ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη και μοντελοποίηση δικτύου επικοινωνίας IoT οντοτήτων και εκτέλεση σεναρίων επίθεσης/άμυνας από εξωτερικούς πράκτορες καθώς και πρόταση τεχνικών/πρωτοκόλλων ασφάλειας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του
ΜΙΧΑΗΛ ΙΩΑΝΝΗ

Επιβλέπων Καθηγητής: Δρ. Παναγιώτης Σαρηγιαννίδης

Κοζάνη 2019

ΕΥΧΑΡΙΣΤΙΕΣ

Με την περάτωση της παρούσας διπλωματικής εργασίας θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Σαρηγιαννίδη Παναγιώτη καθώς και τον διδακτορικό φοιτητή Ράδογλου Γραμματίκη Παναγιώτη. Τον πρώτο, για την εμπιστοσύνη που μου έδειξε στην εκπόνηση της παρούσας διπλωματικής εργασίας και τον δεύτερο για τις παραγωγικές υποδείξεις του και το πολύ καλό κλίμα συνεργασίας που διαμόρφωσε συμβάλλοντας τα μέγιστα για την κατάρτιση της διπλωματικής μου εργασίας

Ιδιαίτερα θερμές ευχαριστίες θέλω να δώσω στην οικογένεια μου για την συνεχή συμπαράσταση, για τις πολύτιμες συμβουλές τους και για όλα όσα μου έχουν προσφέρει όλα αυτά τα χρόνια της ζωής μου αλλά και των σπουδών μου.

Περιληψη

Η παρούσα διπλωματική έχει ως σκοπό την απόδειξη των κενών ασφαλείας του Διαδικτύου των Αντικειμένων (Internet of Things - IoT) με τη χρήση της τεχνικής των Κατανεμημένων Επιθέσεων Άρνησης Παροχής Υπηρεσιών. Στην ανάπτυξη της εργασίας παρουσιάζονται συνοπτικά η δομή των IoT, γενικές πληροφορίες καθώς και μορφές επιθέσεων οι οποίες το απειλούν αφού γίνεται όλο και πιο διευρυμένο και δημοφιλή. Η ραγδαίως αναπτυχθείσα ανάγκη του ανθρώπου για άμεση διάθεση δεδομένων και πληροφοριών σε πραγματικό χρόνο έχει οδηγήσει το κόσμο της τεχνολογίας στη δημιουργία μίας νέας μορφής δικτύων τα οποία υλοποιούνται με τη συμμετοχή διασυνδεδεμένων συσκευών, οι οποίες έχουν τη δυνατότητα να συλλέξουν και να αποστείλουν πληροφορίες σε πραγματικό χρόνο. Η μορφολογία και η δομή των δικτύων αυτών παρουσιάζει μεγάλη ετερογένεια όσο προς τις οντότητες αλλά και όσο ως προς τις τεχνολογίες που συμμετέχουν. Η γενική μορφή όμως των δικτύων αυτών χωρίζεται σε δύο μεγάλες κατηγορίες. Τα κλειστά/ιδιωτικά IoT δίκτυα όπως χαρακτηρίζονται τα τοπικά/ιδιωτικά δίκτυα π.χ. οικιακά, εταιρικά, και τα ανοικτά δίκτυα όπως αυτά ορίζονται τα δημόσια δίκτυα ευρείας χρήσης και κάλυψης. Η δομή αυτών των δικτύων διαφέρει αρκετά, παρόλο που έχουν την ίδια λογική και σκοπό ύπαρξης. Και τα δύο μορφής δίκτυα αποτελούνται από συσκευές οι οποίες αλληλοεπιδρούν σε πραγματικό χρόνο αποστέλλοντας και παραλαμβάνοντας πληροφορίες. Τα πιθανά οφέλη του IoT μπορούν να χαρακτηριστούν και ως απεριόριστα, όπως επίσης και οι εφαρμογές του που μπορούν να αλλάξουν ριζικά τον τρόπο με τον οποίο εργαζόμαστε και ζούμε.

Στα παρακάτω κεφάλαια αρχικώς θα αναλυθεί η γενική δομή της μορφολογίας του IoT και στη συνέχεια θα γίνει εκτενέστερη αναφορά ως προς τα κενά και τα προβλήματα ασφάλειας, τα οποία αντιμετωπίζουν τα δίκτυα αυτά. Στην εργασία περιλαμβάνεται πειραματικό μέρος το οποίο υλοποιεί μία Κατανεμημένη Επίθεση Άρνησης Παροχής Υπηρεσιών σε εικονικό περιβάλλον κλειστού IoT δικτύου.

Το πειραματικό μέρος επικεντρώνεται στην απόδειξη της ευπάθειας των δικτύων αυτών με τη συγκεκριμένη μορφή επίθεσης η οποία μπορεί να υλοποιηθεί με διάφορους τρόπους και μεθόδους. Οι οντότητες που εξαπολύουν τις επιθέσεις υλοποιούνται με τη χρήση αντικειμενοστραφής γλώσσας προγραμματισμού. Οι δικτυακές οντότητες-πελάτες που υλοποιούνται έχουν τη δυνατότητα αποστολής δικτυακής κίνησης πρωτοκόλλου HTTPS προς τον εξυπηρετητή.Οι επιτιθέμενες οντότητες-πελάτες εξαπολύουν ταυτόχρονη επίθεση προς τον εξυπηρετητή με σκοπό να προκαλέσουν την άρνηση παροχής υπηρεσιών από τον εξυπηρετητή προς τους νόμιμους πελάτες που εξυπηρετεί

Λέξεις κλειδιά: IoT δίκτυα, ασφάλεια, DDoS, θεωρία παιγνίων, DDoS

ABSTRACT

The purpose of this diploma thesis is to demonstrate the security gaps in the Internet of Things (IoT) using a Distributed Denial of Service Attack (DDoS). The development of the thesis summarizes the structure of DPA, general information as well as forms of attacks that threaten the IoT networks as they become more and more popular. The continuously rapid developed human need for immediate availability of real-time information has led the world of technology to the creation of a new form of networking that is implemented with the participation of interconnected devices, being able to collect and send information in real-time . The morphology and structure of these networks is very heterogeneous both for the entities and for the technologies involved. The general form of these networks is divided into two major categories. Closed / private IoT networks such as local / private networks, e.g. home, corporate, and open networks as defined by public broadband and coverage networks. The structure of these networks varies considerably, however they have the same logic and purpose of existence. Both previous categories consist of devices that interact in real-time by sending and receiving information. The potential benefits of IoT can be described as unlimited as well as its applications that can radically change the way we work and live.

The chapters below will initially analyze the general structure of IoT, and then describe and analyze in detail the gaps and the security issues involved in these networks. The work includes an experimental part that implements a DDoS attack in a virtual closed loop network environment.

The experimental part focuses on demonstrating the vulnerability of these networks to a particular form of attack which can be implemented in various ways and methods. Entities launching attacks are implemented using an object-oriented programming language. The client entities have the ability to send HTTPS network traffic to the server, The malicious client entities launch a simultaneous attack on the server; hence the server is not able to respond to the legitimate users.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

ΕΝΟΤΗΤΑ 1

1.1 Εισαγωγή

Η δομή της σημερινής πραγματικότητας δημιουργεί συνεχώς νέες ανάγκες. Η κάλυψη των συγκεκριμένων αναγκών έχει απαιτούμενες τεχνολογίες, όπως το IoT. Με τον όρο IoT περιγράφεται η πλήρης συνένωση και λειτουργικότητα δικτύων και οντοτήτων, τα οποία αλληλοεπιδρούν μεταξύ τους σε πραγματικό χρόνο, κάτω από ένα ευρύτερο και ενιαίο δίκτυο όπου παρέχει κάλυψη και επικοινωνία σε οποιοδήποτε χρόνο και οποιοδήποτε γεωγραφικό σημείο [44]. Η δυνατότητα διάθεσης πληροφοριών οποιαδήποτε στιγμή δίνει στον άνθρωπο τεράστιες δυνατότητες, όπως για παράδειγμα τη σωστή και έγκυρη πληροφόρηση για τις καιρικές συνθήκες και την κυκλοφοριακή κατάσταση στους δρόμους. Επίσης είναι ένα μεγάλο βήμα στην ανεξαρτητοποίηση των συσκευών, καθώς έτσι δίνεται στον άνθρωπο η δυνατότητα να συλλέγει δεδομένα σε πραγματικό χρόνο χωρίς τη βοήθεια του ανθρώπινου παράγοντα με αποτέλεσμα οι συσκευές αυτές να είναι σε θέση να παίρνουν αποφάσεις για τον άνθρωπο, όπως π.χ., ο ηλεκτρονικός εγκέφαλος του οχήματος να γνωρίζει σε ποιους δρόμους υπάρχει κυκλοφοριακή συμφόρηση και να οδηγεί τον επιβάτη στον προορισμό του από μία δευτερεύουσα διαδρομή.

Αν και όλα τα προαναφερθέντα πλεονεκτήματα δίνουν τεράστιες δυνατότητες, στην πράξη δημιουργούν διάφορα προβλήματα που προκύπτουν από την κακή και κακόβουλη χρήση της τεχνολογίας, δηλαδή προβλήματα ασφάλειας που ξεκινούν από την παραβίαση, κλοπή/μη εξουσιοδοτημένη τροποποίηση προσωπικών δεδομένων μέχρι και την καταστροφή μεγάλων συστημάτων, κλοπή τραπεζικών λογαριασμών, πρόσβαση σε στρατιωτικό/κρατικό εξοπλισμό/δεδομένα κλπ._Τα IoT δίκτυα δύναται να υπάρξουν σε διάφορους τομείς (αυτοκινητοβιομηχανία, ιατρικό τομέα, κλπ.) όπου σε κάθε τομέα αν και η ευρύτερη λογική-ιδέα είναι η ίδια, διαφέρουν ως προς τις απειλές που αντιμετωπίζουν, αλλά και ως προς τη δομή τους.

Ο όρος IoT είναι είναι σχετικά ένας νέος όρος στον κόσμο της τεχνολογίας καθώς είναι μόλις 16 ετών. Η πραγματική ιδέα όμως για συνδεδεμένες οντότητες εισάγεται για πρώτη φορά, στη δεκαετία του '70[1]. Την εποχή εκείνη, η ιδέα ονομζαόταν συχνά «ενσωματωμένο διαδίκτυο» ή «διάχυτο υπολογιστικό σύστημα»[1]. Ο πραγματικός όρος IoT σχεδιάστηκε από τον Kevin Ashton το 1999 κατά τη διάρκεια της εργασίας του στο Procter & Gamble. Ο Ashton, ο οποίος εργαζόταν στη βελτιστοποίηση της αλυσίδας εφοδιασμού, ήθελε να προσελκύσει την προσοχή της ανώτερης διοίκησης σε μία νέα τεχνολογία που ονομάζεται RFID. Επειδή το διαδίκτυο ήταν η νέα τάση το 1999, έτσι ονόμασε την παρουσίασή που θα έκανε για την καινούργια αυτή τεχνολογία IoT. Παρά το γεγονός ότι ο Kevin κέντρισε το ενδιαφέρον ορισμένων στελεχών της εταιρείας P & G, ο όρος IoT δεν έτυχε ευρείας προσοχής για τα επόμενα 10 χρόνια.

Η έννοια του IoT άρχισε να κερδίζει κάποια δημοτικότητα το καλοκαίρι του 2010.
Την ίδια χρονιά, η κινεζική κυβέρνηση ανακοίνωσε ότι θα κάνει το IoT στρατηγική προτεραιότητα σε πενταετές σχέδιο[44]. Το 2011, η εταιρεία έρευνας της αγοράς Gartner, η οποία εφηύρε το περίφημο «hype-cycle για αναδυόμενες τεχνολογίες», περιελάβανε ένα νέο αναδυόμενο φαινόμενο στη λίστα τους: IoT[44].

Την επόμενη χρονιά (2000) το θέμα του συνεδρίου LeWeb ήταν το IoT. Ταυτόχρονα, τα δημοφιλή περιοδικά τεχνολογίας όπως το Forbes, το Fast Company και το Wired αρχίζουν να χρησιμοποιούν τον όρο IoT για την περιγραφή του φαινομένου αυτού[1]. Τον Οκτώβριο του 2013, η IDC δημοσίευσε μία έκθεση που αναφέρει ότι το IoT θα είναι μία αγορά 8,9 τρισεκατομμυρίων δολαρίων το 2020[1]. Ο όρος IoT έκανε την παρουσία του αισθητή στις αγορές τον Ιανουάριο του 2014, όπου η Google ανακοίνωσε την αγορά του Nest για 3,2δις δολάρια[1]. Ο ορισμός που δίνει σήμερα η Παγκόσμία Ένωσης Τηλεπικοινωνιών(International Telecommunication Union), προσδιορίζει το IoT ως μία παγκόσμία υποδομή για την κοινωνία της πληροφορίας, επιτρέποντας την παροχή προηγμένων υπηρεσιών μέσω διασύνδεσης (φυσικών και εικονικών) αντικειμένων που βασίζονται σε υπάρχουσες και εξελισσόμενες διαλειτουργικές πληροφορίες και τεχνολογίες επικοινωνίας [2].

1.1.2 Περίληψη

Στις Ενότητες που ακολουθούν παρουσιάζεται συνοπτικά η δομή και ο τρόπος λειτουργίας του IoT καθώς και των στοιχείων που το συνθέτουν. Επίσης γίνεται αναφορά στις απειλές που αντιμετωπίζει, περιγραφή των βασικών μορφών επιθέσεων που το απειλούν όπως και πειραματική αναπαράσταση DDoS επίθεσης.

1.2 Κατάσταση Ασφαλείας στο IoT

Ένα από τα βασικά προβλήματα που αντιμετωπίζει προς το παρόν το IoT είναι η ασφάλεια. Είναι σημαντικό να αναφερθεί ότι ακόμη δεν έχει καθιερωθεί, ή πιο σωστά δεν έχει προτυποποιηθεί κάποιο πρότυπο που θα εφαρμόζεται και θα διασφαλίζει την ασφάλειά στα δίκτυα αυτά, παρά μόνο προτάσεις από την επιστημονική κοινότητα[3]. Η τεχνολογία IoT αντιμετωπίζει σοβαρά προβλήματα και κενά ασφαλείας τα οποία προέρχονται από διάφορα επίπεδα της υλοποίησης του. Ως κύρια προβλήματα ασφαλείας μπορούν να χαρακτηριστούν:

1. Η περιορισμένη επεξεργαστική δύναμη αρκετών από τις συμμετέχοντες οντότητες (π.χ. αισθητήρες, κινητές συσκευές). Σε μία τέτοιας μορφής δομή δικτύωσης, η συντριπτική πλειοψηφία των συμμετεχόντων οντοτήτων είναι δικτυακές συσκευές, αισθητήρες κλπ. Τέτοιας μορφής συσκευές έχουν περιορισμένη επεξεργαστική δύναμη με αποτέλεσμα οι αμυντικές τους ικανότητες τους να είναι από υποβαθμισμένες.

2. Η περιορισμένη χωρητική δύναμη των συσκευών. Όσον αφορά τις πιο μεγάλες συσκευές προφανώς θα χρησιμοποιηθούν άλλες μορφές τεχνικών επίθεσης. Μία μεγάλη συσκευή ή καλύτερα ένα δυνατό σύστημα έχει επεξεργαστική δύναμη ικανή να χρησιμοποιήσει σύνθετους μηχανισμούς κρυπτογράφησης, έχει δυνατό firewall, καθώς και ανθρώπινο δυναμικό για την επίβλεψη του. Για τους λόγους αυτούς χρησιμοποιούνται άλλες μορφές επιθέσεων όπου έχουν ως αποτέλεσμα την άρνηση παροχής υπηρεσιών. Όσο μεγάλη και να είναι η χωρητικότητα της μνήμης ενός συστήματος και η επεξεργαστική δύναμη που διαθέτει, δεν παύουν η δύναμη αυτή και η χωρητικότητα να είναι συγκεκριμένου μεγέθους.
3. Κενά ασφαλείας στα υπάρχοντα πρωτόκολλα
   Αρκετά από τα πρωτόκολλα που χρησιμοποιούνται σήμερα έχουν σχεδιαστεί σε πιο παλιές δεκαετίες και έχουν κατά καιρούς προσβληθεί από διάφορους κακόβουλους χρήστες. Αν και η χρήση τους είναι αναγκαία και σημαντική, η ανάγκη για εξεύρεση πιο σύγχρονων πρωτοκόλλων είναι επιτακτική. Τα νέα πρωτόκολλα, θα πρέπει να είναι πιο δυναμικά και πιο έξυπνα με την έννοια ότι θα πρέπει να έχουν τη δυνατότητα να προσαρμόζονται στα περιβάλλοντα στα οποία ενεργούν και στις απειλές που αντιμετωπίζουν.

ΕΝΟΤΗΤΑ 2

2.1 Επιθέσεις Άρνησης Παροχής Υπηρεσιών

Ο όρος DoS χρησιμοποιείται για να περιγραφεί η επίθεση η οποία έχει ως σκοπό να εντοπίσει ή να αποτρέψει τη χρήση συστημάτων, δικτύων ή εφαρμογών με την εξάντληση των πόρων τους όπως η μνήμη, μονάδες επεξεργασίας, εύρος ζώνης του δικτύου ή/και αποθηκευτικού χώρου. Οι διάφορες επιθέσεις αν και ακολουθούν την ίδια λογική, δηλαδή την εξάντληση των πόρων του επεξεργαστή και του δικτύου με στόχο την άρνηση παροχής υπηρεσιών, διαφέρουν ως προς τις μορφές τους, αναλόγως του τρόπου με τον οποίο εκτελούνται και της εφαρμογής που θέτουν ως στόχο. Στη συνέχεια θα παρουσιαστούν μερικές από τις πιο βασικές κατηγορίες επιθέσεις που έχουν ως αποτέλεσμα την άρνηση παροχής υπηρεσιών.

2.2 Βασικές Επιθέσεις Άρνησης Εξυπηρέτησης

2.2.1 Επίθεση στο εύρος ζώνης του δικτύου

Στοχεύοντας το εύρος ζώνης ενός δικτύου, εξαντλείται η διαθεσιμότητα των διαδικτυακών συνδέσμων που συνδέουν τον εξυπηρετητή με ένα δίκτυο[43]. Βάσει της φύσης των δικτύων, σε περίπτωση μίας υπερφορτωμένης TCP/IP δικτυακής σύνδεσης μία μεγάλη μερίδα χρηστών, τυχαιοκρατικά επιλεγμένη, θα έρθει αντιμέτωπη με υποβαθμισμένης ποιότητας παροχή υπηρεσιών ή και καθόλου παροχή. Από την πλευρά του επιτιθέμενου αυτό επιτυγχάνεται με την αποστολή δικτυακού φόρτου, ο οποίος κατά ένα μεγάλο ποσοστό αποτελείται από κακόβουλα δικτυακά πακέτα, τα οποία αποστέλλονται άμεσα από τον επιτιθέμενο ή μέσω άλλων δικτυακών μονάδων που διαχειρίζεται ο επιτιθέμενος. Πιο συγκεκριμένα σε μία τέτοια επίθεση, ο επιτιθέμενος στέλνει ένα μεγάλο αριθμό πακέτων έτσι ώστε να καταναλώσει το περιορισμένο εύρος ζώνης ή να εξαντλήσει τους πόρους του δικτύου του θύματος. Οι πόροι δικτύου όπως οι

δρομολογητές, οι διακομιστές και τα τείχη προστασίας έχουν περιορισμένη χωρητικότητα. Όταν δέχονται επίθεση και υπερφορτωθούν, οι τελικοί χρήστες δεν θα μπορέσουν να περάσουν, επειδή δεν υπάρχει εύρος ζώνης για να χρησιμοποιήσουν τα δίκτυα υποδομής. Η πιο κοινή επίθεση είναι η πλημμύρα. Σε αυτήν την επίθεση, ένα μεγάλο ποσό πακέτων TCP, UDP και ICMP που φαίνονται νόμιμα αποστέλλονται στον κεντρικό υπολογιστή-στόχο (συνήθως με πλαστά IP) από μεγάλο αριθμό υπολογιστών (bots). Οι πλημμύρες TCP-, SYN-, ACK-All εμπίπτουν στην κατηγορία αυτή. Για παράδειγμα, οι επιθέσεις SYN-Flood αποστέλλουν μεγάλο αριθμό πακέτων αίτησης TCP SYN με παραμορφωμένες διευθύνσεις IP προέλευσης. Ο στοχευμένος εξυπηρετητής καταλήγει σε μία πολύ μεγάλη λίστα μισάνοικτων συνδέσεων (το αίτημα για ολοκλήρωση παραμένει ανοιχτό), το οποίο καταναλώνει πόρους και καθιστά πιο δύσκολο για τους κανονικούς χρήστες να συνδεθούν στο τελικό σύστημα.

Είναι σημαντικό να αναφερθεί ότι η συχνότητα αποστολής και το μέγεθος των πακέτων που χρειάζονται σε κάθε επίθεση είναι ανάλογη των δυνατοτήτων του εξυπηρετητή.

2.2.2 Επίθεση στους πόρους του υλικού του συστήματος

Δεύτερη κατηγορία, ορίζεται η κατηγορία των επιθέσεων οι οποίες έχουν σαν στόχο, τους πόρους του υλικού του δικτύου, κάτι που οδηγεί στο ίδιο αποτέλεσμα, όπως και στην προηγούμενη κατηγορία[40]. Για το συγκεκριμένο στόχο, τα πακέτα που αποστέλλονται καταναλώνουν τους επεξεργαστικούς και τους χωρικούς πόρους του συστήματος. Αυτό περιλαμβάνει, προσωρινές ουρές, οι οποίες κρατούν σε αναμονή τα πακέτα που καταφθάνουν και δεν μπορούν να τα διαχειριστούν τη δεδομένη στιγμή.
Οι πόροι ενός δικτύου περιλαμβάνει το εύρος ζώνης, τη μνήμη,το χώρο στο δίσκο, χρόνο CPU κ.λπ. Οι επιτιθέμενοι, στοχεύουν σε αυτούς τους πόρους και εμποδίζουν τους χρήστες που έχουν πρόσβαση σε αυτές. Για παράδειγμα, στην επίθεση δικτύου "SYN flood", ο εισβολέας προσπαθεί να δημιουργήσει μία σύνδεση με το μηχάνημα του θύματος και καταναλώνει υπερβολικά τις δομές δεδομένων του πυρήνα, οι οποίες αποτελούν ζωτικής σημασίας πόρο για τη δημιουργία συνδέσεων δικτύου. Οι εισβολείς μπορούν επίσης να καταναλώσουν το εύρος ζώνης του δικτύου. Αυτό γίνεται επιτυγχάνεται με τη δημιουργία ενός μεγάλου αριθμού πακέτων δεδομένων που μεταφέρονται στο δίκτυό του θύματος.

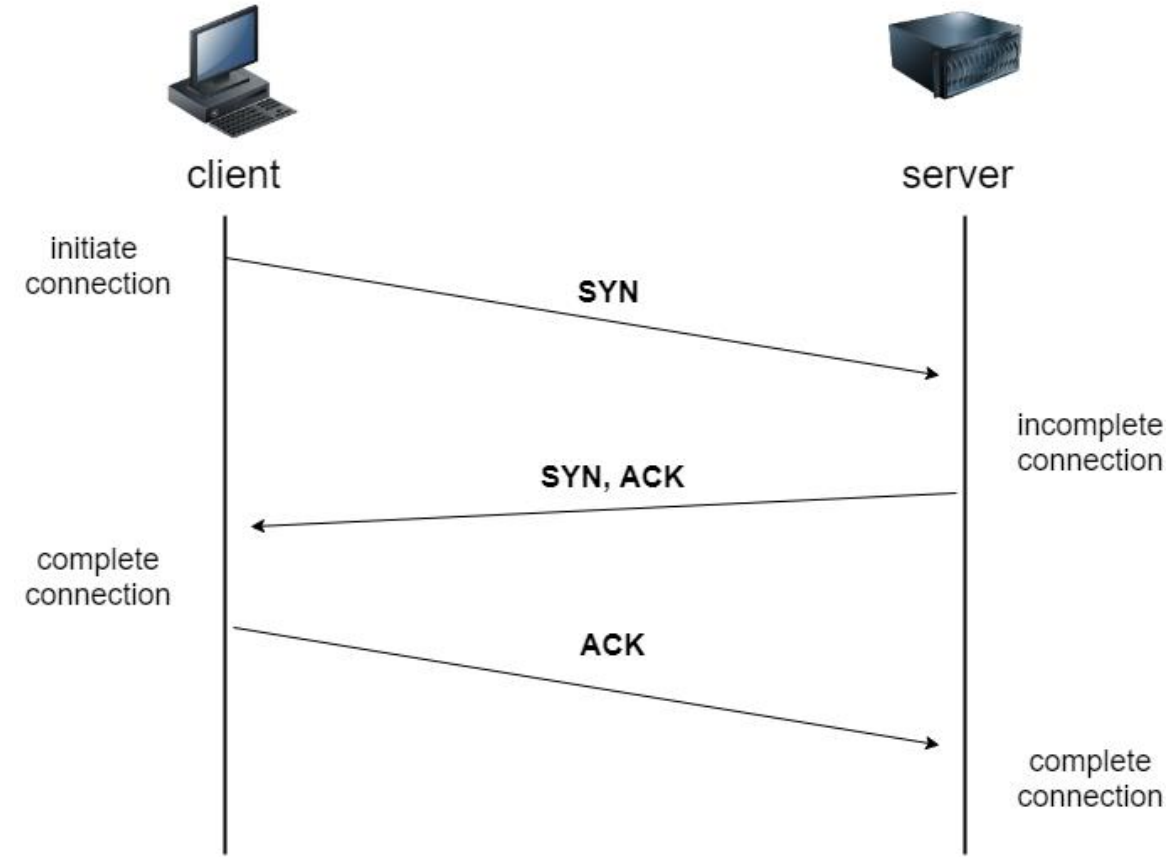
Εκτός από το εύρος ζώνης του δικτύου, οι επιτιθέμενοι μπορούν επίσης να καταναλώσουν πολλούς άλλους κρίσιμους πόρους. Ορισμένα από τα συστήματα διαθέτουν πολύ περιορισμένο αριθμό δομών δεδομένων που διατίθενται για τη διατήρηση πληροφοριών. Οι επιτιθέμενοι ενδέχεται να δημιουργήσουν έναν συγκεκριμένου τύπου κώδικα, που έχει δυνατότητα να πολλαπλασιάσει το μέγεθος των δεδομένων δημιουργώντας πολλαπλά αντίγραφα όλων των δεδομένων που είναι αποθηκευμένα σε μία δομή δεδομένων. Με αυτό το τρόπο, καταναλώνεται ι όλος ο ελεύθερος αποθηκευτικός χώρος που είναι ήδη περιορισμένος με αποτέλεσμα να δημιουργηθεί πρόβλημα στη λειτουργία του συστήματος. Η βάση δεν μπορεί να αποθηκεύσει νέα δεδομένα, κατ επέκταση το σύστημα δεν μπορεί να προσφέρει υπηρεσίες στους χρήστες του.

2.2.3 Επίθεση στους πόρους των εφαρμογών του συστήματος

Η τρίτη κατηγορία επιθέσεων DoS είναι αυτή των εφαρμογών[44]. Για παράδειγμα, η δυνατότητα ενός δικτυακού εξυπηρετητή να εκτελεί ερωτήματα σε μία βάση δεδομένων είναι μία εφαρμογή. Το κάθε ερώτημα προφανώς καταναλώνει ένα ποσοστό από τους πόρους του εξυπηρετητή. Ο επιτιθέμενος, αποστέλλει ένα αριθμό ερωτημάτων προς τον εξυπηρετητή με αποτέλεσμα αρχικά την αδυναμία του εξυπηρετητή να επεξεργαστεί ερωτήματα από διαφορετικές πηγές, προκαλώντας κατά αυτόν τον τρόπο την παροχή χαμηλής ποιότητας υπηρεσιών προς τους υπόλοιπους χρήστες. Η συνεχιζόμενη αποστολή πακέτων φέρει ως αποτέλεσμα την ολική εξάντληση των πόρων του χρήστη και την αδυναμία παροχής υπηρεσιών.
Οι επιθέσεις αυτές καθίστανται βραχύτερες σε διάρκεια αλλά αυξάνονται σε συχνότητα, πολυπλοκότητα και επιμονή. Αυτό σημαίνει ότι οι επιτιθέμενοι στοχεύουν έναν διακομιστή ιστού ή έναν διακομιστή εφαρμογών και τον πλημμυρίζουν με αρκετή επισκεψιμότητα για να το φέρουν εκτός σύνδεσης. Εξαιτίας αυτού, οι επιθέσεις στο στρώμα εφαρμογών είναι λιγότερο δαπανηρές για τους επιτιθέμενους αφού δεν χρειάζονται συστήματα με μεγάλες δυνατότητες για να εξαπολύσουν μίας τέτοιας μορφής επίθεση όπως επίσης δεν χρειάζεται η χρήση πολύπλοκων τεχνικών για να επιτεθούν. Ακόμη μία παράμετρος είναι ότι οι επιθέσεις αυτές, θεωρούνται πιο δύσκολες ως προς την αντιμετώπιση τους από τον αμυνόμενο σε σύγκριση με τις επιθέσεις που στοχεύουν στο επίπεδο του δικτύου. μία τέτοια επίθεση είναι η επίθεση με πακέτα HTTP.

2.2.4 Επίθεση πλημμύρας SYN

Στα TCP/IP δίκτυα η διαδικασία εγκαθίδρυσης μίας σύνδεσης μεταξύ ενός πελάτη και ενός εξυπηρετητή ονομάζεται χειραψία τριών κατευθύνσεων. Όπως διαφαίνεται και στο σχήμα (b) , αρχικά ο πελάτης αποστέλλει ένα πακέτο SYN προς τον εξυπηρετητή, αυτός με τη σειρά του απαντάει με ένα πακέτο SYN-ACK και ο πελάτης επιβεβαιώνει την παραλαβή του πακέτου με ένα πακέτο ACK. Αν ο πελάτης δεν παραλάβει αμέσως το επιθυμητό πακέτο θα πρέπει να περιμένει ένα συγκεκριμένο χρονικό διάστημα μέχρι την αποστολή του επόμενου. Σε μία DoS επίθεση με SYN πακέτα, ο πελάτης όπου σε αυτή την περίπτωση θα είναι ο επιτιθέμενος, αποστέλλει συνεχώς πακέτα SYN χωρίς να περιμένει για την ανάλογη ανταπόκριση από τον εξυπηρετητή με σκοπό να υπερχειλίσει τους πίνακες καταχώρησης του εξυπηρετητή.



σχήμα a Διαδικασία εγκαθίδρυσης επικοινωνίας με τη τεχνική χειραψίας τριών κατευθύνσεων

2.3 Επιθέσεις πλημμύρας

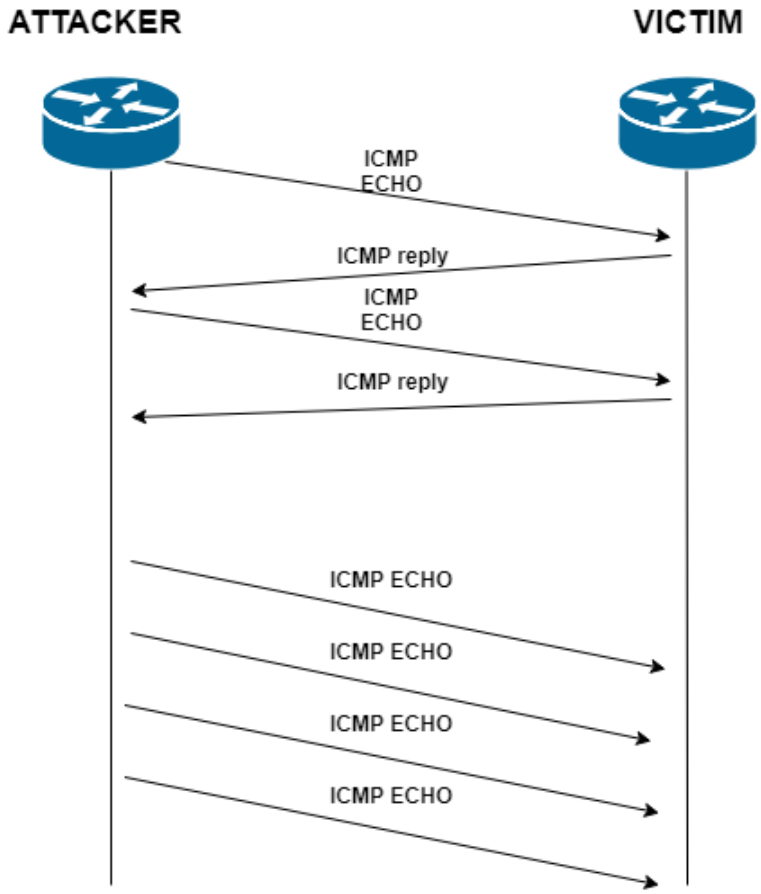
Οι επιθέσεις πλημμύρας διαφοροποιούνται αναλόγως με το ποιο πρωτόκολλο χρησιμοποιείται στην επίθεση[47]. Σε όλες τις περιπτώσεις επιθέσεων ο στόχος είναι η υπερχείλιση της δικτυακής χωρητικότητας του εξυπηρετητή ή και υπερφόρτωσης του εξυπηρετητή έτσι ώστε να μην μπορεί να εξυπηρετήσει το φόρτο που καταφθάνει. Τα πρωτόκολλα που χρησιμοποιούνται συνήθως στις επιθέσεις αυτές είναι τα ICMP, UDP,TCP SYN, SIP, HTTP κλπ.

2.3.1 Επιθέσεις Πλημμύρας ICMP

Το ICMP είναι ένα πρωτόκολλο υποστήριξης της επικοινωνίας στο δίκτυο[48]. Χρησιμοποιείται από συσκευές δικτύου, συμπεριλαμβανομένων και των δρομολογητών, για την αποστολή μηνυμάτων σφάλματος και λειτουργικών πληροφοριών που υποδεικνύουν, για παράδειγμα, ότι μία ζητούμενη υπηρεσία δεν είναι διαθέσιμη ή ότι δεν είναι δυνατή η πρόσβαση σε έναν κεντρικό υπολογιστή ή έναν δρομολογητή. Το ICMP διαφέρει από τα πρωτόκολλα μεταφοράς, όπως τα TCP και UDP, επειδή δεν χρησιμοποιείται συνήθως για την ανταλλαγή

δεδομένων μεταξύ συστημάτων, ούτε χρησιμοποιείται συχνά από εφαρμογές δικτύου τελικού χρήστη.

Κατά την επίθεση αυτή ο επιτιθέμενος συντρίβει το θύμα με πακέτα ICMP "αιτήματος echo" όπως διαφαίνεται στο σχήμα (c). Αυτό είναι πιο αποτελεσματικό χρησιμοποιώντας την επιλογή πλημμυρών ping που στέλνει τα πακέτα ICMP όσο πιο γρήγορα γίνεται χωρίς να περιμένουν απαντήσεις. Οι περισσότερες εφαρμογές του ping απαιτούν από τον χρήστη να είναι προνομιούχος προκειμένου να καθορίσει την επιλογή πλημμυρών. Είναι πιο επιτυχημένη αν ο επιτιθέμενος έχει μεγαλύτερο εύρος ζώνης από το θύμα. Ο επιτιθέμενος ελπίζει ότι το θύμα θα ανταποκριθεί με τα πακέτα ICMP "echo reply", καταναλώνοντας έτσι τόσο το εξερχόμενο εύρος ζώνης.



σχήμα b Επίθεση υπερχείλισης με χρήση ICMP echo πακέτα

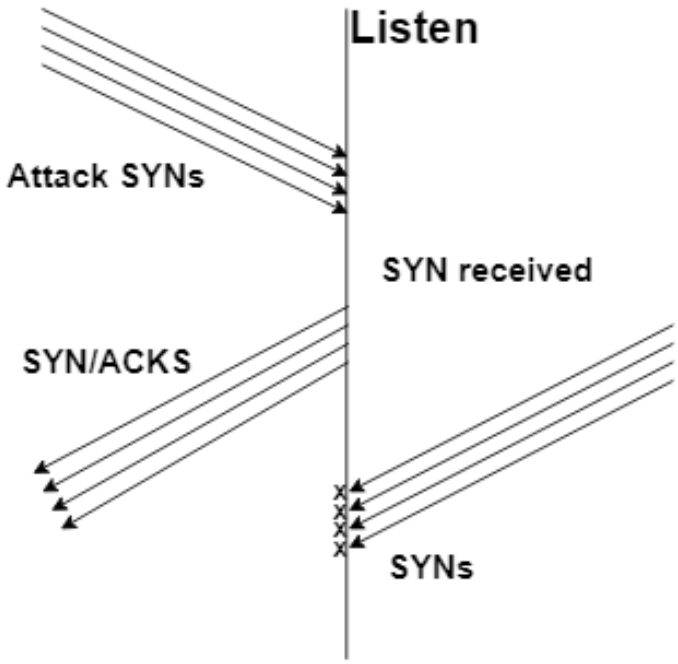
2.3.2 Επιθέσεις Πλημμύρας UDP

Η επίθεση πλημμύρας UDP υπάγεται κι αυτή στην κατηγορία των επιθέσεων πλημμύρας[50]. Εδώ ο επιτιθέμενος ξεκινά μία επίθεση DoS εκδίδοντας μία εντολή επίθεσης προς τα κύρια προγράμματα ελέγχου του τα οποία χρησιμεύουν ως οι επιτιθέμενες οντότητες. Η εντολή αυτή περιέχει στοιχεία όπως τη διεύθυνση του θύματος, τη διάρκεια ζωής του πακέτου, τις μεθόδους επίθεσης κλπ. Οι επιτιθέμενες οντότητες έπειτα εξαπολύουν την επίθεση προς το θύμα στέλνοντας πακέτα UDP προς το θύμα με μία πλαστογραφημένη IP ως διεύθυνση πηγής. Το θύμα κατά τη λήψη αυτών των πακέτων, στέλνει την επιβεβαίωση στην διεύθυνση IP της πηγής, αλλά δεν λαμβάνει καμία απάντηση με τη σειρά του και

συνεχίζει να περιμένει. Τελικά όταν το θύμα εγκαταλείπει την επικοινωνία, όλοι του οι πόροι έχουν καταναλωθεί οδηγώντας το σύστημα σε συντριβή. Οι επιτιθέμενες οντότητες πολλές φορές, έχουν υπό τον έλεγχο τους κι άλλες δικτυακές οντότητες οι οποίες μπορούν να αποστείλουν δικτυακή κίνηση προς το θύμα κάτι το οποίο αυξάνει το μέγεθος της επίθεσης. Αυτό εξασφαλίζει την πλημμύρα του συστήματος καταναλώνοντας όλο το εύρος ζώνης και άλλους πόρους του συστήματος. Στην επίθεση DoS, ακολουθείται ακριβώς η ίδια λογική και τεχνική με διαφορά όμως οτι ο επιτιθέμενος εξαπολύει την επίθεση του απευθείας προς το θύμα χωρίς τη χρήση ενδιάμεσων συστημάτων.

2.3.3 Επιθέσεις Πλημμύρας TCP SYN

Μία ακόμη εναλλακτική μέθοδος για την υλοποίηση επίθεσης πλημμύρας είναι αυτή της χρήσης πακέτων πρωτοκόλλου[46]. Συνήθως, τα πακέτα αυτά θα είναι TCP SYN, δηλαδή πακέτα αίτησης σύνδεσης. Ο στόχος της επίθεσης αυτής παρομοίως και με των υπολοίπων επιθέσεων ίδιου τύπου είναι η αποστολή μεγάλου αριθμού πακέτων με σκοπό την υπερχείλιση του δικτύου και τη δέσμευση επεξεργαστικών πόρων από τον επεξεργαστή. Στο σχήμα (c) διαφαίνεται η διαδικασία της επίθεσης.

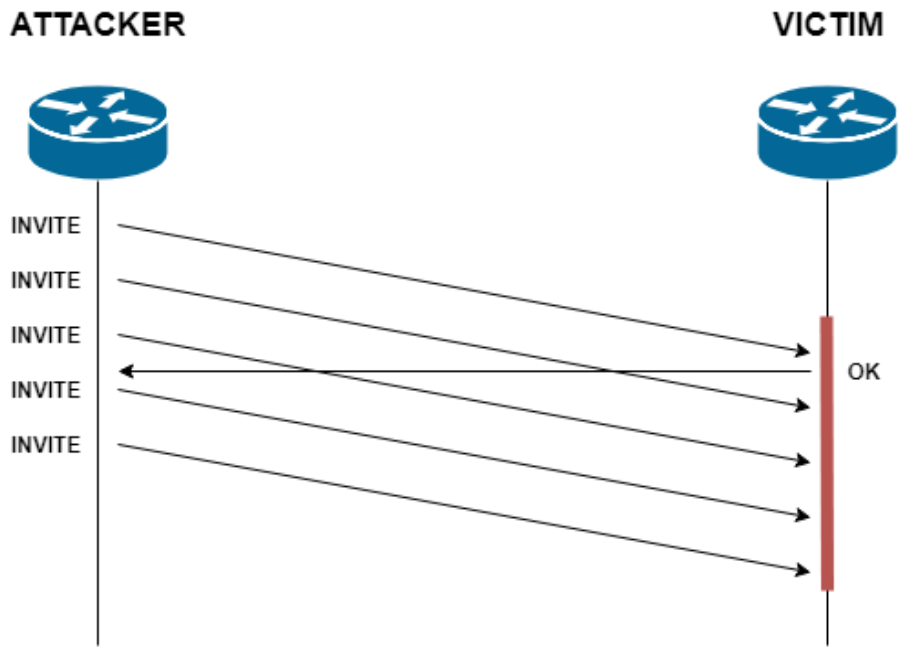


σχήμα c Διαδικασία επίθεσης υπερχείλισης με TCP SYN πακέτα

2.3.4 Επιθέσεις Πλημμύρας SIP

Το πρωτόκολλο SIP είναι το βασικό πρωτόκολλο που χρησιμοποιείται για την υλοποίηση οποιασδήποτε VoIP εφαρμογής. Το πρωτόκολλο αυτό, είναι ένα αρκετά απλό πρωτόκολλο, το οποίο έχει παρόμοια σύνταξη με το HTTP πρωτόκολλο. Οι δύο κατηγορίες μηνυμάτων που χρησιμοποιεί το SIP είναι αυτές της πρόσκλησης(INVITE) και της απάντησης(RESPONSE). Το INVITE είναι συγκεκριμένο πακέτο πρόσκλησης όπως αυτό καθορίζεται από το RFC 3261 το

οποίο διαφέρει στις λεπτομέρειες του είδους της επαφής που θα αποστείλει ο αποστολέας, ενώ για την απάντηση υπάρχουν αρκετά πακέτα τα οποία αποστέλλονται αναλόγως του τρόπου αντίδρασης του εξυπηρετητή ή της SIP οντότητας που λαμβάνει την πρόσκληση[51]. Ο επιτιθέμενος, μπορεί να επιτύχει το στόχο του χρησιμοποιώντας μόνο πακέτα πρόσκλησης. Η συνεχής αποστολή πακέτων πρόσκλησης προς τον στόχο, αρχικά θα εξαντλήσει την επεξεργαστική δύναμη της εφαρμογής που δέχεται τα μηνύματα με αποτέλεσμα να συντριβεί, ενώ ταυτόχρονα θα επιφέρει μεγάλο επεξεργαστικό φόρτο και στον επεξεργαστή στον οποίο είναι εγκατεστημένη η εφαρμογή. Αν τα πακέτα πρόσκλησης είναι έγκυρα τότε ο εξυπηρετητής θα απαντήσει με πακέτα ανάλογα για τη συνέχιση της διαδικασίας εγκαθίδρυσης της κλήσης (200 OK, 407 Proxy Authentication κλπ). Αν τα πακέτα αυτά δεν είναι έγκυρα, τότε ο εξυπηρετητής θα απαντήσει με πακέτα που θα τερματίζουν τη διαδικασία (404 error code, 504 bad gateway κλπ). Και στις δύο περιπτώσεις ο επιτιθέμενος θα έχει καταφέρει την εξάντληση των επεξεργαστικών και δικτυακών πόρων του εξυπηρετητή ή της SIP οντότητας.Στο πιο κάτω σχήμα αναπαρίσταται η διαδικασία αποστολής INVITE πακέτων.



σχήμα d Επίθεση πλημμύρας με βάση το πρωτόκολλο HTTP

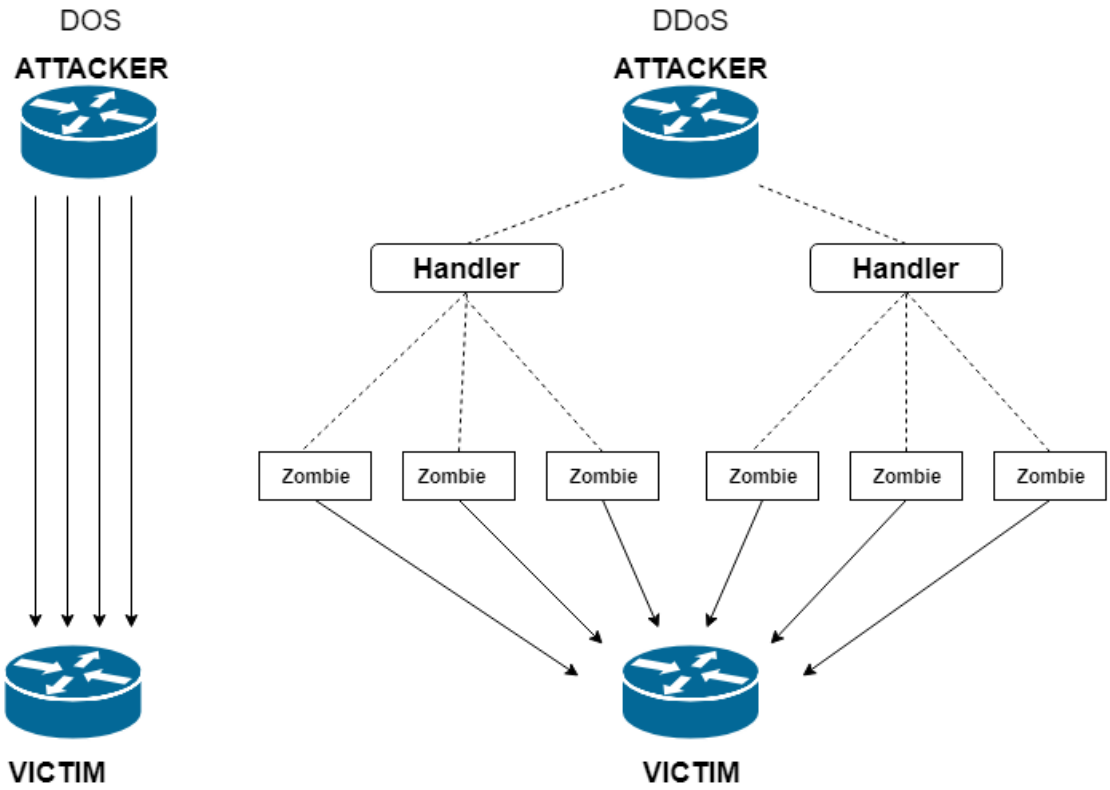
2.3.5 Επιθέσεις με βάση το πρωτόκολλο HTTP

Σε μία επίθεση πλημμύρας πρωτοκόλλου HTTP, ο επιτιθέμενος βομβαρδίζει τον εξυπηρετητή με HTTP πακέτα αιτήσεων[52]. Ένα πακέτο αίτησης του πρωτοκόλλου HTTP μπορεί να φέρει διαφορετικής μορφής αίτησης όπως για παράδειγμα, αίτηση σύνδεσης-επικοινωνίας με τον εξυπηρετητή, αίτηση για απόκτηση ενός μεγάλου αρχείου κλπ. Αυτές οι διαδικασίες, αναλόγως του μεγέθους και της ποσότητας τους επιφέρουν την αδυναμία του στόχου να εξυπηρετήσει άλλες υπηρεσίες και εν τέλει στην άρνηση παροχής υπηρεσιών. Όπως διαφαίνεται στη σχηματική αναπαράσταση στο σχήμα (d), ο επιτιθέμενος αποστέλλει πολλαπλά πακέτα ατήματος αίτησης σύνδεσης με το θύμα χωρίς όμως να περιμένει απάντηση για καθένα από τα αιτήματα αυτά. Το θύμα στην προσπάθεια του να τα επεξεργαστεί, χρησιμοποιεί όλους του τους διατιθέμενους πόρους παρόλα αυτά λόγω ότι τα πακέτα είναι συνεχόμενα είναι αδύνατον να

ανταπεξέλθει στις επαρκώς σε όλες τις αιτήσεις να εξυπηρετήσει άλλους πελάτες. Η επίθεση θεωρείται επιτυχής, όταν το θύμα δεν μπορεί να εξυπηρετήσει άλλους πελάτες όπως επίσης όταν σταματήσει να εξυπηρετεί και τους ήδη συνδεδεμένους χρήστες.

2.4 Επιθέσεις Κατανεμημένης Άρνησης Παροχής Υπηρεσιών

Η κατηγορία αυτή παρουσιάζει μία ιδιαιτερότητα σε σύγκριση με τις υπόλοιπες, καθώς αυτό που τη διαφοροποιεί δεν είναι στο που συγκεκριμένα στοχεύει (επεξεργαστικούς πόρους, εύρος ζώνης κλπ.) ή ποια τεχνική επίθεσης χρησιμοποιεί, αλλά στον τρόπο με τον οποίο διεξάγεται η επίθεση κάτι που την κάνει να διαφέρει από την επίθεση DoS όπως διαφαίνεται η σύγκριση τους στο σχήμα (e). Αναγνωρίζοντας τις αδυναμίες των επιθέσεων που διεξάγονται από ένα σύστημα, η κατηγορία αυτή έχει σαν χαρακτηριστικό τη διεξαγωγή επιθέσεων από πολλαπλά συστήματα ταυτόχρονα με τη χρήση συμβιβασμένων συσκευών και λοιπών δικτυακών οντοτήτων. Ο επιτιθέμενος φροντίζει με διάφορους μεθόδους, να αποκτήσει τον έλεγχο των οντοτήτων αυτών με άγνοια των χρηστών τους, με σκοπό τη χρησιμοποίηση τους για αποστολή δικτυακού φόρτου προς ένα στόχο κατά τη διάρκεια μίας επίθεσης. Η χρήση και ο έλεγχος των οντοτήτων αυτών χωρίζεται σε μία ιεραρχική δομή, έτσι ώστε να μην χρειάζεται συνεχής επίβλεψη όλων των οντοτήτων. Πιο συγκεκριμένα, ο επιτιθέμενος χρησιμοποιεί ένα μικρό αριθμό συστημάτων τα οποία δρουν σαν χειριστές των υπολοίπων. Έτσι, με την αποστολή μερικών εντολών προς τους χειριστές, ο επιτιθέμενος μπορεί να ελέγξει όλες τις οντότητες που έχει στην κατοχή του.



σχήμα e Εικονική απεικόνιση της δομής DoS και DDoS επιθέσεων

Ένα από τα πρώτα και πιο γνωστά εργαλεία για την επίτευξη DDoS επιθέσεων είναι το TFN. Η αρχική μορφή του εργαλείου στόχευε Sun Solaris συστήματα, μετέπειτα όμως γράφτηκε ξανά και μετονομάστηκε σε TFN2K. Στη νέα του μορφή μπορούσε να τρέχει και για UNIX, Solaris και Window NT συστήματα. Ο πράκτορας δηλαδή η οντότητα που δρούσε με σκοπό την υλοποίηση της επίθεσης στο εργαλείο ήταν ένα κακόβουλο λογισμικό, το οποίο αντιγραφόταν και έτρεχε σε ένα, ζόμπι σύστημα. Ήταν ικανό να πραγματοποιεί επιθέσεις πλημμύρας ICMP, UDP, SYN όπως επίσης επιθέσεις ενίσχυσης ICMP. Το λογισμικό αυτό βασιζόταν στο μεγάλο αριθμό συμβιβασμένων συστημάτων, και τις εντολές δομής επιπέδων έτσι ώστε να βρίσκει τη "διαδρομή" που οδηγούσε πίσω προς τον επιτιθέμενο. Σε γενικές γραμμές, η επίθεση υλοποιούταν με απλές εντολές τις οποίες χρησιμοποιούσε ο χειριστής στα συμβιβασμένα συστήματα. Ο επιτιθέμενος αποκτούσε πρόσβαση στα συστήματα αυτά χρησιμοποιώντας οποιοδήποτε μηχανισμό μπορούσε να του παρέχει πρόσβαση σε τερματικό έτσι ώστε να μπορεί να τρέξει το πρόγραμμα χειριστή με τις επιθυμητές επιλογές. Ο κάθε χειριστής, είχε τη δυνατότητα να ελέγχει ένα μεγάλο αριθμό συστημάτων πρακτόρων χρησιμοποιώντας μία λίστα ταυτοποίησης.

Η επικοινωνία μεταξύ του χειριστή και των πρακτόρων ήταν κρυπτογραφημένη και μπορούσε να αναμιχθεί με αριθμό ψεύτικων πακέτων κάτι το οποίο έκανε ακόμη πιο δύσκολη τη διαδικασία της επίβλεψης και ανάλυσης της δικτυακής κίνησης. Αξίζει να σημειωθεί ότι και οι επικοινωνίες μεταξύ χειριστή και πρακτόρων, όπως και οι επιθέσεις μπορούσαν να υλοποιηθούν με την αποστολή τυχαίων TCP, UDP και ICMP πακέτων. Έκτοτε έχουν υλοποιηθεί πολλά άλλα εργαλεία DDoS επίθεσης όπως τα Torshammer, Windows_DNS_Attack_Tool, GoodBye κ.α. τα οποία χρησιμοποιούν ακόμη πιο ανεπτυγμένες τακτικές και πληθώρα άλλων πρωτοκόλλων για την εκτέλεση των επιθέσεων τους [53].

2.5 Επιθέσεις αντανάκλασης και ενίσχυσης

Σε αντίθεση με τις DDoS επιθέσεις, όπου οι ενδιάμεσες οντότητες ήταν συμβιβασμένες συσκευές οι οποίες τυγχάνουν διαχείρισης από τον επιτιθέμενο, οι επιθέσεις ανάκλασης και ενίσχυσης χρησιμοποιούν τις φυσιολογικές λειτουργίες δικτυακών συστημάτων.

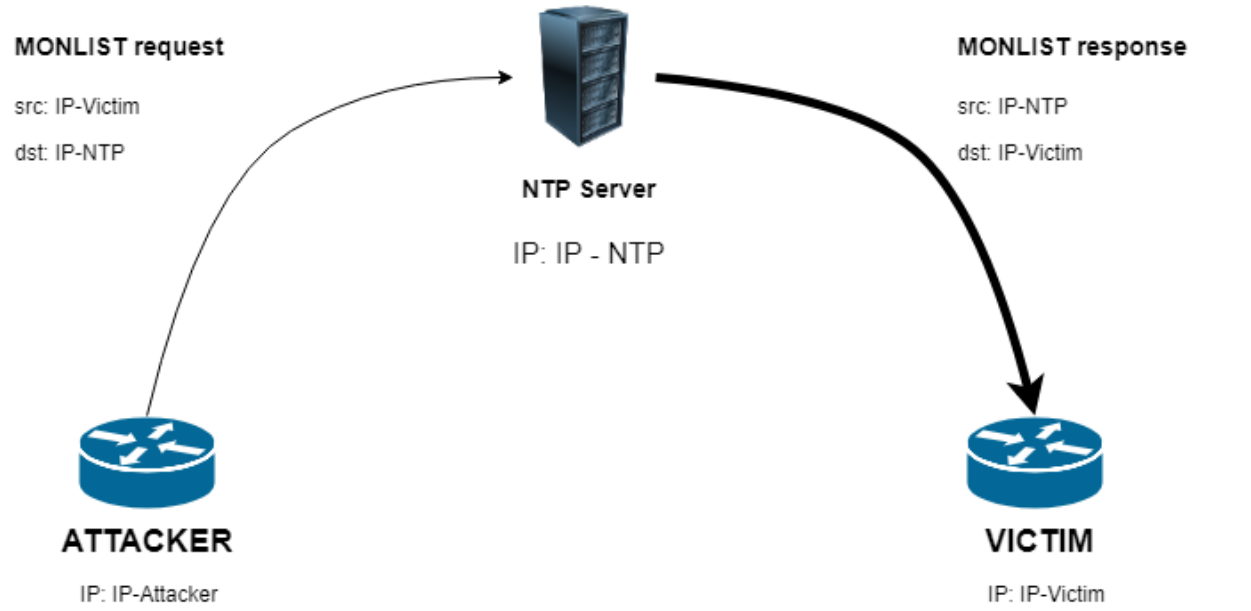
Ο επιτιθέμενος αποστέλλει ένα δικτυακό πακέτο σε μία υπηρεσία που τρέχει σε έναν οποιοδήποτε εξυπηρετητή χρησιμοποιώντας σαν πηγαία διεύθυνση τη διεύθυνση του θύματος. Έπειτα, ο εξυπηρετητής ανταποκρίνεται αποστέλλοντας ένα δικτυακό πακέτο στη ψεύτικη διεύθυνση απ' όπου ήρθε αρχικά το πακέτο. Η πραγματοποίηση της διαδικασίας αυτής προς ένα αριθμό τυχαίων εξυπηρετητών, θα δημιουργήσει μία πλημμύρα από δικτυακά πακέτα ανταπόκρισης προς τον εξυπηρετητή θύμα με αποτέλεσμα την αποδυνάμωση του εξυπηρετητή και την άρνηση παροχής υπηρεσιών. Το γεγονός ότι σε αυτές τις μορφές επιθέσεων χρησιμοποιούνται δικτυακά συστήματα χωρίς την ανάγκη παρεμβολής στη λειτουργία τους κάνει τον εντοπισμό του επιτιθέμενου ακόμη πιο δύσκολο. Επίσης, λόγω του ότι για την επίθεση χρησιμοποιούνται οι φυσιολογικές λειτουργίες ενός συστήματος κάνει την επίθεση πολύ πιο απλή.

2.5.1 Επιθέσεις ανάκλασης

Οι επιθέσεις ανάκλασης είναι μία πανομοιότυπη τεχνική επίθεσης όπως αυτή περιγράφηκε στο σχήμα (f) αφού στις επιθέσεις αυτές χρησιμοποιούνται φυσιολογικές λειτουργίες τυχαία επιλεγμένων εξυπηρετητών με σκοπό τη δρομολόγηση δικτυακής κίνησης πακέτων ανταπόκρισης από τους εξυπηρετητές που δέχτηκαν πακέτα αίτησης προς τον εξυπηρετητή θύμα

με αποτέλεσμα την πλημμύρα και την άρνηση παροχής υπηρεσιών.

Κατά τεχνική αυτή, ο επιτιθέμενος θα προσπαθήσει να χρησιμοποιήσει μία υπηρεσία η οποία θα δημιουργήσει ένα πακέτο ανταπόκρισης πολύ μεγαλύτερο από αυτό της αίτησης, καθώς αυτό θα δημιουργήσει μία πολύ μεγαλύτερη κίνηση από το ενδιάμεσο σύστημα προς το στόχο απ' ότι αυτή από το σύστημα του επιτιθέμενου προ το ενδιάμεσο σύστημα. Για τις επιθέσεις αυτές μπορεί να χρησιμοποιηθεί οποιαδήποτε αποδεκτή TCP ή UDP υπηρεσία.



σχήμα f Επίθεση Ανάκλασης

2.5.2 Επιθέσεις ενίσχυσης

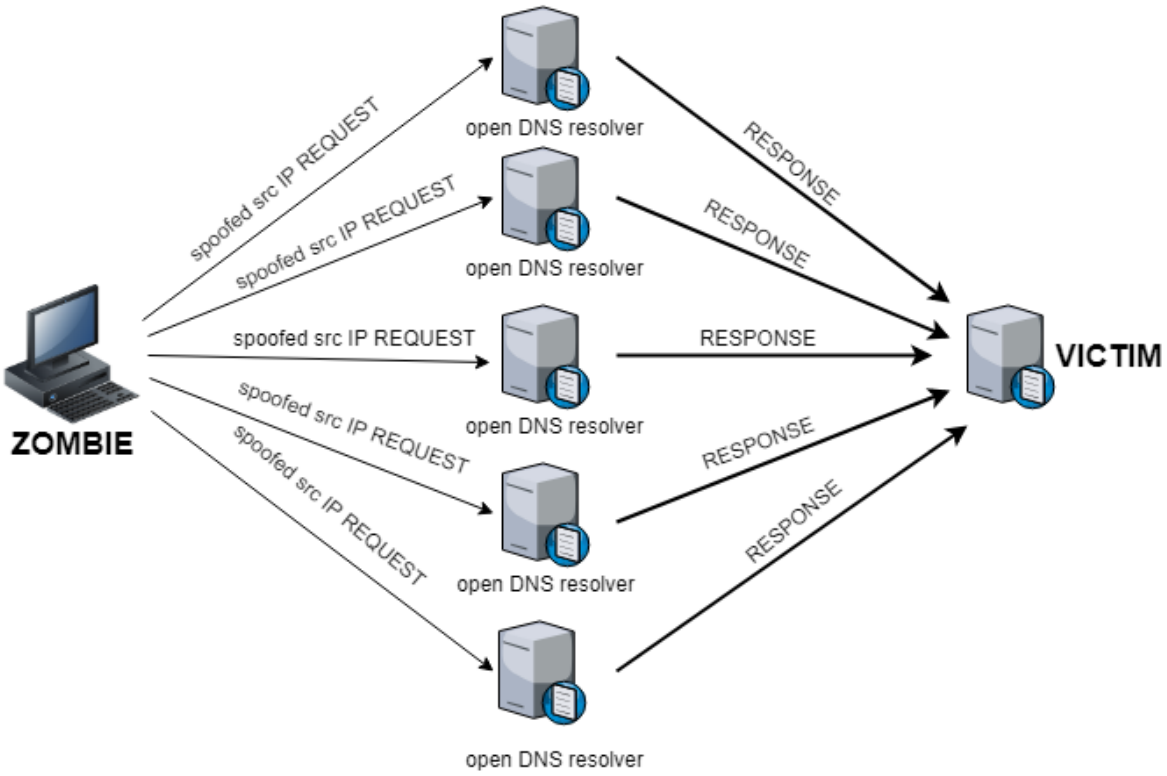
Οι επιθέσεις ενίσχυσης είναι μία παραλλαγή των επιθέσεων ανάκλασης. Αυτό που τις καθιστά διαφορετική κατηγορία είναι το γεγονός ότι επιτυγχάνουν την παραγωγή πολλαπλών δικτυακών πακέτων ανταπόκρισης για κάθε ένα πακέτο αίτησης. Αυτό επιτυγχάνεται με το να κατευθύνουν τα αρχικά πακέτα αίτησης από τις ενδιάμεσες οντότητες προς τις διευθύνσεις αναμετάδοσης του δικτύου στόχου κάτι το οποίο έχει ως αποτέλεσμα την ανταπόκριση από όλες τις δικτυακές οντότητες που συμμετέχουν στο εν λόγω δίκτυο. Η πιο συνηθισμένη υπηρεσία που χρησιμοποιείται σε αυτές τις επιθέσεις είναι η εντολή δικτύωσης ping η οποία χρησιμοποιεί ICMP πακέτα αντήχησης, καθώς είναι μία από τις πιο βασικές υπηρεσίες του TCP/IP και συνήθως επιτρέπεται από τα διάφορα συστήματα.

2.5.2.1 Επιθέσεις Ενίσχυσης DNS

Οι επιθέσεις αυτές, χρησιμοποιούν την τεχνική της ανάκλασης στοχεύοντας αρχικά προς DNS συστήματα έτσι ώστε να τα χρησιμοποιήσουν σαν ενδιάμεσες οντότητες. Οι επιτιθέμενοι συνήθως επιλέγουν DNS συστήματα με καλές δικτυακές συνδέσεις έτσι ώστε να μπορέσουν να δρομολογήσουν τη μεγαλύτερη δυνατή δικτυακή κίνηση προς το στόχο. Με ένα μικρό UDP πακέτο αίτησης της τάξης των 60-bytes, ο επιτιθέμενος μπορεί να επιτύχει τη δημιουργία UDP πακέτου ανταπόκρισης της τάξης των 512-bytes το οποίο είναι συνήθως το μέγιστο επιτρεπόμενο μέγεθος πακέτου που επιτρέπουν τα διάφορα συστήματα. Τα πακέτα αυτά σε

συνδυασμό με ένα μεγάλο αρχείο διαδικτυακών ονομάτων που μπορεί να κατέχει ένας DNS εξυπηρετητής, μπορούν να επιφέρουν το επιθυμητό αποτέλεσμα.

Παρόλα αυτά μία πιο εκτεταμένη DNS επίθεση ενίσχυσης, μπορεί να πραγματοποιηθεί με τη χρήση ενός DNS εξυπηρετητή στο ρόλο της ενδιάμεσης οντότητας, ο οποίος δημιουργεί αιτήσεις προς άλλους DNS εξυπηρετητές. Αυτή η τεχνική βασίζεται στη δυνατότητα των DNS εξυπηρετητών να μπορούν να αποστείλουν αίτηση σε άλλους DNS εξυπηρετητές με σκοπό την εξυπηρέτηση αιτήματος ενός δικού τους πελάτη. Στο σχήμα (g) αναπαρίσταται η διακεκριμένη επίθεση.



σχήμα g Δομή επίθεσης ανάκλασης

2.6 Τρόποι Άμυνας κατά DoS επιθέσεων

Για την αντιμετώπιση μίας DoS επίθεσης, ο διαχειριστής του συστήματος και γενικότερα του δικτύου μπορεί να πάρει κάποια μέτρα έτσι ώστε να αποφευχθεί ή να εξομαλυνθεί η οποιαδήποτε ενέργεια επίθεσης. Οι ενέργειες αυτές χωρίζονται σε τέσσερις βασικές κατηγορίες, οι οποίες εφαρμόζονται σε διαφορετικά στάδια της επίθεσης.

1. Ενέργειες Αποτροπής και Περιορισμού Δικαιωμάτων
   Η πρώτη κατηγορία, Αποτροπής και Περιορισμού Δικαιωμάτων αποτελείται από ένα αριθμό μέτρων και μηχανισμών, οι οποίοι επιτρέπουν στο διαχειριστή να αντέξει μία επίθεση χωρίς να χρειαστεί να αποκοπεί η παροχή υπηρεσιών στις νόμιμες οντότητες. Επίσης, οι τεχνικές αυτές περιλαμβάνουν ενισχυμένα μέτρα πολιτικής σχεδίασης δικτύων όσον αφορά την κατανάλωση πόρων από την κάθε οντότητα, όπως επίσης η χρησιμοποίηση εφεδρικών πόρων. Επιπρόσθετα, οι μηχανισμοί αποτροπής, τροποποιούν τα συστήματα και τα πρωτόκολλα έτσι ώστε να μειωθεί η πιθανότητα μίας επικείμενης

επίθεσης.

2. Ενέργειες Ανίχνευσης και Φιλτραρίσματος
   Η δεύτερη κατηγορία, Ανίχνευσης και Φιλτραρίσματος, αποτελείται από μηχανισμούς οι οποίοι επιχειρούν να ανιχνεύσουν την επίθεση και να αντιδράσουν άμεσα, κάτι που ελαχιστοποιεί τις αρνητικές επιπτώσεις στο θύμα. Η ανίχνευση περιλαμβάνει την παρατήρηση για ύποπτες συμπεριφορές και μοτίβα περιλαμβάνοντας π.χ., συγκεκριμένες διαδικτυακές κινήσεις, άγνωστες διευθύνσεις με τις οποίες έρχεται σε επαφή το σύστημα, μη ασφαλείς ιστοχώροι κλπ.
3. Ανίχνευσης Πηγής Επίθεσης και Ταυτοποίηση
   Η τρίτη κατηγορία, Ανίχνευσης Πηγής Επίθεσης και Ταυτοποίηση, ορίζεται ως η κατηγορία που έχει ως στόχο την εύρεση της πηγής της επίθεσης. Λόγω των φύσεων και του τρόπου διεξαγωγής μίας επίθεσης η οποία συνήθως θα προέρχεται από ένα μεγάλο αριθμό πηγών η διαδικασία αυτή πολύ πιθανόν να είναι χρονοβόρα.
   Αντίδραση
4. Η τέταρτη και τελευταία κατηγορία, είναι αυτή της Αντίδρασης, η οποία έχει ως στόχο την αποκοπή και την εξάλειψη μίας επίθεσης. Στο στάδιο αυτό, οι αμυνόμενοι προσπαθούν με τεχνικές μεθόδους να ισοσταθμήσουν την επίδραση της επίθεσης και να την ανακόψουν. Κύριο μέλημα τους είναι να περισώσουν όσο μεγαλύτερο τμήμα είναι δυνατόν, από τη μονάδα που δέχεται την επίθεση. Η ταχύτητα της διεκπεραίωσης των τριών παραπάνω κατηγοριών θα επιφέρει καλύτερα αποτελέσματα κατά το στάδιο της αντίδρασης.

Η διαβάθμιση των κατηγοριών γίνεται με βάση του χρόνου κατά τον οποίο εφαρμόζονται. Η πρώτη κατηγορία εφαρμόζεται κατά τον σχεδιασμό του δικτύου άρα και πριν την οποιαδήποτε επικείμενη επίθεση. Η δεύτερη κατηγορία υλοποιείται κατά τη διάρκεια της επίθεσης, η τρίτη κατηγορία υλοποιείται κατά τη διάρκεια και έπειτα της επίθεσης και τέλος η τέταρτη κατηγορία εφαρμόζεται επίσης μετά την επίθεση.

Με βάση όλες τις επιθέσεις που περιγράφηκαν παραπάνω, είναι πλέον αποδεκτό να θεωρηθεί ως γεγονός πλέον ότι ένας οργανισμός, ο οποίος διαχειρίζεται ένα δίκτυο και γενικότερα ένα σύστημα με δικτυακά συνδεδεμένες οντότητες πρέπει να χρησιμοποιεί τεχνικές και μηχανισμούς, οι οποίοι του επιτρέπουν να επιβλέπει και να ελέγχει τη δικτυακή κίνηση, όπως επίσης και τα διάφορα μοτίβα έτσι ώστε να εξάγει στατιστικά στοιχεία με σκοπό να έχει μέτρο σύγκρισης. Έχοντας στα χέρια του τα δεδομένα αυτά, ο διαχειριστής του συστήματος είναι σε θέση να αντιληφθεί μία δυσλειτουργία ενός λογισμικού ή φυσικού μηχανήματος κάτι το οποίο μπορεί να εκμεταλλευτεί ο επιτιθέμενος.

Το πρώτο βήμα όταν ανιχνευτεί μία DoS επίθεση είναι να τακτοποιηθεί το είδος της επίθεσης άρα και κατά επέκταση ο τρόπος προσέγγισης της. Κατά τη διαδικασία της ταυτοποίησης, οι υπάλληλοι του οργανισμού αναλύουν τα πακέτα τα οποία καταφθάνουν με σκοπό την εύρεση του είδους της επίθεσης. Σε περίπτωση που ο οργανισμός δεν διαθέτει τα απαραίτητα μέσα ή προσωπικό, τότε θα απευθυνθεί στον πάροχο της δικτυακής του γραμμής έτσι ώστε να προχωρήσουν στις απαραίτητες διαδικασίες. Αναλόγως του είδους της επίθεσης χρησιμοποιούνται και τα κατάλληλα φίλτρα για την αποκοπή του συγκεκριμένου είδους πακέτων. Τα φίλτρα αυτά θα εγκατασταθούν συνήθως στους δρομολογητές του παρόχου. Σε περίπτωση που η επίθεση δεν διεξάγεται με την τεχνική της μαζικής αποστολής δικτυακών πακέτων αλλά στοχεύει σε μία δυσλειτουργία του συστήματος ή μίας εφαρμογής, όπως οι επιθέσεις τύπου Άνθρωπος στη Μέση, τότε η δυσλειτουργία αυτή θα πρέπει να βρεθεί και να

διορθωθεί. Επίσης, με σκοπό την αποτροπή μελλοντικών επιθέσεων, ο οργανισμός μπορεί να ζητήσει από τον πάροχο να ανιχνεύσει την πηγή της επίθεσης έτσι ώστε να πάρει συγκεκριμένα μέτρα. Ωστόσο αν ο επιτιθέμενος χρησιμοποιεί ψεύτικες διευθύνσεις αυτό δεν είναι εφικτό.

Σε περίπτωση όμως μίας εκτεταμένης και συντονισμένης επίθεσης πλημμύρας από ένα μεγάλο αριθμό διανεμημένων συστημάτων ή συστημάτων ανάκλασης, το φιλτράρισμα ενός ικανοποιητικού αριθμού πακέτων πολύ πιθανόν να μην είναι δυνατό έτσι ώστε να αποκατασταθεί η δικτυακή διασύνδεση. Στην περίπτωση αυτή, ο οργανισμός θα πρέπει να ακολουθήσει μία διαφορετική στρατηγική, όπως είναι η χρήση εφεδρικών εξυπηρετητών ή η άμεση εκμίσθωση νέων εξυπηρετητών σε διαφορετική τοποθεσία από αυτή του οργανισμού καθώς και η χρήση νέων διευθύνσεων. Εάν ο οργανισμός δεν έχει προβλέψει να πάρει εναλλακτικά μέτρα, τότε η επίπτωση της επίθεσης θα είναι η εκτεταμένη διακοπή δικτυακής σύνδεσης κάτι το οποίο μπορεί να εξελιχθεί σε μεγαλύτερης κλίμακας πρόβλημα εάν ο οργανισμός βασίζεται στη σύνδεση αυτή για τις λειτουργίες του.

ΕΝΟΤΗΤΑ 3

3.1 Τα αντικείμενα στο IoT - Ανάλυση συσκευών και των ιδιοτήτων τους

Όπως κάθε δίκτυο έτσι και το IoT αποτελείται από διάφορες οντότητες. Αυτό που κάνει όμως ξεχωριστό το IoT είναι ότι δεν συμμετέχουν μόνο φυσικές συσκευές και πρωτόκολλα αλλά και άλλων μορφών δικτυακές οντότητες όπως π.χ., το σύννεφο όπου οι οποίες οντότητες αλληλοεπιδρούν μεταξύ τους σε πραγματικό χρόνο.

Το IoT, μπορεί να εφαρμοστεί σε ποικίλους τομείς της ανθρώπινης δραστηριότητας, οι οποίοι διαφέρουν μεταξύ τους. Η διαφορά αυτή επεκτείνεται επιπρόσθετα στην αντίστοιχη δραστηριότητα, το σκοπό και την υλοποίηση της κάθε εφαρμογής. Οι κύριοι τομείς που εφαρμόζουν την τεχνολογία IoT είναι αυτοί της Μεταφοράς, Υγείας, Βιομηχανίας όπως επίσης και για σκοπούς άμεσης ανταπόκρισης σε επείγων περιστατικά φυσικής και μή καταστροφής, όπως πυρκαγιές σε δάση, καταστροφές σε απομακρυσμένες βάσεις τηλεπικοινωνιών, ύδρευσης, ηλεκτροδότησης κλπ. Όπως διαφαίνεται, σε κάθε ένα από αυτούς τους τομείς, χρησιμοποιούνται ίδιας κατηγορίας αλλά διαφορετικού σκοπού λειτουργίας οντότητες.

Η ετερογένεια και ετερολειτουργικότητα των οντοτήτων αυτών, δυσχεραίνει τον προσδιορισμό και την κατηγοριοποίηση τους, παρόλα αυτά πιο κάτω θα επιδιωχθεί μία προσπάθεια κατηγοριοποίησης και ομαδοποίησης βάση των αναγκών και των λειτουργιών τους. Για να κατανοηθεί καλύτερα η λογική, η οποία ακολουθείται για την ομαδοποίηση των οντοτήτων σε κατηγορίες, είναι αναγκαίο να προσδιοριστούν πρώτα τα βασικά στοιχεία που απαιτούνται έτσι ώστε να λειτουργεί μία δομή IoT[3]. Η δομή λειτουργικότητας του IoT αποτελείται από έξι βασικά στοιχεία (όπως αυτά διαφαίνονται και στο σχήμα (h)):

1. Ταυτοποίηση
   Όπως τονίζεται σε πολλά σημεία της εργασίας, η ταυτοποίηση είναι αναπόσπαστο κομμάτι της ορθής λειτουργικότητας του IoT. Υπάρχουν αρκετές μέθοδοι ταυτοποίησης για το IoT όπως είναι αυτές των ηλεκτρονικών κωδικών για προϊόντα και οι μοναδικοί κωδικοί για αντικείμενα ή οπουδήποτε μπορεί να εφαρμοστεί η χρήση τους[4]. Η ταυτοποίηση των οντοτήτων είναι μεγάλης σημασίας καθώς αυτό διαφοροποιεί την ταυτότητα τους από τη διεύθυνση τους. Ένα αναγνωριστικό αναφέρεται στο όνομα της οντότητας ενώ η διεύθυνση αναφέρεται στη διεύθυνση του μέσα στο δίκτυο. Η διαφοροποίηση αυτή είναι επιτακτικής ανάγκης, καθώς η ταυτοποίηση δεν είναι ευρέως μοναδική έτσι σε συσχετισμό με την διευθυνσιοδότηση, καθίσταται εφικτή η μοναδική αναγνώριση των αντικειμένων.
2. Ανίχνευση
   Με τον όρο ανίχνευση περιγράφεται η διαδικασία συλλογής δεδομένων αναλόγως των αντικειμένων που τις συλλέγουν και η αποστολή τους σε μίας μορφής αποθηκευτικής μονάδας. Τα δεδομένα που συλλέγονται, αναλύονται έτσι ώστε να μπορούν να χρησιμοποιηθούν για συγκεκριμένες ανάγκες αναλόγως από τις απαιτούμενες υπηρεσίες που θα ζητηθούν. Οι ανιχνευτές αυτοί μπορεί να είναι έξυπνοι αισθητήρες, ενεργοποιητές ή συσκευές αισθητήρων που μπορούν να φορεθούν. Για παράδειγμα, υπάρχουν εταιρείες οι οποίες προσφέρουν τέτοιας μορφής αισθητήρων και εφαρμογών κινητής τηλεφωνίας, οι οποίες επιτρέπουν στους χρήστες τους να παρακολουθούν και να ελέγχουν χιλιάδες έξυπνες συσκευές μέσα σε κτίρια χρησιμοποιώντας μόνο τις έξυπνες

συσκευές τους.

3. Η επικοινωνία είναι ο ακρογωνιαίος λίθος για την λειτουργία του IoT.Η επικοινωνία αυτή επιτυγχάνεται με τη χρήση διαφόρων, και διαφορετικών μεταξύ τους τεχνολογιών και πρωτοκόλλων αφού σε ένα IoT οι συμμετέχοντες οντότητες παρουσιάζουν ένα ευρύ φάσμα ετερογένειας. Συνήθως οι κόμβοι επικοινωνίας θα πρέπει να λειτουργούν με χαμηλή ισχύ έτσι ώστε να αποφευχθούν οι απώλειες και θόρυβος στα κανάλια των επικοινωνιακών συνδέσεων. Κάποια από τα πιο διαδεδομένα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται είναι αυτά των WiFI, Bluetooth, IEEE 802.15.4, Z-wave και LTE-Advanced. Επίσης γίνεται χρήση και ορισμένων ειδικών τεχνολογιών επικοινωνίας όπως η RFID, NFC και UWB. Η RFID είναι η πρώτη τεχνολογία που χρησιμοποιείται για την υλοποίηση της ιδέας του M2M. Η ετικέτα RFID αντιπροσωπεύει ένα απλό τσιπ ή ετικέτα προσαρμοσμένη για την παροχή ταυτότητας σε αντικείμενα. Η συσκευή ανάγνωσης RFID μεταδίδει ένα σήμα ερωτήματος στην ετικέτα και λαμβάνει ένα ανακλώμενο σήμα από την ετικέτα, το οποίο μεταβιβάζεται στη βάση δεδομένων. Η βάση δεδομένων συνδέεται με ένα κέντρο επεξεργασίας για να εντοπίσει αντικείμενα που βασίζονται (10 έως 200 m) [5]. Το πρωτόκολλο NFC λειτουργεί σε ζώνη υψηλών συχνοτήτων στα 13,56 MHz και υποστηρίζει ρυθμό δεδομένων μέχρι 424 kbps. Το εύρος που ισχύει είναι μέχρι 10 cm και η επικοινωνία γίνεται μεταξύ ενεργών αναγνωστών και παθητικών ετικετών ή μεταξύ δύο ενεργών αναγνωστών [6]. Η τεχνολογία UWB έχει σχεδιαστεί για να υποστηρίζει τις επικοινωνίες σε περιοχές χαμηλής κάλυψης των οποίων οι εφαρμογές για τη σύνδεση αισθητήρων αυξήθηκαν πρόσφατα αφού χρησιμοποιεί χαμηλή ενέργεια και διαθέτει υψηλό εύρος ζώνης[7]. μία άλλη τεχνολογία επικοινωνίας είναι το WiFi που χρησιμοποιεί ραδιοκύματα για την ανταλλαγή δεδομένων μεταξύ των αντικειμένων που βρίσκονται εντός εύρους 100μ[8]. Το Bluetooth παρουσιάζει μία τεχνολογία επικοινωνίας που χρησιμοποιείται για την ανταλλαγή δεδομένων μεταξύ συσκευών σε μικρές αποστάσεις με χρήση ραδιοκυμάτων μικρού μήκους για την ελαχιστοποίηση της κατανάλωσης ρεύματος [9]. Το πρότυπο 802.15.4 καθορίζει τόσο ένα φυσικό επίπεδο όσο και ένα μέσο ελέγχου πρόσβασης για ασύρματα δίκτυα χαμηλής κατανάλωσης με ικανές και κλιμακούμενες επικοινωνίες [10].

   Το LTE είναι αρχικά ένα πρότυπο ασύρματης επικοινωνίας για μεταφορά δεδομένων υψηλής ταχύτητας μεταξύ κινητών τηλεφώνων που βασίζονται σε τεχνολογίες δικτύων GSM / UMTS [11]. Το LTE-A μπορεί να καλύψει συσκευές ταχείας κίνησης όπως επίσης και να παρέχει υπηρεσίες ραδιοτηλεοπτικών εκπομπών. Το LTE-A (LTE Advanced) είναι ένα αναβαθμισμένη έκδοση του LTE, συμπεριλαμβανομένης της επέκτασης εύρους ζώνης, η οποία υποστηρίζει μέχρι 100 MHz, χωρική πολυπλεκτική-εκτεταμένη κάλυψη, υψηλότερη απόδοση και χαμηλότερες λανθάνουσες περιόδους [12].

4. Υπολογισμός

   μία ακόμη πολύ σημαντική παράμετρος για την υλοποίηση του IoT είναι η υπολογιστική του δύναμη. Με τον όρο υπολογιστική δύναμη εννοούμε τους μικροελεγκτές, μικροεπεξεργαστές και εφαρμογές λογισμικού, οι οποίες αποτελούν την κεντρική μονάδα επεξεργασίας και η συνολική υπολογιστική ικανότητα τους αντιπροσωπεύει την υπολογιστική ικανότητα του IoT. Η συνεργασία των στοιχείων αυτών παίρνει μέρος σε πλατφόρμες IoT. Με τον όρο πλατφόρμα περιγράφουμε ένα σύνολο υλικού οι οποίες τρέχουν συγκεκριμένο λειτουργικό σύστημα, καθώς και διάφορες άλλες εφαρμογές λογισμικού με σκοπό την παροχή υπηρεσιών IoT. Μέχρι σήμερα έχουν αναπτυχθεί διάφορες πλατφόρμες όπως το Arduino, UDOO, FriendlyARM, Intel Galileo, Raspberry

PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle και T-Mote Sky. Ανάμεσα στα διάφορα λειτουργικά συστήματα που χρησιμοποιούν οι πλατφόρμες, κάποια παρέχουν την ικανότητα παροχής υπηρεσιών σε πραγματικό χρόνο κάτι το οποίο μπορεί να χρησιμοποιηθεί σαν βάση για την περαιτέρω ανάπτυξη της τεχνολογίας IoT. Οι πλατφόρμες αυτές αναπτύσσονται από διάφορες εταιρείες που δραστηριοποιούνται σε διάφορους τομείς του IoT όπως για παράδειγμα εταιρείες αυτοκινητοβιομηχανίας όπου σε συνεργασία με τη Google ίδρυσαν την Ανοιχτή Συμμαχία Αυτοκινητοβιομηχανίας και σχεδιάζουν να φέρουν καινούργια χαρακτηριστικά στην Android πλατφόρμα για να επιταχύνουν την υιοθέτηση του παραδείγματος του Διαδικτύου των Οχημάτων [13].

Ένα άλλο μεγάλο σημαντικό υπολογιστικό κομμάτι του IoT είναι πλατφόρμες τεχνολογίας σύννεφου. Οι πλατφόρμες αυτές παρέχουν τις απαραίτητες εγκαταστάσεις για έξυπνα αντικείμενα, όπως τη δυνατότητα αποστολής δεδομένων στο σύννεφο, την επεξεργασία μεγάλου όγκου δεδομένων σε πραγματικό χρόνο με απώτερο αποτέλεσμα να επωφεληθούν οι τελικοί χρήστες από τη γνώση που προέρχεται από τα συλλεγόμενα δεδομένα.

5. Υπηρεσίες

   Οι υπηρεσίες στο IoT κατηγοριοποιούνται κυρίως σε τέσσερις κατηγορίες[14][15]. μία από τις κατηγορίες είναι οι υπηρεσίες σχετιζόμενες με την ταυτότητα. Υπηρεσίες που σχετίζονται με την ταυτότητα είναι οι πιο βασικές και σημαντικές, οι οποίες χρησιμοποιούνται σε άλλες υπηρεσίες αφού οποιαδήποτε εφαρμογή που πρέπει να φέρει ένα αντικείμενο από τον φυσικό κόσμο στον κόσμο της πληροφορικής πρέπει πρώτα να τα αναγνωρίσει τα αντικείμενα αυτά.

   Δεύτερη κατηγορία είναι αυτή της συλλογής πληροφοριών. Οι υπηρεσίες αυτές έχουν ως σκοπό τη συλλογή και σύνοψη των πρώτων δεδομένων, όπως οι μετρήσεις που προέρχονται από τους διάφορους αισθητήρες. Οι CAS ενεργούν πάνω από τις υπηρεσίες συλλογής πληροφοριών και χρησιμοποιούν τα συλλεγόμενα δεδομένα με σκοπό να πάρουν αποφάσεις και να αντιδράσουν αναλόγως. Εντούτοις, οι γενικευμένες υπηρεσίες έχουν ως στόχο την παροχή CAS οποτεδήποτε και οπουδήποτε είναι απαραίτητες και κάποιος τις χρειάζεται. Ο τελικός σκοπός της δομής αυτής είναι να φτάσουν στο επίπεδο να μπορούν να ανταποκριθούν στις ανάγκες των χρηστών ανά πάσα στιγμή. Ωστόσο, αυτό δεν είναι εύκολα εφικτό δεδομένου ότι υπάρχουν πολλές δυσκολίες και προκλήσεις που πρέπει πρώτα να αντιμετωπιστούν.

6. Σημασιολογία

   Η Σημασιολογία στο IoT αναφέρεται στην ικανότητα εξαγωγής γνώσεων έξυπνα από διαφορετικά μηχανήματα για την παροχή των απαιτούμενων υπηρεσιών. Η εξαγωγή γνώσης περιλαμβάνει την ανακάλυψη και τη χρήση πόρων και πληροφοριών μοντελοποίησης. Επίσης, περιλαμβάνει την αναγνώριση και ανάλυση δεδομένων έτσι ώστε να παρθεί η σωστή απόφαση για την παροχή της ακριβής υπηρεσίας[16]. Έτσι, η σημασιολογία αντιπροσωπεύει τον εγκέφαλο του IoT με την αποστολή αιτημάτων στον σωστό προορισμό. Αυτή η απαίτηση υποστηρίζεται από τεχνολογίες σημασιολογικού ιστού, όπως το πλαίσιο περιγραφής πόρων και τη γλώσσα οντολογικού ιστού.

3.2 Αρχιτεκτονική και Πρωτόκολλα Επικοινωνίας στο IoT

Σε όλα τα δίκτυα υπάρχει μία δομή και μία συγκεκριμένη διαδικασία που ακολουθείται για την εκπλήρωση μίας διεργασίας. Έτσι και στο IoT, αναλόγως του σκοπού που εξυπηρετεί το κάθε δίκτυο,

υπάρχει συγκεκριμένη και προκαθορισμένη μορφολογία, αρχιτεκτονική και πρωτόκολλα που χρησιμοποιούνται.

3.3 Αρχιτεκτονική και Επίπεδα - Ανάλυση

Κάθε πληροφοριακό δίκτυο, ακολουθεί μία δομημένη αρχιτεκτονική βασισμένη στην αλυσιδωτή αλληλουχία επιπέδων ή αλλιώς ιεραρχική δομή, όπου το κάθε επίπεδο αποτελείται από διαφορετικές ιδιότητες και εξυπηρετεί μία συγκεκριμένη λειτουργία στο δίκτυο. Την ίδια λογική δομή ακολουθεί και το IoT. Προφανώς το κάθε επίπεδο αποτελείται από άλλα εσωτερικά υποεπίπεδα, όπου το καθένα αναλαμβάνει συγκεκριμένη εργασία/λειτουργία με σκοπό την υλοποίηση του γενικού σκοπού του επιπέδου. Τα επίπεδα για το IoT όπως επίσης η δομή και οι λειτουργίες τους θα πρέπει να θεωρηθούν σαν μία γενική προσέγγιση της δομής του IoT καθώς το κάθε δίκτυο διαφέρει αναλόγως του σκοπού και των αναγκών που εξυπηρετεί καθώς και του περιβάλλοντος που αναπτύσσεται και δραστηριοποιείται. Επίσης, πρέπει να σημειωθεί ότι ακόμη δεν έχει ακόμη κάποια συγκεκριμένη δομή και συγκεκριμένα επίπεδα για το IoT. Στο παρόν στάδιο υπάρχουν διάφορες προτάσεις από την επιστημονική κοινότητα. Πιο κάτω παρουσιάζεται μία από τις προτεινόμενες αρχιτεκτονικές και πιο συγκεκριμένα αυτή των πέντε επιπέδων[17].

Επίπεδο Αντικειμένων: Το επίπεδο αυτό καθιστά το πρώτο επίπεδο και αποτελείται από τις συσκευές/αισθητήρες και γενικώς την πλειοψηφία των φυσικών αντικειμένων του δικτύου.
Σκοπός του είναι η συλλογή δεδομένων και η μεταβίβαση τους στο επόμενο επίπεδο μέσω ασφαλών καναλιών.

Επίπεδο Αφαίρεσης Αντικειμένων: Η κύρια υπευθυνότητα του επιπέδου αυτού, είναι η μεταφορά των δεδομένων που παρέλαβε από το επίπεδο Αντικειμένων προς το επίπεδο Διαχείρισης Υπηρεσιών. Τα δεδομένα μεταφέρονται μέσω ασφαλών καναλιών χρησιμοποιώντας μία πλειάδα τεχνολογιών μεταφοράς δεδομένων κυρίως ασύρματης διάδοσης. Μερικές εξ αυτών είναι οι RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared ZigBee. Το επίπεδο αυτό διαχειρίζεται σε δευτερεύων βαθμό και άλλες λειτουργίες όπως την επεξεργασία δεδομένων στο σύννεφο και διεργασίες διαχείρισης δεδομένων.

Επίπεδο Διαχείρισης Υπηρεσιών: Η βασική λειτουργία του επιπέδου αυτού, είναι η διασύνδεση μίας υπηρεσίας με τον αιτών της βάση διεύθυνσης. Πιο συγκεκριμένα, οι λειτουργίες του είναι η επεξεργασία των λαμβανομένων δεδομένων, η λήψη αποφάσεων και η αποστολή των αναγκαίων υπηρεσιών μέσω του ενσύρματου δικτύου και πρωτοκόλλων. Ένα σημαντικό πλεονέκτημα του επιπέδου, είναι ότι επιτρέπει στους προγραμματιστές των IoT αντικειμένων να δουλεύουν με ετερογενή αντικείμενα χωρίς οι δυνατότητες του να περιορίζονται από συγκεκριμένες πλατφόρμες συσκευών.

Επίπεδο Εφαρμογών: Το επίπεδο εφαρμογών παρέχει τις ζητούμενες από τους πελάτες υπηρεσίες. Για παράδειγμα, όταν ένας πελάτης ζητήσει πληροφορίες όπως η θερμοκρασία και η υγρασία για μία δεδομένη στιγμή, το επίπεδο εφαρμογών είναι υπεύθυνο για να μεταφέρει αυτές τις πληροφορίες προς τον χρήστη.

Επιχειρηματικό Επίπεδο: Το επίπεδο αυτό είναι υπεύθυνο για τη διαχείριση των υπηρεσιών και των δραστηριοτήτων του δικτύου. Πιο συγκεκριμένα, οι βασικές του εργασίες είναι η δημιουργία μοντέλων, γράφων, διαγραμμάτων ροής κ.λπ. βάσει στα δεδομένα που λαμβάνει από το Επίπεδο Εφαρμογών. Επίσης, σαν περεταίρω εργασίες, έχει τη σχεδίαση, ανάλυση, υλοποίηση, αξιολόγηση, επίβλεψη και ανάπτυξη στοιχείων που σχετίζονται με τα IoT συστήματα. Τα αποτελέσματα όλων αυτών των δραστηριοτήτων, καθιστούν δυνατή τη βέλτιστη

και αποτελεσματική λειτουργία του δικτύου αφού η επίβλεψη του δικτύου έχει σημαντική αξία στην επιβεβαίωση της σωστής λειτουργίας, στην αναδημιουργία/αναδιοργάνωση των στοιχείων που συνθέτουν το δίκτυο, όπως επίσης και γενικά στη σωστή διαχείριση του δικτύου ανά πάσα στιγμή.

σχήμα h - Τα συνθετικά στοιχεία του IoT[47]

3.4 Βασικά Πρωτόκολλα Επικοινωνίας - Περιγραφή

Για την ορθή λειτουργία του IoT απαιτείται η χρήση των αντίστοιχων πρωτοκόλλων τα οποία αποτελούν το σύνολο κανόνων με τους οποίους αλληλοεπιδρούν μεταξύ τους οι οντότητες.

A. Πρωτόκολλα Εφαρμογών

1. CoAP(Constrained Application Protocol)
   Το CoAP έχει σχεδιαστεί για να επιτρέπει σε απλές συσκευές περιορισμένων δυνατοτήτων να ενταχθούν στο IoT ακόμη και μέσω περιορισμένων δικτύων με χαμηλό εύρος ζώνης και χαμηλή διαθεσιμότητα. Το πρωτόκολλο χρησιμοποιείται γενικά για επικοινωνία από μηχανή σε μηχανή (M2M). Το CoAP λειτουργεί ως ένα είδος HTTP, επιτρέποντας σε συσκευές περιορισμένων δυνατοτήτων όπως αισθητήρες ή ενεργοποιητές να επικοινωνούν με το IoT, να ελέγχονται και να διαβιβάζουν τα δεδομένα τους ως μέρος ενός συστήματος. Το πρωτόκολλο έχει σχεδιαστεί για να προσφέρει αξιοπιστία σε δίκτυα χαμηλού εύρους ζώνης και υψηλής συμφόρησης μέσω της χαμηλής ισχύος έλξης και της χαμηλής γενικής χρήσης του δικτύου. Η αποτελεσματικότητα του ΠΠΕ μπορεί λοιπόν να επιτρέψει σε συσκευές που λειτουργούν με χαμηλή ποιότητα σήματος να στέλνουν τα δεδομένα τους αξιόπιστα ή να επιτρέπουν σε ένα δορυφόρο που βρίσκεται σε τροχιά να διατηρεί την απομακρυσμένη επικοινωνία του με επιτυχία. Παρά την ικανότητα του ΠΠΕ να τρέχει σε μικρές συσκευές, υποστηρίζει δίκτυα με δισεκατομμύρια κόμβους.
2. Message Queuing Telemetry Transport(MQTT)
   Το OMTM είναι ένα πρωτόκολλο ανταλλαγής μηνυμάτων όπου στόχο έχει τη σύνδεση των ενσωματωμένων συσκευών και δικτύων με τις εφαρμογές. Η λειτουργία σύνδεσης χρησιμοποιεί ένα μηχανισμό δρομολόγησης (ένας προς ένα, ένας προς πολλούς, πολλοί προς πολλούς) και καθιστά το MQTT ως το βέλτιστο πρωτόκολλο σύνδεσης για το IoT και M2M. Χρησιμοποιεί το μοντέλο δημοσίευσης / εγγραφής για να παρέχει ευελιξία και απλότητα στην υλοποίηση και είναι κατάλληλο για συσκευές περιορισμένων πόρων που χρησιμοποιούν αναξιόπιστους ή χαμηλού εύρους ζώνης συνδέσμους. Πολλές εφαρμογές σε διάφορους τομείς χρησιμοποιούν το CoAP όπως π.χ. ο τομέας της υγείας, παρακολούθησης, μέτρησης ενέργειας και οι ειδοποιήσεις του Facebook.Επομένως, το πρωτόκολλο ΠΠΕ αντιπροσωπεύει ένα ιδανικό πρωτόκολλο ανταλλαγής μηνυμάτων για

τις επικοινωνίες IoT και M2M και είναι σε θέση να παρέχει δρομολόγηση για μικρές, φθηνές, χαμηλής ισχύος και χαμηλής μνήμης συσκευές σε ευάλωτα δίκτυα και δίκτυα χαμηλού εύρους ζώνης.

3. Extensible Messaging and Presence Protocol (XMPP)
   Το XMPP είναι ένα IETF πρότυπο για την αποστολή/παραλαβή άμεσων μηνυμάτων το οποίο χρησιμοποιείται για συνομιλίες με πολλούς συμμετέχοντες, για κλήσεις φωνής, εικόνας και τηλεπαρουσίας. Το XMPP επιτρέπει στους χρήστες να επικοινωνούν μεταξύ τους με την αποστολή άμεσων μηνυμάτων στο διαδίκτυο ανεξαρτήτως του λειτουργικού συστήματος που χρησιμοποιούν. Επίσης επιτρέπει εφαρμογές IM για την επίτευξη ελέγχου ταυτότητας, ελέγχου πρόσβασης, μέτρηση ασφάλειας, κρυπτογράφηση από άκρο σε άκρο και από κόμβο σε κόμβο, και συμβατότητα με άλλα πρωτόκολλα.
4. Advanced Message Queuing Protocol (AMQP)
   Το ΑΠΡΜ είναι ένα πρωτόκολλο ανοιχτού προτύπου εφαρμογής για εφαρμογές IoT που εστιάζει στα περιβάλλοντα που έχουν ως κύριο γνώμονα τα μηνύματα. Υποστηρίζει αξιόπιστη επικοινωνία μέσω αποστολής μηνυμάτων με διάφορες τεχνικές συμπεριλαμβανομένων και θεμελιακών τεχνικών όπως αυτών της "το πολύ μίας φοράς", "τουλάχιστον μίας φοράς" και "ακριβώς μία φοράς". Το ΑΠΡΜ απαιτεί ένα αξιόπιστο πρωτόκολλο μεταφοράς όπως το TCP για την ανταλλαγή μηνυμάτων. Ορίζοντας ένα πρωτόκολλο ενσύρματου επιπέδου, το πρωτόκολλο μπορεί να επιτύχει επικοινωνία σημείου προς σημείο. Επίσης υποστηρίζει το μοντέλο επικοινωνίας δημοσίευσης/εγγραφής ορίζοντας ένα επίπεδο μηνυματοδοσίας πάνω από το επίπεδο μεταφοράς του. Το ΑΠΡΜ υποστηρίζει δύο είδη μηνυμάτων, τα γυμνά-ασχολίαστα μηνύματα που παρέχονται από τον αποστολέα και τα μηνύματα με σχόλιο που εμφανίζονται στον παραλήπτη.
5. Data Distribution Service (DDS)
   Είναι ένα πρωτόκολλο δημοσίευσης-εγγραφής για επικοινωνίες M2M σε πραγματικό χρόνο. Σε αντίθεση με άλλα πρωτόκολλα δημοσιεύσης-εγγραφής βασίζεται σε μία αρχιτεκτονική που η διαδικασία επικοινωνίας υλοποιείται χωρίς την ανάγκη μεσάζοντα και επίσης χρησιμοποιεί πακέτα multicast για να επιτύχει εξαιρετική QoS. Τα χαρακτηριστικά της αρχιτεκτονικής του, ταιριάζει πολύ καλά με τους περιορισμούς που έχει το IoT και το M2M, όπως η ανάγκη επικοινωνίας σε πραγματικό χρόνο. Επίσης υποστηρίζει 23 πολιτικές QoS μέσω των οποίων μία ποικιλία κριτηρίων για την επικοινωνία όπως είναι η ασφάλεια, η επείγουσα αναγκαιότητα, η προτεραιότητα, η ανθεκτικότητα, η αξιοπιστία κ.λπ. που μπορούν να αντιμετωπιστούν από τον προγραμματιστή. Η αρχιτεκτονική DDS ορίζει δύο επίπεδα: Το δεδομενοκεντρικό επίπεδο δημοσίευσης/εγγραφής(DCPS) και το δεδομενοτοπικό επίπεδο ανοικοδομησης. Το DCPS είναι υπεύθυνο για την παροχή των πληροφοριών στους συνδρομητές. Το DLRL από την άλλη πλευρά, είναι ένα προαιρετικό στρώμα και χρησιμεύει ως διεπαφή με τις λειτουργίες DCPS. Διευκολύνει την κατανομή των κατανεμημένων δεδομένων μεταξύ των κατανεμημένων αντικειμένων [19].

Στο επίπεδο DCPS ασχολούνται πέντε οντότητες με τη ροή δεδομένων :

- Η οντότητα Εκδότης που διαδίδει τα δεδομένα
- Η οντότητα Γραφέας Δεδομένων που χρησιμοποιείται από την εφαρμογή για να αλληλεπιδρά με τον Εκδότη σχετικά με τις τιμές και τις μεταβολές των δεδομένων που

αφορούν συγκεκριμένο τύπο. Η συσχέτιση του Γραφέα Δεδομένων και του Εκδότη δείχνει ότι η εφαρμογή πρόκειται να δημοσιεύσει τα συγκεκριμένα δεδομένα σε ένα παρεχόμενο πλαίσιο.

- Η οντότητα Συνδρομητής λαμβάνει τα δημοσιευμένα δεδομένα και τα παραδίδει στους αιτούντες
- Η οντότητα Αναγνώστης Δεδομένων που χρησιμοποιείται από το Συνδρομητή για πρόσβαση στα ληφθέντα δεδομένα.
- Η οντότητα Θέμα η οποία είναι αναγνωρίσιμη από έναν τύπο δεδομένων και ένα όνομα. Τα Θέματα συσχετίζουν τους Γραφείς Δεδομένων με τους Αναγνώστες Δεδομένων. Η μετάδοση δεδομένων είναι επιτρεπτή εντός ενός τομέα DDS ο οποίος είναι ένα εικονικό περιβάλλον για συνδεδεμένη δημοσίευση και εγγραφή εφαρμογών.

Β. Πρωτόκολλα Ανίχνευσης Υπηρεσίας

Η κλιμακωτή ανάπτυξη του IoT απαιτεί κάποιας μορφής μηχανισμού για τη διαχείριση πόρων, ο οποίος θα είναι σε θέση να καταγράψει και να ανακαλύψει πόρους και υπηρεσίες με αυτοδιαμορφωμένο, αποτελεσματικό και δυναμικό τρόπο. Τα πιο κυρίαρχα πρωτόκολλα σε αυτή την περιοχή είναι το DNS πολλαπλής διανομής(mDNS) και DNS Service Discovery (DNS-SD) που μπορούν να ανακαλύψουν πόρους και υπηρεσίες που προσφέρονται από συσκευές του IoT. Αν και αυτά τα δύο πρωτόκολλα είχαν αρχικά σχεδιαστεί για συσκευές με πλεονασμό πόρων, υπάρχουν μελέτες έρευνας οι οποίες υιοθετούν πιο ελαφριές εκδόσεις των πρωτοκόλλων αυτών για περιβάλλοντα IoT[20][21].

1. Domain Name System (mDNS)
   μία βασική υπηρεσία για εφαρμογές IoT όπως η ανταλλαγή άμεσων μηνυμάτων είναι η υπηρεσία ανάλυσης ονόματος. Το mDNS είναι μία τέτοια υπηρεσία η οποία μπορεί να εκτελέσει τη διεργασία ενός διακομιστή unicast DNS [22]. Το mDNS είναι ευέλικτο λόγω του ότι ο χώρος ονομάτων DNS είναι χρησιμοποιείται τοπικά χωρίς την ανάγκη επιπλέον κατανάλωσης πόρων του συστήματος ή ειδικής διαμόρφωσης για τη λειτουργία του. Είναι μία κατάλληλη επιλογή για ενσωματωμένες συσκευές που βασίζονται στο Διαδίκτυο λόγω του ότι α) Δεν υπάρχει ανάγκη για χειροκίνητη αναδιάρθρωση ή επιπλέον διαχείριση για τον έλεγχο των συσκευών β) είναι σε θέση να τρέξει χωρίς υποδομή και γ) δύναται να λειτουργείκαι σε περίπτωση αποτυχίας λειτουργίας της υποδομής. Το mDNS ρωτά τα ονόματα αποστέλλοντας ένα μήνυμα πολυεκπομπής IP σε όλους τους κόμβους του τοπικού τομέα. Με αυτό το ερώτημα, ο υπολογιστής-πελάτης ζητά από τις συσκευές που έχουν αυτό το όνομα να απαντήσουν πίσω. Όταν το μηχάνημα-στόχος λάβει το όνομά του, πολυεκπέμπει την απάντηση η οποία περιέχει την IP διεύθυνση του. Όλες οι συσκευές στο δίκτυο που λαμβάνουν το μήνυμα απόκρισης ενημερώνουν την τοπική τους κρύπτη χρησιμοποιώντας το όνομα και τη διεύθυνση IP που έλαβαν.
2. Domain Name System-Service Discovery (DNS-SD)
   Η λειτουργία ζευγαρώματος των απαιτούμενων υπηρεσιών από πελάτες που χρησιμοποιούν mDNS ονομάζεται Ανίχνευση Υπηρεσίας με βάση το Διακομιστή Ονόματος Τομέα (DNS-SD). Χρησιμοποιώντας αυτό το πρωτόκολλο, οι πελάτες μπορούν να ανακαλύψουν ένα σύνολο επιθυμητών υπηρεσιών σε ένα συγκεκριμένο δίκτυο χρησιμοποιώντας τυπικά μηνύματα DNS. DNS-SD, όπως και το mDNS, είναι μέρος των πρωτοκόλλων με μηδενική ανάγκη διαμόρφωσης για τη σύνδεση μηχανών

χωρίς την ανάγκη εξωτερική διαχείριση ή διαμόρφωση [58]. Ουσιαστικά, το DNS-SD χρησιμοποιεί το mDNS για την αποστολή πακέτων DNS σε συγκεκριμένες διευθύνσεις πολυεκπομπής μέσω του UDP. Υπάρχουν δύο κύρια βήματα για να υλοποιηθεί η Υπηρεσία ανίχνευσης: Η εύρεση του ονόματος του ξενιστή της απαιτούμενης υπηρεσίας όπως εκτυπωτές και αντιστοίχιση των IP διευθύνσεων με τα ονόματα των ξενιστών τους. Η εξεύρεση των ονομάτων του κάθε ξενιστή είναι πολύ σημαντική για το λόγο ότι οι διευθύνσεις IP ενδέχεται να αλλάξουν, ενώ τα ονόματα δεν αλλάζουν. Η λειτουργία ζευγαρώματος πολυεκπέμπει λεπτομέρειες σχετικά με το δίκτυο, όπως η διεύθυνση IP και ο αριθμός δικτυακής θύρας σε κάθε συνδεδεμένο ξενιστή. Χρησιμοποιώντας το DNS-SD, τα ονόματα της κάθε συσκευής μέσα στο δίκτυο, μπορούν να διατηρηθούν σταθερά για όσο το δυνατόν πιο πολύ καιρό με στόχο να αυξηθεί η εμπιστοσύνη και η αξιοπιστία.

Γ. Πρωτόκολλα Υποδομής

1. Routing Protocol for Low Power and Lossy Networks (RPL): Το RPL είναι ένα πρωτόκολλο δρομολόγησης για ασύρματα δίκτυα με χαμηλή κατανάλωση ρεύματος και γενικά ευάλωτο σε απώλεια πακέτων. Πρόκειται για ένα ενεργό πρωτόκολλο βασισμένο στην ίδια δομή όπως το πρωτόκολλο IEEE 802.15.4, βελτιστοποιημένο για επικοινωνία πολλαπλών αναπηδήσεων και επικοινωνία πολλών προς ένα, επίσης υποστηρίζει και μηνύματα από ένα προς ένα. Αυτό το πρωτόκολλο καθορίζεται στα RFC5867, RFC5826, RFC5673 και RFC5548. Το RPL μπορεί να υποστηρίξει μία μεγάλη ποικιλία στρωμάτων σύνδεσης, συμπεριλαμβανομένων εκείνων με περιορισμούς, με πιθανές απώλειες ή που χρησιμοποιούνται σε συσκευές με περιορισμένους πόρους. Αυτό το πρωτόκολλο μπορεί γρήγορα να δημιουργήσει διαδρομές μέσα στο δίκτυο, να μοιράσει τις γνώσεις δρομολόγησης και να προσαρμόσει την τοπολογία με έναν αποτελεσματικό τρόπο. Ο πυρήνας του RPL είναι ο Προσανατολισμένος Προς τον Προορισμό Ακυκλικός Γράφος-DODAG που δείχνει ένα διάγραμμα δρομολόγησης των κόμβων. Ο DODAG αναφέρεται σε ένα κατευθυνόμενο ακυκλικό γράφημα με μία μόνο ρίζα. Κάθε κόμβος του DODAG γνωρίζει τους κόμβους γονείς του αλλά δεν έχει πληροφορίες για τα σχετικά παιδιά. Επίσης, το RPL διατηρεί τουλάχιστον μία διαδρομή προς τη ρίζα για κάθε κόμβο και ένα προτιμότερο γονέα για να ακολουθήσει μία ταχύτερη πορεία έτσι ώστε να αυξηθεί η απόδοση. Προκειμένου να διατηρηθεί η τοπολογία της δρομολόγησης και να διατηρηθούν οι πληροφορίες δρομολόγησης, το RPL χρησιμοποιεί τέσσερις τύπους μηνυμάτων ελέγχου. Το πιο σημαντικό μήνυμα είναι η Πληροφορία Αντικειμένου DODAG (DIO) που χρησιμοποιείται για να διατηρήσει την τρέχουσα κατάταξη (επίπεδο) του κόμβου, να καθορίσει την απόσταση κάθε κόμβου από τη ρίζα με βάση μερικές συγκεκριμένες μετρήσεις και να επιλέξει την προτιμώμενη γονική διαδρομή. Ο άλλος τύπος μηνύματος είναι αυτός της Διαφήμισης Προορισμού Αντικειμένου (DAO). Το RPL παρέχει υποστήριξη κυκλοφορίας προς τα άνω και προς τα κάτω χρησιμοποιώντας μηνύματα DAO με τα οποία αποστέλλει πληροφορίες του προορισμού σε επιλεγμένους κόμβους γονείς. Ο τρίτος τύπος μηνύματος είναι αυτός της Αίτησης Πληροφοριών DODAG(DIS) που χρησιμοποιείται από το ένα κόμβο για την απόκτηση μηνυμάτων DIO από έναν άλλο προσβάσιμο γειτονικό κόμβο.Ο τελευταίος τύπος μηνύματος είναι αυτός της Επιβεβαίωσης DAO (DAO-ACK) που είναι μία απάντηση σε ένα μήνυμα DAO και αποστέλλεται από ένα DAO κόμβο παραλήπτη που μπορεί να είναι γονέας DAO ή ρίζα DODAG. Οι δρομολογητές RPL λειτουργούν κάτω από έναν από τους δύο τρόπους

λειτουργίας (MOP): Των λειτουργιών Αποθήκευσης ή Μη Αποθήκευσης. Στη λειτουργία μη αποθήκευσης, τα δρομολόγια RPL δρομολογούνται προς χαμηλότερα επίπεδα βάσει της διεύθυνσης IP της πηγής, ενώ στον τρόπο αποθήκευσης, η καθοδική πορεία είναι με βάση την IPv6 διεύθυνση του προορισμού .

2. 6LowPAN

   Το 6LoWPAN είναι ένα ακρωνύμιο του IPv6 σε ασύρματα δίκτυα ιδιωτικής περιοχής χαμηλής κατανάλωσης. Το 6LoWPAN είναι το όνομα μίας ομάδας εργασίας που συνάπτεται στην περιοχή του Διαδικτύου του IETF. Η ιδέα του 6LoWPAN προέρχεται από την ιδέα ότι "το Διαδίκτυο θα μπορούσε και πρέπει να εφαρμοστεί ακόμη και στις μικρότερες συσκευές" και ότι οι συσκευές χαμηλής κατανάλωσης με περιορισμένες δυνατότητες επεξεργασίας θα πρέπει να μπορούν να συμμετέχουν στο IoT. Η ομάδα IETF ανέπτυξε το πρότυπο αυτό με σκοπό να καλύψει τις ανάγκες των μικρών συσκευών όπως περιορισμένο μέγεθος πακέτου (π.χ., μέγιστο 127 byte για IEEE 802.15.4), διάφορα μήκη διευθύνσεων και χαμηλό εύρος ζώνης[23][24][25]. Το 6LoWPAN είναι η προδιαγραφή των υπηρεσιών χαρτογράφησης που απαιτούνται από το IPv6 μέσω WPAN χαμηλής ισχύος για τη διατήρηση ενός δικτύου IPv6. Το πρότυπο αυτό χρησιμοποιεί την τεχνική συμπίεσης κεφαλίδας έτσι ώστε να μειώσει την εναέρια μετάδοση, τον κατακερματισμό και για να ικανοποιήσει το περιορισμο Μεγιστης Μονάδας Μετάδοσης του IPv6 (MTU), όπως επίσης να αυξήσει την προώθηση στο Επίπεδο Διασύνδεσης για την υποστήριξη της διανομής πολλαπλών αναπηδήσεων.

3. IEEE 802.15.4

   Το πρωτόκολλο δημιουργήθηκε για να ορίσει ένα υπόστρωμα ανάμεσα στο επίπεδο Μέσου Ελέγχου Πρόσβασης (MAC) και το Φυσικό Επίπεδο (PHY) για τα ασύρματα ιδιωτικά δίκτυα χαμηλού ρυθμού (LR-WPAN) [26]. Λόγω των προδιαγραφών του, όπως η χαμηλή κατανάλωση ενέργειας, χαμηλός ρυθμός δεδομένων, χαμηλό κόστος και υψηλή απόδοση μηνυμάτων το πρωτόκολλο αυτό χρησιμοποιείται από τα IoT και M2M. Παρέχει αξιόπιστη επικοινωνία, λειτουργικότητα σε διαφορετικές πλατφόρμες και μπορεί να χειριστεί ένα μεγάλο αριθμό κόμβων (περίπου 65k). Επίσης παρέχει ένα υψηλό επίπεδο ασφάλειας με τη χρήση υπηρεσιών κρυπτογράφησης και πιστοποίησης. Ωστόσο, δεν εγγυάται την Ποιότητα Υπηρεσίας. Το πρωτόκολλο αυτό είναι η βάση για το πρωτόκολλο ZigBee καθώς και τα δυο εστιάζουν στην παροχή υπηρεσιών χαμηλής ταχύτητας δεδομένων σε συσκευές περιορισμένης ισχύος και δημιουργούν μία πλήρη στοίβα πρωτοκόλλων δικτύου για WSNs. Το IEEE 802.15.4 υποστηρίζει τρεις ζώνες καναλιών συχνότητας και χρησιμοποιεί μία μέθοδο διάχυτου φάσματος άμεσης αλληλουχίας. Με βάση τα χρησιμοποιούμενα κανάλια συχνότητας, το φυσικό στρώμα μεταδίδει και λαμβάνει δεδομένα σε τρεις ρυθμούς δεδομένων: 250 kbps στα 2,4 GHz, 40 kbps στα 915 MHz και 20 kbps στα 868 MHz. Η χρήση υψηλότερων συχνοτήτων παρέχει υψηλή απόδοση και χαμηλή λανθάνουσα κατάσταση ενώ οι χαμηλότερες συχνότητες παρέχουν καλύτερη ευαισθησία και κάλυψη μεγαλύτερων αποστάσεων. Για τη μείωση πιθανών συγκρούσεων, το Μέσο Ελέγχου Πρόσβασης IEEE 802.15.4 χρησιμοποιεί το πρωτόκολλο CSMA / CA. Το πρότυπο IEEE 802.15.4 υποστηρίζει δύο τύπους δικτυακών κόμβων: συσκευές πλήρους και μειωμένης λειτουργίας. Η συσκευή πλήρης (FFD) μπορεί να χρησιμεύσει ως Ιδιωτικό Δίκτυο Περιοχής ή ως κανονικός κόμβος. Τα FFDs μπορούν να αποθηκεύσουν έναν πίνακα δρομολόγησης στη μνήμη τους και εφαρμόσουν νέα πλήρης Μέσο Ελέγχου Πρόσβασης(MAC). Επίσης μπορούν να επικοινωνούν με οποιαδήποτε άλλη συσκευή χρησιμοποιώντας οποιαδήποτε διαθέσιμη

τοπολογία. Σε αντίθεση, οι συσκευές μειωμένης λειτουργίας (RFD) , είναι πολύ απλοί κόμβοι με περιορισμένους πόρους. Μπορούν να επικοινωνούν μόνο με ένα συντονιστή και περιορίζονται σε μία τοπολογία αστέρα. Οι τυπικές τοπολογίες για τη διαμόρφωση των δικτύων IEEE 802.15.4 είναι αυτές των αστέρα,σημείου προς σημείο και συστάδες. Η τοπολογία αστέρα περιέχει τουλάχιστον ένα FFD που βρίσκεται στο κέντρο της τοπολογίας και ο σκοπός του είναι να διαχειρίζεται και να ελέγχει όλους τους άλλους κόμβους στο δίκτυο. Η τοπολογία σημείου προς σημείο περιέχει ένα συντονιστή Ιδιωτικού Δικτύου Περιοχής και οι άλλοι κόμβοι επικοινωνούν μεταξύ τους στο ίδιο δίκτυο ή με άλλα δίκτυα μέσω ενδιάμεσων κόμβων. Η τοπολογία συστάδας είναι μία ειδική περίπτωση της ομότιμης τοπολογίας σημείου προς σημείο και αποτελείται από έναν συντονιστή Ιδιωτικού Δικτύου Περιοχής

4. Το Bluetooth Low Energy (BLE) ή αλλιώς το έξυπνο Bluetooth χρησιμοποιεί ραδιοσήματα μικρής εμβέλειας που λειτουργεί με ελάχιστη κατανάλωση ισχύος για μεγαλύτερο χρονικό διάστημα (ακόμα και για χρόνια) σε σύγκριση με τις προηγούμενες του εκδόσεις. Η δυνατότητα χορικής του κάλυψης (περίπου 100 μέτρα) είναι δέκα φορές πιο μεγάλη από το κλασικό Bluetooth και η καθυστέρηση του είναι 15 φορές μικρότερη. Το BLE μπορεί να λειτουργήσει με ισχύ μετάδοσης από 0,01 mW μέχρι 10 mW. Λόγω αυτών των χαρακτηριστικών το Bluetooth Χαμηλής Ενέργειας είναι ένας καλός υποψήφιος για εφαρμογές IoT [27][28]. Το πρότυπο BLE αναπτύχθηκε με πολύ γρήγορους ρυθμούς από τους κατασκευαστές έξυπνων τηλεφώνων και είναι πλέον διαθέσιμο στα περισσότερα μοντέλα έξυπνων συσκευών. Η δυνατότητα χρήσης του πρωτοκόλλου αυτού χρησιμοποιείται για επικοινωνίες μεταξύ οχημάτων καθώς και για Δίκτυα Ασύρματες Επικοινωνιών[27][29]. Σε σύγκριση με το ZigBee, το BLE είναι πιο αποτελεσματικό όσον αφορά την κατανάλωση ενέργειας και την αναλογία μετάδοσης ενέργειας ανά μεταδιδόμενο κομμάτι [30]. Η στοίβα δικτύου του BLE έχει ως εξής: στο χαμηλότερο επίπεδο της υπάρχει φυσικό επίπεδο που μεταδίδει και λαμβάνει bits. Πάνω από το φυσικό επίπεδο, υπάρχουν οι υπηρεσίες του επιπέδου συνδέσμων που περιλαμβάνουν τη μεσαία πρόσβαση, την εγκαθίδρυση συνδέσεων, τον έλεγχο σφαλμάτων και την παροχή ελέγχου ροής. Στη συνέχεια, υπάρχει το επίπεδο Ελέγχου Λογικής Σύνδεσης και το πρωτόκολλο προσαρμογής (L2CAP) που παρέχουν την πολυπλεξία για τα κανάλια δεδομένων, τον κατακερματισμό και την επανασυναρμολόγηση των μεγαλύτερων πακέτων. Τα υπόλοιπα πιο πάνω επίπεδα είναι το Γενικό Πρωτόκολλο Χαρακτηριστικών (GATT) το οποίο παρέχει αποτελεσματική συλλογή δεδομένων από αισθητήρες και το Γενικό Πρωτόκολλο Πρόσβασης (GAP) το επιτρέπει στην εφαρμογή να διαμορφώνεται και να λειτουργεί σε διαφορετικές μορφές, όπως η διαφήμιση ή η σάρωση, η έναρξη σύνδεσης και η διαχείριση της σύνδεσης. Το BLE επιτρέπει στις συσκευές να λειτουργούν ως “κύριοι” ή “σκλάβοι” σε μία τοπολογία αστέρα. Για το μηχανισμό ανακάλυψης, οι “σκλάβοι” στέλνουν διαφημίσεις σε ένα ή περισσότερα κανάλια διαφήμισης. Για να ανακαλυφθούν ως “σκλάβοι”, τα κανάλια αυτά σαρώνονται από τις “κύριες” συσκευές. Οι συσκευές βρίσκονται σε κατάσταση αναστολής λειτουργίας εκτός από την ώρα που οι δύο συσκευές ανταλλάσσουν δεδομένα.
5. EPCglobal

   Ο Electronic Product Code(EPC) είναι ένας μοναδικός αναγνωριστικός αριθμός που αποθηκεύεται σε μία ετικέτα RFID και ουσιαστικά χρησιμοποιείται στη διαχείριση της αλυσίδας εφοδιασμού για την ταυτοποίηση αντικειμένων. Το EPCglobal ως ο αρχικός

υπεύθυνος οργανισμός για την ανάπτυξη του EPC, διαχειρίζεται τις τεχνολογίες των προτύπων EPC και RFID. Η υποκείμενη αρχιτεκτονική χρησιμοποιεί τις διαδικτυακές RFID τεχνολογίες μαζί με φθηνές ετικέτες και αναγνώστες RFID για να μοιράζονται πληροφορίες σχετικά με τα προϊόντα [31]. Αυτή η αρχιτεκτονική αναγνωρίζεται ως μία πολλά υποσχόμενη τεχνική για το μέλλον του IoT λόγω του ανοίγματος της, της επεκτασιμότητας, της διαλειτουργικότητας και της αξιοπιστίας της πέρα από την υποστήριξή της στις βασικές ανάγκες του IoT όπως τα αναγνωριστικά αντικειμένων και ο εντοπισμός υπηρεσίας. Τα EPC ταξινομούνται σε τέσσερις τύπους: 96-bit, 64-bit (I), 64-bit (II) και 64-bit (III). Όλοι οι τύποι EPC 64-bit υποστηρίζουν περίπου 16.000 εταιρείες με μοναδική ταυτότητα, καλύπτουν 1 έως 9 εκατ. προϊόντα τύπου Lion και 33 εκατομμύρια σειριακούς αριθμούς για κάθε τύπο προϊόντος. Ο τύπος 96-bit υποστηρίζει περίπου 268 εκατομμύρια εταιρείες με μοναδικές ταυτότητες, 16 εκατομμύρια κλάσεις προϊόντων και 68 δις σειριακούς αριθμούς για κάθε τάξη. Το σύστημα RFID χωρίζεται σε δύο βασικά στοιχεία: τον αναμεταδότη ραδιοκυμάτων (ετικέτα) και τον αναγνώστη ετικετών. Η ετικέτα αποτελείται από δύο συστατικά: ένα τσιπ για την αποθήκευση της μοναδικής ταυτότητας του αντικειμένου και μία κεραία για να επιτρέψει στο τσιπ να επικοινωνήσει με τον αναγνώστη ετικέτας χρησιμοποιώντας ραδιοκύματα. Ο αναγνώστης ετικετών δημιουργεί μία περιοχή ραδιοσυχνοτήτων για την αναγνώριση αντικειμένων μέσω των ανακλώμενων ραδιοκυμάτων της ετικέτας. Η λειτουργία RFID στέλνει τον αριθμό της ετικέτας στον αναγνώστη της ετικέτας χρησιμοποιώντας ραδιοκύματα. Μετά από αυτό, ο αναγνώστης διαβιβάζει αυτόν τον αριθμό σε μία συγκεκριμένη υπολογιστική εφαρμογή που ονομάζεται Υπηρεσίες Ονομασίας Αντικειμένων (ONS). Ένα ONS αναζητά τα στοιχεία της ετικέτας σε μία βάση δεδομένων, όπως το πότε και το πού έχει κατασκευαστεί. Το EPC Global Network μπορεί να χωριστεί σε πέντε μέρη: στο EPC, στο σύστημα ταυτότητας, στο ενδιάμεσο λογισμικό EPC, στις Υπηρεσίες Ανακάλυψης και στις Υπηρεσίες Πληροφοριών EPC. Το EPC ως μοναδικός αριθμός σε αντικείμενα, αποτελείται από δύο μέρη. Το σύστημα ταυτοποίησης συνδέει τις ταυτότητες του EPC σε μία βάση δεδομένων χρησιμοποιώντας EPC αναγνώστες μέσω του middleware. Η υπηρεσία εντοπισμού είναι ο μηχανισμός του EPCglobal για την εύρεση των απαιτούμενων δεδομένων από τις ετικέτες χρησιμοποιώντας το ONS. Η δεύτερη γενιά ετικετών EPC (αποκαλούμενες ετικέτες Gen 2), που ξεκίνησε στα μέσα του 2006, στοχεύει στην κάλυψη προϊόντων διαφορετικών εταιρειών σε παγκόσμια κλίμακα. Μία ετικέτα Gen 2 παρέχει καλύτερες υπηρεσίες στους πελάτες σε σύγκριση με την πρώτη γενιά ετικετών (γνωστή ως παθητική RFID) σε χαρακτηριστικά όπως: διαλειτουργικότητα κάτω από ετερογενή αντικείμενα, υψηλή απόδοση για όλες τις απαιτήσεις, υψηλή αξιοπιστία και φθηνές ετικέτες και αναγνώστες.

6. LTE-A (Μακροπρόθεσμη Εξέλιξη-Ανεπτυγμένη)

   Το LTE-A περιλαμβάνει ένα σύνολο κυψελωτών πρωτοκόλλων επικοινωνίας που ταιριάζουν καλά με τις επικοινωνίες τύπου μηχανής (MTC) και τις δομές IoT ειδικά για έξυπνες πόλεις όπου αναμένεται μακροπρόθεσμη αντοχή για τις υποδομές. Επιπλέον, υπερέχει άλλες λύσεις τύπου κυψέλης όσον αφορά το κόστος υπηρεσίας και την επεκτασιμότητα. Στο φυσικό επίπεδο, το LTE-A χρησιμοποιεί ορθογώνιο διαιρέτη συχνότητας (OFDMA) μέσω της οποίας το εύρος ζώνης του καναλιού χωρίζεται σε μικρότερες ζώνες που ονομάζονται μπλοκ φυσικών πόρων (PRB). Επίσης το LTE-A χρησιμοποιεί μία τεχνική εξάπλωσης φάσματος φορέα πολλαπλών συστατικών (CC) η οποία επιτρέπει τη χρήση μέχρι και πέντε ζωνών των 20-MHz. Η αρχιτεκτονική του

δικτύου LTE-A στηρίζεται σε δύο βασικά μέρη. Το πρώτο είναι το Δίκτυο Κορμού (CN) το οποίο ελέγχει τις κινητές συσκευές και ασχολείται με τις ροές των πακέτων IP. Το άλλο μέρος είναι το Δίκτυο Πρόσβασης Ραδιοφώνου (RAN) το οποίο διαχειρίζεται την ασύρματη επικοινωνία και την πρόσβαση στο ραδιόφωνο και εγκαθιδρύει πρωτόκολλα επιπέδου χρήστη και επιπέδου ελέγχου. Το RAN αποτελείται κυρίως από βάσεις σταθμούς (που ονομάζονται επίσης εξελιγμένοι NodeBs) που είναι συνδεδεμένοι μεταξύ τους με τη διεπαφή X2 . Το RAN και το CN είναι συνδεδεμένα μέσω της διεπαφής S1. Οι συσκευές κινητής τηλεφωνίας ή συσκευές MTC μπορούν να συνδεθούν με τους σταθμούς βάσης απευθείας μέσω της πύλης MTC (MTCG). Επίσης μπορούν να έχουν άμεση επικοινωνία με άλλες συσκευές MTC. Ωστόσο, το πρωτόκολλο αυτό έχει να αντιμετωπίσει προκλήσεις όπως υψηλή δικτυακή συμφόρηση όταν μεγάλος αριθμός συσκευών εισέρχονται στο δίκτυο. μία άλλη πρόκληση είναι ότι μπορεί να διακυβευτεί η QoS όταν συσκευές MTC προσπαθήσουν να έχουν πρόσβαση στο δίκτυο μέσω επιλογής eNB ή MTCG.

7. Z-Wave

   Το Z-Wave ως πρωτόκολλο ασύρματης επικοινωνίας χαμηλής ενεργειακής κατανάλωσης για οικιακά δίκτυα αυτοματισμού έχει ευρέως χρησιμοποιηθεί για εφαρμογές τηλεχειρισμού σε έξυπνα σπίτια [32]. Αυτό το πρωτόκολλο είχε αρχικά αναπτυχθεί από την ZenSys (επί του παρόντος Sigma Designs) και αργότερα χρησιμοποιήθηκε και αναπτύχθηκε από τη Z-Wave Alliance. Το Z-Wave μπορεί να καλύψει περίπου 30 μέτρα επικοινωνία από σημείο προς σημείο και έχει ειδικά αναπτυχθεί για εφαρμογές που απαιτούν περιορισμένη μετάδοση δεδομένων όπως ο έλεγχος του φωτός, ο έλεγχος οικιακών συσκευών, η έξυπνη ενέργεια και ο έλεγχο πρόσβασης HVAC, φορετό σύστημα ελέγχου υγείας και ανίχνευση πυρκαγιάς. Το Z-Wave λειτουργεί σε ζώνες ISM (περίπου 900 MHz) και επιτρέπει ταχύτητα μετάδοσης 40 kbps. Οι πρόσφατες εκδόσεις υποστηρίζουν επίσης μέχρι 200 kbps. Το επίπεδο MAC διαθέτει μηχανισμό αποφυγής συγκρούσεων. Η δυνατότητα αποστολής προαιρετικών μηνυμάτων τύπου ACK εγγυάται αξιόπιστη μετάδοση των πακέτων. Η αρχιτεκτονική του πρωτοκόλλου, διαθέτει δύο είδη κόμβων, τους ελεγκτές και τους «σκλάβους». Οι ελεγκτές διαχειρίζονται τους σκλάβους στέλνοντας εντολές προς αυτούς. Για σκοπούς δρομολόγησης, ο ελεγκτής διατηρεί έναν πίνακα ολόκληρης της τοπολογίας του δικτύου. Η δρομολόγηση σε αυτό το πρωτόκολλο εκτελείται με τη μέθοδο δρομολόγησης πηγής, στην οποία ο ελεγκτής υποβάλλει τη διαδρομή μέσα σε ένα πακέτο. Οι αναφορές μέχρι τώρα υποδεικνύουν ότι η απόδοση του πρωτοκόλλου Z-Wave είναι πιο αποτελεσματική από αυτήν του ZigBee [33].

3.5 Επιθέσεις Άρνησης Εξυπηρέτησης στο IoT

Η ασφάλεια παρουσιάζει σημαντική πρόκληση για την εφαρμογή του IoT λόγω της έλλειψης κοινού προτύπου και αρχιτεκτονικής για την ασφάλεια του IoT. Σε ετερογενή δίκτυα, όπως στην περίπτωση του IoT, δεν είναι εύκολο να διασφαλιστεί η ασφάλεια και η ιδιωτικότητα των χρηστών. Η βασική λειτουργικότητα του IoT βασίζεται στην ανταλλαγή πληροφοριών μεταξύ δισεκατομμυρίων έως μέχρι και τρισεκατομμυρίων αντικειμένων συνδεδεμένα στο Διαδίκτυο. Μερικά από τα μεγαλύτερα προβλήματα που απειλούν την ασφάλεια του IoT είναι η διασφάλιση του απορρήτου καθώς οι λειτουργίες πρόσβασης μεταξύ συσκευών IoT χωρίς παρεμβολές. Η εξασφάλιση ασφαλής ανταλλαγής δεδομένων είναι απαραίτητη για να αποφευχθεί η απώλεια ή η υπονόμευση της ιδιωτικής ζωής. Ένας κατασκευαστής μπορεί απλά να επιτρέπει την ανάγνωση

των δεδομένων ενώ ένας άλλος να επιτρέπει μέχρι και τον έλεγχο της συσκευής. Λόγω του γεγονότος αυτού έχουν προταθεί ορισμένες λύσεις όπως η ομαδοποίηση των ενσωματωμένων συσκευών σε εικονικά δίκτυα και κάθε συσκευή θα υπάρχει μόνο σε ένα εικονικό δίκτυο. μία άλλη προσέγγιση είναι να υποστηριχθεί ο έλεγχος πρόσβασης στο επίπεδο εφαρμογών με βάση τον κατασκευαστή [34].

3.6 Επιθέσεις Άρνησης Εξυπηρέτησης και απειλές της ασφάλειας στο IoT

Οι Επιθέσεις Άρνησης Εξυπηρέτησης στο IoT καθιστά μία μορφή απειλής της οποίας τα αποτελέσματα είναι σοβαρά, εμφανή και κάποιες φορές μη αναστρέψιμα. Η φύση των επιθέσεων αυτών, τις κάνει πολύ πιο δύσκολα αντιμετωπίσιμες γεγονός που αυξάνει τη σημαντικότητα της ενίσχυσης της ασφάλειας στο IoT. Οι υπάρχων τεχνικές ασφάλειας μπορούν να χρησιμοποιηθούν εν μέρη με κάποια ενίσχυση και αναβάθμιση, παρόλα αυτά καινούργιες τεχνικές και μέθοδοι είναι αναγκαίες για να αντιμετωπίσουν τις καινούργιες απειλές. Μερικές από τις υπάρχουσες απειλές όπως εν μέρη και οι προτεινόμενες λύσεις παρουσιάζονται παρακάτω:

1. Επιθέσεις DTLS DoS και αντιμετώπιση τους με τη χρήση cookies
   Λόγω της φύσης του πρωτοκόλλου UDP που δεν βασίζεται σε διαδικασία σύνδεσης πριν την έναρξη αποστολής πληροφοριών μέσω δύο κόμβων, το DTLS, είναι ευάλωτο σε αρκετές επιθέσεις άρνησης παροχής υπηρεσιών. Για να μετριαστεί αυτή η απειλή, η χειραψία του DTLS έχει επεκταθεί με μία τεχνική ανταλλαγής cookies. Συγκεκριμένα, το αντικείμενο πελάτης αποστέλλει ένα πακέτο ClientHello προς το διακομιστή με σκοπό την έναρξη ανταλλαγής πληροφοριών. Πριν ο διακομιστής διαθέσει τους κατάλληλους πόρους για μία νέα διασύνδεση με τον πελάτη, ο πελάτης πρέπει να αποδείξει την ικανότητά του να λαμβάνει πακέτα που απευθύνονται στη συγκεκριμένη IP διεύθυνση που δήλωσε. Αυτό γίνεται με την αναπαραγωγή cookies που παρέχει ο διακομιστής μέσω ενός είδος μηνύματος επονομαζόμενο ως HelloVerifyRequest όπου περιέχει ένα νέο cookie, του οποίου η διαδικασία παραγωγής δεν πρέπει να καταναλώνει τους πόρους του διακομιστή.. Με τη λήψη του HelloVerifyRequest, ο πελάτης αναμεταδίδει το ClientHello με το ληφθέν cookie. Τέλος, ο διακομιστής μπορεί να επαληθεύσει το cookie και να προχωρήσει με τη χειραψία[43].
2. Πρωτόκολλο ταυτοποίησης στοιχείων TESLA για αντιμετώπιση επιθέσεων ως προς την ασφάλεια των δεδομένων
   Το IoT αναφέρεται σε μοναδικά αναγνωρίσιμα φυσικά αντικείμενα και τις εικονικές αναπαραστάσεις τους σε μία δομή Διαδικτυακού τύπου[37]. Τεχνολογίες όπως η RFID, οι ασύρματες επικοινωνίες μικρής εμβέλειας, ο εντοπισμός σε πραγματικό χρόνο και τα δίκτυα αισθητήρων γίνονται ολοένα και πιο διαδεδομένα, φέρνοντας το IoT σε εμπορική χρήση. Υπάρχει ένα ευρύ φάσμα δικτύων (WSNs, VANETs, RFID, Έξυπνων Τηλεφώνων κ.α.), τα οποία συμμετέχουν στην οικοδόμηση του IoT. Λόγω αυτού του τεράστιου εύρους φάσματος εφαρμογών, τα στοιχεία στο IoT, επικοινωνούν μέσω μηνυμάτων εκπομπής, τα οποία καθιστούν αποτελεσματική τη διάδοση των μηνυμάτων. Αντίστοιχα, η εξασφάλιση της ασφάλειας στο πρωτόκολλο επικοινωνίας εκπομπής έρχεται στο προσκήνιο της έρευνας. Η ασφάλεια των δεδομένων που διακινούνται σε ένα IoT δίκτυο είναι ένα σημαντικό και ευάλωτο ζήτημα αφού υπάρχει μια πληθώρα επιθέσεων που στοχεύει στην υποκλοπή των δεδομένων αυτών όπως είναι π.χ. η MITM.

Ένας άλλος τρόπος επίθεσης προς την διάδοση επικοινωνιών είναι με επίθεση στους διαύλους επικοινωνιών π.χ. με μια DoS επίθεση προς τις συμμετέχοντες συσκευές. Για να υλοποιηθεί μια τέτοια επίθεση, ο επιτιθέμενος πρέπει πρώτα να αποκτήσει πρόσβαση στο δίκτυο των συσκευών. Μια διαδεδομένη τεχνική απόκτησης πρόσβασης στο δίκτυο είναι η παράτυπη αντιγραφή της ταυτότητας μερικών από τις ήδη συμμετέχοντες οντότητες. Το TESLA (Πρωτόκολλο Αυθεντικοποίησης Χρονικά Αποτελεσματικό και Ανθεκτικό στις Απώλειες) είναι ένα ελαφρύ πρωτόκολλο επικοινωνίας μετάδοσης για τον έλεγχο της ταυτότητας της πηγής το οποίο μπορεί να αποτρέψει την υποκλοπή της ταυτότητας και να επιδείξει αντοχή σε DoS επιθέσεις. Χρησιμοποιεί ασύμμετρες κρυπτογραφικές και έχει σχεδιαστεί για τη μετάδοση ταυτότητας σε ασύρματα δίκτυα ad-hoc. Υπάρχουν δύο εκδόσεις επέκτασης του TESLA: TESLA ++ και μTESLA. Το TESLA ++ είναι ένα ανθεκτικό πρωτόκολλο προς επιθέσεις DoS το οποίο σχεδιάστηκε από την TESLA και για VANET. Μπορεί να ανεχθεί τόσο τις επιθέσεις στην υπολογιστική μονάδα των αντικειμένων όσο και στη μνήμη τους. Το μTESLA έχει σχεδιαστεί για WSNs και μπορεί να καλύψει τις απαιτήσεις περιορισμού της ενέργειας στα WSNs. Είναι δύσκολο να γίνει ασφαλής η μετάδοση, επειδή: 1) τα πακέτα μπορεί να χαθούν, αλλά πολλές εφαρμογές μετάδοσης δεν μπορούν να τα αναμεταδίδουν, 2) οι δέκτες πρέπει συχνά να επεξεργάζονται τα δεδομένα τη στιγμή που φτάνουν τα πακέτα, αντί να τα βάζουν σε μία στοίβα αναμονής, 3) οι δέκτες είναι ετερογενείς, με πολύ διαφορετικό εύρος ζώνης και υπολογιστικούς πόρους 4) η ομάδα δεκτών μπορεί να είναι δυναμική, με τα μέλη που συμμετέχουν να έρχονται και να φεύγουν από την ομάδα ανά πάσα στιγμή. Οι τέσσερις χαρακτήρες ενός δικτύου εκπομπής δείχνουν ότι η επίθεση DoS είναι πολύ πιθανό να βλάψει το δίκτυο και να εκθέσει τη μετάδοση των μηνυμάτων στους επιτιθέμενους. Τόσο το TESLA ++ όσο και το μTESLA είναι τροποποιημένα σε σύγκριση με το TESLA. Ωστόσο, υπάρχουν πολλές διαφορές μεταξύ των δύο αυτών πρωτοκόλλων. Το TESLA ++ δεν μπορεί να ανταπεξέλθει στις απαιτήσεις του περιορισμού ενέργειας στο WSN. Από την άλλη το μTESLA δεν μπορεί να αντέξει την επίθεση DoS που βασίζεται στη μνήμη. Εάν ένα WSN χρειάζεται να επικοινωνεί με ένα VANET, για παράδειγμα, οι WSN σταθμοί βάσης είναι χρήσιμοι για την παρακολούθηση ατυχημάτων, όπου εδώ μπορεί να υπάρξει πρόβλημα πλήρης υλοποίησης της ασφάλειας μεταξύ των δύο.. Η κύρια ιδέα του πρωτοκόλλου TESLA είναι ότι ο αποστολέας επικολλά σε κάθε πακέτο ένα MAC που υπολογίζεται με ένα κλειδί *k* γνωστό μόνο στον εαυτό του. Ο δέκτης ρυθμίζει το ληφθέν πακέτο χωρίς να είναι σε θέση να το πιστοποιήσει. Λίγο αργότερα, ο αποστολέας αποκαλύπτει το κλειδί *k* και ο δέκτης μπορεί να πιστοποιήσει το πακέτο. Συνεπώς, αρκεί ένα ενιαίο MAC ανά πακέτο για την παροχή αυθεντικοποιημένης μετάδοσης, υπό τον όρο ότι ο δέκτης έχει συγχρονίσει το ρολόι του με αυτού του αποστολέα από πριν. Το TESLA είναι ανθεκτικό στις υπολογιστικές επιθέσεις DoS, αλλά είναι ευάλωτο σε επιθέσεις DoS που στοχεύουν στη μνήμη. Στο TESLA, για να αντιμετωπιστεί αυτή η DoS επίθεση που βασίζεται στη μνήμη, το TESLA ++ παρέχει τον ίδιο υπολογιστικό έλεγχο αποτελεσματικότητας ως TESLA με μειωμένες απαιτήσεις μνήμης.

3. Επιθέσεις Πλημμύρας Ενδιαφέροντος σε Δίκτυα Αντικειμένων βασισμένα σε ICN
   Η (ICN) είναι ένα σημαντικό πρότυπο δικτύωσης για το IoT. Το πρότυπο ICN εγγενώς διαθέτει κάποια χαρακτηριστικά ασφαλείας, αλλά φέρνει επίσης αρκετές ευπάθειες. Η σημαντικότερη από αυτές είναι οι Πλημμύρες Συμφερόντων, η οποία είναι ένας νέος τύπος επίθεσης DoS και έχει ακόμα πιο σοβαρές επιπτώσεις σε ολόκληρο το δίκτυο στο

ICN παρά στο παραδοσιακό πρότυπο IP. Ο μηχανισμός που προτείνεται για την άμβλυνση της επίθεσης πλημμύρας συμφερόντων βασίζεται στην ανίχνευση της επίθεσης και τον αντίστοιχο μετριασμό εφαρμόζοντας μέτρα στους δρομολογητές που βρίσκονται στα άκρα του δικτύου, καθώς είναι αυτοί που συνδέονται άμεσα με τους επιτιθέμενους. Χρησιμοποιώντας στατιστικά στοιχεία το ποσοστό ικανοποίησης στην εισερχόμενη διεπαφή κάποιων δρομολογητών στα άκρα, τα κακόβουλα ονόματα-προθέματα ή διεπαφές μπορούν να ανακαλυφθούν, και στη συνέχεια να μειωθεί ή να επιβραδυνθεί ανάλογα. Με τη βοήθεια των πληροφοριών του δικτύου, τα εντοπισμένα κακόβουλα ονόματα-προθέματα και οι διασυνδέσεις μπορούν επίσης να διανεμηθούν γρήγορα σε όλο το δίκτυο και η επίθεση μπορεί να μετριαστεί γρήγορα. Τα αποτελέσματα προσομοίωσης δείχνουν ότι ο προτεινόμενος μηχανισμός μπορεί να μειώσει την επίδραση των επιθέσεων Πλημμύρας συμφερόντων γρήγορα, και η απόδοση του δικτύου μπορεί να ανακάμψει αυτόματα στην κανονική κατάσταση χωρίς να βλάψει τους νόμιμους χρήστες.

4. Επιθέσεις Πλημμύρας σε IoT βασισμένα σε 6LoWPAN
   Οι IoT εφαρμογές του πρωτοκόλλου 6LoWPAN έχει κάποιες ελλείψεις όπως περιορισμένους πόρους από πλευράς ισχύος, επεξεργασίας, μνήμης, χώρου και αξιόπιστη επικοινωνία όσον αφορά το ποσοστό απώλειας και συγκρούσεων πακέτων [35]. Ένας αντίπαλος μπορεί να επωφεληθεί από αυτές τις αδυναμίες για να ξεκινήσει διαφορετικά είδη επιθέσεων. Πιο συγκεκριμένα, οι επιθέσεις άρνησης εξυπηρέτησης θεωρούνται ότι έχουν αρνητικές επιπτώσεις στη διατάραξη WSN επικοινωνιών. Οι παραδοσιακές λύσεις ασφάλειας που υπάρχουν ήδη στο κόσμο του IP όπως οι μηχανισμοί κρυπτογράφησης δεν είναι εφαρμόσιμες στις περιορισμένων δυνατοτήτων 6LoWPAN συσκευές. Τα δίκτυα αισθητήρων είναι ιδιαίτερα επιρρεπή σε επιθέσεις που σχετίζονται με την προστασία της ιδιωτικής ζωής, την ανάλυσης κυκλοφορίας, τις φυσικές επιθέσεις και κυρίως τις επιθέσεις DoS. Μία από τις επιθέσεις αυτές, είναι η DoS στο επίπεδο MAC του δικτύου όπου στοχοποιείται ο κόμβος της μονάδας παροχής ρεύματος του αισθητήρα. Αυτός ο τύπος επιθέσεων μπορεί να μειώσει τη διάρκεια ζωής του αισθητήρα από χρόνια σε ημέρες κάτι το οποίο θα έχει καταστροφικές επιπτώσεις στη δικτυακή ζωή του αισθητήρα. Το 6LoWPAN βρίσκεται ακόμη υπό εξέλιξη με τις σχετιζόμενες τεχνολογίες: Πρωτόκολλο Επιπέδου Περιορισμένης Εφαρμογής (CoAP) και Δρομολόγηση πάνω σε δίκτυα χαμηλής απώλειας ισχύος (RPL). Εκ φύσεως, οι συσκευές IoT δεν έχουν μόνο παθητικό ρόλο, αλλά και ενεργητικό. Μπορούν να χρησιμοποιηθούν στην απομακρυσμένη παρακολούθηση και εντοπισμό συσκευών, όπως επίσης στην παρακολούθηση της τοποθεσίας και τον προορισμό των χρηστών τους, κάτι το οποίο εισβάλλει στην ιδιωτική ζωή των χρηστών και συλλέγει ευαίσθητες πληροφορίες.
   Οι πληροφορίες αυτές θα μπορούσε να αξιοποιηθούν από τον επιτιθέμενο για διάφορους σκοπούς. Από αυτό το γεγονός προκύπτει ότι τα πρωτόκολλα που σχετίζονται με το 6LoWPAN θα πρέπει να αναλυθούν προσεκτικά για τυχόν ευπάθειες. Γενικά είναι δύσκολο να βρεθεί μία επίθεση DoS πριν από το σημείο όπου η υπηρεσία σταματήσει να είναι διαθέσιμη.
5. Επίθεση Καταστολής μηνυμάτων DIO με επανάληψη αποστολής πληροφοριών
   μία επίθεση καταστολής DIO, μπορεί να υποβαθμίσει σοβαρά την υπηρεσία δρομολόγησης στο RPL. Η επίθεση προκαλεί τους κόμβους του θύματος να καταστέλλουν τη μετάδοση των μηνυμάτων DIO, τα οποία είναι τα μηνύματα του RPL που είναι απαραίτητα για την κατασκευή της τοπολογίας δρομολόγησης[36]. Αυτό

προκαλεί μία γενική υποβάθμιση της ποιότητας των δρομολογίων που μπορεί να οδηγήσει, τελικά, σε κατατμήσεις δικτύων. Σε αντίθεση με άλλες επιθέσεις RPL, η επίθεση καταστολής DIO δεν απαιτεί ο αντίπαλος να δημιουργήσει ψευδή μηνύματα RPL. Αρκεί να αναπαράγει περιοδικά μηνύματα που έχουν ακουστεί προηγουμένως. Η επίθεση μπορεί έτσι να πραγματοποιηθεί χωρίς να κλέβονται κλειδιά κρυπτογράφησης από νόμιμους κόμβους. Η επίθεση καταστολής DIO χρησιμοποιεί την τεχνική επανάληψης, η οποία είναι μία κλασική τεχνική επίθεσης, για έναν ριζικά διαφορετικό σκοπό. Πράγματι, η τεχνική επανάληψης χρησιμοποιείται συνήθως για να κάνει το θύμα να δεχτεί παλιές πληροφορίες ως καινούργιες. Από την άλλη πλευρά, η επίθεση καταστολής DIO κάνει το θύμα να πιστεύει ότι οι πληροφορίες δρομολόγησης που πρόκειται να στείλει έχουν ήδη μεταδοθεί πολλές φορές από άλλους κόμβους. Η επίθεση υποβαθμίζει σοβαρά την υπηρεσία δρομολόγησης, και από ενεργειακής άποψης κοστίζει πολύ λιγότερο ενεργειακά από μία Επίθεση Παρεμβολών. Ο στόχος της επίθεσης καταστολής DIO είναι να διακόψει ή να επιβραδύνει τη μετάδοση των μηνυμάτων DIO στο δίκτυο. Σε αυτή την επίθεση, ο αντίπαλος μεταδίδει επανειλημμένα ένα μήνυμα DIO που θεωρείται συνεπές από τους κόμβους λήψης. Εάν οι κόμβοι λαμβάνουν αρκετά συνεπείς μηνύματα DIO, θα καταστείλουν τη δική τους μετάδοση μηνυμάτων DIO. Δεδομένου ότι τα μηνύματα DIO χρησιμοποιούνται έτσι ώστε οι κόμβοι να ανακαλύψουν τους γείτονες τους και την τοπολογία του δικτύου, η συνεχής καταστολή τους μπορεί να προκαλέσει ορισμένους κόμβους να παραμείνουν κρυμμένοι και ορισμένες διαδρομές να παραμείνουν ανεύρετες. Το αποτέλεσμα είναι μία γενική υποβάθμιση της ποιότητας των διαδρομών ή στην χειρότερη περίπτωση, την κατάτμηση του δικτύου. Ένας απλός τρόπος για να ξεκινήσει μία επίθεση καταστολής DIO είναι με την παρακολούθηση ενός μηνύματος DIO από έναν νόμιμο κόμβο και στη συνέχεια να επαναληφθεί πολλές φορές με μία σταθερή συχνότητα. Οι περιβάλλον νόμιμοι κόμβοι θα θεωρήσουν τα επαναλαμβανόμενα DIO ως συνεπή.

6. Επιθέσεις DoS στην αρχιτεκτονική του λειτουργικού συστήματος του δικτύου - Network Operating System(NOS)

   Επίθεση στις πηγές δεδομένων: Μία ή περισσότερες πηγές δεδομένων ενδέχεται να διακυβεύονται από μία κακόβουλη οντότητα που προσπαθεί να υπερχειλίσει το εύρος ζώνης ή το buffer της μνήμης τους[38]. Σε μία τέτοια κατάσταση, η ίδια η πλατφόρμα του IoT δεν θα επηρεαστεί άμεσα, αλλά ίσως μέρος της να πρέπει να απομονωθεί λόγω πιθανής εξάντλησης των πόρων δικτύου που εξαντλούνται από τέτοιους συμβιβασμένους κόμβους. Επιπλέον, ορισμένες υπηρεσίες θα επηρεαστούν, και δεν θα λαμβάνουν πλέον δεδομένα από αυτό το τμήμα του δικτύου. μίας τέτοιας μορφής επίθεση μπορεί να διεξαχθεί μέσω υπάρχων κοινών στρατηγικών, όπως έγχυση επιπλέον κυκλοφορίας στο δίκτυο, η εμπλοκή στη κυκλοφορία του δικτύου, η υποκλοπή δρομολογίων κλπ.

   Επίθεση στο NOS: Ένα ή περισσότερα NOS μπορεί να παραβιάζονται άμεσα από εξωτερικούς επιτιθέμενους κατά την εξάντληση των πόρων τους όσον αφορά την κατοχή μνήμης (δηλ. η μονάδα αποθήκευσης ακατέργαστων δεδομένων μπορεί να υπερχειλίσει), τον αριθμό των ταυτόχρονων συνδέσεων και το υπολογιστικό φορτίο. Εκτός αυτού τα NOS δεν θεωρούνται ως περιορισμένες συσκευές, οι πόροι τους είναι πολύτιμοι για να διασφαλιστεί η άμεση εξυπηρέτηση στους χρήστες. Για τους λόγους αυτούς, εάν ένα ή περισσότερα NOS λαμβάνουν ένα τεράστιο ποσό άχρηστων δεδομένων από μία κακόβουλη οντότητα (μεταμφιεσμένη σαν μή εγγεγραμμένη-καταχωρημένη πηγή) τότε οι υπολογιστικοί πόροι και οι πόροι μνήμης θα χρησιμοποιηθούν για άχρηστες

διεργασίες και τότε δεν θα μπορεί το σύστημα να παραδώσει έγκυρες πληροφορίες προς τους ενδιαφερόμενους χρήστες σε λογικό χρονικό διάστημα. μία τέτοια περίπτωση θα μπορούσε εύκολα να γίνει πραγματικότητα αφού

τα ΛΣΔ αντιμετωπίζουν τόσο τις εγγεγραμμένες όσο και τις μη καταχωρημένες πηγές (οι οποίες και οι δύο δικαιούνται εξίσου να συνδεθούν με το NOS) το ίδιο χωρίς την ανάγκη για έλεγχο ταυτότητας.

7. Επίθεση σκουληκοτρυπας

μία επίθεση σκουληκότρυπας είναι ένας ειδικός τύπος επίθεσης στα δίκτυα αισθητήρων, όπου δύο συνωστισμένοι κόμβοι που δρουν στο ρόλο του επιτιθέμενου, χρησιμοποιούν συνδέσμους σκουληκότρυπας για να καταγράψουν και να επαναλάβουν τα επικοινωνούντα μηνύματα προκειμένου για διαταράξουν το πρωτόκολλο δικτύου[39]. Για να ξεκινήσει μία επίθεση σκουληκότρυπας, οι δύο κακόβουλοι κόμβοι δημιουργούν μεταξύ τους έναν απευθείας δίαυλο επικοινωνίας παρακάμπτοντας τους διάφορους ενδιάμεσους κόμβους. Το καθιερωμένο κανάλι μπορεί να είναι ζεύξη επικοινωνίας υψηλής ταχύτητας εκτός ζώνης ή λογική σήραγγα μέσα στη ζώνη. Όταν δημιουργηθεί το κανάλι ο σύνδεσμος σκουληκότρυπας προσελκύει το μεγαλύτερο μέρος της κυκλοφορίας αφού τα πακέτα ελέγχου που διαπερνούν τη σκουληκότρυπα διαφημίζουν μία πολύ καλύτερη μετρική συνδέσμου. Η επιλογή τέτοιων συνδέσμων καταλήγει σε άρνηση εξυπηρέτησης, που επηρεάζει σοβαρά την απόδοση του δικτύου. Λόγω της φύσης της διαδικασίας ανάπτυξης, θεωρείται ότι κανένας κόμβος δεν χρήζει πλήρης εμπιστοσύνης αφού υπάρχει έλλειψη μοντέλου εμπιστοσύνης στο δίκτυο. Εκτός αυτού, οι κόμβοι δεν γνωρίζουν την πραγματική τους θέση και δεν είναι εξοπλισμένοι με εργαλεία επαλήθευσης της τοποθεσίας τους. Όταν ξεκινήσει μία επίθεση σκουληκότρυπας δημιουργείται ένας σύνδεσμος από κακόβουλους κόμβους. Ένας από αυτούς τους δύο κόμβους διαφημίζει μία σύνδεση με χαμηλή μετρική και προσελκύει την κυκλοφορία που προέρχεται από τους γειτονικούς κόμβους. Το επόμενο βήμα αυτού του κόμβου είναι το άλλο άκρο του συνδέσμου της σκουληκότρυπας. Στην πραγματικότητα όμως, οι κακόβουλοι κόμβοι δεν είναι γείτονες. Ως αποτέλεσμα, η κυκλοφορία του δικτύου παρακάμπτεται μέσω του συνδέσμου της σκουληκότρυπας και χάνεται. Οι κακόβουλοι κόμβοι οι οποίο σχηματίζουν τη σύνδεση σκουληκότρυπας επιτρέπεται να μετακινούνται μέσα στο δίκτυο όπως και οι νόμιμοι κόμβοι. Αναλόγως των σκοπών του επιτιθέμενου η επίθεση αυτή μπορεί να οδηγήσει σε εξάντληση των πόρων του συστήματος, απόκτηση μη εξουσιοδοτημένης πρόσβασης σε τομείς του δικτύου και σε παρεμπόδιση της δρομολόγησης στο δίκτυο.

Πλημμύρα Πακέτων Αναγνώρισης

Οι αλγόριθμοι δρομολόγησης σε συστήματα που βασίζονται σε αισθητήρες χρειάζονται αναγνωρίσεις από καιρό σε καιρό. Σε αυτό το είδος επίθεσης άρνησης παροχής υπηρεσιών, ένας κακόβουλος κόμβος στέλνει ψευδείς πληροφορίες στους γειτονικούς κόμβους με τη βοήθεια αυτών των αναγνωρίσεων. Μία από αυτές τις περιπτώσεις είναι αυτή της τριμερούς χειραψίας TCP με τη χρήση πακέτων SYN,ACK και SYN/ACK[40].

8. Επίθεση DoS με βάση το μονοπάτι

Σε αυτόν τον τύπο επιθέσεων DoS, ο επιτιθέμενος κυριεύει τους κόμβους των αισθητήρων από μεγάλες αποστάσεις, με το να πλημμυρίζει τα μονοπάτια επικοινωνίας πολλαπλών αναπηδήσεων από-άκρο-σε-άκρο, είτε με πακέτα που έχουν επαναληφθεί είτε με παρωχημένα πακέτα που έχουν εγχυθεί στο δίκτυο. Αυτή η επίθεση καταναλώνει το εύρος ζώνης του δικτύου και επιτυγχάνει την εξάντληση της ενέργειας των κόμβων. Ο

συνδυασμός ελέγχου και αντικατάστασης ταυτότητας πακέτων μπορεί να αποτρέψει την επίθεση DoS που βασίζεται σε μονοπάτια. Σε αυτή την τεχνική ένας αντίπαλος εγχέει επαναλαμβανόμενα πακέτα για να πλημμυρίσει την επικοινωνία από άκρο σε άκρο μεταξύ δύο κόμβων, κάθε κόμβος στο μονοπάτι προς το σταθμό βάσης προωθεί το πακέτο, αλλά εάν αποστέλλεται μεγάλος αριθμός πλαστών πακέτων, τότε όλα αυτά θα γίνουν πλημμυρισμένα[41]. Επίσης για την αποτροπή μίας τέτοιας επίθεσης, ένας ενδιάμεσος κόμβος θα μπορούσε να βρίσκεται στη μέση και να ανιχνεύει ψεύτικα πακέτα ή πακέτα που έχουν επαναληφθεί και στη συνέχεια να τα απορρίπτει. Ένας τρόπος για την ανίχνευση παρωχημένων πακέτων είναι με το να δημιουργεί ο κόμβος πηγής ένα ξεχωριστό κοινόχρηστο κλειδί με άλλους κόμβους αισθητήρων στο μονοπάτι επικοινωνίας. Στη συνέχεια ο αποστολέας χρησιμοποιεί κάθε κλειδί για να παράγει χωριστά πληροφορίες πιστοποίησης / ακεραιότητας για κάθε πακέτο για να ικανοποιήσει κάθε κόμβο κατά μήκος της διαδρομής. Ωστόσο, το πολύ περιορισμένο μέγεθος πακέτου σε WSNs καθιστά δύσκολη την ενσωμάτωση τόσο μεγάλης ποσότητας πληροφοριών επαλήθευσης στο πακέτο του αποστολέα, π.χ. έναν κώδικα επαλήθευσης μηνυμάτων 8-byte (MAC)για κάθε κόμβο στη διαδρομή. Επιπλέον, αυτό επιβάλλει επιβάρυνση στον αποστολέα, ο οποίος πρέπει να γνωρίζει εκ των προτέρων κάθε κόμβο στη διαδρομή για να στείλει τις σχετικές πληροφορίες επαλήθευσης

9. Επιθέσεις Μαύρης τρύπας και Επιθέσεις Καταβόθρας

   Οι επιθέσεις αυτές εμπίπτουν στην κατηγορία των επιθέσεων στο επίπεδο του δικτύου, στις οποίες ο εισβολέας επιχειρεί να προσελκύσει όλη την κυκλοφορία προς το μέρος του, με ψευδείς πληροφορίες δρομολόγησης[42]. Οι σταθμοί βάσης είναι οι μόνοι δικαιολογημένοι καταβόθρες σε ασύρματο δίκτυο αισθητήρων. Ωστόσο, ο κακόβουλος κόμβος σχηματίζει μία μεταφορική καταβόθρα όπου είναι ιδιαίτερα ελκυστική στους περιβάλλοντες κόμβους σε σχέση με τον υφιστάμενο αλγόριθμο δρομολόγησης. Ο συμβιβασμένος κόμβος στην καρδιά της καταβόθρας μπορεί πλέον να εκτελεί επιλεκτική προώθηση ή επεξεργασία δεδομένων. Αυτή είναι μία σοβαρή απειλή για την ασφάλεια δεδομένου ότι τα πολύτιμα δεδομένα τροφοδοτούνται σε έναν κακόβουλο κόμβο ο οποίος προσποιείται ότι έχει μία εξαιρετικά υψηλής ποιότητας διαδρομή ή μία πιθανότερη συντομότερη διαδρομή προς το σταθμό βάσης. Ο σταθμός βάσης ενός WSN είναι τόσο απίστευτα ευάλωτος στις προσκρούσεις, καθώς διαθέτει πολλές δυνατότητες επικοινωνίας και επίσης, καθώς τα περισσότερα δίκτυα ακολουθούν μία μέθοδο προώθησης διαδρομής ελάχιστου κόστους. Η επίθεση καταβόθρας είναι μία μεγάλη απειλή για την ασφάλεια καθώς εκτός του οτι μπορεί να προκαλέσει την άρνηση παροχής υπηρεσιών στο δίκτυο λόγω της εξάντλησης των πόρων των συμμετεχόντων κόμβων αλλά και αυτές του δικτύου, ευαίσθητα δεδομένα καταλήγουν στα χέρια ενός κακόβουλου χρήστη. Η επίθεση Μαύρης Τρύπας δεν διαφέρουν σε τίποτα από την επίθεση Καταβόθρας εκτός από το γεγονός η επίθεση αυτή καταρρίπτει τα πακέτα άρα δεν γίνεται υποκλοπή δεδομένων.

ΕΝΟΤΗΤΑ 4

4.1 Περιγραφή διαδικασίας πειράματος

Στο πειραματικό μέρος προσομοιώνεται επίθεση DDoS χρησιμοποιώντας HTTP πακέτα. Το συγκεκριμένο περιβάλλον προσομοίωσης είναι ένα IoT δίκτυο συσκευών που συμμετέχουν στο ίδιο τοπικό δίκτυο. Οι οντότητες που χρησιμοποιούνται σαν συμβιβασμένες συσκευές θα μπορούσαν να είναι συσκευές που συμμετέχουν σε ένα IoT δίκτυο και χρησιμοποιούνται κακόβουλα λόγω του συμβιβασμού. Ο εξυπηρετητής αντιπροσωπεύει το κεντρικό κόμβο του δικτύου αυτού. Σε πραγματικά σενάρια, το δίκτυο αυτό θα μπορούσε να ήταν για παράδειγμα ένα IoT δίκτυο αισθητήρων σε απομακρυσμένη γεωγραφικά περιοχή. Σε αυτήν την περίπτωση ο εξυπηρετητής θα ήταν η πύλη προς τα ανώτερα επίπεδα της αρχιτεκτονικής του ευρύτερου δικτύου και οι επιτιθέμενοι θα μπορούσαν να αποτελούνταν από τις συσκευές-αισθητήρες. Ένα άλλο παράδειγμα πραγματικού σεναρίου θα μπορούσε το IoT δίκτυο αυτό να είναι ένα οικιακό δίκτυο το οποίο αποτελείται από οικιακές συσκευές και ένα κεντρικό κόμβο συνδεδεμένο με το Διαδίκτυο. Αναλόγως της φύσης του δικτύου και του σκοπού που εξυπηρετεί, θα χρησιμοποιείται και το ανάλογο πρωτόκολλο. Στην περίπτωση του πειράματος που προσομοιώνεται, οι συσκευές είναι δικτυακές οντότητες με τη δυνατότητα αποστολής HTTP πακέτων.

Ο επιτιθέμενος, εκμεταλλεύεται δικτυακές συσκευές τις οποίες έχει στη διάθεση του και τις χρησιμοποιεί για κακόβουλες ενέργειες. Οι συσκευές αυτές ανήκουν στο ίδιο τοπικό δίκτυο με τον εξυπηρετητή και ο επιτιθέμενος τις χρησιμοποιεί για αποστολή συνεχόμενων δικτυακών πακέτων HTTP- μέσω των συσκευών αυτών- χρησιμοποιώντας τη μέθοδο POST, χωρίς να αναμένει την αντίστοιχη απόκριση για κάθε απεσταλμένο πακέτο. Η ίδια μορφή επίθεσης μπορεί να υλοποιηθεί και με τη χρήση διαφορετικών δικτυακών πακέτων(ICMP, SIP κλπ) .

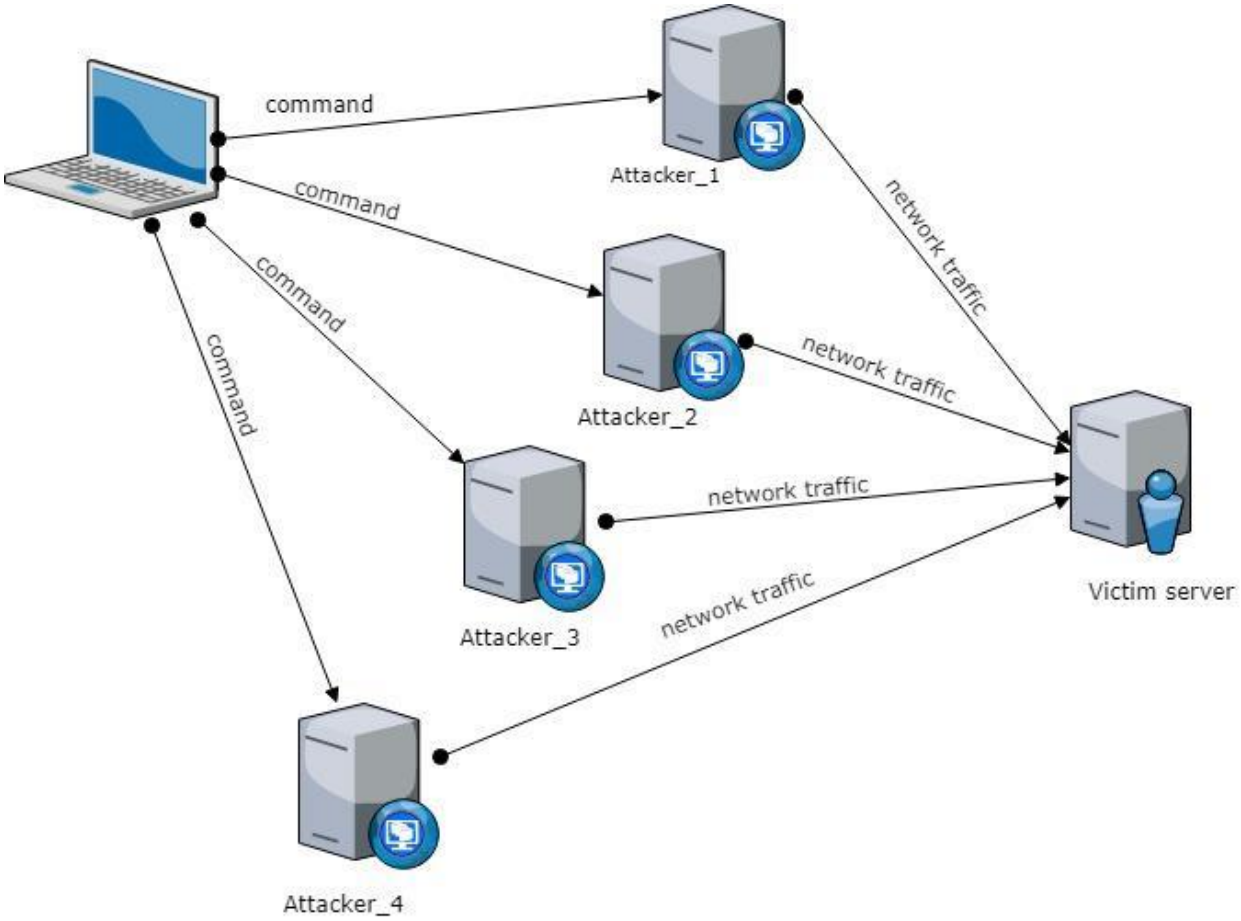
Η συγκεκριμένη διαδικασία, οδηγεί στην αδυναμία απόκρισης του αποδέκτη και κατ' επέκταση στην αδυναμία της αντίστοιχης παροχής υπηρεσιών. μία DDoS είναι μία προσπάθεια έτσι ώστε να φέρει το στόχο σε θέση να μην μπορεί να διαθέσει μία διαδικτυακή υπηρεσία, χάρη στην κυκλοφορία πακέτων που καταφθάνουν από πολλαπλές πηγές (σε κάποιες περιπτώσεις και από μία πηγή) με αποτέλεσμα η επεξεργαστική δυνατότητα του στόχου να εξαντλείται.

4.2 Συμβιβασμένες συσκευές και η χρήση τους

Στο πειραματικό κομμάτι της εργασίας, προσομοιώνεται DDoS επίθεση με χρήση δικτυακών οντοτήτων οι οποίες επιτίθενται αποστέλλοντας δικτυακά πακέτα προς τον εξυπηρετητή όπως φαίνεται στο σχήμα (i). Οι συμβιβασμένες δικτυακές οντότητες βρίσκονται στο ίδιο ιδιωτικό δίκτυο με τον εξυπηρετητή. Για χάρη της προσομοίωσης, ο κώδικάς έχει τοποθετηθεί στις οντότητες αυτές. Οι επιτιθέμενες οντότητες είναι αντικείμενα γλώσσας προγραμματισμού. Σε πραγματικό σενάριο, οι οντότητες θα είχαν συμβιβαστεί με την τοποθέτηση κώδικα χωρίς να είναι εις γνώσιν των φυσικών χρηστών τους ή του διαχειριστή τους. Ο χρήστης του προγράμματος εκκινεί τις οντότητες οι οποίες αποστέλλουν δικτυακά πακέτα HTTP POST προς τον εξυπηρετητή. Θεωρητικά, ο χρήστης εκκινεί όσες οντότητες χρειαστεί μέχρι ωσότου να καταναλώσει τους πόρους του εξυπηρετητή. Στη προσομοίωση εκκινείται η λειτουργία τεσσάρων επιτιθέμενων οντοτήτων. Οι συμμετέχοντες οντότητες επεξηγούνται καλύτερα στη

συνέχεια.

Για την υλοποίηση του πειράματος χρησιμοποιήθηκε το ενσωματωμένο περιβάλλον ανάπτυξης Netbeans και η γλώσσα προγραμματισμού Java. Για την παρατήρηση της απόδοσης/χρήσης του επεξεργαστή χρησιμοποιήθηκε το αντίστοιχο εργαλείο του Λειτουργικού Συστήματος Windows Task Manager/Performance. Για την υλοποίηση των εικονικών μηχανημάτων χρησιμοποιήθηκε το Εικονικό Περιβάλλον Oracle VM.

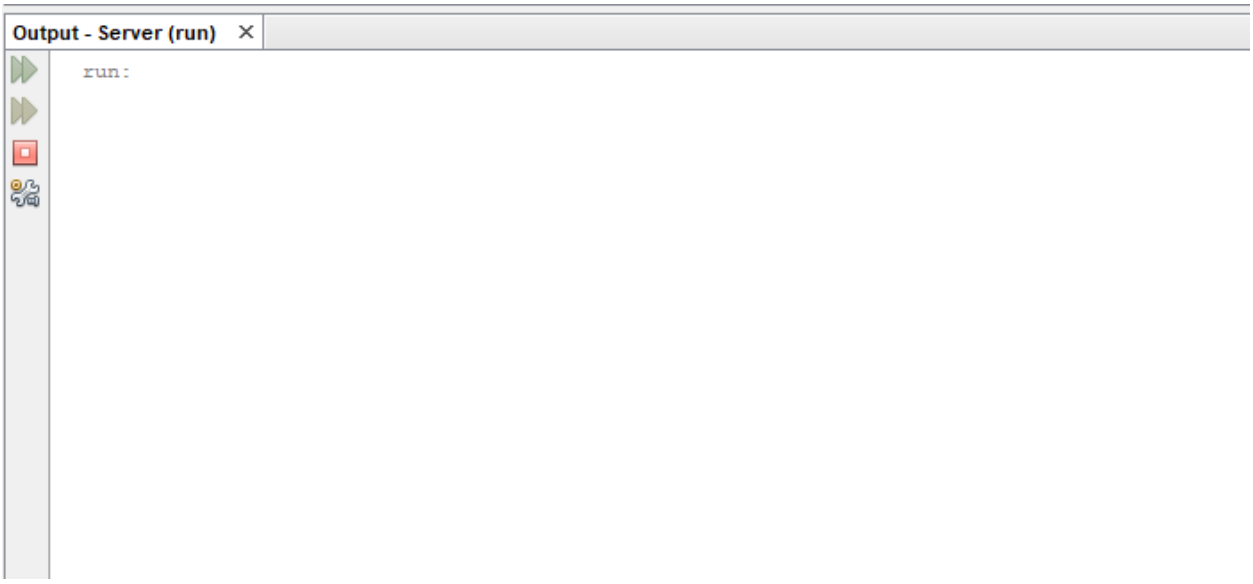


σχήμα i Γενικό σχεδιάγραμμα της δομής των δικτύων κατά τη διαδικασία της επίθεσης

4.3 Διαδικασία προσομοίωσης

Εξυπηρετητής-Server:

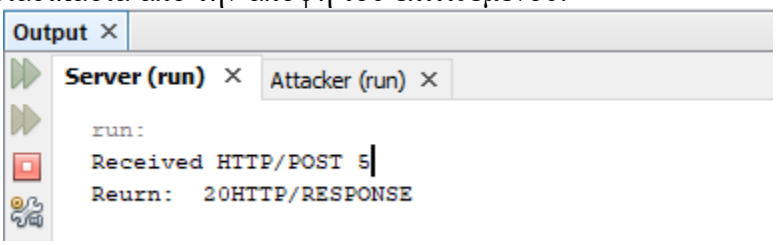
Αρχικά εκκινείται η λειτουργία του server-εξυπηρετητή ο οποίος ακούει στην πόρτα 80. Η συγκεκριμένη πόρτα είναι η προκαθορισμένη πόρτα για πακέτα HTTP. Το στιγμιότυπο στην σχήμα (j) απεικονίζει τη λειτουργία του εξυπηρετητή πριν την έναρξη οποιασδήποτε επίθεσης. Στο σημείο αυτό ο εξυπηρετητής είναι σε θέση να δεχτεί και να ανταποκριθεί σε εισερχόμενες συνδέσεις. Ο εξυπηρετητής χρησιμοποιεί την IP διεύθυνση 192.168.1.17.



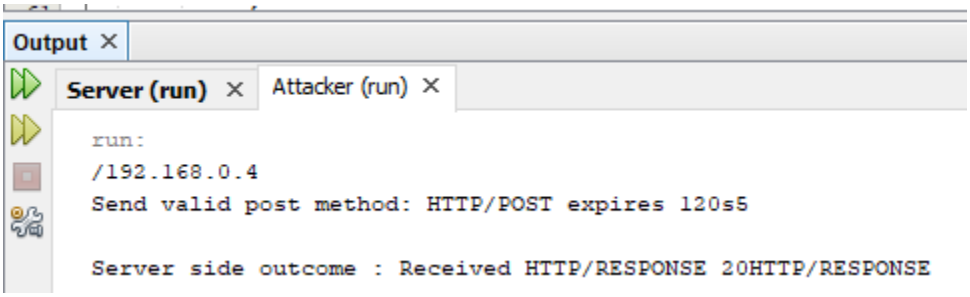
σχήμα j Στιγμιότυπο λειτουργίας εξυπηρετητή πριν την έναρξη της επίθεσης

Επιτιθέμενες οντότητες - Attacker, Attacker_2, Attacker_3, Attacker_4:

Οι οντότητες αυτές είναι εικονικά μηχανήματα που συμμετέχουν στο δίκτυο και αλληλοεπιδρούν με τον εξυπηρετητή φυσιολογικά. Το εικονικό κουτί που φιλοξενεί τα μηχανήματα βρίσκεται στον ίδιο υπολογιστή με τον εξυπηρετητή. Η κάθε οντότητα χρησιμοποιεί διαφορετική IP διεύθυνση. Οι οντότητες Attacker, Attacker_2, Attacker_3, Attacker_4 χρησιμοποιούν τις IP 192.168.1.13, 192.168.1.14, 192.168.1.15, 192.168.1.16 αντίστοιχα. Οι επιτιθέμενες οντότητες αποστέλλουν HTTP POST πακέτα στον εξυπηρετητή και ο εξυπηρετητής με τη σειρά του απαντά με HTTP Response πακέτα σαν απάντηση προς την πρόσκληση. Στα σχήματα (k, l) διαφαίνεται η διαδικασία αποστολής και απάντησης από και προς τον επιτιθέμενο και τον εξυπηρετητή. Στο σχήμα (k) αποτυπώνεται η διαδικασία, όπως αυτή διαφαίνεται από την άποψη του εξυπηρετητή και στο σχήμα (l) αποτυπώνεται η ίδια διαδικασία από την άποψη του επιτιθέμενου.

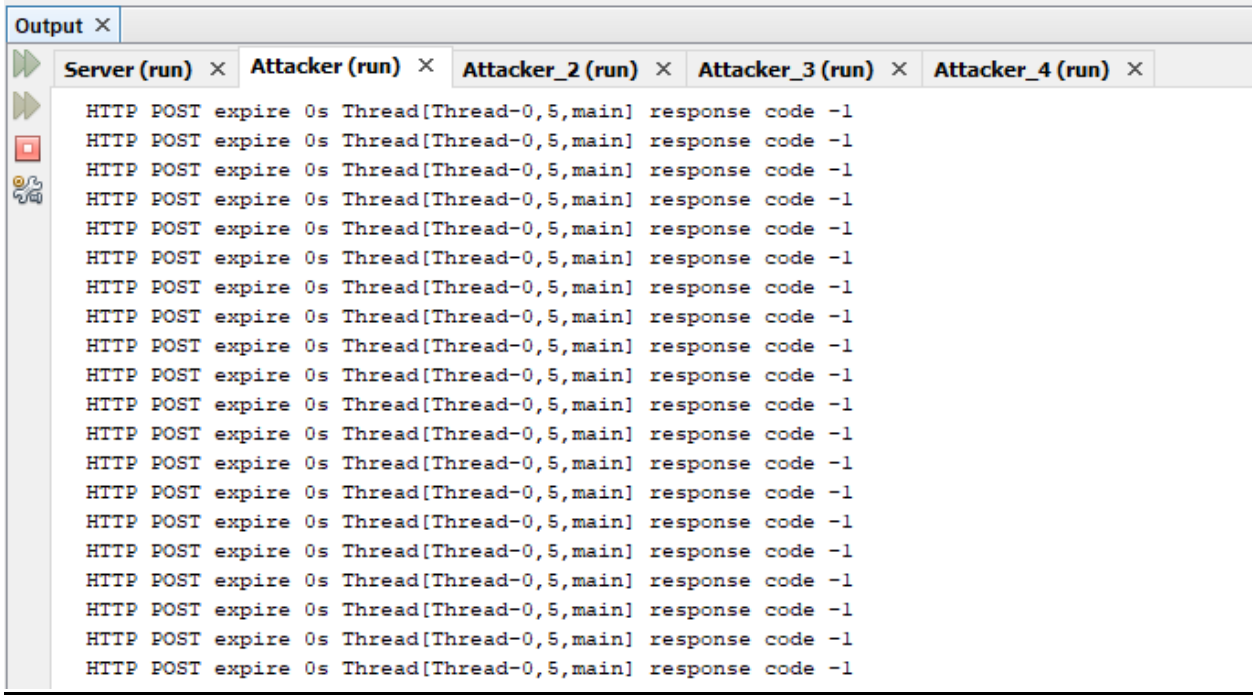


σχήμα k Άποψη αποστολής και εξυπηρέτησης πακέτων ως προς τον επιτιθέμενο



σχήμα l Άποψη αποστολής και εξυπηρέτησης πακέτων ως προς τον επιτιθέμενο

Έπειτα, οι οντότητες Attacker, Attacker_2, Attacker _3, Attacker_4 (εικόνες γ,δ,ε,ζ) οι οποίες αντιπροσωπεύουν τα εικονικά μηχανήματα, εξαπολύουν μία συνεχόμενη ροή πακέτων HTTP προς τον εξυπηρετητή μέχρι ο εξυπηρετητής να μην έχει τη δυνατότητα να αντιδράσει αφού θα έχουν εξαντληθεί όλοι οι αντίστοιχοι επεξεργαστικοί πόροι. Στο περιβάλλον προσομοίωσης, η εξάντληση αυτή διαφαίνεται από τα υψηλά επίπεδα χρήσης τα οποία φτάνει ο επεξεργαστής (100% απόδοσης/χρήσης) της συσκευής .

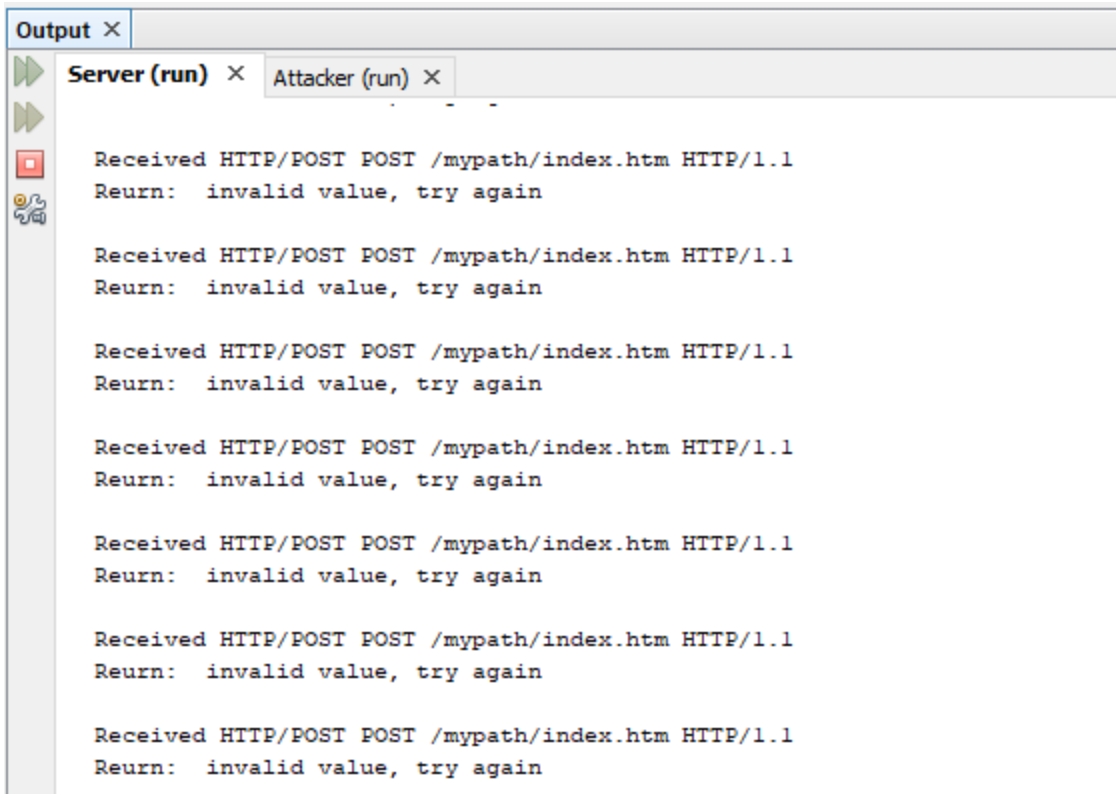


σχήμα m Αποστολή HTTP πακέτων POST από την άποψη της οντότητας Attacker

σχήμα n Αποστολή HTTP πακέτων POST από την άποωη της οντότητας Attacker_2

σχήμα ο Αποστολή πακέτων POST από την άποψη της οντότητας Attacker_3

σχήμα q Αποστολή HTTP πακέτων POST από την άποωη της οντότητας Attacker_4

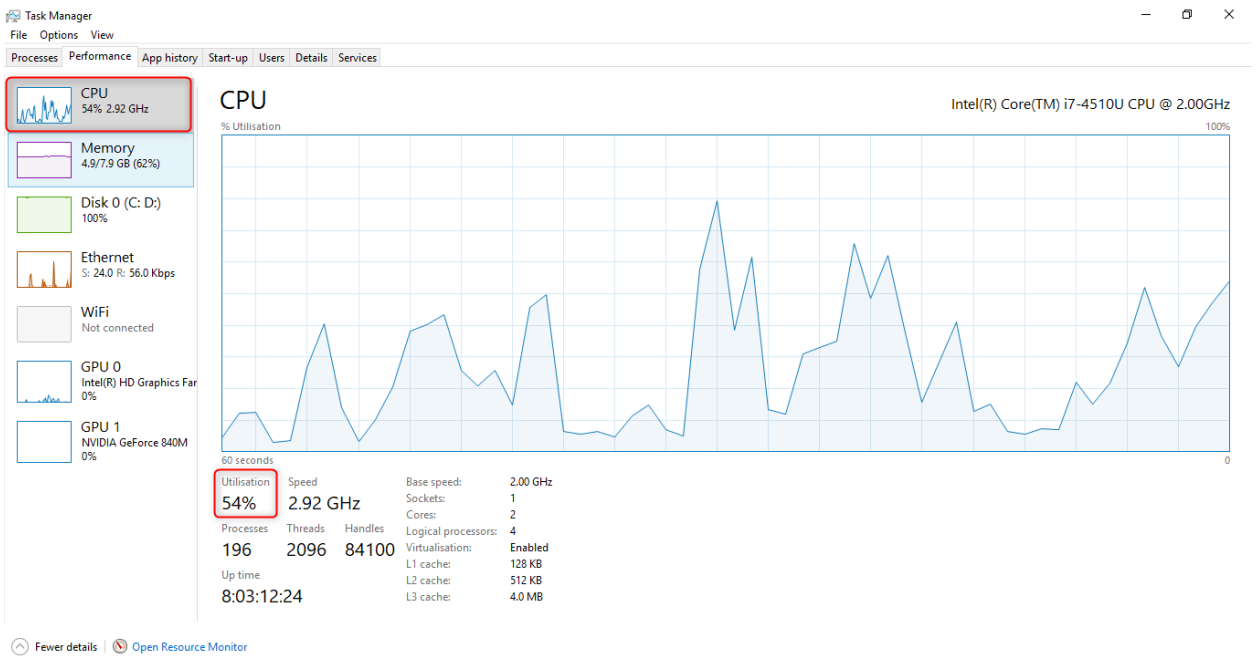


σχήμα r Παραλαβή και απάντηση πακέτων από την άποψη του εξυπηρετητή

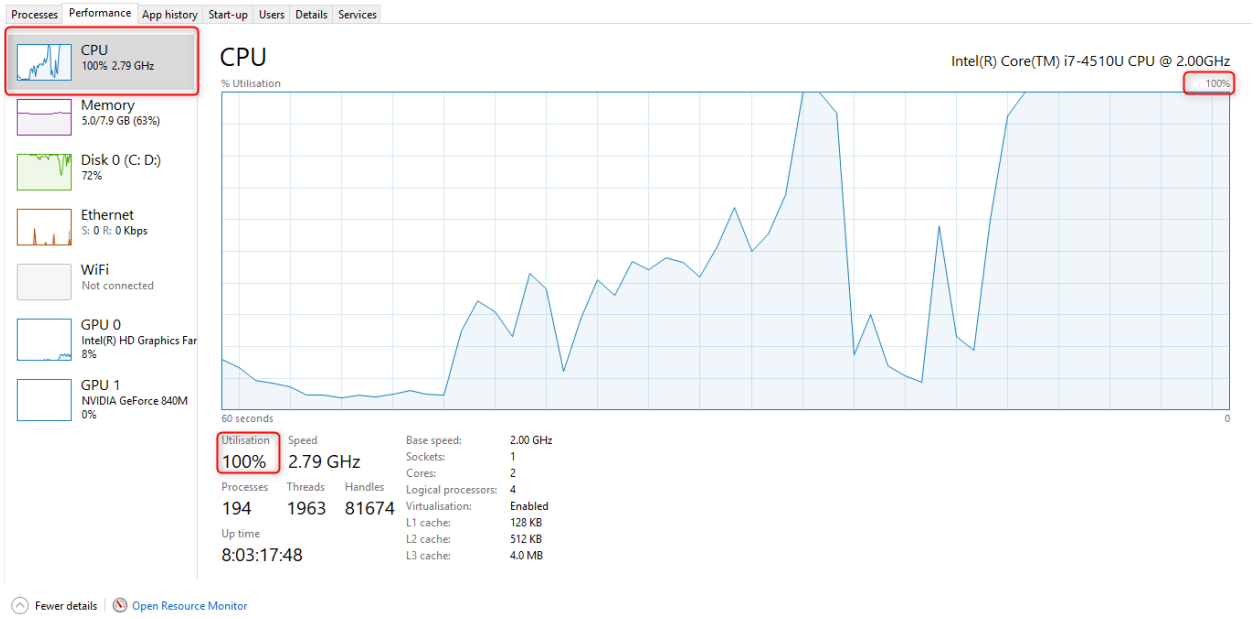
Στο σχήμα (q) παρατηρούνται τα πακέτα τα οποία καταφθάνουν στον εξυπηρετητή και το αντίστοιχο μήνυμα απόρριψης. Ο εξυπηρετητής, απορρίπτει τα πακέτα αυτά λόγω λανθασμένης σύνταξης καθώς τα πακέτα δεν περιέχουν τη τιμή Expires, η οποία καθορίζει το χρονικό διάστημα αποστολής του επόμενου πακέτου POST από το τελευταίο απεσταλμένο σε περίπτωση που δεν παραληφθεί απάντηση από τον διακομιστή.

4.4 Αποτελέσματα προσομοίωσης και επεξήγηση

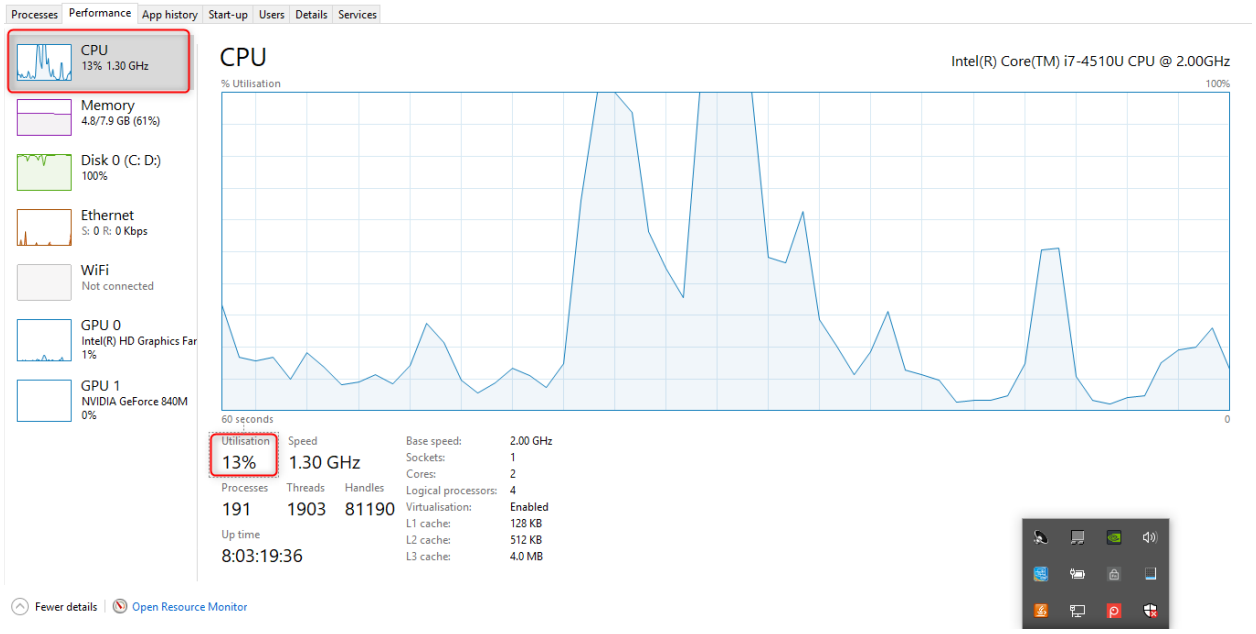
Όπως διαφαίνεται στα στιγμιότυπα από το διάγραμμα απόδοσης του επεξεργαστή, πριν την έναρξη της επίθεσης τα επίπεδα χρήσης του επεξεργαστή κινούνται σε φυσιολογικά επίπεδα. Τα επίπεδα χρησιμοποίησης/απόδοσης του επεξεργαστή κατά την ώρα της επίθεσης, έχουν φτάσει στο 100%. Το φαινόμενο αυτό παρατηρείται λόγω των πολλαπλών δικτυακών πακέτων που δέχεται ο υπολογιστής και στην αδυναμία του να τα επεξεργαστεί. Στα σχήματα (s, t, u) αντίστοιχα, βλέπουμε τα επίπεδα χρησιμοποίησης/απόδοσης πριν, κατά τη διάρκεια και μετά το πέρας της επίθεσης.



σχήμα s Επίπεδο χρήσης/απόδοσης ου επεξεργαστή πριν την έναρξη της επίθεσης



σχήμα t Επίπεδο χρήσης/απόδοσης του επεξεργαστή κατά τη διάρκεια της επίθεσης



σχήμα υ Επίπεδο χρήσης/απόδοσης του επεξεργαστή μετά το πέρας της επίθεσης

Ενότητα 5

5.1 Συμπεράσματα

Τα πειραματικά αποτελέσματα που έχει επιφέρει η προσομοίωση επίθεσης DDoS καταδεικνύουν την ευκολία με την οποία ένας κακόβουλος χρήστης μπορεί να δημιουργήσει μεγάλης κλίμακας επιπτώσεις σε ένα σύστημα ανεξαρτήτως των δυνατοτήτων και ικανοτήτων του συστήματος αυτού επίθεσης. Η ευκολία αυτή, σε συνάρτηση με τη ραγδαία ανάπτυξη και εφαρμογή της τεχνολογίας IoT εγείρει μεγάλες ανησυχίες για την ασφάλεια των συστημάτων και των προσωπικών δεδομένων των χρηστών. Οι πολλαπλές παράμετροι ασφάλειας, δηλαδή η ευκολία των επιθέσεων και η πληθώρα των τεχνικών, αναγκάζει τους κατασκευαστές και την επιστημονική κοινότητα να χρησιμοποιούν πολλές και ακόμη πιο πολύπλοκες δικλείδες ασφαλείας σε όλες τις δομές και τα επίπεδα ενός συστήματος (στην κατασκευή υλικού και πρωτόκολλα) κυρίως για την πρόληψη αλλά και την καταπολέμηση, με αποτέλεσμα να αυξάνεται ραγδαία το κόστος κατασκευής και διατήρησης των διαφόρων συστημάτων.

Μία άλλη παράμετρος που αυξάνει τη δυσκολία αντιμετώπισης των διαφόρων επιθέσεων, είναι η μεγάλη διαφορά αναγκαίας δυναμικότητας ανάμεσα σε θύμα και επιτιθέμενο. Πιο συγκεκριμένα, σε μία περίπτωση επίθεσης όπως η DDoS , ο αμυνόμενος χρειάζεται να έχει πολλαπλάσιους διατιθέμενους πόρους για να αμυνθεί από αυτούς που χρειάζεται ο επιτιθέμενος για να επιτεθεί. Θεωρητικά, με τα κατάλληλα εργαλεία και τη σωστή προεργασία, ο επιτιθέμενος μπορεί να εκκινήσει μία επίθεση προς ένα σύστημα με τεράστιες δυνατότητες μόνο με τη χρήση ενός προσωπικού υπολογιστή όπως π.χ., με τον έλεγχο δημόσιων DNS, συμβιβασμένων δικτυακών συσκευών κλπ. Επίσης η ευκολία που μπορεί να εξαπολύσει μία επίθεση είναι αρκετά μεγάλη καθώς απλά χρειάζεται ένα σχετικά καλό δίκτυο που μπορεί να διαχειριστεί την αποστολή πολλαπλών πακέτων και με την αναγκαία συχνότητα.

5.2 Μελλοντικές Επεκτάσεις

Το θεωρητικό κομμάτι της εργασίας δίνει μία γενική εικόνα της τεχνολογίας IoT ως προς τη δομή και τις απειλές που αντιμετωπίζει παρουσιάζοντας την αρχιτεκτονική δομή του IoT, τα πρωτόκολλα που χρησιμοποιούνται, τις οντότητες που συμμετέχουν και τις δυνατότητες τους. Επίσης παρουσιάζει τις κύριες τεχνικές και μεθόδους επιθέσεων που χρησιμοποιούνται με έμφαση στην DDoS επίθεση.

Σαν μελλοντική επέκταση η εργασία θα μπορούσε να επεκταθεί και να εστιάσει σε προβλήματα ασφαλείας συγκεκριμένου σημείου, όπως συγκεκριμένη μορφολογία δικτύου (π.χ., δίκτυο αισθητήρων, οικιακό δίκτυο κλπ), πρωτόκολλα που εξυπηρετούν συγκεκριμένη διαδικασία (π.χ. πρωτόκολλα διάδοσης), τεχνικές ασφάλειας (π.χ. αναδιοργάνωση και πιο έξυπνη χρήση υφιστάμενων τεχνικών, πρόταση καινούργιου πρωτοκόλλου, τεχνικής κλπ)
με σκοπό την εξαγωγή συμπερασμάτων για προβλήματα της συγκεκριμένης δομής.

Σε τρίτο στάδιο τα αποτελέσματα αυτά, τα οποία θα αποτελούν εξειδικευμένα συμπεράσματα, θα μπορούσαν να αποτελέσουν μία βάση για την δημιουργία προτάσεων επίλυσης ή και επίλυση με πρόταση/υλοποίηση νέου πρωτοκόλλου, τεχνικής, εργαλείου κλπ για την αντιμετώπιση και την ουσιαστική επίλυση του συγκεκριμένου ζητήματος ασφαλείας.

ΑΝΑΦΟΡΕΣ

[1] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[2]https://www.google.com/url?q=https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx&sa=D&ust=1549301186085000&usg=AFQjCNGxkL0pAQmZlGBMTOxwxa7lIaYArQ

[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash on Internet of Things: A survey on Enabling Technologies, Protocols, and Applications pp. 2350 section IV

[4] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiqui-tous computing and the

[5]R. Want, "An introduction to RFID technology," IEEE Pervasive Comput., vol. 5, no. 1, pp. 25–33, Jan.–Mar. 2006.

[6]R. Want, "Near field communication," IEEE Pervasive Comput., vol.10,no. 3, pp. 4–7, Jul./Sep. 2011.

[7] R. S. Kshetrimayum, "An introduction to UWB communication systems," IEEE Potentials, vol. 28, no. 2, pp. 9–13, Mar./Apr. 2009.

[8] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," IEEE Wireless Commun., vol. 12, no. 1, pp. 12–26, Feb. 2005.

[9]P. McDermott-Wells, "What is Bluetooth?" IEEE Potentials, vol. 23,no. 5, pp. 33–35, Jan. 2005.

[10] "Press releases detail: Bluetooth technology website," Bluetooth Tech-nol.Website,Kirkland,WA,USA,Sep.2014[Online].Available:http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=197

[11]IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std.

802. 15. 4-2011, 2011.

[12] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas,"LTE-Advanced:

Next-generation wireless broadband technology [In-vited Paper]," IEEE Wireless Commun., vol. 17, no. 3, pp. 10–22,Jun. 2010.

[13]pen Auto Alliance, Oct. 20, 2014. Available: http://www.openautoalliance.net/

[14]X. Xiaojiang, W. Jianli, and L. Mingdong, "Services and key technologies of the Internet of Things," ZTE Commun., Shenzhen, China, vol. 2,p. 011, 2010.

[15]M. Gigli and S. Koo, "Internet of Things: Services and applications categorization," Adv. Internet Things, vol. 1, no. 2, pp. 27–31, Jul. 2011.

[16]P. Barnaghi, W. Wang, C. Henson, and K. Taylor, "Semantics for the Internet of Things: Early progress and back to the future," Proc. IJSWIS, vol. 8, no. 1, pp. 1–21, Jan. 2012.

[17]Internet of Things: A Survey on Enabling Technologies, Protocols, and ApplicationsAla Al-Fuqaha, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, Mehdi Mohammadi, Student Member, IEEE, Mohammed Aledhari, Student Member, IEEE, and Moussa Ayyash, Senior Member, IEEE, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015

[18] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in Proc. 3rd Int. Conf. COMSWARE, 2008, pp. 791–798.

[19] C. Esposito, S. Russo, and D. Di Crescenzo, "Performance assessment of OMG compliant data distribution middleware," in Proc. IEEE IPDPS, 2008, pp. 1–8.

[20]A. J. Jara, P. Martinez-Julia, and A. Skarmeta, "Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service dis- covery for the web of things," in Proc. 6th Int. Conf. IMIS Ubiquitous Comput., 2012, pp. 731–738.

[21]. Klauck and M. Kirsche, "Chatty things—Making the Internet of Things readily usable for the masses with XMPP," in Proc. 8th Int. Conf. CollaborateCom, 2012, pp. 60–69.

[22] S. Cheshire and M. Krochmal, "Multicast DNS," Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6762, 2013.

[23] M. R. Palattella et al., "Standardized protocol stack for the Internet of (important) things," IEEE Commun. Surveys Tuts., vol. 15, no. 3,pp. 1389–1406, 3rd Quart. 2013.

[24] J. Ko et al., "Connecting low-power and lossy networks to the Internet," IEEE Commun. Mag., vol. 49, no. 4, pp. 96–101, Apr. 2011.

[25]J. W. Hui and D. E. Culler, “Extending IP to low-power, wireless personal area networks,” IEEE Internet Comput., vol. 12, no. 4, pp. 37–45,Jul./Aug. 2008.

[26]IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802. 15. 4-2011, 2011.

[27] R. Frank, W. Bronzi, G. Castignani, and T. Engel, “Bluetooth low energy: An alternative technology for VANET applications,” in Proc. 11th Annu. Conf. WONS, 2014, pp. 104–107.

[28] Decuir, “Introducing Bluetooth smart: Part 1: A look at both classic and new technologies,” IEEE Consum. Electron. Mag., vol. 3, no. 1, pp. 12–18, Jan. 2014.

[29]E. Mackensen, M. Lai, and T. M. Wendt, “Bluetooth low energy (BLE) based wireless sensors,” in IEEE Sens., 2012, pp. 1–4.

[30]M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, “How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4,” in Proc. IEEE WCNCW, 2012, pp. 232–237.

[31]E. C. Jones and C. A. Chung, RFID and Auto-ID in Planning and Logistics: A Practical Guide for Military UID Applications. Boca Raton,FL, USA: CRC Press, 2011.

[32]C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” IEEE Commun. Mag., vol. 48, no. 6, pp. 92–101, Jun. 2010.

[33]C. Withanage, R. Ashok, C. Yuen, and K. Otto, “A comparison of the popular home automation technologies,” in Proc. IEEE ISGT Asia, 2014,

pp. 600–605.

[34]I. Ishaq et al., “IETF standardization in the field of the Internet of Things (IoT): A survey,” J. Sens. Actuator Netw., vol. 2, pp. 235–287,2013.

[35] Denial-of-Service detection in 6LoWPAN based Internet of Things, 2013 IEEE 9th International Conference on Wireless COnference and Mobile Computing, Networking and COmmunications ()WiMobpp. 600-601

[36] DIO Suppression Attack Against Routing in the Internet of Things, IEEE Communication Letters, vol. 21, no. 11, November 2017, pp.2525

[37] DOS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things, 2012 International Conference on Selected Topics in Mobile and Wireless Networking, pp.60-61

[38] REATO: REActing TO Dinail of Service attacks in the Internet of Things, Computer Networks 2018, pp. 4

[39]EyeSim: A Mobile Application for Visual-Assisted Wormhole Attack Detection in IoT-enabled WSNs, 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)

[40] A Review of Security Concerns in Internet of Things, Journal of Computer and Communication, 2017, 5, 121-136, pp. 126

[41] Defending against Path-based DoS Attacks in Wireless Sensor Networks, Department of Computer Science of Colorado Boulder, Colorado USA

[42] Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management, Computers and Communications, 2008. ISCC 2008. IEEE Simposium

[43]DoS Attacks Analysis and Improvements in DTLS Protocol for Internet of Thing

[44]https://www.ietf.org/topics/iot/

[45] A Mechanism for Securing IoT-enabled Applications at the Fog Layer, Nadeem Abbas , Muhammad Asim, Noshina Tariq, Thar Baker, and Sohail Abbas, 18 February 2019

[46] Using the Cumulative Sum Algorithm Against Distributed Denial of Service Attacks in Internet of Things Using the Cumulative Sum Algorithm Against Distributed Denial of Service Attacks in Internet of Things, Pheeha Machaka1, Andre McDonald, Fulufhelo Nelwamondo, and Antoine Bagula

[47] Internet of Things: A Survey on EnablingTechnologies, Protocols, and Applications

[48] Denial of Service (DoS) attack with UDP Flood, Li Xiamoming, Valon Sejdini, Hasan Chowdhury

[48] Detection and Prevention of ICMP Flood DDOS Attack, Harshita, International Journal of New Technology and Research (IJNTR) ISSN:2454-4116, Volume-3, Issue-3, March 2017 Pages 63-69

[49] Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications Ala Al-Fuqaha, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, Mehdi Mohammadi, Student Member, IEEE,Mohammed Aledhari, Student Member, IEEE, and Moussa Ayyash, Senior Member, IEEE, IEEE communications surveys and tutorials, VOL. 17, NO. 4, 2015

[50] Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks, AArti Singh, dimple Juneja August 2010

[51] RFC 3361, Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers, The Internet Society (2002)

[52]A Survey on HTTP Flooding Attack Detection and Mitigating Methodologies, Apurv Verma, April 2016

[53] Traffic characteristics of common DoS tools, Vit Bukac, April 2014

[54] RFC 2616 Hypertext Transfer Protocol – HTTP/1.1, June 1999