπηρετητών από DDoS επιθέσεις σε παραδοσιακά δίκτυα, με χρήση ενδιάμεσου μεταγωγέα OpenFlow. **97**
Σχήμα 20: Καμπύλες ROC των αλγορίθμων πρώτου και δεύτερου επιπέδου ανίχνευσης δικτυακών ανωμαλιών **100**
Σχήμα 21: Διακύμανση της εντροπίας των Διευθύνσεων IP προορισμού και Θυρών Μεταφοράς προορισμού **101**
Σχήμα 22: Ανίχνευση επίθεσης DDoS μέσω του αλγορίθμου BCS **102**
Σχήμα 23: Μέσος αριθμός πακέτων που λαμβάνονται (μπλε) και αποστέλλονται (κόκκινο) από το θύμα προς τις πηγές της επίθεσης. Ο λόγος ληφθέντων προς απεσταλμένων πακέτων φθάνει έως και 31:1. ..... **103**

Σχήμα 24: Κατανομή των κακόβουλων διευθύνσεων IP που βρίσκονται στο CAIDA DDoS Attack 2007 Dataset, στον IPv4 χώρο. **104**
Σχήμα 25: Κατανομή των κακόβουλων πακέτων σε /24 δίκτυα..... **104**
Σχήμα 26: Αφαιρετική απεικόνιση του προτεινόμενου συνεργατικού μηχανισμού για την αποκοπή κατανεμημένων επιθέσεων..... **108**
Σχήμα 27: Επιμέρους μονάδες οι οποίες συνθέτουν τον μηχανισμό αντιμετώπισης κατανεμημένων επιθέσεων CAMM **110**
Σχήμα 28: Σχηματική απεικόνιση των κυριότερων κλάσεων του προτύπου IODEF **116**
Σχήμα 29: Σχηματική απεικόνιση υψηλού επιπέδου της συλλογής δεδομένων CAIDA AS Relationships Dataset, από όπου αντλήθηκαν δεδομένα για την προσομοίωση τοπολογιών μεγάλης κλίμακας. **118**
Σχήμα 30: Πρώτο σενάριο αξιολόγησης συνεργατικού μηχανισμού: αντιμετώπιση κατανεμημένης επίθεσης από δύο γειτονικά SDN domain. **119**
Σχήμα 31: Αριθμός άφιξης πακέτων ανά δευτερόλεπτο στο θύμα, κατά τη διάρκεια της κατανεμημένης επίθεσης. **120**
Σχήμα 32: Δεύτερο σενάριο αξιολόγησης συνεργατικού μηχανισμού: εξομοίωση συνεργατικής αντιμετώπισης κατανεμημένων επιθέσεων σε τοπολογίες μεγάλης κλίμακας, αποτελούμενες από χιλιάδες SDN domains. **122**
Σχήμα 33: Αριθμός εγγραφών στον συνοριακό μεταγωγέα Openflow του SDN domain που εξυπηρετεί το θύμα μίας επίθεσης DDoS, ανάλογα με το ποσοστό των γειτονικών SDN domains που συνεισφέρουν στην αντιμετώπιση της επίθεσης αυτής. **123**

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1: Ένα σύνολο πεδίων επικεφαλίδων, μετρητών και ενεργειών αποτελούν μια εγγραφή του πίνακα ροών ενός μεταγωγέα OF..... **24**
Πίνακας 2: Πληροφορίες που αποτελούν κριτήριο για την αντιστοίχιση ενός πακέτου με μία συγκεκριμένη εγγραφή του πίνακα ροών ενός μεταγωγέα OF. **25**
Πίνακας 3: Λίστα με τους διαθέσιμους μετρητές. **25**
Πίνακας 4: Σύνολο των Actions που μπορεί να υποστηρίζονται από έναν μεταγωγέα OpenFlow. **26**
Πίνακας 5: Πεδία των επικεφαλίδων των πακέτων τα οποία χρησιμοποιούνται για την αντιστοίχιση ενός πακέτου με μία OpenFlow εγγραφή στον πίνακα ροών ενός μεταγωγέα OF. **48**
Πίνακας 6: Παράδειγμα εγγραφών στον πίνακα ροών ενός μεταγωγέα OF για την υλοποίηση μίας δικατευθυντικής επικοινωνίας. **50**
Πίνακας 7: Κατηγοριοποίηση κακόβουλων δικτυακών ανωμαλιών βάσει της μεταβολής της εντροπίας. **54**
Πίνακας 8: Χαρακτηριστικές παράμετροι πειραμάτων που διεξήχθησαν. **62**
Πίνακας 9: Σύγκριση της επεξεργαστικής ισχύς και του αριθμού εγγραφών ροών που απαιτούνται από έναν μεταγωγέα OF για συλλογή δεδομένων μέσω της sFlow μεθόδου και μέσω της εγγενούς OF μεθόδου, χρησιμοποιώντας και συγκρίνοντας τα αποτελέσματα για πολλαπλές μεθόδου. **69**
Πίνακας 10: Σύγκριση της κατανάλωσης επεξεργαστικής ισχύος του OF Controller όταν χρησιμοποιείται η sFlow μέθοδος συλλογής δεδομένων και όταν χρησιμοποιείται η εγγενής μέθοδος του πρωτοκόλλου OpenFlow. Η σύγκριση αυτή πραγματοποιείται κάνοντας χρήση πολλαπλών μεθόδων ανίχνευσης..... **70**
Πίνακας 11: Ενδεικτική μορφή των εγγραφών στον πίνακα ροών ενός μεταγωγέα OF, για την αποκοπή διαφορετικών τύπων δικτυακών ανωμαλιών. **73**
Πίνακας 12: Παράδειγμα εγγραφών ροών οι οποίες εγκαθιδρύονται για την επαναπροώθηση της κανονικής κίνησης (Σειρά Β), και την απόρριψη μιας συγκεκριμένης κακόβουλης ροής (Σειρά Μ). **90**
Πίνακας 13: Σύγκριση τριών αλγορίθμων ανίχνευσης δικτυακών ανωμαλιών, σε όρους κατανάλωσης πόρων συστήματος και ακρίβειας ανίχνευσης. **99**
Πίνακας 14: Αντιστάθμιση αριθμού εγγραφών για την αποκοπή κακόβουλων ροών και παράπλευρων απωλειών κατά τη χρήση του αλγορίθμου *Block-All*..... **105**

1 Εισαγωγή

Οι διαχειριστές των Κέντρων Δεδομένων (Data Centers) και των παρόχων Υπηρεσιών Νέφους (Cloud Services) έχουν πλέον αυξημένες απαιτήσεις όσον αφορά την εγκαθίδρυση και παραμετροποίηση ενός προγραμματιζόμενου δικτυακού περιβάλλοντος. Ταυτόχρονα, οι παραδοσιακές αρχιτεκτονικές αποδεικνύεται ότι δυσχεράνουν τόσο την καινοτομία, όσο και τις διαδικασίες διαχείρισης και παραμετροποίησης των δικτυακών συσκευών. Επιπλέον, κατασκευαστές δικτυακών συσκευών προσφέρουν κλειστά πρωτόκολλα και λογισμικές διεπαφές (software interfaces) για την επικοινωνία μεταξύ του Επιπέδου Ελέγχου και του Επιπέδου Δεδομένων των συσκευών. Η πρακτική αυτή τείνει να περιορίζει τους διαχειριστές δικτύων, οι οποίοι εγκλωβίζονται στη χρήση πρωτοκόλλων τα οποία δεν υποστηρίζονται από όλους τους κατασκευαστές, αφού δεν είναι προτυποποιημένα.

Τα Δίκτυα Οριζόμενα από Λογισμικό (Software-Defined Networks – SDN) [1] εμφανίζονται ως μία υποσχόμενη, εναλλακτική αρχιτεκτονική δικτύων, όπου τα Επίπεδα Ελέγχου και Δεδομένων είναι πλήρως διαχωρισμένα. Διαδικασίες οι οποίες σχετίζονται τόσο με την ευφυΐα των δικτυακών συσκευών, όσο και την κατάσταση της συνολικής δικτυακής υποδομής, μπορούν να προσφέρονται στους διαχειριστές ως λογικά κεντρικοποιημένες μέθοδοι [2]. Το πρωτόκολλο OpenFlow (OF) [1], ως μία από τις πιο διαδεδομένες μεθόδους δημιουργίας ευφυών προγραμματιζόμενων δικτύων, επιτρέπει τον προγραμματισμό του Επιπέδου Ελέγχου του δικτυακού υποστρώματος μέσω κεντρικών εφαρμογών λογισμικού.

Ανάμεσα στα κυριότερα πλεονεκτήματα των δικτύων SDN συγκαταλέγονται: (α) η επιβολή πολιτικών προώθησης μέσω δυναμικού καθορισμού συγκεκριμένων δικτυακών ροών δεδομένων (network flows), και (β) η δυνατότητα που προσφέρεται σε έναν κεντρικό Ελεγκτή (Controller) να έχει πλήρη εικόνας της κατάστασης του δικτύου σε πραγματικό χρόνο. Συνεπώς, μέσω του πρωτοκόλλου OF καθίσταται δυνατός ο προγραμματιστικός έλεγχος πλήθους Δικτυακών Λειτουργιών (Network Functions - NFs) οι οποίες σχετίζονται άμεσα με τον έλεγχο των ροών δεδομένων. Χαρακτηριστικά παραδείγματα τέτοιων λειτουργιών αποτελούν: (α) η διαχείριση κίνησης (traffic management), (β) η ισοκατανομή φορτίου (load-balancing), (γ) η δρομολόγηση (routing) και (δ) η διαχείριση πύρινου τείχους (firewall).

Ταυτόχρονα, η συνεχής αύξηση των απαιτήσεων των χρηστών όσον αφορά τον διακινούμενο όγκο δεδομένων και την ποιότητα των προσφερόμενων υπηρεσιών, οδήγησε τους παρόχους υπηρεσιών δικτύου στην ανάγκη για επιτάχυνση των διαδικασιών εγκατάστασης, παραμετροποίησης και υποστήριξης των προσφερόμενων Δικτυακών Λειτουργιών. Στα παραδοσιακά δικτυακά περιβάλλοντα, τέτοιες λειτουργίες είναι άρρηκτα συνδεδεμένες με τις αντίστοιχες δικτυακές συσκευές, κάθε μία από τις οποίες υλοποιεί και προσφέρει μία συγκεκριμένη Δικτυακή Λειτουργία. Προκειμένου να ξεπεραστούν οι περιορισμοί και η ανελαστικότητα των υλοποιημένων-μέσω-εξοπλισμού Δικτυακών Λειτουργιών, οι πάροχοι επέλεξαν την ενσωμάτωση κλασσικών τεχνικών εικονικοποίησης στο επίπεδων των δικτυακών υπηρεσιών, επιδιώκοντας την προσφορά Δικτυακών Λειτουργιών μέσω λογισμικού. Αν και το πρωτόκολλο OF προσφέρει δυνατότητες κεντρικής διαχείρισης μέσω λογισμικού, η υλοποίηση των Δικτυακών Λειτουργιών μέσω λογισμικού απαιτεί το συνδυασμό και την ελαστική διαχείριση τόσο δικτυακών, όσο και υπολογιστικών και αποθηκευτικών πόρων.

Οι ανάγκες των παρόχων για πλήρη αποσυσχέτιση των υπηρεσιών από τη δικτυακή υποδομή οδήγησε στην Εικονικοποίηση Δικτυακών Λειτουργιών (Network Function Virtualisation – NFV) [3]. Βασικό χαρακτηριστικό της αρχιτεκτονικής NFV αποτελεί η ύπαρξη ενός επιπέδου εικονικοποίησης (Virtualisation Layer), μέσω του οποίου φυσικοί υπολογιστικοί, αποθηκευτικοί και δικτυακοί πόροι της υποδομής χρησιμοποιούνται για τη δημιουργία Εικονικοποιημένων Δικτυακών Λειτουργιών (Virtualised Network Functions – VNFs).

Μία χαρακτηριστική εφαρμογή η οποία μπορεί να επωφεληθεί των συνεργειών που προκύπτουν μέσω του συνδυασμού πρωτοκόλλων SDN και NFV αρχιτεκτονικής, αποτελεί η προστασία της υποδομής από δικτυακές επιθέσεις. Ιδιαίτερη σημασία δίνεται πλέον στην αντιμετώπιση Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας (DDoS) , οι οποίες επιδιώκουν να επηρεάσουν την ομαλή λειτουργία δημόσιων (για τον Internet) υπηρεσιών. Το πλήθος και όγκος κίνησης των επιθέσεων DDoS έχει αυξηθεί δραματικά, ιδιαίτερα όταν συγκεκριμένες επιθέσεις εκμεταλλεύονται αδυναμίες ευρέως διαδεδομένων πρωτοκόλλων (π.χ. DNS, NTP). Ως αποτέλεσμα, κάθε κακόβουλο πακέτο προκαλεί απάντηση πολλαπλάσιου όγκου (Amplification DDoS Attack [4]), αυξάνοντας δραματικά τον συνολικό όγκο της επίθεσης, και επηρεάζοντας τόσο την απόδοση του θύματος, όσο και της δικτυακής υποδομής η οποία φιλοξενεί το θύμα. Συνεπώς, οι παραδοσιακές λύσεις για την αντιμετώπιση επιθέσεων DDoS συχνά αδυνατούν να αντιμετωπίσουν έγκαιρα και αποτελεσματικά τέτοιες επιθέσεις.

Ένας από τους βασικούς στόχους της συγκεκριμένης διατριβής είναι να μελετηθεί και να αξιολογηθεί η δυνατότητα συνδυασμού χαρακτηριστικών του πρωτοκόλλου OpenFlow και της NFV προσέγγισης, με στόχο την ανίχνευση και αντιμετώπιση δικτυακών επιθέσεων με τρόπο αποδοτικό και ταυτόχρονα κλιμακώσιμο. Η συνολική λειτουργία ενός μηχανισμού προστασίας της υποδομής ενάντια σε δικτυακές επιθέσεις, μπορεί να διαχωριστεί σε τρεις επιμέρους διαδικασίες: (α) τη συλλογή στατιστικών δεδομένων όσον αφορά τις δικτυακές ροές δεδομένων, (β) την ανίχνευση και αναγνώριση δικτυακών ανωμαλιών, και (γ) την αντιμετώπιση των ανιχνευμένων ανωμαλιών. Στα πλαίσια της παρούσας διατριβής, έμφαση δίνεται αφενός στις μεθόδους συλλογής στατιστικών δεδομένων δικτύου, και αφετέρου στην αποτελεσματική προστασία παραδοσιακών και SDN δικτύων από κατανεμημένες επιθέσεις τύπου DDoS, διαφυλάσσοντας την προσβασιμότητα και λειτουργικότητα του θύματος.

Συγκεκριμένα, πρώτος στόχος της διατριβής είναι η υλοποίηση και αξιολόγηση πρωτότυπου μηχανισμού για την προστασία SDN δικτύων, σε πραγματικό χρόνο, από επιθέσεις τύπου DDoS, Διάδοσης Κακόβουλου Λογισμικού (Worm Outbreaks), και Ανίχνευσης Δικτυακών Υπηρεσιών (Port Scanning). Η διαδικασία ανίχνευσης δικτυακών ανωμαλιών στηρίζεται σε στατιστικά δεδομένα τα οποία συλλέγονται από τη δικτυακή υποδομή, και αφορούν τις υπάρχουσες ροές δεδομένων (flows) σε αντίστοιχα (σταθερού μεγέθους) χρονικά διαστήματα. Η ανίχνευση ανωμαλιών βάσει των στατιστικών των ροών δεδομένων σε παραδοσιακές δικτυακές υποδομές, έχει αποδειχθεί ικανή στην αναγνώριση διαφόρων μορφών ανωμαλιών της δικτυακής κίνησης [5], [6], [7]. Όσον αφορά τα δίκτυα SDN, εξαιρετικά σημαντική κρίνεται η μέθοδος με την οποία συλλέγονται τα απαραίτητα στατιστικά δεδομένα, και ιδιαίτερα (α) η επίδραση της κάθε μεθόδου στη διαδικασία ανίχνευσης ανωμαλιών, και (β) η δυνατότητα συλλογής δεδομένων υπό κλίμακα.

Έτσι, υλοποιήθηκαν και αξιολογήθηκαν δύο διαφορετικές προσεγγίσεις για την παρακολούθηση της δικτυακής κίνησης. Η πρώτη, αφορά τη συλλογή δεδομένων μέσω της εγγενούς μεθόδου που προσφέρει το πρωτόκολλο OpenFlow, και υλοποιείται μέσω περιοδικής εξαγωγής όλων των μετρητών οι οποίοι είναι συσχετισμένοι με κάθε ροή OpenFlow (όπως αυτές διατηρούνται στους πίνακες ροών των μεταγωγέων OpenFlow). Η δεύτερη προσέγγιση υιοθετεί το πρωτόκολλο sFlow [8] για τη δειγματοληψία των επικεφαλίδων των πακέτων και την περιοδική αντιστοίχισή τους με τις εγγραφές στους πίνακες ροών των μεταγωγέων OpenFlow, στοχεύοντας σε μία πιο κλιμακώσιμη λύση. Τα δεδομένα τα οποία συλλέγονται σε κάθε περίπτωση, χρησιμοποιούνται για την τροφοδοσία ενός αλγορίθμου ανίχνευσης ανωμαλιών βασισμένου στη μεταβολή της εντροπίας

συγκεκριμένων χαρακτηριστικών των επικεφαλίδων πακέτων (π.χ. Διεύθυνση IP πηγής/προορισμού, Θύρα μεταφοράς πηγής/προορισμού). Μέσω της διαδικασίας αυτής, αξιολογείται η επίδραση των επιλεγμένων μεθόδων συλλογής δεδομένων στη διαδικασία ανίχνευσης ανωμαλιών (π.χ. ακρίβεια ανίχνευσης, ποσοστό ψευδών-αληθών αναφορών, κλπ.). Επιπλέον, ο προτεινόμενος μηχανισμός εκμεταλλεύεται την εγγενή δυνατότητα του πρωτοκόλλου OF για δυναμική μεταβολή (μέσω λογισμικού) των εγγραφών στου πίνακες ροών ενός μεταγωγέα OF, στοχεύοντας στην αποκοπή της δικτυακής κίνησης η οποία σχετίζεται με τυχόν ανιχνευθείσες ανωμαλίες. Ως αποτέλεσμα, προκύπτει μία δικτυακή υπηρεσία τύπου VNF, ικανή να αναγνωρίσει ανωμαλίες σε πραγματικό χρόνο, και να αποτρέψει την εξάπλωσή τους στο εσωτερικό της δικτυακής υποδομής.

Επίσης, προτείνεται και μελετείται μια αρθρωτή και κλιμακώσιμη αρχιτεκτονική, η οποία βασίζεται στη χρήση ενδιάμεσων μεταγωγέων OF σε παραδοσιακά δικτυακά περιβάλλοντα, και στοχεύει στην απόρριψη κακόβουλων πηγών επιθέσεων τύπου DDoS. Η ανίχνευση των δικτυακών ανωμαλιών στηρίζεται σε ένα μηχανισμό δύο επιπέδων, για βελτιστοποίηση της διαχείρισης των πόρων συστήματος. Παράλληλα προτείνεται και αξιολογείται μία μέθοδος για τη δυναμική αναδρομολόγηση του συνόλου των ροών (οι οποίες προορίζονται για το θύμα της επίθεσης DDoS) προς έναν μεταγωγέα OF. Στη συνέχεια, ο Ελεγκτής του μεταγωγέα (OpenFlow Controller) αναλαμβάνει να διαχωρίσει και να αποκόψει τις κακόβουλες ροές, και να αναδρομολογήσει τις καλοήθεις ροές προς τον αρχικό τους προορισμό. Κρίσιμο ζήτημα στη συγκεκριμένη προσέγγιση αποτέλεσε η κλιμακωσιμότητά της, η οποία σχετίζεται άμεσα με τη χωρητικότητα του πίνακα ροών ενός μεταγωγέα OF, προκειμένου να υποστηρίξει την επιλεκτική αποκοπή των κακόβουλων ροών, το πλήθος τον οποίων μπορεί να αντιστοιχεί σε χιλιάδες μοναδικές εγγραφές στον πίνακα ροών του μεταγωγέα. Έτσι, προσαρμόστηκε και υλοποιήθηκε μία μέθοδος ενοποίησης κακόβουλων ροών σε επίπεδο IP. Το επίπεδο ενοποίησης (όπως θα εξηγηθεί αναλυτικότερα στη συνέχεια) εξαρτάται άμεσα από τις αριθμό των διαθέσιμων εγγραφών σε ένα μεταγωγέα OF, επιδιώκοντας ταυτόχρονα την ελαχιστοποίηση των παράπλευρων απωλειών (αναγκαστική αποκοπή καλόβουλων ροών). Ο συνολικός μηχανισμός αποκοπής ακολουθεί την τάση των αρχιτεκτονικών NFV, δηλαδή την υλοποίηση σαν μια λογική διαδικασία η οποία εξαρτάται από το λογισμικό, αποφεύγοντας τη χρήση εξοπλισμού (hardware) συγκεκριμένων προδιαγραφών.

Επιπλέον, στα πλαίσια της παρούσας διατριβής, διερευνάται και αξιολογείται η δυνατότητα δημιουργίας συνεργατικών μοντέλων μεταξύ γειτονικών δικτυακών περιοχών (SDN domains) για την από κοινού αντιμετώπιση κατανεμημένων δικτυακών επιθέσεων. Οι

δικτυακές περιοχές οι οποίες μελετούνται, ανήκουν σε συνορεύοντα Αυτόνομα Συστήματα ενώ, θεωρείται ως προαπαιτούμενο η υποστήριξη SDN πρωτοκόλλων όπως το OpenFlow, για την ελαστική και δυναμική εξυπηρέτηση των ροών. Ακόμη, για την δημιουργία των συνεργατικών σχημάτων, προτείνεται ένας μηχανισμός φήμης ο οποίος λειτουργεί ως ένα κίνητρο συνεργασίας μεταξύ γειτονικών δικτυακών περιοχών, αποθαρρύνοντας τες από το να υιοθετήσουν μυωπικές και ιδιοτελής πολιτικές. Ως αποτέλεσμα, ένα SDN domain το οποίο εξυπηρετεί το θύμα μίας κατανεμημένης επίθεσης, έχει τη δυνατότητα να ζητήσει τη συνδρομή των δικτυακών περιοχών οι οποίες άθελά τους εξυπηρετούν την προώθηση των κακόβουλων ροών, προκειμένου να κατανεμηθεί η διαδικασία αποκοπής της επίθεσης. Βασικό στοιχείο της προτεινόμενης προσέγγισης, αποτελεί το γεγονός πως η θετική ή αρνητική στάση (ως προς την δέσμευση δικτυακών πόρων για την αντιμετώπιση της επίθεσης) που θα τηρήσει το κάθε SDN domain στο μονοπάτι της επίθεσης, θα επηρεάσει αναλόγως και το επίπεδο φήμης του. Ένα SDN domain με χαμηλό επίπεδο φήμης είναι λιγότερο πιθανό να δεχθεί τη συνδρομή των γειτονικών του δικτυακών περιοχών, στην περίπτωση που εκείνο ζητήσει την από κοινού αντιμετώπιση μίας κατανεμημένης επίθεσης τύπου DDoS.

Αξίζει να σημειωθεί ότι η αξιολόγηση (μέσω προσομοιώσεων και εξομοιώσεων) των προτεινόμενων μεθόδων, στηρίχθηκε στη χρήση πραγματικών δεδομένων, τόσο όσον αφορά τη δικτυακή κίνηση, όσο και τις τοπολογίες Internet οι οποίες χρησιμοποιήθηκαν για την αξιολόγηση της μεθόδου συνεργατικής αντιμετώπισης κατανεμημένων δικτυακών επιθέσεων. Τα ανώνυμα αυτά δεδομένα προέρχονταν αφενός από το δίκτυο παραγωγής του Εθνικού Μετσόβιου Πολυτεχνείου, και αφετέρου από το Center for Applied Internet Data Analysis (CAIDA).

Με βάση την ανάλυση και την παρατήρηση των πειραματικών αποτελεσμάτων της συγκεκριμένης διατριβής, υποστηρίζεται πως μέσω των συνεργειών που προκύπτουν από το συνδυασμό του πρωτοκόλλου OpenFlow και των αρχιτεκτονικών τύπου NFV, μπορεί να προκύψει πλήθος νέων μεθόδων για την συνολική και στοχευμένη αντιμετώπιση των δικτυακών επιθέσεων, ειδικότερα εάν ληφθούν υπ’ όψιν δυνατότητες όπως: προγραμματιστική διαχείριση, κεντρικοποιημένη επιβολή πολιτικών προώθησης ή δρομολόγησης, αποσύνδεση των δικτυακών λειτουργιών από το φυσικό υπόστρωμα, και δυναμικός συνδυασμός Εικονικοποιημένων Δικτυακών Λειτουργιών για την δημιουργία υψηλού επιπέδου συστημάτων υποστήριξης τηλεπικοινωνιών (OSS/BSS).

Η διατριβή διαρθρώνεται σε επιμέρους ενότητες ως εξής:

- Στο Κεφάλαιο 2 γίνεται μία συνοπτική παρουσίαση νέων πρωτοκόλλων των Δικτύων Νέας Γενιάς, ταξινομώντας τα σε πρωτόκολλα κατάλληλα για τη δημιουργία Δικτύων Επικάλυψης (Overlay Networks) και πρωτόκολλα για τη δημιουργία ευφυών προγραμματιζόμενων δικτύων τύπου SDN. Ιδιαίτερη σημασία δίνεται στο πρωτόκολλο OpenFlow, το οποίο αποτελεί και αναπόσπαστο στοιχείο των μηχανισμών που προτείνονται στα πλαίσια της διατριβής.

- Στο Κεφάλαιο 3 παρουσιάζονται οι κυριότερες μέθοδοι, μέσω των οποίων είναι δυνατή η συλλογή στατιστικής πληροφορίας σε πραγματικό χρόνο, σχετικά με την κίνηση και τις ροές δεδομένων σε παραδοσιακές δικτυακές υποδομές. Επιπρόσθετα, παρουσιάζεται κάποιες ενδεικτικές προσεγγίσεις οι οποίες εμφανίζονται στη βιβλιογραφία, και αφορούν στην εξαγωγή στατιστικής πληροφορίας σε δίκτυα SDN.

- Στο Κεφάλαιο 4 πραγματοποιείται μία αναλυτική παρουσίαση της βιβλιογραφίας σχετικά με: (α) την ανίχνευση δικτυακών επιθέσεων σε παραδοσιακά και SDN δίκτυα, (β) τον περιορισμό της κακόβουλη κίνησης, αλλά και (γ) εναλλακτικές προσεγγίσεις οι οποίες έχουν προταθεί σχετικά με την συνεργασία Αυτόνομων Συστημάτων για την από κοινού αντιμετώπιση επιθέσεων και κακόβουλων πηγών κίνησης.

- Στο Κεφάλαιο 5 περιγράφεται ένας νέος μηχανισμός που αναπτύχθηκε στα πλαίσια της διατριβής για την ανίχνευση δικτυακών επιθέσεων τύπου DDoS, Worm Propagation και Port Scanning, και την αντιμετώπισή τους, με στόχο τον περιορισμό της επίδρασης που μπορεί να έχουν τέτοιες επιθέσεις στη συνολική δικτυακή υποδομή. Ιδιαίτερη έμφαση δίνεται στη μέθοδο συλλογής των δεδομένων που αφορούν στις δικτυακές ροές, παρουσιάζοντας μία εκτενή σύγκριση δύο μεθόδων και την επίδρασή τους στην ανίχνευση ανωμαλιών δικτύου.

- Στο Κεφάλαιο 6 αναλύεται η προτεινόμενη μέθοδος ανίχνευσης και αντιμετώπισης κατανεμημένων επιθέσεων DDoS σε παραδοσιακά δίκτυα

(legacy networks), χρησιμοποιώντας μεταγωγείς OpenFlow ως ενδιάμεσους (middlebox). Συγκεκριμένα, περιγράφονται οι αλγόριθμοι που υιοθετήθηκαν τόσο για την ανίχνευση επιθέσεων DDoS, όσο και για τη βέλτιστη συνάθροιση εγγραφών στους πίνακες ενός μεταγωγέα OpenFlow για την αποκοπή του συνόλου των κακόβουλων ροών δεδομένων. Ιδιαίτερη έμφαση δίνεται στην κλιμακωσιμότητα της προτεινόμενης προσέγγισης, ώστε να είναι σε θέση μία δεδομένη δικτυακή περιοχή να αντιμετωπίσει επιθέσεις DDoS μεγάλης κλίμακας.

- Στο Κεφάλαιο 7 προτείνεται και αξιολογείται η δημιουργία συνεργατικών σχημάτων μεταξύ γειτονικών δικτυακών περιοχών βασισμένων στη φήμη, με στόχο την από κοινού αντιμετώπιση κατανεμημένων δικτυακών επιθέσεων. Η προσέγγιση αυτή αξιολογείται μέσα από εκτενή πειράματα προσομοίωσης και εξομοίωσης, προκειμένου να καταστούν εμφανή τόσο τα πλεονεκτήματα για όλες τις δικτυακές περιοχές οι οποίες συνεργάζονται, όσο και η αναγκαιότητα εισαγωγής μοντέλων φήμης, κάτι το οποίο μπορεί να λειτουργήσει ως κίνητρο για την διατήρηση τέτοιων συνεργατικών σχημάτων.

- Τέλος στο Κεφάλαιο 8, παρουσιάζονται τα συμπεράσματα και οι κατευθύνσεις μελλοντικής έρευνας που προέκυψαν κατά την εκπόνηση της παρούσας διατριβής.

2 Δίκτυα Νέας Γενιάς (Future Internet Networks)

Η δικτύωση και η ευρεία χρήση υπηρεσιών Internet θεωρείται δεδομένη στα σύγχρονα ακαδημαϊκά αλλά και επιχειρηματικά περιβάλλοντα. Συσκευές όπως μεταγωγείς (switches), δρομολογητές (routers), τείχη προστασίας (firewalls) κ.α., αποτελούν τον κορμό της δικτυακής υποδομής όλων των σύγχρονων επιχειρήσεων. Στις παραδοσιακές δικτυακές υποδομές, οι απαραίτητες διεργασίες ελέγχου και προώθησης της πληροφορίας υλοποιούνται σε κάθε μία δικτυακή συσκευή ξεχωριστά.

Το σύνολο μιας παραδοσιακής δικτυακής συσκευής μπορεί να διαχωριστεί σε τρία λειτουργικά επίπεδα τα οποία καθορίζουν τη λειτουργία ολόκληρου του δικτύου [9]:

- **Επίπεδο Προώθησης Δεδομένων (Data/Forwarding Plane):** Κάθε δικτυακή συσκευή υλοποιεί τοπικά το Επίπεδο Προώθησης Δεδομένων, το οποίο πραγματοποιεί λειτουργίες όπως (i) προώθηση πακέτων, (ii) αντιστοίχηση διευθύνσεων IP προορισμού με βάση το μέγιστο κοινό πρόθεμα (Longest Common Prefix - LCP), και (iii) εφαρμογή Λίστας Ελέγχου Πρόσβασης (Access-Control Lists - ACLs).

- **Επίπεδο Ελέγχου (Control Plane):** Το Επίπεδο Ελέγχου καθορίζει τη μέθοδο προώθησης των πακέτων, κάνοντας χρήση κατάλληλων αλγορίθμων. Χαρακτηριστικό παράδειγμα είναι τα μηνύματα τύπου Border Gateway Protocol (BGP) [10] που ανταλλάσσονται μεταξύ γειτονικών δικτυακών περιοχών (network domains). Με τον τρόπο αυτό το Επίπεδο Ελέγχου κάθε συσκευής είναι ικανό να λάβει αποφάσεις σχετικά με τη διαδρομή που θα ακολουθήσει το κάθε πακέτο.

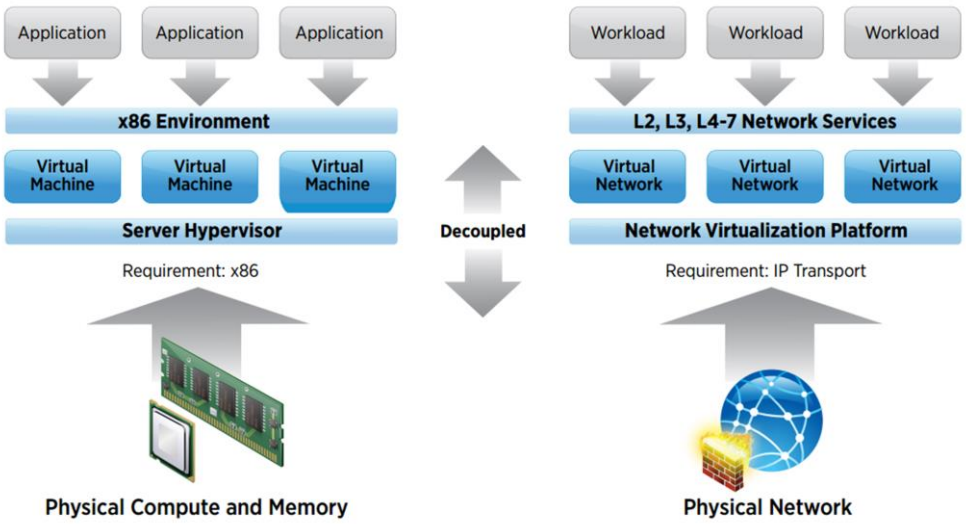
- **Επίπεδο Διαχείρισης (Management Plane):** Το Επίπεδο Διαχείρισης είναι υπεύθυνο για την συλλογή και ανάλυση της πληροφορίας που προκύπτει μέσω της παρακολούθησης της δικτυακής κίνησης (network monitoring). Η διαδικασία ανάλυσης της πληροφορίας αυτής, αλλά και της πιθανής ανίχνευσης εισβολών και παραμετροποίησης του Καταλόγου Ελέγχου Πρόσβασης αποτελούν τμήμα του Επιπέδου Διαχείρισης.

Στα παραδοσιακά δίκτυα παραγωγής, κάθε συσκευή υλοποιεί ανεξάρτητα την τριμερή αυτή διαίρεση. Ακόμη, η κατά κόρον χρήση ιδιόκτητου κλειστού λογισμικού (proprietary software), αλλά και ο διαμοιρασμός του συνολικού ελέγχου των Λειτουργιών Δικτύου

(Network Functions) σε πολλαπλές δικτυακές οντότητες δυσχεραίνει την ομαλή διαχείριση των δικτύων. Το φαινόμενο αυτό γίνεται πιο εμφανές όσο διαδίδεται η χρήση εμπορικών εφαρμογών οι οποίες δρουν κατανεμημένα και απαιτούν το διαμοιρασμό της δικτυακής κίνησης σε πολλαπλές Εικονικές Μηχανές (Virtual Machines) οι οποίες μπορεί κάλλιστα να βρίσκονται σε διαφορετικούς δικτυακούς τομείς (βλ. Google [11]).

Τα σύγχρονα δίκτυα πρέπει να είναι ικανά να εξυπηρετήσουν τις αυξανόμενες ανάγκες Τηλεπικοινωνιακών Παρόχων και Κέντρων Υπολογιστικών Δεδομένων (Data Centers). Τα περιβάλλοντα αυτά απαιτούν: (i) μετανάστευση εικονικών μηχανών, (ii) δυναμικό επαναπρογραμματισμό των δικτύων, (iii) εφαρμογή πολιτικών με συνέπεια (consistently) σε όλες τις συσκευές, (iv) κλιμακώσιμες υποδομές, και (v) αποφυγή κλειδώματος σε συγκεκριμένο κατασκευαστή (vendor lock-in) [2].

Τις ανάγκες αυτές καλούνται πλέον να εξυπηρετήσουν τα πρωτόκολλα μέσω των οποίων υλοποιούνται δίκτυα νέας γενιάς. Τέτοια πρωτόκολλα εισάγουν στα δίκτυα έννοιες όπως ‘προγραμματισιμότητα’ (programmability), ‘ελαστικότητα’ (elasticity) και ‘κατ’ αίτηση’ (on-demand), οι οποίες μέχρις στιγμής αφορούσαν μόνο τη διαχείριση υπολογιστικών και αποθηκευτικών πόρων. Η βιομηχανία της Πληροφορικής έχει αποκτήσει μεγαλύτερη αποτελεσματικότητα και ευελιξία ως άμεσο αποτέλεσμα της εικονικοποίησης (virtualization) των πόρων [12]. Την αντίστοιχη λογική της αφαιρετικότητας (abstraction) και της δημιουργίας ‘δεξαμενών’ (pools) δικτυακών πόρων υπόσχονται τα δίκτυα νέας γενιάς. Στο Σχήμα 1 γίνεται εμφανής η αναλογία μεταξύ υπολογιστικής και δικτυακής εικονικοποίησης. Στόχος είναι η αποτελεσματικότερη και ευέλικτη εκμετάλλευση



Σχήμα 1: Αναλογία Εικονικοποίησης Υπολογιστικών και Δικτυακών Πόρων

Πηγή: VMware® Network Virtualization Design Guide

υπαρκτών υποδομών για τη δημιουργία λογικών δικτυακών υποδομών. Γενικά, οι τεχνολογίες των δικτύων νέας γενιάς μπορούν να διαχωριστούν σε δύο κύριες κατηγορίες· (α) πρωτόκολλα που προσφέρουν ελαστικότητα και κλιμακωσιμότητα μέσω δικτύων επικάλυψης (overlay networks), και (β) πρωτόκολλα τα οποία εισάγουν επιπλέον την έννοια των Δικτύων Οριζόμενων-από-Λογισμικό (Software-Defined Networks), επιτρέποντας έτσι τον κεντρικό έλεγχο και επιβολή εξειδικευμένων πολιτικών.

2.1 Δίκτυα Επικάλυψης μέσω Νέων Πρωτοκόλλων Ενθυλάκωσης Πλαισίων

Αν και η έννοια των δικτύων επικάλυψης (Overlay Networks) δεν είναι νέα, τα τελευταία χρόνια απέκτησε ιδιαίτερο ενδιαφέρον λόγω της αφαιρετικότητας (abstraction) που εισάγει, χωρίς να απαιτούνται σημαντικές μεταβολές της φυσικής υποδομής. Η αφαιρετικότητα επιτυγχάνεται με τη χρήση νέων πρωτοκόλλων ενθυλάκωσης δικτυακών πλαισίων (network frames), τα οποία σχεδιάστηκαν με κύριο γνώμονα την επίλυση προβλημάτων κλιμάκωσης και κινητικότητας (mobility) σε Data Centers. Ενδεικτικά, κάποια από τα πιο διαδεδομένα πρωτόκολλα επικάλυψης είναι: (i) Virtual Extensible LAN (VXLAN [13]), (ii) Network Virtualization using Generic Routing Encapsulation (NVGRE [14]), (iii) Stateless Transport Tunneling (STT [15]), (iv) Location/Identifier Separation Protocol (LISP [16]).

Τα δίκτυα επικάλυψης, εν γένει, χαρακτηρίζονται από εικονικά δίκτυα αποτελούμενα από (λογικά) συνδεδεμένους κόμβους, και τα οποία μοιράζονται μια ενιαία φυσική υποδομή. Μέσω δικτύων επικάλυψης καθίσταται δυνατή η ανάπτυξη δικτυακών εφαρμογών, χωρίς μεταβολή της φυσικής υποδομής [17]. Μέσω των τεχνολογιών επικάλυψης κατέστη δυνατή η κλιμάκωση των δικτυακών υποδομών, στρέφοντας το βάρος περισσότερο στις συσκευές που βρίσκονται στο άκρο της επικάλυψης (edge devices) και λιγότερο στον κορμό του δικτύου. Επίσης, λόγω της χρήσης ενός κεντρικού σημείου διαχείρισης, είναι δυνατή η εύκολη εφαρμογή κεντρικών πολιτικών. Ταυτόχρονα, οι διαχειριστές δικτύων σε περιβάλλοντα πολλαπλών ενοικιαστών (multitenant environments) είναι ικανοί να αναθέσουν λογικούς δικτυακούς πόρους χωρίς αλλαγή της φυσικής υποδομής. Τέλος, παρακάμπτονται περιορισμοί που εμφανίζονται συνήθως σε Data Centers λόγω του μικρού διαθέσιμου αριθμού μεμονωμένων Virtual LANs.

Τα δίκτυα επικάλυψης προσέφεραν άμεση λύση σε προβλήματα όπως τα παραπάνω, αλλά ταυτόχρονα έφεραν νέους περιορισμούς. Συγκεκριμένα, χρήστες και διαχειριστές αντιμετωπίζουν μειωμένη οπτική της δικτυακής υποδομής λόγω του επιπέδου αφαίρεσης το οποίο αποκρύπτει το φυσικό υπόστρωμα. Ακόμη, οι διαχειριστές του δικτύου καλούνται να αναγνωρίσουν σφάλματα, όχι μόνο σε περίπλοκες δικτυακές υποδομές, αλλά και σε ένα σύνολο από αντιστοιχίσεις μεταξύ φυσικών και εικονικών πόρων. Σαν μία πιο συνολική και ριζοσπαστική λύση εμφανίστηκαν τα Δίκτυα Οριζόμενα από Λογισμικό (Software-Defined Networks).

2.2 Δίκτυα Οριζόμενα από Λογισμικό (Software-Defined Networks)

Τα δίκτυα SDN αποτελούν μία καινούρια αρχιτεκτονική, και ταυτόχρονα μια καινοτόμα προσέγγιση που στοχεύει στην επίλυση προβλημάτων διαχείρισης και κλιμάκωσης που αναφέρθηκαν παραπάνω. Τα SDN εισάγουν στους δικτυακούς πόρους την έννοια του προγραμματισμού, προσφέροντας δυνατότητες παραμετροποίησης και ελέγχου μέσω εφαρμογών λογισμικού. Επίσης, χαρακτηριστικό γνώρισμα των δικτύων SDN αποτελεί ο πλήρης διαχωρισμός του Επιπέδου Ελέγχου και Επιπέδου Προώθησης. Αποφεύγοντας πλέον τη λογική της πλήρης ενσωμάτωσης των παραδοσιακών δικτύων, οι δικτυακές συσκευές μετατρέπονται σε απλές συσκευές προώθησης πακέτων. Παράλληλα, όλη η ευφυΐα -η οποία ουσιαστικά αποτελεί το Επίπεδο Ελέγχου- μεταφέρεται σε ένα (λογικά) κεντρικό Ελεγκτή (Controller). Ο διαχωρισμός αυτός προσφέρει σημαντική ευελιξία όσον αφορά την παραμετροποίηση των δικτυακών συσκευών, ενώ ταυτόχρονα απλοποιεί εγγενώς και τη διαδικασία εφαρμογής κεντρικοποιημένων πολιτικών [18].

Οι Ελεγκτές υλοποιούν τα επίπεδα αφαίρεσης που απαιτούνται, προκειμένου να είναι δυνατός ο προγραμματιστικός έλεγχος και η διαχείριση της υποδομής μέσω εφαρμογών. Συγκεκριμένα, στο [19] οι συγγραφείς διακρίνουν ως απαραίτητα επίπεδα αφαίρεσης τα: (α) Αφαιρετικό Επίπεδο Ελέγχου (Control Abstraction Layer) μέσω του οποίου υποστηρίζονται μέθοδοι για τον έλεγχο της υποδομής και τον τρόπο με τον οποίο θα προωθηθούν τα πακέτα, και (β) Αφαιρετικό Επίπεδο Διαχείρισης, μέσω του οποίου υλοποιούνται διαδικασίες παρακολούθησης και παραμετροποίησης των δικτυακών συσκευών. Παράλληλα, το κάθε Επίπεδο Αφαίρεσης εκθέτει την αντίστοιχη διεπαφή (interface) προς τις συσκευές. Μέσω των διεπαφών αυτών πραγματοποιείται η επικοινωνία

μεταξύ των Επιπέδων Ελέγχου και Προώθησης, με τη χρήση κατάλληλων πρωτοκόλλων. Κάποια από τα πιο αντιπροσωπευτικά πρωτόκολλα είναι:

- **ForCES:** Το πρωτόκολλο Forwarding and Control Element Separation (ForCES [20]) προτάθηκε ως μία προσέγγιση για τον πλήρη διαχωρισμό των Επιπέδων Ελέγχου και Προώθησης. Ακόμη, περιλαμβάνει ένα μοντέλο για την προδιαγραφή της πληροφορίας που ανταλλάσσεται μεταξύ των Στοιχείων Ελέγχου (Control Elements – CE) και των Στοιχείων Προώθησης (Forwarding Element – FE). Συνεπώς, είναι δυνατός ο καθορισμός Λογικών Λειτουργικών Δομών (Logical Function Blocks – LFBs), στοχεύοντας στην περιγραφή των συσκευών, των δυνατοτήτων τους, και των δικτυακών 'γεγονότων' που παράγουν.

- **OpenFlow:** Το πρωτόκολλο OpenFlow (OF) αναπτύχθηκε αρχικά από το Πανεπιστήμιο Stanford, ενώ πλέον συντηρείται και εξελίσσεται από τον οργανισμό Open Networking Foundation (ONF). Πρωταρχικό του στόχος, ήταν να παρέχει στους ερευνητές μία συνολική λύση, ώστε να μπορούν να χρησιμοποιούν και να δοκιμάζουν πειραματικά πρωτόκολλα στο πραγματικό δίκτυο παραγωγής [1]. Μέσω του πρωτοκόλλου OF κατέστη δυνατός ο έλεγχος πολλαπλών μεταγωγέων OF, μέσω ενός λογικά κεντρικοποιημένου Ελεγκτή (OF Controller). Κάθε μεταγωγέας OF, διατηρεί έναν ή περισσότερους πίνακες ροών. Τα πακέτα που εισέρχονται στον μεταγωγέα αντιστοιχίζονται με μία από αυτές τις εγγραφές του πίνακα, ώστε να καθοριστεί η μέθοδος με την οποία θα γίνει η προώθηση του εκάστοτε πακέτου.

- **NETCONF/YANG:** Το Network Configuration Protocol (NETCONF) [21] παρέχει μηχανισμούς για την εγκαθίδρυση, μεταχείριση και διαγραφή παραμέτρων των δικτυακών συσκευών. Οι εν λόγω διαδικασίες πραγματοποιούνται μέσω κλήσεων σε απομακρυσμένες διαδικασίες (Remote Procedure Calls – RPC), κωδικοποιώντας την πληροφορία με βάση το πρότυπο XML. Ταυτόχρονα, έχει αναπτυχθεί η γλώσσα YANG [22] για τη μοντελοποίηση των πληροφοριών, των παραμέτρων και των εντολών μου ανταλλάσσονται μέσω του πρωτοκόλλου NETCONF.

- **PCEP:** Στην αρχιτεκτονική του Path Computation Element (PCE) [23], ορίζεται μία οντότητα, ικανή να υπολογίσει διαδρομές-μονοπάτια τα οποία μπορεί να ακολουθήσει μία υπηρεσία (ή ένα σύνολο υπηρεσιών). Η αρχιτεκτονική αυτή αναπαριστά μία οπτική

των δικτύων, όπου ο υπολογισμός διαδρομών, η από-άκρο-σε-άκρο σηματοδοσία, και η προώθηση των πακέτων, είναι τρεις τελείως διαχωρισμένες διαδικασίες. Για το σκοπό αυτό χρησιμοποιείται το πρωτόκολλο Patch Communication Protocol (PCEP) [24], το οποίο χρησιμοποιείται για την επικοινωνία μεταξύ ενός Path Computation Client (PCC) και ενός PCE, ή πολλαπλών PCE.

- **OpFlex:** Το πρωτόκολλο OpFlex [25], παρουσιάστηκε από τη Cisco, και υλοποιεί μία δηλωτική μέθοδο ελέγχου, για τη μεταφορά και επιβολή πολιτικών από έναν Ελεγκτή Πολιτικών, σε ένα σύνολο έξυπνων συσκευών, ικανών να κατανοήσουν και να υλοποιήσουν τις πολιτικές αυτές. Στην πραγματικότητα, μοιάζει αρκετά με εργαλεία όπως το Puppet [26] ή το CFEngine [27], μέσω των οποίων είναι δυνατή η χρήση δηλωτικών γλωσσών για την παραμετροποίηση πόρων εξυπηρετητών.

2.2.1 Πρωτόκολλο OpenFlow (OpenFlow Protocol)

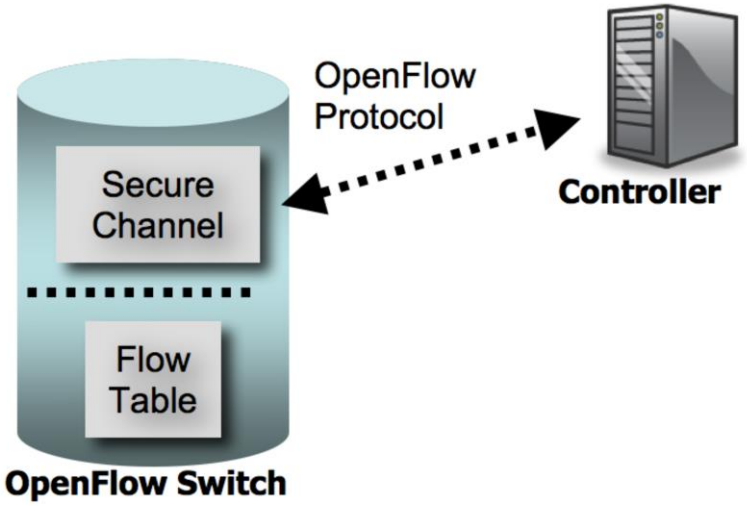
Η συγκεκριμένη διατριβή εστιάζεται στη χρήση του πρωτοκόλλου OpenFlow, μέσω του οποίου είναι δυνατός ο προγραμματιστικός έλεγχος των δικτυακών συσκευών, αλλά και η ελαστική παραμετροποίησή τους.

2.2.1.1 Ο Μεταγωγέας OpenFlow

Σε γενικές γραμμές, κύριο συστατικό της αρχιτεκτονικής που προτείνεται μέσω του πρωτοκόλλου OpenFlow, είναι ο μεταγωγέας OpenFlow, ο οποίος περιέχει έναν ή περισσότερους πίνακες ροών (flow tables), οι οποίοι χρησιμοποιούνται για την αντιστοίχιση και προώθηση των πακέτων, και έναν ασφαλή δίαυλο επικοινωνίας (secure channel) προς έναν OpenFlow Controller. Ο OF Controller, μέσω του πρωτοκόλλου OF, διαχειρίζεται τον μεταγωγέα OF, όπως υποδεικνύει και το Σχήμα 2.

Ο πίνακας ροών περιέχει εγγραφές για τις αντίστοιχες ροές (flows), καθώς και μετρητές (Counters) και ενέργειες (Actions) συσχετισμένες με κάθε μία εγγραφή. Κάθε πακέτο που εισέρχεται στον μεταγωγέα OF, αντιπαραβάλλεται με τις εγγραφές του αντίστοιχου πίνακα ροών. Σε περίπτωση αντιστοίχησης με κάποια εγγραφή, εφαρμόζονται τα Actions που αφορούν τη συγκεκριμένη εγγραφή, αλλιώς το πακέτο προωθείται στον OF

Controller μέσω του secure channel. Από εκείνο το σημείο, ο Controller είναι υπεύθυνος για τη διαδρομή που θα ακολουθήσει το πακέτο, προσθέτοντας ή αφαιρώντας εγγραφές στον πίνακα ροών του μεταγωγέα [28].



Σχήμα 2: Ένας OpenFlow μεταγωγέας επικοινωνεί με έναν OF Controller μέσω ασφαλούς σύνδεσης (secure channel) χρησιμοποιώντας το πρωτόκολλο OpenFlow.
Πηγή : OpenFlow Switch Specification Version 1.0.0

Κάθε εγγραφή του πίνακα ροών περιέχει πεδία επικεφαλίδων (header fields) τα οποία αντιπαραβάλλονται με τα αντίστοιχα πεδία κάθε πακέτου που εισέρχεται στον μεταγωγέα OF, μετρητές που ανανεώνονται για κάθε πακέτο που αντιστοιχίζεται με μία συγκεκριμένη εγγραφή και ενέργειες τα οποία εφαρμόζονται σε περίπτωση αντιστοίχησης, ακολουθώντας τη μορφή που υποδεικνύει ο Πίνακας 1.

Πεδία Επικεφαλίδων	Μετρητές	Ενέργειες

Πίνακας 1: Ένα σύνολο πεδίων επικεφαλίδων, μετρητών και ενεργειών αποτελούν μια εγγραφή του πίνακα ροών ενός μεταγωγέα OF.

Ο Πίνακας 3 δείχνει και τα 12 πεδία επικεφαλίδων, βάσει των οποίων προσδιορίζεται μία εγγραφή του πίνακα ροών. Αυτά τα 12 πεδία είναι που θα συγκριθούν με τα αντίστοιχα πεδία κάθε πακέτου που διέρχεται από τον μεταγωγέα OF. Κάθε πεδίο μπορεί να έχει είτε μια συγκεκριμένη τιμή, είτε έναν χαρακτήρα αναπλήρωσης (wildcard) οπότε και η σύγκρισή του με το αντίστοιχο πεδίο ενός πακέτου θα είναι πάντα αληθής.

Σε κάθε μεταγωγέα OF διατηρούνται μετρητές για κάθε πίνακα, ροή, πόρτα του μεταγωγέα (switch port) και ουρά αναμονής. Ο Πίνακας 2 αναφέρεται στο σύνολο των μετρητών που διατηρούνται από ένα OpenFlow switch.

Ingress Port	Ether src	Ether dst	Ether type	VLAN id	VLAN Priority	IP src	IP dst	IP proto	IP ToS Bits	TCP/ UDP Src Port	TCP/ UDP Dst Port

Πίνακας 3: Πληροφορίες που αποτελούν κριτήριο για την αντιστοίχιση ενός πακέτου με μία συγκεκριμένη εγγραφή του πίνακα ροών ενός μεταγωγέα OF.

Κάθε εγγραφή είναι συσχετισμένη με μία λίστα από Actions (η λίστα μπορεί να περιέχει από μηδέν έως οσαδήποτε Actions), που υποδεικνύουν στον μεταγωγέα πώς να διαχειριστεί τα πακέτα που αντιστοιχούν. Αν δεν υπάρχει κάποιο Action προώθησης (forward) στη λίστα, τότε το πακέτο απορρίπτεται (drop).

Counter	Bits
Per Table	
Active Entries	32
Packet Lookups	64
Packet Matches	64
Per Flow	
Received Packets	64
Received Bytes	64
Duration (seconds)	32
Duration (nanoseconds)	32
Per Port	
Received Packets	64
Transmitted Packets	64
Received Bytes	64
Transmitted Bytes	64
Receive Drops	64
Transmit Drops	64
Receive Errors	64
Transmit Errors	64
Receive Frame Alignment Errors	64
Receive Overrun Errors	64
Receive CRC Errors	64
Collisions	64
Per Queue	
Transmit Packets	64
Transmit Bytes	64
Transmit Overrun Errors	64

Πίνακας 2: Λίστα με τους διαθέσιμους μετρητές.
[Πηγή: OpenFlow Switch Specification Version 1.0.0]

Ένας μεταγωγέας μπορεί να απορρίψει μία καινούρια εγγραφή που πρόκειται να εισαχθεί, σε περίπτωση που δεν μπορεί να επεξεργαστεί τη λίστα των Actions που συμπεριλαμβάνει η συγκεκριμένη εγγραφή. Θεωρώντας αυτό ως δεδομένο, ένας

μεταγωγέας OF δεν είναι απαραίτητο να υποστηρίζει όλα τα είδη Actions που προδιαγράφει το πρωτόκολλο OpenFlow (όπως τα απαριθμεί και ο Πίνακας 4), αλλά πρέπει να υποστηρίζει τουλάχιστον αυτά με την ένδειξη "REQUIRED", τα οποία θεωρούνται απαραίτητα για τις βασικές λειτουργίες του πρωτοκόλλου OF. Όταν ένας μεταγωγέας OF συνδεθεί με τον Controller του, τότε τον ενημερώνει σχετικά με το ποια από τα προαιρετικά ("OPTIONAL") Actions υποστηρίζει.

Ενέργεια	**Λειτουργία**	**Αναγκαιότητα**
FORWARD	Προώθηση πακέτων προς οποιοδήποτε φυσικό port, καθώς και προς τα παρακάτω εικονικά: • ALL • CONTROLLER • LOCAL • TABLE • IN_PORT	*REQUIRED*
FORWARD	Προώθηση πακέτων τα παρακάτω εικονικά ports: • NORMAL: • FLOOD	*OPTIONAL*
ENQUEUE	Προσθήκη του πακέτου σε ουρά μίας port για περεταίρω προώθηση	*OPTIONAL*
DROP	Απόρριψη πακέτου μέσω εγγραφής flow η οποία δεν περιέχει κανένα action ορισμένο	*REQUIRED*
MODIFY-FIELD	Μεταβολή των επικεφαλίδων ενός πακέτου από τον μεταγωγέα OpenFlow	*OPTIONAL*

Πίνακας 4: Σύνολο των Actions που μπορεί να υποστηρίζονται από έναν μεταγωγέα OpenFlow.

Το πιο σύνηθες Action ενός μεταγωγέα OF, με βάση το οποίο γίνεται και η προώθηση των πακέτων είναι το FORWARD. Κάθε μεταγωγέας πρέπει υποχρεωτικά να μπορεί να προωθήσει ένα πακέτο προς οποιαδήποτε φυσική port, καθώς και προς τις παρακάτω εικονικές:

- ALL: Προώθηση ενός πακέτου προς όλες τις διεπαφές (interfaces) του switch, εκτός από την διεπαφή εισόδου.
- CONTROLLER: Αποστολή 128 bits (ή και ολόκληρου) του πακέτου προς τον Controller
- LOCAL: Αποστολή του πακέτου στο networking stack του ίδιου του switch
- TABLE: Πραγματοποιεί κάποιες ενέργειες στο flow-table του ίδιου του switch. Το action αυτό αφόρα μόνο packet-out μηνύματα
- IN_PORT: Στέλνει το πακέτο από την πόρτα εισόδου

Εκτός από αυτές τις πέντε εικονικές πόρτες, ένας μεταγωγέας OF μπορεί προαιρετικά να υποστηρίζει και τις επόμενες δύο:

- NORMAL: προώθηση πακέτων με βάση το "παραδοσιακό μονοπάτι" προώθησης (traditional forwarding path) που υποστηρίζει το switch (π.χ. MAC learning)
- FLOOD: προώθηση του πακέτου με βάση το ελάχιστο Spanning Tree, χωρίς να συμπεριλαμβάνεται το port εισόδου του πακέτου

2.2.1.2 Ο OpenFlow Controller

Ένας OF Controller αποτελεί μία πλατφόρμα ελέγχου ενός δικτύου υπολογιστών και παρέχει ένα προγραμματιστικό περιβάλλον στους διαχειριστές του δικτύου. Με αυτό τον τρόπο μπορούν να δημιουργηθούν εφαρμογές (applications) που θα χρησιμοποιούνται από τον Controller ώστε να λαμβάνονται αποφάσεις για τη διαχείριση και παρακολούθηση του δικτύου σε πραγματικό χρόνο. Ο κύριος σκοπός αυτών των εφαρμογών είναι να "αποφασίσουν" πώς και αν θα δρομολογηθεί κάθε πακέτο σε ένα δίκτυο υπολογιστών.

Στην περίπτωση που κάποιο νέο πακέτο εισέλθει στον μεταγωγέα και δεν συσχετιστεί με κάποια από τις υπάρχουσες εγγραφές του πίνακα ροών, τότε θα αποσταλεί στον Controller. Ένα τέτοιο πακέτο συνήθως αποτελεί την αιτία για την δημιουργία μιας νέας εγγραφής στον πίνακα ροών ενός μεταγωγέα OF (flow initiation). Όμως μπορεί μέσω των εφαρμογών του Controller, να ορισθεί ότι πρέπει να ληφθούν όλα τα πακέτα μιας συγκεκριμένης κατηγορίας ή πρωτοκόλλου, πράγμα που σημαίνει ότι δεν θα δημιουργηθεί ποτέ η καινούρια εγγραφή. Γενικά ο Controller χρησιμοποιεί τις πληροφορίες που συλλέγει ή παράγει ο ίδιος για νέες ροές και γεγονότα που συμβαίνουν στο δίκτυο το οποίο ελέγχει, ώστε να ανανεώνει την οπτική που έχει για το δίκτυο αυτό κάθε στιγμή. Για τον λόγο αυτό,

όλοι οι Controllers βασίζουν τη λειτουργία και τις αποφάσεις τους σε δικτυακά γεγονότα (events). Σαν γεγονός, χαρακτηρίζεται κάθε τι που θα συμβεί στο δίκτυο που ελέγχει ο OF Controller, και το οποίο μπορεί να έχει ενδιαφέρον για κάποια από τις εφαρμογές του.

2.3 Εικονικοποίηση Δικτυακών Λειτουργιών

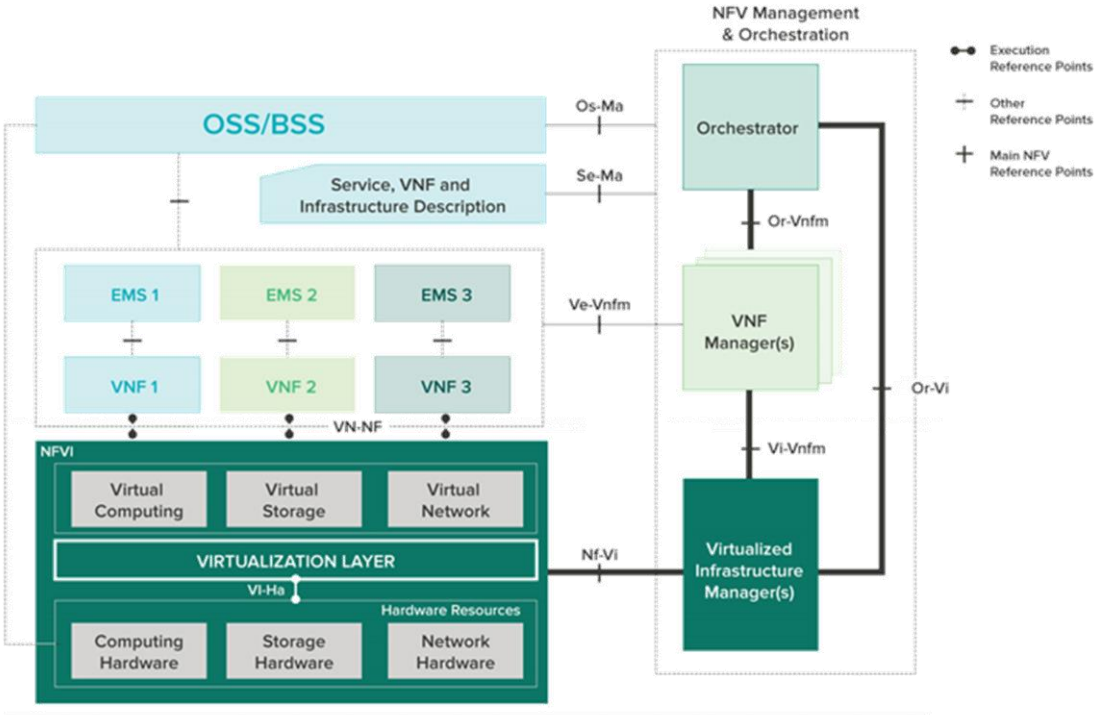
Στις παραδοσιακές δικτυακές αρχιτεκτονικές, οι δικτυακές λειτουργίες (Network Functions – NFs) υλοποιούνται συνδυάζοντας εξοπλισμό και λογισμικό συγκεκριμένου σκοπού, τα οποία συχνά αναφέρονται ως δικτυακοί κόμβοι (network nodes) και δικτυακά στοιχεία (network elements). Μέσω της Εικονικοποίησης Δικτυακών Λειτουργιών (Network Function Virtualisation – NFV) εισάγεται μία πληθώρα νέων παραμέτρων σχετικών με την υλοποίηση και παροχή δικτυακών υπηρεσιών [29]. Ενδεικτικά, μπορούν να αναφερθούν:

- *Αποσυσχέτιση του λογισμικού από τον εξοπλισμό στον οποίο εκτελείται:* Το λογισμικό μπορεί να εξελίσσεται ανεξάρτητα από τον εξοπλισμό, αφού δεν είναι πλέον δεμένα με συγκεκριμένα network elements.

- *Ευέλικτη εγκατάσταση δικτυακών υπηρεσιών:* Η αποσυσχέτιση υλικών και λογισμικών παραγόντων επιτρέπει την επαναχρησιμοποίηση και βελτιστοποίηση του σχεδιασμού των πόρων υποδομής, επιτρέποντας την παροχή διαφορετικών υπηρεσιών σε διαφορετικές χρονικές στιγμές. Υποθέτοντας ότι το σύνολο του εξοπλισμού και των λογισμικών πόρων βρίσκονται συναθροισμένοι σε συγκεκριμένα σημεία της υποδομής (Points of Presence – PoPs), καθίσταται δυνατή η περεταίρω αυτοματοποίηση της εγκαθίδρυσης (νέων) δικτυακών λειτουργιών μέσω λογισμικού. Η αυτοματοποίηση επιτυγχάνεται μέσω εκμετάλλευσης πολλαπλών τεχνολογιών νέφους (π.χ. OpenStack [30]) και δικτύου (π.χ. OpenFlow), επιτρέποντας στους διαχειριστές την εγκαθίδρυση νέων δικτυακών υπηρεσιών γρηγορότερα, πάνω από το ίδιο φυσικό υπόστρωμα.

- *Δυναμική διαχείριση:* Ο διαχωρισμός των δικτυακών λειτουργιών σε ανεξάρτητες μονάδες λογισμικού παρέχει αυξημένες δυνατότητες ευέλικτης διαχείρισης και κλιμάκωσης των VNFs. Επιτρέπεται έτσι η προσαρμογή των VNF βάσει της πραγματικής δικτυακής κίνησης.

Η αρχιτεκτονική NFV περιγράφει την υλοποίηση NFs αποκλειστικά ως λογισμικές οντότητες, οι οποίες εκτελούνται σε μία υποδομή NFV (NFV Infrastructure – NFVI). Στο Σχήμα 3 παρουσιάζεται μία γενικευμένη επισκόπηση των κύριων δομικών στοιχείων μίας αρχιτεκτονικής NFV. Μέσω των στοιχείων αυτό, καθίσταται εφικτή η δυναμική κατασκευή και διαχείριση Εικονικοποιημένων Δικτυακών Λειτουργιών (Virtualised Network Functions – VNFs), αλλά και ο προσδιορισμός των μεταξύ τους σχέσεων όσον αφορά τα δεδομένα, τη διαχείριση, τις αλληλεξαρτήσεις και άλλα χαρακτηριστικά τους.



Σχήμα 3: Επισκόπηση των κύριων δομικών στοιχείων μίας αρχιτεκτονικής NFV

3 Παρακολούθηση Δικτυακής Κίνησης

Η παρακολούθηση (monitoring) της δικτυακής κίνησης είναι μία από της κυριότερες διαδικασίες οι οποίες σχετίζονται με την διαχείριση δικτύων. Αποτελεί αναπόσπαστο τμήμα πολλών σύγχρονων συστημάτων, τα οποία μπορεί να παρακολουθούν ένα δίκτυο: (α) για λόγους ανίχνευσης σφαλμάτων (fault detection), (β) για λόγους βελτίωσης των παρεχόμενων υπηρεσιών (Quality of Service και Quality of Experience), ή (γ) για λόγους ασφάλειας δικτύου και ανίχνευσης εισβολών (intrusion detection).

Για διαδικασίες όπως, επί παραδείγματι, το πρώτο στάδιο ανίχνευσης σφαλμάτων όπου ελέγχεται η προσβασιμότητα μιας συσκευής από το δίκτυο, υπάρχουν εργαλεία όπως το telnet, το ping, το ssh, κλπ. Όμως για λειτουργίες όπως η ανεύρεση δικτυακών ανωμαλιών είναι απαραίτητη η συλλογή και ανάλυση είτε ολόκληρων των πακέτων που διέρχονται από το δίκτυο, είτε των επικεφαλίδων τους, κάτι το οποίο επιτυγχάνεται μέσω των μεθόδων που αναφέρονται κατωτέρω.

3.1 Μέθοδοι και Πρωτόκολλα Παρακολούθησης Δικτυακής Κίνησης

3.1.1 Το πρωτόκολλο SNMP

Το πρωτόκολλο SNMP (Simple Network Management Protocol) [31] αποτελεί ένα από τα κυριότερα εργαλεία για την παρακολούθηση δικτύων και τη συλλογή πληροφοριών από τις συσκευές που το απαρτίζουν. Μέσω του SNMP είναι δυνατή η συλλογή πληροφοριών σχετικά με το εύρος ζώνης που καταναλώνεται και τον όγκο των δεδομένων τα οποία μεταφέρονται μέσω του υπό-παρακολούθηση δικτύου. Ακόμη είναι δυνατή η χρήση του πρωτοκόλλου για την παρακολούθηση των πόρων συστήματος, οι οποίοι χρησιμοποιούνται σε κάθε συσκευή του δικτύου, όπως η μνήμη RAM, οι επεξεργαστικοί κύκλοι (CPU), κ.α.

Η αρχιτεκτονική που ορίζεται από πρωτόκολλο SNMP, διακρίνει τρία κύρια δομικά στοιχεία: (α) τις διαχειριζόμενες συσκευές (managed devices), (β) τους πράκτορες (agents), και (γ) το σύστημα διαχείρισης δικτύου (Network Management System – NMS). Οι διαχειριζόμενες συσκευές πρέπει να έχουν υλοποιημένο έναν SNMP agent, και μέσω αυτού να αποστέλλουν πληροφορίες και στατιστικά δεδομένα στο σύστημα NMS, χρησιμοποιώντας το πρωτόκολλο SNMP.

Όμως συχνά, η πληροφορία η οποία μπορεί να συλλεχθεί μέσω του πρωτοκόλλου SNMP, δεν είναι επαρκής για διαδικασίες όπως η ανίχνευση εισβολών και δικτυακών ανωμαλιών.

3.1.2 Έλεγχος του εσωτερικού των πακέτων (Deep Packet Inspection)

Μία από τις μεθόδους που χρησιμοποιούνται ευρέως, είναι η συλλογή όλων των πακέτων που διέρχονται από μία κεντρική διεπαφή μιας συνοριακής δικτυακής συσκευής, τα οποία αντιγράφονται και στέλνονται μέσω συγκεκριμένων διεπαφών των δικτυακών συσκευών. Οι διεπαφές αυτές χαρακτηρίζονται ως SPAN Interfaces ή Monitoring Ports, και σκοπός τους είναι η αντιγραφή του πακέτων που διέρχονται από ορισμένες διεπαφές μιας συσκευής και η αποστολή των αντιγράφων προς ένα σύστημα συλλογής, όπου θα γίνει λεπτομερής ανάλυσή τους. Χαρακτηριστικό παράδειγμα τέτοιου συστήματος είναι το Snort [32], το οποίο αναλύει τα πακέτα που φθάνουν σε αυτό (επικεφαλίδες και ωφέλιμο φορτίο), πραγματοποιώντας μια διαδικασία η οποία ονομάζεται deep packet inspection. Με τον τρόπο αυτό, προσπαθεί να αναγνωρίσει χαρακτηριστικά γνωρίσματα που μπορεί να υπάρχουν είτε στις επικεφαλίδες των πακέτων, είτε στα δεδομένα που εκείνα μεταφέρουν (payload), τα οποία θα το βοηθήσουν να ανιχνεύσει μια πιθανή δικτυακή ανωμαλία ή μία δικτυακή επίθεση.

Από τις μεθόδους παρακολούθησης της δικτυακής κίνησης οι οποίες αναλύονται στα 3.1.1 – 3.1.4, το deep packet inspection είναι η πιο απαιτητική, όσον αφορά στην κατανάλωση πόρων του συστήματος ανάλυσης. Εκτός από την ανάλυση περιεχομένων των πακέτων, η μέθοδος αυτή επιφορτίζει το δίκτυο με αντίγραφα της πραγματικής κίνησης, κάτι το οποίο μπορεί να συνεπάγεται τεράστιο όγκο δεδομένων, σε περιβάλλοντα με υψηλούς ρυθμούς μεταγωγής πακέτων. Ακόμη, η εξαγωγή χρήσιμων στατιστικών συμπερασμάτων μέσω αυτής της μεθόδου συλλογής δεδομένων, δεν είναι αυτονόητη διαδικασία, ακόμη και για τους πιο έμπειρους διαχειριστές δικτύων [33].

3.1.3 Το πρωτόκολλο NetFlow

Το πρωτόκολλο NetFlow [34] παρουσιάστηκε από τη Cisco, για την παροχή στους διαχειριστές των δικτύων πληροφοριών για τις ροές (flows) του δικτύου τους. Οι δικτυακές συσκευές (μεταγωγείς και δρομολογητές) οι οποίες υποστηρίζουν το πρωτόκολλο NetFlow,

συλλέγουν δεδομένα για τις ροές, και τα εξάγουν σε διαχειριστικά συστήματα (Collectors). Οι Collectors συγκεντρώνουν τα δεδομένα αυτά, προκειμένου να εξάγουν χρήσιμα συμπεράσματα. Μέσω αυτών, είναι δυνατή η εξαιρετικά λεπτομερής και αναλυτική μέτρηση στατιστικών που αφορούν τις ροές δεδομένων του δικτύου.

Για το πρωτόκολλο NetFlow, μία ροή ορίζεται ως μια ακολουθία πακέτων μονής κατεύθυνσης, τα οποία χαρακτηρίζονται από ένα σύνολο κοινών χαρακτηριστικών και διατρέχουν μία δικτυακή συσκευή. Οι ροές αυτές συλλέγονται και περιοδικά εξάγονται στο εξωτερικό διαχειριστικό σύστημα, τον NetFlow Collector. Τα στοιχεία των ροών είναι εξαιρετικά αναλυτικά, περιέχοντας πληροφορίες όπως διευθύνσεις IP, μετρητές πακέτων και bytes, χρονικές στιγμές, Type of Service bits (TOS), θύρες εφαρμογής, διεπαφές εισόδου και εξόδου του μεταγωγέα, κλπ. Το NetFlow μπορεί να παρακολουθεί και να καταγράφει όλα τα πακέτα των ροών, ή να πραγματοποιεί δειγματοληψία.

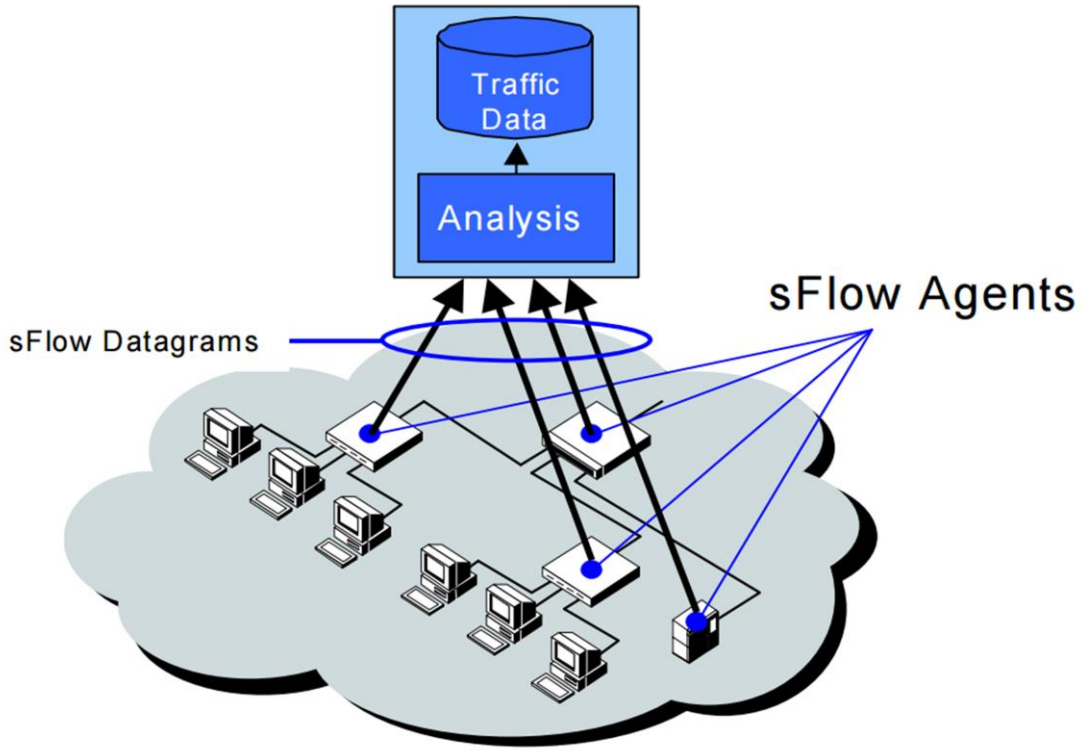
3.1.4 Το πρωτόκολλο sFlow

Το πρωτόκολλο sFlow [8] αποτελεί μία τεχνολογία δειγματοληψίας και καταγραφής επικεφαλίδων Επιπέδου 2 έως και 5 (Data-Link, Network, Transport και Application Layer) των πακέτων ενός δικτύου ανεξάρτητα από ροές. Υποστηρίζεται από πολλούς κατασκευαστές δικτυακών συσκευών, όπως η Dell, η Hewlett Packard, η NEC, κ.α., και βρίσκεται υλοποιημένο σε δρομολογητές και μεταγωγείς των κατασκευαστών αυτών από το 2001. Το sFlow παρέχει τη δυνατότητα συνεχούς δειγματοληπτικής παρακολούθησης της δικτυακής κίνησης (σε επίπεδο πακέτων) σε επιλεγμένες ή όλες τις διεπαφές (ports) μιας δικτυακής συσκευής ταυτόχρονα.

Το sFlow βασίζεται σε έναν sFlow Agent, που είναι ουσιαστικά μια διαδικασία υλοποιημένη σε λογισμικό, και η οποία προσφέρεται ως τμήμα του λογισμικού δικτυακής διαχείρισης της εκάστοτε δικτυακής συσκευής. Ο sFlow Agent συνδυάζει τους μετρητές που αφορούν κάθε διεπαφή της συσκευής, και τα δείγματα ροών σε ένα ενιαίο datagram, και τα στέλνει σε ένα εξωτερικό σύστημα συλλογής, τον sFlow Collector. Τυπικά, η δειγματοληψία πραγματοποιείται μέσω των Ολοκληρωμένων Κυκλωμάτων Ειδικών Εφαρμογών (Application-Specific Integrated Circuits - ASICs), ώστε να επιτυγχάνεται ταχύτατα η δειγματοληψία.

Ουσιαστικά, η επεξεργασία που διεξάγει ένας sFlow Agent είναι αρκετά περιορισμένη. Μόνος του στόχος, είναι συσκευασία δεδομένων μέσα σε sFlow datagrams, τα οποία

αποστέλλονται άμεσα, μέσω του δικτύου, στον sFlow Collector. Έτσι, η άμεση αποστολή των δεδομένων περιορίζει τις απαιτήσεις του sFlow Agent σε μνήμη και επεξεργαστική ισχύ. Στο Σχήμα 4 απεικονίζονται τα βασικά στοιχεία που απαρτίζουν ένα δίκτυο, στο οποίο γίνεται δειγματοληψία μέσω του πρωτοκόλλου sFlow. Οι sFlow Agents που βρίσκονται στις δικτυακές συσκευές της υποδομής, στέλνουν μία ροή sFlow datagrams προς έναν κεντρικό sFlow Collector. Εκεί, οι πληροφορίες που συλλέγονται μπορούν να αναλυθούν, με στόχο την εξαγωγή χρήσιμων συμπερασμάτων για τις ροές των πακέτων (σε πραγματικό χρόνο), και να προσφέρουν μία από-άκρο-σε-άκρο οπτική της κατάστασης του δικτύου.



Σχήμα 4: Ενδεικτική αρχιτεκτονική του sFlow: sFlow Agents και Collector.
Πηγή: http://www.sflow.org/

3.2 Παρακολούθηση δικτυακής κίνησης σε Δίκτυα Οριζόμενα από Λογισμικό

Λόγω των δυνατοτήτων προγραμματιστικής διαχείρισης των δικτύων SDN, έχουν προταθεί επιπρόσθετες μέθοδοι για την παρακολούθηση της δικτυακής κίνησης και τη συλλογή στατιστικών δεδομένων σε περιβάλλοντα SDN που υποστηρίζουν το πρωτόκολλο OpenFlow (OF).

Αρχικά, το OF προσφέρει εγγενώς μια μέθοδο συλλογής δεδομένων για τις ροές του δικτύου. Η μέθοδος αυτή, βασίζεται στην ανταλλαγή πληροφοριών μεταξύ μεταγωγέα OF και OF Controller. Όπως καθορίζεται από το πρωτόκολλο OF, ο Controller στέλνει περιοδικά αιτήματα τύπου *flow-stats request*, ζητώντας από τον εκάστοτε μεταγωγέα OF το σύνολο του πίνακα ροών που εκείνος διατηρεί, μαζί με τους αντίστοιχους μετρητές.

Στην εργασία [35] προτείνεται μία νέα μέθοδος για τη συλλογή στατιστικής πληροφορίας των ροών, με την ανάπτυξη ενός προσαρμοστικού αλγορίθμου, ο οποίος ελέγχει τη χρονική και χωρική συνάθροιση των ροών για την εξαγωγή στατιστικών μετρήσεων. Βασίζεται σε ένα μοντέλο γραμμικής πρόβλεψης, μειώνοντας έτσι τον όγκο της υπό επεξεργασία πληροφορίας. Να σημειωθεί όμως πως τέτοιες μέθοδοι απαιτούν την επέκταση του πρωτοκόλλου OF ώστε να υποστηρίζει επιπρόσθετες δυνατότητες μέσω του πεδίου Action.

Ακόμη μία υποσχόμενη μέθοδος συλλογής στατιστικών όσον αφορά της ροές δεδομένων ενός δικτύου παρουσιάζεται στην εργασία [36]. Οι συγγραφείς προτείνουν την επέκταση του OpenFlow firmware με στόχο τη δειγματοληψία σε επίπεδο ροής (flow monitoring). Κύριο χαρακτηριστικό της προσέγγισης αυτής αποτελεί η προσθήκη ενός νέου OpenFlow Action για την δειγματοληψία των ροών, μέσω του οποίου είναι δυνατή η επιλογή της μεθόδου με την οποία θα πραγματοποιηθεί η δειγματοληψία. Οι υποστηριζόμενες μέθοδοι είναι: (α) Η στοχαστική, όπου βάσει μίας προκαθορισμένης πιθανότητας να επιλεχθεί το γεγονός αντιστοίχισης ενός δεδομένου πακέτου σε μία ροή του πίνακα OpenFlow, αντιστοιχίζεται ένας τυχαίος αριθμός από 0 έως 1 σε κάθε πακέτο και εάν ο αριθμός αυτός είναι μεγαλύτερος της προκαθορισμένης πιθανότητας, τότε πραγματοποιείται η δειγματοληψία. (β) Η ντετερμινιστική, όπου για κάθε k πακέτα που αντιστοιχίζονται σε μία ροή, επιλέγονται m δείγματα, αγνοώντας τις δ αρχικές αντιστοιχίσεις. Αν και οι μέθοδοι αυτές μπορούν να προσφέρουν εξαιρετικά αποτελέσματα εάν τροφοδοτηθούν σε έναν αλγόριθμο ανίχνευσης ανωμαλιών δικτύου, εντούτοις προϋποθέτουν τη χρήση τροποποιημένου λογισμικού για την υλοποίηση του πρωτοκόλλου OpenFlow, κάτι που μπορεί να οδηγήσει σε περιπτώσεις έλλειψης συμβατότητας μεταξύ μεταγωγέων OpenFlow και OpenFlow Controller.

Στην εργασία [37] οι συγγραφείς προτείνουν την παθητική συλλογή στατιστικών δεδομένων εκμεταλλευόμενοι τη ανταλλαγή σηματοδοσίας μεταξύ μεταγωγέων OpenFlow και OpenFlow Controller. Συγκεκριμένα, χρησιμοποιούνται τα γεγονότα *Packet-In* και *Flow-Removed* που αντιλαμβάνεται ο Controller, αντίστοιχα όταν ένα νέο πακέτο αστοχεί στον πίνακα ροών του μεταγωγέα ή όταν μία ροή εκπνέει. Έτσι δίνεται η δυνατότητα

υπολογισμού του μέσου βαθμού χρήσης των ζεύξεων, βάσει των μετρητών που διατηρούνται για κάθε εγγραφή του πίνακα ροών ενός μεταγωγέα OpenFlow, και για όσο διάστημα η εγγραφή αυτή είναι ενεργή. Όμως, ο αριθμός των πακέτων που αντιστοιχούν σε κάθε ροή γίνεται γνωστός μόνο όταν η αντίστοιχη εγγραφή λήξει, και κατά συνέπεια η μέθοδος αυτή δεν μπορεί να υιοθετηθεί για την ανίχνευση ανωμαλιών δικτύου σε πραγματικό χρόνο.

Τέλος, οι συγγραφείς στο [1] προτείνουν την χρήση της τεχνικής mirroring, ώστε να αποστέλλονται αντίγραφα των πακέτων σε συσκευή υπεύθυνη για την παρακολούθηση του δικτύου. Όμως, συνήθως, τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems – IDS) ή οι αλγόριθμοι Ανίχνευσης Ανωμαλιών χρειάζονται είτε το ωφέλιμο φορτίου μερικών πακέτων, είτε τις επικεφαλίδες κάθε πακέτου. Έτσι, δημιουργώντας πλήρη αντίγραφα όλων των πακέτων, μπορεί να οδηγηθούμε σε άσκοπη κατανάλωση πολύτιμων δικτυακών πόρων.

4 Ανίχνευση και Αντιμετώπιση Ανωμαλιών Δικτύου

Μέσω των ανωτέρω μεθόδων, είναι δυνατή η συλλογή στατιστικής πληροφορίας για τις ροές δεδομένων δικτύων, είτε αυτά είναι σύγχρονα SDN δίκτυα είτε όχι. Η πληροφορία αυτή μπορεί να χρησιμοποιηθεί για την ανίχνευση δικτυακών ανωμαλιών, με απώτερο στόχο την ανίχνευση και την αποτροπή ή τον περιορισμό δικτυακών επιθέσεων. Στην ενότητα αυτή περιγράφονται μερικές από τις πιο γνωστές εμπορικές λύσεις για προστασία υποδομών και υπηρεσιών από δικτυακές επιθέσεις. Επιπλέον, παρουσιάζονται διαφορετικές προσεγγίσεις που στηρίζονται στην ανίχνευση ανωμαλιών δικτύου, έχοντας ως στόχο την ανίχνευση ανωμαλιών που προέρχονται κυρίως από επιθέσεις όπως είναι οι Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (Distributed Denial of Service attacks - DDoS) [38] και οι αυτοδιαδιδόμενοι ιοί (Worms) [39]. Τέλος παρατίθενται κάποιες αντιπροσωπευτικές ερευνητικές προσεγγίσεις που έχουν προταθεί για την (συνεργατική ή μη) αντιμετώπιση δικτυακών επιθέσεων.

4.1 Εμπορικές Υπηρεσίες Αντιμετώπισης Δικτυακών Επιθέσεων DDoS

Οι σύγχρονες επιθέσεις DDoS δεν αποσκοπούν μόνο στην εξάντληση του διαθέσιμου εύρους ζώνης, αλλά μπορεί να στοχεύουν (α) στον περιορισμό της λειτουργικότητας εσωτερικών δικτυακών συσκευών της υποδομής οι οποίες λαμβάνουν αποφάσεις με βάση την κατάσταση των συνδέσεων (TCP connection state) όπως Intrusion Prevention Systems (IPS) ή Firewalls, και (β) στον περιορισμό πρόσβασης σε συγκεκριμένες εφαρμογές όπως HTTP, Voice over IP (VoIP), DNS, SMTP κ.α. Κοινοί τύποι επιθέσεων DDoS είναι οι:

- *Volumetric DDoS (Ογκομετρική Επίθεση DDoS):* Οι επιθέσεις αυτές πραγματοποιούνται από κατανεμημένα συνεργαζόμενα μολυσμένα συστήματα, τα οποία μεταδίδουν φαινομενικά καλοήθη κίνηση, προσπαθώντας να εξαντλήσουν το διαθέσιμο εύρος ζώνης στο εσωτερικό της δικτυακής περιοχής που εξυπηρετεί μία υπηρεσία-στόχο ή μεταξύ της υπηρεσία αυτής και του υπόλοιπου Internet.
- *TCP State-Exhaustion DDoS*: Τέτοιες επιθέσεις αποσκοπούν στην υπερχείλιση των πινάκων κατάστασης σύνδεσης (π.χ. connection state tables σε Stateful Firewalls [40]) οι οποίοι αποτελούν κύριο χαρακτηριστικό σε δικτυακό εξοπλισμό παραγωγής, όπως Ισοσταθμιστές Κίνησης (Load-Balancers), Τείχη Προστασίας (Firewalls) και Εξυπηρετητές Υπηρεσιών (Application Servers)

- *Application Layer DDoS*: Οι επιθέσεις αυτές είναι αρκετά αποτελεσματικές αφού μπορούν με σχετικά χαμηλό ρυθμό αποστολής πακέτων να επηρεάσουν την ικανότητα ενός εξυπηρετητή να επικοινωνήσει με τους πελάτες του. Χαρακτηριστικό παράδειγμα είναι οι επιθέσεις τύπου HTTP GET flood, οι οποίες αναγκάζουν τους εξυπηρετητές να απαντήσουν σε πολλαπλά HTTP ερωτήματα που προέρχονται από μολυσμένες υπολογιστικά δίκτυα (botnets). Στοχεύοντας συγκεκριμένα στην υπηρεσία HTTP και όχι στο διαθέσιμο δικτυακό εύρος ζώνης είναι συνήθως πιο εύκολο να αποκοπεί ένας εξυπηρετητής.

Οι εμπορικές μέθοδοι αντιμετώπισης δικτυακών επιθέσεων μπορούν να διαχωριστούν στις ακόλουθες κατηγορίες: (i) *On-Premise*, όπου τοποθετείται στην υπό προστασία υποδομή εξοπλισμός ειδικού σκοπού, (ii) *Cloud Platforms*, δηλαδή μέσω υπηρεσιών νέφους οι οποίες προσφέρουν λειτουργικότητα Δικτύων Διανομής Περιεχομένου (Content Delivery Network – CDN), και (iii) *Hybrid*, δηλαδή μέσω υβριδικών προσεγγίσεων των δύο παραπάνω μεθόδων.

Ενδεικτικά, η εταιρία Arbor Networks [41] προσφέρει λύσεις On-Premise και Hybrid για την προστασία δικτυακών υποδομών από επιθέσεις DDoS, μέσω των συνολικών λύσεων Arbor Peakflow και Arbor Cloud αντίστοιχα. Συγκεκριμένα, η μονάδα Arbor Peakflow SP είναι υπεύθυνη για το συνδυασμό δεδομένων που συλλέχθηκαν μέσω πρωτοκόλλων NetFlow, SNMP, BGP, αλλά και μέσω deep-packet inspection, ώστε να δημιουργηθούν συγκεκριμένα προφίλ για κάθε εξυπηρετητή της υποδομής. Τα προφίλ αυτά μπορεί να αφορούν το ρυθμό μετάδοσης πακέτων, το μέγιστο και ελάχιστον όγκο πακέτων, κ.α. Στη συνέχεια, εφόσον αναγνωριστούν ανωμαλίες βάσει απόκλισης των τιμών από τα προφίλ που δημιουργήθηκαν, το δικτυακό στοιχείο Επιπέδου Δεδομένων Arbor Peakflow TMS (Threat Management System) [42] μπορεί να αναγνωρίσει και να αποκόψει την κακόβουλη κίνηση που σχετίζεται με επιθέσεις DDoS. Τέτοιες επιθέσεις αντιμετωπίζονται μέσω εγκατάστασης του TMS «εν σειρά» στη δικτυακή υποδομή, ή σε νεότερη έκδοση, μέσω αναδρομολόγηση της κίνησης προς το TMS το οποίο αναγνωρίζει και αποκόπτει τα κακόβουλα πακέτα. Να σημειωθεί ότι στην εργασία αυτή (Κεφάλαιο 6) προτείνεται αντίστοιχος μηχανισμός με χρήση πρωτοκόλλων SDN τα οποία προσφέρουν δυνατότητες προγραμματισμού και ανοιχτών APIs.

Επιπλέον, η Arbor ακολουθώντας την τάση για εικονικοποίηση (virtualization) δικτυακών υπηρεσιών, και σε συνεργασία με την Cisco, υλοποίησαν το δρομολογητή Cisco ASR 9000 vDDoS Protection. Μέσω του δρομολογητή αυτού είναι δυνατή η υλοποίηση του TMS ως εικονική υπηρεσία (virtual function) του δρομολογητή, αυξάνοντας της

δυνατότητες κλιμακώσιμης αντιμετώπισης κατανεμημένων επιθέσεων μεγάλης κλίμακας. Στην περίπτωση της υβριδικής προσέγγισης (Arbor Cloud), αντί του TMS, η κίνηση του θύματος μίας δικτυακής επίθεσης δρομολογείται προς υποδομές νέφους (scrubbing centers) όπου γίνεται ο διαχωρισμός και αποκοπή της κακόβουλης κίνησης.

Οι πλατφόρμες νέφους (Cloud Platforms) προσφέρουν μία εναλλακτική προσέγγιση για την αντιμετώπιση κατανεμημένων επιθέσεων, αποφεύγοντας την αγορά ακριβού και κλειστού εμπορικού εξοπλισμού. Αφού οι ογκομετρικές κατανεμημένες επιθέσεις στηρίζονται στη δημιουργία υπέρμετρα μεγάλου δικτυακού φορτίου, οι πλατφόρμες νέφους αναδρομολογούν την κίνηση του θύματος μέσω CDNs ώστε να εξυπηρετούνται όγκοι δικτυακής κίνησης που μπορεί να φτάνουν τα 400Gbps [43] χωρίς να διακόπτονται οι δικτυακές υπηρεσίες που εξυπηρετούν το υποδίκτυο του θύματος μέσα στο παγκόσμιο Internet. Χαρακτηριστικά παραδείγματα τέτοιων υπηρεσιών προσφέρουν οι εταιρίες Incapsula [44] και CloudFlare [45]. Συγκεκριμένα, σε περίπτωση επίθεσης DDoS η εταιρία Incapsula ακούει και στη συνέχεια μεταδίδει μηνύματα τύπου BGP Announcement εκ μέρους του δρομολογητή του πελάτη, αφού πρώτα εγκαθιδρύσει ένα τούνελ GRE μεταξύ του δρομολογητή του πελάτη και της δικής της υπηρεσίας. Συνεπώς, όλη η κίνηση του θύματος διαχειρίζεται από τους εξυπηρετητές του Cloud Platform, και αφού αποκοπεί η κακόβουλη κίνηση, τα υπόλοιπα πακέτα επαναδρομολογούνται προς το θύμα της επίθεσης. Αξίζει να σημειωθεί πως ο αριθμός των Data Center ανά τον κόσμο που τροφοδοτούν τις υπηρεσίες αντιμετώπισης επιθέσεων DDoS ακόμη και μεγαλύτερων του 1Tbps, ανέρχεται σε 28 για την Incapsula και 76 για την CloudFlare.

4.2 Μέθοδοι Ανίχνευσης Ανωμαλιών Δικτύου

Μια διαδεδομένη κατηγορία μεθόδων ανίχνευσης ανωμαλιών βασίζεται στην έννοια της εντροπίας [46] η οποία χαρακτηρίζει τις κατανομές συγκεκριμένων μετρικών σχετικών με την κίνηση του δικτύου. Η εντροπία μετρά την τυχαιότητα ενός συνόλου στοιχείων. Οι υψηλές τιμές εντροπίας δηλώνουν μια διασκορπισμένη κατανομή πιθανότητας των στοιχείων, ενώ οι χαμηλές τιμές εντροπίας δηλώνουν τη συγκέντρωση της κατανομής γύρω από συγκεκριμένα στοιχεία. Η εντροπία έχει χρησιμοποιηθεί εκτενώς για την ανίχνευση worms στις εργασίες [47], [48], [6]. Συνήθεις κατανομές χαρακτηριστικών γνωρισμάτων της κίνησης του δικτύου που είναι πολύτιμες στην ανίχνευση ανωμαλιών δικτύων είναι οι κατανομές διευθύνσεων IP πηγής (source IP address), διευθύνσεων IP προορισμού

(destination IP address), θύρας πηγής (TCP/UDP source port) και θύρας προορισμού (TCP/UDP destination port). Παραδείγματος χάριν, μια επίθεση τύπου worm propagation που προέρχεται από ένα μολυσμένο υπολογιστή που προσπαθεί να μολύνει άλλους υπολογιστές στο Διαδίκτυο, οδηγεί στη μείωση της εντροπίας των διευθύνσεων IP πηγής. Η μολυσμένη μηχανή παράγει έναν μεγάλο αριθμό ροών αναγκάζοντας την ίδια διεύθυνση IP πηγής να κυριαρχεί στη κατανομή ροών των διευθύνσεων IP πηγής.

Μία άλλη κατηγορία αλγορίθμων ανίχνευσης ανωμαλιών δικτύου αποτελούν οι αλγόριθμοι Ανίχνευσης με Αλλαγή Χρονικής Στιγμής (Change Point Detection) [49], [50], [51] οι οποίοι μπορούν και απομονώνουν την αλλαγή ενός στατιστικού στοιχείου του δικτύου που προκαλείται συνήθως από επιθέσεις. Αυτοί οι αλγόριθμοι αποθηκεύουν τα στοιχεία κίνησης του δικτύου ως μία χρονική ακολουθία (χρονοσειρά). Εάν μια επίθεση αρχίσει στη χρονική στιγμή *t*, η χρονική ακολουθία θα παρουσιάσει κάποια στατιστική αλλαγή γύρω από το χρονική στιγμή *t* και μετέπειτα. Ένα παράδειγμα τέτοιου αλγορίθμου είναι ο αλγόριθμος CUSUM (Cumulative Sum). Για να εντοπίσει μια επίθεση, ο CUSUM προσδιορίζει τις αποκλίσεις ανάμεσα στις πραγματικές τιμές και στις αναμενόμενες μέσες τιμές της χρονικής ακολουθίας. Εάν η διαφορά υπερβαίνει κάποιο ανώτατο όριο, οι επαναλαμβανόμενες αυξήσεις στα στατιστικά του CUSUM θα σηματοδοτήσουν την ανίχνευση μιας επίθεσης. Κατά τη διάρκεια των χρονικών διαστημάτων που περιέχουν μόνο κανονική κίνηση στο δίκτυο, η διαφορά είναι κάτω από αυτό το όριο. Μέσω του καθορισμού του ορίου, ο αλγόριθμος CUSUM μπορεί να επηρεαστεί σε σχέση με την καθυστέρηση της ανίχνευσης και τα και λανθασμένα ποσοστά ανίχνευσης.

4.3 Ανίχνευση Ανωμαλιών Δικτύου σε Δίκτυα Οριζόμενα από Λογισμικό

Η πρώτη προσέγγιση για δημιουργία ενός μηχανισμού IDS το οποίο θα βασίζεται σε στατιστικά ροών και θα εκμεταλλεύεται τις δυνατότητες του OF εμφανίστηκε στην εργασία [52], όπου το πρωτόκολλο OF χρησιμοποιήθηκε για να διαχειριστεί ταυτόχρονα την προώθηση πακέτων αλλά και τη συλλογή στατιστικών στοιχείων για τις ροές πακέτων. Στην εργασία αυτή δεν έγινε καμία ανάλυση σχετικά με προβλήματα που μπορεί να προκύψουν λόγω (α) του περιορισμένου μεγέθους των πινάκων ροών και (β) της επιβάρυνσης του Επιπέδου Ελέγχου εξαιτίας των συνεχών αναζητήσεων στους πίνακες ροών για την ανάκτηση των αντίστοιχων μετρητών. Επιπλέον, η προτεινόμενη μέθοδος προσεγγίζει μόνο την ανίχνευση επιθέσεων DDoS, ενώ η ανάλυση της αποδοτικότητας του

αλγορίθμου περιορίζεται μόνο στον προτεινόμενο αλγόριθμο και όχι στις συνολικές επιδόσεις του συστήματος. Τέλος, δεν γίνεται καμία αναφορά στις επιπτώσεις των δικτυακών ανωμαλιών στο Επίπεδο Ελέγχου του SDN δικτύου.

Μία επόμενη προσπάθεια για ανίχνευση ανωμαλιών σε περιβάλλοντα SDN εμφανίζεται στην εργασία [53], όπου υλοποιούνται ετερογενείς αλγόριθμοι ανίχνευσης ανωμαλιών, αποσκοπώντας στην επιβεβαίωση της καταλληλότητάς τους για χρήση σε περιβάλλοντα Small Office / Home Office (SOHO). Οι συγγραφείς πρότειναν τον αποκεντρωμένο έλεγχο κατανεμημένων δικτυακών συσκευών χαμηλών επιδόσεων για αποτελεσματική ανίχνευση και αντιμετώπιση των επιθέσεων κοντά στην πηγή τους. Λόγω της προσήλωσης σε περιβάλλοντα SOHO, η εργασία τους παρουσιάζει πειραματικά αποτελέσματα για την αποδοτικότητα αλγορίθμων ανίχνευσης ανωμαλιών/εισβολών σε χαμηλούς ρυθμούς μετάδοσης πληροφορίας (από 60 έως 12.000 πακέτα ανά δευτερόλεπτο). Επιπλέον, η αντιμετώπιση των ανιχνευμένων ανωμαλιών αφήνεται ως μελλοντική εργασία, χωρίς να προτείνεται καμία προσέγγιση για το θέμα αυτό. Να σημειωθεί πως στα πλαίσια της παρούσας διατριβής μελετούνται συστήματα ανίχνευσης ανωμαλιών βασισμένα σε μεταγωγείς OF ικανούς να εξυπηρετήσουν ροές δεδομένων οι οποίες χαρακτηρίζονται από υψηλό ρυθμό μετάδοσης πληροφορίας (έως 130.000 πακέτα ανά δευτερόλεπτο), αναλύοντας πιθανούς περιορισμούς της χωρητικότητας του πίνακα ροών των μεταγωγέων, και τις επιπτώσεις των ανωμαλιών στο Επίπεδο Ελέγχου.

4.4 Αντιμετώπιση Ανωμαλιών Δικτύου

Η προστασία των δικτυακών συσκευών από κακόβουλες επιθέσεις, και εν γένει η επιβολή πολιτικών για την ασφάλεια μίας δικτυακής υποδομής, έχει αποδειχθεί ότι αποτελεί μία πολύ κρίσιμη υπηρεσία των σύγχρονων δικτύων.

Η αντιμετώπιση δικτυακών ανωμαλιών (π.χ. Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας - DDoS) επιτυγχάνεται παραδοσιακά μέσω εγκαθίδρυσης λίστας ελέγχου πρόσβασης (access control list) είτε σε δικτυακή συσκευή στην περιοχή του θύματος, είτε στο ίδιο το λειτουργικό σύστημα του εξυπηρετητή ο οποίος είναι το θύμα της εκάστοτε επίθεσης [54]. Μέσω της πρακτικής αυτής κατασπαταλώνται δικτυακοί πόροι, ενώ συνήθως απαιτείται και η εγκατάσταση εξοπλισμού υψηλών προδιαγραφών ακριβώς πριν από το σημείο όπου θα αντιμετωπιστεί η ανωμαλία. Ο εξοπλισμός αυτός θα πρέπει να είναι ικανός να εξυπηρετήσει σημαντικό όγκο κακόβουλης κίνησης σε περιπτώσεις επιθέσεων.

Εναλλακτικά, ο πάροχος του θύματος μπορεί να προσφέρει λύση εγκαθιδρύοντας λίστες πρόσβασης ή εξοπλισμό συγκεκριμένου σκοπού (π.χ. Firewall) κοντά στο άκρο του δικτύου του. Όμως η μέθοδος αυτή αυξάνει σημαντικά το λειτουργικό κόστος του παρόχου, ειδικά αν αναλογιστεί κανείς των αριθμό πελατών τους οποίους πρέπει να εξυπηρετεί –και να προστατεύει- ο πάροχος.

Νεότερες προτάσεις στηρίζονται στην αρχιτεκτονική NFV, σύμφωνα με την οποία υπηρεσίες προστασίας της δικτυακής υποδομής υλοποιούνται και εγκαθίστανται ως Εικονικοποιημένες Δικτυακές Λειτουργίες (Virtualised Network Functions - VNFs [55]). Ειδικότερα, η αποσυσχέτιση των Επιπέδων Ελέγχου και Προώθησης Δεδομένων που προσφέρουν τα πρωτόκολλα SDN, και συγκεκριμένα το πρωτόκολλο OpenFlow, ενισχύει τις δυνατότητες για εικονικοποίηση και δυναμικό διαχωρισμό δικτυακών υπηρεσιών όπως η προστασία από δικτυακές επιθέσεις. Έτσι, επιτρέπεται ο σχεδιασμός και η εγκατάσταση κλιμακώσιμων υπηρεσιών, πιθανόν σε κατανεμημένα συστήματα, τα οποία όμως ελέγχονται ως μία ενιαία λογική εφαρμογή.

Μία τέτοια προσέγγιση παρουσιάστηκε στην εργασία [56], όπου παρουσιάζεται μία γλώσσα scripting, υποστηριζόμενη από μία εφαρμογή για OpenFlow Controller, η οποία επιτρέπει την παραγωγή και επιβολή περιορισμών στις νέες εγγραφές OpenFlow. Στόχος είναι η προστασία της δικτυακής υποδομής ή των εξυπηρετητών που μπορεί να φιλοξενούνται σε μία τέτοια υποδομή. Η σχετική εργαλειοθήκη υποστηρίζει την δημιουργία υπομονάδων-ελεγκτών για συνεργασία της συγκεκριμένης εφαρμογής με δημοφιλείς εφαρμογές ασφάλειας δικτύων (π.χ. Snort). Βέβαια η συγκεκριμένη προσέγγιση προϋποθέτει ότι το σύνολο των παραδοσιακών δικτυακών μεταγωγέων της προστατευόμενης υποδομής, έχουν αντικατασταθεί από αντίστοιχους μεταγωγείς οι οποίοι υποστηρίζουν το πρωτόκολλο OpenFlow.

Όπως έχει προαναφερθεί, οι εφαρμογές ασφάλειας δικτύων είναι στενά συνδεδεμένες με την επιβολή πολιτικών τόσο στα παραδοσιακά δίκτυα, όσο και σε δίκτυα νέας γενιάς τα οποία υποστηρίζουν πρωτόκολλα SDN και έχουν υλοποιηθεί ακολουθώντας τις σύγχρονες αρχιτεκτονικές τύπου NFV. Ένα χαρακτηριστικό παράδειγμα για την επιβολή πολιτικών σε δίκτυα SDN παρουσιάζεται στην εργασία [57], όπου μέσω μίας συγκεκριμένης εργαλειοθήκης (framework) είναι δυνατός ο καθορισμός δυναμικών πολιτικών για τον έλεγχο πρόσβασης σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο OpenFlow.

4.5 Συνεργασία Αυτόνομων Συστημάτων για Αντιμετώπιση Ανωμαλιών Δικτύου

Συχνά, οι διαχειριστές μεγάλων δικτυακών υποδομών καλούνται να αντιμετωπίσουν κατανεμημένες επιθέσεις τύπου DDoS, όπου κάποιος από τους εξυπηρετητές οι οποίοι φιλοξενούνται στην δεδομένη υποδομή δέχεται πολύ περισσότερα αιτήματα (ή όγκο κίνησης) από όσα μπορεί να εξυπηρετήσει. Μια ειδική κατηγορία τέτοιων επιθέσεων είναι η περίπτωση των Amplification DDoS Attacks, όπου πολλαπλά πακέτα μικρού μεγέθους στέλνονται από κατανεμημένες πηγές μέσω του Internet, αλλά η απάντηση σε κάθε ένα πακέτο είναι πολλαπλάσιου μεγέθους (π.χ DNS Amplification Attacks [4]). Τέτοιες επιθέσεις χαρακτηρίζονται όχι μόνο από πάρα πολλές κακόβουλες πηγές (συχνά με πλαστογραφημένες διευθύνσεις IP), αλλά και από τεράστιο όγκο δεδομένων ο οποίος μπορεί να δημιουργήσει προβλήματα τόσο στον εξυπηρετητή-στόχο, όσο και στη δικτυακή υποδομή η οποία τον εξυπηρετεί.

Σε τέτοιες περιπτώσεις κατανεμημένων επιθέσεων μπορεί, να αποδειχθεί ιδιαίτερα χρήσιμη η συνεργασία γειτονικών δικτυακών περιοχών οι οποίες αναμεταδίδουν υποσύνολα της κακόβουλης κίνησης. Ένα τέτοιο μοντέλο συνεργασίας προτείνεται στην προσέγγιση FireCircle [58], με την υιοθέτηση του BGP Flowspec [59], μέσω του οποίου μπορούν να διαδοθούν, μεταξύ συνορευόντων δικτυακών περιοχών, κανόνες για την αποκοπή κακόβουλων πηγών. Τα προτερήματα της εν λόγω προσέγγισης έγκεινται: (α) στην αντιστοίχηση και αποκοπή ροών δεδομένων βάσει πληροφοριών Επιπέδου 3 και Επιπέδου 4, και (β) στον διαμοιρασμό και μεταφορά της διαδικασίας αποκοπής πιο κοντά στις πηγές. Παρά τα πλεονεκτήματά της, η μέθοδος αυτή προϋποθέτει την υποστήριξη του πρωτοκόλλου BGP Flowspec (που ακόμη δεν είναι καθολικά υιοθετημένη), ενώ απαιτεί χειροκίνητη εισαγωγή-στόχευση ξεχωριστά για κάθε μία εκ των κακόβουλων πηγών οι οποίες μπορεί να ανέρχονται σε χιλιάδες.

Μία ακόμη μέθοδος συνεργατικής αντιμετώπισης κατανεμημένων επιθέσεων προτείνεται στην εργασία [60]. Οι συγγραφείς προτείνουν αρχικά την εισαγωγή του IP Option *Record-Route (RR)* προκειμένου να αναγνωρίζονται οι κακόβουλες πηγές οι οποίες συμμετέχουν σε μία κατανεμημένη επίθεση. Μόλις αναγνωριστεί μία τέτοια πηγή εγκαθίσταται ένας κανόνας στην πύλη εισόδου (gateway) του θύματος για την αποκοπή της πηγής αυτής. Στη συνέχεια, επιδιώκεται η επικοινωνία με το κοντινότερο δυνατό -στην πηγή- συνοριακό δρομολογητή, από τον οποίο και ζητείται η αποκοπή της κακόβουλης πηγής. Ένα πλεονέκτημα της συγκεκριμένης μεθόδου προκύπτει από τη χρήση της επιλογής

RR, μέσω της οποίας μπορεί να εντοπιστεί η κακόβουλη πηγή ακόμη και αν έχει πλαστογραφηθεί η διεύθυνσή της (IP spoofing). Όμως η επιλογή RR χαρακτηρίζεται από αναξιόπιστη λειτουργικότητα και για το λόγο αυτό συνήθως δεν είναι ενεργοποιημένη στους δρομολογητές του Internet.

5 Ανίχνευση και Αντιμετώπιση Ανωμαλιών σε Περιβάλλοντα SDN

5.1 Εισαγωγή

Στη βιβλιογραφία εμφανίζονται ποικίλες μέθοδοι ανίχνευσης δικτυακών ανωμαλιών μέσω της επεξεργασίας στατιστικών δεδομένων που αφορούν τις δικτυακές ροές που παρατηρούνται σε ένα δεδομένο δίκτυο. Τέτοιες μέθοδοι, όπως αναφέρεται και στις αναφορές [5], [6], [7] έχουν αποδειχθεί ικανές να ανιχνεύσουν χαρακτηριστικά για δικτυακές ανωμαλίες όλων των ειδών, είτε αυτές είναι καλόβουλες είτε κακόβουλες. Ανάμεσα στις μεθόδους αυτές, η ανίχνευση μέσω μεταβολής της εντροπίας συγκεκριμένων χαρακτηριστικών των δικτυακών ροών έχει αποδειχθεί αρκετά αποδοτική, ειδικότερα λόγω της ικανότητάς της να χαρακτηρίζει την τυχαιότητα των στοιχείων ενός συνόλου δεδομένων, καταδεικνύοντας έτσι πιθανές δικτυακές ανωμαλίες [61], [62].

Αρχικός στόχος της παρούσας διατριβής είναι η ανίχνευση δικτυακών ανωμαλιών σε δίκτυα SDN, μέσω απότομων μεταβολών της εντροπίας συγκεκριμένων μετρικών που θα αναλυθούν στη συνέχεια. Σημαντικός παράγοντας στην προσπάθεια αυτή είναι η μέθοδος συλλογής στατιστικών δεδομένων για τις ροές (flow-based monitoring). Για το σκοπό αυτό υλοποιήθηκαν και συγκρίθηκαν δύο μέθοδοι: (α) συλλογή μέσω της εγγενούς μεθόδου συλλογής στατιστικών δεδομένων που προσφέρει το OF πρωτόκολλο, και (β) συλλογή μέσω του πρωτοκόλλου sFlow το οποίο στηρίζεται στη δειγματοληψία πακέτων και την εξαγωγή των επικεφαλίδων τους. Παράλληλα, μελετείται η επίδραση της κάθε μεθόδου στην ακρίβεια των αποτελεσμάτων της διαδικασίας ανίχνευσης ανωμαλιών που υιοθετήθηκε, καταγράφοντας αντίστοιχες καμπύλες Receiver Operating Characteristic (ROC curves). Επιπροσθέτως, διερευνείται η αξιολογείται η καταλληλότητα των προαναφερθέντων μηχανισμών συλλογής στατιστικών δεδομένων για την τροφοδότηση και άλλων γνωστών μεθόδων ανίχνευσης ανωμαλιών. Τέλος προτείνεται ένας μηχανισμός ο οποίος, εκμεταλλευόμενος τις δυνατότητες του OF για δυναμική δημιουργία και εφαρμογή κανόνων προώθησης πακέτων μέσω του OF Controller, είναι ικανός να αντιμετωπίσει τυχόν ανιχνευθείσες δικτυακές ανωμαλίες.

5.2 Σχεδιαστικές Αρχές και Περιγραφή Αρχιτεκτονικής

5.2.1 Σχεδιαστικές αρχές

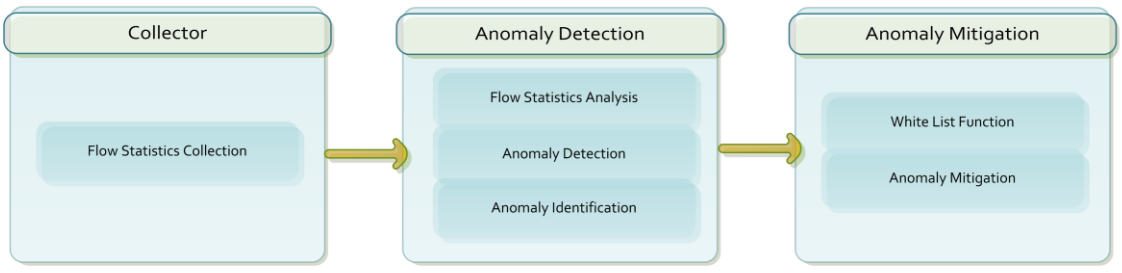
Οι σχεδιαστικές αρχές της προτεινόμενης αρχιτεκτονικής για την ανίχνευση ανωμαλιών και την αντιμετώπισή τους, σε περιβάλλοντα SDN, είναι:

- *Αρθρωτός σχεδιασμός για πλήρη αποσυσχέτιση των διαδικασιών συλλογής δεδομένων, ανίχνευσης ανωμαλιών και αντιμετώπισης ανωμαλιών.*

  Ο σχεδιασμός περιλαμβάνει τρία δομικά στοιχεία (modules) τα οποία διαχωρίζουν λογικά τις απαιτούμενες διεργασίες, όπως φαίνεται στο Σχήμα 5. Το πρώτο στοιχείο είναι υπεύθυνο για τη συλλογή στατιστικών δεδομένων για τις ροές πακέτων. Η σχεδίαση και η μέθοδος υλοποίησης του συγκεκριμένου στοιχείου, επιτρέπουν την εφαρμογή διαφόρων μεθόδων για τη συλλογή της απαιτούμενης πληροφορίας. Το σύνολο των στατιστικών δεδομένων που θα συλλεχθεί θα αναλυθεί από το δεύτερο κύριο δομικό στοιχείο της αρχιτεκτονικής, το οποίο είναι υπεύθυνο για την ανίχνευση δικτυακών ανωμαλιών και την αναγνώριση του θύματος της επίθεσης. Η επιλογή κατάλληλου αλγορίθμου εξαρτάται κυρίως από το εκάστοτε δικτυακό περιβάλλον και τα χαρακτηριστικά δικτυακής κίνησης. Τέλος, το τρίτο δομικό στοιχείο είναι υπεύθυνο για τον περιορισμό της κακόβουλης κίνησης και στηρίζεται στην εκμετάλλευση δυνατοτήτων του πρωτοκόλλου OF για δυναμική μεταβολή των κανόνων προώθησης.

- *Συμβατότητα με συσκευές OpenFlow Επιπέδου 2 και Επιπέδου 3.*

  Η προτεινόμενη αρχιτεκτονική αποσυνδέει πλήρως τη συλλεχθείσα στατιστική πληροφορία από τις διαδικασίες ανίχνευσης και αντιμετώπισης ανωμαλιών. Κατά συνέπεια, μπορεί να χρησιμοποιηθεί οποιοδήποτε είδος δικτυακών συσκευών, με μόνη προϋπόθεση την υποστήριξη του πρωτοκόλλου OpenFlow v1.0 ή νεότερου. Οι



Σχήμα 5: Αρχιτεκτονική άποψη του προτεινόμενου συστήματος για περιβάλλοντα SDN.

συσκευές αυτές μπορεί να υποστηρίζουν είτε λειτουργίες προώθησης Επιπέδου 2 (μεταγωγείς οι οποίοι στην πλειοψηφία τους υποστηρίζουν το πρωτόκολλο sFlow), είτε λειτουργίες δρομολόγησης Επιπέδου 3 (μεταγωγείς-δρομολογητές οι οποίοι συχνά υποστηρίζουν το πρωτόκολλο NetFlow [34]).

- *Εξάλειψη περιορισμών σχετικών με το OpenFlow που μπορεί να προκύψουν κατά τη διαδικασία συλλογής στατιστικής πληροφορίας.*
  Σε περιβάλλοντα τα οποία υποστηρίζουν αμιγώς το πρωτόκολλο OpenFlow, η συλλογή στατιστικών απαιτεί πρόσβαση στους μετρητές κάθε εγγραφής η οποία είναι αποθηκευμένη στον πίνακα ροών κάθε συσκευής OpenFlow. Συνεπώς, δεν μπορούν να χρησιμοποιηθούν συγκεντρωτικοί κανόνες μιας και οι αλγόριθμοι ανίχνευσης ανωμαλιών απαιτούν στατιστικά για κάθε μεμονωμένη ροή δεδομένων (micro-flow). Ως micro-flow ορίζεται το σύνολο των πακέτων τα οποία έχουν στις επικεφαλίδες μία κοινή διεύθυνση IP πηγής και μία κοινή διεύθυνση προορισμού, ενώ ταυτόχρονα έχουν κοινή πόρτα πηγής Επιπέδου 4 και κοινή πόρτα προορισμού Επιπέδου 4. Όμως ειδικά σε περιπτώσεις σημαντικής αύξησης των μεμονωμένων ροών (όπως π.χ. σε επιθέσεις DDoS), απαιτείται συνήθως η χρήση συγκεντρωτικών κανόνων. Στην παρούσα εργασία προτείνεται μία νέα μέθοδος που στηρίζεται στη χρήση του πρωτοκόλλου sFlow, μέσω της οποίας αποφεύγεται η χρήση των εγγενών μεθόδων του OpenFlow για συλλογή στατιστικών δεδομένων. Έτσι, εξαλείφεται η απαίτηση για πρόσβαση στους μετρητές πακέτων κάθε ροής ξεχωριστά, ενώ μπορεί –χωρίς να επηρεάζεται πλέον η διαδικασία ανίχνευσης ανωμαλιών- να εφαρμοστεί οποιοσδήποτε αλγόριθμος απαιτείται για την εγκαθίδρυση κανόνων προκειμένου να προωθούνται κατάλληλα τα πακέτα. Ταυτόχρονα, αποφορτίζεται το Επίπεδο Ελέγχου, αφού δεν χρησιμοποιείται πλέον το πρωτόκολλο OF για την παρακολούθηση της δικτυακής κίνησης. Σε διαφορετική περίπτωση, κάνοντας χρήση των εγγενών μεθόδων παρακολούθησης και καταμέτρησης, οι δικτυακές ανωμαλίες οδηγούν και σε εκτεταμένη ανταλλαγή μηνυμάτων μεταξύ ενός μεταγωγέα OF και ενός OF Controller, προκαλώντας συμφόρηση στο Επίπεδο Ελέγχου.

- *Εκμετάλλευση των αποσυσχετισμένων Επιπέδων Ελέγχου και Δεδομένων για ταχεία ανίχνευση και αντιμετώπιση δικτυακών ανωμαλιών σε πραγματικό χρόνο.*
  Η διαδικασία ανίχνευσης ανωμαλιών είναι εξαιρετικά απαιτητική όσον αφορά τους πόρους συστήματος (επεξεργαστικοί κύκλοι και μνήμη RAM), και προς το παρόν δεν είναι δυνατή η εκτέλεση τέτοιων αλγορίθμων σε δικτυακό εξοπλισμό. Παράλληλα, η

αντιμετώπιση των ανωμαλιών σε πραγματικό χρόνο απαιτεί μηχανισμούς ικανούς για ταχεία επαναπροσαρμογή των αλγορίθμων προώθησης πακέτων. Για τον λόγο αυτό, αναθέτουμε σε έναν OF Controller την ευθύνη για την προσαρμογή των πινάκων ροών όλων των συσκευών που υποστηρίζουν το πρωτόκολλο OpenFlow, ορίζοντας συγκεκριμένους κανόνες που αφορούν την κακόβουλη κίνηση (π.χ. απόρριψη των κακόβουλων ροών), αντιμετωπίζοντας έτσι την επίθεση.

- *Κλιμακώσιμη διαχείριση των δεδομένων παρακολούθησης δικτυακής κίνησης χρησιμοποιώντας τεχνικές δειγματοληψίας.*

  Η προτεινόμενη προσέγγιση επιτρέπει την μεταφορά του φόρτου καταμέτρησης και ανάλυσης των μετρητών κάθε ροής σε κάποιο εξωτερικό στοιχείο, ανεξάρτητο από το Επίπεδο Ελέγχου. Η δυνατότητα αυτή ελαχιστοποιεί τις πιθανότητες για εξάντληση των πόρων συστήματος (π.χ. CPU, RAM, λανθάνουσα μνήμη-cache των πινάκων ροών) σε περιπτώσεις αυξημένης χρήσης. Αυτό επιτυγχάνεται μέσω της δειγματοληψίας πακέτων που προσφέρει το πρωτόκολλο sFlow, μειώνοντας σημαντικά τον όγκο των δεδομένων που μεταφέρονται και περιέχουν στατιστικές πληροφορίες για τις ροές δεδομένων. Παράλληλα αποφεύγεται η χρήση εξειδικευμένου εξοπλισμού (Firewall, Συστήματα IDS κ.α.).

5.2.2 Αρχιτεκτονικά στοιχεία

Η ανίχνευση και αντιμετώπιση κακόβουλων δικτυακών ανωμαλιών χρησιμοποιεί ένα υποσύνολο των δώδεκα πεδίων τα οποία ορίζουν ροές πακέτων σύμφωνα με το πρωτόκολλο OpenFlow (OF protocol v1.0 [28]) όπως δείχνει και ο Πίνακας 5. Οι τιμές των πεδίων για κάθε ροή διατηρούνται αποθηκευμένες στους πίνακες ροών των μεταγωγέων OF, σε αυτές μπορούμε να διακρίνουμε τέσσερις σημαντικά πεδία (πέραν των πεδίων που αφορούν τις επικεφαλίδες των πακέτων) τα οποία εκμεταλλευόμαστε: (i) το πεδίο Action το οποίο αν και με ποιον τρόπο θα προωθηθεί ένα πακέτο σε περίπτωση που οι τιμές των επικεφαλίδων του αντιστοιχούν με τις αντίστοιχες τιμές μιας αποθηκευμένης ροής του πίνακα, (ii) το πεδίο soft-timeout το οποίο ορίζει το μέγιστο διάστημα κατά το οποίο μπορεί να διατηρηθεί μία εγγραφή ροής στον πίνακα χωρίς να έχει γίνει μία αντιστοίχιση πακέτου με τη συγκεκριμένη ροή, (iii) ο αριθμός των πακέτων που έχουν αντιστοιχηθεί με κάθε

εγγραφή ροής του πίνακα, και (iv) η τιμή του πεδίο Priority η οποία ορίζει τις προτεραιότητες μεταξύ εγγραφών οι οποίες μπορεί να επικαλύπτονται μερικώς.

LAYER 1	LAYER 2					LAYER 3				LAYER 4	
IN PORT	ETHER			VLAN		IP				PORT	
	src	dst	Type	id	PCP	src	dst	proto	TOS	src	dst

Πίνακας 5: Πεδία των επικεφαλίδων των πακέτων τα οποία χρησιμοποιούνται για την αντιστοίχιση ενός πακέτου με μία OpenFlow εγγραφή στον πίνακα ροών ενός μεταγωγέα OF.

Η αρχιτεκτονική του προτεινόμενου μηχανισμού αποτελείται από τρία κύρια δομικά στοιχεία όπως φαίνεται και στο Σχήμα 5: (i) τον Συλλέκτη – Collector, (ii) το στοιχείο Ανίχνευσης Ανωμαλιών – Anomaly Detection, και (iii) το στοιχείο Αντιμετώπισης Ανωμαλιών – Anomaly Mitigation.

5.2.2.1 Συλλέκτης στατιστικών πληροφοριών

Ο Συλλέκτης είναι το στοιχείο το οποίο και είναι υπεύθυνο για την συλλογή στατιστικών δεδομένων, κάτι το οποίο είναι απαραίτητο προκειμένου να επιτευχθεί η ανίχνευση πιθανών ανωμαλιών στις ροές πακέτων. Το στοιχείο συλλέγει στατιστική πληροφορία για τις ροές και περιοδικά μεταδίδει στο στοιχείο Ανίχνευσης Ανωμαλίας τα δεδομένα που έχει συλλέξει.

Όσον αφορά τη συλλογή στατιστικής πληροφορίας, η εργασία εστιάζει στη μελέτη δύο διαφορετικών μεθόδων. Η πρώτη μέθοδος αφορά τη συλλογή στατιστικών μέσω της εγγενούς μεθόδους που υποστηρίζεται από το πρωτόκολλο OpenFlow [52], [53], όπου τα δεδομένα συγκεντρώνονται μέσω περιοδικών ερωτημάτων για όλες τις εγγραφές ροών των μεταγωγέων OF. Η δεύτερη μέθοδος χρησιμοποιεί ένα μηχανισμό για τη συλλογή δεδομένων παρακολούθησης ροών πακέτων, πραγματοποιώντας δειγματοληψία. Για το σκοπό αυτό επιλέχτηκε το πρωτόκολλο sFlow, καθώς είναι μια λύση η οποία υποστηρίζεται από τις συσκευές Επιπέδου 2 σχεδόν όλων των κατασκευαστών.

5.2.2.2 Ανίχνευση ανωμαλιών

Τα δεδομένα που συγκεντρώνονται στο πρώτο δομικό στοιχείο τις εφαρμογής αποτελούν την είσοδο για τον αλγόριθμο ανίχνευσης ανωμαλιών, και παραδίδονται

περιοδικά, ύστερα από σταθερά καθορισμένα χρονικά διαστήματα. Στην συγκεκριμένη περίπτωση επιλέχθηκε το χρονικό διάστημα αυτό να είναι 30 δευτερόλεπτα, ώστε να επιτυγχάνεται ανίχνευση σε σχεδόν πραγματικό χρόνο, όπως φαίνεται και σε αντίστοιχες μελέτες στη βιβλιογραφία [63], [64]. Μετά από κάθε διάστημα 30 δευτερολέπτων, το εν λόγω στοιχείο ελέγχει κάθε ροή πακέτων (μέσω των στατιστικών δεδομένων τα οποία έχει αποκτήσει) και αποκαλύπτει δικτυακές ανωμαλίες. Οι ανωμαλίες αυτές μπορεί να σχετίζονται με ένα σύνολο ροών, και αναλόγως την φύση του αλγορίθμου και της ανωμαλίας είναι δυνατή ακόμη και η αποκάλυψη πιθανών κακόβουλων χρηστών/εισβολέων ή των θυμάτων της επίθεσης.

Η προτεινόμενη αρχιτεκτονική, χάρη στη διαλειτουργικότητα των κυρίων δομικών στοιχείων, υποστηρίζει τη χρήση οποιουδήποτε αλγορίθμου, όπως στατιστικής ανίχνευσης ανωμαλιών [65], μάθησης μηχανής (machine learning) [66], ή και εξόρυξης δεδομένων (data mining) [67], όπως μπορεί να τεκμηριωθεί και από σχετικές αναφορές της βιβλιογραφίας [68], [69]. Η πρότυπη υλοποίηση της μεθόδου η οποία παρουσιάζεται εδώ, στηρίχθηκε σε αλγόριθμο ο οποίος ελέγχει για απότομες μεταβολές στην αλλαγή της εντροπίας συγκεκριμένων πεδίων των επικεφαλίδων των πακέτων, όπως αναλύεται εκτενώς και στην επόμενη παράγραφο. Μέσω του μηχανισμού μας, μπορούν να ανιχνευθούν αποτελεσματικά δικτυακές επιθέσεις όπως DDoS, Worm propagation και Port scanning όπως αναλύεται σε επόμενη παράγραφο του κεφαλαίου. Ακόμη μέσω της συγκεκριμένης μεθόδου είμαστε σε θέση να αναγνωρίσουμε τόσο το είδος της επίθεσης, όσο και το θύμα (ή τον θύτη αναλόγως τον τύπο επίθεσης). Αυτό επιτυγχάνεται μέσω συσχέτισης συγκεκριμένων δικτυακών μετρικών, και στη συνέχει η πληροφορία αυτή μεταφέρεται στο στοιχείο το οποίο είναι υπεύθυνο για τη λήψη μέτρων με στόχο την αντιμετώπιση της επίθεσης.

5.2.2.3 Αντιμετώπιση ανωμαλιών (Anomaly Mitigation)

Το στοιχείο Αντιμετώπισης Ανωμαλιών στοχεύει στην εξουδετέρωση δικτυακών ανωμαλιών οι οποίες ανιχνεύονται. Για το σκοπό αυτό εισάγει συγκεκριμένες εγγραφές στους πίνακες ροών των μεταγωγέων OF (ή τροποποιεί υφιστάμενες εγγραφές), ώστε να αποκοπούν οι κακόβουλες ροές πακέτων. Είναι πιθανό βέβαια να υπάρξουν καλόβουλες ροές πακέτων, οι οποίες όμως τυγχάνει να ερμηνεύονται ως κακόβουλες. Προκειμένου να αποφεύγονται γεγονότα αποκοπής τέτοιας κίνησης, το στοιχείο Αντιμετώπισης Ανωμαλιών

υποστηρίζει και τη λειτουργία *White List*, μέσω της οποίας μπορούμε να εξαιρέσουμε συγκεκριμένες διευθύνσεις IPs από τη διαδικασία αποκοπής κίνησης.

5.3 Συλλογή Δεδομένων για Ανίχνευση και Αντιμετώπιση Ανωμαλιών σε SDNs

5.3.1 Συλλογή στατιστικών δεδομένων για ροές πακέτων σε SDN

5.3.1.1 Η εγγενής μέθοδος του πρωτοκόλλου OpenFlow

Η εγγενής μέθοδος συλλογής στατιστικών δεδομένων μέσω OF βασίζεται στην ανταλλαγή πληροφοριών μεταξύ μεταγωγέα OF και OF Controller. Όπως καθορίζεται από το πρωτόκολλο OF, ο Controller στέλνει περιοδικά αιτήματα τύπου *flow-stats request*, ζητώντας από τον εκάστοτε μεταγωγέα OF το σύνολο του πίνακα ροών που διατηρεί, μαζί με τους αντίστοιχους μετρητές.

Οι μετρητές σε έναν πίνακα ροών, ανανεώνονται μόνο όταν ένα πακέτο αντιστοιχίζεται με μία συγκεκριμένη ροή κατά τη διαδικασία αναζήτησης κατάλληλης ροής για την προώθηση του πακέτου. Συνεπώς, η διαδικασία συλλογής στατιστικών δεδομένων μέσω της εγγενούς OF μεθόδου εξαρτάται άμεσα και από τον αλγόριθμο προώθησης των πακέτων, του OF Controller. Στην περίπτωσή μας, όπου στον αλγόριθμο προώθησης εμπλέκεται και ο μηχανισμός αντιμετώπισης δικτυακών ανωμαλιών, χρησιμοποιούνται και πεδία των Επιπέδων 3 και 4 για την προώθηση πακέτων μέσω των μεταγωγέων OF. Έτσι οι εγγραφές του πίνακα ροών προκύπτουν ως ένας συνδυασμός των μεταβλητών {A, B, C, D, E, F, G, H, X, Y}, τις οποίες περιγράφει ο Πίνακας 6, όπου εμφανίζονται δύο εγγραφές ροών ως αντιπροσωπευτικό παράδειγμα υλοποίησης μιας δικατευθυντικής επικοινωνίας. Όποιο πεδία είναι αδιάφορο ως προς την τιμή του, παίρνει ως τιμή ένα χαρακτήρα αναπλήρωσης (wildcard) ούτως ώστε να αντιστοιχίζεται με οποιαδήποτε τιμή.

LAYER 1	LAYER 2					LAYER 3				LAYER 4	
INPORT	ETHER			VLAN		IP				PORT	
	src	dst	type	id	PCP	src	dst	Proto	TOS	src	dst
X	A	D	G	*	*	B	E	H	*	C	F
Y	D	A	G	*	*	E	B	H	*	F	C

Πίνακας 6: Παράδειγμα εγγραφών στον πίνακα ροών ενός μεταγωγέα OF για την υλοποίηση μίας δικατευθυντικής επικοινωνίας.

Η συλλογή δεδομένων μέσω της εγγενούς πραγματοποιείται όταν ένας μεταγωγέας OF απαντήσει σε ένα *flow-stats request* αίτημα το οποίο έχει σταλεί από τον OF Controller. Ο μεταγωγέας αποστέλλει πολλαπλά πακέτα, κάθε ένα από τα οποία περιέχει ένα μεγάλο μέρος των εγγραφών που περιέχει στον πίνακα ροών του. Ο αριθμός των πακέτων εξαρτάται αφενός από τον συνολικό αριθμό των εγγραφών που διατηρεί ο μεταγωγέας μια δεδομένη χρονική στιγμή, και αφετέρου από τον τύπο του μεταγωγέα (π.χ. μεταγωγείς OF NEC IP8800 μεταδίδουν περίπου 160 εγγραφές ανά πακέτο, ενώ μεταγωγείς OF τύπου OVS μεταδίδουν περίπου 620 εγγραφές ανά πακέτο). Τα πακέτα που αποστέλλονται, εκτός των πεδίων κάθε ροής, περιέχουν και τους αντίστοιχους μετρητές πακέτων και bytes για κάθε μία. Όμως οι μετρητές αυτοί περιέχουν το σύνολο των πακέτων που αντιστοιχήθηκαν με κάθε εγγραφή από τη στιγμή που εισάχθηκε η εγγραφή αυτή για πρώτη φορά, ενώ ο αλγόριθμος ανίχνευσης ανωμαλιών χρειάζεται μόνο τον αριθμό των πακέτων που αντιστοιχήθηκαν με κάθε ροή κατά το τελευταίο χρονικό παράθυρο μέτρησης. Για το λόγο αυτό, ο OF Controller χρειάζεται να διατηρεί και την κατάσταση του πίνακα ροών, όπως την έμαθε από τον μεταγωγέα OF κατά τη διάρκεια του προηγούμενου χρονικού παραθύρου μέτρησης. Έτσι ο Controller μπορεί να συγκρίνει τις δύο καταστάσεις του πίνακα ροών, και βρίσκοντας τη διαφορά μεταξύ των μετρητών κάθε ροής, να βρει τις τιμές κάθε μετρητή που αντιστοιχούν στο τρέχον χρονικό παράθυρο μέτρησης.

Χρησιμοποιώντας την μέθοδο αυτή για τη συλλογή στατιστικών δεδομένων, είναι δυνατή η συλλογή και ανάλυση της δικτυακής κίνησης στο σύνολό της, και με πλήρη λεπτομέρεια, μιας και δεν συμβαίνει κανενός είδους δειγματοληψία κατά τη διαδικασία συλλογής δεδομένων. Η μέθοδος αυτή έχει εφαρμοστεί επιτυχημένα [52], [53] για την παρακολούθηση της δικτυακής κίνησης σε περιβάλλοντα που χαρακτηρίζονται από χαμηλό έως μέτριο όγκο κίνησης.

Η προσέγγιση αυτή όμως έχει συγκεκριμένα μειονεκτήματα, τα οποία γίνονται εμφανή και αποδεικνύονται ιδιαίτερα κρίσιμα, όσο αυξάνεται ο ρυθμός μετάδοσης/εξυπηρέτησης πακέτων. Λόγω του ότι χρειάζεται πληροφορία Επιπέδου 2 και Επιπέδου 3 για κάθε ροή πακέτων ώστε να είναι εφικτή η συλλογή στατιστικών, ο αριθμός των εγγραφών ροών σε ένα πίνακα ροών μπορεί να αυξηθεί υπερβολικά (δεκάδες χιλιάδες ροές πακέτων σε κάθε δεδομένη χρονική στιγμή), επηρεάζοντας έτσι την απόδοση των μεταγωγέων. Ως χαρακτηριστικό παράδειγμα, για την προώθηση 50Mbps κίνησης με αυτόν τον τρόπο, απαιτούν την εισαγωγή περίπου 24.000 διαφορετικών ροών, με κάθε ένα να διατηρείται για τουλάχιστον 30 δευτερόλεπτα στον πίνακα ροών. Όμως, πολλές από τις εμπορικές συσκευές-μεταγωγείς που υποστηρίζουν το πρωτόκολλο OpenFlow, δεν μπορούν να

διατηρήσουν σε μία δεδομένη χρονική στιγμή περισσότερες από 4.000 εγγραφές. Έτσι, η μέθοδος αυτή για τη συλλογή δεδομένων, μπορεί να εφαρμοστεί αποτελεσματικά μόνο σε περιπτώσεις μεταγωγέων οι οποίοι υλοποιούνται σε λογισμικό (π.χ. Open vSwitch – OVS [70]). Λόγω του ότι είναι υλοποιημένοι σε αποκλειστικά σε λογισμικό, οι μεταγωγείς αυτοί μπορούν να διατηρήσουν έναν εξαιρετικά μεγάλο αριθμό εγγραφών, όμως δεν μπορούν να προωθήσουν κίνηση σε ρυθμό-ροής (line-rate) σε αντίθεση με τους μεταγωγείς οι οποίοι είναι υλοποιημένοι σε φυσικό εξοπλισμό (hardware).

Το πιο σημαντικό μειονέκτημα της συγκεκριμένης μεθόδου, είναι το γεγονός ότι μια επίθεση η οποία αποτελείται από μετάδοση χιλιάδων διαφορετικών ροών σε υψηλούς ρυθμούς, μπορεί έμμεσα να οδηγήσει σε επίθεση άρνησης υπηρεσίας (Denial of Service – DoS) στο ίδιο το Επίπεδο Ελέγχου. Αυτό θα συμβεί λόγω του τεράστιου αριθμού μηνυμάτων σηματοδοσίας τύπου *packet-in* τα οποία θα δημιουργηθούν από τον μεταγωγέα OF και θα αποσταλούν στον Controller με στόχο την εγκαθίδρυση ίσου αριθμού νέων εγγραφών ροών στον πίνακα ροών του μεταγωγέα OF.

5.3.1.2 Μέθοδος συλλογής πληροφορίας βασισμένη στο πρωτόκολλο sFlow

Αποσκοπώντας στην υπερπήδηση εμποδίων τα οποία εμφανίζονται στην εγγενή μέθοδο του OF για συλλογή δεδομένων, προτείνουμε μία νέα μέθοδο όπου εκμεταλλευόμαστε τις δυνατότητες δειγματοληψίας του πρωτοκόλλου sFlow. Η προτεινόμενη τεχνική διαχωρίζει τη διαδικασία συλλογής δεδομένων από τη διαδικασία προώθησης της δικτυακής κίνησης, αφού μέσω της δειγματοληψίας πακέτων συγκεντρώνονται στατιστικά στοιχεία για τις ροές. Για το σκοπό αυτό, η συγκεκριμένη μέθοδος δειγματοληπτεί πακέτα τα οποία φτάνουν σε έναν μεταγωγέα, και μέσω των επικεφαλίδων τους ταξινομεί τις απαιτούμενες εγγραφές ροών, και στη συνέχεια ανανεώνοντας τους αντίστοιχους μετρητές. Στην πειραματική υλοποίηση η συλλογή και ταξινόμηση δειγμάτων των ροών γίνεται στον OF Controller, όπου δημιουργήθηκε συγκεκριμένη εφαρμογή για αυτόν το σκοπό (sFlow Collector). Στη συνέχεια η εφαρμογή αυτή μεταδίδει τα στατιστικά δεδομένα στο στοιχείο Ανίχνευσης Ανωμαλιών για περεταίρω ανάλυση.

Η μέθοδος αυτή μπορεί να εφαρμοστεί σε συστήματα μεγάλης κλίμακας καθώς επιτρέπει, σε περιπτώσεις μεγάλου αριθμού ροών, την ομαδοποίηση αναλυτικών ροών σε πιο γενικευμένες στον πίνακα ροών ενός μεταγωγέα OF. Η γενίκευση αυτή, που αφορά στην προώθηση πακέτων μόνο και όχι στη συλλογή στατιστικών δεδομένων, μπορεί να

πραγματοποιηθεί μέσω wildcards και προτεραιοτήτων κατ' αναλογία με το prefix aggregation που πραγματοποιείται σε παραδοσιακούς δρομολογητές IP. Σαν συνέπεια, μπορεί να επιτευχθεί σημαντική μείωση του αριθμού των απαιτούμενων εγγραφών στον πίνακα ροών ενός μεταγωγέα OF, ξεπερνώντας περιορισμούς που έχουν προαναφερθεί και οι οποίοι σχετίζονται με το μέγεθος του πίνακα ροών σε πραγματικές συσκευές προώθησης δικτυακής κίνησης. Παράλληλα, μέσω του sFlow Collector μαζεύονται επαρκή δεδομένα για αξιόπιστη ανίχνευσης πιθανών δικτυακών επιθέσεων.

Αναλυτικότερα, καθώς ο sFlow Collector συλλέγει δείγματα πακέτων σε πραγματικό χρόνο, ανανεώνει –ανά συγκεκριμένα χρονικά διαστήματα- τους αντίστοιχους μετρητές που διατηρεί. Έτσι δεν υπάρχει ποια η ανάγκη διατήρησης της πρότερης κατάστασης ενός πίνακα ροών. Συνεπώς η μέθοδος αυτή μειώνει σημαντικά την πολυπλοκότητα του αλγορίθμου συλλογής στατιστικών δεδομένων, οδηγώντας σε χαμηλότερες απαιτήσεις σε πόρους συστήματος. Όπως θα αναλυθεί σε επόμενη ενότητα, μέσω της μεθόδου αυτής κατέστη δυνατή η αύξηση του όγκου της δικτυακής κίνησης που μπορεί να συλλεχθεί και να αναλυθεί κατά δέκα φορές, σε σύγκριση με την εγγενή μέθοδο που αναλύθηκε.

5.3.2 Ανίχνευση και χαρακτηρισμός δικτυακών ανωμαλιών μέσω Εντροπίας

Για την ανάλυση της δικτυακής κίνησης, την ανίχνευση ανωμαλιών και την κατηγοριοποίησή τους, υιοθετήθηκε μία μέθοδος βασισμένη στις εντροπία χαρακτηριστικών πεδίων των επικεφαλίδων των πακέτων [61]. Η μέθοδος αυτή είναι ανεξάρτητη από τα χαρακτηριστικά της εκάστοτε τοπολογίας ή της δικτυακής κίνησης, και μπορεί να εφαρμοστεί για την παρακολούθηση και προστασία κάθε δικτυακού περιβάλλοντος [71].

Η εντροπία H(X) [72] ενός συνόλου X = {x_1, x_2, …. x_n} ορίζεται ως:

$$H(X) = -\sum_{i=1}^{N} p_i \log_2(p_i) \qquad (5.1),$$

όπου N είναι ο αριθμός στοιχείων που περιλαμβάνονται στο σύνολο στοιχείων X και p_i είναι η πιθανότητα $P[X = x_i]$. Η εντροπία μετράει πόσο τυχαία είναι κατανεμημένο ένα σύνολο στοιχείων. Οι υψηλές τιμές εντροπίας δηλώνουν μια διασκορπισμένη κατανομή πιθανότητας, ενώ οι χαμηλές τιμές εντροπίας δείχνουν τη συγκέντρωση μιας κατανομής στοιχείων. Οι τιμές της εντροπίας, όπως αυτή ορίζεται στη σχέση (5.1), κυμαίνονται μεταξύ

0 και $log_2 N$. Προκειμένου να υπάρξει μία μετρική ανεξάρτητη του αριθμού των διαφορετικών τιμών του συνόλου, ομαλοποιούμε την εντροπία διαιρώντας την τιμή *H(X)* με τη μέγιστη τιμή της $log_2 N$. Η τιμή της ομαλοποιημένης εντροπίας δίνεται από την σχέση (5.2):

$$H_n(X) = -\frac{\sum_{i=1}^{N} p_i \log_2(p_i)}{\log_2 N} \quad (5.2),$$

όπου οι τιμές της κυμαίνονται μεταξύ *(0,1)*.

Για τη συγκεκριμένη εφαρμογή, έχει ιδιαίτερη σημασία η παρακολούθηση και καταγραφή της μεταβολής της εντροπίας τεσσάρων πεδίων των επικεφαλίδων των πακέτων, και συγκεκριμένα: (i) διεύθυνση IP πηγής (*srcIP*), (ii) διεύθυνση IP προορισμού (*dstIP*), (iii) πόρτα Επιπέδου 4 πηγής (*srcPort*), και (iv) πόρτα Επιπέδου 4 προορισμού (*dstPort*). Με βάση την εντροπία των προαναφερθέντων χαρακτηριστικών, υλοποιήσαμε και χρησιμοποιήσαμε τον συγκεκριμένο αλγόριθμο για την ανάδειξη δικτυακών ανωμαλιών, και συγκεκριμένα: (α) Επιθέσεις DDoS, (β) Διάδοση Κακόβουλου Λογισμικού (Worm Propagation), και (γ) Ανίχνευση Υπηρεσιών (Port Scanning). Ο Πίνακας 7 αναφέρεται στις τυπικές αυτές δικτυακές ανωμαλίες, και σε συγκεκριμένες μεταβολές της εντροπίας χαρακτηριστικών της κίνησης που βοηθούν στην αναγνώρισή τους.

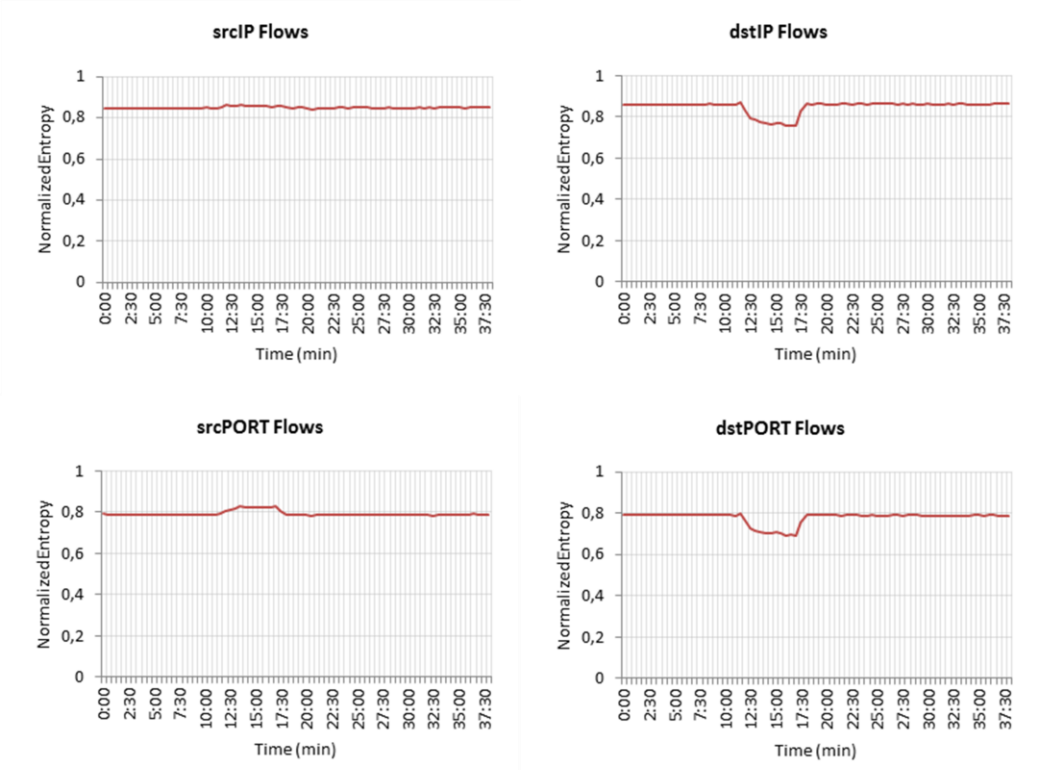
Ανωμαλία	Περιγραφή	Μεταβολή Εντροπίας
Distributed denial of service (DDoS) attack	Επίθεση σε μία συγκεκριμένη υπηρεσία, καθιστώντας την μη διαθέσιμη στους υπόλοιπους χρήστες της.	Σημαντική μείωση σε *dstIP* και *dstPort*.
Worm propagation	Ένα αυτό-αναπαραγώμενο πρόγραμμα το οποίο προσπαθεί να μολύνει άλλα συστήματα, εκμεταλλευόμενο συγκεκριμένα κενά ασφαλείας.	Σημαντική μείωση σε *srcIP* και *dstPort*.
Port Scanning	Αποστολή συγκεκριμένου τύπου πακέτων σε ένα μεγάλο εύρος θυρών Επιπέδου 4, με σκοπό την ανεύρεση υπηρεσιών οι οποίες βρίσκονται σε λειτουργία.	Σημαντική μείωση *srcIP*, *dstIP*. Σημαντική μείωση σε *dstPort* αν ο επιτιθέμενος χρησιμοποιεί τυχαίο αριθμό για τις θύρες πηγής.

Πίνακας 7: Κατηγοριοποίηση κακόβουλων δικτυακών ανωμαλιών βάσει της μεταβολής της εντροπίας.

Για παράδειγμα, σε υποθετικό συμβάν όπου ένας μολυσμένος υπολογιστής-εξυπηρετητής προσπαθεί να μεταδώσει κακόβουλο λογισμικό σε άλλους υπολογιστές του

δικτύου (περίπτωση Worm Propagation), παρατηρείται μείωση της εντροπίας της διεύθυνσης IP πηγής (*srcIP*). Το κακόβουλο σύστημα προκαλεί σημαντικό αριθμό ροών, με αποτέλεσμα η διεύθυνση IP του να επικρατεί στην κατανομή ροών σε σχέση με τη διεύθυνση IP πηγής. Αντίστοιχα, σε περιπτώσεις Port Scanning, αυξάνεται σημαντικά η εντροπία των θυρών προορισμού (*dstPort*), λόγω επικοινωνίας του επιτιθέμενου με πολλές διαφορετικές πόρτες Επιπέδου 4. Με βάση τις διακυμάνσεις αυτές, ο Controller είναι σε θέση να αντιληφθεί την παρουσία μιας δικτυακής ανωμαλίας, χρησιμοποιώντας προκαθορισμένα κατώφλια για τον έλεγχο της μεταβολής της εντροπίας συγκεκριμένων πεδίων.

Στο Σχήμα 6 φαίνεται η μεταβολή της εντροπίας των προαναφερθέντων τεσσάρων μετρικών, κατά τη διάρκεια μιας ενδεικτικής επίθεσης DDoS, δέκα λεπτά μετά την έναρξη της διαδικασίας παρακολούθησης και ανάλυσης της δικτυακής κίνησης. Όπως είναι εμφανές στο σχήμα, οι τιμές της εντροπίας των διευθύνσεων IP προορισμού και θυρών προορισμού Επιπέδου 4 αντίστοιχα μειώνονται σημαντικά κατά τη διάρκεια της επίθεσης, καταδεικνύοντας την ύπαρξη μίας δικτυακής ανωμαλίας και συγκεκριμένα της επίθεσης DDoS.



Σχήμα 6: Μεταβολή της εντροπίας των πεδίων srcIP, dstIP, srcPort, dstPort των επικεφαλίδων των πακέτων, κατά τη διάρκεια μίας επίθεσης τύπου DDoS.

5.3.3 Αναγνώριση θύματος/θύτη και αντιμετώπιση δικτυακών επιθέσεων

Στις προηγούμενες παραγράφους αναλύθηκαν οι μέθοδοι παρακολούθηση της δικτυακής κίνησης και την ανεύρεση πιθανών κακόβουλων επιθέσεων. Πριν ο μηχανισμός προχωρήσει στην ανεύρεση μεθόδων για την αντιμετώπιση μιας επίθεσης, είναι απαραίτητη αναγνώριση είτε του θύματος είτε του θύτη (αναλόγως τον τύπο της επίθεσης). Το συγκριτικό πλεονέκτημα του πρωτοκόλλου OpenFlow για την αντιμετώπιση δικτυακών ανωμαλιών είναι εμφανές, αφού είναι άρρηκτα συνδεδεμένο με τη διαδικασία προώθησης πακέτων σε Επίπεδα 2 έως 4.

Νέα flows εγκαθιδρύονται στους πίνακες ροών των μεταγωγέων OF μαζί με ένα αντίστοιχο πεδίο (*action)* το οποίο καθορίζει πώς και αν θα προωθηθούν τα πακέτα τα οποία θα αντιστοιχιστούν με μία εγγραφή. Οι πιο κοινές τιμές του πεδίου action είναι: (i) *Forward,* (ii) *Drop,* και (iii) *Modify-field* [28]. Η τιμή *Forward,* ανατίθεται σε κάθε ροή η οποία αντιστοιχεί σε καλόβουλη κίνηση, και η οποία πρέπει να προωθηθεί κανονικά. Αντίθετα η τιμή *Drop* αφορά τα flows εκείνα, τα οποία αντιστοιχούν σε κακόβουλη κίνηση και πρέπει να απορριφθούν από τη συσκευή, χωρίς να προωθηθούν. Επιπλέον, ορίζουμε προκαθορισμένες τιμές Προτεραιότητας (πεδίο *Priority*) για κάθε διαφορετική τιμή του πεδίου *Action*. Στις εγγραφές του πίνακα ροών, οι οποίες προορίζονται να μεταφέρουν καλόβουλη κίνηση, ανατίθεται χαμηλή τιμή Προτεραιότητας, ενώ στις εγγραφές οι οποίες εγκαθιδρύθηκαν για την αποκοπή της κακόβουλης κίνησης ανατίθεται υψηλή τιμή προτεραιότητας. Έτσι, ένας κανόνας *Drop* θα έχει πάντοτε προτεραιότητα.

Ο μηχανισμός Ανίχνευσης Ανωμαλιών, στηριζόμενος στις παρατηρήσεις που εκθέτουμε στον Πίνακας 7 κατηγοριοποιεί τις επιθέσεις και θέτει το σύστημα σε κατάσταση συναγερμού. Παραδείγματος χάριν, αν ο συναγερμός ενεργοποιήθηκε λόγω σημαντικής μείωσης της εντροπίας των μετρικών *dstIP* και *dstPort,* τότε ο αλγόριθμος αντιλαμβάνεται ότι η δικτυακή ανωμαλία που αναγνωρίστηκε ήταν στην πραγματικότητα μία επίθεση DDoS. Με αντίστοιχο τρόπο κατηγοριοποιούνται οι δικτυακές ανωμαλίες και για τις υπόλοιπες κατηγορίες του Πίνακας 7. Στη συνέχεια αναλύονται στατιστικά δεδομένα που σχετίζονται με την επίθεση που ανιχνεύθηκε, χρησιμοποιώντας ιστορικά δεδομένα ώστε να ταυτοποιηθεί είτε ο επιτιθέμενος, είτε το θύμα της επίθεσης. Συγκεκριμένα, σε περίπτωση επίθεσης DDoS, αναγνωρίζεται το υπολογιστής/θύμα της επίθεσης καθώς και η υπηρεσία η οποία δέχεται την επίθεση, ενώ για τα υπόλοιπα ήδη επιθέσεων ανιχνεύεται ο επιτιθέμενος. Σε γενικές γραμμές, στόχος της συγκεκριμένης διαδικασίας είναι η αναγνώριση ενός

υπολογιστή-εξυπηρετητή και της αντίστοιχης υπηρεσίας, ώστε αποκόπτοντάς τα να αντιμετωπιστεί η δικτυακή ανωμαλία χωρίς να υπερφορτώνεται άσκοπα το δίκτυο.

Μόλις ο μηχανισμός Ανίχνευσης Ανωμαλιών αναγνωρίσει τον ζητούμενο στόχο (είτε αυτός είναι ο επιτιθέμενος είτε το θύμα), μεταφέρει την πληροφορία αυτή στον μηχανισμό Αντιμετώπισης Ανωμαλιών. Ο μηχανισμός αυτός είναι σε θέση να δημιουργήσει νέες εγγραφές ροών σε έναν μεταγωγέα OF, ή να τροποποιήσει υφιστάμενες εγγραφές, χρησιμοποιώντας σαν δεδομένα την διεύθυνση IP του στόχου και την πόρτα της υπηρεσίας που πρέπει να αποκοπεί. Στη νέα αυτή ροή, το πεδίο *Action* παίρνει την τιμή *Drop,* ώστε να αποκόπτεται η αντίστοιχη κίνηση.

Γενικά, ο αλγόριθμος Ανίχνευσης Ανωμαλιών μπορεί να αναγνωρίσει χαρακτηριστικά γνωρίσματα κακόβουλης κίνησης, όπως αυτά έχουν προαναφερθεί. Όμως, υπάρχουν κάποιες καλόβουλες δικτυακές ανωμαλίες, οι οποίες επηρεάζουν τις τιμές της εντροπίας των επικεφαλίδων με τρόπο όμοιο με εκείνο συγκεκριμένων κακόβουλων επιθέσεων. Παραδείγματος χάριν, μία δικτυακή ανωμαλία τύπου Flash Crowd θα προκαλούσε σημαντική πτώση στις τιμές της εντροπίας των πεδίων *dstIP* και *dstPort*, όπως ακριβώς και στην περίπτωση μιας επίθεσης DDoS. Έτσι, αποσκοπώντας στην αποφυγή περιπτώσεων αποκοπής νόμιμης δικτυακής κίνησης, υλοποιήθηκε και εφαρμόστηκε στο σύστημα η λειτουργία *White List,* δηλαδή μιας λίστας από συνδυασμούς διευθύνσεων IP και θυρών Επιπέδου 4, για τις οποίες ξέρουμε ότι είναι πιθανόν να επιδείξουν μη ομαλή συμπεριφορά, αλλά η δικτυακή κίνηση η οποία αντιπροσωπεύουν θα είναι νόμιμη. Συνεπώς, πριν ο μηχανισμός Αντιμετώπισης Ανωμαλιών εισάγει μια εγγραφή στον πίνακα ροών για την αποκοπή ενός αναγνωρισμένου στόχου, ελέγχει πρώτα τις εγγραφές που σχετίζονται με την *Whitelist.* Η λίστα αυτή είναι δυνατόν να ελέγχεται είτε από έναν αυτοματοποιημένο μηχανισμό, ή από έναν διαχειριστή δικτύου. Στη συγκεκριμένη περίπτωση, για λόγους συντομίας, επιλέχθηκε η δεύτερη περίπτωση.

5.4 Μεθοδολογία – Αποτελέσματα

Στην παράγραφο αυτή, παρουσιάζεται η αξιολόγηση της προτεινόμενης αρχιτεκτονικής που συνδυάζει τα πρωτόκολλα OpenFlow και sFlow για ανίχνευση και αντιμετώπιση κακόβουλων δικτυακών ανωμαλιών. Εστιάζουμε κυρίως στην απόδοση μεταγωγέων (software και hardware) οι οποίοι υποστηρίζουν ταυτόχρονα τα πρωτόκολλα OpenFlow και sFlow, ενώ πειραματιζόμαστε με διαφορετικούς ρυθμούς αποστολής και εξυπηρέτησης πακέτων, από χαμηλούς ρυθμούς οι οποίοι προσομοιώνουν δίκτυα μικρομεσαίων εταιριών,

έως αρκετά υψηλούς ρυθμούς προσομοιώνοντας δίκτυα παραγωγής μεγάλων εταιριών ή ιδρυμάτων. Κατά τη διαδικασία αυτή, αναδεικνύουμε τα πλεονεκτήματα του πρωτοκόλλου OF στην αναγνώριση και την αντιμετώπιση κακόβουλων επιθέσεων, βασιζόμενοι στις δυνατότητες του NOX OF Controller [73].

Ο NOX είναι ένας OF Controller, η λειτουργία του οποίου βασίζεται στην κατανάλωση και αξιοποίηση δικτυακών γεγονότων (network events) [74]. Συνεπώς, για τους σκοπούς της συγκεκριμένης προσέγγισης, ο NOX χρησιμοποιείται ως μια προγραμματιστική διεπαφή υψηλού επιπέδου, δρώντας με βάση δικτυακά γεγονότα. Χρησιμοποιώντας τη Διεπαφή Προγράμματος Εφαρμογής (Application Programming Interface – API), τα τρία κύρια δομικά στοιχεία της προτεινόμενης αρχιτεκτονικής υλοποιήθηκαν ως ανεξάρτητες εφαρμογές του NOX Controller, με κάθε ένα υπεύθυνο αντίστοιχα για τη συλλογή στατιστικών δεδομένων, τον περιοδικό υπολογισμό της εντροπίας ανά μετρική, και τέλος την τροποποίηση του πίνακα ροών για την αντιμετώπιση της επίθεσης.

Συγκεκριμένα, ο αλγόριθμος Ανίχνευσης Ανωμαλιών υλοποιήθηκε ως μία εφαρμογή του NOX Controller. Σε περίπτωση ανίχνευσης τυχόν ανωμαλίας, τα αποτελέσματα μεταφέρονται στην εφαρμογή Αντιμετώπισης Ανωμαλιών, η οποία θα επιληφθεί για την εγκαθίδρυση ή τροποποίηση των απαραίτητων εγγραφών ροών. Η εφαρμογή αυτή αναπτύχθηκε επίσης ως μία εφαρμογή του NOX Controller, ώστε να είναι ανεξάρτητη από τη μέθοδο ανίχνευσης ανωμαλιών που μπορεί να επιλεγεί από έναν διαχειριστή. Η πρακτική αυτή, δίνει στον διαχειριστή την ικανότητα να αναπτύξει ή να χρησιμοποιήσει οποιαδήποτε μέθοδο ανίχνευσης επιθυμεί, αρκεί να μεταδώσει στην εφαρμογή Αντιμετώπισης Ανωμαλιών τα απαραίτητα δεδομένα, στην κατάλληλη μορφή. Η αξιολόγησης της αποδοτικότητας της προτεινόμενης αρχιτεκτονικής βασίστηκε σε πραγματική κίνηση, προερχόμενη από πολλαπλά σημεία του δικτύου του Ε.Μ.Π.

5.4.1 Πειραματική τοπολογία και λεπτομέρειες υλοποίησης

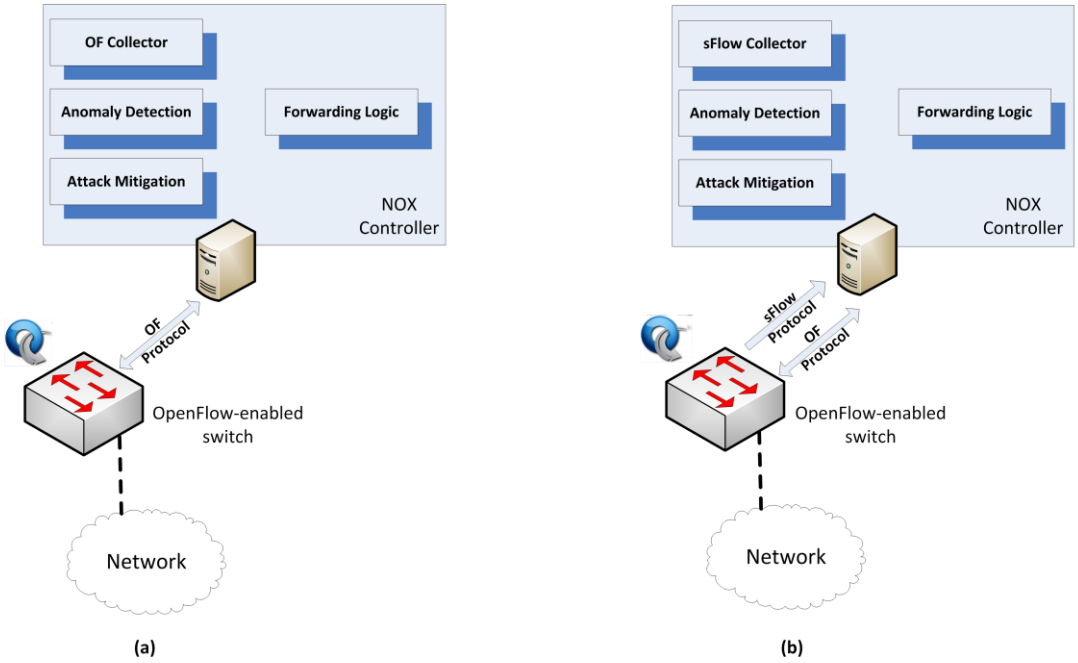
Όλα τα δομικά στοιχεία και οι αλγόριθμοι που περιγράφονται, υλοποιήθηκαν σε γλώσσα Python. Ακόμη, για την διεξαγωγή των πειραμάτων ήταν απαραίτητη η χρήση μεταγωγέων OF, οι οποίοι να υποστηρίζουν και το πρωτόκολλο sFlow. Για το λόγο αυτό, υιοθετήθηκε για το μεγαλύτερο μέρος της μελέτης, υλοποίηση του Open vSwitch (OVS) [75], το οποίο αποτελεί έναν μεταγωγέα υλοποιημένο μέσω λογισμικού (software switch), ικανό να διαχειριστεί υψηλούς ρυθμούς δικτυακής κίνησης. Ο ρυθμός εξυπηρέτησης πακέτων επικυρώθηκε με το λογισμικό NTOP [76], μέσω του οποίου παρακολουθούνταν η

εξερχόμενη κίνηση του OVS. Με τον τρόπο αυτό επιβεβαιώθηκαν οι προσδοκίες μας για τις επιδόσεις του OVS, αφού κατέστη δυνατή η αξιόπιστη μεταγωγή πακέτων με ρυθμούς έως 100Mbps με ταυτόχρονη εξαγωγή δειγμάτων sFlow εφαρμόζοντας ρυθμό δειγματοληψίας 1/64, καθώς και έως 500Mbps με sFlow ρυθμό δειγματοληψίας 1/256. Για να επιτευχθούν οι συγκεκριμένοι ρυθμοί μεταγωγής πακέτων, το λογισμικό του OVS εγκαταστάθηκε σε εξυπηρετητή με δύο πυρήνες των 3GHz και 8GB μνήμη RAM. Τα πειράματα με υψηλούς ρυθμούς της τάξης των 500Mbps επαναλήφθηκαν κάνοντας χρήση ενός μεταγωγέα NEC IP8800/S3640, ώστε να διερευνηθεί η εφαρμοσιμότητα της προτεινόμενης λύσης σε πραγματικούς μεταγωγείς OF, υλοποιημένους σε hardware, ικανούς να εξυπηρετήσουν πακέτα σε line-rate.

Στο Σχήμα 7 φαίνεται η πειραματική υποδομή, καθώς και οι εφαρμογές του NOX Controller που υλοποιήθηκαν και χρησιμοποιήθηκαν για την αξιολόγηση της προτεινόμενης χρήσης, εκμεταλλευόμενοι στη μία περίπτωση τις εγγενείς δυνατότητες του OpenFlow για συλλογή στατιστικών δεδομένων, και στη δεύτερη περίπτωση κάνοντας χρήση του πρωτοκόλλου sFlow. Τα πειράματά μας βασίστηκαν σε πιλοτική εγκατάσταση με έναν μεταγωγέα OF για τη διερεύνηση της εφαρμοσιμότητας (proof of concept) σε διαφορετικού τύπου μεταγωγείς OF.

Πιο συγκεκριμένα, για δικτυακή κίνηση χαμηλού ρυθμού, αξιολογήθηκαν και συγκρίθηκαν οι δύο εναλλακτικές μέθοδοι συλλογής στατιστικών για τις ροές. Αρχικά, για την περίπτωση της εγγενούς μεθόδου συλλογής δεδομένων OF, ορίστηκε συγκεκριμένη τιμή για το *idle-timeout* κάθε εγγραφής στον πίνακα ροών. Το *idle-timeout* ορίστηκε στα 31 δευτερόλεπτα αφού η χρονική διαφορά μεταξύ δύο διαδοχικών μετρήσεων ήταν 30 δευτερόλεπτα, ώστε να μην προλάβει να λήξει η εγγραφή πριν την εκτέλεση της μέτρησης.

Για την περίπτωση της συλλογής στατιστικών μέσω του πρωτοκόλλου sFlow, υλοποιήθηκε και χρησιμοποιήθηκε ένας sFlow Collector ως εφαρμογή του NOX Controller, η οποία δρα παράλληλα με δευτερεύουσα εφαρμογή του NOX, η οποία καθορίζει την λογική προώθησης πακέτων σε μεταγωγείς OF, πραγματοποιώντας μια τυπική διαδικασία MAC learning. Όπως έχει ήδη επεξηγηθεί, στη θέση της συγκεκριμένης εφαρμογής για την προώθηση των πακέτων μπορεί να χρησιμοποιηθεί οποιαδήποτε άλλη, χωρίς να επηρεάζεται η διαδικασία συλλογής στατιστικών μέσω του πρωτοκόλλου sFlow.



Σχήμα 7: Κύρια δομικά στοιχεία της προτεινόμενης αρχιτεκτονικής για ανίχνευση και αντιμετώπιση δικτυακών ανωμαλιών για τις περιπτώσεις: (α) Εγγενούς OF μεθόδου συλλογής δεδομένων, και (β) μεθόδου συλλογής δεδομένων βασισμένη στο πρωτόκολλο sFlow.

5.4.2 Καταγραφή και αναπαραγωγή πραγματικής δικτυακής κίνησης

Στοχεύοντας στην αξιολόγηση της προτεινόμενης μεθόδου ανίχνευσης και αντιμετώπισης δικτυακών ανωμαλιών εξομοιώνοντας διαφορετικά δικτυακά περιβάλλοντα, συλλέχθηκε πραγματική κίνηση από τρία διαφορετικά σημεία του Ε.Μ.Π. Αρχικά, αξιολογήθηκε η αποδοτικότητα της προτεινόμενης μεθόδου σε συνθήκες σχετικά χαμηλής δικτυακής κίνησης, χρησιμοποιώντας κίνηση που καταγράφηκε στο εργαστήριο NETMODE της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π. Με αυτόν τον τρόπο προσομοιώθηκε ένα περιβάλλον τύπου Small Office / Home Office (SOHO), με τον μέσω ρυθμό κίνησης, προερχόμενης από 35 εξυπηρετητές, να κυμαίνεται στα 50Mbps.

Για την περεταίρω αξιολόγηση του μηχανισμού, πραγματοποιήθηκαν πειράματα με υψηλότερους ρυθμούς κίνησης, περίπου 100Mbps, εξομοιώνοντας ένα μικρού μεγέθους Data Center. Για το σκοπό αυτό συλλέχθηκε κίνηση από ένα τμήμα της συνολικής δικτυακής κίνησης του Ε.Μ.Π. Τέλος, για την προσομοίωση δικτυακών συνθηκών μεγαλύτερης κλίμακας, συλλέχθηκε κίνηση από ολόκληρο το Ε.Μ.Π. Ο μέσος ρυθμός κίνησης, τη δεδομένη χρονική περίοδο, κυμάνθηκε στα 500Mbps. Η συλλεχθείσα κίνηση

των 50Mbps και 100Mbps, αντιστοιχεί σε διάρκεια μίας εβδομάδας, ενώ η κίνηση των 500Mbps αντιστοιχεί σε διάρκεια δύο ημερών, λόγω του τεράστιου όγκου των αρχείων που προέκυψαν κατά την καταγραφή. Οι καταγραφές αυτές χρησιμοποιήθηκαν για την αξιολόγησης της ακρίβειας και των δυνατοτήτων ανίχνευσης του προτεινόμενου μηχανισμού στην περίπτωση χρήσης της εγγενούς μεθόδου OF, και στην περίπτωση χρήσης του πρωτοκόλλου sFlow.

Για την αναπαραγωγή της καταγεγραμμένης δικτυακής κίνησης χρησιμοποιήθηκε το εργαλείο *Tcpreplay* [77], μέσω του οποίου επιτεύχθηκε η εισαγωγή και αναπαραγωγή των πακέτων σε μία συγκεκριμένη θύρα του μεταγωγέα OF της πειραματικής τοπολογίας. Το *Tcpreplay* προσφέρει επίσης τη δυνατότητα αναπαραγωγής της καταγεγραμμένης κίνησης σε πραγματικό ρυθμό. Για την αναπαραγωγή κακόβουλης κίνησης χρησιμοποιήσαμε την εργαλειοθήκη *Scapy* [78], μέσω του οποίου μπορούν να κατασκευάζονται και να αποστέλλονται πακέτα, ορίζοντας προγραμματιστικά τις τιμές των διαφόρων πεδίων των επικεφαλίδων τους (π.χ. *src/dst IP, src/dst Port, IP protocol,* κλπ.). Έτσι, για την προσομοίωση επιθέσεων DDoS, δημιουργήσαμε πακέτα *SYN* με προκαθορισμένη διεύθυνση IP προορισμού και θύρα προορισμού Επιπέδου 4, και τυχαίες διευθύνσεις IP πηγής και θύρες πηγής. Για την περίπτωση επίθεσης τύπου Worm Propagation δημιουργήσαμε κίνηση με τον ίδιο τρόπο, με τη μόνη διαφορά ότι το ζευγάρι διεύθυνσης IP και θύρας προορισμού ήταν τυχαίο, ενώ ήταν προκαθορισμένο το ζευγάρι πηγής. Τέλος για την περίπτωση του Port Scanning, κατασκευάστηκαν και εισήχθησαν πακέτα με συγκεκριμένες διευθύνσεις IP πηγής και προορισμού, και τυχαία καθοριζόμενες τιμές θυρών Επιπέδου 4 πηγής και προορισμού.

5.4.3 Πειράματα ανίχνευσης ανωμαλιών μέσω προσομοίωσης

Για την αποτελεσματική αξιολόγηση του προτεινόμενου μηχανισμού, δοκιμάσαμε τους αλγορίθμους, προσομοιώνοντας διαφορετικά δικτυακά περιβάλλοντα, μεταβάλλοντας τις τιμές των παρακάτω τριών μεταβλητών: (i) μέσος ρυθμός κανονικής κίνησης, (ii) ρυθμός δειγματοληψίας, και (iii) ρυθμός κακόβουλης κίνησης. Οι αντίστοιχες τιμές φαίνονται αναλυτικά στον Πίνακας 8. Για κάθε πειραματική κατηγορία, παράλληλα με την κανονική κίνηση (προερχόμενη από καταγραφές κίνησης του Ε.Μ.Π. όπως αναφέρθηκε παραπάνω), εισήχθησαν στο δίκτυο πακέτα κατασκευασμένα μέσω του *Scapy*, προσομοιώνοντας επιθέσεις DDoS, Worm Propagation και Port Scanning, σε ποικίλους ρυθμούς.

Συγκεκριμένα, πραγματοποιήθηκαν τα εξής πειράματα:

- Μέσος ρυθμός κίνησης 50Mbps, πραγματοποιώντας συλλογή στατιστικών δεδομένων και με τις δύο μεθόδους που έχουν αναλυθεί (εγγενής OF μέθοδος και μέθοδος βασισμένη στο sFlow). Στην περίπτωση της sFlow μεθόδου ο ρυθμός δειγματοληψίας ήταν 1/64. Και στις δύο περιπτώσεις εκμεταλλευτήκαμε τις δυνατότητες του OVS ως μεταγωγέα OF.
- Μέσος ρυθμός κίνησης 100Mbps, με συλλογή δεδομένων μέσω της μεθόδου sFlow, εφαρμόζοντας ρυθμό δειγματοληψίας 1/64 πακέτα σε μεταγωγέα OVS.
- Μέσος ρυθμός κίνησης 500Mbps, με συλλογή δεδομένων μέσω της μεθόδου sFlow, εφαρμόζοντας ρυθμό δειγματοληψίας 1/256 πακέτα σε μεταγωγέα OVS. Στη συνέχεια πραγματοποιήθηκε το ίδιο πείραμα χρησιμοποιώντας ως μεταγωγέα OF το NEC IP8800/S3640, αποσκοπώντας στην αξιολόγηση του προτεινόμενου μηχανισμού με πραγματικές συσκευές hardware του εμπορίου.

Πείραμα	**Average Traffic Rate (Mbps)**	**Sampling Rate**		**Attack rate (pkts/sec)**
1	50	No Sampling (Native OF)	1/64 (sFlow)	50 - 200
2	100	1/64 (sFlow)		200-500
3	500	1/256 (sFlow)		1000-2500

Πίνακας 8: Χαρακτηριστικές παράμετροι πειραμάτων που διεξήχθησαν.

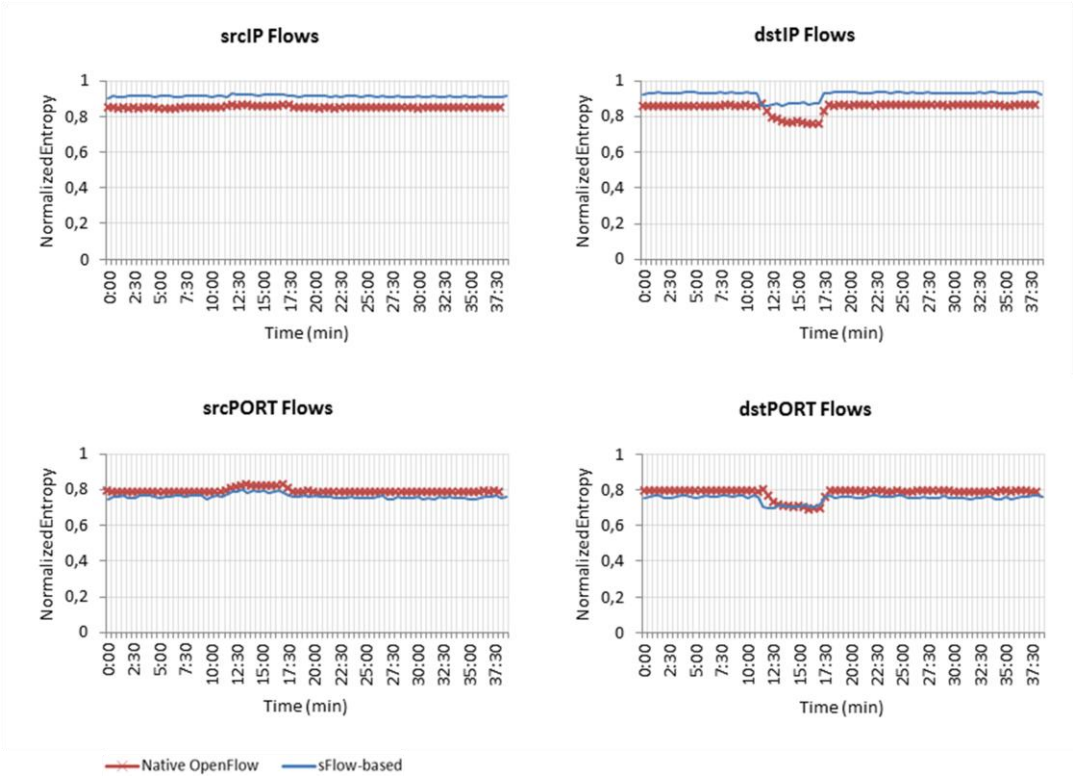
Στόχος του πρώτου πειράματος είναι να αποδειχθεί ότι και οι δύο μέθοδοι συλλογής στατιστικών δεδομένων μπορούν να εφαρμοστούν αποτελεσματικά για την ανίχνευση πιθανών ανωμαλιών σε περιβάλλοντα χαμηλής κίνησης. Ταυτόχρονα, συγκρίνονται οι δύο διαθέσιμες προσεγγίσεις, οι οποίες έχουν περιγραφεί και αφορούν την παρακολούθηση της δικτυακής κίνησης και τη συλλογή στατιστικών δεδομένων, με απώτερο στόχο την αξιολόγηση της επάρκειας της πληροφορίας που συλλέγεται στην περίπτωση του sFlow, λόγω δειγματοληψίας.

Για το σκοπό αυτό, σε κάθε περίπτωση, αναπαράχθηκε η κίνηση των 50Mbps που συλλέχθηκε από τμήμα του δικτύου του Ε.Μ.Π., ενώ παράλληλα έγινε προσομοίωση επιθέσεων DDoS, Worm propagation και Port Scanning. Προκειμένου να αξιολογηθεί η μέθοδος σε ποικίλους ρυθμούς μετάδοσης κακόβουλης κίνησης, πραγματοποιήθηκαν επιθέσεις με 50, 100 και 200 πακέτα ανά δευτερόλεπτο. Αναλογικά με την κανονική κίνηση

η οποία κυμαινόταν μεταξύ 12.000 – 13.000 πακέτα το δευτερόλεπτο, η κακόβουλη κίνηση ήταν ιδιαίτερα χαμηλή.

5.4.3.1 Ανίχνευση επιθέσεων με βάση την εντροπία

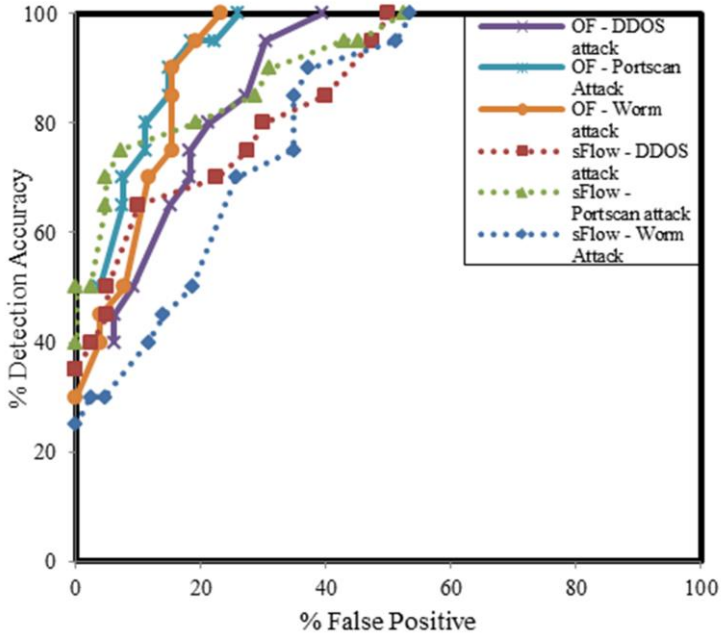
Για τη σύγκριση των δύο μεθόδων συλλογής στατιστικών δεδομένων (sFlow και εγγενής μέθοδος OF) σε περιπτώσεις επιθέσεων, πραγματοποιήθηκαν μετρήσεις που βασίστηκαν σε δεδομένα (dataset) από επιθέσεις που καταγράφηκαν στο δίκτυο του Ε.Μ.Π. Στο Σχήμα 8 παρουσιάζεται η μεταβολή της εντροπίας των ροών όσον αφορά τα πεδία Source IP, Destination IP, Source Port και Destination Port, αντιπαραβάλλοντας σε κάθε περίπτωση τις τιμές που προέκυψαν συλλέγοντας δεδομένα μέσω τις εγγενούς μεθόδου OF, με εκείνες που προέκυψαν μέσω της μεθόδου η οποία βασίζεται στο sFlow. Μέσω της σύγκρισης αυτής, είναι εμφανής η ομοιότητα των αποτελεσμάτων σε κάθε περίπτωση, επιβεβαιώνοντας την επάρκεια της πληροφορίας η οποία συλλέγεται μέσω του sFlow για την ανίχνευση δικτυακών ανωμαλιών, παρόλο που το sFlow συλλέγονται δειγματοληπτικά οι επικεφαλίδες από 1 ανά 64 πακέτα, ενώ η εγγενής μέθοδος του OF καταγράφει όλα τα πακέτα.



Σχήμα 8: Υπολογισμός της μεταβολής της εντροπίας μέσω (α) της εγγενούς OpenFlow μεθόδου, και (β) κάνοντας χρήση του πρωτοκόλλου sFlow

Στη συνέχεια, παρουσιάζονται και αναλύονται οι καμπύλες ROC, μέσω των οποίων απεικονίζονται τα ποσοστά αληθώς-θετικών (True-Positive) και ψευδώς-θετικών (False-Positive) επιθέσεων που αναγνώρισε ο αλγόριθμος ανίχνευσης ανωμαλιών, για κάθε διαφορετικό τύπο επίθεσης, και για κάθε διαφορετική μέθοδο συλλογής δεδομένων.

Το Σχήμα 9 απεικονίζει τις καμπύλες Receiver Operating Characteristics (ROC) για τα πειράματα της πρώτης κατηγορίας, όπως αυτές περιγράφονται στον Πίνακας 8. Όπως ήταν αναμενόμενο, η ανίχνευση ανωμαλιών στην περίπτωση χρήσης του OF για της συλλογή πληροφορίας είναι ακριβής, λόγω του ότι δεν υπάρχει δειγματοληψία. Έτσι, στην περίπτωση αυτή επιτυγχάνεται 100% ανίχνευση δικτυακών ανωμαλιών, με ποσοστά False-Positives κυμαινόμενα μεταξύ 23% και 39,3%, ανάλογα με τον τύπο της ανωμαλίας. Εφαρμόζοντας την μέθοδο συλλογής στατιστικών μέσω sFlow επιτυγχάνεται επίσης ανίχνευση ανωμαλιών 100%, με ποσοστό False-Positives περίπου 50% για κάθε τύπο επίθεσης. Όμως, όπως θα αναλυθεί και σε επόμενη παράγραφο, ο απαιτούμενοι υπολογιστικοί πόροι στην δεύτερη περίπτωση ήταν σημαντικά μειωμένοι, σε σύγκριση με την περίπτωση της OF μεθόδου.

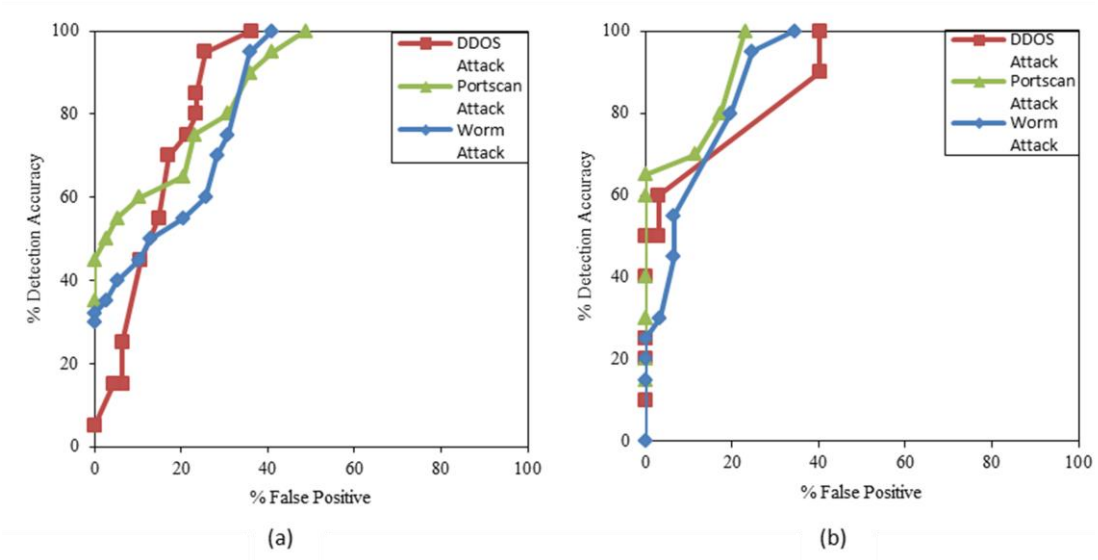


Σχήμα 9: Καμπύλες ROC για την ανίχνευση επιθέσεων DDoS, Worm Propagation και Port Scanning μέσω μεταβολής της εντροπίας, κάνοντας χρήση στατιστικών δεδομένων που συλλέχθηκαν (α) μέσω της εγγενούς OF μεθόδου, και (β) μέσω του πρωτοκόλλου sFlow.

Τα πειραματικά αποτελέσματα έδειξαν ότι σε περιβάλλοντα που χαρακτηρίζονται από χαμηλούς ρυθμούς μεταγωγής πακέτων, μπορούν να παραβλεφθούν τα μειονεκτήματα της εγγενούς μεθόδου OF για συλλογή στατιστικών δεδομένων, όπως αυτά έχουν αναλυθεί.

Όμως, σε περιβάλλοντα υψηλής κίνησης (που προσομοιώνονται με τα πειράματα που ακολουθούν για ρυθμούς 100 και 500 Mbps), η μέθοδος αυτοί θα είχε εξαιρετικά υψηλές απαιτήσεις υπολογιστικών πόρων, ώστε να γίνει αποτελεσματικά η προώθηση των πακέτων, αλλά και η περιοδική ανίχνευση ανωμαλιών στο δίκτυο. Αυτό μπορεί να εισάγει καθυστέρηση στην προώθηση των πακέτων, όπως φάνηκε κατά την πειραματική διαδικασία. Επιπροσθέτως, κατά τη διάρκεια εισαγωγής κακόβουλης κίνησης σε περιβάλλοντα υψηλής κίνησης, παρατηρήθηκε το φαινόμενο πρόκλησης επίθεσης DoS στο Επίπεδο Ελέγχου της υποδομής, λόγω υπερβολικής σηματοδοσίας και υπερφόρτωσης των επεξεργαστικών πόρων του OF Controller. Αντιθέτως, υιοθετώντας την μέθοδο sFlow σε περιβάλλοντα υψηλής κίνησης, παρατηρήθηκε σημαντική μείωση των απαιτούμενων πόρων στο Επίπεδο Ελέγχου. Σε επόμενη παράγραφο παρουσιάζονται και αναλύονται εκτενέστερα οι μετρήσεις αυτές.

Στο Σχήμα 10(α) παρουσιάζουμε τις καμπύλες ROC για την δεύτερη κατηγορία πειραμάτων του Πίνακας 8. Για τα πειράματα αυτά. η κανονική κίνηση ήταν περίπου 100 Mbps, με τον μέσο ρυθμό πακέτων να φτάνει στα 25.000 πακέτα το δευτερόλεπτο. Ακόμη, εξομοιώθηκαν πολλαπλές επιθέσεις, με ρυθμούς πακέτων 200, 350 και 500 πακέτα ανά δευτερόλεπτο. Όπως φαίνεται στο Σχήμα 10(β), χρησιμοποιώντας το sFlow για τη συλλογή στατιστικών δειγμάτων, επιτεύχθηκε ποσοστό ανίχνευσης 100%, έχοντας ποσοστό False-Positive 40%, 42% και 50% για επιθέσεις τύπου DDoS, Worm Propagation και Port Scanning αντίστοιχα.



Σχήμα 10: (α) Καμπύλες ROC για τα πειράματα που πραγματοποιήθηκαν σε κίνηση 100 Mbps, (β) Καμπύλες ROC για τα πειράματα που πραγματοποιήθηκαν σε κίνηση 500 Mbps.

Στο Σχήμα 10(β) εμφανίζονται οι καμπύλες ROC για την τελευταία κατηγορία πειραμάτων υψηλής κίνησης. Στην περίπτωση αυτή η κανονική κίνηση ήταν 500 Mbps κατά μέσο όρο, με τον μέσο ρυθμό πακέτων να βρίσκεται στα 130.000 πακέτα το δευτερόλεπτο. Όπως φαίνεται και στο σχήμα, επιτεύχθηκε ποσοστό ανίχνευσης 100%, έχοντας ταυτόχρονα ποσοστό False-Positive 23%, 27% και 34% για επιθέσεις Port Scanning, DDoS και Worm Propagation αντίστοιχα.

Στο Σχήμα 10 παρατηρήθηκε ότι εφαρμόζοντας δειγματοληψία 1/256 πακέτα σε κίνηση της τάξης των 500 Mbps, επιτεύχθηκε πιο ακριβής ανίχνευση επιθέσεων σε σχέση με τις προηγούμενες δύο κατηγορίες πειραμάτων. Αυτό οφείλεται στο γεγονός ότι τα περιβάλλοντα υψηλής κίνησης εξυπηρετούν χιλιάδες διαφορετικές ροές πακέτων, ανεξάρτητων υπολογιστών/εξυπηρετητών. Συνεπώς, είναι πιο εύκολη η ανίχνευση ανωμαλιών μέσω μεταβολών στις εντροπίες των πεδίων των επικεφαλίδων των πακέτων, παρά την εφαρμογή δειγματοληψίας της τάξης των 1/256 πακέτων.

Τέλος, επαναλήφθηκαν τα πειράματα της τρίτης κατηγορίας, αντικαθιστώντας το OVS με έναν NEC IP880/S3640 μεταγωγέα. Κατά τη σύγκρισή τους με την περίπτωση του OVS, τα αποτελέσματα ήταν πανομοιότυπα, επιβεβαιώνοντας την υπόθεση ότι η προτεινόμενη αρχιτεκτονική μπορεί να εφαρμοστεί για την προστασία υποδομών οι οποίες χρησιμοποιούν εμπορικό εξοπλισμό μεταγωγέων OF.

5.4.3.2 Ανίχνευση επιθέσεων με βάση τον αλγόριθμο TRW-CB

Προκειμένου να αξιολογηθεί πληρέστερα η καταλληλότητα της μεθόδου sFlow για συλλογή στατιστικών, υλοποιήθηκε και δεύτερη μέθοδος ανίχνευσης ανωμαλιών βασισμένη στον αλγόριθμο Threshold Random Walk with Credit Based connection rate limiting (TRW-CB) [79]. Ο αλγόριθμος TRW-CB είναι ευρέως διαδεδομένος για την αξιόπιστη ανίχνευση επιθέσεων Worm Propagation και Port Scanning, οι οποίες μπορεί να χαρακτηρίζονται από χαμηλό ρυθμό μετάδοσης δεδομένων, και άρα δεν είναι προφανής η διαδικασία αναγνώρισής τους.

Στην ενότητα αυτή, παρουσιάζονται πειραματικά αποτελέσματα χρησιμοποιώντας τον αλγόριθμο TRW-CB, ως τη βασική μέθοδο ανίχνευσης ανωμαλιών του προτεινόμενου μηχανισμού. Η μέθοδος αυτή αποθηκεύει στατιστικά στοιχεία ξεχωριστά για κάθε έναν εξυπηρετητή που βρίσκεται μέσα στο εκάστοτε προστατευόμενο δίκτυο, και για το λόγο αυτό είναι πιο εύκολη η ανίχνευση σημαντικών μεταβολών που σχετίζονται με τα χαρακτηριστικά της κανονικής κίνησης. Αντίθετα, η μέθοδος της εντροπίας, η οποία έχει

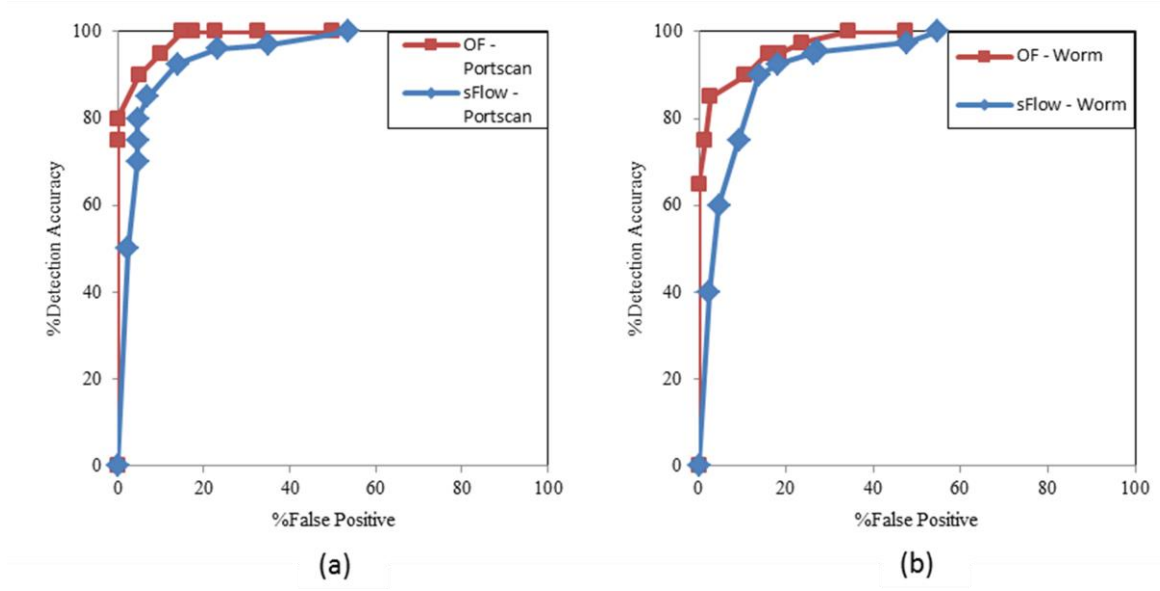
ήδη αξιολογηθεί στην ενότητα 5.4.3.1, εκμεταλλεύεται βασικά μοντέλα που χαρακτηρίζουν τη δικτυακή κίνηση, και χρησιμοποιώντας προκαθορισμένα πεδία των επικεφαλίδων επιδιώκει να ανιχνεύσει παρεκκλίσεις των τιμών των πεδίων αυτών από τα συνηθισμένα επίπεδα.

Στα πειράματα που πραγματοποιήθηκαν, ο συγκεκριμένος αλγόριθμος τροφοδοτήθηκε με δεδομένα και από της δύο μεθόδους συλλογής στατιστικής πληροφορίας (sFlow και εγγενής μέθοδος OF), ξεχωριστά. Στη συνέχεια, συγκρίθηκαν τα αποτελέσματα που προέκυψαν, και αναλύθηκε η ανταλλαγή (trade-off) μεταξύ ακρίβειας αποτελεσμάτων και κατανάλωσης πόρων.

Ο αλγόριθμος TRW-CB υλοποιήθηκε ως μία ανεξάρτητη εφαρμογή του NOX Controller. Πρόγονος του αλγορίθμου αυτού ήταν ο Threshold Random Walk (TRW) [80], μέσω του οποίου είναι δυνατή η ανίχνευση επιθέσεων Port Scanning, βάσει παρατήρησης των επιτυχών συνδέσεων μεταξύ ενός εξυπηρετητή και των απομακρυσμένων πελατών οι οποίοι έρχονται σε επαφή μαζί του. Συγκεκριμένα, ο αλγόριθμος TRW αξιοποιεί τη διαφορά μεταξύ της συχνότητας με την οποία εμφανίζονται επιτυχημένες συνδέσεις από καλοήθεις πελάτες, σε σύγκριση με την συχνότητα με την οποία αποτυχίες σύνδεσης λόγω κακόβουλων πελατών (οι οποίοι πραγματοποιούν επιθέσεις Port Scanning). Ο αλγόριθμος TRW-CB αποτελεί την επέκταση του TRW, επιβάλλοντας την συνεχή παρακολούθηση ενός πελάτη -ακόμη και αν αυτός έχει αναγνωριστεί ως καλοήθης πελάτης-, ώστε να είναι δυνατή η αναγνώριση επιθέσεων τύπου Worm Propagation. Ακόμη, ο αλγόριθμος TRW-CB έχει τη δυνατότητα περιορισμού του εύρους ζώνης που καταναλώνει ένας πελάτης, ώστε σε περίπτωση καθυστερημένης διάγνωσης μιας επίθεσης τύπου Worm Propagation, να αποφεύγεται η γρήγορη εξάπλωση του κακόβουλου λογισμικού στο δίκτυο.

Σχήμα 11 απεικονίζεται η ακρίβεια που επιτυγχάνεται με αλγόριθμο ανίχνευσης TRW-CB στις δύο μεθόδους συλλογής στατιστικής πληροφορίας, για τις περιπτώσεις (α) επιθέσεων τύπου Port Scanning, και (β) επιθέσεων τύπου Worm Propagation. Κατά τη διεξαγωγή των συγκεκριμένων πειραμάτων, η κανονική κίνηση του δικτύου χαρακτηριζόταν από μέσο ρυθμό μετάδοσης πληροφορίας 50 Mbps, ενώ οι επιθέσεις Worm Propagation και Port Scanning αποτελούνταν από ένα μείγμα επιθέσεων, με ρυθμό μετάδοσης πακέτων 50 και 100 πακέτα ανά δευτερόλεπτο, ακολουθώντας το μοντέλο του Πειράματος 1 στον Πίνακας 8 ανωτέρω. Όπως είναι εμφανές, τα αποτελέσματα που βασίζονται στη συλλογή δεδομένων μέσω sFlow σε σύγκριση με εκείνα της εγγενούς μεθόδου OF, εμφανίζουν μια ελαφρά αύξηση στον αριθμό των False-Positives, προκειμένου να επιτευχθεί ποσοστό ανίχνευσης επιθέσεων μεγαλύτερο του 85%. Όμως,

μέσω του sFlow επιτυγχάνεται σημαντική μείωση στην κατανάλωση πόρων συστήματος, όπως αναλύεται και στην ακόλουθη ενότητα, προσφέροντας μια κλιμακώσιμη λύση.



Σχήμα 11: Καμπύλες ROC για την απόδοση του αλγορίθμου TRW-CB χρησιμοποιώντας δεδομένα από την εγγενή OF μέθοδο συλλογής και μέσω του πρωτοκόλλου sFlow, υπό συνθήκες: (a) Επιθέσεων Port Scanning, και (b) Επιθέσεων Worm Propagation.

5.4.3.3 Αξιολόγηση απόδοσης συστήματος

Σε αυτήν την ενότητα, θα αναλυθεί η κατανάλωση πόρων, τόσο στη μεριά του OF Controller, όσο και του μεταγωγέα OF, για οποιοδήποτε συνδυασμό από τις μεθόδους συλλογής στατιστικών δεδομένων, και τις μεθόδους ανίχνευσης ανωμαλιών που έχουν αναλυθεί στα ανωτέρω. Στόχος είναι η εκτίμηση της δυνατότητας που προσφέρει το sFlow για μείωση του φόρτου που προστίθεται στο Επίπεδο Ελέγχου, όταν απαιτείται η συνεχής συλλογή και παρακολούθηση των στατιστικών των ροών δεδομένων μέσα στο δίκτυο. Ο βαθμός χρησιμοποίησης της κεντρικής μονάδας επεξεργασίας, τόσο στον εξυπηρετητή που φιλοξενεί τον OF Controller, όσο και στους μεταγωγείς OF, αποτελεί βασική ένδειξη για την κλιμακωσιμότητα του προτεινόμενου μηχανισμού. Ακόμα, ο αριθμός των εγγραφών που υπάρχουν αποθηκευμένες σε έναν πίνακα ροών OpenFlow μπορεί να επηρεάσει την ταχύτητα προώθησης των πακέτων, καθώς για κάθε πακέτο κάθε ροής πρέπει να ελεγχθεί ολόκληρος ο πίνακας ροών, ώστε να διαπιστωθεί αν οι τιμές των επικεφαλίδων του συγκεκριμένου πακέτου αντιστοιχούν με κάποια αποθηκευμένη εγγραφή.

Στον Πίνακας 9, συγκρίνεται η μέση κατανάλωση υπολογιστικών κύκλων -στην πλευρά του μεταγωγέα OF-, όταν πραγματοποιείται ανίχνευση ανωμαλιών (και με τις δύο εναλλακτικές μεθόδους) χρησιμοποιώντας στη μία περίπτωση δεδομένα που έχουν συλλεχθεί μέσω της εγγενούς μεθόδου OpenFlow, και στην άλλη μέσω του πρωτοκόλλου sFlow. Επιπλέον, στον Πίνακας 9 φαίνεται ο μέσος αριθμός εγγραφών που υπάρχουν στον πίνακα ροών. Τέλος, πραγματοποιούμε τις ίδιες συγκρίσεις για την περίπτωση όπου πραγματοποιείται επίθεση της τάξης των 200 πακέτων ανά δευτερόλεπτο, και απεικονίζουμε τον μέσο αριθμό ροών που υπήρχαν στον πίνακα ροών κατά τη διάρκεια της επίθεσης. Η κανονική κίνηση κατά τη διάρκεια της επίθεσης υπερέβαινε ελάχιστα τα 50 Mbps. Όπως μπορούμε να παρατηρήσουμε, ο βαθμός χρησιμοποίησης της CPU όταν χρησιμοποιείται η μέθοδος sFlow μειώνεται από το 61% στο 39% για την περίπτωση όπου χρησιμοποιείται ο αλγόριθμος μεταβολής εντροπίας και από 58% σε 39% για την περίπτωση του TRW-CB . Αντίστοιχα, ο απαιτούμενος αριθμός εγγραφών στον πίνακα ροών ενός μεταγωγέα OF μειώθηκε από τις 7.685 στις 351 εγγραφές για την πρώτη περίπτωση, και από 2606 σε 351 για την δεύτερη.

	50Mbps Background Traffic		**50Mbps Background Traffic with 200pps attack injected**	
	Average Number of Flows	**CPU usage**	**Average Number of Flows**	**CPU usage**
Entropy-based with sFlow	217	32%	351	39%
TRW-CB with sFlow	217	32%	351	39%
Entropy-based with Native OF	5184	47%	7685	61%
TRW-CB with Native OF	2022	42%	2606	58%

Πίνακας 9: Σύγκριση της επεξεργαστικής ισχύς και του αριθμού εγγραφών ροών που απαιτούνται από έναν μεταγωγέα OF για συλλογή δεδομένων μέσω της sFlow μεθόδου και μέσω της εγγενούς OF μεθόδου, χρησιμοποιώντας και συγκρίνοντας τα αποτελέσματα για πολλαπλές μεθόδου.

Ένα άλλο στοιχείο που προκύπτει από τον Πίνακας 9 αφορά στο μέσο αριθμό των εγγραφών ροών και στη χρήση της CPU του μεταγωγέα OF. Για την περίπτωση του sFlow (δύο πρώτες γραμμές του πίνακα) ο μεταγωγέας OF επιβαρύνεται με το ίδιο φορτίο

προώθησης πακέτων ανεξαρτήτως του αλγορίθμου που χρησιμοποιείται για την ανίχνευση ανωμαλιών. Αυτό δικαιολογείται από το γεγονός ότι η εφαρμογή του NOX που προσφέρει ουσιαστικά και την ευφυΐα για την προώθηση των πακέτων, είναι τελείως αποσυνδεδεμένη από τις εφαρμογές που πραγματοποιούν τη συλλογή στατιστικών και την ανίχνευση ανωμαλιών. Αντίθετα με τη συλλογή στατιστικών μέσω της εγγενούς μεθόδου OF η διαφορά των εγγραφών των απαιτούμενων ροών που εμφανίζεται για την μέθοδο της εντροπίας (7.685 όταν υπάρχει επίθεση) σε σχέση με την μέθοδο TRW-CB (2.606), οφείλεται στο ότι η πρώτη μέθοδος χρειάζεται και πληροφορία του Επιπέδου 4 για την ανίχνευση, ενώ η δεύτερη χρησιμοποιεί μόνο πληροφορία του Επιπέδου 3 με αποτέλεσμα την σύμπτυξη των ροών σε λιγότερες εγγραφές.

Εκτός από την κατανάλωση υπολογιστικών πόρων των μεταγωγέων OF, μείζονος σημασίας κριτήριο είναι και η επιβάρυνση της CPU του OF Controller ο οποίος μπορεί να επηρεαστεί σημαντικά από τους μηχανισμούς συλλογής δεδομένων. Στον Πίνακας 10 απεικονίζεται το κέρδος που προκύπτει στην κατανάλωση υπολογιστικών πόρων του OF Controller από τη χρήση της μεθόδου sFlow, σε σύγκριση με την εγγενή μέθοδο OF. Όπως προκύπτει από τον πίνακα, όταν δεν υπάρχει κακόβουλη κίνηση, η χρήση της CPU μειώνεται μέσω του sFlow (από 42% σε 25% για την μέθοδο με της εντροπίας και από 48% σε 27% για την μέθοδο TRW-CB). Κατά τη διάρκεια επίθεσης, η αντίστοιχη μείωση είναι ακόμη πιο εμφανής (από 63% σε 31% για τη μέθοδο της εντροπίας και από 60% σε 32% για την μέθοδος TRW-CB).

	50Mbps Traffic	**50Mbps with 200pps attack injected**
Entropy-based with sFlow	25%	31%
TRW-CB with sFlow	27%	32%
Entropy-based with Native OF	42%	63%
TRW-CB with Native OF	48%	60%

Πίνακας 10: Σύγκριση της κατανάλωσης επεξεργαστικής ισχύος του OF Controller όταν χρησιμοποιείται η sFlow μέθοδος συλλογής δεδομένων και όταν χρησιμοποιείται η εγγενής μέθοδος του πρωτοκόλλου OpenFlow. Η σύγκριση αυτή πραγματοποιείται κάνοντας χρήση πολλαπλών μεθόδων ανίχνευσης.

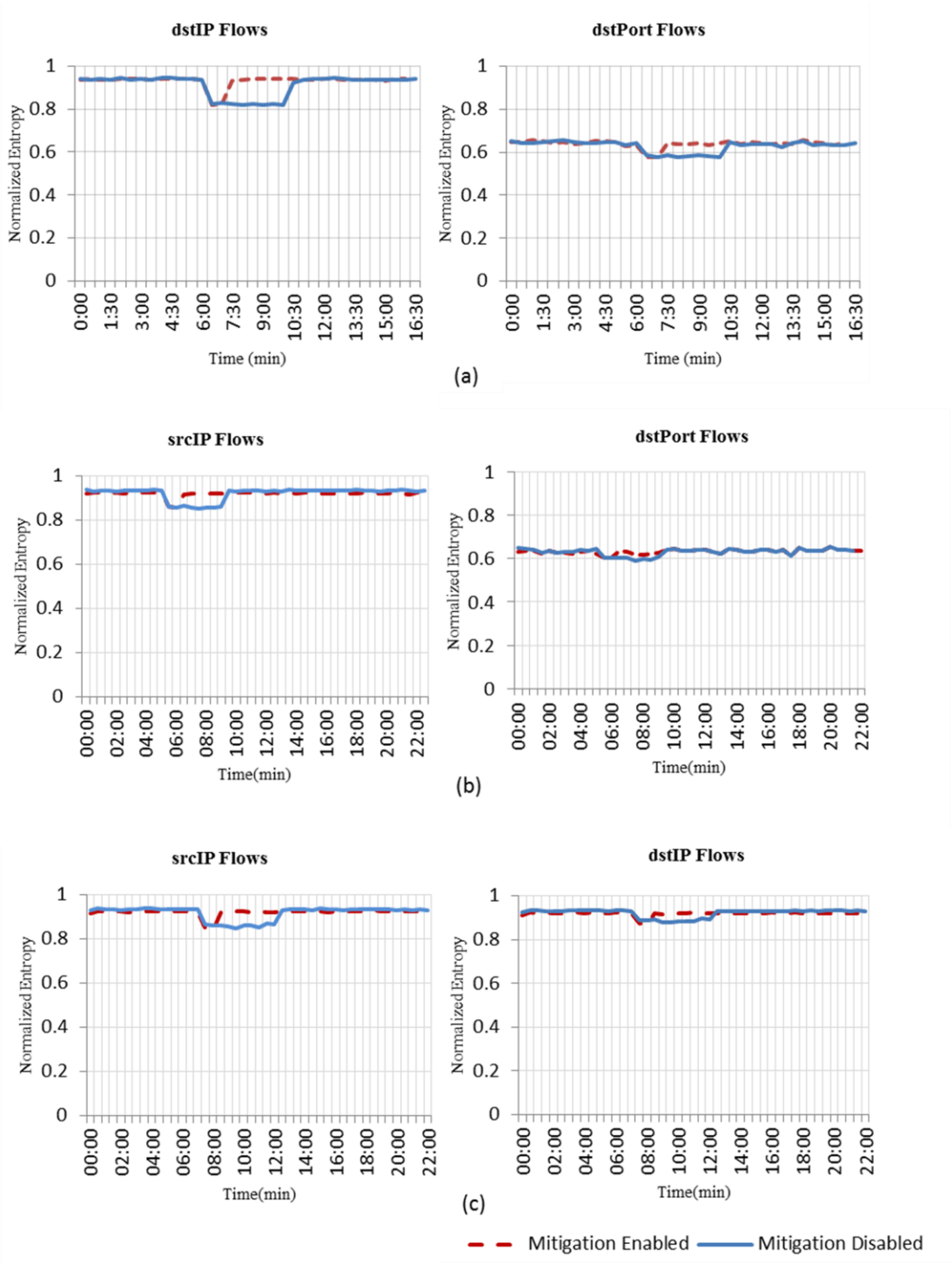
5.4.4 Αντιμετώπιση ανωμαλιών σε δίκτυα SDN

Στις προηγούμενες ενότητες συγκρίθηκαν οι μέθοδοι συλλογής στατιστικών δεδομένων, βάσει πολλαπλών αλγορίθμων ανίχνευσης ανωμαλιών. Σε αυτή την υποενότητα επιδεικνύονται οι δυνατότητες του πρωτοκόλλου OpenFlow για χρήση σε συστήματα αντιμετώπισης δικτυακών ανωμαλιών, καθώς και ο λόγος για τον οποίον η sFlow μέθοδος συλλογής δεδομένων υλοποιήθηκε ως ένα κύριο δομικό στοιχείο σε περιβάλλοντα SDN.

Για πειράματα που σχετίζονται με την αντιμετώπιση των ανωμαλιών, χρησιμοποιήθηκε το ίδιο σύνολο δεδομένων κίνησης (dataset) το οποίο χρησιμοποιήθηκε και για το πείραμα στην ενότητα 5.4.3.1. Συγκεκριμένα, μόλις ο αλγόριθμος ανιχνεύσει μία δικτυακή ανωμαλία, και αφού τη χαρακτηρίσει ως επίθεση DDoS στην θύρα *N* ενός εξυπηρετητή *A*, ο μηχανισμός Αντιμετώπισης Ανωμαλιών είναι σε θέση να αποκόψει τις ροές που σχετίζονται με την κακόβουλη κίνηση. Στο Σχήμα 12(a) απεικονίζονται οι τιμές της εντροπίας εκείνων των επικεφαλίδων, οι οποίες καταδεικνύουν επίθεση τύπου DDoS. Με διακεκομμένη γραμμή εμφανίζονται οι τιμές της εντροπίας όταν χρησιμοποιείται ο μηχανισμός Αντιμετώπισης Ανωμαλιών, ενώ με συνεχή γραμμή εμφανίζονται οι τιμές της εντροπίας όταν δεν χρησιμοποιείται ο συγκεκριμένος μηχανισμός, και άρα δεν αντιμετωπίζεται η επίθεση. Όπως είναι αναμενόμενο, μόλις αναγνωριστεί και περιοριστεί η κακόβουλη κίνηση, οι τιμές της εντροπίας επιστρέφουν στα φυσιολογικά τους επίπεδα. Κατ' αντιστοιχία, στο Σχήμα 12(b) και στο Σχήμα 12(c) εμφανίζονται τα αποτελέσματα αντιμετώπισης επιθέσεων τύπου Worm Propagation και Port Scanning αντίστοιχα. Είναι εμφανές, ότι και στις δύο αυτές περιπτώσεις, οι τιμές της σχετικής με την κάθε επίθεση εντροπίας, επιστρέφουν στα φυσιολογικά τους επίπεδα μόλις χρησιμοποιηθεί ο μηχανισμός Αντιμετώπισης Ανωμαλιών.

Στα πειράματά μας χρησιμοποιήθηκε χρονικό παράθυρο 30 δευτερολέπτων μεταξύ δύο διαδοχικών εκτελέσεων του αλγορίθμου Ανίχνευσης Ανωμαλιών για την ανάλυση των στατιστικών δεδομένων που συλλέχθηκαν σε αυτό το χρονικό παράθυρο. Κατόπιν αυτών των περιοδικών στατιστικών αναλύσεων, τα αποτελέσματα αποστέλλονται στο μηχανισμό Αντιμετώπισης Ανωμαλιών, ο οποίος γνωρίζει πλέον όλους τους συνδυασμούς των μεταβλητών *{A, N}* (όπως αναφέρθηκαν και στην προηγούμενη παράγραφο).

Ένας απλός τρόπος για την καταστολή μιας επίθεσης DDoS είναι ο αποκλεισμός όλης της κίνησης η οποία σχετίζεται με τον εξυπηρετητή ο οποίος δέχεται την επίθεση. Αυτό δικαιολογείται από το γεγονός ότι, οι πηγές από τις οποίες προέρχονται η κατανεμημένη αυτή επίθεση, μετριούνται σε χιλιάδες, και συνεπώς, ο αποκλεισμός κάθε μίας πηγής θα



Σχήμα 12: Απεικόνιση της μεταβολής της εντροπίας χαρακτηριστικών μεγεθών κατά τη διάρκεια επιθέσεων: (a) DDoS, (b) Worm Propagation, και (c) Port Scanning, με χρήση (κόκκινο) και χωρίς χρήση (μπλε) του μηχανισμού Ανίχνευσης Ανωμαλιών.

απαιτούσε συνολικά χιλιάδες κανόνες στον πίνακα ροών, κάτι το οποίο δεν είναι κλιμακώσιμο και στις περισσότερες των περιπτώσεων δεν είναι και εφικτό λόγω περιορισμών στο μέγεθος του πίνακα ροών των μεταγωγέων OF. Για τους λόγους αυτούς, ο

μηχανισμός Αντιμετώπισης Ανωμαλιών εισάγει στον πίνακα ροών μία νέα εγγραφή για την κίνηση που αφορά το θύμα της επίθεσης, προσθέτοντας το Action *Drop*, όπως φαίνεται και στον Πίνακας 11. Ο κανόνας αυτός, ουσιαστικά, αποτελείται από δύο εγγραφές στον πίνακα ροών, ώστε να καλύπτονται και οι δύο κατευθύνσεις (αποστολή-από και αποστολή-προς τον εξυπηρετητή). Ακόμη, στις εγγραφές αυτές αναθέτουμε προτεραιότητα υψηλότερη από αυτήν που χρησιμοποιείται για τους κανονικούς κανόνες προώθησης ροών. Τέλος, ορίζουμε την τιμή του *idle-timeout* ώστε οι εγγραφές να λήγουν μετά από ένα προκαθορισμένο διάστημα από τη στιγμή που θα γίνει η τελευταία αντιστοίχισή τους με ένα πακέτο.

ATTACK TYPE	LAYER 1	LAYER 2					LAYER 3				LAYER 4	
	IN PORT	ETHER			VLAN		IP				PORT	
		Src	dst	type	id	PCP	src	dst	proto	TOS	src	dst
DDoS	*	*	*	0x0800	*	*	*	A	0x06	*	*	N
DDoS	*	*	*	0x0800	*	*	A	*	0x06	*	N	*
WORM	*	*	*	0x0800	*	*	A	*	0x06	*	*	N
WORM	*	*	*	0x0800	*	*	*	A	0x06	*	N	*
SCAN	*	*	*	0x0800	*	*	A	B	0x06	*	*	*
SCAN	*	*	*	0x0800	*	*	B	A	0x06	*	*	*

Πίνακας 11: Ενδεικτική μορφή των εγγραφών στον πίνακα ροών ενός μεταγωγέα OF, για την αποκοπή διαφορετικών τύπων δικτυακών ανωμαλιών.

Για την αντιμετώπιση των επιθέσεων τύπου Port Scanning ή Worm Propagation, εφαρμόζουμε ακριβώς την ίδια λογική. Μόνη διαφορά είναι τα πεδία στα οποία ως τιμή ανατίθεται το wildcard. Συγκεκριμένα, σε περιπτώσεις Worm Propagation, στόχος είναι η αποκοπή του μολυσμένου υπολογιστή *A*, ο οποίος προσπαθεί να μεταδώσει κακόβουλο λογισμικό μέσω της θύρας *N* ενός άλλου υπολογιστή. Στην περίπτωση επιθέσεων Port Scanning, είναι συνηθισμένη η αποκοπή των ροών μεταξύ του υπολογιστή *A* ο οποίος διεξάγει το Port Scanning, και ολόκληρου του υποδικτύου *B* το οποίο δέχεται την επίθεση. Ο λόγος για τον οποίο αποκόπτουμε όλες τις ροές από τον *A* προς όλους τους υπολογιστές/εξυπηρετητές του *B*, είναι διότι κατά πάσα πιθανότητα, ο *A* θα προσπαθήσει να ελέγξει τις διαθέσιμες υπηρεσίες σε ολόκληρο το δίκτυο, στην προσπάθειά του να βρει τρωτά σημεία.

6 Κλιμακώσιμη Αντιμετώπιση Ανωμαλιών σε Παραδοσιακά Δικτυακά Περιβάλλοντα μέσω πρωτοκόλλου OpenFlow

6.1 Εισαγωγή

Στην προηγούμενη ενότητα παρουσιάστηκε ένας ολοκληρωμένος μηχανισμός για SDN υποδομές, ο οποίος είναι ικανός να διευκολύνει τους παρόχους, προσφέροντας δυνατότητες αυτοματοποιημένου περιορισμού της κίνησης προς ή από το θύμα. Μία άλλη προσέγγιση για τη δυναμική αντιμετώπιση επιθέσεων σε παραδοσιακά δίκτυα αποτελεί ο μηχανισμός Remotely Triggered Black-Holing (RTBH), ο οποίος εμφανίζεται [81] ως μία μέθοδος διαμοιρασμού στατικών κανόνων αναδρομολόγησης. Μέσω του RTBH, κίνηση η οποία προορίζεται για τον εξυπηρετητή-θύμα είναι δυνατό να ανακατευθυνθεί προς μια ανύπαρκτη δικτυακή διεπαφή (black hole) και συνεπώς να απορριφθεί.

Στην παρούσα ενότητα προτείνεται μία ολοκληρωμένη μέθοδος για την επέκταση της λειτουργικότητας του RTBH, μέσω: (α) δυναμικής παραμετροποίησης του μηχανισμού RTBH και αυτόματης ενεργοποίησής του μόλις ανιχνευθεί μία δικτυακή ανωμαλία, και (β) διάθεσης και εκμετάλλευσης λειτουργιών των προγραμματιζόμενων δικτύων (μέσω του πρωτοκόλλου OpenFlow) σε παραδοσιακά δικτυακά περιβάλλοντα.

Η λειτουργία αντιμετώπισης δικτυακών ανωμαλιών προσφέρεται ως μία Εικονικοποιημένη Δικτυακή Λειτουργία (Virtualized Network Function – VNF) στα πλαίσια του μοντέλου Εικονικοποίησης Δικτυακών Λειτουργιών (Network Function Virtualisation – NFV) όπως αυτό περιγράφεται και στο [29]. Κύριο χαρακτηριστικό της εν λόγω προσέγγισης είναι η αποφυγή χρήσης κλειστών ή/και υψηλών προδιαγραφών εξοπλισμού, αφού η διαδικασία μπορεί πλέον να επιτευχθεί μέσω κοινών εξυπηρετητών στους οποίους όμως εγκαθίσταται το απαιτούμενο λογισμικό. Ακόμη, η κίνηση από και προς το θύμα μια επίθεσης αναδρομολογείται προς έναν μεταγωγέα OF ο οποίος λειτουργεί ως ένας ενδιάμεσος (middlebox) και ελέγχεται από έναν OF Controller. Το στοιχείο αυτό, μαζί με τη δυναμική παραμετροποίηση του μηχανισμού RTBH, επιτρέπει λεπτομερή και στοχευμένη χειραγώγηση της δικτυακής κίνησης. Έτσι μπορεί να μετατραπεί η αντιμετώπιση επιθέσεων DDoS σε μία λογική διαδικασία τύπου VNF.

Επιπροσθέτως, στην ενότητα αυτή μελετάται και προτείνεται μία προσέγγιση η οποία βελτιώνει σημαντικά την κλιμακωσιμότητα της ανωτέρω λογικής διαδικασίας. Συγκεκριμένα, παρουσιάζεται ένας μηχανισμός ενοποίησης και επιλεκτικής απόρριψης

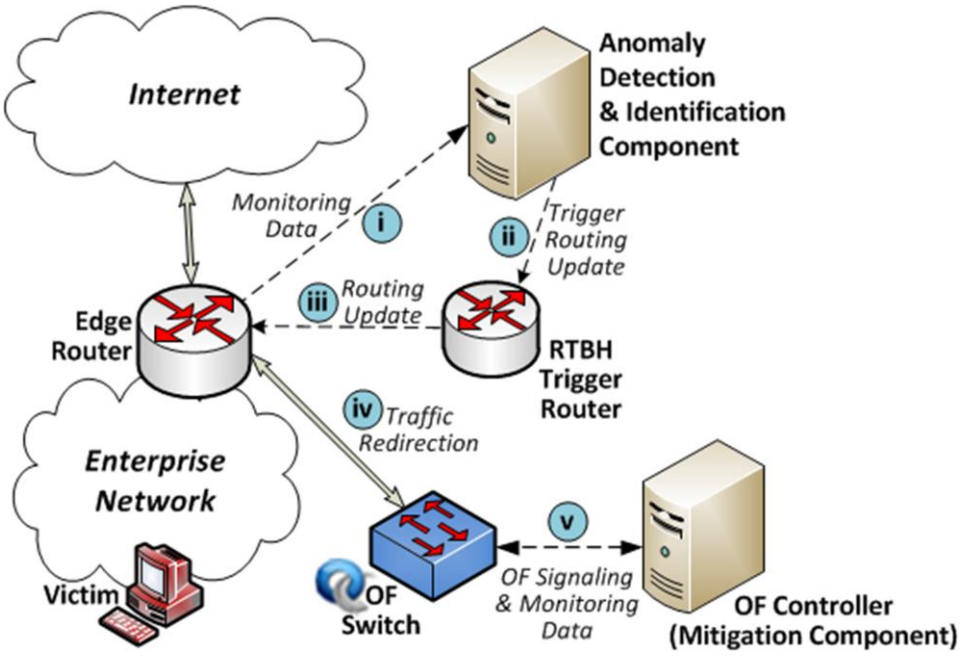
όλων κακόβουλων ροών, συνυπολογίζοντας (α) τη χωρητικότητα του πίνακα ροών του ενδιάμεσου μεταγωγέα OF, και (β) τον συνολικό αριθμό των κακόβουλων ροών.

Προκειμένου να εκτιμηθεί η αποτελεσματικότητα της συνολικής προτεινόμενης αρχιτεκτονικής αναπτύχθηκε και εγκαταστάθηκε πρότυπη έκδοση στο εργαστήριο. Η πρότυπη υλοποίηση συμπεριλαμβάνει μία διαδικασία ανίχνευσης δικτυακών ανωμαλιών πολλαπλών επιπέδων, η οποία τροφοδοτεί τα στοιχεία εκείνα τα οποία απαρτίζουν την λογική διαδικασία αντιμετώπισης επιθέσεων DDoS.

6.2 Σχεδιαστικές Αρχές και Περιγραφή Αρχιτεκτονικής

6.2.1 Σχεδιαστικές αρχές

Η προτεινόμενη αρχιτεκτονική απεικονίζεται σε υψηλό-αφαιρετικό επίπεδο στο Σχήμα 13: Θεωρούμε εξυπηρετητές σε μία δικτυακή περιοχή (Enterprise Network) οι οποίοι επικοινωνούν με το υπόλοιπο Internet μέσω ενός συνοριακού δρομολογητή (edge router) ο οποίο παράλληλα μεταφέρει στατιστικά δεδομένα στη μονάδα Ανίχνευσης και Αναγνώρισης Ανωμαλιών (Anomaly Detection and Identification – ADI) όπως φαίνεται στο Σχήμα 13-i.



Σχήμα 13: Προτεινόμενη αρχιτεκτονική αντιμετώπισης δικτυακών επιθέσεων σε παραδοσιακά περιβάλλοντα, με χρήση μεταγωγέα OpenFlow ως ενδιάμεσο

Μόλις ανιχνευθεί μία επίθεση ενεργοποιείται η μονάδα η οποία είναι υπεύθυνη για τη λειτουργία RTBH (Σχήμα 13-ii) και ενημερώνει καταλλήλως το συνοριακό δρομολογητή (Σχήμα 13-iii) ώστε εκείνος με τη σειρά του να αναδρομολογήσει την κίνηση του θύματος, κατευθύνοντάς την προς έναν ενδιάμεσο μεταγωγέα OF (Σχήμα 13-iv). Ο OF Controller ο οποίος ελέγχει τον μεταγωγέα αυτόν, είναι ικανός να διαχωρίσει τις κακόβουλες από τις καλόβουλες ροές και κατόπιν να εισάγει στον μεταγωγέα τις απαραίτητες εγγραφές ώστε οι κακόβουλες ροές να απορριφθούν, ενώ η υπόλοιπη κίνηση να επιστραφεί προς τον αρχικό της προορισμό που είναι το θύμα της επίθεσης (Σχήμα 13-v). Η μέθοδος αυτή αντικαθιστά τον κλασσικό μηχανισμό RTBH, ο οποίος απορρίπτει το σύνολο της κίνησης η οποία κατευθύνεται προς το θύμα.

Οι σχεδιαστικές αρχές της προτεινόμενης προσέγγισης βασίζονται στις εξής ιδιότητες:

- *Διαχείριση της κακόβουλης κίνησης σε επίπεδο ροών, προστατεύοντας παράλληλα την προσβασιμότητα του θύματος της επίθεσης:* Αντί της αποκοπής όλων της κίνησης προς το θύμα, ο προτεινόμενος μηχανισμός προσφέρει τη δυνατότητα αναδρομολόγησης της κίνησης αυτής προς έναν μεταγωγέα OF, ικανό να διαχειριστεί την κίνηση σε επίπεδο ροών. Από το σημείο αυτό, τα κακόβουλα πακέτα θα απορρίπτονται, ενώ η κανονική κίνηση θα επιστρέφει πίσω στον αρχικό δρομολογητή, ώστε να προωθηθεί κανονικά προς το (μέχρι πρότινος) θύμα της επίθεσης. Με τον τρόπο αυτό, διατηρείται η προσβασιμότητα του θύματος από τους καλόβουλους χρήστες, ενώ αποκόπτεται η επίθεση DDoS.

- *Πλήρης διαχωρισμός των βασικών λειτουργιών του συστήματος:* Βασικό χαρακτηριστικό της προτεινόμενης αρχιτεκτονικής είναι ο αρθρωτός σχεδιασμός. Για το σκοπό αυτό, οι βασικές λειτουργίες του μηχανισμού υλοποιήθηκαν ως τρία λογικά ανεξάρτητα δομικά στοιχεία ακολουθώντας τα πρότυπα NFV για αυτοματοποιημένη διάθεση και ελαστικότητα στη διαχείριση των πόρων (υπολογιστικών, αποθηκευτικών και δικτυακών). Έτσι, υλοποιήθηκαν δομικά στοιχεία (modules) υπεύθυνα για: (α) την εξαγωγή στατιστικών δεδομένων για τις ροές, ανίχνευση ανωμαλιών και αναγνώρισή τους, (β) τη διάδοση στατικών κανόνων δρομολόγησης για την αναδρομολόγηση της κίνησης του θύματος, και (γ) την αναγνώριση των κακόβουλων ροών και απόρριψη των αντίστοιχων πακέτων, με ταυτόχρονη επιστροφή της υπόλοιπης κίνησης πίσω στο θύμα της επίθεσης.

- *Δυναμική ενεργοποίηση του μηχανισμού RTBH:* Προκειμένου να είναι εφικτή η αντιστοίχιση της κίνησης του θύματος μέσω του μηχανισμού RTBH, απαιτείται μία συσκευή-σκανδαλιστής (trigger device), η οποία θα διαδώσει στους συνοριακούς δρομολογητές έναν στατικό κανόνα δρομολόγησης (static route) αμέσως μόλις ανιχνευθεί η επίθεση και αναγνωριστεί το θύμα της μέσω του στοιχείου ADI δύο επιπέδων. Το τελευταίο ενεργοποιεί αυτόματα τον μηχανισμό RTBH ώστε να αποσταλούν οι απαραίτητοι στατικοί κανόνες δρομολόγησης στις συσκευές που συμμετέχουν στην κατάλληλη BGP κοινότητα, μέσω του πρωτοκόλλου iBGP [10]. Κύριο χαρακτηριστικό του προτεινόμενου μηχανισμού είναι η απομακρυσμένη και δυναμική παραμετροποίηση και ενεργοποίηση της συγκεκριμένης συσκευής, ώστε να διαδώσει το στατικό κανόνα.

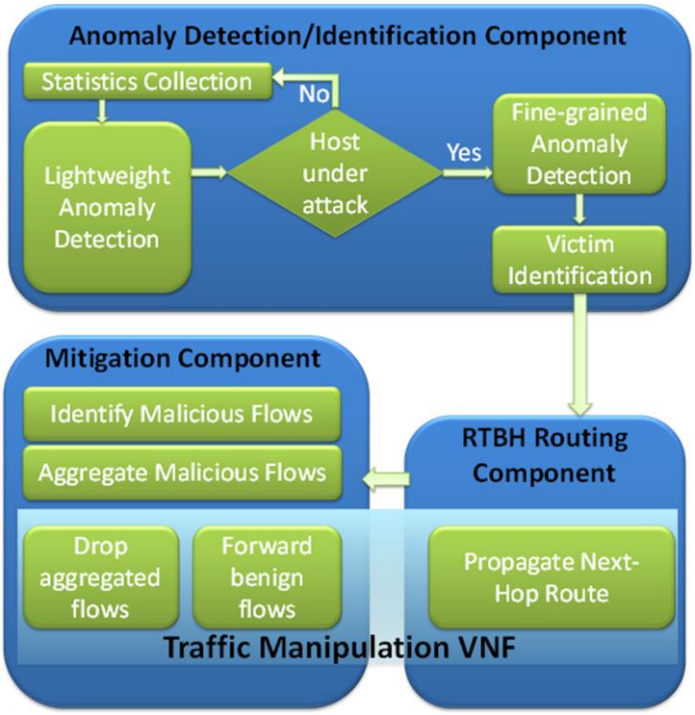
- *Κλιμακώσιμη προσέγγιση για την αποκοπή κακόβουλων ροών σε μεταγωγείς OpenFlow:* Οι πίνακες ροών των φυσικών μεταγωγέων OF στηρίζονται στις δυνατότητες μνημών τύπου Ternary Content Addressable Memory (TCAM). Οι μνήμες αυτές, αν και προσφέρουν αυξημένη ταχύτητα προσπέλασης, υποστηρίζουν έναν αρκετά περιορισμένο αριθμό εγγραφών. Η προσέγγιση που παρουσιάζεται, επιτρέπει την βελτιστοποίηση στην χρήση ακριβών πόρων όπως οι TCAMs, ομαδοποιώντας τις κακόβουλες πηγές με βάση τα Μέγιστα Κοινά Προθέματα (Longest Common Prefixes - LCP) των διευθύνσεων IP. Ταυτόχρονα, συνυπολογίζονται και τα ακόλουθα: (α) η χωρητικότητα των μεταγωγέων OF (όσον αφορά τις εγγραφές στον πίνακα ροών), (β) ο βαθμός συμμετοχής κάθε κακόβουλης πηγής στην δεδομένη επίθεση τύπου DDoS, και (γ) οι παράπλευρες απώλειες που μπορεί να συνεπάγεται η αποκοπή ενός συγκεκριμένου προθέματος (prefix), όπου ως παράπλευρη απώλεια χαρακτηρίζεται η αποκοπή μία καλόβουλης πηγής.

- *Αντιμετώπιση περιορισμών συσκευών σε παραδοσιακά δικτυακά περιβάλλοντα:*
  Η αντιμετώπιση επιθέσεων τύπου DDoS δυσχεραίνεται συνήθως λόγω του μεγάλου όγκου κακόβουλης κίνησης η οποία εξαπολύεται στην δικτυακή υποδομή η οποία φιλοξενεί το θύμα μίας επίθεσης, αλλά και των χιλιάδων κακόβουλων πηγών οι οποίες συμμετέχουν στην επίθεση αυτή. Προκειμένου να αντιμετωπιστούν αποτελεσματικά και με τρόπο κλιμακώσιμο τέτοιες επιθέσεις, προτείνεται η χρήση κανόνων τύπου exact match, όπου αυτό είναι δυνατό. Οι κανόνες αυτοί δεν περιέχουν πεδία αναπλήρωσης

(wildcard fields), τους οποίους και μπορούν να διαχειριστούν οι μεταγωγείς σε πολύ μεγαλύτερο αριθμό [82].

6.2.2 Αρχιτεκτονικά στοιχεία

Όπως προαναφέρθηκε, η γενική αρχιτεκτονική του προτεινόμενου μηχανισμού ανίχνευσης και αντιμετώπισης δικτυακών ανωμαλιών αποτελείται από τρία πλήρως διαχωρισμένα δομικά στοιχεία, (i) την μονάδα Ανίχνευσης και Αναγνώρισης Ανωμαλιών (Anomaly Detection and Identification – ADI), (ii) την μονάδα RTBH, και (iii) την μονάδα Αντιμετώπισης Ανωμαλιών (Anomaly Mitigation), όπως απεικονίζονται και στο Σχήμα 14. Το σχήμα αυτό μετατρέπει το δίκτυο σε ένα προγραμματιζόμενο περιβάλλον μέσω ενός μεταγωγέα OF ο οποίος χρησιμοποιείται ως μία ενδιάμεση συσκευή σε παραδοσιακά επιχειρησιακά δίκτυα, και ο οποίος αποτελεί αναπόσπαστο τμήμα της αρχιτεκτονικής. Παράλληλα, εισάγονται μέθοδοι οι οποίες επιτυγχάνουν στην ανίχνευση και την αντιμετώπιση δικτυακών επιθέσεων με αποτελεσματικό και κλιμακώσιμο τρόπο. Ακόμη, τμήματα των μονάδων Αντιμετώπισης Ανωμαλιών και RTBH ομαδοποιούνται και λειτουργούν συνεργατικά ως μια Εικονικοποιημένη Δικτυακή Λειτουργία (VNF), ακολουθώντας βασικές αρχές των αρχιτεκτονικών NFV [83], όπως η προγραμματιζόμενη, αυτοματοποιημένη παροχή και παραμετροποίηση δικτυακών υπηρεσιών.



Σχήμα 14: Γενική επισκόπηση των κύριων στοιχείων που αποτελούν την προτεινόμενη αρχιτεκτονική προσέγγιση.

6.2.2.1 Μονάδα ανίχνευσης και αναγνώρισης ανωμαλιών

Σκοπός της συγκεκριμένη μονάδας είναι η παρακολούθηση και η ανίχνευση ύποπτων μεταβολών σε μετρικές που αφορούν τη δικτυακή κίνηση. Όπως φαίνεται και στο Σχήμα 14, η συγκεκριμένη μονάδα ADI, αποτελείται από τρεις λογικά διαχωρισμένες διαδικασίες.

Η πρώτη διαδικασία αφορά τη συλλογή στατιστικών δεδομένων για τις ροές πακέτων από τον συνοριακό δρομολογητή. Τα δεδομένα αυτά είναι απαραίτητα για τη διαδικασία ανίχνευσης ανωμαλιών. Η διαδικασία αυτή συλλέγει συνεχώς δείγματα μέσω του πρωτοκόλλου sFlow [84], και περιοδικά τα αποστέλλει στην επόμενη κατά σειρά διαδικασία για περαιτέρω επεξεργασία και ανίχνευση ανωμαλιών. Λόγω της λογικής πλήρους διαχωρισμού που εφαρμόστηκε κατά τη σχεδίαση του συνολικού μηχανισμού, η διαδικασία συλλογής είναι ανεξάρτητη από τον αλγόριθμο ανίχνευσης ανωμαλιών που χρησιμοποιείται. Κατά συνέπεια, θα μπορούσαν εναλλακτικά να χρησιμοποιηθούν και άλλες μέθοδοι ή πρωτόκολλα για τη συλλογή στατιστικών, όπως το NetFlow [34], αναλόγως με τις δυνατότητες του εκάστοτε δρομολογητή.

Η δεύτερη κατά σειρά διαδικασία της μονάδας ADI αφορά στην ανίχνευση ανωμαλιών, και υλοποιήθηκε ως δύο διακριτά λογικά επίπεδα για λόγους απόδοσης συστήματος και ακρίβειας στην αναγνώριση ανωμαλιών. Αρχικά χρησιμοποιείται ένας αλγόριθμος ανίχνευσης ανωμαλιών μικρής πολυπλοκότητας ο οποίος επεξεργάζεται τα πρωτογενή στατιστικά δεδομένα που συλλέγονται, αναζητώντας ασυνήθιστες ποιοτικές μεταβολές της δικτυακής κίνησης. Ο αλγόριθμος αυτός αποτελεί και το πρώτο λογικό επίπεδο της διαδικασίας ανίχνευσης ανωμαλιών. Στην περίπτωση κατά την οποία ανιχνευθεί ύποπτη συμπεριφορά ενός υποσυνόλου των ροών δεδομένων (στις οποίες αναλύεται το σύνολο της δικτυακής κίνησης) αναλαμβάνει το δεύτερο λογικό επίπεδο της μονάδας ανίχνευσης να επιτελέσει λεπτομερή επισκόπηση των στατιστικών δεδομένων, με σκοπό την ανίχνευση-επιβεβαίωση πιθανών επιθέσεων DDoS στο δίκτυο.

Ακολούθως, εφόσον ανιχνευθεί μία DDoS επίθεση, ενεργοποιείται η τρίτη κατά σειρά διαδικασία της μονάδας ADI, η οποία επιδιώκει την αναγνώριση του θύματος της επίθεσης. Κατόπιν, μεταφέρει στην μονάδα RTBH τις απαραίτητες πληροφορίες (δηλ. την διεύθυνση IP του θύματος), με απώτερο σκοπό την αντιμετώπιση της ανιχνευθείσας επίθεσης.

Λόγω του αρθρωτού σχεδιασμού της μονάδας ADI, ο διαχειριστής της δικτυακής υποδομής είναι ελεύθερος να επιλέξει τον κατάλληλο αλγόριθμο ανίχνευσης ανωμαλιών για κάθε επίπεδο. Η απόφαση αυτή λαμβάνεται με βάσει τα ποιοτικά χαρακτηριστικά της δικτυακής κίνηση (δηλ. τον τύπο κίνησης που εξυπηρετεί συνήθως ένα δεδομένο δίκτυο),

καθώς και τους υπολογιστικούς πόρους οι οποίοι είναι διαθέσιμοι για τη διαδικασία ανίχνευσης. Η αλγόριθμοι οι οποία υιοθετήθηκαν στην συγκεκριμένη προσέγγιση παρουσιάζονται αναλυτικά σε επόμενη παράγραφο.

6.2.2.2 Μονάδα RTBH

Σε περιπτώσεις χρήσης της τυπικής RTBH μεθόδου, τα πακέτα προς τη διεύθυνση IP του θύματος επαναδρομολογούνται προς μια μη υπαρκτή διεπαφή (null interface). Έτσι, οι δυνατότητες της μεθόδου RTBH περιορίζονται μόνο στην απόρριψη της κίνησης η οποία θα αντιστοιχηθεί με τον στατικό κανόνα δρομολόγησης. Εφαρμόζοντας λοιπόν την συγκεκριμένη μέθοδο για την κίνησης ενός θύματος το οποίο δέχεται επίθεση DDoS, το θύμα μπορεί να αποκοπεί από ολόκληρο το Internet. Αντιθέτως, η προτεινόμενη Εικονικοποιημένη Δικτυακή Λειτουργία επιτρέπει την αναδρομολόγηση της κίνησης του θύματος προς έναν μεταγωγέα OF, μέσω του οποίου μπορεί να γίνει επισκόπηση των πακέτων σε επίπεδο ροής, πετυχαίνοντας αποδοτική στοχοποίηση της κακόβουλης κίνησης. Για το σκοπό αυτό, η μονάδα ADI είναι ικανή να παραμετροποιήσει τη δεύτερη κύρια μονάδα της αρχιτεκτονικής, τη μονάδα RTBH, η οποία αποτελεί ταυτόχρονα και τον σκανδαλιστή του μηχανισμού RTBH. Μέσω του RTBH διαδίδεται ο απαραίτητος στατικός κανόνας αναδρομολόγησης στους συνοριακούς δρομολογητές, αξιοποιώντας τις δυνατότητες που προσφέρει το πρωτόκολλο iBGP (όπως αναλύεται παρακάτω). Σκοπός είναι η αναδρομολόγηση της κίνησης του θύματος προς έναν μεταγωγέα OF. Η διαδικασία αυτή επιτρέπει την δυναμική και ελεγχόμενη μέσω λογισμικού χειραγώγηση της κίνησης του θύματος, προσδίδοντας χαρακτηριστικά αρχιτεκτονικών NFV σε δικτυακά περιβάλλοντα τα οποία στηρίζονται κατά κύριο λόγω σε παραδοσιακές δικτυακές συσκευές. Εν συνεχεία, αναλαμβάνει η μονάδα Αντιμετώπισης Ανωμαλιών να αναγνωρίσει, να διαχωρίσει και τελικά να περιορίσει την κακόβουλη κίνηση.

6.2.2.3 Μονάδα Αντιμετώπισης Ανωμαλιών

Το τρίτο κύριο δομικό στοιχείο της προτεινόμενης αρχιτεκτονικής, η Μονάδα Αντιμετώπισης Ανωμαλιών (Anomaly Mitigation Component - AMC) περιλαμβάνει τρεις ανεξάρτητες διαδικασίες. Η πρώτη διαδικασία αφορά στην αναγνώριση των κακόβουλων ροών, βάσει δικτυακών στατιστικών τα οποία παράγονται και εξάγονται μέσω του

μεταγωγέα OF. Η κακόβουλη κίνηση διαχωρίζεται από την κανονική κίνηση βάσει της ασυμμετρίας του λόγου αποστολής και λήψης πακέτων ανά ροή. Το ποιοτικό αυτό χαρακτηριστικό της κίνησης εξάγεται μέσω δειγματοληψίας πακέτων η οποία επιτελείται πλέον από τον μεταγωγέα OpenFlow. Η δεύτερη διαδικασία επιδιώκει την ενοποίηση κακόβουλων ροών βάσει των διευθύνσεων IP των πηγών τέτοιων ροών. Η τρίτη διαδικασία της μονάδας Αντιμετώπισης Ανωμαλιών είναι υπεύθυνη για την εγκαθίδρυση κατάλληλων εγγραφών στον πίνακα ροών του μεταγωγέα OF, ούτως ώστε τα κανονικά/μη-κακόβουλα πακέτα να επιστρέφουν μέσω της θύρας εισόδου του μεταγωγέα OF και να επανακατευθύνονται προς το θύμα της επίθεσης, όπου ήταν και ο αρχικός τους προορισμός. Όπως γίνεται εμφανές και στο Σχήμα 14, η λειτουργικότητα αυτή της επιλεκτικής απόρριψης ροών σε συνεργασία με την αναδρομολόγηση ροών μέσω της μονάδα RTBH, οριοθετεί μία Εικονικοποιημένη Δικτυακή Λειτουργία (VNF) υπεύθυνη για την «κατά παραγγελία» χειραγώγηση δικτυακών ροών δεδομένων με σκοπό τον περιορισμό της κακόβουλης κίνησης.

Βασικό στοιχείο της μονάδας AMC είναι η συνάθροιση κακόβουλων ροών σε πιο γενικευμένες ροές, με σκοπό την εξοικονόμηση εγγραφών στον πίνακα ροών του μεταγωγέα OF, και κατά συνέπεια την βελτίωση της κλιμακωσιμότητας της περιγραφόμενης προσέγγισης. Η συνάθροιση υλοποιείται μέσω του μηχανισμού Longest Common Prefix (LCP) που περιγράφεται στην ενότητα 6.3.4. Η αποτελεσματικότητα του μηχανισμού αυτού εξαρτάται από παράγοντες όπως (α) φυσικοί περιορισμοί του μεταγωγέα OF (π.χ. αριθμός διαθέσιμων εγγραφών στον πίνακα ροών του μεταγωγέα OF), (β) πολιτικές οι οποίες έχουν πιθανώς καθοριστεί από τους διαχειριστές (π.χ. αν ο διαχειριστής επιθυμεί την αποκοπή του συνόλου τον ανιχνευμένων κακόβουλων ροών, ή μόνο εκείνων των οποίων ο όγκος κίνησης ξεπερνά κάποιο κατώφλι).

6.3 Αναλυτική Περιγραφή Κύριων Δομικών Στοιχείων

6.3.1 Αλγόριθμοι ανίχνευσης και αναγνώρισης ανωμαλιών

Στην ενότητα αυτή παρουσιάζονται και αναλύονται λεπτομερώς οι αλγόριθμοι που υιοθετήθηκαν για την υλοποίηση της μονάδας ADI. Η συγκεκριμένη μονάδα βασίζεται σε δύο αλγορίθμους για τα αντίστοιχα επίπεδα ανίχνευσης ανωμαλιών, και σε έναν αλγόριθμο για την αναγνώριση του θύματος. Η ADI παραμετροποιεί δυναμικά την RTBH μονάδα ακολούθως της ανίχνευσης μία επίθεσης DDoS, ενώ ενημερώνει για την ανάκληση του

στατικού κανόνα αναδρομολόγησης μόλις αντιληφθεί την παύση της κακόβουλης κίνησης κατά του αρχικού θύματος.

6.3.1.1 Πρώτο επίπεδο ανίχνευσης ανωμαλιών μέσω εντροπίας

Στο πρώτο επίπεδο ανίχνευσης δικτυακών ανωμαλιών υιοθετήθηκε η μέθοδος παρακολούθησης της μεταβολής της εντροπίας συγκεκριμένων ποιοτικών χαρακτηριστικών των δικτυακών ροών δεδομένων, όπως έχει ήδη περιγραφεί στην Ενότητα 5.3.2. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για την αναγνώριση αλλαγών στα χαρακτηριστικά της δικτυακής κίνησης, χωρίς να εξαρτάται από την εκάστοτε δικτυακή τοπολογία ή συγκεκριμένα χαρακτηριστικά της κίνησης [61].

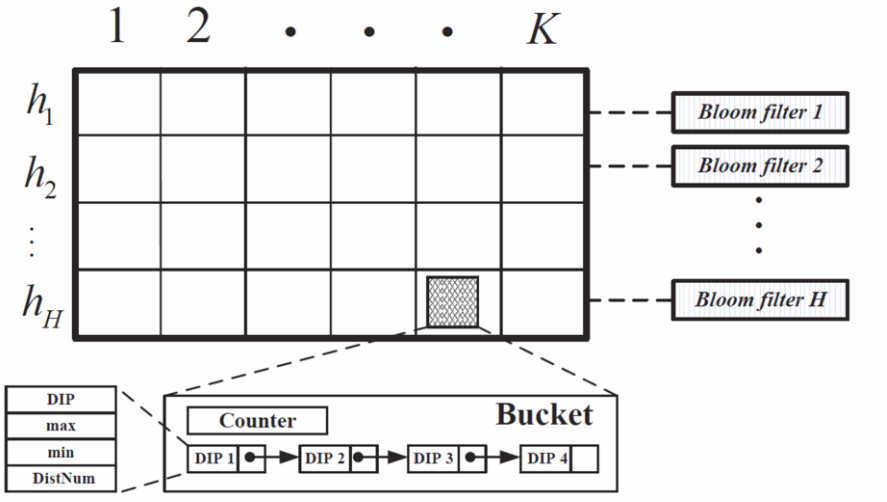
Για τους σκοπούς της συγκεκριμένης εφαρμογής (δηλ. της ανίχνευσης επιθέσεων τύπου DDoS), κρίθηκε χρήσιμη η παρακολούθηση της μεταβολής της εντροπίας συγκεκριμένων μεταβλητών όπως η διευθύνσεις IP προορισμού καθώς και οι TCP πόρτες προορισμού. Όπως έχει ήδη αναλυθεί, σε περίπτωση επίθεσης DDoS αναμένεται να υπάρξει σημαντική πτώση στην εντροπία κυρίως των διευθύνσεων IP προορισμού, αλλά και των θυρών TCP.

Μέσω της παρατήρησης τέτοιων μεταβολών, η μονάδα ADI αντιλαμβάνεται την παρουσία δικτυακών ανωμαλιών συγκρίνοντας την τιμή της εντροπίας των ανωτέρω μεταβλητών με αντίστοιχες τιμές κατωφλίου που έχουν καθοριστεί, και οι οποίες έχουν αποφασιστεί με ευρετικές μεθόδους. Κατόπιν, αναλαμβάνει το δεύτερο επίπεδο ανίχνευσης ανωμαλιών να επιβεβαιώσει την ύπαρξη επίθεσης μέσω λεπτομερούς ανάλυσης των ροών. Μια τέτοιου τύπου ανάλυση συνεπάγεται και σημαντικό κόστος όσον αφορά τους υπολογιστικούς πόρους της εκάστοτε υποδομής, ιδιαίτερα αν αυτή η διαδικασία επιτελείται συνεχόμενα. Για το σκοπό αυτό υλοποιήθηκε και το πρώτο επίπεδο ανίχνευσης μέσω της μεταβολής της εντροπίας, αφού έχει αποδειχθεί ότι η μέθοδος αυτή είναι ικανή να ανιχνεύσει δικτυακές ανωμαλίες σε περιβάλλοντα που χαρακτηρίζονται από υψηλές ταχύτητες μεταγωγής πακέτων, παράγοντας σχετικά περιορισμένο ποσοστό ψευδών αναφορών (false-positives) χωρίς να εξαντλεί τους διαθέσιμους υπολογιστικούς πόρους (Ενότητα 5.4.3).

6.3.1.2 Λεπτομερής ανάλυση των δικτυακών ροών ως δεύτερο επίπεδο ανίχνευσης ανωμαλιών και αναγνώρισης του θύματος

Το δεύτερο επίπεδο της μονάδας ADI βασίζεται στον αλγόριθμο μετρήσεων δομών τύπου sketch προς τις δύο κατευθύνσεις (Bidirectional Count Sketch – BCS), ο οποίος παρουσιάζεται και αναλύεται διεξοδικά στην εργασία [85]. Μέσω του συγκεκριμένου αλγορίθμου είναι δυνατή η λεπτομερής ανάλυση της δικτυακής κίνησης, με σκοπό τον εντοπισμό επιθέσεων DDoS.

Οι δομές τύπου sketch τις οποίες χρησιμοποιεί ο συγκεκριμένος αλγόριθμος, είναι δομές δεδομένων οι οποίες χρησιμοποιούνται για να αποθηκεύσουν την περίληψη ενός μεγάλου συνόλου δεδομένων [86]. Όπως φαίνεται και στο Σχήμα 15, ως *K*-ary Sketch χαρακτηρίζεται μία δομή δεδομένων (πίνακας) η οποία αποτελείται από *H* πίνακες (γραμμές της δομής Sketch) κατακερματισμού (hash tables) μεγέθους *K*. Για κάθε γραμμή επιλέγεται τυχαία μία συνάρτηση κατακερματισμού από ένα δεδομένο σύνολο συναρτήσεων. Ακόμη, κάθε πεδίο περιέχει ένα κλειδί k_i και μία τιμή u_i συσχετισμένη με το κλειδί αυτό. Για κάθε νέα εγγραφή $s_i = (k_i, u_i)$, η τιμή u_i προστίθεται σε εκείνα τα buckets στα οποία αντιστοιχεί το κλειδί k_i (κατακόρυφη στήλη στο Σχήμα 15). Μία συνάρτηση αναζήτησης είναι ικανή να επιστρέψει την ελάχιστη τιμή η οποία αντιστοιχεί σε δεδομένο κλειδί k_i. Έτσι, μέσω της αναζήτησης αυτής, αποκαλύπτονται τα κλειδιά εκείνα τα οποία εμφανίζονται με μεγαλύτερη συχνότητα στην δομή sketch, διασταυρώνοντας τα κλειδιά με τα buckets εκείνα που διατηρούν αποθηκευμένες τις υψηλότερες τιμές. Η διαδικασία αυτή είναι πολύ σημαντική καθώς μπορεί να εφαρμοστεί όχι μόνο για να αποκαλύπτει μια επίθεση, αλλά ταυτόχρονα και να καταδεικνύει το θύμα της επίθεσης αυτής.

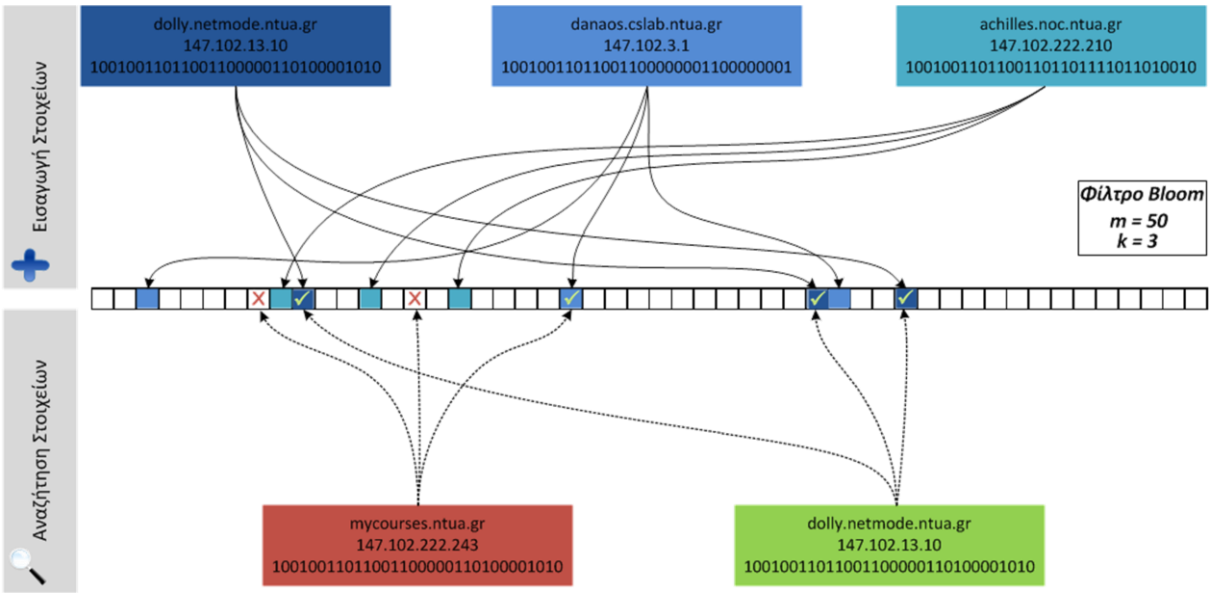


Σχήμα 15: Γραφική απεικόνιση της BCS δομής δεδομένων, βασισμένη στις δομές τύπου *K*-ary Sketch.

Η δικτυακή κίνηση του θύματος μιας επίθεσης τύπου DDoS συνήθως χαρακτηρίζεται από υψηλά ποσοστά ασυμμετρίας όσον αφορά τα πακέτα που λήφθηκαν προς εκείνα τα οποία έχουν αποσταλεί από το θύμα. Αυτό συμβαίνει για δύο κυρίως λόγους: (α) ένας εξυπηρετητής μπορεί να απαντήσει σε έναν πεπερασμένο αριθμό αιτημάτων-συνδέσεων οι οποίες γίνονται προς αυτόν, και (β) συχνά οι διευθύνσεις IP πηγής είναι πλαστογραφημένες και ως εκ τούτου ο εξυπηρετητής θα αναγκαστεί να ματαιώσει την επικοινωνία με τέτοιες διευθύνσεις. Με βάση αυτή τη λογική, υλοποιήθηκε η δομή BCS στα πλαίσια της αρχιτεκτονικής που περιγράφεται στον κεφάλαιο αυτό.

Συγκεκριμένα, οι διευθύνσεις IP προορισμού (Destination IP – *DIP*) χρησιμοποιούνται ως κλειδιά για την ενημέρωση της δομής BCS κατά τα πρότυπα των δομών *K*-ary Sketch, Σχήμα 15. Η διαφορά έγκειται στο γεγονός ότι αντί να αυξάνονται οι αντίστοιχοι μετρητές (τιμές u_i) κατά μία μονάδα για κάθε νέο πακέτο ή δείγμα κίνησης (τα οποία δειγματοληπτούνται από συνοριακές δικτυακές συσκευές οι οποίες υποστηρίζουν το πρωτόκολλο sFlow [84]), οι μετρητές αυξάνονται μόνο όταν μία διεύθυνση IP προορισμού εμφανίζεται σε μία νέα δικτυακή ροή (flow). Επιπλέον, χρησιμοποιούνται *H* φίλτρα Bloom [87] (Bloom Filter – BF) των *m* bits και *k* συναρτήσεων κατακερματισμού ώστε να εκτιμάται προσεγγιστικά κάθε φορά αν μία δεδομένη δικτυακή ροή (με δεδομένη διεύθυνση IP προορισμού) έχει ξαναεμφανιστεί στην δομή BCS. Ως φίλτρο Bloom ορίζεται μία δομή δεδομένων, ικανή να εκτιμήσει γρήγορα και αποδοτικά είτε αν ένα στοιχείο *«μπορεί να υπάρχει»*, ή αν *«σίγουρα δεν υπάρχει»* σε ένα δεδομένο σύνολο. Αναλόγως τον αριθμό των στοιχείων που πρόκειται να φιλοξενηθούν στο δομή αυτή, υπολογίζονται οι παράμετροι *m* και *k* ώστε να προσεγγίζεται η επιθυμητή πιθανότητα σφάλματος (false positive).

Ένα ενδεικτικό παράδειγμα χρήσης των φίλτρων Bloom φαίνεται στο Σχήμα 16. Για λόγους απλότητας ορίστηκαν *m=50* και *k=3*, ενώ για τους σκοπούς της συγκεκριμένης μελέτης, ορίστηκαν *m=95.841* και *k=7* ώστε υποστηρίζονται πάνω από 10.000 διαφορετικές διευθύνσεις IP, με την πιθανότητα σφάλματος να κυμαίνεται στο 1%. Στο παράδειγμα φαίνεται η εισαγωγή συγκεκριμένων διευθύνσεων IP (σε δυαδική μορφή) οι οποίες αντιστοιχούν σε εξυπηρετητές του Ε.Μ.Π. Κατά την εισαγωγή κάθε στοιχείου, συμπληρώνονται τα αντίστοιχα τρία πεδία του πίνακα, ένα για κάθε συνάρτηση κατακερματισμού. Μέσω των ίδιων συναρτήσεων πραγματοποιείται και η αναζήτηση, και λαμβάνεται θετική απάντηση μόνο εφόσον και τα τρία πεδία που θα προκύψουν βρεθούν συμπληρωμένα. Έτσι, μία αναζήτηση για την IP *147.102.13.10* θα επιστρέψει θετική απάντηση (*«μπορεί να υπάρχει»*) ενώ για την *147.102.222.243* αρνητική απάντηση (*«σίγουρα δεν υπάρχει»*).



Σχήμα 16: Ενδεικτικό παράδειγμα χρήσης Φίλτρου Bloom με *m=50* και *k=3*.

Μέσω των BFs, μόλις βρεθεί μία ροή η οποία να ικανοποιεί την αντίθετη κατεύθυνση μίας υπάρχουσας ροής, τότε ο αντίστοιχος μετρητής της τελευταίας στη δομή BCS μειώνεται κατά μία μονάδα. Έτσι, τα πεδία με υψηλές τιμές καταδεικνύουν τόσο την ανώμαλη δικτυακή συμπεριφορά, αλλά και τη διεύθυνση IP του θύματος της επίθεσης (ως το αντίστοιχο κλειδί της δομής BCS).

Για κάθε bucket, όπως έχει οριστεί και φαίνεται και στο Σχήμα 15, εάν ισχύει η τιμή του μετρητή $BCS[h][k].counter$ επαληθεύει την ακόλουθη συνθήκη, τότε επιβεβαιώνεται η ύπαρξη δικτυακής ανωμαλίας:

$$BCS[h][k].counter - \overline{C[h]} \geq b \cdot D[h] \qquad (6.1),$$

όπου β είναι μία παράμετρος ευρετικής προσαρμογής, $C[h]$ είναι η μέση τιμή των μετρητών και $D[h]$ η αντίστοιχη απόκλιση.

Για την αναγνώριση του θύματος μίας επίθεσης DDoS απαιτείται η συσχέτιση μίας διεύθυνσης IP προορισμού με έναν πλήθος διευθύνσεων IP πηγής (Source IP – SIP). Μια τέτοια πρακτική, όμως, είναι πολύ πιθανό να εξαντλήσει μεγάλο τμήμα των διαθέσιμων υπολογιστικών πόρων (κυρίως μνήμη RAM). Έτσι, υιοθετήθηκε η μέθοδος αναγνώρισης κατά προσέγγιση, όπως αναλύεται στην εργασία [85]. Συγκεκριμένα, για κάθε διεύθυνση *DIP* η οποία διατηρείται στη δομή BCS, επιλέγεται μία συνάρτηση κατακερματισμού h μέσω της οποίας αντιστοιχίζεται κάθε *SIP* σε μία τιμή στο διάστημα [0,1]. Εν συνεχεία, η

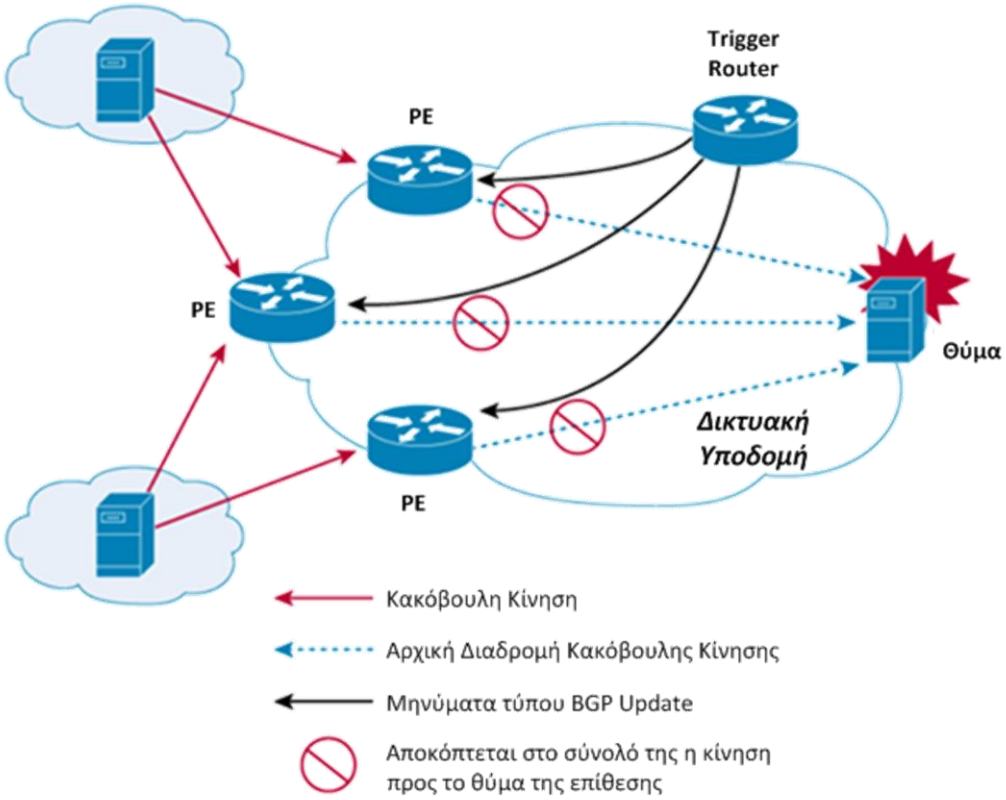
$h(\cdot)$ εφαρμόζεται σε όλες τις διευθύνσεις *SIP* οι οποίες σχετίζονται με τη δεδομένη *DIP*, διατηρώντας τη μέγιστη τιμή *max* και την ελάχιστη *min*. Μέσω των τιμών αυτών, υπολογίζεται προσεγγιστικά ο αριθμός *DistNum* των ξεχωριστών διευθύνσεων *SIP* ως $\frac{1}{2} \cdot (\frac{1}{min} + \frac{1}{1-max})$. Το θύμα της επίθεσης αναγνωρίζεται ως η διεύθυνση *DIP* η οποία ικανοποιεί τη συνθήκη $DistNum \geq TH_{DistNum}$ όπου το κατώφλι $TH_{DistNum}$ ορίζεται από το διαχειριστή του δικτύου. Ενδεικτικά στο [88] αναφέρονται τιμές για το *DistNum* οι οποίες συνήθως είναι κοντά στο 0 ενώ σε περιπτώσεις επίθεσης ξεπερνούν την τιμή 1.000.

6.3.2 Μέθοδος RTBH για την αναδρομολόγηση ύποπτης δικτυακής κίνησης

Στόχος της μεθόδου RTBH είναι η αποκοπή της κακόβουλης κίνησης στο άκρο της δικτυακής περιοχής η οποία φιλοξενεί το θύμα, μέχρις ότου πάψει να υφίσταται η αντίστοιχη επίθεση. Έτσι, εφαρμόζονται φίλτρα με βάση την διεύθυνση IP προορισμού, επιτρέποντας την διάδοση σε όλο το δίκτυο, μιας διαδρομής η οποία οδηγεί σε ένα black-hole interface (null interface) [81]. Τα φίλτρα αυτά αντιστοιχίζονται με πακέτα σε επίπεδο διεύθυνσης IP, και συνεπώς, σε περίπτωση επίθεσης DDoS, όλη η κίνηση η οποία προορίζεται για το θύμα, θα αναδρομολογηθεί από τους συνοριακούς δρομολογητές προς το null interface ώστε να απορριφθούν τα αντίστοιχα πακέτα. Μέσω της μεθόδου RTBH, αποφεύγεται η άσκοπη χρήση εσωτερικών δικτυακών πόρων για την εξυπηρέτηση της κακόβουλης κίνησης, αφού η κίνηση αυτή αποκόπτεται από τους συνοριακούς δρομολογητές, όπως φαίνεται και στο Σχήμα 17.

Κύριο δομικό στοιχείο της μεθόδου RTBH, αποτελεί ένας δρομολογητής ο οποίος αναλαμβάνει το ρόλο του μηχανισμού-σκανδαλιστή, μέσω του οποίου διαδίδεται η διαδρομή που οδηγεί στο προαναφερθέν null interface. Ο δρομολογητής αυτός πρέπει να έχει ομότιμη (peer) σχέση με τους υπόλοιπους συνοριακούς δρομολογητές του δικτύου, μέσω του πρωτοκόλλου iBGP [10]. Η απαιτούμενη προετοιμασία του συγκεκριμένου δρομολογητή, περιλαμβάνει: (i) την εγκαθίδρυση και παραμετροποίηση του null interface, μέσω του οποίου θα απορρίπτονται όλα τα πακέτα τα οποία θα προορίζονται προς μία προκαθορισμένη, μη-χρησιμοποιούμενη διεύθυνση IP, και (ii) έναν αντίστοιχο στατικό κανόνα εγκαθιδρυμένο στον δρομολογητή αυτό. Ο δρομολογητής με τη σειρά του, διανέμει τον κανόνα αυτόν στους iBGP peers, μέσω ενός μηνύματος τύπου *BGP UPDATE*. Με τον τρόπο αυτό, ορίζεται το επόμενο βήμα (next hop) ως το null interface για όλα τα πακέτα τα οποία κατευθύνονται προς το θύμα μιας επίθεσης DDoS. Συνεπώς, όλα τα πακέτα τα οποία προορίζονται για το θύμα, είτε είναι κακόβουλα είτε όχι, θα οδηγηθούν προς το null

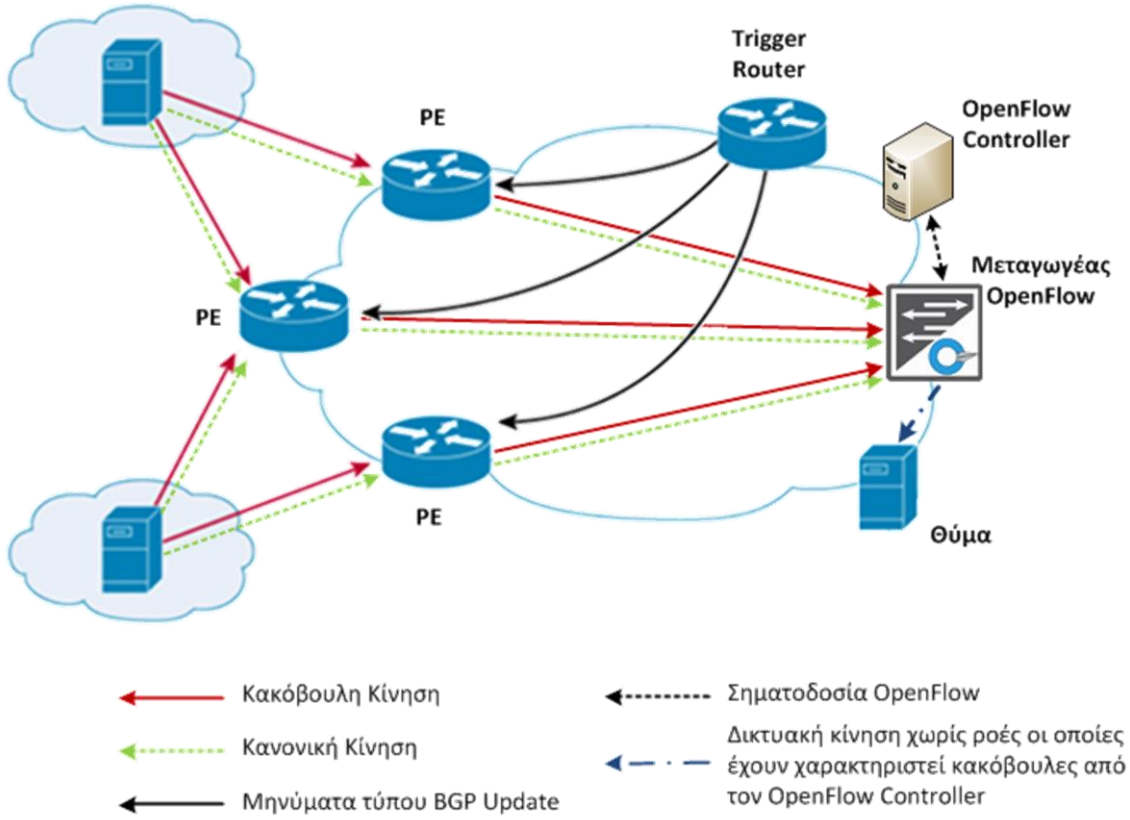
interface που έχει διαφημιστεί από τον δρομολογητή-σκανδαλιστή, και ακολούθως θα απορριφθούν.



Σχήμα 17: Παραδοσιακή μέθοδος Remotely Triggered Black Hole (RTBH)
Πηγή: Cisco Systems, « Remotely Triggered Black Hole Filtering - Destination Based and Source Based» [116]

Η λύση που προσφέρεται μέσω του RTBH έχει αποδειχθεί ότι περιορίζει τα καταστροφικά αποτελέσματα που μπορεί να έχει μία επίθεση DDoS, και τα οποία μπορεί να επηρεάσουν ολόκληρο το δίκτυο το οποίο φιλοξενεί το θύμα της επίθεσης. Όμως η μέθοδος αυτή καθιστά το θύμα απροσπέλαστο από ολόκληρο το Internet, επιτυγχάνοντας έτσι τον αρχικό σκοπό της επίθεσης DDoS. Η μέθοδος που προτείνεται σε αυτήν την ενότητα, επαναδρομολογεί την κίνηση προς τη διεύθυνση IP του θύματος προς έναν μεταγωγέα OF. Μέσω των δυνατοτήτων που προσφέρει το πρωτόκολλο OF, για αντιστοίχιση πακέτων βάσει των τιμών των πεδίων των επικεφαλίδων που ανήκουν στα Επίπεδα 2 έως και 4, είναι δυνατή η αντιστοίχιση της κίνησης σε επίπεδο ροής, επιτρέποντας την αποκοπή μόνο της κακόβουλης κίνησης, μόλις αυτή διαχωριστεί από την κανονική. Η κανονική κίνηση, στη συνέχεια, μπορεί να προωθηθεί πίσω, προς τον συνοριακό δρομολογητή από όπου ήρθε, και από εκεί προς το θύμα της επίθεσης. Με τον τρόπο αυτό, διαφυλάσσεται η προσβασιμότητα του θύματος, ενώ παράλληλα αντιμετωπίζεται η επίθεση, και οι παράπλευρες συνέπειες που

μπορεί αυτή να επιφέρει στο υπόλοιπο δίκτυο. Ο OF Controller αποτελεί στοιχείο-κλειδί για το διαχωρισμό των κακόβουλων και καλόβουλων ροών, καθώς και για την αναδρομολόγηση των κανονικών πακέτων πίσω προς τον αρχικό τους προορισμό, όπως αναλύεται και στην επόμενη ενότητα. Ενδεικτικά, η προτεινόμενη διαδικασία φαίνεται στο Σχήμα 18.



Σχήμα 18: Προτεινόμενη προσέγγιση για τη βελτίωση της μεθόδου RTBH

Για την περεταίρω αυτοματοποίηση της διαδικασίας αναδρομολόγησης, η μονάδα ADI είναι σε θέση να διαχειριστεί και να παραμετροποιήσει απομακρυσμένα τον μηχανισμό ενεργοποίησης του RTBH σε υποδομές legacy, προσδίδοντάς του δυνατότητες χειραγώγησης της δικτυακής κίνησης ως μια διαδικασία VNF. Οι παράμετροι τις οποίες μεταβιβάζει η μονάδα ADI στην συσκευή RTBH αφορούν στην περιγραφή του θύματος της επίθεσης, και συνεπώς, περιγράφουν το τμήμα της δικτυακής κίνησης το οποίο πρέπει να αναδρομολογηθεί προς τον μεταγωγέα OF. Τέλος, μέσω της μονάδας ADI, θα γίνει αντιληπτή η παύση της επίθεσης, και στη συνέχεια η συσκευή RTBH θα ανακαλέσει όποια στατική εγγραφή έχει διαδώσει. Αξίζει να σημειωθεί επίσης, ότι ο μεταγωγέας OF τοποθετείται στο άκρο του δικτύου του θύματος, κοντά σε συνοριακό δρομολογητή. Με τον

τρόπο αυτό, αποφεύγονται παράπλευρες συνέπειες που θα επέφερε μία επίθεση DDoS, όπως άσκοπη κατανάλωση εύρους ζώνης και επεξεργαστικής ισχύος.

6.3.3 Αντιμετώπιση επιθέσεων DDoS

Βασικό στοιχείο της προτεινόμενης αρχιτεκτονικής είναι ο OF Controller, ο οποίος είναι υπεύθυνος για την αντιμετώπιση και τελικά το φιλτράρισμα της κακόβουλης κίνησης. Γενικά, ο Controller έχει τη δυνατότητα να εγκαθιδρύει και να παραμετροποιεί τις εγγραφές του πίνακα ροών ενός μεταγωγέα OF, επηρεάζοντας έτσι τη συνολική ροή της δικτυακής κίνησης [1]. Γίνεται επομένως εμφανές το πλεονέκτημα που προσφέρει η χρήση του OF για την αντιμετώπιση ανωμαλιών, αφού το πρωτόκολλο OF είναι γενικότερα συνδεδεμένο με τη δικτυακή λειτουργία (network function) προώθησης πακέτων. Τα δομικά στοιχεία που αποτελούν τη μονάδα Αντιμετώπισης Ανωμαλιών της συγκεκριμένης αρχιτεκτονικής (όπως αυτά φαίνονται και στο Σχήμα 14), είναι υλοποιημένα ως ανεξάρτητες εφαρμογές του OF Controller, και συνεργάζονται σειριακά, με στόχο τον περιορισμό της κακόβουλης κίνησης.

6.3.3.1 Αναγνώριση και αποκοπή κακόβουλων ροών

Για την αναγνώριση και τον διαχωρισμό των κακόβουλων ροών, χρησιμοποιούμε ως μετρική την ασυμμετρία των απεσταλμένων και ληφθέντων πακέτων για κάθε εξυπηρετητή [89], ως απόδειξη της ορθότητας και λειτουργικότητας του προτεινόμενου μηχανισμού (proof of concept). Λόγω του σχεδιασμού της μονάδας Αντιμετώπισης Ανωμαλιών, μπορεί να χρησιμοποιηθεί οποιοσδήποτε αλγόριθμος είναι ικανός να αναγνωρίσει κακόβουλες ροές μέσω δειγμάτων επικεφαλίδων πακέτων τα οποία έχουν συλλεχθεί μέσω του πρωτοκόλλου sFlow [84]. Ο αλγόριθμος που χρησιμοποιήθηκε, στηρίζεται στο γεγονός ότι συνήθως τα λειτουργικά συστήματα εξυπηρετητών δεν θα επιτρέψουν την επ' άπειρον απάντηση σε ερωτήματα τύπου *TCP SYN* τα οποία μπορεί να προέρχονται από κακόβουλες πηγές. Η αναλογία μεταξύ των ληφθέντων και των απεσταλμένων πακέτων, συνήθως δεν υπερβαίνει τα 4,5 πακέτα προς 1 αντίστοιχα [89]. Με έναν αντίστοιχο τρόπο μπορεί να γίνει η αναγνώριση κακόβουλων ροών UDP, μόνο που σε αυτές τις περιπτώσεις, δεν είναι εύκολος ο προσδιορισμός του λόγου ληφθέντων προς απεσταλμένων πακέτων, αφού ο καθορισμός του αναμενόμενου λόγου εξαρτάται από τις υπηρεσίες UDP που φιλοξενούνται από το εκάστοτε δίκτυο [90].

Η ανάλυση του λόγου ασυμμετρίας πραγματοποιείται συλλέγοντας δείγματα sFlow και κατηγοριοποιώντας τα σε ροές οι οποίες αφορούν στο θύμα. Δικτυακές ροές οι οποίες

εμφανίζουν εξαιρετικά υψηλά ποσοστά ασυμμετρίας, τα οποία ξεπερνούν ένα κατώφλι που έχει οριστεί βάσει εμπειρικών μεθόδων, θεωρούνται κακόβουλες και αποκόπτονται, ενώ όλες οι υπόλοιπες επαναπροωθούνται προς τον αρχικό τους προορισμό. Για την υλοποίηση των αποφάσεων αυτών, ο OF Controller εγκαθιδρύει νέες εγγραφές στον πίνακα ροών του μεταγωγέα OF.

Οι νέες εγγραφές, συνοδεύονται και από ένα συγκεκριμένο Action. Τα πιο συχνά χρησιμοποιούμενα Actions είναι τα *Forward*, *Drop* και *Modify-field* [28]. Συγκεκριμένα, για την κανονική (καλόβουλη) κίνηση, αντί για το *Forward* χρησιμοποιείται το *OFPP_IN_PORT* μέσω του οποίου τα πακέτα επιστρέφουν από την θύρα του μεταγωγέα από την οποία εισήλθαν. Αντίθετα, για τις κακόβουλες ροές εφαρμόζεται το *Drop*, ώστε να απορρίπτονται τα αντίστοιχα πακέτα. Επιπλέον, χρησιμοποιούνται προκαθορισμένες τιμές για το πεδίο Priority, αναλόγως με το Action το οποίο αντιστοιχεί σε μια συγκεκριμένη εγγραφή. Έτσι, αναθέτουμε χαμηλή τιμή Priority σε ροές οι οποίες αντιστοιχούν σε κανονική κίνηση, και υψηλή τιμή σε ροές οι οποίες αντιστοιχούν σε κακόβουλη κίνηση, ώστε οι τελευταίες να έχουν πάντοτε προτεραιότητα.

	L1	**L2**			**L3**			**L4**		**ACTION**	**PRIO RITY**
	In port	***ETHER***			***IP***			***Port***		***OutPort***	
		src	***dst***	***type***	***src***	***dst***	***Port***	***src***	***dst***		
B	X	*	*	*	*	*	*	*	*	0xfff8	10
M	X	*	*	0x 0800	S	D	0x06	*	*	-	100

Πίνακας 12: Παράδειγμα εγγραφών ροών οι οποίες εγκαθιδρύονται για την επαναπροώθηση της κανονικής κίνησης (Σειρά B), και την απόρριψη μιας συγκεκριμένης κακόβουλης ροής (Σειρά M).

Στον Πίνακας 12 εμφανίζονται ενδεικτικά δύο εγγραφές του πίνακα ροών, όπου η πρώτη αντιπροσωπεύει την επαναπροώθηση της κανονικής κίνησης μέσω της θύρας του μεταγωγέα OF από την οποία εισήλθε, ενώ η δεύτερη αντιπροσωπεύει την ροή που εγκαθιδρύεται για την αποκοπή μιας κακόβουλής ροής. Για την αποκοπή των κακόβουλων ροών, ο OF Controller πρέπει να ορίσει τα πεδία των πρωτοκόλλων που αντιστοιχούν στα Επίπεδα 2 και 3, μαζί με τις διευθύνσεις IP πηγής *(S)* και προορισμού *(D)*. Για τις ροές αυτές, ορίζεται ένας υψηλός αριθμός προτεραιότητας, ενώ το πεδίο *outport* παραμένει κενό, κάτι το οποίο υποδεικνύει στον μεταγωγέα OF ότι τα πακέτα τα οποία θα αντιστοιχηθούν με την συγκεκριμένη εγγραφή πρέπει να απορριφθούν. Τέλος, στα υπόλοιπα πεδία ορίζεται

η τιμή wildcard. Αντίθετα, για την επαναπροώθηση της κανονικής κίνησης από τη θύρα εισόδου *(X)*, ορίζεται μία εγγραφή με χαμηλή τιμή προτεραιότητας, στην οποία η τιμή του πεδίου *outport*, ορίζεται ως *0xFFF8*, υπονοώντας το *Action OFPP_IN_PORT*. Σύμφωνα με τις προδιαγραφές του πρωτοκόλλου OF [28], η τιμή αυτή ορίζει μία «δεσμευμένη θύρα» (reserved port), επιβάλλοντας στον μεταγωγέα OF να προωθήσει τα πακέτα μέσω της θύρας από την οποία εκείνα εισήλθαν στη συσκευή.

Αξίζει να σημειωθεί ότι σε αντίθεση με τους μεταγωγείς OF οι οποίοι υλοποιούνται μέσω λογισμικού, οι φυσικοί μεταγωγείς OF μπορούν να υποστηρίξουν έναν πεπερασμένο αριθμό ροών οι οποίες να περιέχουν χαρακτήρες wildcard. Ο αριθμός αυτός είναι σημαντικά περιορισμένος σε σχέση με τον αριθμό ροών που ορίζονται με πλήρη συμπλήρωση (exact matches). Ενδεικτικά στην περίπτωση του HP-2920 μεταγωγέα OpenFlow υποστηρίζονται 1.500 εγγραφές ανά switching module. Η προτεινόμενη προσέγγιση επιτρέπει τη χρήση κανόνων αποκοπής τύπου exact match, όπου όμως θα πρέπει να ορίζονται εκτός από συγκεκριμένες διευθύνσεις IP πηγής και προορισμού, και συγκεκριμένες θύρες του Επιπέδου 4 (TCP/UDP ports). Σαν αποτέλεσμα, μπορεί να αυξηθούν υπέρμετρα οι απαιτούμενοι κανόνες για την αντιμετώπιση μίας επίθεσης DDoS.

6.3.4 Κλιμακώσιμη αντιμετώπιση ανωμαλιών με συνάθροιση κακόβουλων ροών

Ο κακόβουλες πηγές οι οποίες συμβάλλουν σε μια δικτυακή επίθεση τύπου DDoS είναι πιθανό να δημιουργήσει χιλιάδες ροές δικτυακής κίνησης προς το θύμα. Προκειμένου να αποκοπούν με αποτελεσματικό τρόπο οι πηγές αυτές, απαιτούν ίσο αριθμό εγγραφών στον πίνακα ροών ενός μεταγωγέα OF. Έτσι προκύπτει άμεση εξάρτηση από την χωρητικότητα του πίνακα ροών, ο οποίος υλοποιείται σε ειδικό εξοπλισμό OpenFlow μέσω μνημών τύπου Ternary Content Addressable Memory (TCAM).

Η μνήμη TCAM είναι ένας ειδικός τύπος μνημών που επιτρέπει τη γρήγορη αντιστοίχιση των επικεφαλίδων κάθε ληφθέντος πακέτου, ανεξαρτήτως του αριθμού των υπαρχόντων εγγραφών. Τέτοιες μνήμες χρησιμοποιούνται σε παραδοσιακούς μεταγωγείς και δρομολογητές και επιτρέπουν την εγκαθίδρυση Λίστας Ελέγχου Πρόσβασης (Access Control List) με βάση πληροφορίες Επιπέδου 2 έως 4 των επικεφαλίδων των πακέτων. Το πρωτόκολλο OpenFlow εκμεταλλεύεται τις TCAMs για την εγκαθίδρυση των απαιτούμενων ροών μέσω του OpenFlow Controller. Όμως οι TCAMs είναι κοστοβόρες

και ενεργοβόρες μνήμες [91], και συνεπώς αποτρέπουν την εγκαθίδρυση μεγάλου αριθμού εγγραφών στους πίνακες ροών [82]. Για παράδειγμα οι μεταγωγείς OF NEC-IP8800 και HP2920 και του εργαστηρίου Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων Τηλεματικής (NETMODE) του Ε.Μ.Π. που χρησιμοποιήθηκαν για την πειραματική επαλήθευση μέρους της εργασίας, υποστηρίζουν μέχρι 1.500 εγγραφές στις μνήμες TCAM.

Στοχεύοντας στην αντιμετώπιση τέτοιων περιορισμών, η Μονάδα Αντιμετώπισης Ανωμαλιών (Anomaly Mitigation Component - AMC) που περιγράφεται στη παρούσα ενότητα αντιμετωπίζει την επιλογή κατάλληλων εγγραφών στον πίνακα ροών ως ένα πρόβλημα εύρεσης πόρων (resource allocation problem). Έτσι, υιοθετείται ο αλγόριθμος *Block-All* όπως αυτός περιγράφεται στην εργασία [92], αποσκοπώντας στην εύρεση εγγραφών για την αποκοπή των κακόβουλων ροών ώστε να επιτυγχάνεται η μέγιστη συνάθροιση κακόβουλων διευθύνσεων IP πηγής. Ο αλγόριθμος ελαχιστοποιεί τον αριθμό των παράπλευρων απωλειών, δηλαδή ροών οι προέρχονται από IP καλοήθων πηγών οι οποίες αποκόπηκαν λόγω της συνάθροισης κακόβουλων ροών σε ευρύτερα προθέματα IP. Η βελτιστοποίηση περιορίζεται από τον διαθέσιμο αριθμό προθεμάτων IP λόγω μεγέθους του πίνακα ροών ενός μεταγωγέα OF.

Η ανεύρεση των βέλτιστων εγγραφών απαιτεί αρχικά τον υπολογισμό ενός δένδρου Μέγιστων Κοινών Προθεμάτων (Longest Common Prefix – LCP tree). Το δένδρο LCP περιλαμβάνει το σύνολο των διευθύνσεων IP οι οποίες προέρχονται και από κακόβουλες και από καλόβουλες πηγές, και επικοινωνούν με το θύμα μίας επίθεσης DDoS, ενώ σε κάθε διεύθυνση IP ανατίθεται ένα βάρος το οποίο καθορίζεται με βάση το βαθμό (ποσοστό) συμμετοχής της συγκεκριμένης IP στο σύνολο της δικτυακής κίνησης προς το θύμα. Πιο συγκεκριμένα, το δένδρο LCP προσδιορίζεται ως μία δομή δεδομένων τύπου δυαδικού δένδρου. Τα φύλλα του δέντρου αντικατοπτρίζουν τις διευθύνσεις IP των κακόβουλων πηγών και οι εσωτερικοί κόμβοι αντιστοιχούν στα κοινά προθέματα *p/l* μεταξύ των δύο παιδιών κάτω από κάθε έναν από τους κόμβους αυτούς. Διατρέχοντας το δένδρο με κατεύθυνση από τα φύλλα προς τη ρίζα του, προσομοιώνεται η διαδικασία ανεύρεσης κοινών προθεμάτων των διευθύνσεων IP από το μεγαλύτερο προς το μικρότερο κοινό πρόθεμα, όπου το μικρότερο είναι πάντα γονέας (όσον αφορά την δενδρική δομή) του μεγαλύτερου.

Δεδομένου ενός δένδρου LCP, μέσω του αλγορίθμου *Block-All* ([92]) υπολογίζεται το σύνολο προθεμάτων διευθύνσεων IP τα οποία πρέπει να αποκοπούν ώστε να ικανοποιούνται οι ακόλουθες προϋποθέσεις:

(α) να αποκόπτεται το σύνολο των κακόβουλων ροών προς το θύμα της επίθεσης (όπως αυτές έχουν αναγνωριστεί από τον OF Controller),

(β) να προκαλούνται όσο το δυνατόν λιγότερες παράπλευρες απώλειες, όπου ως τέτοιες χαρακτηρίζονται καλόβουλες ροές δεδομένων οι οποίες αποκόπτονται αναγκαστικά κατά τη διαδικασία βέλτιστης συνάθροισης κακόβουλων ροών, ενώ

(γ) ο συνολικός αριθμός των προθεμάτων IP που πρέπει τελικά θα αποκοπούν, να είναι μικρότερος ή ίσος από το σύνολο των διαθέσιμων εγγραφών στον πίνακα ροών του μεταγωγέα OF.

Ο αλγόριθμος επαναλαμβάνεται σε σταθερά χρονικά διαστήματα διάρκειας T (π.χ. 30 sec), στη διάρκεια των οποίων γίνεται αναγνώριση των διευθύνσεων IP πηγής *i* οι οποίες δημιουργούν κακόβουλη κίνηση προς το θύμα, καθώς και εκείνων που δεν μετέχουν στην επίθεση. Στη συνέχεια ο αλγόριθμος Block-All συγκλίνει στον καθορισμό του συνόλου των προθεμάτων *p/l* προς αποκοπή με κριτήριο την ελαχιστοποίηση παράπλευρων απωλειών, και με περιορισμό στον αριθμό τους λόγω χωρητικότητας του πίνακα ροών του μεταγωγέα OF. Ο χρόνος σύγκλισης κυμαίνεται σε λίγα sec εξαρτάται από τον αριθμό των IP και τους διαθέσιμους πόρους συστήματος (περίπου 10 sec στα πειράματα της παρούσας εργασίας).

Η βελτιστοποίηση σε κάθε χρονικό διάστημα T αφορά στην ελαχιστοποίηση της συνολικής καλοήθους κίνησης η οποία αποκόπτεται λόγω της συνάθροισης:

$$\min \sum_{p/l} g_{p/l} \cdot x_{p/l} \qquad (6.2),$$

όπου $x_{p/l}$ είναι η δυαδική μεταβλητή που αφορά στην συμμετοχή του προθέματος *p/l* στην λίστα προθεμάτων προς αποκοπή. Το κόστος αποκοπής $g_{p/l}$ του προθέματος *p/l* υπολογίζεται ως το άθροισμα των βαρών w_i όλων των IP *i* που περιλαμβάνεται στο πρόθεμα *p/l*, και έχουν θετική τιμή αν είναι καλοήθης η διεύθυνση IP, και 0 αν είναι κακοήθης:

$$g_{p/l} = x_{p/l} \sum_{\iota \in p/l} w_i \qquad (6.3)$$

Στην παρούσα διατριβή, το βάρος w_i ορίστηκε ως ο λόγος της συνολικής καλοήθους κίνησης προς το θύμα από την πηγή *i,* ως προς τη συνολική κίνηση (καλοήθη και κακοήθη), όπως μετρήθηκε στο διάστημα T.

Ξεκινώντας από τα φύλλα και ανερχόμενοι προς τη ρίζα του δυαδικού δένδρου LCP, για κάθε επίπεδό του υπολογίζεται ο αριθμός των κανόνων οι οποίοι απαιτούνται για την αποκοπή $F_{p/l}$ προθεμάτων για κάθε κόμβο *p/l* του επιπέδου, μαζί με τις όποιες παράπλευρες απώλειες κόστους $z_{p/l}$. Σε κάθε επίπεδο, για κάθε ζευγάρι των γειτονικών κόμβων (siblings) s_l (αριστερά) και s_r (δεξιά), ο αλγόριθμος αναγνωρίζει το ελάχιστο πλήθος προθεμάτων προς αποκοπή, ακολουθώντας μια διαδικασία επαναληπτικού δυναμικού προγραμματισμού:

$$z_{p/l}(F_{p/l}) = min_{n=1,\dots,F_{p/l}-1}\{z_{s_l}(F_{p/l}-n) + z_{s_r}(n)\},\ F_{p/l} > 1 \qquad (6.4),$$

με οριακές συνθήκες για τα φύλλα και τους ενδιάμεσους κόμβους του δένδρου LCP:

$$z_{leaf}(F) = 0 \quad \forall F \geq 1, \qquad z_{p/l}(1) = g_{p/l} \quad \forall p/l \qquad (6.5),$$

όπου:

- *p/l* είναι ένα πρόθεμα IP εσωτερικού κόμβου του δένδρου,
- $z_{p/l}(.)$ οι παράπλευρες απώλειες που προκύπτουν από $F_{p/l}$ κανόνες αποκοπής (εγγραφές) που αντιστοιχούν σε έναν εσωτερικό κόμβο του δένδρου,
- $z_{leaf}(.)$ οι παράπλευρες απώλειες που προκύπτουν από έναν κανόνα για την αποκοπή ενός φύλλου του δένδρου και είναι πάντα 0 (υπενθυμίζεται ότι από τα φύλλα του δένδρου έχουν αφαιρεθεί όλες οι διευθύνσεις IP που δεν μετέχουν στην επίθεση)
- $F_{p/l}$ ο συνολικός αριθμός των απαιτούμενων εγγραφών αποκοπής για τα προθέματα κάτω από τον κόμβο *p/l*
- *n* ο αριθμός των κανόνων στο δεξί υποδένδρο
- $(F_{p/l} - n)$ ο συνολικός αριθμός των κανόνων κάθε φορά στο αριστερό υποδένδρο.

Για την ανεύρεση των βέλτιστων προθεμάτων IP για κάθε ζευγάρι γειτονικών κόμβων με κοινό γονέα του δυαδικού δένδρου, ο αλγόριθμος υπολογίζει τον ελάχιστον αριθμό προθεμάτων για το δεξί υποδένδρο και αντιστοίχως για το αριστερό, επιδιώκοντας οι κανόνες αυτοί να προκαλέσουν τις ελάχιστες δυνατές παράπλευρες απώλειες. Η διαδικασία αυτή επαναλαμβάνεται για κάθε κόμβο και επίπεδο του δένδρου LCP, έως ότου ο συνολικός αριθμός $F = \sum_{p/l} F_{p/l}$ των προθεμάτων προς αποκοπή (και συνεπώς των απαραίτητων εγγραφών ροών) ενός επιπέδου, να είναι μικρότερος από την προκαθορισμένη χωρητικότητα F_{max} του πίνακα ροών του μεταγωγέα OF, οπότε και συγκλίνει ο αλγόριθμος.

Η αξία του συγκεκριμένου αλγορίθμου έγκειται στο γεγονός ότι συνήθως οι πηγές των επιθέσεων τύπου DDoS είναι χιλιάδες μολυσμένοι υπολογιστές, μέσω των οποίων επιδιώκεται να εξαντληθούν οι πόροι του εξυπηρετητή-θύματος. Μελέτες όμως έχουν δείξει οι κακόβουλες πηγές τείνουν να βρίσκονται συγκεντρωμένες σε συγκεκριμένα δίκτυα, έχοντας συνεπώς κοινά προθέματα IP [93], [94], [95]. Η συγκεντρωτική αυτή τάση οφείλεται στο γεγονός ότι η κακόβουλη κίνηση πηγάζει συνήθως από ανεπαρκώς διαχειριζόμενα δικτυακά περιβάλλοντα, όπου οι διευθύνσεις IP των μολυσμένων (πιθανώς) εξυπηρετητών-υπολογιστών ανήκουν στο ίδιο μπλοκ του συνολικού πεδίου διευθύνσεων

IP. Με βάσει την παρατήρηση αυτή, μέσω του αλγορίθμου Block-All μπορούν να μειωθούν σημαντικά οι απαιτούμενες εγγραφές για την αποκοπή όλων των μολυσμένων υπολογιστούν που συμμετέχουν σε μία δικτυακή επίθεση. Ακόμη, η μέθοδος αυτή είναι πλήρως συμβατή και με τη χρήση εγγραφών στον πίνακα ροών τύπου exact-match, αφού είναι δυνατόν στις εγγραφές αυτές να οριστούν εύρη πηγών και προορισμών διευθύνσεων IP, αλλά και θυρών του Επιπέδου Μεταφοράς. Να σημειωθεί πως στην περίπτωση του μεταγωγέα λογισμικού Open vSwitch [75], για τη συνάθροιση των θυρών ο Ελεγκτής μπορεί σε κάθε εγγραφή να εφαρμόσει μάσκα bitwise της μορφής <*θύρα*>/<*μάσκα*>.

6.4 Αξιολόγηση και Πειραματικά Αποτελέσματα

Για την εκτίμηση της επίδοσης και της καταλληλότητας της προτεινόμενης προσέγγισης για εφαρμογή σε δίκτυα παραγωγής αναπτύχθηκε πρότυπη έκδοση λογισμικού που εγκαταστάθηκε σε περιβάλλον δοκιμών του εργαστηρίου NETMODE του Ε.Μ.Π. Βασική παράμετρος στην υλοποίηση του πρότυπου μηχανισμού ήταν η διατήρηση του αρθρωτού σχεδιασμού των επιμέρους μονάδων, προκειμένου να προσφέρεται η δυνατότητα δοκιμής διαφορετικών αλγοριθμικών προσεγγίσεων. Συγκεκριμένα, η μονάδα ADI αναπτύχθηκε ως ένα ανεξάρτητο στοιχείο το οποίο προσέφερε λειτουργικότητα ανίχνευσης δικτυακών ανωμαλιών πολλαπλών επιπέδων μέσω συλλογής και ανάλυσης δειγμάτων τύπου sFlow. Η μονάδα AMC για την αντιμετώπιση των ανωμαλιών, αναπτύχθηκε μέσω επέκτασης του POX OpenFlow Controller, ο οποίος λαμβάνει αποφάσεις με βάσει δικτυακά γεγονότα (event-based Controller), και είναι ικανός να παραμετροποιεί τους πίνακες ροών μεταγωγέων OpenFlow τύπου Open vSwitch (OVS) [75]. Ο Ελεγκτής POX προέκυψε μέσω μεταφοράς του αρχικού NOX Controller [74] σε γλώσσα προγραμματισμού Python. Τα επιμέρους στοιχεία της μονάδας AMC υλοποιήθηκαν ως ανεξάρτητες εφαρμογές του POX Controller, προσδίδοντας δυνατότητες συλλογής στατιστικών δεδομένων, αναγνώρισης κακόβουλων πηγών και συνάθροισης αυτών, καθώς και περιορισμού της κακόβουλης κίνησης.

Για την εκτίμηση της απόδοσης του μηχανισμού υπό πραγματικές, χρησιμοποιήθηκε πραγματική κίνηση καθ’ όλη τη διάρκεια των πειραμάτων. Για την προσομοίωση της κανονικής κίνησης συλλέχθηκε και χρησιμοποιήθηκε κίνηση από το δίκτυο του Ε.Μ.Π. Ο μέσος ρυθμός της κίνησης φθάνει στα 500 Mbps. Όσον αφορά την κακόβουλη κίνηση, χρησιμοποιήθηκε κίνηση την οποία παρείχε ο οργανισμός CAIDA, και συγκεκριμένα το

σύνολο δεδομένων CAIDA ‘DDoS Attack 2007’ [96]. Η διάρκεια της καταγεγραμμένης επίθεσης πλησιάζει την μία ώρα, ενώ οι κακόβουλες πηγές έχουν ανωνυμοποιηθεί μέσω του αλγορίθμου CryptoPAn προκειμένου να διατηρείται η σχέση μεταξύ πηγών οι οποίες ανήκουν στο ίδιο δικτυακό πρόθεμα (prefix-preserving) [97].

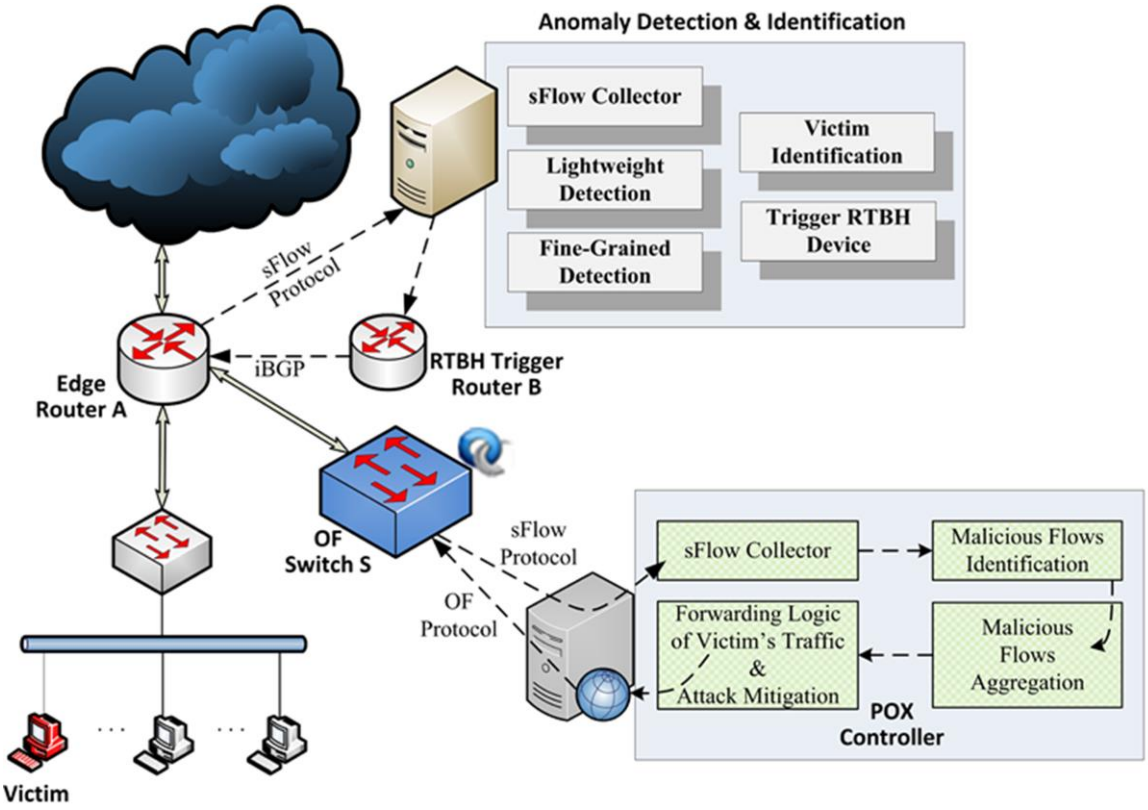
Το σύνολο δεδομένων της CAIDA, ήταν ιδανικό για την διαδικασία αξιολόγησης που ακολουθήθηκε, αφού κατά την εκκίνησή του ο ρυθμός αποστολής δεδομένων κυμαινόταν μόλις στα 200 kbps, ενώ στη συνέχει αυξανόταν έως και τα 80 Mbps. Έτσι, κατέστη δυνατή η αξιολόγηση του προτεινόμενου μηχανισμού και υπό συνθήκες υψηλού και υπό συνθήκες χαμηλού όγκου μεταφοράς δεδομένων. Τέλος, όσον αφορά τη διαδικασία συλλογής δεδομένων, χρησιμοποιήθηκε το πρωτόκολλο sFlow, με ρυθμό δειγματοληψίας 1 προς 128 πακέτα.

6.4.1 Πειραματική διάταξη

Σχήμα 19 παρουσιάζεται η συνολική αρχιτεκτονική όπου ο προτεινόμενος μηχανισμός εφαρμόζεται σε παραδοσιακά δίκτυα, τα οποία δεν υποστηρίζουν εγγενώς το πρωτόκολλο OF. Για τη διεξαγωγή των πειραμάτων, ήταν απαραίτητη η χρήση ενός μεταγωγέα OF ως ενδιάμεσου (OF Switch S στο Σχήμα 19), ο οποίος να υποστηρίζει ταυτόχρονα και το πρωτόκολλο sFlow. Για το σκοπό αυτό χρησιμοποιήθηκε το OVS, το οποίο αποτελεί την πιο διαδεδομένη λύση μεταγωγέα υλοποιημένου σε λογισμικό. Το λογισμικό του OVS εγκαταστάθηκε σε έναν εξυπηρετητή, με 8GB μνήμη RAM και δύο πυρήνες των 3GHz. Ως δρομολογητές χρησιμοποιήθηκαν αφ’ ενός ακόμη ένας εξυπηρετητής με ίδια χαρακτηριστικά, όπου εγκαταστάθηκε το λογισμικό δρομολόγησης Quagga [98] για το συνοριακό δρομολογητή A (Edge Router A), ενώ για τη συσκευή RTBH B (RTBH Trigger Router B) χρησιμοποιήθηκε το λογισμικό ExaBGP [99], το οποίο λειτουργεί ως μία διαδικασία παρασκηνίου (background daemon). Μέσω κώδικα γραμμένου σε γλώσσα Python, η μονάδα ADI παραμετροποιεί τις ανακοινώσεις τις οποίες θα κάνει το ExaBGP μέσω του πρωτοκόλλου iBGP. Σαν αποτέλεσμα, το ExaBGP ανακοινώνει ένα /32 πρόθεμα IP το οποίο αντιστοιχεί στη διεύθυνση IP του θύματος, και ανήκει στην κοινότητα BGP *RTBH* η οποία έχει προκαθοριστεί στον δρομολογητή A. Η ίδια λειτουργικότητα θα μπορούσε να επιτευχθεί μέσω ενός κανονικού δρομολογητή Επιπέδου 3 ο οποίος να υποστηρίζει το πρωτόκολλο BGP αντί του ExaBGP.

Καθ’ όλη τη διάρκεια των πειραμάτων, ο συνοριακός δρομολογητής A είναι υπεύθυνος για τη δρομολόγηση των πακέτων, ενώ παράλληλα εξάγει δείγματα sFlow, τα οποία

συλλέγονται από τη μονάδα ADI. Σε περίπτωση που ο μηχανισμός ανίχνευσης ανωμαλιών ανακαλύψει επίθεση DDoS, ενεργοποιείται η Συσκευή B η οποία διαδίδει στους ομότιμους (peer) δρομολογητές (στη συγκεκριμένη περίπτωση στον δρομολογητή A) έναν στατικό κανόνα δρομολόγησης, ώστε να επαναδρομολογείται η κίνηση του θύματος προς την διεύθυνση IP του OF Controller, και συνεπώς προς τον μεταγωγέα OF.



Σχήμα 19: Κύρια δομικά στοιχεία της προτεινόμενης αρχιτεκτονικής προσέγγισης για την προστασία εξυπηρετητών από DDoS επιθέσεις σε παραδοσιακά δίκτυα, με χρήση ενδιάμεσου μεταγωγέα OpenFlow.

Το σύνολο της δικτυακής κίνησης η οποία επαναδρομολογείται με τον ανωτέρω τρόπο, συλλαμβάνεται από τον ενδιάμεσο μεταγωγέα OF ο οποίος με τη σειρά του αποστέλλει δείγματα sFlow στον συνδεδεμένο POX Controller. Τα δείγματα αναλύονται ώστε να αναγνωριστούν και να διαχωριστούν οι κακόβουλες ροές. Παράλληλα ο Controller καθοδηγεί τον μεταγωγέα ώστε να επαναπροωθήσει τις καλοήθεις ροές πίσω προς τον Δρομολογητή A. Κατά συνέπεια, ο μεταγωγέας προκαλεί την προώθηση των αντίστοιχων πακέτων βάσει φίλτρων (filter-based forwarding ή Policy-based Routing - PBR), μεταβάλλοντας καταλλήλως τις επικεφαλίδες των πακέτων και εισάγοντας κατάλληλο

Virtual Local Area Network Identifier (VLAN ID). Αντίστοιχα, πρέπει να έχει παραμετροποιηθεί ο Δρομολογητής Α, ώστε να δρομολογεί μέσω PBR πακέτα τα οποία έχουν προσημανθεί με ένα χαρακτηριστικό VLAN ID, προς το θύμα της επίθεσης.

6.4.2 Αξιολόγηση πολυεπίπεδης προσέγγισης ανίχνευσης επιθέσεων DDoS

Στην παρούσα ενότητα παρουσιάζεται μία εκτενής αξιολόγηση της προτεινόμενης πολυεπίπεδης προσέγγισης ανίχνευσης Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας (DDoS). Αρχικά, παρουσιάζονται συγκριτικά αποτελέσματα που προέκυψαν μέσω της πειραματικής διαδικασίας, και τα οποία οδήγησαν στην υιοθέτηση του μηχανισμού ανίχνευσης ανωμαλιών δύο επιπέδων. Εν συνεχεία, παρουσιάζονται και αναλύονται τα αποτελέσματα που προέκυψαν σχετικά με την αξιολόγηση του πρωτότυπου μηχανισμού ο οποίος αναπτύχθηκε και δοκιμάσθηκε.

6.4.2.1 Αλγόριθμοι ανίχνευσης επιθέσεων: κατανάλωση πόρων και ακρίβεια ανίχνευσης

Σημαντικές παράμετροι για την καταλληλότητα των αλγορίθμων ανίχνευσης ανωμαλιών είναι τόσο η κλιμακωσιμότητά τους, όσο και η αντιστάθμιση μεταξύ ακρίβειας και κατανάλωσης πόρων (συνήθως η υψηλή αποτελεσματικότητα αλγορίθμων συνοδεύεται και από υψηλές απαιτήσεις σε πόρους συστήματος). Στην παράγραφο αυτή παρουσιάζεται μία εκτενής σύγκριση δύο διαφορετικών αλγορίθμων σαν πρώτο επίπεδο ανίχνευσης ανωμαλιών. Συγκεκριμένα, αντιπαραβάλλονται μία τεχνική Modified Count-Min Sketch (MCS) η οποία προτείνεται στην εργασία [85], με την προσέγγιση η οποία βασίζεται στη παρατήρηση της μεταβολής στην εντροπία συγκεκριμένων μεταβλητών (η οποία και επιλέχθηκε τελικά).

Εν συντομία, η τεχνική MCS στηρίζεται στην συνάθροιση πολυδιάστατων ροών σε λιγότερες διαστάσεις μέσω δομών δεδομένων τύπου *K*-ary sketch. Όπως αναλύθηκε και σε προηγούμενη ενότητα, χρησιμοποιείται την διεύθυνση IP προορισμού των πακέτων ως κλειδί, για την αποθήκευση του αριθμού των πακέτων που αντιστοιχούν σε κάθε διεύθυνση. σε αυτή τη δομή δεδομένων. Στη συνέχεια, με την τεχνική του Εκθετικά Σταθμισμένου Κινητού Μέσου (Exponentially Weighted Moving Average – EWMA) ελέγχεται αν η τιμή του αριθμού των πακέτων που αντιστοιχούν σε κάθε IP ξεπερνά ένα κατώφλι, κάτι το οποίο καταδεικνύει την πιθανότητα ύπαρξης δικτυακής επίθεσης.

Ο Πίνακας 13 αναφέρει το βαθμό χρήσης της Κεντρικής Μονάδας Επεξεργασίας του υπολογιστή που χρησιμοποιήθηκε για τη φιλοξενία της μονάδας ADI. Παρουσιάζονται οι μετρήσεις που αφορούν στους δύο αλγορίθμους ανίχνευσης ανωμαλιών σε πρώτο επίπεδο, και οι τιμές αυτές αντιπαραβάλλονται με την αντίστοιχη τιμή για την τεχνική BCS του δευτέρου επιπέδου. Η προσέγγιση μέσω εντροπίας εμφανίζει συγκριτική μείωση χρήσης επεξεργαστικών κύκλων περίπου 15%. Αν και η βελτίωση αυτή δεν είναι από μόνη της ιδιαίτερα σημαντική, η κατανάλωση πόρων από τον αλγόριθμο MCS εξαρτάται άμεσα από τον αριθμό των συναρτήσεων κατακερματισμού (hash functions) που θα χρησιμοποιηθούν στη δομή sketch, κάτι το οποίο έχει άμεσο αντίκτυπο και στην ακρίβεια ανίχνευσης (περισσότερες συναρτήσεις κατακερματισμού ισοδυναμούν με υψηλότερη ακρίβεια αλλά και σημαντικά υψηλότερη κατανάλωση επεξεργαστικών πόρων). Επιπλέον, στον Πίνακας 13 εμφανίζεται το κέρδος σε κατανάλωση πόρων μνήμης τους συστήματος, το οποίο προκύπτει μέσω της προσθήκης του πρώτου επιπέδου ανίχνευσης αντί της χρήσης μόνο της τεχνικής BCS. Συγκεκριμένα παρατηρήθηκε μείωση στην κατανάλωση μνήμης κατά 19,55% και 24,16% για χρήση της τεχνικής ανίχνευσης μέσω μεταβολής εντροπίας ή μέσω MCS, αντίστοιχα σε σύγκριση με τον αλγόριθμο BCS.

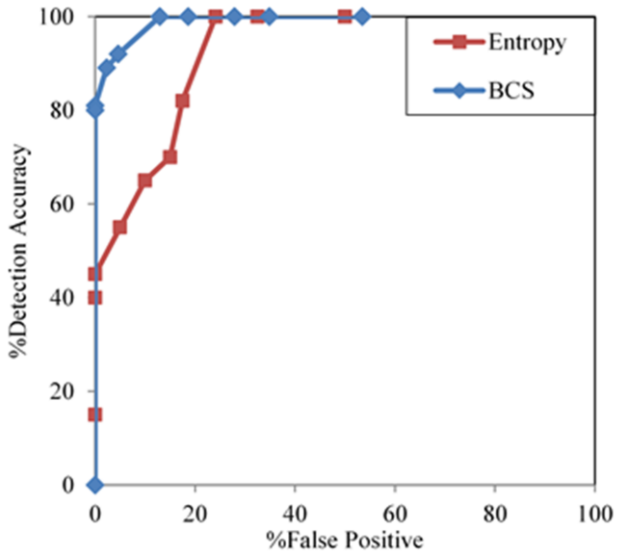
		Πρώτο Επίπεδο Ανίχνευσης		Δεύτερο Επίπεδο Ανίχνευσης
		Entropy-based	MCS	BCS
Πόροι Συστήματος	Μέση Κατανάλωση CPU (%)	34.32	40.24	61.4
	Οικονομία Μνήμης μέσω προσθήκης πρώτου επιπέδου ανίχνευσης (%)	19.55	24.16	-
Ακρίβεια Ανίχνευσης	Ποσοστό False-Positives για 100% ακρίβεια στην ανίχνευση ανωμαλιών (%)	26	32	14

Πίνακας 13: Σύγκριση τριών αλγορίθμων ανίχνευσης δικτυακών ανωμαλιών, σε όρους κατανάλωσης πόρων συστήματος και ακρίβειας ανίχνευσης.

Τέλος, στον Πίνακας 13 συγκρίνεται η ακρίβεια των τριών αλγορίθμων, δηλαδή ο αριθμός των γεγονότων False-Positive τα οποία προκύπτουν σε κάθε έναν, ώστε να επιτυγχάνεται ποσοστό ανίχνευσης επιθέσεων κοντά στο 100%. Η τεχνική ανίχνευσης μέσω

μεταβολής εντροπίας προκάλεσε ποσοστό γεγονότων False-Positive της τάξης του 26%, σε σύγκριση με τον αλγόριθμο MCS που εμφάνισε 34%. Βέβαια, ο σημαντικά αναλυτικότερος αλγόριθμος BCS επιτυγχάνει τη μεγαλύτερη ακρίβεια, προκαλώντας μόλις 14% γεγονότων False-Positive. Δεδομένης της καλύτερης απόδοσης του αλγορίθμου ανίχνευσης μέσω εντροπίας σε σχέση με τον MCS, επιλέχθηκε ο πρώτος για την ανίχνευση δικτυακών ανωμαλιών σε πρώτο επίπεδο, συνοδευόμενος από τον αλγόριθμο BCS ως μία πιο ακριβής (αλλά κοστοβόρα σε όρους πόρων συστήματος) μέθοδο ανίχνευσης ανωμαλιών σε δεύτερο επίπεδο.

Για την περεταίρω εκτίμηση της ακρίβειας των αλγορίθμων που επιλέχθηκαν, το Σχήμα 20 απεικονίζει τις καμπύλες τύπου Receiver Operating Characteristic (ROC Curves). Με τον τρόπο αυτό αποτυπώνονται τα ποσοστά True-Positives και False-Positives για τους αλγορίθμους πρώτου και δεύτερου επιπέδου, οι οποίοι επιλέχθηκαν. Τα αποτελέσματα αυτά προέκυψαν μέσω πολλαπλών πειραμάτων τα οποία πραγματοποιήθηκαν, και χαρακτηρίζονταν από μεταβλητά κατώφλια καθώς και διαφορετικά φορτία κακόβουλης κίνησης.

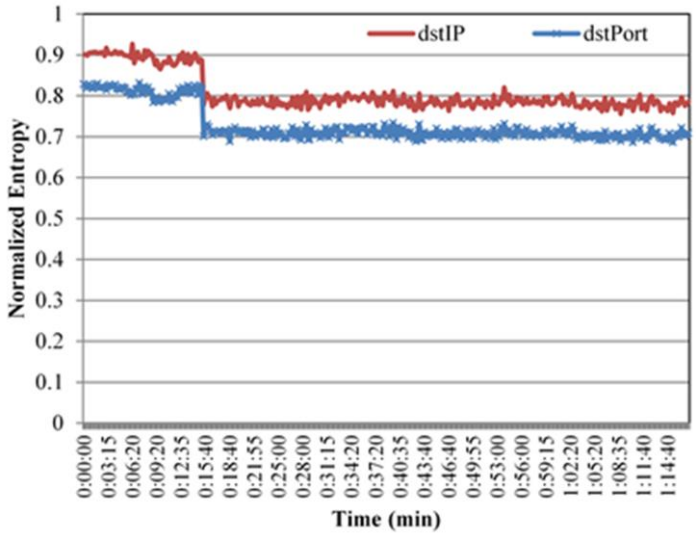


Σχήμα 20: Καμπύλες ROC των αλγορίθμων πρώτου και δεύτερου επιπέδου ανίχνευσης δικτυακών ανωμαλιών

6.4.2.2 Πειραματικά αποτελέσματα ανίχνευσης και αναγνώρισης δικτυακών επιθέσεων DDoS

Το Σχήμα 21 απεικονίζει τις μεταβολές στην εντροπία των διευθύνσεων IP και θυρών μεταφοράς προορισμού, όπως αυτές προέκυψαν μέσω του πρώτου επιπέδου αναγνώρισης

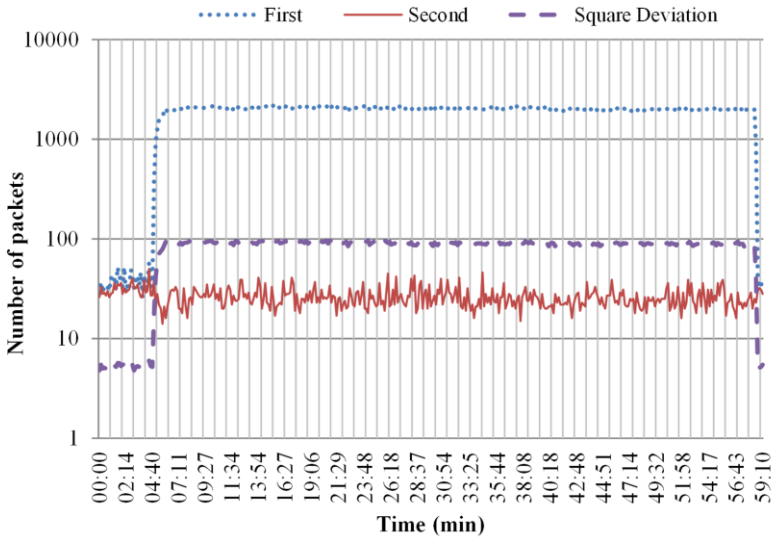
ανωμαλιών. Κατά τη διάρκεια μιας επίθεσης τύπου DDoS, η εντροπία των μεταβλητών αυτών αναμένεται να μειωθεί σημαντικά. Όπως γίνεται εμφανές και στο σχήμα, πριν την επίθεση υπάρχουν μόνο μικρές διακυμάνσεις, ενώ μόλις η επίθεση κλιμακωθεί παρατηρείται στο γράφημα μία σημαντική πτώση της εντροπίας των διευθύνσεων IP και των θυρών μεταφοράς προορισμού, καταδεικνύοντας έτσι την ύπαρξη δικτυακής ανωμαλίας. Υπενθυμίζεται ότι τα πειράματα πραγματοποιήθηκαν συνδυάζοντας την καταγεγραμμένη δικτυακή επίθεση του συνόλου δεδομένων 'CAIDA DDoS attack 2007', με καλόβουλη ανώνυμη κίνηση του δικτύου του Ε.Μ.Π.



Σχήμα 21: Διακύμανση της εντροπίας των Διευθύνσεων IP προορισμού και Θυρών Μεταφοράς προορισμού

Με αντίστοιχο τρόπο διεξήχθησαν και οι πειραματικές δοκιμές για τον αλγόριθμο BCS στο δεύτερο επίπεδο ανίχνευσης ανωμαλιών του προτεινόμενου μηχανισμού. Η μέθοδος BCS βασίζεται στις δομές sketch και επιδιώκει να εντοπίσει διευθύνσεις IP εντός του δικτύου οι οποίες να εμφανίζουν σημαντική απόκλιση από το μέσο όρο. Στο Σχήμα 22 εμφανίζεται, σε περιοδικές μετρήσεις των 10 δευτερολέπτων, η διαφορά των δύο διευθύνσεων IP με τα περισσότερα δείγματα. Ακόμη, στο Σχήμα 22 απεικονίζεται η τιμή τις μέσης τετραγωνικής απόκλισης (mean square deviation) επίσης ανά 10 δευτερόλεπτα. Η γραμμή με τις βούλες δείχνει την τιμή της διαφοράς του αριθμού των δειγμάτων που αντιστοιχούν στην διεύθυνση IP με τα περισσότερα πακέτα, από τη μέση τιμή, και η οποία όπως φαίνεται είναι σημαντικά μεγαλύτερη από την αντίστοιχη και της μέσης τιμής δειγμάτων ανά IP, σε σχέση με την αντίστοιχη μέση τετραγωνική απόκλιση κατά τη

διάρκεια της επίθεσης. Έτσι, όχι μόνο επιβεβαιώνεται η ύπαρξη επίθεσης DDoS, αλλά υποδεικνύεται και το θύμα της επίθεσης αυτής.

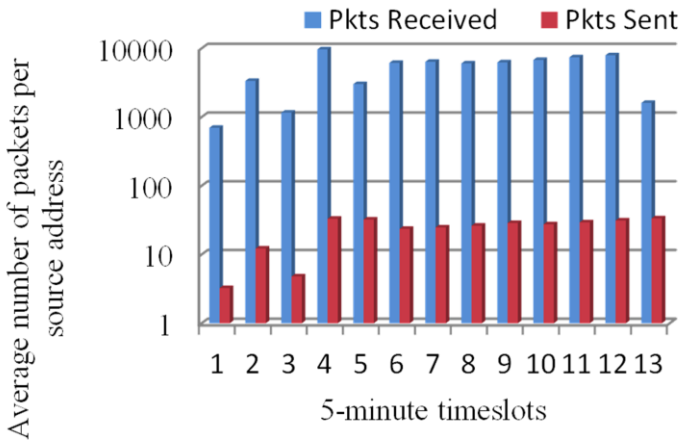


Σχήμα 22: Ανίχνευση επίθεσης DDoS μέσω του αλγορίθμου BCS

6.4.2.3 Συνάθροιση και αποκοπή κακόβουλων πηγών βάσει προθεμάτων IP

Όπως αναλύθηκε σε προηγούμενη παράγραφο, οι κακόβουλες πηγές αναγνωρίζονται λόγω της ασυμμετρίας των ροών από το θύμα προς την κάθε πηγή και από την κάθε πηγή προς το θύμα. Παρατηρήθηκε πως μόλις κορυφωθεί η επίθεση DDoS (περίπου 15 λεπτά μετά την έναρξή της), κατά μέσο όρο ο λόγος των πακέτων που παραλαμβάνει το θύμα προς τα πακέτα που εκείνο αποστέλλει είναι 31:1. Το συμπέρασμα αυτό προκύπτει και από το Σχήμα 23, όπου απεικονίζεται ο λόγος αυτός για διαστήματα των πέντε λεπτών. Έτσι, πηγές οι οποίες εμφανίζουν τέτοια συμπεριφορά, κατηγοριοποιούνται ως κακόβουλες, και συνεπώς επιδιώκεται η αποκοπή τους μέσω του ενδιάμεσου μεταγωγέα OF.

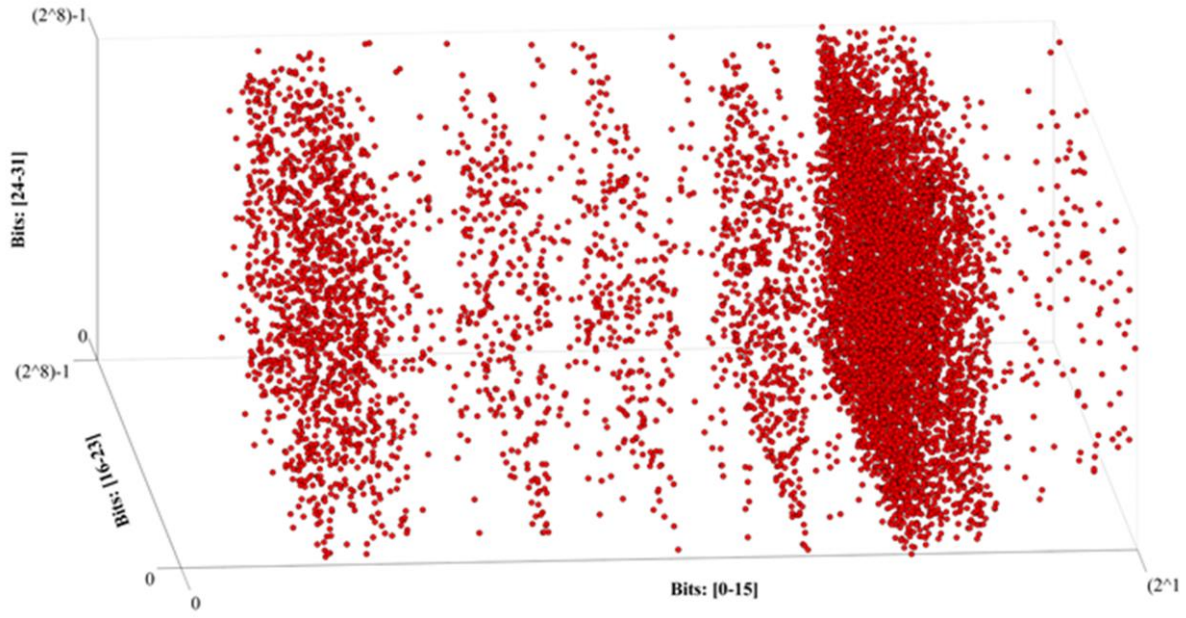
Στο σύνολο δεδομένων της CAIDA παρατηρήθηκε η παρουσία περισσότερων από 60.000 κακόβουλων γεγονότων, προερχόμενων από 9.312 κακόβουλες πηγές. Αυτό συνεπάγεται την ανάγκη για χρήση ενός ίσου αριθμού εγγραφών στον πίνακα ροών του μεταγωγέα OF, προκειμένου να είναι εφικτή η αποκοπή όλης της κακόβουλης κίνησης. Όμως, οι πίνακες ροών των περισσότερων φυσικών (hardware) μεταγωγέων OF υπολείπονται κατά πολύ αυτού του αριθμού, κάνοντας δύσκολη την εφαρμογή της συγκεκριμένης μεθόδου (εξαιρώντας τις περιπτώσεις όπου χρησιμοποιείται μεταγωγέας OF, υλοποιημένος σε λογισμικό όπως το OVS).



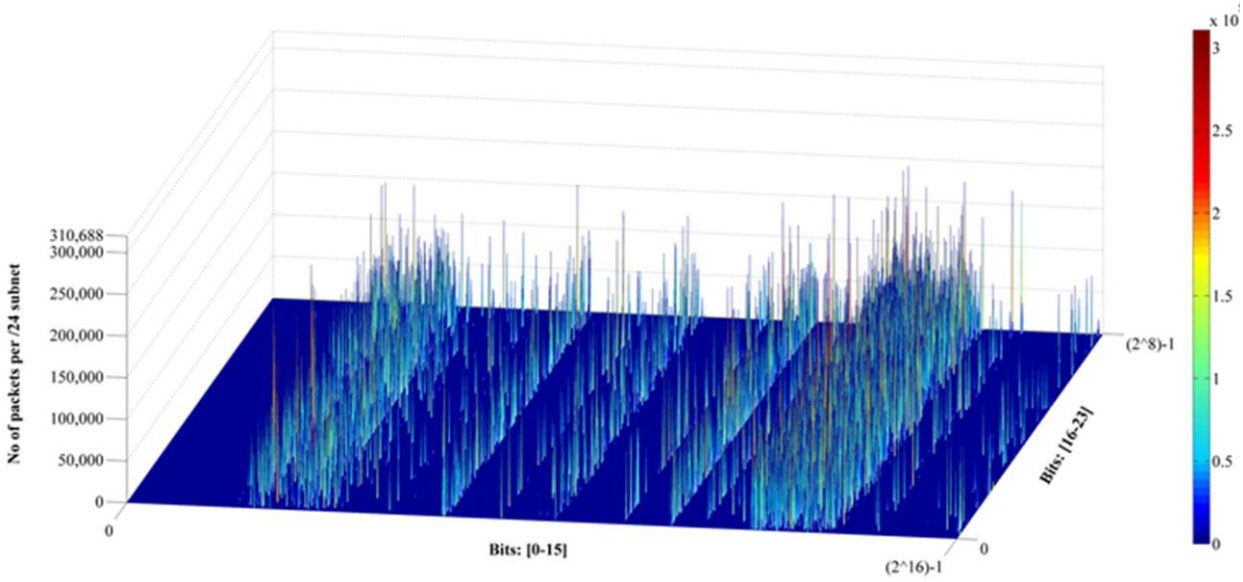
Σχήμα 23: Μέσος αριθμός πακέτων που λαμβάνονται (μπλε) και αποστέλλονται (κόκκινο) από το θύμα προς τις πηγές της επίθεσης. Ο λόγος ληφθέντων προς απεσταλμένων πακέτων φθάνει έως και 31:1.

Μελετώντας την καταγεγραμμένη κίνηση της CAIDA, παρατηρήθηκε ότι οι κακόβουλες πηγές εμφανίζονται συγκεντρωμένες γύρω από συγκεκριμένα προθέματα IP, και δεν είναι ομοιόμορφα κατανεμημένες στο πεδίο τιμών των διευθύνσεων IP. Στο Σχήμα 24 φαίνεται η κατανομή όλων των κακόβουλων διευθύνσεων IP, όπου ο άξονας X αφορά τα 16 πιο σημαντικά bit μιας διεύθυνσης IPv4 (/16 δίκτυα), ο άξονας Y αφορά τα επόμενα 8 bits (/24 δίκτυα), και ο άξονας Z τα τελευταία 8 bits. Αντίστοιχα, στο Σχήμα 25 φαίνεται ο αριθμός των πακέτων –και συνεπώς το αντίστοιχο τμήμα της κακόβουλης κίνησης- που προέρχεται από κάθε υποδίκτυο μέσα σε ένα από προαναφερθέντα /16 δίκτυα.

Βάσει των παραπάνω παρατηρήσεων, και με στόχο τη βελτίωση της κλιμακωσιμότητας του προτεινόμενου μηχανισμού αποκοπής κακόβουλων ροών, υιοθετήθηκε ο αλγόριθμος ομαδοποίησης *Block-All* (όπως έχει ήδη περιγραφεί σε προηγούμενη παράγραφο). Ο αλγόριθμος επαναλαμβάνεται περιοδικά ανά σταθερά χρονικά διαστήματα 30sec. καθ' όλη τη διάρκεια της επίθεσης DDoS (~1 ώρα). Στόχος του είναι η αναγνώριση του βέλτιστου συνόλου προθεμάτων διευθύνσεων IP προκειμένου να συναθροίζονται οι κακόβουλες ροές, υπό τους περιορισμούς τόσο της χωρητικότητας του πίνακα ροών του εκάστοτε μεταγωγέα OpenFlow, όσο και των παράπλευρων απωλειών. Ως παράπλευρες απώλειες χαρακτηρίζονται καλόβουλες ροές οι οποίες θα πρέπει αναγκαστικά να αποκοπούν προκειμένου να επιτευχθεί η βέλτιστη συνάθροιση κακόβουλων ροών χωρίς να υπερχειλίζει ο πίνακας ροών.



Σχήμα 24: Κατανομή των κακόβουλων διευθύνσεων IP που βρίσκονται στο CAIDA DDoS Attack 2007 Dataset, στον IPv4 χώρο.



Σχήμα 25: Κατανομή των κακόβουλων πακέτων σε /24 δίκτυα

Ο Πίνακας 14 παρουσιάζει τα αποτελέσματα των πειραμάτων που πραγματοποιήθηκαν, εξομοιώνοντας μεταγωγείς OF με μέγιστο αριθμό κανόνων (χωρητικότητα) από 1.000 έως 10.000 εγγραφές. Για τη διαδικασία αυτή χρησιμοποιήθηκαν μεταγωγείς υλοποιημένοι σε λογισμικό (Open vSwitch) ώστε να υπάρχει η δυνατότητα εξομοίωσης μεγάλων πινάκων ροών. Ενδεικτικά, από τις 9.312 μοναδικές κακόβουλες πηγές στο σύνολο δεδομένων της

CAIDA, η Μονάδα Αντιμετώπισης Ανωμαλιών κατέληξε στην εισαγωγή 2.175 εγγραφών (πετυχαίνοντας 76,64% μείωση μέσω συνάθροισης), με τις παράπλευρες απώλειες να κυμαίνονται στο 18,3%. Η πρακτική αυτή, δίνει τη δυνατότητα χρήσης φυσικών μεταγωγέων OF μετρίου κόστους, οι οποίοι συνήθως δεν υποστηρίζουν περισσότερες από 4000 ταυτόχρονες εγγραφές στις μνήμες TCAM που διαθέτουν.

Χωρητικότητα Πίνακα Ροών (# Κανόνων)	Απαιτούμενος αριθμός κανόνων για την αποκοπή όλων των κακόβουλων πηγών	Ποσοστό απομείωσης απαιτούμενων κανόνων	Παράπλευρες απώλειες (# καλόβουλων ροών)	Ποσοστό αποκοπής καλόβουλων ροών	Καλόβουλες ροές οι οποίες προωθούνται στο θύμα
10,000	9,312	-	0	0 %	49754
7,500	7,272	21.91 %	265	0.5 %	49489
5,000	4,186	55.05 %	3294	6.6 %	46460
3,000	2,175	76.64 %	9109	18.3 %	40645
1,000	936	89.95 %	19866	39.9 %	29888

Πίνακας 14: Αντιστάθμιση αριθμού εγγραφών για την αποκοπή κακόβουλων ροών και παράπλευρων απωλειών κατά τη χρήση του αλγορίθμου *Block-All*

7 Αντιμετώπιση Κατανεμημένων Επιθέσεων σε Ευφυή Προγραμματιζόμενα Δίκτυα μέσω Συνεργατικών Σχημάτων Βασισμένων στη Φήμη

7.1 Εισαγωγή

Στις προηγούμενες ενότητες αναλύθηκαν μηχανισμοί για την προστασία παραδοσιακών αλλά και ευφυών προγραμματιζόμενων δικτύων από κακόβουλες επιθέσεις. Όμως, όσον αφορά Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (Distributed Denial of Service – DDoS), η αντιμετώπισή τους είναι πιθανόν να οδηγήσει στην κατανάλωση σημαντικών πόρων συστήματος και δικτύου. Στη συγκεκριμένη ενότητα προτείνεται ένας μηχανισμός για τη δημιουργία συνεργατικών σχημάτων μεταξύ ευφυών δικτυακών περιοχών ενδιάμεσης διέλευσης (transit SDN domains) οι οποίες άθελά τους προωθούν την κακόβουλη κίνησης προς ένα θύμα επίθεσης DDoS που φιλοξενείται σε ένα τελικό SDN domain. Ο μηχανισμός αυτός επιτρέπει την αποκοπή της κακόβουλης κίνησης με αποτελεσματικό και κλιμακώσιμο τρόπο, υποστηρίζοντας: (α) την δημιουργία και διατήρηση συνεργατικών σχημάτων μεταξύ SDN domains, βασισμένων στη φήμη και (β) την κατανεμημένη αντιμετώπιση επιθέσεων DDoS από τα συνεργαζόμενα SDN domains, τα οποία αναλαμβάνουν να μεταφέρουν σταδιακά τη διαδικασία αποκοπής κακόβουλων ροών όσο το δυνατόν πιο κοντά στις πηγές τους.

Στα πλαίσια αυτά, περιγράφεται ένας μηχανισμός ο οποίος αξιοποιεί τις δυνατότητες δικτυακού προγραμματισμού που προσφέρει το πρωτόκολλο OpenFlow [1] εσωτερικά σε μία δικτυακή περιοχή, αλλά και τις αυξημένες δυνατότητες σηματοδοσίας μεταξύ γειτονικών περιοχών τις οποίες προσφέρει το πρωτόκολλο SDNi [100] αξιοποιώντας τη σηματοδοσία BGP. Θεωρείται δεδομένο ότι όλοι οι δικτυακοί τομείς υιοθετούν το πρωτόκολλο OpenFlow (SDN-enabled), και συγκεκριμένα ότι: (α) οι δικτυακές συσκευές στα άκρα τους υποστηρίζουν το πρωτόκολλο OF, και (β) οι συσκευές αυτές ελέγχονται από έναν ή περισσότερους OF Controllers. Για τις ανάγκες υλοποίησης του συγκεκριμένου μηχανισμού, επεκτάθηκε το πρωτόκολλο SDNi προκειμένου να επιτρέπει την διάδοση αναφορών δικτυακών επιθέσεων (μεταξύ γειτονικών SDN domains), διαμορφωμένες σύμφωνα με το πρότυπο της IETF Incident Object Description Exchange Format (IODEF) [101], [102]. Οι αναφορές ανταλλάσσονται μεταξύ γειτονικών SDN domains, ενσωματωμένες ως Universal Resource Identifiers (URIs) στην σηματοδοσία BGP του Επιπέδου Ελέγχου. Οι παραλήπτες τους αναλαμβάνουν την περεταίρω διάδοσή τους σε

SDN domains τα οποία βρίσκονται πιο κοντά στις πηγές μίας επίθεσης DDoS, ζητώντας ταυτόχρονα την αποκοπή του συνόλου των κακόβουλων ροών τις οποίες προωθούν. Τελικά, με τον τρόπο αυτό επιχειρείται η αποκοπή κακόβουλων επιθέσεων σε περιοχές πιο κοντά στις πηγές (upstream) και διευκολύνεται το SDN domain το οποίο εξυπηρετεί το θύμα μιας κατανεμημένης επίθεσης, το οποίο καταναλώνει σημαντικά λιγότερους δικτυακούς πόρους (εύρος ζώνης και αριθμός κανόνων που πρέπει να τοποθετηθούν στις συνοριακές συσκευές του domain-θύματος) για την αντιμετώπιση της επίθεσης αυτής. Το ίδιο κέρδος προκύπτει βεβαίως και για τα ενδιάμεσα (transit) SDN domains που βρίσκονται στο μονοπάτι των κακόβουλων ροών, αφού αποκόπτοντας τις κακόβουλες ροές εξοικονομούν εύρος ζώνης διέλευσης. Το κέρδος αυτό λειτουργεί και ως κίνητρο για τη δημιουργία και διατήρηση του συνεργατικού σχήματος σε περιβάλλοντα πολλαπλών περιοχών (multi-domain).

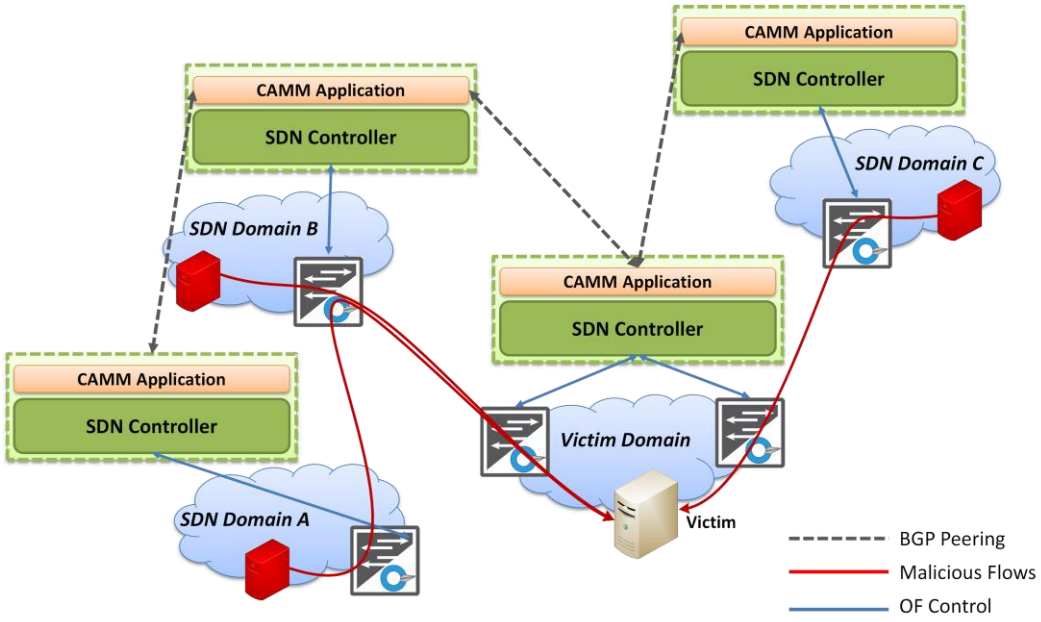
Να σημειωθεί ότι η συνεργατική αντιμετώπιση επιθέσεων είναι καθιερωμένη πρακτική μεταξύ διαχειριστών των υποδικτύων στο Internet, η οποία υλοποιείται offline μεταξύ Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας (Computer Emergency Response Teams – CERTs). Ο προτεινόμενος μηχανισμός προάγει την online συνεργατική αντιμετώπιση κατανεμημένων επιθέσεων με τη χρήση αυτοματοποιημένων αναφορών του προτύπου IODEF. Για την αξιολόγησή του, αναπτύχθηκε και δοκιμάστηκε στο εργαστήριο πρότυπη έκδοση του μηχανισμού. Στόχος των πειραμάτων ήταν η εκτίμηση της αποτελεσματικότητας και κλιμακωσιμότητας του συγκεκριμένου μηχανισμού.

7.2 Γενική Αρχιτεκτονική

7.2.1 Περιγραφή προτεινόμενης προσέγγισης

Στο Σχήμα 26 απεικονίζεται (σε αφαιρετικό επίπεδο) μία κατανεμημένη επίθεση προς έναν εξυπηρετητή, καθώς και ο συνεργατικός μηχανισμός για την αποκοπή αυτής. Στο σχήμα εμφανίζονται τόσο γειτονικά, όσο και απομακρυσμένα (ως προς το θύμα) SDN domains τα οποία εν αγνοία τους εξυπηρετούν κακόβουλες ροές προερχόμενες από πηγές οι οποίες συμμετέχουν σε μία επίθεση DDoS. Για την αποκοπή τους εισάγεται ο Συνεργατικός Μηχανισμός Αντιμετώπισης Επιθέσεων (Cooperative Attack Mitigation Mechanism – CAMM) ο οποίος προτείνεται σαν μια νέα εφαρμογή για SDN Controllers. Η ακολουθία βημάτων του CAMM είναι: (α) η ενεργοποίηση του μηχανισμού CAMM, μόλις ανιχνευθεί μία κατανεμημένη επίθεση στο SDN domain το οποίο εξυπηρετεί το θύμα, (β) η διάδοση σχετικών αναφορών (ως IODEF reports) στα γειτονικά domains τα οποία εξυπηρετούν την

προώθηση των κακόβουλων ροών, (γ) η καταγραφή των αναφορών αυτών από τους παραλήπτες-εφαρμογές CAMM των γειτονικών περιοχών (SDN Domains B και C στο Σχήμα 26) ως αιτήματα για την αποκοπή των κακόβουλων ροών, (δ) η ενεργοποίηση μηχανισμών αποκοπής κακόβουλων ροών μέσω εγγραφών στους πίνακες ροών συσκευών OpenFlow (εφόσον αυτό ενδείκνυται από το μηχανισμό φήμης), και (ε) η περεταίρω προώθηση των αναφορών σε νέα γειτονικά upstream SDN domains (π.χ. SDN Domain A στο Σχήμα 26) έως ότου η διαδικασία φθάσει στις πηγές της επίθεσης.



Σχήμα 26: Αφαιρετική απεικόνιση του προτεινόμενου συνεργατικού μηχανισμού για την αποκοπή κατανεμημένων επιθέσεων

Οι βασικές σχεδιαστικές αρχές σύμφωνα με τις οποίες και υλοποιήθηκε η εφαρμογή CAMM συμπεριλαμβάνουν:

- *Αναγνώριση διαδρομής κακόβουλων ροών (attack paths):* Τα SDN domains αναγνωρίζουν τους άμεσα γειτονικούς τομείς οι οποίοι εξυπηρετούν κακόβουλες ροές δεδομένων, πλησιάζοντας έτσι προς τις πηγές μίας επίθεσης DDoS. Η επιτυχής αναγνώριση βασίζεται στο συνδυασμό πληροφοριών του SDN Controller, τις οποίες καθιστά διαθέσιμες μέσω διεπαφής Αναπαραστατικής Μεταφοράς Κατάστασης (Representational State Transfer – REST).

- *Συλλογική αντιμετώπιση κατανεμημένων επιθέσεων:* Η εφαρμογή CAMM επιτρέπει σε γειτονικά SDN domains να συνάψουν προσωρινές σχέσεις συνεργασίας με αυτοματοποιημένο τρόπο, στοχεύοντας στην αντιμετώπιση δικτυακών απειλών οι

οποίες επηρεάζουν τα domains αυτά. Κάθε transit SDN domain κατά μήκος της διαδρομής των δικτυακών ροών μίας κατανεμημένης επίθεσης, δύναται να δεσμεύσει επιλεκτικά εγγραφές στους πίνακες ροών OpenFlow ώστε να συνδράμει στη διαδικασία αντιμετώπισης μίας κατανεμημένης επίθεσης. Η απόφαση για δέσμευση των εγγραφών αυτών λαμβάνεται με βάσει τη φήμη της περιοχής που εξυπηρετεί το θύμα της επίθεσης, η οποία εξαρτάται άμεσα από το επίπεδο συνεργασίας που προσέφερε ο τελευταίος σε περασμένα αντίστοιχα περιστατικά.

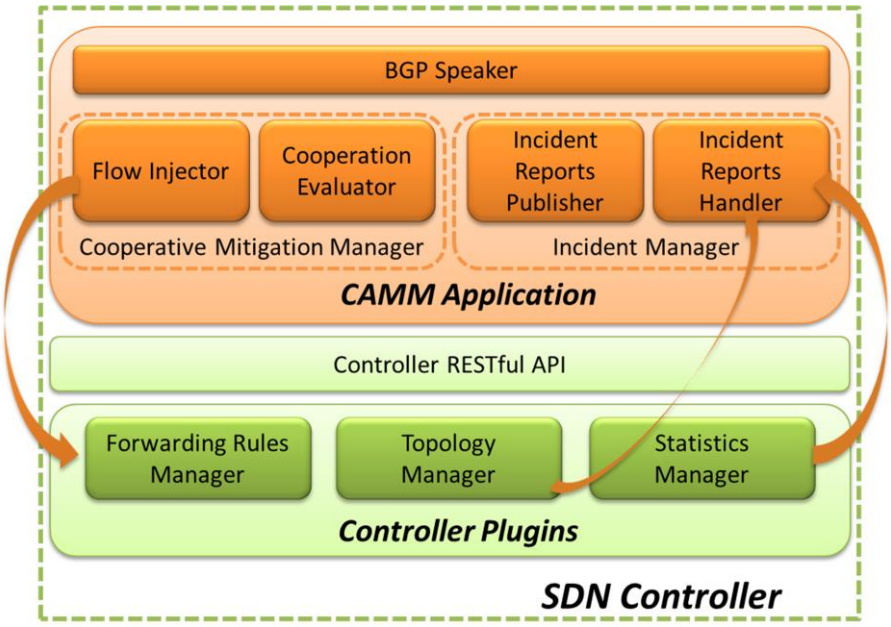
- *Διάδοση αναφορών επιθέσεων προς δικτυακούς τομείς κοντά στις πηγές:* Μέσω της εφαρμογής CAMM οι SDN Controllers γειτονικών περιοχών ανταλλάσουν δείκτες σε αναφορές επιθέσεων με τη μορφή Ενιαίων Αναγνωριστικών Πόρων (Uniform Resource Identifiers – URIs). Η ανταλλαγή των αναφορών επιτεύχθηκε μέσω της επέκτασης του πρωτοκόλλου SDNi, προκειμένου να επιτρέπει την αποστολή μηνυμάτων IODEF [102] σε SDN domains τα οποία εξυπηρετούν τις κακόβουλες ροές δεδομένων. Κάθε ενδιάμεσο domain αποστέλλει μία σχετική αναφορά προς γειτονικά domains πλησιέστερα προς τις πηγές της επίθεσης, εξοικονομώντας δικτυακούς πόρους (δικτυακό εύρος ζώνης αλλά και εγγραφές σε πίνακες ροών OpenFlow) για όλα τα SDN domains που βρίσκονται πιο κοντά στο θύμα της επίθεσης.

- *Κατανεμημένη αντιμετώπιση επιθέσεων DDoS σε επίπεδο ροών:* Οι εγγραφές σε πίνακες ροών συνοριακών μεταγωγέων OpenFlow αποτελούν έναν πολύτιμο πόρο της δικτυακής υποδομής, κυρίως λόγω του περιορισμένου μεγέθους τους αλλά και της υψηλής κατανάλωσης ενέργειας [103]. Ένα SDN domain θα έπρεπε να αφιερώσει σημαντικό αριθμό εγγραφών προκειμένου να αποκόψει μία κατανεμημένη επίθεση στο σύνολό της και με λεπτομερή ανάλυση ώστε να μην επηρεαστεί η κανονική κίνηση. Αντίθετα, η εφαρμογή CAMM μεταφέρει τη διαδικασία αποκοπής κακόβουλων ροών όσο το δυνατόν πιο κοντά στις πηγές, κατανέμοντας τις εγγραφές στα ενδιάμεσα SDN domains, και διευκολύνοντας έτσι τον καθολικό περιορισμό της επίθεσης.

- *Ενίσχυση συνεργατικότητας μεταξύ Αυτόνομων Περιοχών SDN:* Ο μηχανισμός φήμης λειτουργεί σαν κίνητρο για τη συνεργατική αντιμετώπιση κατανεμημένων επιθέσεων, ενθαρρύνοντας τη συνδρομή στην αντιμετώπισή τους μιας και αναδεικνύει περιοχές καλής συμπεριφοράς, οι οποίες και αναμένουν αντίστοιχη αρωγή από γειτονικές τους περιοχές όταν αυτή χρειαστεί.

7.2.2 Δομικά στοιχεία εφαρμογής για το Επίπεδο Ελέγχου

Η εφαρμογή CAMM υιοθετεί και επεκτείνει τις δυνατότητες της εφαρμογής SDNi [104] του OpenDaylight SDN Controller (ODL) [105], ο οποίος είναι ένας από τους πιο διαδεδομένους Ελεγκτές για περιβάλλοντα SDN. Να σημειωθεί ότι το SDNi επικεντρώνεται στην ανταλλαγή πληροφοριών μεταξύ γειτονικών SDN domains, τα οποία όμως βρίσκονται υπό την εποπτεία ενός μοναδικού παρόχου (ανήκουν στο ίδιο Αυτόνομο Σύστημα). Αντίθετα, η προτεινόμενη προσέγγιση υιοθετεί το πρωτόκολλο SDNi για την επικοινωνία γειτονικών SDN domains, τα οποία μάλιστα μπορεί να ανήκουν σε ανεξάρτητες αρχές διαχείρισης. Για να καταστεί αυτό εφικτό, υλοποιήθηκε ένας μηχανισμός φήμης μέσω του οποίου είναι δυνατή η δημιουργία και διατήρηση ενός μοντέλου εμπιστοσύνης μεταξύ δικτυακών περιοχών στα άκρα γειτονικών Αυτόνομων Συστημάτων, με στόχο την από κοινού αντιμετώπιση επιθέσεων DDoS.



Σχήμα 27: Επιμέρους μονάδες οι οποίες συνθέτουν τον μηχανισμό αντιμετώπισης κατανεμημένων επιθέσεων CAMM

Στη γενική αρχιτεκτονική προσέγγιση, όπως αυτή απεικονίζεται και στο Σχήμα 27, διακρίνονται τρεις ανεξάρτητες λειτουργικές μονάδες, και συγκεκριμένα οι *Cooperative Mitigation Manager*, *Incident Manager*, και *BGP Speaker*.

1. Η μονάδα *Cooperative Mitigation Manager (CMM)* καθορίζει τις πολιτικές, σύμφωνα με τις οποίες ένα SDN domain θα δράσει κατόπιν της λήψης μίας αναφοράς επίθεσης. Η μονάδα CMM αποτελείται από δύο υπομονάδες οι οποίες διαχωρίζουν σε λογικό

επίπεδο τις απαιτούμενες λειτουργικότητες, τις Cooperation Evaluator (CE) και Flow Injector (FI). Η πρώτη είναι υπεύθυνη για τη λήψη αποφάσεων οι οποίες αφορούν στη συμμετοχή η μη του εν λόγω SDN domain σε συνεργατικό σχήμα για την αντιμετώπιση μίας επίθεσης DDoS. Η δεύτερη υπομονάδα έχει τη δυνατότητα εγκαθίδρυσης κανόνων για την αποκοπή εκείνων των ροών δεδομένων που συμπεριλαμβάνονται στο αρχείο XML (IODEF) που υποδεικνύεται από το URI στην αναφορά επίθεσης. Να σημειωθεί ότι η απόφαση για συμμετοχή σε τέτοιου τύπου συνεργατικά σχήματα, λαμβάνεται με βάσει το επίπεδο φήμης του SDN domain το οποίο και αποστέλλει την αναφορά επίθεσης. Αν η υπομονάδα CE κρίνει ότι το SDN domain στο οποίο ανήκει πρέπει να συνδράμει στη διαδικασία αποκοπής μίας κατανεμημένης επίθεσης, τότε ενημερώνει κατάλληλα την υπομονάδα FI και την μονάδα Incident Manager για περεταίρω διάδοση της αναφοράς επίθεσης (όπως περιγράφεται στη συνέχεια).

2. Η μονάδα *Incident Manager (IM)* αποτελεί και το κυριότερο δομικό στοιχείο του προτεινόμενου μηχανισμού, μέσω του οποίου είναι εφικτή η συνάθροιση των απαιτούμενων δεδομένων για την δημιουργία των αναφορών επιθέσεων, η διαμόρφωσή τους κατά τα πρότυπα IODEF, και η προσπέλασή τους από τους τομείς-παραλήπτες. Στη μονάδα IM διακρίνονται δύο κύρια στοιχεία, τα Incident Reports Handler (IRH) και Incident Reports Publisher (IRP). Το IRH για το SDN domain του θύματος, δημιουργεί αναφορές XML κατά τα πρότυπα IODEF, οι οποίες διατηρούνται τοπικά στον SDN Controller της περιοχής του θύματος. Παράλληλα, καθοδηγεί το IRP ώστε εκείνο να καταστήσει τις αναφορές αυτές προσβάσιμες στα γειτονικά SDN domain, ορίζοντας ένα μοναδικό URI για κάθε μία. Αντίστοιχα, το IRH για transit ή attack source SDN domains, είναι υπεύθυνο για τη συλλογή μηνυμάτων IODEF τα οποία αφορούν σε μία εν ενεργεία δικτυακή επίθεση, καθώς και για την προώθηση της σχετικής αναφοράς στην μονάδα CMM ώστε να ληφθεί η απαραίτητη απόφαση περί συνδρομής ή μη στην αντιμετώπιση της επίθεσης.

3. Η μονάδα *BGP Speaker* επιτρέπει σε γειτονικούς SDN Controllers την ανταλλαγή URIs, τα οποία παραπέμπουν σε ενεργές αναφορές επιθέσεων. Συγκεκριμένα, η μονάδα είναι ικανή: (α) να προσπελαύνει μηνύματα SDNi τα οποία μεταδίδονται ενθυλακωμένα σε μηνύματα σηματοδοσίας BGP, (β) να εξάγει το αντίστοιχο URI το οποίο δείχνει στο σημείο ανάκτησης της αναφοράς επίθεσης, και (γ) να μεταφέρει το URI της αναφοράς στη μονάδα IM για λήψη και περεταίρω επεξεργασία της αντίστοιχης αναφοράς IODEF.

7.3 Συνεργατικά Σχήματα Φήμης για Αντιμετώπιση Κατανεμημένων Επιθέσεων

7.3.1 Μηχανισμός φήμης μεταξύ ευφυών δικτυακών περιοχών

Μέσω των αναφορών επιθέσεων, είναι πιθανό να ζητηθεί από κάποιο ενδιάμεσο SDN domain η εισαγωγή εκατοντάδων εγγραφών ροών προκειμένου να προσδιοριστούν λεπτομερώς και να αποκοπούν κακόβουλες ροές δεδομένων. Αυτό μπορεί να οδηγήσει τους διαχειριστές των περιοχών αυτών στην υιοθέτηση μίας μυωπικής και ιδιοτελούς πολιτικής. Τέτοιες πολιτικές μπορούν να αποφευχθούν μέσω της δημιουργίας και διατήρησης μοντέλων εμπιστοσύνης μεταξύ των SDN domains. Έτσι, αναπόσπαστο χαρακτηριστικό του προτεινόμενου μηχανισμού είναι η φήμη και εμπιστοσύνη μεταξύ SDN domains τα οποία ελέγχονται από ανεξάρτητες διαχειριστικές αρχές, και τυγχάνει να βρίσκονται μεταξύ του θύματος και ορισμένων πηγών μίας κατανεμημένης επίθεσης. Η υπομονάδα CE (Cooperation Evaluator) είναι υπεύθυνη σε κάθε SDN domain για την απόφαση περί συνδρομής ή μη στη συνεργατική αποκοπή μία κατανεμημένης επίθεσης, πάντα κατόπιν αιτήματος (αναφοράς επίθεσης) από γειτονικό SDN domain. Η προσέγγιση αυτή στοχεύει στην εξοικονόμηση δικτυακών πόρων, αποφεύγοντας τη δέσμευσή τους για συνδρομή στην αντιμετώπιση μίας κατανεμημένης επίθεσης, όταν το αίτημα για συνδρομή προέρχεται από ένα SDN domain με χαμηλό επίπεδο φήμης (συνεργατικότητας). Το επίπεδο φήμης γειτονικών SDN domains διατηρείται από την υπομονάδα CE σε κάθε domain, κατά αντιστοιχία με τον υπολογισμό του επιπέδου εμπιστοσύνης, όπως αυτό ορίζεται στην εργασία [106]. Στις επόμενες υποενότητες αναλύεται η μέθοδος υπολογισμού του επιπέδου φήμης.

7.3.1.1 Μηχανισμός φήμης μεταξύ γειτονικών περιοχών SDN

Για την εκτίμηση του επιπέδου φήμης μεταξύ δύο προσκείμενων SDN domains, η CE του κάθε ενός υιοθετεί μία κατανομή *Beta(a, b)* [107] για το άλλο domain, ακολουθώντας την τροποποιημένη προσέγγιση κατά Bayes όπως περιγράφεται στην εργασία [108]. Οι παράμετροι *a* και *b* της κατανομής ανανεώνονται κάθε φορά που το domain ζητά τη συνδρομή του γειτονικού domain. Κατά την *n + 1* ανανέωση, οι τιμές των παραμέτρων α_{n+1} για την *a* και b_{n+1} *για την b* υπολογίζονται αναδρομικά ως εξής:

$$a_{n+1} = a_n \cdot u + s,\ b_{n+1} = b_n \cdot u + (1 - s), \quad (7.1)$$

$$a_0 = b_0 = 1,$$

όπου το *s* θεωρείται 1 αν το γειτονικό domain συνδράμει στην αντιμετώπιση μίας επίθεσης DDoS, και 0 αν δεν συνδράμει. Το *u* είναι ένας συντελεστής απόσβεσης (depreciation factor), ώστε να εξασθενεί σταδιακά το βάρος παλαιότερων τιμών των παραμέτρων *a* και *b*.

Το επίπεδο φήμης (reputation score) του προσκείμενου SDN domain ορίζεται ως η μέση τιμή της κατανομής έπειτα από *n* επαναλήψεις, και υπολογίζεται ως $a_n /(a_n+b_n)$ [107].Στην περίπτωση όπου το SDN domain αυτό ζητήσει στο μέλλον τη συνδρομή για την αντιμετώπιση μιας κατανεμημένης επίθεσης, τότε εάν το επίπεδο φήμης (η μέση τιμή της κατανομής Beta) είναι μεγαλύτερο ή ίσο από ένα κατώφλι *R*, η υπομονάδα CE επιτρέπει την δέσμευση των ζητούμενων κανόνων στον πίνακα ροών του συνοριακού μεταγωγέα OpenFlow.

Συνεπώς, μία θετική απάντηση από τη CE ακολουθείται και από την εισαγωγή των απαιτούμενων κανόνων στον πίνακα ροών μέσω της υπομονάδας Flow Injector (FI). Η FI επικοινωνεί με το Forwarding Rules Manager (FRM) του SDN Controller για να μεταφέρει την απαιτούμενη πληροφορία, ώστε το FRM με τη σειρά του να εγκαταστήσει τους κατάλληλους OpenFlow κανόνες για την αποκοπή των κακόβουλων ροών. Στους κανόνες αυτούς μπορούν να οριστούν οσαδήποτε πεδία της χαρακτηριστικής εγγραφής OpenFlow [28], ενώ για τους σκοπούς του πρότυπου μηχανισμού που αναπτύχθηκε χρησιμοποιήθηκε μόνο το πεδίο *SourceIP* (διεύθυνση IP πηγής). Η προαναφερθείσα επικοινωνία μεταξύ FI και FRM πραγματοποιείται μέσω της προγραμματιστικής διεπαφής τύπου REST (RESTful API) [109] του SDN Controller.

Ένα SDN domain το οποίο και αιτείται τη συνδρομή ενός προσκείμενου domain, αντιλαμβάνεται την απόφαση του τελευταίου περί συνδρομής η μη αναλόγως με το αν οι ροές που ήδη έχει βάλει το πρώτο για την αντιμετώπιση της επίθεσης, λήξουν και άρα αφαιρεθούν από τον πίνακα ροών του δικού του μεταγωγέα OpenFlow. Αναλυτικότερα, αμέσως μετά την ανίχνευση μίας επίθεσης DDoS, το SDN domain το οποίο και εξυπηρετεί-φιλοξενεί το θύμα της επίθεσης καταναλώνει ιδίους πόρους (εγγραφές στους δικούς του μεταγωγείς OpenFlow) για την αποκοπή των κακόβουλων ροών που εντοπίστηκαν. Αν στη συνέχεια, γειτονικοί δικτυακοί τομείς αφιερώσουν δικτυακούς πόρους για τον περιορισμό ενός υποσυνόλου των κακόβουλων ροών, τότε οι αρχικοί κανόνες του domain-θύματος θα λήξουν λόγω της παραμέτρου *idle-timeout* [28].

Αξίζει να σημειωθεί ότι ένα Αυτόνομο Σύστημα είναι πιθανόν να αποτελείται από περισσότερα του ενός SDN domains. Για τις περιπτώσεις αυτές θεωρείται δεδομένο ότι τα SDN domains στο εσωτερικό του AS έχουν μεταξύ τους πλήρη εμπιστοσύνη (αφού βρίσκονται υπό την ίδια διαχειριστική αρχή), και κατά συνέπεια θα εμφανιστούν συνεργάσιμα. Αυτό είναι συνεπακόλουθο του μοντέλου μεταβατικής εμπιστοσύνης (transitive trust [106]) και προϋποθέτει ότι το συνοριακό SDN domain θα λάβει θετική απόφαση για συνδρομή στην αντιμετώπιση μίας επίθεσης. Έτσι η συγκεκριμένη πρόταση, θεωρεί Αυτόνομα Συστήματα τα οποία προτυποποιούνται σύμφωνα με τις παραδοσιακές αρχιτεκτονικές IP/BGP του παγκόσμιου Internet, θεωρώντας ότι μελλοντικά οι συνοριακές συσκευές θα υποστηρίζουν πρωτόκολλα SDN. Η υιοθέτηση του ανεξάρτητου Επιπέδου Ελέγχου μέσω εξωτερικού SDN Controller διευκολύνει σημαντικά στην υλοποίηση του μηχανισμού CAMM. Βεβαίως, η προτεινόμενη συνεργατική υποδομή μπορεί να εφαρμοστεί και στις υπάρχουσες παραδοσιακές υποδομές με κατάλληλη προγραμματιστική παρέμβαση στις λίστες ελέγχου πρόσβασης (ACLs) των συνοριακών δρομολογητών (π.χ. με πρωτόκολλο διαχείρισης NETCONF με απευθείας παρέμβαση του διαχειριστή στις συνοριακές δικτυακές συσκευές).

7.3.1.2 Μηχανισμός φήμης για αποσυνδεδεμένους τομείς SDN

Ευφυείς Δικτυακοί Τομείς οι οποίοι ανήκουν σε Αυτόνομα Συστήματα τα οποία δεν συνορεύουν, δεν έχουν προηγούμενη εμπειρία σχετικά με το επίπεδο συνεργατικότητας του κάθε ενός. Έτσι, ένα SDN domain μπορεί κατά τη λήψη μίας αναφοράς επίθεσης η οποία αφορά ένα άλλο απομακρυσμένο domain, να υιοθετήσει τη γνώμη ενός ευυπόληπτου (reputable) γειτονικού domain. Για το λόγο αυτό, τα ενδιάμεσα SDN domains πρέπει να τροποποιήσουν την αρχική αναφορά της περιοχής που εξυπηρετεί το θύμα της επίθεσης, και να συμπεριλάβουν το επίπεδο συνεργατικότητας (φήμης) που εκείνα γνωρίζουν για αυτήν. Κατόπιν, το ενδιάμεσο SDN domain θα συγκεντρώσει την πληροφορία που μαζεύει από όλα τα γειτονικά domains για το domain-θύμα, και θα χρησιμοποιήσει μία προσέγγιση σταθμισμένου μέσου όρου (όπως περιγράφεται στην εργασία [110] για ομότιμα δίκτυα) ώστε να αποκτήσει μία πρώτη άποψη για την φήμη της περιοχής του θύματος.

7.3.2 Διάδοση και ανάλυση αναφορών κατανεμημένων επιθέσεων

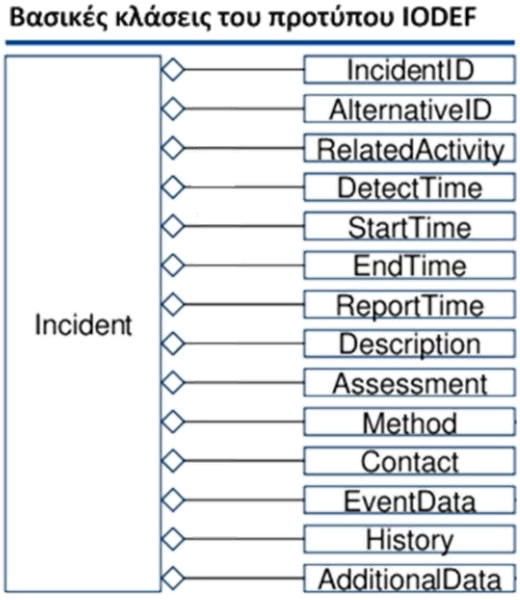
Οι διαμορφωμένες κατά IODEF αναφορές επιθέσεων δημιουργούνται αρχικά από το σύστημα Incident Reports Handler (IRH) της εφαρμογής CAMM στο SDN domain του θύματος. Θεωρείται πως έχει προηγηθεί η ανίχνευση της επίθεσης DDoS και η αναγνώριση των κακόβουλων πηγών μέσω ενός Συστήματος Ανίχνευσης Εισβολών (IDS). Βάσει της λίστας των κακόβουλων πηγών, το IRH ζητά από εφαρμογές του SDN Controller όλες τις πληροφορίες οι οποίες είναι απαραίτητες προκειμένου να αναγνωριστεί το άμεσα γειτονικό SDN domain το οποίο εξυπηρετεί κάθε μία από τις κακόβουλες ροές. Στη συγκεκριμένη υλοποίηση, χρησιμοποιήθηκαν οι εξής εφαρμογές του OpenDaylight (ODL) Controller: (α) Topology Manager για την αναγνώριση της συνολικής τοπολογίας του SDN domain, και (β) Statistics Manager για την παρακολούθηση μετρητών οι οποίοι συνοδεύουν τις ροές στους πίνακες των μεταγωγέων OF οι οποίοι βρίσκονται στα άκρα του domain.

Το IRH της περιοχής του θύματος, χρησιμοποιώντας τις πληροφορίες που συγκεντρώνει μέσω των παραπάνω εφαρμογών, δημιουργεί για κάθε γειτονικό SDN domain μία συγκεκριμένη αναφορά σχετικά με την κατανεμημένη επίθεση, απαριθμώντας τις κακόβουλες ροές δεδομένων τις οποίες αυτό εξυπηρετεί. Εν συνεχεία, το IRP δημοσιεύει τις αναφορές αυτές αναθέτοντας σε κάθε μία ένα συγκεκριμένο URI και διαθέτοντάς την μέσω του RESTful API.

Τα γειτονικά SDN domains, μέσω των δικών τους IRH, λαμβάνουν την αναφορά επίθεσης που τα αφορά καλώντας το URI που αντιστοιχεί στην κάθε αναφορά. Κατόπιν λήψης μίας αναφοράς επίθεσης διαμορφωμένης κατά IODEF, το IRH προσπελαύνει την αναφορά αυτή και μεταφέρει τη μεταφέρει στη μονάδα CMM ως ένα νέο αίτημα συνδρομής στην αντιμετώπιση μίας κατανεμημένης επίθεσης.

Το στοιχείο IRH υλοποιήθηκε επεκτείνοντας την πρόσθετη εφαρμογή SDNi Aggregator του ODL Controller, η οποία αποτελεί τμήμα της εφαρμογής ODL-SDNi [104]. Η αρχική υλοποίηση του πρωτοκόλλου SDNi προδιαγράφει τη διαδικασία ανταλλαγής μηνυμάτων (π.χ. τοπολογίας και συντονισμένης προώθησης ροών) μεταξύ SDN domains στο ίδιο Αυτόνομο Σύστημα (intra-AS) που ελέγχονται από ομότιμους (peer) SDN Controllers. Στα πλαίσια του προτεινόμενου μηχανισμού, επεκτάθηκε το SDNi ώστε να καλύπτει την ανταλλαγή μηνυμάτων μεταξύ SDN domains τα οποία ελέγχονται από ανεξάρτητες διαχειριστικές αρχές (Autonomous Systems). Σημαντικό μέρος της εν λόγω επέκτασης αφορά στην προσθήκη του προαναφερθέντος μηχανισμού φήμης, ώστε να είναι εφικτή η δημιουργία και διατήρηση σχέσεων εμπιστοσύνης μεταξύ των γειτονικών SDN domains.

Για την τυποποίηση των αναφορών επιθέσεων υιοθετήθηκε η διαμόρφωση κατά τα πρότυπα του IODEF, μιας και αυτή η μέθοδος περιγραφής XML είναι κατανοητή στον άνθρωπο (διαχειριστή) αλλά και εύκολα προσπελάσιμη από λογισμικό (Σχήμα 28). Στο πεδίο *EventData* της IODEF αναφοράς συμπεριλαμβάνονται οι κακόβουλες διευθύνσεις IP πηγής οι οποίες εξυπηρετούνται από το SDN domain στο οποίο απευθύνεται η κάθε αναφορά. Η λίστα αυτή ανανεώνεται κάθε φορά που η αναφορά αυτή προωθείται ένα βήμα πιο κοντά στις πηγές τις επίθεσης. Κατά την προώθηση της αναφοράς από ένα ενδιάμεσο SDN domain σε κάποιο άλλο, συμπεριλαμβάνεται στο πεδίο *History* το επίπεδο φήμης του SDN domain του θύματος. Τέλος, στα πεδία *IncidentID* και *AlternativeID* διατηρούνται τα URIs που αντιστοιχούν στην τρέχουσα αναφορά της επίθεσης (όταν ένα ενδιάμεσο domain την αποστέλλει σε κάποιο άλλο), αλλά και στην αρχική αναφορά της που δημιουργήθηκε από το SDN domain του θύματος. Με τον τρόπο αυτό διαπιστώνεται αν υπάρχουν (κακόβουλες ή μη) παραποιήσεις στο σύνολο των ροών το οποίο ζητείται να αποκοπεί.



Σχήμα 28: Σχηματική απεικόνιση των κυριότερων κλάσεων του προτύπου IODEF

7.3.3 Συνδυασμός BGP και SDNi για την διάδοση αναφορών επιθέσεων DDoS

Η μονάδα BGP Speaker επιτρέπει σε ένα SDN domain να αιτείται τη συνδρομή ενός γειτονικού domain για την αντιμετώπιση μιας επίθεσης τύπου DDoS. Τέτοιες αιτήσεις μεταφέρονται με χρήση του πρωτοκόλλου SDNi πάνω από συνόδους BGP. Προκειμένου να υποστηρίζεται αυτή η λειτουργικότητα, επεκτάθηκε το στοιχείο SDNi Wrapper της

εφαρμογής ODL-SDNi. Η αρχική λειτουργικότητα που προσέφερε το SDNi Wrapper αφορούσε: (α) την αρχικοποίηση μίας συνόδου BGP μεταξύ των γειτονικών domains μέσω ενός μηνύματος BGP τύπου *OPEN*, και στη συνέχεια (β) την σειριοποίηση ή προσπέλαση αιτημάτων για ανταλλαγή πληροφορίας μεταξύ γειτονικών SDN domains όπως έχει προαναφερθεί. Η επέκταση του SDNi Wrapper αφορούσε στην προσθήκη του *Content-URI Address Family* [111] ως *BGP Capability*. Έτσι, οι ODL μπορούν να ανταλλάσουν μηνύματα τύπου *BGP UPDATE*, στα οποία να συμπεριλαμβάνεται και ο τύπος πεδίου *Content-URI* στο πεδίο *Network Layer Reachability Information (NLRI)* [112]. Τα πεδία τύπου *Content-URI* περιλαμβάνουν το URI το οποίο παραπέμπει στην αντίστοιχη IODEF αναφορά, επιτρέποντας έτσι την έμμεση ανταλλαγή μηνυμάτων IODEF μεταξύ γειτονικών domains.

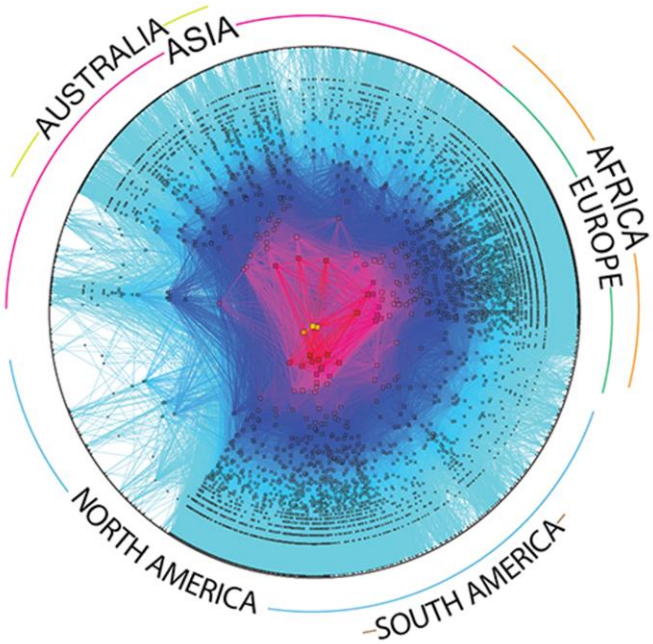
Απαραίτητη προϋπόθεση για τη λειτουργία του BGP Speaker είναι η αναγνώριση των μηνυμάτων SDNi BGP μεταξύ των πακέτων σηματοδοσίας που ανταλλάσσονται κατά τη διάρκεια μίας συνόδου BGP. Στην υλοποίηση της εργασίας αυτής, τα πακέτα SDNi αναγνωρίζονται εφόσον σε ένα μήνυμα *BGP UPDATE* είναι κενά τα πεδία *Withdrawn Routes* και *Path Attribute*. Για τα πακέτα SDNi, το URI που βρίσκεται στο πεδίο NLRI, μεταφέρεται στη μονάδα Incident Manager.

7.4 Αξιολόγηση Προτεινόμενης Προσέγγισης

Για τις ανάγκες υλοποίησης και αξιολόγησης του πρωτότυπου μηχανισμού, οι προαναφερθείσες επεκτάσεις υλοποιήθηκαν σε γλώσσα Java για την πλατφόρμα OpenDaylight (ODL). Η απόδειξη της λειτουργικότητας (proof of concept) του μηχανισμού CAMM πραγματοποιήθηκε σε εργαστηριακό περιβάλλον δοκιμών (testbed) αποτελούμενο από τρία SDN domains, στο οποίο εισήχθη κανονική και κακόβουλη κίνηση τύπου DDoS προς προκαθορισμένο θύμα. Η κανονική κίνηση προερχόταν από την αναπαραγωγή καταγεγραμμένων δειγμάτων κίνησης από το δίκτυο του Ε.Μ.Π. Οι κακόβουλες ροές αναπαράχθηκαν από σύνολο δεδομένων του Center for Applied Internet Data Analysis (CAIDA) και αναγνωρίστηκαν μέσω του μηχανισμού ανίχνευσης και αναγνώρισης δικτυακών ανωμαλιών που περιγράφεται στο Κεφάλαιο 6, και αντιμετωπίστηκαν μέσω του προτεινόμενου μηχανισμού CAMM.

Στη συνέχεια ελέγχθηκε η αποτελεσματικότητα του προτεινόμενου συνεργατικού μοντέλου, μέσω πειραμάτων προσομοίωσης τοπολογιών μεγάλης κλίμακας. Για τα συγκεκριμένα πειράματα χρησιμοποιήθηκε εργαστηριακή υποδομή βασισμένη σε τέσσερις

υπολογιστικές μονάδες, ενώ για τη προσομοίωση σύνθετων τοπολογιών του σύγχρονου Internet χρησιμοποιήθηκαν σύνολα δεδομένων τα οποία παρείχε το CAIDA. Συγκεκριμένα, για την προσομοίωση πραγματικών τοπολογιών σε επίπεδο Αυτόνομων Συστημάτων, χρησιμοποιήθηκαν οι γράφοι του AS Relationships Dataset [113]. Το συγκεκριμένο Dataset απεικονίζεται στο σύνολό του, στο Σχήμα 29.



Σχήμα 29: Σχηματική απεικόνιση υψηλού επιπέδου της συλλογής δεδομένων CAIDA AS Relationships Dataset, από όπου αντλήθηκαν δεδομένα για την προσομοίωση τοπολογιών μεγάλης κλίμακας.
Πηγή: [112] http://www.caida.org/research/topology/as_core_network/pics/2014

Στα πειράματα που πραγματοποιήθηκαν, χρησιμοποιήθηκαν υποσύνολα του ανωτέρω Dataset τα οποία περιείχαν δέντρα όπου ρίζα ήταν το Αυτόνομο Σύστημα το οποίο φιλοξενούσε το θύμα, ενώ φύλλα ήταν τα Αυτόνομα Συστήματα τα οποία φιλοξενούσαν τις πηγές της επίθεσης. Σε κάθε πείραμα προσομοιώθηκαν τοπολογίες οι οποίες αποτελούνταν κατά μέσο όρο από 10.000 Αυτόνομα Συστήματα. Ακόμη, οι υπο-γράφοι του Dataset οι οποίοι επιλέχθηκαν κάθε φορά ικανοποιούσαν τις ακόλουθες απαιτήσεις: (α) δημιουργήθηκαν με βάση έγκυρες ιεραρχικές σχέσεις όπως αυτές ορίζονται στην εργασία [114], και (β) η απόσταση από το Αυτόνομο Σύστημα του θύματος μέχρι οποιαδήποτε κακόβουλη πηγή δεν ήταν μεγαλύτερη από 6 Αυτόνομα Συστήματα (η απόσταση αυτή ικανοποιείται από το 95% των Αυτόνομων Συστημάτων του σημερινού Internet [115]).

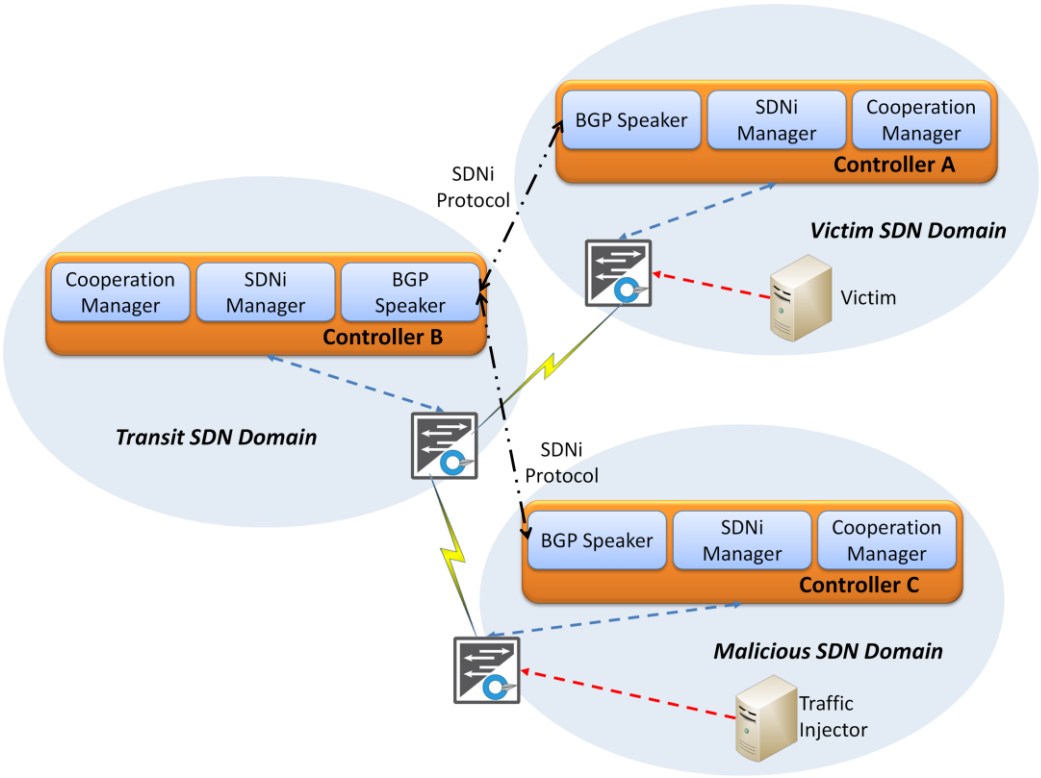
Δεδομένα επιθέσεων DDoS αναπαράχθηκαν από το CAIDA DDoS Attack 2007 Dataset, το οποίο όπως αναλύθηκε και στο Κεφάλαιο 6 περιέχει 9.312 μοναδικές κακόβουλες πηγές, προερχόμενες από 4.186 /16 δίκτυα. Η κίνηση αυτή συνδυάστηκε με

καταγεγραμμένη και ανωνυμοποιημένη κίνηση από το τοπικό δίκτυο του Ε.Μ.Π. Κατά τη διάρκεια των πειραμάτων θεωρήθηκε ότι οι τρέχουσες τοπολογίες IPv4 θα προσομοιάζουν με αυτόνομες περιοχές SDN. Κατά συνέπεια, θεωρήθηκε ότι τα 4186 δίκτυα του DDoS Dataset αντιστοιχούν σε 4186 ξεχωριστά Αυτόνομα Συστήματα τα οποία τα οποία αποτελούν τα φύλλα των γράφων που χρησιμοποιήθηκαν στην πειραματική διαδικασία.

7.4.1 Αξιολόγηση σε περιβάλλον περιορισμένης κλίμακας

Το εργαστηριακό περιβάλλον δοκιμών για το proof of concept αποτελείται από τα ακόλουθα τρία SDN domains, όπως φαίνεται και στο Σχήμα 30:

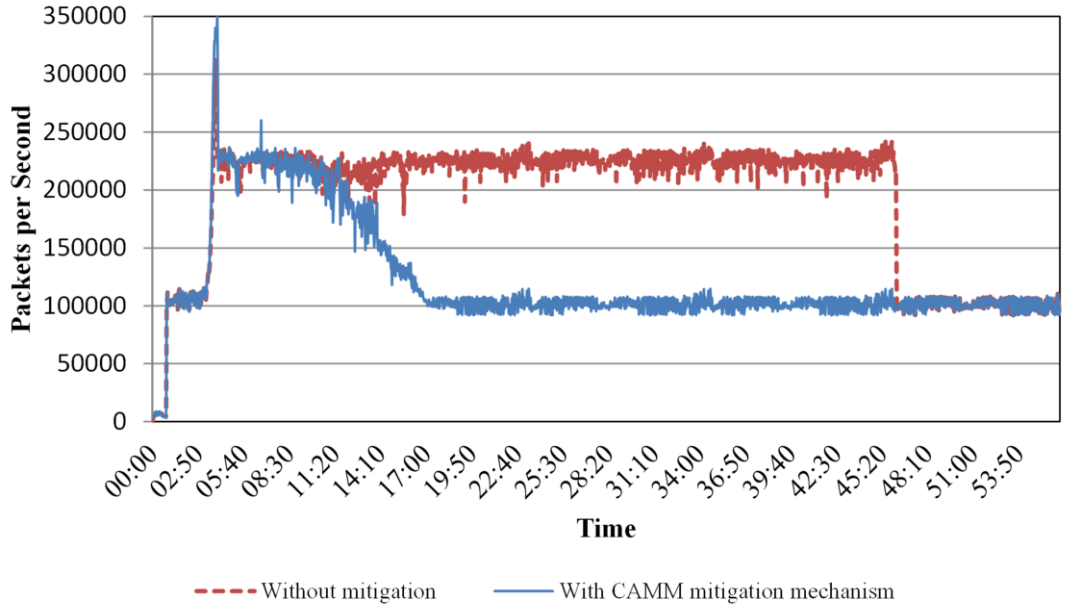
- **Victim SDN Domain (VSD):** Το SDN domain το οποίο φιλοξενεί το θύμα της επίθεσης.
- **Transit SDN Domain (TSD):** Ενδιάμεσο SDN domain, το οποίο εν αγνοία του εξυπηρετεί κακόβουλες ροές δεδομένων και τις προωθεί προς το θύμα της επίθεσης.
- **Malicious SDN Domain (MSD):** Το SDN domain το οποίο συνήθως εν αγνοία του, και λόγω πλημμελούς εσωτερικής διαχείρισης, φιλοξενεί μολυσμένες υπολογιστικές μονάδες οι οποίες λειτουργούν ως γεννήτριες κακόβουλης κίνησης.



Σχήμα 30: Πρώτο σενάριο αξιολόγησης συνεργατικού μηχανισμού: αντιμετώπιση κατανεμημένης επίθεσης από δύο γειτονικά SDN domain.

Κάθε ένας από τους παραπάνω δικτυακούς τομείς έχει έναν μεταγωγέα OpenFlow στο άκρο του, ο οποίος προωθεί την κίνηση προς τις γειτονικές δικτυακές περιοχές. Οι μεταγωγείς ελέγχονται από ODL Controllers (ένας σε κάθε domain) στους οποίους έχει εγκατασταθεί η πρότυπη έκδοση της προτεινόμενης εφαρμογής CAMM. Παράλληλα, οι μονάδες BGP Speaker των προσκείμενων SDN domains αποτελούν BGP peers ώστε να είναι δυνατή η ανταλλαγή SDNi μηνυμάτων. Η υπολογιστική μονάδα που φαίνεται στο domain MSD στο Σχήμα 30 είναι υπεύθυνη για την αναπαραγωγή κακόβουλης και καλοήθους κίνησης, η οποία σταδιακά θα φτάσει μέχρι το θύμα. Μία ακόμη υπολογιστική μονάδα έχει τοποθετηθεί στο domain VSD, σαν στόχος της επίθεσης για τους σκοπούς του πειράματος. Το τρίτο domain (TSD) είναι απλά ένα ενδιάμεσο SDN domain, και εν αγνοία του προωθεί την κίνηση από την πηγή (MSD) προς το θύμα (VSD).

Στο Σχήμα 31 φαίνεται ο αριθμός των πακέτων που φτάνουν ανά δευτερόλεπτο στο θύμα της επίθεσης. Στα πρώτα πέντε λεπτά υπάρχει μόνο καλοήθης κίνηση η οποία αντιστοιχεί σε περίπου 100.000 πακέτα το δευτερόλεπτο. Στη συνέχεια εισάγεται και η κακόβουλη κίνηση, οπότε η μέση ροή πακέτων που φτάνουν στο θύμα ανέρχεται σε 220.000 πακέτα ανά δευτερόλεπτο. Η κόκκινη διακεκομμένη γραμμή στο Σχήμα 31 αντιπροσωπεύει τον αριθμό πακέτων ανά δευτερόλεπτο που φτάνουν στο θύμα κατά τη διάρκεια της επίθεσης, αν δεν λειτουργούσε η εφαρμογή CAMM. Η συνεχής μπλε γραμμή δείχνει το αποτέλεσμα του προτεινόμενου μηχανισμού αποκοπής κατανεμημένων επιθέσεων.



Σχήμα 31: Αριθμός άφιξης πακέτων ανά δευτερόλεπτο στο θύμα, κατά τη διάρκεια της κατανεμημένης επίθεσης.

Στο domain VSD εγκαταστάθηκε ο μηχανισμός ανίχνευσης ανωμαλιών που περιγράφηκε στην προηγούμενη ενότητα. Μέσω αυτού αναγνωρίστηκαν σύνολα κακόβουλων διευθύνσεων IP πηγής σε επαναλαμβανόμενα χρονικά παράθυρα των 30 δευτερολέπτων. Στη συνέχεια τα σύνολα αυτά προωθήθηκαν στην εφαρμογή CAMM, από όπου μεταδόθηκαν ως αναφορές επίθεσης προς τους τομείς TSD και MSD ώστε να αποκοπούν οι αντίστοιχες ροές πακέτων.

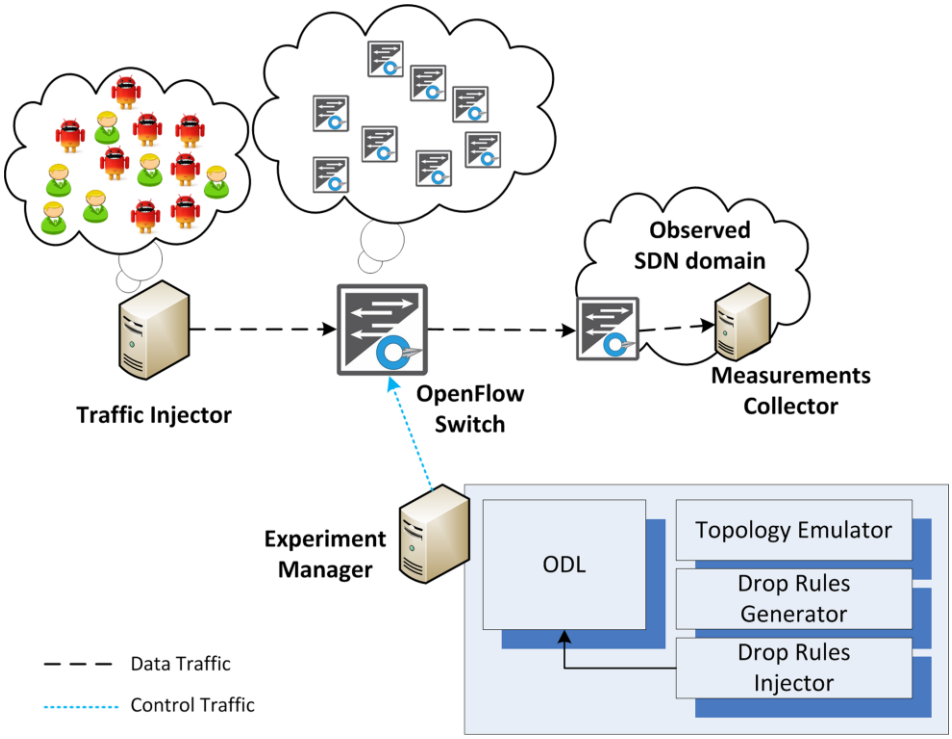
Το πείραμα έδειξε πως ο συνεργατικός μηχανισμός CAMM πέτυχε στον περιορισμό της κακόβουλης κίνησης με σταδιακή αποκοπή κακόβουλων ροών λόγω της συνεχιζόμενης εμφάνισης ή επανεμφάνισης κακόβουλων πηγών μεταξύ διαδοχικών περιόδων μέτρησης (30 sec). Η αποκοπή ολοκληρώθηκε σε 18 min (ενώ η διάρκεια της επίθεσης ήταν 60 min) με την πλήρη καταγραφή και περιορισμό όλων των κακόβουλων πηγών του dataset.

7.4.2 Υλοποίηση περιβάλλοντος προσομοίωσης και πειράματα μεγάλης κλίμακας

Η προαναφερθείσα πειραματική τοπολογία δεν ήταν δυνατό να υποστηρίξει πειραματισμούς μεγάλης κλίμακας με μεγάλο αριθμό δικτυακών περιοχών και αντίστοιχων SDN Controllers. Για το λόγο αυτό ομαδοποιήθηκαν οι απαιτούμενες δικτυακές συσκευές σε διασυνδεδεμένες λογικές μονάδες. Συγκεκριμένα, ο πειραματισμός για περιβάλλοντα μεγάλης κλίμακας στηρίχθηκε στην υλοποίηση τεσσάρων πραγματικών μονάδων για την εικονικοποίηση των απαιτούμενων δικτυακών λειτουργιών, όπως φαίνεται στο Σχήμα 32:

α) OpenFlow Switch: Η συσκευή αυτή αντανακλά το σύνολο των μεταγωγέων OF οι οποίοι βρίσκονται στα άκρα όλων των προσομοιωμένων ευφυών δικτυακών περιοχών (SDN domains). Στον μεταγωγέα καταφθάνει δικτυακή κίνηση η οποία προκύπτει από την αναπαραγωγή των αντίστοιχων συνόλων δεδομένων της CAIDA και του Ε.Μ.Π. Τα πακέτα είτε θα προωθηθούν προς το θύμα της επίθεσης (*Victim SDN Domain*), ή θα αποκοπούν βάσει οδηγιών που θα λάβει ο μεταγωγέας OF από τον ODL Controller της μονάδας *Experiment Manager*.

β) Experiment Manager: Η μονάδα αυτή απλοποιεί την διαδικασία πειραματισμού μεγάλης κλίμακας, επιτρέποντας την προσομοίωση τοπολογιών (και συμπεριφοράς) χιλιάδων Αυτόνομων Συστημάτων, τα οποία εξάγονται από το CAIDA AS Relationship Dataset. Η μονάδα Experiment Manager για κάθε SDN domain προσομοιώνει τον μηχανισμό ο οποίος προσφέρει στους αντίστοιχους μεταγωγείς OF την ευφυΐα για την προώθηση πακέτων. Αυτό το πετυχαίνει χάρις στον ODL Controller τον οποίο



Σχήμα 32: Δεύτερο σενάριο αξιολόγησης συνεργατικού μηχανισμού: εξομοίωση συνεργατικής αντιμετώπισης κατανεμημένων επιθέσεων σε τοπολογίες μεγάλης κλίμακας, αποτελούμενες από χιλιάδες SDN domains.

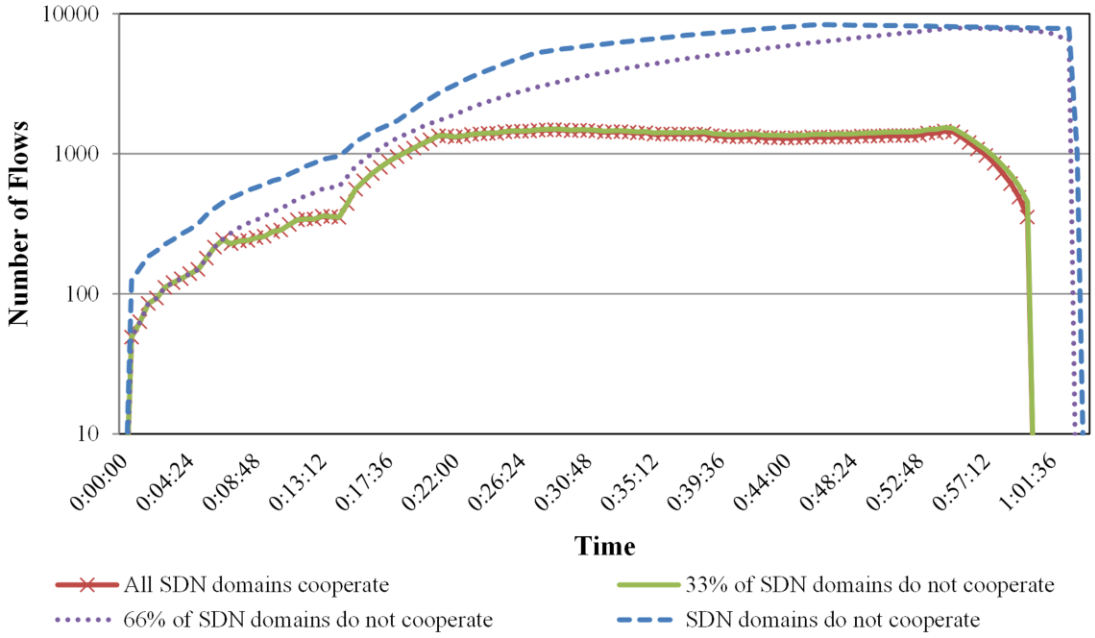
χρησιμοποιεί, και μέσω του οποίου εισάγει στην μονάδα *OpenFlow Switch* (Σχήμα 32) κατάλληλες εγγραφές για την αποκοπή κακόβουλων ροών (τον ODL Controller καθοδηγεί η υπομονάδα *Drop Rules Injector*). Ένας ακόμη ρόλος της μονάδας *Experiment Manager* είναι η επιλογή κατάλληλων υπο-γράφων (δένδρων) από το σύνολο δεδομένων CAIDA AS Relationships Dataset, και η ανάθεση σε κάθε φύλλο του δένδρου ενός IP προθέματος /16 από τα προθέματα τα οποία εμφανίζονται στο CAIDA DDoS Attack 2007 Dataset. Επιπλέον, για κάθε SDN domain, η μονάδα αυτή υπολογίζει και καταγράφει το επίπεδο φήμης των υπόλοιπων SDN domains, αναλαμβάνοντας επί της ουσίας τον ρόλο του Cooperation Manager για κάθε εξομοιωμένο SDN domain. Έτσι, η υπομονάδα *Drop Rules Generator* λαμβάνει αποφάσεις σχετικά με το ποιες κακόβουλες ροές θα αποκοπούν και πότε, με βάση το επίπεδο φήμης SDN domains που υλοποιούν τον μηχανισμό CAMM.

γ) Traffic Injector: Η μονάδα αυτή δέχεται ως είσοδο τα καταγεγραμμένα σύνολα δεδομένων της CAIDA και του Ε.Μ.Π. και τα αναπαράγει μέσω του εργαλείου Tcpreplay και την μεταδίδει στη μονάδα OpenFlow Switch.

δ) Observed SDN Domain: Η μονάδα αυτή αντιπροσωπεύει το υπό-παρακολούθηση SDN domain του θύματος, όπου συλλέγονται οι μετρήσεις μέσω της υπομονάδας

Measurements Collector (αριθμός πακέτων που φθάνουν στο συγκεκριμένο SDN domain ανά δευτερόλεπτο και αριθμός νέων OpenFlow ροών δεδομένων οι οποίες εγκαθίστανται στον συνοριακό μεταγωγέα OF του domain ανά δευτερόλεπτο).

Στο Σχήμα 33 απεικονίζονται πειραματικά αποτελέσματα τα οποία επιβεβαιώνουν την αποτελεσματικότητα της εφαρμογής CAMM, και αφορούν τον απαιτούμενο αριθμό κανόνων OpenFlow στον συνοριακό μεταγωγέα OF του θύματος (*Observed SDN Domain*) προκειμένου να αποκοπεί το σύνολο των κακόβουλων ροών της επίθεσης DDoS. Για τις ανάγκες του συγκεκριμένου πειράματος περιορίστηκε ο αριθμός κανόνων που μπορούσε να διαθέσει το κάθε ενδιάμεσο SDN domain σε 500 εγγραφές. Ο περιορισμός αυτός προκύπτει από το γεγονός ότι ένας μεταγωγέας OF που διαθέτει 4.000 εγγραφές συνολικά (όπως μεταγωγείς μεσαίας κλίμακας υλοποιημένοι σε φυσικό εξοπλισμό π.χ. HP-5406 [116]), θα χρησιμοποιήσει το μεγαλύτερο μέρος των διαθέσιμων εγγραφών για τις ανάγκες προώθησης της καλοήθους κίνησης.



Σχήμα 33: Αριθμός εγγραφών στον συνοριακό μεταγωγέα Openflow του SDN domain που εξυπηρετεί το θύμα μίας επίθεσης DDoS, ανάλογα με το ποσοστό των γειτονικών SDN domains που συνεισφέρουν στην αντιμετώπιση της επίθεσης αυτής.

Υλοποιήθηκαν τέσσερα σενάρια ανάλογα με το ποσοστό συνεργατικότητας των ενδιάμεσων SDN domains, δηλαδή την εκ των προτέρων ορισμένη διαθεσιμότητα των περιοχών αυτών για συμμετοχή στην συνεργατική διαδικασία. Όπως φαίνεται στο Σχήμα 33, στην περίπτωση όπου είναι διαθέσιμοι για συνεργασία όλοι οι ενδιάμεσοι δικτυακοί τομείς κατά μήκος των μονοπατιών της επίθεσης, το SDN domain του θύματος χρειάζεται

περίπου 81% λιγότερους κανόνες σε σύγκριση με την περίπτωση που πρέπει με δικούς του πόρους να αποκόψει το σύνολο της κακόβουλης κίνησης. Αντίστοιχα πειράματα διεξήχθησαν για ποσοστά μη συνεργατικών περιοχών 33% και 66%, όπου παρατηρήθηκε μείωση 80% και 30% αντίστοιχα, σε σχέση με την περίπτωση μη συνεργασίας. Σημειώνεται ότι, για λόγους ρεαλισμού και εξαιτίας της περιοδικής επανεμφάνισης συγκεκριμένων ροών δεδομένων στο σύνολο δεδομένων DDoS, οι κανόνες οι οποίοι εγκαταστάθηκαν είχαν ορισμένη την παράμετρο *idle-timeout* στα 300 δευτερόλεπτα, όπως είναι και η συνήθης πρακτική για Reflexive Access Lists [117].

Τέλος, διενεργήθηκε μία ακόμη πειραματική διαδικασία, προκειμένου να αξιολογηθούν τα οφέλη που προκύπτουν για τα ενδιάμεσα SDN domains από τον μηχανισμού φήμης για γειτονικούς τομείς. Όπως αναφέρθηκε και στην ανάλυση του συγκεκριμένου μηχανισμού σε προηγούμενη ενότητα, κάθε SDN domain αποτιμά το επίπεδο συνεργατικότητας των γειτονικών του SDN domains μέσου του μηχανισμού CAMM. Έτσι, ένα domain θα αποφύγει να αφιερώσει δικούς του πόρους για την αντιμετώπιση μίας επίθεσης DDoS, εφόσον το θύμα της επίθεσης εξυπηρετείται από ένα SDN domain το οποίο στο παρελθόν έχει επιδείξει έλλειψη συνεργατικότητας. Για τις ανάγκες του συγκεκριμένου πειράματος, αναπαράχθηκαν πολλαπλές διαδοχικές επιθέσεις DDoS. Η απόδοση μετρήθηκε σε ενδιάμεσο Observed SDN domain και όχι στην περιοχή του θύματος. Ακόμη, ορίστηκε ότι το 33% του συνόλου των SDN domains δεν θα συμμετείχε στη διαδικασία αποκοπής των επιθέσεων. Με την ολοκλήρωση του πειράματος, παρατηρήθηκε ότι το επιλεγμένο ενδιάμεσο SDN domain αφιέρωσε 42% λιγότερες εγγραφές για την αποκοπή τμημάτων των επιθέσεων. Η μείωση αυτή επιτεύχθηκε αποφεύγοντας την δημιουργία νέων εγγραφών για τον περιορισμό κακόβουλων ροών που επηρέαζαν τομείς οι οποίοι δεν συμμετείχαν στην αντιμετώπιση προηγούμενων επιθέσεων και άρα είχαν πολύ χαμηλό επίπεδο φήμης. Αξίζει να σημειωθεί ότι παρά τη σημαντική μείωση των εγγραφών από μέρους του συγκεκριμένου ενδιάμεσου SDN domain, το επίπεδο συνεργατικότητάς του (και επομένως η φήμη του) παρέμεινε υψηλή απέναντι στα υπόλοιπα συνεργατικά υψηλής φήμης SDN domains.

8 Συμπεράσματα - Μελλοντική Έρευνα

Στο κεφάλαιο αυτό συνοψίζουμε τα αποτελέσματα και την προσφορά της διατριβής στον τομέα της ανίχνευσης και αντιμετώπισης ανωμαλιών δικτύου, τόσο σε παραδοσιακά, όσο και σε ευφυή προγραμματιζόμενα δίκτυα SDN. Επίσης γίνεται αναφορά σε θέματα μελλοντικής εργασίας και επέκτασης των ερευνητικών αποτελεσμάτων της διατριβής που παρουσιάζουν ιδιαίτερο πρακτικό και ερευνητικό ενδιαφέρον.

8.1 Συμπεράσματα

Στην παρούσα διδακτορική διατριβή μελετήθηκαν πλεονεκτήματα τα οποία μπορεί να προσφέρει η προγραμματιστική παραμετροποίηση των δικτυακών συσκευών μέσω του πρωτοκόλλου OpenFlow, εστιάζοντας στην αντιμετώπιση δικτυακών επιθέσεων, και τον περιορισμό των επιπτώσεών τους στην γενικότερη υποδομή μίας δικτυακής περιοχής. Οι κρατούσες πρότερες ερευνητικές-αναπτυξιακές προσπάθειες εστίαζαν είτε στην ενσωμάτωση παραδοσιακών συστημάτων ανίχνευσης και αποτροπής δικτυακών εισβολών (IDS/IPS) σε δίκτυα SDN, ή στην υιοθέτηση αλγορίθμων σχεδιασμένων για παραδοσιακά δίκτυα προκειμένου να ανιχνεύονται δικτυακές ανωμαλίες. Οι προσεγγίσεις αυτές παρουσιάζουν ενδιαφέρον και η λειτουργία τους μπορεί να θεωρηθεί αξιόπιστη λόγω της εκτεταμένης χρήσης τους στα παραδοσιακά δίκτυα. Εντούτοις δεν επαρκούν για την καταπολέμηση των σύγχρονων κατανεμημένων δικτυακών επιθέσεων, οι οποίες συνήθως προκαλούνται από χιλιάδες ανεξάρτητες πηγές, ενώ χαρακτηρίζονται από μεταφορά τεράστιου όγκου δεδομένων, κάτι το οποίο επηρεάζει όχι μόνο το θύμα της επίθεσης, αλλά και τη συνολική δικτυακή υποδομή την οποία διατρέχουν. Ειδικότερα, επιθέσεις τύπου DDoS είναι δυνατόν να οδηγήσουν στην πλημμύρα του ίδιου του Επιπέδου Ελέγχου των δικτυακών υπηρεσιών σε περίπτωση που ο σχεδιασμός δεν συμπεριλαμβάνει την υιοθέτηση απαιτητικών λύσεων (συνήθως κλειστών και υψηλού κόστους) για τη συλλογή στατιστικών δεδομένων και την αποτελεσματική προστασία των δικτυακών υποδομών και υπηρεσιών.

Με την υιοθέτηση λύσεων SDN δίνεται πλέον η δυνατότητα για αναλυτική επεξεργασία ροών δεδομένων σε πολλαπλά επίπεδα πρωτοκόλλων, με αντίστοιχες λειτουργίες προώθησης πακέτων. Η ευφυΐα συγκεντρώνεται έξω από το Επίπεδο Προώθησης Δεδομένων σε SDN Controllers οι οποίοι ελέγχουν τους μεταγωγείς ενώ εκθέτουν τις λειτουργίες Επιπέδου Ελέγχου σε διαχειριστικές οντότητες μέσω ανοιχτών

προγραμματιστικών διεπαφών (APIs). Τα ανωτέρω χαρακτηριστικά επιτρέπουν την αποτελεσματική ευφυή αντιμετώπιση απειλών τόσο στην ανίχνευση ανωμαλιών, όσο και στην αντιμετώπισή τους. Οι προτεινόμενες λύσεις στην παρούσα διατριβή αφορούν στις δυνατότητες που διανοίγονται μέσω πρωτοκόλλων SDN (π.χ. OpenFlow), για την προστασία παραδοσιακών δικτυακών υποδομών από δικτυακές επιθέσεις τύπου DDoS, αλλά και την εφαρμογή τους σε αμιγώς SDN περιβάλλοντα. Να τονιστεί πάντως, πως το κεντρικοποιημένο Επίπεδο Ελέγχου που χαρακτηρίζει τις υποδομές SDN μπορεί να αποτελέσει στόχο επιθέσεων και επομένως οι εξωτερικοί SDN Controllers χρήζουν ιδιαίτερης προστασίας.

Αρχικά, στα πλαίσια της συγκεκριμένης διατριβής, έγινε αξιολόγηση της εγγενούς μεθόδου του πρωτοκόλλου OpenFlow (έκδοση 1.0) όσον αφορά στη συλλογή στατιστικών δεδομένων των δικτυακών ροών, και τη χρήση αυτών για την ανίχνευση ανωμαλιών σε περιβάλλοντα SDN. Η μελέτη έδειξε ότι δεν είναι κλιμακώσιμη η περιοδική εξαγωγή -από τους πίνακες ροών των μεταγωγέων OpenFlow- στατιστικών δεδομένων για τις δικτυακές ροές, ιδιαίτερα σε περιβάλλοντα τα οποία εξυπηρετούν μεγάλους όγκους δικτυακής κίνησης. Επιπλέον, η μέθοδος αυτή, σε περίπτωση επιθέσεων τύπου DDoS, μπορεί να οδηγήσει σε φαινόμενα τύπου DoS για το Επίπεδο Ελέγχου της υποδομής. Έτσι, προτάθηκε μία συνδυαστική προσέγγιση για την προστασία από δικτυακές ανωμαλίες, η οποία περιλαμβάνει: (α) δειγματοληπτική συλλογή στατιστικών δεδομένων βάσει του πρωτοκόλλου sFlow, (β) ανίχνευση δικτυακών επιθέσεων τύπου DDoS, Port Scanning και Worm Propagation, μέσω μίας μεθόδου η οποία βασίζεται στη μεταβολή της εντροπίας συγκεκριμένων πεδίων των επικεφαλίδων των πακέτων, και (γ) καθολική αποκοπή της κίνησης η οποία σχετίζεται με τις ανιχνευθείσες ανωμαλίες, προγραμματιστικά, μέσω του πρωτοκόλλου OpenFlow.

Ο μηχανισμός αυτός αποπλέκει τη διαδικασία συλλογής δεδομένων από την πληροφορία η οποία διατηρείται στους πίνακες προώθησης των μεταγωγέων OpenFlow, ενώ μειώνει τις ανάγκες ανταλλαγής σηματοδοσίας μεταξύ μεταγωγέων και OpenFlow Controller. Πειραματικές μετρήσεις στα πλαίσια της διατριβής έδειξαν ότι η ακρίβεια στην ανίχνευση ανωμαλιών με την προτεινόμενη δειγματοληπτική μέθοδος μπορεί να είναι συγκρίσιμη, σε περιβάλλοντα χαμηλής δικτυακής κίνησης, με την μέθοδο που προσφέρει εγγενώς το πρωτόκολλο OpenFlow. Επιπλέον, σε περιβάλλοντα υψηλής δικτυακής κίνησης η μέθοδος περιοδικών αιτημάτων συλλογής στατιστικών δεδομένων μέσω OF δεν είναι εφικτή λόγω υπερβολικής κατανάλωσης πόρων του Controller. Η εγγενής μέτρηση και αντιμετώπιση επιθέσεων μέσω του OF Controller εισάγει μεγάλη πολυπλοκότητα αφενός

μεν λόγω έλλειψης δυνατοτήτων δειγματοληψίας, αφετέρου δε λόγω της διαπλοκής των Επιπέδων Διαχείρισης και Ελέγχου σε κοινούς μηχανισμούς. Αντίθετα παρατηρήθηκε ότι τα δεδομένα που συλλέγονται δειγματοληπτικά σε εξωτερική μονάδα μέσω του πρωτοκόλλου sFlow μπορούν να χρησιμοποιηθούν για την αξιόπιστη ανίχνευση δικτυακών ανωμαλιών.

Για την ενδελεχή αξιολόγηση της προτεινόμενης μεθόδου, ελέγχθηκε η συμπεριφορά του συνολικού μηχανισμού δοκιμάζοντας τη χρήση διαφορετικών αλγορίθμων ανίχνευσης ανωμαλιών (π.χ. TRW-CB). Τα πειραματικά αποτελέσματα έδειξαν ότι η δειγματοληπτική μέθοδος εμφανίζει ανώτερη συμπεριφορά όσον αφορά την κατανάλωση πόρων συστήματος, διατηρώντας παράλληλα την αξιοπιστία των αλγορίθμων ανίχνευσης σε αποδεκτά επίπεδα.

Στη συνέχεια, προτάθηκε και αναλύθηκε η χρήση του OpenFlow για την βελτίωση της μεθόδου Remotely-Triggered Black Holing (RTBH), με στόχο την αντιμετώπιση κατανεμημένων επιθέσεων DDoS σε παραδοσιακά δίκτυα. Συγκεκριμένα, έγινε χρήση των δυνατοτήτων του OpenFlow για προγραμματιστική διαχείριση και προώθηση των ροών δεδομένων. Σε συνδυασμό με τις δυνατότητες αναδρομολόγησης που προσφέρει η μέθοδος RTBH, έγινε δυνατή η μεταφορά χαρακτηριστικών των Εικονικοποιημένων Δικτυακών Λειτουργιών (VNFs) αρχιτεκτονικών NFV σε παραδοσιακά δίκτυα. Ο προτεινόμενος μηχανισμός προσφέρει τη συνολική λειτουργία προώθησης πακέτων που αφορούν το θύμα μίας επίθεσης DDoS, ως ένα VNF υλοποιημένο σε λογισμικό. Η προσέγγιση αυτή είναι ικανή για αντιστοίχιση και διαχείριση της δικτυακής κίνησης σε επίπεδο ροών, εισάγοντας έτσι δυνατότητες επιλεκτικής αποκοπής των κακόβουλων ροών. Ως αποτέλεσμα, μπορεί να αντιμετωπιστεί μία κατανεμημένη επίθεση, ενώ παράλληλα να διατηρηθεί η προσβασιμότητα στην υπηρεσία του θύματος την οποία στόχευε εξαρχής η επίθεση.

Κύριο στοιχείο της συγκεκριμένη προσέγγισης είναι η κλιμακωσιμότητά της, προκειμένου να καθίσταται δυνατή η αντιμετώπιση κατανεμημένων επιθέσεων μεγάλης κλίμακας. Έτσι, υλοποιήθηκε ένας πολυεπίπεδος μηχανισμός για την ανίχνευση και αναγνώριση δικτυακών ανωμαλιών, στοχεύοντας στην μείωση της κατανάλωσης πόρων συστήματος. Επιπλέον, προκειμένου να βελτιωθεί περαιτέρω η δυνατότητα κλιμάκωσης της προτεινόμενης προσέγγισης, υλοποιήθηκε ένας μηχανισμός βασισμένος στην συνάθροιση ροών βάσει των Μέγιστων Κοινών IP Προθεμάτων (Longest Common Prefixes). Ο μηχανισμός αυτός προσέφερε τη δυνατότητα βέλτιστης συνάθροισης των κακόβουλων ροών στους πίνακες προώθησης του μεταγωγέα OpenFlow ο οποίος χρησιμοποιήθηκε ως ενδιάμεσος μηχανισμός για την αποκοπή των ροών αυτών. Η πειραματική διαδικασία έδειξε

ότι λόγω της συνήθους συγκέντρωσης των κακόβουλων πηγών σε συγκεκριμένα προθέματα IP, μέσω του αλγορίθμου συνάθροισης, μπορεί να αποφευχθεί η ανάγκη χρήσης μεταγωγέων OpenFlow υψηλού κόστους, οι πίνακες προώθησης των οποίων χαρακτηρίζονται από αυξημένη χωρητικότητα εγγραφών για ροές δεδομένων.

Τέλος, η διατριβή ολοκληρώνεται με την πρόταση και αξιολόγηση μίας μεθόδου για το σχηματισμό συνεργατικών σχημάτων αποκλειστικά μεταξύ δικτυακών περιοχών SDN οι οποίες βρίσκονται στο μονοπάτι κατανεμημένων δικτυακών επιθέσεων. Στόχος είναι ο διαμοιρασμός της διαδικασίας αποκοπής επιθέσεων DDoS μεταξύ γειτονικών δικτυακών περιοχών SDN, και τελικά η προώθηση της διαδικασίας αυτής όσο το δυνατόν πιο κοντά στις πηγές τους. Εξ' ορισμού, μία τέτοια προσέγγιση περιορίζει τις απαιτήσεις δικτυακών πόρων για την αντιμετώπιση κατανεμημένων επιθέσεων, όσον αφορά το SDN domain που εξυπηρετεί το θύμα της επίθεσης. Η προτεινόμενη προσέγγιση εισάγει ένα μηχανισμό για τη διάδοση αναφορών επιθέσεων, μεταδίδοντας δείκτες URI μέσω σηματοδοσίας BGP. Με τον τρόπο αυτόν, ζητείται από κάθε SDN domain στο μονοπάτι τη επίθεσης να αποκόψει τις κακόβουλες ροές τις οποίες εκείνο εξυπηρετεί. Στην περίπτωση όπου κάποιες δικτυακές περιοχές δεν συνεργαστούν, τότε οι ροές της επίθεσης αποκόπτονται αναγκαστικά από το SDN domain το οποίο εξυπηρετεί το θύμα. Έτσι, προκειμένου να υπάρχει κίνητρο για τη συμμετοχή σε τέτοια συνεργατικά σχήματα, προτείνεται η χρήση ενός μηχανισμού φήμης για την αξιολόγηση της συνεργατικότητας μεταξύ των δικτυακών περιοχών. Τα πειραματικά αποτελέσματα απέδειξαν ότι ένας τέτοιος μηχανισμός θα επιτρέψει τη συμμετοχή ενός SDN domain στην καταπολέμηση μίας κατανεμημένης επίθεσης μόνο στην περίπτωση που η περιοχή του θύματος αναμένεται να εμφανίσει ανταποδοτική συμπεριφορά σε μελλοντικές αντίστοιχες επιθέσεις.

8.2 Θέματα Μελλοντικής Έρευνας

Ενδιαφέρον στοιχείο στην προτεινόμενη μεθοδολογία, όσον αφορά στην αντιμετώπιση επιθέσεων σε παραδοσιακά δίκτυα, αποτελεί η διαδικασία λεπτομερούς ανάλυσης των δικτυακών ροών για την ανίχνευση ύποπτων γεγονότων, και την αναγνώριση του θύματος μίας επίθεσης. Στον τομέα αυτό, χρήζει περαιτέρω έρευνας και πειραματισμού η δυναμική επιλογή και χρήση διαφορετικών αλγορίθμων ως δεύτερο επίπεδο ανίχνευσης ανωμαλιών δικτύου, με βάση τις ενδείξεις που συγκεντρώνονται μέσω του πρώτου επιπέδου, όπως αυτά διαχωρίζονται στο Κεφάλαιο 6. Ένας τέτοιος μηχανισμός αναμένεται να οδηγήσει σε πιο

αξιόπιστα αποτελέσματα, αφού επιλέγοντας κατάλληλους αλγόριθμους κατά περίπτωση, θα μειωθεί το ποσοστό των ψευδώς-αληθών (false-positive) αναφορών, και θα επιτυγχάνεται ακριβέστερη διάκριση μεταξύ κακόβουλων και καλοηθών δικτυακών ανωμαλιών, όπως οι περιπτώσεις DDoS και Flash Crowd.

Επίσης, μια άλλη κατεύθυνση μελλοντικής έρευνας επάνω στο πρόβλημα που μελετά η παρούσα διατριβή, είναι η μελέτη μεθόδων συλλογικής αντιμετώπισης κατανεμημένων επιθέσεων από γειτονικές δικτυακές περιοχές, οι οποίες μπορεί να μην υποστηρίζουν κάποιο πρωτόκολλο SDN, μέσω πρωτοκόλλων διαχείρισης και παραμετροποίησης νέας γενιάς όπως το NETCONF. Μία τέτοια προσέγγιση θα συντελέσει στην διευκόλυνση της μετάβασης από τα παραδοσιακά δίκτυα παραγωγής σε ευφυή προγραμματιζόμενα δίκτυα. Επιπλέον, θα είναι ιδιαίτερα χρήσιμη η μελέτη σεναρίων όπου SDN domains μπορούν να εκμεταλλευτούν τέτοιους συνεργατικούς μηχανισμούς, σκοπίμως η μη, οδηγώντας σε περιπτώσεις αποκοπής καλοήθους ροών δεδομένων, ή ακόμη και επηρεασμού της πολιτικής που εφαρμόζουν γειτονικές δικτυακές περιοχές για την προώθηση της κίνησης.

Τέλος, απαιτείται η μελέτη μεθόδων προστασίας των SDN Controllers από στοχευμένες επιθέσεις, μιας και το κεντρικοποιημένο Επίπεδο Ελέγχου αποτελεί κομβικό σημείο της ομαλής λειτουργίας του δικτύου.

9 Δημοσιεύσεις

9.1 Διεθνή Επιστημονικά Περιοδικά με Κρίση

1. K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras and V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", *Computer Networks*, *Elsevier*, vol. 62, pp. 122-136, April 2014.

2. K. Giotis, G. Androulidakis, V. Maglaris, "A Scalable Anomaly Detection and Mitigation Architecture for Legacy Networks via an OpenFlow Middlebox", *Security and Communication Networks*, *Wiley*, DOI: 10.1002/sec.1368, October 2015.

9.2 Πρακτικά Διεθνών Επιστημονικών Συνεδρίων με Κρίση

1. K. Giotis, G. Androulidakis, V. Maglaris, "Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks", in Proc. of *European Workshop on Software Defined Networks 2014 (EWSDN14)*, Budapest, Hungary, September 2014.

2. K. Giotis, Y. Kryftis, V. Maglaris, "Policy-based Orchestration of NFV Services in Software-Defined Networks", in Proc. of *1st IEEE Conference on Network Softwarization (NetSoft 2015)*, London, UK, April 2015.

3. C. Argyropoulos, S. Mastorakis, K. Giotis, G. Androulidakis, D. Kalogeras and V. Maglaris, "Control-Plane Slicing Methods in Multi-Tenant Software Defined Networks", in Proc. of *IFIP/IEEE Integrated Network Management Symposium (IEEE IM 2015)*, Ottawa, Canada, May 2015.

4. J. Ortiz, J. I. Aznar, A. Mendiola, K. Giotis, "SDN Integration and Management Solutions for Campus Network Enhanced Services", in Proc. of *19th Conference on Innovations in Clouds, Internet and Networks (ICIN 2016)*, Paris, France, March 2016.

5. K. Giotis, M. Apostolaki, V. Maglaris, “A Reputation-Based Collaborative Schema for the Mitigation of Distributed Attacks in SDN Domains”, to appear in Proc. of *IEEE/IFIP Network Operations and Management Symposium (NOMS ’16)*, Istanbul, Turkey, April 2016.

10 Βιβλιογραφία

[1] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: enabling innovation in campus networks," in *SIGCOMM Comput. Commun. Rev. 38, 2*, March 2008.

[2] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks," in *ONF White Paper*, 2012.

[3] ETSI Group Specification, "ETSI GS NFV-MAN 001 V1.1.1 - Network Functions Virtualisation (NFV); Management and Orchestration," Available at: http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf, 2014.

[4] United States Computer Emergency Readiness Team (US-CERT), "DNS Amplification Attacks," Available at: https://www.us-cert.gov/ncas/alerts/TA13-088A, 2013.

[5] M. Kim, H. Kong, S. Hong, S. Chung and J. Hong, "A Flow-Based Method for Abnormal Network Traffic Detection," *Network Operations and Management Symposium 2004 (NOMS 2004)*, p. 599–612, 2004.

[6] A. Lahkina, M. Crovella and C. Diot, "Mining Anomalies Using Traffic Feature Distributions," in *Proc. of ACM SIGCOMM 2005*, Philadelphia, PA, USA, August 2005.

[7] D. Brauckhoff, M. May and B. Plattner, "Flow-Level Anomaly Detection - Blessing or Curse?," in *IEEE INFOCOM 2007, Student Workshop*, Anchorage, 2007.

[8] sFlow, "Traffic Monitoring using sFlow," Available at: http://www.sflow.org/sFlowOverview.pdf, 2003.

[9] J. Rexford, A. Greenber, G. Hjalmtysson, D. Maltz, A. Myers, G. Xie, J. Zhan and H. Zhang, "Network-wide decision making: Toward a wafer-thin control plane," in *Proceedings of HotNets III*, 2004.

[10] Y. Rekhter, T. Li and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," in *RFC4271*, January 2006.

[11] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu., J. Zolla, U. Hölzle, S. Stuart and A. Vahdat, "B4: Experience with a Globally-Deployed Software Defined WAN," in *Proceedings of SIGCOMM '13*, Hong Kong, 2013.

[12] VMware, "VMware Network Virtualization Design Guide," Technical White Paper, January 2013.

[13] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," RFC7348, 2014.

[14] P. Garg and Y. Wang, "NVGRE: Network Virtualization using Generic Routing Encapsulation," IETF Internet Draft, 2014.

[15] B. Davie and J. Gross, "A Stateless Transport Tunneling Protocol for Network Virtualization (STT)," IETF Internet Draft, 2014.

[16] M. Smith, D. Dutt, D. Farinacci and F. Maino, "Layer 2 (L2) LISP Encapsulation Format," IETF Internet Draft, 2013.

[17] CISCO, "Data Center Overlay Technologies," White Paper, 2013.

[18] D. Kreutz, F. Ramos, P. Verissimo, C. Rothenberg, S. Azodolmolky and S. Uhlig,

"Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, pp. 14-79, Jan. 2015.

[19] E. Haleplidis, K. Pentikousis, S. Denazis, J. Hadi Salim, D. Meyer and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology," RFC 7426, 2015.

[20] A. Doria, J. Hadi Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal and J. Halpern, "Forwarding and Control Element Separation (ForCES) Protocol Specification," RFC 5810, March 2010.

[21] R. Enns, M. Bjorklund, J. Schoenwaelder and A. Bierman, "Network Configuration Protocol (NETCONF), RFC6241," June 2011.

[22] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," RFC 6020, 2010.

[23] A. Farrel, J.-P. Vasseur and J. Ash, "A Path Computation Element (PCE)-Based Architecture," RFC 4655, 2006.

[24] J. Vasseur and J. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)," RFC 5440, 2009.

[25] Cisco, "OpFlex: An Open Policy Protocol," 2015.

[26] Puppet Labs, "Puppet: Defusing the Server Management Explosion," Available at: https://puppetlabs.com/wp-content/uploads/2011/08/PL_WP_Defusing_Server_Management_Explosion.pdf, 2011.

[27] CFEngine, "Adopting CFEngine in Your Organization," Available at: https://auth.cfengine.com/archive/manuals/st-adopt, 2009.

[28] Open Networking Foundation (ONF), "OpenFlow Switch Specification Version 1.0.0 (Wire Protocol 0x01)," 2009.

[29] ETSI Group Specification, "Network Functions Virtualisation (NFV); Use Cases2," Available at: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf, October 2013.

[30] A. Abdelrazik, G. Bunce, K. Cacciatore, K. Hui, S. Mahankali and F. Van Rooyen, "OPENSTACK WHITE PAPER - Adding Speed and Agility to Virtualized Infrastructure with OpenStack," in *https://www.openstack.org/assets/pdf-downloads/virtualization-Integration-whitepaper-2015.pdf*, 2015.

[31] D. Levi, P. Meyer and B. Stewart, "Simple Network Management Protocol (SNMP) Applications," RFC 3413, 2002.

[32] "SNORT," Available at: https://www.snort.org.

[33] Solarwinds, "The Reference Guide to Network Management Protocols," Available at: http://www.solarwinds.com/resources/whitepapers/SolarWinds_Network_Mgmt_Protocols.pdf.

[34] B. Claise, "Cisco Systems NetFlow Services Export Version 9," RFC 3954, 2004.

[35] Y. Zhang, "An adaptive flow counting method for anomaly detection in SDN," in *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies(CoNEXT '13)*, New York, NY, USA, 2013.

[36] S. Shirali-Shahreza and Y. Ganjali, "Efficient Implementation of Security Applications in OpenFlow Controller with FleXam," in *Proceedings of the 2013 IEEE 21st Annual Symposium on High-Performance Interconnects (HOTI '13). IEEE*

Computer Society, Washington, DC, USA, 2013.

[37] C. Yu, C. Lumezanu, Y. Zhang, V. Singh, G. Jiang and H. V. Madhyastha, "FlowSense: monitoring network utilization with zero measurement cost," in *Proceedings of the 14th international conference on Passive and Active Measurement (PAM'13)*, Berlin, 2013.

[38] C. Douligeris and A. Mitrokotsa, "DDoS atacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643-666, 2004.

[39] N. Weaver, V. Paxson, S. Staniford and R. Cunningham, "A Taxonomy of Computer Worms," in *Proc. of the First ACM Workshop on Rapid Malcode (WORM)*, Washington DC, USA, October 2003.

[40] D. Newman, «RFC 2647».

[41] Arbor Networks, Available at: http://www.arbornetworks.com/.

[42] Arbor Networks, "PeakFlow TMS," http://resources.arbornetworks.com/i/584787-arbor-networks-tms-data-sheet?hubItemID=150656412.

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

[44] Imperva Incapsula Inc., Available at: https://www.incapsula.com/.

[45] CloudFlare Inc, Available at: https://www.cloudflare.com/.

[46] T. Cover and J. Thomas, "Elements of Information Theory," in *Wiley & Sons, Second Edition*, June 2006.

[47] S. Ranjan, S. Shah, A. Nucci, M. Munafo, R. Cruz and S. Muthukrishnan, "DoWitcher: Effective Worm Detection and Containment in the Internet Core," in *26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, Anchorage, Alaska, USA, May 2007.

[48] W. Yu, X. Wang, D. Xuan and D. Lee, "Effective Detection of Active Worms with Varying Scan Rate," in *Second International Conference on Security and Privacy in Communication Networks, (IEEE SecureComm 2006)*, Baltimore, MD, USA, August 2006.

[49] R. B. Blazek, H. Kim, B. Rozovskii and A. Tartakovsky, "A novel approach to detection of Denial of Service attacks via adaptive sequential and batch sequential change point detection methods," in *Proc. of IEEE Workshop Information Assurance and Security*, New York, USA, June 2001.

[50] H. Wang, D. Zhang and K. G. Shin, "Change-Point Monitoring for the Detection of DoS Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 4, pp. 193-208, 2004.

[51] T. Peng, C. Leckie and K. Ramamohanarao, "Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring," in *Proc. of the Third International IFIP-TC6 Net-working Conference*, Athens, Greece, May 2004.

[52] R. Braga, E. Mota and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *LCN '10 Proceedings of the 2010 IEEE 35th Conference on Local Computer*, 2010.

[53] S. A. Mehdi, J. Khalid and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *In RAID'11*, 2011.

[54] Cisco Systems, "Strategies to Protect Against Distributed Denial of Service (DDoS)

Attacks," Available at: http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.pdf, 2014.

[55] European Telecommunications Standards Institute (ETSI), "Network Functions Virtualisation – Introductory White Paper," *SDN and OpenFlow World Congress*, 22-24 October 2012.

[56] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu and M. Tyson, "FRESCO: Modular composable security services for software-defined networks," in *Proceedings of Network and Distributed Security Symposium*, 2013.

[57] A. K. Nayak, A. Reimers, N. Feamster and R. Clark, "Resonance: dynamic access control for enterprise networks," in *Proceedings of the 1st ACM workshop on Research on enterprise networking (WREN '09)*, New York, NY, USA, 2009.

[58] L. Poulopoulos, M. Mamalis and A. Polyrakis, "FireCircle: GRNET's approach to advanced network security services' management via bgp flow-spec and NETCONF," in *Proceedings of the 28th TERENA Networking Conference*, 2012.

[59] P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch and D. McPherson, "Dissemination of Flow Specification Rules, RFC5575," August 2009.

[60] K. Argyraki and D. R. Cheriton, "Scalable Network-layer Defense Against Internet Bandwidth-Flooding Attacks," *IEEE/ACM Transactions on Networking*, vol. 4, no. 17, pp. 1284-1297, August 2009.

[61] G. Androulidakis, V. Chatzigiannakis and S. Papavassiliou, "Network Anomaly Detection and Classification via Opportunistic Sampling," *IEEE Network: The Magazine of Global Internetworking - Special issue title on recent developments in network intrusion detection*, vol. 23, no. 1, pp. 6-12, January/February 2009.

[62] A. Wagner and B. Plattner, "Entropy Based Worm and Anomaly Detection in Fast IP Networks," in *WETICE '05 Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise*, 2005.

[63] C. Siaterlis and V. Maglaris, "One step ahead to multisensor data fusion for DDoS detection," *Journal of Computer Security*, vol. 13, no. 5, pp. 779-806, 2005.

[64] L. Quyen, M. Zhanikeev and Y. Tanaka, "Detecting and identifying network anomalies by component analysis," in *APNOMS'06 Proceedings of the 9th Asia-Pacific international conference on Network Operations and Management: management of Convergence Networks and Services*, 2006.

[65] S. Staniford, J. A. Hoagland and J. M. McAlerney, "Practical automated detection of stealthy portscans," *Journal of Computer Security 10*, pp. 105-136, 2002.

[66] T. Ahmed, B. Oreshkin and M. Coates, "Machine learning approaches to network anomaly detection," in *SYSML'07 Proceedings of the 2nd USENIX workshop on Tackling computer systems problems with machine learning techniques*, 2007.

[67] S.-Y. Wu and E. Yen, "Data mining-based intrusion detectors," *Expert Systems with Applications*, vol. 36, no. 3, pp. 5605 - 5612, April 2006.

[68] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security (Elsevier)*, vol. 28, pp. 18-28, February-March 2009.

[69] A. Patcha and J.-M. Park., "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, pp. 3448-3470, 2007.

[70] J. Pettit, J. Gross, B. Plaff, M. Casado and S. Crosby, "Virtual switching in an era of advanced Edges," in *2nd Workshop on Data Center – Converged and Virtual Ethernet*

Switching (DC-CAVES), ITC 22, September 2010.

[71] S. Shah, A. Nucci, M. Munafo, R. Cruz and S. Muthukrishnan, "DoWitcher: Effective Worm Detection and Containment in the Internet Core," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007.

[72] T. Cover and J. Thomas, "Elements of Information Theory," in *Wiley & Sons, Second Edition*, June 2006.

[73] NOX Controller, Available at: http://www.noxrepo.org.

[74] N. Gude, T. Koponen, J. Pettit, B. Plaff, M. Casado, N. McKeown and S. Shenker, "NOX: towards an operating system for networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 3, pp. 105-110, July 2008.

[75] B. Pfaff, J. Pettit, T. Koponen, K. Amidon, M. Casado and S. Shenker, "Extending networking into the virtualization layer," in *8th ACM Workshop on Hot Topics in Networks (HotNets-VIII)*, New York City, 2009.

[76] L. Deri and S. Suin, "Effective traffic measurement using ntop," *IEEE Communications Magazine*, vol. 38, no. 5, pp. 138-143.

[77] "Tcpreplay," Available at http://tcpreplay.synfin.net.

[78] SCAPY, Available at: http://hg.secdev.org/scapy.

[79] E. Schechter, J. Jung and A. W. Berger, "Fast Detection of Scanning Worm Infections," in *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID)*, 2004.

[80] J. Jung, V. Paxson, A. Berger and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," in *Proc. IEEE Symposium on Security and Privacy*, 2004.

[81] W. Kumari and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding, RFC5635," August 2009.

[82] A. Curtis, J. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma and S. Banerjee, "DevoFlow: scaling flow management for high-performance networks," in *Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM '11)*, New York, NY, USA, 2011.

[83] Open Networking Foundation, "OpenFlow-enabled SDN and Network Functions Virtualization," Available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf.

[84] P. Phaal and M. Lavine, "sFlow Version 5," Available at: http://sflow.org/sflow_version_5.txt.

[85] H. Liu, Y. Sun and M. S. Kim, "A Scalable DDoS Detection Framework with Victim Pinpoint Capability," *Journal of Communications*, vol. 6, no. 9, pp. 660-670, December 2011.

[86] A. C. Gilbert, Y. Kotidis, S. Muthukrishnan and M. J. Strauss, "Quicksand: Quick summary and analysis of network data," in *DIMACS, Tech. Rep. 2011-43*, 2001.

[87] A. Broder and M. Mitzenmacher, "Network Applications of Bloom Filters: A Survey," *Internet Mathematics*, vol. 1, no. 4, pp. 485-509, 2005.

[88] H. Liu, Y. Sun and M. Kim, "Fine-Grained DDoS Detection Scheme Based on Bidirectional Count Sketch," in *Proceeding of the International Conference on Computer Communication Networks (ICCCN'11)*, 2011.

[89] C. Kreibich, A. Warfield, J. Crowcroft, S. Hand and I. Pratt, "Using packet symmetry

to curtail malicious traffic," in *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, November 2005.

[90] C. Siaterlis and B. Maglaris, "Detecting DDoS Attacks with Passive Measurement based Heuristics," in *Proc IEEE Symposium on Computer and Communication (ISCC)*, June 2004.

[91] K. Pagiamtzis and A. Sheikholeslami, "Content-addressable memory (CAM) circuits and architectures: A tutorial and survey," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 3, p. 712–727, 2006.

[92] F. Soldo, K. Argyraki and A. Markopoulou, "Optimal source-based filtering of malicious traffic," *IEEE/ACM Transactions on Networking*, vol. 2, no. 20, p. 381–395, 2012.

[93] Z. Mao, V. Sekar, O. Spatscheck, J. Van Der Merwe and R. Vasudevan, "Analyzing large DDoS attacks using multiple data sources," in *ACM SIGCOMM Workshop on Large Scale Attack*, 2006.

[94] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in *Proceedings of ACM SIGCOMM*, 2006.

[95] S. Venkataramn, S. Sen, O. Spatscheck, P. Haffner and D. Song, "Exploiting network structure for proactive spam mitigation," in *Proceedings of Usenix Security'07*, 2007.

[96] CAIDA, "The CAIDA UCSD "DDoS Attack 2007 Dataset"," Available at: http://www.caida.org/data/passive/ddos-20070804_dataset.xml.

[97] J. Fan, J. Xu, M. H. Ammar and S. Moon, "Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme," *Comput. Netw.*, vol. 46, no. 2, pp. 253-272, October 2004.

[98] "Quagga Routing Software Suite," Available at: http://www.nongnu.org/quagga.

[99] "ExaBGP," Available at: https://github.com/Exa-Networks/exabgp.

[100] H. Yin, H. Xie, T. Tsou, D. Lopez, P. Aranda and R. Sidi, "SDNi: A Message Exchange Protocol for Software Defined Networks (SDNS) across Multiple Domains," in *Internet Research Task Force Internet-Draft*, 2012.

[101] R. Danyliw, J. Meijer and Y. Demchenko, "The Incident Object Description Exchange Format," in *RFC 5070*, December 2007.

[102] B. Trammell, "RFC 6885 - Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry," July 2012.

[103] K. Phemius, M. Bouet and J. Leguay, "DISCO: Distributed Multi-domain SDN Controllers," in *2014 IEEE NOMS*, Krakow, May 2014.

[104] "OpenDaylight-SDN Interface Application," Available at: https://wiki.opendaylight.org/view/ODL-SDNi_App.

[105] J. Medved, A. Tkacik, R. Varga and K. Gray, "OpenDaylight: Towards a Model-Driven SDN Controller Architecture," in *IEEE 15th International Symposium on World of Wireless, Mobile and Multimedia Networks*, Sydney, 2014.

[106] A. Jsang, R. Ismail and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, pp. 618-644, March 2007.

[107] J. Berger, "Statistical Decision Theory and Bayesian Analysis," *Springer, Second Edition*, 1985.

[108] S. Buchegger and J. Y. L. Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks," Available at: http://citeseerx.ist.psu.edu/viewdoc/, 2003.

[109] "OpenDaylight Platform," Available at: https://www.opendaylight.org/.

[110] K. D. Sepandar, M. T. Schlosser and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," in *ACM Proceedings of the 12th international conference on World Wide Web*, Budapest, May 2003.

[111] R. Chandra and J. Scudder, "RFC 3392 - Capabilities Advertisement with BGP-4," November 2002.

[112] H. Gredler, J. Medved, S. Previdi and A. Farrel, "North-Bound Distribution of Link-State and TE Infromation using BGP (IETF Draft)," Available at: https://tools.ietf.org/html/draft-gredler-idr-lsdistribution-02, 2012.

[113] CAIDA, "The CAIDA AS Relationships Dataset, 20140801," Available at: http://www.caida.org/data/as-relationships/, 2014.

[114] L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 733-745, December 2001.

[115] D. Magoni and J. J. Pansiot, "Analysis of the Autonomous System Network Topology," in *SIGCOMM Comp. Com. Rev. 31*, July 2001.

[116] Hewlett Packard, "OpenFlow v1.3 Administrator Guide K/KA/WB 15.17," June 2015.

[117] Cisco Systems, "Cisco IOS Security Configuration Guide, Release 12.2," Avaialbe at: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfreflx.html, 2006.

[118] Cisco Systems, "White Paper: Remotely Triggered Black Hole Filtering - Destination Based and Source Based," Available at: http://www.cisco.com/web/about/security/intelligence/blackhole.pdf, 2005.