Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων
Και Μηχανικων Υπολογιστων
Τομεας Επικοινωνιων, Ηλεκτρονικης &
Συστηματων Πληροφορικης

Συνεργατικό Σύστημα Αντιμετώπισης Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας σε Περιβάλλον Πολλαπλών Διαχειριστικών Περιοχών

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ
του

ΓΕΩΡΓΙΟΥ Ν. ΚΟΥΤΕΠΑ
Διπλωματούχου Ηλεκτρολόγου Μηχανικού &
Μηχανικού Υπολογιστών Ε.Μ.Π. (1996)
Αθήνα, Μάιος 2006

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων
Τομεας Επικοινωνιων, Ηλεκτρονικης &
Συστηματων πληροφορικης

Συνεργατικό Σύστημα Αντιμετώπισης Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας σε Περιβάλλον Πολλαπλών Διαχειριστικών Περιοχών

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

ΓΕΩΡΓΙΟΥ Ν. ΚΟΥΤΕΠΑ

Διπλωματούχου Ηλεκτρολόγου Μηχανικού &
Μηχανικού Υπολογιστών Ε.Μ.Π. (1996)

Συμβουλευτική Επιτροπή: Βασίλειος Μάγκλαρης
Εμμανουήλ Πρωτονοτάριος
Εμμανουήλ Σκορδαλάκης

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή τη 12η Μαΐου 2006.

...	...	...
Β. Μάγκλαρης	Ε. Πρωτονοτάριος	Μ. Αναγνώστου
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
...	...	...
Ε. Συκάς	Σ. Παπαβασιλείου	Ν. Κοζύρης
Καθηγητής Ε.Μ.Π.	Επ. Καθηγητής Ε.Μ.Π.	Επ. Καθηγητής Ε.Μ.Π.

...
Σ. Κάτσικας
Καθηγητής
Παν. Αιγαίου

. . .

ΓΕΩΡΓΙΟΣ Ν. ΚΟΥΤΕΠΑΣ
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Στη Νατάσσα

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή αφορά σε συνεργατικές μεθόδους αντιμετώπισης Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας (Distributed Denial of Service Attacks – DDoS), κακόβουλων μεταδόσεων μεγάλου όγκου κίνησης που έχουν σκοπό την εξάντληση δικτυακών (συνήθως) ή υπολογιστικών πόρων στο δίκτυο-στόχο. Οι επιθέσεις αυτού του είδους παρουσιάζουν έναν αριθμό από ιδιαιτερότητες οι οποίες καταστούν δύσκολη την αντιμετώπιση τους αποκλειστικά στον τελικό στόχο τους (παραποίηση πραγματικού αποστολέα της επιθετικής κίνησης, συνδυασμός πολλών απομακρυσμένων πηγών αποστολής κίνησης, αιφνίδια εξέλιξη, δυσκολία ανίχνευσης και διαχωρισμού από γεγονότα νόμιμης αυξημένης κίνησης κ.λπ.).

Η ακολουθούμενη μεθοδολογία βασίζεται στο επιτυχημένο μοντέλο συνεργασίας ανάμεσα σε ομάδες ασφαλείας CERT (Computer Emergency Response Teams) διαφορετικών δικτύων (domains), με διαδικασίες εξασφάλισης εμπιστοσύνης (trust management). Προτείνεται ένα παρόμοιο πλαίσιο ανταλλαγής πληροφοριών για την αντιμετώπιση των επιθέσεων DDoS στα δίκτυα απ' όπου διέρχεται η επιθετική κίνηση. Για να καταστεί αυτό δυνατόν τα δίκτυα που ζητούν να συνεργαστούν δημιουργούν ένα ειδικό Υπερκείμενο (overlay) δίκτυο, τη *Συνεργατική Υποδομή*. Η υλοποίηση της Υποδομής γίνεται με την εγκατάσταση ειδικών συστημάτων λογισμικού σε κάθε δίκτυο, των *Συνεργατικών Οντοτήτων*, που παραμένουν υπό τοπικό έλεγχο.

Αρχικά, παρουσιάζονται τα κύρια ζητήματα που θέτει μια τέτοια κατανεμημένη προσέγγιση του προβλήματος των επιθέσεων DDoS. Στη συνέχεια, αναλύονται και επιδεικνύονται, μέσα από ενδεικτικές υλοποιήσεις, οι απαιτήσεις και προδιαγραφές του συστήματος με εναλλακτικές τεχνολογίες διαμόρφωσης του υπερκείμενου δικτύου. Με τη λειτουργία της Συνεργατικής Υποδομής, σε τοπικό επίπεδο και ως συντονισμένο σύνολο, επιτυγχάνεται η ανίχνευση (detection) και η παρακολούθηση της διαδρομής (trace-back) της επίθεσης. Κύριος σχεδιαστικός στόχος είναι η αποσύνδεση της διαδικασίας συνεργατικής ανίχνευσης μέσω της Υποδομής από τη μέθοδο ανίχνευσης, τις ρυθμίσεις και την ακρίβεια των κατά τόπους συστημάτων IDS. Επιπλέον, κάθε δίκτυο ανεξάρτητα μπορεί να αναλάβει ενέργειες αντιμετώπισης οι οποίες θα περιορίσουν την επίδραση της επίθεσης κατά μήκος της συνολικής διαδρομής της.

Η Συνεργατική Υποδομή αποτελεί ένα ασφαλές και ευέλικτο πλαίσιο για τη διαχείριση ασφάλειας σε περιβάλλον πολλαπλών συνεργαζόμενων δικτύων. Με ανάλυση και προσομοιώσεις καταδεικνύεται ότι η λειτουργία της μπορεί να βελτιώσει τα αποτελέσματα ανίχνευσης με την αύξηση του βαθμού εμπιστοσύνης μεταξύ των συνεργαζόμενων δικτύων.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Επιθέσεις DDoS, Πολλαπλά Δίκτυα (domains), Συνεργατική αντιμετώπιση, Ανίχνευση, Παρακολούθηση διαδρομής, Αντιμετώπιση

Mitigation of DDoS Attacks via a Cooperative Multi-Domain Infrastructure

Doctoral Dissertation by Georgios N. Koutepas

National Technical University of Athens, Greece
Department of Electrical and Computer Engineering

Supervisor: Prof. Vasilis Maglaris

ABSTRACT

In this work we propose a cooperative architecture for the detection, path tracing and mitigation of Distributed Denial of Service (DDoS) attacks. These are malicious high volume traffic streams that target network or server system resources of a site. DDoS attacks are difficult to counter by exclusive actions at the victim site due to a number of characteristics, such as highly distributed attack sources, address spoofing, rapid escalation of attacks, difficulty to distinguish from legitimate high-traffic events.

Our model builds on the successful CERT (Computer Emergency Response Teams) paradigm of cooperation between different trusted sites. We employ a similar approach for automatically building an infrastructure for exchanging DDoS detection reports among independent cooperating domains. The networks (administrative domains) wishing to participate in this scheme form a *Cooperative Framework* via an overlay network. This is organized by the deployment, at each site, of specialized software modules, the *Cooperative Entities* that are controlled by local domain administrators.

We first present the main issues of such a cooperative approach pertaining to DDoS attacks. The formation of the Cooperative Framework overlay is demonstrated for a number of different low level communication technologies. It is shown that the infrastructure achieves cooperative detection and path tracing, regardless of the individual site IDS detection methodologies and performance. Each site may choose an independent attack mitigation policy aiming to limit the effects of a DDoS attack along its entire path (propagation tree).

Our Cooperative Framework forms a reliable and flexible solution for managing security information in a multi-domain environment. This is reinforced by both analytic and simulation experiments demonstrating the feasibility, stable operation and performance of the Framework. Finally, we show that cooperative detection improves as the trust level among sites increases.

KEYWORDS: DDoS, Multi-domain, Cooperation, Detection, Attack Trace-Back, Mitigation

Πρόλογος

Η Διατριβή αυτή αποτελεί μία πρόταση αντιμετώπισης των Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας (Distributed Denial of Service Attacks - DDoS), ενός ιδιαίτερα σοβαρού και διαδεδομένου προβλήματος στο Διαδίκτυο σήμερα. Η προσέγγιση που ακολουθείται στην εργασία έχει σε μεγάλο βαθμό προκύψει από την εμπειρία του γράφοντος στο χώρο της ασφάλειας επί σειρά ετών, τόσο στον ακαδημαϊκό όσο και στον επαγγελματικό χώρο.

Ευκαιρία για ν' ασχοληθώ με θέματα ασφάλειας υπολογιστικών συστημάτων και δικτύων μού είχε δοθεί ήδη από το ακαδ. έτος 1995-1996, περίοδο εκπόνησης της διπλωματικής μου εργασίας (στο εργαστήριο NETMODE), όταν αυτά τα ζητήματα ήταν ακόμα σχετικά νέα.

Με την έναρξη της επαγγελματικής μου δραστηριότητας οι πρώτες αυτές γνώσεις ενισχύθηκαν περαιτέρω και μπήκαν σε πρακτική εφαρμογή. Καθοριστικό ρόλο για τη μετέπειτα επαγγελματική μου εξέλιξη αλλά και στο σχεδιασμό της παρούσας εργασίας έπαιξε η ευκαιρία που είχα, κατά την περίοδο 1996-1998, να αποτελέσω μέλος της ομάδας του Κέντρου Ελέγχου Δικτύου του Ε.Μ.Π. Στο διάστημα αυτό ήλθα σε επαφή με τα σημαντικότερα πρακτικά ζητήματα ασφαλείας σε δίκτυα μεγάλης κλίμακας, όπως του Ε.Μ.Π. και του Εθνικού Δικτύου Έρευνας και Τεχνολογίας (τη διαχείριση του οποίου είχε το Κ.Ε.Δ. του Ε.Μ.Π.). Επιπλέον στο διάστημα αυτό συμμετείχα ενεργά στη δημιουργία της πρώτης Ελληνικής Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας (Computer Emergency Response Team – CERT), του GRNET-CERT. Χάρη στον επιστημονικό υπεύθυνο του Κ.Ε.Δ. τότε, και κύριο επιβλέποντα αυτού του διδακτορικού, καθηγητή Β. Μάγκλαρη, είχα την ευκαιρία στα πλαίσια της εργασίας για το GRNET-CERT να παρευρεθώ σε δύο ετήσια συνέδρια του Forum of Incident Response and Security Teams (FIRST) το 1998 στο Μεξικό και το 1999 στην Αυστραλία. Η απευθείας επαφή με τα μέλη κάποιων από τις καλύτερες ομάδες ασφαλείας στον κόσμο, όπως και με κορυφαίους ειδικούς στον τομέα, είχε καταλυτική δράση στην κατανόηση θεμάτων ασφαλείας και την εξέλιξη των ιδεών που μελλοντικά θα αποτελούσαν τον πυρήνα της παρούσας διατριβής.

Εν τω μεταξύ το παγκόσμιο περιβάλλον ασφαλείας εξελίχθηκε δυναμικά ακολουθώντας την αλματώδη ανάπτυξη του Διαδικτύου παγκοσμίως. Το πρώτο σημαντικό περιστατικό ασφαλείας που συνέβη μετά την έλευση του έτους 2000 ήταν η μεγάλης κλίμακας επιθέσεις DDoS εναντίον δικτυακών τόπων σημαντικών εμπορικών και ειδησεογραφικών εταιριών [Comp00]. Οι επιθέσεις αυτές έγιναν ευρύτατα γνωστές και έδειξαν πρώτη φόρα πόσο πραγματικές και επικίνδυνες για τη σύγχρονη κοινωνία της δικτύωσης και της πληροφορίας είναι απειλές προς την τεχνική υποδομή της (τις λεγόμενες «Κρίσιμες Υποδομές»

– "Critical Infrastructure"). Με το περιστατικό αυτό οι Επιθέσεις Άρνησης Υπηρεσίας και, συμβολικά, έδειξαν ότι ανήκουν στις προκλήσεις ασφάλειας του νέου αιώνα.

Μετά τα τρομοκρατικά χτυπήματα της 11ης Σεπτεμβρίου 2001, οι επιθέσεις DDoS αναδείχθηκαν τμήμα ενός ευρύτερου περιβάλλοντος ασφαλείας με νέες άμεσες προκλήσεις. Οι μοντέρνες αυτές προκλήσεις – προς την τεχνική υποδομή του Διαδικτύου και της κοινωνίας της Πληροφορίας γενικότερα – είναι η προστασία των υποδομών επικοινωνίας η οποία πλέον είναι αναπόσπαστο κομμάτι της σύγχρονης ζωής· για τους χρήστες η πρόκληση βρίσκεται στη διασφάλιση από απειλές, χωρίς όμως να στερηθούν δεδομένες ευκολίες και κυρίως το κεκτημένο δικαίωμα του ιδιωτικού απόρρητου.

Μέσα σε αυτό το διαρκώς εξελισσόμενο περιβάλλον ασφαλείας, ο γράφων επιχείρησε να προσεγγίσει το πρόβλημα των επιθέσεων DDoS, χρησιμοποιώντας τα διδάγματα που είχε αποκομίσει από την επαγγελματική και ακαδημαϊκή του δραστηριότητα: τη σημασία προστασίας κρίσιμων δικτυακών πόρων, τη συνεργασία ομάδων CERT σε περιβάλλον εμπιστοσύνης, την ανάγκη διαχειριστικής ανεξαρτησίας κάθε δικτύου, ακόμα και κατά το χειρισμό περιστατικών ασφάλειας, τη σημασία της ταχύτητας αντίδρασης σε περιστατικά.

Ευχαριστίες

Εν πρώτοις θέλω να εκφράσω τις θερμότατες ευχαριστίες μου στον επιβλέποντα αυτή τη διατριβή, Καθηγητή κ. Βασίλη Μάγκλαρη, για τη συνεχή καθοδήγηση και την αμέριστη συμπαράσταση του καθ' όλη τη διάρκεια της συνεργασίας μας. Χάρη στις γνώσεις, την πείρα και τις πολύτιμες οδηγίες του η εργασία αυτή απέκτησε πληρότητα και βάθος.

Θα ήθελα να ευχαριστήσω επίσης τα μέλη της Συμβουλευτικής Επιτροπής: κ. Ε. Πρωτονοτάριο, Καθηγητή Ε.Μ.Π. (μέλος και της Εξεταστικής Επιτροπής) και κ. Ε. Σκορδαλάκη, Καθηγητή Ε.Μ.Π, καθώς και τα μέλη της Εξεταστικής Επιτροπής: κ. Μ. Αναγνώστου, Καθηγητή Ε.Μ.Π., κ. Ε. Συκά, Καθηγητή Ε.Μ.Π., κ. Σ. Παπαβασιλείου Επικ. Καθηγητή Ε.Μ.Π., κ. Ν. Κοζύρη, Επικ. Καθηγητή Ε.Μ.Π. και κ. Σ. Κάτσικα, Καθηγητή του Πανεπιστημίου Αιγαίου.

Πρέπει ακόμη να ευχαριστήσω όλους τους ανθρώπους που στάθηκαν κοντά μου και με στήριξαν αυτόν τον καιρό, τόσο στην εκπόνηση αυτής της εργασίας όσο και προσωπικά.

Ιδιαίτερες ευχαριστίες πρέπει να εκφραστούν στους δύο ανθρώπους χάρη στη βοήθεια και υποστήριξη των οποίων ολοκληρώθηκε με επιτυχία η εργασία αυτή:

Το συνάδελφο Φώτη Σταματελόπουλο, τον «παλιό» του εργαστηρίου NETMODE. Σημαντικό μέρος της εργασίας αυτής οφείλεται στις συζητήσεις που

είχαμε, στη συνεχή παρότρυνση και στο αδελφικό, θα τολμούσα να πω, ενδιαφέρον του για την επιτυχία μου.

Τη Νατάσσα Τοκαρέβσκαγια, που στάθηκε στο πλευρό μου, με στήριξε συνεχώς, μου χάρισε το χαμόγελο και στη διάρκεια όλης αυτής της προσπάθειας μου έδωσε κουράγιο να συνεχίσω.

Φυσικά, πολλές ευχαριστίες οφείλονται σε όλους τους συνάδελφους του εργαστηρίου NETMODE (παλιότερους και νεότερους) που δημιούργησαν αυτά τα χρόνια ένα πολύ ζεστό και όμορφο περιβάλλον, έγιναν πραγματικοί φίλοι. Θέλω ιδιαίτερα να ευχηθώ στο συνάδελφο και φίλο Δημήτρη Βελένη «περαστικά» και δύναμη για να είναι και πάλι σύντομα κοντά μας γερός και πνευματώδης όπως πάντα!

Πολλές ευχαριστίες επίσης στους πρώην διπλωματικούς συνεργάτες που συνεισέφεραν σημαντικά στην επιτυχία αυτής της εργασίας: τον (Δρα. εδώ και πολύ καιρό) Παναγιώτη Αστήθα, τους συναδέλφους πλέον Σάκη Μώραλη και Βασίλη Χατζηγιαννάκη, και τους Νίκο Πουγούνια, Πέτρο Αλευρά, Κυριακή Λεβαντή, Δημήτρη Φιλιππίδη και Γιώργο Κωτσόλη.

Ευχαριστώ επίσης τους ανθρώπους στους οποίους οφείλω τα πάντα, τους Γονείς μου Μαρία και Νίκο.

Τέλος, ευχαριστώ από βάθους ψυχής το δάσκαλο μου Ι.Χ.Σ.

Γιώργος Κουτέπας
Αθήνα, Μάιος 2006

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Τμημάτων Κώδικα

Κεφάλαιο 1

Εισαγωγή

1.1 Περιγραφή του Προβλήματος

Οι *Επιθέσεις Άρνησης Υπηρεσίας* (*Denial of Service Attacks – DoS*) αποτελούν μια από τις εκδηλώσεις της συνεχιζόμενης αντιπαράθεσης ανάμεσα σε εκείνους που επιδιώκουν την παραβίαση και εκείνους που επιζητούν την προστασία υπολογιστικών συστημάτων. Με την παγίωση της χρήσης του Διαδικτύου στη δεκαετία του 1990 και την καθιέρωση του ως σημαντικού μέσου επικοινωνίας και ανταλλαγής ιδεών αλλά και ως παράγοντα της παγκόσμιας οικονομίας, άρχισαν να γίνονται φανερά τα σημαντικά ζητήματα ασφαλείας που προκύπτουν από τη γενικευμένη συνδεσιμότητα υπολογιστικών συστημάτων. Το Διαδίκτυο αποτέλεσε το νέο πεδίο οικονομικού ανταγωνισμού και μπήκε στο στόχαστρο παράνομων δραστηριοτήτων και κακόβουλων ενεργειών. Οι απειλές ασφαλείας έχουν πολλαπλασιαστεί και διαφοροποιηθεί ως προς τους σκοπούς και τις μεθόδους τους.

Οι Πολιτικές και τα Μέτρα Ασφαλείας έχουν σταδιακά και σε κάποιο βαθμό

αυξήσει την κατανόηση των απειλών ασφαλείας από τις εταιρείες, τις κυβερνήσεις και το κοινό και έχουν μειώσει τις πιθανότητας άμεσων παραβιάσεων συστημάτων. Στα τέλη της δεκαετίας του 1990 άρχισαν να εξελίσσονται νέες, έμμεσες, απειλές κατά των προσβάσιμων από το Διαδίκτυο υπολογιστικών πόρων. Οι απειλές αυτές, οι *Επιθέσεις Άρνησης Υπηρεσίας*, δεν αποβλέπουν στην καθ' αυτή παραβίαση συστημάτων αλλά στην παρεμπόδιση τους να παρέχουν χρήσιμες υπηρεσίες σε οποιονδήποτε, ουσιαστικά στην αχρήστευση τους. Τα περιστατικά αυτού του είδους κλιμακώθηκαν θεαματικά στην αρχή του 2000 με συστηματικές και αυτοματοποιημένες επιθέσεις εξάντλησης των δικτυακών και υπολογιστικών πόρων, ως *Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας* (*Distributed Denial of Service Attacks – DDoS*). Χαρακτηριστικές ήταν οι επιθέσεις σε έναν αριθμό από σημαντικές εταιρείες του Διαδικτύου (Yahoo, eBay, Buy.com, Amazon.com και CNN.com) στο διάστημα 7-9 Ιανουαρίου 2000 [Comp00]. Ο οικονομικές επιπτώσεις αλλά και ο αντίκτυπος στην κοινή γνώμη ήταν τέτοιοι που οι επιθέσεις αυτές χαρακτηρίστηκαν «θανατηφόρες» για το Διαδίκτυο αλλά και για την παγκόσμια οικονομική δραστηριότητα γενικότερα, όπως εκφράζεται χιουμοριστικά στο Σχήμα 1.1 που παρουσιάζει ένα σκίτσο του 2000. Στην εποχή μετά τα τρομοκρατικά χτυπήματα της 11ης Σεπτεμβρίου 2001 και την επακόλουθη ενεργοποίηση ασφαλείας οι επιθέσεις DDoS θεωρούνται και σημαντική απειλή εναντίον των κρίσιμων υποδομών (critical infrastructure) των κρατών.

Σχήμα 1.1: Σκίτσο του Kevin Siers στην εφημερίδα The Charlotte Observer που αποδίδει χιουμοριστικά τον αντίκτυπο των επιθέσεων DDoS του 2000

Μια σειρά από χαρακτηριστικά καθιστούν την επίδραση αυτού του είδους των επιθέσεων σημαντική:

- Υψηλή ταχύτητα εξέλιξης με μεγάλο όγκο κίνησης
- Πολλαπλά σημεία προέλευσης για τα οποία όμως συνήθως υπάρχει δυσκολία προσδιορισμού λόγω της χρήσης μεθόδων συγκάλυψης (IP address spoofing)
- Μικρή δυνατότητα ελέγχου και αντίδρασης στο τελικό θύμα

Το σημαντικό πρόβλημα των επιθέσεων DDoS, η σφοδρότητα και ταχύτητα εξέλιξης των περιστατικών στα οποία χρησιμοποιούνται αλλά και οι αδυναμίες

των υπαρχόντων λύσεων αποτέλεσαν το έναυσμα της παρούσας διατριβής.

Η αποτελεσματική αντιμετώπιση των επιθέσεων DDoS απαιτεί μεγάλης κλίμακας συνεργασίες ανάμεσα σε πολλά διαφορετικά δίκτυα. Αυτό έχει αποδειχτεί στην πράξη με τις επικοινωνίες των διαχειριστών δικτύων σε περιπτώσεις επιθέσεων, που μεταφέρουν πληροφορίες αντιμετώπισης βασιζόμενοι στις σχέσεις συνεργασίας και την προσωπική εμπιστοσύνη. Προφανώς μια τέτοια προσέγγιση δεν προσφέρει ταχύτητα, αυτοματισμό ή δυνατότητες κλιμάκωσης.

1.2 Η Εξέλιξη μιας Ιδέας για τη Λύση του Προβλήματος

Από το 1996, όταν τα προβλήματα ασφαλείας στο Διαδίκτυο αφορούσαν κατά κύριο λόγο απλά περιστατικά παραβίασης, στο Ελληνικό Ακαδημαϊκό Διαδίκτυο [Gune][1] είχε προταθεί από την ομάδα που ήταν επιφορτισμένη με την ανάπτυξη υπηρεσιών ασφαλείας (μέλος της οποίας ήταν και ο γράφων) η δημιουργία ενός ξεχωριστού δικτύου για την ανταλλαγή επικοινωνιών σε περιπτώσεις έκτακτων περιστατικών. Η πρόταση αυτή προέβλεπε τη δημιουργία καναλιών εξασφαλισμένου εύρους με τη χρήση ιδιωτικών εικονικών δικτύων τα οποία θα τερματίζονταν στα κατά τόπους κέντρα διαχείρισης δικτύων και θα παρείχαν κρυπτογραφημένες επικοινωνίες. Το έργο οδήγησε στην υλοποίηση ενός πρωτότυπου τέτοιου δικτύου το οποίο δοκιμάστηκε επιτυχώς και παρουσιάστηκε στο [Prev99].

Ο γράφων είχε επίσης την ευκαιρία να παρακολουθήσει από κοντά την εκπό-

[1] Επρόκειτο για το έργο GUnet, ανάπτυξης υπηρεσιών για τα ελληνικά ακαδημαϊκά ιδρύματα τα οποία διασυνδέονται διαμέσου του Εθνικού Δικτύου Έρευνας και Τεχνολογίας.

νηση του διδακτορικού του Π. Αστήθα [Αστη01] στο οποίο γινόταν συνδυασμός αναφορών από πολλά σημεία ενός τοπικού δικτύου προκειμένου να διαπιστωθούν σύνθετα και μικρού αντίκτυπου (small footprint) περιστατικά ασφαλείας. Η εργασία αυτή οδήγησε στην ανάπτυξη ορισμένων τεχνικών συλλογής στοιχείων που καταδείκνυαν διάφορα περιστατικά [Asti01b] και στην υλοποίηση ενός κεντρικού (σε επίπεδο Τοπικού Δικτύου) σημείου αναφοράς, όπου δεδομένα μπορούσαν να συνδυαστούν και να οδηγήσουν σε ανίχνευση ακόμα και αν οι επιμέρους αισθητήρες δεν είχαν διαγνώσει ένα συγκεκριμένο περιστατικό.

Ένα άλλο στοιχείο στην εξέλιξη της παρούσας διατριβής ήταν η λύση για το συντονισμό μεταξύ αυτόνομων διασυνδεμένων δικτυακών οντοτήτων στο έργο ΠΕΝΕΔ99 [Πενε99]. Στο έργο αυτό επιχειρήθηκε να δοθεί μια λύση σε προβλήματα διαχείρισης από άκρο-σε-άκρο (end-to-end) σε περιβάλλον πολλαπλών δικτύων (network administrative domains), κυρίως εξασφάλισης εύρους ζώνης (bandwidth). Η λύση που προκρίθηκε, αναλύθηκε και υλοποιήθηκε δοκιμαστικά ήταν η χρήση ενδιάμεσων συστημάτων συνεργασίας («χειριστών bandwidth» –"bandwidth brokers") σε κάθε ένα επιμέρους δίκτυο, οι οποίοι (βάσει των αιτημάτων των τελικών χρηστών) επικοινωνούσαν μεταξύ τους, ανέλυαν το πρόβλημα σε επίπεδο domain και μέσω συνεργατικών μηχανισμών έλυναν τα διαχειριστικά αιτηματα από άκρο-σε-άκρο. Τα κύρια αποτελέσματα και συμπεράσματα της εργασίας αυτής παρουσιάζονται στο [Stam01].

Την περίοδο 1996-1998 ο γράφων συμμετείχε στην προσπάθεια του Κέντρου Ελέγχου Δικτύου του Ε.Μ.Π. για δημιουργία του GRNET-CERT, της πρώτης στον Ελληνικό χώρο Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας (Compuputer Emergency Responce Team – CERT), με σκοπό να παρέχει υπηρεσίες στο Ελληνικό Ακαδημαϊκό Δίκτυο και τους χρήστες του. Στα πλαίσια

αυτής της εργασίας αποκτήθηκε σημαντική εμπειρία πάνω στον τρόπο λειτουργίας αυτών των ομάδων καθώς και για τις διαδικασίες συνεργασίας μεταξύ τους: οι ομάδες αυτές δημιουργούν ένα «ιστό» εμπιστοσύνης μεταξύ τους ώστε σε περίπτωση ανάγκης η επικοινωνία τους να είναι ευκολότερη. Παρόλα αυτά το κύριο συμπέρασμα ήταν ότι οποιαδήποτε συνεργασία έπρεπε να γίνει αποκλειστικά ανάμεσα σε ανθρώπους-μέλη των ομάδων αυτών με χρονοβόρες διαδικασίες, όπως τα τηλεφωνήματα και το ηλεκτρονικό ταχυδρομείο. Η διαπίστωση αυτή συνέτεινε στην κατανόηση της αξίας αυτόματων λύσεων συνεργασίας μεταξύ διαφορετικών φορέων.

Τέλος μια από τις προταθείσες ερευνητικές λύσεις στις επιθέσεις DDoS αποτέλεσε το έναυσμα της παρούσας διατριβής: Στην εργασία τους [Maha02] οι R. Mahajan, S. Bellovin και οι συνεργάτες τους παρέχουν μια ικανοποιητική προσέγγιση για την ανίχνευση (με μεγάλη λεπτομέρεια) επιθέσεων DDoS. Οι ανωτέρω πρότειναν το πρωτόκολλο *Pushback* για τη μεταβίβαση της πληροφορίας ανίχνευσης μεταξύ δρομολογητών προς την κατεύθυνση της διαφαινόμενης πηγής της επιθετικής κίνησης. Οι κατά τόπους δρομολογητές αναλαμβάνουν τη λήψη μέτρων περιορισμού της κίνησης[2].

1.3 Η Προτεινόμενη Λύση

Η προτεινόμενη στην παρούσα διατριβή λύση επιδίωξε αρχικά να ξεπεράσει το πρόβλημα της κλιμάκωσης σε πολλαπλά δίκτυα (domains) που φαινόταν να περιορίζει διάφορες από τις προταθείσες λύσεις εναντίον των επιθέσεων DDoS. Οι επιθέσεις αυτές είναι σε πολύ μεγάλο βαθμό κατανεμημένες και διαπερνούν

[2]Η λύση αυτή παρουσιάζεται με μεγαλύτερη λεπτομέρεια στο κεφ. 2 και συγκρίνεται αναλυτικά με την προτεινόμενη στην παρούσα διατριβή λύση στο κεφ. 6

μεγάλο αριθμό δικτύων πριν καταλήξουν στον τελικό στόχο. Στο δίκτυο-στόχο δεν είναι δυνατός ο άμεσος έλεγχος της εισερχόμενης κίνησης· είναι πλέον αργά για να ληφθούν μέτρα αποφυγής της κατάληψης δικτυακών πόρων στην κατεύθυνση εισόδου. Ένας τέτοιος έλεγχος πρέπει αναγκαστικά να γίνει στο δίκτυο (ή τα δίκτυα) που αποτελούν προηγούμενα βήματα στο μονοπάτι της επίθεσης. Πολλές από τις προταθείσες λύσεις ενώ έχουν τη δυνατότητα να ανιχνεύσουν μια επίθεση DDoS, να μεταδώσουν από σύστημα σε σύστημα την πληροφορία και να εφαρμόσουν μέτρα καταστολής της, αναγκαστικά σταματούν στα όρια της δικτυακής τους περιοχής.

Το συγκεκριμένο πρόβλημα παρουσιάζει κάποιες ομοιότητες με αυτό της συνεργατικής διαχείρισης δικτυακών πόρων από άκρο-σε-άκρο διαμέσου πολλαπλών domains[3] δέσμευσης bandwidth σε διαφορετικά δίκτυα (ανεξάρτητες δικτυακές διαχειριστικές περιοχές – domains[4]) που μεσολαβούν ανάμεσα σε δύο απομακρυσμένα άκρα και το οποίο αναφέρθηκε προηγουμένως. Στη διατριβή αυτή χρησιμοποιούνται ανεξάρτητες Οντότητες υλικού και λογισμικού, οι «*Συνεργατικές Οντότητες*» οι οποίες λειτουργώντας σε κάθε δίκτυο διασυνδέονται σε ένα γενικότερο υπερκείμενο (overlay) δίκτυο αυτόματης και ασφαλούς συνεργασίας, τη «*Συνεργατική Υποδομή*». Το πρότυπο λειτουργίας αυτής της συνεργασίας δίνεται από τις ομάδες CERT με αυτοματοποίηση όμως των αντίστοιχων ενεργειών.

Η διατριβή αυτή μελετά όλα τα θέματα που τίθενται από αυτή τη λύση για την αντιμετώπιση των επιθέσεων DDoS:

- Είδος της πληροφορίας που πρέπει να μεταφέρεται μεταξύ των μελών της

[3]βλέπε και το [Stam01] που αναφέρθηκε προηγουμένως

[4]Ταυτίζονται επίσης με το Αυτόνομο Σύστημα (Autonomous System – AS) που χρησιμοποιείται κατά τη δρομολόγηση με το πρωτόκολλο BGP.

Συνεργασίας για την ανταλλαγή πληροφοριών ανίχνευσης μεταξύ των δικτύων (domains/Autonomous Systems)

- Τρόπος χρήσης της επικοινωνιακής υποδομής χαμηλού επιπέδου.
- Πρωτόκολλα επικοινωνίας και μεταφοράς της ανωτέρω πληροφορίας.
- Σημασία που αποδίδεται στα μηνύματα επικοινωνίας και συμπεράσματα που μπορούν να εξαχθούν από την ανταλλασσόμενη πληροφορία: επιβεβαίωση ανίχνευσης του περιστατικού, κύρια χαρακτηριστικά του, μονοπάτι που ακολουθεί από δίκτυο σε δίκτυο.
- Ανάληψη ενεργειών αντιμετώπισης περιστατικού με παράλληλη διατήρηση της διαχειριστικής ανεξαρτησίας κάθε δικτύου.

Η εργασία επίσης, εξετάζει τις κύριες παραμέτρους που επηρεάζουν τη λειτουργία των επιμέρους συστημάτων σε κάθε δίκτυο αλλά και της συνολικής Συνεργατικής Αρχιτεκτονικής.

Τέλος, μέσω προσομοιώσεων, αναλύεται η επίδοση της προτεινόμενης λύσης σε ένα περιβάλλον πολλαπλών δικτύων, για διάφορες επιδόσεις ανίχνευσης πρωτογενούς επιπέδου (στα τοπικά συστήματα ανίχνευσης – Intrusion Detection Systems), και για διάφορες περιπτώσεις βαθμού εμπιστοσύνης μεταξύ των δικτύων. Τα αποτελέσματα δείχνουν ότι η προτεινόμενη αρχιτεκτονική μπορεί να επιτύχει συνολική και αυτόματη ανίχνευση περιστατικών DDoS καθώς και εντοπισμό των διαδρομών τους αποτελεσματικότερα από οποιαδήποτε λύση αντιμετώπισης σε ένα μοναδικό δίκτυο. Επιπλέον, από τα αποτελέσματα των προσομοιώσεων φαίνεται ότι η αποδοτικότητα της πρότασης είναι ευθέως

ανάλογη του βαθμού συνεργασίας που θα επιλέξουν να έχουν μεταξύ τους τα επιμέρους δίκτυα.

1.4 Παρουσίαση των Περιεχομένων

Η παρούσα εργασία διαρθρώνεται ως εξής:

Το Κεφάλαιο 2 παρουσιάζει μια εις βάθος ανάλυση των Επιθέσεων Άρνησης Υπηρεσίας (DoS και DDoS) και των κύριων ζητημάτων που θέτουν για οποιαδήποτε προσέγγιση αντιμετώπισης, ποιες είναι οι κύριες ερευνητικές κατευθύνσεις σε αυτόν τον τομέα και ποιες οι πιο γνωστές και χαρακτηριστικές λύσεις σε κάθε κατηγορία.

Στο Κεφάλαιο 3 γίνεται η παρουσίαση της προτεινόμενης λύσης της Συνεργατικής Αρχιτεκτονικής. Παρουσιάζονται τα κύρια τμήματα που την αποτελούν και πως διαρθρώνεται σε ένα περιβάλλον πολλαπλών δικτυακών διαχειριστικών περιοχών (domains). Γίνεται επίσης μια αναλυτική παρουσίαση των διαφορετικών μεθοδολογιών επικοινωνίας που μπορούν να χρησιμοποιηθούν για την υλοποίηση της Συνεργατικής Υποδομής και τα κύρια χαρακτηριστικά που εμφανίζει η κάθε προσέγγιση. Τέλος παρατίθενται τα θέματα ασφάλειας της προτεινόμενης αρχιτεκτονικής και πως αυτά μπορούν να αντιμετωπιστούν αποτελεσματικά.

Στο Κεφάλαιο 4 γίνεται μια εις βάθος παρουσίαση της αρχιτεκτονικής του λογισμικού και της λειτουργίας του βασικού τμήματος της Συνεργατικής Υποδομής, της Συνεργατικής Οντότητας (Cooperative Entity). Πρόκειται για το σύστημα που εγκαθίσταται σε κάθε ένα δίκτυο (domain) και προσφέρει υπηρεσίες επικοινωνιών, ανάλυσης πληροφοριών και ανάληψης ενεργειών σύμφωνα με τις ρυθμίσεις λειτουργίας που αποφασίζονται από τις τοπικές πολιτικής δια-

χείρισης. Στο κεφάλαιο αυτό παρουσιάζεται επίσης ένας αλγόριθμός βάσει του οποίου είναι δυνατή από τη συλλογή των επιμέρους πληροφοριών να καταδειχθεί ένα (τουλάχιστον) τμήμα του δικτυακού μονοπατιού της επίθεσης DDoS.

Στο Κεφάλαιο 5 παρουσιάζονται μια σειρά από προσομοιώσεις που έγιναν προκειμένου να μελετηθεί η λειτουργία της Συνεργατικής Υποδομής. Αρχικά αναλύονται τα αναμενόμενα χαρακτηριστικά των κύριων παραγόντων που επηρεάζουν μια τέτοια προσομοίωση (λειτουργία συστημάτων IDS, χαρακτηριστικά επιθέσεων, λειτουργία δικτύων επικοινωνίας της Συνεργατικής Υποδομής) και εξηγούνται οι επιλογές που έγιναν στην προσομοίωσή τους. Παρουσιάζονται τα αποτελέσματα των προσομοιώσεων που αφορούν τις κύριες παραμέτρους ρύθμισης της Συνεργατικής Υποδομής και αξιολογείται η αποτελεσματικότητα της παρούσας κατανεμημένης προσέγγισης.

Τέλος, στο Κεφάλαιο 6 η λύση συγκρίνεται με άλλες αντίστοιχες που έχουν προταθεί για την αντιμετώπιση του ίδιου προβλήματος. Στη συνέχεια παρουσιάζονται τα συμπεράσματα της παρούσας εργασίας καθώς και θέματα που μπορούν να αποτελέσουν αντικείμενο μελλοντικών επεκτάσεων όπως και περαιτέρω έρευνας.

Κεφάλαιο 2

Επιθέσεις Άρνησης Υπηρεσίας

2.1 Εισαγωγή - Η Εξέλιξη των Επιθέσεων DoS

Ο χαρακτηρισμός «Επιθέσεις Άρνησης Υπηρεσίας» (Denial of Service – DoS) αναφέρεται σε περιστατικά ασφαλείας που αποσκοπούν στη διατάραξη της κανονικής λειτουργίας υπολογιστικών συστημάτων ή δικτύων. Οι επιθέσεις DoS, αφορούν στη μείωση απόδοσης υπολογιστικών συστημάτων, ή δικτυακών συνδέσεων, χωρίς να έχει μεσολαβήσει κάποια παραβίαση. Πρόκειται για επιθέσεις πού δεν έχουν ως σκοπό την άμεση παραβίαση και την απόκτηση ελέγχου αλλά την παρεμπόδιση εκτέλεσης λειτουργιών. Αποτελούν έτσι απειλές διαφορετικές από αυτές που τα καθιερωμένα πρότυπα ασφάλειας είναι σχεδιασμένα να αντιμετωπίσουν, όπως είναι π.χ. η μη εξουσιοδοτημένη πρόσβαση, η υποκλοπή δεδομένων κ.λπ.

Οι επιθέσεις αυτού του είδους συνήθως πραγματοποιούνται από άτομα που δεν έχουν τη δυνατότητα ή το ενδιαφέρον να αποκτήσουν άμεση πρόσβαση στα υπολογιστικά συστήματα. Η φιλοσοφία των επιθέσεων άρνησης υπηρεσίας είναι

να διαταραχθεί η παροχή πόρων και υπηρεσιών στο Διαδίκτυο προς τους νόμιμα ενδιαφερόμενους. Εντούτοις, σε ορισμένες περιπτώσεις, τα ίδια περιστατικά μπορούν να χρησιμοποιηθούν για να υπερφορτώσουν ή έστω να απασχολήσουν τα «Συστήματα Ανίχνευσης Επιθέσεων» (Intrusion Detection Systems - IDS) και διαχειριστές, ώστε να περάσουν απαρατήρητες άλλες τεχνικές παράνομης εισόδου στα συστήματα με σκοπό τον έλεγχο ή και την αλλοίωση πληροφοριών.

Η κύρια αιτία για την εμφάνιση αυτού του είδους των επιθέσεων είναι η επικράτηση του Διαδικτύου ως το κύριο περιβάλλον οικονομικής δραστηριότητας. Προβλήματα μη διαθεσιμότητας συστημάτων και υπηρεσιών γίνονται γνωστά και αποκτούν ιδιαίτερη σημασία. Περιστατικά που στο παρελθόν θα περνούσαν απαρατήρητα έχουν άμεση επίδραση στο θύμα, τόσο οικονομική, όσο και στο κύρος του (μέσω της δημοσιότητας). Οι επιθέσεις άρνησης υπηρεσίας έχουν αυξημένο «αντίκτυπο» με μικρή μόνον προσπάθεια και μηδαμινό οικονομικό κόστος από την πλευρά του επιτιθέμενου, είναι συνεπώς μια ιδιαίτερα αποδοτική μέθοδος προσβολής ενός «στόχου». Στις περισσότερες περιπτώσεις δεν είναι δυνατόν να γίνει γνωστή η ταυτότητα του επιτιθέμενου. Το χαρακτηριστικό αυτό καθιστά τις επιθέσεις DoS ελκυστικές και για υποστήριξη αθέμιτων συμφερόντων. Ελεγχόμενες από κυβερνήσεις, θεωρητικά, μπορούν να αποτελέσουν αποτελεσματικό όπλο κυβερνοπολέμου.

Από τεχνικής πλευράς, σημαντικό ρόλο στην εξάπλωση των επιθέσεων DoS έπαιξε η τάση για την «ανοικτή» διασύνδεση των πληροφοριακών συστημάτων. Το στοιχείο αυτό εξέθεσε κρίσιμα (mission critical) συστήματα στις συγκεκριμένες απειλές, ακόμα και στις περιπτώσεις ισχυρής προστασίας τους από μη εξουσιοδοτημένη πρόσβαση. Η γενίκευση της χρήσης δικτυακών υπηρεσιών από το ευρύ κοινό αποκάλυψε και συνεχώς συνεχίζει να αποκαλύπτει προβλή-

ματα και αδυναμίες που δεν είχαν προβλεφθεί εξ αρχής. Προβλήματα εμφανίστηκαν ακόμα και στις υλοποιήσεις πρωτοκόλλων υποδομής του Διαδικτύου [Cert97] δημιουργώντας απειλές σε κάθε συνδεδεμένο σύστημα. Η πληροφορία για τις αδυναμίες αυτές σε πολλές περιπτώσεις διαδίδεται προτού γίνει δυνατή η δημιουργία και εγκατάσταση μέτρων προστασίας.

Μεγάλος αριθμός μη προστατευμένων προσωπικών υπολογιστών βρίσκεται σχεδόν μονίμως[1] συνδεδεμένος στο Διαδίκτυο επιτρέποντας σε κακόβουλους χρήστες, με μεθόδους που θα εξηγηθούν στη συνέχεια, να τους χρησιμοποιήσουν ως ενδιάμεσους σταθμούς (χωρίς τη γνώση και θέληση τους) για αυτοματοποιημένες επιθέσεις μεγάλης κλίμακας. Οι μη προστατευμένοι προσωπικοί υπολογιστές αποτελούν μια τεράστια «δεξαμενή» άντλησης δικτυακών πόρων για την πραγματοποίηση των επιθέσεων.

2.1.1 Εκμετάλλευση Προβλημάτων του Λογισμικού (Software Exploits)

Οι πιο απλές επιθέσεις άρνησης υπηρεσίας ξεκίνησαν ως δραστηριότητα που είχε ως στόχο συγκεκριμένους υπολογιστές χωρίς να μεσολαβήσει παραβίαση τους. Τα μέσα που χρησιμοποιούνται είναι προβλήματα και παραβλέψεις στην υλοποίηση λειτουργικών συστημάτων (ειδικότερα, σε πολλές περιπτώσεις, η ατελής υλοποίηση δικτυακών πρωτοκόλλων επικοινωνίας), ή προγραμμάτων εφαρμογής. Οι επιθέσεις αυτές εκμεταλλεύονται προβλήματα του λογισμικού για να διαταράξουν τη φυσιολογική λειτουργία.

[1] Οι συνδέσεις ADSL [Webo-a] και Cable Modem [Webo-b], αρκετά διαδεδομένες πλέον, επιτρέπουν τη συνεχή συνδεσιμότητα σε υψηλές ταχύτητες, χωρίς καμμία παρέμβαση από την πλευρά του χρήστη.

Οι επιθέσεις στο δικτυακό λογισμικό (protocol stack software), εκμεταλλεύονται την άμεση σύνδεση του με τον πυρήνα του λειτουργικού συστήματος. Μπορούν έτσι να επηρεάσουν άμεσα το υπολογιστικό σύστημα στόχο σε κρίσιμες λειτουργίες. Ορισμένα από τα προβλήματα είναι τόσο σημαντικά που ενδέχεται να οδηγήσουν στην επανεκκίνηση του υπολογιστή (reboot) ή και στην πλήρη διακοπή λειτουργίας του ("crash"). Ενδεικτικά αναφέρονται:

– Teardrop Attack: Ορισμένες υλοποιήσεις του μηχανισμού κατακερματισμού και επανασύνδεσης πακέτων IP δε μπορούσαν να χειριστούν τμήματα πακέτων που είχαν επικαλύψεις μεταξύ τους. Το αποτέλεσμα ήταν η διακοπή λειτουργίας του συστήματος όταν λαμβάνονταν τέτοια πακέτα IP. Η κύρια εφαρμογή που χρησιμοποιήθηκε για επίθεση με αυτό τον τρόπο είχε το όνομα «Teardrop» [Cert97].

– Ping of Death: Ο επιτιθέμενος αποστέλλει ένα πακέτο ICMP-echo-request μεγέθους μεγαλύτερου από το μέγιστο επιτρεπόμενο από τις προδιαγραφές του πρωτοκόλλου IP. Ο λήπτης δεν καταφέρνει να επανασυνδέσει τα τμήματα πακέτου που προκύπτουν και οδηγείται σε διακοπή λειτουργίας ή επανεκκίνηση [Inse96].

Ένας πολύ μεγάλος αριθμός λειτουργικών συστημάτων βρέθηκε να έχει αδυναμία σε αυτές και άλλες παρόμοιες επιθέσεις. Ακόμα και η λήψη ενός μοναδικού πακέτου, κατάλληλα κατασκευασμένου από κακόβουλη εφαρμογή, μπορεί να οδηγήσει στην απενεργοποίηση του συστήματος λήπτη. Η επαναφορά στην κανονική λειτουργία απαιτεί συνήθως επανεκκίνηση του συστήματος, με αντίστοιχο κίνδυνο απώλειας δεδομένων. Επίσης, η διαδικασία αυτή δεν εξασφαλίζει ότι το πρόβλημα δε θα επαναληφθεί στο μέλλον. Το σύστημα παραμένει

ευάλωτο μέχρι την εφαρμογή διορθωτικού κώδικα (patches).

Κατά αντίστοιχο τρόπο, και οι εφαρμογές που παρέχουν τις υπηρεσίες του συστήματος (π.χ. οι εξυπηρετητές Web) μπορούν να αποτελέσουν στόχο κάποιας τέτοιας επίθεσης που θα προσπαθήσει να εκμεταλλευτεί γνωστές αδυναμίες τους. Για παράδειγμα:

– Ο εξυπηρετητής Web IIS, στην έκδοση 5.0, επανεκκινείται όταν λάβει κλήσεις τύπου WebDAV με πολλαπλούς χαρακτήρες ελληνικού ερωτηματικού (semicolon – ;) [Osvd01]. Το πρόβλημα λύθηκε με διορθωτικό κώδικα της κατασκευάστριας εταιρείας [Micr01].

Οι περισσότερες από αυτές τις επιθέσεις είναι δυνατόν, εφόσον γίνουν γνωστή η μέθοδος που χρησιμοποιούν και τα ειδικά χαρακτηριστικά τους, να ανιχνευτούν από Δικτυακά Συστήματα Ανίχνευσης Επιθέσεων (Network Intrusion Detection Systems - NIDS) και να εμποδιστούν στα εξωτερικά συστήματα δικτυακής προστασίας (firewalls). Τα προβλήματα που τις προκαλούν μπορούν να διορθωθούν απ' ευθείας με την εφαρμογή διορθωτικού κώδικα στο απειλούμενο σύστημα λογισμικού. Ο κίνδυνος παραμένει εντούτοις από τυχόν αδυναμίες που θα εντοπιστούν μελλοντικά και θα γίνουν γνωστές σε κύκλους που ενδιαφέρονται να τις εκμεταλλευτούν προτού δημιουργηθούν οι απαραίτητες διορθώσεις. Είναι χαρακτηριστικό το γεγονός ότι νέες αδυναμίες χρησιμοποιούνται και για την «αστραπιαία» εξάπλωση [Stan02] [Cert01] «αυτόματα διαδιδόμενων ιών» (worms), με πολύ έντονες συνέπειες. Η μοναδική προφύλαξη που μπορεί να υπάρξει για τέτοιες μη προβλέψιμες απειλές είναι η συνεχής και έγκαιρη ενημέρωση των διαχειριστών υπολογιστικών συστημάτων για όλες τις νέες αδυναμίες και τους τρόπους προφύλαξης από αυτές. Ο διαχειριστής του εταιρικού

δικτύου (enterprise network) πρέπει να αναζητά ενημέρωση και από την ανεπίσημη κοινότητα των ασχολουμένων με την ασφάλεια (λίστες ηλεκτρονικού ταχυδρομείου, ιστοσελίδες κ.λπ.) και από επίσημους φορείς που αναλαμβάνουν να παρακολουθήσουν και να αντιμετωπίσουν τέτοιες απειλές, όπως οι ομάδες CERT[2] [Cert].

2.1.2 Επιθέσεις Εξάντλησης Πόρων

Επιθέσεις κερματισμού πακέτων IP, όπως το Teardrop, αποδεικνύουν ότι η υλοποίηση των συνηθισμένων δικτυακών πρωτοκόλλων, παρά την επιτυχία στη λειτουργία του Διαδικτύου, δεν είναι άριστη. Όταν οι κατασκευαστές κατάφεραν να περιορίσουν τις προφανείς αδυναμίες που οδηγούσαν στην παύση κανονικής λειτουργίας των συστημάτων, οι επιθέσεις εστιάστηκαν στην εξάντληση των υπολογιστικών ή δικτυακών πόρων τους. Χαρακτηριστική είναι η περίπτωση της επίθεσης SYN:

– Στην επίθεση αυτή αποστέλλεται ένας μεγάλος αριθμός καθ' όλα νόμιμων κλήσεων σύνδεσης υπηρεσίας TCP. Για κάθε μια από τις κλήσεις αυτές το σύστημα δηλώνει τη διαθεσιμότητα του και δεσμεύει κάποιους πόρους για να μπορέσει να προσφέρει τη ζητούμενη υπηρεσία. Ο επιτιθέμενος δεν προτίθεται να συνεχίσει και να ολοκληρώσει, σύμφωνα προς τις προδιαγραφές του TCP (three way handshake), τη σύνδεση με τον εξυπηρετητή. Εφόσον οι ίδιες, μη ολοκληρωμένες κλήσεις συνεχιστούν θα επέλθει κάποιο σημείο που οι διαθέσιμοι πόροι θα περιοριστούν σε τέτοιο βαθμό που, είτε θα απενεργοποιηθεί το σύστημα, είτε θα συνεχίσει

[2]Computer Emergency Response Teams–Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας.

μεν να λειτουργεί αλλά σε πολύ χαμηλές ταχύτητες και με περιορισμένες ουσιαστικά τις δυνατότητές του [Cert96].

Ένα χαρακτηριστικό αυτού του είδους των επιθέσεων είναι επίσης ότι, συνήθως, προκειμένου να μεγιστοποιηθούν οι συνέπειες χρησιμοποιούνται περισσότεροι του ενός επιτιθέμενοι υπολογιστές. Οι επιτιθέμενοι αποκτούν τον έλεγχο κάποιων συστημάτων και τα καθοδηγούν ώστε αυτά συγχρονισμένα να αποστείλουν παρόμοια κακόβουλη κίνηση προς το θύμα. Επίσης σε αυτού του είδους τις επιθέσεις χρησιμοποιήθηκε για πρώτη φορά η τακτική της παραποίησης της διεύθυνσης IP (address spoofing) του αποστολέα της κακόβουλης κίνησης για να μη μπορεί να εντοπισθεί και να σταματηθεί άμεσα. Και τα δύο αυτά, βασικά, χαρακτηριστικά των επιθέσεων αναλύονται περισσότερο στη συνέχεια. Τα μέτρα που λαμβάνονται για την προστασία των κρίσιμων πόρων έχουν τη μορφή διορθώσεων (patches) του δικτυακού κώδικα του λειτουργικού συστήματος. Τα μοντέρνα λειτουργικά συστήματα λαμβάνουν πλέον μέτρα ελέγχου της διάθεσης των πόρων και θέτουν αυστηρά όρια για τον τερματισμό του χρόνου αναμονής για μη ενεργές κλήσεις. Επίσης θεωρείται γενικώς καλή πρακτική να μην ενεργοποιούνται «θύρες» TCP ή UDP που αντιστοιχούν σε υπηρεσίες χωρίς πρακτική χρησιμότητα για την εξυπηρέτηση χρηστών. Ομοίως, συστήματα που αφορούν κρίσιμες (mission critical) υπηρεσίες οφείλουν να είναι επαρκώς προστατευμένα με μέτρα επαύξησης της διαθεσιμότητας και της απόδοσης τους, όπως πολλαπλούς εξυπηρετητές και συστήματα κατανομής της κίνησης. Όσον αφορά την παραποίηση διευθύνσεων, είναι δυνατόν να ελέγχονται στους παρόχους δικτυακών υπηρεσιών (Internet Service Providers — ISPs) τα πακέτα για διευθύνσεις αποστολέα που δεν αντιστοιχούν στο δίκτυο προέλευσης τους. Η

διαδικασία αυτή είναι μια ακόμα καλή πρακτική που μπορεί να αποτρέψει την αποστολή παραποιημένων πακέτων.

Οι αρχικές επιθέσεις εξάντλησης πόρων ευάλωτων υπολογιστικών συστημάτων κατέδειξαν ότι υπολογιστικοί και δικτυακοί πόροι μπορούν να αποτελέσουν στόχους. Ο επόμενος στόχος, που αποτελεί την πλέον διαδεδομένη επίθεση άρνησης υπηρεσίας σήμερα, ήταν το διαθέσιμο δικτυακό εύρος (bandwidth) του θύματος.

– Μια από τις πρώτες επιθέσεις αυτού του είδους ήταν η «πλημμύρα πακέτων ping» (ping flood), γνωστή επίσης και ως «Smurf attack» [Cert98]. Χρησιμοποιείται ένα μη κατάλληλα διασφαλισμένο ενδιάμεσο δίκτυο, στο οποίο στέλνεται ένα πακέτο ICMP-echo-request τη διεύθυνση «γενικής εκπομπής» (broadcast address). Το πακέτο είναι κατασκευασμένο κατά τέτοιο τρόπο ώστε η διεύθυνση αποστολέα να είναι αυτή του θύματος. Όλοι οι υπολογιστές στο τοπικό δίκτυο θα το λάβουν και θα απαντήσουν με ICMP-echo-reply προς το θύμα. Η επίθεση θα καταλάβει εύρος δικτύου πολλαπλασιαζόμενο επί τον αριθμό συστημάτων που θα απαντήσουν δημιουργώντας εν τέλει μια «πλημμύρα» κίνησης. Θεωρείται έτσι ότι η επίθεση έχει ένα «πολλαπλασιαστικό παράγοντα ενίσχυσης» (attack amplification factor). Η προστασία από αυτού του είδους την επίθεση μπορεί να είναι μόνον προληπτική εφόσον οι διαχειριστές των δικτύων ακολουθούν μια σειρά από «καλές πρακτικές». Μεταξύ αυτών περιλαμβάνεται και η απαγόρευση πακέτων ICMP προς τη διεύθυνση γενικής εκπομπής (IP directed broadcasts) ειδικά αν αυτά προέρχονται εκτός του δικτύου [Cisc-a].

2.2 Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας

2.2.1 Περιγραφή

Οι «Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας» (Distributed Denial of Service Attacks - DDoS) εναντίον δικτυακών πόρων, είναι οι πλέον διαδεδομένες σήμερα αλλά ταυτόχρονα και οι δυσκολότερες στην αντιμετώπιση. Πρόκειται για συντονισμένες, από πολλές πηγές, αποστολές κίνησης προς έναν ή περισσότερους υπολογιστές ενός δικτύου. Σκοπός τους, είναι η εξάντληση των υπολογιστικών πόρων του συστήματος στόχου, ή συνηθέστερα, του διαθέσιμου εύρους ζώνης του δικτύου σε τέτοιο βαθμό που να καθίσταται προβληματική η συνδεσιμότητα με το υπόλοιπο Διαδίκτυο. Το πρόβλημα επιτείνεται λόγο μιας σειράς ειδικών χαρακτηριστικών των επιθέσεων αυτού του είδους και κυρίως της κατανεμημένης φύσης της κακόβουλης κίνησης.

Η κατανεμημένη επίθεση άρνησης υπηρεσίας είναι μια διαδικασία πολλών βημάτων. Οι επιτιθέμενοι χρησιμοποιούν ένα αριθμό από συστήματα παραβιασμένα (hacked) και ελεγχόμενα με εισηγμένο κώδικα «δούρειο ίππο» ("trojaned"). Αρχικά, μετά από παραβίαση, εγκαθιστούν δύσκολα ανιχνεύσιμο κώδικα, σε ένα αριθμό από συστήματα που θα παίζουν το ρόλο του πρώτου επιπέδου, των «ελεγκτών» της επίθεσης ("masters"). Τα συστήματα αυτά είναι που αναλαμβάνουν επίσης την οικοδόμηση μιας υποδομής κατάλληλης για την πραγματοποίηση επιθέσεων με την παραβίαση και τον έλεγχο επιπλέον συστημάτων. Με μεθοδική εξέταση εντοπίζουν υπολογιστές, στη συνηθέστερη περίπτωση προσωπικούς, με γνωστές αδυναμίες τις οποίες στη συνέχεια χρησιμοποιούν για να

αποκτήσουν τον έλεγχο τους[3]. Σε αυτούς, χωρίς την επίγνωση των χρηστών τους εγκαθίσταται «προγράμματα ελέγχου» που θα επιτελέσουν τις λειτουργίες της επίθεσης[4]. Είναι δυνατόν η ύπαρξη της παραβίασης να μη γίνει γνωστή, εκτός αν χρησιμοποιηθεί κάποιο προσωπικό σύστημα δικτυακής προστασίας (personal firewall) ή αναλυθεί το σύστημα με ειδικά εργαλεία ασφαλείας (audit tools). «Κλασικές» μέθοδοι μόλυνσης με ιούς (viruses) ή αυτόματα διαδιδόμενους ιούς (worms) είναι επίσης δυνατόν να χρησιμοποιηθούν για την αυτοματοποιημένη διάδοση των προγραμμάτων ελέγχου [Netc04]. Τα κακόβουλα προγράμματα που έχουν εισαχθεί παραμένουν σε ανενεργή κατάσταση, μέχρι να λάβουν την κατάλληλη εντολή, και τα συστήματα φορείς περιγράφονται με τον όρο «ζόμπι» ("zombies") ή "bots"[5]. Αποτελούν τα εκτελεστικά όργανα της επίθεσης, αντιπροσώπους ("agents") δεύτερου επιπέδου. Η μορφή μιας Κατανεμημένης Επίθεσης Άρνησης Υπηρεσίας, όπως περιγράφτηκε, φαίνεται στο σχήμα 2.1.

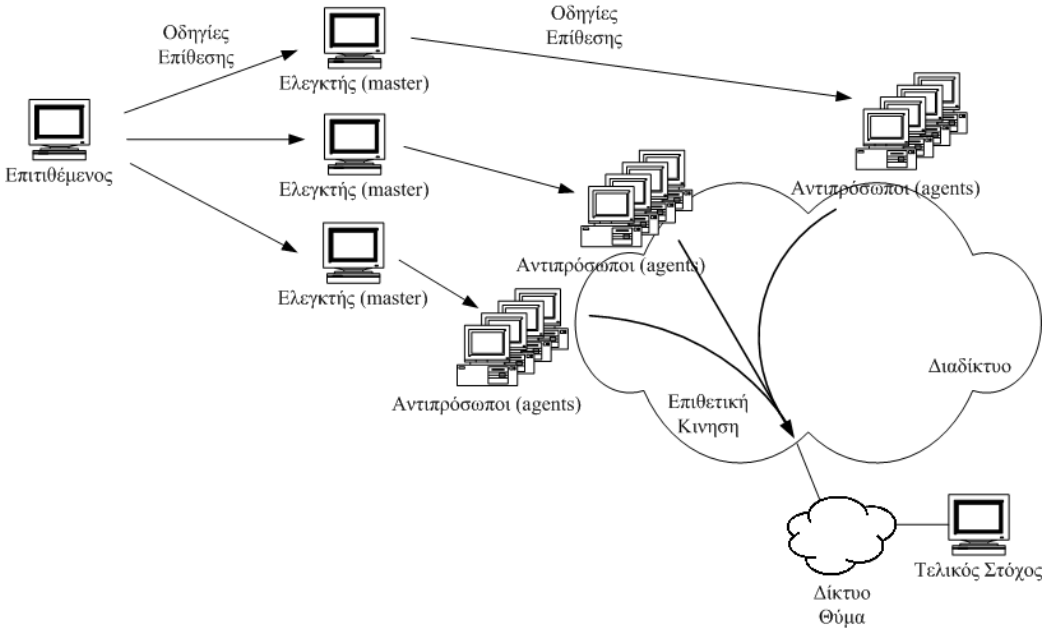
Η οργάνωση της υποδομής επιθέσεων με τον έλεγχο αντιπροσώπων γίνεται απόλυτα αυτοματοποιημένα με εργαλεία λογισμικού που είναι διαθέσιμα στο Διαδίκτυο και περιγράφονται ως «εργαλεία απόκτησης δικαιωμάτων διαχειριστή» (rootkits). Παραδείγματα αυτών είναι τα "Trinoo" [Ditt99a], "Stacheldraht"[6] [Ditt99b]και "TFN2K" [Barl00]. Πρόκειται για συλλογές προγραμμάτων που για διάφορες αρχιτεκτονικές και λειτουργικά συστήματα αναλαμβάνουν αυτόματα τις διαδικασίες εξεύρεσης υπολογιστών με αδυναμίες και εγκατάστα-

[3]Ο «έλεγχος» σε αυτή την περίπτωση δεν είναι αναγκαστικά απόλυτος, όπως σε παλαιότερα είδη επιθέσεων. Οι χρήστες εξακολουθούν να μπορούν να χρησιμοποιήσουν το σύστημα ενώ εκτελούνται, εν αγνοία τους, και άλλες εφαρμογές.

[4]Εννοείται ότι παρόμοιος κώδικας μπορεί να χρησιμοποιηθεί και για την υποκλοπή πληροφοριών από τον υπολογιστή.

[5]Από το "robot".

[6]Μεταφράζεται ως «Αγκαθωτό Συρματόπλεγμα».



Σχήμα 2.1: Οργάνωση επίθεσης DDoS

σης του κώδικα των αντιπροσώπων.

Η υποδομή επίθεσης που έχει δημιουργηθεί ελέγχεται με διάφορους τρόπους. Για παράδειγμα, μια από τις μεθόδους που χρησιμοποιούνται είναι η σύνδεση των κακόβουλων προγραμμάτων σε ιδιωτικούς χώρους δικτυακών συζητήσεων (Internet Relay Chat—IRC), όπου ο επιτιθέμενος μπορεί να μεταδώσει κατάλληλες οδηγίες για τη λειτουργία τους [Gibs04]. Εντούτοις είναι δυνατόν να υπάρχουν πολλά επίπεδα στη διαδικασία ελέγχου, με τον οργανωτή της επίθεσης να δίνει οδηγίες στο πρώτο επίπεδο, σε ένα μικρό αριθμό από «ελεγκτές», οι οποίοι στη συνέχεια να ενεργοποιούν το δεύτερο επίπεδο όπου οι αντιπρόσωποι θα εκτελέσουν την επίθεση. Το σύστημα ελέγχου της υποδομής δίνει στον επιτιθέμενο την ευελιξία να επιλέγει και να αλλάζει στόχους, να ενεργοποιεί και να απενεργοποιεί διαφορετικές πηγές ή να αλλάζει τα χαρακτηριστικά της

κίνησης ανάλογα με την αντίδραση των δικτύων στόχων. Η τελευταία δυνατότητα μπορεί να καταστήσει πολλά από τα αμυντικά μέτρα ανώφελα ειδικά αν δε συνδυάζονται με γρήγορες αντιδράσεις[7].

Όταν δεχτούν την κατάλληλη εντολή τα κακόβουλα προγράμματα στους υπό έλεγχο υπολογιστές θα ξεκινήσουν την αποστολή δικτυακής κίνησης προς το στόχο. Η κίνηση αυτή μπορεί να είναι σε οποιοδήποτε πρωτόκολλο (TCP, UDP ή ICMP) ή θύρα επικοινωνίας (port). Στην πηγή, λόγο του μικρού της μεγέθους, η δικτυακή αυτή κίνηση είναι δύσκολο να γίνει αντιληπτή (αν και υπάρχουν ερευνητικές προσπάθειες σε αυτή τη κατεύθυνση [Reih02]). Αντιθέτως κοντά στον προορισμό όλες οι ροές κίνησης[8] (flows) συνδυάζονται και έχουν σαν αποτέλεσμα τη μεγάλη επιβάρυνση του θύματος. Ακόμα και αν το δίκτυο στόχος απορρίψει την κακόβουλη εισερχόμενη κίνηση στο δρομολογητή εισόδου (ingress router) αυτή θα εξακολουθήσει να καταλαμβάνει εύρος ζώνης στη γραμμή και να αποκλείει τη φυσιολογική επικοινωνία.

Τα σύγχρονα λειτουργικά συστήματα παρέχουν προγραμματιστική υποδομή (συναρτήσεις "raw sockets") που επιτρέπει στο χρήστη τη δημιουργία πακέτων δεδομένων ειδικών χαρακτηριστικών (και κατ' επέκταση με παραποιημένες διευθύνσεις αποστολέα—spoofing). Η δυνατότητα αυτή ισχύει για τους χρήστες

[7]Μια Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας που στοχεύει στην εξάντληση δικτυακών πόρων, ιδιαίτερα δύσκολο να αντιμετωπιστεί, είναι η λεγόμενη "Whack-A-Mole" όπου τα χαρακτηριστικά της κακόβουλης κίνησης αλλάζουν διαρκώς. Είναι δυνατόν περιοδικά να ενεργοποιούνται διαφορετικές ομάδες επιτιθέμενων και να εναλλάσσονται τα πρωτόκολλα και οι θύρες.

[8]Αναφέρεται ο όρος «ροή κίνησης» με την ίδια σημασία που έχει όταν χρησιμοποιείται ως παράμετρος μέτρησης της απόδοσης του δικτύου κατά τον ορισμό που έχει γίνει για το εργαλείο Cisco Netflow [Cisc-net]: μια ομάδα πακέτων από την ίδια προέλευση προς τον ίδιο τελικό προορισμό που απέχουν χρονικά μεταξύ τους ένα συγκεκριμένο (μικρό) χρονικό διάστημα.

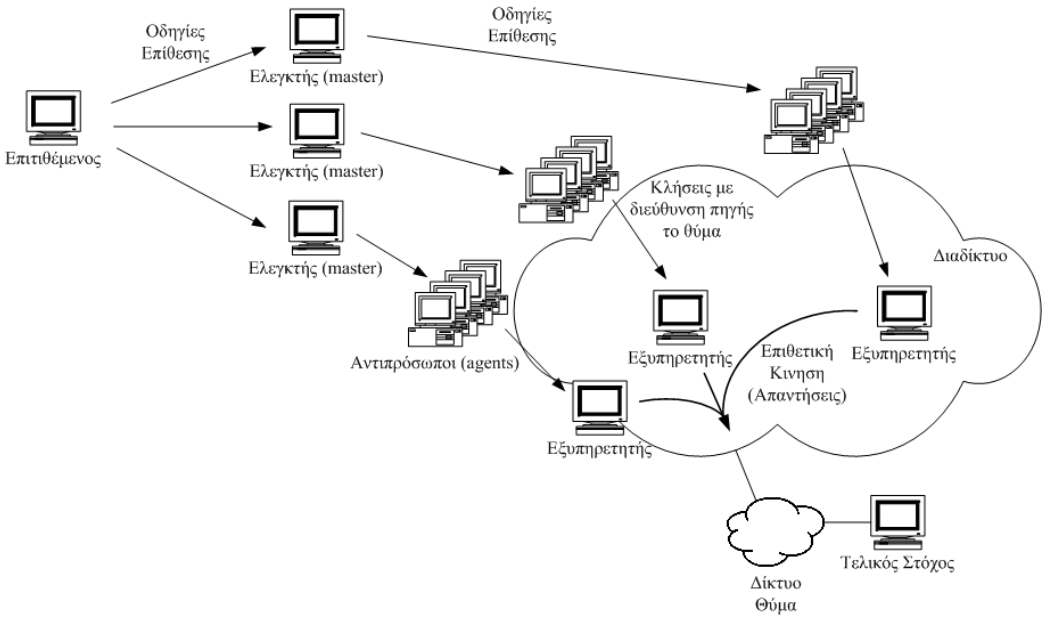
με δικαιώματα διαχειριστή[9] στα Linux/UNIX, για όλους τους χρήστες στα MS-Windows XP[10], ενώ δεν ήταν διαθέσιμη στις προγενέστερες εκδόσεις των MS-Windows. Έτσι τα πακέτα που χρησιμοποιούνται στις επιθέσεις άρνησης υπηρεσίας έχουν παραποιημένη τη διεύθυνση αποστολέα ώστε να μην είναι η πραγματική τους. Αυτό καθιστά αδύνατη την εύρεση των ελεγχόμενων συστημάτων που πραγματοποιούν τις επιθέσεις με απλή αναζήτηση της διεύθυνσης τους.

Εκτός από πολλαπλά επίπεδα οργάνωσης και ελέγχου, μια κατανεμημένη επίθεση άρνησης υπηρεσίας είναι δυνατόν να χρησιμοποιεί και πολλαπλά επίπεδα μεταβίβασης της κακόβουλης κίνησης. Τα συστήματα που εκτελούν την επίθεση αντί να στείλουν τα ίδια μία ροή κίνησης προς το θύμα πραγματοποιούν νόμιμες κλήσεις σε εξυπηρετητές του Διαδικτύου, παραποιώντας όμως στο πακέτο τη διεύθυνση του αποστολέα (αυτού που κάνει την αίτηση υπηρεσίας) ώστε να είναι αυτή του θύματος. Οι εξυπηρετητές απαντώντας κανονικά (εκτελώντας το δικό τους τμήμα του TCP three-way-handshake) στέλνουν τον ίδιο όγκο κίνησης προς το θύμα (στη μορφή πακέτων TCP/ACK-SYN). Η μέθοδος αυτή έχει την ονομασία «επίθεση ανάκλασης» (reflection attack) [Paxs01] είναι ιδιαίτερα δύσκολο να αντιμετωπιστεί. Η μορφή της απεικονίζεται στο σχήμα 2.2.

Στην πλευρά του θύματος ενδεχόμενο φιλτράρισμα της κακόβουλης κίνησης σημαίνει αποκοπή δημοφιλών προορισμών του Διαδικτύου που συνεχίζουν τις απαντήσεις στις κακόβουλες κλήσεις. Εξάλλου, ορισμένες μορφές αυτής της επίθεσης χρησιμοποιούν και πρωτόκολλα TCP που είναι απαραίτητα στη

[9] Για συστήματα μοναδικού χρήστη η διαφορά δεν έχει σημασία αν αυτοί το χρησιμοποιούν πάντα με δικαιώματα διαχειριστή.

[10] Η δυνατότητα αυτή έχει αφαιρεθεί με την αναβάθμιση λογισμικού (Service Pack) επιπέδου 2



Σχήμα 2.2: Επίθεση DDoS μέσω Ανάκλασης

λειτουργία του Διαδικτύου, όπως π.χ. το DNS, το BGP[11] και άλλα.

2.2.2 Χαρακτηριστικά και Κατηγοριοποιήσεις των Επιθέσεων DDoS

Μια επίθεση DDoS παρουσιάζει στον τελικό αποδέκτη (αλλά και στα ενδιάμεσα δίκτυα που διατρέχει κατά την πορεία της) ένα αριθμό από χαρακτηριστικά που την περιγράφουν με συγκεκριμένο τρόπο και τη διακρίνουν από νόμιμες δραστηριότητες αλλά και από άλλες, πιθανά ταυτόχρονες, επιθέσεις. Τα στοιχεία αυτά χρησιμοποιούνται από τα συστήματα IDS για την περιγραφή της μετά την ανίχνευση της. Τα χαρακτηριστικά που εμφανίζει ένα περιστατικό χρησι-

[11] Το συγκεκριμένο πρωτόκολλο ανταλλάσσει πληροφορίες δρομολόγησης μεταξύ αυτονόμων διαχειριστικών περιοχών (Autonomous Systems) μέσα από συνδέσεις TCP.

μοποιούνται για να κατανοηθεί το είδος της επίθεσης, να εντοπιστούν και να παρεμποδιστούν οι ροές κίνησης που ανήκουν σε αυτή, να προσδιοριστεί αν εμφανίσεις της ίδιας ροής σε διαφορετικές χρονικές στιγμές αφορούν το ίδιο γεγονός, και αν διαφορετικοί υπολογιστές αποτελούν στόχους της ίδιας επίθεσης. Εις βάθος ανάλυση της επίθεσης μπορεί επίσης να υποδείξει τα εργαλεία και τη μέθοδο που χρησιμοποιήθηκαν. Τα κύρια χαρακτηριστικά των επιθέσεων DDoS είναι:

- *Το πρωτόκολλο που χρησιμοποιείται* (TCP, UDP ICMP κ.λπ.). Υπάρχουν όμως και επιθέσεις που χρησιμοποιούν ταυτόχρονα πολλά διαφορετικά πρωτόκολλα και θύρες (ports). Οι τελευταίες είναι συνήθως επιθέσεις κατανάλωσης δικτυακού εύρους.

- *Η θύρα (ή θύρες) επικοινωνίας που θα χρησιμοποιηθεί.*

- *Τα είδη των πακέτων ενός πρωτοκόλλου που χρησιμοποιούνται* (π.χ. ICMP-echo-reply, TCP-SYN κ.λπ.).

- *Το εύρος των διευθύνσεων IP που αποτελούν το στόχο.* Επιθέσεις εξάντλησης υπολογιστικών πόρων ενός εξυπηρετητή κατευθύνονται μόνον σε αυτόν. Στην περίπτωση που ο σκοπός είναι οι δικτυακοί πόρων οι υπολογιστές — προορισμός της επίθεσης μπορεί να περιλαμβάνουν ακόμα και όλες τις διευθύνσεις IP που έχουν αποδοθεί στο δίκτυο του θύματος. Μπορούμε έτσι να θεωρήσουμε ότι ανήκουν στην ίδια επίθεση ροές κίνησης οι οποίες κατευθύνονται σε διαφορετικούς υπολογιστές εφόσον (α) εμφανίζουν ίδια τα υπόλοιπα χαρακτηριστικά[12] και (β) οι υπολογι-

[12] Π.χ. συγκεκριμένα πρωτόκολλα και θύρες.

στές στόχοι ανήκουν στο ίδιο υποδίκτυο ή γενικότερα στον ίδιο χώρο διευθύνσεων IP (address space).

- *Το χρονικό διάστημα που θα μεσολαβήσει ανάμεσα σε δύο αποστολές επιθετικής κίνησης.* Ανάλογα με τις επιλογές πολιτικής ενός δικτύου για το χρονικό αυτό διάστημα (που υλοποιούνται στη διαμόρφωση των συστημάτων IDS) δύο διαφορετικές εμφανίσεις της ίδιας επίθεσης μπορεί να θεωρηθούν ως ένα ή ξεχωριστά περιστατικά. Στη δεύτερη περίπτωση η επίθεση θα πρέπει να ανιχνευτεί και να αντιμετωπιστεί εξ αρχής.

Η θεωρητική κατηγοριοποίηση του επιθέσεων DDoS είναι γενικότερη και δε γίνεται μόνον με βάση τα χαρακτηριστικά που παρατηρούνται στη διαδρομή και τον τελικό αποδέκτη αλλά και με βάση τις τεχνικές και τις μεθοδολογίες που χρησιμοποιήθηκαν.

Στο [Mirk04] γίνεται μια συστηματική ταξινόμηση με βάση όλα τα διαφορετικά χαρακτηριστικά που μπορεί να έχει μια τέτοια επίθεση σε διάφορα στάδια της εξέλιξης της:

- Βαθμό αυτοματισμού
- Μεθόδους εξάπλωσης και οργάνωσης της υποδομής επίθεσης
- Μεθόδους ελέγχου της
- Είδος διευθύνσεων πηγής στα πακέτα που αποστέλλονται
- Συμπεριφορά και δυνατότητα χαρακτηρισμού της επιθετικής κίνησης
- Είδος στόχου και επίδραση σε αυτόν.

Η ταξινόμηση αυτή προβλέπει θεωρητικά και επιθέσεις DoS που είναι μεν δυνατές αλλά δεν έχουν ακόμα παρατηρηθεί.

Μια παρόμοια ταξινόμηση των επιθέσεων DoS και DDoS γίνεται και στο [Doul04], όπου οι παράμετροι που χρησιμοποιούνται είναι:

- Ο βαθμός αυτοματοποίησης.
- Η τεχνική επίθεσης («πλημμύρα» πακέτων, επιθέσεις με συντελεστή ενίσχυσης, εκμετάλλευση αδυναμιών πρωτοκόλλων, χρήση «κακώς σχηματισμένων»—malformed—πακέτων).
- Η δυναμική της εξέλιξης της επίθεσης.
- Τα αποτελέσματα της επίθεσης στο στόχο.

Στο [Huss03] ακολουθείται μια ελαφρά διαφορετική προσέγγιση για να κατηγοριοποιηθούν αποκλειστικά επιθέσεις DDoS κατάληψης δικτυακού εύρους με βάση στοιχεία που συλλέγονται κατά τη διάρκεια τους. Χρησιμοποιείται η ανάλυση των επικεφαλίδων (headers) των πακέτων και η ύπαρξη ή όχι απότομης κλιμάκωσης στην επιθετική κίνηση. Επίσης προτείνεται η «φασματική» ανάλυση της κίνησης. Σε αυτή εξετάζονται οι συχνότητες πακέτων διαφορετικών ειδών. Με βάση αυτά τα χαρακτηριστικά συνάγεται το πλήθος των πηγών κίνησης (μία ή περισσότερες) και αν πρόκειται για απ' ευθείας προσβολή ή επίθεση «ανάκλασης».

Τέλος στο [Stan02] οι Staniford και συνεργάτες αναλύουν τις μεθοδολογίες και παρουσιάζουν τα θεωρητικά όρια για την ταχύτητα και το εύρος εξάπλωσης των αυτόματα διαδιδόμενων ιών (worms). Οι ιοί αυτοί παίζουν ιδιαίτερα ση-

μαντικό ρόλο στην αυτοματοποιημένη απόκτηση ελέγχου υπολογιστών για τη δημιουργία μιας υποδομής επίθεσης DDoS.

2.2.3 IPv6 και Επιθέσεις DDoS

Η νέα έκδοση του πρωτοκόλλου IP, το IPv6, πρόκειται να δημιουργήσει ένα νέο περιβάλλον ασφαλείας στο οποίο οι επιθέσεις DDoS έχουν το δυναμικό να αποτελέσουν σημαντική απειλή. Στο IPv6 ισχύουν οι ίδιες τεχνικές διενέργειας επιθέσεων άρνησης υπηρεσίας αλλά προστίθενται και νέες δυνατότητες απόκρυψης της κίνησης ή της πηγής της. Ήδη υπάρχουν εργαλεία διενέργειας τέτοιων επιθέσεων που λειτουργούν σε περιβάλλον IPv6, όπως το 6to4DDos [Warf03]. Υπάρχουν επίσης επιθετικά προγράμματα που ενσωματώνουν τμήματα κώδικα που επιτρέπει τη λειτουργία τους (εκτός του IPv4) και στο IPv6, όπως ένας αυτόματα διαδιδόμενος ιός (worm) που ανιχνεύτηκε και αναλύθηκε στα πλαίσια του προγράμματος Honeynet [Srem02]. Στο περιβάλλον IPv6 η επίδραση των επιθέσεων DDoS εξειδικεύεται στις κατωτέρω κατηγορίες:

Παραποίηση Διευθύνσεων

Σε ένα αποκλειστικό περιβάλλον IPv6 παραμένει το πρόβλημα παραποίησης διευθύνσεων πηγής πακέτων για απόκρυψη του πραγματικού αποστολέα. Προσφέρεται όμως ένα νέο χαρακτηριστικό που διευκολύνει τον έλεγχο στους παρόχους (όπως ορίζει το RFC 2827 [Ferg00]) για πακέτα με διευθύνσεις αποστολέα που δεν αντιστοιχούν στο χώρο διευθύνσεων του δικτύου προέλευσης τους.

Στο IPv6, για να διευκολυνθεί η δρομολόγηση, οι διευθύνσεις αποδίδονται με τρόπο που να μπορούν να ομαδοποιηθούν ανά περιοχή προέλευσης (από πιο

γενικευμένη σε πιο συγκεκριμένη). Κάθε διεύθυνση IPv6 (Aggregatable Global Unicast Address) χρησιμοποιεί τα πρώτα 64 bit της (από τα 128 συνολικά) για συλλογική (aggregated) πληροφορία προέλευσης που χωρίζεται σε τμήματα υψηλού επιπέδου, επόμενου επιπέδου και επιπέδου οργανισμού. Είναι έτσι δυνατόν σε διαφορετικά επίπεδα της δρομολόγησης να οριστούν φίλτρα ελέγχου της ορθής προέλευσης των πακέτων [Hind98].

Όπως και στο IPv4, όμως, το φιλτράρισμα αυτού του είδους (κατά το RFC 2827) είναι προαιρετικό για τους παρόχους. Επιπλέον το πλήθος των διευθύνσεων IPv6 σε ένα υποδίκτυο είναι τέτοιο που ακόμα και με φιλτράρισμα σε ισχύ κάποιος επιτιθέμενος μπορεί να χρησιμοποιήσει παραποιημένες αλλά νόμιμης προέλευσης διευθύνσεις [Conv04].

Επιθέσεις με Παράγοντα Ενίσχυσης

Στο IPv6 έχει αφαιρεθεί η έννοια της διεύθυνσης γενικής εκπομπής (broadcast address). Έτσι αποκλείονται επιθέσεις με την αποστολή πακέτων ICMP σε αυτή (τύπου "Smurf"), που παρουσιάζουν Συντελεστή Ενίσχυσης (Amplification Factor).

Έχουν όμως δημιουργηθεί γενικευμένες (global) διευθύνσεις multicast για ειδικές, κλιμακούμενες ομαδοποιήσεις κόμβων, π.χ. διευθύνσεις για όλους τους κόμβους στο ίδιο δικτυακό μέσο (link-local σύμφωνα με την ορολογία του IPv6), όλους τους κόμβους στο ίδιο υποδίκτυο (site-local στην ορολογία του IPv6), όλους τους δρομολογητές site-local, όλους τους εξυπηρετητές NTP του Διαδικτύου, κ.λπ.

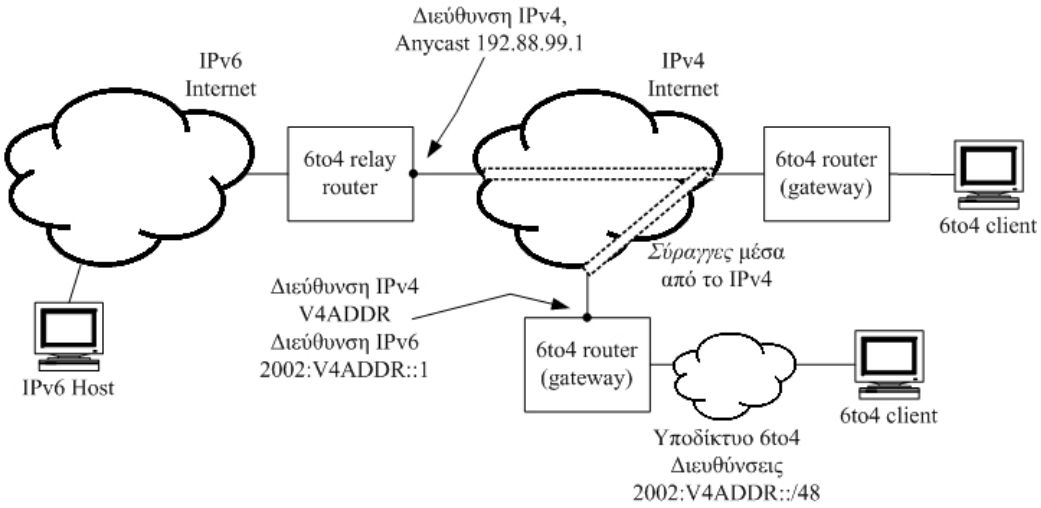
Για να αποτραπούν επιθέσεις Ενίσχυσης, οι προδιαγραφές του IPv6 απαγορεύουν την παραγωγή μηνυμάτων ICMPv6 σε απάντηση πακέτων στις γενικευ-

μένες διευθύνσεις multicast. Αν αυτό τηρηθεί και στις υλοποιήσεις του IPv6 τότε αποτρέπεται ο κίνδυνος επιθέσεων αυτού του τύπου στο νέο πρωτόκολλο. Στο [Conv04], οι Convery και συνεργάτες αναφέρουν ότι έχουν γίνει πειράματα που δείχνουν ότι πολλά δημοφιλή λειτουργικά συστήματα ακολουθούν το πρότυπο και πράγματι δεν απαντούν σε πακέτα προς τις γενικευμένες διευθύνσεις multicast τα οποία έχουν παραποιημένες διευθύνσεις πηγής. Εντούτοις, στην ίδια εργασία αναφέρεται ότι δεν είναι ακόμα εξακριβωμένο (λόγο ασάφειας στο σχετικό πρότυπο) τι κίνδυνος επιθέσεων Ενίσχυσης υπάρχει από πακέτα ICMP που στέλνονται με μια από τις γενικευμένες διευθύνσεις multicast ως (κατασκευασμένη) διεύθυνση πηγής.

Μικτά περιβάλλοντα v4–v6

Προβλήματα ασφαλείας δημιουργούν και οι (προσωρινοί) μεταβατικοί μηχανισμοί που χρησιμοποιούνται για τη συνύπαρξη των δύο εκδόσεων του πρωτοκόλλου IP στη διάρκεια της μετάβαση στο νέο πρωτόκολλο. Σήραγγες (tunnels) χρησιμοποιούνται εκτεταμένα για συνδέσεις διαμέσου δικτύων τα οποία δεν υποστηρίζουν την επιθυμητή έκδοση πρωτοκόλλου. Η κίνηση που περνά από τις σήραγγες, σε πολλές περιπτώσεις δεν έχει προβλεφτεί από τις πολιτικές ασφαλείας. Μπορεί έτσι να διαπεράσει συστήματα δικτυακής ασφαλείας (firewalls) και τους ελέγχους που αυτά θέτουν, επειδή δεν έχουν τη δυνατότητα να διερευνήσουν ταυτόχρονα και τα δύο πρωτόκολλα. Το πρόβλημα επιτείνεται από την ύπαρξη δυναμικών και αυτόματων μηχανισμών δημιουργίας σηράγγων.

Ο κύριος μηχανισμός για την επικοινωνία υπολογιστών ή δικτύων IPv6 πάνω από δίκτυα IPv4 είναι το 6to4 που περιγράφεται στο RFC 3056 [Carp01]. Προφέρει αυτόματη και δυναμική συνδεσιμότητα ανάμεσα σε συστήματα που



Σχήμα 2.3: Ενδεικτικές συνδεσμολογίες ανάμεσα σε δίκτυα IPv4 και IPv6 με τη χρήση του μηχανισμού του RFC 3056 (6to4)

ζητούν να χρησιμοποιήσουν IPv6 μέσα σε δίκτυα IPv4 (6to4 hosts) και περιοχές αποκλειστικά IPv6. Ένα παράδειγμα τέτοιας συνδεσιμότητας, τροποποιημένο από το [Savo04] φαίνεται στο σχήμα 2.3.

Όπως φαίνεται στο σχήμα 2.3 οι πύλες (gateways) 6to4 παίρνουν μια διεύθυνση IPv6 με πρόθεμα 2002: που βασίζεται στη διεύθυνση IPv4 που ήδη διαθέτουν. Είναι δυνατόν μέσα από ένα δίκτυο IPv6 να αποσταλεί κίνηση επίθεσης προς ένα σύστημα IPv4 κατασκευάζοντας κατάλληλα μια διεύθυνση προορισμού IPv6/6to4 [Warf03]. Αυτό συμβαίνει επειδή οι σήραγγες υλοποιούνται δυναμικά ανά περίπτωση. Το ίδιο μπορεί να γίνει και από ένα σύστημα IPv4[13] με ταυτόχρονη απόκρυψη της προέλευσης.

Κατά τον ίδιο τρόπο μπορούν να γίνουν επιθέσεις Ανάκλασης (Reflection attacks) στέλνοντας στο δρομολογητή 6to4 κατασκευασμένα πακέτα με τελικό

[13]Με τη διαδρομή: σύστημα IPv4 – 6to4 router και αφαίρεση της προέλευσης IPv4 – σύστημα στόχος IPv4 του οποίου η διεύθυνση έχει περιγραφεί στο IPv6/6to4

προορισμό συστήματα IPv6 και αποστολέα (αντικανονικά) κάποιο άλλο σύστημα IPv6.

Στις επικοινωνίες ανάμεσα σε ένα δικτυακό χώρο IPv6 και συστήματα 6to4 είναι δυνατόν να χρησιμοποιηθούν διαφορετικοί κόμβοι 6to4 ανά κατεύθυνση. Το γεγονός αυτό επιβάλει οι κόμβοι 6to4 να αποδέχονται όλες τις συνδέσεις προς αυτούς [Savo04]. Είναι έτσι δυνατόν να κατευθυνθεί μέσω αυτών κίνηση με προορισμό ένα σύστημα IPv6 η οποία θα έχει εν-θυλακωθεί σε πακέτα IPv4. Οι κόμβοι 6to4 θα αφαιρέσουν τη διεύθυνση προέλευσης IPv4 και θα προωθήσουν τα πακέτα IPv6 προσφέροντας έτσι απόκρυψη του αποστολέα. Ακόμα και διευθύνσεις που θα φιλτράρονταν λόγο μη νόμιμων διευθύνσεων από το δίκτυο πηγής μπορούν έτσι να γίνουν δεκτές. Το καθ' αυτό πρόβλημα επίθεσης DoS όμως σε αυτή την περίπτωση δεν είναι τόσο σοβαρό επειδή οι κόμβοι 6to4 δημιουργούν οι ίδιοι «στενωπό» (bottleneck) στη διάβαση της κακόβουλης κίνησης, τόσο από πλευράς υπολογιστικής ισχύος όσο και από πλευράς διαθέσιμου εύρους ζώνης [Savo04] [Stra04].

Ένας «αναμεταδότης» 6to4 (6to4 relay) μπορεί επίσης να χρησιμοποιηθεί και για τοπικές επιθέσεις (στο υποδίκτυο IPv4 στο οποίο συνδέεται) με αποστολές πακέτων στη διεύθυνση γενικής εκπομπής (broadcast). Αν ανήκει σε υποδίκτυο v4 της μορφής `A.B.C.0/24` ο επιτιθέμενος (από το IPv6) μπορεί να στείλει πακέτα με διεύθυνση 6to4 που μεταφράζεται `A.B.C.255`. Αν δε, δεν έχει ληφθεί πρόνοια για φιλτράρισμα τέτοιου είδους πακέτων αυτά μπορεί να αποσταλούν ακόμα και σε απομακρυσμένες διευθύνσεις προκαλώντας επιθέσεις Ενίσχυσης. Το πρόβλημα διορθώνεται εύκολα με την επιλογή φίλτρων που απαγορεύουν διευθύνσεις 6to4 αυτού του είδους [Stra04].

Υπάρχει επίσης ένας αριθμός από επιπλέον μεταβατικούς μηχανισμούς, όπως

το Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) [Temp04], οι διαφόρων ειδών σήραγγες (με ή χωρίς «ενδιάμεσους»—tunnel brokers) και ο μηχανισμός Dual-stack Transition Mechanism (DSTM) [Boun02] (για συστήματα με διπλές δικτυακές ρυθμίσεις–IPv4/IPv6). Αυτοί είτε χρησιμοποιούν το μηχανισμό 6to4 για διασυνδέσεις πέρα από το υποδίκτυο που χρησιμοποιεί ISATAP, είτε υπόκεινται σε τυπικά ζητήματα ασφαλείας ρύθμισης και διαχείρισης σηράγγων, είτε δεν εμφανίζουν γνωστά προβλήματα με επιθέσεις DDoS (DSTM).

Σημειώνεται ότι ακόμα και αν οι απειλές για τα δίκτυα IPv6 δε χρησιμοποιηθούν άμεσα σε επιθέσεις DDoS, μπορούν να διευκολύνουν (ή να υποκρύψουν) τη διαδικασία παραβίασης υπολογιστών και εξάπλωσης των προγραμμάτων ελέγχου μιας υποδομής επίθεσης DDoS. Γενικότερα το IPv6 είναι ένα νέο περιβάλλον, με το οποίο οι διαχειριστές δεν είναι εξοικειωμένοι και αντίστοιχα πολλά θέματα ασφαλείας δεν είναι καλώς κατανοητά. Υπάρχει έτσι δυσκολία στην εκπόνηση πολιτικών ασφαλείας και την υιοθέτηση βέλτιστων πρακτικών.

2.2.4 Εξάπλωση των Επιθέσεων Άρνησης Υπηρεσίας στο Διαδίκτυο

Περιστατικά ασφαλείας που σχετίζονται με επιθέσεις DDoS εμφανίζονται συχνά στην επικαιρότητα, ειδικά αν έχουν στόχους μεγάλης σημασίας. Ένα από τα πρώτα περιστατικά, που πήραν αρκετά μεγάλες διαστάσεις ώστε να απασχολήσουν τα διεθνή μέσα ενημέρωσης, ήταν η επίθεση σε έναν αριθμό από σημαντικές εταιρείες του Διαδικτύου (Yahoo, eBay, Buy.com, Amazon.com και CNN.com) στο διάστημα 7-9 Ιανουαρίου 2000. Ο δικτυακός τόπος της

εταιρείας Yahoo παρέμεινε εκτός λειτουργίας για τρεις ώρες στις 7 Ιανουαρίου 2000 και ακολούθησαν νέες επιθέσεις, στη διάρκεια των οποίων η διαθεσιμότητα των δικτυακών τόπων–στόχων έπεσε στο 0% (από το σύνηθες 95% - 98%) [Comp00]. Οι επιθέσεις αυτές αφορούσαν κυρίως την εξάντληση του διαθέσιμου δικτυακού εύρους ζώνης των θυμάτων με τη χρήση, πιθανόν, εργαλείων όπως το "Trinoo" και το "Tribe Flood Network" (παρεμφερές εργαλείο, αλλά σε μεγαλύτερο βαθμό κατανεμημένης λειτουργίας) [Ditt99a] που εξαπολύουν ένα μεγάλο αριθμό από πακέτα διαφόρων ειδών.

Άλλα περιστατικά εξίσου μεγάλης σημασίας ήταν:

- Επιθέσεις που διήρκεσαν συνολικά επτά ημέρες και στόχευαν τους κύριους εξυπηρετητές (DNS, web, ηλεκτρονικό ταχυδρομείο) εξανάγκασαν το Βρετανικό πάροχο δικτυακών υπηρεσιών *Cloud Nine* σε ολική διακοπή εργασιών στις 22 Ιανουαρίου 2002 [Regi02].

- Στις 21 Οκτωβρίου 2002 υπήρξε μια ταυτόχρονη επίθεση DoS προς όλους τους Εξυπηρετητές Δικτυακής Ονοματολογίας Ρίζας (Root Name Servers). Μια επιτυχής επίθεση θα μπορούσε να έχει σαν αποτέλεσμα τη διακοπή παροχής υπηρεσίας DNS σε ολόκληρο το Διαδίκτυο. Σε διάστημα λίγο πάνω από μία ώρα εστάλησαν 50 έως 100 Mbps (που μεταφράζεται σε 100 έως 200 χιλιάδες πακέτα ανά δευτερ.) ανά εξυπηρετητή, δίνοντας συνολική κίνηση επίθεσης 900 Mbps (1,8 Mpkts/sec). Η κίνηση ήταν πακέτα διαφόρων ειδών (ICMP, TCP SYN[14], κατακερμάτισμένα πακέτα TCP και UDP). Αν και οι ίδιοι εξυπηρετητές δεν παρουσίασαν προβλήματα λόγω της υπερεπάρκειας (overprovisioning) πόρων, πολλές κλήσεις

[14]Τα συγκεκριμένα πακέτα εκτός από το εύρος δικτύου εξαντλούν και υπολογιστικούς πόρους του παραλήπτη.

πελατών σε αυτό το διάστημα δεν μπόρεσαν να τους φτάσουν [Vixi02].

Το Computer Security Institute στην ετήσια έρευνα για την ασφάλεια που εκπονεί σε συνεργασία με το FBI υπολογίζει τις οικονομικές απώλειες από επιθέσεις DoS και DDoS (στις Η.Π.Α) στα 65 εκατομμύρια δολάρια για το 2003 [Csi03] και στα 26 εκατομμύρια δολάρια για το 2004 [Csi04]

Στη διεθνή βιβλιογραφία μεγάλο μέρος της έρευνας αφιερώνεται σε μεθόδους ανακάλυψης των επιθέσεων, διακοπής ή ανάσχεσης τους και αντιμετώπισης των επιπτώσεων τους. Υπάρχουν επίσης εκτεταμένες αναλύσεις για τα σημαντικότερα εργαλεία λογισμικού που μπορεί να χρησιμοποιηθούν για την πραγματοποίηση αυτών των επιθέσεων, όπως η πολύ γνωστή λίστα του Dittrich στο [Ditt04]. Από τη λειτουργία αυτών των εργαλείων είναι δυνατόν να εξαχθούν συμπεράσματα για το είδος της κίνησης που προβλέπεται να παράγουν. Δεν υπάρχουν όμως πολλές μελέτες για το πόσο εκτεταμένες είναι εν τέλει οι επιθέσεις DDoS στο Διαδίκτυο και τι επίδραση έχουν στη λειτουργία του. Σε μεγάλο βαθμό αυτό εξαρτάται από το εύρος της εξάπλωσης των κακόβουλων προγραμμάτων σε συστήματα «ξενιστές» (hosting systems) και από το βαθμό ενεργοποίησης των υποδομών επίθεσης που περιγράφτηκαν προηγουμένως.

Μια ουσιαστική ανάλυση για το βαθμό εξάπλωσης των επιθέσεων DDoS στο Διαδίκτυο έχει γίνει στην κλασική εργασία του Moore στο [Moor01] και βασίζεται σε μια στατιστική ανάλυση πακέτων που καταλήγουν σε ένα δίκτυο Κλάσης Α (Class A) σαν αποτέλεσμα επίθεσης κάπου άλλου. Η λογική είναι ότι τα πακέτα κακόβουλης κίνησης έχουν παραποιημένες τις διευθύνσεις αποστολέα με τυχαίο τρόπο. Κατά συνέπεια τα πακέτα-απαντήσεις του θύματος σε αυτά μπορεί να καταλήξουν οπουδήποτε στο Διαδίκτυο και ένα δίκτυο Κλάσης

Α στατιστικά θα λάβει πολλά από αυτά τα πακέτα (θεωρητικά το 1/256 του συνόλου). Τα πακέτα αυτά ονομάζονται «σκεδασμένη κίνηση» ("backscatter"). Η μεθοδολογία αυτή, αν και συζητήσιμη για την ορθότητα της[15], χρησιμοποιήθηκε για να βγουν μια σειρά από συμπεράσματα που δίνουν μια εικόνα για τη εξάπλωση των επιθέσεων DDoS. Τα κυριότερα από αυτά είναι:

- Υπάρχει συνεχής και σταθερή εμφάνιση επιθέσεων DDoS στο Διαδίκτυο. Καταμετρήθηκαν περίπου 12.000 επιθέσεις σε διάστημα τριών εβδομάδων

- Ορισμένες επιθέσεις φτάνουν σε ρυθμούς αποστολής κακόβουλης κίνησης της τάξης των 500.000 πακέτων ανά δευτερόλεπτο, τη στιγμή που ακόμα και 500 πακέτα SYN ανά δευτερόλεπτο είναι δυνατόν να καταστήσουν ένα εξυπηρετητή μη διαθέσιμο σε μια επίθεση εξάντλησης πόρων (επίθεση SYN) [Darm00]. Το γενικό συμπέρασμα είναι ότι οι περισσότερες επιθέσεις DDoS μπορούν να επηρεάσουν ακόμα και θύματα με μεγάλο πλήθος δικτυακών πόρων πολύ δε περισσότερο τυπικά δίκτυα «φύλλα» (leaf networks) ενός ISP (π.χ. με γραμμή σύνδεσης 2Mbps)

- Το μεγαλύτερο ποσοστό (80%) των επιθέσεων διαρκεί μέχρι 30 λεπτά με τις περισσότερες από αυτές (50% του συνολικού αριθμού) να μην υπερβαίνουν τα 5 λεπτά. Εντούτοις υπάρχουν και περιπτώσεις επιθέσεων που συνεχίζονται για ημέρες.

- Υπάρχουν επιθέσεις που επαναλαμβάνονται προς το ίδιο θύμα μετά τη μεσολάβηση κάποιας διακοπής.

[15] Εξετάζει μόνον επιθέσεις που παραποιούν τις διευθύνσεις αποστολέα επιλέγοντας τυχαία μέσα από όλες τις διευθύνσεις του Internet με αποτέλεσμα να υποτιμά τον πραγματικό βαθμό εξάπλωσης των επιθέσεων DDoS (π.χ. επιθέσεις που επιλέγουν παραποιημένες διευθύνσεις από μικρό, εύρος, επιθέσεις «ανάκλασης» κ.λπ.).

Στο [Huss03] οι Hussain και συνεργάτες παρουσιάζουν τα αποτελέσματα από την παρακολούθηση και ανάλυση επιθέσεων DDoS εναντίον ενός δικτύου που περιλαμβάνει κατά προσέγγιση το 0,105% του αποδομένων διευθύνσεων IP. Σύμφωνα με τις παρατηρήσεις τους στο διάστημα από τον Ιούλιο έως το Νοέμβριο του 2002 και με προβολή σε όλο το πλήθος διευθύνσεων IP, πρέπει να συνέβαιναν τουλάχιστον 10.000 επιθέσεις DDoS ανά μήνα σε ολόκληρο το Διαδίκτυο.

Ορισμένες άλλες εργασίες παρουσιάζουν επίσης ενδιαφέροντα στοιχεία για την επίδραση αυτών των επιθέσεων. Στο [Lan03], οι Lan και συνεργάτες εξετάζουν την επίδραση επιθέσεων DDoS σε ένα δίκτυο με αρκετούς πόρους για να αντεπεξέλθει επιτυχώς. Αναφέρεται ότι ακόμα και στην περίπτωση που οι δικτυακές συνδέσεις παραμείνουν υπο-χρησιμοποιούμενες υπάρχει αύξηση της τάξης του 230% στην καθυστέρηση των ερωτήσεων DNS και αύξηση κατά 30% στην καθυστέρηση της κίνησης δικτυακού ιστού (web). Οι συγγραφείς υποστηρίζουν ότι αυτό οφείλεται στην επίδραση της επιπλέον κίνησης στους δρομολογητές και συγκεκριμένα τη μεγαλύτερη μέση κατάληψη της μνήμης (buffers) και τις αυξημένες ανάγκες επεξεργασίας.

Στο [Sung02] αναλύεται (με τη χρήση του εργαλείου Netflow) η κίνηση από μια επίθεση DDoS που πραγματοποιήθηκε το 2001 σε ένα δίκτυο του Πανεπιστημίου Georgia Tech με στόχο κάποιους εξυπηρετητές. Τα αποτελέσματα δείχνουν ότι:

- Η συνολική διάρκεια της επίθεσης ήταν περίπου 90 λεπτά και από τη στιγμή της έναρξης της παρουσίασε ιδιαίτερα απότομη αύξηση της κακόβουλης κίνησης.

- Οι διευθύνσεις που χρησιμοποιήθηκαν για την απόκρυψη του αποστολέα (address spoofing) επιλέγονται ομοιόμορφα από όλες τις θεωρητικά διαθέσιμες διευθύνσεις IP του Διαδικτύου. Αντίστοιχη ομοιομορφία παρατηρήθηκε στην επιλογή θυρών επικοινωνίας.

- Επηρεάστηκε ιδιαίτερα η δυνατότητα των υπολογιστών στόχων να πραγματοποιήσουν άλλες συνδέσεις, εξυπηρέτησης νόμιμων αιτήσεων.

Επίσης επιβεβαιώθηκαν κάποια φαινόμενα προβλεπτά από τη λειτουργία των πρωτοκόλλων TCP και ICMP:

- Η κίνηση που παρατηρήθηκε ανά κατεύθυνση παρουσίαζε αυξημένα εισερχόμενα πακέτα TCP SYN και αυξημένα εξερχόμενα πακέτα TCP SYN-ACK και TCP SYN-RST.

- Η κίνηση σηματοδοσίας του Διαδικτύου (ICMP) αυξήθηκε επίσης κατά τη διάρκεια της επίθεσης λόγο πολλών μη υπαρκτών διευθύνσεων IP.

Τέλος στο [Chan02] παρουσιάζονται κάποια πειραματικά αποτελέσματα για την ανθεκτικότητα δικτυακών εξυπηρετητών σε επιθέσεις εξάντλησης πόρων (επιθέσεις SYN) με βάση τους χρόνους που διατηρούν ανοικτή μια μη ολοκληρωμένη σύνδεση TCP. Για τις εκδόσεις λειτουργικών συστημάτων που ήταν τα πλέον σύγχρονα κατά την περίοδο της έρευνας (2002) ήταν αρκετός ένας αριθμός από συνδέσεις κατά το ήμισυ ανοικτές $N \leq 10.000$ για την πλήρη διακοπή χρήσιμης λειτουργίας τους. Ειδικότερα, στις περιπτώσεις των λειτουργικών Linux και BSD ήταν αρκετές $N \leq 6.000$ συνδέσεις που αντιστοιχούσαν στις δυνατότητες μιας απλής τηλεφωνικής σύνδεσης (dialup) χωρητικότητας 56Kbps. Ως προς τις επιθέσεις αποστολής μεγάλου όγκου κίνησης αρκεί η αποστολή πακέτων

ICMP με ρυθμό ενός ανά δευτερόλεπτο από 5.000 ελεγχόμενους υπολογιστές για να γεμίσει μια γραμμή T1, χωρητικότητας 1,544Mbps. Σε περίπτωση που τα πακέτα στέλνονται με υψηλότερους ρυθμούς απαιτούνται ακόμα λιγότεροι υπολογιστές. Το ίδιο αποτέλεσμα μπορεί να δημιουργηθεί με μια αντίστοιχη επίθεση ανάκλασης όπου 5.000 υπολογιστές (εξυπηρετητές) θα στείλουν απαντητικά πακέτα προς το θύμα. Το αποτέλεσμα αυτό όμως μπορεί να δημιουργηθεί από πολύ λιγότερα επιθετικά συστήματα αν κάθε ένα αναλάβει αποστείλει τα πακέτα δημιουργίας της κίνησης σε έναν αριθμό από εξυπηρετητές.

2.3 Αντιμετώπιση Επιθέσεων

2.3.1 Συστήματα Ανίχνευσης Επιθέσεων (IDS)

Όπως προκύπτει από μελέτες ταξινόμησης των προβλημάτων ασφαλείας, όπως αυτή στο [Land94] τα υπολογιστικά συστήματα, ασχέτως κατασκευαστή και λειτουργίας, είναι ευάλωτα σε πολλαπλές απειλές, η δε πλήρης εξασφάλιση τους είναι τόσο τεχνικά δύσκολη όσο και οικονομικά ασύμφορη. Παράλληλα, η ευρύτατη σύνδεση στο περιβάλλον του Διαδικτύου εκθέτει σε νέες απειλές και δημιουργεί την ανάγκη για μια αυτοματοποιημένη μέθοδο ανίχνευσης των περιστατικών ασφαλείας. Την ανάγκη αυτή επιχειρούν να καλύψουν τα Συστήματα Ανίχνευσης Επιθέσεων (Intrusion Detection Systems—IDS).

Ένα IDS παρακολουθεί το περιβάλλον στο οποίο είναι εγκατεστημένο (υπολογιστικό σύστημα ή δίκτυο) και επιχειρεί να ανιχνεύσει, βάση διαφόρων μεθόδων, το κατά πόσον υφίσταται κάποιο περιστατικό ασφαλείας. Η λειτουργία των IDS σε ένα δίκτυο γίνεται παράλληλα με τα συστήματα δικτυακής προστα-

σίας (firewalls) και στοχεύει στις απειλές που έχουν καταφέρει να περάσουν από αυτά ή έχουν εσωτερική προέλευση. Αντίθετα με τις εφαρμογές ανάλυσης διαμορφώσεων (configuration analysis), όπως τα ιστορικά Cops [Farm90] και Satan [Ceri95], τα IDS παρέχουν σε κάποιο βαθμό αυτοματοποίηση και σε ορισμένες περιπτώσεις τη δυνατότητα ενεργής αντίδρασης.

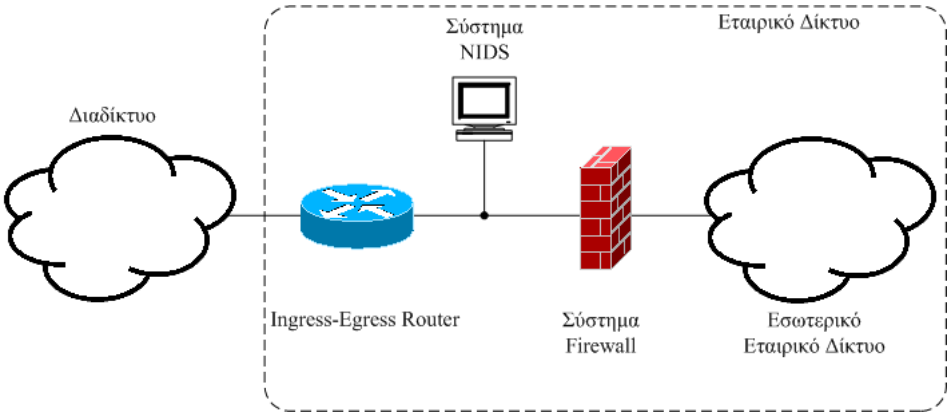
Η αρχιτεκτονική ενός τυπικού συστήματος IDS αποτελείται από τα βασικά τμήματα:

Α. Το τμήμα συλλογής πληροφοριών («αισθητήρες»–sensors)

Το τμήμα αυτό μπορεί να παρακολουθεί τις παραμέτρους λειτουργίας ενός συγκεκριμένου υπολογιστικού συστήματος, οπότε πρόκειται για IDS ελέγχου υπολογιστή (Host Based IDS), ή να καταγράφει κίνηση από το δίκτυο (ιδανικά κάθε πακέτο που περνάει από το δικτυακό μέσο όπου είναι εγκατεστημένο), οπότε μιλάμε για δικτυακό IDS (Network Based IDS—NIDS). Το σχήμα 2.4 δίνει μια εδεικτική τοπολογία για την τοποθέτηση ενός NIDS στο σημείο διασύνδεσης ενός δικτύου.

Ανάλογα με το αν χρησιμοποιούνται ένα ή περισσότερα σημεία συλλογής πληροφοριών έχουμε τα κεντρικά (centralized) ή τα κατανεμημένα (distributed) συστήματα IDS. Τα τελευταία παρέχουν μεν τη δυνατότητα απόκτησης περισσότερης πληροφορίας αλλά θέτουν μια σειρά από νέα προβλήματα: τον έλεγχο των επιμέρους τμημάτων, τη δυνατότητα κλιμάκωσης της λειτουργίας, την αποφυγή δημιουργίας μεγάλου όγκου κίνησης από τις αναφορές, την ανάλυση της πληροφορίας, την ασφάλεια των ανταλλαγών.

Μια αρκετά διαδεδομένη προσέγγιση στα κατανεμημένα συστήματα IDS



Σχήμα 2.4: Ενδεικτική εγκατάσταση Network Intrusion Detection System (NIDS). Η τοποθέτηση του πριν από το Σύστημα Δικτυακής Προστασίας (Firewall) εξασφαλίζει τη δυνατότητα παρακολούθησης όλης της κίνησης προς το εταιρικό δίκτυο, πριν αυτή υποστεί οποιασδήποτε μορφής φιλτράρισμα.

υλοποιείται με τη χρήση αυτόνομων προγραμματιστικών διεργασιών (autonomous agents) [Spaf00]. Πρόκειται για εφαρμογές που εγκαθίστανται σε διάφορα σημεία ενός δικτύου, όπου ζητείται, λειτουργούν αυτόνομα με αποτέλεσμα να έχουν αρκετά μεγάλη ευελιξία: πολλές μπορούν ταυτόχρονα να λειτουργούν επιτελώντας διαφορετικές λειτουργίες συλλογής στοιχείων, δεν επηρεάζουν το σύνολο σε περίπτωση προβλημάτων, επιμέρους τμήματα μπορούν εύκολα να ρυθμιστούν ή να αντικατασταθούν.

Β. Το τμήμα ανάλυσης της πληροφορίας ενός συστήματος IDS

Το τμήμα αυτό διαπιστώνει την ύπαρξη ενός περιστατικού. Η ανάλυση γίνεται με δύο βασικές μεθοδολογίες:

1. Τη σύγκριση των στοιχείων που συλλέγονται με συγκεκριμένες «υπογραφές» ("signatures"), ήδη γνωστών επιθέσεων που το IDS έχει αποθηκευ-

μένες από πριν. Η μέθοδος αυτή αποκαλείται ανίχνευση της κακής χρήσης (misuse detection). Έχει το πλεονέκτημα της μεγάλης ακρίβειας στην ανακάλυψη γνωστών επιθέσεων αλλά αδυνατεί να ανιχνεύσει νέες επιθετικές μεθόδους. Οι «υπογραφές» περιλαμβάνουν γνωστά χαρακτηριστικά των επιθέσεων, όπως:

- Είδος πακέτου
- Μέγεθος πακέτων
- Περιεχόμενα σύμβολα κ.λπ. (packet payload) σε συγκεκριμένους συνδυασμούς (patterns)

  – Παραδείγματα τέτοιας ανάλυσης είναι η εφαρμογή snort [Casw03] και το σύστημα Network Flight Recorder (NFR) [Nfr04], Δικτυακά IDS, τα οποία συλλέγουν και εξετάζουν μεμονωμένα πακέτα για το κατά πόσον ταιριάζουν με τις υπογραφές γνωστών περιστατικών.

Η τεχνική μπορεί να συμπληρωθεί με επιπλέον αλγορίθμους που αναλύουν πολλαπλά πακέτα και συνδυασμούς τους. Το σύστημα NIDS αναλαμβάνει την ανασύνθεση της κίνησης όπως αυτή θα καταλήξει τελικά στους υπολογιστές παραλήπτες. Σκοπός είναι η αντιμετώπιση επιθέσεων όπου η κακόβουλη κίνηση αποκρύβεται με κατακερματισμένα ή επαναλαμβανόμενα πακέτα καθώς και πακέτα με αλλαγμένη τη σειρά αποστολής. Μια επιπλέον τεχνική επίθεσης που χρησιμοποιείται είναι η αποστολή ενός πακέτου επίθεσης με παράμετρο TTL τέτοια που να εξασφαλίζει πως θα φτάσει στο σύστημα στόχο μαζί με πολλά άλλα, που αποκρύπτουν το

σκοπό του, τα οποία όμως έχουν μικρότερη τιμή στην παράμετρο Time to Live (TTL)[16].

2. Τη στατιστική ανάλυση κάποιων παραμέτρων ώστε να αναγνωριστεί η απόκλιση από τις συνηθισμένες τιμές τους. Αν αυτή η απόκλιση ξεπεράσει κάποια όρια που έχουν τεθεί το σύστημα την ανιχνεύει ως επίθεση. Η μέθοδος αυτή βασίζεται στην ανίχνευση στατιστικών ανωμαλιών, γι' αυτό ονομάζεται ανίχνευση ανωμαλιών (anomaly detection). Αν και μπορεί να ανιχνεύσει πιθανά νέα ήδη επιθέσεων η μέθοδος αυτή παρουσιάζει το πρόβλημα των εσφαλμένων θετικών ανιχνεύσεων (false positives) μια και σε πολλές περιπτώσει μια μη αναμενόμενη αλλαγή στη συμπεριφορά ων χρηστών ή τη χρήση των συστημάτων μπορεί να εκληφθεί ως επίθεση. Λύση σε αυτό το πρόβλημα προσφέρει η συνδυασμένη ανάλυση πληροφορίας από πολλές πηγές (data fusion) [Siat04] ώστε η τελική απόφαση να μη βασιστεί σε ένα μόνον στοιχείο. Οι επιθέσεις DDoS αποτελούν χαρακτηριστικό παράδειγμα ανίχνευσης με βάση την απόκλιση του όγκου της κίνησης (ή κάποιων συγκεκριμένων μόνον χαρακτηριστικών της[17]) από τα συνηθισμένα επίπεδα. Οι παράμετροι που παρακολουθούνται μπορούν να είναι και περισσότερο σύνθετες, όπως για παράδειγμα, σε ένα IDS ελέγχου υπολογιστή, οι ακολουθίες των κλήσεων προς το λειτουργικό σύστημα (system calls) [Asti01b].

Γ. Πιθανά επιπλέον τμήματα ενός συστήματος IDS

- Μια βάση για την αποθήκευση των περιστατικών.

[16] Οι τεχνικές αυτές ("evasion techniques") επιδιώκουν να «παραπλανήσουν» τα συστήματα NIDS.

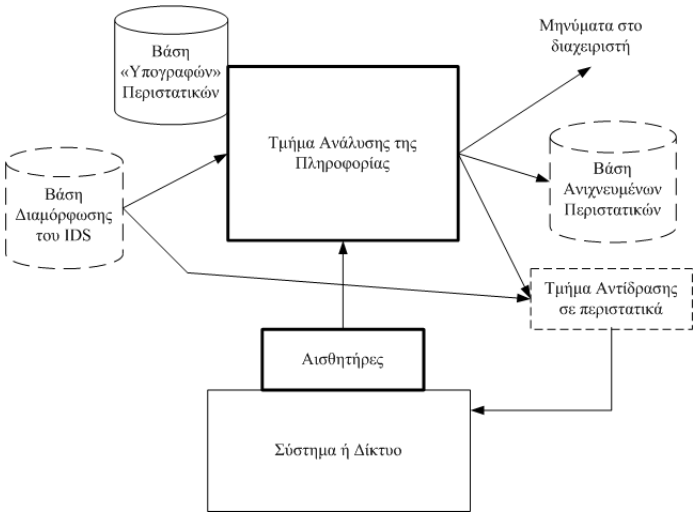
[17] Π.χ. Στις επιθέσεις SYN αυξάνεται υπέρογκα το πλήθος των συγκεκριμένων πακέτων.

- Μηχανισμοί επικοινωνίας για την αποστολή αναφορών και τον απομακρυσμένο έλεγχο.

- Ένα τμήμα διαμόρφωσης (configuration) για την προσαρμογή της λειτουργίας σε νέες απαιτήσεις και πολιτικές και την ανανέωση των υπογραφών επιθέσεων (σε συστήματα ανάλυσης κακής χρήσης).

- Ένα τμήμα αντίδρασης στην επίθεση. Το συγκεκριμένο δεν είναι ιδιαίτερα σύνηθες λόγο του κινδύνου λήψης μέτρων ως αντίδραση σε κάποια εσφαλμένα θετική ανίχνευση.

Το σχήμα 2.5 δίνει το απλοποιημένο διάγραμμα ενός συστήματος IDS (παρόμοιο με αυτό που παρουσιάζεται στο [Deba99]), που περιλαμβάνει τα κύρια τμήματα που περιγράφηκαν.



Σχήμα 2.5: Βασική αρχιτεκτονική ενός συστήματος IDS

Η ικανότητα ενός συστήματος IDS αποτιμάται με μια σειρά παραμέτρους:

- *Την ακρίβεια του* (Accuracy). Τί συχνότητα εμφάνισης έχουν οι εσφαλμένα θετικές ανιχνεύσεις (false positives) δηλαδή η θεώρηση νόμιμων λειτουργιών ως επιθέσεις

- *Την απόδοση του* (Performance). Πόσο γρήγορα μπορεί να συλλέξει στοιχεία και να επεξεργαστεί αναφορές. Ειδικά σε περιπτώσεις όπου υπάρχει μεγάλη ροή πληροφορίας (π.χ. τα συστήματα NIDS που παρακολουθούν δικτυακές συνδέσεις υψηλής ταχύτητας ή το σημείο συγκέντρωσης των αναφορών ενός κατανεμημένου IDS), η απόδοση θα κρίνει κατά πόσον μπορεί να υπάρξει ανίχνευση περιστατικών σε πραγματικό χρόνο.

- *Την πληρότητα ανίχνευσης* (Completeness). Το χαρακτηριστικό αυτό αφορά στο ποσοστό επιθέσεων που το σύστημα IDS θα καταφέρει να ανιχνεύσει και είναι ιδιαίτερα δύσκολο να αξιολογηθεί επειδή είναι αδύνατον να είναι γνωστά εκ των προτέρων όλα τα είδη προβλημάτων ασφάλειας[18].

Επιπλέον στο [Deba99] προτείνονται δύο ακόμα παράμετροι αποτίμησης:

- *Η αντοχή σε επιθέσεις προς το ίδιο το σύστημα IDS* (Fault Tolerance). Το χαρακτηριστικό αυτό έχει ιδιαίτερη σημασία για τη συνέχιση της λειτουργίας και την παροχή χρήσιμων υπηρεσιών από το IDS, ειδικά στη διάρκεια ειδικών καταστάσεων.

- *Η ταχύτητα κατάληξης σε συμπεράσματα* (Timeliness). Η παράμετρος αυτή αφορά στη δυνατότητα άμεσης ενημέρωσης των διαχειριστών και

[18] Ακόμα και τα IDS ανακάλυψης ανωμαλιών είναι προσαρμοσμένα, κατά περίπτωση, σε συγκεκριμένα χαρακτηριστικά συστημάτων ή δικτύων που παρακολουθούν και δεν εγγυώνται μια «ολιστική» θεώρηση της ασφάλειας.

κατ' επέκταση μειώνει το χρόνο αντίδρασης. Ο χρόνος που θα μεσολαβήσει από τη στιγμή της εκδήλωσης μιας επίθεσης μέχρι τη θετική ανακάλυψη του περιστατικού αναφέρεται ως το «πρόβλημα ταχύτερης ανίχνευσης» (Quickest Attack Detection Problem) [Chan02]. Είναι έτσι δυνατόν, σε περίπτωση πολύ μεγάλου χρόνου ανίχνευσης (με σκοπό να περιοριστούν οι εσφαλμένα θετικές ανιχνεύσεις —false positives) αυτή τελικά να περάσει απαρατήρητη.

Για τις επιθέσεις DDoS όπου έχουμε αποστολή ροών δεδομένων παρουσιάζεται και ένα ακόμα ζήτημα ως προς τον χρονικό προσδιορισμό των επιθέσεων· η διάρκεια διατήρησης της «ενεργοποιημένης» κατάστασης του συστήματος IDS, δηλαδή το διάστημα μετά την παρέλευση του οποίου η νέα εμφάνιση μιας επίθεσης DDoS καταχωρείται ως διαφορετικό περιστατικό.

Η προδιαγραφή IDMEF

Η ύπαρξη πολλών διαφορετικών αναγκών ασφάλειας αλλά και ο εμπορικός ανταγωνισμός έχει οδηγήσει στη δημιουργία ενός μεγάλου πλήθους διαφόρων συστημάτων IDS· ειδικό λογισμικό που λειτουργεί σε κοινούς υπολογιστές, ή εξειδικευμένα υπολογιστικά συστήματα, εμπορικές λύσεις ή εφαρμογές ανοικτού λογισμικού (open software). Η προδιαγραφή Intrusion Detection Message Exchange Format (IDMEF) [Deba04], εργασία σε εξέλιξη (Work in Progress) από την ομάδα εργασίας Intrusion Detection Working Group του IETF ορίζει τρόπους περιγραφής πληροφορίας και διαδικασίες ανταλλαγής για το μοίρασμα δεδομένων ανάμεσα σε συστήματα IDS, συστήματα αντίδρασης σε περιστατικά και εφαρμογές διαχείρισης που χρειάζεται να συνεργαστούν. Οι χρήστες

προκειμένου να καταλήξουν σε ένα βέλτιστο περιβάλλον ασφαλείας μπορούν να επιλέξουν την εγκατάσταση πολλών διαφορετικών συστημάτων IDS, ανάλογα με τη λειτουργικότητα τους και τα ισχυρά και αδύναμα στοιχεία τους. Το πρότυπο εξασφαλίζει ότι αυτά θα παρέχουν τις αναφορές τους σε μια παρόμοια μορφή.

Το μοντέλο δεδομένων του IDMEF ορίζει μια αντικειμενοστραφή αναπαράσταση της πληροφορίας στα μηνύματα ανάμεσα στα συστήματα IDS και υλοποιείται στη γλώσσα XML (eXtended Markup Language).

Τα προφανή σημεία χρήσης του προτύπου IDMEF είναι (ανάλογα με την αρχιτεκτονική του κάθε IDS) η μεταφορά δεδομένων από συστήματα αισθητήρων σε οντότητες ανάλυσης της πληροφορίας και η μεταφορά μηνυμάτων προς το διαχειριστή και τις σχετικές εφαρμογές ασφάλειας. Επιπλέον το IDMEF μπορεί να φανεί χρήσιμο για τις εξής περιπτώσεις:

- Βάσεις δεδομένων που συγκεντρώνουν πληροφορίες για περιστατικά από διαφορετικά συστήματα IDS ώστε να είναι δυνατή η ανάλυση τους από κοινού.
- Συστήματα που εκτελούν συνδυασμό γεγονότων ασφαλείας
- Συστήματα διαχείρισης που μπορούν να παρουσιάσουν στην ίδια διαχειριστική εφαρμογή πληροφορίες από διαφορετικά συστήματα[19].
- Ανταλλαγή πληροφοριών ανάμεσα σε οργανισμούς και ομάδες (π.χ. ομάδες CERT ή διωκτικές αρχές) που διαχειρίζονται περιστατικά ασφαλείας.

[19]Κατά τον ίδιο τρόπο που σήμερα το κάνουν με τις πληροφορίες από MIB του SNMP.

Η ίδια ομάδα εργασίας του IETF έχει παρουσιάσει ως εργασία εν εξελίξει (Work in Progress) το πρωτόκολλο επιπέδου εφαρμογής Intrusion Detection Exchange Protocol (IDXP) [Fein02] για την ανταλλαγή μηνυμάτων IDMEF. Το IDXP βασίζεται (αποτελεί ένα «προφίλ λειτουργίας») στο γενικότερο μοντέλο Blocks Extensible Exchange Protocol (BEEP) [Rose01b]. Το τελευταίο προσφέρει μια υποδομή για ανταλλαγές στο επίπεδο εφαρμογής, με σύνδεση (connection-oriented) και ασύγχρονη μετάδοση πληροφορίας. Η επιβεβαίωση της ταυτότητας των επικοινωνούντων μερών, η ασφάλεια καθώς και άλλα χαρακτηριστικά της επικοινωνίας παρέχονται από την υποδομή του BEEP με τη χρήση «προφίλ λειτουργίας».

Το IDXP ορίζει πως θα επικοινωνήσουν δύο οποιεσδήποτε οντότητες IDS μεταξύ τους (IDXP peers), απευθείας ή και με σήραγγες επιπέδου εφαρμογής με τη χρήση αντιπροσώπων (proxies).

2.3.2 Τεχνικές Αντιμετώπισης Επιθέσεων DDoS

Ακολουθεί μια επισκόπηση τριών τομέων αντιμετώπισης που αφορούν στις τρεις πλευρές του προβλήματος: ανίχνευση (detection), παρακολούθηση - ανακάλυψη της διαδρομής (traceback) και αντίδραση (reaction) σε επιθέσεις DDoS. Η παρουσίαση δεν έχει σκοπό να είναι εξαντλητική αλλά να καταδείξει τις κυριότερες ερευνητικές κατευθύνσεις και να δημιουργήσει το πλαίσιο μέσα στο οποίο θα παρουσιαστεί η προτεινόμενη λύση.

Ανάλυση των διαφόρων μηχανισμών άμυνας ενάντια στις επιθέσεις DDoS υπάρχει επίσης στο [Chan02] όπου γίνεται μια συστηματοποιημένη παρουσίαση και αξιολόγηση τους. Στο [Mirk04] γίνεται από τους Mirkovic και συνεργάτες

μια μικρής κλίμακας ταξινόμηση των αμυντικών μέτρων σύμφωνα με τα χαρακτηριστικά:

- Τομέας εξασφάλισης: Σύστημα ή πρωτόκολλο
- Μέθοδος πρόληψης DoS: Παρακολούθηση πόρων, πολλαπλασιασμός πόρων
- Στρατηγική ανίχνευσης της επίθεσης: Ανίχνευση ανωμαλίας ή κακής χρήσης, μηνύματα τρίτων
- Στρατηγική αντίδρασης: Αναγνώριση κακόβουλων συστημάτων, έλεγχος του χρησιμοποιούμενου δικτυακού εύρους, φιλτράρισμα, αλλαγές στην τοπολογία
- Βαθμός συνεργασίας μεταξύ των συστημάτων αντιμετώπισης της επίθεσης
- Ο χώρος εγκατάστασης τους: Στο θύμα, στην πηγή, ενδιάμεσα

Ορισμένες μεθοδολογίες αντιμετώπισης μπορεί να υπάγονται σε πολλές κατηγορίες ταυτόχρονα. Μια ταξινόμηση επιθέσεων DDoS και μηχανισμών άμυνας γίνεται επίσης στο [Doul04] από τους Δουλιγέρη και συνεργάτες.

Ανίχνευση

Η ανίχνευση μιας εξελισσόμενης κατανεμημένης επίθεσης άρνησης υπηρεσίας βασίζεται σε τεχνικές διάγνωσης ανωμαλίας. Πέρα από την καθ' αυτή ανακάλυψη μιας επίθεση DDoS η πρόκληση για έναν διαχειριστή ή ένα αυτόματο σύστημα IDS είναι να καταφέρουν να διαχωρίσουν περιστατικά φυσιολογικής

αύξησης της κίνησης[20] από πραγματικές κακόβουλες επιθέσεις. Μέρος της διαδικασίας ανίχνευσης είναι και ο προσδιορισμός των χαρακτηριστικών της κίνησης επίθεσης. Τα χαρακτηριστικά αυτά θα επιτρέψουν να διαχωριστεί από νόμιμες επικοινωνίες ή άλλες (ταυτόχρονες) επιθέσεις, και θα προσδιορίσουν τυχόν μέτρα αντιμετώπισης της. Η δυσκολία που παρουσιάζει το πρόβλημα της ανίχνευσης έγκειται αφ' ενός στην εξασφάλιση της απαραίτητης υπολογιστικής ισχύος ώστε να γίνει με επαρκή ταχύτητα η ανάλυση στοιχείων (ειδικά από υψηλής ταχύτητας αισθητήρες), αφ' ετέρου στην εγκυρότητα και απόδοση των αλγορίθμων που θα χρησιμοποιηθούν για την ανάλυση.

Ο Πίνακας 2.1 παρουσιάζει τις κυριότερες μεθόδους ανίχνευσης επιθέσεων DDoS. Απ' ευθείας ανίχνευση γίνεται στο δίκτυο-θύμα με την παρατήρηση αυξημένης κίνησης (ή και συμφόρησης) στη γραμμή διασύνδεσης. Για την ανακάλυψη ανωμαλιών στην κίνηση αυτή πρέπει να καταγραφεί, κατά τον ίδιο τρόπο που αυτό γίνεται στα συστήματα Network IDS (NIDS), και στη συνέχεια να αναλυθούν διάφορα χαρακτηριστικά της. Η διαδικασία καταγραφής της κίνησης (traffic capture) σε δικτυακές συνδέσεις υπερυψηλής ταχύτητας (έως Gbps) δημιουργεί, λόγω όγκου μεγάλες απαιτήσεις απόδοσης.

– Κοινά συστήματα NIDS (όπως π.χ. το Snort) είναι προσανατολισμένα σε χρήση σε LANs ή μικρές εταιρικές συνδέσεις. Σε αυτά τα περιβάλλοντα μπορούν να υποστηρίξουν λειτουργικότητα εντοπισμού επιθέσεων DDoS (με προσθήκη λογισμικού διάγνωσης ανωμαλιών). Απαιτούν όμως δικτυακό υλικό (hardware) υψηλών επιδόσεων για να μπορέσουν να λειτουργήσουν σε γραμμές υψηλών ταχυτήτων. Σε διαφορετική περίπτωση

[20] Που οφείλεται π.χ. στη δημοσίευση ιστοσελίδων αυξημένου ενδιαφέροντος. Το φαινόμενο περιγράφεται με τον όρο «ξαφνικό πλήθος» ("flash crowd").

<table>
<tr><th colspan="3">Ανιχνευση Επιθεσεων DDoS</th></tr>
<tr><th>Στο Θυμα</th><th>Στο Μονοπατι της Επιθεσης</th><th>Στην Πηγη</th></tr>
<tr><td colspan="2">Κοινες Λυσεις</td><td>Καταγραφή & ανάλυση Εξερχόμενων Ροών (D-Ward)</td></tr>
<tr><td colspan="2">Μετρήσεις από Access Control Lists (ACLs)</td><td rowspan="11"></td></tr>
<tr><td colspan="2">Παρακολούθηση Επιβάρυνσης Δρομολογητών</td></tr>
<tr><td colspan="2">Δειγματοληψία Διερχόμενης Κίνησης</td></tr>
<tr><td colspan="2">Μέτρηση ροών (Netflow)</td></tr>
<tr><td colspan="2">Χρήση Network Processors</td></tr>
<tr><td colspan="2">Συνδυασμός μεθόδων (π.χ. με τις IPs)</td></tr>
<tr><td>Ανιχνευση στο Θυμα</td><td>Κατανεμημενη Ανιχνευση</td></tr>
<tr><td>Συμφόρηση Γραμμής Διασύνδεσης</td><td>Cooperative Intrusion Traceback and Response (CITRA)</td></tr>
<tr><td>Μετρήσεις Απορριπτόμενων Πακέτων</td><td>Global Defence Infrastructure (GDI)</td></tr>
<tr><td>NIDS Τοπικού Δικτύου</td><td>Coordinated Suppression of Simultaneous Attacks (COSSACK)</td></tr>
<tr><td></td><td>Συνεργατικές Οντότητες</td></tr>
</table>

Πίνακας 2.1: Κύριες μεθοδολογίες ανίχνευσης επιθέσεων DDoS

παρουσιάζονται διαλείψεις στις καταγραφές τους.

Το πρόβλημα του μεγάλου όγκου κίνησης είναι δυνατόν να περιοριστεί, υπό διάφορες συνθήκες, με κατάλληλες τεχνικές δειγματοληψίας (packet sampling) όπως παρουσιάζεται στο [Esta01]. Άλλη προσέγγιση είναι η χρησιμοποίηση εξειδικευμένου δικτυακού υλικού που διαθέτει ικανότητα χειρισμού και επεξεργασίας της κίνησης χωρίς αυτή να χρειάζεται να περάσει από τον επεξεργαστή του υπολογιστικού συστήματος. Αυτό επιτυγχάνεται στο μέρος του υλικού

με ειδικούς επεξεργαστές (network processors) και στο μέρος του λογισμικού με υλοποίηση αλγορίθμων βελτιστοποιημένων ειδικά για τις εργασίες που θα κληθούν να αναλάβουν [Kohl00]. Η ύπαρξη τμήματος με λογισμικό προσφέρει ευελιξία στη λειτουργία με διαφορετικά πρωτόκολλα. Network processors έχουν αναπτυχθεί με κλειστή αρχιτεκτονική και κώδικα προσαρμοσμένο για συγκεκριμένους κατασκευαστές δικτυακού εξοπλισμού αλλά και ανοικτής αρχιτεκτονικής και κώδικα, όπως π.χ. το liberouter [Libe04][21].

Η μετρούμενη αύξηση της χρησιμοποίησης μιας γραμμής μπορεί να οφείλεται σε φυσιολογικά αίτια και επομένως απαιτείται ανάλυση του είδους και του προορισμού της κίνησης και η παρακολούθηση των ενεργών δικτυακών συστημάτων. Απλές πρακτικές προς αυτή την κατεύθυνση είναι:

- Μετρήσεις από λίστες ελέγχου πρόσβασης (Access Control Lists—ACLs) που καταγράφουν ορισμένες διελεύσεις πακέτων (permit lists) [Behr02].

- Η παρακολούθηση του φόρτου δρομολογητών, όπως περιγράφεται στο [Behr02]. Εξετάζεται η διαφορά ανάμεσα στο συνολικό φόρτο και το φόρτο διακοπών (interrupt CPU load) στον επεξεργαστή του δρομολογητή. Σχετική ισότητα υποδεικνύει μεγάλη επιβάρυνση για απλή μεταγωγή πακέτων (packet switching), άρα το πέρασμα μεγάλου όγκου κίνησης προς την ίδια κατεύθυνση. Μεγάλη αύξηση αυτής της διαφοράς σημαίνει επιβάρυνση του δρομολογητή από κίνηση που κατευθύνεται ειδικά σε αυτόν, άρα πιθανόν να πρόκειται για επίθεση DoS εναντίον του.

[21] Ο εξειδικευμένος αυτός δικτυακός εξοπλισμός αναπτύσσεται για μια ευρύτερη χρησιμοποίηση στη διαχείριση δικτύων, π.χ. δημιουργία δρομολογητών υψηλών επιδόσεων, υλοποίηση πολιτικών ποιότητας υπηρεσίας (Quality of Service — QoS), έκδοση στατιστικών δικτύου κ.λπ.

– Μέτρηση του πλήθους των πακέτων που απορρίπτονται από υπερχείλιση των ουρών του δρομολογητή (drops), όπως προτείνεται στο [Maha02] και καθορισμός των γενικών ομάδων κίνησης (aggregates) με βάση τα κοινά χαρακτηριστικά των απορρίψεων.

Οι μέθοδοι αυτές επιτρέπουν την καλύτερη διάκριση των αιτιών της συμφόρησης του δικτύου και, εφόσον ανιχνευτεί μια εξελισσόμενη επίθεση, εντοπίζουν τα χαρακτηριστικά τής. Μέθοδοι ανίχνευσης υψηλότερης ακρίβειας βασίζονται στη λεπτομερή ανάλυση της εισερχόμενης κίνησης, π.χ. ο μηχανισμός Netflow της Cisco [Cisc-net]. Με βάση αυτές τις μετρήσεις ροών μπορούν να υλοποιηθούν συστήματα IDS διάγνωσης ανωμαλιών για περιστατικά DDoS. Αναλογικά μεγάλη αύξηση πακέτων σε σχέση με τις ροές κίνησης αποτελεί ένδειξη για την ύπαρξη μιας συνεχούς αποστολής δεδομένων από τις ίδιες πηγές προς τις ίδιες κατευθύνσεις που μπορεί π.χ. να οφείλεται σε επίθεση «πλημμύρα πακέτων ping» (ping flood)[22]. Δυσανάλογα πολλές ροές και αύξηση του λόγου ροών προς πακέτα δείχνουν την αποστολή μικρού αριθμού πακέτων από μεγάλο αριθμό πολλών διαφορετικών διευθύνσεων, π.χ. επίθεση SYN. Οι παράμετροι αυτοί μπορούν να συνδυαστούν και με άλλα δεδομένα όπως το εύρος των διευθύνσεων παραλήπτη, τα συγκεκριμένα είδη των πακέτων κ.λπ. Τα στοιχεία αυτά μπορούν να διαγνώσουν κάποια περιστατικά DDoS ακόμα και αν η κίνηση δεν παρουσιάζει συνολικά σημαντικές διαφορές όπως παρουσιάζεται στο [Kots01]. Στα επόμενα αναφέρονται ορισμένες σχετικές προσεγγίσεις:

– Το εργαλείο «*Πανόπτης*» [Κοτσ00], που αναπτύχθηκε στο Κέντρο Δικτύων του ΕΜΠ, πραγματοποιεί αναλύσεις που βασίζονται σε αποτυ-

[22] Δείτε σχετικά την ενότητα 2.1.2.

πώσεις της κίνησης από το Netflow. Συγκεντρώνει πληροφορίες κίνησης από τους δρομολογητές στα άκρα μεγάλων δικτύων (δρομολογητές συνόρου—border routers). Σε κάθε δρομολογητή, οι συνδέσεις (interfaces) του δρομολογητή εξετάζονται ανά ζευγάρια για το πλήθος πακέτων και ροών (flows) κίνησης που διεκπεραιώνουν. Οι μετρήσεις αυτές ελέγχονται για σημαντικές στατιστικές αποκλίσεις σε σχέση με προηγούμενες μετρήσεις. Στη συνέχεια το σύστημα ορίζει αυτόματα φίλτρα στους δρομολογητές εισόδου του δικτύου σύμφωνα με τα συμπεράσματα που προκύπτουν από την ανάλυση κίνησης που έχει κάνει. Σε νεότερες εκδόσεις το σύστημα λειτουργεί στο IPv6 και διατηρεί αρχείο μετρήσεων ώστε μεγάλες διαφοροποιήσεις της κίνησης να αντιπαραβάλλονται με τη συμπεριφορά της σε αντίστοιχες χρονικές στιγμές στο παρελθόν (π.χ. αυξημένη κίνηση στην έναρξη της εργάσιμης ημέρας) [Ανδρ03].

– Μια παρόμοια αντιμετώπιση ακολουθείται στο Ευρωπαϊκο έργο SCAMPI [Scam04]. Χρησιμοποιούνται κάρτες δικτύου (Network Interface Cards–NICs) και Network Processors σε περιβάλλον ταχυτήτων της τάξης Gbps. Για κάθε μια από διάφορες παραμέτρους της κίνησης που παρακολουθούνται αναγνωρίζεται ως ύποπτο γεγονός η υπέρβαση του μέσου όρου σε κάθε μία από έναν αριθμό («παράθυρο») από διαδοχικές δειγματοληψίες.

– Ορισμένες προσεγγίσεις δε βασίζονται αποκλειστικά την παρακολούθηση της κίνησης αλλά λαμβάνουν υπ' όψιν και άλλα χαρακτηριστικά των επιθέσεων DDoS για την ανίχνευσή τους. Στο [Peng04] παρακολουθείται το πλήθος διευθύνσεων IP πηγής προς ένα δίκτυο και αναλύονται οι νέες διευθύνσεις που καταγράφονται σε σχέση με τον αριθμό πακέτων που

παρουσιάζονται ταυτόχρονα. Στη διάρκεια κάποιας ύποπτης ανωμαλίας οι διαφορετικοί συνδυασμοί των ταυτόχρονων αλλαγών στους αριθμούς πακέτων και στο πλήθος των εντελώς νέων διευθύνσεων μπορούν να υποδείξουν κατά προσέγγιση αν πρόκειται για φυσιολογική κίνηση, «ξαφνικό πλήθος» (νόμιμη αύξηση της κίνησης — "flash crowd"), ή επίθεση DDoS με μεγάλο βαθμό κατανομής.

– Οι προηγούμενες μέθοδοι είναι επίσης δυνατόν να εφαρμοστούν σε οποιοδήποτε σημείο κατά μήκος του μονοπατιού μιας επίθεσης. Στο [Reih02] προτείνεται το "*D-Ward*", ένα σύστημα αντιμετώπισης των επιθέσεων DDoS στην πηγή τους. Ύποπτα περιστατικά εντοπίζονται με την καταγραφή των εξερχόμενων ροών κίνησης και τη σύγκριση τους με μοντέλα νόμιμης κίνησης.

Οι λύσεις που παρουσιάστηκαν δεν κλιμακώνονται σε περισσότερες της μίας διαχειριστικής περιοχής στο Διαδίκτυο (Administrative Domains) ώστε να συνδυάσουν στοιχεία από αυτά. Ο κεντρικός έλεγχος των μεθόδων αυτών σε κάθε περιοχή (domain) αποτρέπει την επέκταση τους σε συνεργατική λειτουργία. Για την κατανεμημένη χρήση τους απουσιάζει η απαραίτητη υποδομή που θα αναλάβει τις επικοινωνίες μεταξύ τους και θα επιτρέψει το συντονισμό της συλλογής στοιχείων και το συνδυασμό της ανάλυσης των αναφορών. Απαιτείται επίσης και η εκπόνηση κοινών πολιτικών αντιμετώπισης. Έτσι, έχουν προταθεί μια σειρά από λύσεις που επιδιώκουν να κάνουν δυνατή τη συνεργασία ανάμεσα σε πολλά δίκτυα.

– Η υποδομή Cooperative Intrusion Traceback and Response (CITRA) [Schn00] [Schn01] [Ster01] οργανώνει τμήματα μεγάλων δικτυακών δια-

χειριστικών περιοχών (domains) σε «συνδεόμενες γειτονιές» ("interconnected neighborhoods") που όλες μαζί ορίζουν μια «κοινότητα» ("Community"). Χρησιμοποιεί ένα ειδικό πρωτόκολλο, το Intruder Detection and Isolation Protocol (IDIP) για τις επικοινωνίες μεταξύ τους. Συσκευές του CITRA (CITRA agents) σε κάθε «γειτονιά» που θα διαπιστώσουν (με τη βοήθεια συστημάτων IDS) κάποια επίθεση, αποστέλλουν τα στοιχεία της με μηνύματα IDIP σε γειτονικές τους μονάδες της κοινότητας. Αν η επίθεση περνάει και από αυτές συγκεντρώνουν στοιχεία για τη διαδρομή της επίθεσης (traceback) και μπορούν να αναλάβουν τοπικά μέτρα αντίδρασης (response). Ταυτόχρονα διαπιστωμένες επιθέσεις μεταδίδονται και σε ένα κεντρικό σημείο διαχείρισης, το «Συντονιστή Ανακάλυψης» ("Discovery Coordinator") ο οποίος έχει τη γενική εικόνα για την κατάσταση ασφαλείας της κοινότητας. Οι αναφορές μεταξύ των CITRA agents ελέγχονται από πολιτικές που μειώνουν τις πολλαπλές επαναλήψεις, αποτρέπουν την αναμετάδοση (από πριν γνωστών) λανθασμένα θετικών ανιχνεύσεων (false positives) και βοηθούν στη σύνοψη (aggregation) μηνυμάτων σχετικού περιεχομένου. Συμπληρωματικές πολιτικές καθορίζουν την εμπιστοσύνη στις ανταλλαγές ανάμεσα σε διαφορετικές «γειτονιές» και τα μέτρα αντίδρασης που θα ληφθούν σε κάθε μία από αυτές.

– Στο [Wan02] οι Wan και συνεργάτες προτείνουν τη δημιουργία μιας «Παγκόσμιας Υποδομής Άμυνας» (Global Defense Infrastructure—GDI) που περιλαμβάνει και το κατανεμημένο σύστημα ανίχνευσης Distributed Attack Detection (DAD). Η υποδομή GDI επιδιώκει να χρησιμοποιήσει

την ανάλυση ανωμαλιών κίνησης[23] για την ανίχνευση επιθέσεων DDoS στους κύριους παρόχους που προσφέρουν υποδομή κορμού (backbone ISPs) για το Διαδίκτυο. Σε κάθε έναν από αυτούς εγκαθίστανται τοπικά συστήματα ανίχνευσης (Local Detection Systems — LDS) που αναλαμβάνουν τέσσερις βασικές λειτουργίες: ανίχνευση περιστατικών ύποπτων για επιθέσεις DDoS, μετάδοση της πληροφορίας ανίχνευσης σε άλλα LDS, διάγνωση για το κατά πόσον υφίσταται μια επίθεση και λήψη μέτρων αντίδρασης. Τα LDS είναι σε μεγάλο βαθμό «αρθρωτά» (modular). Η αρχιτεκτονική αυτή επιτρέπει τη χρησιμοποίηση εξειδικευμένου υλικού στο τμήμα παρακολούθησης της κίνησης, ενώ σε διάφορα σημεία μπορούν να εγκατασταθούν και επιπλέον LDS παρακολούθησης με μειωμένη την υπόλοιπη λειτουργικότητα τους. Η επικοινωνία μεταξύ των LDS σε διαφορετικά σημεία της υποδομής GDI επιτρέπει την από κοινού λήψη μέτρων σε μεγάλο τμήμα του Διαδικτύου ταυτόχρονα. Μέτρα αντίδρασης λαμβάνονται σε εκείνες τις θύρες των δρομολογητών υποδομής (backbone routers) που αναγνωρίζονται να έχουν μεγάλη συνεισφορά στην επίθεση[24]. Στήν ίδια εργασία [Wan02] υποστηρίζεται με προσομοιώσεις ότι το σύστημα έχει την πιο θετική επίδραση για την αναχαίτιση επιθέσεων στις περιπτώσεις μικρού προς μεσαίου μεγέθους επιθέσεων ως προς τη συμμετοχή επιτιθέμενων (2,5%-7,5% του συνολικού αριθμού των κόμβων του Διαδικτύου).

[23] Συγκεκριμένα ανωμαλίες στον όγκο της κίνησης. Κατ' αυτό τον τρόπο, στις συνδέσεις κορμού (backbone links) που παρακολουθούνται υπάρχει θετική αναγνώριση μόνο σε περιπτώσεις σημαντικών επιθέσεων που αφορούν ολόκληρο το Διαδίκτυο.

[24] Έτσι το σύστημα δε μπορεί να έχει ιδιαίτερη συνεισφορά σε περιπτώσεις εξαιρετικά μεγάλων επιθέσεων (που έχουν ως πηγές γύρω στο 15%-25% των κόμβων που Διαδικτύου) γιατί η επιθετική κίνηση προέρχεται από όλες τις κατευθύνσεις ταυτόχρονα.

– Στο [Papa03] προτείνεται το σύστημα Coordinated Suppression of Simultaneous Attacks (COSSACK) που εγκαθιστά εξειδικευμένο λογισμικό σε σημεία σύνδεσης μεταξύ συνεργαζόμενων δικτύων. Το λογισμικό δημιουργεί έτσι ένα εξειδικευμένο κόμβο ("watchdog") ο οποίος για τη διαχειριστική του περιοχή λαμβάνει αναφορές από διαφόρων ειδών συστήματα IDS και καταλήγει σε αποφάσεις πάνω στην ύπαρξη εισερχόμενης επίθεσης σε συνεργασία με τους κόμβους watchdog άλλων δικτύων. Στη συνέχεια μπορεί να αναλάβει μέτρα αντίδρασης με το φιλτράρισμα της επιθετικής κίνησης. Τα στοιχεία του περιστατικού αναμεταδίδονται στους κόμβους με τη χρήση μιας υποδομής multicast και χρησιμοποιείται ένα ειδικό κανάλι για κάθε περιστατικό. Κάθε κόμβος watchdog που λαμβάνει μια αναφορά περιστατικού εξετάζει το δίκτυο του για να ανιχνεύσει τυχόν εξερχόμενη κίνηση επίθεσης από αυτό και αν κάτι τέτοιο ισχύει λαμβάνει μέτρα διακοπής της. Στο τμήμα της ανίχνευσης το COSSACK πέρα από την απλή ανακάλυψη ενός περιστατικού το ταξινομεί επίσης με βάση την ανάλυση της ταχύτητας αύξησης της κίνησης[25] και τη «φασματική» συμπεριφορά της. Η αξία των συγκεκριμένων στοιχείων έχει διαφανεί από την ανάλυση επιθέσεων DDoS που γίνεται στο [Huss03][26].

Στην παρούσα εργασία η προσέγγιση των Συνεργατικών Οντοτήτων επιδιώκει να δημιουργήσει μια υποδομή για την συνεργατική ανίχνευση και αντιμετώπιση επιθέσεων DDoS. Τα CITRA, GDI και COSSACK συγκρίνονται με την προτεινόμενη προσέγγιση στο κεφάλαιο 6.

[25] Για να πάρει ενδείξεις κατά πόσον προέρχεται από κεντρική πηγή (centralized) ή είναι κατανεμημένη.

[26] Παρουσιάζεται στην ενότητα 2.2.2 αυτού του κεφαλαίου.

Ανακάλυψη της Διαδρομής

Η ανακάλυψη της διαδρομής που ακολουθεί μια επίθεση για να καταλήξει στο θύμα επιτρέπει, αν γίνει κατά τη διάρκεια ενός περιστατικού, τη συνεργασία ανάμεσα σε κάποια από τα δίκτυα για την από κοινού ανάσχεση της. Στην περίπτωση αυτή ο εντοπισμός του μονοπατιού θα πρέπει να γίνει πολύ σύντομα[27] και με μεγάλη ακρίβεια. Ακόμα όμως και μετά από το τέλος του περιστατικού η ανακάλυψη της πλήρους διαδρομής μπορεί να οδηγήσει στα υπολογιστικά συστήματα πηγές της επίθεσης και να αποτρέψει την περαιτέρω χρησιμοποίηση τους. Στη συντριπτική τους πλειοψηφία οι επιθέσεις άρνησης υπηρεσίας επιχειρούν να καλύψουν τα ίχνη τους χρησιμοποιώντας την παραποίηση της διεύθυνσης IP του αποστολέα. Έτσι, η αναγνώριση τόσο της πραγματικής πηγής τους όσο και της διαδρομής που ακολουθήθηκε καθίσταται εξαιρετικά δυσχερής. Αυτοματοποιημένες διαδικασίες ανακάλυψης της διαδρομής απαιτούν συνήθως να προϋπάρχουν κατάλληλες υποδομές ανίχνευσης και παρακολούθησης. Κάποιες, που προτείνουν αλλαγές στην υποδομή και τη λειτουργία του Διαδικτύου, απαιτούν τη συμφωνία των επίσημων οργάνων κατευθύνσεως του Διαδικτύου (π.χ. IETF).

Ο Πίνακας 2.2 δίνει τις κυριότερες μεθόδους και ερευνητικές προτάσεις που ακολουθούνται στο πρόβλημα της ανακάλυψης της διαδρομής μιας ροής κίνησης και χωρίζονται σε τρεις κύριες κατηγορίες [Lee02]:

Α. Σήμανση (marking) κάποιων πακέτων με πληροφορία για το δρόμο

[27] Όπως προκύπτει από το [Moor01], η πολύ σύντομη διάρκεια πολλών επιθέσεων αχρηστεύει προσπάθειες αναζήτησης και παρακολούθησης της διαδρομής από τους διαχειριστές των δικτύων σε πραγματικό χρόνο.

που ακολούθησαν

Με αυτό τον τρόπο παρέχεται μια ένδειξη της διαδρομής των πακέτων προς τον τελικό προορισμό τους. Η σήμανση γίνεται με «υπερφόρτωση» (overloading) κάποιων ήδη υπαρχόντων πεδίων των πακέτων IP.

Ανακαλυψη της Διαδρομης		
Σημανση Πακετων	Αποστολη Πακετων Αναφορας	Παρακολουθηση της Διαδρομης προς την Πηγη
Καταγραφή Τμημάτων της Διαδρομής	Ειδικά Μηνύματα ICMP (itrace)	Ανάλυση Αρχείων Καταγραφή IDS
Εγγραφές Σήμανσης με Hash Values		Καταγραφή και Αποθήκευση Πακέτων
Αλγεβρική Κωδικοποίηση της Διαδρομής		Υπερκείμενο Δίκτυο Ανακάλυψης (Centertrack)
		Έλεγχος των Δρομολογητών (Pushback)
		Ανάλυση των Πακέτων που Διαπέρασαν τα Μέτρα Ασφαλείας (DPF)
		Υποδομές Συνεργασίας Δικτύων (CITRA, Συνεργατικές Οντότητες)

Πίνακας 2.2: Τεχνικές για την ανακάλυψη της διαδρομής μιας επίθεσης DDoS

– Στο [Sava00] αναλύονται διάφορες μέθοδοι σήμανσης πακέτων IP (με τυχαίο ή προκαθορισμένο σχήμα δειγματοληψίας). Το θύμα μπορεί, θεωρητικά, να ανασυνθέσει τη διαδρομή εξετάζοντας τη σήμανση πάνω στα πακέτα. Ακόμα και μια πολύ αραιή σήμανση πακέτων, εφόσον η κακόβουλη κίνηση της επίθεσης θα υπερτερεί της νόμιμης, προσφέρει αρκετά στοιχεία για την αναγνώριση του μονοπατιού. Στην εργασία προτείνεται η εγγραφή

στα πακέτα IP τυχαίων τμημάτων της διαδρομής τους (edge sampling). Αυτό μπορεί να επιτευχθεί με προσθήκη εγγραφών των διευθύνσεων IP από δύο (τυχαίους) δρομολογητές στη διαδρομή μαζί με την απόσταση μεταξύ τους. Η πληροφορία μεταφέρεται με «υπερφόρτωση» του Πεδίου Αναγνώρισης στην επικεφαλίδα του πακέτου IP (IP Identification field) που κανονικά χρησιμοποιείται από κατακερματισμένα πακέτα. Η μέθοδος εξασφαλίζει τη λειτουργία της ακόμα και αν δεν υλοποιείται σε κάθε δίκτυο. Οι συγγραφείς εκτέλεσαν προσομοιώσεις με σήμανση στο 1/25 των πακέτων και βρήκαν ότι ακόμα και οι μακρύτερες διαδρομές (25-30 κόμβοι) μπορούν να αναγνωριστούν με μεγάλο βαθμό βεβαιότητας μετά τη λήψη 4.000 πακέτων, ένας αριθμός αρκετά μικρός με δεδομένο το μεγάλο πλήθος πακέτων που παράγουν οι επιθέσεις DDoS.

– Στο [Song01] η μεθοδολογία αυτή επεκτείνεται και αντί για απλή καταγραφή διευθύνσεων IP κατά τη διαδρομή του πακέτου χρησιμοποιούνται συναρτήσεις κατακερματισμού για μικρότερο μέρος της ίδιας πληροφορίας. Για τη λειτουργία της μεθόδου υπάρχει η προϋπόθεση ο τελικός παραλήπτης πρέπει να γνωρίζει σε κάποιο βαθμό την τοπολογία πριν το δίκτυο του. Επίσης προτείνεται ένα σχήμα για την επιβεβαίωση της ταυτότητας του δρομολογητή (authentication) πάνω στη σήμανση που κάνει.

– Μια διαφορετική προσέγγιση για τη σήμανση των πακέτων προτείνει την αλγεβρική κωδικοποίηση των διαδρομών που έχουν αυτά ακολουθήσει [Dean01]. Η μέθοδος βοηθά στην εξάλειψη του «θορύβου» από νόμιμη κίνηση και στην ανακατασκευή πολλαπλών διαδρομών.

Β. Αποστολή πακέτων «αναφοράς» που θα «συνοδεύουν» τα πακέτα

κανονικής κίνησης

Τα πακέτα αυτά δίνουν ενδείξεις στον τελικό προορισμό για τα σημεία απ' όπου πραγματικά πέρασε η κίνηση που λαμβάνει.

– Η μεθοδολογία αυτή, με το όνομα "itrace", οφείλεται στο Bellovin και εξετάστηκε από τον οργανισμό IETF για προτυποποίηση έως το στάδιο του Internet Draft [Bell00]. Ένας δρομολογητής που θα υλοποιήσει αυτή τη λύση επιλέγει ένα από τα πακέτα που διεκπεραιώνει και στέλνει προς τον ίδιο προορισμό ένα μήνυμα ICMP (ICMP Traceback message) με πληροφορίες για αυτό το πακέτο και το σημείο απ' όπου έχει περάσει. Η συχνότητα επιλογής πακέτων για τη δημιουργία των μηνυμάτων itrace προτείνεται στο ένα ανά 20.000 και είναι ελεγχόμενη από το διαχειριστή. Ο τελικός παραλήπτης μπορεί να συνδυάσει κάποια από τα πακέτα που έλαβε με τα μηνύματα ICMP για να ανακαλύψει την πραγματική προέλευση τους. Στο [Mank01] εξετάζονται διάφορες πιθανές αδυναμίες του σχήματος, όπως το γεγονός ότι κοντά στις πηγές της επίθεσης (όπου η κακόβουλη κίνηση είναι συγκριτικά μικρή) δε θα παράγονται αρκετά μηνύματα itrace. Προσδιορίζονται ως «χρήσιμα» τα μηνύματα itrace τα οποία αντιστοιχούν σε πακέτα επίθεσης και τα οποία ο παραλήπτης ενδιαφέρεται να λάβει. Οι συγγραφείς προτείνουν τη χρήση του BGP για τη διανομή «ψηφίων πρόθεσης παραλαβής» (intention bit) μηνυμάτων itrace από ενδιαφερόμενους κόμβους καθώς και το μηχανισμό αποστολής «χρήσιμων» μηνυμάτων.

Γ. Αναζήτηση σε κόμβους που μεταφέρουν κίνηση προς το θύμα

– Η ανάλυση αρχείων καταγραφής (log files) από εφαρμογές ανίχνευσης

γίνεται μετά το περιστατικό αλλά μπορεί να αποδώσει χρήσιμα αποτελέσματα εφόσον τέτοια αρχεία τηρούνται σε ένα μεγάλο αριθμό δικτύων ώστε να περιλαμβάνονται σημαντικά τμήματα της διαδρομής.

– Στο [Snoe01] προτείνεται μια μέθοδος για την ανακάλυψη της διαδρομής μετά το περιστατικό που αφορά την προσωρινή καταγραφή των πακέτων που έχουν περάσει από ένα δίκτυο. Η καταγραφή αφορά τμήμα μόνον από κάθε πακέτο. Γίνονται ομαδοποιήσεις ομοειδών πακέτων (digests)[28] και χρησιμοποιείται μια συνάρτηση κατακερματισμού (hash function) για την αποθήκευση σε ένα κατάλληλο σχήμα Βάσης Δεδομένων. Σε κάθε δίκτυο που υλοποιεί τη μέθοδο ειδικά συστήματα αναζήτησης σε αυτή τη βάση είναι δυνατόν να αποκαλύψουν τη διαδρομή μιας ροής πακέτων. Απαιτείται να είναι γνωστός ο τελευταίος δρομολογητής του δικτύου στόχου και η αναζήτηση να γίνεται μέσα σε εύλογο χρονικό διάστημα από το περιστατικό (π.χ. 1-2 ημέρες).

– Στην αναγνώριση της διαδρομής της επίθεσης με τη χρήση εναλλακτικών οδεύσεων η κακόβουλη κίνηση μπορεί να παρακολουθείται με την αποστολή της μέσω ενός υπερκείμενου δικτύου (overlay network). Στη μεθοδολογία CenterTrack [Ston00], η οποία υλοποιείται στο εσωτερικό μεγάλων δικτύων παρόχων διασύνδεσης (ISPs), δημιουργούνται σήραγγες τύπου εικονικής ιδιωτικής σύνδεσης (Virtual Private Network links—VPN) από όλους τους δρομολογητές άκρου (edge routers) προς ένα κεντρικό σημείου του δικτύου. Στη διάρκεια ενός περιστατικού DDoS όλη η κίνηση προς το θύμα (επιθετική ή νόμιμη) δρομολογείται κανονικά

[28] Η τεχνική μειώνει τις ανάγκες αποθηκευτικού χώρου και εξασφαλίζει απόρρητο για τις επικοινωνίες, ένα σημαντικό ζήτημα στην περίπτωση της καταγραφής κίνησης.

προς το θύμα ώστε να μην επηρεάζεται η συνδεσιμότητα του. Με παρακολούθηση της κίνησης μόνον στις σήραγγες (αντί για ολόκληρο το δίκτυο) μπορούν να εντοπιστούν τα σημεία (δρομολογητές) εισόδου της επιθετικής κίνησης στο δίκτυο και να τεθούν εκεί τα κατάλληλα φίλτρα ή να ενημερωθούν τα διασυνδεόμενα εκεί δίκτυα κορμού υψηλότερου επιπέδου. Για να λειτουργήσει η μέθοδος η επίθεση πρέπει να διαρκέσει αρκετά ώστε ο πάροχος να έχει το χρόνο να δρομολογήσει την κίνηση του θύματος μέσα από τις σήραγγες. Το σχήμα 2.6 παρουσιάζει την αρχιτεκτονική Centertrack.

Σχήμα 2.6: Το σύστημα CenterTrack και το υπερκείμενο δίκτυο που δημιουργεί [Ston00]

– Η μεθοδολογία "*Pushback*" [Maha02] [Ioan02] ακολουθεί διαφορετική προσέγγιση. Ενημερώνει (με τη χρήση ειδικού πρωτοκόλλου) διαδοχικά

τους δρομολογητές που βρίσκονται πάνω στο μονοπάτι της επίθεσης ακολουθώντας αντίθετη διαδρομή, από το θύμα προς την πηγή. Κάθε ένας δρομολογητής αποκαλύπτει τον επόμενο (ή τους επόμενους) σε αυτή τη διαδρομή. Ταυτόχρονα παίρνει μέτρα αντιμετώπισης της επίθεσης. Απαιτείται όμως η εγκατάσταση και λειτουργία ειδικού λογισμικού σε κάθε έναν δρομολογητή καθώς και η δυνατότητα πρόσβασης σε αυτόν από την πολιτική ασφαλείας του δικτύου. Στο εσωτερικό ενός δικτύου η μέθοδος μπορεί να λειτουργήσει πολύ αποδοτικά. Όσο μακρύτερα από το θύμα όμως είναι ένα δίκτυο και όσο μικρότερη είναι η επίδραση της επίθεσης στο ίδιο, τόσο μικρότερο κίνητρο έχει ώστε να λάβει μέτρα για την μείωση της επίδρασης της επίθεσης και να συνεισφέρει στην ανακατασκευή του μονοπατιού της.

– Σε μια διαφορετική προσέγγιση το Route Based Distributed Packet Filtering (DPF) [Park01] παρέχει μια συνολική πρόταση ανίχνευσης και αντίδρασης σε επιθέσεις DDoS. Οι δρομολογητές κορμού (Core Routers) του Διαδικτύου καλούνται να υλοποιήσουν τον έλεγχο και το φιλτράρισμα της κίνησης ανάλογα με το αν προέρχεται από τις προβλεπόμενες (με βάση τους πίνακες δρομολόγησης) διευθύνσεις προέλευσης. Η μέθοδος DPF βασίζεται στην εφαρμογή αυτού του μέτρου σε ολόκληρο το Διαδίκτυο με την υλοποίηση του λεγόμενου «συστήματος δικτυακής προστασίας ολόκληρου του Διαδικτύου» ("Internet Firewall").Αποδεικνύεται ότι εφόσον ακόμα και ένα μικρό ποσοστό (περίπου 20%) από δρομολογητές κορμού υλοποιήσει αυτή τη μεθοδολογία είναι απλό να ανακαλυφθούν οι πηγές από για εκείνες επιθέσεις που θα καταφέρουν να διαπεράσουν την

υποδομή προστασίας που περιγράφτηκε.

Αντίδραση στην Επίθεση

Για τον έλεγχο της εισερχόμενης κίνησης σε ένα δίκτυο είναι απαραίτητο να ληφθούν μέτρα στα προηγούμενα από το στόχο δίκτυα, από όπου διοχετεύεται αυτή η κίνηση. Από το ίδιο το δίκτυο-θύμα είναι δυνατόν να γίνει φιλτράρισμα ή διακοπή της ροής της κακόβουλης κίνησης στα σημεία εξωτερικής διασύνδεσης. Αυτό όμως θα έχει σαν αποτέλεσμα μόνον την αποτροπή της εισόδου της στο εσωτερικό του δικτύου, ενώ παραμένει το πρόβλημα της ανάλωσης του δικτυακού εύρους στη γραμμή διασύνδεσης.

Αναγκαία για την ανάσχεση μια επίθεσης DDoS είναι η συνεργασία των δικτυακών περιοχών διαχειριστικής ευθύνης (administrative domains) που διασχίζει. Οι προσπάθειες αντίδρασης κατά τη διάρκεια του γεγονότος της επίθεσης μπορεί να εκδηλωθούν από μια ή πολλές δικτυακές περιοχές (domains). Δίκτυα κορμού και πάροχοι (ISPs) είναι δυνατόν να μειώσουν τα αποτελέσματα μιας επίθεσης προς ένα «δίκτυο φύλλο» (”leaf” network) με τον ορισμό ειδικών παρεμποδιστικών ή περιοριστικών φίλτρων στους δρομολογητές εξόδου προς το θύμα.

Κατά συνέπεια η προειδοποίηση για την εκδήλωση της και τα τεχνικά χαρακτηριστικά της πρέπει να μεταδοθούν από τα σημεία ανίχνευσης του περιστατικού (συνήθως το δίκτυο θύμα) προς τα δίκτυα κορμού όπου θα υλοποιηθούν μέτρα. Οι επικοινωνίες αυτές είναι μεταξύ των διαχειριστών των δικτύων με μη αυτοματοποιημένες μεθόδους: ηλεκτρονικό ταχυδρομείο ή απ’ ευθείας συνομιλίες. Διαδικασίες μη ορισμένες με σαφήνεια και μη αυτοματοποιημένες δεν παρέχουν την ταχύτητα που απαιτείται για το χειρισμό τέτοιων περιστατι-

κών. Επιπλέον δεν υπάρχει τυποποίηση στα δεδομένα που θα ανταλλαγούν. Το δικτυακό πρωτόκολλο IDMEF [Deba04], επιδιώκει να δημιουργήσει τέτοια πρότυπα περιγραφής των περιστατικών αλλά δεν ορίζει κάποια συγκεκριμένη μεθοδολογία στην ανταλλαγή αυτών των μηνυμάτων.

Ένας πρόσθετος παράγοντας δυσκολίας είναι η συνήθης έλλειψη συγκεκριμένης πολιτικής αντιμετώπισης των επιθέσεων, ειδικά εάν αυτές αφορούν κάποιο άλλο δίκτυο. Η ανάληψη βοηθητικών μέτρων στη διαδρομή της επίθεσης εξαρτάται από την καλή θέληση του διαχειριστή κάθε δικτύου, τις τοπικές πολιτικές ασφαλείας και τις εταιρικές προτεραιότητες.

Αντιδραση σε Επιθεσεις DDoS		
Προληπτικη	**Κατασταλτικη**	
	Σε μια Δικτυακη Περιοχη	**Κατανεμημενη**
Απόρριψη Πακέτων με Διεύθυνση Πηγής που δε συμφωνεί με την Προέλεση τους (RFC 2827, DPF)	Υλοποίηση Φίλτρων	Global Defence Infrastructure (GDI)
	Διακοπή της Κίνησης προς τον Η/Υ στόχο (Blackholing)	Cooperative Intrusion Traceback and Response (CITRA)
	«Κέντρα Καθαρισμού» της Κίνησης	Coordinated Suppression of Simultaneous Attacks (COSSACK)
		Διαδοχική Συνεργασία Δρομολογητών (Pushback)
		Συνεργατικές Οντότητες

Πίνακας 2.3: Μέθοδοι αντιμετώπισης επιθέσεων DDoS

Όπως παρουσιάζεται στον Πίνακα 2.3 οι δυνατές λύσεις αντιμετώπισης των επιθέσεων DDoS μπορούν να κατηγοριοποιηθούν ως προληπτικές (proactive) ή κατασταλτικές (reactive).

– Μια πολύ τυπική προληπτική αντίδραση είναι η παρεμπόδιση πακέτων με διευθύνσεις προέλευσης που δεν αντιστοιχούν στις εφαρμοζόμενες πολιτικές δρομολόγησης. Η μέθοδος DPF [Park01] προτείνει την εφαρμογή αυτού του μέτρου σε ολόκληρο το Διαδίκτυο. Προφανώς όσο μεγαλύτερος αριθμός δρομολογητών κορμού συμμετέχει τόσο πιο αποδοτικό θα είναι το αποτέλεσμα κατά των επιθέσεων DDoS. Εντούτοις η μέθοδος έχει αδυναμίες: χρειάζεται αποδοτική υλοποίηση των αλγορίθμων φιλτραρίσματος, με δεδομένο ότι πρόκειται για δρομολογητές που χειρίζονται μεγάλους όγκους κίνησης. Επιπλέον υπάρχουν περιπτώσεις που η ακριβής δρομολόγηση δεν είναι γνωστή και έτσι η μέθοδος μπορεί να οδηγήσει σε παρεμπόδιση νόμιμων επικοινωνιών. Είναι επίσης φανερό ότι η αποδοτικότητα του μέτρου μειώνεται όσο πλησιάζουμε προς περιφερειακά σημεία του Διαδικτύου[29].

– Η ίδια μέθοδος μπορεί επίσης να εφαρμοστεί σε επίπεδο δικτυακής περιοχής (domain) ως μέρος της πολιτικής ασφαλείας. Σε αυτή την περίπτωση η υλοποίηση γίνεται στους δρομολογητές εξόδου (egress routers) και αφορά την παρεμπόδιση πακέτων που δεν έχουν διεύθυνση προέλευσης από το συγκεκριμένο δίκτυο. Η πρακτική αυτή, περιγράφεται και από το RFC 2827 [Ferg00], και μέχρι σήμερα έχει περιορισμένη εφαρμογή.

[29]Επειδή δε θα υπάρχει πολύ μεγάλο τμήμα νόμιμων πηγών προερχόμενο από μία κατεύθυνση.

– Όταν η επίθεση έχει σα στόχο μόνον ένα συγκεκριμένο σύστημα, μια πρακτική που χρησιμοποιείται είναι η πλήρης διακοπή της κίνησης προς αυτό στο ακριβώς προηγούμενο δίκτυο (αυτό του παροχέα δικτυακής σύνδεσης) [Behr02]. Η μέθοδος ονομάζεται «διοχέτευση σε μαύρη τρύπα» ("blackholing") και μπορεί να υλοποιηθεί πολύ εύκολα στους δρομολογητές του Παροχέα. Επιπλέον δεν έχει ιδιαίτερο υπολογιστικό κόστος επειδή χρησιμοποιείται ο μηχανισμός δρομολόγησης αντί αυτού του φιλτραρίσματος. Αν και ολοκληρώνει την άρνηση δικτυακής σύνδεσης προς το θύμα αποκόπτοντας το ουσιαστικά από το Διαδίκτυο, η γραμμή του δικτύου πελάτη ανακουφίζεται από την κακόβουλη κίνηση.

– Μια νεότερη πρόταση [Agar04] συνδυάζει την επιλογή νέας δρομολόγησης για την κίνηση του θύματος μέσα από σήραγγες (όπως το CenterTrack πιο πάνω) με μια παραλλαγή της μεθόδου αποκοπής της επιθετικής κίνησης προς το τελικό θύμα. Στο δίκτυο του παροχέα δημιουργούνται σήραγγες (VPNs) από τους δρομολογητές εισόδου προς ένα σημείο ελέγχου. Στη συνέχεια όλη η κίνηση προς το θύμα οδηγείται από αυτό το δρόμο στο σημείο ελέγχου όπου ειδικός εξοπλισμός («Κέντρα Καθαρισμού»—"Cleaning Centers") αναλαμβάνει να διαχωρίσει και να απορρίψει τα πακέτα που χρησιμοποιούνται στην επίθεση. Στη συνέχεια μέσα από άλλες σήραγγες η (νόμιμη πλέον) κίνηση καταλήγει στον παραλήπτη. Με την εγκατάσταση κατάλληλων κανόνων δρομολόγησης στο σημείο σύνδεσης του δικτύου πελάτη και η εξερχόμενη κίνηση από αυτόν θα περάσει από τον ίδιο δρόμο και την ίδια διαδικασία πριν βγει στο υπόλοιπο δίκτυο. Η λύση αυτή απαιτεί τη γρήγορη ανίχνευση των επιθέσεων, την αλλαγή στη

δρομολόγηση προς και από συγκεκριμένα δίκτυα πελάτες και, κυρίως, την ικανότητα για ακριβή εντοπισμό της κακόβουλης κίνησης προς και από το θύμα.

Η προτεινόμενη σε αυτή την εργασία λύση υπάγεται στην κατηγορία των αυτόματων, κατανεμημένων συστημάτων αντίδρασης όπου ένας αριθμός από δίκτυα συνεργάζονται και συντονίζουν τις ενέργειες τους προκειμένου να μειώσουν τα αποτελέσματα μιας επίθεσης. Άλλες αντίστοιχες προσεγγίσεις περιλαμβάνουν την υποδομή CITRA, τα συστήματα GID και COSSACK και τη χρήση της λύσης Pushback για περισσότερα του ενός δίκτυα.

2.4 Συμπεράσματα

Συνοψίζοντας την προηγούμενη ανάλυση καταλήγουμε σε ορισμένα βασικά στοιχεία που χαρακτηρίζουν τις επιθέσεις DDoS και βοηθούν στην καλύτερη κατανόηση του φαινομένου:

- Τα έντονα αποτελέσματα των επιθέσεων DDoS και η απόκρυψη της πραγματικής τους προέλευσης τις κάνει ελκυστικές σε μεγάλο αριθμό περιπτώσεων, όπως η ανεπίσημη προώθηση αθέμιτων (οικονομικών ή πολιτικών) συμφερόντων, η προβολή «περιθωριακών» κύκλων του Διαδικτύου (Internet Underground) και η υποστήριξη διαμαχών και εκδίκησης ανάμεσα σε άτομα.

- Σε πολλές περιπτώσεις υπάρχει ιεραρχία πολλών επιπέδων για τον έλεγχο της επίθεσης. Έτσι ο επιτιθέμενος δε χρειάζεται παρά να ελέγχει ένα μικρό αριθμό από συστήματα που με τη σειρά τους θα μεταφέρουν οδηγίες

και θα εκκινήσουν τα επόμενα επίπεδα που θα πραγματοποιήσουν την επίθεση.

- Τα συστήματα που πραγματοποιούν την επίθεση μπορούν να είναι οπουδήποτε στον κόσμο, πιθανά ακολουθώντας τις περιοχές εξάπλωσης αυτόματων προγραμμάτων δημιουργίας της υποδομής επίθεσης.

- Τα συστήματα αυτά, όπως και η ακριβής διαδρομή της κακόβουλης κίνησης, συνήθως, δεν είναι δυνατόν να ανακαλυφθούν άμεσα λόγο χρήσης παραποιημένων διευθύνσεων αποστολέα.

- Το πρόβλημα της ανίχνευσης των επιθέσεων DDoS και διαχωρισμού τους από περιστατικά αυξημένης κίνησης είναι ιδιαίτερα πολύπλοκο. Απαιτείται η παρακολούθηση δικτυακών συνδέσεων και εξοπλισμού σε πραγματικό χρόνο και η εφαρμογή μεθόδων ανίχνευσης που έχουν τη δυνατότητα να εντοπίζουν τα χαρακτηριστικά μιας επίθεσης DDoS σε ένα διαρκώς εξελισσόμενο περιβάλλον ασφαλείας.

- Η ανάσχεση της επίθεσης πρέπει να αναγκαστικά πραγματοποιηθεί στα προηγούμενα βήματα, στους πάροχους δικτυακών υπηρεσιών, πριν το δίκτυο του θύματος. Επομένως δημιουργείται η ανάγκη για την κλιμάκωση της αντιμετώπισης σε δίκτυα παρόχων και κορμού με τον κατάλληλο συντονισμό και την έγκαιρη και έμπιστη ανταλλαγή πληροφοριών μεταξύ τους.

Αντίστοιχα προκύπτουν και μια σειρά από απαιτήσεις για ένα αποδοτικό σύστημα αντιμετώπισης των επιθέσεων DDoS:

- Έγκαιρος εντοπισμός της επίθεσης σε κατά μήκος της διαδρομής που ακολουθεί προς το θύμα. Ιδιαίτερα σημαντικός είναι ο προσδιορισμός αυτού του μονοπατιού.

- Σύντομη και αυτοματοποιημένη ενημέρωση για την εξέλιξη της σε όσο το δυνατόν περισσότερα δίκτυα μπορούν να συνεισφέρουν στην καταπολέμηση της (από αυτά που βρίσκονται πάνω στο διαδρομή), πριν το δίκτυο του θύματος.

- Ανάγκη για διαφορετικού τύπου ενέργειες σε κάθε διαφορετικό δίκτυο, σύμφωνες με τις ικανότητες, ανάγκες και εταιρικές πολιτικές του. Οι πολιτικές αυτές όμως θα πρέπει να είναι εξ' αρχής αποφασισμένες για αμεσότητα στην αντίδραση.

- Ευελιξία κατά την αντιμετώπιση της επίθεσης ώστε να είναι δυνατή η προσαρμογή στην αλλαγή των χαρακτηριστικών της. Τα μέτρα που θα εφαρμοστούν, απαιτούν συνεχή έλεγχο για την επιβεβαίωση της καταλληλότητας τους. Επειδή ορισμένες επιθέσεις παρουσιάζουν μεταβλητότητα στη συμπεριφορά τους χρειάζεται παρακολούθηση και τυχόν τροποποιήσεις στα μέτρα ώστε αυτά να παραμείνουν αποτελεσματικά.

- Το σύστημα αντίδρασης πρέπει να παρέχει ασφάλεια πρόσβασης ώστε να μη μπορεί να χρησιμοποιηθεί με κάποιο τρόπο από τους επιτιθέμενους για να προκαλέσει επιπλέον προβλήματα ή περιορισμούς στη φυσιολογική κίνηση.

- Επειδή η αντιμετώπιση των επιθέσεων γίνεται στα δίκτυα κορμού ενός ISP, για να αναλάβει αυτός να βοηθήσει, πιθανόν χωρίς άμεσο οικονομικό

όφελος, θα πρέπει η λύση να έχει λογικές απαιτήσεις εξοπλισμού και διαχειριστικής εργασίας.

- Η λύση θα πρέπει να προσφέρει οφέλη σε όλους τους συμμετέχοντες ώστε να είναι επιθυμητή η υλοποίηση της. Διαφορετικά θα πρέπει να είναι με κάποιο τρόπο ενταγμένη στην οικονομική σχέση των δικτύων ISPs[30] και πελατών, πιθανά με κάποια χρέωση της υπηρεσίας αντιμετώπισης DDoS. Αναφέρεται ότι πρόσφατα η εταιρεία MCI άρχισε να προσφέρει τέτοια υπηρεσία αντιμετώπισης DDoS ως μέρος των συμβολαίων παροχής επιπέδου υπηρεσίας (Service Level Agreements – SLAs) [Info04].

Ας σημειωθεί ότι τη στιγμή αυτή δεν υπάρχει αποδεκτός τρόπος αξιολόγησης και σύγκρισης της αποτελεσματικότητας διαφόρων λύσεων απέναντι σε κάποια συγκεκριμένη ομάδα επιθέσεων που θα χρησιμοποιηθεί ως μετρητικό πρότυπο (benchmark) [Mirk04].

Είναι φανερό ότι οι απαιτήσεις από ένα σύστημα αντιμετώπισης των επιθέσεων DDoS διαφέρουν αρκετά μεταξύ τους, είναι δε δύσκολο να ικανοποιηθούν όλες από μια και μόνον λύση. Όπως θα φανεί στη συνέχεια οι ανωτέρω διαπιστώσεις αποτέλεσαν τις κύριες κατευθύνσεις κατά το σχεδιασμό της προτεινόμενης λύσης ώστε να ικανοποιούνται από αυτή οι περισσότερες απαιτήσεις πελατών και διαχειριστών δικτυακών υπηρεσιών.

[30] Στις περιπτώσεις παρόχων που χρεώνουν των πελάτη με βάση τον όγκο δεδομένων που μεταφέρονται οι επιθέσεις DDoS μπορεί βραχυπρόθεσμα να θεωρηθούν μέχρι και συμφέρουσες.

Κεφάλαιο 3

Η Προτεινόμενη Αρχιτεκτονική

3.1 Εισαγωγή - Παρουσίαση της προτεινόμενης λύσης

Στο προηγούμενο κεφάλαιο αναλύθηκαν η εξέλιξη και τα κύρια χαρακτηριστικά των κατανεμημένων επιθέσεων άρνησης υπηρεσίας (επιθέσεις DDoS). Έχοντας τα δεδομένα αυτά ως σημείο εκκίνησης, στο παρόν κεφάλαιο παρουσιάζεται μια λύση που παρέχει τη δυνατότητα κατανεμημένης ανίχνευσης επιθέσεων, με συμπληρωματικό στοιχείο την παράλληλη αναγνώριση των διαδρομών τους. Η έγκαιρη και, κυρίως, η ακριβής ανίχνευση είναι το πρώτο βήμα για οποιουδήποτε είδους αυτοματοποίηση της αντίδρασης στις επιθέσεις DDoS. Ορίζεται επίσης μια μέθοδος που συνδυάζει τις ενέργειες πολλών διαφορετικών δικτύων παρέχοντας αποτελεσματικές, αυτοματοποιημένες και κατανεμημένες δράσεις εναντίον αυτών των επιθέσεων. Προς την κατεύθυνση εκπλήρωσης των δύο αυτών στόχων (ανίχνευση και αντίδραση) επιλέγεται η δημιουργία μιας κοινότητας

από δικτυακές περιοχές (domains) οι οποίες, με τον κατάλληλο συντονισμό, θα αναλαμβάνουν από κοινού ενέργειες κατά των επιθέσεων DDoS.

Στο θέμα της ανίχνευσης ένα κατανεμημένο σύστημα προσφέρει πληροφορίες που έχουν συλλεχθεί από πολλούς αισθητήρες (sensors), τοποθετημένους στο ίδιο στοιχείο δικτύου (network element) ή σε διαφορετικά, απομακρυσμένα μεταξύ τους, σημεία, από διαφορετικά συστήματα IDS και με διαφορετικές μεθόδους[1]. Στο σημείο (ή σημεία) συνολικής συγκέντρωσης αυτών των πληροφοριών υπάρχει μια ευρύτερη εικόνα της κατάστασης ασφαλείας, ιδανική προϋπόθεση για την αναγνώριση της εξέλιξης και της διαδρομής μιας επίθεσης DDoS που διέρχεται από πολλά δίκτυα.

Η προσέγγιση αυτή έχει τους εξής στόχους:

1. Βελτίωση του βαθμού πληρότητας (Completeness)[2] ανίχνευσης επιθέσεων, δηλαδή αύξηση του αριθμού επιθέσεων που θα γίνει δυνατόν να ανιχνευτούν, ή αντίστοιχα μείωση του ποσοστού «μη-αναγνωρίσεων» πραγματικών επιθέσεων (False Negatives).

2. Μέσω συνδυασμού αναφορών, λειτουργία των επιμέρους συστημάτων IDS με ρυθμίσεις μικρότερης ευαισθησίας άρα και μεγαλύτερη ακρίβεια (Accuracy) - μικρότερη πιθανότητα για εσφαλμένα θετικές αναγνωρίσεις (False Positives). Η μικρότερη παραγωγή αναφορών θα αναπληρωθεί με την επιπλέον διαθέσιμη πληροφορία συνολικά.

[1] Για την εκμετάλλευση αυτού του περιβάλλοντος απαιτείται προσεκτικός σχεδιασμός ενός συστήματος που θα υποστηρίζει μια τέτοια λειτουργία (π.χ. με την αρχιτεκτονική συλλογής πληροφοριών, τη μορφή των δεδομένων, τις μεθοδολογίες χειρισμού τους κ.λπ.), ώστε αυτό να μπορεί να καταλήξει στην παραγωγή χρήσιμων και αξιόπιστων αποτελεσμάτων κατ' αυτόν τον τρόπο.

[2] Δείτε σχετικά την ενότητα 2.3.1 στο κεφάλαιο 2 για πλήρη εξήγηση των όρων

Επιπλέον, ειδικά για την αντιμετώπιση των επιθέσεων DDoS στην παρούσα διατριβή τέθησαν οι στόχοι:

3. Αυτόματη λειτουργία του συνεργατικού σχήματος και υψηλή ταχύτητα αντίδρασης σε περιστατικά (οπωσδήποτε καλύτερη από μη αυτοματοποιημένες λύσεις).

4. Αναγνώριση της διαδρομής της επίθεσης.

Η προσέγγιση ενός κατανεμημένου συστήματος αισθητήρων στην ανίχνευση επιθέσεων θέτει και μια σειρά από απαιτήσεις, οι κυριότερες από τις οποίες είναι:

- Η ομαλή κλιμάκωση του πλήθους των αισθητήρων (δηλαδή ξεχωριστών πηγών πληροφορίας) διατηρώντας και συντονίζοντας τον έλεγχο τους[3].

- Η ρύθμιση των αισθητήρων ώστε να συλλέξουν πληροφορία που να είναι χρήσιμη στην εξαγωγή συμπερασμάτων.

- Το μοντέλο ροής της πληροφορίας και των συμπερασμάτων των τοπικών συστημάτων IDS προς ένα κεντρικό σημείο: ενδιάμεσα επίπεδα που απαιτούνται, βαθμός επεξεργασίας της πληροφορίας, συγκέντρωση (aggregation) και μείωση όγκου κατά τη μεταφορά της πληροφορίας μεταξύ επιπέδων.

- Ο τρόπος χρησιμοποίησης της διαθέσιμης επιπλέον πληροφορίας ώστε να έχει θετική συνεισφορά στο πρόβλημα της πληρότητας ανίχνευσης.

[3] Υπενθυμίζουμε ότι ξεχωριστές πηγές πληροφορίας μπορεί να προκύπτουν από κατάλληλα φιλτραρισμένες μετρήσεις στο ίδιο ή διαφορετικά σημεία του δικτύου.

- Η αποτροπή φαινομένων υπερφόρτωσης του δικτύου από την αποστολή/ανταλλαγή πληροφοριών ανάμεσα στα σημεία συλλογής και συγκέντρωσης τους.

- Το επίπεδο στο οποίο θα γίνεται ο έλεγχος και η ρύθμιση των αισθητήρων και των συστημάτων IDS (τοπικά ή από ένα κεντρικό σημείο).

Στο θέμα της υλοποίησης ενεργειών αντιμετώπισης των επιθέσεων DDoS, οποιαδήποτε λύση ενεργής αντίδρασης μπορεί να είναι αποτελεσματική (ή έστω εφικτή) μόνον εφόσον περιλαμβάνει δίκτυα που βρίσκονται πριν από αυτό του θύματος[4]. Η βοηθητική επέμβαση δικτυακών περιοχών πριν το ίδιο το θύμα μπορεί, μειώνοντας τον τελικό όγκο της κίνησης επίθεσης να μειώσει την επίδρασή της. Στην ιδανική περίπτωση θα ενεργοποιείται η συνεργασία όσο το δυνατόν περισσότερων δικτύων πάνω στο μονοπάτι της επίθεσης. Για να γίνει όμως δυνατή μια τέτοια συνεργασία αντίδρασης τίθενται θέματα τόσο πολιτικά, όπως η ανεξαρτησία δράσης και η συμφωνία με τις εταιρικές πολιτικές σε κάθε δίκτυο, όσο και τεχνικά όπως η διατήρηση της ασφάλειας και το είδος και η ένταση των μέτρων που θα χρησιμοποιηθούν.

Η προτεινόμενη σε αυτή την διατριβή λύση αφορά στη χρησιμοποίηση ενός Υπερκείμενου Δικτύου (Overlay Network) που θα συνδέει διαφορετικές, συνεργαζόμενες δικτυακές περιοχές (domains)[5]. Τα συνεργαζόμενα δίκτυα με τη συμμετοχή τους δημιουργούν την «Υπερκείμενη Συνεργατική Υποδομή»

[4]Βλέπε σχετικά τα συμπεράσματα του τμήματος 2.2

[5]Με τον όρο Δικτυακή Περιοχή (Domain) εννοείται σε αυτή την εργασία ένα δίκτυο το οποίο είναι κάτω από μια κοινή διαχείριση και για το οποίο ισχύουν κοινές πολιτικές ασφαλείας. Για πρακτικούς λόγους θεωρούμε εδώ ότι ταυτίζεται με την έννοια του Αυτόνομου Δικτύου (Autonomous Network – AS) όπως αυτή χρησιμοποιείται στη Διαδικτυακή δρομολόγηση. Οι μονάδες της προτεινόμενης αρχιτεκτονικής είναι Αυτόνομα Δίκτυα. Στη συνέχεια του κειμένου οι όροι «δίκτυο» και «δικτυακή περιοχή» χρησιμοποιούνται εναλλακτικά με την ίδια σημασία.

("Cooperative Overlay Infrastructure")[6]. Μέσω αυτής λαμβάνουν και συνεισφέρουν υπηρεσίες ανίχνευσης (δημιουργείται έτσι ένα κατανεμημένο σύστημα IDS) και αντίδρασης σε επιθέσεις DDoS. Η Υπερκείμενη Υποδομή ορίζει ένα κοινό χώρο ενεργειών εναντίον περιστατικών DDoS.

Οι κύριες κατευθύνσεις σχεδιασμού του Υπερκείμενου Δικτύου (Overlay Network) είναι:

- Διατήρηση της διαχειριστικής ανεξαρτησίας του κάθε επιμέρους δικτύου. Κάθε δίκτυο μπορεί να συνεισφέρει στην Υποδομή χωρίς όμως να χρειαστεί να δώσει οποιαδήποτε διαχειριστικά δικαιώματα σε τρίτους. Επιπλέον οι ενέργειες αντίδρασης σε μια επίθεση DDoS ακολουθούν τοπικές επιλογές και πολιτικές.

- Επικοινωνία «από έναν σε πολλούς» (τύπου Multicast), επιπέδου IP ή επιπέδου εφαρμογής με σκοπό να αποφεύγεται η επιβάρυνση του δικτύου από τις ανταλλαγές μηνυμάτων.

- Υποδομή επικοινωνίας με ασφάλεια και επιβεβαίωση των επικοινωνούντων μερών.

- Ισοτιμία ανάμεσα στα δίκτυα-μέλη της Συνεργατικής Υποδομής, κατά το πρότυπο μεθοδολογιών peer-to-peer. Κάθε μέλος μπορεί να συνδεθεί να απομακρυνθεί ή να αποκοπεί (λόγω επιθετικών ενεργειών) από το Υπερκείμενο Δίκτυο χωρίς να αυτό να χρειαστεί αλλαγή στον τρόπο λειτουργίας του. Κατά τον ίδιο τρόπο παρακάμπτονται τυχόν εμπόδια που τίθενται από τρίτα, μη συνεργαζόμενα δίκτυα.

[6] Στη συνέχεια χρησιμοποιείται ο όρος «Υπερκείμενο Δίκτυο» ή «Συνεργατική Υποδομή».

- Χρήση μεθόδων «ψηφοφορίας με βάρη» (weighted voting) για την εξαγωγή συμπερασμάτων από τις αναφορές που ανταλλάσσονται.

Με τις επιλογές που έχουν γίνει στο σχεδιασμό του Υπερκείμενου Δικτύου επιδιώκεται να αντιμετωπιστούν επίσης τα θέματα που τίθενται από ένα κατανεμημένο σύστημα και αναφέρθηκαν ανωτέρω.

Η Συνεργατική Υποδομή υλοποιείται βάσει των εξής χαρακτηριστικών:

- Η λειτουργία εξασφαλίζεται ανεξάρτητα από τη μέθοδο διασύνδεσης χαμηλού επιπέδου ανάμεσα στα δίκτυα-μέλη. Κάποιες πιθανές μεθοδολογίες διασύνδεσης είναι:
  - Χρήση multicast επιπέδου IP εφόσον λειτουργεί ήδη μεταξύ των δικτύων-μελών
  - Δίκτυα peer-to-peer που υλοποιούν μηχανισμούς multicast επιπέδου εφαρμογής με χρήση ειδικών διαδικασίων εξεύρεσης ομότιμων κόμβων και ανταλλαγής μηνυμάτων
  - Περιβάλλοντα «Πλέγματος» (τύπου Grid) [Fost01] τα οποία παρέχουν μια πλήρη υποδομή ασφαλών επικοινωνιών, υπηρεσιών καταλόγου και ανταλλαγής μηνυμάτων[7].
- Τα μηνύματα εντός του Υπερκείμενου Δικτύου συντάσσονται στη γλώσσα XML σύμφωνα με την υπό ολοκλήρωση προδιαγραφή του IETF, Intrusion Detection Message Exchange Format (IDMEF) [Deba04]. Είναι

[7] Από τις πιο πάνω μεθοδολογίες η χρήση IP multicast και η συνδεσιμότητα peer-to-peer, όπως αναλύεται στη συνέχεια, δοκιμάστηκαν και πειραματικά με θετικά αποτελέσματα ως προς τη δυνατότητα δημιουργίας του Υπερκείμενου Δικτύου, τη σταθερότητα του και την ορθότητα λειτουργίας.

έτσι δυνατή η ανταλλαγή τυποποιημένων στοιχείων με υπάρχοντα ή μελλοντικά συστήματα IDS καθώς και με άλλες εφαρμογές που ακολουθούν το ίδιο πρότυπο.

- Τα δίκτυα-μέλη διατηρούν την ανεξαρτησία τους ως προς το βαθμό συμμετοχής τους αλλά και ως προς τις επιλογές των ενεργειών που θα αναλάβουν. Παρά την από κοινού λειτουργία, κάθε δίκτυο δε χρειάζεται να εκχωρήσει διαχειριστικά του δικαιώματα προκειμένου να γίνει δυνατή η υλοποίηση ενεργειών αντίδρασης.

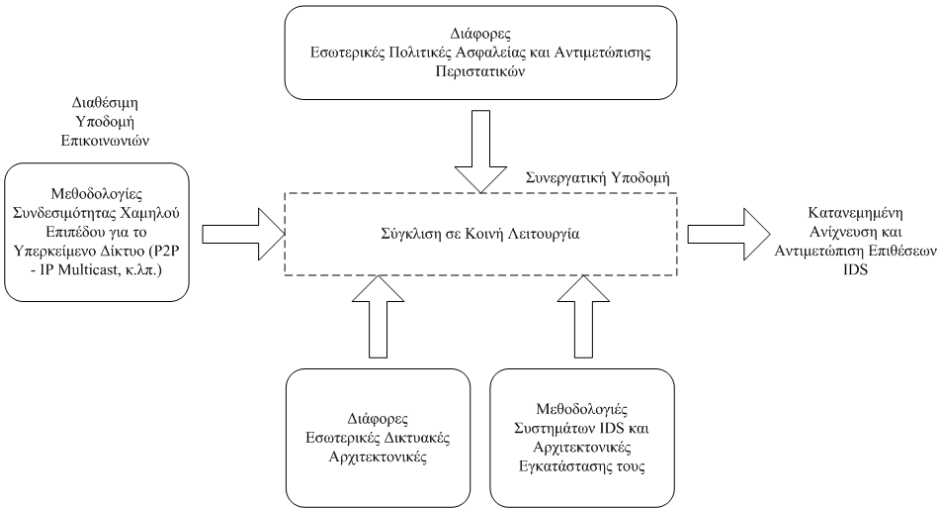
- Η φύση της συμμετοχής αλλά και η μέθοδος τοπικών αποφάσεων κάθε δικτύου-μέλους στο Υπερκείμενο Δίκτυο είναι σε μεγάλο βαθμό παραμετροποιήσιμα μέσω των ρυθμίσεων που μπορεί να γίνουν, π.χ. στην απόδοση διαφορετικών βαρών (βάσει του βαθμού εμπιστοσύνης) στα μηνύματα διαφορετικής προέλευσης, στην ταχύτητα ενεργοποίησης για κάποιο περιστατικό, στην ένταση ενεργειών αντίδρασης κ.λπ.

Η Συνεργατική Υποδομή παρέχει ένα ιδιαίτερα ευέλικτο σχήμα συνεργασίας που επικεντρώνεται στην ανεξαρτησία των δικτύων-μελών. Στο σημείο αυτό διαφοροποιείται σημαντικά από άλλες παρόμοιες προσεγγίσεις που χρησιμοποιούν επίσης κατανεμημένα περιβάλλοντα αντιμετώπισης επιθέσεων (π.χ. τα CITRA, GDI, COSSACK, η μεθοδολογία "Pushback" κ.λπ. που αναφέρθηκαν στην ενότητα 2.3.2[8]).

Συνοψίζοντας, η Συνεργατική Υποδομή σκοπεύει στην συνεργασία παρέχοντας ταυτόχρονα πολλούς βαθμούς ανεξαρτησίας για κάθε δίκτυο. Η τοποθέτηση της Συνεργατικής Υποδομής σε σχέση με τα διάφορα επίπεδα οργάνω-

[8]Πλήρεις συγκρίσεις ανάμεσα στις διαφορετικές λύσεις γίνονται στο κεφάλαιο 6

σης των λειτουργιών του δικτύου ενός οργανισμού παρουσιάζεται στο Σχήμα 3.1.



Σχήμα 3.1: Τοποθέτηση της Συνεργατικής Υποδομής σε σχέση με τα διάφορα επίπεδα οργάνωσης λειτουργιών ενός δικτύου

Το Υπερκείμενο Δίκτυο υλοποιείται με την εγκατάσταση και χρήση ενός ειδικού υπολογιστικού συστήματος σε κάθε ένα από τα συνεργαζόμενα δίκτυα· τη «Συνεργατική Οντότητα κατά των Επιθέσεων DDoS» ("Cooperative Counter-DDoS Entity"). Τα επιμέρους υπολογιστικά αυτά συστήματα θα αναφέρονται ως «Συνεργατικές Οντότητες» ή απλά ως «Οντότητες».

Τα συνεργαζόμενα δίκτυα (δηλαδή δικτυακοί χώροι με κοινή διαχείριση — ουσιαστικά BGP Autonomous Systems) αποτελούν τους «κόμβους» της Συνεργατικής Αρχιτεκτονικής που σχηματίζεται.

Η Συνεργατική Οντότητα αναλαμβάνει τη διασύνδεση των «κοντινών» συνεργαζόμενων δικτύων και την υλοποίηση του Υπερκείμενου Δικτύου χρησιμοποιώντας το εκάστοτε διαθέσιμο δικτυακό υπόβαθρο και προσαρμόζοντας

τις λειτουργίες της στις ιδιαιτερότητες του. Με τον τρόπο αυτό η προτεινόμενη αρχιτεκτονική μπορεί να κάνει χρήση διαφορετικών μεθοδολογιών σε κάθε περίπτωση και να εκμεταλλευτεί τυχόν ειδικά χαρακτηριστικά (ανάλογα με το πλήθος δικτύων, την τοπολογία, τις απαιτήσεις ασφαλείας κ.λπ.). Η κάθε Συνεργατική Οντότητα, υπό τον έλεγχο του δικτύου στο οποίο έχει εγκατασταθεί, εξάγει συμπεράσματα με βάση τοπικά και απομακρυσμένης προέλευσης στοιχεία, ενώ αναλαμβάνει τοπικές ενέργειες αντίδρασης.

Η αποδοτικότητα της προτεινόμενης λύσης για χρήση ενάντια σε επιθέσεις DDoS αποτιμάται από:

- Την ικανότητα ανίχνευσης της επίθεσης με τη χρήση της κατανεμημένης προσέγγισης, τόσο σε επιμέρους δίκτυα όσο και συνολικά στο μονοπάτι που αυτή διατρέχει (detection).

- Τη χρησιμότητα που μπορεί να έχει το χρησιμοποιούμενο σχήμα στην ανάσχεση των επιθέσεων (reaction).

Η αποδοτικότητα εξαρτάται επίσης από τον αριθμό των δικτύων-μελών της Υποδομής και την «κατάλληλη» τοποθέτηση τους ως προς τη διαδρομή της επίθεσης.

Στο ζήτημα της ανίχνευσης η κύρια συνεισφορά της αρχιτεκτονικής είναι μια νέα μεθοδολογία αναγνώρισης του μονοπατιού της επίθεσης (traceback) χωρίς πολύπλοκες διαδικασίες και ειδικές υλοποιήσεις όπως αυτές που αναφέρθηκαν στην ενότητα 2.3 (π.χ. σήμανση πακέτων, αποστολή πακέτων itrace κ.λπ.) Παράλληλα, κάθε ένα από τα δίκτυα-μέλη μπορεί να επιτύχει καλύτερα τοπικά αποτελέσματα ανίχνευσης εμπιστευόμενο και χρησιμοποιώντας τα συμπεράσματα των άλλων δικτύων της Υποδομής.

Στον τομέα της αντίδρασης μια μικρή κοινότητα δικτύων-μελών μπορεί να

έχει ουσιαστική συνεισφορά εφόσον αυτά είναι πάνω στη διαδρομή της επίθεσης και δρουν συντονισμένα. Τα μεγαλύτερα οφέλη από τη λειτουργία της αρχιτεκτονικής αναμένονται με την κλιμάκωση της συμμετοχής σε αυτή μέσα από το συνδυασμό στοιχείων ανίχνευσης από πολλές διαθέσιμες πηγές και τη συντονισμένη, κατανεμημένη αντίδραση στην επίθεση.

3.2 Φιλοσοφία της «Κοινότητας» Συνεργαζόμενων Δικτύων

Η «εγγραφή» δικτύων σε μια συμφωνία συνεργασίας καθώς και η ανταλλαγή πληροφοριών μεταξύ τους ακολουθεί το πρότυπο συνεργασίας των Ομάδων Αντιμετώπισης Περιστατικών ασφαλείας (CERTs). Κάθε ομάδα CERT έχει μια συγκεκριμένη περιοχή ευθύνης ("constituency")[9] και συνεργάζεται με άλλες αντίστοιχες ομάδες που θεωρεί έμπιστες. Υπάρχουν σχήματα συνεργασίας όπου η διαδικασία αυτή εδραιώνεται μέσα από διαδικασίες πιστοποίησης[10] και συμφωνίες. Κατά παρόμοιο τρόπο, στην προτεινόμενη λύση η «κοινότητα» των συνεργαζόμενων δικτύων οργανώνεται μέσα από συμφωνίες μεταξύ των ενδιαφερόμενων μερών. Ήδη, στο σημερινό σκηνικό της ασφάλειας, πολλά δίκτυα ανταλλάσσουν πληροφορίες και τεχνικές για θέματα ασφαλείας, ειδικά δε κατά τη διάρκεια σοβαρών περιστατικών καταλήγουν σε συνεργασίες *ad hoc*[11]. Το

[9] Σε πολλές περιπτώσεις ταυτίζεται με μια δικτυακή περιοχή.

[10] Είναι χαρακτηριστική η Ευρωπαϊκή πρωτοβουλία δημιουργίας ενός έμπιστου δικτύου συνεργασίας ανάμεσα σε (κυρίως ακαδημαϊκές) ομάδες CERT με τον τίτλο «Υποστήριξη από Έμπιστο Μέλος» ("Trusted Introducer") [Ti].

[11] Στην πράξη πολλά δίκτυα συνεργάζονται με αυτό τον τρόπο αλλά μόνο τη στιγμή που εκδηλώνεται η επίθεση με αποτέλεσμα να χάνεται πολύτιμος χρόνος και να υπάρχουν προβλήματα αποτελεσματικότητας. Πρέπει δε η συνεργασία αυτή να ενταχθεί στην ισχύουσα εμπορική σχέση μεταξύ των δύο μερών.

προτεινόμενο Υπερκείμενο Δίκτυο επιδιώκει να οργανώσει εκ των προτέρων και να θέσει σε συγκεκριμένα πλαίσια αυτές τις συνεργασίες.

Ο σχεδιασμός για το προτεινόμενο Υπερκείμενο Δίκτυο χρησιμοποιεί ένα σχετικά μικρό αριθμό δικτύων, και επικεντρώνεται σε μικρές ομάδες, κοινών αναγκών και επιδιώξεων. Έτσι δεν απαιτεί συμφωνίες μεταξύ πολλών μερών και την έγκριση των αρχών διοίκησης — governance (ICANN) και προτυποποίησης του Διαδικτύου (IETF), κάτι που ισχύει σε άλλες μεγαλύτερης κλίμακας προσεγγίσεις, όπως αυτή της «Παγκόσμιας Υποδομής Άμυνας» (Global Defense Infrastructure - GDI) [Wan02][12]. Πολύ μεγάλος αριθμός συμμετεχόντων και ειδικά από διαφορετικές γεωγραφικά περιοχές, άρα και με αρκετά διαφορετικά συμφέροντα, θα δυσκολεύει σε μεγάλο βαθμό την επίτευξη μιας συμφωνίας.

Εντούτοις τίθεται το ερώτημα του κατά πόσον τα διάφορα μέρη θα δεχτούν να συμμετάσχουν σε ένα συνεργατικό σχήμα όπου θα χρειαστεί να αφιερώσουν πόρους (άψυχους και έμψυχους) και να συνεισφέρουν πληροφορίες. Εμπορικά δίκτυα παρόχων πιθανά να μην έχουν άμεσες απώλειες από μια επίθεση DDoS ενώ αντιθέτως τέτοιου είδους κίνηση μπορεί να επιφέρει κέρδη εφόσον υπάρχει ένα σχήμα χρέωσης βασισμένο στον όγκο (κατάσταση απ' την οποία ο πάροχος κερδίζει σε κάθε περίπτωση, win-win case). Ορισμένοι συγγραφείς υποστηρίζουν [Mirk04] ότι το πρόβλημα είναι παρόμοιας μορφής με αυτό της νομοθετικής ρύθμισης της χρήσης κοινά διαθέσιμων πόρων (όπως προτείνεται στο [Hard68]) και ότι απαιτείται ένα γενικό νομοθετικό ρυθμιστικό πλαίσιο πριν διευρυνθεί η αποδοχή οποιασδήποτε κατανεμημένης λύσης.

Διαφαίνεται καθαρά ότι οι εμπλεκόμενοι φορείς - υπεύθυνοι δικτύων έχουν

[12] Σε αυτή προτείνεται η τοποθέτηση σε κύρια δίκτυα κορμού του Διαδικτύου μηχανισμών ανάλυσης της κίνησης και ανάσχεσης επιθέσεων DDoS. Παρουσιάζεται στην ενότητα 2.3

τα κίνητρα να συνεργαστούν λόγω της συνεχούς αύξησης του ενδιαφέροντος και της ευαισθητοποίησης για θέματα ασφάλειας (security awareness) αλλά και για το κοινό όφελος. Για παράδειγμα, μακροπρόθεσμα, ένας πάροχος θα ωφεληθεί περισσότερο από την προστασία και διατήρηση της ομαλής λειτουργίας ενός δικτύου-πελάτη παρά από τη χρέωση της κίνησης η οποία θα τον θέσει εκτός αγοράς. Επιπλέον, υπηρεσίες προστασίας από επιθέσεις DDoS ήδη εισάγονται σε συμφωνίες Παροχής Υπηρεσίας Συγκεκριμένου Επιπέδου (Service Level Agreements - SLAs) [Info04], μια ένδειξη ότι μπορεί να υπάρξουν και οι κατάλληλες συμφωνίες με οικονομικό αντικείμενο για τέτοιες συνεργασίες.

Ως πρότυπο παρόμοιας φύσης θεωρούνται εδώ υφιστάμενες συμφωνίες διασύνδεσης και ανταλλαγής κίνησης (peering agreements) μεταξύ δικτύων. Το γεγονός ότι αυτές οι συμφωνίες υφίσταται και λειτουργούν αποτελεσματικά[13] δίνει μια ένδειξη για το εφικτό της συνεργασίας. Κατά εντελώς αντίστοιχο τρόπο το προτεινόμενο Υπερκείμενο Δίκτυο παρέχει τα εργαλεία για την υιοθέτηση συγκεκριμένων πολιτικών στις ανταλλαγές μεταξύ δικτύων ακολουθώντας τις εταιρικές απαιτήσεις. Γίνεται η υπόθεση ότι το μοντέλο συνεργασίας για θέματα ασφαλείας είναι απλούστερο από ότι για θέματα ανταλλαγής κίνησης άρα και οι συμφωνίες ευκολότερες[14]. Εν τέλει το κατάλληλο οικονομικό μοντέλο ή οι ενδεχόμενες νομοθετικές ρυθμίσεις χρειάζεται να εξεταστούν εις βάθος και αποτελούν αντικείμενο μελλοντικής μελέτης πέραν της παρούσας εργασίας. Η προτεινόμενη λύση παρέχει ένα τεχνικό υπόβαθρο, επαρκώς ευέλικτο ώστε να προσαρμοστεί σε ειδικές ανάγκες που θα προκύψουν με την εξέταση του

[13] Ακόμα και αν μεσολαβούν συναλλαγές οικονομικής ή τεχνικής φύσης για να γίνουν αποδεκτές.

[14] Αντιμετωπίζεται ένα πρόβλημα που μπορεί να έχει δυνάμει αρνητικές επιπτώσεις (άμεσες ή έμμεσες) για όλους.

προβλήματος από αυτή την σκοπιά.

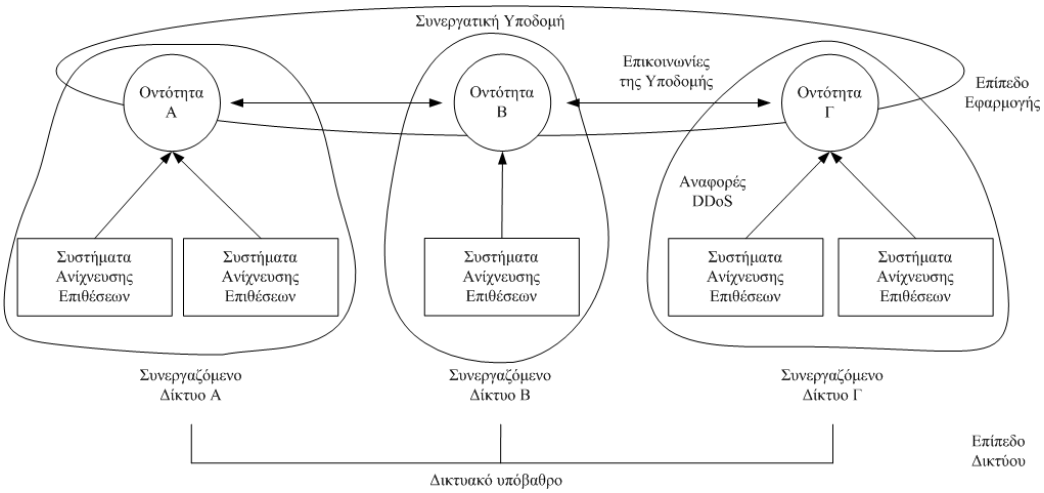
Στην όλη προσπάθεια προσέγγισης και επίτευξης συμφωνίας ανάμεσα στα δίκτυα που θα αποτελέσουν τη Συνεργατική Υποδομή, υπάρχουσες συνεργασίες μεταξύ των ομάδων CERT μπορούν να παίξουν υποστηρικτικό ρόλο, τόσο με την εδραίωση της εμπιστοσύνης όσο και σε πρακτικά θέματα, όπως π.χ. οι ανταλλαγές κλειδιών κρυπτογραφίας, η διευθέτηση διαφωνιών κ.λπ.

Η διερεύνηση του ρυθμιστικού πλαισίου για την υιοθέτηση μιας κοινά αποδεκτής πολιτικής ασφαλείας δεν αποτελεί αντικείμενο της διατριβής αυτής που επικεντρώνεται σε ζητήματα σχεδιασμού και υλοποιησης μιας συνεργατικής υποδομής ανίχνευσης και αντιμετώπισης επιθέσεων σε δίκτυα πολλαπλών Αυτόνομων Συστημάτων (Autonomous Systems) – διαχειριστικών περιοχών.

3.3 Περιγραφή της Αρχιτεκτονικής

3.3.1 Τα Συνεργαζόμενα Δίκτυα

Βασική μονάδα της Συνεργατικής Αρχιτεκτονικής είναι η δικτυακή περιοχή (domain). Μια ενδεικτική εικόνα της εγκατάστασης του Υπερκείμενου Δικτύου και της σύνδεσης των τμημάτων του σε σχέση με τα διάφορα επίπεδα δικτυακής διασύνδεσης δίνεται στο Σχήμα 3.2.



Σχήμα 3.2: Υλοποίηση της Συνεργατικής Υπερκείμενης Υποδομής πάνω από το υπάρχον δικτυακό υπόβαθρο

Κάθε δίκτυο εντάσσεται στο Υπερκείμενο Δίκτυο με την εγκατάσταση και ενεργοποίηση της Συνεργατικής Οντότητας σε αυτό. Το δικτυακό υπόβαθρο (οι διασυνδέσεις του δικτύου με άλλους κόμβους) χρησιμοποιείται είτε άμεσα (π.χ. με τη χρήση διαθέσιμων επικοινωνιών multicast) είτε έμμεσα (π.χ. με τη χρήση συνδέσεων unicast για την υλοποίηση υπηρεσιών multicast επιπέδου εφαρμογής) για την υλοποίηση της διασύνδεσης υψηλού επιπέδου. Η λειτουργικότητα του Συνεργατικού Δικτύου ως προς τα είδη των μηνυμάτων που ανταλλάσσονται και τους αλγορίθμους λειτουργίας που χρησιμοποιούνται τροποποιείται ελαφρά ανάλογα με το είδος επικοινωνίας χαμηλού επιπέδου που θα επιλεγεί.

Το Υπερκείμενο Δίκτυο που δημιουργείται είναι επίπεδο στη διάρθρωση του με όλους τους κόμβους – δίκτυα (AS) ισότιμους μεταξύ τους. Δεν παίζει ρόλο η φυσική τοπολογία ούτε η ιεραρχική θέση ενός κόμβου – δικτύου π.χ. πάρο-

χος δικτυακών υπηρεσιών σε τελικούς χρήστες (Tier 3 ISP), διεθνές δίκτυο διασύνδεσης (Tier 1 ISP) κ.λπ.

Για να γίνει εφικτή η συνεργασία απαιτείται για κάποια ζητήματα λειτουργίας η συμφωνία σε κοινά αποδεκτές ρυθμίσεις. Τα κυριότερα από αυτά είναι:

- *Συμφωνία τρόπου διασύνδεσης.* Τα δίκτυα πρέπει να συμφωνήσουν σε κοινή μέθοδο επικοινωνίας στο χαμηλό επίπεδο, προκειμένου να είναι δυνατή η επικοινωνία μεταξύ τους αλλά και να ρυθμιστούν αντιστοίχως οι Οντότητες. Η επιλογή μεθόδου μπορεί να γίνει σύμφωνα με την εκάστοτε διαθεσιμότητα της υποδομής χαμηλού επιπέδου ή ανάλογα με τις απαιτήσεις που δημιουργούνται από το πλήθος των συνεργαζόμενων δικτύων και την ανάγκη για περαιτέρω διάδοση των μηνυμάτων τους (πέρα από την τοπική ομάδα).

- *Πλήρης ανταλλαγή στοιχείων.* Βασική αρχή στην οποία στηρίζεται η λειτουργία του Υπερκείμενου Δικτύου (με τον τρέχοντα σχεδιασμό) είναι ότι όλα τα δίκτυα-μέλη λαμβάνουν όλα τα μηνύματα. Η μέθοδος μετάδοσης των μηνυμάτων είναι «από έναν σε πολλούς», σύμφωνα με τη μέθοδο multicasting. Έτσι, προκειμένου τα μηνύματα να φτάσουν σε όλα τα μέλη της Συνεργατικής Υποδομής θα πρέπει να υπάρχει η δέσμευση για την αναμετάδοση των μηνυμάτων από κάθε δίκτυο ακόμα και αν δε χρησιμοποιηθούν στο ίδιο.

- *Παράκαμψη μη συνεργαζόμενων δικτύων.* Είναι λογικό να υποθέσουμε την πιθανότητα κάποια δίκτυα σε μια περιοχή να επιλέξουν να μη συμμετάσχουν στη συνεργασία. Σε αυτή την περίπτωση τα μέλη του Υπερκείμενου Δικτύου θα πρέπει να επιλέξουν τη λειτουργία του κατά τρόπο

ώστε να παρακαμφθούν τα «ουδέτερα» τμήματα. Μία τέτοια μέθοδος, για παράδειγμα, είναι η λειτουργία σηράγγων (tunnels) διαμέσου αυτών των περιοχών. Η λύση αυτή είναι ιδιαίτερα δημοφιλής σε δίκτυα IP Multicast αλλά θα πρέπει να εξασφαλιστεί ότι υλοποιείται με τον ίδιο τρόπο στα δύο άκρα που επιθυμούν να επικοινωνήσουν. Με τη διαδικασία αυτή η μη συμμετέχουσα περιοχή καθίσταται «διαφανής» για το Υπερκείμενο Δίκτυο.

- *Κοινή κατανόηση των επιθέσεων.* Τα δίκτυα θα πρέπει να έχουν προσδιορίσει τα χαρακτηριστικά βάσει των οποίων διακρίνονται οι επιθέσεις μεταξύ τους, ώστε να έχουν κοινή πολιτική ανίχνευσης τους. Πέραν των τεχνικών λεπτομερειών[15], που αναμένονται κοινές σε όλες τις περιπτώσεις, σημαντική παράμετρος είναι το χρονικό όριο βάσει του οποίου διαχωρίζονται ως διαφορετικές επιθέσεις οι εμφανίσεις ενός περιστατικού με τα ίδια χαρακτηριστικά. Επισημαίνεται ότι ο προσδιορισμός ενός τέτοιου ορίου είναι διαφορετικός από την ταχύτητα και τη διάρκεια ενεργοποίησης ενός δικτύου σε ένα περιστατικό. Οι τελευταίες αυτές παράμετροι παραμένουν στην ευχέρεια καθενός επιμέρους δικτύου.

- *Τυποποιημένη μέθοδος ανταλλαγής μηνυμάτων.* Θα πρέπει να επιλεγεί μια κοινή διαδικασία ανταλλαγής μηνυμάτων με ασφάλεια καθώς και τα κοινά σημασιολογικά στοιχεία τους (semantics). Στην παρούσα εργασία επιλέχθηκε η σύνταξη των μηνυμάτων σε XML κατά το πρότυπο υπό διαμόρφωση (work in progress) IDMEF.

[15] Π.χ. Διεύθυνση τελικού στόχου, πρωτόκολλο, θύρα επικοινωνίας. Δείτε σχετικά τους τρόπους κατηγοριοποίησης των επιθέσεων [16] που παρουσιάστηκαν στην Ενότητα 2.2.2.

- *Βασική συμφωνία για την αντιμετώπιση των περιστατικών.* Θα πρέπει να υπάρχει από κοινού συμφωνία για την ανάγκη ανάληψης ενεργειών στις περιπτώσεις περιστατικών. Πέρα από αυτή τη βασική αρχή το είδος και η ένταση των ενεργειών αντιμετώπισης μιας επίθεσης αποτελούν πρωτοβουλία των επιμέρους δικτύων. Ας σημειωθεί ότι μπορούν να συνάπτονται επιμέρους συμφωνίες μεταξύ των δικτύων, π.χ. συμφωνίες παροχής υπηρεσίας συγκεκριμένου επιπέδου (SLAs) κ.λπ.

Το τελευταίο στοιχείο αναμένεται να παρέχει επίσης ένα πλαίσιο επιχειρηματικής συνεργασίας δικτύων-πελατών με τα δίκτυα κορμού στις περιπτώσεις επιθέσεων DDoS προς τα πρώτα.

Η πλήρης ανεξαρτησία των δικτύων εντούτοις διατηρείται για ένα μεγάλο πλήθος άλλων ζητημάτων που αφορούν κυρίως:

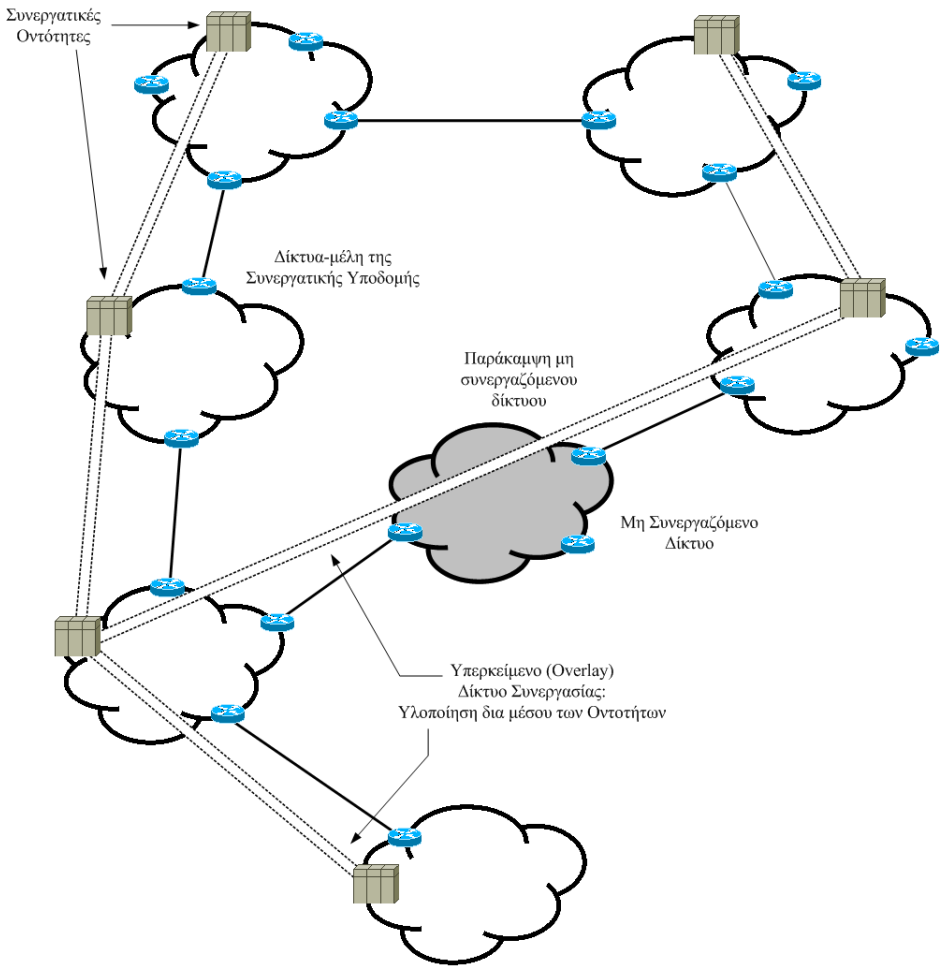
- *Ενέργειες αντιμετώπισης περιστατικών.* Πιο συγκεκριμένα:
  - Το χρόνο (την ταχύτητα) εφαρμογής μέτρων
  - Την ένταση των μέτρων. Το θέμα αυτό μπορεί να αφορά τόσο στη διάρκεια εφαρμογής τους όσο και στην ένταση τους, εφόσον αναφέρονται σε διαδικασίες ελέγχου της κακόβουλης κίνησης (ποσοστό ρύθμισης της).
  - Τα σημεία εφαρμογής των μέτρων. Αν και μια λογική επιλογή είναι να επιβληθούν οποιεσδήποτε ρυθμίσεις στα σημεία εισόδου της κίνησης στο δίκτυο, ώστε αυτή να μην επιβαρύνει τον υπόλοιπο κορμό του, υπάρχει η δυνατότητα για εναλλακτικές επιλογές, π.χ. κάποιο κεντρικό σημείο όπου ο διαχειριστής θα διατηρεί όλες τις ρυθμίσεις αντιμετώπισης περιστατικών κ.λπ.

- *Επίπεδα σημασίας και εμπιστοσύνης για τα εισερχόμενα μηνύματα.* Αν και το Υπερκείμενο Δίκτυο προσφέρει ένα βασικό επίπεδο ασφάλειας και αξιοπιστίας των συμμετεχόντων κάποια από τα μέρη είναι δυνατόν να αποφασίσουν τον επιλεκτικό χειρισμό των εισερχόμενων μηνυμάτων. Κάτι τέτοιο μπορεί να οφείλεται στην αβεβαιότητα για την ακρίβεια των συστημάτων IDS ενός δικτύου-μέλους ή την εμπιστοσύνη για το επίπεδο ασφαλείας που επικρατεί σε αυτό (π.χ. ένας εμπορικός πάροχος μπορεί να μη συμφωνεί με τις πολιτικές ασφαλείας ενός ακαδημαϊκού δικτύου). Ο επιλεκτικός χειρισμός μπορεί να αφορά στην τοποθέτηση ενός «παράγοντα αξιοπιστίας» στα εισερχόμενα μηνύματα από συγκεκριμένα δίκτυα-πηγές.

- *Αυτονομία στην επιλογή τοπικών συστημάτων IDS.* Υπάρχει μεγάλο εύρος διαφορετικών επιλογών που έχουν καλυφθεί ήδη στην ενότητα 2.3.1.

- *Επιλογή παραμέτρων λειτουργίας των Οντοτήτων.* Το συγκεκριμένο ζήτημα αφορά στην ελεύθερη επιλογή του κάθε δικτύου για τη συμπεριφορά της τοπικής Συνεργατικής Οντότητας.

Το Σχήμα 3.3 παρουσιάζει μια ενδεικτική υλοποίηση του Υπερκείμενου Δικτύου σε ένα δικτυακό περιβάλλον όπου ορισμένα δίκτυα έχουν επιλέξει να μη συμμετάσχουν στη συνεργασία.



Σχήμα 3.3: Ενδεικτική εγκατάσταση της Συνεργατικής Υπερκείμενης Υποδομής σε μια ομάδα δικτύων

Βασική λειτουργία της Συνεργατικής Υπερκείμενης Υποδομής

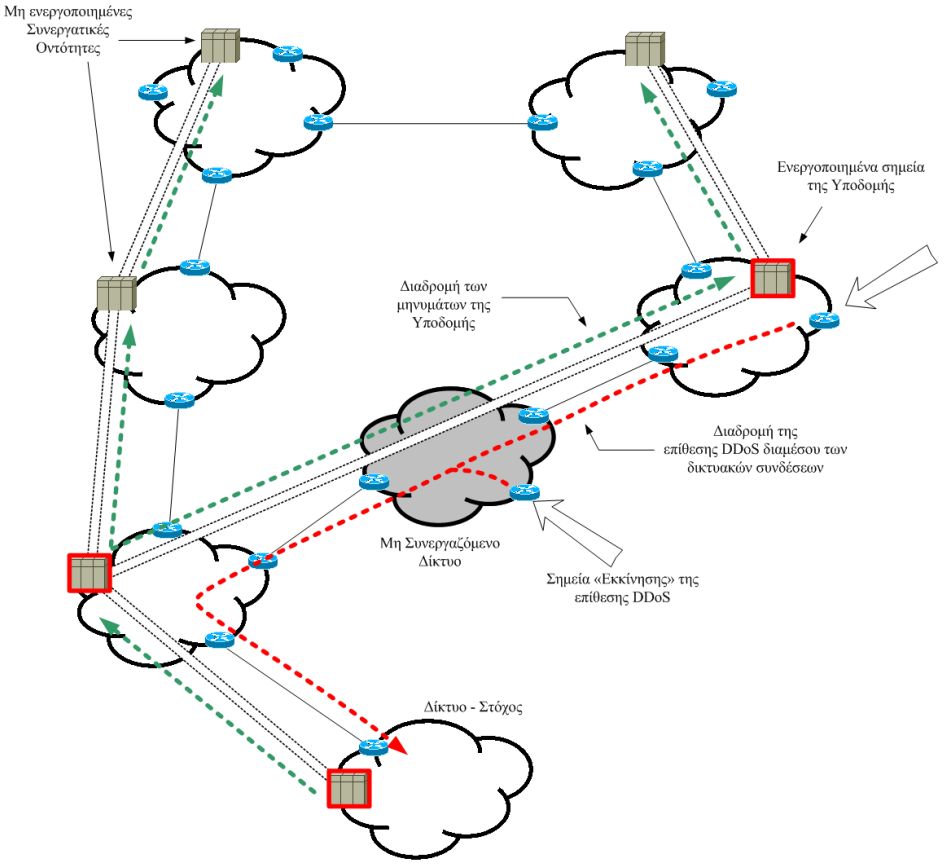
Κατά τη διάρκεια μιας επίθεσης DDoS η ανίχνευση της μπορεί να γίνει σε κάποια από τα δίκτυα του Υπερκείμενου Δικτύου που βρίσκονται πάνω στη διαδρομή της κίνησης. Η ανίχνευση θα εξαρτηθεί από τις μεθόδους που θα χρησιμοποιηθούν και την ευαισθησία των συστημάτων IDS. Εντούτοις, αν η επίθεση δεν ανιχνευτεί νωρίτερα, το τελικό θύμα θα αντιμετωπίσει άμεση υποβάθμιση κάποιων υπηρεσιών λόγω υπερβολικής χρησιμοποίησης των πόρων. Το γεγονός αυτό θα έχει σαν αποτέλεσμα την εκπομπή ενός μηνύματος Προειδοποίησης (Alert) από την τοπική Συνεργατική Οντότητα ή, σε περίπτωση πλήρους διακοπής της συνδεσιμότητας, μια σχετική ένδειξη για το υπόλοιπο Υπερκείμενο Δίκτυο.

Κάθε ένα από τα δίκτυα που θα λάβει Alert θα το συνδυάσει[17] με στοιχεία από τα τοπικά συστήματα IDS για να διαπιστώσει κατά πόσον η ροή της κακόβουλης κίνησης διέρχεται μέσα από αυτό. Ο συνδυασμός των Alerts, των (πιθανών) ενδείξεων διακοπής κάποιων σημείων της υποδομής καθώς και των τοπικών αναφορών θα ενεργοποιήσουν σε κάποιο βαθμό τη Συνεργατική Οντότητα η οποία διαδοχικά θα περάσει στις καταστάσεις «*Πιθανής Ύπαρξης Περιστατικού*» (Suspicion State) και «*Ενεργοποίησης*» (Alert State). Οι καταστάσεις αυτές απεικονίζουν το βαθμό ενεργοποίησης ενός δικτύου για ένα περιστατικό σύμφωνα με τις επιλογές του διαχειριστή του. Όσο πιο κοντά είναι ένα από τα δίκτυα του Υπερκείμενου Δικτύου στο τελικό θύμα (εφόσον βρίσκεται στο μονοπάτι της επίθεσης) τόσο πιο έντονες θα είναι οι ανωμαλίες που θα ανιχνευτούν από τα συστήματα IDS τα οποία και θα παράγουν περισ-

[17] Τη λειτουργία αυτή την αναλαμβάνει η Οντότητα.

σότερες αναφορές. Κατά συνέπεια, οι Οντότητες του Υπερκείμενου Δικτύου θα περνούν στην κατάσταση *Ενεργοποίησης* με μεγαλύτερη πιθανότητα όσο προσεγγίζουμε το δίκτυο-θύμα. Το ίδιο γεγονός εξασφαλίζει ότι τα μέτρα αντιμετώπισης θα ληφθούν κυρίως στη διαδρομή της επίθεσης όπου τα μηνύματα ανίχνευσης θα είναι πιο επίμονα. Το τελικό βήμα είναι η αυτόματη ενεργοποίηση διαδικασιών φιλτραρίσματος της κακόβουλης κίνησης, στα κατάλληλα σημεία σε κάθε ένα δίκτυο, ώστε να μειωθούν τα αποτελέσματα της επίθεσης.

Το Σχήμα 3.4 δίνει μια αναπαράσταση της λειτουργίας του Υπερκείμενου Δικτύου που μόλις περιγράφηκε



Σχήμα 3.4: Ενδεικτική ενεργοποίηση της Συνεργατικής Υπερκείμενης Υποδομής κατά τη διάρκεια μιας επίθεσης

3.3.2 Οι Συνεργατικές Οντότητες

Σε κάθε συνεργαζόμενο δίκτυο εγκαθίσταται ένα σύστημα με λογισμικό που υλοποιεί την τοπική του Συνεργατική Οντότητα. Αυτή αναλαμβάνει τις επικοινωνίες και υλοποιεί το Υπερκείμενο Δίκτυο. Πρόκειται για μια «αρθρωτή» (modular) πλατφόρμα λογισμικού που συγκεντρώνει τις σχετικές λειτουργίες. Όλες οι Οντότητες είναι ισότιμες μεταξύ τους. Αλληλεπιδρούν κατά τρόπο που να μην έχει επίδραση στην ασφάλεια τους και χωρίς να θέτουν σε επιπλέον

κινδύνους τα δίκτυα που είναι εγκατεστημένες. Η κύρια λειτουργικότητα των Οντοτήτων αφορά στη διεκπεραίωση των επικοινωνιών του Υπερκείμενου Δικτύου[18]. Οι επικοινωνίες αυτές διεξάγονται με ασφάλεια από υποκλοπές και επιβεβαίωση της ταυτότητας των επικοινωνούντων μερών. Τα μηνύματα που ανταλλάσσονται είναι διατυπωμένα σε XML, όπως προαναφέρθηκε, σύμφωνα με το πρότυπο IDMEF. Το πρότυπο αυτό ορίζει μηνύματα δύο ειδών: Μηνύματα Κανονικής Λειτουργίας (Heartbeats) και Μηνύματα Προειδοποίησης (Alerts). Τα Heartbeats είναι περιοδικά εκπεμπόμενες ενημερώσεις ότι κάποια Συνεργατική Οντότητα είναι σε λειτουργία και σε σύνδεση με το Υπερκείμενο Δίκτυο. Χρησιμοποιούνται κατά περίπτωση, ανάλογα με το δίκτυο βασικής συνδεσιμότητας που χρησιμοποιείται, π.χ. στα δίκτυα IP Multicast επιβεβαιώνουν τη λειτουργία του δικτύου διασύνδεσης υποβάθρου, ενώ με τη χρήση δικτύων peer-to-peer) οι διατιθέμενες λειτουργίες υλοποίησης τα καθιστούν μη αναγκαία. Τα Alerts αποστέλλονται όταν διαγνωστεί κάποιο περιστατικό από τη Συνεργατική Οντότητα. Χρησιμοποιώντας τη δυνατότητα που δίνει το πρότυπο IDMEF η βασική περιγραφή των μηνυμάτων σε XML (Document Type Definition - DTD) επεκτάθηκε ώστε να καλύψει όλες τις επιπλέον ανάγκες λειτουργίας του Υπερκείμενου Δικτύου. Παραδείγματα συγκεκριμένων μηνυμάτων δίνονται στο Κεφάλαιο 4.

Σε τοπικό επίπεδο, σε κάθε ένα από τα δίκτυα της συνεργασίας, η Συνεργατική Οντότητα βρίσκεται στην κορυφή της (πιθανά υπάρχουσας) ιεραρχίας συστημάτων IDS τα οποία την τροφοδοτούν με τις αναφορές τους[19]. Οι υπηρε-

[18] Ακόμα και αν το προτεινόμενο δίκτυο δε χρησιμοποιηθεί στο τμήμα του που αφορά στην ενεργή αντίδραση σε επιθέσεις παραμένει χρήσιμο ως εξειδικευμένο μέσο μεταφοράς μηνυμάτων που αφορούν την ασφάλεια.

[19] Δηλαδή, οι κορυφές των ιεραρχιών των επιμέρους δικτύων δημιουργούν, όπως αναφέρθηκε μια επίπεδη, μη ιεραρχική αρχιτεκτονική πάνω στο Υπερκείμενο Δίκτυο.

σίες ανίχνευσης που παρέχονται από τα συστήματα IDS γίνονται έτσι διαθέσιμες στα υπόλοιπα μέλη της κοινότητας. Η Οντότητα αποτελεί το σημείο συγκέντρωσης και ανάλυσης των αναφορών ασφαλείας τοπικής (από συστήματα IDS) και εξωτερικής προέλευσης.

Οι διάφορες αναφορές ανάλογα με την προέλευση τους και την εμπιστοσύνη που έχει ο διαχειριστής προς την αντίστοιχη πηγή αποκτούν εισερχόμενα βάρη και συνεισφέρουν σε διαφορετικό βαθμό στην τελική διαπίστωση ενός περιστατικού. Τα μηνύματα μπορεί να διαθέτουν επίσης και ένα βαθμό βεβαιότητας προερχόμενο από τον αποστολέα τους. Για ένα συγκεκριμένο περιστατικό η Οντότητα περνά διαδοχικά σε κατάσταση «Υποψίας» ή «Πιθανής Ύπαρξης Περιστατικού» (Suspicion State) και στη συνέχεια κατάσταση «Ενεργοποίησης» (Alert State) βάσει του πλήθους των μηνυμάτων, της σοβαρότητας τους και της αξιοπιστίας του αποστολέα. Η μετάβαση ανάμεσα στις καταστάσεις επιτελείται εφόσον η «συσσώρευση» (accumulation) βεβαιότητας από τα διάφορα μηνύματα, για τη διαπίστωση ενός περιστατικού, ξεπεράσει την τιμή κάποιων ορίων (thresholds) εντός σύντομου χρονικού διαστήματος. Οι τιμές αυτών των ορίων ορίζονται από το διαχειριστή της Οντότητας τοπικά. Κατ' αυτόν τον τρόπο η Οντότητα υλοποιεί τη μέθοδο ψηφοφορίας «βασισμένη σε βάρη» (weighted voting) στην οποία όμως συνυπάρχει και η χρονική παράμετρος.

Βασιζόμενο στην Οντότητα, που παίζει το ρόλο «αντιπρόσωπου» (proxy) της Συνεργατικής Υποδομής, κάθε δίκτυο-μέλος μπορεί να συμμετέχει σε αυτή χωρίς να χρειάζεται να εκχωρηθούν εσωτερικά διαχειριστικά δικαιώματα. Σε τοπικό επίπεδο, κάθε Συνεργατική Οντότητα ελέγχεται από πολιτικές λειτουργίας και αντίδρασης. Παραδείγματα τέτοιων ρυθμίσεων είναι:

- Η παράμετρος εμπιστοσύνης που αποδίδεται στα μηνύματα κάθε συνερ-

γαζόμενου δικτύου.

- Ένας μετρητής χρόνου που αρχίζει να μετράει αντίστροφα από μια αρχική τιμή μετά από κάθε λήψη μηνύματος σχετικού με κάποιο παρακολουθούμενο περιστατικό και ανανεώνει την τιμή του με κάθε νέο μήνυμα. Ο χρόνος αυτός αντιστοιχεί στην διάρκεια «διέγερσης» της Οντότητας από ένα μοναδικό μήνυμα.

- Τα «κατώφλια βεβαιότητας» (certainty thresholds) υπέρβαση των οποίων από τη συσσώρευση μηνυμάτων για κάποιο περιστατικό προκαλεί μετάβαση της Οντότητας στην επόμενη κατάσταση ενεργοποίησης.

Εντούτοις, οι παράμετροι αυτοί, όπως και η λειτουργία των συστημάτων IDS που παρέχουν τη βασική είσοδο στοιχείων στο σύστημα μπορεί να επιλεγούν (μετά από συμφωνία) να είναι κοινά για όλα τα δίκτυα της Υποδομής.

Μετά το πέρασμα σε κατάσταση «Ενεργοποίησης» η Οντότητα θα επιδιώξει να αναγνωρίσει την τοποθέτηση του δικτύου στο οποίο είναι εγκατεστημένη ως προς το μονοπάτι της επίθεσης (πιθανή πηγή, δίκτυο διέλευσης, στόχος της επίθεσης ή μη σχετιζόμενη) βοηθούμενη από τα μηνύματα που έχει λάβει από το Υπερκείμενο Δίκτυο, χωρίς έτσι να χρειαστεί να εκτελέσει πολύπλοκες διαδικασίες παρακολούθησης και ανακάλυψης της διαδρομής (traceback) που προτείνονται από πολλούς ερευνητές (βλέπε σχετικά την Ενότητα 2.3.2). Από υπάρχουσες πολιτικές αντίδρασης θα αναζητήσει την κατάλληλη για την αντιμετώπιση του συγκεκριμένου περιστατικού που έχει αναλύσει, και θα την υλοποιήσει αντιδρώντας έτσι στην επίθεση DDoS ανεξάρτητα αλλά παράλληλα με τις υπόλοιπες ομότιμες Οντότητες στα άλλα δίκτυα.

3.3.3 Τα Συστήματα Ανίχνευσης Επιθέσεων (Intrusion Detection Systems)

Τα Συστήματα IDS στοιχειοθετούν τη βασική ικανότητα ανίχνευσης κάθε δικτύου. Μια βασική περιγραφή της λειτουργίας τους έγινε στην Ενότητα 2.3.1. Η Συνεργατική Υποδομή δε θέτει συγκεκριμένους κανόνες και περιορισμούς ως προς το είδος, τον τρόπο λειτουργίας και τη διάταξη των μονάδων αυτών. Άλλωστε η φιλοσοφία του συνεργατικού Συστήματος βασίζεται σε ανεξαρτησία από τις τεχνολογίες, τις υλοποιήσεις και τα προϊόντα στα οποία βασίζονται τα τοπικά συστήματα IDS. Επίσης θεωρείται ότι η οποιαδήποτε κλιμάκωση της αρχιτεκτονικής IDS (συσκευές πολλαπλών επιπέδων) και συγκέντρωση (aggregation) των πληροφοριών γίνεται προκειμένου να εξυπηρετήσει τοπικές ανάγκες του δικτύου και δεν αφορά τη λειτουργία του Υπερκείμενου Δικτύου. Ως προς την αρχιτεκτονική εγκατάστασης των συστημάτων IDS, η Συνεργατική Οντότητα έχει παρόμοιο ρόλο με οποιαδήποτε άλλη διαχειριστική εφαρμογή η οποία ζητά να χρησιμοποιήσει τα αποτελέσματα ανίχνευσης.

Οι προϋποθέσεις που τίθενται προκειμένου μια ή περισσότερες εφαρμογές IDS να ενταχθούν και να χρησιμοποιηθούν στη Συνεργατική Υποδομή είναι:

- Η λειτουργία των συστημάτων IDS με αντικείμενο την ανίχνευσης επιθέσεων DDoS. Η μέθοδος που θα χρησιμοποιηθεί για την ανίχνευση δεν παίζει ρόλο. Η Συνεργατική Οντότητα όμως, είναι σε θέση να ορίζει βάρη στα μηνύματα που δέχεται από ένα IDS ανάλογα με την εμπιστοσύνη που έχει στη χρησιμοποιούμενη μέθοδο. Επίσης, εφόσον το σύστημα IDS αποδίδει «συντελεστή βεβαιότητας» στην ανίχνευση στα μηνύματα του, η Οντότητα είναι δυνατόν να τον χρησιμοποιήσει στην εξαγωγή των

συμπερασμάτων της.

- Η έκδοση τελικών συμπερασμάτων για ένα συγκεκριμένο δίκτυο – κόμβο της Συνεργατικής Υποδομής. Η Συνεργατική Οντότητα δεν αναλαμβάνει την επεξεργασία δεδομένων για να διατηρήσει την ανεξαρτησία της από τις πιθανές διαφορετικές υλοποιήσεις χαμηλού επιπέδου, τις διαφορετικές μεθόδους λειτουργίας αισθητήρων κ.λπ.

- Στοιχεία περιστατικού. Οι αναφορές των συστημάτων IDS πρέπει κατ' ελάχιστον να περιλαμβάνουν:

  - Διεύθυνση (ή περιοχή διευθύνσεων) τελικού στόχου (σύστημα, ομάδα συστημάτων ή δίκτυο).
  - Πρωτόκολλο και θύρα που χρησιμοποιεί η κακόβουλη κίνηση.
  - Δίκτυο εισόδου και δίκτυο εξόδου της κίνησης στη διαδρομή προς το θύμα.
  - Χρονική σήμανση της αναφοράς.
  - Προαιρετικά ένα βαθμό βεβαιότητας για το περιστατικό.

- Σύνταξη των μηνυμάτων σε XML σύμφωνα με την προδιαγραφή IMDEF. Αποστολή των δύο ειδών μηνυμάτων που προβλέπει το πρότυπο αυτό (Alerts και Heartbeats). Ακόμα κι αν το σύστημα IDS δεν προβλέπει μια τέτοια λειτουργικότητα είναι πολύ απλή η υλοποίηση ενός ενδιάμεσου συστήματος που θα μετατρέπει τα μηνύματα σύμφωνα με το πρότυπο. Για παράδειγμα, μια τέτοια υλοποίηση πραγματοποιήθηκε στο εργαστήριο NETMODE του Ε.Μ.Π. στα πλαίσια διπλωματικής εργασίας [Ανδρ03] και αφορούσε στη διαμόρφωση μηνυμάτων ανίχνευσης του συστήματος Snort

[Casw03] με τη χρήση ενός «μετα-επεξεργαστή» (post-processor) που προβλέπεται από την αρχιτεκτονική του εργαλείου, ώστε να ακολουθούν το πρότυπο IDMEF (το XML DTD)[20].

3.4 Επικοινωνίες στην Αρχιτεκτονική

Ένα από τα σημαντικότερα προβλήματα που πρέπει να αντιμετωπίσει οποιαδήποτε κατανεμημένη αρχιτεκτονική που βασίζεται στις ανταλλαγές μηνυμάτων είναι να αποφύγει την εκτός ελέγχου κλιμάκωση αυτών των επικοινωνιών και τη δημιουργία έτσι επιπλέον (επιβαρύνουσας) κίνησης. Στην περίπτωση που εξετάζουμε το πρόβλημα είναι ιδιαίτερα σημαντικό γιατί οι επικοινωνίες αυτές θα πρέπει να γίνονται σε δίκτυα που πιθανόν να βρίσκονται ήδη σε κορεσμό εξ' αιτίας μιας επίθεσης DDoS. Το τελευταίο στοιχείο αποτελεί επίσης και περιοριστικό παράγοντα για συνεχείς επικοινωνίες δύο κατευθύνσεων μεταξύ οποιωνδήποτε κόμβων.

Η προτεινόμενη προσέγγιση εξέτασε λύσεις σε αυτό το πρόβλημα τόσο ως προς τη δυνατότητα υλοποίησης του Υπερκείμενου Δικτύου όσο και ως προς τον έλεγχο του πλήθους των παραγόμενων μηνυμάτων[21]. Η αντιμετώπιση του προβλήματος στην παρούσα εργασία γίνεται κατά κύριο λόγο με τη χρήση μεθόδων αποστολής μηνυμάτων «από έναν σε πολλούς». Σε μια σειρά από πειραματικές υλοποιήσεις, εξετάστηκε εναλλακτικά η χρήση επικοινωνίας multicast επιπέδου IP και δίκτυα επιπέδου εφαρμογής – υπερκείμενα (overlay) δίκτυα

[20] Πιο συγκεκριμένα τα μηνύματα συντάσσονται σύμφωνα με το εξελιγμένο IDMEF DTD που χρησιμοποιείται στις επικοινωνίες του Υπερκείμενου Δικτύου. Δείτε σχετικά το Τμήμα 4.3.2.

[21] Αφορά στη μεθοδολογία παραγωγής μηνυμάτων, τις προϋποθέσεις δημιουργίας τους και τον έλεγχο του πλήθους τους μέσω της εσωτερικής λειτουργίας της Συνεργατικής Οντότητας. Παρουσιάζεται αναλυτικά στο Κεφάλαιο 4.

peer-to-peer. Ταυτόχρονα ορισμένα χρήσιμα οργανωτικά χαρακτηριστικά στοιχεία αυτών των μεθόδων χρησιμοποιήθηκαν ως πρόσθετα πλεονεκτήματα της Συνεργατικής Αρχιτεκτονικής δίνοντας λειτουργικότητα που δε θα ήταν δυνατή με απλές επικοινωνίες unicast («ένας προς έναν»).

Ιδιαίτερη επιδίωξη της λύσης είναι η ανεξαρτησία από το δικτυακό υπόβαθρο για την εγκατάσταση και τη λειτουργία του Υπερκείμενου δικτύου. Κεντρικό στοιχείο στη φιλοσοφία της Συνεργατικής Υποδομής είναι να μπορεί να υλοποιηθεί με διαφορετικούς τρόπους, κάνοντας χρήση οποιωνδήποτε μέσων δικτυακής σύνδεσης χαμηλού επιπέδου είναι διαθέσιμα σε κάθε περίπτωση. Έμφαση δίνεται επίσης στη δυνατότητα ξεπεράσματος εμποδίων που μπορεί πιθανά να τεθούν σε χαμηλό επίπεδο ώστε σε κάθε περίπτωση να εξασφαλίζεται βασική συνδεσιμότητα μεταξύ των κόμβων της.

Επιπλέον υπάρχει μια σειρά από εναλλακτικές προσεγγίσεις στο ίδιο πρόβλημα που παρουσιάζουν επίσης χρήσιμα χαρακτηριστικά. Τέτοια είναι το περιβάλλον «Πλέγματος» (Grid). Η τελευταία αυτή μέθοδος δεν επιβεβαιώθηκε με υλοποίηση στα πλαίσια της παρούσας διατριβής.

3.4.1 Μεθοδολογίες IP Multicast

Οργάνωση και λειτουργία της Αρχιτεκτονικής με IP Multicast

Με τη χρήση του multicast στο επίπεδο IP επιλύεται το πρόβλημα των πολλαπλών επικοινωνιών μεταξύ των οντοτήτων με έναν απλό τρόπο που είναι ήδη διαθέσιμος σε πολλά δίκτυα, τόσο ερευνητικά όσο και παραγωγής. Η Συνεργατική Οντότητα δε χρειάζεται να λύσει περίπλοκα θέματα (δε χρειάζεται να διαθέσει υπολογιστικούς πόρους) για την οργάνωση του δικτύου η οποία ανα-

λαμβάνεται εξ' ολοκλήρου από την υποδομή των δικτύων που τη φιλοξενούν.

Ορίζεται ένα αποκλειστικό κανάλι (ομάδα multicast – multicast group) και οι επικοινωνίες του Υπερκείμενου Δικτύου πραγματοποιούνται εντός αυτού. Η ομάδα multicast αυτή ορίζεται με τη χρήση μιας συγκεκριμένης διεύθυνσης IP από τις δεσμευμένες για επικοινωνίες multicast[22]. Τα συνεργαζόμενα δίκτυα συμφωνούν εκ των προτέρων για το ποια θα είναι αυτή η ομάδα όπως και άλλα θέματα όπως η λειτουργία σηράγγων (tunnels) διαμέσου άλλων, μη συνεργαζόμενων, δικτύων που δεν υποστηρίζουν το IP multicast.

Υπάρχει επίσης η δυνατότητα χρησιμοποίησης «ασφαλούς multicast» (secure multicast) [Smug05]. Στην εκδοχή αυτή της επικοινωνίας multicast η σύνδεση με τον κοντινότερο δρομολογητή διασύνδεσης γίνεται μετά από επιβεβαίωση της ταυτότητας με τη χρήση κωδικού ασφαλείας. Η διαχείριση και διανομή αυτών των κωδικών πρόσβασης μπορεί εύκολα να γίνει στα πλαίσια των υπολοίπων συμφωνιών για τη δημιουργία της αρχιτεκτονικής. Εντούτοις, η χρήση του ασφαλούς multicast δεν αξιολογήθηκε λεπτομερώς στα πλαίσια της παρούσας εργασίας, επειδή το πρωτόκολλο δεν έχει ακόμα εξελιχθεί αρκετά.

Οι επικοινωνίες μεταξύ Οντοτήτων υλοποιούνται εύκολα με την προσθήκη υποστήριξης multicast στην υλοποίηση τους[23]. Η υποστήριξη αυτή αφορά:

α. Στη σύνδεση με το αντίστοιχο κανάλι επικοινωνίας multicast που έχει οριστεί για τη Συνεργατική Αρχιτεκτονική (δηλαδή τις διαδικασίες που απαιτούνται από το πρωτόκολλο IGMP (Internet Group Management Protocol) για σύνδεση με τον πιο κοντινό δρομολογητή ή και αυτές που

[22] Πρόκειται για τις διευθύνσεις IP εντός του διαστήματος 224.0.0.0-239.255.255.255.

[23] Η Οντότητα χρειάζεται βέβαια να υποστηρίζει και τις επικοινωνίες με την τοπική ιεραρχία Συστημάτων IDS εφόσον αυτή δεν είναι επίσης τύπου multicast.

ορίζονται από το «ασφαλές multicast» (secure multicast) εφόσον αυτό χρησιμοποιείται.

β. Στην επικοινωνία με την αποστολή και λήψη πακέτων multicast μέσω της κατάλληλης προγραμματιστικής υποδομής (Application Programming Interface – API).

Η λειτουργία κατ' αυτόν τον τρόπο προϋποθέτει την ύπαρξη και υποστήριξη multicast από τα δίκτυα που θα συμμετέχουν στη Συνεργατική Υποδομή. Διάφορα από τα δυναμικά πρωτόκολλα σύνδεσης του multicast είναι επίσης κατάλληλα: Τα PIM (Protocol-Independent Multicast) Πυκνής Δομής (Dense Mode), το MBGP (Multi-protocol extensions to BGP4), και ο συνδυασμός MBGP/MSDP (Multicast Source Discovery Protocol)/PIM Αραιής Δομής (Sparse Mode) είναι κάποια από αυτά [Alme00]. Για τις μεθόδους αυτές έχουν παρουσιαστεί παραδείγματα δικτύων τα οποία λειτουργούν κανονικά [Alme00] οπότε στην παρούσα εργασία θεωρείται ότι πρόκειται για ένα πρόβλημα λυμένο και πέραν του αντικειμένου της.

Λόγω των καλώς ορισμένων συμμετεχόντων συστημάτων (δηλαδή συνδρομητών multicast) και του μικρού πλήθους τους σε κάθε δίκτυο η διατήρηση του δέντρου διασύνδεσης (multicast tree) και η συντήρηση της ομάδας multicast[24] είναι ντε-φάκτο ευκολότερη από άλλες τυπικές χρήσεις τέτοιων υπηρεσιών όπου τα συστήματα πελάτες multicast συνδέονται και αποσυνδέονται διαρκώς από το δίκτυο.

Στην Αρχιτεκτονική πρέπει να προβλέπεται το ενδεχόμενο προβλημάτων στο χαμηλότερο επίπεδο και η λειτουργία της να επηρεάζεται κατά το δυνατόν

[24]Πρόκειται για τις διαδικασίες δυναμικής συμμετοχής συστημάτων στην ομάδα multicast, διαγραφής ανενεργών «κλαδιών» του δέντρου διασύνδεσης (inactive branch pruning) κ.λπ.

λιγότερο από αυτά. Η υποστήριξη multicast από τα συνεργαζόμενα δίκτυα θα πρέπει να είναι επαρκής για να στηριχτεί σε αυτό μια υπηρεσία που σχετίζεται με ζητήματα ασφαλείας.

Για το λόγο αυτό, λύσεις βασισμένες στο multicast, χρησιμοποιούνται τα μηνύματα κανονικής λειτουργίας ("heartbeats") του IDMEF που ενημερώνουν για τυχόν προβλήματα επικοινωνίας είτε λόγω αστοχίας κάποιας Συνεργατικής Οντότητας είτε εξ' αιτίας του δικτύου. Γενικά, στο σχεδιασμό των Οντοτήτων υπάρχουν επαρκείς έλεγχοι ώστε ένα τεχνικό πρόβλημα να μην ενεργοποιήσει αναγκαστικά μια εσφαλμένα θετική ανίχνευση.

Τη στιγμή αυτή οι υπηρεσίες multicast δεν αποτελούν υπηρεσία προτεραιότητας ή δεν υποστηρίζονται ακόμα σε πολλά εμπορικά δίκτυα (ISPs). Η διατήρηση του δένδρου διασύνδεσης και η δρομολόγηση multicast είναι επίσης αρκετά πολύπλοκες διαδικασίες, ειδικά μεταξύ διαφορετικών domains [Alme00]. Σε αρκετές περιπτώσεις δε, υπάρχουν δυσκολίες στην υποστήριξη από τους κατασκευαστές δρομολογητών. Όλα αυτά είναι προβλήματα που πρέπει να αντιμετωπιστούν ως ζητήματα συνεργασίας στη διαχείριση των δικτύων.

Ανάλυση χρήσης του IP Multicast

Η χρήση του IP Multicast παρουσιάζει επιπλέον μια σειρά από συγκεκριμένα πλεονεκτήματα στην οργάνωση και λειτουργία της Υποδομής:

- *Δυνατότητες ελεγχόμενης κλιμάκωσης της αρχιτεκτονικής.* Η ύπαρξη ενός υπόβαθρου επικοινωνίας με multicast επιτρέπει την οργάνωση και την κλιμάκωση της αρχιτεκτονικής με την επιλογή κατάλληλων τιμών για την παράμετρο TTL (αριθμός επιτρεπόμενων βημάτων από κόμβο σε κόμ-

βο – Time To Live) των πακέτων που ανταλλάσσονται. Οι επικοινωνίες του Υπερκείμενου Δικτύου διεκπεραιώνονται σε ένα συγκεκριμένο κανάλι (δεσμευμένη διεύθυνση IP multicast) και τα μηνύματα μπορούν να φτάσουν μέχρι τα σημεία που επιλέγεται αυτό να μεταδίδεται. Επιπλέον ακόμα και εντός του ίδιου του Υπερκείμενου Δικτύου είναι δυνατόν να οριστούν αποστάσεις μετάβασης των μηνυμάτων ορίζοντας στην παράμετρο TTL την ακτίνα μετάδοσης γύρω από τον αποστολέα που μπορούν να φτάσουν. Έτσι τα μηνύματα από μια Συνεργατική Οντότητα μπορούν να διανέμονται μόνον σε γειτονικά δίκτυα (στις εκεί Οντότητες). Η συνδεσιμότητα multicast εξασφαλίζει αυτόματα την απουσία «βρόχων» (loops) στο δίκτυο διασύνδεσης των Οντοτήτων.

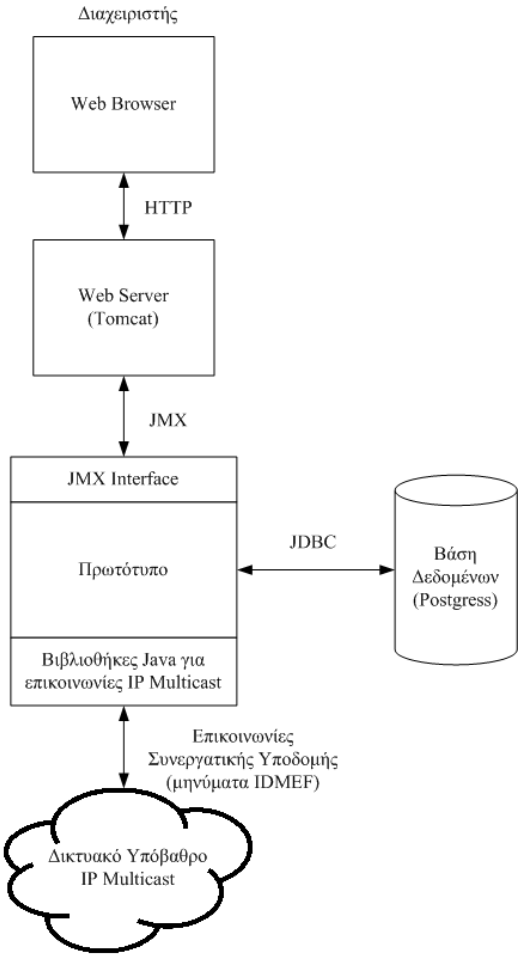
- *Παράλληλη λειτουργία εφεδρικών Οντοτήτων.* Η μέθοδος IP Multicast επιτρέπει την «παθητική» παρακολούθηση ενός καναλιού από μια Οντότητα χωρίς να αποκαλύπτει τη διεύθυνση της. Έτσι είναι δυνατόν περισσότερες της μίας Οντότητες να λειτουργούν παράλληλα σε κάθε δίκτυο, ακόμα και σε διαφορετικά σημεία του ως εφεδρικές. Οι επιπλέον Οντότητες μπορούν να λαμβάνουν τα ίδια μηνύματα με την κύρια και να διατηρούν την ίδια κατάσταση λειτουργίας. Σε περίπτωση που η κύρια Συνεργατική Οντότητα τεθεί εκτός λειτουργίας είτε λόγω αστοχίας είτε λόγω επίθεσης οι επιπλέον διαθέσιμες Οντότητες μπορούν να αναλάβουν (με μια διαδικασία ανακάλυψης του προβλήματος και επιλογής νέας κύριας) λειτουργικό ρόλο. Επιπλέον η διασπορά τους αυτή ακόμα και σε διαφορετικά υποδίκτυα εξασφαλίζει ότι δε θα τεθούν όλες ταυτόχρονα εκτός λειτουργίας από μία μόνον επίθεση.

Υλοποίηση της Λύσης IP Multicast

Στα πλαίσια της διπλωματικής εργασίας [Χατζ02] έγινε και η πειραματική επιβεβαίωση της δυνατότητας της λειτουργίας της Αρχιτεκτονικής με IP Multicast. Πιο συγκεκριμένα, λειτούργησε επιτυχώς ένα δίκτυο βασισμένο σε IP Multicast μέσω του οποίου ανταλλάσσονται μηνύματα προειδοποίησης (Alerts) και Κανονικής Λειτουργίας (Heartbeats) δομημένα σε XML κατά το πρότυπο IDMEF. Στον παραλήπτη τα μηνύματα αναλύονται και μεταφέρουν την πληροφορία που περιέχουν σε μία Βάση Καταγραφής Αναφορών. Η υλοποίηση έγινε σε Java και εντάχθηκε στο διαχειριστικό πλαίσιο της προγραμματιστικής υποδομής Java Management Extensions (JMX) [Jmx04][25]. Ένα web interface παρέχει στο διαχειριστή τη δυνατότητα να ελέγχει τις εισερχόμενες αναφορές σε μια Οντότητα (από τοπικές ή απομακρυσμένες πηγές). Σε ρόλο αντίστοιχο προς ένα αυτοματοποιημένο σύστημα ενεργοποίηση της Οντότητας, ο διαχειριστής μπορεί επίσης να εκτελεί αναζητήσεις (τύπου ερωτημάτων SQL) στις αποθηκευμένες αναφορές ώστε να τις συνδυάσει και να εντοπίσει περιστατικά.

Το Σχήμα 3.5 δίνει μια γενική απεικόνιση της αρχιτεκτονικής του πρωτοτύπου που περιγράφηκε.

[25] Δείτε σχετικά τις λεπτομέρειες της αρχιτεκτονικής της Οντότητας στο Κεφ. 4



Σχήμα 3.5: Αρχιτεκτονική πρωτοτύπου Οντότητας που χρησιμοποιεί IP Multicast

Συμπεράσματα από τη χρήση IP Multicast

Από το σχεδιασμό της λειτουργίας της Αρχιτεκτονικής με τη χρήση IP Multicast και από τα αποτελέσματα της υλοποίησης και λειτουργίας του πρωτοτύπου προκύπτουν τα εξής συμπεράσματα:

- Οι Οντότητες μπορούν να συνδεθούν με το υποκείμενο εγκατεστημένο δίκτυο IP Multicast και να επικοινωνήσουν αποτελεσματικά δημιουργώντας το δίκτυο (επιπέδου εφαρμογής) της Συνεργατικής Υποδομής.

- Αναγκαία συνθήκη για τις επικοινωνίες της Υποδομής αποτελεί η ύπαρξη και ορθή λειτουργία του δικτύου Multicast (δημιουργία δένδρων δρομολόγησης, σύνδεση απομονωμένων κλάδων, διεκπεραίωση αιτήσεων επέκτασης της συνδεσιμότητας multicast κ.λπ.) και μάλιστα μεταξύ διαφορετικών δικτύων (domains). Η συνδεσιμότητα αυτή απαιτεί πολιτική δέσμευση των συμμετεχόντων δικτύων, την δέσμευση αντίστοιχων υπολογιστικών πόρων (συστημάτων, λογισμικού κ.λπ.) και εργασία από τους κατά τόπους διαχειριστές για την υλοποίηση της και τη λύση τυχόν προβλημάτων.

- Λόγω της εξάρτησης από εξωτερική υποδομή διασύνδεσης σε επίπεδο IP (Multicast Tree) η Συνεργατική Υποδομή (η οποία λειτουργεί σε ανώτερο επίπεδο) χρειάζεται να υλοποιεί επιπλέον μηχανισμούς επιβεβαίωσης της συνδεσιμότητας μεταξύ των δικτύων-κόμβων της (με τη μορφή Μηνυμάτων Κανονικής Λειτουργίας – Heartbeats).

- Τέλος, με τη χρήση της προγραμματιστικής υποδομής JMX (ή άλλης αντίστοιχης) είναι δυνατή η «κατά τμήματα» (modular) υλοποίηση και

διαχείριση της Συνεργατικής Οντότητας. Η προσέγγιση αυτή δίνει τη δυνατότητα για επιμέρους έλεγχο των τμημάτων της Οντότητας, επιτρέπει τμηματικές αναβαθμίσεις και ρυθμίσεις χωρίς συνολική διαδικασία επανεκκίνησης (rebooting) και δίνει τη δυνατότητα για κατανομή λειτουργιών σε περισσότερα του ενός υπολογιστικά συστήματα.

3.4.2 Χρήση δικτύου peer-to-peer (επιπέδου εφαρμογής) για συνεργασία μικρής κλίμακας

Η τεχνική επικοινωνίας peer-to-peer έχει γνωρίσει ευρεία εξάπλωση τα τελευταία χρόνια, ως μέσο για τη δημιουργία υπερκείμενων (overlay) δικτύων μεταφοράς περιεχομένου, αποφεύγοντας την ανάγκη ύπαρξης ενός κεντρικού κόμβου. Λόγω της διαδεδομένης χρήσης της (κυρίως ανταλλαγές αρχείων), η μεθοδολογία peer-to-peer, έχει εξελιχθεί κατά τέτοιο τρόπο ώστε να ξεπερνά δικτυακά εμπόδια (π.χ. Συστήματα Δικτυακής Προστασίας – Firewalls) ή μη συνεργαζόμενα τμήματα του δικτύου και να διατηρείται σε λειτουργία ακόμα και υπό ιδιαίτερα αντίξοες συνθήκες (π.χ. χαμηλές ταχύτητες συνδεσιμότητας). Ένα δίκτυο τέτοιου τύπου υλοποιείται στο επίπεδο εφαρμογής και όλοι οι κόμβοι είναι απόλυτα ισότιμοι μεταξύ τους. Τα χαρακτηριστικά αυτά είναι ιδιαίτερα χρήσιμα και για τη Συνεργατική Υποδομή. Ένα υπερκείμενο δίκτυο peer-to-peer μπορεί να χρησιμοποιηθεί, για τη μεταφορά των μηνυμάτων μεταξύ των Οντοτήτων, αντί για αρχεία. Η κύρια διαφορά από τη λύση IP Multicast είναι ότι οι ίδιες οι Οντότητες χρειάζεται να υλοποιούν τη λειτουργικότητα διασύνδεσης, αντί να χρησιμοποιούν ήδη ένα υλοποιημένο δίκτυο. Στις Οντότητες γίνεται χρήση των προγραμματιστικών υποδομών (Application Program Interfaces –

APIs) που παρέχονται τυποποιημένες από διάφορες υλοποιήσεις επικοινωνιών peer-to-peer. Παράλληλα, η χρήση τεχνικών peer-to-peer παρέχει (όπως και η λύση με IP Multicast) ειδικά χαρακτηριστικά, χρήσιμα στη λειτουργία και την οργάνωση της Συνεργατικής Αρχιτεκτονικής. Επιτυγχάνεται έτσι:

- Η αυτόματη οργάνωση της αρχιτεκτονικής, η δρομολόγηση και η μετάδοση των μηνυμάτων «από έναν σε πολλούς».
- Η δυνατότητα συνέχισης της λειτουργίας της αρχιτεκτονικής ακόμα και αν κάποιοι από τους κόμβους της έχουν τεθεί εκτός λειτουργίας λόγω αστοχίας ή υπερφόρτωσης του δικτύου. Πιο συγκεκριμένα πολλές προσεγγίσεις peer-to-peer είναι ειδικά βελτιστοποιημένες για την περίπτωση ύπαρξης πολλών κόμβων με μεγάλη συχνότητα εισόδου και εξόδου μελών στο υπερκείμενο δίκτυο.
- Συνολική επεξεργασία των πληροφοριών σχετικά με την επίθεση (ειδικότερα καταγραφή της διαδρομής της) από κάποιο κόμβο που αναλαμβάνει αυτόματα το ρόλο της συγκέντρωσης στοιχείων, πέρα από τις επιμέρους διαπιστώσεις των υπολοίπων Οντοτήτων.
- Δημιουργία ομάδων δικτύων που συνεργάζονται στην από κοινού αντιμετώπιση συγκεκριμένων περιστατικών που τα αφορούν.

Σχηματισμός του δικτύου

Όπως και στην περίπτωση του IP Multicast το υπερκείμενο δίκτυο σχηματίζεται και ξεκινά τη λειτουργία του πριν την εμφάνιση οποιουδήποτε περιστατικού. Μετά την ανίχνευση ενός περιστατικού οργανώνεται σε συγκεκριμένες ομαδοποιήσεις ενεργοποιώντας εκείνους τους κόμβους της τοπολογίας που φαίνεται

να σχετίζονται με αυτό. Η όλη διαδικασία συμμετοχής στο δίκτυο και ανακάλυψης των άλλων κόμβων που λειτουργούν γίνεται μεν από τη Συνεργατική Οντότητα πρακτικά όμως αναλαμβάνεται από τη λειτουργικότητα peer-to-peer που ενσωματώνει αυτή· δεν είναι απαραίτητο να αναπτυχθεί εκ του μηδενός.

Κατά την αρχική φάση δημιουργίας του δικτύου, ο κάθε κόμβος που ενεργοποιείται επιχειρεί να ανακαλύψει άλλους ομότιμους και να γίνει μέρος της οργανωμένης υποδομής peer-to-peer. Η διαδικασία που ακολουθείται είναι τυπική για τη συμμετοχή σε οργανωτικά σχήματα τέτοιου είδους. Στο πρώτο βήμα γίνεται σύνδεση με έναν κόμβο που ήδη λειτουργεί, ο οποίος θα εκτελέσει τις απαραίτητες διαδικασίες επιβεβαίωσης της ταυτότητας και αποδοχής του νέου μέλους. Η ανακάλυψη του πρώτου κόμβου είναι δυνατόν να γίνει με έναν αριθμό από διαφορετικούς τρόπους:

Α. Χρησιμοποιείται ένας γενικότερα γνωστός εξυπηρετητής σύνδεσης γενικής χρήσης. Ο εξυπηρετητής αυτός μπορεί να έχει δημόσιο χαρακτήρα και να παρέχει υπηρεσίες σε πολλά διαφορετικά δίκτυα peer-to-peer που λειτουργούν εν παραλλήλω· παραπέμπει στον πιο κοντινό κόμβο της Συνεργατικής Υποδομής χωρίς κανένα επιπλέον έλεγχο. Στη συνέχεια ο Συνεργατικός κόμβος θα πραγματοποιήσει τις διαδικασίες ελέγχου πρόσβασης κ.λπ. και θα δώσει τις απαραίτητες πληροφορίες για τους υπόλοιπους κόμβους του Υπερκείμενου Δικτύου που λειτουργούν ήδη. Η προσέγγιση αυτή, μπορεί να προκαλέσει προβλήματα στην περίπτωση που οι εξυπηρετητές υποστούν οι ίδιοι επίθεση DDoS ή παραβιαστούν και περάσουν στον έλεγχο τρίτων. Για το μεν πρώτο πρόβλημα είναι δυνατόν ο νέος κόμβος να δοκιμάζει έναν αριθμό από διαφορετικούς και απομακρυ-

σμένους μεταξύ τους εξυπηρετητές, αποφεύγοντας ένα μοναδικό σημείο αστοχίας. Το δεύτερο πρόβλημα δεν είναι μεν σε θέση να οδηγήσει σε άμεση παραβίαση του Συνεργατικού Δικτύου (υπάρχουν επιπλέον διαδικασίες ελέγχου πρόσβασης)[26] αλλά μπορεί να κάνει γνωστούς κάποιους από τους κόμβους του θέτοντας τους έτσι σε κίνδυνο.

Β. Στα πλήρως ισότιμα δίκτυα peer-to-peer, κάθε κόμβος μπορεί να παίξει το ρόλο του εξυπηρετητή σύνδεσης. Έτσι ο νέος κόμβος στέλνει αίτηση σε έναν ήδη υπάρχοντα κόμβο (του Συνεργατικού Δικτύου) που είναι γνωστός (με την IP) του εξ' αρχής αλλά δεν έχει κάποια ιδιαίτερη εξειδίκευση. Η επικοινωνία αυτή μπορεί να λάβει χώρα σε οποιαδήποτε δικτυακή θύρα (αποφασισμένη εξ' αρχής) προκειμένου να μειωθεί η πιθανότητα της παρακολούθησης από τρίτους που την αναμένουν.

Γ. Μπορεί τέλος να χρησιμοποιηθεί μια μικτή λύση με τη χρήση ενός ειδικού καναλιού IP Multicast. Ο νέος κόμβος εκπέμπει σε αυτό μια αίτηση σύνδεσης και τυχόν υπάρχοντες κόμβοι απαντούν απευθείας (σε unicast) συνεχίζοντας τη διαδικασία αποδοχής. Στα μηνύματα multicast αυτά τίθεται μια συγκεκριμένη, μικρή τιμή της παραμέτρου TTL ώστε η προσπάθεια αναζήτησης να περιοριστεί σε τοπικό επίπεδο. Ένα πιθανό πρόβλημα δημιουργείται από το ενδεχόμενο όλοι οι υπόλοιποι κόμβοι βρίσκονται σε μεγαλύτερη απόσταση από την τιμή της παραμέτρου TTL. Εντούτοις με δεδομένο ότι οι λεπτομέρειες του δικτύου έχουν κανονιστεί εξ αρχής μπορεί αντίστοιχα να ορίζεται και η κατάλληλη τιμή της παραμέτρου ώστε να εξασφαλίζεται η μετάδοση μέχρι κάποιο κόμβο που λειτουργεί. Όπως

[26] Πρόκειται άλλωστε για εξυπηρετητή σύνδεσης «γενικής χρήσης» που δεν έχει επιπλέον στοιχεία για τη Συνεργατική Υποδομή πέρα από τις διευθύνσεις κάποιων κόμβων της.

αναφέρθηκε πιο πάνω η μέθοδος IP Multicast επιτρέπει στον κόμβο να διατηρήσει την ανωνυμία του ως προς τη διεύθυνση IP.

Μετά την αρχική ανακάλυψη ενός τουλάχιστον κόμβου της Συνεργατικής Υποδομής που λειτουργεί ήδη ο νέος κόμβος πρέπει να περάσει τη διαδικασία αποδοχής με επιβεβαίωση της ταυτότητας του. Ο νέος κόμβος ενημερώνεται από τον εξυπηρετητή για άλλους κόμβους που λειτουργούν σε κοντινή απόσταση και τις υπηρεσίες που αυτοί παρέχουν. Ο κόμβος εξυπηρέτησης κρατάει έναν κατάλογο με δείκτες σε αυτές. Στην τρέχουσα υλοποίηση οι υπηρεσίες είναι δεδομένες – ανταλλαγές μηνυμάτων – αλλά μπορούν να επεκταθούν αν χρειαστεί και σχεδιαστεί κάτι τέτοιο. Ακολουθεί η φάση ανακάλυψης του πλήρους δικτύου με σημαντική ανταλλαγή σηματοδοσίας. Ο κάθε νέος κόμβος στέλνει ένα αριθμό μηνυμάτων προς τους κόμβους που λειτουργούν ήδη και περιμένει για κάποιο διάστημα τις απαντήσεις τους. Κατά τον τρόπο αυτό μαθαίνει τις διαδρομές που θα επιτρέψουν τη βέλτιστη δρομολόγηση μηνυμάτων διαμέσου του Υπερκείμενου Δικτύου. Η τελική οργάνωση του δικτύου γίνεται χωρίς τη μεσολάβηση κάποιας κεντρικής αρχής ελέγχου.

Από τη στιγμή που το Υπερκείμενο Δίκτυο είναι σε λειτουργία, εκμεταλλευόμενο τα χαρακτηριστικά των δικτύων peer-to-peer, διατηρεί τη συνδεσιμότητα και παραμένει σε λειτουργία ασχέτως προβλημάτων που μπορεί να παρουσιαστούν στη λειτουργία κάποιων κόμβων. Ακόμα και στην περίπτωση απενεργοποίησης κάποιων κόμβων τα μηνύματα θα δρομολογηθούν μέσω του δικτύου κατά τον κατάλληλο τρόπο με χρήση της πληροφορίας δρομολόγησης που ο αποστολέας έχει εξασφαλίσει ο ίδιος. Η διαδικασία συγκέντρωσης πληροφοριών για τη δομή του δικτύου επαναλαμβάνεται τακτικά.

Το ίδιο το υπερκείμενο δίκτυο peer-to-peer φροντίζει για τη λειτουργία του στο επίπεδο εφαρμογής παρακάμπτοντας θέματα χαμηλότερων επιπέδων. Είναι χαρακτηριστικό ότι σε αυτή την περίπτωση δε γίνεται χρήση των μηνυμάτων κανονικής λειτουργίας ("heartbeats"), όπως συμβαίνει στην περίπτωση χρήσης της δικτυακής υποδομής Multicast (ενότητα 3.4.1).

Οργάνωση κατά τη διάρκεια ενός περιστατικού

Μια βασική λειτουργικότητα του Υπερκείμενου Δικτύου που υλοποιείται έτσι είναι η μεταβίβαση αναφορών στο εσωτερικό του με τη μέθοδο «από έναν σε πολλούς», εντελώς αντίστοιχα με τον τρόπο που αυτό θα συνέβαινε σε ένα δίκτυο IP Multicast.

Το ιδιαίτερο χαρακτηριστικό που προσφέρει η συνδεσμολογία peer-to-peer είναι ότι η αρχιτεκτονική είναι δυναμικά εξελισσόμενη και αντιδρά με ειδικό τρόπο για κάθε ένα περιστατικό. Σκοπός είναι η δυναμική οργάνωση εκείνων ακριβώς των κόμβων που έχουν κάποια εμπλοκή με το περιστατικό ώστε αφ' ενός να αναδείξουν τη διαδρομή της επίθεσης DDoS αφ' ετέρου να έχουν τη δυνατότητα για μια συντονισμένη και κατευθυνόμενη αντίδραση. Με την ανίχνευση ενός νέου περιστατικού δημιουργείται ένα «*Σημείο Συντονισμού*» (*"Rendezvous Point" – RP*) ειδικά για αυτό. Σκοπός του είναι να συγκεντρώσει όλες τις υπάρχουσες πληροφορίες, να καταλήξει σε συμπεράσματα για το περιστατικό και να οργανώσει τα δίκτυα που εμπλέκονται (ακόμα και αν σε κάποια από αυτά δεν έχει γίνει καμία ανίχνευση).

Ρόλο *RP* παίζει το πρώτο δίκτυο το οποίο θα αναγνωρίσει το νέο περιστατικό. Επειδή όμως είναι πολύ πιθανό αυτό να είναι και το τελικό θύμα της επίθεσης DDoS, υπάρχει η πρόβλεψη να μη χρησιμοποιείται *RP* το οποίο έχει

διευθύνσεις από το δίκτυο που είναι ο τελικός προορισμός της κακόβουλης κίνησης. Επίσης λύνονται με αυτόματο τρόπο περιπτώσεις που θα εμφανιστούν περισσότερα του ενός RP για το ίδιο περιστατικό ταυτόχρονα. Το RP στέλνει ενημερώσεις για τη δημιουργία της νέας ομαδοποίησης σε όλα τα μέλη της Συνεργατικής Υποδομής. Αυτά τα μηνύματα προειδοποίησης (Alerts) διαδίδονται με multicast επιπέδου εφαρμογής διαμέσου του δικτύου peer-to-peer, προσφέρουν επιπλέον στοιχεία για την ανίχνευση του περιστατικού στις Οντότητες που εμπλέκονται, ενώ ενημερώνουν και για την ύπαρξη της Ομαδοποίησης. Κάθε Οντότητα της Συνεργατικής Αρχιτεκτονικής που θα αναγνωρίσει επίσης το ίδιο περιστατικό (με τα ίδια χαρακτηριστικά και στόχο) γίνεται μέλος της ίδιας ομαδοποίησης.

Στη συνέχεια τα μέλη αυτής της ομάδας μπορούν να ανταλλάσσουν στοιχεία μεταξύ τους ώστε να συντονιστεί η διαδικασία προσδιορισμού της διαδρομής της επίθεσης και να αποδώσει καλύτερα αποτελέσματα. Τα μέλη της ομάδας αποστέλλουν κατ' ελάχιστο στο RP τη διαδρομή που η επίθεση ακολουθεί σε σχέση με το δίκτυο τους: δίκτυο [27] εισόδου της κίνησης, δίκτυο εξόδου. Είναι επίσης δυνατόν σε τοπικό επίπεδο και με πολύ μικρή επιβάρυνση του δικτύου να συλλέξουν επιπλέον στοιχεία. Τέτοια πληροφορία είναι τα επόμενα δίκτυαβήματα της διαδρομής της επίθεσης προς το στόχο, τουλάχιστον για ένα μικρό αριθμό βημάτων και αντλείται από τις πληροφορίες δρομολόγησης (π.χ. από το πρωτόκολλο BGP) ή δικτυακά εργαλεία (όπως π.χ. η εφαρμογή traceroute). Η ανασύνθεση αυτών των πληροφοριών μπορεί να αποδώσει τη διαδρομή της επίθεσης προς το στόχο περιλαμβάνοντας και δίκτυα τα οποία δεν αποτελούν

[27] Το Δίκτυο – Αυτόνομο Σύστημα (Autonomous System — AS), όπως αυτό ορίζεται στο πρωτόκολλο δικτυακής δρομολόγησης Border Gateway Protocoll (BGP).

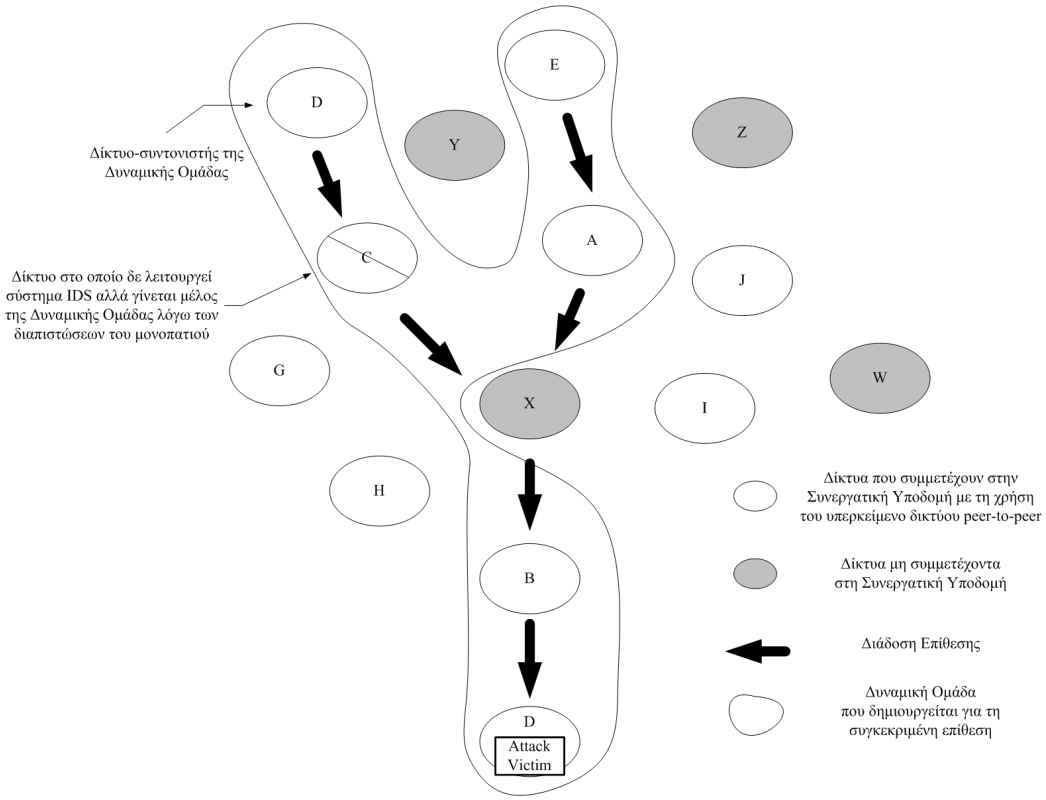
τμήματα του Υπερκείμενου Δικτύου. Επιπλέον, δίκτυα μέλη του Υπερκείμενου Δικτύου, που ενδεχομένως δεν έχουν εντοπίσει το περιστατικό ή δε διαθέτουν ενεργό σύστημα IDS, εφόσον βρεθούν πάνω στο ίδιο μονοπάτι μπορούν να ενεργοποιηθούν και να πάρουν μέρος στην ομαδοποίηση (και κατ' επέκταση στην αντιμετώπιση του περιστατικού).

Η λειτουργία αυτή μπορεί να επαναλαμβάνεται ταυτόχρονα και ανεξάρτητα για πολλά διαφορετικά περιστατικά που γίνονται αντιληπτά στη Συναργατική Υποδομή. Σε κάθε περίπτωση δημιουργείται το αντίστοιχο RP και οργανώνονται οι αντίστοιχες ομαδοποιήσεις.

Στη συνέχεια, η αντίδραση στο περιστατικό ορίζεται από τις Οντότητες και την εσωτερική τους διαμόρφωση και λειτουργία όπως αυτή παρουσιάζεται στο Κεφάλαιο 4. Παρά τη χρήση ενός «κεντρικού σημείου» (του RP) ανάλυσης του περιστατικού, παραμένουν σε τοπικό έλεγχο θέματα όπως:

- Η αποδοχή και απόδοση βαρύτητας στα εισερχόμενα μηνύματα απομακρυσμένης προέλευσης.
- Η εκτίμηση της σοβαρότητας του περιστατικού
- Η επιλογή του είδους αντίδρασης

Το Σχήμα 3.6 δίνει ενδεικτικά την οργάνωση και λειτουργία της Συνεργατικής Υποδομής με τη χρήση βασικού δικτύου peer-to-peer.



Σχήμα 3.6: Οργάνωση και λειτουργία της Συνεργατικής Υποδομής με τη χρήση peer-to-peer

Υλοποίηση Πρωτοτύπου

Για τη δοκιμή της προσέγγισης του Υπερκείμενου Συνεργατικού Δικτύου με εργαλεία peer-to-peer έγινε η υλοποίηση ενός πρωτοτύπου με τη χρήση της προγραμματιστικής υποδομής (API) του συστήματος peer-to-peer JXTA [Jxta], στα πλαίσια της διπλωματικής εργασίας [Πουγ04]. Πιο συγκεκριμένα, υλοποιήθηκαν και δοκιμάστηκε η λειτουργία των εξής στοιχείων:

- Το σύστημα JXTA αναλαμβάνει το σχηματισμό του αρχικού δικτύου peer-to-peer και της εισαγωγής νέων κόμβων σε αυτό. Αυτό επιτυγ-

χάνεται με ανταλλαγές μηνυμάτων του JXTA στη φάση της οργάνωσης του.

- Ανιχνεύσεις (εικονικές κατά τους πειραματισμούς) σε κάποια από τα δίκτυα της Συνεργατικής Υποδομής που υποδείκνουν επιθέσεις DDoS διαδίδονται στο υπερκείμενο δίκτυο μηνύματα με IDMEF που μεταφέρουν τα σχετικά στοιχεία. Η μετάδοση αυτή επιτυγχάνεται μεταξύ των κόμβων peer-to-peer με multicast επιπέδου εφαρμογής

- Γίνεται δυναμική δημιουργία ομάδων (dynamic group formation) βάσει των ανιχνεύσεων ενός περιστατικού DDoS από ορισμένα από τα δίκτυα της Συνεργατικής Υποδομής.

- Χρησιμοποιείται ο κόμβος-*Σημείο Συντονισμού* (RP), ο οποίος συγκεντρώνει επιμέρους πληροφορίες διαδρομής από τους κόμβους-μέλη της δυναμικής ομάδας. Οι πληροφορίες αυτές βασίζονται σε στοιχεία εξόδου του εργαλείου traceroute. Στη συνέχεια σε κάθε περίπτωση γίνεται (στο βαθμό που αυτό είναι εφικτό από τις συγκεντρωμένες πληροφορίες) η ανακατασκευή του μονοπατιού επίθεσης προς το στόχο.

Συμπεράσματα από τα δίκτυα Peer-to-Peer για συνεργασία μικρής κλίμακας

Οι δοκιμές υλοποίησης της Συνεργατικής Αρχιτεκτονικής με τη χρήση του βασικού συστήματος peer-to-peer JXTA κατέδειξαν τα εξής συμπεράσματα:

- Η τεχνολογία peer-to-peer προσφέρει μια αξιόπιστη πλατφόρμα διασύνδεσης πάνω στην οποία μπορεί να εγκατασταθεί και να λειτουργήσει το

σύστημα της Συνεργατικής Υποδομής. Μεγάλο τμήμα της υλοποίησης του βασικού δικτύου συνεργασίας αναλαμβάνεται και συντηρείται αυτόματα από δοκιμασμένες και αξιόπιστες τεχνολογίες peer-to-peer. Είναι απαραίτητη όμως η ενσωμάτωση των αντίστοιχων προγραμματιστικών βιβλιοθηκών στη υλοποίηση της Συνεργατικής Οντότητας.

- Η οργάνωση για την αντιμετώπιση ενός περιστατικού αναλαμβάνεται από διαφορετικό *Σημείο Συντονισμού* (RP) σε κάθε περίπτωση επίθεσης. Άρα δεν αποτελεί μοναδικό κρίσιμο σημείο το οποίο θα μπορούσε να αποτελέσει στόχο ξεχωριστής επίθεσης.

- Στο σημείο *Σημείο Συντονισμού* (RP) συγκεντρώνονται στοιχεία:

  α. από πολλά σημεία που εκτείνονται σε όλο το μονοπάτι της επίθεσης

  β. που περιέχουν πληροφορία πέρα από την απλή διαπίστωση του περιστατικού. Αντιθέτως, με τη χρήση της πληροφορίας διαδρομής προς το τελικό στόχο (από το BGP ή με το εργαλείο traceroute) είναι δυνατή η πληρέστερη ανακατασκευή του μονοπατιού της επίθεσης.

  Έτσι, δίκτυα που δεν έχουν τα ίδια ανιχνεύσει το περιστατικό (λόγω ανεπάρκειας ή μη διαθεσιμότητας συστήματος IDS) μπορούν, λαμβάνοντας τις συγκεντρωτικές ενημερώσεις, να συμπεράνουν[28] ότι αποτελούν μέρος της διαδρομής της επίθεσης και να λάβουν επίσης μέτρα ως επιπλέον σημεία αντιμετώπισης της.

[28] Εφόσον αποδίδουν επαρκή βαθμό εμπιστοσύνης στις απομακρυσμένες αναφορές.

3.4.3 Χρήση δικτύων peer-to-peer σε μεγάλη κλίμακα

Δίκτυα peer-to-peer με δρομολόγηση βασισμένη σε κλειδί

Η περιγραφείσα προηγουμένως χρήση δικτύων peer-to-peer αποτελεί την απλή προσέγγιση και περιορίζεται σε περιπτώσεις μικρής εξάπλωσης του Υπερκείμενου Δικτύου. Τα σύγχρονα δίκτυα p2p είναι βελτιστοποιημένα στην αποδοτική τοποθέτηση και αναζήτηση περιεχομένου σε μεγάλη κλίμακα. Αυτό επιτυγχάνεται με τη δεικτοδότηση (indexing) του περιεχόμενου ώστε ονόματα αρχείων να αντιστοιχούν σε θέσεις στο σύστημα αποθήκευσης (δηλαδή τους κόμβους του δικτύου peer-to-peer). Η δρομολόγηση προς τον κόμβο υπεύθυνο για το κλειδί προορισμού γίνεται με συγκεκριμένο τρόπο και ακολουθεί τη γενική ονομασία «Δρομολόγηση βασισμένη σε κλειδί» (Key-Based Routing). Σε υψηλότερα επίπεδα λειτουργικότητας υλοποιούνται διάφορες μεθοδολογίες οργάνωσης και δρομολόγησης πάνω στη βασική, όπως:

- *Distributed Hash Tables — DHT (Κατανεμημένοι Πίνακες Κατακερματισμού).* Υλοποιούν τις αντιστοιχήσεις κλειδί-τιμή όπου το κλειδί αφορά κάποιο κόμβο του δικτύου p2p.

- *Distributed Object Location and Routing — DOLR.* Στην περίπτωση αυτή παρέχεται μια υπηρεσία κατανεμημένου καταλόγου. Κάθε αντίγραφο αποθηκευμένου αντικειμένου στο δίκτυο έχει ένα χαρακτηριστικό κωδικό. Αυτός αντιστοιχίζεται στον κωδικό εκείνου του κόμβου που κατέχει τις πληροφορίες για τις τοποθεσίες αποθήκευσης του αντικειμένου.

- *CAST.* Χρησιμοποιεί multicast επιπέδου εφαρμογής ή τη μέθοδο Any-

cast[29] ώστε η επικοινωνία να είναι κλιμακούμενη ανάλογα με το μέγεθος του δικτύου. Επικεντρώνεται στην επικοινωνία ανάμεσα σε μέλη ομάδων.

Ως προς τη δρομολόγηση του υπερκείμενου δικτύου που σχηματίζεται υπάρχουν μέθοδοι:

- Βασισμένες στις μικρότερες διαθέσιμες δικτυακές διαδρομές, π.χ. στα δίκτυα CAN (Content Addressable Networks) [Ratn01] και Chord [Stoi01].
- Βασισμένες σε τοπικά βελτιστοποιημένους πίνακες δρομολόγησης που ενημερώνονται τακτικά, όπως στα δίκτυα Tapestry [Zhao01] και Pastry [Cast02].

Ένα μεγάλο πλήθος δικτυακών εφαρμογών βασίζεται στη λειτουργικότητα των πιο πάνω συστημάτων προκειμένου να προσφέρει κατανεμημένες υπηρεσίες, π.χ. επικοινωνιών multicast επιπέδου εφαρμογής, αποθήκευσης περιεχομένου (αποκεντρωμένα συστήματα αρχείων) κ.λπ.

Λειτουργία της Συνεργατικής Υποδομής σε δίκτυα peer-to-peer KBR

Τα δομημένα υπερκείμενα (overlay) δίκτυα peer-to-peer είναι ιδιαίτερα δημοφιλή ως πλατφόρμες κατασκευής ανθεκτικών κατανεμημένων συστημάτων μεγάλης

[29] Όλα τα συστήματα που προσφέρουν την υπηρεσία Anycast αποκτούν (ως δευτερεύουσα διεύθυνση IP) την ίδια γνωστή διεύθυνση την οποία διαφημίζουν στη δρομολόγηση. Η διαφήμιση Anycast μπορεί να αφορά μια δικτυακή περιοχή που περιλαμβάνει ακόμα και μόνον μία διεύθυνση (routing prefix /32). Οποιοσδήποτε αναζητήσει το δρόμο προς το σύστημα με αυτή τη διεύθυνση θα το δει (από πλευράς δρομολόγησης) από «πολλούς δρόμους» ("multihomed") και θα επιλέξει το συντομότερο από αυτούς· δηλαδή το πιο κοντινό του σύστημα με τη συγκεκριμένη διεύθυνση Anycast ανάμεσα σε αυτούς που διαφημίζονται με το πρωτόκολλο BGP [Kuro]. Έτσι ένα νέο σύστημα που ζητά να συνδεθεί στο δίκτυο peer-to-peer χρησιμοποιεί τη γνωστή αυτή διεύθυνση και δρομολογείται αυτόματα στον πιο κοντινό του κόμβο.

κλίμακας. Η δομή γράφου που χρησιμοποιούν επιτρέπει την αναζήτηση αντικειμένων με ανταλλαγή $O(logN)$ [Stoi01] μηνυμάτων σε ένα υπερκείμενο δίκτυο με N κόμβους (π.χ. στο δίκτυο peer-to-peer Pastry). Η ενοποιημένη αρίθμηση τόσο για τις διευθύνσεις κόμβων όσο και την κωδικοποιημένη αναπαράσταση του περιεχομένου επιλέχθηκε ως μέθοδος για την οργάνωση της Συνεργατικής Υποδομής και ως μέθοδος ανταλλαγής των μηνυμάτων της.

Από την πλευρά των δικτύων-μελών της Συνεργατικής Υποδομής, σε κάθε κόμβο που προστίθεται, ανατίθεται τυχαία (π.χ. χρησιμοποιώντας το αποτέλεσμα μιας συνάρτησης κατακερματισμού — hash function — που εφαρμόζεται στη διεύθυνση IP της Οντότητας) ένα μοναδικό αναγνωριστικό (nodeID).

Από την πλευρά των περιστατικών DDoS υπάρχει μια σειρά από κύρια χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για την αναγνώριση τους κατά μοναδικό τρόπο:

- Πρωτόκολλο και θύρα της κακόβουλης κίνησης
- Τύπος πακέτων
- Διεύθυνση (ή περιοχή διευθύνσεων) IP του τελικού στόχου

Τα στοιχεία αυτά περιέχονται στα μηνύματα IDMEF που ανταλλάσσουν οι Οντότητες μεταξύ τους. Μέσω της εφαρμογής της κατάλληλης συνάρτησης κατακερματισμού σε αυτά τα στοιχεία, κάθε περιστατικό DDoS μπορεί να αντιστοιχηθεί σε ένα μοναδικό αναγνωριστικό (Globally Unique Identifier — GUID) που παίρνει τιμές στον ίδιο χώρο τιμών με τα αναγνωριστικά των κόμβων του δικτύου peer-to-peer (nodeIDs).

Με την παραγωγή ενός μοναδικού αναγνωριστικού για μια συγκεκριμένη επίθεση DDoS είναι δυνατόν να γίνεται αυτόματα ο διαχωρισμός των αναφορών

που αναφέρονται σε αυτή. Η επαλληλία με τα αναγνωριστικά κόμβων χρησιμοποιείται ώστε όλες οι αναφορές που σχετίζονται μεταξύ τους να δρομολογούνται στον ίδιο κόμβο του δικτύου που θα λειτουργεί ως σημείο συγκέντρωσης τους.

Ο κόμβος που θα επιλεγεί για τη συγκέντρωση των αναφορών θα είναι εκείνος με nodeID «πλησιέστερα» στην τιμή του GUID της επίθεσης και ονομάζεται «κόμβος-ρίζα». Χρησιμοποιείται το «μέτρο εγγύτητας» του (εκάστοτε) δικτύου peer-to-peer που χρησιμοποιείται για τους ενεργούς κόμβους του. Η τεχνική αυτή μιμείται τη λειτουργία «δημοσίευσης περιεχομένου» των δικτύων peer-to-peer. Εναλλακτικά, κόμβοι με κοντινά nodeIDs μπορούν να αποτελέσουν επίσης εναλλακτικά (δευτερεύοντα) σημεία συγκέντρωσης των πληροφοριών επίθεσης.

Με τον τρόπο επιλογής αναγνωριστικών κόμβων και περιστατικών επιτυγχάνεται:

- Ο κόμβος-ρίζα να μη σχετίζεται άμεσα με το μονοπάτι της επίθεσης (και άρα να μην επηρεάζεται αρνητικά από την επίθεση αυτή).
- Η συνγκέντρωση πληροφοριών για κάθε επίθεση αναλαμβάνεται από διαφορετικό δίκτυο-κόμβο (ή κόμβους).
- Ο κόμβος συγκέντρωσης πληροφοριών είναι γενικά γνωστός σε κάθε κόμβο που θέλει να αποστείλει αναφορά χωρίς τη χρησιμοποίηση μιας κεντρικής υπηρεσίας διανομής της πληροφορίας. Η διανομή των μηνυμάτων προς αυτόν αναλαμβάνεται από την υποδομή peer-to-peer.

Στην προηγούμενη περίπτωση (τμήμα 3.4.2) το υπερκείμενο δίκτυο peer-to-peer χρησιμοποιήθηκε μόνο για να παρέχει μια υποδομή μεταφοράς των μηνυμάτων των δικτύων-μελών, και ο κόμβος RP έχει βασική λειτουργικότητα συγκέντρωσης στοιχείων. Στην περίπτωση των δικτύων peer-to-peer που χρησιμοποιούν

Δρομολόγηση Βασισμένη σε Κλειδί, η Οντότητα στον κόμβο-ρίζα (ή ακόμα και κάποιο διαφορετικό σύστημα) συγκεντρώνει τα στοιχεία της επίθεσης. Επιπλέον υπάρχει δυνατότητα για εξάπλωση των σημείων συλλογής στοιχείων στο χώρο του Διαδικτύου.

Η καθ' αυτή δρομολόγηση των μηνυμάτων αναλαμβάνεται από το ίδιο το δίκτυο peer-to-peer. Τα μηνύματα που συγκεντρώνονται στη συνέχεια στον κόμβο-ρίζα περιέχουν επιπλέον πληροφορίες που έχουν συλλέγει τοπικά σε κάθε επιμέρους δίκτυο-μέλος της Συνεργατικής Υποδομής. Ένα σημαντικό τμήμα αυτής είναι η πληροφορία μονοπατιού που συγκεντρώνεται από πολλές πηγές. Κάθε ένα δίκτυο-μέλος της Υποδομής παρέχει ένα μικρό τμήμα του μονοπατιού (αυτό το οποίο γνωρίζει).

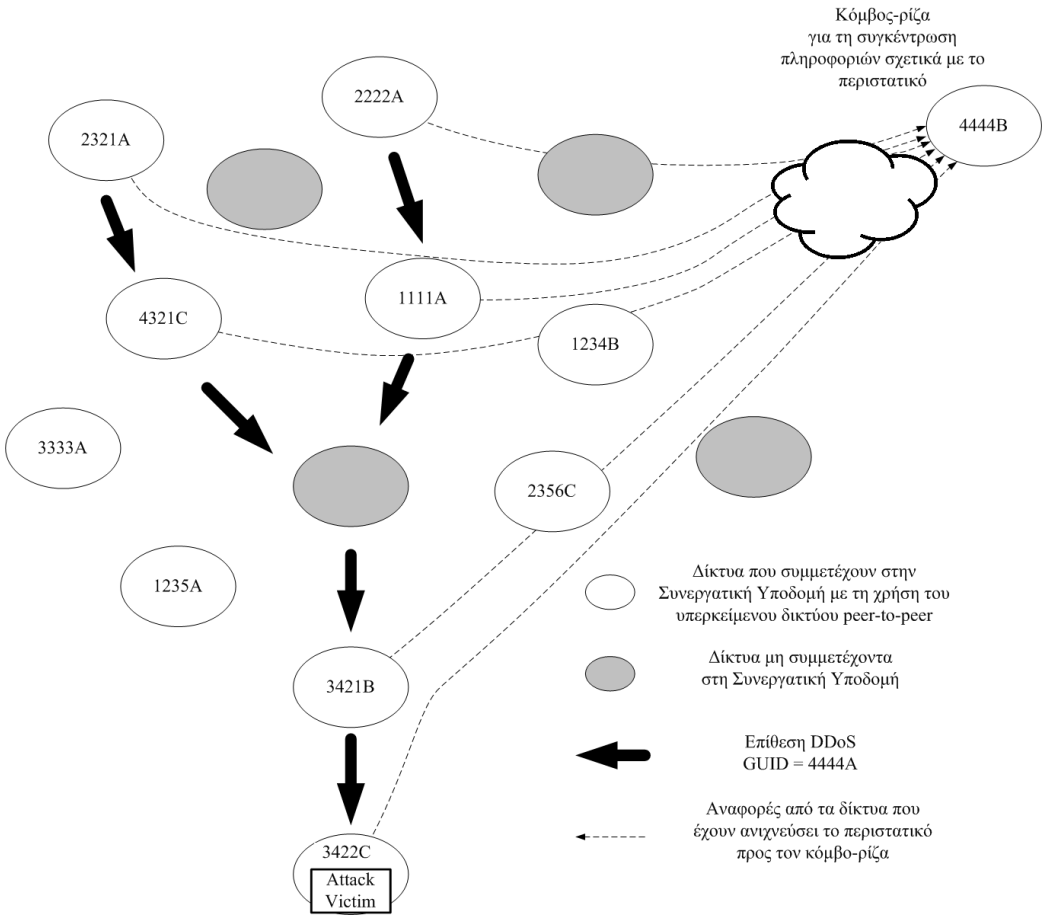
Κατά τον ίδιο τρόπο που γίνεται η συγκέντρωση πληροφοριών για μια επίθεση DDoS σε ένα κόμβο-ρίζα, είναι δυνατή και η ανάκτηση τους από αυτόν. Γίνεται η υπόθεση ότι ένας κόμβος του δικτύου peer-to-peer θα αναζητήσει αυτή την πληροφορία εφόσον έχει ήδη, σε κάποιο βαθμό τουλάχιστον, ανιχνεύσει την επίθεση, οπότε θα γνωρίζει τα χαρακτηριστικά βάσει των οποίων θα μπορεί να κάνει την αναζήτηση στον αντίστοιχο κόμβο-ρίζα.

Ως προς αυτές τις συγκεντρωμένες πληροφορίες επίθεσης υπάρχουν δύο εναλλακτικές προσεγγίσεις:

- Ο κόμβος-ρίζα να επεξεργάζεται όλες τις εισερχόμενες πληροφορίες (κυρίως τα επιμέρους τμήματα του μονοπατιού) προκειμένου να παρέχει κατά το δυνατόν πληρέστερη απεικόνιση της επίθεσης.

- Η εργασία αυτή (του συνδυασμού) να επαφίεται στους κόμβους που θα αναζητήσουν τις συγκεντρωμένες πληροφορίες.

Στο Σχήμα 3.7 παρουσιάζεται ενδεικτικά η συγκέντρωση αναφορών για μια συγκεκριμένη επίθεση, όπως περιγράφηκε.



Σχήμα 3.7: Λειτουργία PUT τοποθέτησης αναφορών από τα δίκτυα-μέλη της Συνεργατικής Υποδομής στον αντίστοιχο κόμβο-ρίζα nodeID το πιο «κοντινό» προς το GUID (Globally Unique Identifier) του περιστατικού.

Θέματα που προκύπτουν με τη λύση peer-to-peer KBR

Εξετάζοντας το μοντέλο peer-to-peer υπάρχει μια σειρά από συγκεκριμένα σημεία[30] όπου πρέπει να εξασφαλιστεί ότι δεν αποτελούν κύριες αδυναμίες που μπορεί να οδηγήσουν στη διακοπή λειτουργίας ολόκληρου του συστήματος. Πιο συγκεκριμένα:

Γνωρίζοντας τις πραγματικές διευθύνσεις IP των συστημάτων που θα αναλάβουν τη διαχείριση ενός περιστατικού ένας επιτιθέμενος θα μπορούσε να παρακολουθήσει τη δικτυακή κίνηση από και προς αυτά, με σκοπό να ανακαλύψει έναν αριθμό από Συνεργατικές Οντότητες εντός της Υποδομής και στη συνέχεια να επιτεθεί σε αυτές. Πιστεύεται ότι η μεγάλη διασπορά που προσφέρει η μέθοδος, σε συνδυασμό με το μεγάλο αριθμό συμμετεχόντων δικτύων θα καθυστερήσει σημαντικά απ' ευθείας επιθέσεις απόκτησης ελέγχου των συστημάτων των Οντοτήτων κάνει δε απαγορευτική την ταυτόχρονη επίθεση σε όλα με επιθέσεις DDoS. Επιπλέον η αξιοπιστία των δικτύων peer-to-peer και η δυνατότητα επίλυσης προβλημάτων που παρουσιάζονται είναι σημαντικός παράγοντας για τη συνέχιση της λειτουργίας του δικτύου.

Η όλη προσέγγιση για να είναι επιτυχής θα χρειαστεί να τύχει ευρείας αποδοχής. Αυτό είναι ένα πρόβλημα που παρουσιάζουν και όλες οι υπόλοιπες προτάσεις αντιμετώπισης των επιθέσεων DDoS που αφορούν συνεργασίες μεγάλης κλίμακας.

Υλοποίηση Πρωτοτύπου

Η αναφερόμενη ανωτέρω προσέγγιση δοκιμάστηκε στην πράξη με τη δημιουργία και πειραματική δοκιμή ενός πρωτοτύπου που βασίστηκε στο σύστημα KBR

[30] Γενικότερα θέματα ασφάλειας καλύπτονται στο τμήμα 3.5.

Bamboo [Bamb05]. Πρόκειται για ένα σύστημα που υλοποιεί ένα Κατανεμημένο Πίνακα Κατακερματισμού (DHT) και είναι σχεδιασμένο ώστε να είναι ανθεκτικό στις συχνές εισόδους και αποχωρίσεις κόμβων από το υπερκείμενο δίκτυο. Το τελευταίο χαρακτηριστικό είναι ιδιαίτερα χρήσιμο στην περίπτωση εγκατάστασης της Συνεργατικής Οντότητας σε μεγάλη κλίμακα. Στο πρωτότυπο, στα πλαίσια της διπλωματικής εργασίας [Λεβα05] υλοποιούνται τα εξής στοιχεία:

- Επιτυγχάνεται η δημιουργία και οργάνωση του βασικού υπερκείμενου δικτύου peer-to-peer με τη χρήση του συστήματος Bamboo.
- Λειτουργία PUT: Για ένα περιστατικό υπολογίζεται το GUID[31] από τα χαρακτηριστικά του και στη συνέχεια τα στοιχεία που το αφορούν στέλνονται μαζί με την τοπική (μερική) εικόνα του μονοπατιού στον αντίστοιχο κόμβο-ρίζα (όπου nodeID κοντινό προς το GUID του περιστατικού). Τα στοιχεία από έναν αριθμό από αναφορές αποθηκεύονται στον κόμβο-ρίζα για το περιστατικό.
- Εφαρμόζεται η λειτουργία GET για την απόκτηση από ένα από τα μέλη της Συνεργατικής Υποδομής της συνολικής πληροφορίας που έχει συγκεντρωθεί από τον κόμβο-ρίζα. Στη συνέχεια γίνεται μερική ανασύνθεση του μονοπατιού της επίθεσης με έναν αλγόριθμο σχηματισμού του πλήρους δένδρου μέσω του συνδυασμού κοινών κόμβων στις επιμέρους αναφορές.

[31] Στο σύστημα Bamboo χρησιμοποιείται η συνάρτηση κατακερματισμού SHA-1

Συμπεράσματα για τα δίκτυα peer-to-peer KBR

Από τη θεωρητική ανάλυση αλλά και την υλοποίηση του πρωτοτύπου προκύπτουν τα εξής συμπεράσματα για τη χρήση δικτύων peer-to-peer KBR ως υπόβαθρο της Συνεργατικής Αρχιτεκτονικής:

- Δίδεται η δυνατότητα δημιουργίας αξιόπιστης δικτυακής υποδομής (overlay) με ευρύτατη γεωγραφική εξάπλωση (έως και πλήρη κάλυψη του Διαδικτύου). Άρα παρέχεται η δυνατότητα εκμετάλευσης περιστατικών που μπορεί να λάβουν χώρα σε δίκτυα μακριά από το τελικό θύμα. Αντίθετα, οι λύσεις Multicast και peer-to-peer μικρής κλίμακας περιορίζονται σε τοπικές ομαδοποιήσεις δικτύων, συνήθως περιορισμένης εμβέλειας.

- Τα σημεία αναγνώρισης της διαδρομής θα είναι ιδιαίτερα διευρυμένα επειδή συγκεντρώνονται στοιχεία από όλο το Διαδίκτυο. Υπάρχει η δυνατότητα να οδηγήσουν κοντινότερα προς τα δίκτυα πηγές της επίθεσης ή ακόμα και να επιτευχθεί σαφής ανίχνευση τους.

- Παρέχει τη δυνατότητα διασποράς κρίσιμων συστημάτων στόσο γεωγραφικά όσο και σε επίπεδο διευθύνσεων IP (διαφορετικά domains). Με τον τρόπο αυτό δυσχεραίνεται η ταυτόχρονη εξουδετέρωση κρίσιμων σημείων λειτουργίας της υποδομής.

- Ο σχεδιασμός και η εξέλιξη των δικτύων peer-to-peer είναι τέτοια ώστε αυτά να μπορούν να υποστούν αλλαγές στους συμμετέχοντες κόμβους ή στις διόδους επικοινωνίας τους χωρίς ιδιαίτερο αντίκτυπο στη λειτουργία τους. Στην αρχιτεκτονική peer-to-peer δεν υπάρχουν ουσιαστικά διακοπές συνδέσεων: η κοινότητα αναδιαρθρώνεται συνεχώς και φροντίζει η

ίδια για τη συνδεσιμότητα της.

- Με την οργάνωση της Συνεργατικής Υποδομής κατά το πρότυπο των δικτύων peer-to-peer, το τμήμα οργάνωσης του δικτύου και της επικοινωνίας σε αυτό είναι δυνατόν να διαχωριστεί από το τμήμα της αντίδρασης σε περιστατικά. Θεωρητικά, είναι δυνατόν να επεκτείνουμε την αρχιτεκτονική σε πολλαπλούς κόμβους συλλογής στοιχείων (π.χ. με την τοποθέτηση τους σε κάθε τοπικό δίκτυο) που ταυτόχρονα θα χρησιμοποιούνται για την επικοινωνία, προσφέροντας αυξημένη αξιοπιστία.

- Η υλοποίηση της λύσης μπορεί να βασιστεί στη μεγάλη πληθώρα έτοιμου (και δωρεάν) λογισμικού που υπάρχει διαθέσιμο. Πιο συγκεκριμένα, εργασία στο πρωτότυπο έδειξε ότι η τροποποίηση υπάρχοντος λογισμικού ώστε υλοποιεί λειτουργικότητα της συνεργατικής Αρχιτεκτονικής είναι σχετικά απλή. Η χρήση του λογισμικού αυτού μπορεί να οδηγήσει σε ένα σταθερό δίκτυο που λειτουργεί κατά το ζητούμενο τρόπο. Επιπλέον, λόγω της απλότητας του λογισμικού, διευκολύνεται η εγκατάσταση της Αρχιτεκτονικής σε μεγάλη κλίμακα (με απλή εγκατάσταση και ενεργοποίηση[32])

- Η λύση μπορεί να υλοποιηθεί σε μεγάλη κλίμακα με την ίδια ευκολία που λειτουργεί ένα δίκτυο peer-to-peer με πολλούς ανεξάρτητους και ευρύτατα κατανεμημένους κόμβους. Σε σχέση με άλλες παρόμοιες προσεγγίσεις μεγάλης κλίμακας δεν παρεμβαίνει στην πολιτική διοίκησης (governance) του Διαδικτύου (ICANN, IETF κ.λπ). Θα μπορούσε έτσι να αποτελέ-

[32] Φυσικά με τον όρο ότι ισχύουν οι προβλέψεις για ασφαλή συνεργασία, όπως αναφέρονται στο τμήμα 3.5

σει και υπηρεσία προσφερόμενη εμπορικά από τους μεγάλους παρόχους (ISPs) ή να «χτιστεί» πάνω σε μια *ad-hoc* συνεργασία (με την απλή εγκατάσταση του αντίστοιχου λογισμικού ανεξάρτητα από τη φυσική τοπολογία του Διαδικτύου).

- Αναφορές μικρής σημασίας ή βεβαιότητας αντί να αγνοούνται συγκεντρώνονται και μπορούν να συνεισφέρουν στην ανίχνευση επιθέσεων μικρού αντίκτυπου (πιθανά τμήματα γενικότερων επιθέσεων).

- Πολλά διαφορετικά ταυτόχρονα περιστατικά δε θα προκαλέσουν υπερφόρτωση του δικτύου ή ενός μοναδικού συστήματος. Αντιθέτως, είναι δυνατή η διαχείριση και επιθέσεων με μεγάλη πολυπλοκότητα στην κίνηση που παράγουν. Τα επιμέρους δίκτυα κόμβοι μπορούν να αναζητήσουν (πολλά διαφορετικά) στοιχεία που αφορούν ένα περιστατικό που έχουν ανιχνεύσει σε πρώτο στάδιο και να ανακατασκευάσουν τα ίδια το δένδρο της επίθεσης για κάθε ένα από τα είδη κίνησης που χρησιμοποιούνται.

3.4.4 Περιβάλλοντα «Πλέγματος» (Grid)

Τα υπολογιστικά περιβάλλοντα «Πλέγματος» (τύπου Grid) χρησιμοποιούνται σήμερα σε ευρεία κλίμακα για την δημιουργία υποδομών διαμοιραζόμενων υπολογιστικών πόρων. Τα ίδια περιβάλλοντα, κάνοντας χρήση κοινών προγραμματιστικών υποδομών, όπως π.χ. τα Web Services, είναι σε θέση να χρησιμοποιηθούν και ως ένα κατανεμημένο περιβάλλον επικοινωνίας. Το περιβάλλον Grid σε ρόλο Ενδιάμεσου Λογισμικού (Middleware), παρέχει ένα κοινό πλαίσιο ελέγχου και επιτρέπει τη μετάβαση σε πλήρως αποκεντρωμένη λειτουργία.

Χαρακτηριστικό τέτοιο παράδειγμα αποτελεί το έργο GRID CC [Grid05],

κύριο αντικείμενο του οποίου αποτελεί η δοκιμή σε σχεδόν «πραγματικό-χρόνο» ενός Grid Middleware ως μέσο για την παρακολούθηση και τον έλεγχο «εικονικών» (virtual) οργάνων (υπό την έννοια της «διαφάνειας» τοποθέτησης και λεπτομερειών λειτουργίας). Η υποδομή Grid χρησιμοποιείται για να μεταφέρει πληροφορίες από, ή προς τα επιστημονικά όργανα (π.χ. επιταχυντές στοιχειωδών σωματιδίων). Οι ελεγκτές των οργάνων αυτών δέχονται εντολές για την εκτέλεση πειραμάτων από διάφορα κέντρα ελέγχου και μεταβιβάζουν τα στοιχεία που συγκεντρώνουν πίσω σε αυτά. Η κατανεμημένη ανίχνευση δικτυακών ανωμαλιών αποτελεί ένα επίσης αντικείμενο έρευνας στο έργο.

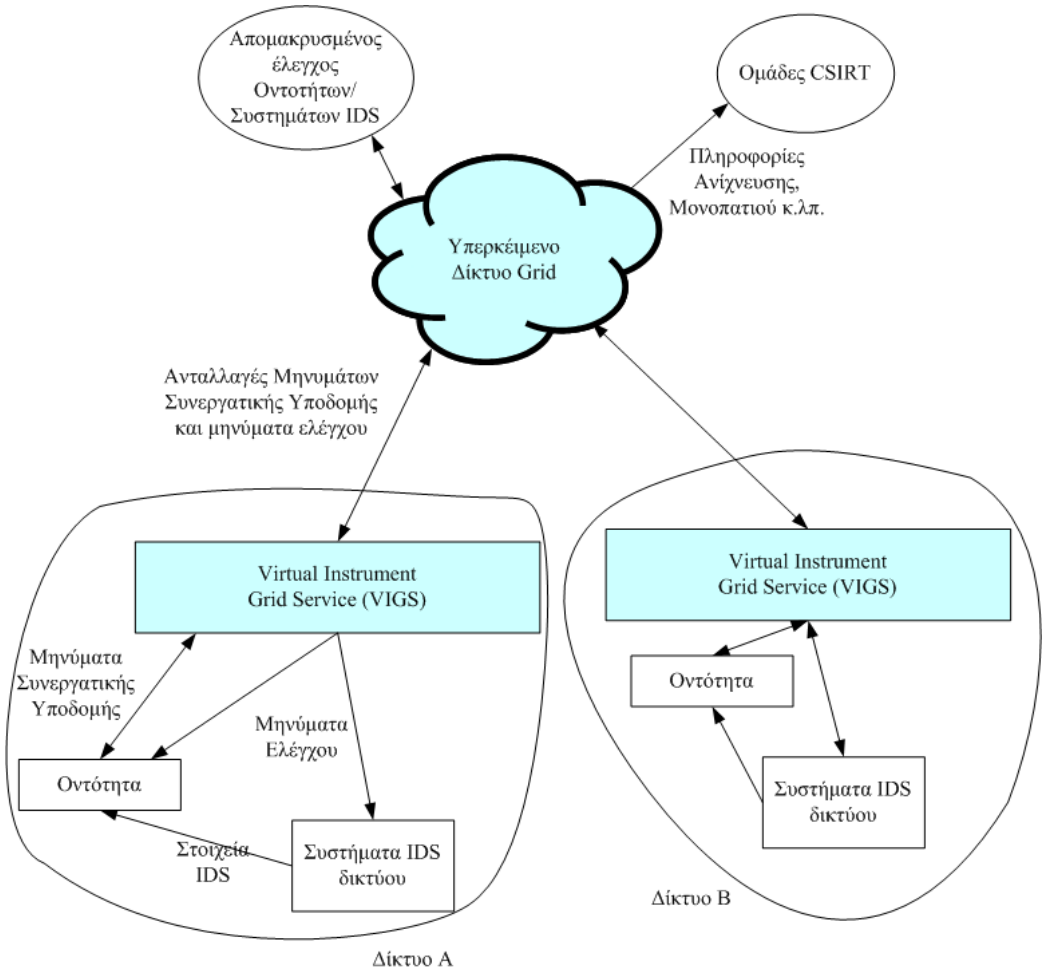
Κατά αντίστοιχο τρόπο ένα δίκτυο Grid μπορεί να αποτελέσει μια εντελώς αυτόματη αποκεντρωμένη πλατφόρμα, κατάλληλη για την υλοποίηση της λύσης της Συνεργατικής Υποδομής. Προς την κατεύθυνση αυτή, οι προδιαγραφές WSRF (Web Services Resource Framework) [Glob05] στα Grids παρέχουν τη δυνατότητα για την αυτόματη κατανομή πόρων (υπολογιστικών ή άλλων). Τα μηνύματα σε XML που ανταλλάσσονται στα πλαίσια της Συνεργατικής Υποδομής μπορεί εύκολα να ενσωματωθούν σε σχήματα Web Services που θα επιτρέψουν την αυτόματη επεξεργασία τους. Θέματα επιβεβαίωσης της ταυτότητας των συνεργαζόμενων μερών και της αυθεντικότητας των μηνυμάτων αναλαμβάνονται από την υπάρχουσα υποδομή των δικτύων Grids.

Το προτεινόμενο κατανεμημένο σύστημα παρέχει τη δυνατότητα συγκέντρωσης πληροφοριών από πολλά σημεία και (μερικής τουλάχιστον) ανασύνθεσης του μονοπατιού επίθεσης. Η λειτουργία των Οντοτήτων συνεργαζόμενων δικτύων μπορεί εντούτοις να παραμείνει η ίδια.

Μια τέτοια προσέγγιση έχει αποτελέσει μέρος της πρότασης [Magl05], που αναφέρεται στη σύνθεση δεδομένων ανίχνευσης από πολλά δίκτυα, με μαθημα-

τική βάση, π.χ. με αλγορίθμους Data Fusion [Siat04]. Για το τμήμα της που αφορά στην ανταλλαγή στοιχείων χρησιμοποιεί την προσέγγιση της Συνεργατικής Υποδομής πάνω από ένα δίκτυο Grid.

Μια αποτύπωση της πιθανής χρήσης ενός περιβάλλοντος Grid για την Συνεργατική Υποδομή παρουσιάζεται στο Σχήμα 3.8. Σε αυτό φαίνεται η χρήση των "instrument elements" (που έχουν αναπτυχθεί από το GRID CC) ως μέσον τόσο για την διεκπεραίωση των επικοινωνιών μεταξύ των Οντοτήτων όσο και για τον απομακρυσμένο έλεγχο των Οντοτήτων και συστημάτων IDS σε ένα δίκτυο. Το τελευταίο στοιχείο παρέχει τη δυνατότητα για επιπλέον λειτουργικότητα σε περίπτωση που τα δίκτυα δεχτούν να παραχωρήσουν τον έλεγχο αυτό σε μια κοινά αποδεκτή αρχή. Επίσης το υπόβαθρο Grid μπορεί να μεταφέρει πληροφορίες προς έμπιστους τρίτους, όπως ομάδες αντιμετώπισης περιστατικών CSIRT (Computer Security Incident Response Teams).



Σχήμα 3.8: Χρήση του περιβάλλοντος Grid ως υπόβαθρο λειτουργίας της Συνεργατικής Υποδομής

3.5 Αξιολόγηση της Αρχιτεκτονικής ως προς την Ασφάλεια και Αξιοπιστία

Καίρια ζητήματα που επηρεάζουν την ασφαλή και αξιόπιστη λειτουργία της αρχιτεκτονικής είναι:

(i) Υποκλοπή μηνυμάτων

Με μέσα επικοινωνίας, όπως για παράδειγμα το IP Multicast τα μηνύματα περνούν μέσα από «δημόσια» κανάλια που οποιοσδήποτε μπορεί να ακούσει χωρίς να χρειαστεί να υποκλέψει άμεσα τις επικοινωνίες. Ένας επιτιθέμενος θα μπορούσε να «συντονιστεί στο κατάλληλο κανάλι» multicast και να παρακολουθεί τις αντιδράσεις του Υπερκείμενου Δικτύου. Στη συνέχεια, όταν αντιληφθεί ότι η επίθεση ανιχνεύτηκε, ανταλλάσσονται μηνύματα και λαμβάνονται μέτρα να στείλει τις κατάλληλες εντολές στα συστήματα που ελέγχει και εκτελούν την επίθεση ("bots") ώστε να αλλάξουν τα χαρακτηριστικά της, αποφεύγοντας τυχόν αμυντικά μέτρα. Κατά τον ίδιο τρόπο θα ήταν δυνατόν να εισάγει πλαστά Alerts τα οποία να περιγράφουν ανύπαρκτα περιστατικά. Αυτά με τη σειρά τους μπορούν να ενεργοποιήσουν αντιδράσεις στις Οντότητες παρεμποδίζοντας έτσι τη νόμιμη κίνηση. Καθαρά σε επίπεδο multicast το πρόβλημα μπορεί να αντιμετωπιστεί με τη χρήση ελέγχου πρόσβασης στα κανάλια που χρησιμοποιούνται. Τέτοιος έλεγχος προσφέρεται με τη χρήση του «Ασφαλούς Multicast» (Secure Multicast) [Perr00] στο οποίο γίνεται επιβεβαίωση της ταυτότητας (authentication) για να επιτραπεί η σύνδεση στα κανάλια. Μια επιπλέον λύση παρέχεται με τη χρήση κρυπτογραφίας και επιβεβαίωσης της ταυτότητας μέσο ψηφιακών πιστοποιητικών, προβλέπεται από την αρχιτεκτονική και περιγράφεται

στη συνέχεια.

(ii) Πιθανότητα διείσδυσης ενός επιτιθέμενου στην αρχιτεκτονική

Ένα τέτοιο περιστατικό μπορεί να έχει σαν αποτέλεσμα είτε την υποκλοπή των επικοινωνιών είτε τη δημιουργία ψευδών αναφορών. Ειδικά το τελευταίο ενδεχόμενο θα μπορούσε να χρησιμοποιηθεί για να οδηγήσει στη δημιουργία προβλημάτων σε νόμιμη κίνηση. Πέραν αυτών η κάθε Συνεργατική Οντότητα έχει δικαιώματα επιβολής κανόνων στα πλαίσια ενός δικτύου. Η πιθανότητα ανασφαλούς λειτουργίας της μηδενίζει την οποιαδήποτε χρησιμότητα μπορεί να έχει στην αντιμετώπιση κάποιου πραγματικού περιστατικού.

Τα θέματα ασφαλείας επικοινωνιών αντιμετωπίζονται θέτοντας συγκεκριμένες προδιαγραφές για τη λειτουργία της αρχιτεκτονικής. Πιο συγκεκριμένα όλες οι επικοινωνίες προβλέπεται να είναι κρυπτογραφημένες (προστασία από υποκλοπή) με την ταχεία μέθοδο του «συμμετρικού κλειδιού» (symmetric key cryptography)[33]. Η Συνεργατική Υποδομή, στη γενική περίπτωση, αφορά ένα συγκεκριμένο και σχετικά μικρό αριθμό συμμετεχόντων δικτύων οπότε η διαδικασία ανταλλαγής του κλειδιού που θα χρησιμοποιηθεί δεν είναι ιδιαίτερα δύσκολη διαδικασία. Για μεγαλύτερο αριθμό συμμετεχόντων (όπως στην περίπτωση γενικευμένης χρήσης ενός δικτύου peer-to-peer) είναι δυνατόν να χρησιμοποιηθεί ένας συνδυασμός εξυπηρετητών διανομής κλειδιών (με εξασφάλιση SSL) και ψηφιακών πιστοποιητικών για την επιβεβαίωση της ταυτότητας των μερών που θα παραλάβουν τα κλειδιά. Πιθανά η διαδικασία έκδοσης αυτών των πιστοποιητικών θα μπορούσε να αναληφθεί και από ομάδες CERT και η αναγκαία εμπιστοσύνη να στηριχθεί στις σχέσεις μεταξύ τους. Η μέθοδος αυτή

[33] Στην υλοποίηση το πρωτοτύπου χρησιμοποιείται τον αλγόριθμο DES

προφανώς θα παρέχει μεγαλύτερη ασφάλεια εφόσον το κάθε κλειδί συμμετρικής κρυπτογραφίας θα έχει χρήση για περιορισμένο χρονικό διάστημα.

Κάθε μήνυμα διαθέτει επίσης επιβεβαίωση της ταυτότητας του αποστολέα με τη χρήση ψηφιακής υπογραφής (προστασία από την εισαγωγή πλαστογραφημένων μηνυμάτων). Η ψηφιακή υπογραφή εισάγεται εύκολα στο σώμα του μηνύματος στα πλαίσια της κωδικοποίησης κατά XML. Είναι δυνατόν να χρησιμοποιηθούν είτε απλά σχήματα δημόσιου-ιδιωτικού κλειδιού (με τη διανομή των δημόσιων κλειδιών με κάποια ασφαλή μέθοδο), είτε ψηφιακά πιστοποιητικά εκδιδόμενα από κάποια γενικά έμπιστη Αρχή Πιστοποίησης (Certification Authority — CA).

Πειραματικά, έχει υλοποιηθεί η μετατροπή των εξόδων ενός τυπικού συστήματος IDS, όπως το Snort, σε μηνύματα XML, δομημένα κατά το IDMEF. Επίσης είναι δυνατόν να προστεθεί σε αυτά εξωτερική (encapsulating) πληροφορία επιβεβαίωσης του αποστολέα, της ακεραιότητας του μηνύματος και του χρόνου αποστολής με τη χρήση ψηφιακών πιστοποιητικών, κρυπτογραφίας και συναρτήσεων κατακερματισμού (hash functions) [Ανδρ03].

Τέλος, στο σώμα των μηνυμάτων εισάγεται και χρονοσήμανση που προστατεύει από την αναπαραγωγή παλαιότερων μηνυμάτων. Είναι προαπαιτούμενος ο χρονικός συγχρονισμός όλων των Οντοτήτων (π.χ. με το πρωτόκολλο ntp).

Πέρα της όποιας προστασίας παρέχει ένα τέτοιο σχήμα η Συνεργατική Αρχιτεκτονική έχει μια επιπλέον ουσιαστική προστασία στον τρόπο που λειτουργεί: οι παραπλανητικές αναφορές (ειδικά από έναν αποστολέα) θα έχουν συνολικά πολύ μικρό βάρος μέσα στο μεγάλο πλήθος αναφορών που θα υπάρξουν συνολικά. Το σύστημα αυτό λειτουργεί τόσο καλύτερα όσο περισσότεροι συμμετέχοντες υπάρχουν στην Υποδομή.

(iii) Περίπτωση παραβίασης ή απώλειας μιας Οντότητας

Ολόκληρη η Συνεργατική Υποδομή βασίζεται στη λειτουργία των Οντοτήτων. Αποτελούν έτσι κρίσιμα σημεία (points of failure). Το θέμα αντιμετωπίζεται από το σχεδιασμό της ίδιας της Συνεργατικής Οντότητας. Αποτελώντας μια ελαφριά, αρθρωτή (modular) και μεταφέρσιμη πλατφόρμα λογισμικού μπορεί να εισαχθεί σε ένα περιβάλλον διαχείρισης ασφαλείας ενός δικτύου και να μεταφερθεί σε κάποιο νέο σύστημα σε περίπτωση αστοχίας υλικού (hardware) του συστήματος. Χάρη στη αρθρωτή της αρχιτεκτονική[34] τμήματα της μπορούν να διακόψουν τη λειτουργία τους σε περιπτώσεις προβλήματος ή αναβάθμισης χωρίς να επηρεάσουν το σύνολο. Σε όλες τις περιπτώσεις διαφορετικών επικοινωνιακών υποβάθρων (multicast, peer-to-peer κ.λπ.) υπάρχει η δυνατότητα παράλληλης λειτουργίας περισσοτέρων της μιας Οντότητες σε ένα δίκτυο. Οι «δευτερεύουσες» Οντότητες παρακολουθούν τα μηνύματα του Υπερκείμενου Δικτύου, γνωρίζουν την κατάσταση της κύριας και είναι δυνατόν να αναλάβουν το ρόλο της εφόσον παραστεί ανάγκη.

Μεγαλύτερο πρόβλημα ενδέχεται να προκαλέσει η απόκτηση ελέγχου ενός κόμβου από μη εξουσιοδοτημένους (κακόβουλους) τρίτους. Μια τέτοια παραβίαση εγείρει μια σειρά από ενδεχόμενα:

- Παρακολούθηση των επικοινωνιών του κόμβου και σταδιακή εκμάθηση όλων των άλλων κόμβων της Συνεργατικής Υποδομής με απώτερο σκοπό τη συνολική επίθεση σε αυτούς. Η Συνεργατική Οντότητα ως πλατφόρμα λογισμικού είναι «μεταφέρσιμη» (portable) σε πολλές διαφορετικές υπολογιστικές αρχιτεκτονικές αποκλείοντας την αξιοποίηση της ίδιας αδυ-

[34] Πρόκειται για τη φιλοσοφία των προγραμματιστικών διεργασιών (autonomous agents) [Cros95] [Spaf00].

ναμίας για πρόσβαση σε όλους τους κόμβους. Επιπλέον, το πλήθος τους αποκλείει την επιτυχία μιας ταυτόχρονης επίθεσης DDoS σε όλες.

- Πρόσβαση στα κλειδιά επικοινωνίας που θα φέρει τον επιτιθέμενο σε θέση να δημιουργεί παραποιημένα μηνύματα και να εισάγει στην κοινότητα ψευδείς πληροφορίες για τη διαδρομή της επίθεσης. Το ενδεχόμενο αυτό εξετάζεται στη συνέχεια.

Αντίστοιχα προβλήματα μπορεί να προκύψουν για τον κόμβο που θα αναλάβει το ρόλο του σημείου συγκέντρωσης πληροφορίας στην περίπτωση peer-to-peer. Το πρόβλημα της μη διαθεσιμότητας ενός τέτοιου κόμβου λύνεται με την ανάθεση των καθηκόντων, αυτόματα σε κάποιον άλλο της ομαδοποίησης.

(iv) Η πιθανότητα αποστολής ψευδών αναφορών από κάποιο παραβιασμένο κόμβο του Συνεργατικού Δικτύου

Το ενδεχόμενο παραβίασης μιας Οντότητας μπορεί να οδηγήσει στην κακόβουλη χρησιμοποίηση της ώστε να αποστέλλονται (καθ' όλα νόμιμες) ψευδείς αναφορές στο Συνεργατικό Δίκτυο. Τέτοιες αναφορές μπορεί να έχουν σα σκοπό τη δημιουργία βεβαιότητας για την ύπαρξη συγκεκριμένου περιστατικού το οποίο θα μπορούσε να οδηγήσει σε ενέργειες παρεμπόδισης νόμιμης κίνησης. Ένας από τους σκοπούς της χρήσης «ψηφοφορίας με βάρη» για την κατάληξη στη διαπίστωση ενός περιστατικού είναι η προστασία από επιθέσεις τέτοιας μορφής. Μία Οντότητα απαιτεί πλήθος μηνυμάτων (τοπικά και από εξωτερικές πηγές) περισσότερα του ενός προκειμένου να περάσει σε καταστάσεις ενεργοποίησης. Ειδικότερα τα βάρη που ανατίθενται στα μηνύματα κάθε κόμβου, αντικατοπτρίζουν την εμπιστοσύνη του παραλήπτη σε αυτό. Χαμηλό επίπεδο

ασφάλειας σε ένα δίκτυο (που μπορεί να οδηγήσει σε παραβίαση) αντιστοιχίζεται σε χαμηλή σημασία μηνυμάτων από αυτό και κατ' επέκταση σε μικρή συνεισφορά στο τελικό συμπέρασμα.

(v) Εμπιστοσύνη στις αυτόματες ενέργειες της Οντότητας

Κάθε επέμβαση της Συνεργατικής Οντότητας σε ένα δίκτυο είναι απόλυτα ελεγχόμενη από προκαθορισμένες πολιτικές ασφαλείας. Ο διαχειριστής του δικτύου είναι σε θέση να γνωρίζει τις ενέργειες που υλοποιούνται ανά πάσα στιγμή μέσο της σύνδεσης της με τα διαχειριστικά εργαλεία. Παρά την αυτόματη λειτουργία της είναι ανά πάσα στιγμή δυνατόν να τροποποιηθούν οι παράμετροι λειτουργίας της (κατ' επέκταση η «ψηφοφορία με βάρη» για την διαπίστωση περιστατικών και τα «κατώφλια βεβαιότητας» για την ανάληψη ενεργειών) ή να αναιρεθούν ενέργειες της. Οι καθ' αυτές ενέργειες αναχαίτισης μιας επίθεσης είναι εκ των προτέρων καθορισμένες, σε συμφωνία με την πολιτική ασφαλείας του δικτύου και πάντα σε συγκεκριμένα χρονικά πλαίσια. Η Οντότητα επιλέγει κάποιες από τις συγκεκριμένες διαθέσιμες περιπτώσεις αντίδρασης. Όλες οι ενέργειες που αναλαμβάνονται από την Οντότητα τέλος έχουν συγκεκριμένη χρονική διάρκεια ισχύος.

(vi) Επίθεση προς το δίκτυο που υποστηρίζει τις επικοινωνίες υποβάθρου για τη Συνεργατική Αρχιτεκτονική (π.χ. IP Multicast)

Ειδική εξέταση πρέπει να γίνει για τις επιπτώσεις κάποιας επίθεσης DDoS εναντίον ενός από τα δίκτυα που συμμετέχουν στη Συνεργατική Υποδομή υπό αυτό το σχήμα επικοινωνίας. Μια τέτοια επίθεση μπορεί να απευθύνεται είτε προς ένα από τα δίκτυα φύλλα του Υπερκείμενου Δικτύου (πιο συνηθισμένη

περίπτωση), είτε προς κάποιο από τα δίκτυα κορμού. Στην πρώτη περίπτωση οι επιθέσεις έχουν συνήθως σημαντικές επιπτώσεις και υπάρχει σοβαρό ενδεχόμενο διακοπής της επικοινωνίας συνολικά[35]. Το γεγονός όμως ότι πρόκειται για δίκτυο φύλλο αποκλείει αυτό το περιστατικό να έχει ευρύτερες επιπτώσεις στις επικοινωνίες του Υπερκείμενου Δικτύου. Η επικοινωνία με τη Συνεργατική Οντότητα στο δίκτυο στόχο θα διακοπεί αλλά ταυτόχρονα το υπόλοιπο Υπερκείμενο Δίκτυο θα προειδοποιηθεί άμεσα για το περιστατικό (από τη διακοπή των μηνυμάτων κανονικής λειτουργίας — "heartbeats") ακόμα και αν αυτό δεν έχει ανιχνευτεί οπουδήποτε αλλού. Στη δεύτερη περίπτωση, που η επίθεση θα έχει ως στόχο κάποιο δίκτυο κορμού, λόγω των συνδέσεων μεγάλης χωρητικότητας αυτών όπως και των εναλλακτικών διαδρομών δεν αναμένεται να υπάρχει πρόβλημα. Η επίθεση θα πρέπει να στοχεύει κάποιο συγκεκριμένο σημείο του δικτύου προκειμένου να είναι αποτελεσματική (άρα δε μπορεί να το θέσει ολόκληρο εκτός λειτουργίας) και, ακόμα και αν υπερφορτώσει κάποιο κλάδο του, αναμένεται να χρησιμοποιηθούν εναλλακτικές διαδρομές και να γίνει ανακατασκευή του δένδρου διασύνδεσης IP Multicast μέσο αυτών. Η όποια (έστω προσωρινή) διακοπή αυτής της διασύνδεσης θα προειδοποιήσει επίσης για την ύπαρξη του περιστατικού.

(vii) Επίθεση κατά ενεργού εξοπλισμού

Ένα ακόμα ενδεχόμενο είναι, σε δίκτυα οποιουδήποτε μεγέθους, η απ' ευθείας επίθεση εναντίον δρομολογητών, είτε με επιθέσεις DDoS, είτε με εκμετάλλευση προβλημάτων ασφαλείας (exploits). Ένα τέτοιο πρόβλημα αποτελεί

[35]Μια χρήσιμη λεπτομέρεια είναι ότι τα μηνύματα multicast χρησιμοποιούν το UDP, πρωτόκολλο που δεν απαιτεί επιβεβαίωση λήψης (acknowledgement). Άρα κάποια Alerts πιθανόν να μπορέσουν να περάσουν προς την Υποδομή μέσο της εξερχόμενης κίνησης, έστω και αν η εισερχόμενη επικοινωνία έχει διακοπεί.

γενικότερη αδυναμία της δικτυακής υποδομής και ως τέτοιο πρέπει να αντιμετωπιστεί από τους διαχειριστές. Αφ' ετέρου προϋποθέτει την ύπαρξη συγκεκριμένων, γνωστών προβλημάτων και καλώς ενημερωμένους επιτιθέμενους που γνωρίζοντας την αρχιτεκτονική και τα συστήματα του δικτύου θα προσπαθήσουν να τα εκμεταλλευτούν.

3.6 Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε η γενική πρόταση της παρούσας διατριβής για την αντιμετώπιση των επιθέσεων DDoS. Η προσέγγιση που προτείνεται έχει ως βασικούς άξονες ανάπτυξης και τα τρία κύρια ζητήματα στη αντιμετώπιση των επιθέσεων DDoS (όπως αναλύθηκαν στο κεφάλαιο 2): την ανίχνευση, την αναγνώριση του μονοπατιού της επίθεσης και την αντίδραση σε αυτή. Προς την κατεύθυνση αυτή προτείνεται η λειτουργία σε κάθε επιμέρους δίκτυο ενός ειδικού συστήματος, της *Συνεργατικής Οντότητας*, που επιτρέπει:

- Τη συγκέντρωση τοπικών αναφορών IDS (από τα συστήματα αποκλειστικά εντός του δικτύου)
- Την ανταλλαγή μηνυμάτων ανίχνευσης μεταξύ των συνεργαζόμενων δικτύων· όλα τα δίκτυα αυτά που επικοινωνούν, έχουν σχέση εμπιστοσύνης και συνεργάζονται συνθέτουν τη *Συνεργατική Υποδομή*.
- Την ανίχνευση περιστατικών σε κάθε επιμέρους δίκτυο βάσει τοπικών και απομακρυσμένων αναφορών στις οποίες είναι δυνατόν να ανατίθενται διαφορετικά βάρη (εμπιστοσύνη).

- Την ανταλλαγή μηνυμάτων μεταξύ των δικτύων για περιστατικά εν εξελίξει, τη συγκέντρωση πληροφοριών που αυξάνουν τη βεβαιότητα ύπαρξης ενός περιστατικού και τη μερική έστω αναγνώριση του μονοπατιού που ακολουθεί η επίθεση.

- Την απόφαση και υλοποίηση τοπικών, σε κάθε επιμέρους δίκτυο, ενεργειών αντίδρασης στο περιστατικό. Οι ενέργειες αυτές μπορούν να είναι κατά τέτοιο τρόπο ρυθμισμένες ώστε να συμφωνούν με τις εκάστοτε ακολουθούμενες πολιτικές.

Σε τοπικό επίπεδο η Συνεργατική Οντότητα αποτελεί το «ενοποιητικό» στοιχείο που επιτρέπει στα διάφορα επίπεδα οργάνωσης ενός δικτύου (πολιτικές ασφαλείας, διαθέσιμες δυνατότητες επικοινωνίας, τοπικά συστήματα IDS κ.λπ.) να συγκλίνουν σε κοινή και συντονισμένη λειτουργία.

Τα κύρια χαρακτηριστικά της Συνεργατικής Υποδομής όπως προκύπτουν, από την θεωρητική ανάλυση και από την υλοποίηση μιας σειράς από πρωτότυπα είναι:

- Τα δίκτυα διατηρούν τη διαχειριστική τους ανεξαρτησία.

- Μεταξύ δικτύων παρέχεται επικοινωνία μεταξύ των μελών της Συνεργατικής Υποδομής με ασφάλεια και χαμηλή επιβάρυνση του δικτύου.

- Για τις επικοινωνίες τόσο με τα τοπικά συστήματα IDS, όσο και μεταξύ των συνεργαζόμενων δικτύων χρησιμοποιείται το (υπό εξέλιξη) πρότυπο IDEMEF της IETF που διευκολύνει τη διαλειτουργικότητα (με συστήματα IDS και άλλα).

- Η Συνεργατική Υποδομή είναι σε θέση να χρησιμοποιήσει μια σειρά από διαφορετικές τεχνικές επικοινωνίας, όπως IP Multicast, υπερκείμενα (overlay) δίκτυα peer-to-peer, μικρής ή μεγάλης κλίμακας, και περιβάλλοντα «Πλέγματος» (Grid). Όπως αποδείχθηκε από την υλοποίηση των πρωτοτύπων είναι δυνατή η εγκατάσταση, οργάνωση, επικοινωνία και σταθερή λειτουργία της Συνεργατικής Υποδομής σε κάθε μια από αυτές τις περιπτώσεις (πλην αυτής του «Πλέγματος» όπου δεν υλοποιήθηκε αντίστοιχο πρωτότυπο).

- Επιπλέον σε κάθε μια από τις αναφερόμενες περιπτώσεις είναι δυνατή η χρησιμοποίηση των ειδικών χαρακτηριστικών της μεθόδου διασύνδεσης ώστε να επιτευχθούν ειδικές λειτουργίες της Συνεργατικής Υποδομής. Πιο χαρακτηριστικά παραδείγματα είναι:

  - Με τη χρήση IP Multicast δίνεται η δυνατότητα σε ένα δίκτυο να λειτουργούν παράλληλα πλήρως ενημερωμένες εφεδρικές Οντοτήτες. Αυτές χωρίς να είναι άμεσα «ορατές» δικτυακά είναι έτοιμες να αναλάβουν τις λειτουργίες της κύριας Συνεργατικής Οντότητας εφόσον αυτό απαιτηθεί.

  - Η χρήση των ειδικών χαρακτηριστικών του κάθε περιστατικού για την οργάνωση και συγκέντρωση στοιχείων σε ένα κόμβο-συντονιστή όταν χρησιμοποιούνται δίκτυα peer-to-peer δρομολόγησης βασισμένης σε κλειδί (Key Based Routing - KBR).

- Η συνεργασία μεταξύ διαφορετικών (και πιθανά απομακρυσμένων) δικτύων παρουσιάζει μια σειρά από ειδικές ανάγκες από πλευράς ασφαλείας

(πιθανότητα υποκλοπής μηνυμάτων, διείσδυσης επιτιθέμενων στην αρχιτεκτονική, επιβεβαίωση και εμπιστοσύνης στα μηνύματα κ.λπ.). Με μια σειρά από τυπικά μέτρα ασφαλείας (ψηφιακά πιστοποιητικά, χρονοσήμανση — timestamping — κ.λπ.) τα οποία επιβεβαιώθηκαν με την χρήση πειραματικού πρωτοτύπου είναι δυνατή η εξασφάλιση της Αρχιτεκτονικής σε ικανοποιητικό βαθμό.

Στα επόμενα κεφάλαια θα παρουσιαστεί η εσωτερική λειτουργία της Συνεργατικής Οντότητας, τα ειδικά χαρακτηριστικά της οποίας επιτρέπουν την δημιουργία της προτεινόμενης Υποδομής. Επίσης θα παρουσιαστεί μια σειρά από προσομοιώσεις της Συνεργατικής Υποδομής συνολικά (με τη συμμετοχή πολλαπλών δικτύων) οι οποίες αποδεικνύουν επίσης την ορθή λειτουργία της και τα πλεονεκτήματα που μπορεί να προσφέρει με τη χρήση της στην αντιμετώπιση επιθέσεων DDoS.

Κεφάλαιο 4

Χαρακτηριστικά και Λειτουργία των Συνεργατικών Οντοτήτων (Cooperative Entities)

4.1 Εισαγωγή

Στο κεφάλαιο αυτό επικεντρωνόμαστε στη λειτουργία και παραμετροποίηση της Συνεργατικής Οντότητας, του κυρίου δομικού στοιχείου της προτεινόμενης αρχιτεκτονικής. Περιγράφεται η αρχιτεκτονική λογισμικού, η εσωτερική λειτουργία και η μεθοδολογία ανάλυσης των μηνυμάτων ώστε να αναγνωριστεί ένα περιστατικό και να εξαχθούν συγκεκριμένα συμπεράσματα για αυτό. Σημειώνεται ότι η εσωτερική λειτουργία της Οντότητας είναι σε μεγάλο βαθμό ανεξάρτητη από το επικοινωνιακό τμήμα της αρχιτεκτονικής, τόσο την υποδομή χαμηλό-

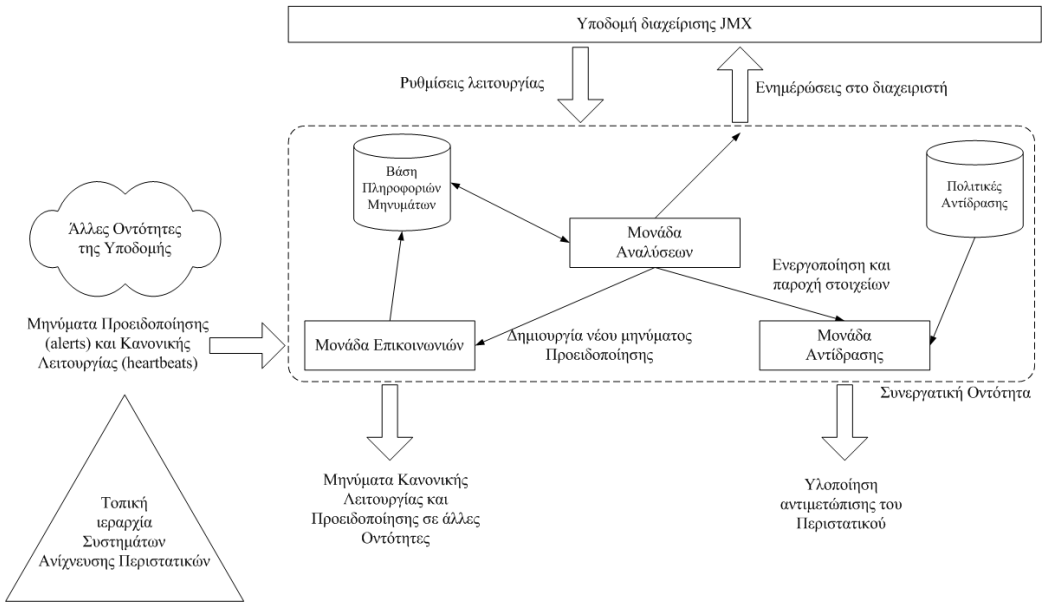
τερου επίπέδου (τη μέθοδο σχηματισμού του Υπερκείμενου Δικτύου[1]), όσο και τα πρωτόκολλα μεταφοράς της πληροφορίας. Κατ' επέκταση, η Οντότητα μπορεί να υλοποιηθεί με διαφορετικούς τρόπους (διαφορετικές πλατφόρμες υλοποίησης, αλγορίθμους λειτουργίας, παραμέτρους διαμόρφωσης κ.λπ.) εφόσον μπορεί να εξασφαλίζει την ανάπτυξη και λειτουργία της αρχιτεκτονικής.

4.2 Τμήματα της Οντότητας

Κατά το σχεδιασμό της εσωτερικής αρχιτεκτονικής λογισμικού της Συνεργατικής Οντότητας έγινε προσπάθεια να ακολουθηθεί η μεθοδολογία της χρήσης αυτόνομων προγραμματιστικών διεργασιών (autonomous agents) οι οποίες λειτουργούν ανεξάρτητα η μια από την άλλη. Η προσέγγιση αυτή έχει μια σειρά από πλεονεκτήματα που παρουσιάζονται αναλυτικά στο [Spaf00] αλλά ουσιαστικά επιτρέπει τον πλήρη διαχωρισμό λειτουργιών, ευελιξία στην εγκατάσταση, τη λειτουργία και τη διαχείριση των διαφορετικών διεργασιών, ενώ, θεωρητικά, ορισμένες από αυτές θα μπορούσαν να εγκατασταθούν και σε διαφορετικά, συστήματα. Η Οντότητα έχει σχεδιαστεί ώστε να προσθέτει μικρή επιβάρυνση στο σύστημα εγκατάστασης. Στο πρωτότυπο η υλοποίηση βασίστηκε στη γλώσσα Java [Gosl00] και την υποδομή διαχείρισης που προσφέρει αυτή ώστε να επιτευχθεί μεταφερσιμότητα του κώδικα σε διαφορετικές υπολογιστικές πλατφόρμες. Η αρχιτεκτονική λογισμικού της Οντότητας παρουσιάζεται στο Σχήμα 4.1.

Η Οντότητα αποτελείται από έναν αριθμό από αυτόνομες, ανεξάρτητες μο-

[1] Εξαίρεση σε αυτό αποτελούν μόνον τα μηνύματα κανονικής λειτουργίας ("Heartbeats") που προβλέπει το πρότυπο IDMEF) που σε ορισμένα είδη υπερκείμενων δικτύων ανταλλάσσονται από την υποδομή ενώ σε άλλα πρέπει να αναλαμβάνονται από την ίδια την Οντότητα. Ο αλγόριθμος λειτουργίας αλλάζει ελάχιστα στις δύο περιπτώσεις ανάλογα με το αν τα χρησιμοποιεί ή όχι.



Σχήμα 4.1: Εσωτερική αρχιτεκτονική και ανταλλαγή μηνυμάτων στη Συνεργατική Οντότητα

νάδες που ενώνονται και λειτουργούν από κοινού κάτω από τη διαχείριση της προγραμματιστικής υποδομής Java Management Extensions (JMX) [Jmx04]. Σύμφωνα με την αρχιτεκτονική του προτύπου αυτού, κάθε μονάδα υλοποιείται ως ένα διαχειριζόμενο πρόγραμμα Java MBean ("Managed Bean"). Η Υποδομή JMX παρέχει τις επικοινωνίες μεταξύ τους και τις απαραίτητες συνδέσεις για να γίνει η διαχείριση τους. Χρησιμοποιώντας το JMX είναι δυνατή η πρόσβαση στις μονάδες με συνδέσεις πρωτοκόλλων (protocol interfaces) πολλών διαφορετικών τύπων, π.χ. ασφαλείς επικοινωνίες HTTP/SSL, SNMP κ.λπ. Μέσω αυτών ο διαχειριστής μπορεί να τροποποιήσει τις παραμέτρους διαμόρφωσης της Οντότητας ή να ελέγξει κάθε μονάδα ξεχωριστά. Η υποδομή JMX επιτρέπει την επέμβαση και την εφαρμογή διαχειριστικών εργασιών σε κάθε μια από τις μονάδες, π.χ. εγκατάσταση νέων εκδόσεων, ενεργοποίηση ή διακοπή της

λειτουργίας τους, στις περισσότερες περιπτώσεις χωρίς να χρειάζεται να επηρεαστεί ολόκληρη η Οντότητα. Επιπλέον, το στοιχείο αυτό δίνει στο διαχειριστή τη δυνατότητα απομακρυσμένης πρόσβασης και διαχείρισης της Οντότητας μέσω ενός κοινού web browser,

4.2.1 Μονάδα Επικοινωνιών

Η Μονάδα αυτή αναλαμβάνει το ρόλο της διασύνδεσης ανάμεσα στην Οντότητα και οποιοδήποτε υπόβαθρο επικοινωνίας έχει επιλεγεί για τη δημιουργία και διασύνδεση του υπερκείμενου δικτύου που υλοποιεί την Υποδομή Αντιμετώπισης Περιστατικών DDoS.

Η μονάδα χειρίζεται τα εισερχόμενα μηνύματα, προειδοποίησης περιστατικού (Alerts) ή ενημέρωσης για κανονική λειτουργία (heartbeats) και υλοποιεί τις εξής λειτουργίες:

- Αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το κοινό κλειδί της ομάδας
- Ελέγχει την αυθεντικότητα της ψηφιακής υπογραφής στο μήνυμα και τη συμφωνία με τα στοιχεία του αποστολέα
- Ελέγχει το χρονική σήμανση του μηνύματος για να αποφευχθούν επιθέσεις επανάληψης μηνυμάτων (replication attacks). Τα στοιχεία ψηφιακής υπογραφής και χρονικής σήμανσης παρέχονται με επικεφαλίδες XML που είναι μέρος του μηνύματος.

Σε περίπτωση που το μήνυμα δεν γίνει αποδεκτό η μονάδα στέλνει μια σχετική ειδοποίηση στο διαχειριστή επειδή ενδέχεται να είναι ένδειξη παραβίασης της Συνεργατικής Υποδομής.

Σε αντίθετη περίπτωση, που το μήνυμα γίνεται κανονικά αποδεκτό, τα κυρίως περιεχόμενα του μηνύματος (στοιχεία XML που ακολουθούν την προδιαγραφή IDMEF) περνούν από ένα λεκτικό αναλυτή και αντλούνται οι πληροφορίες που περιέχονται σε κάθε πεδίο. Οι πληροφορίες του μηνύματος, μαζί με το χρόνο παραλαβής αποθηκεύονται στη βάση δεδομένων για τα μηνύματα. Η βάση αυτή διαθέτει στη συνέχεια τις πληροφορίες των μηνυμάτων στις υπόλοιπες μονάδες της Οντότητας[2] [Χατζ02].

Η Μονάδα Επικοινωνιών αναλαμβάνει επίσης και την αποστολή των εξερχόμενων μηνυμάτων από την Οντότητα: αυτόματη αποστολή μηνυμάτων κανονικής λειτουργίας της Οντότητας και τυχόν μηνυμάτων προειδοποίησης προς τη Συνεργατική Υποδομή (φροντίζοντας ταυτόχρονα θέματα, όπως η χρονική σήμανση, η ψηφιακή υπογραφή και η κρυπτογράφηση τους).

4.2.2 Μονάδα Αναλύσεων

Είναι ο κύριος μηχανισμός συνδυασμού και ανάλυσης των πληροφοριών που λαμβάνει η Οντότητα από τοπικές και απομακρυσμένες πηγές. Η μονάδα αυτή διατηρεί μια κατάσταση λειτουργίας για κάθε ένα περιστατικό εν εξελίξει. Ανάλογα με τις παραμέτρους ρύθμισης της λειτουργίας της Οντότητας, που καθορίζουν την ευαισθησία και τους χρόνους απόκρισης της, και τα μηνύματα που θα λάβει θα περάσει από την παρακολούθηση στο χειρισμό του περιστατικού.

Περνώντας στη διαδικασία ενεργοποίησης για ένα περιστατικό ο μηχανισμός της Οντότητας θα αναλάβει:

- Την ανάλυση του περιστατικού βάσει των μηνυμάτων που έχουν ληφθεί

[2] Τα μηνύματα κανονικής λειτουργίας (δείτε στη συνέχεια) δεν αποθηκεύονται ξεχωριστά αλλά ανανεώνουν μόνο το χρόνο τελευταίας λήψης τους.

ώστε να διαπιστωθούν τα χαρακτηριστικά του και κυρίως η τοποθέτηση του δικτύου στο πάνω στη διαδρομή που ακολουθεί η επίθεση.

- Την ενημέρωση της διαχειριστικής εφαρμογής για την ύπαρξη του περιστατικού.
- Τη δημιουργία, υπό κατάλληλες προϋποθέσεις, ενός μηνύματος προειδοποίησης και την απόδοση του στη Μονάδα Επικοινωνιών για αποστολή στις υπόλοιπες Οντότητες.
- Την ενεργοποίηση της Μονάδας Αντίδρασης με τα αποτελέσματα της ανάλυσης ώστε, εφόσον υπάρχει η κατάλληλη πολιτική αντιμετώπισης να αναληφθούν τα αντίστοιχα μέτρα.

4.2.3 Μονάδα Αντίδρασης

Σε αυτή τη μονάδα οι πληροφορίες και οι ανάλυση για το περιστατικό που έχει ενεργοποιήσει την Οντότητα αντιστοιχίζονται σε πολιτικές αντίδρασης. Εάν υπάρχει η κατάλληλη πολιτική η μονάδα αυτή αναλαμβάνει να υλοποιήσει και τα αντίστοιχα μέτρα τον ενεργό εξοπλισμό του δικτύου για την αντιμετώπιση της επίθεσης.

4.3 Λειτουργία της Οντότητας

4.3.1 Καταστάσεις λειτουργίας και παράμετροι διαμόρφωσης

Η Οντότητα επιτελεί τη λειτουργία της περνώντας από μια σειρά από καταστάσεις για κάθε περιστατικό που θα παρακολουθήσει, βάση ορισμένων παραμέτρων ρύθμισης. Σημειώνεται ότι η Οντότητα μπορεί ταυτόχρονα να παρακολουθεί περισσότερα του ενός περιστατικά και να μεταβαίνει σε διαφορετική κατάσταση λειτουργίας για κάθε ένα από αυτά ανάλογα με την εξέλιξη του. Οι καταστάσεις και οι μεταβάσεις μεταξύ τους φαίνονται στο Σχήμα 4.2 και είναι οι εξής:

1. *Down - Κατάσταση μη λειτουργίας*. Η Οντότητα βρίσκεται σε αυτή την κατάσταση κατά την εκκίνηση, μέχρι να ενεργοποιηθεί η μονάδα επικοινωνιών, ή με διαχειριστική επέμβαση. Η κατάσταση αυτή διακόπτει την παρακολούθηση όλων των γεγονότων εν εξελίξει. Είναι επίσης η μοναδική περίπτωση που η Οντότητα δεν εκπέμπει τακτικά μηνύματα κανονικής λειτουργίας της (για τις αρχιτεκτονικές που τα χρησιμοποιούν).

2. *Normal - Φυσιολογική κατάσταση λειτουργίας*. Η Οντότητα θα βρεθεί σε αυτή την κατάσταση όταν θα έχει ολοκληρώσει την εκκίνηση της, και θα παραμείνει σε αυτή όσο συνεχίζει να λαμβάνει κανονικά μηνύματα λειτουργίας (Heartbeats) από άλλες ομότιμες Οντότητες και δεν έχει λάβει κανένα μήνυμα προειδοποίησης (Alert) για κάποιο περιστατικό. Από πλευράς υλοποίησης, επειδή κάθε κατάσταση ενεργοποίησης είναι συνδεδεμένη με ένα περιστατικό, η φυσιολογική κατάσταση δεν υφίσταται πραγματικά, αλλά υποδεικνύει ότι δεν έχει ενεργοποιηθεί καμία μετάβαση

Σχήμα 4.2: Καταστάσεις της Συνεργατικής Οντότητας και μεταβάσεις μεταξύ τους

σε κατάσταση υποψίας. Για τις αρχιτεκτονικές όπου γίνεται χρήση μηνυμάτων κανονικής λειτουργίας, στην κατάσταση αυτή γίνεται απλά μια παρακολούθηση για την λήψη αυτών των μηνυμάτων εντός των προβλεπόμενων χρονικών διαστημάτων. Το χρονικό διάστημα αναμονής ορίζεται από την παράμετρο *Heartbeat_timeout* και αν για κάποια Οντότητα της συνεργασίας ξεπεραστεί μεταφερόμαστε την επόμενη κατάσταση ενεργοποίησης.

3. *Suspicion - Κατάσταση πιθανής ύπαρξης περιστατικού.* Αν η Οντότητα λάβει έστω και ένα μήνυμα προειδοποίησης θα περάσει σε αυτή την κατάσταση. Το ίδιο θα συμβεί στις περιπτώσεις που έχει ξεπεραστεί το χρονικό όριο για τη λήψη ενός μηνύματος κανονικής λειτουργίας από μια από τις άλλες Οντότητες. Τα στοιχεία του μηνύματος προειδοποίησης καταγράφονται και ξεκινά η παρακολούθηση του πιθανού περιστατικού. Μέρος αυτής της παρακολούθησης είναι η δημιουργία ενός «Μετρητή Βεβαιότητας» για το περιστατικό, *Notification_counter*, ο οποίος καταγράφει το συνολικό αριθμό μηνυμάτων που έχουν παραληφθεί και έχουν σχέση με αυτό το περιστατικό. Συνολικά η «συσσώρευση» βεβαιότητας για το περιστατικό είναι μια μορφή «ψηφοφορίας με βάρη» (weighted voting) αλλά με τη συμμετοχή της παραμέτρου του χρόνου.

   Κάθε νέο μήνυμα που λαμβάνεται από την Οντότητα εξετάζεται κατά πόσον έχει σχέση με κάποιο από τα υπάρχοντα περιστατικά. Αν πράγματι ανήκει σε ένα από αυτά τότε θα αυξήσει το μετρητή *Notification_counter*. Η ταχύτητα αύξησης του μετρητή αυτού καθορίζει τη μετάβαση στην επόμενη κατάσταση λειτουργίας της Οντότητας.

Υπάρχει η δυνατότητα ώστε ορισμένα μηνύματα να αξιολογούνται με διαφορετικό τρόπο ως προς την αξία τους, επομένως και για το πόσο θα αυξήσουν το μετρητή *Notification_counter*. Πιο συγκεκριμένα, μηνύματα που προέρχονται από τα Συστήματα Ανίχνευσης Επιθέσεων του δικτύου στο οποίο ανήκει η Οντότητα παραλήπτης αυξάνουν την τιμή του *Notification_counter* κατά ένα συντελεστή ίσο με την παράμετρο *Local_value*. Η επιλογή αυτή έχει γίνει ώστε τα τοπικά μηνύματα να χειρίζονται ως υψηλότερης αξίας και πιο έμπιστα από αυτά που προέρχονται από απομακρυσμένα, ξένα δίκτυα. Αυτό το χαρακτηριστικό είναι χρήσιμο για δίκτυα που είναι αποδέκτες μιας επίθεσης ώστε να επιτυγχάνουν συντομότερη μετάβαση σε επόμενες καταστάσεις που συνεπάγονται και την εκπομπή μηνυμάτων ενημέρωσης. Επιπλέον αναμένεται μεγαλύτερη πιθανότητα εντοπισμού μιας επίθεσης DDoS από δίκτυα τα οποία βρίσκονται πάνω στο μονοπάτι της διαδρομής της και κοντύτερα στον τελικό στόχο. Τα δίκτυα αυτά θα έχουν έτσι την ευκαιρία να αντιδράσουν έγκαιρα. Για προσδιορισμό της ταχύτητας λήψης των τοπικών μηνυμάτων προειδοποίησης χρησιμοποιείται και ένας ξεχωριστός μετρητής, ειδικά για αυτά, ο *Local_counter*.

Προς την ίδια κατεύθυνση λειτουργούν και μερικές ακόμα παράμετροι της υλοποίησης: κάθε μήνυμα (προειδοποίησης) περιστατικού φέρει τη βεβαιότητα του αποστολέα για την αναφορά που κάνει, *Confidence_count*. Επίσης σε κάθε συνεργαζόμενο δίκτυο αποδίδεται μια παράμετρος εμπιστοσύνης, *Sender_confidence* ανάλογα με τη σχέση που έχει το δίκτυο

παραλήπτης με αυτό[3]. Ένας μετρητής χρόνου με αρχική τιμή την παράμετρο *Suspicious_timeout* αρχίζει να μετράει αντίστροφα μετά από κάθε λήψη μηνύματος σχετικού με το περιστατικό και ανανεώνει την τιμή του με κάθε νέο μήνυμα. Συνεχιζόμενη αδυναμία λήψης μηνυμάτων κανονικής λειτουργίας δεν αυξάνει κανέναν από τους μετρητές, απλά διατηρεί την Οντότητα στην ίδια κατάσταση. Είναι προτιμητέο η παράμετρος *Heartbeat_timeout* να είναι μεγαλύτερη από το μέγιστο χρόνο που μπορεί να μεσολαβήσει για την λήψη ενός νέου μηνύματος κανονικής λειτουργίας.

Τέλος κρατείται η διάρκεια του περιστατικού (με καταγραφή του χρονικού σημείου στο οποίο αυτό ξεκίνησε - πότε ελήφθη το πρώτο σχετικό μήνυμα) ώστε να μπορεί να εκτιμηθεί πόσο γρήγορα έχει αυτό εξελιχθεί μέχρι το πέρασμα της Οντότητας στην επόμενη κατάσταση λειτουργίας. Ο χρόνος εξέλιξης του περιστατικού είναι η παράμετρος *Event_time*.

4. *Alert - Κατάσταση Ενεργοποίησης*. Η Οντότητα περνά σε αυτή την κατάσταση για κάποιο περιστατικό, εφόσον ο μετρητής *Notification_counter* ξεπεράσει την τιμή της παραμέτρου *Alert_threshold*. Η Οντότητα παραμένει σε αυτή την κατάσταση για διάστημα ίσο με την παράμετρο *Alerted_timeout*. Ο χρόνος αυτός ανανεώνεται εφόσον ληφθούν νέα μηνύματα προειδοποίησης. Με την εξάντληση του χρονικού ορίου η Οντότητα επιστρέφει στην κατάσταση Suspicion με αλλαγή στην τιμή του μετρητή *Notification_counter* στην τιμή *Alert_threshold* μειωμένη κατά μια παράμετρο *Tolerance*. Η μείωση αυτή γίνεται ώστε να μην υπάρχει συνεχής

[3]Η παράμετρος αυτή μπορεί να αντικατοπτρίζει τις επιχειρηματικές σχέσεις ή πολιτικές προς άλλα δίκτυα χωρίς όμως να παρεμποδίζεται η ουσιαστική συνεργασία μεταξύ τους.

εναλλαγή ανάμεσα στις δύο καταστάσεις. Εννοείται ότι:

$$2 \leq Tolerance \leq Alert\_threshold$$

Δηλαδή, η τιμή του *Notification_counter* θα μειωθεί τουλάχιστον κατά 2, με δεδομένο επίσης ότι οπωσδήποτε Alert_threshold ≥ 2.

Η μετάβαση στην Κατάσταση Ενεργοποίησης συνεπάγεται μια σειρά από ενέργειες (ανάλογα με τις ρυθμίσεις που έχει κάνει ο διαχειριστής για την λειτουργία της Οντότητας):

- Αναλύονται τα μηνύματα που έχουν ληφθεί για το περιστατικό ώστε να βγει συμπέρασμα για την τοποθέτηση του δικτύου ως προς το μονοπάτι της επίθεσης[4]. Ο συνδυασμός των διαφορετικών περιπτώσεων θα οδηγήσει και στην αντίστοιχη αντίδραση.
- Στέλνεται ενημέρωση στη μονάδα διαχείρισης του δικτύου ώστε ο διαχειριστής να γνωρίζει για τα περιστατικά σε εξέλιξη.
- Ενεργοποιείται ο Μηχανισμός Αντίδρασης στην επίθεση. Εφόσον υπάρχει η αντίστοιχη πολιτική, η μονάδα αυτή αναλαμβάνει να την υλοποιήσει. Η ειδοποίηση για ενεργοποίηση της μονάδας αυτής περιλαμβάνει τα στοιχεία του περιστατικού της επίθεσης και στοιχεία του μονοπατιού που αφορούν το δίκτυο. Στη συνέχεια τυχόν ενέργειες αναλαμβάνονται από αυτή τη μονάδα ανάλογα με το τί υπαγορεύει η πολιτική για σχετικές περιπτώσεις και αντίστοιχα προς τα

[4]Οι πιθανές περιπτώσεις που αναλύονται στη συνέχεια είναι: (α)το δίκτυο είναι πηγή της επίθεσης ή πάνω στο μονοπάτι της, (β) είναι πάνω στο μονοπάτι της, (γ) είναι ο στόχος της επίθεσης ή (δ) είναι εκτός του μονοπατιού επίθεσης.

συγκεκριμένα τεχνικά χαρακτηριστικά της επίθεσης. Εφόσον υλοποιηθούν μέτρα κατά της επίθεσης θεωρούμε ότι η Οντότητα είναι στην επόμενη κατάσταση λειτουργίας.

5. *Reacting - Κατάσταση αντίδρασης*. Η παραμονή σε αυτή την κατάσταση γίνεται για όσο διάστημα υλοποιείται κάποια πολιτική αντιμετώπισης της επίθεσης. Η επιστροφή από αυτή την κατάσταση γίνεται στην κατάσταση Suspicion και έχει τα ίδια χαρακτηριστικά με την κατάσταση Alert:

$$Notification\_counter = Alert\_threshold - Tolerance$$

Ο χρόνος παραμονής στην κατάσταση αυτή επίσης ανανεώνεται εφόσον ληφθούν νέα μηνύματα προειδοποίησης για το ίδιο περιστατικό.

Η επιλογή να θεωρείται διαφορετική κατάσταση η περίπτωση ενεργής αντίδρασης έγινε ώστε ο διαχειριστής να γνωρίζει ανά πάσα στιγμή αν έχουν τεθεί σε ισχύ μέτρα στο δίκτυο και, εφόσον το επιλέξει, να επεμβαίνει. Πιθανές επεμβάσεις του διαχειριστή μπορεί να είναι η διακοπή της υλοποιημένης πολιτικής αντίδρασης ή η ανανέωση της με νέα, η οποία θα εφαρμοστεί άμεσα από τη μονάδα αντίδρασης.

Ο Πίνακας 4.1 συνοψίζει τις παραμέτρους που χρησιμοποιούνται για τη ρύθμιση της λειτουργίας (configuration parameters) της Οντότητας και ο Πίνακας 4.2 παρουσιάζει τα πληροφοριακά στοιχεία που χρησιμοποιούνται στη λειτουργία της Οντότητας.

Παραμετρος	Εξηγηση
Heartbeat_timeout	Το χρονικό διάστημα για το οποίο η Οντότητα θα περιμένει να λάβει ένα μήνυμα Κανονικής Λειτουργίας (heartbeat) από άλλη γειτονική Οντότητα. Αν αυτό ξεπεραστεί χωρίς λήψη τέτοιου μηνύματος η Οντότητα θα περάσει σε κατάσταση «Υποψίας Περιστατικού» (Suspicion State) αλλά χωρίς συσχέτιση με συγκεκριμένο περιστατικό.
Local_value	Συντελεστής βάρους για τα μηνύματα που προέρχονται από τα τοπικά (από το ίδιο δίκτυο με την Οντότητα) συστήματα IDS.
Sender_confidence	Συντελεστής εμπιστοσύνης που ανατίθεται στα μηνύματα από τον παραλήπτη ανάλογα με τον αποστολέα.
Suspicious_timeout	Αρχική τιμή μετρητή που μετράει αντίστροφα μετά τη μετάβαση σε κατάσταση «Υποψίας Περιστατικού» (Suspicion State) και ανανεώνεται με κάθε λήψη νέου μηνύματος σχετικού με το περιστατικό.
Alert_threshold	Τιμή όριο για την παράμετρο *Notification_counter* πέραν του οποίου η Οντότητα περνά σε κατάσταση «Ενεργοποίησης» (Alert State) για κάποιο περιστατικό.
Alerted_timeout	Αρχική τιμή μετρητή χρόνου που μετράει αντίστροφα μετά τη μετάβαση σε κατάσταση «Ενεργοποίησης» (Alert State) και ανανεώνεται με κάθε λήψη νέου μηνύματος σχετικού με το περιστατικό.
Local_notification_threshold	Όριο για την τιμή $Local\_counter/Event\_time$ προκειμένου να παραχθεί ένα μήνυμα προειδοποίησης (Alert) από την Οντότητα.
Tolerance	Τιμή μείωσης του μετρητή *Notification_counter* από την τιμή *Alert_threshold* όταν η Οντότητα επιστρέψει σε κατάσταση «Υποψίας Περιστατικού» από κατάσταση «Ενεργοποίησης». Ισχύει $Notification\_counter = Alert\_threshold - Tolerance$

Πίνακας 4.1: Παράμετροι ρύθμισης της Οντότητας

ΠΑΡΑΜΕΤΡΟΣ	ΕΞΗΓΗΣΗ
Notification_counter	Ένας μετρητής («συσσωρευτής») βεβαιότητας, βάσει των μηνυμάτων που έχουν παραληφθεί για ένα περιστατικό. Για κάθε διαφορετικό περιστατικό δημιουργείται και ένας μετρητής αυτού του είδους. Αυξάνεται κατά το βάρος που θα δοθεί σε κάθε εισερχόμενο μήνυμα που αφορά το συγκεκριμένο περιστατικό.
Event_time	Χρόνος διάρκειας του περιστατικού από την πρώτη εμφάνιση μηνύματος.
Local_counter	Μετρητής του αριθμού μηνυμάτων που προήλθαν από τοπικά συστήματα IDS
Confidence_count	Συντελεστής βεβαιότητας του αποστολέα για ένα εισερχόμενο μήνυμα.
S	Σοβαρότητα Επίθεσης, S, όπου: $S = (N - A + 1)/E$ και E η (κανονικοποιημένη) τιμή της παραμέτρου *Event_time*, N η τιμή της παραμέτρου *Notification_counter*, A η τιμή της παραμέτρου *Alert_threshold*

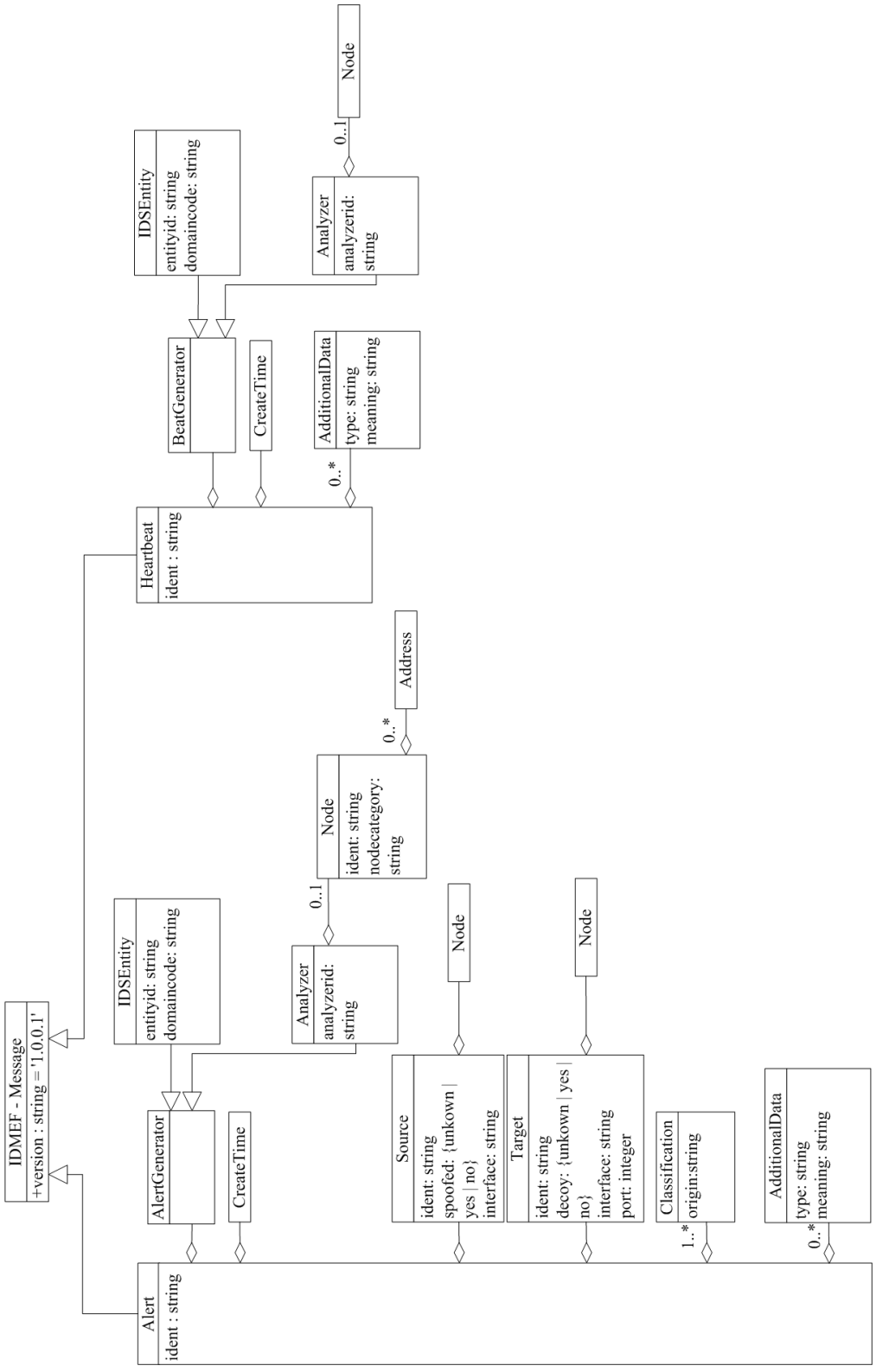
Πίνακας 4.2: Πληροφοριακά στοιχεία κατά τη λειτουργία της Οντότητας

4.3.2 Μηνύματα που ανταλλάσσονται

Η Επέκταση του προτύπου IDMEF

Τα μηνύματα συντάσσονται στη γλώσσα XML (eXtended Markup Language) σύμφωνα προς τη λογική λειτουργίας και τους ορισμούς του προτύπου IMDEF [Deba04]. Το πρότυπο αυτό έχει σχεδιαστεί για τις επικοινωνίες μεταξύ Συστημάτων Ανίχνευσης Επιθέσεων (Intrusion Detection Systems - IDS) και ορίζει τους κανόνες σύνταξης (Document Type Definition - DTD) των σχετικών μηνυμάτων σε XML. Κατά την παρούσα εργασία το DTD του IDMEF, επε-

κτάθηκε (όπως προβλέπεται στην ίδια την προδιαγραφή), ώστε να περιλαμβάνει επιπλέον πληροφορίες χρήσιμες για τη λειτουργία της Συνεργατικής Υποδομής. Πιο συγκεκριμένα (στο πεδίο `Additional Data`) προστέθηκαν πληροφορίες σχετικά με τα προηγούμενα και επόμενα δίκτυα που ακολουθεί η διαδρομή μιας επίθεσης ως προς το σύστημα που αναγνωρίζει το περιστατικό. Το εκτεταμένο DTD παρουσιάζεται σχηματικά στο Σχήμα 4.3 στη συνέχεια.



Σχήμα 4.3: Το πλήρες IDMEF DTD, όπως αυτό επεκτάθηκε και χρησιμοποιήθηκε στα πλάισια της παρούσας εργασίας

Είδη μηνυμάτων και πεδία τους

Κατά τον ορισμό του DTD χρησιμοποιούνται μηνύματα δύο ειδών:

α. Μηνύματα κανονικής λειτουργίας (heartbeats). Προέρχονται από άλλες ομότιμες Οντότητες και δίνουν μια ένδειξη ότι τόσο αυτές όσο και το δίκτυο λειτουργούν κανονικά. Ένα ενδεικτικό τέτοιο μήνυμα δίνεται στο Τμήμα Κώδικα 4.1.

β. Μηνύματα προειδοποίησης (Alerts). Αυτά μπορεί να προέλθουν είτε από Συστήματα Ανίχνευσης Επιθέσεων τα οποία λειτουργούν στο ίδιο δίκτυο με την Οντότητα παραλήπτη είτε από άλλες Οντότητες που έχουν διαπιστώσει κάποιο περιστατικό ασφαλείας εν εξελίξει. Ένα ενδεικτικό τέτοιο μήνυμα δίνεται στο Τμήμα Κώδικα 4.2.

```
<Heartbeat ident="1234">
<Analyzer analyzerid="Domain_A_Entity-123"></Analyzer>

<CreateTime ntpstamp="0x12345678.0x87654321">
2003-04-01T03:44:56,01+02:00
</CreateTime>

</Heartbeat>
```

Τμήμα Κώδικα 4.1: Παράδειγμα μηνύματος τύπου Heartbeat

Και τα δύο είδη μηνυμάτων περιέχουν τις πληροφορίες που μεταφέρουν, οριοθετημένες με επικεφαλίδες (tags) XML, δομημένες ιεραρχικά, σύμφωνα με τους (επαυξημένους) κανόνες περιγραφής εγγράφων του (DTD) του IDMEF.

Η προδιαγραφή IDMEF περιλαμβάνει μια πληθώρα στοιχείων αλλά παρουσιάζονται εδώ αυτά που συγκεκριμένα χρησιμοποιούνται στη λειτουργία της Οντότητας:

- Το αναγνωριστικό `ident` (identification) χρησιμοποιείται μόνον για την αρχειοθέτηση των μηνυμάτων τύπου Heartbeat και Alert στον αποστολέα.

- Κάθε Οντότητα μέλος της Συνεργατικής Υποδομής (Cooperative Infrastructure) έχει ένα μοναδικό κωδικό ο οποίος χαρακτηρίζει το δίκτυο αποστολέα (ή το τοπικό Σύστημα IDS) και επιτρέπει την απόδοση διαφορετικής βαρύτητας στο εισερχόμενο μήνυμα. Ο κωδικός αυτός περιέχεται στον προσδιορισμό `analyzerid`.

- Το αναγνωριστικό `ident` στους προσδιορισμούς πηγής (`Source`) και προορισμού (`Target`) του περιστατικού αναφέρεται σε δίκτυα που είτε ανήκουν στη Συνεργατική Υποδομή είτε δεν ανήκουν σε αυτή αλλά είναι άμεσα γειτονικά σε αυτή. Σε κάθε Οντότητα υπάρχει ένας κατάλογος από αυτά τα δίκτυα και τις συνδέσεις μεταξύ τους. Η πληροφορία αυτή όπως θα φανεί στη συνέχεια χρησιμοποιείται για τον προσδιορισμό του μονοπατιού της επίθεσης. Τα μηνύματα προειδοποίησης (Alerts) μπορεί να έχουν πολλαπλούς προσδιορισμούς πηγής εφόσον αυτοί αναφέρονται στην ίδια επίθεση (η κίνηση από μια επίθεση DDoS μπορεί να εισέρχεται σε ένα δίκτυο από πολλά διαφορετικά σημεία ταυτόχρονα).

- Το στοιχείο `Service` δίνει συγκεκριμένες πληροφορίες για το περιστατικό, όπως πρωτόκολλο και θύρα επικοινωνίας

```
<Alert ident="67890">
<Analyzer analyzerid="Domain_A_Entity-123"></Analyzer>

<CreateTime ntpstamp="0x12344321.0x87655678">
2003-04-01T03:45:57,03+02:00
</CreateTime>

<Source ident="X">
<Service>
<Portlist>25, 80</Portlist>
</Service>
</Source>

<Source ident="Y">
<Service>
<Portlist>25, 80</Portlist>
</Service>
</Source>

<Target ident="D">
<Node>
<Address category="7">147.102.13.10</Address>
</Node>
</Target>

<Classification origin="1">SYN Attack</Classification>
<AdditionalData type="8", meaning="Description">
DoS
</AdditionalData>

<AdditionalData type="8", meaning="Next-Hop Domain">
B
</AdditionalData>

</Alert>
```

Τμήμα Κώδικα 4.2: Παράδειγμα μηνύματος τύπου Alert: Η επίθεση DDoS έχει στόχο το σύστημα με IP 147.102.13.10 στο (υποθετικό) δίκτυο D, που εμφανίζεται στο Σχήμα 4.5

- Τα πρόσθετα στοιχεία `Classification` και `AdditionalData` παρέχουν πρόσθετες πληροφορίες για το περιστατικό. Το αρχικό πρότυπο IDMEF αν και χρήσιμο είναι σχεδιασμένο αποκλειστικά για την επικοινωνία μεταξύ Συστημάτων Ανίχνευσης επιθέσεων. Για να καλύψει τις ανάγκες του προτεινόμενου προτύπου έπρεπε να επεκταθεί, διαδικασία που προβλέπεται από τον ορισμό του. Σύμφωνα με αυτόν τον ορισμό οι επεκτάσεις γίνονται χρησιμοποιώντας τον προσδιορισμό `AdditionalData`. Στην περίπτωση των μηνυμάτων που χρησιμοποιεί το προτεινόμενο σύστημα το στοιχείο `AdditionalData` περιέχει το «επόμενο» δίκτυο στο μονοπάτι της επίθεσης όπως το αναγνωρίζει ο αποστολέας του μηνύματος.

- Τα στοιχεία Πηγής, Προορισμού, «Επόμενου Δικτύου» και των τεχνικών χαρακτηριστικών παρέχουν αρκετές πληροφορίες για τη μοναδική αναγνώριση μιας επίθεσης και βοηθούν στην εξαγωγή συμπερασμάτων για την τοποθέτηση των διαφόρων δικτύων πάνω στο μονοπάτι.

4.3.3 Παραγωγή των μηνυμάτων

Αυτή γίνεται από τη Μονάδα Ανάλυσης της Οντότητας. Η προτεινόμενη Συνεργατική Υποδομή έχει ως ένα από τους κύριους σκοπούς της να αποφύγει τον πολλαπλασιασμό των μηνυμάτων προειδοποίησης στο δίκτυο. Έτσι σε κάθε περίπτωση γίνεται η προσπάθεια να αποφεύγεται η επανάληψη πληροφορίας[5]. Τα μηνύματα προειδοποίησης είναι αποτέλεσμα των ενημερώσεων των τοπικών Συστημάτων Ανίχνευσης Επιθέσεων και παράγονται όταν ισχύουν ταυτόχρονα

[5] Φυσικά οι Οντότητες επαναλαμβάνουν τα μηνύματα σε χαμηλό επίπεδο (υποστηρίζοντας επικοινωνία Multicast επιπέδου εφαρμογής - περίπτωση επικοινωνιών peer-to-peer) όταν δε χρησιμοποιείται κάποια δικτυακή υποδομή που αναλαμβάνει αυτή την ενέργεια (επικοινωνία Multicast επιπέδου IP)

μια σειρά από συγκεκριμένες συνθήκες:

1. Η Οντότητα πρέπει να βρίσκεται σε Κατάσταση Ενεργοποίησης (Alert State).

2. Η Οντότητα έχει περιέλθει σε κατάσταση Ενεργοποίησης για ένα περιστατικό επίθεσης DDoS

3. Η Οντότητα χρειάζεται να βασίσει την παραγωγή νέων μηνυμάτων στις αναφορές ανίχνευσης των τοπικών Συστημάτων IDS. Κατ' αυτόν τον τρόπο, νέα μηνύματα θα παράγονται μόνον εφόσον υπάρξει διαθέσιμη νέα πληροφορία για μετάδοση. Έτσι, ένα νέο μήνυμα παράγεται σε μια από τις εξής δύο περιπτώσεις:

   α. Η Οντότητα έχει περιέλθει σε κατάσταση Ενεργοποίησης αποκλειστικά από μηνύματα από το τοπικό δίκτυο (τα τοπικά Συστήματα IDS).

   β. Σε περίπτωση που υπάρχουν μηνύματα για το ίδιο περιστατικό και από εξωτερικές πηγές, ο ρυθμός άφιξης των ενημερώσεων τοπικής προέλευσης υπερβαίνει ένα προκαθορισμένο όριο. Το όριο αυτό καθορίζεται από την παράμετρο ρύθμισης *Local_notification_threshold*. Ο ρυθμός άφιξης των τοπικών μηνυμάτων βρίσκεται από το πηλίκο:

   $$Local\_counter/Event\_time$$

   Η παράμετρος *Local_counter* μετρά τα μηνύματα τοπικής προέλευσης για ένα περιστατικό και *Event_time* είναι ο χρόνος που μεσολάβησε

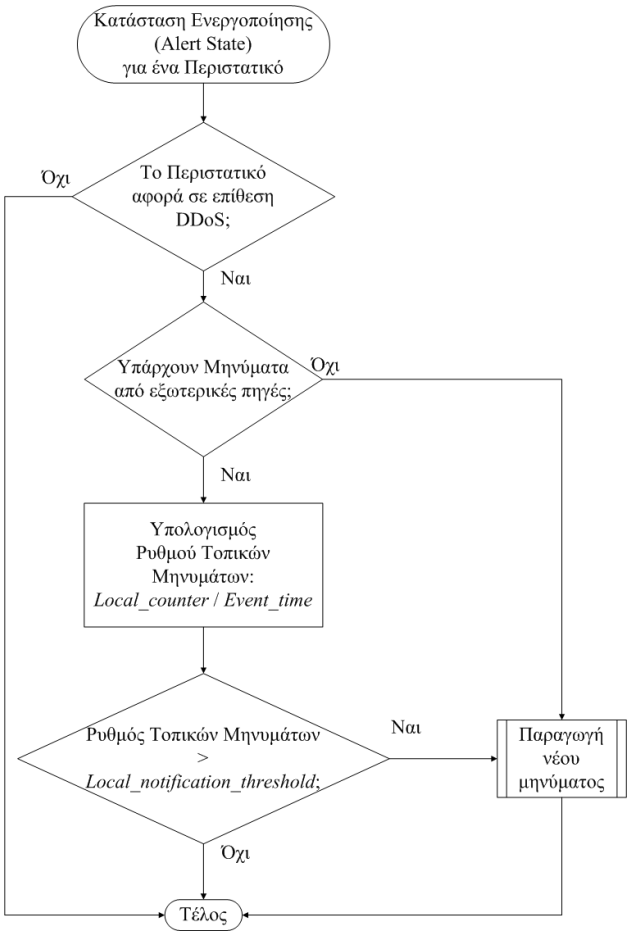
από τη στιγμή άφιξης του πρώτου μηνύματος για το περιστατικό μέχρι τη στιγμή μετάβασης της Οντότητας στην Ενεργοποιημένη Κατάσταση.

Η παραπάνω διαδικασία απόφασης για την παραγωγή μηνύματος από μια Οντότητα παρουσιάζεται συνολικά ως διάγραμμα ροής (Flowchart) στο Σχήμα 4.4. Η λογική αυτού του αλγορίθμου παραγωγής μηνυμάτων είναι ότι η ταχεία συσσώρευση τοπικών ενημερώσεων συνεπάγεται μεγαλύτερη πιθανότητα το δίκτυο στο οποίο είναι εγκατεστημένη η Οντότητα να βρίσκεται πάνω στη διαδρομή της επίθεσης.

4.3.4 Ανάλυση των περιστατικών

Όπως αναφέρθηκε, με τη μετάβαση της Οντότητας στην κατάσταση Ενεργοποίησης εκτελούνται μια σειρά από ενέργειες, η κυριότερη από τις οποίες είναι η ανάλυση των μηνυμάτων που σχετίζονται με το περιστατικό, ώστε να βγει συμπέρασμα ως προς τη μορφή και τη διαδρομή της επίθεσης. Τα στοιχεία που έχουν συλλεχθεί από τα μηνύματα και χρησιμοποιούνται για αυτό το σκοπό είναι τα εξής:

- Αποστολέας μηνύματος
- Δίκτυο πηγή της επίθεσης
- Στόχος της επίθεσης. Αυτός μπορεί να είναι ένα μόνον σύστημα ή ολόκληρη ομάδα από διευθύνσεις οι οποίες όμως ανήκουν στο ίδιο δίκτυο. Συνήθως η δρομολόγηση κίνησης ανάμεσα σε δικτυακούς χώρους Αυτόνομων Συστημάτων του πρωτοκόλλου Border Gateway Protocol (BGP)



Σχήμα 4.4: Αλγόριθμος Παραγωγής Μηνυμάτων

– BGP Autonomous Systems (AS) γίνεται γενικευμένα (aggregated) για όλες τις διευθύνσεις που περιλαμβάνει το AS προορισμού. Επομένως είναι λογική για το ίδιο περιστατικό η αναζήτηση όλων των διευθύνσεων που ανήκουν στην ίδια ομαδοποίηση δρομολόγησης.

- Επόμενο δίκτυο στο μονοπάτι της επίθεσης, όπως αυτό αναγνωρίζεται από τον αποστολέα του μηνύματος.

- Τύπος της επίθεσης: πρωτόκολλο (IP, TCP, UDP, ICMP κ.λπ.) είδος πακέτου ή θύρα αναλόγως.
- Ο χρόνος που σημειώθηκε το περιστατικό ώστε να γίνει η χρονική συσχέτιση.

Ο προσδιορισμός ότι ένα μήνυμα αναφέρεται σε ένα συγκεκριμένο περιστατικό γίνεται από τη συμφωνία των πληροφοριών για το στόχο (που δίνεται από το στοιχείο Target του μηνύματος), τον τύπο της κακόβουλης κίνησης (που εξάγεται από τα στοιχεία `Service` και `AdditionalData` του μηνύματος) και την κοντινή χρονική απόσταση[6].

Από τη συνολική ανάλυση των μηνυμάτων που έχουν αποθηκευτεί για το περιστατικό προκύπτουν διάφορα συμπεράσματα για την πιθανή τοποθέτηση του δικτύου της Οντότητας σε σχέση με τη διαδρομή της επίθεσης:

α. Το δίκτυο είναι η πηγή της επίθεσης.

β. Το δίκτυο είναι πάνω στο μονοπάτι διέλευσης της επίθεσης· αυτή το διασχίζει με συγκεκριμένα σημεία εισόδου και εξόδου.

γ. Η επίθεση δεν διέρχεται από αυτό.

δ. Η Οντότητα δεν είναι σε θέση να αποφασίσει βάσει των διαθέσιμων πληροφοριών.

Πέρα από τις πληροφορίες μηνυμάτων που είναι αναγκαίες για να βγουν αυτά τα συμπεράσματα είναι επίσης απαραίτητη η γνώση από την Οντότητα της

[6] Παράμετρος του χρόνου κατά τη μετάβαση της Οντότητας προς την κατάσταση Ενεργοποίησης εξασφαλίζει την τελευταία προϋπόθεση.

διαδρομής προς το στόχο σε επίπεδο δικτύων (domains) για το σκοπό αυτό μπορεί να χρησιμοποιηθεί η πληροφορία που προσφέρεται από το πρωτόκολλο διαδικτυακής δρομολόγησης BGP [Rekh95] για τη διασύνδεση και απόσταση μεταξύ των Αυτόνομων Συστημάτων (Autonomous Systems, δηλαδή domains στην περίπτωση μας) προς το στόχο, ή τα βήματα προς τον στόχο με στοιχεία του *traceroute*.

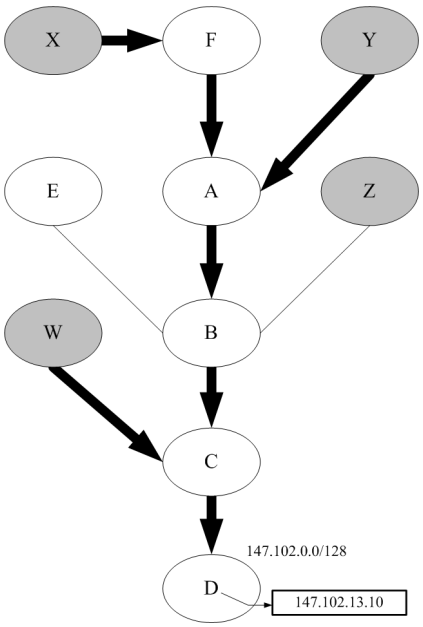
Για την παρουσίαση της διαδικασίας διαπίστωσης της τοποθέτησης του δικτύου ως προς το μονοπάτι της επίθεση παρατίθεται το επόμενο παράδειγμα:

Έστω το δίκτυο του Σχήματος 4.5 με τους λευκούς κόμβους να αντιπροσωπεύουν δίκτυα που συμμετέχουν στη Συνεργατική Υποδομή (κόμβοι A, B, C, D, E και F) και τους γκρίζους κόμβους δίκτυα που δε συμμετέχουν στην Υποδομή (κόμβοι W, X, Y και Z). Τα βέλη είναι η μετάδοση της κίνησης μιας επίθεσης DDoS διαμέσου του δικτύου αυτού. Η επίθεση έχει ως στόχο το σύστημα `147.102.13.10` στο δίκτυο D (που περιλαμβάνεται στην περιοχή διευθύνσεων `147.102.0.0/128`).

Στο παράδειγμα θα εξετάσουμε τη διαδικασία συμπερασμάτων για την Οντότητα του δικτύου B.

Στο δίκτυο B θα καταρτιστεί ο Πίνακας 4.3 με τις πληροφορίες που προκύπτουν από τα μηνύματα προειδοποίησης που έχει λάβει από τα συνεργαζόμενα δίκτυα[7].

[7]Το «Επόμενο Βήμα της Επίθεσης» αναφέρεται από τη σκοπιά του αποστολέα του μηνύματος.



Σχήμα 4.5: Ενδεικτικό δίκτυο ππου χρησιμοποιείται στο παράδειγμα

	Αποστολέας Μηνύματος	**Δίκτυο Πηγή της Επίθεσης**	**Επόμενο Βήμα της Επίθεσης**	**Δίκτυο Στόχος της Επίθεσης**	**Τύπος Περιστατικού**
1	A	F	B	D	1(πακέτα SYN, θύρα 22)
2	A	Y	B	D	1
3	C	B	D	D	1
4	C	W	D	D	1
5	D	C	Κανένας	D	1
6	F	X	A	D	1

Πίνακας 4.3: Συγκέντρωση στο δίκτυο B των πληροφοριών για το περιστατικό

Ο κόμβος B γνωρίζει από τα μηνύματα προειδοποίησης (alerts) ότι ο κόμβος D είναι ο τελικός στόχος. Έτσι μέσω των πληροφοριών δρομολόγησης μεταξύ αυτόνομων κοινοτήτων (Autonomous Systems - AS) που παρέχει το πρωτόκολλο BGP μπορεί να συμπεράνει τη διαδρομή προς το στόχο (σε επίπεδο δρομολόγησης AS) ως B-C-D.

Τα στοιχεία που αποδίδει η ανάλυση των γραμμών (rows) του πίνακα στο δίκτυο B έχει ως εξής:

Συμπεράσματα από τη γραμμή 1:

- Το δίκτυο B είναι στο δρόμο από το A προς τον τελικό στόχο D. Η διαπίστωση αυτή γίνεται από το γεγονός ότι το B χαρακτηρίζεται ως «Επόμενο Βήμα» στη διαδρομή προς το στόχο. Το δίκτυο B είναι σε θέση να επιβεβαιώσει αυτό το χαρακτηρισμό χρησιμοποιώντας για το στόχο την πληροφορία διαδρομής προς το στόχο.

- Τμήμα της διαδρομής της επίθεσης που διαπιστώνεται F-A-B

Συμπεράσματα από τη γραμμή 2:

Τα ίδια συμπεράσματα με τη γραμμή 1 και επιπλέον

- Τμήμα της διαδρομής της επίθεσης που διαπιστώνεται Y-A-B

Συμπεράσματα από τη γραμμή 3:

- Το δίκτυο B είναι πιθανή πηγή της επίθεσης. Το συμπέρασμα αυτό προκύπτει από τη διαθέσιμη πληροφορία που χαρακτηρίζει το δίκτυο B ως «Δίκτυο Πηγή» και επιβεβαιώνεται από την πληροφορία δρομολόγησης.

- Τμήμα της διαδρομής της επίθεσης που διαπιστώνεται B-C-D

Συμπεράσματα από τη γραμμή 4:

- Το δίκτυο B δεν αναφέρεται το ίδιο στο μήνυμα αλλά από την πληροφορία διαδρομής από το B προς το δίκτυο στόχο μπορεί να διαπιστωθεί ότι η διαδρομή που αναφέρεται στο εξεταζόμενο μήνυμα αφορά ένα άλλο μονοπάτι που συγκλίνει προς τον τελικό στόχο D στο δίκτυο C. Αυτό επειδή το δίκτυο C (που εμφανίζεται στο μήνυμα) έχει διαπιστωθεί ότι είναι και πάνω στη διαδρομή από το B στο στόχο.

- Τμήμα της διαδρομής της επίθεσης που διαπιστώνεται W-C-D

Συμπεράσματα από τη γραμμή 5:

- Δε μπορούμε να συμπεράνουμε από τη συγκεκριμένη γραμμή του πίνακα αν το δίκτυο B είναι στη διαδρομή επίθεσης ή πιθανή πηγή. Εντούτοις εδώ επαναλαμβάνεται το τμήμα C-D της διαδρομής από το B στο στόχο, το οποίο είναι και το κοινό τμήμα της διαδρομής που προκύπτει από τις γραμμές 3 και 4 του πίνακα.

- Τμήμα της διαδρομής της επίθεσης που διαπιστώνεται C-D

Συμπεράσματα από τη γραμμή 6:

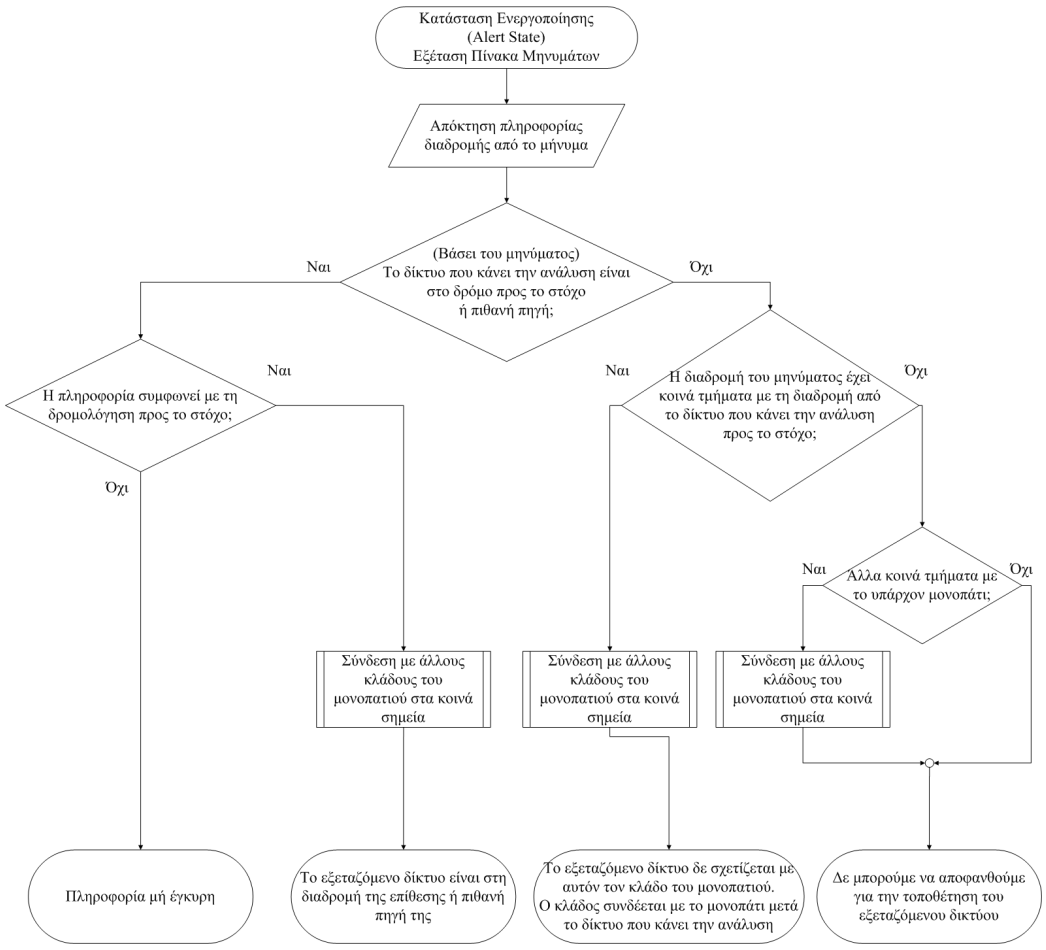
- Η διαδρομή της επίθεσης προκύπτει ως X-F-A. Εφόσον κανένα από τα προηγούμενα δίκτυα δεν περιλαμβάνεται στη διαδρομή από το δίκτυο B προς τον τελικό στόχο καταλήγουμε είτε ότι αποτελούν διαφορετικό κλάδο της επίθεσης, είτε είναι δίκτυα πριν το B στο δρόμο προς το στόχο. Ο (τελικός) συνδυασμός με τις προηγούμενες πληροφορίες διαδρομών αποκαλύπτει ότι πρόκειται για την τελευταία περίπτωση.

- Άρα, το δίκτυο B είναι στη διαδρομή προς τον τελικό στόχο D. Χρησιμοποιούμε και πάλι την πληροφορία δρομολόγησης BGP προς το τελικό θύμα.

Σύνοψη Αποτελεσμάτων για τον κόμβο B:

- Τελική διαπίστωση διαδρομής: X-F-A-B-C-D, Y-A-B-C-D και W-C-D
- Το δίκτυο που πραγματοποίησε την ανάλυση είναι πάνω στο μονοπάτι ή και πηγή της επίθεσης. Προτεινόμενα σημεία εφαρμογής μέτρων εναντίον της επίθεσης: Τα Σημεία Διασύνδεσης του AS B με τα AS A και C

Τα αποτελέσματα αυτά, εφόσον η Οντότητα έχει περιέλθει στην Κατάσταση Ενεργοποίησης θα μεταφερθούν στο Μηχανισμό Αντίδρασης. Το διάγραμμα ροής απόφασης για την τοποθέτηση του δικτύου ως προς την επίθεση καθώς και τη δημιουργία του μονοπατιού παρουσιάζεται στο Σχήμα 4.6. Αντίστοιχες ενέργειες διαπίστωσης του μονοπατιού πραγματοποιούν και οι υπόλοιποι κόμβοι της Συνεργατικής Υποδομής, με τελικό αποτέλεσμα την ταυτοποίηση των αντίσοτοιχων τμημάτων του.



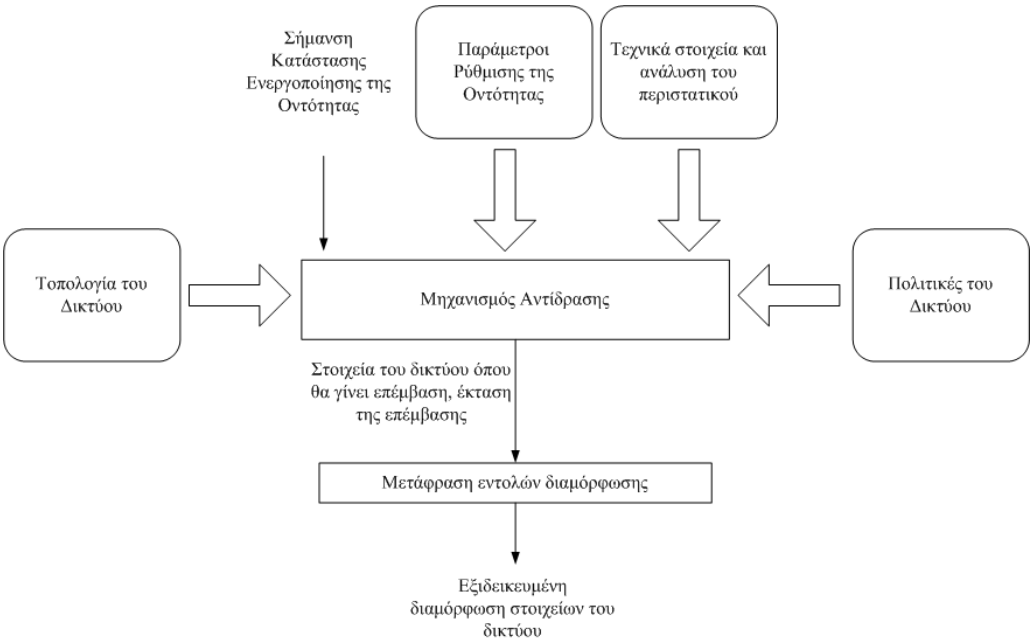
Σχήμα 4.6: Διάγραμμα ροής για τη διαπίστωση της τοποθέτησης του εξεταζόμενου δικτύου ως προς τη διαδρομή της επίθεσης

Μια πολύ ειδική περίπτωση που θεωρείται ακραία και μάλλον απίθανη είναι η πιθανότητα η Οντότητα να έχει περιέλθει σε Κατάσταση Ενεργοποίησης με την πλειοψηφία των μηνυμάτων να υποδεικνύουν ότι είναι εκτός μονοπατιού επίθεσης. Ακόμα και σε αυτή την περίπτωση το χειρότερο αποτέλεσμα που μπορεί να έχουμε είναι η λήψη μέτρων εναντίον της επίθεσης σε κάποιο δίκτυο το οποίο δεν είναι στη διαδρομή της επίθεσης. Στην περίπτωση αυτή το αποτέλεσμα θα είναι να επηρεαστεί μη κακόβουλη κίνηση η οποία θα έχει χαρακτηριστικά παρόμοια με αυτά της επίθεσης προς το δίκτυο θύμα. Αλλά παρόμοια μέτρα σε διαφορετικά δίκτυα, πιο κοντά στο θύμα, θα έχουν το αποτέλεσμα ούτως ή άλλως του περιορισμού αυτής της κίνησης.

4.3.5 Αντίδραση σε ένα περιστατικό

Αφότου εδραιωθεί η ύπαρξη ενός περιστατικού η Οντότητα χρησιμοποιεί τα στοιχεία της ανάλυσης για να αποφασίσει τις κατάλληλες ενέργειες. Στην ενδεικτική υλοποίηση της Οντότητας αυτές αναφέρονται στη βασική αντίδραση της αποκοπής της κακόβουλης κίνησης στο κατάλληλο σημείο του δικτύου, ανάλογα με την τοποθέτηση του δικτύου ως προς την επίθεση. Ο σχεδιασμός όμως υποστηρίζει και τη χρησιμοποίηση διαφορετικών πολιτικών φιλτραρίσματος της κακόβουλης κίνησης. Η αντίδραση στην επίθεση περιγράφεται από έναν αριθμό από προαποφασισμένες πολιτικές, διαφορετικές εφόσον αυτό είναι επιθυμητό, σε κάθε δίκτυο.

Ο Μηχανισμός Αντίδρασης καλείται με την είσοδο της Οντότητας στην Κατάσταση Ενεργοποίησης. Συνδυάζει στοιχεία, όπως παρουσιάζεται από το Σχήμα 4.7, από τις παραμέτρους διαμόρφωσης της Οντότητας, τα αποτελέσμα-



Σχήμα 4.7: Συνδυασμός Παραμέτρων - Στοιχείων Πολιτικής του Δικτύου

τα της Μονάδας Ανάλυσης (τεχνικά στοιχεία της επίθεσης και ανάλυση του περιστατικού), και τις προεπιλεγμένες πολιτικές. Οι πολιτικές αυτές διατυπώνονται σε μια από τις γλώσσες περιγραφής δικτύου και διαμόρφωσης ενεργών στοιχείων.

Μέσω των πολιτικών διατυπώνεται ένας αριθμός από διαφορετικές επεμβάσεις στη διέλευση της κίνησης από το δίκτυο. Οι διαφοροποιήσεις μπορούν να αναφέρονται τόσο σε διαφορετικές διάρκειες διακοπής της κακόβουλης κίνησης όσο και σε διαφορετικά ποσοστά παρεμπόδισης της, ορίζοντας διαφορετικές προδιαγραφές για το φιλτράρισμα της κακόβουλης κίνησης που αντιστοιχεί σε διαφορετικές επιθέσεις.

Επιπλέον εισαγωγή στοιχείων (input) στο Μηχανισμό Αντίδρασης αποτελεί η περιγραφή της τοπολογίας του δικτύου με τις ενεργές συσκευές του. Δίνεται

έμφαση στην ακριβή περιγραφή των ενεργών συσκευών στα σημεία διασύνδεσης με άλλα δίκτυα και η εισαγωγή πληροφοριών για τα γειτονικά δίκτυα (περιοχή διευθύνσεων IP).

Ο Μηχανισμός Αντίδρασης χρησιμοποιεί τα στοιχεία από τα μηνύματα που έχει λάβει η Οντότητα για να αξιολογήσει τη σοβαρότητα του περιστατικού. Ένα μέτρο αυτής έχει επιλεγεί να είναι ο μετρητής της συνολικής σοβαρότητας του περιστατικού («συσσωρευτής βεβαιότητας») *Notification_counter*. Αυτός με τη σειρά του επηρεάζεται από την τοπική προέλευση των μηνυμάτων (παράμετρος Local_value), την εμπιστοσύνη του αποστολέα για την προειδοποίηση (παράμετρος *Confidence_count*) και την εμπιστοσύνη που αναθέτει η Οντότητα στις αναφορές καθενός αποστολέα (παράμετρος *Sender_confidence*). Σημαντικό ρόλο στη διάγνωση της σοβαρότητας του περιστατικού παίζει το κατά πόσο ο μετρητής αυτός έχει ξεπεράσει το όριο ενεργοποίησης της Οντότητας (παράμετρος *Alert_threshold*). Επίσης χρησιμοποιείται και ο χρόνος μέσα στον οποίο εξελίχθηκε το περιστατικό, από τη στιγμή που στάλθηκε το πρώτο σχετικό μήνυμα, μέχρι την ενεργοποίηση της Οντότητας παράμετρος *Event_time*). Καταλήγουμε έτσι στη διαπίστωση της σοβαρότητας του περιστατικού με τον υπολογισμό ενός εμπειρικού μέτρου που θα χρησιμοποιηθεί για την επιλογή της αντίστοιχης πολιτικής. Έτσι, ως Σοβαρότητα Επίθεσης, S, ορίζουμε το αποτέλεσμα:

$$S = (N - A + 1)/E$$

όπου:

- N είναι η τιμή της παραμέτρου *Notification_counter* (ο «Συσσωρευτής Βεβαιότητας» για το περιστατικό) τη στιγμή που η Οντότητα πέρασε σε

Κατάσταση Ενεργοποίησης

- A είναι η τιμή του ορίου, *Alert_threshold*, πέρα από το οποίο η Οντότητα πραγματοποιεί τη μετάβαση σε Ενεργοποιημένη Κατάσταση.

- E είναι η (κανονικοποιημένη) τιμή της μέτρησης *Event_time*, ο χρόνος που χρειάστηκε από τη στιγμή άφιξης του πρώτου σχετικού μηνύματος μέχρι τη μετάβαση της Οντότητας στην Ενεργοποιημένη Κατάσταση.

Η Σοβαρότητα S, επομένως αποτυπώνει το πόσο έχει ξεπεραστεί το όριο Ενεργοποίησης και με τι ταχύτητα. Η τιμή που προκύπτει είναι μεγαλύτερη του μηδενός (0) και συνεχώς αυξανόμενη μια και υπολογίζεται μόνον όταν η Οντότητα είναι ενεργοποιημένη, οπότε ισχύει $N > A$. Η τιμή της S θα αυξάνεται στις περιπτώσεις:

- Όπου έχουμε μεγάλη «συσσώρευση βεβαιότητας» για ένα περιστατικό με σημαντική υπέρβαση του ορίου Ενεργοποίησης (μεγάλη τιμή $N - A$)

- Όπου ένα περιστατικό φαίνεται να εξελίσσεται με μεγάλη ταχύτητα, οπότε η Οντότητα έχει περάσει σε κατάσταση Ενεργοποίησης σε πολύ μικρό χρονικό διάστημα *Event_time*.

Το προβλεπόμενο διάστημα τιμών της Σοβαρότητας S διαχωρίζεται σε τμήματα (όχι αναγκαστικά ίσα), τόσα, όσες οι επιθυμητές πολιτικές αντίδρασης. Έτσι ανάλογα με το διάστημα στο οποίο κυμαίνεται η παράμετρος S επιλέγεται η πολιτική αντίδρασης που αντιστοιχεί στην προβλεπόμενη σοβαρότητα του περιστατικού.

Σκοπός αυτής της ανάλυσης ήταν η κατανόηση των παραμέτρων που μπορούν να χρησιμοποιηθούν για τον καθορισμό της σοβαρότητας μιας επίθεσης

και η εξαγωγή ενός μέτρου σύγκρισης της σοβαρότητας των επιθέσεων ώστε να επιλέγεται η κατάλληλη κάθε φορά πολιτική. Το ποια θα είναι αυτή αλλά και τι δυνατότητες παρέμβασης θα παρέχει είναι θέμα υλοποίησης αλλά και επιλογής εργαλείων επέμβασης στο δίκτυο.

Από πλευράς υλοποίησης δοκιμάστηκε μέσω προσομοιώσεων ένας μηχανισμός αντίδρασης σε περιστατικά DDoS μετά το πέρασμα μιας Οντότητας σε Alert State. Τα στοιχεία εξέλιξης του περιστατικού (αριθμός τοπικών ή απομακρυσμένων μηνυμάτων, χρόνος μέσα στον οποίο η Οντότητα ενεργοποιήθηκε) χρησιμοποιήθηκαν για τον υπολογισμό και την ανάθεση «Βαθμού Σοβαρότητας» στο περιστατικό. Στη συνέχεια στοιχεία της τοπολογίας του δικτύου σε συνδυασμό με βασικές πολιτικές αντίδρασης βάσει της σοβαρότητας συνδυάστηκαν για να αποτελέσουν είσοδο στο εργαλείο Netspoc [Nets] που παράγει αυτόματα Λίστες Ελέγχου Πρόσβασης (Access Control Lists) για τους κατάλληλους (ανάλογα με το περιστατικό) δρομολογητές του δικτύου. Το εργαλείο αυτό, αν και προσέφερε μικρό βαθμό ευελιξίας κατέδειξε ότι η εφαρμογή πολιτικών αντιμετώπισης μπορεί να γίνει με αυτόματο τρόπο. Τα μέτρα που εφαρμόστηκαν ήταν το πλήρες φιλτράρισμα της επιθετικής κίνησης προς τον τελικό στόχο, διαχωρίστηκαν δε μόνο ως προς το χρόνο διάρκειας της εφαρμογής τους [Αλευ05].

4.4 Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε η αρχιτεκτονική και η εσωτερική λειτουργία της Συνεργατικής Οντότητας, του βασικού συστήματος που κάνει δυνατή τη δημιουργία της Συνεργατικής Υποδομής. Τα κυριότερα χαρακτηριστικά των

Οντοτήτων που έχουν βασική σημασία για την κατανόηση της φιλοσοφίας λειτουργίας της Αρχιτεκτονικής αλλά και για την ανάλυση των αποτελεσμάτων των προσομοιώσεων που ακολουθούν είναι τα εξής:

- Η αρχιτεκτονική λογισμικού της Οντότητας είναι χωρισμένη σε τμήματα (modules) ακολουθώντας το πρότυπο των αυτόνομων προγραμματιστικών διεργασιών (autonomous agents). Είναι έτσι δυνατή επιλεκτικά η διακοπή λειτουργίας, η αναβάθμιση και η επανεκκίνηση επιμέρους τμημάτων της Οντότητας.

- Η Οντότητα περνά διαδοχικά σε καταστάσεις ενεργοποίησης (Normal State – Suspicion State – Alert State) «συσσωρεύοντας» βεβαιότητα για κάποιο περιστατικό. Σε επίπεδο πολλαπλών δικτύων η διάκριση αυτή μπορεί να καταδείξει τα σημεία που ένα περιστατικό γίνεται πιο έντονα αντιληπτό.

- Η λειτουργία της Οντότητας ελέγχεται με μια σειρά από παραμέτρους από τον τοπικό διαχειριστή κάθε επιμέρους δικτύου. Οι παράμετροι αυτοί μεταξύ άλλων μπορούν να καθορίσουν την «εμπιστοσύνη» (βάρος — weight) που θα αποδοθεί σε απομακρυσμένες αναφορές, ποιο επίπεδο συσσώρευσης βεβαιότητας θα θεωρηθεί ως ασφαλής ένδειξη περιστατικού και για πόσο διάστημα η Οντότητα θα παραμείνει σε μια κατάσταση ενεργοποίησης όσο δε λαμβάνει νέες αναφορές. Στην πράξη κάποιες από αυτές τις παραμέτρους είναι προτιμότερο να αποφασίζονται από κοινού από όλα τα δίκτυα προκειμένου να υπάρχει κοινή συμπεριφορά των συμμετεχόντων στη Συνεργασία.

- Τα μηνύματα που στέλνονται από τα δίκτυα-κόμβους της Συνεργατικής Αρχιτεκτονικής περιέχουν (με επέκταση της προδιαγραφής IDMEF του IETF) την πληροφορία προηγούμενου και επόμενου δικτύου (όπως συμπε-ραίνονται στο δίκτυο-αποστολέα) στο μονοπάτι της επίθεσης. Η πληροφορία αυτή συγκεντρώνεται σε κάθε κόμβο-παραλήπτη και όταν αυτός περάσει σε κατάσταση Alert χρησιμοποιείται ώστε (α) να διαγνωστεί η θέση του κόμβου πάνω στο μονοπάτι της επίθεσης και (β) να διαπιστωθεί το μεγαλύτερο δυνατό τμήμα του μονοπατιού.

- Βάσει των χαρακτηριστικών της επίθεσης αλλά και τη διαγνωσμένη τοποθέτηση του δικτύου-κόμβου πάνω στο μονοπάτι της επίθεσης είναι δυνατόν να προσαρμοστεί το είδος, η ένταση της αντίδρασης στην επίθεση καθώς και το σημείο εφαρμογής της. Τα ανωτέρω τεκμηριώθηκαν με σχετικές υλοποιήσεις σε μικρή κλίμακα που πραγματοποιήσαμε.

Στο επόμενο κεφάλαιο ακολουθεί η ανάλυση της λειτουργίας της Συνεργατικής Υποδομής ως γενικό σύνολο, μέσω προσομοίωσης.

Κεφάλαιο 5

Προσομοίωση και Ανάλυση της Λειτουργίας του Συνεργατικού Υπερκείμενου Δικτύου

5.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζονται μια σειρά από πειραματικές δοκιμές που έγιναν πάνω στη λειτουργία και τη συμπεριφορά της Συνεργατικής Υποδομής. Οι δοκιμές αυτές έγιναν μέσω προσομοίωσης κάποιων περιστατικών επιθέσεων DDoS σε ενδεικτικό δίκτυο με πολλαπλά domains. Τα συστήματα IDS καθώς και τα τοπολογικά χαρακτηριστικά των επιμέρους domains (AS) μοντελοποιήθηκαν με μια σειρά από παραδοχές συμβατές με την τρέχουσα εμπειρία από τη διαχείριση δικτύων όπως αυτά του Ε.Μ.Π. και του Ε.Δ.Ε.Τ.

5.2 Σκοποί της προσομοίωσης

Το Υπερκείμενο Συνεργατικό Δίκτυο, όπως φάνηκε από τα κεφάλαια 3 και 4 συνθέτει ένα πολύπλοκο σύστημα συνολικά το οποίο επηρεάζεται στη λειτουργία του από πολλές διαφορετικές παραμέτρους τόσο εσωτερικά (δείτε τους σχετικούς πίνακες για τις παραμέτρους διαμόρφωσης των Οντοτήτων του κεφ. 4), όσο και εξωτερικά.

Αστάθμητοί εξωτερικοί παράγοντες που μπορούν να επηρεάσουν αυτή τη λειτουργία είναι:

1. Οι ιδιαιτερότητες των συστημάτων IDS σε κάθε επιμέρους δίκτυο (επαναλαμβάνοντας τα συμπεράσματα του τμήματος 2.3.1): η μεθοδολογία αναγνώρισης, οι παράμετροι ρύθμισης (και κατ΄ επέκταση τα χαρακτηριστικά «φυσιολογικής» κίνησης στο συγκεκριμένο δίκτυο), το χρονικό παράθυρο ανίχνευσης, η πιθανή χρήσης «βαθμών βεβαιότητας»[1].

2. Άλλα ζητήματα που είναι δυνατόν να εμποδίσουν την ομαλή ανταλλαγή αποτελεσμάτων και κατά συνέπεια την αποτελεσματική λειτουργία του Υπερκείμενου Δικτύου, π.χ. διαθεσιμότητα γραμμών λόγω επίθεσης κ.λπ.

Κύριος σκοπός των προσομοιώσεων σε αυτή την εργασία είναι η διαπίστωση της συμπεριφοράς του Συνεργατικού Δικτύου ως προς τα εξής:

- Πληρότητα της συνεργατικής ανίχνευσης (κατά πόσον όλα τα δίκτυαμέλη αντιλήφθηκαν το ίδιο περιστατικό που τα αφορούσε). Αυτό αφορά

[1] Δηλαδή το κατά πόσον το σύστημα IDS χρησιμοποιεί μια «κλιμακωτή» ανίχνευση (με ανάθεση βαθμού βεβαιότητας) των περιστατικών αντί για ανίχνευση δύο καταστάσεων (υπάρχει ή δεν υπάρχει περιστατικό)

τη Συνεργατική Υποδομή συνολικά πέρα από την κατά τόπους πληρότητα που παρουσιάζουν τα επιμέρους συστήματα IDS.

- Ταχύτητα συνολικής ανίχνευσης για ολόκληρη τη Συνεργατική Υποδομή (εφόσον επιτεύχθηκε κάτι τέτοιο).
- Ευαισθησία σε πιθανές λάθος ανιχνεύσεις (False Positives) σε κάποια μόνον από τα επιμέρους δίκτυα της Υποδομής.

Η συμπεριφορά αυτή ζητείται να αξιολογηθεί βάσει των κυρίων παραμέτρων ρύθμισης των Οντοτήτων της Συνεργατικής Αρχιτεκτονικής, ώστε να καθοριστεί η επίδραση τους και να αξιολογηθούν πιθανές ρυθμίσεις που θα επιφέρουν καλύτερα αποτελέσματα στις ζητούμενες λειτουργίες.

Προς αυτή την κατεύθυνση είναι επιθυμητό να προσομοιωθεί η επίδραση των αναφερόμενων εξωτερικών παραγόντων κατά τρόπο που να αποτελεί κατά το δυνατόν σταθερή (ανά επανάληψη της προσομοίωσης) εξωτερική είσοδο (διέγερση) του συστήματος ενώ το βάρος της επίδρασης στο σύστημα να αποδοθεί στις παραμέτρους διαμόρφωσης των Οντοτήτων.

5.3 Συνολική Λειτουργία της Συνεργατικής Υποδομής

Συνοψίζοντας την παρουσίαση της Συνεργατικής Υποδομής του κεφ. 4, η προβλεπόμενη ροή λειτουργίας της στην πράξη (ασχέτως του χρησιμοποιούμενου υποβάθρου χαμηλού επιπέδου και των εσωτερικών λεπτομερειών υλοποίησης) αναμένεται να έχει ως εξής:

1. Ένα περιστατικό επίθεσης ανιχνεύεται από το τοπικό σύστημα (ή ιεραρχία συστημάτων) IDS σε ένα ή περισσότερα δίκτυα - μέλη της Υποδομής.

2. Οι Οντότητες των δικτύων που πραγματοποίησαν την ανίχνευση, εφόσον για το συγκεκριμένο περιστατικό έχουν περάσει στην κατάσταση Ενεργοποίησης (Alerted State), μεταδίδουν σε όλα τα μέλη της υποδομής τη σχετική πληροφορία.

3. Οι παραλήπτες της αναφοράς, ανάλογα με τις ρυθμίσεις που έχουν γίνει στις δικές τους Οντότητες, περνούν επίσης ή όχι σε κατάσταση ενεργοποίησης. Το πέρασμα αυτό βασίζεται τόσο σε τυχόν υπάρχουσες εσωτερικές αναφορές τους (από τα τοπικά συστήματα IDS) όσο και από τη συσσώρευση βεβαιότητας που προκύπτει από τις ληφθείσες απομακρυσμένες αναφορές.

4. Με το πέρασμα στην κατάσταση Ενεργοποίησης (Alert State) δημιουργούν ή όχι τις δικές τους αναφορές προς την Υποδομή βάσει του βαθμού τοπικής προέλευσης των μηνυμάτων που οδήγησαν στην κατάσταση αυτή.

5. Με το πέρας του περιστατικού είτε υπάρχει ένα σχετικό μήνυμα ενημέρωσης από τα συστήματα IDS είτε περνάει ο χρόνος αναμονής σε κατάσταση Ενεργοποίησης με αποτέλεσμα σταδιακά η Υποδομή να επιστρέφει σε κατάσταση Φυσιολογικής λειτουργίας (Normal State).

5.4 Σύνοψη των λειτουργιών συστημάτων IDS για ανίχνευση περιστατικών DDoS

Η αυτόματη ανίχνευση επιθέσεων DDoS βασίζεται στην παρατήρηση «ανωμαλιών» σε κάποιες παραμέτρους χρησιμοποίησης του δικτύου (σε αντίθεση με την διερεύνηση γνωστών χαρακτηριστικών —«υπογραφές» —που χρησιμοποιούνται για την ανίχνευση επιθέσεων άλλου είδους). Η αναγνώριση των παραμέτρων γίνεται συγκρίνοντας αυτό που θωρείται «φυσιολογική» λειτουργία του δικτύου με την τρέχουσα κατάσταση που επικρατεί και εφόσον παρατηρηθούν διαφοροποιήσεις πέραν ενός ορίου θεωρείται ότι υπάρχει κάποιο περιστατικό εν εξελίξει.

Με αυτή την προσέγγιση τίθεται μια σειρά από ζητήματα που αφορούν τη συμπεριφορά των IDS ως εισόδων της προσομοίωσης. Τα ζητήματα αυτά εξαρτώνται μερικώς από τον αλγόριθμο ανίχνευσης που χρησιμοποιείται και απαιτείται να αναλυθούν για να προσεγγιστούν ως προς την επίδραση τους στην προσομοίωση. Τα σημαντικότερα είναι:

1. Η μία ή περισσότερες παράμετροι λειτουργίας του δικτύου που θα τεθούν υπό παρακολούθηση προκειμένου να διαπιστωθούν ανωμαλίες. Σε πρόσφατες ερευνητικές προσπάθειες υπάρχει ποικιλία προτάσεων για διάφορες παραμέτρους που μπορούν να βοηθήσουν την ανίχνευση συγκεκριμένων ειδών επιθέσεων[2]. Ενδεικτικά αναφέρονται:

   - Οι αναλογίες πακέτων ενός συγκεκριμένου είδους ως προς το συνολικό μέγεθος της κίνησης για ανίχνευση επιθέσεων "SYN floods"

[2] Δείτε τη σχετική ανάλυση στο κεφ. 2

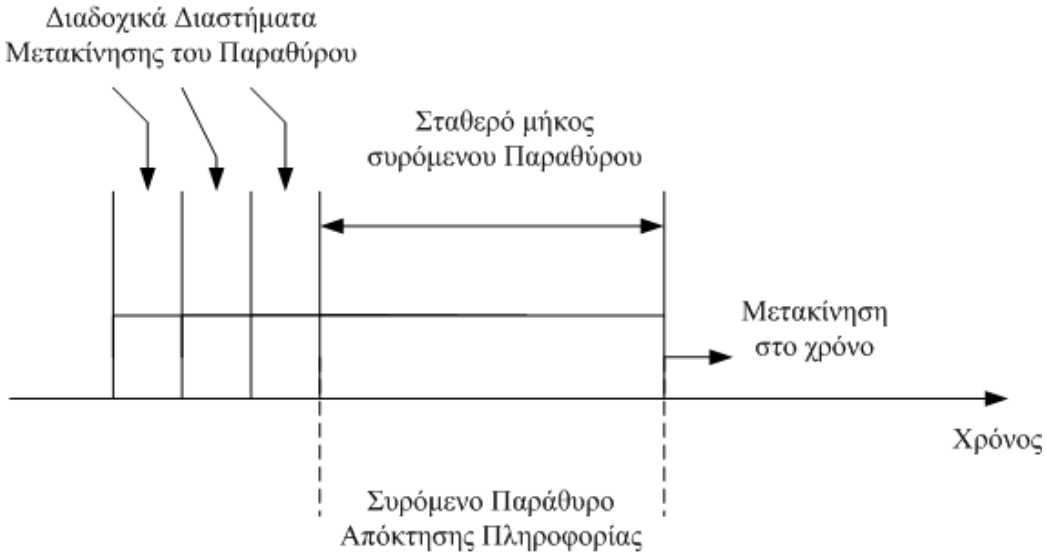
[Maha02]. Η μέθοδος αυτή καταλήγει στη διαπίστωση του συγκεκριμένου είδους της επίθεσης.

- Η αναλογία δικτυακών ροών με μικρό αριθμό πακέτων [Andr04] κ.λπ.

Είναι δυνατόν επίσης να γίνει συνδυασμός πολλών διαφορετικών παραμέτρων με διαφορετικούς βαθμούς συνεισφοράς στην εδραίωση βεβαιότητας για διαφορετικές επιθέσεις [Siat04].

2. Το τι θεωρείται φυσιολογική κίνηση βάσει του οποίου θα γίνουν οι συγκρίσεις με τις τρέχουσες τιμές. Πιθανές επιλογές είναι:

   - Χρήση των χαρακτηριστικών της κίνησης από συγκεκριμένα διαστήματα στα οποία ήταν δεδομένη η απουσία επιθετικών περιστατικών.
   - Χρήση μέσων ή μέγιστων τιμών των παραμέτρων που θα παρακολουθηθούν, με προέλευση τα ίδια διαστήματα «φυσιολογικής» λειτουργίας
   - Χρήση «συρόμενου παραθύρου» ("sliding window") για τη σύγκριση της τρέχουσας (υπό εξέταση) κίνησης με τις τιμές της σε ένα πρόσφατο διάστημα (αλγόριθμος «προσαρμοζόμενων ορίων» —"adaptive threshold"). Μια απεικόνιση της μεθόδου «συρόμενου παραθύρου» δίνεται στο Σχήμα 5.1. Ζητήματα που τίθενται με αυτή την προσέγγιση είναι (α) η αδυναμία ανίχνευσης διαφοροποιήσεων με πολύ αργούς ρυθμούς εξέλιξης ή μικρές συνολικά διαφοροποιήσεις, (β) η ανάγκη ανίχνευσης στο πρώτο χρονικό διάστημα σύγκρισης. Και στις δύο προηγούμενες περιπτώσεις αν δεν επιτευχθεί το συντομό-

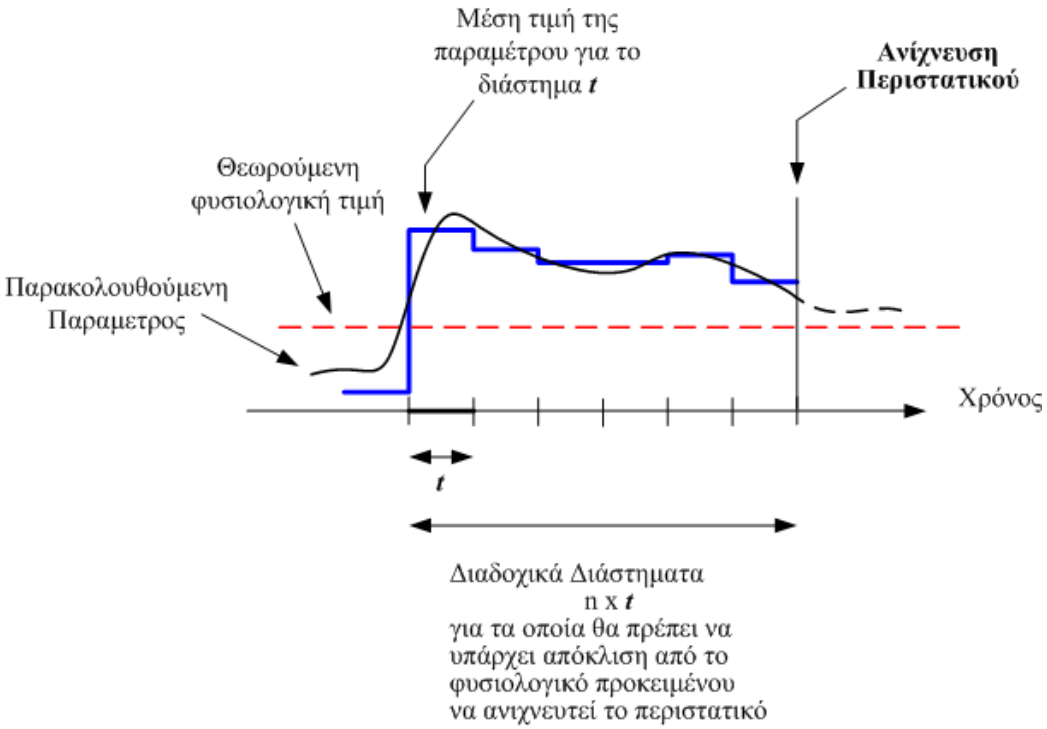


Σχήμα 5.1: Μέθοδος «συρόμενου παραθύρου» κατά την περίοδο «εκμάθησης»

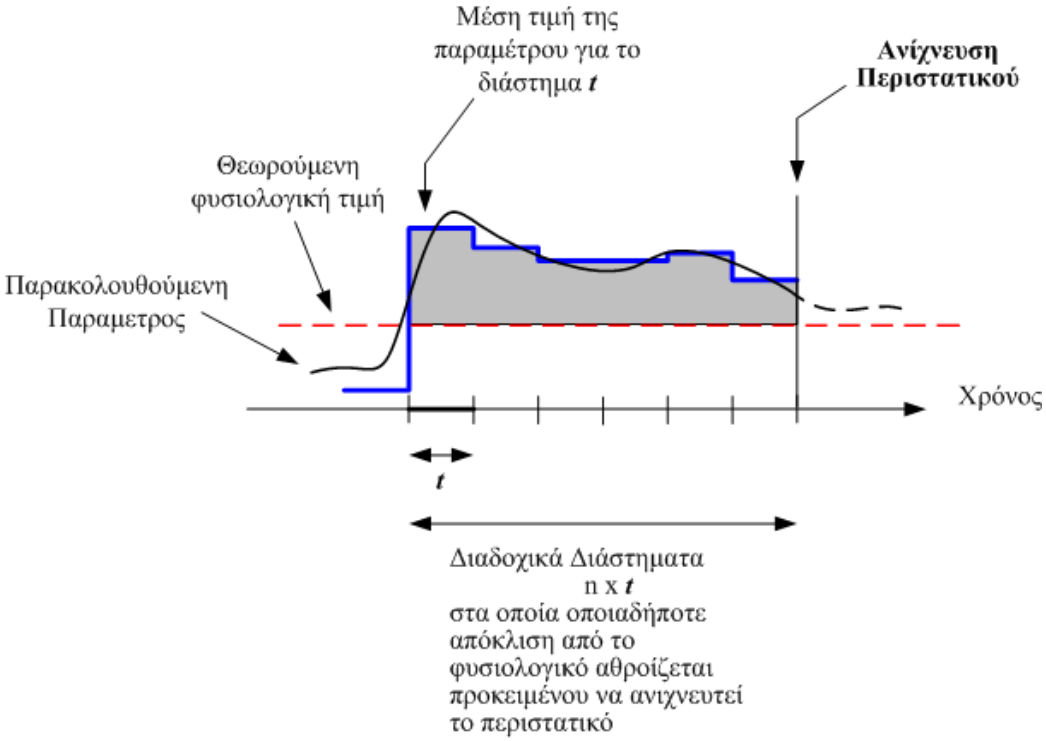
τερο η ανίχνευση οι τιμές της «προβληματικής» κίνησης θα αποτελέσουν μετά από λίγο (λόγω του «συρόμενου παραθύρου») μέρος αυτού που θεωρείται «νόρμα» σύγκρισης. Επίσης σε περίπτωση που αναγνωριστεί επιτυχώς το περιστατικό πρέπει να ληφθούν πρόνοια ώστε να μην εισάγονται πλέον τρέχοντα στοιχεία στο μηχανισμό του «συρόμενου παραθύρου».

3. Το χρονικό διάστημα μέσα στο οποίο θα γίνει η ανίχνευση. Ανά σύστημα IDS είναι δυνατή η χρήση ενός ή περισσοτέρων διαστημάτων σύγκρισης ανάλογα με τον αλγόριθμο ανίχνευσης. Έτσι σε αλγορίθμους παρατήρησης και σύγκρισης της τρέχουσας λειτουργίας σε σχέση με τη θεωρούμενη ως «φυσιολογική» συμπεριφορά (π.χ. αλγόριθμος «προσαρμοζόμενων ορίων») έχουμε τη χρήση ενός ή περισσοτέρων διαστημάτων σύγκρισης

στα οποία θα πρέπει να έχουμε απόκλιση άνω ενός ορίου για να ανιχνευτεί ένα περιστατικό. Η μέθοδος αυτή απεικονίζεται στο Σχήμα 5.2. Σε άλλες περιπτώσεις υπάρχει συνδυασμός της χρήσης των διαστημάτων ανίχνευσης, όπως στον αλγόριθμο «Συσσωρευμένων Αθροισμάτων» —"Cumulative Sum" ή CUSUM [Siri04]. Το Σχήμα 5.3 παρουσιάζει τη μέθοδο αυτή.



Σχήμα 5.2: Χρήση της μεθόδου "Adaptive Threshold" κατά την περίοδο ανίχνευσης



Σχήμα 5.3: Χρήση της μεθόδου "Cumulative Sum" κατά την περίοδο ανίχνευσης

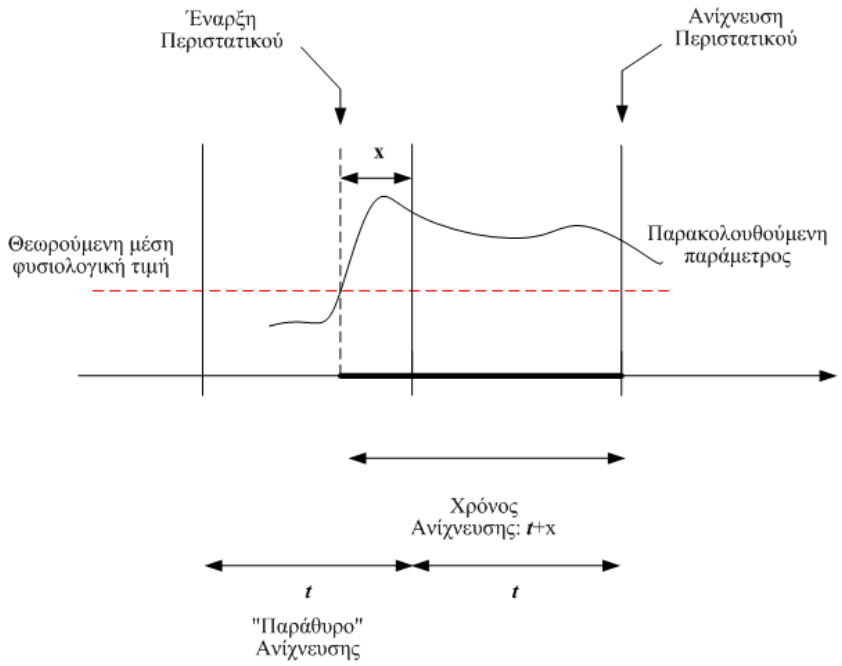
4. Η ύπαρξη ή όχι διαφορετικών επιπέδων βεβαιότητας ανίχνευσης

5.4.1 Εξέταση του χρόνου ανίχνευσης

Για την ανίχνευση των περιστατικών, αν χρησιμοποιηθεί η κοινή πρακτική του «παραθύρου» ανίχνευσης, μήκους t, έχουμε τα εξής ενδεχόμενα:

1. Η έναρξη του περιστατικού να είναι λίγο πριν, έστω χρονικό διάστημα x, την εκκίνηση νέου παραθύρου αναγνώρισης. Σε αυτή την περίπτωση δε θα υπάρξει ανίχνευση στο αμέσως επόμενο σημείο ελέγχου αλλά θα χρειαστεί να μεσολαβήσει άλλο ένα διάστημα t ώστε να «συσσωρευτεί»

βεβαιότητα (όπως περιγράφηκε προηγουμένως) για την ύπαρξη περιστατικού, όπως φαίνεται στο Σχήμα 5.4.

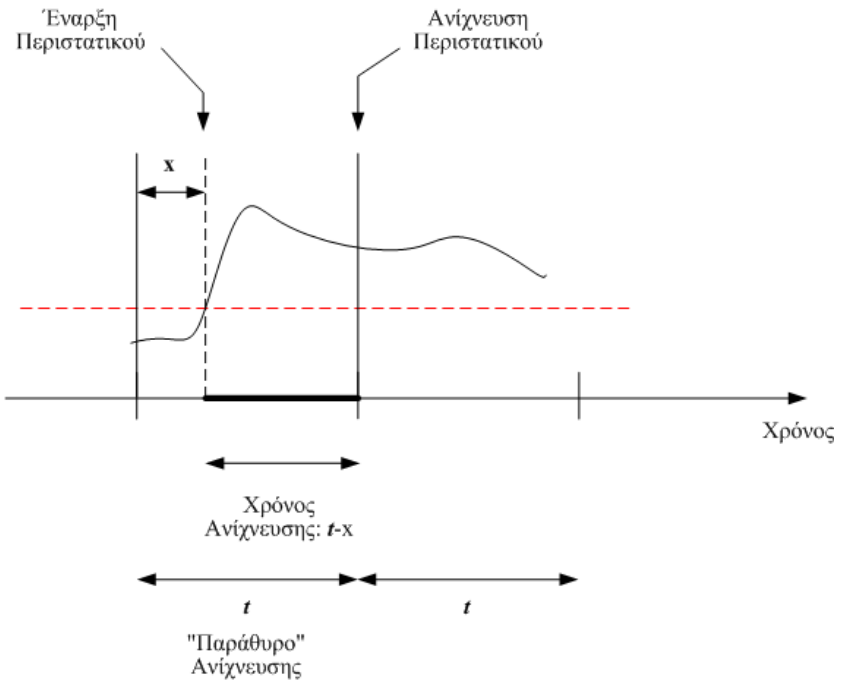


Σχήμα 5.4: Χρόνος που μεσολαβεί για την ανίχνευση του περιστατικού ίσος με $t + x$

Σε αυτή την περίπτωση ο χρόνος που θα μεσολαβήσει για την ανίχνευση του περιστατικού θα είναι:

$$\omega = t + x \tag{5.1}$$

2. Η έναρξη του περιστατικού να είναι λίγο μετά, κατά χρονικό διάστημα x, την εκκίνηση νέου παραθύρου αναγνώρισης. Αυτό θα δώσει χρόνο στο σύστημα IDS να συσσωρεύσει βεβαιότητα και να ανιχνεύσει το περιστατικό κατά τον επόμενο έλεγχο παραθύρου ανίχνευσης. Η περίπτωση αυτή φαίνεται στο Σχήμα 5.5.



Σχήμα 5.5: Χρόνος που μεσολαβεί για την ανίχνευση του περιστατικού ίσος με $t - x$

Ο χρόνος που θα μεσολαβήσει για την ανίχνευση του περιστατικού θα είναι:

$$\omega = t - x \tag{5.2}$$

Συνοψίζοντας τις σχέσεις 5.1 και 5.2 καταλήγουμε στη γενικότερη διατύπωση:

$$\omega = t + x \tag{5.3}$$

όπου για το x ισχύει:

$$-t < x < t \tag{5.4}$$

Διευκρινιστικά, ανάλογα με τις τιμές του x έχουμε για το συνολικό χρόνο ανίχνευσης ω:

- Αν το x βρίσκεται στην περιοχή του μηδενός, τότε ο χρόνος ανίχνευσης της επίθεσης ω τοποθετείται στην περιοχή του t, δηλαδή η αρχή του περιστατικού ταυτίζεται με την αρχή του παραθύρου.

- Αν το x είναι στην περιοχή του t, τότε το ω είναι στην περιοχή $2t$ και έχουμε την περίπτωση όπου το περιστατικό ξεκίνησε κοντά στην αρχή ενός παραθύρου αναγνώρισης αλλά (πιθανά λόγω μικρής έντασης) δεν ανιχνεύτηκε παρά μόνον όταν συμπληρώθηκε και δεύτερο παράθυρο ανίχνευσης.

- Αν το x είναι στην περιοχή του $-t$, έχουμε ω στην περιοχή 0. Η εξήγηση αυτής της περίπτωσης είναι ότι το περιστατικό ξεκίνησε λίγο πριν το τέλος του παραθύρου ανίχνευσης αλλά παρόλα αυτά ανιχνεύτηκε (πιθανά λόγω μεγάλης έντασης)

Καταλήγουμε έτσι ότι το ω ανήκει στο διάστημα $(0, 2t)$.

Στην πράξη, κατά το σχεδιασμό μιας προσομοίωσης που περιλαμβάνει πολλαπλά δίκτυα υπάρχουν δύο αστάθμητοι παράγοντες:

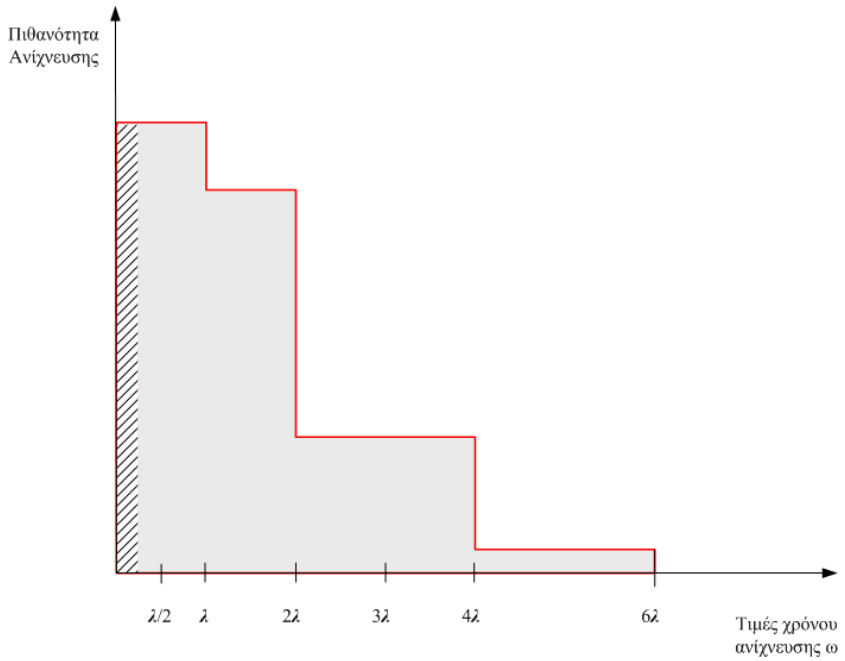
1. Ακόμα και αν το περιστατικό εμφανιστεί σε κάθε ένα δίκτυο την ίδια στιγμή δε θα υπάρχει συγχρονισμός ως προς το σημείο που βρίσκεται το παράθυρο ανίχνευσης του συστήματος IDS σε κάθε δίκτυο. Έτσι σε κάθε ένα δίκτυο θα γίνει τυχαία η ανίχνευση μετά από χρόνο ω που παίρνει τιμές στο διάστημα $(0, 2t)$, όπως αναλύθηκε προηγουμένως.

2. Κάθε δίκτυο (domain) επιλέγει για τα τοπικά συστήματα IDS διαφορετικό μήκος παραθύρου αναγνώρισης t.

Ως προς το ζήτημα 1. είναι φανερό ότι ο χρόνος ανίχνευσης ω για κάθε ένα από τα δίκτυα που θα συμπεριλαμβάνονται στην προσομοίωση θα έχει τυχαία τιμή στο διάστημα $(0, 2t)$ ακολουθώντας την ομοιόμορφη κατανομή.

Ως προς το ζήτημα 2., κάνουμε την υπόθεση ότι τα διάφορα δίκτυα επιλέγουν μια κοινή, πρακτική τιμή λ ως μήκος παραθύρου ανίχνευσης, π.χ, τα 5 λεπτά, καθώς και κάποια πολλαπλάσια (ή υποπολλαπάσια) αυτής με φθίνουσα πιθανότητα. Λαμβάνοντας υπ' όψιν το ότι για κάθε μήκος παραθύρου ανίχνευσης t θα ισχύει και πάλι χρόνος ανίχνευσης στο διάστημα $(0, 2t)$ και με λεπτομερή ανάλυση καταλήγουμε στην κατανομή της πιθανότητας χρόνου ανίχνευσης από οποιοδήποτε από τα μέλη της Συνεργατικής υποδομής όπως φαίνεται στο Σχήμα 5.6. Το Σχήμα αυτό δίνει τις *πιθανότητες* για το *χρόνο μέσα στον οποίο θα επιτευχθεί η ανίχνευση* σε *οποιοδήποτε* από τα μέλη της Συνεργατικής Υποδομής.

Στις προσομοιώσεις δοκιμάστηκε η περίπτωση τα δίκτυα της Υποδομής να επιλέγουν διάφορα παράθυρα ανίχνευσης μήκους $n * \lambda$ (με $n = 1/2,\ 1,\ 2$ και 3). Οι προσομοιώσεις όμως έδειξαν ότι δεν υπάρχει ουσιαστική διαφορά στα αποτελέσματα σε σχέση με την επιλογή κοινού παραθύρου ανίχνευσης για κάθε δίκτυο της Συνεργατικής Υποδομής.



Σχήμα 5.6: Πιθανότητα για το χρόνο ανίχνευσης σε οποιοδήποτε από τα μέλη της Συνεργατικής Υποδομής

5.5 Προϋποθέσεις και Απλοποιήσεις που ελήφθησαν υπ' όψιν

Βάσει όλων των ανωτέρω, καθώς και εξ' αιτίας της έλλειψης αντίστοιχων μελετών στη βιβλιογραφία ως προς τις ακολουθούμενες ρυθμίσεις των συστημάτων IDS ανίχνευσης ανωμαλιών αποφασίστηκαν μια σειρά από προσεγγίσεις στην προσομοίωση ως εξής:

1. Τα συστήματα IDS που βρίσκονται σε δίκτυα πιο κοντά στο τελικό στόχο, κατά τέτοιο τρόπο ώστε να διέρχεται από αυτά μεγαλύτερος όγκος συγκλίνουσας κίνησης, έχουν υψηλότερη πιθανότητα να ανιχνεύσουν ένα περιστατικό DDoS λόγω της μεγαλύτερης ανωμαλίας συνολικά στην τελι-

κή κίνηση. Πιο συγκεκριμένα επιλέχθηκαν πιθανότητες ανίχνευσης $0,95$ και $0,90$ ανάλογα με το πόσο αυξάνεται η απόσταση του δικτύου μέλους από τον τελικό στόχο. Όπως θα φανεί στη συνέχεια, για κάποιες προσομοιώσεις δοκιμάστηκαν και διαφορετικές πιθανότητες ανίχνευσης των περιστατικών, από $0,50$ έως $0,95$.

2. Αντιθέτως, όλα τα δίκτυα έχουν ίδιες πιθανότητες να παρουσιάσουν λανθασμένες ανιχνεύσεις (false positives). Ως αποτελέσματα λανθασμένης εκτίμησης αυτές δεν υπόκεινται στην ίδια συμπεριφορά με τα πραγματικά περιστατικά επιθετικής κίνησης. Επίσης θεωρούμε μοναδικές ανά δίκτυο τις περιπτώσεις λανθασμένων ανιχνεύσεων, δηλαδή δε συνεπάγονται παράλληλη αντίστοιχη ανίχνευση σε άλλο δίκτυο της Υποδομής[3].

3. Για κάθε κύκλο προσομοίωσης σε κάθε δίκτυο-μέλος θα γίνει ανίχνευση του περιστατικού με μικρότερη ή μεγαλύτερη πιθανότητα σύμφωνα με την τοποθέτηση του σε σχέση με το μονοπάτι της επίθεσης (όπως προσεγγίσαμε στο (1) πιο πάνω). Θεωρούμε έτσι τη πιθανότητα ανίχνευσης σε ένα σημείο από το οποίο διέρχεται λιγότερη κίνηση μειωμένη κατά 0,05.

4. Εφόσον πρόκειται να επιτευχθεί η ανίχνευση περιστατικού σε ένα δίκτυο, για το χρόνο που θα γίνει αυτό όλα τα δίκτυα επιλέγουν κοινό παράθυρο ανίχνευσης μήκους $\lambda = 5$ λεπτά ή 300 βήματα (sec) προσομοίωσης. Ο χρόνος ανίχνευσης σε ένα δίκτυο θα είναι τυχαίος με ομοιόμορφη κατανομή στο διάστημα $(0, 2t)$.

[3]Μια λανθασμένη ανίχνευση μπορεί να οφείλεται σε μια «φυσιολογική» ανωμαλία της κίνησης (που έχει την ονομασία «ξαφνικό πλήθος» —"flash crowd") οπότε θα ανιχνευτεί σε περισσότερα του ενός δίκτυα. Μια τέτοια ανωμαλία όμως ούτως ή άλλως είναι ένα εξαιρετικό γεγονός που πρέπει να αναγνωριστεί σε επίπεδο πολλαπλών δικτύων, ακόμα και αν δεν έχει κακόβουλη προέλευση.

5. Η Συνεργατική Υποδομή μελετάται στη συμπεριφορά της για διάφορες διάρκειες επιθέσεων που ακολουθούν τα αποτελέσματα που έχουν γίνει στην καθοριστική για το αντικείμενο ανάλυση του Moore [Moor01][4]: επιλέχθηκαν τα χρονικά μήκη που φάνηκαν να επικρατούν στα διαγράμματα κατανομής διάρκειας επιθέσεων και φαίνονται στον Πίνακα 5.1.

Διαρκεια Επιθεσης	**Βηματα Προσομοιωσης (1 δευτερολεπτου)**
1 λεπτό	60
2 λεπτά	120
5 λεπτά	300
10 λεπτά	600
20 λεπτά	1200
30 λεπτά	1800
1 ώρα	3600
2 ώρες	7200
2,5 ώρες	9000

Πίνακας 5.1: Οι χρόνοι επιθέσεων που χρησιμοποιήθηκαν

Σημειώνεται ότι και η μικρότερη ακόμα διάρκεια περιστατικού θεωρείται σημαντική ως προς το μήκος παραθύρου (των 5 λεπτών) και για αυτό το λόγο δε γίνεται διαφορετικός χειρισμός ως προς την κατανομή που δίνει τις πιθανότητες για χρονικά διαστήματα ανίχνευσης στο συνεργατικό περιβάλλον.

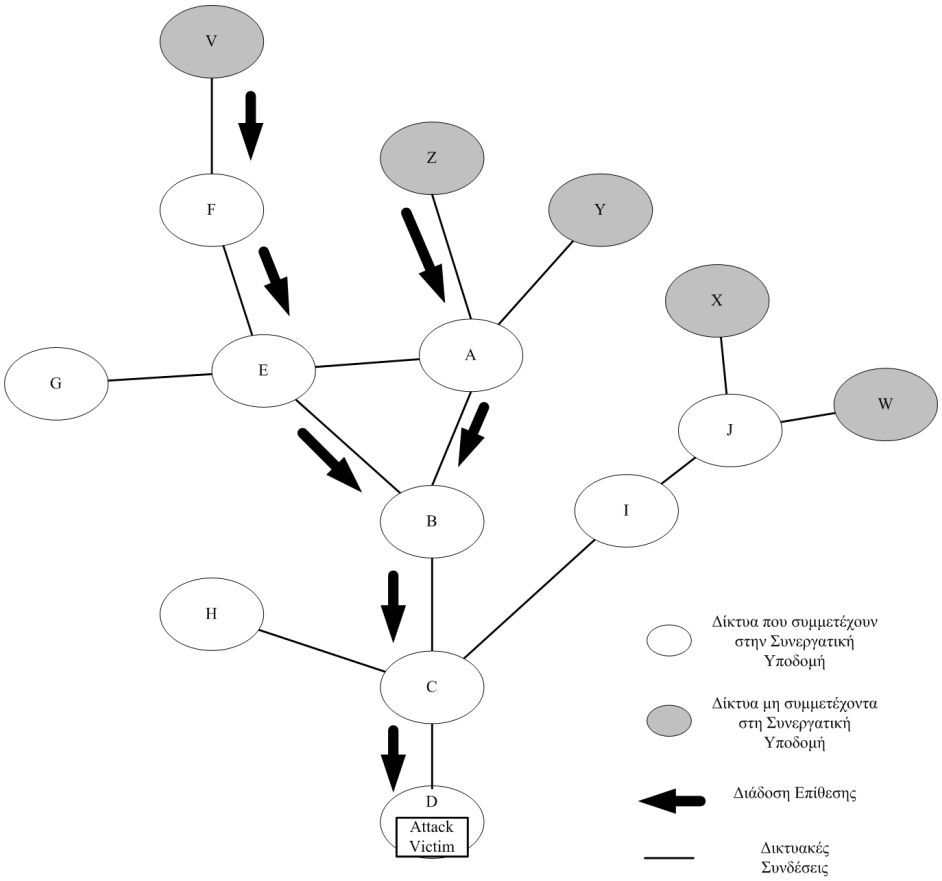
6. Η ανίχνευση έχει μόνον δύο πιθανές καταστάσεις (θετική ή αρνητική).

7. Το «βάρος» που αποδίδεται στις αναφορές –η «συνεισφορά» των αναφορών στην ανίχνευση της ύπαρξης ενός περιστατικού από μια Οντότητα

[4] Δείτε περισσότερα σχετικά στο κεφ. 2.

είναι 1,0 για ενημερώσεις που προέρχονται από το τοπικό σύστημα IDS και 0,8 για αυτές που προέρχονται από άλλα δίκτυα. Όπως θα παρουσιαστεί, σε κάποιες προσομοιώσεις δοκιμάστηκαν διαφορετικές τιμές για το «βάρος» που αποδόθηκε στις απομακρυσμένες αναφορές.

Το δίκτυο που χρησιμοποιήθηκε κατά την προσομοίωση φαίνεται στο Σχήμα 5.7



Σχήμα 5.7: Το δίκτυο που χρησιμοποιήθηκε στην προσομοίωση

5.6 Παράμετροι προς Έλεγχο

Παράμετροι που ελέγχθηκαν για τον τρόπο με τον οποίο επηρεάζουν τη λειτουργία της Συνεργατικής Υποδομής είναι οι εξής:

- *Alert_Threshold*. Πρόκειται για το όριο «βεβαιότητας» πάνω από το οποίο εδραιώνεται η διαπίστωση ύπαρξης ενός περιστατικού. Η ένδειξη «βεβαιότητας» προκύπτει με τη λήψη διαδοχικών μηνυμάτων (τοπικών ή απομακρυσμένων—τα τελευταία με διαφορετική συνεισφορά) που αφορούν το ίδιο περιστατικό.

- *«Εμπιστοσύνη» (απόδοση βάρους) σε απομακρυσμένες αναφορές*. Τα δίκτυα–μέλη επιλέγουν το βαθμό που αναφορές από απομακρυσμένες πηγές (άλλα δίκτυα) θα συνεισφέρουν στην εδραίωση της βεβαιότητας για την ύπαρξη ενός περιστατικού.

- *Timeouts*. Η παράμετρος Suspicion Timeout ορίζει πόσο διάστημα θα παραμείνει το σύστημα στην κατά το ήμισυ ενεργοποιημένη κατάσταση (Suspicion State) επομένως πόσο ευαίσθητο θα είναι σε διαδοχικές ενημερώσεις με μεγάλα χρονικά διαστήματα μεταξύ τους. Η παράμετρος Alerted Timeout έχει την ίδια σημασία της ευαισθησίας για την παραμονή στην ενεργοποιημένη κατάσταση. Οι τιμές για τους χρόνους αυτούς πρέπει να είναι συγκρίσιμες με το μέσο χρόνο ανίχνευσης του περιστατικού από το IDS.

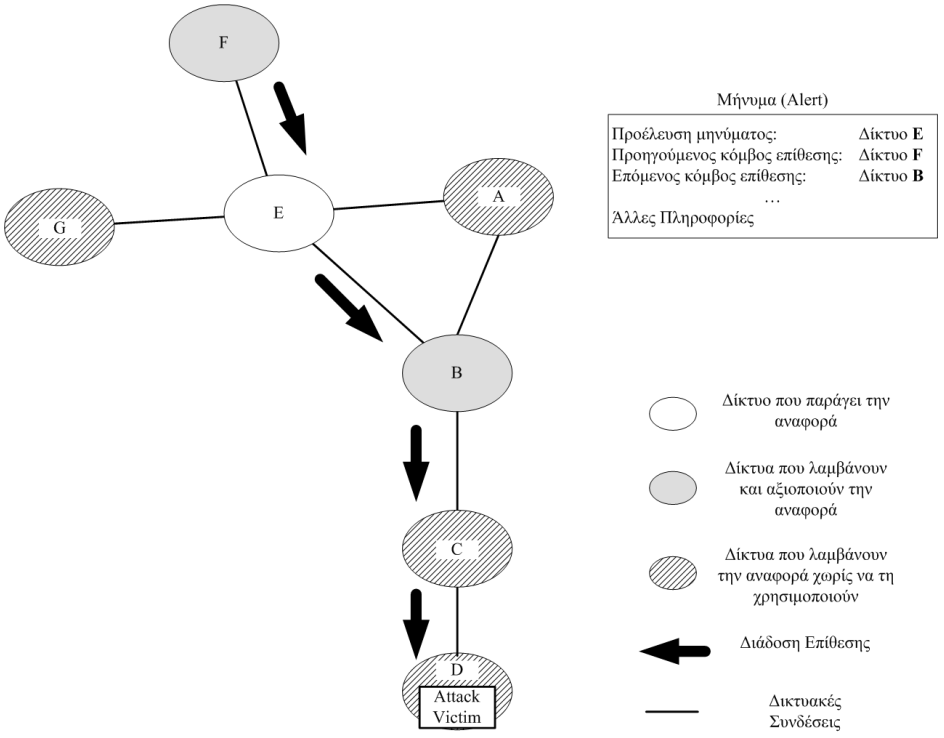
Επιπλέον αξιολογήθηκαν κάποιες (εξωτερικές) παράμετροι ανεξάρτητες από τη λειτουργία των ίδιων των Οντοτήτων οι οποίες εντούτοις παίζουν σημαντικό ρόλο στην τελική συμπεριφορά της συνεργατικής Αρχιτεκτονικής:

- *Πιθανότητες ανίχνευσης του περιστατικού.* Δοκιμάστηκαν μια σειρά από διαφορετικές περιπτώσεις ρυθμίσεων των συστημάτων IDS στα δίκτυα-μέλη της Υποδομής. Ανάλογα με τη ρύθμιση του ένα IDS μπορεί να δείχνει μικρότερη ή μεγαλύτερη ευαισθησία σε ανωμαλίες που σηματοδοτούν την πιθανή ύπαρξη ενός περιστατικού. Το πρόβλημα των συστημάτων ανίχνευσης ανωμαλιών είναι ότι υψηλή ευαισθησία μπορεί να οδηγήσει σε λανθασμένες ανιχνεύσεις (False Positives) ενώ αντιθέτως χαμηλή ευαισθησία μπορεί να έχει ως αποτέλεσμα επιθέσεις να περάσουν απαρατήρητες (False Negatives). Χρησιμοποιώντας διαφορετικές πιθανότητες ανίχνευσης στα δίκτυα πάνω στη διαδρομή ενός περιστατικού προσομοιώνουμε τα αποτελέσματα διαφορετικών ρυθμίσεων ευαισθησίας των αντίστοιχων συστημάτων IDS.

- *Χρήση Πληροφορίας Τοπολογίας από τα μηνύματα.* Στο κεφ. 4 είδαμε πως αφότου υπάρξει πέρασμα στην κατάσταση Ενεργοποίησης (Alert State) η πληροφορία Τοπολογίας που περιέχεται στα μηνύματα χρησιμοποιείται για την ανακάλυψη της σχέσης του δικτύου που έχει ενεργοποιηθεί με το μονοπάτι του περιστατικού. Σε κάποιες προσομοιώσεις ελέγχθηκε το κατά πόσον η πληροφορία αυτή μπορεί επίσης να χρησιμοποιηθεί ως παράγοντας αποδοχής ή όχι μιας απομακρυσμένης αναφοράς περιστατικού.

Πιο συγκεκριμένα, στις περιπτώσεις αυτές, κάθε δίκτυο–μέλος που λαμβάνει μια αναφορά περιστατικού ελέγχει το κατά πόσον περιλαμβάνεται στο περιεχόμενο του μηνύματος ως σημείο προέλευσης της επιθετικής κίνησης ή ως επόμενο δίκτυο (πρώτο βήμα) στο μονοπάτι της μετά τον αποστολέα. Ένα παράδειγμα αυτής της τεχνικής, παρουσιάζεται στο Σχήμα 5.8 για ένα υποσύνολο του

δικτύου της προσομοίωσης του Σχήματος 5.7. Το δίκτυο Ε βλέπει ως πηγή της κίνησης το δίκτυο F και ως πρώτο επόμενο βήμα της το δίκτυο Β και θα περιλάβει αυτή την πληροφορία στα μηνύματα που θα στείλει προς την κοινότητα. Στην περίπτωση που επιλέγουμε να χρησιμοποιήσουμε την πληροφορία τοπολογίας, από τα δίκτυα που θα λάβουν μια αναφορά από το δίκτυο Ε θα την αξιοποιήσουν μόνον τα F και Β. Αναμενόμενη συμπεριφορά στην περίπτωση αυτή είναι να μην ενεργοποιηθεί κανένα δίκτυο εκτός του μονοπατιού



Σχήμα 5.8: Χρήση πληροφορίας τοπολογίας πρώτου επιπέδου

Με τη χρήση της πληροφορίας τοπολογίας παρουσιάζεται εντούτοις το εξής πρόβλημα: Για κάθε μετάβαση ενός δικτύου–μέλους σε κατάσταση Ενεργοποίησης αποστέλλεται μόνο ένα μήνυμα. Έτσι, ένα δίκτυο πάνω στο μονοπάτι

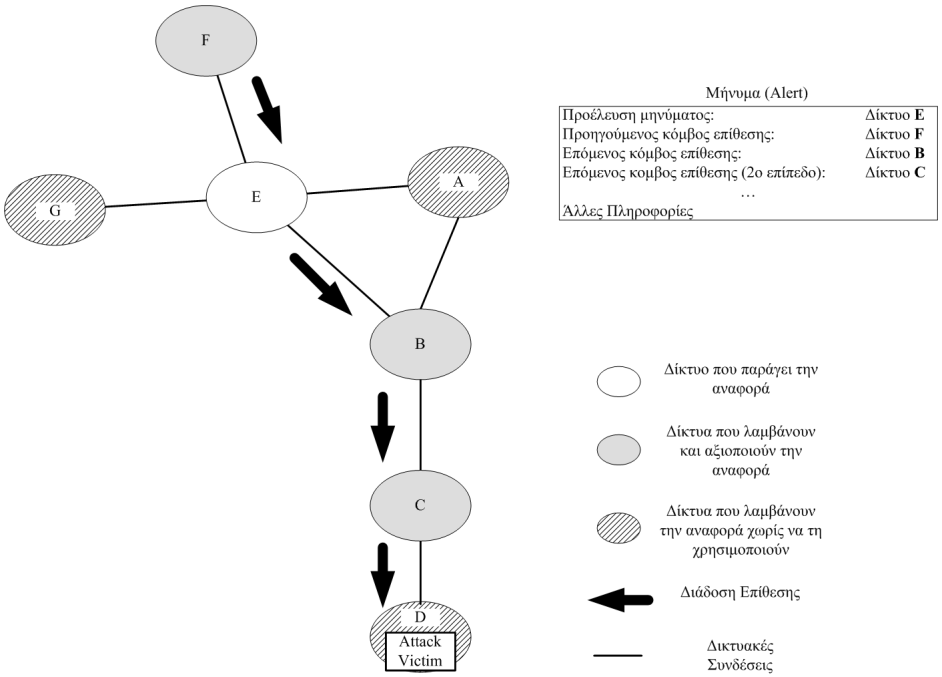
της επίθεσης, στο οποίο το τοπικό IDS δεν έχει ανιχνεύσει το περιστατικό θα έχει ως πηγή πληροφόρησης μόνον ένα ή (το πολύ 2) απομακρυσμένα μηνύματα με αποτέλεσμα να έχει μικρότερη πιθανότητα μετάβασης στην Ενεργοποιημένη κατάσταση. Πιθανές λύσεις αντιμετώπισης αυτού του προβλήματος είναι οι εξής:

- Χρήση πολύ χαμηλού επιπέδου «βεβαιότητας» για τη μετάβαση σε Ενεργοποιημένη Κατάσταση (Alert State) ακόμα και μετά τη λήψη περιορισμένου αριθμού μηνυμάτων. Δημιουργείται έτσι πρόβλημα ισχυρής αντίδρασης ακόμα και σε περιπτώσεις λανθασμένων ανιχνεύσεων (false Positives). Αυτό μπορεί (σε κάποιο βαθμό) να αντισταθμιστεί με την απαίτηση λήψης μηνυμάτων από δύο τουλάχιστον απομακρυσμένα δίκτυα–μέλη της Υποδομής.

- Πολλαπλές, διαδοχικές αποστολές μηνυμάτων από δίκτυα τα οποία έχουν περάσει στην κατάσταση Ενεργοποίησης. Στην περίπτωση αυτή διατρέχουμε τον κίνδυνο ένα δίκτυο το οποίο έχει κάνει λάθος ανίχνευση να «πλημμυρίσει» το δίκτυο με μηνύματα, κάτι το οποίο αντιβαίνει στη φιλοσοφία σχεδιασμού της λύσης της παρούσας εργασίας (κεφ. 3).

- Χρήση της τοπολογίας για την αναγνώριση μηνυμάτων αλλά και ενσωμάτωση και πληροφορίας «δεύτερου βήματος» σε αυτά. Η λήψη και χρησιμοποίηση αυτών από τα δίκτυα-παραλήπτες θα γίνεται όπως και προηγουμένως (απαίτηση για συμμετοχή σε κάποιο δίκτυο που αναφέρεται στο μήνυμα ως μέλος του μονοπατιού) αλλά θα μπορούν να ενημερωθούν περισσότερα δίκτυα. Στο προηγούμενο παράδειγμα του δικτύου του Σχήματος 5.7, η πληροφορία που θα σταλεί από το δίκτυο E εκτός των

δικτύων F (πηγή της κίνησης) και B (πρώτο βήμα της κίνησης) θα περιλαμβάνει επίσης το δίκτυο C ως δεύτερο βήμα της κίνησης. Η τεχνική αυτή παρουσιάζεται στο Σχήμα 5.9.



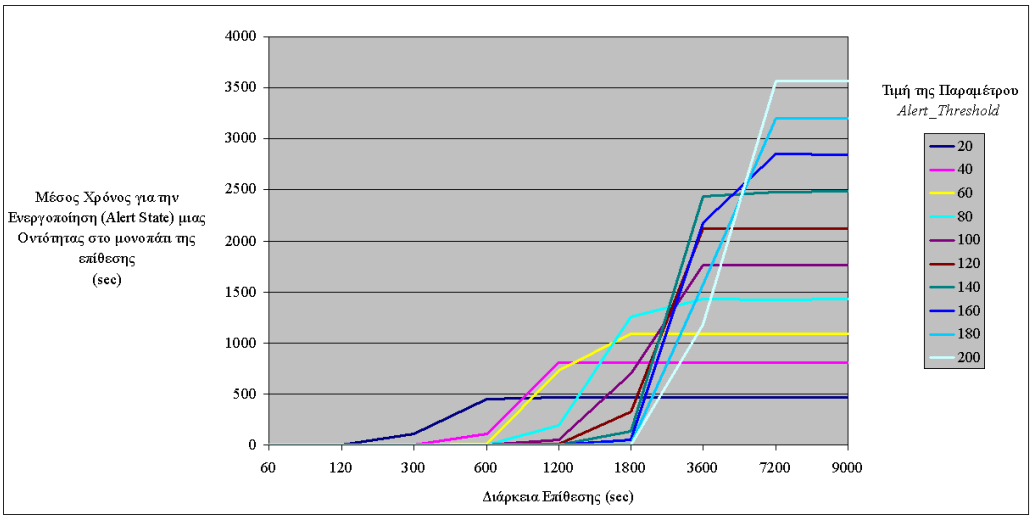
Σχήμα 5.9: Χρήση πληροφορίας τοπολογίας δευτέρου επιπέδου

Η τελευταία περίπτωση θεωρήθηκε ως πιο απλή και υλοποιήθηκε σε κάποιες προσομοιώσεις προκειμένου να δοκιμαστεί η επίδραση που θα είχε στη λειτουργία της Αρχιτεκτονικής.

5.7 Αποτελέσματα των Προσομοιώσεων

5.7.1 *Alert_Threshold*

Η πρώτη προσομοίωση αφορά στην επίδραση της τιμής της παραμέτρου *Alert_Threshold* στο χρόνο που παίρνει σε μια Οντότητα, πάνω στο μονοπάτι επίθεσης, να φτάσει στην Κατάσταση Ενεργοποίησης (Alert State). Η ίδια διερεύνηση έγινε για διάφορες διάρκειες περιστατικού. Τα αποτελέσματα φαίνονται στο Σχήμα 5.10 όπου για διάφορες τιμές του *Alert_Threshold* δίνονται οι μέσοι όροι των χρόνων για Ενεργοποίηση μιας Οντότητας στο μονοπάτι ανάλογα με τη διάρκεια του περιστατικού:

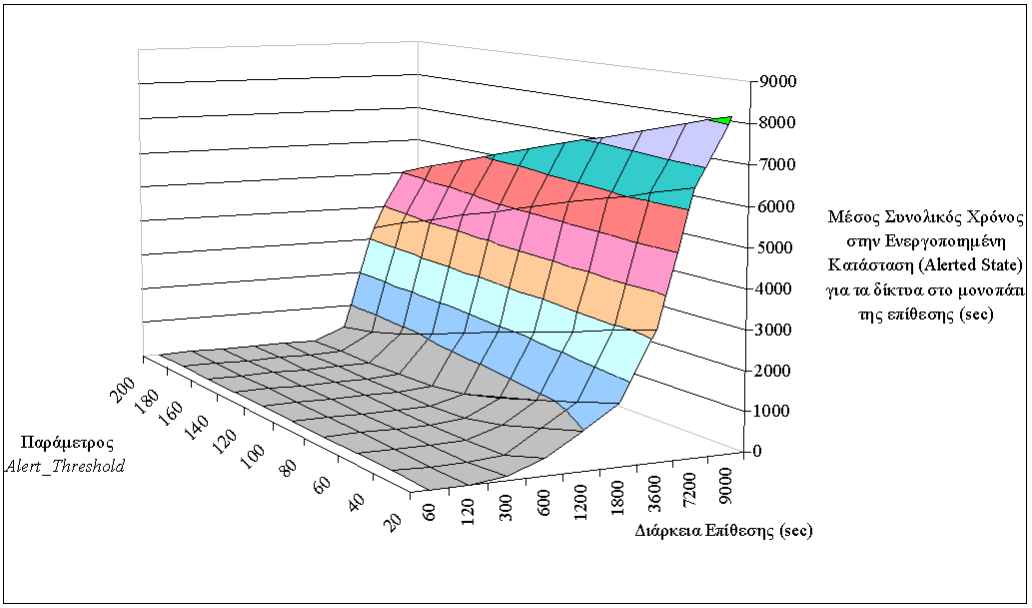


Σχήμα 5.10: Επίδραση της τιμής *Alert_Threshold* στο μέσο χρόνο Ενεργοποίησης Οντότητας στο μονοπάτι της επίθεσης

Τα αποτελέσματα δείχνουν ότι, κατά το αναμενόμενο, χαμηλότερη τιμή *Alert_Threshold* επιτρέπει τη συντομότερη μετάβαση σε Alert State. Η επίδραση στην ταχύτητα έχει ακόμα μεγαλύτερη σημασία σε περιστατικά μικρότερης διάρκειας όπου είναι αναγκαία η σύντομη ανίχνευση πριν ολοκληρωθεί η δράση

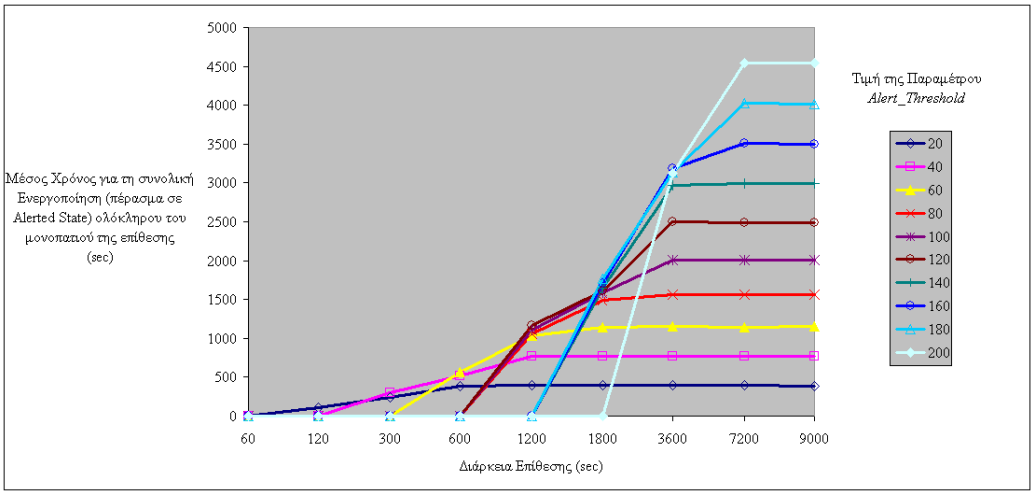
τους.

Στη συνέχεια εξετάζουμε το συνολικό μέσο χρόνο παραμονής στην Κατάσταση Alert State συναρτήσει της τιμής *Alert_Threshold* και της διάρκειας της επίθεσης. Το Σχήμα 5.11 που προκύπτει αποκαλύπτει ότι η Οντότητες παραμένουν στην Ενεργοποιημένη Κατάσταση για διάστημα ανάλογο της διάρκειας της επίθεσης, γεγονός που δίνει μια ένδειξη για τη σταθερότητα του συστήματος αφότου επέτυχε την Ενεργοποίηση.



Σχήμα 5.11: Απεικόνιση της επίδρασης της παρμέτρου *Alert_Threshold* στο μέσο χρόνο παραμονής στην Κατάσταση Ενεργοποίησης Alert State για διάφορες διάρκειες επιθέσεων

Εξετάζοντας τη συμπεριφορά ολόκληρου του μονοπατιού το οποίο ακολουθεί η επίθεση (στο δίκτυο του σχήματος 5.7 οι διαδρομές που περιλαμβάνουν τα δίκτυα F-E-B-C-D και A-B-C-D) έχουμε την απεικόνιση της στο Σχήμα 5.12.



Σχήμα 5.12: Επίδραση της παραμέτρου *Alert_Threshold* στο μέσο χρόνο που απαιτείται για να ενεργοποιηθεί ολόκληρο το μονοπάτι της επίθεσης

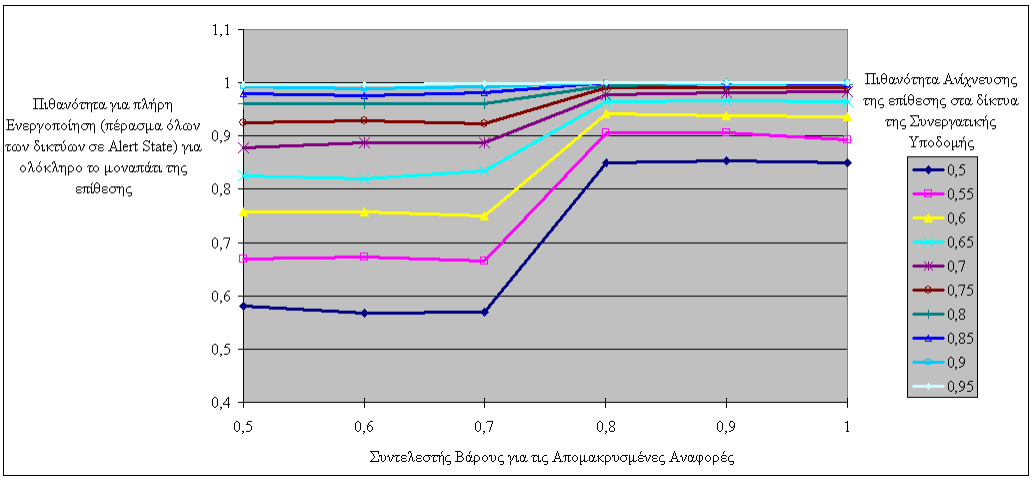
Το σχήμα αυτό υποδεικνύει ότι σε κάθε περίπτωση διάρκειας επίθεσης απαιτείται μια ελάχιστη τιμή για το *Alert_Threshold* ώστε να επιτύχουμε ενεργοποίηση ολόκληρου του μονοπατιού.

Συμπερασματικά καταλήγουμε ότι η επιλογή μικρότερων τιμών *Alert_Threshold* έχει ως αποτέλεσμα τη μεγαλύτερη ευαισθησία της αρχιτεκτονικής ακόμα και σε περιστατικά μικρής διάρκειας. Αν εξασφαλιστεί ότι θα απαιτηθούν τουλάχιστον δύο μηνύματα συνολικά (και ενδεχομένως περισσότερα αν πρόκειται για απομακρυσμένα[5]) για να φτάσει η Οντότητα σε Κατάσταση Ενεργοποίησης τότε έχουμε αποκλείσει σε μεγάλο βαθμό την επίδραση των λανθασμένων ανιχνεύσεων (False Positives) στη συνεργατική Υποδομή Συνολικά, ακόμα και αν έχουμε Ενεργοποίηση κάποιων από τα επιμέρους δίκτυα.

[5] Αυτό εξασφαλίζεται με τη διαφορετική συνεισφορά των απομακρυσμένων μηνυμάτων.

5.7.2 «Εμπιστοσύνη» (απόδοση βάρους) σε απομακρυσμένες αναφορές

Στην προσομοίωση αυτή δοκιμάστηκαν διαφορετικά βάρη για τις απομακρυσμένες αναφορές και συνδυάστηκαν με διαφορετικές ευαισθησίες των επιμέρους συστημάτων IDS στο να ανακαλύψουν το περιστατικό (το οποίο στην προσομοίωση μεταφράζεται σε πιθανότητες ανίχνευσης). Το Σχήμα 5.13 δίνει τα αποτελέσματα αυτών των δοκιμών ως προς τις πιθανότητες Ενεργοποίησης (πέρασμα σε Alert State) όλων των δικτύων της Υποδομής πάνω στο μονοπάτι της επίθεσης[6].



Σχήμα 5.13: Επίδραση του συντελεστή συνεισφοράς απομακρυσμένων μηνυμάτων στις πιθανότητες Ενεργοποίησης (πέρασμα σε Alert State) όλων των δικτύων της Υποδομής πάνω στο μονοπάτι της επίθεσης

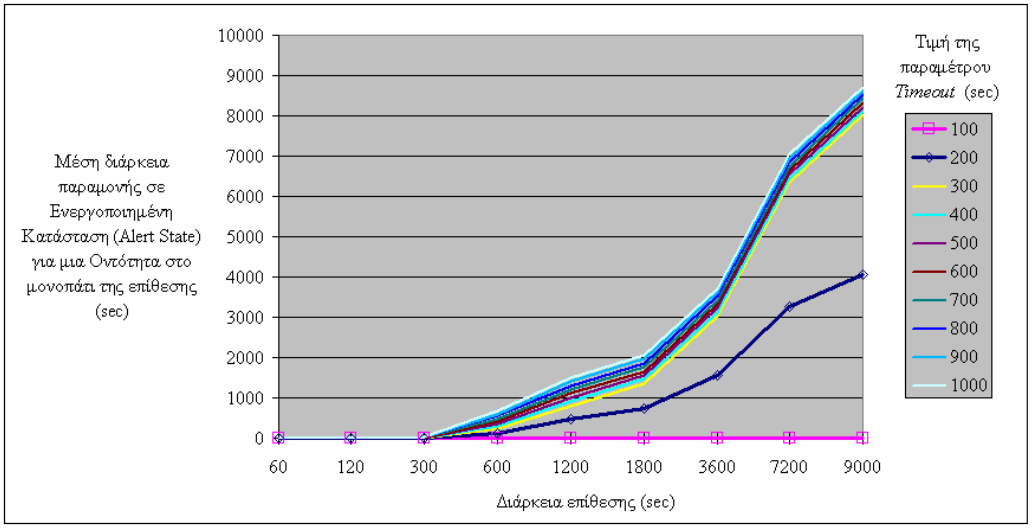
Χαμηλά βάρη συνεισφοράς των απομακρυσμένων μηνυμάτων αντιστοιχούν στην κατάσταση όπου κάθε Συνεργαζόμενο δίκτυο στην Υποδομή λειτουργεί με μεγάλο βαθμό ανεξαρτησίας, «αποκομμένο» από τα άλλα. Αντιθέτως όσο

[6] Η προσομοίωση αυτή αφορά επιθέσεις μιας διάρκειας μόνον 1 ώρας (3600 δευτερολέπτων).

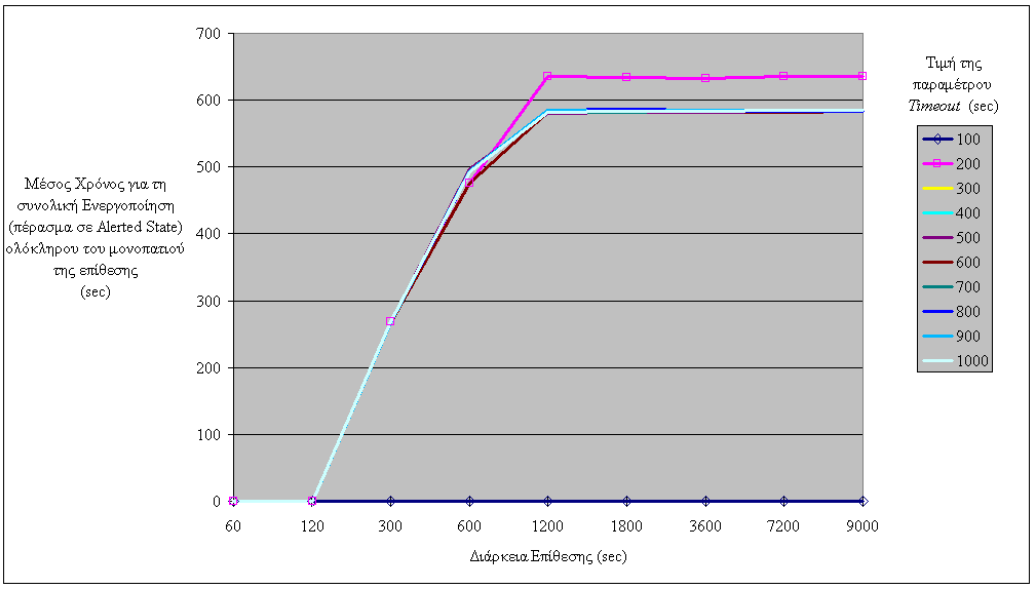
αυξάνονται τα βάρη αυτά τόσο τα δίκτυα συνεργάζονται περισσότερο, καταλήγοντας σε πλήρη αποδοχή των απομακρυσμένων αποτελεσμάτων και απόλυτη «διασύνδεση». Παρατηρούμε τη σημαντική συνεισφορά των βαρών που αποδίδονται στα απομακρυσμένα μηνύματα στην πιθανότητα ενεργοποίησης της Υποδομής άνω του 80%) ακόμα και στις περιπτώσεις χαμηλών επιδόσεων (ποσοστά ανίχνευσης) των επιμέρους συστημάτων IDS.

5.7.3 *Timeouts*

Οι χρόνοι αναμονής μεταξύ διαδοχικών μηνυμάτων μελετήθηκαν ως προς την επίδραση τους στη σταθερότητα της κατάστασης Ενεργοποίησης και το μέσο χρόνο για τη την ενεργοποίηση του πλήρους μονοπατιού του περιστατικού. Τα αποτελέσματα που προκύπτουν από αυτές τις δοκιμές φαίνονται στα σχήματα 5.14 και 5.15.



Σχήμα 5.14: Επίδραση των παραμέτρων *Timeout* στο χρόνο που μια Οντότητα πάνω στο μονοπάτι της επίθεσης παραμένει σε κατάσταση Ενεργοποίησης (Alert State)



Σχήμα 5.15: Επίδραση των παραμέτρων *Timeout* στις πιθανότητες Ενεργοποίησης (πέρασμα σε Alert State) όλων των δικτύων της Υποδομής πάνω στο μονοπάτι της επίθεσης

Και στις δύο περιπτώσεις παρατηρούμε ότι μετά από ένα μεταβατικό στάδιο στις περιπτώσεις των πολύ χαμηλών τιμών των χρόνων αναμονής (ως προς τους χρόνους ανίχνευσης και αντίδρασης των συστημάτων IDS) η επίδραση τους είναι σταθερή για διάφορες διάρκειες επιθέσεων. Άλλα ενδιαφέροντα συμπεράσματα που προκύπτουν:

- Από το Σχήμα 5.14 βλέπουμε ότι οι Οντότητες παραμένουν κατά μέσο όρο σε ενεργοποίηση (Alert State) χρόνο ανάλογο της διάρκειας της επίθεσης επιδεικνύοντας σταθερότητα για τιμές των *timeouts* άνω των αρχικών τιμών.

- Από το Σχήμα 5.15 παρατηρούμε ότι για μια σχετικά χαμηλή τιμή *Alert_Threshold* που είχε επιλεγεί για αυτή την προσομοίωση και σε κάθε περίπτωση *timeouts* (πλην των αρχικών τιμών) ο μέσος χρόνος για την Ενεργοποίηση

ολόκληρου του μονοπατιού της επίθεσης είναι κάτω από τα 600 δευτερόλεπτα (10 λεπτά) για κάθε περιστατικό με διάρκεια άνω των 10 λεπτών. Το δίκτυο συνολικά αντιδρά οριακά ταχύτερα από το μέγιστο χρόνο $2t$ (600 δευτερόλεπτα) για την ενεργοποίηση επιμέρους IDS στα δίκτυα που ανίχνευσαν την επίθεση (ακόμα και αν η επίθεση δεν έχει ανιχνευτεί σε όλα τα δίκτυα–μέλη).

5.7.4 Πληροφορία Τοπολογίας

Δοκιμάστηκαν οι δύο περιπτώσεις χρήσης πληροφορίας τοπολογίας που αναφέρονται στο τμήμα 5.6. Κάθε αναφορά ανίχνευσης επίθεσης από ένα δίκτυο περιείχε στοιχεία για το προηγούμενο και τα επόμενα (ένα ή δύο) βήματα του μονοπατιού της. Οι αναφορές διανέμονται κανονικά μέσω του Υπερκείμενου Δικτύου αλλά γίνονται δεκτές από ένα δίκτυο-παραλήπτη μόνον εφόσον το αφορούν άμεσα.

Έγινε η προσομοίωση δύο διαφορετικών περιπτώσεων ενσωμάτωσης πληροφορίας στα μηνύματα προειδοποίησης ως εξής:

- Αναφορά στο προηγούμενο και το αμέσως επόμενο δίκτυο από αυτό που στέλνει την αναφορά (μόνον γείτονες 1ου επιπέδου).
- Αναφορά στο προηγούμενο και επόμενα δύο δίκτυα στο μονοπάτι της επίθεσης (γείτονες μέχρι και 2ου επιπέδου).

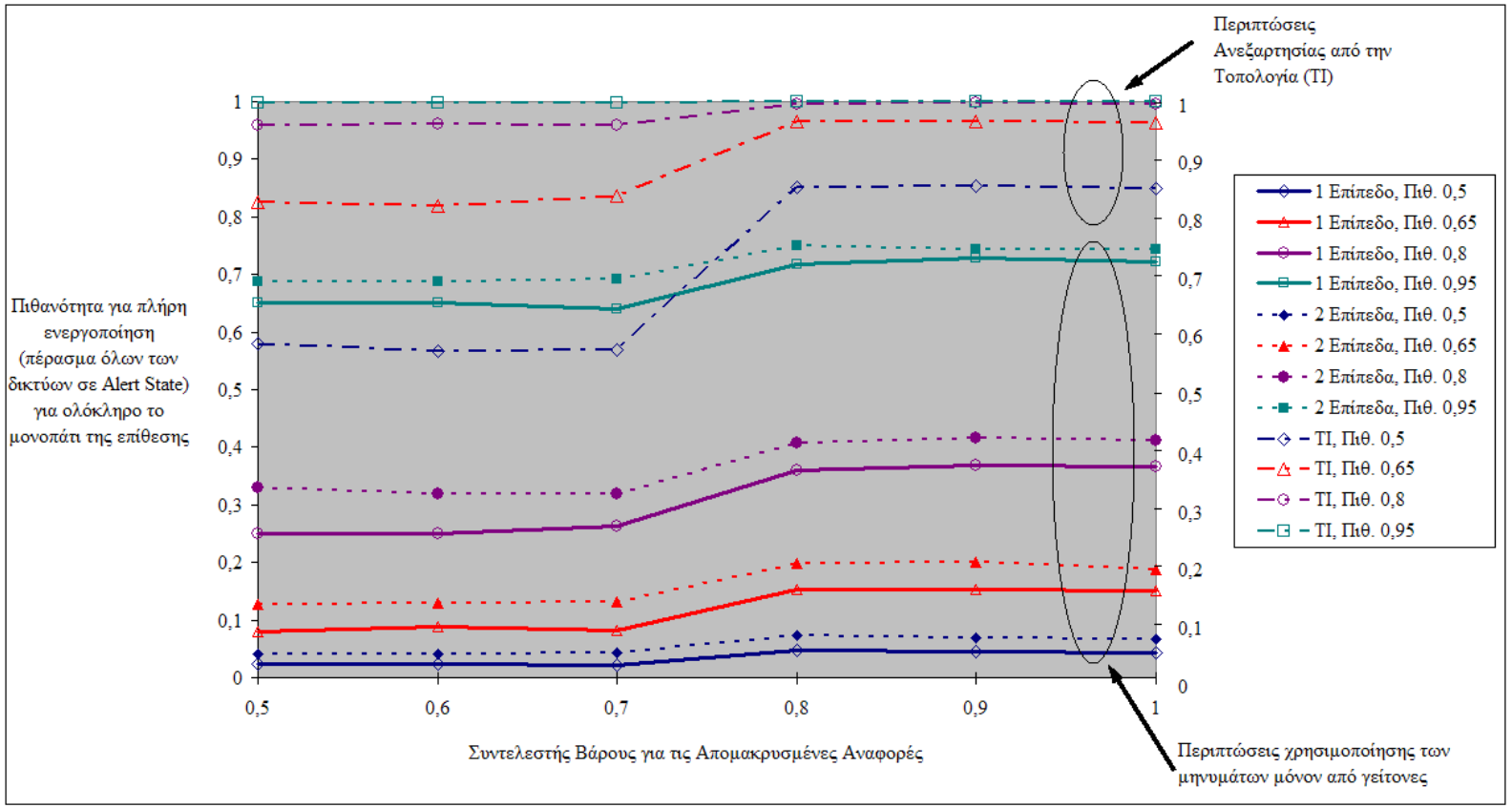
Οι δύο αυτές προσεγγίσεις αποδοχής αναφορών δοκιμάστηκαν για την επίδραση που θα είχαν στην ενεργοποίηση ολόκληρου του μονοπατιού της επίθεσης σε σχέση επίσης με την απόδοση διαφορετικών βαρών στα απομακρυσμένα μηνύματα και για διάφορες πιθανότητες (ευαισθησίες ανίχνευσης). Συγκρίθηκαν

επίσης με την περίπτωση πλήρους διάδοσης (και χρησιμοποίησης) των ανάφορών από όλα τα μέλη της Συνεργατικής Υποδομής όπως αυτή παρουσιάστηκε στο τμήμα 5.7.2. Από την προσομοίωση προέκυψαν τα αποτελέσματα του παρουσιάζονται αριθμητικά στον Πίνακα 5.2 και γραφικά στο Σχήμα 5.16.

Συντελεστης Βαρους	Πιθανοτητα Ανιχνευσης												
	0,50			**0,65**			**0,80**			**0,95**			
	1E	2E	TI	1E	2E	TI	1E	2E	TI	1E	2E	TI	
0,5	0,02	0,04	0,58	0,08	0,13	0,83	0,25	0,33	0,96	0,65	0,69	0,99	
0,6	0,02	0,04	0,57	0,09	0,13	0,82	0,25	0,32	0,96	0,65	0,69	0,99	
0,7	0,02	0,04	0,57	0,08	0,13	0,84	0,26	0,32	0,96	0,64	0,69	1,00	
0,8	0,05	0,07	0,85	0,15	0,20	0,97	0,36	0,41	1,00	0,72	0,75	1,00	
0,9	0,05	0,07	0,85	0,15	0,20	0,97	0,37	0,42	1,00	0,73	0,74	1,00	
1	0,04	0,07	0,85	0,15	0,19	0,96	0,37	0,41	1,00	0,72	0,74	1,00	

Πίνακας 5.2: Πιθανότητα Ενεργοποίησης (Alert State) ολόκληρου του μονοπατιού επίθεσης (για διάφορες πιθανότητες ανίχνευσης και διάφορες αποδόσεις βαρών σε απομακρυσμένα μηνύματα) όταν γίνεται χρησιμοποίηση της πληροφορίας που περιέχεται στα μηνύματα, μόνον στους γείτονες 1ου επιπέδου (1E) του αποστολέα, στους γείτονες 1ου και 2ου επιπέδου (2E), ή σε όλα τα μέλη της Συνεργατικής Υποδομής (Topology Independent – TI).

Τα αποτελέσματα αυτά δείχνουν, κατ' αρχάς υποδεέστερες επιδόσεις όταν οι αναφορές αξιοποιούνται μόνον στους γείτονες πρώτου και δεύτερου επιπέδου σε σχέση με την περίπτωση αξιοποίησης τους από όλους τους κόμβους της αρχιτεκτονικής ανεξαρτήτως τοπολογίας (Topology Independent – TI) σε όλα τα μέλη της Συνεργατικής Υποδομής. Αυτό οφείλεται στο ότι στην πρώτη περίπτωση η πληροφορία ανίχνευσης διαδίδεται σε πολύ λιγότερους παραλήπτες. Έτσι τα διάφορα δίκτυα έχουν διαθέσιμη σημαντικά λιγότερη πληροφορία προκειμένου να καταλήξουν σε ανίχνευση. Το συμπέρασμα αυτό επιβεβαιώνεται και από την (οριακά) καλύτερη επίδοση που παρατηρείται στην περίπτωση διάδοσης των μηνυμάτων μέχρι και τους γείτονες δεύτερου επιπέδου.



Σχήμα 5.16: Πιθανότητες Ενεργοποίησης (πέρασμα σε Alert State) όλων των δικτύων της Υποδομής πάνω στο μονοπάτι της επίθεσης με τη χρησιμοποίηση της πληροφορίας που περιέχεται στα μηνύματα, μόνον από γείτονες 1ου επιπέδου (συνεχής γραμμή), από γείτονες 1ου και 2ου επιπέδου (εστιγμένη γραμμή) και σε όλη τη Συνεργατική Υποδομή — Topology Independent (TI) — (διακεκομμένη γραμμή).

Πρέπει πάντως να τονιστεί μια άλλη σημαντική πλευρά (που προκύπτει από τα αποτελέσματα των προσομοιώσεων αλλά δεν απεικονίζεται στο διάγραμμα): Δεν υπήρξε κανενός βαθμού ενεργοποίηση των Οντοτήτων εκείνων που δεν είχαν άμεση σχέση με το μονοπάτι της επίθεσης. Το συμπέρασμα που προκύπτει είναι ότι ακόμα και αν μειώθηκε σημαντικά η συνολική ενεργοποίηση του μονοπατιού ή όποια ενεργοποίηση Οντοτήτων συνέβη ήταν άμεσα σχετιζόμενη με το περιστατικό και αποκλειστικά μέσα στο μονοπάτι του.

5.8 Συμπεράσματα

Από τα προηγούμενα αποτελέσματα της προσομοίωσης καταλήγουμε στα εξής συμπεράσματα:

- Η τιμή της παραμέτρου *Alert_Threshold* είναι προτιμότερο να είναι χαμηλή ώστε μια Οντότητα να περνάει σύντομα σε κατάσταση Ενεργοποίησης (Alert State) ανιχνεύοντας ακόμα και επιθέσεις πολύ μικρής διάρκειας. Η ρύθμιση λειτουργίας της των Οντοτήτων ώστε να προϋποθέτουν την ύπαρξη αναφορών από τουλάχιστον δύο πηγές αποτρέπει τον κίνδυνο ύπαρξης λανθασμένων ανιχνεύσεων (False Positives) λόγω υπερβολικής ευαισθησίας.

- Η Συνεργατική Υποδομή παρουσιάζει τις καλύτερες επιδόσεις ανίχνευσης όταν υπάρχει αυξημένη «εμπιστοσύνη» μεταξύ των μελών της που μεταφράζεται σε απόδοση υψηλότερου «βάρους» («σημασίας») στα απομακρυσμένα μηνύματα. Το αποτέλεσμα αυτό μπορεί να αντισταθμίσει τυχόν χαμηλή ευαισθησία των τοπικών συστημάτων IDS που με τη σειρά του

προστατεύει από περιστατικά λανθασμένων αναγνωρίσεων. Αντίστοιχα καλύτερες επιδόσεις συνολικά εξασφαλίζει η διάδοση των αναφορών στο μεγαλύτερο δυνατό αριθμό μελών της Συνεργατικής Υποδομής.

- Οι χρόνοι αναμονής μεταξύ διαδοχικών μηνυμάτων (*Timeouts*) μετά από ένα μεταβατικό όριο πολύ χαμηλών τιμών παρουσιάζουν παρόμοια επίδραση στη λειτουργία της Συνεργατικής Υποδομής για διάφορες διάρκειες επιθέσεων.

- Οι διαχειριστές μπορούν να επιλέξουν να απορρίπτουν μηνύματα που δεν αφορούν άμεσα τα δίκτυα τους. Η επίδοση της Συνεργατικής Υποδομής στη συνολική ανίχνευση επιθέσεων θα μειωθεί αλλά επίσης θα αποτραπούν εντελώς οποιεσδήποτε ενεργοποιήσεις Οντοτήτων εκτός μονοπατιού επίθεσης. Από άποψη επίδοσης πάντως συνίσταται η μέγιστη αλληλεπίδραση. Ο σχεδιασμός αποστολής μηνυμάτων στο δίκτυο «από έναν σε πολλούς» (τεχνικές multicast) εγγυάται ότι δε θα υπάρξει υπερφόρτωση του δικτύου από μηνύματα μεταξύ των Οντοτήτων. Επιπλέον, η πολυπλοκότητα χρήσης πληροφοριών τοπολογίας από το BGP δε δικαιολογεί την πιθανή επιδείνωση των επιδόσεων.

Κεφάλαιο 6

Συγκρίσεις με άλλες Λύσεις, Συμπεράσματα της Εργασίας, Θέματα Μελλοντικής Διερεύνησης

6.1 Συγκρίσεις με άλλες λύσεις

Στο Κεφάλαιο 2 έγινε μια παρουσίαση των κυριοτέρων πρόσφατων ερευνητικών προτάσεων αντιμετώπισης των επιθέσεων DDoS. Στην παρούσα ενότητα αξιολογούνται άλλες λύσεις που προσεγγίζουν τη φιλοσοφία και τις μεθοδολογίες της παρούσας εργασίας και συγκρίνονται με την προτεινόμενη αρχιτεκτονική. Οι συγκρίσεις αυτές θα καταδείξουν καλύτερα ορισμένες λεπτομέρειες της προτεινόμενης προσέγγισης.

6.1.1 Σύγκριση με τη λύση COSSACK

Το σύστημα COSSACK αναπτύχθηκε από στο USC και παρουσιάζεται στην εργασία [Papa03] του Χ. Παπαδόπουλου και των συνεργατών του. Η λύση ενεργοποιείται σε δίκτυα στα «άκρα» του Διαδικτύου (edge networks). Όπως και στην παρούσα διατριβή γίνεται η προσπάθεια να αντιμετωπιστεί το πρόβλημα της χαμηλής ακρίβειας των συνήθων τεχνικών ανίχνευσης περιστατικών DDoS (που χρησιμοποιούν τη διάγνωση ανωμαλιών – anomaly detection) με την συνεισφορά πληροφοριών από διάφορες πηγές.

Το σύστημα υλοποιείται με την εγκατάσταση ειδικού λογισμικού παρακολούθησης και επικοινωνίας ("watchdog") στα σημεία διασύνδεσης (egress points) δικτύων άκρου (edge/client networks). Τα watchdogs ελέγχουν την εισερχόμενη στο δίκτυο κίνηση για να εντοπίσουν περιστατικά DDoS και να καθορίσουν τα χαρακτηριστικά στοιχεία της αντίστοιχης κίνησης. Στη συνέχεια με χρήση ενός μηχανισμού επικοινωνιών multicast μέσω του δικτύου peer-to-peer Yoid [Yoid00] αποστέλλουν αυτή την πληροφορία στην κοινότητα ώστε εκείνα τα δίκτυα άκρου απ' όπου ξεκινάει η επιθετική κίνηση να λάβουν μέτρα εναντίον της. Χαρακτηριστικά, ένα συγκεκριμένο multicast group δημιουργείται για τις επικοινωνίες ανάμεσα σε όλα τα εμπλεκόμενα στο ίδιο περιστατικό watchdogs.

Η λύση COSSACK αποβλέπει στην αντιμετώπιση του προβλήματος από άκρο σε άκρο (end-to-end) ενεργώντας στα δύο άκρα του Διαδικτύου που ενέχονται στο περιστατικό: το θύμα και τα δίκτυα προέλευσης. Η πρόταση προβλέπει επίσης τον έλεγχο των δικτύων προέλευσης από τα τοπικά watchdog για την ανακάλυψη των υπολογιστών που χρησιμοποιούνται στην επίθεση

(zombies[1]) και τη λήψη μέτρων αντιμετώπισης της επίθεσης σύμφωνα με τις τοπικές πολιτικές ασφαλείας, κατά παρόμοιο τρόπο με τη Συνεργατική Υποδομή.

Οι διαφορές ανάμεσα στις δύο προσεγγίσεις συνοψίζονται στα εξής:

- Η κύρια διαφορά του COSSACK από την προτεινόμενη Συνεργατική Υποδομή είναι ότι το πρώτο επικεντρώνεται σε ενέργειες στα άκρα του Διαδικτύου με σκοπό να σταματήσει την επίθεση στο δίκτυο πηγής. Η αποστολή πληροφοριών από το σημείο που το περιστατικό ανιχνεύεται (κοντά στο θύμα) αποβλέπει στην ενίσχυση της βεβαιότητας εντοπισμού του στην πηγή του. Αντιθέτως, η προτεινόμενη στη διατριβή Συνεργασία αποβλέπει στην ανταλλαγή πληροφοριών ανίχνευσης, την αυτοματοποίηση επικοινωνιών και το συντονισμό ενεργειών στην ομάδα δικτύων (domains) στην περιοχή του θύματος· Η φιλοσοφία που υιοθετήσαμε είναι η ανίχνευση και αντίδραση στην περιοχή του θύματος. Ο λόγος για την προσέγγιση μας είναι η σε κάποιο βαθμό ευκολότερη συνεργασία (ad hoc ή και μέσω εμπορικών συμφωνιών) στη ίδια δικτυακή περιοχή απ' ότι σε απομακρυσμένα σημεία του Διαδικτύου.

- Στο COSSACK τα σημεία ανίχνευσης είναι αποκλειστικά τα σημεία διασύνδεσης των δικτύων άκρου. Στη Συνεργατική Υποδομή που αναπτύξαμε, η ανίχνευση ενός περιστατικού μπορεί να γίνει από οποιοδήποτε από τα δίκτυα κοντά στο θύμα· τα μηνύματα που θα ανταλλαχθούν αποβλέπουν: στην εξασφάλιση της πληροφορίας από περισσότερες από μια πηγές, στην επιβεβαίωση της και στην ανακάλυψη της διαδρομής της επίθεσης, ώστε να διαφανούν τα πιθανά σημεία λήψης μέτρων. Επίσης εξασφαλίζουμε

[1] Δείτε τη σχετική περιγραφή στην ενότητα 2.2.1 για τα συστήματα υπολογιστών που χρησιμοποιούνται (συνήθως χωρίς γνώση των χρηστών τους) στην εκτέλεση επιθέσεων.

την ενεργοποίηση της υποδομής ακόμα και στην περίπτωση αποκοπής του τελικού δικτύου – θύματος λόγω της σφοδρότητας της επίθεσης.

- Στο COSSACK τα ειδικά συστήματα (watchdogs) αναλαμβάνουν τα ίδια το ρόλο της ανίχνευσης των περιστατικών και έχουν την ευελιξία να χρησιμοποιήσουν διάφορες τεχνικές (ενδεικτικά: πληροφορίες netflow, στοιχεία SNMP κ.λπ.). Για το λόγο αυτό πρέπει να τοποθετηθούν στο σύνορο του δικτύου. Αντιθέτως οι Συνεργατικές Οντότητες είναι χρήστες (καταναλωτές) των στοιχείων που λαμβάνουν σε τοπικό επίπεδο από (ανεξάρτητα) συστήματα IDS.

Συμπερασματικά, η Συνεργατική Οντότητα που παρουσιάστηκε στη παρούσα διατριβή διαχωρίζει σαφώς τις λειτουργίες ανίχνευσης και επικοινωνίας με τις άλλες Οντότητες. Επομένως δεν περιορίζει τα σημεία τοποθέτησης της Οντότητας και επιτρέπει ανεξαρτησία στην επιλογή συστημάτων IDS σε κάθε δίκτυο, αντίθετα με το σύστημα COSSACK το οποίο οριοθετεί με αυστηρότητα τα σημεία τοποθέτησης των εξειδικευμένων συστημάτων του. Η εμπειρία από τη λειτουργία του Διαδικτύου δείχνει πως τα διάφορα δίκτυα (domains) δεν υπακούουν σε ομοιόμορφους κανόνες διαχείρισης και δεν υιοθετούν αναγκαστικά κοινά συστήματα IDS.

6.1.2 Σύγκριση με την υποδομή GDI

Η «Παγκόσμια Υποδομή Άμυνας», GDI (Global Defense Infrastructure) που προτείνεται από τους Wan και άλλους στο [Wan02] προβλέπει τη χρήση ειδικών, τοπικών Συστημάτων Ανίχνευσης επιθέσεων DDoS (Local Detection Systems — LDSes) σε στρατηγικά σημεία σε ολόκληρο το Διαδίκτυο, όπως π.χ. τα

κύρια σημεία ανταλλαγής κίνησης (Internet Exchanges) κ.λπ. Τα LDS κατατάσσονται σε «πλήρως» ("Fully") και «μερικώς» ("Minimally") υλοποιημένα με αντίστοιχες δυνατότητες ανίχνευσης-αντίδρασης ή μόνον αντίδρασης. Τα εγκατεστημένα LDS συνθέτουν το Κατανεμημένο Σύστημα Ανίχνευσης Επιθέσεων (Distributed Attack Detection System — DAD). Η κατανεμημένη αυτή αρχιτεκτονική οργανώνεται και λειτουργεί με την ανταλλαγή μηνυμάτων ανάμεσα στα LDS. Τα LDS είναι δομημένα με αρθρωτό τρόπο (modular), αποτελούμενα από μονάδες διαφορετικών λειτουργιών (ανάλυση κίνησης, ανίχνευση επιθέσεων, αντίδραση στις επιθέσεις κ.λπ.) οι οποίες είναι δυνατόν να διαμοιραστούν και σε διαφορετικά υπολογιστικά συστήματα. Τα «Πλήρη» LDS αναζητούν περιστατικά επιθέσεων DDoS βασιζόμενα τόσο στους ενσωματωμένους αισθητήρες, όσο και στα μηνύματα προειδοποίησης (Alert) που λαμβάνουν από γειτονικά συστήματα. Η ανταλλαγή μηνυμάτων εντός του GDI πραγματοποιείται με τη χρήση τεχνικής «αξιόπιστου πλημμυρίσματος» ("reliable flooding") και τα μηνύματα κωδικοποιούνται σε IDMEF.

Στην προσέγγιση αυτή η αντιμετώπιση των επιθέσεων γίνεται με την εγκατάσταση φίλτρων περιορισμού της κίνησης στους δρομολογητές κορμού του Διαδικτύου στους οποίους είναι εγκατεστημένα τα LDS. Τα «ελαφρύτερης» υλοποίησης LDS χρησιμοποιούνται αποκλειστικά για την εγκατάσταση τέτοιων φίλτρων περιορισμού της κίνησης σε ακόμα περισσότερα σημεία παρουσίας χωρίς λειτουργία ανίχνευσης.

Η προσέγγιση αυτή παρουσιάζει πολλές ομοιότητες με την προτεινόμενη στην παρούσα εργασία (μηνύματα IDMEF, «αρθρωτή» αρχιτεκτονική λογισμικού, μετάδοση αποτελεσμάτων ανίχνευσης την κοινότητα, εγκατάσταση φίλτρων περιορισμού κίνησης για την αντιμετώπιση των επιθέσεων DDoS). Εντού-

τοις, οι δύο λύσεις έχουν διαφορετικούς στόχους, κλίμακα εγκατάστασης και μεθοδολογίες ανίχνευσης.

Στην προσέγγιση της παρούσας διατριβής οι ίδιες οι Συνεργατικές Οντότητες δεν υλοποιούν λειτουργίες ανίχνευσης αλλά διαχειρίζονται τοπικές (από συστήματα IDS) και απομακρυσμένες αναφορές για να καταλήξουν σε συμπεράσματα ύπαρξης ή όχι περιστατικών με υψηλό βαθμό βεβαιότητας. Μπορεί να υποστηριχθεί ότι τα διαφορετικά συστήματα IDS παρέχουν συνολικά καλύτερες πιθανότητες ανίχνευσης λόγω των διαφορετικών προσεγγίσεων που μπορεί να χρησιμοποιηθούν μεταξύ διαφόρων δικτύων.

Από την πλευρά διαχείρισης των αποτελεσμάτων το κάθε δίκτυο της Συνεργατικής Αρχιτεκτονικής μπορεί να επιλέξει να αποδώσει μεγαλύτερη ή μικρότερη εμπιστοσύνη στα απομακρυσμένα μηνύματα από συγκεκριμένες προελεύσεις αφήνοντας έτσι στον κάθε διαχειριστή την πρωτοβουλία για την «ομογενοποίηση» των αποτελεσμάτων που λαμβάνει κατά τον τρόπο που θεωρεί καλύτερο.

Η Συνεργατική Αρχιτεκτονική αποτελεί ένα σύστημα διαχείρισης και συντονισμού *ανεξάρτητων* σε μεγάλο βαθμό ενεργειών εναντίον των επιθέσεων DDoS στα πλαίσια μιας *γενικά μικρής ομαδοποίησης* δικτυακών περιοχών (domains), χωρίς να προϋποθέτει την εγκατάσταση εξωτερικού εξοπλισμού στα όρια ευθύνης των ανεξάρτητων διαχειριστικών περιοχών. Αντιθέτως, η περίπτωση του GDI είναι αμφίβολο αν θα γίνει αποδεκτή στο περίπλοκο περιβάλλον του Διαδικτύου καθώς παρεμβαίνει σε ζητήματα ιδιαίτερα ευαίσθητα, όπως αυτά της ασφάλειας[2].

Τέλος, μια άλλη σημαντική διαφορά είναι ότι η Συνεργατική Οντότητα που

[2]Οι διάφορες χώρες έχουν διαφορετικό νομικό καθεστώς ως προς την προστασία των υποδομών.

χρησιμοποιείται στην παρούσα εργασία αποτελεί *εσωτερικό* τμήμα[3] κάθε συμμετέχουσας στη Συνεργασία διαχειριστικής περιοχής, επιτρέποντας έτσι υψηλό βαθμό εμπιστοσύνης και δυνατότητα ρύθμισης (configuration) σύμφωνα με τις τοπικές πολιτικές και προτεραιότητες.

6.1.3 Σύγκριση με το πλαίσιο CITRA

Το σύστημα CITRA (Cooperative Intrusion Traceback and Response framework) [Schn00], [Ster01] αποτελεί επίσης εργασία που παρουσιάζει ομοιότητες με την παρούσα. Χρησιμοποιεί την έννοια των «κοινοτήτων» (δικτυακές περιοχές – domains) οι οποίες οργανώνονται σε τοπικές ομαδοποιήσεις (neighborhoods). Σε κάθε κοινότητα πραγματοποιείται ανίχνευση περιστατικών με επικέντρωση στα σημεία διασύνδεσης με άλλα δίκτυα (boundary points). Αναφορές ανίχνευσης διανέμονται στους κοντινούς γείτονες με αποτέλεσμα να είναι δυνατή η παρακολούθηση (tracing) της διαδρομής της επίθεσης και η λήψη μέτρων εναντίον της. Στο CITRA χρησιμοποιούνται «οδηγίες» (directives) αντιμετώπισης του περιστατικού ανεξάρτητα προς το είδος των δικτυακών συσκευών που είναι εγκατεστημένες στα διάφορα σημεία[4]. Οι επικοινωνίες εντός της υποδομής χρησιμοποιούν το εξειδικευμένο πρωτόκολλο IDIP (Intruder Detection and Isolation Protocol).

Οι διαφορές με την παρούσα εργασία επικεντρώνονται στα εξής:

- Το πλαίσιο CITRA, επικεντρώνεται σε διαχείριση ασφαλείας συστημάτων

[3] Υπό πλήρη τοπικό έλεγχο.

[4] Υπενθυμίζεται ότι στο κεφ. 4 της παρούσας εργασίας δοκιμάστηκε η παρόμοια προσέγγιση υλοποίησης μέτρων ελέγχου της κακόβουλης κίνησης ανεξάρτητα από τις εγκατεστημένες συσκευές (ή ακόμα και την εσωτερική αρχιτεκτονική του δικτύου) και η μετάφραση τους στις συγκεκριμένες ιδιαιτερότητες του εκάστοτε δικτύου με το (πειραματικό) εργαλείο Netspoc.

IDS και μεμονωμένων στοιχείων του δικτύου. Η Συνεργατική Αρχιτεκτονική λειτουργεί σε ανώτερο διαχειριστικό επίπεδο (χαρακτηριστικά δεν αναλαμβάνει το ρόλο ανίχνευσης) με σκοπό την αυτοματοποίηση και την επιτάχυνση της συνεργασίας ανεξάρτητων δικτύων (domains).

- Στο CITRA χρησιμοποιείται αποκλειστικά το πρωτόκολλο IDIP για τη διακίνηση πληροφοριών. Δημιουργείται έτσι η απαίτηση υποστήριξης του ειδικού αυτού πρωτοκόλλου σε όλα τα στοιχεία του δικτύου που πρόκειται να το χρησιμοποιήσουν καθώς και οι αντίστοιχες ρυθμίσεις ασφαλείας στο δίκτυο ώστε να επιτρέπεται η διέλευση του. Η παρούσα λύση χρησιμοποιεί την εκάστοτε διαθέσιμη μέθοδο χαμηλού επιπέδου (π.χ. peer-to-peer, multicast κ.λπ.) για το σχηματισμό του υπερκείμενου δικτύου (overlay network) ώστε να εξασφαλίζει μεν τη μέθοδο «από έναν σε πολλούς» να μη δεσμεύεται όμως από συγκεκριμένες τεχνολογικές λύσεις και να χρησιμοποιεί την πλέον πρόσφορη. Επίσης, στη Συνεργατική Υποδομή δίνεται βάρος στη χρήση του υπό εξέλιξη προτύπου IDMEF, για την κωδικοποίηση της πληροφορίας, το οποίο αποτελεί την περισσότερο αποδεκτή αυτή τη στιγμή λύση για να χρησιμοποιηθεί ως ενοποιητικός παράγοντας με πολλά διαφορετικά στοιχεία ασφαλείας (συστήματα IDS, άλλες συσκευές που χρησιμοποιούν το πρωτόκολλο κ.λπ.).

6.1.4 Σύγκριση με τη μέθοδο Pushback

Στα [Maha02] και [Ioan02] οι R. Mahajan και οι συνεργάτες του προτείνουν μια λύση για τον έλεγχο κίνησης υψηλού φόρτου. Η λύση αυτή υλοποιείται απ' ευθείας στα δικτυακά στοιχεία (δρομολογητές) τόσο για το τμήμα ανίχνευ-

σης της επιθετικής κίνησης όσο και για την αντιμετώπιση της. Μια επίθεση DDoS ανιχνεύεται από την υπέρβαση κάποιων ορίων απόρριψης πακέτων στις ουρές προώθησης ενός δρομολογητή. Στη συνέχεια επισημαίνονται και ομαδοποιούνται εκείνα τα τμήματα κίνησης που είναι υπεύθυνα για την φόρτωση του δικτύου. Τα τμήματα αυτά αποκαλούνται high bandwidth aggregates. Η επισήμανση τους γίνεται με δειγματοληψία (sampling) της κίνησης που απορίπτεται από ένα κάποιο ήδη υπάρχοντα μηχανισμό «αποσυμφόρησης» (π.χ. το Random Early Detection – RED) και η ομαδοποίηση σύμφωνα με κάποια κοινά στοιχεία (π.χ. τελικό στόχο, χαρακτηριστικά πρωτοκόλλου κ.λπ.) που παρουσιάζουν.

Το σύστημα (στο δρομολογητή), έχοντας αναγνωρίσει τα συγκεκριμένα χαρακτηριστικά της επιθετικής κίνησης ορίζει φίλτρα περιορισμού της στο δρομολογητή και μεταδίδει την πληροφορία ανίχνευσης σε άλλους δρομολογητές ανώτερου επιπέδου (στην ιεραρχία διασύνδεσης) χρησιμοποιώντας ένα ειδικό πρωτόκολλο που προτάθηκε για το σκοπό αυτό και αποκαλέστηκε Pushback. Αυτό έχει σαν αποτέλεσμα τον εντοπισμό βήμα-βήμα του μονοπατιού της επίθεσης προς τη γενική κατεύθυνση της πηγής της και το σταδιακό έλεγχο του δικτυακού εύρους που καταναλώνει.

Αν και η εργασία αυτή αποτέλεσε έναυσμα για την παρούσα διατριβή υπάρχουν σημαντικές διαφορές ανάμεσα στις δύο προσεγγίσεις που επικεντρώνονται στα εξής:

- Η προτεινόμενη στη διατριβή λύση ενεργοποιείται σε ανώτερο επίπεδο διαχείρισης. Η προσέγγιση που ακολουθείται στην παρούσα εργασία είναι κατά κύριο λόγο η προσφορά της κατάλληλης Συνεργατικής υποδομής που θα διευκολύνει τη συνεργασία μεταξύ διαφορετικών δικτύων (domains).

Βασική σχεδιαστική κατεύθυνση αποτελεί η ανεξαρτησία από τα συστήματα ανίχνευσης (IDS).

- Η λύση Pushback, σε αντίθεση με τη Συνεργατική Αρχιτεκτονική παρουσιάζει δυσκολίες στην κλιμάκωση πέρα από τα διαχειριστικά όρια ενός συγκεκριμένου δικτύου τόσο λόγω ζητημάτων εμπιστοσύνης όσο και λόγω της ανάγκης για δικαιώματα διαχειριστή στις συσκευές που απαιτούνται για επεμβάσεις χαμηλού επιπέδου τέτοιου είδους.

- Για τη υλοποίηση της λύσης Pushback απαιτείται η συνεργασία όλων των δρομολογητών ενός Αυτόνομου Συστήματος, μέχρι τους δρομολογητές συνόρου (edge routers), δηλαδή μέχρι τα όρια διαχειριστικής αρμοδιότητας της περιοχής που υλοποιεί το πρωτόκολλο Pushback. Αντιθέτως, στην παρούσα προσέγγιση δεν απαιτείται αναγκαστικά η πλήρης κάλυψη όλων των διαχειριστικών περιοχών που πιθανόν να εμπλέκονται σε μια επίθεση.

6.2 Συμπεράσματα από τη διατριβή

Στη διατριβή αυτή παρουσιάστηκε μια αρχιτεκτονική η οποία επιδιώκει κατά το δυνατόν να προσφέρει μια ολοκληρωμένη λύση στο πρόβλημα των επιθέσεων DDoS. Το πρόβλημα αυτό προσεγγίζεται και στις τρεις περιοχές αντιμετώπισης: την ανίχνευση, τον προσδιορισμό του μονοπατιού και την αντίδραση. Η πρόταση της παρούσας εργασίας είναι η συνεργασία μεταξύ διαφορετικών δικτυακών περιοχών (domains) μέσω ενός μηχανισμού που μπορεί να εξασφαλίσει αυτοματισμό, ταχύτητα, ασφάλεια και διαχειριστική ανεξαρτησία. Τα συνεργαζόμενα

δίκτυα συνθέτουν τη Συνεργατική Υποδομή.

Ο τρόπος που προτείνεται να επιτευχθεί αυτή η συνεργασία είναι με τη λειτουργία ενός εξειδικευμένου συστήματος, της Συνεργατικής Οντότητας, υπό τοπικό έλεγχο σε κάθε ένα από τα δίκτυα, το οποίο:

- Δημιουργεί ένα υπερκείμενο (overlay) δίκτυο επικοινωνίας ανάμεσα στα δίκτυα το οποίο είναι χαμηλού φόρτου, χρησιμοποιεί τη διαθέσιμη κάθε φορά τεχνολογία διασύνδεσης.

- Αναλαμβάνει τη επεξεργασία αναφορών (τοπικών και απομακρυσμένων), ώστε να περάσει σταδιακά, ανάλογα με το βαθμό συσσώρευσης βεβαιότητας, στην επιβεβαίωση ύπαρξης περιστατικών (Alert State).

- Αναλύει τη διαθέσιμη πληροφορία ώστε να προσδιορίσει το μονοπάτι (ή τουλάχιστον κάποιο μέρος του) της επίθεσης και την τοποθέτηση του οικείου δικτύου σε σχέση με αυτό.

- Αναλαμβάνει μέτρα περιορισμού και ελέγχου της κίνησης της επίθεσης ακολουθώντας τις τοπικές πολιτικές κάθε δικτύου, προσαρμόζοντας την αντίδραση στη σφοδρότητα της επίθεσης και επιλέγοντας τα σημεία επέμβασης σύμφωνα με τη διαδρομής της.

Τα κύρια χαρακτηριστικά της Συνεργατικής Υποδομής που συντίθεται κατά αυτόν τον τρόπο συνοψίζονται στα εξής:

- Τα συμμετέχοντα δίκτυα διατηρούν πλήρως τη διαχειριστική τους ανεξαρτησία

- Η Συνεργατική Υποδομή αποτελεί ένα σύστημα διαχείρισης αναφορών· γίνεται πλήρης διαχωρισμός από την καθ' αυτή λειτουργία ανίχνευσης

και χρησιμοποιούνται τα αποτελέσματα από τα διαθέσιμα σε κάθε δίκτυο συστήματα IDS. Το χρησιμοποιούμενο πρωτόκολλο IDMEF παίζει το ρόλο ενοποιητικού μέσου με τη σύνταξη των αναφορών διαφορετικών συστημάτων κατά κοινό πρότυπο στη γλώσσα XML.

- Υπάρχει η δυνατότητα χρήσης πολλών διαφορετικών τεχνικών/πρωτοκόλλων επικοινωνίας (ανάλογα με τη διαθεσιμότητα τους) για τη δημιουργία του υπερκείμενου δικτύου και την ανταλλαγή μηνυμάτων με χαμηλό φόρτο δικτύου («από έναν σε πολλούς»)

- Σε τοπικό επίπεδο η Συνεργατική Υποδομή αποτελεί ενοποιητικό στοιχείο για τις διαχειριστικές λειτουργίες[5].

- Είναι δυνατή η κλιμάκωση της Υποδομής σε μεγάλο αριθμό δικτύων ενώ προβλέπεται η παράκαμψη μη συνεργαζόμενων δικτυακών περιοχών.

- Κάθε ένα από τα δίκτυα της Συνεργασίας μπορεί να επιλέξει το βαθμό εμπιστοσύνης (βάρος) που θα αποδώσει στις απομακρυσμένες (ή ακόμα και τις τοπικές) αναφορές. Η απόδοση εμπιστοσύνης καθορίζει το πόσο θα επηρεαστεί από τα συμπεράσματα άλλων και μπορεί να απεικονίζει συσχετίσεις του πραγματικού κόσμου (εταιρικές σχέσεις, συμφωνίες, αποκλεισμό μη έμπιστων μερών κ.λπ.).

Τα πιο πάνω χαρακτηριστικά αναλύθηκαν θεωρητικά και δοκιμάστηκαν με την υλοποίηση μιας σειράς από πρωτότυπα. Σε αυτά επιβεβαιώθηκε η λειτουργία των διαφόρων τμημάτων της Υποδομής και η δυνατότητα χρήσης εναλλακτικών τεχνικών και μεθόδων διασύνδεσης της.

[5] Δείτε σχετικά το σχήμα 3.1 στο κεφ. 3.

Επιπλέον, πραγματοποιήθηκε μια σειρά από προσομοιώσεις τα αποτελέσματα των οποίων καταλήγουν στα εξής συμπεράσματα για τη Συνεργατική Υποδομή ως συνολικό σύστημα:

- Η Υποδομή είναι δυνατόν να λειτουργήσει σταθερά και να περάσει σταδιακά σε κατάσταση πλήρους ενεργοποίησης (Alert State) όλων των δικτύων μελών πάνω στο μονοπάτι μιας επίθεσης.

- Η συνολική επίδοση ανίχνευσης βελτιώνεται όσο αυξάνεται ο βαθμός εμπιστοσύνης μεταξύ των επιμέρους δικτύων της Συνεργασίας.

- Το προηγούμενο αποτέλεσμα ισχύει και όταν τα ποσοστά επιτυχίας ανίχνευσης στα επιμέρους δίκτυα είναι χαμηλά. Ένα σημαντικό συμπέρασμα είναι ότι η Υποδομή μπορεί να επιτρέψει τη ρύθμιση των κατά τόπους συστημάτων IDS σε χαμηλή ευαισθησία (αποτρέποντας τις λανθασμένες αναγνωρίσεις – false positives) και να την αντισταθμίσει με τη συνολική προσφορά πληροφορίας.

- Οι προσομοιώσεις έδειξαν επίσης καλύτερη απόδοση στην ανίχνευση ακόμα και για περιστατικά μικρής διάρκειας όταν κρατούνται χαμηλά τα όρια (χρόνου και συσσώρευσης βεβαιότητας) για τη μετάβαση κάθε μιας Συνεργατικής Οντότητας στην κατάσταση Ενεργοποίησης (Alert State).

6.3 Δυνατές μελλοντικές επεκτάσεις

Η Συνεργατική Υποδομή αποτελεί ένα σύστημα που λειτουργεί σε πολλά επίπεδα (συνεργασία μεταξύ δικτύων, πρωτόκολλα επικοινωνίας, ενσωμάτωση με

το σύστημα διαχείρισης, εσωτερική αρχιτεκτονική Οντοτήτων κ.λπ.). Αν και αποτελεί ένα γενικό σύστημα ασφαλείας που λειτουργεί ως σύνολο, ο σχεδιασμός του κατά επιμέρους τμήματα επιτρέπει την ευελιξία για αλλαγές, πιθανές βελτιώσεις, καθώς και δοκιμές νέων τεχνικών. Πολλά σημεία μπορούν ενδεχομένως να αλλάξουν ώστε να αποδώσουν καλύτερα αποτελέσματα ή πιθανά να επεκτείνουν τη λειτουργικότητα της Αρχιτεκτονικής σε νέες περιοχές που δεν είναι άμεσα προφανείς. Στο τμήμα αυτό συγκεντρώνονται οι πιο ενδιαφέρουσες από αυτές τις προτάσεις που μπορούν να αποτελέσουν αντικείμενο μελλοντικών επεκτάσεων και αντίστοιχης διερεύνησης.

- Γενίκευση της Αρχιτεκτονικής ώστε να αποτελέσει το πλαίσιο συντονισμού δράσεων ασφαλείας για μια γενικότερη αντιμετώπιση θεμάτων και περιστατικών πέραν των επιθέσεων DDoS. Σε μια τέτοια γενίκευση της χρήσης οι δυνατότητες ομαδοποιήσεων και σταδιακής κλιμάκωσης που προσφέρουν τα δίκτυα peer-to-peer και το IP multicast μπορεί να επιτρέψει τη δημιουργία συγκεκριμένων «περιοχών ασφαλείας» κατά το πρότυπο της οργάνωσης ευθύνης των ομάδων CERTs ("Constituencies")

- Πιθανός πλήρης διαχωρισμός ανάμεσα στο επικοινωνιακό κομμάτι και το κομμάτι της αντίδρασης. Ο διαχωρισμός αυτός υφίσταται ήδη σε επίπεδο αρχιτεκτονικής λογισμικού με τη χρήση διαφορετικών λειτουργικών μονάδων. Αν ολοκληρωθεί ώστε να υπάρχει η δημιουργία δύο διαφορετικών τύπων Οντοτήτων (πλήρους και επικοινωνίας/συλλογής στοιχείων)[6] θα μπορεί να επεκταθεί και να γενικευτεί η εγκατάσταση του «απλού» τύπου Οντότητας (πιθανά με παράλληλη λειτουργία του σχετικού λογισμικού σε

[6] Με παραπλήσιο τρόπο προς το DAD – δείτε πιο πάνω

άλλα γενικής χρήσης συστήματα).

- Χρησιμοποίηση εργαλείων διαχειριστικής πολιτικής τόσο σε επίπεδο οργάνωσης μεταξύ διαφορετικών δικτύων («αποδεκτές» επικοινωνίες και απόδοση εμπιστοσύνης σε επομακρυσμένα μηνύματα) όσο και σε επίπεδο εσωτερικής λειτουργίας: μετάβαση από τις παραμέτρους διαμόρφωσης σε αρχεία πολιτικής για την ίδια τη συνεργατική Οντότητα.

- Στην αρχιτεκτονική peer-to-peer είναι ενδεχομένως δυνατόν το Σημείο Συντονισμού (RP) να απόκτησει επιπλέον λειτουργικότητα. Είναι δυνατόν έτσι σε αυτό να διατηρείται πλήρης πληροφορία δικτυακής διασύνδεσης και δρομολόγησης (αντί να αποκτάται αυτή από το πρωτόκολλο δρομολόγησης ή με εργαλεία όπως το traceroute). Η προσέγγιση αυτή δεν υιοθετήθηκε στο πρώτο στάδιο εξέτασης του προβλήματος αφ' ενός για λόγους απλότητας (η αναπαράσταση μεγάλου μέρους του δικτύου στην Οντότητα δημιουργεί ειδικές απαιτήσεις στην υλοποίηση) αφ' ετέρου δε για να εξεταστεί η απλούστερη δυνατή περίπτωση.

- Θα ήταν ενδιαφέρον να διερευνηθεί η προσαρμογή της λειτουργίας της Συνεργατικής Αρχιτεκτονικής στα χαρακτηριστικά λειτουργίας των κατά τόπους συστημάτων IDS. Βέβαια στη βιβλιογραφία δεν υπάρχει ένα κοινό μέτρο αξιολόγησης αυτών των συστημάτων αλλά αυτό θα μπορούσε να γίνει και εμπειρικά με τον καθορισμό μιας «γενικά εκτιμώμενης» (στα πλαίσια της Συνεργατικής Υποδομής) ακρίβειας των συστημάτων IDS σε κάθε δίκτυο. Οι τρόποι προσαρμογής της υποδομής σε μια τέτοια πληροφορία μπορεί να είναι:

  - Με την πιθανή ρύθμιση της παραγωγής μηνυμάτων από την Οντότητα σε αντιστοιχία με την αναμενόμενη ακρίβεια (ποσοστά false positives) των τοπικών IDS
  - Σε κάθε δίκτυο οι παραλήπτες απομακρυσμένων μηνυμάτων να αποδίδουν βάρος στα μηνύματα από κάθε δίκτυο ανάλογα με την αξιολόγηση των συστημάτων IDS του αποστολέα. Με τον παρόντα σχεδιασμό, αυτό είναι δυνατόν για κάθε επιμέρους διαχειριστή αλλά μπορεί να γίνεται στα πλαίσια της Συνεργασίας κατά κάποιο αυτόματο τρόπο

- Χρήση εξειδικευμένου φιλτραρίσματος με μερική αποκοπή της συγκεκριμένης επιθετικής κίνησης προς το τελικό δίκτυο-στόχο ώστε αυτή να μελετηθεί πιθανά (α) ως προς τα χαρακτηριστικά της που ενδέχεται να εμπλουτίσουν βάσεις χαρακτηριστικών (signatures) για επιθέσεις (π.χ. του συστήματος Snort) και (β) για τρόπους λειτουργίας Worms και άλλων τύπων αυτόματα διαδιδόμενου κακόβουλου λογισμικού.

- Χρήση «επιπέδων λειτουργίας»: Συμμετοχή μεν στη Συνεργατική Υποδομή για απόκτηση των πληροφοριών και της υποδομής επικοινωνίας, ανταπόκριση όμως μόνον σε περιστατικά που αφορούν συγκεκριμένα δίκτυα και/ή συγκεκριμένα χαρακτηριστικά επιθετικής κίνησης σύμφωνα με εταιρικές συμφωνίες κ.λπ. Αυτό είναι ένα χαρακτηριστικό που αν εφαρμοστεί μειώνει μεν την ισοτιμία των κόμβων επιτρέπει όμως κάποια επιπλέον λειτουργικότητα. Η σκοπιμότητα του είναι θέμα διερεύνησης.

- Ανταλλαγή επιπλέον πληροφορίας μεταξύ των Οντοτήτων που να αναδεικνύουν τον όγκο της κίνησης που φαίνεται να δημιουργεί η επίθεση σε

διάφορα σημεία παρουσίας της Συνεργατικού Υποδομής. Η ανασύνθεση της μπορεί να υποδείξει τις κύριες διαδρομές της κακόβουλης κίνησης και κατ' επέκταση την κατεύθυνση προς την οποία βρίσκονται περισσότερα τα δίκτυα πηγές.

- Στα δίκτυα peer-to-peer είναι δυνατή η χρήση πολλαπλών επιπέδων κατακερματισμού της πληροφορίας περιστατικού. Στο κεφ. 3 εξετάζεται η χρήση δικτύων peer-to-peer με δρομολόγηση βασισμένη σε κλειδί (Key Based Routing – KBR) ως υπόβαθρο επικοινωνίας αλλά και οργάνωσης της Συνεργατικής Υποδομής. Προβλέπεται έτσι η πληροφορία του περιστατικού (πρωτόκολλο και θύρα της κακόβουλης κίνησης, τύπος πακέτων, περιοχή διευθύνσεων του τελικού στόχου κ.λπ.) να αποτελεί την είσοδο μιας συνάρτησης κατακερματισμού (Hash-function) για να οριστεί ο κόμβος της Υποδομής που θα συγκεντρώνει στη συνέχεια τις πληροφορίες για το συγκεκριμένο περιστατικό.

  Αντί για τη χρήση της συνολικής πληροφορίας του περιστατικού ως είσοδο της συνάρτησης κατακερματισμού είναι δυνατόν η διεργασία αυτή να γίνεται κατά τμήματα μόνον αυτής της πληροφορίας. Το αποτέλεσμα του κατακερματισμού κάθε επιμέρους τμήματος πληροφορίας περιστατικού μπορεί να χρησιμοποιηθεί ως «διεύθυνση» ενός κόμβου αποθήκευσης στο δίκτυο peer-to-peer KBR. Τα στοιχεία για το περιστατικό μπορούν να αποθηκευτούν στους *συγκεκριμένους* κόμβους που προκύπτουν από το κατακερματισμό κάθε τμήματος της πληροφορίας. Κάθε ένας τέτοιος κόμβος έτσι, συγκεντρώνει αυτομάτως την πλήρη εικόνα για όλα τα περιστατικά που παρουσιάζουν ένα συγκεκριμένο χαρακτηριστικό (π.χ. είδος

πρωτοκόλλου TCP). Αντιστρόφως, κάποιος που ζητά στατιστικές πληροφορίες για τα περιστατικά βάσει συγκεκριμένου χαρακτηριστικού είναι δυνατόν να αναζητήσει γενικευμένα στοιχεία στον αντίστοιχο κόμβο του δικτύου peer-to-peer που προκύπτει από την εφαρμογή της συνάρτησης κατακερματισμού στο χαρακτηριστικό αυτό.

- Πιθανή χρησιμοποίηση της επιπλέον λειτουργικότητας που προσφέρει το IP Multicast στο IPv6 (προκαθορισμένα Multicast groups για συγκεκριμένες ομάδες συσκευών — π.χ. δρομολογητές — και συγκεκριμένες περιοχές —Link Local - Site Local) για δημιουργία συγκεκριμένων ομαδοποίησεων (π.χ. γεωγραφικών ή εμπορικών) ανάμεσα στα δίκτυα που συμμετέχουν στη Συνεργατική Υποδομή. Όπως αναφέρεται αλλού στη διατριβή, κάτι τέτοιο μπορεί να επιτευχθεί στο IPv4 με τον έλεγχο της παραμέτρου Time to Live (TTL) στα πακέτα.

- Ο μηχανισμός των μηνυμάτων κανονικής λειτουργίας (Heartbeats) στις περιπτώσεις που χρησιμοποιείται στην τρέχουσα προσέγγιση[7] απλά προκαλεί μια μετάβαση σε κατάσταση Υποψίας Ύπαρξης Περιστατικού (Suspicion State). Μελλοντικά μπορεί να χρησιμοποιηθεί για την ενεργοποίηση συγκεκριμένων ελέγχων προς την κατεύθυνση που υποδεικνύουν οι (μη) λήψεις των μηνυμάτων αυτών.

[7] Όταν γίνεται χρήση επικοινωνιών υποβάθρου IP Multicast. Δείτε σχετικά την ενότητα 3.4.1.

Βιβλιογραφία

[Agar04] S. Agarwaly, T. Dawson, and C. Tryfonas, *DDoS Mitigation via Regional Cleaning Centers*, Sprint ATL Research Report Rr04-Atl-013177, Jan. 2004

[Alme00] K. Almeroth, *The Evolution of Multicast: From the MBone to Inter-Domain Multicast to Internet2 Deployment*, IEEE Network, vol. 14, pp. 10-20, January/February 2000

[Andr04] G. Androulidakis, V. Chatzigiannakis, M. Grammatikou, and F. Stamatelopoulos, *Network Flow-Based Anomaly Detection of DDoS Attacks*, TERENA Networking Conference 2004, Rhodes June 2004

[Asti01b] P. Astithas, V. Pappas, and B. Maglaris, *Detecting Intrusions by Monitoring System Processes*, in Proceedings of the 8th HPOVUA Plenary Workshop on Network and Systems Management, Berlin, Germany, June 2001

[Bamb05] The Bamboo Distributed Hash Table web pages, accessed Dec. 27, 2005, `http://bamboo-dht.org/`

[Barl00] Jason Barlow and Woody Thrower, *TFN2K — An Analysis*, Revision: 1.3, AXENT Security Team, Feb. 10, 2000 (Updated Mar. 7, 2000), `http://packetstormsecurity.com/distributed/TFN2k_Analysis-1.3.txt`

[Behr02] M. Behringer, *Tracing DoS Attacks*, Hi Tech 2002 Workshop, Limmerick, IE, June 2002

[Bell00] S. Bellovin, *ICMP Traceback Messages*, IETF Internet Draft, Mar. 2000 (work in progress) draft-bellovin-itrace-00.txt

[Boun02] J. Bound, L. Toutain, O. Medina, F. Dupont, H. Afifi, and A. Durand, *Dual-stack Transition Mechanism (DSTM)*, IETF Internet Draft, December 2002 (work in progress) draft-ietf-ngtrans-dstm-08.txt

[Carp01] B. Carpenter and K. Moore, *Connection of IPv6 Domains via IPv4 Clouds*, RFC 3056, February 2001, `http://www.ietf.org/rfc/rfc3056.txt`

[Cast02] M. Castro, P. Druschel, A-M. Kermarrec and A. Rowstron, *One ring to rule them all: Service discovery and binding in structured peer-to-peer overlay networks*, SIGOPS European Workshop, France, September, 2002

[Casw03] B. Caswell and J. Hewlett, *Snort Users Manual 2.2.0*, The Snort Project, 2003, `http://www.snort.org/docs/snort_manual/`

[Ceri95] Cerias Web Pages, *Info About Satan*, Jun 2, 1995, `http://www.cerias.purdue.edu/about/history/coast/satan.php`

[Cert] CERT Coordination Center web pages, accessed July 2004, `http://www.cert.org/`

[Cert01] CERT CC, *Advisory CA-2001-26 Nimda Worm*, Sep. 18, 2001, `http://www.cert.org/advisories/CA-2001-26.html`

[Cert96] CERT CC, *Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks*, Sep 19, 1996, `http://www.cert.org/advisories/CA-1996-21.html`

[Cert97] CERT CC, *Advisory CA-1997-28 IP Denial-of-Service Attacks*, Dec. 19, 1997, `http://www.cert.org/advisories/CA-1997-28.html`

[Cert98] CERT CC, *Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks*, Jan 5, 1998, `http://www.cert.org/advisories/CA-1998-01.html`

[Chan02] Rocky Chang, *Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial*, IEEE Communications Magazine, pp. 42–51, October 2002

[Cisc-a] Cisco Corporation, *Improving Security on Cisco Routers*, Document ID: 13608, `http://www.cisco.com/warp/public/707/21.html`

[Cisc-net] Cisco Systems Web Site, *Cisco IOS Software Netflow*, accessed Jul. 26, 2004, `http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml`

[Comp00] Ann Harrison, *Cyberassaults hit Buy.com, eBay, CNN and Amazon, Computerworld web site*, Feb. 9, 2000, accessed Aug 30, 2004, `http://www.computerworld.com/news/2000/story/0,11280,43010,00.html`

[Conv04] S. Convery and D Miller, *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)*, Presentation at the 17th NANOG, May 24, 2004

[Cros95] M. Crosbie, *Defending a Computer System Using Autonomous Agents*, in proc. of the 18th NISSC conference, Oct. 1995

[Csi03] R. Richardson, *2003 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2003

[Csi04] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, *2004 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, Aug. 2004

[Darm00] T. Darmohray and R. Oliver, *Hot Spares for DoS Attacks*, ;login: magazine, 25(7), July 2000

[Dean01] D. Dean, M. Franklin, and A. Stubblefield, *An Algebraic Approach to IP Traceback*, Network and Distributed System Security Symposium, NDSS '01, February 2001

[Deba04] H. Debar, D. Curry, and B. Feinstein, *The Intrusion Detection Message Exchange Format*, IETF Internet Draft, July 8, 2004 (work in progress) draft-ietf-idwg-idmef-xml-12

[Deba99] Herve Debar, Marc Dacier, and Andreas Wespi, *Towards a Taxonomy of Intrusion-Detection Systems*, Computer Networks, Special issue on computer network security, 31(9), April 1999, pp. 805–822

[Ditt04] D. Dittrich, *Distributed Denial of Service (DDoS) Attacks/tools*, Web pages accessed Jul. 26, 2004, `http://staff.washington.edu/dittrich/misc/ddos/`

[Ditt99a] David Dittrich, *The Dos Project's "Trinoo" Distributed Denial of Service Attack Tool*, October 21, 1999, `http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt`

[Ditt99b] David Dittrich, *The "Stacheldraht" Distributed Denial of Service Attack Tool*, Dec. 31, 1999, `http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt`

[Doul04] Christos Douligeris and Aikaterini Mitrokotsa, DDoS Attacks and Defence Mechanisms: Classification and State-of-the-art, Computer Networks Journal 44(2004), pp. 643–666

[Esta01] C. Estan and G. Varghese, *New directions in traffic measurement and accounting*, in Proceedings of the 2001 ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, Nov. 2001, pp. 75–80

[Farm90] D. Farmer and E. Spafford, *The COPS Security Checker System*, USENIX Conference Proceedings, Anaheim, CA, Summer 1990, pp. 165–170

[Fein02] B. Feinstein, G. Matthews, and J. White, *The Intrusion Detection Exchange Protocol (IDXP)*, IETF Internet Draft, October 22, 2002 (work in progress) draft-ietf-idwg-beep-idxp-07

[Ferg00] P. Ferguson and D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, RFC 2827, May 2000, `http://www.ietf.org/rfc/rfc2827.txt`

[Fost01] I. Foster, C. Kesselman, and S. Tuecke, *The Anatomy of the Grid: Enabling Scalable Virtual Organizations*, Intl. Journal of High Performance Computing Applications, Vol. 15(3), pp. 200–222, 2001 `http://www.globus.org/research/papers/anatomy.pdf`

[Frin98] D. Frincke, D. Tobin, J. McConnell, J. Marconi and D. Polla, *A Framework for Cooperative Intrusion Detection*, Proceedings of the 21st National Information Systems Security Conference, pp. 361–373, October 1998

[Gibs04] Steve Gibson, *The Strange Tale of the Denial of Service Attacks Against GRC.COM*, Gibson Research Corporation web site, accessed Jul. 26, 2004, `http://grc.com/dos/grcdos.htm`

[Glob05] The Globus Alliance, *The WS-Resource Framework*, accessed Dec. 27, 2005, `http://www.globus.org/wsrf/`

[Gosl00] J. Gosling, B. Joy, G. Steele, and G. Bracha, *Java^{TM} Language Specification, 2nd Edition*, Addison Wesley, 2000

[Grid05] GRIDCC Project Home Page, accessed Dec. 27, 2005, `http://www.gridcc.org/`

[Gune] Σελίδες Ωεβ Ελληνικού Ακαδημαϊκού Δικτύου – GUnet, `ηττπ://ωωω.γυνετ.γρ/`

[Hard68] G. Hardin, *The Tragedy of the Commons*, Science Magazine, Vol. 162, Issue 3859, pp. 1243-1248, Dec. 1968

[Hind98] R. Hinden, M. O'Dell, S. Deering, *An IPv6 Aggregatable Global Unicast Address Format*, RFC 2374, July 1998, `http://www.ietf.org/rfc/rfc2374.txt`

[Huss03] Alefiya Hussain, John Heidemann, and Christos Papadopoulos, *A Framework for Classifying Denial of Service Attacks*, in the Proceedings of SIGCOMM 2003, 2003

[Info04] M. Villano, *MCI to Offer New Protection Against Denial-Of-Service Attacks*, Information week web site, Mar. 01, 2004

[Inse96] Insecure.org, *Ping of Death*, Oct. 21, 1996, `http://www.insecure.org/sploits/ping-o-death.html`

[Ioan02] J. Ioannidis, S. Bellovin, *Implementing Pushback: Router-Based Defence Against DDoS Attacks*, Network and Distributed System Security Symposium, NDSS 2002, San Diego, CA, Feb. 2002

[Jmx04] Java Management Extensions (JMX) Technology Overview, Sep. 2004 `http://java.sun.com/j2se/1.5.0/docs/guide/jmx/overview/JMXoverviewTOC.html`

[Jxta] JXTA Project's web pages, accessed Jan. 2005 `http://www.jxta.org/`

[Kohl00] M. Kohler, *NP Complete*, Embedded Systems Programming Journal, November 2000, pp. 45–60

[Kots01] C. Kotsokalis, D.Kalogeras, and B. Maglaris, *Router-Based Detection of DoS and DDoS Attacks*, HP OpenView University Association (HPOVUA) Conference '01, Berlin, Germany, June 2001

[Kuro] Kuro5hin.org Inc, *Anycast Addressing on the Internet* web pages, accessed March 2006 `http://aharp.ittns.northwestern.edu/papers/k5-anycast/index.html`

[Lan03] Kun-chan Lan, Alefiya Hussain and Debojyoti Dutta, *Effect of Malicious Traffic on the Network*, Passive and Active Measurement Workshop (PAM), San Diego, April, 2003

[Land94] C. Landwehr, A. Bull, J. McDermott, and W. Choi, *A Taxonomy of Computer Program Security Flaws*, ACM Computing Surveys, 26 (3), Sept. 1994, pp. 211–254

[Lee02] S. Lee, C. Shields, Technical, *Legal, and Societal Challenges to Automated Attack Traceback*, IEEE IT Professional Magazine May/June 2002, Vol. 4 (No. 3), pp. 12–18

[Libe04] Liberouter web site, accessed Sep. 6, 2004, `http://www.liberouter.org`

[Magl05] V. Maglaris, S. Papavassiliou, C. Siaterlis, A. Lenis, A. Moralis, and G. Koutepas, *Proposal for a Network Anomaly Detection Application in GRIDCC*, Technical Proposal, January 10, 2005

[Maha02] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, *Controlling High Bandwidth Aggregates in the Network*, ACM SIGCOMM Computer Communications Review 32:3, July 2002, pp. 62–73

[Mank01] A. Mankin, D. Massey, C.L Wu, S.F Wu, L. Zhang, *On the Design of "Intention-Driven" ICMP Traceback*, IEEE International Conference on Computer Communications and Networks (ICCCN), Oct 2001

[Micr01] Microsoft Corporation, *Microsoft Security Bulletin MS01-044*, Aug 15, 2001, `http://www.microsoft.com/technet/security/bulletin/MS01-044.mspx`

[Mirk04] Jelena Mirkovic and Peter Reiher, *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communications Review, Volume 34, Number 2: April 2004

[Moor01] David Moore, Geoffrey Voelker, and Stefan Savage, *Inferring Internet Denial-of-Service Activity*, Proc. 10th USENIX Security Symposium, 2001

[Netc04] Netcraft Web Site, *Fast-Moving Virus Launches DDoS on SCO*, Jan 24, 2004, `http://news.netcraft.com/archives/2004/01/27/fastmoving_virus_launches_ddos_on_sco.html`

[Nets] NetSPoC, a Network Security Policy Compiler, Documentation Web Pages, accessed Feb. 2005 `http://netspoc.berlios.de/netspoc.html`

[Nfr04] Network Flight Recorder web pages, accessed Sep. 3, 2004, `http://www.nfr.com`

[Osvd01] Open source Vulnerability Database, *Microsoft IIS Invalid WebDAV Request DoS*, disclosure date: May 6, 2001, `http://www.osvdb.org/displayvuln.php?osvdb_id=5606`

[Papa03] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, *COSSACK: Coordinated Suppression of Simultaneous Attacks*, In Proceedings of DISCEX III, Arlington VA, April 2003

[Park01] K. Park and H. Lee, *On the Effectiveness of Route-Based Packet Filtering for Distributed DDoS Attack Prevention in Power-Law Internets*, In Proc. of the 2001 ACM SIGCOMM, 2001

[Paxs01] V. Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, Computer Communication Review 31(3), July 2001

[Peng04] T. Peng, C. Leckie, and R. Kotagiri, *Proactively Detecting DDoS Attack Using Source IP Address Monitoring*, Networking 2004, Athens, Greece, May 2004

[Perr00] A. Perrig, R. Canetti, J.D. Tygar, and D. Xiaodong Song, *Efficient Authentication and Signing of Multicast Streams over Lossy Channels*, in Proc. of IEEE Security and Privacy Symposium, PCTS 2000, pp. 56-73, May 2000

[Prev99] V. Prevelakis, *A Secure Station for Network Monitoring and Control*, 8th USENIX Security Symposium, Washington DC, 1999

[Ratn01] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, *A scalable content-addressable network*, Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, p.161–172, August 2001, San Diego, California, United States

[Regi02] Tim Richardson, *Cloud Nine blown away, blames hack attack*, The Register web site, Jan. 22, 2002, accessed Aug 30, 2004, `http://www.theregister.co.uk/2002/01/22/cloud_nine_blown_away_blames/`

[Rekh95] Y. Rekhter, T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 1771, Mar. 1995, `http://www.ietf.org/rfc/rfc1771.txt`

[Reih02] P. Reiher, J. Mirkovic, and G. Prier, *Attacking DDoS at the Source*, 10th IEEE International conference on Network Protocols, Paris, France, Nov. 2002

[Rose01a] E. Rosen, A. Viswanathan, R. Callon, *Multiprotocol Label Switching Architecture*, RFC 3031, Jan. 2001, `http://www.ietf.org/rfc/rfc3031.txt`

[Rose01b] Rose, M., *The Blocks Extensible Exchange Protocol Core*, RFC 3080, March 2001, `http://www.ietf.org/rfc/rfc3080.txt`

[Sava00] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, *Practical Network Support for IP Traceback*, In Proceedings of the 2000 ACM SIGCOMM Conference, pp. 295–306, Stockholm, Sweden, Aug. 2000

[Savo04] P. Savola, C. Patel, *Security Considerations for 6to4*, IETF Internet Draft, July 18, 2004 (work in progress) draft-ietf-v6ops-6to4-security-04.txt

[Scam04] Scaleable Monitoring Platform for the Internet (SCAMPI) Project consortium, *Distributed Security Applications for the Internet using SCAMPI*, SCAMPI Project Deliverable E2.1, May 2004

[Schn00] D. Schnackenberg, K. Djahandari, and D. Sterne, *Infrastructure for Intrusion Detection and Response*, In Proceedings of the DARPA Information Survivability Conference and Exposition, Anaheim, CA, USA, January 2000

[Schn01] D. Schnackengerg, H. Holliday, R. Smith, K. Djahandari, and D. Sterne, *Cooperative Intrusion Traceback and Response Architecture (CITRA)*, In Proceedings of the DARPA Information Survivability Conference and Exposition II, 2001, DISCEX '01, Vol.1, pp. 56–68

[Siat04] C. Siaterlis and B. Maglaris, *Towards Multisensor Data Fusion for Dos Detection*, Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 439–446

[Siri04] V.A. Siris and F. Papagalou, *Application of anomaly detection algorithms for detecting SYN flooding attacks*, Proceedings of the 2004 IEEE Global Telecommunications Conference, GLOBECOM '04

[Smug05] The Secure Multicast Research Group (SMuG), accessed Dec. 27, 2005, `http://www.securemulticast.org/smug-index.htm`

[Snoe01] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, and W. Strayer, *Hash-Based IP Traceback*, In Proc. of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2001

[Song01] D. Song and A. Perrig, *Advanced and Authenticated Marking Schemes for IP Traceback*, IEEE Infocomm 2001

[Spaf00] Eugene H. Spafford and Diego Zamboni, *Intrusion Detection Using Autonomous Agents*, Computer Networks, 34(4), October 2000, pp. 547–570

[Srem02] Joe Sremack and Jim Yuill, *Forensic Challenge 25*, The Honeynet Project and North Carolina State University, Nov. 2002, `http://project.honeynet.org/scans/scan25/sol/NCSU/main.html`

[Stam01] F. Stamatelopoulos, G. Koutepas, P. Astithas, and B. Maglaris, *End-to-End, Multiple-Domain Bandwidth Management*, poster, HP OpenView University Association (HPOVUA) Conference '01, Berlin, Germany, June 2001

[Stan02] S. Staniford, V. Paxson, and N. Weaver, *How to 0wn the internet in your spare time*, 2002, in Proceedings of the 11th USENIX Security Symposium

[Ster01] D. Sterne, K. Djahandari, B. Wilson, B. Babson, D. Schnackenberg, H. Holliday, and T. Reid, *Autonomic Response to Distributed Denial of Service Attacks*, In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, RAID 2001, Davis, CA, USA, pp. 134–149, October 2001

[Stoi01] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and Hari Balakrishnan, *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications*, Proceedings of the ACM SIGCOMM '01 Conference, Aug. 2001, San Diego, California

[Ston00] R. Stone, *CenterTrack: An IP Overlay Network for Tracking DoS Floods*, 9th USENIX Security Symposium, Denver, CO, Aug. 2000

[Stra04] T. Strauf et. al., *Operational procedures for secured management with transition mechanisms (version 2)*, 6Net Project Deliverable 6.2.2, May 2004

[Sung02] Minho Sung, Markus Haas, and Jun Xu, *Analysis of DoS attack traffic data*, 2002 FIRST Conference, Hawaii, June 2002

[Temp04] F. Templin, T. Gleeson M. Talwar, and D. Thaler, *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*, IETF Internet Draft, May26, 2004 draft-ietf-ngtrans-isatap-22.txt

[Ti] Trusted Introducer for CSIRTs in Europe, Terena Trusted Introducer web pages, accessed Jan. 2005 `http://www.ti.terena.nl`

[Town99] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, *Layer Two Tunneling Protocol "L2TP"*, RFC 2661, Aug. 1999, `http://www.ietf.org/rfc/rfc2661.txt`

[Vale04] F. Valeur, G. Vigna, C.Kruegel, and R. Kemmerer, *A Comprehensive Approach to Intrusion Detection Alert Correlation*, IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 3, pp. 146-169, July-September 2004

[Vixi02] Paul Vixie, Gerry Sneeringer, Mark Schleifer, *Events of 21-Oct-2002*, Web page, November 24, 2002, accessed Aug 30, 2004, `http://d.root-servers.org/october21.txt`

[Wan02] K. K. Wan and R.Chang, *Engineering of a Global Defence Infrastructure for DDoS Attacks*, In Proc. of IEEE International Conference on Networking, Aug. 2002

[Warf03] M. Warfield, *Security Implications of IPv6*, white paper, Internet Security Systems, 2003

[Webo-a] Webopedia Computer Dictionary, *ADSL*, accessed July 2004, `http://www.webopedia.com/TERM/A/ADSL.html`

[Webo-b] Webopedia Computer Dictionary, *Cable Modem*, accessed July 2004, `http://www.webopedia.com/TERM/c/cable_modem.html`

[Yoid00] P. Francis, Y. Pryadkin , P. Radoslavov, R. Govindan, B. Lindell, *Yoid: Your Own Internet Distribution*, `http://www.icir.org/yoid/`

[Zhao01] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph, *Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing*, Technical Report, UCB/CSD-01-1141, University of California at Berkeley, Apr 2001

[Αλευ05] Π. Αλευράς, *Μηχανισμός Αυτόματης Υλοποίησης Πολιτικών για Αντιμετώπιση Επιθέσεων ΔΔοΣ*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Νοέμβριος 2005

[Ανδρ03] Γ. Ανδρουλιδάκης, *Ανάπτυξη Κατανεμημένου Συστήματος Ανίχνευσης Επιθέσεων σε Δίκτυα Υπολογιστών*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Ιούνιος 2003

[Αστη01] Π. Αστήθας, *Ανίχνευση Επιθέσεων σε Δίκτυα Υπολογιστών*, Διδακτορική Διατριβή, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Μάιος 2001

[Κοτσ00] Κ. Κοτσωκάλης, *Panoptis: Αναγνώριση Denial of Service (DoS) attacks με το Cisco NetFlow*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Φεβρουάριος 2001

[Λεβα05] Κ. Λεβαντή, *Χρησιμοποίηση ενός Content-Addressable Δικτύου Peer-To-Peer σε ένα Σύστημα για την Αντιμετώπιση Επιθέσεων DDoS*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Ιούνιος 2005

[Πενε99] *Διαχείριση Δικτυακών Υπηρεσιών με Εγγύηση Ποιότητας*, Τελική Έκθεση Προόδου Φυσικού Αντικειμένου, Πρόγραμμα Ενίσχυσης Ερευνητικού Δυναμικού ΠΕΝΕΔ 99, Επιχειρησιακό Πρόγραμμα Ερευνάς και Τεχνολογίας ΕΠΕΤ ΙΙ, Κωδικός Έργου: 99 ΕΔ-259, Οκτώβριος 2001

[Πουγ04] Ν. Δ. Πουγούνιας, *Δημιουργία Peer-to-Peer Δικτύου Συνεργασίας με Σκοπό την Αποτελεσματική Αντιμετώπιση Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσίας*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Φεβρουάριος 2004

[Χατζ02] Β. Χατζηγιαννάκης, *Κατανεμημένο Δίκτυο Αντιμετώπισης Επιθέσεων (Υλοποίηση Συστήματος Επικοινωνίας και Διαχείρισης)*, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π., Σεπτέμβριος 2002

S.D.G.