ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Ασφάλεια των πρωτοκόλλων στα χαμηλότερα επίπεδα του IoT: Μία έρευνα για τις επιθέσεις, την πρόληψη και την αντιμετώπιση τους»

Του φοιτητή Κορτέση Νικόλαου
Αρ. Μητρώου: 164681

Επιβλέπων καθηγητής
Αμανατιάδης Δημήτριος

Μάιος 2025

Τίτλος Π.Ε. «Ασφάλεια των πρωτοκόλλων στα χαμηλότερα επίπεδα του IoT: Μία έρευνα για τις επιθέσεις, την πρόληψη και την αντιμετώπιση τους»

Κωδικός Π.Ε. 25111

Ονοματεπώνυμο φοιτητή/τών: Κορτέσης Νικόλαος

Ονοματεπώνυμο εισηγητή : Αμανατιάδης Δημήτριος

Ημερομηνία ανάληψης Π.Ε. 06/02/2025

Ημερομηνία περάτωσης Π.Ε. 30/05/2025

//

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος

Πρόλογος

Το συγκεκριμένο θέμα για αυτή την πτυχιακή, οφείλεται στο ενδιαφέρον για την ασφάλεια στο Διαδίκτυο των πραγμάτων, στο πως μπορούμε να προλάβουμε τυχών επιθέσεις στα χαμηλότερα επίπεδα αυτού και πως μπορούμε να τις αντιμετωπίσουμε. Το Διαδίκτυο των πραγμάτων μπαίνει στην καθημερινή μας ζωή όλο και πιο πολύ, γεγονός που παρουσιάζει ιδιαίτερες προκλήσεις ασφαλείας που απαιτούν δημιουργικές λύσεις. Τέτοιες λύσεις μπορεί να προσφέρει η μελέτη των πρωτοκόλλων των χαμηλότερων επιπέδων του Διαδικτύου των πραγμάτων και η ανάλυση των ευπαθειών καθενός από αυτά.

Περίληψη

Το διαδίκτυο των πραγμάτων (Internet of Things - IoT) βρίσκεται παντού γύρω μας. Κάποιες έρευνες υποστηρίζουν ότι οι συνδεδεμένες συσκευές θα φτάσουν έως τις 30 δισεκατομύρια έως και το 2030. Η εργασία αυτή εξετάζει τα πρωτόκολλα που χρησιμοποιούνται στα χαμηλότερα επίπεδα του IoT, εστιάζοντας στην ασφάλεια και τις πιθανές ευπάθειες τους. Θα γίνει ανάλυση των βασικών πρωτοκόλλων επικοινωνίας (Sigfox, Zigbee, LoRa και άλλα) και της λειτουργικότητας τους. Θα διερευνηθούν οι πιο συχνές επιθέσεις που στοχεύουν αυτές τις υποδομές. Η εργασία περιλαμβάνει τις μεθόδους πρόληψης και αντιμετώπισης αυτών των επιθέσεων, συμπεριλαμβανομένων βέλτιστων πρακτικών ασφάλειας και σύγχρονων μηχανισμών ανίχνευσης απειλών. Στόχος της έρευνας είναι η ενίσχυση της ασφάλειας των IoT συστημάτων, προσφέροντας προτάσεις για την προστασία των ευπαθειών τους.

«Security of protocols at the lower levels of IoT:

A survey of attacks, prevention, and their handling»

«Kortesis Nikolaos»

Abstract

The Internet of Things (IoT) is everywhere around us. Some research suggests that connected devices will reach up to 30 billion by 2030. This work examines the protocols used at the lower levels of the IoT, focusing on security and their potential vulnerabilities. An analysis of the main communication protocols (Sigfox, Zigbee, LoRa and others) and their functionality will be performed. The most common attacks targeting these infrastructures will be investigated. The work includes methods for preventing and mitigating these attacks, including best security practices and modern threat detection mechanisms. The aim of the research is to enhance the security of IoT systems, offering suggestions for protecting their vulnerabilities.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
6TiSCH	IPv6 over the TSCH mode of IEEE 802.15.4e
ACL	Access Control List
AI	Artificial Intelligence
AIIPoT	Adaptive Intelligent-Interaction Honeypot
ARP	Address Resolution Protocol
BL	Bluetooth
BLE	Bluetooth Low Energy
CNN	Convolutional Neural Networks
DDoS	Distributed Denial of Service
DBN	Deep Belief Networks
DL	Deep Learning
DNN	Deep Neural Networks
DNS	Domain Name System
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DTLS	Datagram Transport Layer Security
DQN	Deep Q-Networks
DVR	Digital Video Recorder
ECC	Elliptic Curve Cryptography
ELM	Extreme Learning Machines
GAN	Generative Adversarial Network
GFSK	Gaussian Frequency Shift Keying
GNN	Graph Neural Networks
HARM	Honeypot for Automated and Repetitive Malware
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IEEE	Institute of Electrical and Electronics Engineers

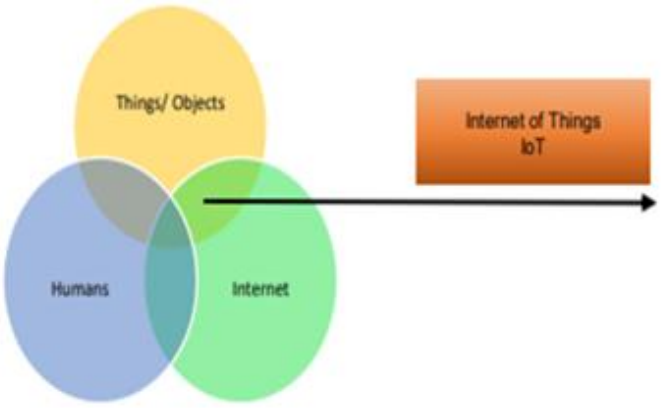
IEFT	Internet Engineering Task Force
IIOT	Industrial Internet of Things
IoE	Internet of Energy
IoS	Internet of Sensors
IoT	Internet of Things
IoV	Internet of Vehicles
IPS	Intrusion Prevention System
KNN	K-Nearest Neighbors
LoRaWAN	Long Range Wide Area Network
LSTM	Long Short-Term Memory
NFC	Near Field Communication
MAC	Message Authentication Code
Machine-to-Machine	M2M
MITM	Man-In-The-Middle
ML	Machine Learning
MLP	Multi-Layer Perceptron
MSG	Micro-Segmentation
MTD	Moving Target Defense
MQTT	Message Queuing Telemetry Transport
P2P	Peer-to-peer
PDoS	Permanent Denial of Service
PIoT	Power IoT
PSO	Particle swarm optimization
RNN	Recurrent Neural Networks
RL	Reinforcement Learning
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low-Power and Lossy Networks
SDN	Software-Defined Networking
SNMP	Simple Network Management Protocol

SOM	Self-Organizing Maps
SUIT	Software Updates for IoT
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UNB	Ultra Narrow Band
WSN	Wirless Sensor Network
XMPP	Extensible Messaging and Presence Protocol

Κεφάλαιο 1ο: Εισαγωγή στο Διαδίκτυο των Πραγμάτων

1.1 Εισαγωγή

Το 1999, ο Kevin Ashton της Procter & Gamble εισήγαγε για πρώτη φορά τον όρο "Internet of Things". Το Διαδίκτυο των Πραγμάτων αναφέρεται σε ένα δίκτυο φυσικών συσκευών, οχημάτων και άλλων φυσικών αντικειμένων που ενσωματώνουν αισθητήρες, λογισμικό και συνδεσιμότητα δικτύου, επιτρέποντάς τους να συλλέγουν και να μοιράζονται δεδομένα. Οι συσκευές IoT - γνωστές και ως "έξυπνα αντικείμενα" - μπορούν να κυμαίνονται από απλές συσκευές "έξυπνου σπιτιού" έως περίπλοκα βιομηχανικά μηχανήματα και συστήματα μεταφοράς. Μπορούμε να πούμε ότι είναι ένα οικοσύστημα όπου οι άνθρωποι, τα αντικείμενα/συσκευές και το διαδίκτυο αλληλοεπιδρούν μεταξύ τους, τέμνονται και γεννούν το IoT, όπως φαίνεται στο σχήμα 1.1 παρακάτω [1].



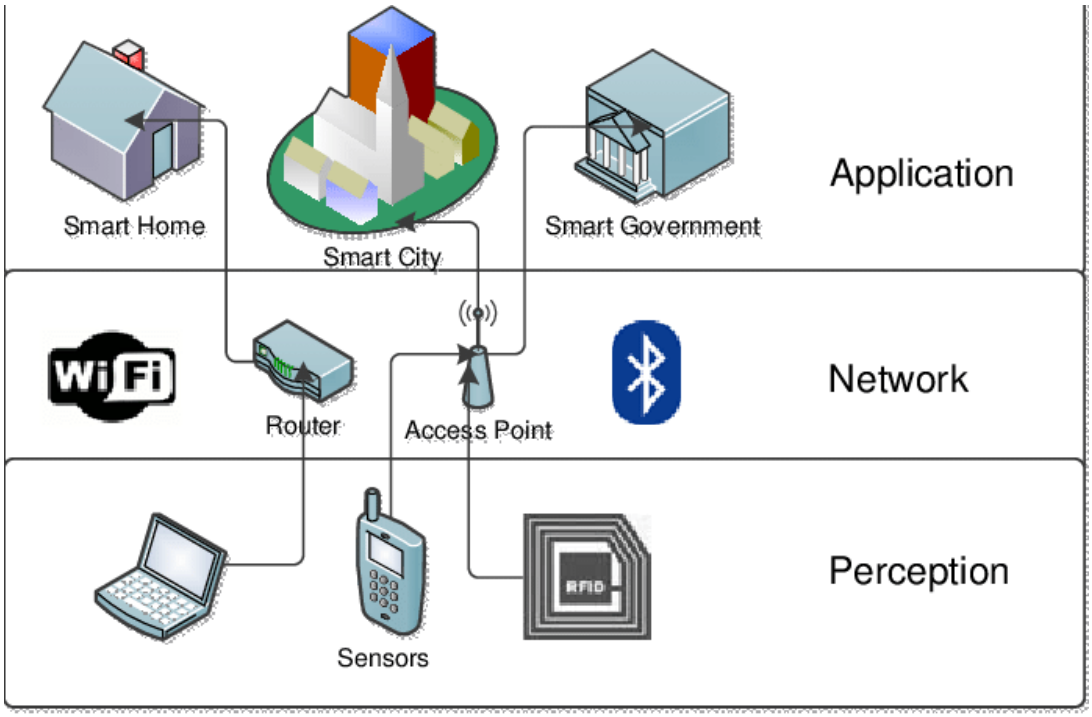
Σχήμα 1.1: Απλή αναπαράσταση του IoT

1.2 Αρχιτεκτονική και Τεχνολογίες του IoT

Στην βιβλιογραφία υπάρχουν διάφορων ειδών αρχιτεκτονικές, όπως η αρχιτεκτονική τριών επιπέδων, η αρχιτεκτονική πέντε επιπέδων, η αρχιτεκτονική υπολογιστικού νέφους και άλλων ειδών. Στην παρούσα πτυχιακή θα ασχοληθούμε με την αρχιτεκτονική τριών επιπέδων (Three-Layer Architecture).

Η αρχιτεκτονική Τριών Επιπέδων περιλαμβάνει:

- **Επίπεδο Αντίληψης (Perception Layer):** Περιλαμβάνει τις συσκευές που συλλέγουν δεδομένα από το περιβάλλον [12].
- **Επίπεδο Δικτύου (Network Layer):** Διαχειρίζεται τη μετάδοση των δεδομένων μέσω δικτύου [12].
- **Επίπεδο Εφαρμογής (Application Layer):** Διαχειρίζεται τις τελικές εφαρμογές που χρησιμοποιούν τα δεδομένα από το IoT για υπηρεσίες και επεξεργασία [12].



Σχήμα 1.2 : Αρχιτεκτονική τριών επιπέδων στο IoT

Η αρχιτεκτονική του IoT περιλαμβάνει αισθητήρες, δίκτυα επικοινωνίας, πλατφόρμες επεξεργασίας δεδομένων και εφαρμογές. Οι τεχνολογίες-κλειδιά περιλαμβάνουν:

- **Ασύρματα Δίκτυα Αισθητήρων (WSN)**:Ένα WSN αποτελείται από πολλούς αυτόνομους κόμβους αισθητήρων που διαθέτουν δυνατότητα ανίχνευσης, επεξεργασίας και ασύρματης επικοινωνίας. Αυτοί οι κόμβοι συλλέγουν δεδομένα από το περιβάλλον και τα στέλνουν σε έναν κεντρικό σταθμό βάσης για επεξεργασία [13].
- **Radio Frequency Identification (RFID)**: Το RFID είναι μια τεχνολογία αναγνώρισης που χρησιμοποιεί ραδιοκύματα για την ασύρματη επικοινωνία μεταξύ μιας συσκευής αναγνώρισης (reader) και ενός ετικετοφορητή (tag) τοποθετημένου σε ένα αντικείμενο. Οι RFID ετικέτες μπορεί να είναι ενεργητικές (με ενσωματωμένη μπαταρία) ή παθητικές (χωρίς μπαταρία, χρησιμοποιούν την ενέργεια του ραδιοσήματος του αναγνώστη για να λειτουργήσουν). Χρησιμοποιείται σε διάφορους τομείς, όπως στη διαχείριση αποθεμάτων, την παρακολούθηση προϊόντων, τη διαχείριση της εφοδιαστικής αλυσίδας και την είσοδο σε κτίρια [14].

- **Near Field Communication (NFC)**: Το NFC είναι μια υποκατηγορία της τεχνολογίας RFID που λειτουργεί σε μικρότερες αποστάσεις (συνήθως έως 10 εκατοστά) και έχει εφαρμογές στον τομέα των πληρωμών, της ασφάλειας και της ανταλλαγής δεδομένων μεταξύ κινητών συσκευών. Το NFC είναι συμβατό με τις υπάρχουσες τεχνολογίες RFID και αποτελεί βασικό στοιχείο στις πιο σύγχρονες υπηρεσίες πληρωμών, όπως το Apple Pay και το Google Wallet [15].

- **Πλατφόρμες Υπολογιστικού Νέφους**: Οι πλατφόρμες υπολογιστικού νέφους (cloud computing platforms) αποτελούν τη βάση για την παροχή υπολογιστικών υπηρεσιών μέσω του διαδικτύου. Οι βασικοί τύποι είναι: Υποδομή ως Υπηρεσία (IaaS), Πλατφόρμα ως Υπηρεσία (PaaS) και Λογισμικό ως Υπηρεσία (SaaS), καθένας εκ των οποίων εξυπηρετεί διαφορετικές ανάγκες σε επίπεδο υποδομής, ανάπτυξης ή τελικής χρήσης [16].

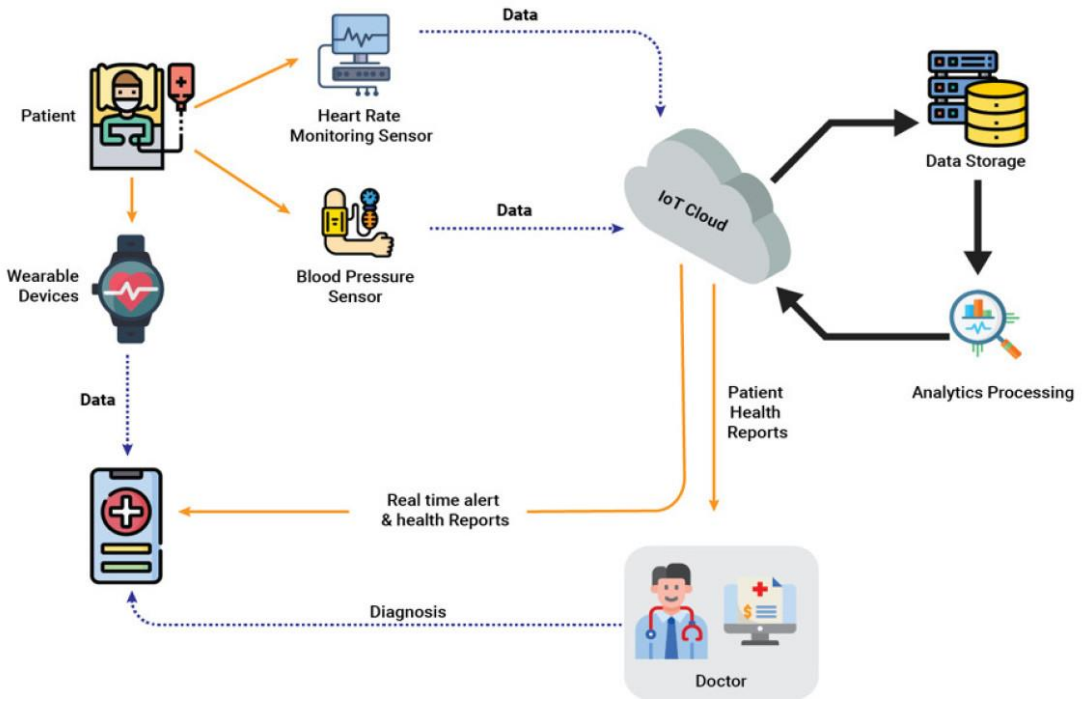
1.3 Εφαρμογές του IoT

Το IoT βρίσκει εφαρμογή σε πολλούς τομείς:

- **Έξυπνες Πόλεις (Smart Cities)**: Οι έξυπνες πόλεις (smart cities) αποτελούν σύγχρονες αστικές περιοχές που αξιοποιούν τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ), το Διαδίκτυο των Πραγμάτων (IoT) και την τεχνητή νοημοσύνη (AI). Σκοπός τους είναι η βελτίωση της ποιότητας ζωής των πολιτών, η ενίσχυση της βιωσιμότητας και η προώθηση της οικονομικής ανάπτυξης. Οι έξυπνες πόλεις ενσωματώνουν τεχνολογίες αιχμής για την αποδοτική διαχείριση των πόρων, την ενίσχυση της συμμετοχής των πολιτών και την προώθηση της καινοτομίας. Χαρακτηρίζονται από τη χρήση ΤΠΕ για τη βελτίωση των υπηρεσιών, την ενίσχυση της βιωσιμότητας και την προώθηση της κοινωνικής συνοχής [17].
Το IoT επιτρέπει την παρακολούθηση και διαχείριση της κυκλοφορίας σε πραγματικό χρόνο μέσω αισθητήρων και έξυπνων φώτων, μειώνοντας τη συμφόρηση και βελτιώνοντας την ασφάλεια. Οι συσκευές IoT μπορούν να παρέχουν δεδομένα για τη ροή των οχημάτων και να προσαρμόζουν τα φανάρια ανάλογα με την κίνηση [89].
Έξυπνοι μετρητές και αισθητήρες IoT βοηθούν στην παρακολούθηση και τη βελτιστοποίηση της κατανάλωσης ενέργειας, ενώ ο έξυπνος φωτισμός δρόμων ενεργοποιείται και ρυθμίζεται ανάλογα με την κίνηση πεζών και οχημάτων, μειώνοντας την ενεργειακή σπατάλη [90].
Τα IoT συστήματα χρησιμοποιούνται για την παρακολούθηση της πλήρωσης κάδων απορριμμάτων, ώστε να γίνεται συλλογή μόνο όταν απαιτείται, μειώνοντας το κόστος και τη ρύπανση [91].
Αισθητήρες IoT μετρούν σε πραγματικό χρόνο την ποιότητα του αέρα, το επίπεδο θορύβου και άλλες περιβαλλοντικές παραμέτρους, βοηθώντας στη λήψη μέτρων για τη βελτίωση της ποιότητας ζωής [92].
Οι έξυπνοι αισθητήρες παρακολουθούν τη χρήση και διαρροές νερού σε δίκτυα ύδρευσης, συμβάλλοντας στη διατήρηση και οικονομία των υδάτινων πόρων [93].
Το IoT χρησιμοποιείται για την εγκατάσταση έξυπνων καμερών και συστημάτων συναγερμού, με δυνατότητα ανάλυσης δεδομένων σε πραγματικό χρόνο για την πρόληψη εγκληματικότητας και την άμεση ανταπόκριση [94].

Σχήμα 1.3 : Γενική αναπαράσταση του όρου Smart City.

- **Υγεία**: Η εφαρμογή του IoT στον τομέα της υγείας (Healthcare IoT) έχει φέρει επανάσταση σε πτυχές όπως η παρακολούθηση ασθενών, η πρόληψη ασθενειών και η αύξηση της αποδοτικότητας των συστημάτων υγείας. Το IoT επιτρέπει τη συνεχή παρακολούθηση ασθενών μέσω αισθητήρων που φοριούνται ή τοποθετούνται στο σπίτι. Αυτά τα συστήματα είναι ιδιαίτερα χρήσιμα για χρόνιες παθήσεις, παρακολούθηση ηλικιωμένων ή αποκατάσταση μετά από νοσηλεία [18]. Έρευνες έχουν δείξει ότι συστήματα IoT μπορούν να παρακολουθούν την κατανάλωση νερού, τον ύπνο και τη σωματική δραστηριότητα σε ηλικιωμένους, με σκοπό την έγκαιρη ανίχνευση προβλημάτων υγείας και την αποστολή ειδοποιήσεων σε φροντιστές [19].

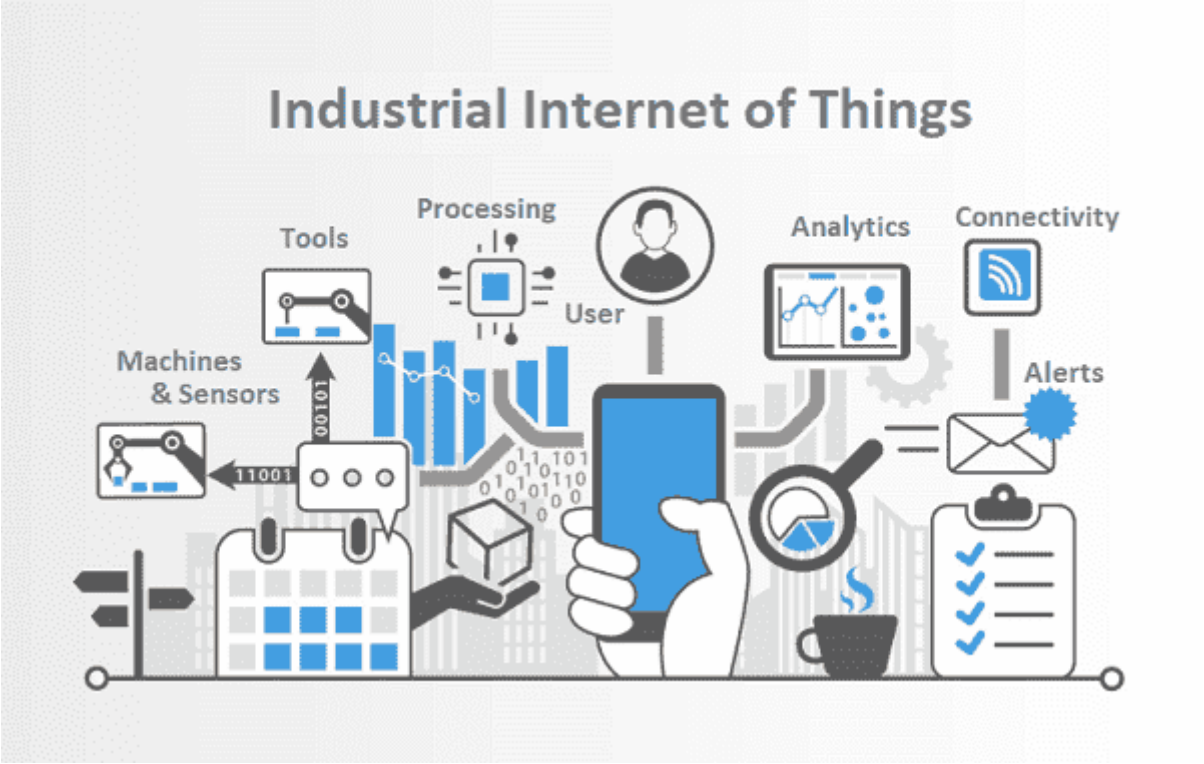


Σχήμα 1.4 : Γενική αναπαράσταση του IoT στην υγεία.

Το IoT χρησιμοποιείται επίσης για την πρόληψη πτώσεων μέσω αισθητήρων που ανιχνεύουν απότομες αλλαγές στη θέση του σώματος ή έλλειψη κίνησης. Παράλληλα, σε νοσοκομειακό περιβάλλον χρησιμοποιούνται συστήματα για την παρακολούθηση της υγιεινής των χεριών του προσωπικού, μειώνοντας τις ενδονοσοκομειακές λοιμώξεις [20].

- **Βιομηχανία**: Η ενσωμάτωση IoT στη βιομηχανία έχει οδηγήσει σε ριζικές αλλαγές στη λειτουργία των εργοστασίων και την παραγωγική διαδικασία. Το λεγόμενο Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) προσφέρει σημαντικά πλεονεκτήματα, όπως ευφυή συντήρηση, αυτοματισμούς και βελτιωμένη παρακολούθηση διαδικασιών [21]. Με την ενσωμάτωση κυβερνο-φυσικών συστημάτων (CPS) και τη χρήση αισθητήρων συνθέτουν το λεγόμενο "έξυπνο εργοστάσιο", με δυνατότητες αυτόματης προσαρμογής της παραγωγής βάσει δεδομένων σε πραγματικό χρόνο [22]. Το IIoT δίνει τη δυνατότητα συνεχούς παρακολούθησης της αλυσίδας εφοδιασμού, αξιοποιώντας RFID και cloud τεχνολογίες για καλύτερη διαχείριση αποθεμάτων [21].
Το IoT επιτρέπει τη συνεχή παρακολούθηση της κατάστασης των μηχανημάτων μέσω αισθητήρων που συλλέγουν δεδομένα όπως δονήσεις, θερμοκρασία και πίεση. Αυτά τα δεδομένα αναλύονται για να

προβλεφθούν οι βλάβες πριν συμβούν, μειώνοντας το χρόνο διακοπής λειτουργίας και το κόστος συντήρησης [76].



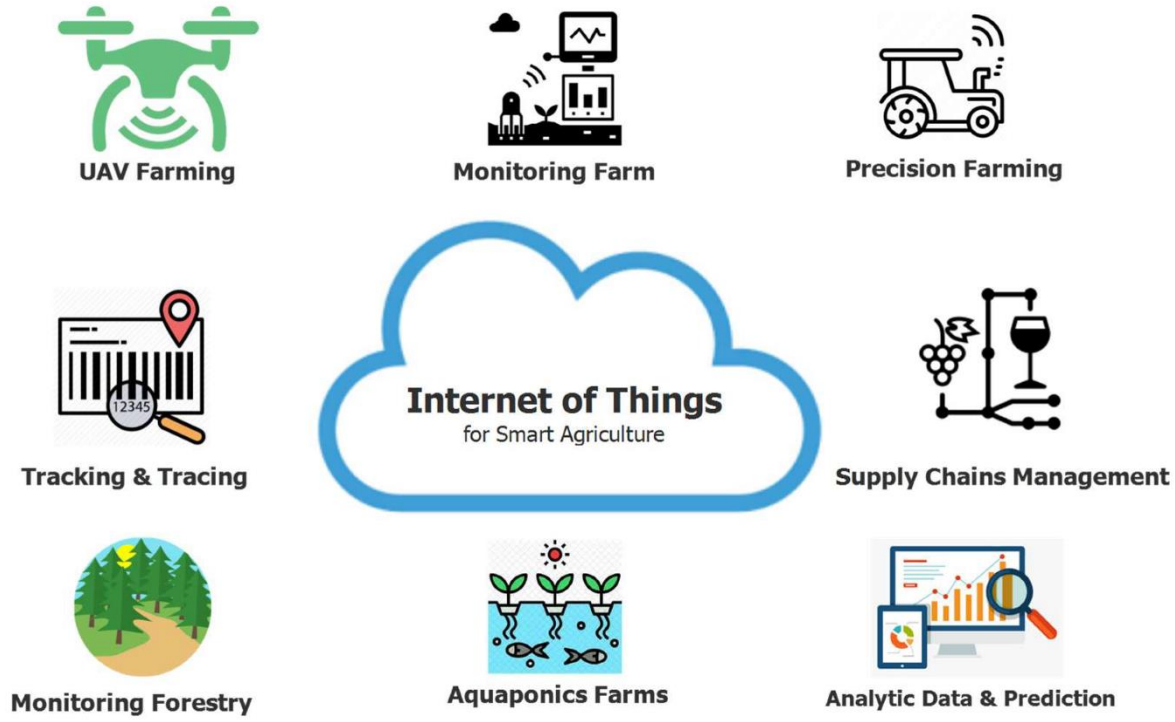
Σχήμα 1.5 : Γενική αναπαράσταση του IoT στην βιομηχανία.

Μέσω της συλλογής δεδομένων από διάφορα σημεία της γραμμής παραγωγής, το IoT βοηθά στον εντοπισμό σημείων συμφόρησης και στη βελτίωση της ροής εργασιών, επιτρέποντας την αύξηση της παραγωγικότητας και τη μείωση της κατανάλωσης ενέργειας [77].
Τα βιομηχανικά συστήματα εξοπλισμένα με IoT μπορούν να ελέγχονται απομακρυσμένα, μειώνοντας την ανάγκη για φυσική παρουσία και επιτρέποντας την άμεση αντίδραση σε αλλαγές ή προβλήματα [78].
Με τη χρήση αισθητήρων και συνδεδεμένων συσκευών, το IoT συμβάλλει στην παρακολούθηση της ασφάλειας των εργαζομένων και στην ακριβή καταγραφή και διαχείριση των αποθεμάτων πρώτων υλών και προϊόντων [79].

Συνεχής συλλογή δεδομένων από τη γραμμή παραγωγής επιτρέπει την ανίχνευση αποκλίσεων ποιότητας σε πραγματικό χρόνο και την άμεση διόρθωση, μειώνοντας τα απόβλητα και βελτιώνοντας τη συνολική ποιότητα [80].

- **Γεωργία**: Η ενσωμάτωση του IoT στη γεωργία έχει φέρει επανάσταση στον τρόπο με τον οποίο καλλιεργούνται και διαχειρίζονται οι γεωργικές εκμεταλλεύσεις. Αυτό οδηγεί σε αυξημένη αποδοτικότητα, βιωσιμότητα και παραγωγικότητα. Με την χρήση του IoT είναι δυνατή η έξυπνη άρδευση, όπου με τη χρήση αισθητήρων για την παρακολούθηση της υγρασίας του εδάφους και των καιρικών συνθηκών επιτρέπει την ακριβή άρδευση, μειώνοντας τη σπατάλη νερού και βελτιώνοντας τις αποδόσεις των καλλιεργειών [23]. Συστήματα IoT με κάμερες και αισθητήρες ανιχνεύουν πρώιμα σημάδια ασθενειών ή προσβολών από παράσιτα, επιτρέποντας έγκαιρες παρεμβάσεις και μειώνοντας τις απώλειες καλλιεργειών [24]. Η ενσωμάτωση του IoT στα θερμοκήπια επιτρέπει τον ακριβή έλεγχο

παραμέτρων όπως η θερμοκρασία, η υγρασία και η φωτεινότητα, βελτιώνοντας την ανάπτυξη των φυτών και μειώνοντας τη σπατάλη πόρων [25].



Σχήμα 1.6 : Γενική αναπαράσταση του IoT στην γεωργία.

Το IoT επιτρέπει τη συνεχή και ακριβή παρακολούθηση παραμέτρων όπως η υγρασία του εδάφους, η θερμοκρασία, το pH, η ηλιακή ακτινοβολία και άλλες περιβαλλοντικές συνθήκες μέσω δικτύων αισθητήρων. Αυτό βοηθά τους αγρότες να λαμβάνουν δεδομένα σε πραγματικό χρόνο και να βελτιστοποιούν την άρδευση και τη λίπανση [81][82].
Η χρήση IoT συσκευών επιτρέπει την αυτοματοποίηση της άρδευσης, όπου τα συστήματα άρδευσης ενεργοποιούνται ή απενεργοποιούνται ανάλογα με τις μετρήσεις υγρασίας του εδάφους και τις καιρικές συνθήκες, μειώνοντας την κατανάλωση νερού και αυξάνοντας την απόδοση της καλλιέργειας [83][84].

Με τη βοήθεια IoT καμερών και αισθητήρων, οι αγρότες μπορούν να ανιχνεύουν ασθένειες, παράσιτα ή έλλειψη θρεπτικών συστατικών στα φυτά, επιτρέποντας γρήγορες παρεμβάσεις και καλύτερη διαχείριση της παραγωγής [85][86].
Στη ζωική παραγωγή, το IoT χρησιμοποιείται για την παρακολούθηση της υγείας και της συμπεριφοράς των ζώων μέσω φορετών αισθητήρων, βελτιώνοντας την ευημερία και την παραγωγικότητα [87].
Το IoT βοηθά στην παρακολούθηση της αποθήκευσης και μεταφοράς γεωργικών προϊόντων, διασφαλίζοντας την ποιότητα και την ασφάλεια των τροφίμων από το χωράφι μέχρι τον καταναλωτή [88].

1.4 Προκλήσεις και Προβληματισμοί

Παρά τα οφέλη, το IoT αντιμετωπίζει προκλήσεις:

- **Ασφάλεια και Ευπάθειες**: Η ασφάλεια παραμένει μία από τις μεγαλύτερες προκλήσεις του IoT. Ευπάθειες που σχετίζονται με την απομακρυσμένη εκτέλεση κώδικα και την πλήρη κατάληψη

συσκευών συνεχώς εντοπίζονται, όπως η πρόσφατη αναφορά για τις ευπάθειες Amnesia:33 και Ripple20. Η διαχείριση αυτών των ευπαθειών καθίσταται ακόμη πιο δύσκολη λόγω της έλλειψης κεντρικής αρχής για την εφαρμογή διορθώσεων και της εξάρτησης από τρίτους προμηθευτές. Επιπλέον, η έλλειψη υποδομών και η περιορισμένη υπολογιστική ισχύς των IoT συσκευών περιορίζουν τις δυνατότητες για εφαρμογή παραδοσιακών μηχανισμών ασφάλειας [26][27].

- **Προστασία Προσωπικών Δεδομένων και Ιδιωτικότητα** : Η συλλογή δεδομένων από τις συσκευές IoT θέτει σοβαρούς προβληματισμούς σχετικά με την προστασία της ιδιωτικότητας. Οι χρήστες συχνά δεν έχουν πλήρη έλεγχο των δεδομένων που συλλέγονται από τις συσκευές τους, και οι πολιτικές απορρήτου συχνά είναι ασαφείς ή αδύναμες. Επίσης, οι συσκευές IoT συχνά δεν προσφέρουν πλήρη ανωνυμία ή αποδοτική κρυπτογράφηση των δεδομένων, γεγονός που αυξάνει τους κινδύνους διαρροής προσωπικών δεδομένων [28].
- **Διαλειτουργικότητα και Πρότυπα**: Η έλλειψη κοινών προτύπων για τις συσκευές και τις τεχνολογίες IoT δημιουργεί προκλήσεις στη διαλειτουργικότητα. Διαφορετικά πρωτόκολλα και πλατφόρμες IoT δεν είναι πάντα συμβατά μεταξύ τους, γεγονός που περιορίζει την αποτελεσματικότητα της δικτύωσης και της επικοινωνίας μεταξύ των συσκευών. Η ανάπτυξη ενιαίων προτύπων και πρωτοκόλλων είναι κρίσιμη για την ομαλή λειτουργία των IoT συστημάτων σε διάφορα περιβάλλοντα. [29].
- **Πολυπλοκότητα και Διαχείριση Δεδομένων**: Η πολυπλοκότητα των IoT συστημάτων και η ανάγκη διαχείρισης μεγάλου όγκου δεδομένων καθιστούν δύσκολη την αποτελεσματική παρακολούθηση και συντήρηση αυτών των δικτύων. Η ανάγκη για εξειδικευμένες λύσεις διαχείρισης και η ύπαρξη διαφορετικών επιπέδων ασφάλειας και υποδομών καθιστούν δύσκολη την διαχείριση σε πραγματικό χρόνο των IoT συστημάτων. Παράλληλα, η ανάγκη για βελτιστοποίηση των διαδικασιών συλλογής και ανάλυσης δεδομένων παραμένει σημαντική πρόκληση [30].
- **Περιβαλλοντικές Επιπτώσεις**: Η μαζική ανάπτυξη του IoT μπορεί να έχει αρνητικές περιβαλλοντικές συνέπειες λόγω της αυξημένης κατανάλωσης ενέργειας και των ηλεκτρονικών αποβλήτων. Παράλληλα, το IoT έχει τη δυνατότητα να προσφέρει λύσεις για την αποδοτικότερη διαχείριση φυσικών πόρων και την παρακολούθηση περιβαλλοντικών παραμέτρων, όπως η ποιότητα του αέρα ή η κατανάλωση ενέργειας, συμβάλλοντας έτσι στην προστασία του περιβάλλοντος. Ωστόσο, η ανάπτυξη πράσινων τεχνολογιών για το IoT παραμένει σημαντική πρόκληση [31].
- **Κανονιστικό Πλαίσιο και Πολιτική**: Η κανονιστική ρύθμιση του IoT είναι απαραίτητη για την εξασφάλιση της ασφάλειας, της ιδιωτικότητας και της διαλειτουργικότητας των συσκευών και των δικτύων. Η έλλειψη καθαρού κανονιστικού πλαισίου για την προστασία των χρηστών και τη διαχείριση των IoT συσκευών προκαλεί δυσκολίες στην ανάπτυξη ασφαλών εφαρμογών. Η πρόκληση είναι η ανάπτυξη ρυθμιστικών πολιτικών που θα επιτρέπουν τη συνεχιζόμενη ανάπτυξη του IoT χωρίς να διακυβεύονται τα δικαιώματα των χρηστών και η ασφάλεια των συστημάτων [32].

1.5 Μελλοντικές Κατευθύνσεις

Το IoT αναμένεται να εξελιχθεί περαιτέρω με την ενσωμάτωση τεχνολογιών όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και η βαθιά μάθηση. Η ανάπτυξη έξυπνων συστημάτων που μπορούν να λαμβάνουν αποφάσεις αυτόνομα είναι ένας από τους κύριους στόχους [5].

Η **ανάπτυξη των 5G και μελλοντικά των 6G** δικτύων θα επιτρέψει τη δημιουργία δικτύων IoT με πολύ χαμηλή καθυστέρηση (latency), μεγαλύτερη αξιοπιστία και πολύ μεγαλύτερο ρυθμό μετάδοσης δεδομένων. Αυτό θα υποστηρίξει εφαρμογές που απαιτούν πραγματικό χρόνο, όπως τα αυτόνομα οχήματα, η τηλεχειρουργική και η έξυπνη πόλη [109][110].

Η ένταξη αλγορίθμων **Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης** στο IoT θα επιτρέψει την αυτονομία και την προγνωστική ανάλυση δεδομένων από τους αισθητήρες, βελτιώνοντας τη λήψη αποφάσεων, τη διαχείριση ενέργειας και την ασφάλεια των συστημάτων [111][112].

Με την αύξηση του αριθμού των IoT συσκευών, αυξάνονται και οι απειλές. Τα μελλοντικά συστήματα IoT θα βασιστούν σε προηγμένες τεχνικές κρυπτογράφησης, αποκεντρωμένες αρχιτεκτονικές (blockchain), και υβριδικά μοντέλα ασφάλειας για να προστατεύσουν τα δεδομένα και τις συσκευές [113][114].

Η χρήση **Edge Computing** και **Fog Computing** θα βοηθήσουν τη μείωση της καθυστέρησης και τη βελτίωση της αποδοτικότητας, οι υπολογιστικές διεργασίες θα μετακινηθούν πιο κοντά στην πηγή των δεδομένων, δηλαδή στα edge devices ή στους τοπικούς servers (fog nodes), μειώνοντας την ανάγκη αποστολής όλων των δεδομένων στο cloud [115][116].

Η ενοποίηση και η **διαλειτουργικότητα** μεταξύ διαφορετικών πρωτοκόλλων και συσκευών IoT θα αποτελέσει κρίσιμο παράγοντα για την ευρεία υιοθέτηση του IoT. Μελλοντικά πρότυπα θα επικεντρωθούν στην καλύτερη συνεργασία και ασφάλεια μεταξύ των συστημάτων [117]. Οι εφαρμογές IoT για την παρακολούθηση και διαχείριση φυσικών πόρων, την ενεργειακή αποδοτικότητα και την κλιματική αλλαγή θα αποτελέσουν βασικό πεδίο ανάπτυξης, συμβάλλοντας στην επίτευξη των στόχων **βιώσιμης ανάπτυξης** (SDGs) [118].

1.6 Επίλογος

Το Internet of Things (IoT) αποτελεί μία από τις σημαντικότερες τεχνολογικές εξελίξεις του 21ου αιώνα, με επιπτώσεις σε κάθε τομέα της ανθρώπινης δραστηριότητας. Μέσα από τη σύνδεση του φυσικού κόσμου με τον ψηφιακό, το IoT προσφέρει νέες δυνατότητες για αυτοματοποίηση, ανάλυση και λήψη αποφάσεων με βάση πραγματικά δεδομένα. Η εξάπλωση του IoT εγείρει σοβαρούς προβληματισμούς θέτοντας την ανάγκη για ανάπτυξη ισχυρών πολιτικών και προτύπων. Το μέλλον του IoT προβλέπεται ακόμη πιο διαδραστικό, με την ενσωμάτωση τεχνητής νοημοσύνης και την προοπτική των αυτόνομων έξυπνων συστημάτων. Η κατανόηση των βασικών αρχών του IoT, των προκλήσεων και των προοπτικών του είναι απαραίτητη για όποιον επιθυμεί να συμβάλει ενεργά στην τεχνολογική καινοτομία της εποχής μας.

Κεφάλαιο 2ο: Ασφάλεια στο Διαδίκτυο των Πραγμάτων

2.1 Εισαγωγή

Το IoT αναφέρεται στη διασύνδεση φυσικών συσκευών με το διαδίκτυο, επιτρέποντας την ανταλλαγή δεδομένων και την αυτοματοποίηση διαδικασιών. Η ραγδαία εξάπλωση του IoT έχει επιφέρει σημαντικές προκλήσεις στον τομέα της ασφάλειας, καθώς οι συσκευές αυτές συχνά παρουσιάζουν ευπάθειες που μπορούν να εκμεταλλευτούν κακόβουλοι παράγοντες.[6]

2.2 Κύριες Απειλές και Ευπάθειες

Οι συσκευές IoT είναι επιρρεπείς σε διάφορες απειλές, όπως:

- **Παθητικές Επιθέσεις**: Υποκλοπή δεδομένων χωρίς την τροποποίησή τους.
- **Ενεργές Επιθέσεις**: Αλλαγή ή καταστροφή δεδομένων, όπως επιθέσεις τύπου Denial of Service.

Η έλλειψη φυσικών μέτρων ασφαλείας και η περιορισμένη υπολογιστική ισχύς των συσκευών καθιστούν δύσκολη την εφαρμογή παραδοσιακών μηχανισμών ασφάλειας.[6]

2.2.1 Παθητικές Επιθέσεις

Οι παθητικές επιθέσεις στο IoT αποτελούν σοβαρή απειλή για την ασφάλεια και την ιδιωτικότητα, καθώς επιτρέπουν σε κακόβουλους παράγοντες να συλλέγουν πληροφορίες χωρίς να γίνονται αντιληπτοί.

Κατηγορίες Παθητικών Επιθέσεων:

- **Υποκλοπή (Eavesdropping)**: Αναγνώριση μη κρυπτογραφημένων δεδομένων μέσω ακρόασης ασύρματων επικοινωνιών [6].
- **Ανάλυση Κυκλοφορίας (Traffic Analysis)**: Παρακολούθηση προτύπων επικοινωνίας για εξαγωγή πληροφοριών σχετικά με τη δομή του δικτύου και τη συμπεριφορά των συσκευών [6].
- **Κακή Λειτουργία Κόμβων (Node Malfunctioning)**: Εκμετάλλευση δυσλειτουργιών συσκευών για συλλογή δεδομένων ή αποδυνάμωση του δικτύου [6].
- **Απενεργοποίηση Κόμβων (Node Outage)**: Απώλεια λειτουργικότητας κόμβων, οδηγώντας σε πιθανές διαρροές πληροφοριών ή παραβίαση της ακεραιότητας του δικτύου [33].
- **Καταστροφή Κόμβων (Node Destruction)**: Φυσική ή λογική καταστροφή συσκευών για απόκτηση πρόσβασης σε αποθηκευμένα δεδομένα [6].

Παραδείγματα Παθητικών Επιθέσεων:

- **Επίθεση Παθητικής Αποκάλυψης Μυστικών**: Επιθέσεις σε πρωτόκολλο αυθεντικοποίησης RFID, όπου ένας επιτιθέμενος μπορεί να αποκαλύψει μυστικά κλειδιά παρακολουθώντας μία μόνο συνεδρία επικοινωνίας [6].
- **Επίθεση Ανάλυσης Κυκλοφορίας σε Έξυπνα Σπίτια**: Η παρακολούθηση ασύρματης κυκλοφορίας σε έξυπνα σπίτια μπορεί να αποκαλύψει ευαίσθητες πληροφορίες για τις δραστηριότητες των χρηστών, ακόμα και χωρίς αποκρυπτογράφηση των δεδομένων [34].

Μέτρα Αντιμετώπισης Παθητικών Επιθέσεων:

- **Κρυπτογράφηση Επικοινωνιών**: Η χρήση ισχυρών αλγορίθμων κρυπτογράφησης προστατεύει τα δεδομένα από υποκλοπή [6].

- **Τεχνικές Απόκρυψης Κυκλοφορίας**: Η εισαγωγή ψευδών πακέτων ή η τροποποίηση προτύπων επικοινωνίας μπορεί να παραπλανήσει επιτιθέμενους που βασίζονται στην ανάλυση κυκλοφορίας [34].
- **Ανίχνευση Ανωμαλιών**: Η παρακολούθηση και ανάλυση της συμπεριφοράς του δικτύου μπορεί να βοηθήσει στον εντοπισμό ύποπτων δραστηριοτήτων [6].
- **Φυσική Ασφάλεια Συσκευών**: Η προστασία των συσκευών από φυσική πρόσβαση μειώνει τον κίνδυνο καταστροφής ή παραβίασης [6].

Συμπεράσματα:

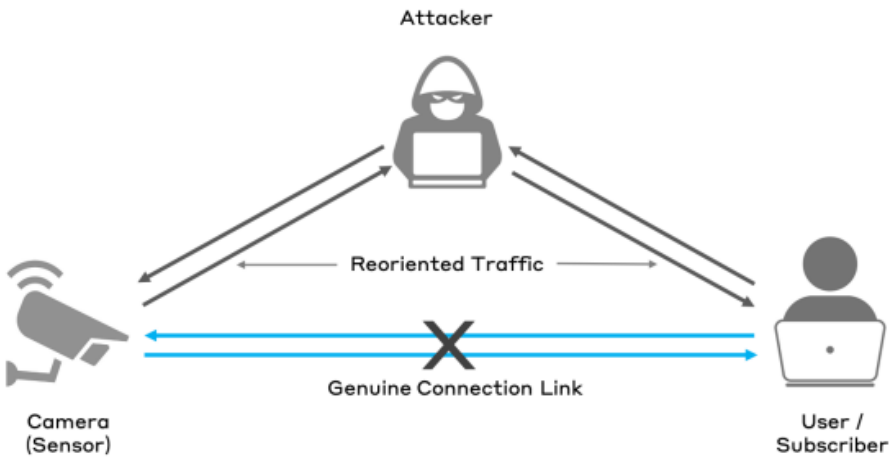
Οι παθητικές επιθέσεις στο IoT είναι δύσκολο να εντοπιστούν και μπορούν να έχουν σοβαρές συνέπειες για την ασφάλεια και την ιδιωτικότητα. Η κατανόηση των τύπων αυτών των επιθέσεων και η εφαρμογή κατάλληλων μέτρων προστασίας είναι κρίσιμη για την ασφαλή λειτουργία των IoT συστημάτων.

2.2.2 Ενεργές Επιθέσεις

Οι ενεργές επιθέσεις στο IoT αποτελούν σημαντική απειλή για την ασφάλεια των συστημάτων, με ποικίλες μορφές και τεχνικές που εξελίσσονται συνεχώς.

Κατηγορίες Ενεργών Επιθέσεων:

- **DDoS μέσω IoT Botnets**: Οι επιθέσεις DDoS που εκτελούνται μέσω botnets αποτελούμενων από συσκευές IoT έχουν αυξηθεί σημαντικά. Οι επιθέσεις αυτές εκμεταλλεύονται την ευπάθεια των συσκευών IoT και μπορούν να προκαλέσουν σοβαρές διαταραχές σε κρίσιμες υποδομές [35].
- **Κακόβουλες Ενέσεις Δεδομένων και Παραποίηση Πληροφοριών**:Οι επιθέσεις που στοχεύουν στην εισαγωγή κακόβουλων δεδομένων ή την παραποίηση υπαρχουσών πληροφοριών μπορούν να προκαλέσουν σοβαρές δυσλειτουργίες. Οι επιθέσεις αυτές εκμεταλλεύονται αδυναμίες στα πρωτόκολλα επικοινωνίας, επιτρέποντας σε επιτιθέμενους να εκτελέσουν απομακρυσμένο κώδικα ή να αποκτήσουν έλεγχο συστημάτων [36].
- **Επιθέσεις MitM**: Οι επιθέσεις MitM επιτρέπουν σε επιτιθέμενους να υποκλέψουν και να τροποποιήσουν την επικοινωνία μεταξύ συσκευών IoT. Η απουσία ισχυρών μηχανισμών κρυπτογράφησης και αυθεντικοποίησης καθιστά τα συστήματα IoT ιδιαίτερα ευάλωτα σε τέτοιες επιθέσεις [37].



Σχήμα 2.1 : Γενική αναπαράσταση της επίθεσης MiTM.

2.3 Πρωτόκολλα Αυθεντικοποίησης

Η αυθεντικοποίηση αποτελεί κρίσιμο στοιχείο για την ασφάλεια του IoT. Διάφορα πρωτόκολλα έχουν αναπτυχθεί για διαφορετικά περιβάλλοντα, όπως:

- **Machine-to-Machine (M2M)**: Επικοινωνία μεταξύ συσκευών χωρίς ανθρώπινη παρέμβαση.
- **Internet of Vehicles (IoV)**: Διασύνδεση οχημάτων για ανταλλαγή πληροφοριών.
- **Internet of Energy (IoE)**: Διαχείριση ενεργειακών πόρων μέσω IoT.
- **Internet of Sensors (IoS)**: Δίκτυα αισθητήρων για συλλογή δεδομένων.

Η επιλογή του κατάλληλου πρωτοκόλλου εξαρτάται από τις απαιτήσεις του εκάστοτε περιβάλλοντος [7].

2.4 Προκλήσεις στην Ασφάλεια και την Ιδιωτικότητα

Η ετερογένεια των συσκευών και η ευρεία διασύνδεσή τους δημιουργούν προκλήσεις. Η **Ασυμβατότητα Πρωτοκόλλων** στο IoT αποτελεί ένα από τα βασικά προβλήματα που επηρεάζουν την ευελιξία και την επεκτασιμότητα των συστημάτων IoT. Διαφορετικά πρωτόκολλα επικοινωνίας, όπως το ZigBee, BLE, και LoRaWAN, έχουν σχεδιαστεί για διαφορετικές απαιτήσεις και περιβάλλοντα, με αποτέλεσμα να μην είναι άμεσα συμβατά μεταξύ τους, γεγονός που δυσχεραίνει την ενσωμάτωση και διαλειτουργικότητα των συσκευών [95], [96]. Οι αιτίες αυτής της ασυμβατότητας μπορεί να είναι διάφορες. Κάποια πρωτόκολλα μπορεί να λειτουργούν σε διαφορετικό επίπεδο [95]. Κάθε πρωτόκολλο ακολουθεί διαφορετικά πρότυπα ασφάλειας, μορφές δεδομένων, και διαδικασίες σύνδεσης [97]. Οι IoT συσκευές διαφέρουν σημαντικά σε επεξεργαστική ισχύ, μνήμη, και ενέργεια, με αποτέλεσμα τα πρωτόκολλα να προσαρμόζονται ανάλογα, δυσχεραίνοντας την ομογενοποίηση [98]. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί συντονισμένες προσπάθειες από την επιστημονική κοινότητα και τη βιομηχανία [8].

2.5 Σύγχρονες Προσεγγίσεις στην Ασφάλεια του IoT

Η ασφάλεια στο IoT αποτελεί κρίσιμο τομέα έρευνας λόγω της αυξανόμενης χρήσης δικτυωμένων συσκευών που συλλέγουν, επεξεργάζονται και ανταλλάσσουν δεδομένα. Οι βασικές προκλήσεις αφορούν την ποικιλομορφία των συσκευών, τους περιορισμούς σε πόρους (μνήμη, επεξεργαστική ισχύ), και το μεγάλο εύρος επιθέσεων.

Η χρήση **πολυεπίπεδων προσεγγίσεων ασφαλείας** είναι απαραίτητη, όπου η ασφάλεια εφαρμόζεται σε κάθε επίπεδο της αρχιτεκτονικής IoT: από το φυσικό επίπεδο και το επίπεδο δικτύου μέχρι το επίπεδο εφαρμογών. Αυτή η στρατηγική εξασφαλίζει ανθεκτικότητα έναντι διαφόρων τύπων απειλών, όπως επιθέσεις σε επίπεδο δικτύου (DDoS), παραβίαση δεδομένων, και κακόβουλο λογισμικό [99].

Λόγω των περιορισμών σε πόρους, προσαρμοσμένα **κρυπτογραφικά πρωτόκολλα** μικρής πολυπλοκότητας έχουν αναπτυχθεί για το IoT. Επιπλέον, η διαχείριση κλειδιών αποτελεί πρόκληση, καθώς απαιτεί ασφαλή αποθήκευση και ανταλλαγή κλειδιών σε περιβάλλοντα με ελάχιστα μέσα ασφαλείας [100].

Η **αυθεντικοποίηση** των συσκευών και των χρηστών είναι κρίσιμη για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Τεχνικές όπως η βιομετρική αυθεντικοποίηση, η χρήση ψηφιακών πιστοποιητικών και οι μηχανισμοί βασισμένοι σε blockchain έχουν προταθεί ως λύσεις [101].

Η **εφαρμογή συστημάτων ανίχνευσης εισβολών** ειδικά προσαρμοσμένων στο IoT έχει σημαντική σημασία για την ανάλυση της κίνησης και την ανίχνευση ανωμαλιών. Τεχνικές μηχανικής μάθησης ενισχύουν τα IDS, δίνοντας τη δυνατότητα αυτόματης προσαρμογής και αναγνώρισης νέων τύπων επιθέσεων [102].

Η **ενσωμάτωση μεθόδων απομόνωσης κρίσιμων τμημάτων** του συστήματος και η χρήση τεχνικών **ανθεκτικότητας** (resilience) είναι τρόποι για να διασφαλίσουν τη συνεχή λειτουργία ακόμη και μετά από επιθέσεις [103].

Η ένταξη **τεχνητής νοημοσύνης** στην ασφάλεια του IoT είναι μια από τις πιο ενεργές περιοχές έρευνας, δεδομένης της πολυπλοκότητας και της δυναμικής φύσης των απειλών που αντιμετωπίζουν τα δίκτυα IoT.

Τα συστήματα **IDS** που βασίζονται σε αλγορίθμους μηχανικής μάθησης, όπως δέντρα αποφάσεων, SVM και νευρωνικά δίκτυα, έχουν αποδειχθεί αποτελεσματικά στην αναγνώριση κακόβουλης δραστηριότητας σε περιβάλλοντα IoT. Η δυνατότητα αυτο-μάθησης και προσαρμογής επιτρέπει την ανίχνευση νέων, άγνωστων επιθέσεων [104].

Με τη χρήση αλγορίθμων **βαθιάς μάθησης** (deep learning), είναι εφικτή η πρόβλεψη επιθέσεων πριν αυτές εκδηλωθούν πλήρως. Τα μοντέλα μαθαίνουν πρότυπα συμπεριφοράς από μεγάλα σύνολα δεδομένων και εντοπίζουν ανωμαλίες σε πραγματικό χρόνο, προσφέροντας προληπτική ασφάλεια [105].

Η τεχνητή νοημοσύνη ενισχύει μεθόδους **βιομετρικής αυθεντικοποίησης** και ανίχνευσης ψεύτικων ταυτοτήτων, βελτιώνοντας την ακρίβεια και μειώνοντας τα ψευδώς θετικά ή αρνητικά σφάλματα σε συστήματα IoT [106].

Η τεχνητή νοημοσύνη επιτρέπει την **αυτοματοποίηση διαδικασιών ασφαλείας**, όπως η διαχείριση ενημερώσεων, η ανάλυση απειλών και η απόκριση σε συμβάντα, μειώνοντας την ανθρώπινη παρέμβαση και αυξάνοντας την ταχύτητα αντίδρασης [107].

Μέσω τεχνικών τεχνητή νοημοσύνη, όπως η ομοσπονδιακή μάθηση (federated learning), μπορεί να επιτευχθεί εκπαίδευση μοντέλων σε κατανεμημένα δεδομένα IoT χωρίς να μετακινούνται ευαίσθητα δεδομένα, ενισχύοντας την προστασία της ιδιωτικότητας [108].

2.6 Σύνολα Δεδομένων

Στον τομέα της ασφάλειας στον κυβερνοχώρο, τα datasets είναι απαραίτητα, ιδίως όταν πρόκειται για την εκπαίδευση μοντέλων ML και DL που έχουν σχεδιαστεί ειδικά για την ασφάλεια του IoT. Παρακάτω, εξετάζονται διάφορα σημαντικά datasets που είναι χρήσιμα για την δημιουργία και την βελτίωση των αλγορίθμων που προορίζονται για τον εντοπισμό, την πρόβλεψη και την αντίδραση σε απειλές. Κάθε dataset προσφέρει πληθώρα πληροφοριών που βοηθούν στην προσομοίωση πραγματικών καταστάσεων, ανεξάρτητα από το αν επικεντρώνεται στην κυκλοφορία του δικτύου, στην συμπεριφορά των botnet ή σε άλλα συγκεκριμένα περιστατικά ασφαλείας.

- **UNSW-NB15**: Το dataset UNSW-NB15 αποτελεί πολύτιμο υλικό για την έρευνα στον τομέα της ανίχνευσης κακόβουλων σε δίκτυα. Περιέχει 2.540.044 εγγραφές, συμπεριλαμβανομένων 2.218.761 περιπτώσεων κανονικής κυκλοφορίας και 321.283 περιπτώσεων κακόβουλης κυκλοφορίας. Αυτό το σύνολο δεδομένων αντιπροσωπεύει εννέα μεγάλες οικογένειες επιθέσεων, παρέχοντας ένα εκτεταμένο και ρεαλιστικό περιβάλλον δοκιμών για τα IDS. Περιλαμβάνει ένα ολοκληρωμένο σύνολο 49 χαρακτηριστικών που καταγράφουν τόσο τα

βασικά στατιστικά στοιχεία όσο και πιο σύνθετα χαρακτηριστικά, τα οποία είναι κρίσιμα για την ανάλυση και την κατανόηση της συμπεριφοράς του δικτύου [317].

- **BoT-IoT**: Το dataset BoT-IoT είναι ένα βασικό εργαλείο προσαρμοσμένο για την ανάλυση της ασφάλειας του IoT. Με πάνω από 73 εκατομμύρια εγγραφές, 9.543 κανονικές και 73.360.900 περιπτώσεις κακόβουλης κίνησης, προσομοιώνει ολοκληρωμένα περιβάλλοντα IoT. Με 45 μοναδικά χαρακτηριστικά ανά εγγραφή, αυτό το dataset είναι ειδικά φτιαγμένο για να μιμείται τα ζητήματα ασφαλείας του IoT στον πραγματικό κόσμο, περιλαμβάνοντας επιθέσεις όπως DDoS, DoS και botnet. Είναι ιδανικό για την δημιουργία και την δοκιμή προηγμένων λύσεων ασφαλείας, όπως μοντέλα μηχανικής και βαθιάς μάθησης, τα οποία εξαρτώνται από μεγάλα και ποικίλα datasets προκειμένου να εντοπίζουν και να αντιμετωπίζουν με ακρίβεια τις πιθανές απειλές [318].
- **NSL-KDD**: Το dataset NSL-KDD είναι μια βελτιωμένη έκδοση του dataset KDD'99, ειδικά σχεδιασμένο για να βελτιώσει την εκπαίδευση και την δοκιμή των IDS. Περιέχει 125.973 εγγραφές εκπαίδευσης και 22.554 εγγραφές δοκιμής, επιτρέποντας την αποτελεσματική αξιολόγηση των μοντέλων χωρίς να απαιτούνται υπερβολικοί υπολογιστικοί πόροι. Το dataset περιέχει 41 χαρακτηριστικά που αντιπροσωπεύουν ένα ευρύ φάσμα δεδομένων. Είναι σημαντικό ότι το NSL-KDD περιλαμβάνει ένα ισορροπημένο μείγμα κανονικής κυκλοφορίας και στοχευμένων επιθέσεων στον κυβερνοχώρο, όπως DoS, R2L (Remote to Local Attack), Probe και U2R (User to Root Attack), παρέχοντας ένα ρεαλιστικό σενάριο για τα IDS [319].
- **N-BaIoT**: Το dataset N-BaIoT έχει σχεδιαστεί ειδικά για την βελτίωση των συστημάτων ασφαλείας IoT έναντι επιθέσεων botnet. Αυτό το πλούσιο σε πόρους dataset περιέχει δεδομένα από ένα ευρύ φάσμα συσκευών IoT, όπως κάμερες ασφαλείας, θερμοστάτες και οθόνες παρακολούθησης βρέφων, οι οποίες έχουν μολυνθεί με διάφορα κακόβουλα λογισμικά, συμπεριλαμβανομένων γνωστών όπως το Mirai και το Bashlite. Διαθέτει μια μεγάλη συλλογή από 115 διαφορετικά χαρακτηριστικά, καταγράφοντας ένα ευρύ φάσμα δεδομένων που παρέχουν πληροφορίες σχετικά με την συμπεριφορά των μολυσμένων συσκευών. Το dataset περιέχει μεγάλο όγκο δεδομένων, συμπεριλαμβανομένων 6.506.674 κακόβουλα και 555.932 μη κακόβουλα δεδομένα [320].
- **IoT-23**: Το dataset IoT-23 περιέχει μια λεπτομερή συλλογή δεδομένων κίνησης δικτύου που έχει σχεδιαστεί ειδικά για την ανάλυση των απειλών ασφαλείας του IoT. Κατηγοριοποιεί είκοσι κακόβουλες και τρεις μη κακόβουλες συσκευές, παρέχοντας μια λεπτομερή κατανόηση των προκλήσεων ασφαλείας. Περιλαμβάνει μεγάλο όγκο δεδομένων που συλλέχθηκαν από το 2018 έως το 2020, με 30.858.735 μη κακόβουλα δεδομένα και 294.449.255 κακόβουλα δεδομένα, αποδεικνύοντας την επικράτηση των απειλών στον κυβερνοχώρο σε περιβάλλοντα IoT. Το κάθε δεδομένο συνοδεύεται με 6 χαρακτηριστικά [321].
- **Edge-IIoT**: Το dataset Edge-IIoT είναι ειδικά σχεδιασμένο για την διερεύνηση των ζητημάτων κυβερνοασφάλειας σε περιβάλλοντα που αφορούν το βιομηχανικό IoT. Περιλαμβάνει πληροφορίες που συλλέχθηκαν από 15 διαφορετικές συσκευές, παράγοντας ένα dataset με 61 χαρακτηριστικά και συνολικά 20.952.648 δεδομένα, που περιλαμβάνουν 9.728.708 κακόβουλα και 11.223.940 κανονικά δεδομένα. Το dataset περιλαμβάνει ένα ευρύ φάσμα τύπων δεδομένων, από λειτουργικές καταστάσεις έως μετρήσεις αισθητήρων, και παρέχει μια ολοκληρωμένη προσομοίωση των αλληλεπιδράσεων στον πραγματικό κόσμο μεταξύ των συσκευών IIoT (Industrial Internet of Things). Επίσης, περιλαμβάνει 14 διαφορετικά είδη επιθέσεων, συμπεριλαμβανομένων μολύνσεων από κακόβουλο λογισμικό και DDoS [322].
- **ToN-IoT**: Το dataset ToN-IoT προορίζεται να διευκολύνει την λεπτομερή έρευνα σχετικά με την ασφάλεια των δικτύων IIoT, περιλαμβάνοντας δεδομένα τόσο για τυπικές λειτουργίες όσο και για πιθανές απειλές ασφαλείας. Περιέχει ένα σύνολο εννέα διαφορετικών τύπων επιθέσεων,

παρέχοντας ένα ευρύ φάσμα κακόβουλων σεναρίων για έρευνα. Το dataset περιέχει ένα ικανοποιητικό όγκο δεδομένων, με 300.000 δεδομένα που έχουν ταξινομηθεί ως κακόβουλα και 161.043 ως μη κακόβουλα δεδομένα. Με 44 χαρακτηριστικά, το ToN-IoT παρέχει μια λεπτομερή εικόνα της συμπεριφοράς του δικτύου και της συσκευής, επιτρέποντας την ανάπτυξη εξελιγμένων μοντέλων ML και DL, ικανών να διακρίνουν μεταξύ κανονικών και ανώμαλων δραστηριοτήτων [297].

- **CTU-13**: Το dataset CTU-13 είναι ένας από τους λίγους διαθέσιμους στο κοινό πόρους που προσφέρει μια λεπτομερή εξέταση διαφόρων δειγμάτων botnet σε 13 διαφορετικά σενάρια. Είναι ειδικά σχεδιασμένο για την εις βάθος ανάλυση της συμπεριφοράς των botnet μέσα στην κυκλοφορία του δικτύου. Συγκεκριμένα, με 1.535.374 δεδομένα ταξινομημένα ως κακόβουλα και 3.181.797 δεδομένα ταξινομημένα ως μη κακόβουλα, το dataset περιέχει μια μεγάλη ποικιλία δεδομένων, επιτρέποντας την αξιόπιστη εκπαίδευση των IDS. Επιπλέον, το dataset περιλαμβάνει μόλις 6 χαρακτηριστικά που είναι απαραίτητα για την ανίχνευση της κίνησης που δημιουργείται από botnet, επιτρέποντας μια πιο αποτελεσματική και στοχευμένη ανάλυση [323].
- **DIDarknet**: Τα datasets CXVPN2016 [105] και ISCXTor2017 [106] συνδυάστηκαν για την δημιουργία του DIDarknet, μιας μεγάλης συλλογής που σχεδιάστηκε κυρίως για την ανάλυση της κυκλοφορίας του darknet σε συνδυασμό με την μη κακόβουλη δραστηριότητα του δικτύου. Υπάρχουν συνολικά 158.659 δεδομένα, εκ των οποίων 24.311 έχουν ταξινομηθεί ως δεδομένα darknet και 134.348 μη κακόβουλα δεδομένα. Με 44 ολοκληρωμένα χαρακτηριστικά ανά εγγραφή, αυτό το dataset βοηθά σημαντικά στην δημιουργία μοντέλων για την αντιμετώπιση της κίνησης από darknet επιθέσεις [324].
- **IoT-Botnet 2020**: Το IoT-Botnet 2020 είναι μια ολοκληρωμένη συλλογή απειλών στον κυβερνοχώρο ειδικά για περιβάλλοντα IoT, όπως DDoS, DoS, σαρώσεις δικτύου και κλοπή πληροφοριών. Διαθέτει συνολικά 1.940.389 δεδομένα, με 97.197 μη κακόβουλα και 1.843.192 κακόβουλα δεδομένα. Επίσης προσφέρει μία λεπτομερή ανάλυση με 85 χαρακτηριστικά ανά εγγραφή [325].
- **CICIDS2017**: Ένας βασικός πόρος για την έρευνα στον τομέα της κυβερνοασφάλειας είναι το dataset CICIDS2017, το οποίο είναι ιδιαίτερα χρήσιμο για τον σχεδιασμό και την αξιολόγηση των IDS. Διαθέτει 2.830.540 δεδομένα που κατανέμονται σε 83 χαρακτηριστικά, με 2.359.087 μη κακόβουλα και 471.453 κακόβουλα δεδομένα. Αυτό το dataset προσομοιώνει την πραγματική κίνηση δικτύου σε έναν μεσαίου μεγέθους οργανισμό, καταγράφοντας τις δραστηριότητες μιας εβδομάδας με 15 διαφορετικούς τύπους επιθέσεων, όπως DDoS, botnets και σαρώσεις θυρών δικτύου [326].

Dataset	Αριθμός Χαρακτηριστικών	Δεδομένα	Μη κακόβουλα Δεδομένα	Κακόβουλα Δεδομένα
UNSW-NB15	49	2.540.044	2.218.761	321.283
BoT-IoT	45	73.370.493	9.543	73.360.900
NSL-KDD	41	148.527	22.554	125.973
N-BaIoT	115	7.062.606	555.932	6.506.674
IoT-23	6	60.307.990	30.858.735	294.449.255
Edge-IIoT	61	20.952.648	11.223.940	9.728.708
ToN-IoT	44	461.043	161.043	300.000
CTU-13	6	4.717.171	3.181.797	1.535.374
DIDarknet	44	158.659	134.348	24.311
IoT-Botnet 2020	85	1.940.389	97.197	1.843.192
CICIDS2017	83	2.830.540	2.359.087	471.453

Σχήμα 2.2 : Σύνοψη των Datasets.

2.7 Επίλογος

Η ασφάλεια στο IoT αποτελεί πολυδιάστατο πρόβλημα που απαιτεί συνδυασμό τεχνολογικών λύσεων, τυποποίησης και συνεχούς έρευνας. Η κατανόηση των απειλών και η ανάπτυξη κατάλληλων μηχανισμών προστασίας είναι απαραίτητες για την ασφαλή ενσωμάτωση του IoT στην καθημερινή ζωή.

Κεφάλαιο 3ο: Πρωτόκολλα στα χαμηλότερα επίπεδα του IoT

3.1 Εισαγωγή

Στο IoT τα πρωτόκολλα των χαμηλότερων επιπέδων διαδραματίζουν καθοριστικό ρόλο στα επίπεδο αντίληψης και δικτύου. Εδώ πραγματοποιείται η συλλογή δεδομένων από αισθητήρες και η μεταφορά τους μέσω κατάλληλων τεχνολογιών επικοινωνίας. Η κατανόηση των σχετικών πρωτοκόλλων είναι απαραίτητη για τον σχεδιασμό αποδοτικών, ασφαλών και επεκτάσιμων συστημάτων IoT.

3.2 Πρωτόκολλα Επιπέδου Δικτύου στο IoT

Στο επίπεδο δικτύου υπάρχουν διάφορα πρωτόκολλα:

- **Routing Protocol for Low-Power and Lossy Networks (RPL)**: Το RPL είναι το πρότυπο πρωτόκολλο δρομολόγησης που αναπτύχθηκε από το IETF για δίκτυα με περιορισμένους πόρους (LLNs), όπως αυτά του IoT.
- **IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)**: Χρησιμοποιεί τεχνικές συμπίεσης και κατακερματισμού των κεφαλίδων IPv6 για να κάνει δυνατή τη μετάδοση μεγάλων πακέτων IPv6 μέσω μικρών δικτύων IEEE 802.15.4, τα οποία χρησιμοποιούνται για εφαρμογές IoT.
- **IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH)**: Το 6TiSCH συνδυάζει το 6LoWPAN με το Time-Slotted Channel Hopping (TSCH), ένα υποσύνολο του IEEE 802.15.4e, για να προσφέρει αξιόπιστη και χαμηλής κατανάλωσης επικοινωνία σε βιομηχανικά δίκτυα IoT.
- **Long Range Wide Area Network (LoRaWAN)**: Το LoRaWAN είναι ένα πρωτόκολλο χαμηλής κατανάλωσης, μεγάλης εμβέλειας, που χρησιμοποιεί την τεχνολογία LoRa για τη μετάδοση δεδομένων σε μεγάλες αποστάσεις.
- **Οικογένεια Πρωτοκόλλων Bluetooth (Bluetooth Classic, Bluetooth Low Energy, Bluetooth Mesh)**: Το πρωτόκολλο Bluetooth, και ιδιαίτερα το Bluetooth Low Energy (BLE), αποτελεί βασικό πυλώνα για την υλοποίηση του IoT, προσφέροντας ασύρματη συνδεσιμότητα χαμηλής ισχύος και κόστους. Το πρωτόκολλο Bluetooth Mesh αποτελεί μια σημαντική εξέλιξη στην ασύρματη επικοινωνία για εφαρμογές του IoT, προσφέροντας επεκτασιμότητα, αξιοπιστία και ενσωματωμένη ασφάλεια.
- **ZigBee** : Το ZigBee είναι μια τεχνολογία δικτύωσης που ανήκει στο IoT και τα χαρακτηριστικά του περιλαμβάνουν χαμηλή κατανάλωση ενέργειας, χαμηλό κόστος και χαμηλή πολυπλοκότητα.[59]
- **SigFox** : Το Sigfox είναι ένα πρωτόκολλο LPWAN (Low Power Wide Area Network) σχεδιασμένο για εφαρμογές του Διαδικτύου των Πραγμάτων (IoT), με στόχο την υποστήριξη συσκευών που απαιτούν μικρή κατανάλωση ενέργειας και περιορισμένη ικανότητα μετάδοσης δεδομένων
- **Z-Wave** : Το Z-Wave είναι μία ευρέως χρησιμοποιούμενη τεχνολογία ασύρματης επικοινωνίας στο IoT που αναπτύχθηκε από τη ZenSys.
- **Wi-Fi** : Το Wi-Fi είναι μία ασύρματη τεχνολογία, το οποίο έχει τις ρίζες του στα πρότυπα IEEE 802.11 και επιτρέπει στις συσκευές να επικοινωνούν ασύρματα, απελευθερώνοντας τες από τους περιορισμούς των φυσικών συνδέσεων [312].

3.2.1 Πρωτόκολλο RPL

Στο RPL, οι συσκευές δημιουργούν ένα κατευθυνόμενο άκυκλο γράφημα (DODAG) το οποίο χρησιμοποιείται για την αποδοτική δρομολόγηση πακέτων δεδομένων μεταξύ συσκευών σε περιορισμένα δίκτυα. Το RPL χρησιμοποιεί δύο βασικές μετρικές για την επιλογή διαδρομών: την ισχύ του σήματος(RSSI) και την καθυστέρηση. Εφαρμόζεται κυρίως σε εφαρμογές που απαιτούν χαμηλή κατανάλωση ενέργειας, όπως η παρακολούθηση περιβάλλοντος και οι έξυπνες πόλεις. [38].

Προκλήσεις σχετικά με το πρωτόκολλο RPL:

- **Αναξιοπιστία σε Δίκτυα με Υψηλή Κίνηση**: Το RPL μπορεί να έχει δυσκολίες σε περιβάλλοντα όπου η κίνηση και η διαχείριση πόρων είναι έντονες. Συσκευές που υποστηρίζουν RPL ενδέχεται να παρεμβάλλονται λόγω υπερφόρτωσης του δικτύου, οδηγώντας σε καθυστερήσεις ή απώλεια πακέτων [38].
- **Επιδόσεις σε Δίκτυα με Μεγάλο Μέγεθος**: Σε μεγάλα δίκτυα, η δρομολόγηση μέσω του DODAG μπορεί να γίνει αναποτελεσματική λόγω του μεγάλου αριθμού κόμβων, με αποτέλεσμα την επιβράδυνση της απόδοσης του δικτύου.

3.2.2 Πρωτόκολλο 6LoWPAN

Ένα βασικό χαρακτηριστικό του 6LoWPAN είναι η συμβατότητά του με το Διαδίκτυο, επιτρέποντας στις συσκευές IoT να αλληλεπιδρούν με άλλες συσκευές ή συστήματα εκτός των ιδιωτικών δικτύων τους. [39].

Προκλήσεις σχετικά με το πρωτόκολλο 6LoWPAN:

- **Συμπίεση Κεφαλίδων**: Η συμπίεση των κεφαλίδων IPv6 μπορεί να προκαλέσει προβλήματα, καθώς η ανάγκη για εξαιρετικά χαμηλή κατανάλωση ενέργειας έρχεται σε αντίθεση με την ανάγκη για μεγάλες, πολύπλοκες κεφαλίδες σε περιβάλλοντα που υποστηρίζουν ασύρματα δίκτυα. Αυτό μπορεί να οδηγήσει σε απώλεια πληροφορίας και μειωμένη απόδοση της επικοινωνίας [39].
- **Συμβατότητα με Παλαιότερες Υποδομές**: Η εφαρμογή του 6LoWPAN σε υπάρχουσες υποδομές δικτύου μπορεί να προκαλέσει προβλήματα συμβατότητας, καθώς απαιτεί την αναβάθμιση ή αντικατάσταση παλαιότερων δικτύων για να υποστηρίξουν IPv6.

3.2.3 Πρωτόκολλο 6TiSCH

Το TSCH επιτρέπει τακτική κατανομή χρόνου για τη μετάδοση πακέτων, μειώνοντας τις παρεμβολές και εξασφαλίζοντας τη σταθερότητα της σύνδεσης. Η αξιοπιστία είναι καθοριστική για το 6TiSCH, και χρησιμοποιείται κυρίως σε περιβάλλοντα που απαιτούν αυστηρούς κανόνες για την καθυστέρηση και την αξιοπιστία, όπως η βιομηχανική αυτοματοποίηση [40].

Προκλήσεις σχετικά με το πρωτόκολλο 6TiSCH:

- **Αναγκαία Χρονική Ακρίβεια**: Για να διασφαλιστεί η αξιοπιστία και η χαμηλή καθυστέρηση του 6TiSCH, απαιτείται απόλυτη ακρίβεια στην κατανομή του χρόνου, κάτι που μπορεί να είναι δύσκολο να επιτευχθεί σε περιβάλλοντα με πολλαπλούς χρήστες και εξωτερικές παρεμβολές [40].
- **Αύξηση Κόστους και Πολυπλοκότητας**: Η ανάγκη για συντονισμό στο επίπεδο του χρόνου και η χρήση του TSCH προσθέτει πολύπλοκες απαιτήσεις στις συσκευές IoT, κάτι που μπορεί να οδηγήσει σε αυξημένο κόστος και σε μεγαλύτερη πολυπλοκότητα στην ανάπτυξή τους.

3.2.4 Πρωτόκολλο LoRaWAN

Το LoRaWAN είναι κατάλληλο για εφαρμογές IoT που απαιτούν μετάδοση μικρών ποσοτήτων δεδομένων σε μεγάλες αποστάσεις, όπως η παρακολούθηση περιβάλλοντος, οι γεωργικές εφαρμογές,

και η διαχείριση απομακρυσμένων συσκευών. Αυτό το πρωτόκολλο χρησιμοποιεί μια ασύμμετρη αρχιτεκτονική με τη χρήση πυλών (gateways), οι οποίες επικοινωνούν με τα "end nodes" μέσω LoRa. Παράλληλα, προσφέρει υψηλή ασφάλεια με ενσωματωμένη κρυπτογράφηση [41].

Προκλήσεις σχετικά με το πρωτόκολλο LoRaWan:

- **Αναγκαίο Εύρος Κάλυψης και Σφάλματα Σήματος**: Το LoRaWAN, αν και παρέχει μεγάλο εύρος, είναι ευαίσθητο σε περιβαλλοντικές παρεμβολές και μπορεί να υποστεί σημαντική εξασθένιση του σήματος σε ορισμένες περιοχές, οδηγώντας σε αυξημένα ποσοστά σφαλμάτων [41].
- **Ασφάλεια και Ιδιωτικότητα**: Το LoRaWAN βασίζεται σε μια δημόσια υποδομή, κάτι που ενδέχεται να δημιουργήσει προβλήματα ασφαλείας και διατήρησης ιδιωτικότητας, καθώς τα δεδομένα ενδέχεται να εκτεθούν σε επιθέσεις κατά την μεταφορά τους.

3.2.5 Πρωτόκολλο Bluetooth

Αρχιτεκτονική και Λειτουργία του **Bluetooth Classic**, γνωστό και ως BR/EDR (Basic Rate/Enhanced Data Rate), λειτουργεί στη ζώνη συχνοτήτων ISM των 2.4 GHz και χρησιμοποιεί 79 κανάλια εύρους 1 MHz. Η αρχιτεκτονική του βασίζεται σε δομή master-slave, επιτρέποντας τη δημιουργία piconet και scatternet δικτύων, όπου μια κύρια συσκευή μπορεί να συνδεθεί με πολλές δευτερεύουσες συσκευές. Υποστηρίζει ρυθμούς μετάδοσης έως 3 Mbps με το EDR, καθιστώντας το κατάλληλο για εφαρμογές που απαιτούν υψηλότερη ταχύτητα, όπως η μετάδοση ήχου και δεδομένων σε πραγματικό χρόνο. Αυτά τα χαρακτηριστικά καθιστούν το Bluetooth Classic κατάλληλο για εφαρμογές που απαιτούν συνεχή ροή δεδομένων και υψηλή ταχύτητα μετάδοσης [55].

Εφαρμογές του Bluetooth στο IoT:

Παρόλο που το Bluetooth Low Energy (BLE) έχει επικρατήσει σε πολλές εφαρμογές IoT λόγω της χαμηλής κατανάλωσης ενέργειας, το Bluetooth Classic εξακολουθεί να χρησιμοποιείται σε περιπτώσεις που απαιτούν υψηλότερους ρυθμούς μετάδοσης και συνεχή ροή δεδομένων. Ενδεικτικά, χρησιμοποιείται σε:

- **Έξυπνες οικιακές συσκευές**: Ηχεία, τηλεοράσεις και συστήματα ψυχαγωγίας που απαιτούν μετάδοση ήχου υψηλής ποιότητας.
- **Ιατρικές συσκευές**: Ορισμένες ιατρικές συσκευές που απαιτούν συνεχή και αξιόπιστη μετάδοση δεδομένων, όπως ορισμένοι τύποι παρακολούθησης καρδιακού ρυθμού.
- **Βιομηχανικές εφαρμογές**: Συστήματα αυτοματισμού που απαιτούν σταθερή και γρήγορη επικοινωνία μεταξύ συσκευών.

Αυτές οι εφαρμογές αναλύονται σε μελέτες που εξετάζουν τη χρήση του Bluetooth Classic σε διάφορα σενάρια του IoT [56].

Ασφάλεια και Προκλήσεις:

Η πολυπλοκότητα του πρωτοκόλλου Bluetooth, με προδιαγραφές που εκτείνονται σε περίπου 3.000 σελίδες, καθιστά δύσκολη την ασφαλή υλοποίησή του. Αυτό έχει οδηγήσει σε ευπάθειες, όπως η "BlueBorne", που επηρέασε δισεκατομμύρια συσκευές, επιτρέποντας σε επιτιθέμενους να αποκτήσουν πρόσβαση σε συσκευές χωρίς φυσική επαφή. Επιπλέον, η διαδικασία σύζευξης μπορεί να παρουσιάσει αδυναμίες, ειδικά όταν δεν εφαρμόζονται τα υψηλότερα διαθέσιμα επίπεδα ασφάλειας. Για την αντιμετώπιση αυτών των προκλήσεων, συνιστάται η χρήση των πιο πρόσφατων εκδόσεων του πρωτοκόλλου και η εφαρμογή βέλτιστων πρακτικών ασφάλειας [57].

Συμπεράσματα και Προτάσεις:

Το Bluetooth Classic παραμένει σημαντικό στο οικοσύστημα του IoT, ιδιαίτερα σε εφαρμογές που απαιτούν υψηλή ταχύτητα και σταθερότητα στη μετάδοση δεδομένων. Ωστόσο, οι προκλήσεις που σχετίζονται με την ασφάλεια και την πολυπλοκότητα του πρωτοκόλλου απαιτούν προσεκτική υλοποίηση και συνεχή ενημέρωση των συσκευών. Οι προγραμματιστές και οι κατασκευαστές θα πρέπει να αξιολογούν τις απαιτήσεις των εφαρμογών τους και να επιλέγουν το κατάλληλο πρωτόκολλο Bluetooth, λαμβάνοντας υπόψη τις ανάγκες σε ταχύτητα, κατανάλωση ενέργειας και ασφάλεια.

3.2.6 Πρωτόκολλο BLE

Βασικά Χαρακτηριστικά του BLE στο IoT:

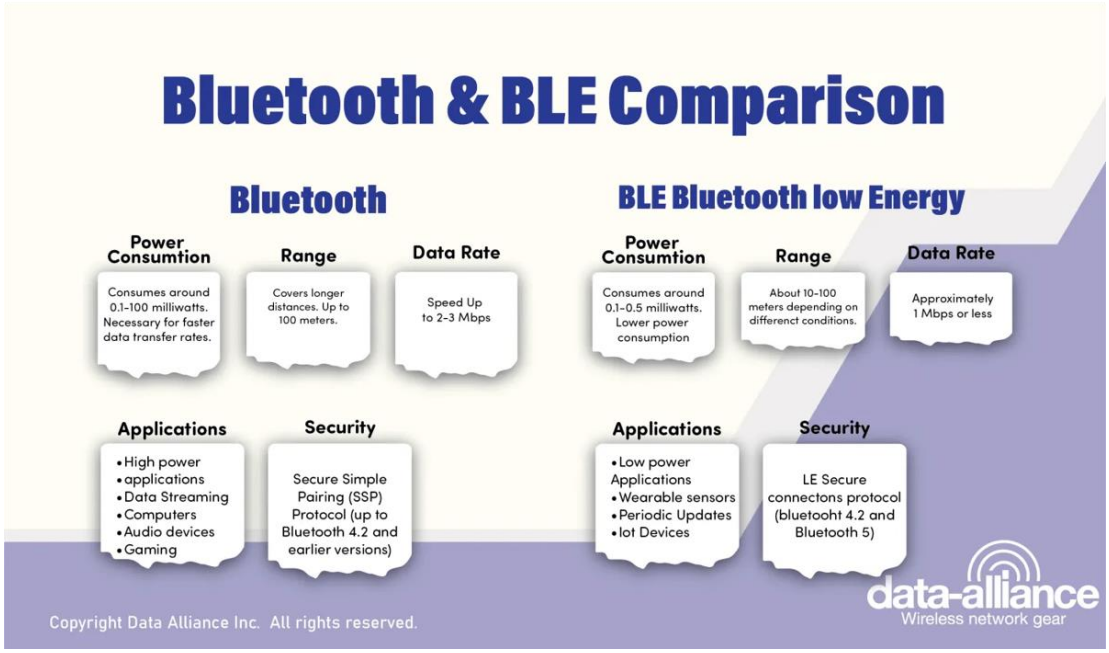
- **Χαμηλή Κατανάλωση Ενέργειας και Απλότητα Ανάπτυξης:** Το BLE σχεδιάστηκε για εφαρμογές που απαιτούν χαμηλή κατανάλωση ενέργειας, επιτρέποντας σε συσκευές να λειτουργούν για μεγάλα χρονικά διαστήματα με μικρές μπαταρίες. Επιπλέον, η απλότητα στην ανάπτυξη και η επαρκής κάλυψη δικτύου καθιστούν το BLE ιδανικό για κόμβους IoT [42].
- **Εξέλιξη του BLE και Υποστήριξη Mesh Networking:** Η εξέλιξη του BLE, ιδιαίτερα με την εισαγωγή του Bluetooth 5.0, ενίσχυσε σημαντικά τις δυνατότητες του πρωτοκόλλου, όπως αυξημένη εμβέλεια και ταχύτητα μετάδοσης. Επιπλέον, η υποστήριξη για mesh networking επιτρέπει την αξιόπιστη επικοινωνία μεταξύ πολλών κόμβων σε δίκτυα IoT [43].
- **Αρχιτεκτονική Πρωτοκόλλου και Βελτιώσεις στο Bluetooth 5:** Η αρχιτεκτονική του BLE περιλαμβάνει τα επίπεδα Controller και Host, βελτιστοποιημένα για σύντομες εκπομπές δεδομένων και λειτουργία χαμηλής ισχύος. Οι βελτιώσεις στο φυσικό επίπεδο (PHY) του Bluetooth 5 ενισχύουν την εμβέλεια και την ταχύτητα σε σχέση με προηγούμενες εκδόσεις [44].

Εφαρμογές του BLE στο IoT:

- **Έξυπνες Οικιακές Συσκευές και Βιομηχανικός Αυτοματισμός:** Το BLE χρησιμοποιείται ευρέως σε εφαρμογές έξυπνων σπιτιών, όπως φωτιστικά, θερμοστάτες και αισθητήρες ασφαλείας, καθώς και σε βιομηχανικά περιβάλλοντα για την παρακολούθηση και τον έλεγχο μηχανημάτων και διαδικασιών [43].
- **Υγειονομική Περίθαλψη και Φορητές Συσκευές:** Συσκευές όπως μετρητές καρδιακών παλμών και γλυκόζης χρησιμοποιούν το BLE για ασφαλή, συνεχή και ενεργειακά αποδοτική μετάδοση δεδομένων, επιτρέποντας την παρακολούθηση της υγείας των ασθενών σε πραγματικό χρόνο [45].
- **BLE Beacons και Εφαρμογές Εντοπισμού:** Τα BLE beacons χρησιμοποιούνται για εφαρμογές εντοπισμού θέσης, όπως στην εσωτερική πλοήγηση σε κτίρια και στην παρακολούθηση περιουσιακών στοιχείων, προσφέροντας χαμηλό κόστος και αυξημένη ακρίβεια [46].

Συγκριτική Ανάλυση Bluetooth Classic και BLE:

Ενώ το BLE έχει σχεδιαστεί για εφαρμογές που απαιτούν χαμηλή κατανάλωση ενέργειας και διαλείπουσα επικοινωνία, το Bluetooth Classic προσφέρει υψηλότερους ρυθμούς μετάδοσης και είναι πιο κατάλληλο για εφαρμογές με συνεχή ροή δεδομένων. Ωστόσο, το BLE υποστηρίζει πιο σύγχρονες λειτουργίες, όπως η σύνδεση με IP δίκτυα μέσω του προφίλ 6LoWPAN, καθιστώντας το πιο ευέλικτο για ορισμένες IoT εφαρμογές [58].



Σχήμα 3.1 : Αναλυτική σύγκριση Bluetooth Classic και BLE.

Ζητήματα Ασφαλείας και Προκλήσεις:

- **Ασφάλεια στο BLE και Απειλές:** Παρόλο που το BLE ενσωματώνει μηχανισμούς ασφαλείας, όπως η κρυπτογράφηση AES-128, εξακολουθούν να υπάρχουν προκλήσεις, όπως η πολυπλοκότητα του πρωτοκόλλου και οι ευπάθειες σε υλοποιήσεις, που μπορούν να οδηγήσουν σε επιθέσεις [47].
- **Προβλήματα στην Ανακάλυψη Συσκευών:** Η διαδικασία ανακάλυψης συσκευών στο BLE μπορεί να παρουσιάσει καθυστερήσεις και προβλήματα, ειδικά σε περιβάλλοντα με πολλές συσκευές, επηρεάζοντας την απόδοση και την αξιοπιστία του δικτύου [48].

Συμπεράσματα:

Το Bluetooth Low Energy αποτελεί κρίσιμο στοιχείο για την ανάπτυξη του IoT, προσφέροντας αποδοτική και ασφαλή ασύρματη επικοινωνία. Ωστόσο, η πολυπλοκότητα του πρωτοκόλλου και οι ευπάθειες που έχουν εντοπιστεί υπογραμμίζουν την ανάγκη για συνεχή έρευνα και βελτίωση στην ασφάλεια και την υλοποίηση του BLE.

3.2.7 Πρωτόκολλο Bluetooth Mesh

Το Bluetooth Mesh βασίζεται στο πρωτόκολλο Bluetooth Low Energy (BLE) και εισάγει μια πολυεπίπεδη αρχιτεκτονική που περιλαμβάνει τα εξής:

- Bluetooth Mesh στο Επίπεδο Αντίληψης:

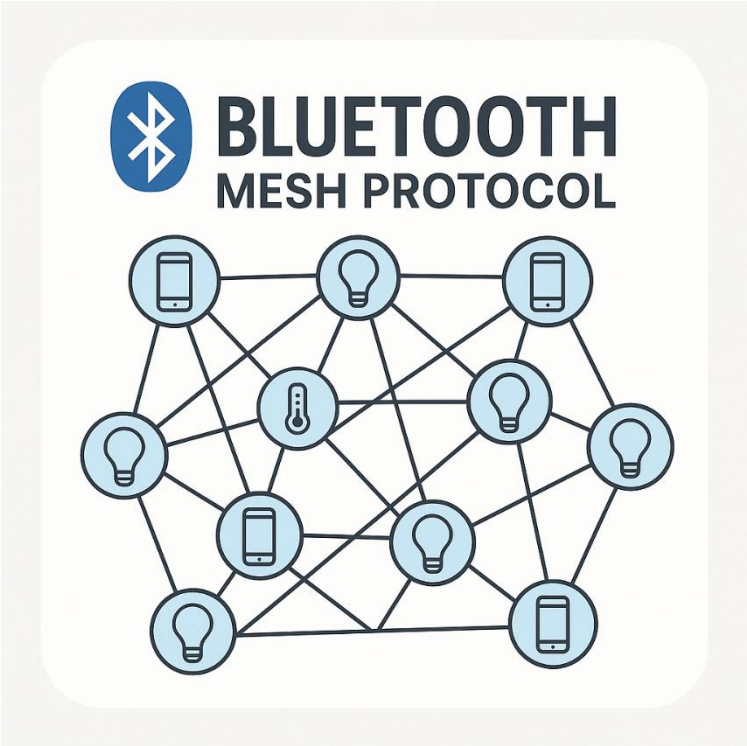
  Στο Επίπεδο Αντίληψης, το Bluetooth Mesh διασφαλίζει τη συλλογή δεδομένων μέσω ασύρματων αισθητήρων και την αποστολή τους σε άλλες συσκευές ή διακομιστές. Στο πλαίσιο του IoT, οι αισθητήρες χρησιμοποιούνται για να παρακολουθούν περιβαλλοντικές παραμέτρους όπως θερμοκρασία, υγρασία και κίνηση. Επειδή το Bluetooth Mesh επιτρέπει τη δημιουργία mesh networks, οι αισθητήρες μπορούν να επικοινωνούν μεταξύ τους μέσω πολλαπλών διαδρομών, καθιστώντας δυνατή τη διαχείριση ενός εκτεταμένου δικτύου [49].
  Το Bluetooth Mesh παρέχει επίσης τη δυνατότητα χαμηλής κατανάλωσης ενέργειας μέσω του BLE, διασφαλίζοντας τη βιωσιμότητα των συσκευών που λειτουργούν με μπαταρίες σε μεγάλες χρονικές περιόδους χωρίς να απαιτούν συχνή αντικατάσταση της μπαταρίας [50].

- Bluetooth Mesh στο Επίπεδο Δικτύου:

  Στο Επίπεδο Δικτύου, το Bluetooth Mesh εξασφαλίζει τη δρομολόγηση και τη μεταφορά των δεδομένων μέσω του mesh routing. Χρησιμοποιεί την τεχνική multi-path routing (μεταφορά μέσω πολλαπλών διαδρομών), η οποία εξασφαλίζει ότι τα δεδομένα μπορούν να φτάσουν στον προορισμό τους ακόμα και αν κάποιος κόμβος αποτύχει. Αυτή η χαρακτηριστική ιδιότητα το καθιστά κατάλληλο για εφαρμογές που απαιτούν υψηλή αξιοπιστία σε μεγάλης κλίμακας περιβάλλοντα, όπως τα έξυπνα κτίρια και οι βιομηχανικές αυτοματοποιήσεις [51]. Το Bluetooth Mesh υποστηρίζει επίσης την ασφάλεια δικτύου μέσω κρυπτογράφησης των μηνυμάτων, εξασφαλίζοντας την εμπιστευτικότητα και ακεραιότητα των δεδομένων που μεταφέρονται. Η προστασία αυτή είναι κρίσιμη για εφαρμογές που χειρίζονται ευαίσθητα δεδομένα, όπως τα βιομηχανικά συστήματα και οι έξυπνοι χώροι υγειονομικής περίθαλψης [52].

- Bluetooth Mesh στο Επίπεδο Εφαρμογής:

  Στο Επίπεδο Εφαρμογής, τα δεδομένα που συλλέγονται και μεταφέρονται μέσω του Bluetooth Mesh χρησιμοποιούνται για την επικοινωνία με εφαρμογές και υπηρεσίες που επεξεργάζονται τα δεδομένα για τη λήψη αποφάσεων. Οι εφαρμογές στο επίπεδο αυτό περιλαμβάνουν τη διαχείριση του φωτισμού, την ενεργοποίηση συσκευών και τη ρύθμιση παραμέτρων του περιβάλλοντος σε πραγματικό χρόνο, βάσει των δεδομένων που λαμβάνονται από τους αισθητήρες [53].



Σχήμα 3.2 : Γενική αναπαράσταση του πρωτοκόλλου Bluetooth mesh.

Η αποτελεσματική διαχείριση των δεδομένων και η ενοποίηση με άλλες πλατφόρμες, όπως τα cloud systems, επιτρέπει την αποθήκευση και ανάλυση μεγάλων ποσοτήτων δεδομένων για την υποστήριξη της διαδικασίας λήψης αποφάσεων. Επίσης, επιτρέπει την ανάπτυξη έξυπνων εφαρμογών που μπορούν να συνδεθούν με έξυπνες πόλεις ή βιομηχανικές υποδομές για την ενίσχυση της λειτουργικότητας και της αποδοτικότητας [54].

Συμπεράσματα:

Το Bluetooth Mesh προσφέρει μια αποδοτική και ευέλικτη λύση για την ανάπτυξη εκτεταμένων δικτύων IoT που εκμεταλλεύονται τα πλεονεκτήματα της χαμηλής κατανάλωσης ενέργειας και της επεκτασιμότητας. Με την εφαρμογή του σε όλα τα επίπεδα της αρχιτεκτονικής τριών επιπέδων του IoT, το Bluetooth Mesh υποστηρίζει τη συλλογή, τη μεταφορά και την επεξεργασία δεδομένων, επιτρέποντας την ανάπτυξη έξυπνων συστημάτων και εφαρμογών σε τομείς όπως τα έξυπνα κτίρια και το βιομηχανικό IoT.

3.2.8 Πρωτόκολλο ZigBee

Στο πρωτόκολλο ZigBee στο **επίπεδο αντίληψης** αφορά τις συσκευές και αισθητήρες που συλλέγουν δεδομένα από το φυσικό περιβάλλον. Στο ZigBee, αυτό αντιστοιχεί στα επίπεδα PHY (Physical) και MAC (Medium Access Control), που ορίζουν τη φυσική μετάδοση και τη διαχείριση πρόσβασης στο ασύρματο μέσο. Υποστηρίζει συχνότητες 2.4 GHz, 915 MHz, 868 MHz με ρυθμό μετάδοσης έως 250 kbps. Χρησιμοποιείται CSMA/CA για αποφυγή συγκρούσεων [60].

Το **Επίπεδο Δικτύου** είναι υπεύθυνο για τη διαχείριση τοπολογίας και δρομολόγησης πακέτων μεταξύ των κόμβων του δικτύου. Υποστηρίζει τοπολογίες αστέρι, δέντρο και πλέγμα. Χρησιμοποιεί πρωτόκολλα δρομολόγησης όπως το AODV. Ενσωματώνει κρυπτογράφηση AES-128 για ασφάλεια. [61], [62].

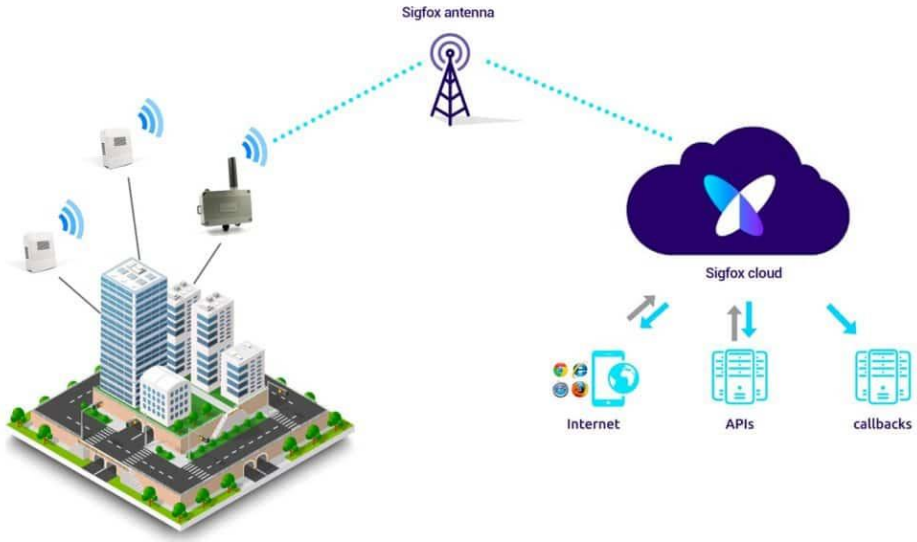
Το **επίπεδο εφαρμογής** περιλαμβάνει το ZigBee Device Object (ZDO), που διαχειρίζεται ρόλους συσκευών και υπηρεσίες, το Application Support Sublayer (APS), που παρέχει λειτουργίες δέσμευσης και ομαδοποίησης και ένα προφίλ εφαρμογών που διασφαλίζουν διαλειτουργικότητα (π.χ. οικιακός αυτοματισμός, βιομηχανική αυτοματοποίηση) [63], [64].

3.2.9 Πρωτόκολλο SigFox

Το **Sigfox** χρησιμοποιεί **αρχιτεκτονική αστέρα** ("star topology") στην οποία οι τερματικές συσκευές επικοινωνούν απευθείας με σταθμούς βάσης, οι οποίοι στη συνέχεια στέλνουν τα δεδομένα στο cloud του Sigfox [65].

Η τεχνολογία βασίζεται στην **Ultra Narrow Band (UNB)** μετάδοση, χρησιμοποιώντας εύρος καναλιού 100 Hz για την **ανοδική ζεύξη** και 1.5 kHz για την **καθοδική**. Η **ανοδική** επικοινωνία χρησιμοποιεί διαφορική δυαδική διαμόρφωση φάσης (**DBPSK**), ενώ η **καθοδική** χρησιμοποιεί **Gaussian Frequency Shift Keying (GFSK)** [65].

Το Sigfox υποστηρίζει κυρίως **μονόδρομη επικοινωνία**, όπου τα πακέτα αναμεταδίδονται **τρεις φορές** σε διαφορετικές συχνότητες για αυξημένη αξιοπιστία [66].



Σχήμα 3.3 : Γενική αναπαράσταση του πρωτοκόλλου SigFox.

Υπάρχει δυνατότητα και **διπλής επικοινωνίας**, αλλά είναι περιορισμένη: επιτρέπονται έως **140 ανοδικά μηνύματα** (uplink) ημερησίως, μέγιστου μεγέθους 12 bytes, και **4 καθοδικά μηνύματα** (downlink), μέχρι 8 bytes το καθένα [67].

Το πρωτόκολλο υποστηρίζει α**υθεντικοποίηση** μέσω μοναδικού αναγνωριστικού συσκευής (Device ID) και συμμετρικού κλειδιού, έ**λεγχο ακεραιότητας** με χρήση **MAC** (Message Authentication Code) και **CRC** και **κρυπτογράγηση AES-128**, χωρίς να είναι ενεργοποιημένη εξ ορισμού, γεγονός που εγείρει ερωτήματα για την ασφάλεια ορισμένων εφαρμογών [68].

Η αποστολή ενός τυπικού μηνύματος (12 bytes) καταναλώνει περίπου **28.1 mA για 8.97 δευτερόλεπτα**, με τη συνολική ενεργειακή κατανάλωση να εξαρτάται από τη συχνότητα μετάδοσης και το μέγεθος του πακέτου. Μεγαλύτερα μηνύματα είναι **ενεργειακά αποδοτικότερα ανά byte** [66].

Παρά τα οφέλη, η μετάδοση σε UNB και η **επαναλαμβανόμενη εκπομπή** πακέτων σε πολλαπλές συχνότητες οδηγεί σε **πιθανές συγκρούσεις** σε περιβάλλοντα με πυκνή συσκευή. Για την αντιμετώπιση αυτών των θεμάτων έχουν προταθεί βελτιώσεις όπως το **SCAP SigFox**, που προσφέρει βελτιωμένη διαχείριση φάσματος [69].

3.2.10 Πρωτόκολλο Z-Wave

Λειτουργεί σε πολλαπλές συχνότητες ανάλογα με την γεωγραφική περιοχή, συνήθως γύρω στα 900 MHz. Οι εμβέλειες μετάδοσης του Z-Wave μπορούν να φτάσουν τα 30 μέτρα σε εσωτερικούς χώρους και έως και τα 100 μέτρα σε εξωτερικούς χώρους, ανάλογα με το περιβάλλον. Όσον αφορά τον ρυθμό δεδομένων, λειτουργεί μεταξύ 9.6 kbps και 100 kbps, θέτοντας την αξιοπιστία και την οικονομία ενέργειας πάνω από την μετάδοση δεδομένων υψηλής ταχύτητας. Λόγω της φήμης του για την αξιοπιστία, την προσιτή τιμή και την χαμηλή κατανάλωση ενέργειας, το Z-Wave είναι μια δημοφιλής επιλογή για λύσεις IoT, ειδικά στον οικιακό αυτοματισμό [310], [311].

3.2.11 Πρωτόκολλο Wi-Fi

Ανάλογα με το χρησιμοποιούμενο πρότυπο IEEE 802.11, μπορεί να υποστηρίξει ένα ευρύ φάσμα ρυθμών μεταφοράς δεδομένων, που κυμαίνονται από 11 Mbps έως 40 Gbps. Μπορεί να καλύψει ένα ευρύ φάσμα απαιτήσεων επικοινωνίας, συμπεριλαμβανομένων εφαρμογών που απαιτούν μεγάλο εύρος ζώνης εκτός από την κανονική περιήγηση στο διαδίκτυο. Το Wi-Fi προσφέρει ευελιξία διπλής ζώνης που λειτουργεί στις ζώνες συχνοτήτων 2.4 GHz και 5 GHz, η οποία βελτιστοποιεί την επιλογή καναλιών, μειώνει τις παρεμβολές και βελτιώνει την συνολική απόδοση. Η ανάπτυξη του WiFi 5 (802.11ac), το οποίο έχει ρυθμό δεδομένων έως και 6.39 Gbps, στο Wi-Fi 6 (802.11ax), το οποίο έχει ρυθμό δεδομένων έως και 9.6 Gbps, και η επερχόμενη αναβάθμιση στο Wi-Fi 7 (802.11be), το οποίο προβλέπεται να αυξήσει ακόμη περισσότερο τον ρυθμό δεδομένων σε 40 Gbps, καταδεικνύει την αφοσίωση για την βελτίωση των δυνατοτήτων που απαιτούνται για την κάλυψη των αυξανόμενων αναγκών των εφαρμογών IoT [313], [314]. Εκτός από την ανάδειξη της αυξημένης αποδοτικότητας και αξιοπιστίας της συνδεσιμότητας, η εξέλιξη αυτή δείχνει μια αξιοσημείωτη αύξηση των ρυθμών μετάδοσης των δεδομένων, υποδεικνύοντας ότι υπάρχει η απαραίτητη υποδομή για την διαχείριση των τεράστιων ποσοτήτων δεδομένων που παράγονται από τις συσκευές IoT και επιτρέποντας ομαλότερες, ταχύτερες και πιο αξιόπιστες επικοινωνίες.

Ένα ενδιάμεσο σημείο πρόσβασης, δεν είναι απαραίτητο για την επικοινωνία P2P χάρη στο Wi-Fi Direct, ένα χαρακτηριστικό της τεχνολογίας Wi-Fi. Το Wi-Fi Direct είναι ένα εργαλείο για την άμεση επικοινωνία μεταξύ των συσκευών στο IoT όταν δεν υπάρχει παραδοσιακή υποδομή δικτύου [313].

Ενσωματωμένο στο πρότυπο 802.11ah, το Wi-Fi HaLow είναι μια εξειδικευμένη ασύρματη λύση που έχει σχεδιαστεί για να ικανοποιεί τις μοναδικές ανάγκες του IoT. Είναι μία τεχνολογία ζώνης συχνοτήτων κάτω του 1 GHz, η οποία είναι μοναδική στο ότι έχει καλύτερη διείσδυση μέσα από εμπόδια και μεγαλύτερη εμβέλεια, γεγονός που την καθιστά ιδανική για ένα ευρύ φάσμα εφαρμογών του IoT. Επίσης το Wi-Fi HaLow δίνει έμφαση στην χαμηλή κατανάλωση ενέργειας, χαρακτηριστικό κρίσιμο για τις εφαρμογές των WSNs [315].

Amendment	Naming Convention	Year	Operating Band	Max Bandwidth	Max Data Rate	PHY	MAC
802.11b	Wi-Fi 1	1999	5 GHz	22 MHz	11 Mbps	DSSS	DCF [1]
802.11a	Wi-Fi 2	1999	2.4 GHz	20 MHz	54 Mbps	OFDM	DCF
802.11g	Wi-Fi 3	2003	2.4 GHz	20 MHz	54 Mbps	MIMO-OFDM	DCF
802.11n	Wi-Fi 4	2008	2.4/5 GHz	40 MHz	600 Mbps	OFDM	DCF + EDCA [2], frame aggregation, BA [3]
802.11ac	Wi-Fi 5	2014	5 GHz	40 MHz	6.39 Gbps	256-QAM, OFDM, DL MIMO, channel bounding	DCF + EDCA, frame aggregation, BA
802.11ah	Wi-Fi HaLow	2017	sub-1 GHz	16 MHz	347 Mbps	OFDM, DL-MU MIMO	EDCA, TWT, RAW [4]
802.11ax	Wi-Fi 6	2019 2020 (6E)	2.4/5 GHz, 6 GHz for Wi-Fi 6E	160 MHz	9.6 Gbps	OFDMA, UL/DL MIMO, channel bounding	DCF + EDCA, frame aggregation, BA, TWT [5], MU channel access
802.11be	Wi-Fi 7	2024	2.4/5/6 GHz	320 MHz	40 Gbps	4096-QAM, Coordinated OFDMA, UL/DL MIMO	HARQ [6] multi-link aggregation, Multi link operation, ...

Σχήμα 3.4 : Περίληψη των διαφόρων χαρακτηριστικών της οικογένειας 802.11 [314].

3.3 Επίλογος

Τα πρωτόκολλα στα χαμηλότερα επίπεδα του IoT αποτελούν το θεμέλιο της επικοινωνίας μεταξύ συσκευών. Η σωστή επιλογή τους εξασφαλίζει ενεργειακή αποδοτικότητα, αξιοπιστία και ευελιξία, προσαρμοσμένη στις απαιτήσεις κάθε εφαρμογής. Καθώς το IoT εξελίσσεται, η κατανόηση αυτών των πρωτοκόλλων παραμένει καθοριστική.

Κεφάλαιο 4ο: Επιθέσεις στα χαμηλότερα επίπεδα του IoT

4.1 Εισαγωγή

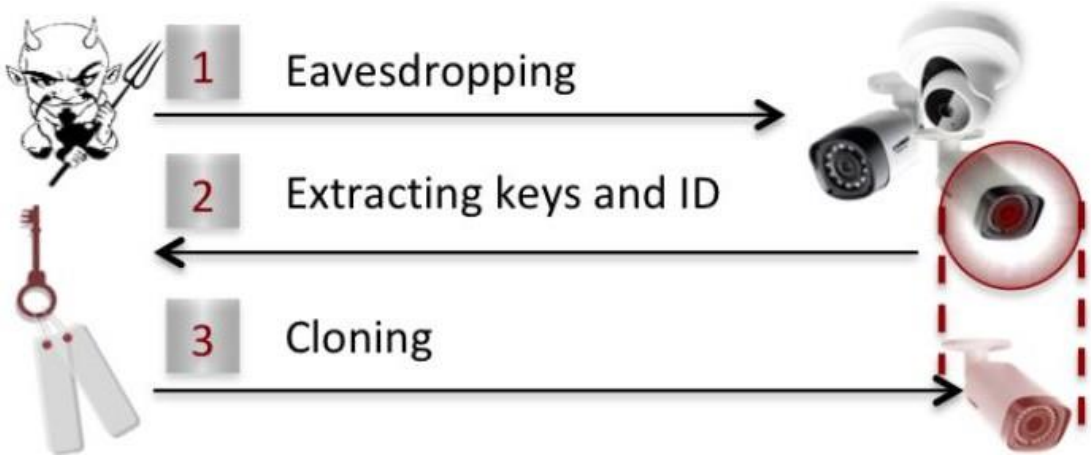
Τα δύο χαμηλότερα επίπεδα του IoT αποτελούν κρίσιμα σημεία για την ασφάλεια, καθώς εμπλέκονται άμεσα στη συλλογή και μετάδοση δεδομένων από και προς τις συσκευές. Η περιορισμένη υπολογιστική ισχύς, οι φυσικοί περιορισμοί των αισθητήρων και η ασύρματη επικοινωνία τα καθιστούν ευάλωτα σε επιθέσεις.

4.2 Επιθέσεις στο επίπεδο Αντίληψης

Το επίπεδο αντίληψης, το οποίο διασυνδέεται απευθείας με τον φυσικό κόσμο για την συλλογή των δεδομένων, λειτουργεί ως η πρώτη γραμμή στην αρχιτεκτονική των συστημάτων IoT. Το παρόν υποκεφάλαιο μετατοπίζεται στην επικέντρωση στις συγκεκριμένες απειλές που στοχεύουν σε αυτό το κρίσιμο επίπεδο. Οι επιθέσεις του επιπέδου αντίληψης εκμεταλλεύονται τις ευπάθειες των αισθητήρων και των συσκευών συλλογής δεδομένων προκειμένου να αλλοιώσουν ή να υποκλέψουν τα μη επεξεργασμένα δεδομένα που είναι απαραίτητα για τις λειτουργίες του IoT. Η ανάλυση που ακολουθεί, αναλύει αυτές τις επιθέσεις και τονίζει το πόσο κρίσιμο είναι να υπάρχουν ισχυρά μέτρα ασφαλείας για την προστασία των βασικών στοιχείων των συστημάτων IoT.

- **Επίθεση Πλευρικού Καναλιού (Side-channel Attack):** Η διαρροή πληροφοριών από την φυσική υλοποίηση μιας συσκευής, όπως η κατανάλωση ενέργειας, οι ηλεκτρομαγνητικές εκπομπές ή οι διακυμάνσεις του χρονισμού, αξιοποιείται από επιθέσεις πλευρικού καναλιού. Οι επιτιθέμενοι μπορούν να αντλήσουν ευαίσθητες πληροφορίες, όπως κρυπτογραφικά κλειδιά ή δεδομένα, εξετάζοντας αυτά τα πλευρικά κανάλια. Για τον προσδιορισμό των μυστικών κλειδιών, οι επιθέσεις ανάλυσης ισχύος για παράδειγμα, παρακολουθούν πόση ισχύ χρησιμοποιεί μια συσκευή κατά την εκτέλεση κρυπτογραφικών λειτουργιών [239]. Με παρόμοιο τρόπο, η ηλεκτρομαγνητική ανάλυση προσπαθεί να αποκρυπτογραφήσει τα κρυπτογραφημένα δεδομένα καταγράφοντας τα σήματα που εκπέμπονται. Τα συστήματα RFID είναι επίσης ευάλωτα σε επιθέσεις πλευρικού καναλιού, ιδίως σε εκείνες που στοχεύουν τα ηλεκτρομαγνητικά σήματα που εκπέμπονται κατά την επικοινωνία μεταξύ των RFID tags και των RFID readers [240].
- **Επίθεση Εξάντλησης Μπαταρίας (Battery Draining Attack):** Η επίθεση που είναι γνωστή ως "εξάντληση της μπαταρίας" έχει ως σκοπό την εξάντληση του ενεργειακού αποθέματος της συσκευής, εμποδίζοντας την να λειτουργήσει κανονικά ή ακόμη και να την θέσουν ολοκληρωτικά εκτός λειτουργίας. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τις ευπάθειες της συσκευής, επιταχύνοντας την εξάντληση των πόρων της μπαταρίας. Αυτές οι επιθέσεις μπορεί να είναι ιδιαίτερα επιβλαβείς σε περιπτώσεις όπου οι συσκευές IoT τοποθετούνται σε σημεία με δύσκολη πρόσβαση και λίγες πηγές ενέργειας ή όταν δεν είναι πρακτικό να αντικαθίστανται συχνά οι μπαταρίες [241], [242].
- **Επίθεση Παρεμβολής (Jamming Attack)**: Η επίθεση παρεμβολής είναι ένας τύπος απειλής, όπου οι κακόβουλοι χρήστες διαταράσσουν σκόπιμα την ασύρματη επικοινωνία τροφοδοτώντας το φάσμα ραδιοσυχνοτήτων με θόρυβο ή σήματα παρεμβολής. Η επίθεση παρεμβολής μπορεί να επηρεάσει την ικανότητα μιας συσκευής IoT να στέλνει ή να λαμβάνει δεδομένα στοχεύοντας στα πρωτόκολλα ασύρματης επικοινωνίας που χρησιμοποιεί η συσκευή. Μπορεί να υπάρξουν σοβαρές επιπτώσεις από αυτή την επίθεση, όπως η απώλεια δεδομένων, η μη διαθεσιμότητα των συστημάτων και η εξάντληση των πόρων [243], [244].

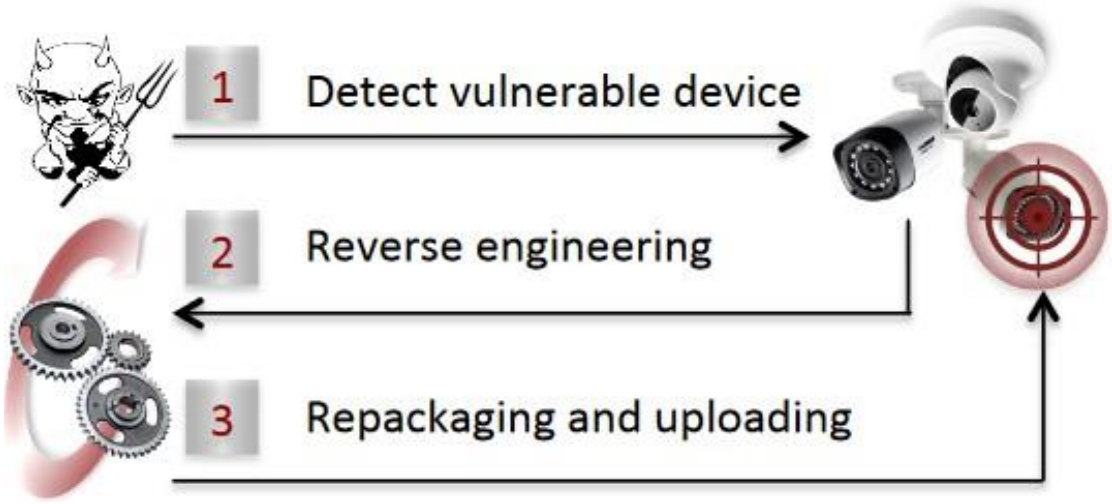
- **Επίθεση Υποκλοπής (Eavesdropping Attack):** Η μη εξουσιοδοτημένη επικοινωνία μεταξύ συσκευών IoT μπορεί να κλαπεί σε επίθεση υποκλοπής, η οποία θα μπορούσε να θέσει σε κίνδυνο τις ευαίσθητες πληροφορίες. Οι επιτιθέμενοι υποκλέπτουν τα πακέτα που αποστέλλονται και λαμβάνονται μεταξύ των συσκευών χωρίς την γνώση ή την συγκατάθεση τους, παρακολουθώντας παθητικά τις ασύρματες μεταδόσεις. Ανάλογα με τον τύπο της εφαρμογής, αυτά τα υποκλαπέντα δεδομένα μπορεί να περιλαμβάνουν ευαίσθητες πληροφορίες ή διαπιστευτήρια της σύνδεσης [245], [242]. Η ασφάλεια και η ιδιωτικότητα των συστημάτων IoT τίθενται σοβαρά σε κίνδυνο από τις επιθέσεις υποκλοπής, ιδίως σε περιβάλλοντα όπου η ασύρματη επικοινωνία είναι κοινή. Για παράδειγμα, οι επιτιθέμενοι μπορούν να υποκλέψουν τα δεδομένα που ανταλλάσσονται μεταξύ συσκευών με δυνατότητα NFC, χρησιμοποιώντας κεραίες που είναι πιο ισχυρές από τις κινητές συσκευές [246].
- **Επίθεση Κατάληψης Κόμβου (Node Capture Attack):** Τα συστήματα IoT είναι ευάλωτα σε επίθεση κατάληψης κόμβου, ιδίως στους κόμβους πύλης (gateway), όπου συγκεντρώνονται σημαντικές λειτουργίες του δικτύου. Οι επιτιθέμενοι παίρνουν τον φυσικό έλεγχο των κομβών πύλης εκμεταλλευόμενοι τις ευπάθειες, γεγονός που τους επιτρέπει την πρόσβαση σε ιδιωτικά δεδομένα, όπως πρωτόκολλα επικοινωνίας και κλειδιά κρυπτογράφησης [244]. Η ακεραιότητα και η εμπιστευτικότητα των δεδομένων που μεταδίδονται στο δίκτυο απειλούνται από αυτή την επίθεση, η οποία μπορεί να καταστήσει δυνατή την υποκλοπή και την τροποποίηση των επικοινωνιών μεταξύ των κόμβων από τους επιτιθέμενους. Επιπλέον, οι παραβιασμένοι κόμβοι πύλης μπορεί να χρησιμοποιηθούν ως σημεία εισόδου για πρόσθετη εκμετάλλευση, δίνοντας στους κακόβουλους χρήστες πρόσβαση για να διεισδύσουν και να θέσουν σε κίνδυνο το περιβάλλον του IoT στο σύνολο του [247].



Σχήμα 4.1: *Φάσεις επίθεσης κατάληψης κόμβου.*

- **Επίθεση Εισαγωγής Ψεύτικων Κόμβων και Κακόβουλων Δεδομένων (Fake Node and Malicious Data Injection Attack):** Αυτή η επίθεση περιλαμβάνει την εισαγωγή κακόβουλων πακέτων δεδομένων στην ροή επικοινωνίας και την προσθήκη μη εξουσιοδοτημένων ή πλαστών συσκευών σε ένα δίκτυο IoT. Μέσω της χρήσης παραπλανητικών συσκευών που μιμούνται αυθεντικούς κόμβους, οι επιτιθέμενοι είναι σε θέση να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και ενδεχομένως να προκαλέσουν βλάβη στις λειτουργίες του συστήματος. Οι επιτιθέμενοι μπορούν να αλλάξουν την συμπεριφορά του συστήματος, να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων και να εξαπατήσουν τους χρήστες ή τις συνδεδεμένες συσκευές εισάγοντας κακόβουλα πακέτα [245]. Επιπλέον, είναι δυνατόν να εισαχθεί κακόβουλος κώδικας στις συσκευές, υποβαθμίζοντας την λειτουργικότητα τους. Η εισαγωγή ψευδών δεδομένων μπορούν να ξεγελάσουν τις συσκευές

διαδίδοντας λανθασμένα αποτελέσματα, τροποποιώντας το λογισμικό ή χειραγωγώντας τις ενδείξεις των αισθητήρων [242].



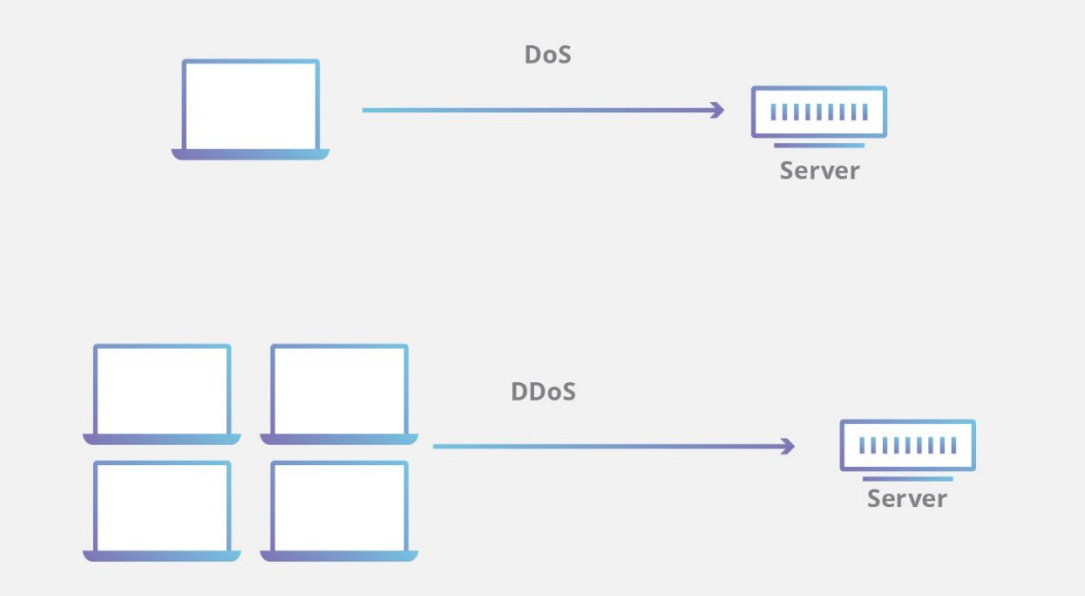
Σχήμα 4.2: Φάσεις τροποποίησης του λογισμικού

- **Επίθεση Αναπαραγωγής (Replay Attack):** Στην επίθεση αναπαραγωγής, έγκυρες μεταδόσεις δεδομένων μεταξύ των συσκευών υποκλέπτονται και επαναμεταδίδονται με κακόβουλο τρόπο σε μεταγενέστερο χρόνο. Οι επιτιθέμενοι ξανά στέλνουν τα πακέτα που έχουν αποσταλεί προηγουμένως στον προοριζόμενο παραλήπτη, με σκοπό να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή να πραγματοποιήσουν μη εξουσιοδοτημένες λειτουργίες [245]. Η επίθεση αναπαραγωγής μπορεί να οδηγήσει σε διάφορους κινδύνους ασφαλείας, όπως παράνομη πρόσβαση σε έξυπνες συσκευές, χειραγώγηση των δεδομένων από αισθητήρες ή διακοπή των υπηρεσιών. Σε ένα περιβάλλον έξυπνου σπιτιού για παράδειγμα, θα ήταν δυνατό για έναν επιτιθέμενο να καταγράψει και να αναπαράγει μία εντολή για το ξεκλείδωμα μιας πόρτας, επιτρέποντας του να εισέλθει στο κτίριο χωρίς εξουσιοδότηση. Επίσης αυτή η επίθεση έχει την δυνατότητα να χειραγωγήσει τις ενδείξεις αισθητήρων, οδηγώντας σε δυσμενή αποτελέσματα.

4.3 Επιθέσεις στο επίπεδο Δικτύου

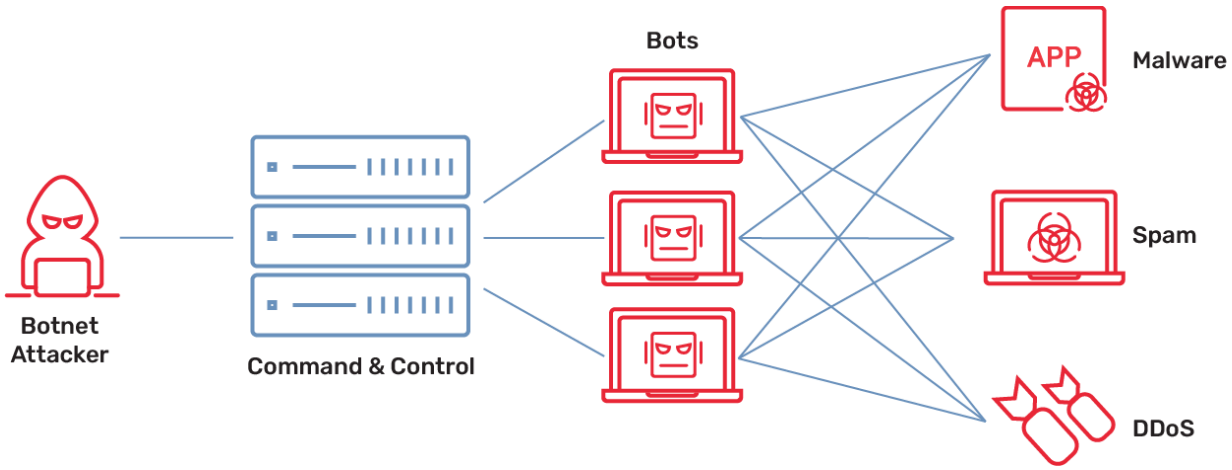
Βάσει ορισμένων ερευνών για την κυβερνοασφάλεια του IoT, υπάρχουν εσωτερικές και εξωτερικές απειλές. Η πιθανότητα εσωτερικής απειλής εμφανίζεται όταν ο επιτιθέμενος βρίσκεται μέσα στο σπίτι ή κοντά σε αυτό. Ενώ η πιθανότητα εξωτερικής απειλής γίνεται μέσω της σύνδεσης στο διαδίκτυο. Μέσω αυτών των δύο τρόπων, ο επιτιθέμενος σκοπεύει να εκθέσει το οικιακό δίκτυο και να παραβιάσει τις συσκευές για να αποκτήσει πρόσβαση στα δεδομένα του καταναλωτή. Οι περισσότερες εξωτερικές απειλές αντιμετωπίζονται με τη χρήση παραδοσιακών μηχανισμών ασφάλειας, όπως τείχη προστασίας (firewalls), Συστήματα Πρόληψης Εισβολών (IPS) και Συστήματα Ανίχνευσης Εισβολών (IDS), τα οποία εγκαθίστανται και ρυθμίζονται στο όριο του Διαδικτύου. Ωστόσο, η αδυναμία των μηχανισμών κρυπτογράφησης και αυθεντικοποίησης στις συσκευές IoT καθιστά απαραίτητο να ληφθούν επιπλέον μέτρα για την εξασφάλιση της ασφάλειας των συσκευών και της εμπιστευτικότητας των δεδομένων [70].

- **Επιθέσεις DoS ή DDoS**: επιθέσεις που θα επηρεάσουν τις στοχευμένες συσκευές και θα έχουν αντίκτυπο στη διαθεσιμότητά τους. Η επίθεση DDoS είναι πιο πολύπλοκη και πιο επικίνδυνη από την επίθεση DoS. Μόλις ο επιτιθέμενος καταφέρει να παραβιάσει πολλές συσκευές, η διάκριση μεταξύ κακόβουλης κίνησης και νόμιμης κίνησης γίνεται δύσκολη [70].



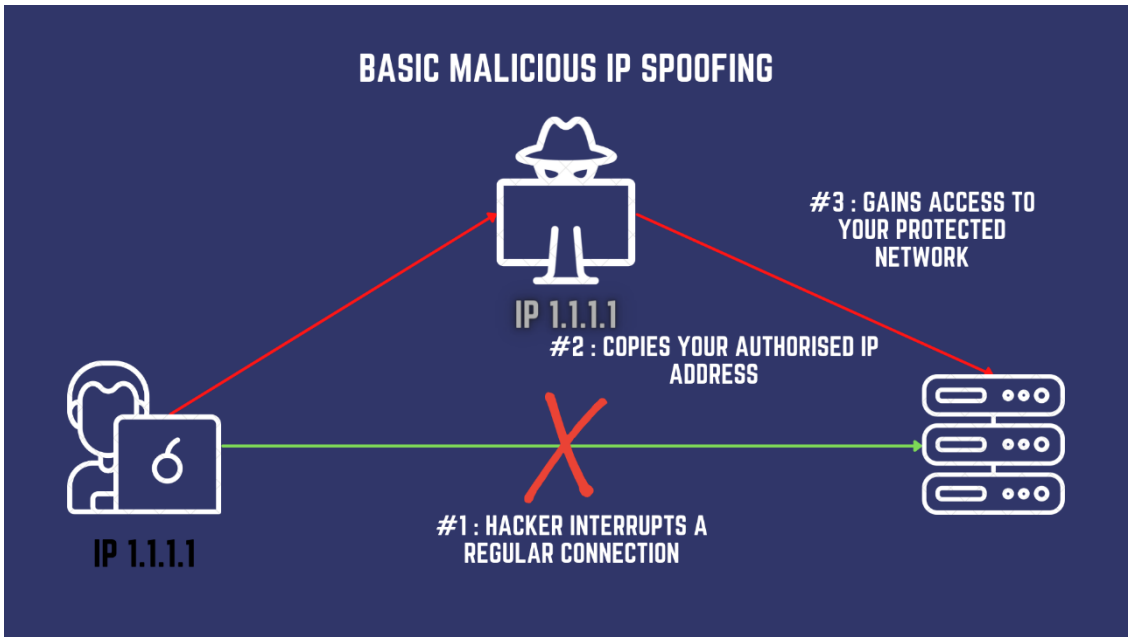
Σχήμα 4.3 : Γενική αναπαράσταση των επιθέσεων DoS και DDoS.

- Τα **IT botnet** χρησιμοποιούνται από τους επιτιθέμενους για να δημιουργήσουν έναν στρατό υποδουλωμένων συσκευών που μπορούν να χρησιμοποιηθούν για να ξεκινήσουν μια επίθεση DDoS σε συγκεκριμένο στόχο. Ο επιτιθέμενος μπορεί να υποδουλώσει μια συσκευή εμφυτεύοντας κακόβουλο λογισμικό που θα δώσει τον έλεγχο της συσκευής στον επιτιθέμενο. Λόγω των αδυναμιών ασφαλείας των συσκευών IoT, αυτές έχουν γίνει οι πλέον προτιμώμενες συσκευές για χρήση ως bots σε ένα botnet. Το 96% των επιθέσεων DDoS παράγεται από τρεις τύπους συσκευών, εκ των οποίων οι περισσότερες είναι συσκευές IoT [70].



Σχήμα 4.4 : Γενική αναπαράσταση της επίθεσης μέσω IT Botnets.

- Η επίθεση **spoofing** συμβαίνει με την προσποίηση νόμιμης ταυτότητας, όπως διεύθυνση IP ή διεύθυνση ελέγχου πρόσβασης μέσου (MAC), που δίνει στον επιτιθέμενο παράνομη πρόσβαση στο σύστημα ή ακόμα και την παρακολούθηση της επικοινωνίας μεταξύ των συσκευών και του διακομιστή εφαρμογών IoT, γεγονός που εκθέτει δεδομένα [70].



Σχήμα 4.5 : Γενική αναπαράσταση της επίθεσης IP Spoofing.

Υπάρχουν διαφόρων ειδών spoofing επιθέσεις:

- ARP Spoofing: Το ARP spoofing συμβαίνει όταν ένας επιτιθέμενος στέλνει πλαστά μηνύματα ARP σε ένα δίκτυο. Συνδέοντας την διεύθυνση IP μιας αξιόπιστης συσκευής στο δίκτυο με την διεύθυνση MAC (Media Access Control) του επιτιθέμενου, αυτό το τέχνασμα τροποποιεί την επικοινωνία ARP. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να κατευθύνει την κυκλοφορία που προοριζόταν για την εν λόγω εξουσιοδοτημένη συσκευή στην δική του συσκευή.
- DNS (Domain Name System) Spoofing: Το DNS spoofing συνεπάγεται στην τροποποίηση των απαντήσεων DNS προκειμένου να ανακατευθήνει την κυκλοφορία από αξιόπιστους servers σε κακόβουλους. Ο επιτιθέμενος έχει την δυνατότητα να τροποποιεί τις εγγραφές DNS και να εξαπατά τις συσκευές ώστε να επικοινωνούν με ψεύτικους ιστότοπους, εκμεταλλεύοντας τις αδυναμίες του πρωτοκόλλου DNS.
- Session Hijacking: Το Session Hijacking είναι μια ιδιαίτερα ύπουλη απειλή, κατά την οποία ο επιτιθέμενος προσπαθεί να κλέψει μια τρέχουσα επικοινωνία μεταξύ δύο συσκευών. Ο επιτιθέμενος εισέρχεται στην συνομιλία απαρατήρητος και κλέβει το αναγνωριστικό της συνεδρίας, το οποίο χρησιμεύει ως μοναδική ταυτοποίηση για κάθε ανταλλαγή. Χρησιμοποιώντας αυτή την τακτική, μπορεί να προσποιηθεί ότι είναι η πραγματική συσκευή και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.

- Επίθεση Δρομολόγησης (Routing Attack): Οι επιθέσεις δρομολόγησης, οι οποίες στοχεύουν στους μηχανισμούς που είναι υπεύθυνοι για την καθοδήγηση της κυκλοφορίας των δεδομένων μεταξύ των κόμβων, αποτελούν σοβαρές απειλές για την αποτελεσματικότητα των δικτύων IoT. Η ικανότητα του δικτύου να παραδίδει τα δεδομένα με ασφάλεια τίθεται σε κίνδυνο από αυτές τις επιθέσεις, οι οποίες εκμεταλλεύονται τις ευπάθειες στα πρωτόκολλα και στους αλγορίθμους δρομολόγησης. Οι επιτιθέμενοι μπορούν να παρεμποδίσουν την επικοινωνία, να αναδρομολογήσουν την κυκλοφορία ή ακόμη και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, αλλοιώνοντας τα μονοπάτια δρομολόγησης [242]. Παρακάτω εξετάζονται οι διάφοροι τύποι επιθέσεων δρομολόγησης που είναι συνηθισμένοι σε περιβάλλοντα του IoT.

- **Επίθεση Μαύρης Τρύπας (Blackhole Attack)**: Ένας παραβιασμένος κόμβος δικτύου, επίσης γνωστός ως κόμβος μαύρης τρύπας, μπορεί να απορρίπτει όλα τα πακέτα δεδομένων που διέρχονται από αυτόν [248]. Υποκλέπτοντας τα πακέτα των νόμιμων κόμβων και εμποδίζοντας τα να φτάσουν στον προορισμό τους, η επίθεση αυτή έχει ως στόχο να παρεμποδίσει την ικανότητα επικοινωνίας των νόμιμων κόμβων. Αφού προσελκύσει την κυκλοφορία, είτε τα χειραγωγεί είτε τα απορρίπτει. Προβάλλοντας τον εαυτό του ως έχοντας την ταχύτερη και καλύτερη διαδρομή προς τον προορισμό, ο κόμβος blackhole συνήθως προσελκύει την κυκλοφορία στον εαυτό του, με σκοπό να τα χειραγωγήσει ή να τα απορρίψει [249].
- Επίθεση Καταβόθρας (Sinkhole Attack): Η επίθεση καταβόθρας είναι μια εξελιγμένη απειλή, στην οποία εμφανίζεται όταν ένας επιτιθέμενος τροποποιεί τις πληροφορίες δρομολόγησης για να κατευθύνει την κυκλοφορία σε ένα κακόβουλο κόμβο. Προκειμένου να ξεγελάσει τους νόμιμους κόμβους ώστε να ανακατευθύνουν τα πακέτα μέσω αυτού, αυτός ο κακόβουλος κόμβος διαφημίζει πλασματικές διαδρομές δρομολόγησης. Ο επιτιθέμενος ελπίζει να προσελκύσει ένα σημαντικό ποσό κίνησης στο δίκτυο εξαπατώντας τις συσκευές, κάνοντας τες να πιστέψουν ότι υπάρχουν καλύτερες διαδρομές. Αυτό θα του δώσει την δυνατότητα να υποκλέψει και να τροποποιήσει τα πακέτα δεδομένων που θα ακολουθήσουν αυτές τις διαδρομές [250], [251].
- Επίθεση Σκουληκότρυπας (Wormhole Attack): Σε μία επίθεση σκουληκότρυπας, κακόβουλοι κόμβοι συνεργάζονται για να δημιουργήσουν μία εικονική σήραγγα που τους επιτρέπει να προωθούν τα πακέτα με υψηλές ταχύτητες μεταξύ τους [252].
- **Επίθεση Επιλεκτικής Προώθησης (Selective Forwarding Attack)**: Η επιλεκτική προώθηση, που μερικές φορές αναφέρεται ως "επίθεση γκρίζας τρύπας (grayhole attack)", είναι επίθεση κατά την οποία ένας κακόβουλος κόμβος επιλέγει ποια πακέτα θα προωθήσει ή θα απορρίψει με βάση την προέλευση ή το περιεχόμενο τους [252]. Η επιλεκτική προώθηση περιλαμβάνει έναν κόμβο που επιλέγει στρατηγικά ποια εισερχόμενα πακέτα θα προωθήσει και ποια θα απορρίψει, σε αντίθεση με τις επιθέσεις blackhole ή sinkhole, όπου οι κόμβοι είτε απορρίπτουν είτε ανακατευθύνουν όλα τα εισερχόμενα πακέτα [248].
- **Επίθεση Sybil**: Ένας κακόβουλος κόμβος θέτει σε κίνδυνο το δίκτυο σε μία επίθεση Sybil χρησιμοποιώντας πολλές ψεύτικες ταυτότητες στον ίδιο φυσικό κόμβο. Αυτός ο κόμβος παριστάνεται ως αξιόπιστος, δίνοντας στον επιτιθέμενο την δυνατότητα να τροποποιήσει τους κανόνες δρομολόγησης [250].
- **Εκμετάλλευση RPL**: Το πρωτόκολλο RPL το οποίο έχει αναλυθεί στο κεφάλαιο 3, είναι ευάλωτο σε διάφορες επιθέσεις λόγω των ευπαθειών του [253]. Οι επιθέσεις που στοχεύουν στη δομή του DODAG, ένα κρίσιμο μέρος του RPL, είναι μεταξύ αυτών των ευπαθειών. Ο βαθμός (rank) DODAG είναι ο στόχος ενός τύπου επίθεσης, κατά την οποία ο επιτιθέμενος χειρίζεται την θέση του στο ιεραρχικό δέντρο για να προσελκύσει μεγάλο αριθμό κόμβων-παιδιών και να κατευθύνει την κυκλοφορία μέσω αυτού. Ένα διαφορετικό είδος επίθεσης είναι όταν δημοσιεύεται ένας υψηλότερος Ασφάλεια το IoT σε χαμηλά επίπεδα 53 αριθμός έκδοσης για το δέντρο DODAG, οδηγώντας τους κόμβους να δημιουργήσουν μία νέα δομή DODAG με βάση τα λανθασμένα δεδομένα. Τέλος, οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιούν πλασματικές διευθύνσεις IP στα μηνύματα DIS (DODAG Information Solicitation), γεγονός που αναγκάζει τους κόμβους να παράγουν μηνύματα DIO (DODAG Information Object), με αποτέλεσμα να επιβαρυνθεί το δίκτυο [248].

- **Εκμετάλλευση 6LoWPAN**: Λόγω της έλλειψης ισχυρών μέτρων ασφαλείας, το πρωτόκολλο 6LoWPAN είναι ευάλωτο σε επιθέσεις. Η έλλειψη ελέγχου ταυτότητας εισάγει μία σοβαρή ευπάθεια που εκμεταλλεύεται από την επίθεση κατακερματισμού (fragmentation attack).

Στέλνοντας κατακερματισμένα πακέτα με πλαστογραφημένες κεφαλίδες και ελέγχοντας την διαδικασία επανασυναρμολόγησης, ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την ευπάθεια για να παρεμποδίσει την επικοινωνία [237], [238] .

Τέτοιου είδους επιθέσεις μπορεί να προκαλέσουν σοβαρές ζημιές στο σύστημα IoT και να εκθέσουν κρίσιμα δεδομένα του καταναλωτή. Επομένως, η ασφάλεια αυτού του επιπέδου είναι πολύ σημαντική για να παρέχει υψηλό επίπεδο προστασίας της ιδιωτικότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

4.4 Ιστορικό επιθέσεων στο IoT

Οι συνέπειες των ευπαθειών του IoT σε αυτή την συνδεδεμένη εποχή υπερβαίνουν κατά πολύ τις παραβιάσεις των δεδομένων και ενέχουν πραγματικούς κινδύνους για τον πραγματικό κόσμο, που κυμαίνονται από την απειλή της ασφάλειας των ευφυών συστημάτων μεταφορών έως την διακοπή ζωτικών υπηρεσιών όπως η παροχή ηλεκτρικής ενέργειας και νερού. Τα προηγούμενα περιστατικά επιθέσεων στο IoT δεν χρησιμεύουν μόνο ως προειδοποιητικές ιστορίες, αλλά παρέχουν επίσης ισχυρή απόδειξη των πραγματικών συνεπειών που προκύπτουν όταν παραμελείται η ασφάλεια του IoT. Ένα παράδειγμα του τρόπου με τον οποίο οι κακόβουλοι εκμεταλλεύονται τις ευπάθειες σε μεγάλη κλίμακα είναι τα botnets, τα οποία είναι δίκτυα μολυσμένων συσκευών υπό τον έλεγχο επιτιθέμενων που πραγματοποιούν συντονισμένες επιθέσεις. Αυτές οι καταγεγραμμένες επιθέσεις αποκαλύπτουν τις πολύπλοκες στρατηγικές και τις ποικίλες προσεγγίσεις που χρησιμοποιούν οι επιτιθέμενοι, έτσι ώστε να κατανοηθούν οι στρατηγικές και να δημιουργηθούν ασφαλέστεροι μηχανισμοί.

Παρακάτω παρουσιάζονται οι γνωστές επιθέσεις, ταξινομημένες με βάση τον αριθμό των παραβιασμένων συσκευών που χρησιμοποιήθηκαν για να έρθει εις πέρας η κάθε επίθεση:

- **Yandex**: Το μέγεθος και η πολυπλοκότητα της επίθεσης DDoS της Yandex, η οποία σημειώθηκε στις 5 Σεπτεμβρίου 2021 και συνδέεται με το botnet Meris, την καθιστούν την μεγαλύτερη επίθεση στην ιστορία. Χρησιμοποιώντας την μέθοδο HTTP (Hypertext Transfer Protocol) pipelining, το botnet μπόρεσε να χρησιμοποιήσει περίπου 250.000 παραβιασμένες συσκευές IoT για να κατακλύσει τους servers της Yandex με 21.8 εκατομμύρια αιτήματα ανά δευτερόλεπτο. Με την χρήση αυτής της τεχνικής, οι επιτιθέμενοι κατάφεραν να πλημμυρίσουν τους servers με ένα τεράστιο όγκο κίνησης, κάνοντας πολλαπλά αιτήματα χωρίς να χρειάζεται να περιμένουν απάντηση [73].
- **OVH**: Στις 22 Σεπτεμβρίου 2016, η OVH, μια γνωστή γαλλική εταιρεία cloud, έγινε στόχος πολλαπλών DDoS επιθέσεων. Οι επιτιθέμενοι πραγματοποίησαν την δεύτερη μεγαλύτερη επίθεση DDoS που έχει καταγραφεί, χρησιμοποιώντας ένα botnet που αποτελούνταν από περίπου 145.607 παραβιασμένες συσκευές IoT, όπως κάμερες IP και DVR. Δύο κύρια κακόβουλα λογισμικά που ήταν υπεύθυνα για τις μολυσμένες συσκευές ήταν το Bashlite και το Mirai. Η κίνηση που δημιουργήθηκε από την επίθεση, κυμάνθηκε από 1.1 Tbps έως 1.5 Tbps και η κάθε συσκευή έστειλε όγκο κίνησης από 1 Mbps έως 30 Mbps. Τα πακέτα που συνδυάστηκαν ήταν TCP/ACK, TCP/Ack+PSH και TCP/SYN [72].
- **Dyn**: Ένα σημαντικό γεγονός συνέβη το 2016, όταν μια επίθεση DDoS είχε ως στόχο την Dyn, μία εταιρεία που προσφέρει υπηρεσίες DNS. Η επίθεση αυτή ήταν αξιοσημείωτη τόσο για το εύρος της όσο και για τον τρόπο λειτουργίας της. Περίπου 100.000 συσκευές IoT με δυνατότητα σύνδεση στο διαδίκτυο, όπως εκτυπωτές, κάμερες IP και οθόνες παρακολούθησης βρεφών, μολύνθηκαν από τους επιτιθέμενους. Χρησιμοποιώντας την θύρα δικτύου 53, η οποία χρησιμοποιείται για την κυκλοφορία DNS, οι συσκευές αυτές χρησιμοποιήθηκαν για να την πλημμυρίσουν με πακέτα TCP και UDP. Στόχος αυτής της πλημμύρας ήταν να υπερφορτωθούν

οι servers της Dyn, ώστε η υπηρεσία DNS να μην λειτουργεί σωστά. Επίσης η επίθεση σχεδιάστηκε για να παράγει αναδρομική (recursive) κυκλοφορία DNS, έτσι ώστε να αναγκάσει τους DNS servers να ξανά προσπαθήσουν αυτόματα να επιλύσουν τα ερωτήματα DNS εάν οι αρχικές προσπάθειες πρόσβασης αποτύγχαναν [72], [74].

- **KrebsOnSecurity.com**: Στα τέλη Σεπτεμβρίου του 2016, μία πολύ μεγάλη επίθεση DDoS έριξε τον ιστότοπο KrebsOnSecurity.com του δημοσιογράφου για θέματα κυβερνοασφάλειας Brian Krebs. Αυτή η επίθεση ήταν ξεχωριστή, καθώς εκτός από το τεράστιο μέγεθος της, πραγματοποιήθηκε με την χρήση μιας συγκεκριμένης μεθοδολογίας. Με την βοήθεια 24.000 συσκευών IoT που είχαν μολυνθεί με το κακόβουλο λογισμικό Bashlite και Mirai, εκτελέστηκε η επίθεση, με αποτέλεσμα ο μέγιστος όγκος της επίθεσης να είναι εντυπωσιακός, 623 Gbps. Οι ψηφιακές συσκευές εγγραφής βίντεο (DVR) και οι κάμερες IP που ήταν συνδεδεμένες στο διαδίκτυο ήταν οι κύριες κακόβουλες συσκευές αυτής της κυβερνοεπίθεσης. Αυτές οι συσκευές παραβιάστηκαν, μολύνθηκαν και στην συνέχεια χρησιμοποιήθηκαν για την δημιουργία ενός botnet, το οποίο χρησιμοποιήθηκε για την έναρξη της επίθεσης DDoS. Χρησιμοποιώντας έγκυρες συνδέσεις μεταξύ των παραβιασμένων συσκευών και του στόχου, η κίνηση αποτελούταν κυρίως από κίνηση GRE, SYN flooding, αιτήσεις GET και αιτήσεις POST [72].
- **Liberia**: Με στόχο το υποθαλάσσιο καλώδιο διαδικτύου της Λιβερίας στις αρχές Νοεμβρίου 2016, σημειώθηκε μια DDoS επίθεση, η οποία πιστεύεται ότι εκτελέστηκε μέσω του Mirai botnet. Ανησυχίες εκφράστηκαν σχετικά με την ικανότητα αυτής της επίθεσης να καταστρέψει Ασφάλεια το IoT σε χαμηλά επίπεδα 55 την συνδεσιμότητα του δικτύου της χώρας, καθώς ένας ερευνητής ισχυρίστηκε ότι η επίθεση είχε μέγεθος 500 Gbps [72].
- **Lappeenranta, Φινλανδία**: Η φινλανδική πόλη Lappeenranta δέχθηκε επίθεση τον χειμώνα του 2016, η οποία είχε ως στόχο τα συστήματα ζεστού νερού και θέρμανσης. Στην επίθεση εκτιμάται ότι χρησιμοποιήθηκε το Mirai botnet [72].
- **Πυρηνικό πρόγραμμα του Ιράν**: Μία από τις πιο προηγμένες επιθέσεις, το σκουλήκι Stuxnet στόχευσε το πυρηνικό πρόγραμμα του Ιράν τον Ιούνιο του 2010. Σχεδιάστηκε για να επιτεθεί σε προγραμματιζόμενους λογικούς ελεγκτές (Programmable Logic Controller, PLC), οι οποίοι χρησιμοποιούνται σε υποδομές και βιομηχανικά συστήματα. Τα PLC αυτοματοποιούσαν τις λειτουργίες των μηχανών και ήταν απαραίτητα για την διαχείριση των φυγοκεντρωτών ουρανίου στο πυρηνικό πρόγραμμα του Ιράν [75].

4.5 Επίλογος

Οι επιθέσεις στα κατώτερα επίπεδα του IoT αποκαλύπτουν τις βαθιές προκλήσεις που συνοδεύουν τη διασύνδεση του φυσικού με τον ψηφιακό κόσμο. Καθώς οι συσκευές γίνονται ολοένα και πιο ενσωματωμένες στην καθημερινή ζωή, οι απειλές που προκύπτουν σε αυτά τα επίπεδα δεν επηρεάζουν μόνο την τεχνολογία, αλλά και την ασφάλεια, την ιδιωτικότητα και την εμπιστοσύνη των χρηστών. Η ενίσχυση της προστασίας σε αυτά τα θεμελιώδη επίπεδα δεν αποτελεί πλέον τεχνική επιλογή, αλλά αναγκαιότητα για ένα ασφαλές και βιώσιμο IoT περιβάλλον.

Κεφάλαιο 5ο: Πρόληψη Επιθέσεων στο IoT

5.1 Εισαγωγή

Το IoT φέρνει επανάσταση σε πολλούς τομείς, αλλά συνοδεύεται από σοβαρούς κινδύνους ασφάλειας λόγω των ευάλωτων σημείων των συσκευών και της μεγάλης κλίμακας διασύνδεσης. Η πρόληψη επιθέσεων αποτελεί κρίσιμο πεδίο έρευνας, με έμφαση σε τεχνικές όπως η ανίχνευση ανωμαλιών, η τεχνητή νοημοσύνη και τα κρυπτογραφικά πρωτόκολλα.

5.2 Μέτρα Πρόληψης στο IoT

Η ανάπτυξη **προσαρμοστικών συστημάτων IDPS**, όπως το IDPIoT, συνδυάζει λειτουργίες ανίχνευσης και πρόληψης εισβολών. Αυτά τα συστήματα εξετάζουν τη συμπεριφορά των πακέτων και, αν εντοπιστεί ύποπτη δραστηριότητα, τα μπλοκάρουν ή τα απορρίπτουν. Η προσέγγιση αυτή ενσωματώνει τεχνικές ανίχνευσης βασισμένες σε υπογραφές και ανωμαλίες, προσφέροντας μια ολοκληρωμένη λύση για την προστασία των συσκευών IoT [121].

Η χρήση **τεχνητής νοημοσύνης** και **μηχανικής μάθησης** έχει αποδειχθεί αποτελεσματική στην ανίχνευση και πρόληψη επιθέσεων στο IoT. Μέθοδοι όπως τα δέντρα αποφάσεων, οι υποστηρικτές διανυσμάτων και τα νευρωνικά δίκτυα χρησιμοποιούνται για την ανάλυση της κυκλοφορίας και την ανίχνευση ανωμαλιών. Επιπλέον, η ενσωμάτωση τεχνικών ενισχυτικής μάθησης επιτρέπει στα συστήματα να προσαρμόζονται δυναμικά σε νέες απειλές, βελτιώνοντας την ακρίβεια και μειώνοντας τα ψευδώς θετικά [122].

Η εφαρμογή μεταευρετικών αλγορίθμων, όπως η **Βελτιστοποίηση με Σμήνη Σωματιδίων (PSO)**, έχει προταθεί για την ενίσχυση της ασφάλειας στο IoT. Οι μέθοδοι αυτές βελτιώνουν την ακρίβεια στην ανίχνευση επιθέσεων όπως η άρνηση υπηρεσίας και οι επιθέσεις χρήστη-σε-ρίζα (U2R), προσφέροντας σημαντική βελτίωση σε σχέση με τις παραδοσιακές τεχνικές [123].

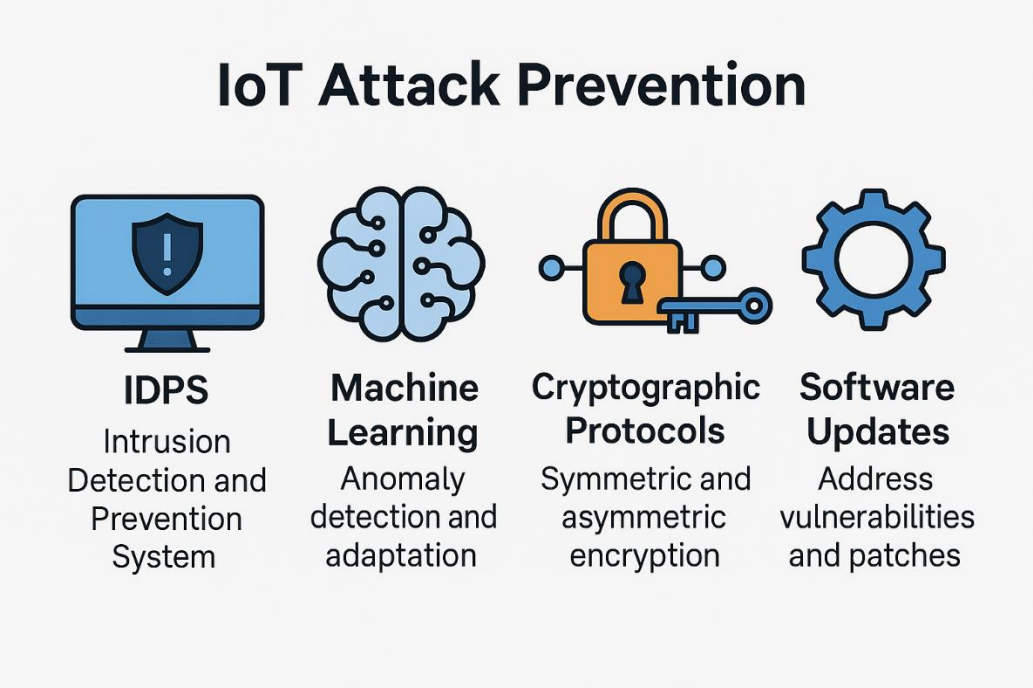
Προηγμένες αρχιτεκτονικές **νευρωνικών δικτύων**, όπως τα SCO-LSTM, έχουν χρησιμοποιηθεί για την ανίχνευση επιθέσεων σε συσκευές IoT-WSN. Η ενσωμάτωση δεδομένων απειλών πληροφοριών ενισχύει την ικανότητα των συστημάτων να ανιχνεύουν επιθέσεις όπως η έγχυση ψευδών δεδομένων και οι επιθέσεις brute force, επιτυγχάνοντας ακρίβεια έως και 99,89% [124].

Η **ενισχυτική μάθηση** προσφέρει δυναμικές λύσεις για την ασφάλεια στο IoT, επιτρέποντας στα συστήματα να μαθαίνουν και να προσαρμόζονται σε μεταβαλλόμενα πρότυπα επιθέσεων. Αυτή η προσέγγιση είναι ιδιαίτερα αποτελεσματική στην ανίχνευση επιθέσεων χαμηλού ρυθμού, οι οποίες είναι δύσκολο να εντοπιστούν με παραδοσιακές μεθόδους [125].

Η **ανίχνευση ανωμαλιών** μέσω συστημάτων IDS και IPS, σε συνδυασμό με **κρυπτογραφικά πρωτόκολλα** όπως η συμμετρική και ασύμμετρη κρυπτογράφηση, ενισχύει την ασφάλεια των συσκευών IoT. Η χρήση τεχνικών blockchain προσφέρει επιπλέον επίπεδα ασφάλειας, εξασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων [126].

Η ανάπτυξη **αυτοπροσαρμοζόμενων honeypots**, που χρησιμοποιούν τεχνικές ενισχυτικής μάθησης, επιτρέπει την ενεργή αλληλεπίδραση με επιτιθέμενους και την προσαρμογή των στρατηγικών

άμυνας σε πραγματικό χρόνο. Αυτές οι μέθοδοι ενισχύουν την ικανότητα των συστημάτων να ανιχνεύουν και να αποτρέπουν επιθέσεις με μεγαλύτερη αποτελεσματικότητα [127].



Σχήμα 5.1 : Μέτρα πρόληψης επιθέσεων στο IoT.

Η χρήση **τεχνικών ανίχνευσης ανωμαλιών**, όπως η παρακολούθηση της συμπεριφοράς των συσκευών και η ανάλυση της κυκλοφορίας δικτύου, συμβάλλει στην έγκαιρη ανίχνευση και αποτροπή επιθέσεων. Η ενσωμάτωση αυτών των τεχνικών με μηχανική μάθηση βελτιώνει την ακρίβεια και την αποτελεσματικότητα των συστημάτων ασφαλείας [128].

Η **δημιουργία εξειδικευμένων συνόλων δεδομένων** που αντικατοπτρίζουν τις πραγματικές συνθήκες του IoT είναι απαραίτητη για την εκπαίδευση και την αξιολόγηση μοντέλων μηχανικής μάθησης. Αυτά τα σύνολα δεδομένων επιτρέπουν την ανάπτυξη πιο ακριβών και αξιόπιστων συστημάτων ανίχνευσης επιθέσεων [129].

5.2.1 Είδη IDPS στο IoT

Τα **Βασισμένα σε υπογραφή IDPS (Signature-based)** συστήματα ανιχνεύουν γνωστές επιθέσεις συγκρίνοντας τη δραστηριότητα με μια βάση δεδομένων υπογραφών γνωστών απειλών. Παρόλο που προσφέρουν υψηλή ακρίβεια για γνωστές επιθέσεις, δεν είναι αποτελεσματικά απέναντι σε νέες, άγνωστες απειλές και απαιτούν συνεχή ενημέρωση της βάσης δεδομένων [130].

Τα **Βασισμένα σε ανωμαλίες IDPS (Anomaly-based)** συστήματα δημιουργούν ένα πρότυπο φυσιολογικής συμπεριφοράς και ανιχνεύουν αποκλίσεις από αυτό. Χρησιμοποιούν τεχνικές όπως στατιστική ανάλυση και μηχανική μάθηση για την ανίχνευση ανωμαλιών. Είναι αποτελεσματικά στην ανίχνευση άγνωστων επιθέσεων, αλλά μπορεί να παράγουν υψηλό ποσοστό ψευδώς θετικών [131].

Τα **Βασισμένα σε Προδιαγραφές (Specification-based)** συστήματα ορίζουν κανόνες για την κανονική λειτουργία και εντοπίζουν αποκλίσεις από αυτούς. Είναι αποτελεσματικά για την ανίχνευση άγνωστων επιθέσεων, αλλά απαιτούν λεπτομερή καθορισμό των κανόνων λειτουργίας, κάτι που μπορεί να είναι χρονοβόρο και επιρρεπές σε σφάλματα [132].

5.2.2 Τεχνικές Ανίχνευσης και Πρόληψης

Η **μηχανική μάθηση** χρησιμοποιείται για την ανάλυση προτύπων κυκλοφορίας και την ανίχνευση ανωμαλιών. Τεχνικές όπως τα νευρωνικά δίκτυα, οι αλγόριθμοι ταξινόμησης και οι αλγόριθμοι συστάδων έχουν εφαρμοστεί με επιτυχία. Ωστόσο, η εφαρμογή τους σε περιβάλλοντα IoT αντιμετωπίζει προκλήσεις λόγω των περιορισμένων πόρων των συσκευών [131].
Η επεξεργασία δεδομένων κοντά στην πηγή τους μειώνει την καθυστέρηση και το φορτίο στο δίκτυο, καθιστώντας την ανίχνευση πιο αποδοτική. Η **υπολογιστική στο άκρο** επιτρέπει την ταχύτερη απόκριση σε απειλές και μειώνει την ανάγκη για μεταφορά μεγάλων όγκων δεδομένων σε κεντρικούς διακομιστές [133].

Η τεχνολογία **blockchain** προσφέρει ένα αποκεντρωμένο και αδιάβλητο πλαίσιο για την καταγραφή και επαλήθευση γεγονότων ασφαλείας. Αυτό ενισχύει την αξιοπιστία των IDPS, καθώς οι καταγραφές δεν μπορούν να αλλοιωθούν και είναι προσβάσιμες από όλους τους συμμετέχοντες στο δίκτυο [134].

5.2.3 Χρήση τεχνητής νοημοσύνης στην πρόληψη επιθέσεων

Η **ενισχυτική μάθηση** (reinforcement learning) έχει εφαρμοστεί για την ανίχνευση επιθέσεων σε δίκτυα IoT, αντιμετωπίζοντας προκλήσεις όπως η ετερογένεια των συσκευών και οι εξελισσόμενες στρατηγικές επιθέσεων. Ένα μοντέλο που βασίζεται στην ενισχυτική μάθηση προσαρμόζει δυναμικά τα κατώφλια ανίχνευσης με βάση την ανατροφοδότηση, επιτυγχάνοντας βελτιωμένη ακρίβεια και μειωμένα ψευδώς θετικά αποτελέσματα [136].

Διάφοροι αλγόριθμοι **μηχανικής μάθησης**, όπως K-Nearest Neighbors (KNN), Naive Bayes και Multi-Layer Perceptron (MLP), έχουν χρησιμοποιηθεί για την ανίχνευση botnet και επιθέσεων DDoS σε δίκτυα IoT. Η χρήση τεχνικών όπως η Συνθετική Υπερδειγματοληψία Μειονοτικών Κλάσεων (SMOTE) συμβάλλει στην αντιμετώπιση της ανισορροπίας των δεδομένων, βελτιώνοντας την απόδοση των μοντέλων [137].

Η **ομοσπονδιακή μάθηση** (federated learning) επιτρέπει την ανίχνευση κακόβουλου λογισμικού σε συσκευές IoT χωρίς την ανάγκη συγκέντρωσης των δεδομένων σε κεντρικό σημείο, διατηρώντας την ιδιωτικότητα των χρηστών. Τα μοντέλα που εκπαιδεύονται με αυτή την προσέγγιση παρουσιάζουν απόδοση συγκρίσιμη με τα κεντρικά μοντέλα, ενώ αντιμετωπίζουν προκλήσεις όπως επιθέσεις δηλητηρίασης δεδομένων [138].

Η χρήση **βαθιών νευρωνικών δικτύων**, όπως τα πολυεπίπεδα MLP με ενεργοποίηση ReLU, έχει αποδειχθεί αποτελεσματική στην ανίχνευση επιθέσεων όπως DDoS και MitM σε βιομηχανικά περιβάλλοντα IoT. Τα μοντέλα αυτά επιτυγχάνουν υψηλή ακρίβεια και χαμηλά ποσοστά ψευδώς θετικών αποτελεσμάτων [139].

Η **ενσωμάτωση τεχνικών εξηγήσιμης τεχνητής νοημοσύνης** (XAI) σε μοντέλα ανάλυσης κινδύνου επιτρέπει την κατανόηση των αποφάσεων των μοντέλων από τους ειδικούς ασφάλειας. Αυτό διευκολύνει την αξιολόγηση και την αντιμετώπιση των κινδύνων σε δυναμικά περιβάλλοντα IoT [140].

Η **χρήση γενετικών μοντέλων τεχνητής νοημοσύνης**, όπως το IDS-Agent, έχει δείξει ικανότητα στην ανίχνευση επιθέσεων μηδενικής ημέρας σε δίκτυα IoT. Το μοντέλο αυτό επιτυγχάνει υψηλά ποσοστά F1 και αναγνώρισης, υπερβαίνοντας προηγούμενες προσεγγίσεις [141].

Μια **συστηματική ανασκόπηση των μεθόδων τεχνητής νοημοσύνης** στην ασφάλεια IoT καταγράφει τις υπάρχουσες τεχνικές, τα πλεονεκτήματα και τις προκλήσεις τους, προσφέροντας κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη [142].

5.2.4 Βελτιστοποίηση με Σμήνη Σωματιδίων (Particle Swarm Optimization - PSO)

Η **Βελτιστοποίηση με Σμήνη Σωματιδίων** αποτελεί έναν ευφυή αλγόριθμο βελτιστοποίησης εμπνευσμένο από τη συλλογική συμπεριφορά σμηνών. Στο πεδίο του IoT, η PSO εφαρμόζεται αποτελεσματικά για την ενίσχυση συστημάτων ανίχνευσης επιθέσεων, καθώς μπορεί να επιλέγει βέλτιστα χαρακτηριστικά, να ρυθμίζει παραμέτρους και να συνεργάζεται με τεχνικές μηχανικής μάθησης. Η χρήση της συμβάλλει σημαντικά στην έγκαιρη αναγνώριση και πρόληψη κυβερνοεπιθέσεων σε κατανεμημένα και ευάλωτα IoT περιβάλλοντα.

Ένα **υβριδικό σύστημα που συνδυάζει PSO με Deep Belief Networks (DBN), Autoencoders και Self-Organizing Maps (SOM)** επιτυγχάνει ακρίβεια έως και 99,99% στην ανίχνευση γνωστών και άγνωστων επιθέσεων σε δίκτυα IoT, χρησιμοποιώντας datasets όπως NSL-KDD, UNSW-NB15 και CICIoT2023 [143].

Η χρήση ενός **υβριδικού μοντέλου που συνδυάζει Autoencoders με Τροποποιημένο PSO (HAEMPSO)** για επιλογή χαρακτηριστικών και Deep Neural Networks (DNN) για ταξινόμηση έχει αποδειχθεί αποτελεσματική στην ανίχνευση επιθέσεων σε IoT, με χρήση των datasets UNSW-NB15 και BoT-IoT [144].

Μια μελέτη προτείνει τη **χρήση του PSO σε συνδυασμό με Extreme Learning Machines (ELM)** για την ανίχνευση εισβολών σε δίκτυα Edge IoT, επιτρέποντας την πραγματική ανίχνευση και καταγραφή των αντικειμένων εισβολής [145].

Η εφαρμογή του PSO σε συνδυασμό με Deep Neural Networks (DNN) σε συστήματα ανίχνευσης εισβολών στο IoMT έχει δείξει ακρίβεια έως και 96% στην ανίχνευση επιθέσεων, χρησιμοποιώντας συνδυασμένα δεδομένα δικτυακής κίνησης και αισθητήρων [146].

Η χρήση **Ενισχυμένης PSO (Enhanced PSO)** για τη βελτιστοποίηση παραμέτρων σε μοντέλα μηχανικής μάθησης, όπως τα Decision Trees, έχει αποδειχθεί αποτελεσματική στην ανίχνευση επιθέσεων, μελέτη που βασίστηκε στα datasets CSE-CIC-IDS 2018 και LITNET-2020 [147].

Μια προσέγγιση που **συνδυάζει Adaptive PSO με Convolutional Neural Networks (CNN)** έχει δείξει αποτελεσματικότητα στην ανίχνευση πολλαπλών τύπων επιθέσεων σε δίκτυα IoT [148].

Η **συνδυασμένη χρήση του PSO** για επιλογή χαρακτηριστικών **και του αλγορίθμου Random Forest** για ταξινόμηση έχει δείξει βελτιωμένη ακρίβεια στην ανίχνευση ανωμαλιών σε δίκτυα IoT, μειώνοντας τα ψευδώς θετικά και ψευδώς αρνητικά αποτελέσματα [149].

5.2.5 Προηγμένες αρχιτεκτονικές Νευρωνικών Δικτύων για ανίχνευση εισβολών στο IoT

Η **συνδυαστική χρήση LSTM και CNN** έχει αποδειχθεί αποτελεσματική στην ανίχνευση επιθέσεων σε IoT δίκτυα. Το μοντέλο LSTM-CNN επιτρέπει την εκμάθηση χρονικών και χωρικών χαρακτηριστικών, βελτιώνοντας την ακρίβεια ανίχνευσης. Μελέτες έχουν δείξει ότι τέτοια μοντέλα επιτυγχάνουν υψηλή απόδοση σε σύνολα δεδομένων όπως το UNSW-NB15 και το BoT-IoT [150].

Τα **GNNs** χρησιμοποιούνται για την ανάλυση γραφημάτων που αναπαριστούν τις σχέσεις μεταξύ συσκευών στο IoT. Αυτά τα δίκτυα είναι ικανά να εντοπίζουν ανωμαλίες και επιθέσεις που εκδηλώνονται μέσω μη γραμμικών σχέσεων μεταξύ των συσκευών [151].

Η **ενισχυτική μάθηση** εφαρμόζεται για την ανάπτυξη δυναμικών συστημάτων ανίχνευσης εισβολών που προσαρμόζονται σε νέες και εξελισσόμενες απειλές. Αυτές οι μέθοδοι επιτρέπουν στα συστήματα να μαθαίνουν από τις αλληλεπιδράσεις τους με το περιβάλλον και να βελτιώνουν την απόδοσή τους με την πάροδο του χρόνου [152].

Οι **αυτοκωδικοποιητές** χρησιμοποιούνται για την ανίχνευση ανωμαλιών στο IoT, αναγνωρίζοντας αποκλίσεις από τα κανονικά πρότυπα δεδομένων. Αυτές οι μέθοδοι είναι ιδιαίτερα χρήσιμες σε περιβάλλοντα με περιορισμένα δεδομένα [153].

5.2.6 Ενισχυτική Μάθηση για την πρόληψη επιθέσεων στο IoT

Η πρόληψη των επιθέσεων στο IoT απαιτεί δυναμικές, ευέλικτες και αυτοματοποιημένες μεθόδους εντοπισμού και αντίδρασης. Η **ενισχυτική μάθηση** έχει αναδειχθεί ως μια πολλά υποσχόμενη προσέγγιση λόγω της ικανότητάς της να μαθαίνει βέλτιστες πολιτικές ασφαλείας μέσα από αλληλεπίδραση με το περιβάλλον και προσαρμογή σε μεταβαλλόμενες συνθήκες.

Η ενισχυτική μάθηση βασίζεται σε έναν *agent* που μαθαίνει να παίρνει αποφάσεις (ενέργειες) σε ένα περιβάλλον, λαμβάνοντας ανταμοιβές ή ποινές, ώστε να μεγιστοποιεί τη συνολική ανταμοιβή. Στο πλαίσιο του IoT, ο agent μπορεί να είναι ένας μηχανισμός ασφαλείας που αναγνωρίζει και αποτρέπει επιθέσεις (π.χ. DoS, επιθέσεις κακόβουλου λογισμικού). Σε αντίθεση με παραδοσιακά συστήματα ανίχνευσης εισβολών (IDS), τα οποία βασίζονται σε στατικές υπογραφές, η ενισχυτική μάθηση μπορεί να προσαρμόζεται σε νέες, μη γνωστές επιθέσεις, καθώς μαθαίνει από τις συνέπειες των ενεργειών του σε πραγματικό χρόνο [154].

Μερικές τεχνικές και αλγόριθμοι που χρησιμοποιούνται είναι οι εξής:

- **Q-Learning και Deep Q-Networks (DQN):** Συχνά χρησιμοποιούνται για την εκμάθηση πολιτικών ενίσχυσης σε δίκτυα IoT για την πρόληψη επιθέσεων [155][156].
- **Multi-agent RL:** Χρήση πολλαπλών agents που συνεργάζονται για ανίχνευση και αντιμετώπιση επιθέσεων σε κατανεμημένα δίκτυα IoT [157].
- **Model-based RL:** Χρήση μοντέλων περιβάλλοντος για πρόβλεψη επιθέσεων και προληπτικές ενέργειες [158].

Εφαρμογές και παραδείγματα:

- Ανίχνευση και Πρόληψη DoS επιθέσεων με τη χρήση DQN για δυναμική διαχείριση πόρων και αποκλεισμό κακόβουλης κίνησης σε συσκευές IoT με περιορισμένη υπολογιστική ισχύ [155]. Η RL βοηθά στην επιλογή βέλτιστων κανόνων firewall που προσαρμόζονται με την πάροδο του χρόνου, μειώνοντας ψευδώς θετικά και αρνητικά αποτελέσματα.
- Προστασία από επιθέσεις μηχανικής μάθησης με τη χρήση RL αλγορίθμων που ανιχνεύουν προσπάθειες παραπλάνησης συστημάτων ML σε IoT περιβάλλοντα, ενισχύοντας την ασφάλεια των μοντέλων [156].
- Προστασία από κακόβουλο λογισμικό και επιθέσεις malware με χρήση multi-agent RL για συνεχή παρακολούθηση και απόκριση σε ύποπτες συμπεριφορές σε δίκτυα IoT [157].

Η χρήση ενισχυτικής μάθησης φέρει πλεονεκτήματα στην πρόληψη επιθέσεων στο IoT. Κάποια από αυτά είναι η αυτονομία στη λήψη αποφάσεων, η προσαρμογή σε μη γνωστές απειλές και η ικανότητα μάθησης σε πραγματικό χρόνο. Ωστόσο, υπάρχουν και ορισμένες προκλήσεις, όπως το υπολογιστικό κόστος σε περιορισμένες συσκευές, η αστάθεια μάθησης σε δυναμικά περιβάλλοντα και η ανάγκη για ασφαλή εκπαίδευση ώστε να μην εκμεταλλεύονται τυχόν επιτιθέμενοι το μοντέλο [158].

5.2.7 Ανίχνευση Ανωμαλιών και Χρήση Κρυπτογραφικών Πρωτοκόλλων

Η **ανίχνευση ανωμαλιών** στο IoT είναι κρίσιμη για την ασφάλεια και αξιοπιστία των συσκευών και των δικτύων. Καθώς οι IoT συσκευές λειτουργούν συχνά σε περιβάλλοντα με περιορισμένους πόρους, απαιτούνται ελαφριές και αποδοτικές μέθοδοι εντοπισμού ύποπτης ή ασυνήθιστης συμπεριφοράς [159].

Μια μελέτη προτείνει τη χρήση **ανάλυσης φασματικής πυκνότητας** και του εκθέτη Hurst για την ανίχνευση ανωμαλιών στην κυκλοφορία δικτύου IoT. Η προσέγγιση αυτή επιτρέπει τον εντοπισμό αποκλίσεων από κανονικά πρότυπα κυκλοφορίας, αξιοποιώντας τη φρακταλική ανάλυση δεδομένων. Τα αποτελέσματα έδειξαν ότι η κυκλοφορία παρουσιάζει μακροπρόθεσμες εξαρτήσεις, με τον εκθέτη Hurst να κυμαίνεται μεταξύ 0.611 και 0.747, υποδεικνύοντας επίμονη συμπεριφορά της κυκλοφορίας [159].

Το πλαίσιο CIoTA χρησιμοποιεί την τεχνολογία **blockchain** για την ενημέρωση ενός αξιόπιστου μοντέλου ανίχνευσης ανωμαλιών μέσω αυτο-επικύρωσης και συναίνεσης μεταξύ συσκευών IoT. Η προσέγγιση αυτή επιτρέπει την αποκεντρωμένη ανίχνευση ανωμαλιών, ενισχύοντας την ασφάλεια του δικτύου χωρίς την ανάγκη για κεντρική αρχή [160].

Μια άλλη προσέγγιση συνδυάζει την **ομοσπονδιακή μάθηση** με την **ομομορφική κρυπτογράφηση** για την ανίχνευση ανωμαλιών στο IoT, διατηρώντας την ιδιωτικότητα των δεδομένων και επιτρέποντας τη συνεργατική εκπαίδευση μοντέλων χωρίς την αποκάλυψη των τοπικών δεδομένων των συσκευών [161].

Η χρήση **κρυπτογραφικών πρωτοκόλλων** είναι ζωτικής σημασίας για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας αυτών των επικοινωνιών [162]. Ωστόσο, οι περιορισμένοι υπολογιστικοί και ενεργειακοί πόροι των IoT συσκευών απαιτούν την εφαρμογή ελαφριών (lightweight) και αποδοτικών κρυπτογραφικών λύσεων [163]. Αλγόριθμοι όπως οι **ChaCha20** και **Elliptic Curve Cryptography (ECC)** έχουν αναδειχθεί κατάλληλοι για τέτοια περιβάλλοντα [164].

Η μελέτη εξετάζει διάφορους **κρυπτογραφικούς αλγορίθμους** που χρησιμοποιούνται στις επικοινωνίες IoT, επισημαίνοντας την ανάγκη για ελαφριές και αποδοτικές λύσεις λόγω των περιορισμένων πόρων των συσκευών. Συγκεκριμένα, ο αλγόριθμος ChaCha20 είναι ένας σύγχρονος αλγόριθμος συμμετρικής κρυπτογράφησης τύπου stream cipher, σχεδιασμένος από τον Daniel J. Bernstein. Αποτελεί βελτίωση του Salsa20 και προσφέρει υψηλή ασφάλεια και ταχύτητα, ακόμα και σε περιορισμένες συσκευές όπως αυτές του IoT [165]. Είναι ελαφρύς, γρήγορος και ανθεκτικός σε επιθέσεις όπως οι κρυπταναλύσεις differential και linear cryptanalysis, χρησιμοποιείται σε πρωτόκολλα όπως το TLS 1.3 και το Google QUIC και είναι κατάλληλος για συσκευές με περιορισμένους πόρους, λόγω απλού σχεδιασμού και χαμηλής κατανάλωσης ενέργειας [166].

Η ECC είναι μια μορφή ασύμμετρης κρυπτογραφίας που βασίζεται στα μαθηματικά των ελλειπτικών καμπυλών πάνω από πεδία πεπερασμένων αριθμών [167]. Προσφέρει υψηλό επίπεδο ασφάλειας με πολύ μικρότερο μέγεθος κλειδιού σε σχέση με RSA, καθιστώντας την ιδανική για το IoT όπου η υπολογιστική ισχύς και η μνήμη είναι περιορισμένες. Χρησιμοποιείται για κρυπτογράφηση, ψηφιακές υπογραφές και ανταλλαγή κλειδιών (π.χ. ECDSA, ECDH). Υποστηρίζει ασφαλή επικοινωνία με μειωμένη κατανάλωση πόρων και ταχύτατη εκτέλεση [162].

5.2.8 Αντιμετώπιση Ευπαθειών και Ενημερώσεις Λογισμικού

Η συνεχής εξάπλωση του IoT έχει οδηγήσει στην ανάγκη για αποτελεσματικούς μηχανισμούς διαχείρισης ευπαθειών και ενημερώσεων λογισμικού. Οι IoT συσκευές συχνά λειτουργούν σε μη ασφαλή περιβάλλοντα και υπόκεινται σε περιορισμούς πόρων, γεγονός που δυσχεραίνει την εφαρμογή παραδοσιακών μοντέλων ασφάλειας.

Το **firmware** των IoT συσκευών αποτελεί ένα κρίσιμο σημείο επιθέσεων, με **ευπάθειες** που προκύπτουν από ελλιπή κρυπτογράφηση, ανεπαρκή ελέγχο πρόσβασης και κακή διαχείριση της μνήμης [254]. Πολλές επιθέσεις εκμεταλλεύονται τις δυνατότητες απομακρυσμένης πρόσβασης μέσω των ενημερώσεων λογισμικού, ειδικά όταν αυτές δεν συνοδεύονται από μηχανισμούς ταυτοποίησης και ελέγχου ακεραιότητας [255].

Η συστηματική κατηγοριοποίηση των ευπαθειών έχει βοηθήσει τους ερευνητές να εντοπίζουν ευάλωτα σημεία σε υποσυστήματα όπως η διαχείριση ενέργειας, η επικοινωνία, και η αποθήκευση [254]. Επιπλέον, οι επιθέσεις συχνά επωφελούνται από τη γενική απουσία μηχανισμών "secure boot" και την αδυναμία εφαρμογής ενημερώσεων χωρίς φυσική πρόσβαση στη συσκευή [256].

Η διαδικασία **ενημέρωσης firmware** πρέπει να διασφαλίζει την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων ενημέρωσης [255]. Σε πολλές περιπτώσεις, η διαδικασία Over-The-Air (OTA) ενημερώσεων είναι ευάλωτη, εφόσον δεν συνοδεύεται από κρυπτογραφημένους και υπογεγραμμένους μηχανισμούς ελέγχου [256].

Αν και έχουν αναπτυχθεί πρότυπα όπως το IETF SUIT (Software Updates for IoT), η υιοθέτηση αυτών από τη βιομηχανία παραμένει περιορισμένη [255]. Επιπλέον, οι ερευνητές αναπτύσσουν πλέον πλαίσια ανάλυσης τα οποία επιτρέπουν τον έλεγχο μιας ενημέρωσης πριν την εφαρμογή της, εξετάζοντας τόσο την πηγή όσο και την πιθανή επίδρασή της στη λειτουργικότητα της συσκευής [255].

Σύγχρονες ερευνητικές προσεγγίσεις αξιοποιούν τεχνολογίες όπως το blockchain και η τεχνητή νοημοσύνη για την ασφαλή διανομή και αξιολόγηση των ενημερώσεων [257]. Μέσω μηχανικής μάθησης, μπορούν να εντοπίζονται πρότυπα κακόβουλης συμπεριφοράς ή παραβιάσεις firmware, ακόμα και χωρίς προηγούμενη γνώση συγκεκριμένων επιθέσεων [258].

Το blockchain, με τη χρήση smart contracts, επιτρέπει την επαλήθευση της παραλαβής μιας ενημέρωσης και αποτρέπει τροποποιήσεις στα πακέτα λογισμικού κατά τη μεταφορά [257]. Παράλληλα, τα hot patches προσφέρουν τη δυνατότητα άμεσης επιδιόρθωσης ευπαθειών χωρίς ανάγκη επανεκκίνησης της συσκευής [256].

5.2.9 Ανάπτυξη Αυτοπροσαρμοζόμενων Honeypots

Η ανάπτυξη **αυτοπροσαρμοζόμενων honeypots** για το IoT αποτελεί ένα κρίσιμο πεδίο έρευνας για την ενίσχυση της ασφάλειας των συνδεδεμένων συσκευών.

Το HoneyIoT είναι ένα σύστημα που χρησιμοποιεί ενισχυτική μάθηση για να προσαρμόζει δυναμικά τις απαντήσεις του σε επιθέσεις, καθιστώντας το λιγότερο ανιχνεύσιμο και πιο αποτελεσματικό στη συλλογή κακόβουλου λογισμικού. Το σύστημα μαθαίνει από πραγματικά ίχνη επιθέσεων και χρησιμοποιεί τεχνικές διαφοροποίησης για να δημιουργεί απαντήσεις υψηλής πιστότητας [259].

Το AIIPot αξιοποιεί τεχνικές μηχανικής μάθησης για να μιμείται την ανθρώπινη συμπεριφορά κατά την αλληλεπίδραση με επιτιθέμενους, αυξάνοντας τη διάρκεια και την ποιότητα των συνεδριών. Αυτό επιτρέπει τη συλλογή πιο πλούσιων δεδομένων από επιθέσεις [260].

Το HARM (Honeypot for Automated and Repetitive Malware) είναι ένα πλαίσιο που ενσωματώνει ενισχυτική μάθηση για την ανάπτυξη προσαρμοστικών και ευέλικτων honeypots. Το σύστημα χρησιμοποιεί αλγορίθμους όπως Q-learning και SARSA για να προσαρμόζει τις πολιτικές του με βάση τις επιθέσεις που δέχεται [261].

Το Asgard είναι ένα honeypot που χρησιμοποιεί ενισχυτική μάθηση για να ισορροπεί μεταξύ της συλλογής δεδομένων από επιθέσεις και της αυτοπροστασίας του. Το σύστημα μπορεί να μπλοκάρει ή να υποκαθιστά κακόβουλες εντολές, μειώνοντας τον κίνδυνο συμβιβασμού [262].

Το SIPHON είναι μια αρχιτεκτονική που επιτρέπει την έκθεση λίγων φυσικών IoT συσκευών μέσω πολλαπλών γεωγραφικά διασκορπισμένων IP διευθύνσεων. Αυτό προσελκύει επιθέσεις από διαφορετικές περιοχές και επιτρέπει τη συλλογή ποικίλων δεδομένων [263].

Το ThingPot επικεντρώνεται στην προσομοίωση ολόκληρης της IoT πλατφόρμας, συμπεριλαμβανομένων των πρωτοκόλλων όπως XMPP και REST API. Αυτό επιτρέπει την παρακολούθηση επιθέσεων σε επίπεδο εφαρμογής και την κατανόηση των στρατηγικών των επιτιθέμενων [264].

Ένα οικοσύστημα honeypot που εξελίσσεται σε φάσεις επιτρέπει την προοδευτική αύξηση της πολυπλοκότητας του honeypot με βάση τη συμπεριφορά των επιτιθέμενων. Αυτό βοηθά στην κατανόηση τόσο αυτοματοποιημένων όσο και ανθρώπινων επιθέσεων [265].

Ένα σύστημα που συνδυάζει honeypot με ανίχνευση ανωμαλιών μπορεί να προσαρμόζεται σε πραγματικό χρόνο σε νέες επιθέσεις, ενισχύοντας την ασφάλεια των IoT συσκευών σε έξυπνα σπίτια [266].

5.2.10 Εφαρμογή Τεχνικών Ανίχνευσης Ανωμαλιών και Αποτροπής Επιθέσεων

Η εφαρμογή τεχνικών ανίχνευσης ανωμαλιών και αποτροπής επιθέσεων στο IoT αποτελεί κρίσιμο πεδίο έρευνας, δεδομένων των αυξανόμενων απειλών και της πολυπλοκότητας των IoT συστημάτων.

Η ανίχνευση ανωμαλιών αποτελεί βασικό μηχανισμό για την αναγνώριση άγνωστων ή μη καταγεγραμμένων επιθέσεων σε IoT περιβάλλοντα. Οι παραδοσιακές τεχνικές μηχανικής μάθησης, όπως οι Random Forests και οι Support Vector Machines, έχουν χρησιμοποιηθεί ευρέως, αλλά παρουσιάζουν περιορισμούς λόγω της ανάγκης για χειροκίνητη εξαγωγή χαρακτηριστικών και της αδυναμίας τους να αντιμετωπίσουν μεγάλα και μη δομημένα δεδομένα. Η βαθιά μάθηση (Deep Learning) προσφέρει λύσεις σε αυτά τα προβλήματα, επιτρέποντας την αυτόματη εξαγωγή χαρακτηριστικών και την αποτελεσματική ανίχνευση ανωμαλιών σε πραγματικό χρόνο [267].

Πέρα από την ανίχνευση, η πρόληψη εισβολών είναι εξίσου σημαντική:

- **Ανιχνευτικά Συστήματα με Βάση το Δίκτυο**: Η χρήση προφίλ κυκλοφορίας δικτύου σε συνδυασμό με μηχανική μάθηση επιτρέπει την ανίχνευση απόπειρων παραβίασης συσκευών και ύποπτων συναλλαγών, με ακρίβεια έως και 98.35% [269].
- **Προσαρμοστικά Συστήματα Ανίχνευσης και Πρόληψης**: Η ανάπτυξη προσαρμοστικών συστημάτων που συνδυάζουν ανίχνευση και πρόληψη επιτρέπει την αυτόματη απόκριση σε επιθέσεις, μειώνοντας τον χρόνο αντίδρασης και την εξάρτηση από ανθρώπινη παρέμβαση [270].

Παρά τις προόδους, υπάρχουν σημαντικές προκλήσεις. Οι IoT συσκευές συχνά διαθέτουν **περιορισμένους υπολογιστικούς πόρους**, καθιστώντας δύσκολη την εκτέλεση πολύπλοκων αλγορίθμων [267]. Η συνεχής ροή δεδομένων από πολλές συσκευές απαιτεί **αποδοτικές μεθόδους επεξεργασίας και ανάλυσης** σε πραγματικό χρόνο [267]. Η συλλογή και ανάλυση δεδομένων πρέπει να γίνεται με τρόπο που διασφαλίζει την **ιδιωτικότητα** των χρηστών και την **ασφάλεια των δεδομένων** [268].

Οι μελλοντικές έρευνες επικεντρώνονται στην ανάπτυξη ελαφρών και αποδοτικών αλγορίθμων, την ενσωμάτωση τεχνικών ομοσπονδιακής μάθησης και την αξιοποίηση της υπολογιστικής ισχύος του cloud και του edge computing για την ενίσχυση της ασφάλειας των IoT συστημάτων.

5.2.11 Ανάπτυξη Εξειδικευμένων Συνόλων Δεδομένων για Εκπαίδευση Μοντέλων

Η ανάπτυξη εξειδικευμένων συνόλων δεδομένων για την εκπαίδευση μοντέλων στο Διαδίκτυο των Πραγμάτων (IoT) αποτελεί κρίσιμο βήμα για την επιτυχή εφαρμογή τεχνικών μηχανικής μάθησης σε τομείς όπως η ασφάλεια, η συντήρηση, η ανάλυση συμπεριφοράς και η διαχείριση πόρων.

Το έργο **IoT-LM** εισάγει το **MultiIoT**, ένα από τα πιο εκτενή **πολυτροπικά σύνολα δεδομένων** για το IoT, με πάνω από 1,15 εκατομμύρια δείγματα από 12 αισθητηριακές μορφές και 8 εργασίες. Το σύνολο αυτό χρησιμοποιείται για την εκπαίδευση μεγάλων γλωσσικών μοντέλων με δυνατότητες ερωταποκρίσεων και διαλόγου βασισμένων σε δεδομένα αισθητήρων . Η προσέγγιση αυτή επιτρέπει την ανάπτυξη μοντέλων που μπορούν να επεξεργάζονται πολυτροπικά δεδομένα σε πραγματικό χρόνο, ενισχύοντας την κατανόηση και την αλληλεπίδραση με το περιβάλλον [271].

Το **Bot-IoT** αναπτύχθηκε για την ανάλυση δικτυακής κυκλοφορίας σε περιβάλλοντα IoT, περιλαμβάνοντας τόσο κανονική όσο και κακόβουλη δραστηριότητα, με έμφαση σε επιθέσεις τύπου botnet. Το σύνολο αυτό χρησιμοποιείται ευρέως για την εκπαίδευση και αξιολόγηση συστημάτων IDS [272].

Το **MQTT-IoT-IDS2020 ε**στιάζει σε επιθέσεις που σχετίζονται με το πρωτόκολλο MQTT, ένα από τα πιο διαδεδομένα πρωτόκολλα επικοινωνίας στο IoT. Το σύνολο αυτό δημιουργήθηκε για την αξιολόγηση τεχνικών μηχανικής μάθησης στην ανίχνευση επιθέσεων σε δίκτυα που χρησιμοποιούν MQTT [273] .

Το **IoT-23** περιλαμβάνει δικτυακή κυκλοφορία από 23 διαφορετικές συσκευές IoT, με σενάρια που καλύπτουν τόσο κανονική όσο και κακόβουλη δραστηριότητα, όπως επιθέσεις Mirai και Gafgyt. Το σύνολο αυτό χρησιμοποιείται για την αξιολόγηση μοντέλων ανίχνευσης ανωμαλιών και εισβολών [272].

Η χρήση **Γενετικών Αντιπαραθετικών Δικτύων (GANs)** επιτρέπει τη δημιουργία συνθετικών συνόλων δεδομένων που προσομοιώνουν επιθέσεις σε περιβάλλοντα IoT. Αυτή η προσέγγιση βοηθά στην αντιμετώπιση της έλλειψης ποικιλίας και ισορροπίας σε υπάρχοντα σύνολα δεδομένων, ενισχύοντας την απόδοση των μοντέλων μηχανικής μάθησης [272].

Τα **MetroPT & ALPI** είναι σύνολα δεδομένων που συλλέγουν σήματα από αισθητήρες σε βιομηχανικά περιβάλλοντα, όπως πίεση, θερμοκρασία και κατανάλωση ρεύματος. Χρησιμοποιούνται για την πρόβλεψη συντήρησης και την ανάλυση ποιότητας παραγωγής σε εφαρμογές IIoT [274].

Προκλήσεις στην Ανάπτυξη Συνόλων Δεδομένων για το IoT:

- **Ετερογένεια Δεδομένων**: Η ποικιλία σε μορφές δεδομένων (π.χ., εικόνες, ήχος, δεδομένα αισθητήρων) και η έλλειψη τυποποίησης καθιστούν δύσκολη τη δημιουργία ενιαίων συνόλων δεδομένων.
- **Ανισορροπία Κλάσεων**: Συχνά, τα δεδομένα περιλαμβάνουν περισσότερα παραδείγματα κανονικής λειτουργίας παρά επιθέσεων, οδηγώντας σε ανισορροπία που επηρεάζει την απόδοση των μοντέλων.
- **Απαιτήσεις Πόρων**: Η επεξεργασία και ανάλυση μεγάλων συνόλων δεδομένων απαιτεί σημαντικούς υπολογιστικούς πόρους, κάτι που μπορεί να είναι περιοριστικό για ορισμένους ερευνητές ή οργανισμούς.

Η ανάπτυξη εξειδικευμένων συνόλων δεδομένων είναι απαραίτητη για την πρόοδο της έρευνας και της εφαρμογής τεχνικών μηχανικής μάθησης στο IoT. Η δημιουργία πολυτροπικών, ισορροπημένων και ρεαλιστικών συνόλων δεδομένων επιτρέπει την εκπαίδευση μοντέλων που μπορούν να ανταποκριθούν στις προκλήσεις της πραγματικής ζωής, ενισχύοντας την ασφάλεια, την αποδοτικότητα και την αξιοπιστία των συστημάτων IoT.

5.2.12 Προκλήσεις και Μελλοντικές Κατευθύνσεις

Οι συσκευές IoT έχουν **περιορισμένη υπολογιστική ισχύ και μνήμη**, καθιστώντας δύσκολη την εφαρμογή πολύπλοκων αλγορίθμων ανίχνευσης. Αυτό απαιτεί την ανάπτυξη ελαφριών και αποδοτικών μοντέλων ανίχνευσης που μπορούν να λειτουργούν αποτελεσματικά σε τέτοια περιβάλλοντα [135].

Η υψηλή συχνότητα **ψευδώς θετικών ανιχνεύσεων** μπορεί να μειώσει την αποτελεσματικότητα των IDPS και να οδηγήσει σε απώλεια εμπιστοσύνης στο σύστημα. Η βελτίωση της ακρίβειας των συστημάτων ανίχνευσης είναι κρίσιμη για την αποδοχή και την αποτελεσματική χρήση τους [135].

Η **ανάπτυξη ελαφριών και αποδοτικών μοντέλων ανίχνευσης** είναι απαραίτητη για την αποτελεσματική προστασία των συσκευών IoT. Αυτά τα μοντέλα πρέπει να είναι ικανά να λειτουργούν με περιορισμένους πόρους και να παρέχουν αξιόπιστη ανίχνευση απειλών [135].

5.3 Επίλογος

Η πρόληψη επιθέσεων στο IoT βασίζεται στην ενίσχυση της ασφάλειας από το σχεδιασμό μέχρι τη λειτουργία, με χρήση κρυπτογράφησης, τακτικών ενημερώσεων και αυστηρών πολιτικών πρόσβασης. Η ευαισθητοποίηση των χρηστών και η συνεχής αξιολόγηση των απειλών συμβάλλουν στην έγκαιρη ανίχνευση και αποτροπή επιθέσεων. Με αυτόν τον τρόπο διασφαλίζεται η αξιοπιστία και η ασφάλεια των διασυνδεδεμένων συσκευών, προστατεύοντας τόσο τα δεδομένα όσο και την υποδομή.

Κεφάλαιο 6ο: Αντιμετώπιση Επιθέσεων στο IoT

6.1 Εισαγωγή

Η ασφάλεια στο IoT αποτελεί κρίσιμο ζήτημα, καθώς οι συσκευές που συμμετέχουν διαθέτουν ορισμένες ευπάθειες. Η αντιμετώπισή τους απαιτεί καινοτόμες τεχνικές, δεδομένης της περιορισμένης υπολογιστικής ισχύος των IoT συσκευών και της ετερογένειας των συστημάτων.

6.2 Αντιμετώπιση επιθέσεων

Μια ολοκληρωμένη λύση για την ανίχνευση και αντιμετώπιση επιθέσεων DDoS και ψευδούς διαμοιρασμού δεδομένων σε περιβάλλοντα IoT προτείνεται μέσω της χρήσης του πρωτοκόλλου SNMP για παρακολούθηση ανωμαλιών στην κυκλοφορία δικτύου, της απόστασης Kullback–Leibler για ανίχνευση, κανόνων ελέγχου πρόσβασης (ACL) για αποκλεισμό γνωστών μοτίβων επιθέσεων και τεχνικών Moving Target Defense (MTD) για μείωση της πιθανότητας επιθέσεων. Τα αποτελέσματα έδειξαν μείωση της πιθανότητας επίθεσης έως και 0,2% [168].

Η χρήση Software-Defined Networking (SDN) σε συνδυασμό με Intrusion Detection Systems (IDS) επιτρέπει την έγκαιρη ανίχνευση και αντιμετώπιση επιθέσεων DDoS. Το προτεινόμενο σύστημα ανιχνεύει επιθέσεις και ενημερώνει τον SDN controller, ο οποίος με τη σειρά του εφαρμόζει κατάλληλες πολιτικές δρομολόγησης για την αποτροπή της επίθεσης [169].

Οι τεχνικές Reinforcement Learning (RL) προσφέρουν δυναμική προσαρμογή στις μεταβαλλόμενες συνθήκες του δικτύου, επιτρέποντας την ανίχνευση και αντιμετώπιση επιθέσεων όπως spoofing, botnets και επιθέσεις routing. Η RL μαθαίνει από το περιβάλλον και προσαρμόζει τις παραμέτρους της σε πραγματικό χρόνο, καθιστώντας την κατάλληλη για εφαρμογές σε έξυπνα δίκτυα, όπως τα smart grids και τα συστήματα μεταφορών [170].

Η εφαρμογή τεχνικών Deep Learning, όπως τα CNN, σε περιβάλλοντα SDN επιτρέπει την ανίχνευση επιθέσεων MitM με υψηλή ακρίβεια (99.96%) και χαμηλό ποσοστό ψευδών συναγερμών (0.02%). Το προτεινόμενο σύστημα ενσωματώνεται σε ένα πλαίσιο Intrusion Detection and Prevention System (IDPS) για την προστασία έξυπνων οικιακών συσκευών [171].

Η προσέγγιση Zero Trust, σε συνδυασμό με τεχνικές Micro-Segmentation (MSG), επιτρέπει τον περιορισμό της πλευρικής κίνησης κακόβουλου λογισμικού εντός του δικτύου. Η εφαρμογή αυτών των τεχνικών σε δίκτυα IoT, όπως τα Power IoT (PIoT), ενισχύει την ασφάλεια μέσω ελέγχου ταυτότητας, αξιοπιστίας εξοπλισμού και ακεραιότητας εφαρμογών [172].

Η χρήση τεχνικών μηχανικής μάθησης, όπως οι ensemble learning classifiers, επιτρέπει την ανίχνευση και αντιμετώπιση επιθέσεων botnet σε συστήματα IoT. Το πλαίσιο IMTIBot διαχωρίζει την κίνηση δικτύου σε κανονική και ανώμαλη, βελτιώνοντας την ακρίβεια ανίχνευσης [173].

Οι επιθέσεις σε βιομηχανικά συστήματα IoT, όπως οι επιθέσεις routing και DoS, μπορούν να αντιμετωπιστούν με τεχνικές όπως το egress filtering, η εξουσιοδότηση και τα εργαλεία παρακολούθησης, όπως τα IDS προσαρμοσμένα για IoT, όπως το SVELTE [174].

6.2.1 Χρήση πρωτοκόλλου SNMP

Το SNMP διαδραματίζει σημαντικό ρόλο στην ασφάλεια του IoT, τόσο ως εργαλείο ανίχνευσης επιθέσεων όσο και ως πιθανό σημείο ευπάθειας.

Χρήση του SNMP για Ανίχνευση και Αντιμετώπιση Επιθέσεων στο IoT:

- **Ανίχνευση Επιθέσεων με Χρήση SNMP και Τεχνικών Άμυνας Κινούμενου Στόχου (MTD):** Μια μελέτη προτείνει τη χρήση του SNMP σε συνδυασμό με την απόσταση Kullback-Leibler (KLD), κανόνες ελέγχου πρόσβασης (ACL) και τεχνικές MTD για την ανίχνευση και αντιμετώπιση επιθέσεων DDoS και ψευδούς εισαγωγής δεδομένων σε περιβάλλοντα cloud IoT. Η προσέγγιση αυτή επιτυγχάνει σημαντική μείωση στην πιθανότητα επιθέσεων και καθυστερήσεων [175].
- **Αξιοποίηση Δεδομένων SNMP-MIB με Τεχνικές Μηχανικής Μάθησης:** Άλλη μελέτη διερευνά τη χρήση δεδομένων από τη Βάση Πληροφοριών Διαχείρισης (MIB) του SNMP για την ανίχνευση ανωμαλιών στο δίκτυο μέσω τεχνικών μηχανικής μάθησης, όπως οι Random Forest, AdaboostM1 και MLP. Τα αποτελέσματα δείχνουν υψηλά ποσοστά ανίχνευσης και ταξινόμησης επιθέσεων, καθιστώντας το SNMP πολύτιμο εργαλείο για την ασφάλεια του IoT [176].

Βέλτιστες Πρακτικές για Ασφαλή Χρήση του SNMP στο IoT:

- **Αναβάθμιση σε SNMPv3:** Η έκδοση SNMPv3 προσφέρει βελτιωμένα χαρακτηριστικά ασφάλειας, όπως αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα μέσω χρήσης αλγορίθμων όπως HMAC-SHA-2 και AES. Η υιοθέτηση του SNMPv3 είναι κρίσιμη για την προστασία των συσκευών IoT [177].
- **Εφαρμογή Πολιτικών Ελέγχου Πρόσβασης:** Η χρήση κανόνων ACL και η περιορισμένη πρόσβαση σε αξιόπιστες διευθύνσεις IP μπορούν να μειώσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης μέσω SNMP [175].
- **Συνδυασμός με Τεχνικές Άμυνας Κινούμενου Στόχου (MTD):** Η δυναμική αλλαγή παραμέτρων του συστήματος καθιστά πιο δύσκολη την πρόβλεψη και εκμετάλλευση ευπαθειών από επιτιθέμενους [175].

6.2.2 Χρήση SDN και Intrusion Detection Systems

Η ενσωμάτωση των τεχνολογιών SDN και των Συστημάτων IDS στο περιβάλλον του IoT έχει αναδειχθεί ως κρίσιμη στρατηγική για την ενίσχυση της ασφάλειας, δεδομένων των περιορισμένων πόρων των IoT συσκευών και της αυξανόμενης πολυπλοκότητας των απειλών.

Η αρχιτεκτονική SDN προσφέρει κεντρική διαχείριση και προγραμματιζόμενη δρομολόγηση, καθιστώντας την ιδανική για την εφαρμογή IDS σε περιβάλλοντα IoT. Η δυνατότητα του SDN να παρέχει συνολική εικόνα του δικτύου επιτρέπει την αποτελεσματικότερη ανίχνευση ανωμαλιών. Για παράδειγμα, το σύστημα IDSIoT-SDL χρησιμοποιεί deep learning (LSTM) για την ανάλυση της κυκλοφορίας και την ανίχνευση εισβολών σε δίκτυα IoT, αξιοποιώντας τα χαρακτηριστικά του SDN για τη συλλογή και ανάλυση δεδομένων ροής [178].

Η χρήση τεχνικών μηχανικής μάθησης (ML) και βαθιάς μάθησης (DL) έχει αποδειχθεί αποτελεσματική στην ανίχνευση επιθέσεων σε δίκτυα SDN. Το σύστημα DeepIDS, για παράδειγμα, εφαρμόζει DL για την ανίχνευση ανωμαλιών σε περιβάλλοντα SDN, επιτυγχάνοντας ακρίβεια έως και 90% με τη χρήση μόνο έξι βασικών χαρακτηριστικών ροής . Επιπλέον, το SATIDS, ένα σύστημα δύο επιπέδων βασισμένο σε βελτιωμένο LSTM, επιτυγχάνει ακρίβεια 96,35% στο σύνολο δεδομένων ToN-IoT και 99,73% στο InSDN [179][182].

Η ανάγκη για κλιμακούμενα και αποδοτικά IDS σε περιβάλλοντα IoT οδήγησε στην ανάπτυξη κατανεμημένων συστημάτων. Μια μελέτη προτείνει ένα κατανεμημένο IDS βασισμένο σε SDN, όπου το δίκτυο διαιρείται σε υποδίκτυα, και κάθε υποδίκτυο χρησιμοποιεί δέντρο αποφάσεων

βελτιστοποιημένο με τον αλγόριθμο Black Hole για την ανίχνευση εισβολών, επιτυγχάνοντας ακρίβεια έως και 99,2% [180].

Η ενσωμάτωση τεχνολογιών όπως το Blockchain με DL βασισμένα IDS σε περιβάλλοντα SDN-IIoT προσφέρει ενισχυμένη ασφάλεια. Μια πρόσφατη πρόταση συνδυάζει ένα IDS βασισμένο σε CNN με ένα σύστημα Blockchain για την ενίσχυση της ασφάλειας τόσο στο επίπεδο εφαρμογής όσο και στο επίπεδο δικτύου, αντιμετωπίζοντας επιθέσεις όπως η εισαγωγή εντολών και κανόνων [181].

Προκλήσεις και Μελλοντικές Κατευθύνσεις:

Παρά τα πλεονεκτήματα, η ενσωμάτωση SDN και IDS στο IoT αντιμετωπίζει προκλήσεις, όπως η ανάγκη για ελαφριά και αποδοτικά μοντέλα λόγω των περιορισμένων πόρων των IoT συσκευών. Επιπλέον, η διαχείριση της πολυπλοκότητας και της ετερογένειας των δεδομένων απαιτεί προηγμένες τεχνικές ανάλυσης και προσαρμογής.

6.2.3 Χρήση μεθόδων Reinforcement Learning

Η RL επιτρέπει σε ένα σύστημα να μαθαίνει μέσω αλληλεπίδρασης με το περιβάλλον του, προσαρμόζοντας δυναμικά τις ενέργειές του για τη βελτιστοποίηση της απόδοσης. Στο πλαίσιο της ασφάλειας του IoT, η RL χρησιμοποιείται για την ανάπτυξη ευέλικτων και προσαρμοστικών Συστημάτων IDS, ικανών να εντοπίζουν και να αντιμετωπίζουν επιθέσεις σε πραγματικό χρόνο. Η χρήση της RL συμβάλλει στη μείωση των ψευδών θετικών και στην καλύτερη προσαρμογή σε νέες απειλές [183].

Εφαρμογές της Ενισχυτικής Μάθησης στην Ανίχνευση Εισβολών:

- **Συστηματική Ανασκόπηση της DRL για IDS στο IoT**: Μια πρόσφατη μελέτη ανασκόπησε τις εφαρμογές της Βαθιάς Ενισχυτικής Μάθησης (Deep Reinforcement Learning - DRL) στην ανίχνευση εισβολών στο IoT, αναδεικνύοντας τη βελτίωση στην ακρίβεια εντοπισμού απειλών και τη μείωση των ψευδών θετικών [183].
- **Υβριδικό IDS με DRL σε Υπολογιστικά Περιβάλλοντα Fog-to-Cloud**: Ένα προτεινόμενο σύστημα συνδυάζει DRL για ανίχνευση σε περιβάλλοντα fog και μεθόδους ensemble για ταξινόμηση επιθέσεων στο cloud, επιτυγχάνοντας υψηλή ακρίβεια και ταχύτητα ανίχνευσης [184].
- **Αντιμετώπιση Επιθέσεων σε WSN μέσω Προσαρμοστικής Κρυπτογράφησης με RL**: Ένα μοντέλο RL προσαρμόζει δυναμικά τα επίπεδα κρυπτογράφησης σε Ασύρματα Δίκτυα Αισθητήρων (WSN), ενισχύοντας την ανθεκτικότητα σε επιθέσεις όπως DDoS και wormhole [185].
- **Πραγματικού Χρόνου Άμυνα σε Επιθέσεις Trigger-Action με DRL**: Το σύστημα IoTWarden χρησιμοποιεί DRL για την ανίχνευση και αντιμετώπιση επιθέσεων που εκμεταλλεύονται αλυσίδες trigger-action σε έξυπνα περιβάλλοντα, επιτυγχάνοντας αποτελεσματική άμυνα με χαμηλό υπολογιστικό κόστος [186].

Η Ενισχυτική Μάθηση προσφέρει δυναμικές και προσαρμοστικές λύσεις για την ενίσχυση της ασφάλειας στο IoT, επιτρέποντας την ανίχνευση και αντιμετώπιση επιθέσεων σε πραγματικό χρόνο. Ωστόσο, απαιτείται προσοχή κατά την εκπαίδευση των μοντέλων RL για την αποφυγή ευπαθειών, όπως οι επιθέσεις backdoor. Η συνεχής έρευνα και η ανάπτυξη ασφαλών και αποδοτικών αλγορίθμων RL είναι κρίσιμη για την προστασία των IoT συστημάτων.

6.2.4 Χρήση μεθόδων Deep Learning

Τα συστήματα IoT είναι ιδιαίτερα ευάλωτα σε διάφορες μορφές κυβερνοεπιθέσεων λόγω της μεγάλης κατανομής, της περιορισμένης υπολογιστικής ισχύος και της έλλειψης κατάλληλων μηχανισμών ασφαλείας [187]. Η χρήση μεθόδων **DL** για την ανίχνευση και αντιμετώπιση επιθέσεων στο IoT έχει εξελιχθεί ως μια πολύ υποσχόμενη προσέγγιση, καθώς οι αλγόριθμοι DL μπορούν να αναγνωρίζουν περίπλοκα μοτίβα από μεγάλους όγκους δεδομένων με αυτοματοποιημένο τρόπο. Οι κύριοι τύποι επιθέσεων που αντιμετωπίζονται με DL περιλαμβάνουν επιθέσεις DoS/DDoS, επιθέσεις εισβολής, spoofing, και επιθέσεις μέσω κακόβουλου λογισμικού (malware) [188].

Μέθοδοι DL που χρησιμοποιούνται:

- **Νευρωνικά Δίκτυα Βαθιάς Μάθησης (Deep Neural Networks, DNNs):** Χρησιμοποιούνται για να ταξινομήσουν τα εισερχόμενα δεδομένα δικτύου ως κανονικά ή κακόβουλα [189].
- **Συνελικτικά Νευρωνικά Δίκτυα (CNNs):** Αξιοποιούνται για την εξαγωγή χαρακτηριστικών από δεδομένα δικτύου και συσκευών IoT, ιδιαίτερα όταν τα δεδομένα έχουν χωρική δομή [190].
- **Επαναλαμβανόμενα Νευρωνικά Δίκτυα (RNNs) και Long Short-Term Memory (LSTM):** Ειδικά χρήσιμα για την ανίχνευση επιθέσεων που έχουν χρονική εξάρτηση, όπως επιθέσεις που εξελίσσονται σε διαδοχικά βήματα [191].
- **Autoencoders:** Χρησιμοποιούνται για ανίχνευση ανωμαλιών σε δεδομένα δικτύου IoT, μαθαίνοντας μια συμπιεσμένη αναπαράσταση των φυσιολογικών δεδομένων και εντοπίζοντας αποκλίσεις [192].

Πλεονεκτήματα των DL μεθόδων:

- **Αυτομάθηση χαρακτηριστικών:** Δεν απαιτούν χειροκίνητη επιλογή χαρακτηριστικών (feature engineering) όπως οι παραδοσιακές μέθοδοι.
- **Ικανότητα γενίκευσης:** Μπορούν να ανιχνεύουν νέες, άγνωστες επιθέσεις βασισμένες σε μοτίβα που δεν έχουν ξαναδεί [189][193].
- **Δυναμική προσαρμογή:** Μπορούν να προσαρμοστούν σε μεταβαλλόμενα μοτίβα επιθέσεων και δικτυακών συνθηκών [194].

Προκλήσεις:

- **Υψηλές απαιτήσεις σε πόρους:** Οι συσκευές IoT έχουν περιορισμένη ισχύ, ενώ τα DL μοντέλα είναι υπολογιστικά βαριά [195].
- **Έλλειψη επαρκών δεδομένων εκπαίδευσης:** Τα δεδομένα που χρησιμοποιούνται συχνά είναι από προσομοιώσεις ή περιορισμένα σύνολα δεδομένων, με αποτέλεσμα μειωμένη απόδοση σε πραγματικές συνθήκες [196].
- **Ανάγκη για ανάλυση ερμηνευσιμότητας:** Τα μοντέλα DL είναι "μαύρα κουτιά", γεγονός που δυσκολεύει την ερμηνεία των αποφάσεων τους, κάτι κρίσιμο στην ασφάλεια [197].

Η εφαρμογή Deep Learning για την ανίχνευση και πρόληψη επιθέσεων στο IoT είναι μια ταχέως αναπτυσσόμενη περιοχή έρευνας με σημαντικές επιτυχίες σε ελεγχόμενα περιβάλλοντα. Ωστόσο, η υλοποίηση σε πραγματικά περιβάλλοντα απαιτεί περαιτέρω βελτιώσεις όσον αφορά την αποδοτικότητα, την προσαρμοστικότητα και την ερμηνευσιμότητα των μοντέλων [193][198].

6.2.5 Zero Trust και Micro-Segmentation

Zero Trust είναι ένα μοντέλο ασφάλειας που βασίζεται στην αρχή "μηδενική εμπιστοσύνη", όπου καμία συσκευή ή χρήστης δεν εμπιστεύεται εκ προοιμίου, ακόμα και αν βρίσκεται μέσα στο δίκτυο. Για το IoT, το Zero Trust εφαρμόζεται με την αυστηρή επαλήθευση ταυτότητας και την ελαχιστοποίηση των δικαιωμάτων πρόσβασης, ώστε να περιορίζεται η πιθανότητα εξάπλωσης επιθέσεων.

Η εφαρμογή Zero Trust σε IoT δίκτυα απαιτεί συνεχή επαλήθευση ταυτότητας των συσκευών και των χρηστών, καθώς και έλεγχο πρόσβασης βάσει πολιτικών που καθορίζουν αυστηρά ποιος και πώς μπορεί να έχει πρόσβαση σε πόρους [199].

Η προσαρμογή του Zero Trust στα IoT δίκτυα αντιμετωπίζει προκλήσεις λόγω της μεγάλης ποικιλίας και των περιορισμένων πόρων των IoT συσκευών, απαιτώντας ελαφριά και ευέλικτα πρωτόκολλα επαλήθευσης [200].

Micro-Segmentation είναι μια τεχνική που χωρίζει το δίκτυο σε μικρά, απομονωμένα τμήματα, ώστε να περιορίζεται η εσωτερική κίνηση και να αποτρέπεται η διάδοση επιθέσεων μέσα στο δίκτυο. Στο πλαίσιο του IoT, η MSG επιτρέπει τον διαχωρισμό των συσκευών ανάλογα με το ρόλο και την ευαισθησία τους, μειώνοντας το εύρος των επιθέσεων σε περίπτωση παραβίασης [201]. Τα δυναμικά συστήματα MSG που βασίζονται σε πολιτικές προσαρμοσμένες σε πραγματικό χρόνο μπορούν να βελτιώσουν σημαντικά την ασφάλεια σε περιβάλλοντα IoT με μεγάλο αριθμό συσκευών [202].

6.2.6 Χρήση μεθόδων Ensemble Learning Classifiers

Η ασφάλεια του IoT είναι κρίσιμη λόγω της μεγάλης εξάπλωσης συσκευών και της ευπάθειάς τους σε επιθέσεις όπως DoS, spoofing, malware, κλπ. Οι παραδοσιακές μέθοδοι ανίχνευσης επιθέσεων συχνά δεν είναι αρκετά αποτελεσματικές, γι’ αυτό και η χρήση ensemble learning classifiers έχει αναδειχθεί ως μία πολλά υποσχόμενη προσέγγιση.

Ensemble learning είναι η τεχνική όπου πολλαπλοί ταξινομητές (classifiers) συνδυάζονται ώστε να παράγουν ένα ισχυρότερο μοντέλο από ό,τι κάθε μεμονωμένος ταξινομητής. Η χρήση αυτής της τεχνικής προσφέρει βελτιωμένη γενίκευση, μεγαλύτερη αντοχή σε θόρυβο και καλύτερη ανίχνευση ανωμαλιών.

Πλεονεκτήματα Ensemble learning:

- **Βελτίωση ανίχνευσης επιθέσεων**: Τα ensemble μοντέλα συνδυάζουν π.χ. decision trees, SVM, και neural networks ώστε να μειώσουν τα false positives και false negatives σε επιθέσεις IoT [203].
- **Αντοχή σε παραπλανητικά δεδομένα**: Χρησιμοποιώντας διαφορετικούς ταξινομητές, το μοντέλο είναι πιο σταθερό απέναντι σε θόρυβο και adversarial επιθέσεις [204].
- **Προσαρμοστικότητα και ευελιξία**: Τα ensemble μοντέλα μπορούν να ενσωματώσουν νέα δεδομένα ή να προσαρμοστούν σε νέες επιθέσεις χωρίς να απαιτείται πλήρης επανεκπαίδευση [205].
- **Εφαρμογές στο IoT**: Τα ensemble μοντέλα έχουν χρησιμοποιηθεί για ανίχνευση DDoS επιθέσεων, κακόβουλου λογισμικού, και ανωμαλιών στα δίκτυα αισθητήρων IoT [206][207].

6.2.7 Χρήση τεχνικών Egress Filtering

Egress filtering είναι μια τεχνική δικτυακού ελέγχου που περιορίζει την κυκλοφορία που εξέρχεται από ένα δίκτυο (outbound traffic), επιτρέποντας μόνο συγκεκριμένες επιτρεπόμενες ροές προς το εξωτερικό δίκτυο. Στην περίπτωση του IoT, όπου πολλές συσκευές είναι ευάλωτες σε επιθέσεις λόγω περιορισμένων πόρων και κακής ασφάλειας, το egress filtering χρησιμοποιείται για να περιορίσει την ικανότητα αυτών των συσκευών να στέλνουν κακόβουλη ή μη εξουσιοδοτημένη κίνηση στο διαδίκτυο.

Λόγοι Χρήσης Egress Filtering στο IoT:

- **Περιορισμός κακόβουλης εξόδου:** Τα IoT devices που έχουν μολυνθεί μπορούν να χρησιμοποιηθούν για επιθέσεις DDoS, spam ή να στέλνουν δεδομένα χωρίς έλεγχο. Το egress filtering εμποδίζει τέτοιες μη εξουσιοδοτημένες εξερχόμενες συνδέσεις [208].
- **Εντοπισμός και απομόνωση συμβάντων:** Μέσω του φιλτραρίσματος, αν εντοπιστούν ασυνήθιστες εξερχόμενες ροές, μπορούν να ληφθούν μέτρα άμεσα ώστε να σταματήσει η εξάπλωση επίθεσης ή η διαρροή δεδομένων [209].
- **Μείωση επιφάνειας επίθεσης:** Με την επιβολή κανόνων που επιτρέπουν μόνο συγκεκριμένα πρωτόκολλα και προορισμούς, μειώνεται ο κίνδυνος για μη εξουσιοδοτημένη πρόσβαση ή χρήση των IoT συσκευών ως "botnet" nodes [210].

Σε περιβάλλοντα με χιλιάδες IoT συσκευές, όπως έξυπνες πόλεις ή βιομηχανικά δίκτυα, το egress filtering μπορεί να εφαρμοστεί σε επίπεδο gateway ή router για να ελέγξει τα δεδομένα που αποστέλλονται προς το cloud ή τρίτους παρόχους [211].

Έρευνες δείχνουν ότι με κατάλληλη ρύθμιση κανόνων egress filtering, οι επιθέσεις τύπου Mirai botnet μειώθηκαν σημαντικά, καθώς το κακόβουλο traffic δεν μπορούσε να βγει από το τοπικό δίκτυο [212].

6.2.8 Χρήση τεχνικών Machine Learning

Είναι σημαντικό να προσεγγιστούν οι μελέτες με οργανωμένο τρόπο, καθώς ξεκινά η ανάλυση των εφαρμογών ML και DL στην ασφάλεια του IoT. Η ανάλυση παρουσιάζει τις έρευνες με χρονολογική σειρά, από τα παλαιότερα προς τα νεότερα, προκειμένου να δοθεί μια σαφής προοπτική για την εξέλιξη και την βελτίωση των τεχνικών ML και DL με την πάροδο του χρόνου. Κάθε έρευνα που πραγματοποιήθηκε αποτελεί μια στάση στην πορεία των τεχνολογιών, δείχνοντας πώς κάθε νέα εξέλιξη βασίστηκε στην προηγούμενη για την αντιμετώπιση όλο και πιο πολύπλοκων ζητημάτων ασφάλειας. Ο Alrashdi κ.ά. [110], διερευνούν την χρήση του ML στον τομέα της ασφάλειας έξυπνων πόλεων χρησιμοποιώντας το dataset UNSW-NB15 και τον αλγόριθμο RF. Η εστίαση τους στην ανίχνευση ανωμαλιών παράγει εντυπωσιακά αποτελέσματα, με accuracy 99.34% και σχεδόν τέλειες βαθμολογίες σε precision, recall και F1-score με ποσοστό 98%, αποδεικνύοντας την αποτελεσματικότητα του RF στον εντοπισμό ακανόνιστων μοτίβων μέσα σε ροές αστικών δεδομένων. Στον τομέα των οπτικών δικτύων, ο Bensalem και η ομάδα του [111], χρησιμοποιούν ένα ANN για την καταπολέμηση των επιθέσεων jamming, ενώ εργάζονται με ένα ιδιωτικό dataset. Η έρευνα τους επιτυγχάνει υψηλό accuracy 99.5%, δείχνοντας τις δυνατότητες του ANN στην προστασία κρίσιμων δικτυακών υποδομών. Ο Hasan και οι συνεργάτες του [112], δοκιμάζουν διάφορα μοντέλα ML και DL, όπως DT, RF και ANNs, στο dataset DS2OS για την αντιμετώπιση διαφόρων τύπων επιθέσεων. Όλα τα μοντέλα επιτυγχάνουν υψηλό accuracy 99.4%, αλλά το μοντέλο RF προτιμάται επειδή υπερτερεί έναντι άλλων κρίσιμων μετρικών όπως το precision, το recall και το F1-score, τα οποία είναι όλα στο 99%. Ο Jan κ.ά. [113], δημιούργησαν ένα καινοτόμο ελαφρύ σύστημα IDS χρησιμοποιώντας τον αλγόριθμο SVM, ειδικά για να ξεπεράσουν τις αδυναμίες που έχουν τα συστήματα IoT, οι οποίες συζητήθηκαν στο κεφάλαιο 6. Η ομάδα διεξήγαγε ενδελεχή έρευνα χρησιμοποιώντας δύο ξεχωριστά πειράματα για να

επικυρώσει την αποτελεσματικότητα του μοντέλου τους υπό διαφορετικές συνθήκες. Στο πρώτο πείραμα, χρησιμοποιώντας ένα ιδιωτικό dataset, το IDS είχε ικανοποιητικές επιδόσεις, επιτυγχάνοντας accuracy 91%. Βασιζόμενοι σε αυτό, διεξήχθη ένα δεύτερο πείραμα με το dataset CICIDS2017 και το σύστημα βελτίωσε σημαντικά το accuracy του, φτάνοντας το 98.35%. Χρησιμοποιώντας ένα DNN βελτιστοποιημένο με διαφορετικούς αλγορίθμους EL, η ομάδα του Liao [74], δημιουργεί ένα σύστημα ελέγχου ταυτότητας για το φυσικό επίπεδο βασισμένο σε DL που προστατεύει από επιθέσεις πλαστογράφησης. Η μελέτη τους όχι μόνο εξετάζει την αποτελεσματικότητα αυτών των αλγορίθμων, αλλά προσφέρει επίσης μια σύγκριση των τεχνικών ελέγχου ταυτότητας με βάση το RMS (Root Mean Square) και το Adam (Adaptive Moment Estimation) με βάση τις διαφορετικές απαιτήσεις. Σύμφωνα με την έρευνα τους, η Adam-based μέθοδος αυθεντικοποίησης έχει την ταχύτερη ταχύτητα σύγκλισης και ένα 97.75% ποσοστό accuracy, αλλά έχει ένα υψηλότερο υπολογιστικό κόστος. Σε αντίθεση, η RMS-based προσέγγιση έχει ένα πιο αργό ποσοστό σύγκλισης αλλά παράγει μια ελαφρώς χαμηλότερο accuracy 96.50%. Αυτό οφείλεται στην σημαντικά χαμηλότερη επιβάρυνση υπολογισμού της. Εξαιτίας της προσαρμοστικότητας, οι χρήστες μπορούν να επιλέξουν την καλύτερη τεχνική αυθεντικοποίησης για τις ανάγκες τους βασισμένη τους υπολογιστικούς πόρους που διαθέτουν. Προκειμένου να εντοπίσουν και να κατηγοριοποιήσουν σοβαρές απειλές δικτύου, όπως blackhole, DDoS, sinkholes και wormholes, οι Thamilarasu και Chawla [114], αναπτύσσουν ένα IDS χρησιμοποιώντας DNN. Με μέσο ποσοστό precision 95%, recall 97% και F1-score 96%, το σύστημα τους αποδίδει σε ικανοποιητικό βαθμό. Οι Wang κ.ά. [115], αναλύουν δεδομένα από μονάδες μετρήσεις φασμάτων (Phasor Measurement Unit, PMU) για να προτείνουν ένα προηγμένο μοντέλο για την ανίχνευση επιθέσεων δικτύου σε διαταραχές των smart grids χρησιμοποιώντας RF ενισχυμένο με AdaBoost. Με accuracy 93.91%, precision 93.8%, recall 93.6% και F1-score 93.5%, η μέθοδος τους ανιχνεύει με επιτυχία 37 διαφορετικές κυβερνοεπιθέσεις. Συνδυάζοντας γενετικούς αλγορίθμους με DBN, ο Zhang και η ομάδα του [116], υλοποιούν ένα ευρηματικό IDS, το οποίο αξιολογείται στο dataset NSL-KDD. Με εντυπωσιακό μέσο accuracy 98.8%, precision 97.3%, recall 97.6% και F1-score 97.4%, αντιμετωπίζουν ένα ευρύ φάσμα επιθέσεων, συμπεριλαμβανομένων των DoS, R2L, U2R και Probe. Οι Abu Al-Haija και Zein-Sabatto [117], χρησιμοποιούν ένα CNN στο dataset NSL-KDD για να αναπτύξουν αυτόνομα συστήματα ανίχνευσης και ταξινόμησης DL για κυβερνοεπιθέσεις. Το σύστημα τους υπερέχει στον εντοπισμό επιθέσεων DoS, R2L, U2R και Probe με accuracy 99.3%, precision 99.04%, recall 99.33% και F1-score 99.18%. Το LightGBM χρησιμοποιείται από τον Alkasassbeh κ.ά [71], για την καταπολέμηση εξελιγμένων επιθέσεων botnet με βάση το dataset N-BaIoT. Επιτυγχάνουν το απόλυτο σε όλες τις μετρικές, 100% accuracy, precision, recall και F1-score, αποδεικνύοντας την αξιοσημείωτη ικανότητα του LightGBM να χειρίζεται προηγμένες επιθέσεις στο IoT. Για MANET δίκτυα, ο Amouri κ.ά [118], παρουσιάζουν ένα IDS δύο σταδίων που στοχεύει σε επιθέσεις DDoS και blackhole. Με βάση ένα ιδιωτικό dataset και ένα αλγόριθμο RF, το σύστημα τους παρουσιάζει μεταβλητή απόδοση υπό διάφορες συνθήκες. Επιτυγχάνει accuracy 98% σε σενάρια υψηλής ισχύος/ταχύτητας των κόμβων και accuracy 90% σε συνθήκες χαμηλής ισχύος/ταχύτητας των κόμβων, αποδεικνύοντας την προσαρμοστικότητα του σε ένα εύρος επιχειρησιακών περιβαλλόντων. Ο Arjoune και οι συνεργάτες [119], του χρησιμοποιούν τον αλγόριθμο RF σε ένα ιδιωτικό dataset για να βελτιώσουν την ασφάλεια του δικτύου έναντι επιθέσεων jamming. Με accuracy 97.5%, το σύστημα τους είναι σε θέση να ανιχνεύει με επιτυχία τέτοιου είδους επιθέσεις. Ο Bagaa κ.ά [120], χρησιμοποιούν το one-class SVM για την υλοποίηση ενός συστήματος IDS σε έξυπνα κτίρια. Για την δοκιμή χρησιμοποιείται το dataset NSL-KDD. Με υψηλό accuracy 99.71%, η μέθοδος τους δείχνει πως το one-class SVM μπορεί να χρησιμοποιηθεί για την προστασία εξελιγμένων συστημάτων διαχείρισης κτιρίων. Ο Chen κ.ά. [121], χρησιμοποιούν το DT σε ένα ιδιωτικό dataset για να δημιουργήσουν ένα αξιόπιστο IDS σχεδιασμένο ειδικά για επιθέσεις DDoS. Τα αξιοσημείωτο accuracy 99.98%, το precision και το recall λίγο πάνω από 97% και η αντίστοιχη βαθμολογία F1-score αναδεικνύουν πόσο καλά τα DTs μπορούν να

διακρίνουν μεταξύ μη κακόβουλης και κακόβουλης κυκλοφορίας. Ο Hoang κ.ά [122], διερευνούν την χρήση των αλγορίθμων k-means και one-class SVM στην ανίχνευση επιθέσεων eavesdropping σε συστήματα που υποστηρίζονται από UAV. Όταν η ισχύς του υποκλοπέα είναι μεταξύ 0 και 10 dB, το one-class SVM αποδίδει καλά με accuracy περίπου 90%. Σε υψηλότερα επίπεδα ισχύος, μεταξύ 12 και 20 dB, ο k-means γίνεται πιο πλεονεκτικός, επιτυγχάνοντας accuracy 99%. Ο Kasturi και οι συνάδελφοι του , χρησιμοποιούν το GB σε ένα ιδιωτικό dataset για να δημιουργήσουν ένα μηχανισμό για την κατηγοριοποίηση διαφόρων ειδών επιθέσεων jamming. Με accuracy 94.2%, το σύστημα τους καθιστά τα ασύρματα δίκτυα πιο ανθεκτικά, επιτρέποντας πιο εξελιγμένη ανίχνευση των απειλών. Η επίθεση που στοχεύει στην τροποποίηση του κυκλώματος των συσκευών IoT, γνωστό ως hardware trojan, αντιμετωπίζεται από τον Khalid κ.ά [123]. Χρησιμοποιώντας ένα DNN σε ένα ιδιωτικό dataset, επιτυγχάνουν accuracy 96.25%, αποδεικνύοντας πόσο χρήσιμα είναι τα DNN για τον εντοπισμό τέτοιων τροποποιήσεων που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα της συσκευής. Ο Peng κ.ά [124], προτείνουν ένα δημιουργικό τρόπο για την δημιουργία "δακτυλικών αποτυπωμάτων" ραδιοσυχνοτήτων που μπορούν να χρησιμοποιηθούν για την μοναδική αναγνώριση διαφόρων συσκευών με την χρήση ενός CNN. Η προσέγγιση τους, η οποία δοκιμάστηκε σε ένα ιδιωτικό dataset, επιτυγχάνει accuracy 99.1% ανοίγοντας την πόρτα για περισσότερα μέτρα ασφαλείας με βάση την αυθεντικοποίηση των συσκευών. Χρησιμοποιώντας τον αλγόριθμο RF που έχει δοκιμαστεί στα datasets UNSW-NB15 και CICIDS2017, ο Rashid κ.ά [125], αναπτύσσουν ένα IDS για την ενίσχυση των υποδομών στις έξυπνες πόλεις. Η μέθοδος τους διαχειρίζεται διάφορες απειλές δικτύου και βελτιώνει την ασφάλεια με ικανοποιητικά ποσοστά accuracy 95.45% και εξίσου ίσες βαθμολογίες precision, recall και F1-score. Στον τομέα της υγειονομικής περίθαλψης, ο Roldan κ.ά [68], παρουσιάζουν ένα σύγχρονο μοντέλο LR που προορίζεται για τον εντοπισμό διαφόρων ειδών επιθέσεων σε πραγματικό χρόνο, συμπεριλαμβανομένων των port scans, DoS, TCP και UDP. Αυτό το μοντέλο είναι μοναδικό, καθώς διατηρεί την ακεραιότητα των ιατρικών συστημάτων, εγγυάται την προστασία των ευαίσθητων δεδομένων και λαμβάνει την μέγιστη βαθμολογία σε όλες τις μετρικές απόδοσης. Με έμφαση στην ασφάλεια δικτύων, ο Saharkhizan κ.ά [126], χρησιμοποιούν ένα μοντέλο LSTM για να αντιμετωπίσουν με επιτυχία επιθέσεις DoS και MitM, αποδεικνύοντας την ικανότητα του μοντέλου σε ένα ιδιωτικό dataset. Η έρευνα τους δείχνει πόσο καλά το LSTM μπορεί να αποκωδικοποιήσει και να μετριάσει σύνθετες απειλές στον κυβερνοχώρο σε περιβάλλοντα IoT, με accuracy 99.62%, precision 99.41%, recall 98.88% και F1-score 99.14%. Στην ανάλυση τους για την ανίχνευση επιθέσεων botnet σε έξυπνες πόλεις, ο Shafiq κ.ά [127], συγκρίνουν τους αλγορίθμους C4.5, RF και NB χρησιμοποιώντας δεδομένα από το dataset BoT-IoT. Παρά το γεγονός ότι οι μετρικές αξιολόγησης ήταν ίδιες, με τιμές accuracy 99.79%, precision 100%, recall 100%, F1-score 100%, επιλέχθηκε ο NB λόγω της πολύ μικρότερης περιόδου εκπαίδευσης. Ο Zhang κ.ά [128], διερευνούν νέες προσεγγίσεις για την ανίχνευση επιθέσεων δικτύου συνδυάζοντας SVM και DBN για τον μετριασμό των επιθέσεων DoS στο dataset CICIDS2017. Αυτή η υβριδική προσέγγιση συνδυάζει το DL με τον υπολογισμό της ροής των δεδομένων για να παράγει accuracy 92.56% καθώς και υψηλά ποσοστά precision 97.7%, recall 97.6% και F1-score 97.6%. Ο Gad κ.ά [63], υλοποιούν ένα σύστημα IDS για VANET χρησιμοποιώντας το XGBoost. Η μέθοδος τους βελτιώνει αποτελεσματικά την ασφάλεια στις επικοινωνίες μεταξύ των οχημάτων και πετυχαίνει υψηλά ποσοστά μετρικής, 97.8% accuracy, precision, recall και F1-score, όταν εφαρμόζεται στο dataset ToN-IoT. Χρησιμοποιώντας AE σε συνδυασμό με SVM και εφαρμόζοντας στο dataset NSL-KDD, ο Lv κ.ά [129], δημιούργησαν ένα IDS που πετυχαίνει accuracy 97.83%. Ο Sarker [130], παρέχει μια διεξοδική εξέταση της ανίχνευσης ανωμαλιών και πολλαπλών επιθέσεων με την χρήση του RF σε διάφορα datasets. Το σύστημα επιτυγχάνει 99% σε όλες τις μετρικές για τις ανωμαλίες και τις πολλαπλές επιθέσεις στο NSL-KDD. Στο dataset UNSW-NB15, οι επιδόσεις ποικίλλουν, με την ανίχνευση ανωμαλιών να σημειώνει σε όλες τις μετρικές 95% και την ανίχνευση πολλαπλών επιθέσεων να σημειώνει χαμηλότερες επιδόσεις 82-83%. Χρησιμοποιώντας το AdaBoost σε ένα ιδιωτικό dataset

που αποτελείται από 130.223 δεδομένα επιθέσεων DoS και 130.284 δεδομένα κανονικής κυκλοφορίας, ο Rachmadi κ.ά [131], επικεντρώνονται στην ανίχνευση επιθέσεων DoS. Το μοντέλο αποδίδει με 95.84% accuracy, 98.29% precision, 93.28% recall και 95.72% F1-score. Με την χρήση πολυδιάστατων CNN (CNN1D, CNN2D, CNN3D) στα datasets BoT-IoT και IoT-23, οι Ullah και Mahmoud [132], δημιουργούν ένα ιδιαίτερο IDS. Ωθούν τα όρια του DL στην ασφάλεια του IoT με την ευφυή προσέγγιση τους, η οποία αποδίδει εξαιρετικές μετρήσεις με 99.90% accuracy, 99.75% precision, 99.85% recall και 99.79% F1-score. Ο Yang κ.ά [133], χρησιμοποιούν one-class SVM για να δημιουργήσουν ένα σύστημα ανίχνευσης που προορίζεται ειδικά για συσκευές IoT με περιορισμένους πόρους. Η προσέγγιση τους επικεντρώνεται στην μείωση των απαιτήσεων μνήμης και του χρόνου υπολογισμού για να ταιριάζει σε εφαρμογές του πραγματικού κόσμου και έχει εφαρμοστεί σε διάφορα datasets, συμπεριλαμβανομένων των CICIDS2017, CTU-13 και ιδιωτικών καταναλωτικών datasets IoT. Ωστόσο, δεν δίνονται συγκεκριμένες μετρήσεις επιδόσεων. Ο Popoola κ.ά [134], χρησιμοποιούν στοιβαγμένα (stacked) RNNs για τον εντοπισμό botnets σε έξυπνα σπίτια, τα οποία αποτελούν ένα βήμα μπροστά από τα τυπικά RNNs λόγω του ότι μπορούν να διαχειρίζονται προβλήματα που υπερπροσαρμογής. Η προσέγγιση τους, όταν εφαρμόζεται στο dataset BoT-IoT, επιτυγχάνει τις απόλυτες βαθμολογίες σε όλες τις μετρικές. Σε παρόμοιο πλαίσιο, ο Pokhrel κ.ά [67], εντοπίζουν botnets με ακρίβεια 99.6% χρησιμοποιώντας τον αλγόριθμο KNN στο ίδιο dataset. Ενώ ο SRNN παρέχει άψογα ποσοστά στις μετρικές, ο απλούστερος αλγόριθμος KNN διατηρεί υψηλά ποσοστά accuracy, καθιστώντας τον ελκυστική επιλογή για περιπτώσεις όπου η υπολογιστική οικονομία και η ταχύτητα είναι σημαντικές. Χρησιμοποιώντας το dataset DIDarknet, ο Abu Al-Haija κ.ά [135], παρουσιάζουν έναν εξελιγμένο μηχανισμό ταξινόμησης που συνδυάζει EL αλγορίθμους και ένα DT. Η μέθοδος τους, η οποία επιτυγχάνει αξιοσημείωτο accuracy ταξινόμησης 99.5%, είναι ειδικά σχεδιασμένη για τον εντοπισμό και την ταξινόμηση σύνθετων απειλών, όπως επιθέσεις darknet και blackhole. Οι Lahasan και Samma [136], δημιουργούν ένα ελαφρύ AE ειδικά για την ασφάλεια του IoT χρησιμοποιώντας μια νέα προσέγγιση που εξοικονομεί πόρους. Το dataset N-BaIoT χρησιμοποιείται για την δοκιμή αυτού του μοντέλου, το οποίο έχει λίγα κρυφά στρώματα και μικρό μέγεθος εισόδου. Επιτυγχάνουν εκπληκτικό accuracy 99% χρησιμοποιώντας μόνο 30 χαρακτηριστικά και τροφοδοτώντας δεδομένα σε 2 κρυμμένους νευρώνες. Οι βαθμολογίες precision, recall και F1-score είναι όλες πολυ υψηλές με τιμή 99%. Ο Liu κ.ά [75], χρησιμοποιούν το LSTM+ για να επεξεργαστούν ένα ιδιωτικό dataset θερμοκρασίας με έμφαση στην αξιοπιστία των δεδομένων σε συστήματα IoT. Στόχος του μοντέλου τους είναι ο εντοπισμός και η διόρθωση ανώμαλων δεδομένων, που αποτελεί βασικό στοιχείο της διατήρησης της ακεραιότητας των δεδομένων σε εφαρμογές IoT. Η εφαρμογή του LSTM+ υποδηλώνει μια εξελιγμένη μέθοδο για την εγγύηση της ακρίβειας και της αξιοπιστίας των δεδομένων, παρόλο που δεν δίνονται συγκεκριμένες μετρήσεις. Ο Salman κ.ά [137], δημιούργησαν ένα ισχυρό σύστημα που χρησιμοποιεί έναν αλγόριθμο RF για να εγγυηθεί την ασφάλεια του IoT, δίνοντας έμφαση στην ανίχνευση κακόβουλης κυκλοφορίας και στην αναγνώριση των συσκευών. Με βάση τα τυποποιημένα μοτίβα κίνησης, το σύστημα αυτό δημιουργεί μοναδικά “δακτυλικά αποτυπώματα” για κάθε συσκευή IoT, επιτρέποντας του να αναγνωρίζει τον συγκεκριμένο τύπο κίνησης που παράγει η κάθε συσκευή. Σαρώνει συνεχώς την κυκλοφορία για αλλαγές που ενδέχεται να υποδηλώνουν παραβίαση της συσκευής ή πιθανές παραβιάσεις της ασφάλειας, αποκλίνοντας από αυτά τα αναμενόμενα μοτίβα. Το μοντέλο επιτυγχάνει accuracy 94.5% για τον προσδιορισμό του τύπου της συσκευής, με precision 81.59%, recall 81.51% και F1-score 81.4%. Έχει επίσης ικανοποιητικές επιδόσεις στην ανίχνευση της ανώμαλης κυκλοφορίας με accuracy 97%, precision 85.81%, recall 86.28% και F1-score 86%. Ο Douiba κ.ά [138], ενισχύουν τις δυνατότητες του IDS σε πολλαπλά datasets, συμπεριλαμβανομένων των Edge-IIoT, BoT-IoT, NSL-KDD και IoT-23, αξιοποιώντας ένα DT σε συνδυασμό EL. Το μοντέλο υπερέχει στην ανίχνευση ανωμαλιών, με μέσο accuracy, precision, recall και F1-score 99.99%.

Πίνακας 6.1: Σύνοψη των Ερευνών

Άρθρο	Χρονολογία	Αλγόριθμος	Dataset	Accuracy	Precision	Recall	F1-score
[275]	2019	RF	UNSW-NB15	99.34%	98%	98%	98%
[276]	2019	ANN	Ιδιωτικό	99.5%	-	-	-
[277]	2019	RF	DS2OS	99.4%	99%	99%	99%
[278]	2019	SVM	Ιδιωτικό CICIDS2017	91% 98.35%	-	-	-
[279]	2019	DNN	Ιδιωτικό	96.50%	-	-	-
[280]	2019	DNN	Ιδιωτικό	-	95%	97%	96%
[281]	2019	RF+AdaBoost	Ιδιωτικό	93.91%	93.8%	93.6%	93.5%
[282]	2019	DBN	NSL-KDD	98.8%	97.3%	97.6%	97.4%
[283]	2020	CNN	NSL-KDD	99.3%	99.04%	99.33%	99.18%
[284]	2020	LightGBM	N-BaIoT	100%	100%	100%	100%
[285]	2020	RF	Ιδιωτικό	a) 98% b) 90%	-	-	-
[286]	2020	RF	Ιδιωτικό	97.5%	-	-	-
[287]	2020	OCSVM	NSL-KDD	99.71%	-	-	-
[288]	2020	DT	Ιδιωτικό	99.98%	97%	97%	97%
[289]	2020	k-means OCSVM	Ιδιωτικό	90% 99%	-	-	-
[290]	2020	DNN	Ιδιωτικό	96.23%	-	-	-
[291]	2020	CNN	Ιδιωτικό	99.1%	-	-	-
[292]	2020	RF	UNSW-NB15 CICIDS2017	95.45%	95.45%	95.45%	95.45%
[293]	2020	LR	Ιδιωτικό	100%	100%	100%	100%
[294]	2020	LSTM	Ιδιωτικό	99.62%	99.41%	98.88%	99.14%
[295]	2020	NB	BoT-IoT	99.79%	100%	100%	100%
[296]	2020	SVM+DBN	CICIDS2017	92.56%	97.7%	97.6%	97.6%
[297]	2021	XGBoost	ToN-IoT	97.8%	97.8%	97.8%	97.8%
[298]	2021	AE	NSL-KDD	97.83%	-	-	-
[299]	2021	RF	NSL-KDD UNSW-NB15	99% a) 95% b) 83%	99% a) 95% b) 83%	99% a) 95% b) 83%	99% a) 95% b) 83%
[300]	2021	AdaBoost	Ιδιωτικό	95.84%	98.29%	93.28%	95.72%
[301]	2021	CNN	BoT-IoT IoT-23	99.90%	99.75%	99.85%	99.79%
[302]	2021	OCSVM	CICIDS2017	-	-	-	-

			CTU-13 Ιδιωτικό				
[303]	2021	SRNN	BoT-IoT	100%	100%	100%	100%
[304]	2021	KNN	BoT-IoT	99.6%	-	-	-
[305]	2022	DT+EL	DIDarknet	99.5%	-	-	-
[306]	2022	AE	N-BaIoT	99%	99%	99%	99%
[307]	2022	LSTM+	Ιδιωτικό	-	-	-	-
[308]	2022	RF	Ιδιωτικό	a) 94.5% b) 97%	81.59% 85.81%	81.5% 86.28%	81.4% 86%
[309]	2023	DT+EL	Edge-IIoT BoT-IoT NSL-KDD IoT-23	99.99%	99.99%	99.99%	99.99%

6.3 Ιστορικό αντιμετώπισης επιθέσεων στο IoT

Οι επιθέσεις σε δίκτυα IoT έχουν αυξηθεί ραγδαία, κυρίως λόγω της αδυναμίας των συσκευών αυτών να υιοθετήσουν ισχυρά μέτρα ασφάλειας. Οι κυριότερες επιθέσεις αφορούν botnets, DDoS, malware, και επιθέσεις παραβίασης δεδομένων.

Μία από τις πιο γνωστές επιθέσεις ήταν το botnet Mirai, που εκμεταλλεύτηκε αδύναμους κωδικούς πρόσβασης σε συσκευές IoT για να πραγματοποιήσει τεράστιες επιθέσεις DDoS. Η αντιμετώπιση περιελάμβανε:

- **Αναβάθμιση firmware** και αλλαγή προεπιλεγμένων κωδικών πρόσβασης [213].
- Ανάπτυξη συστημάτων ανίχνευσης και πρόληψης εισβολών ειδικά σχεδιασμένων για IoT [214].
- Χρήση τεχνικών **μηχανικής μάθησης** για την ανίχνευση ασυνήθιστης κίνησης που υποδηλώνει επίθεση [215].

Πολλά malware εκμεταλλεύονται ευπάθειες λογισμικού IoT. Η προσέγγιση περιλαμβάνει:

- Εφαρμογή **πολυεπίπεδων αμυντικών στρατηγικών** (multi-layered security), π.χ., τείχη προστασίας, κρυπτογράφηση και πιστοποίηση [216].
- Χρήση **sandboxing** για την απομόνωση της εκτέλεσης δυνητικά επικίνδυνου κώδικα [217].

Η ανάπτυξη και υιοθέτηση προτύπων όπως το **IEEE 802.1X** για ασφάλεια δικτύου και το **DTLS (Datagram Transport Layer Security)** για κρυπτογράφηση σε συσκευές με περιορισμένους πόρους έχει παίξει καθοριστικό ρόλο [218].

Πρόσφατα, μελέτες προτείνουν τη χρήση blockchain για την αύξηση της ασφάλειας του IoT, προσφέροντας αποκεντρωμένη επαλήθευση ταυτότητας και αδιάβλητο ιστορικό συναλλαγών μεταξύ συσκευών [219].

6.3.1 Επίθεση Mirai Botnet

Το Mirai botnet αποτελεί μια από τις πιο γνωστές απειλές για τα δίκτυα IoT, καθώς εκμεταλλεύεται συσκευές με αδύναμους κωδικούς πρόσβασης και μη ενημερωμένο λογισμικό, προκειμένου να δημιουργήσει μεγάλες επιθέσεις τύπου DDoS [220]. Η αντιμετώπιση αυτής της απειλής απαιτεί πολυεπίπεδη προσέγγιση.

Η ενίσχυση της ασφάλειας των συσκευών IoT είναι κρίσιμη. Η αλλαγή των προεπιλεγμένων κωδικών πρόσβασης και η εφαρμογή ισχυρών πολιτικών διαχείρισης κωδικών πρόσβασης μειώνουν σημαντικά τον κίνδυνο επιθέσεων τύπου Mirai [221]. Παράλληλα, η τακτική ενημέρωση του λογισμικού των συσκευών για την επιδιόρθωση ευπαθειών αποτελεί ουσιαστικό μέτρο πρόληψης, καθώς οι παλιές εκδόσεις περιέχουν γνωστά κενά ασφαλείας που εκμεταλλεύεται το botnet [222].

Η χρήση τεχνικών ανίχνευσης και φιλτραρίσματος στο δίκτυο συμβάλλει στην έγκαιρη ανίχνευση και απομόνωση των μολυσμένων συσκευών. Η ανάλυση της κυκλοφορίας δικτύου με τη χρήση αλγορίθμων μηχανικής μάθησης μπορεί να εντοπίσει ασυνήθιστη συμπεριφορά που παραπέμπει σε επιθέσεις Mirai, ενώ η εφαρμογή φίλτρων σε επίπεδο δικτύου, όπως κανόνες firewall και περιορισμοί rate limiting, μειώνει τις επιπτώσεις των επιθέσεων DDoS [223][224].

Η υιοθέτηση νέων αρχιτεκτονικών ασφαλούς IoT δικτύου, όπως οι λύσεις βασισμένες σε blockchain ή άλλες κατανεμημένες τεχνολογίες αυθεντικοποίησης, ενισχύει την αξιοπιστία και την ασφάλεια των συσκευών, καθιστώντας πιο δύσκολη την παραβίαση και την πρόσβαση από κακόβουλους παράγοντες [225].

Η συνεργασία μεταξύ παρόχων υπηρεσιών, κατασκευαστών και τελικών χρηστών είναι απαραίτητη για την αποτελεσματική αντιμετώπιση του προβλήματος. Η ενημέρωση και η ευαισθητοποίηση σχετικά με τις απειλές του Mirai συμβάλλουν στην υιοθέτηση ασφαλέστερων πρακτικών και την αποφυγή των κοινών λαθών που εκμεταλλεύεται το botnet [226].

6.3.2 Επίθεση BrickerBot

Το BrickerBot είναι ένα κακόβουλο λογισμικό (malware) που στοχεύει συσκευές IoT με σκοπό να τις καταστρέψει μόνιμα ("permanent denial of service" ή PDoS), μέσω της διαγραφής κρίσιμων αρχείων και της καταστροφής της μνήμης αποθήκευσης των συσκευών. Το BrickerBot, παρόμοιο με το Mirai, εκμεταλλεύεται ευπαθείς συσκευές με αδύναμους ή προεπιλεγμένους κωδικούς και μη ενημερωμένο λογισμικό [227].

Η αντιμετώπιση του BrickerBot απαιτεί κυρίως προληπτικά μέτρα και σχεδιασμό συστημάτων που να είναι ανθεκτικά σε τέτοιες επιθέσεις. Καταρχάς, η κύρια προτεραιότητα είναι η βελτίωση της ασφάλειας των IoT συσκευών μέσω της αλλαγής των προεπιλεγμένων κωδικών πρόσβασης και της εφαρμογής ισχυρών πολιτικών διαχείρισης κωδικών [228]. Επιπλέον, η τακτική και αυτόματη ενημέρωση του firmware των συσκευών μειώνει τις ευπάθειες που μπορεί να εκμεταλλευτεί το κακόβουλο λογισμικό [222].

Η υιοθέτηση αρχιτεκτονικών ασφαλούς δικτύου που περιλαμβάνουν συστήματα IDS ειδικά προσαρμοσμένα για IoT, επιτρέπει την έγκαιρη ανίχνευση και απόκριση σε ύποπτη δραστηριότητα, όπως προσπάθειες πρόσβασης από BrickerBot [229]. Η χρήση τεχνικών μηχανικής μάθησης για την ανάλυση συμπεριφοράς δικτύου έχει αποδειχθεί αποτελεσματική στην αναγνώριση προτύπων επίθεσης που συχνά διαφεύγουν από παραδοσιακές λύσεις [230].

Η διασφάλιση ότι οι συσκευές IoT λειτουργούν σε απομονωμένα ή "ασφαλή" δίκτυα (network segmentation) περιορίζει το εύρος της επίθεσης, αποτρέποντας την επέκταση του BrickerBot σε άλλες συσκευές ή τμήματα του δικτύου [231]. Η χρήση firewall και συστημάτων φιλτραρίσματος κυκλοφορίας με ειδικούς κανόνες για το IoT μειώνει επίσης τις πιθανότητες επιτυχούς επίθεσης [224].

Η συνεργασία μεταξύ κατασκευαστών συσκευών, παρόχων δικτύου και τελικών χρηστών είναι κρίσιμη. Η ενημέρωση για τους κινδύνους και η εκπαίδευση στη σωστή χρήση και διαχείριση των συσκευών IoT μπορούν να μειώσουν σημαντικά τον αριθμό των ευπαθειών που εκμεταλλεύεται το BrickerBot [226].

6.3.3 Επίθεση VPNFilter

Το VPNFilter είναι ένα πολυλειτουργικό malware που στοχεύει κυρίως οικιακούς και μικρού μεγέθους routers και άλλες συσκευές IoT. Το κακόβουλο αυτό λογισμικό είναι ικανό να συλλέγει δεδομένα, να εκτελεί εντολές απομακρυσμένα και να καταστρέφει συσκευές μέσω “bricking” [232]. Το VPNFilter έχει προκαλέσει σημαντικές ανησυχίες για την ασφάλεια δικτύων IoT, λόγω της πολυπλοκότητας και της επιθετικότητάς του.

Η αντιμετώπιση του VPNFilter απαιτεί ένα συνδυασμό τεχνικών και οργανωτικών μέτρων. Η εφαρμογή τακτικών ενημερώσεων λογισμικού firmware σε όλες τις IoT συσκευές είναι καθοριστική για την κάλυψη ευπαθειών που εκμεταλλεύεται το malware [222]. Η αλλαγή των προεπιλεγμένων κωδικών πρόσβασης και η υιοθέτηση αυστηρών πολιτικών διαχείρισης κωδικών μειώνουν τις πιθανότητες επιτυχούς εισβολής [233].

Για την ανίχνευση και αποτροπή επιθέσεων VPNFilter, οι τεχνολογίες ανίχνευσης εισβολών (IDS) που βασίζονται σε μηχανική μάθηση και ανάλυση δικτυακής συμπεριφοράς έχουν αποδειχθεί ιδιαίτερα αποτελεσματικές. Με την παρακολούθηση ασυνήθιστης κυκλοφορίας και πρότυπων που παραπέμπουν σε επίθεση, μπορούν να εντοπιστούν οι μολυσμένες συσκευές και να ληφθούν μέτρα απομόνωσης [229][230].

Η αρχιτεκτονική των δικτύων πρέπει να υποστηρίζει το network segmentation ώστε να περιορίζεται η εξάπλωση του malware σε ολόκληρο το δίκτυο [231]. Η υλοποίηση πολιτικών firewall και κανόνων φιλτραρίσματος, ειδικά προσαρμοσμένων για IoT, συνεισφέρει στην περαιτέρω αποτροπή της μόλυνσης [224].

Η συνεργασία μεταξύ κατασκευαστών συσκευών, παρόχων υπηρεσιών διαδικτύου και χρηστών είναι επίσης κρίσιμη. Η εκπαίδευση των χρηστών στην ασφαλή χρήση των συσκευών και η γρήγορη ανταπόκριση σε ενδεχόμενες επιθέσεις μειώνουν το συνολικό ρίσκο από το VPNFilter [226].

6.3.4 Επίθεση Reaper Botnet

Το Reaper Botnet (γνωστό και ως IoTroop) είναι ένα εξελιγμένο malware που στοχεύει συσκευές IoT, όπως κάμερες ασφαλείας, routers και άλλες έξυπνες συσκευές. Σε αντίθεση με το Mirai, το Reaper εκμεταλλεύεται ευπάθειες λογισμικού και όχι μόνο αδύναμους κωδικούς πρόσβασης, καθιστώντας την ανίχνευση και αντιμετώπιση πιο περίπλοκη [234].

Η αντιμετώπιση του Reaper απαιτεί πολυεπίπεδη προσέγγιση. Η τακτική ενημέρωση και patching του firmware των συσκευών IoT είναι ζωτικής σημασίας, καθώς το Reaper εκμεταλλεύεται γνωστές ευπάθειες που έχουν ήδη διορθωθεί σε νεότερες εκδόσεις λογισμικού [222]. Η υιοθέτηση ισχυρών

πολιτικών διαχείρισης κωδικών, όπως η αποφυγή προεπιλεγμένων και αδύναμων κωδικών, αποτελεί βασικό μέτρο πρόληψης [235].

Η χρήση συστημάτων ανίχνευσης εισβολών (IDS) και ανάλυσης δικτυακής κυκλοφορίας που βασίζονται σε τεχνικές μηχανικής μάθησης επιτρέπει την έγκαιρη αναγνώριση της ύποπτης δραστηριότητας και των μοτίβων που σχετίζονται με το Reaper Botnet. Αυτές οι λύσεις μπορούν να εντοπίσουν μη φυσιολογική συμπεριφορά, ακόμα και σε περιπτώσεις που το malware κρύβεται πίσω από νόμιμη κίνηση [229][236].

Η τμηματοποίηση segmentation των δικτύων IoT, δηλαδή η απομόνωση κρίσιμων συσκευών σε ξεχωριστά υποδίκτυα, περιορίζει την εξάπλωση του botnet σε άλλες συσκευές και δίκτυα [231]. Τα firewall και τα συστήματα φιλτραρίσματος δικτυακής κίνησης, ειδικά ρυθμισμένα για το IoT περιβάλλον, αποτελούν επίσης σημαντικό εργαλείο για την αποτροπή επιθέσεων [224].

Η ευαισθητοποίηση των χρηστών και η συνεργασία μεταξύ των κατασκευαστών συσκευών, των παρόχων υπηρεσιών και των φορέων ασφάλειας είναι κρίσιμες για την πρόληψη και την αντιμετώπιση επιθέσεων από το Reaper Botnet. Η εκπαίδευση στην ασφαλή χρήση των συσκευών και η εφαρμογή καλών πρακτικών μπορούν να μειώσουν σημαντικά το εύρος των ευπαθειών [226].

6.4 Επίλογος

Η αντιμετώπιση των επιθέσεων στο IoT απαιτεί ολοκληρωμένη προσέγγιση που συνδυάζει τεχνικά μέτρα, ενημέρωση χρηστών και συνεχή παρακολούθηση. Με την αύξηση της διασύνδεσης των συσκευών, η ασφάλεια πρέπει να αποτελεί προτεραιότητα από το στάδιο του σχεδιασμού, εξασφαλίζοντας την προστασία των δεδομένων και τη σταθερότητα των συστημάτων. Μόνο έτσι μπορούμε να εκμεταλλευτούμε πλήρως τα οφέλη του IoT, μειώνοντας ταυτόχρονα τους κινδύνους από κακόβουλες επιθέσεις.

Κεφάλαιο 7ο: Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Η παρούσα εργασία ανέδειξε τις σοβαρές προκλήσεις που αντιμετωπίζει η ασφάλεια των πρωτοκόλλων στα κατώτερα επίπεδα του IoT, εστιάζοντας τόσο στις ευπάθειες που εκμεταλλεύονται επιτιθέμενοι όσο και στις τεχνικές πρόληψης και αντιμετώπισης των επιθέσεων. Η ανάλυση έδειξε ότι πολλά από τα χρησιμοποιούμενα πρωτόκολλα στερούνται επαρκών μηχανισμών ασφαλείας, κυρίως λόγω περιορισμένων υπολογιστικών πόρων και της ανάγκης για χαμηλή κατανάλωση ενέργειας. Παρόλο που υπάρχουν λύσεις όπως ελαφριά πρωτόκολλα κρυπτογράφησης και μηχανισμοί ανίχνευσης εισβολών, απαιτείται περαιτέρω έρευνα και βελτίωση για την αποτελεσματική προστασία των συσκευών. Η ασφάλεια στο IoT δεν αποτελεί μόνο τεχνική πρόκληση αλλά και κρίσιμο παράγοντα για την ευρύτερη αποδοχή και αξιοπιστία των αντίστοιχων τεχνολογιών στο μέλλον.

Η έρευνα παρείχε παραδείγματα διάφορων τύπων επιθέσεων, καθώς και ιστορικό από μεγάλες επιθέσεις στο παρελθόν και τεχνικές που χρησιμοποιήθηκαν για την αντιμετώπιση τους. Αναφέρθηκαν, επίσης, τρόποι πρόληψης, ώστε να αποφευχθούν παρόμοιου τύπου επιθέσεις στο μέλλον.

Μελλονικά, η ανάπτυξη ελαφριών και αποδοτικών μοντέλων ανίχνευσης είναι απαραίτητη για την αποτελεσματική προστασία συσκευών σε οικοσυστήματα IoT. Αυτά τα μοντέλα πρέπει να μπορούν να λειτουργούν με περιορισμένους πόρους και να παρέχουν αξιόπιστη ανίχνευση απειλών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Rahul Sharma, Nitin Pandey, Sunil Kumar Khatri, 2017. Analysis of IoT security at network layer pp. 586-588

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645–1660.

[3] Elksasy, M. S. (2023). Understanding the Internet of Things (IoT) Concepts, Applications and Standards: An Overview. Delta University Scientific Journal, 6(1), 205–210.

[4] Internet Society. (2015). The Internet of Things (IoT): An Overview.

[5] Baiyere, A., Topi, H., Venkatesh, V., Wyatt, J., & Donnellan, B. (2020). The Internet of Things (IoT): A Research Agenda for Information Systems. Communications of the Association for Information Systems, 47.

[6] Butun, I., Österberg, P., & Song, H. (2019).Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616–644.

[7] Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016).Authentication Protocols for Internet of Things: A Comprehensive Survey.

[8] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, 100129.

[9] Uprety, A., & Rawat, D. B. (2021).Reinforcement Learning for IoT Security: A Comprehensive Survey. IEEE Internet of Things Journal, 8(11), 8693–8706.

[10] Aung, Y. L., Christian, I., Dong, Y., Ye, X., Chattopadhyay, S., & Zhou, J. (2025). Generative AI for Internet of Things Security: Challenges and Opportunities.

[11] Domínguez-Bolaño et al. (2024). An overview of IoT architectures, technologies, and existing open-source projects

[12] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Springer.

[13] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey.

[14] Want, R. (2006). An introduction to RFID technology. IEEE Pervasive Computing.

[15] Ko, H., & Lee, S. (2016). Development of NFC based smart mobile service system for efficient communication. Journal of Applied Science and Engineering.

[16] B. Sotiriadou & E. Karadimitriou, Υπολογιστικό Νέφος και Κατηγορίες Υπηρεσιών, ResearchGate, 2016.

[17] Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology.

[18] Islam, S.M.R. et al. (2015). "The Internet of Things for Health Care: A Comprehensive Survey." IEEE Access.

[19] Yamada, M. et al. (2023). "An IoT-Based Monitoring System for Elderly Living Alone." Electronics, MDPI.

[20] Park, J. et al. (2022). "IoT for Healthcare: Hand Hygiene Monitoring in Hospitals." BMC Health Services Research.

[21] Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M. (2016). "Software-defined industrial Internet of Things in the context of Industry 4.0". IEEE Sensors Journal, 16(20), 7373–7380.

[22] Lu, Y., & Cecil, J. (2016). "An Internet of Things (IoT)-based collaborative framework for advanced manufacturing". The International Journal of Advanced Manufacturing Technology.

[23] Farooq, M. S., Riaz, S., Abid, A., Umer, T., & Zikria, Y. B. (2020). "Role of IoT Technology in Agriculture: A Systematic Literature Review."

[24] ScienceDirect (2023). "Internet of Things and smart sensors in agriculture: Scopes and challenges."

[25] ScienceDirect (2024). "A comprehensive review on smart and sustainable agriculture using IoT technologies."

[26] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). "Internet of Things Security and Forensics: Challenges and Opportunities."

[27] Khanam, F., et al. (2020). "Security Challenges in Internet of Things: A Survey." MDPI Electronics.

[28] Butzin, M., et al. (2022). "Revisiting the internet of things: New trends, opportunities and grand challenges." Frontiers.

[29] Elkhodr, M., et al. (2016). "The Internet of Things: New Interoperability, Management and Security Challenges."

[30] Khan, M. Z., et al. (2021). "Reliable Internet of Things: Challenges and Future Trends." MDPI Electronics.

[31] Radu, L.-D. (2018). "Environmental Issues in Internet of Things: Challenges and Solutions." Acta Universitatis Danubius. Œconomica.

[32] Martens, C. D. P., et al. (2022). "Challenges in the implementation of internet of things projects and actions to overcome them." Technovation.

[33] Safkhani, M., & Bagheri, N. (2017). Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. The Journal of Supercomputing.

[34] Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In Thirteenth Symposium on Usable Privacy and Security.

[35] Tinshu Sasi, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, Shahrear Iqbal (2024). A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges.

[36] Hossein Pourrahmani, Adel Yavarinasab, Amir Mahdi Hosseini Monazzah, Jan Van Herle (2023). A Review of the Security Vulnerabilities and Countermeasures in the Internet of Things Solutions: A Bright Future for the Blockchain.

[37] Rishit Lakhani (2023). Cybersecurity Threats in Internet of Things (IoT) Networks: Vulnerabilities and Defense Mechanisms.

[38] Tripathi, J., De Oliveira, J. C., & Vasseur, J. P. (2022). A survey of RPL enhancements and their impact on performance. Computer Communications.

[39] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials.

[40] Buratti, C., Conti, A., Dardari, D., & Verdone, R. (2022). An overview on wireless sensor networks technology and evolution

[41] Adelantado, F., Vilajosana, X., Tuset-Peiró, P., Martínez, B., Melia-Seguí, J., & Watteyne, T. (2017). Understanding the Limits of LoRaWAN. Future Internet.

[42] Al-Shareeda, M. A., Saare, M. A., Manickam, S., & Karuppayah, S. (2023). Bluetooth low energy for internet of things: review, challenges, and open issues. Indonesian Journal of Electrical Engineering and Computer Science.

[43] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2023). Evolution of Bluetooth Technology: BLE in the IoT Ecosystem.

[44] VINCENT ONOTU FACHE. (2023). BLUETOOTH LOW ENERGY. Mediterranean Publications.

[45] Maggie Ezzat Gaber Gendy, Phi Tham, Flynn Harrison, Mehmet Rasit Yuce (2023). Comparing Efficiency and Performance of IoT BLE and RFID-Based Systems. PMC.

[46] Kang Eun Jeon, James She, Perm Soonsawad, Pc Ng. (2018). BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities. ResearchGate.

[47] Andrea Lacava, Valerio Zottola, Alessio Bonaldo, Francesca Cuomo, Stefano Basagni. (2022). Securing Bluetooth Low Energy networking: An overview of security issues and solutions. ScienceDirect.

[48] Pierluigi Locatelli, Massimo Perri, Daniel Mauricio Jimenez Gutierrez, Andrea Lacava, Francesca Cuomo. (2023). Device discovery and tracing in the Bluetooth Low Energy domain. ScienceDirect.

[49] Xia, S., & Chen, Z. (2018). Bluetooth Mesh: A New Era of Wireless Connectivity for IoT. IEEE Internet of Things Journal.

[50] Liu, X., & Wang, F. (2019). Energy Efficiency in Bluetooth Mesh for IoT Applications. International Journal of Computer Science and Engineering.

[51] Al-Fuqaha, A., & Guizani, M. (2018). Mesh Networks and Smart Cities: Enabling IoT Applications. IEEE Access.

[52] Zhang, W., & Liu, Y. (2020). Security in Bluetooth Mesh Networks: Challenges and Solutions. IEEE Transactions on Industrial Informatics.

[53] Park, M., & Lee, J. (2020). Applications of Bluetooth Mesh in Smart Buildings and Homes. IEEE Transactions on Smart Grid.

[54] Bhat, S., & Elakkiya, R. (2021). Cloud-based IoT Systems using Bluetooth Mesh for Smart Cities. Journal of Cloud Computing.

[55] Jinxiao Zhang. (2023) "The application of bluetooth technology in the internet of things", ResearchGate.

[56] Jinxiao Zhang. (2023) "The application of bluetooth technology in the internet of things", ResearchGate.

[57] Daniele Antonioli, Nils Ole Tippenhauer, Kasper Rasmussen, Mathias Payer. (2020) "BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy".

[58] Sunil Cheruvu et al. (2020) "Bluetooth Low Energy and Bluetooth Classic Comparison", ResearchGate.

[59] Suhas Kulkarni, Uttam Ghosh, Haribabu Pasupuleti (2015) "Considering Security For ZigBee Protocol Using Message Authentication Code"

[60] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials.

[61] Gungor, V. C., & Hancke, G. P. (2009). "Industrial wireless sensor networks: Challenges, design principles, and technical approaches." IEEE Transactions on Industrial Electronics

[62] Anastasi, G., Conti, M., Di Francesco, M., & Passarella, A. (2009). "Energy conservation in wireless sensor networks: A survey." Ad Hoc Networks

[63] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges." 2012 10th International Conference on Frontiers of Information Technology.

[64] Suciu, G., & Telea, A. (2015). "Wireless communication in IoT: ZigBee vs. WiFi." Proceedings of the 18th International Conference on System Theory, Control and Computing (ICSTCC).

[65] F. Gamarra et al., "Energy Consumption Model of SCHC Packet Fragmentation over Sigfox LPWAN," Sensors, vol. 22, no. 6, 2022.

[66] F. Gamarra et al., "A Sigfox Energy Consumption Model," Sensors, vol. 19, no. 3, 2019.

[67] J. Altmann et al., "Evaluation of next-generation low-power communication technology to replace GSM in IoT-applications," IET Communications, vol. 14, no. 18, pp. 3016–3023, 2020.

[68] M. Noura, M. Atiquzzaman, M. Gaedke, "Analysis on functionalities and security features of Internet of Things related protocols," Wireless Networks, 2022.

[69] P. Alemany et al., "SCAP SigFox: A Scalable Communication Protocol for Low-Power Wide-Area IoT Networks," Sensors, vol. 23, no. 7, 2023.

[70] Ali Maki AlAali, Abdulla AlAteeq, Wael Elmedany (2022) "Cybersecurity Threats and Solutions of IoT Network Layer"

[71] Fereidouni, H., Fadeitcheva, O. and Zalai, M. (2025), IoT and Man-in-the-Middle Attacks. Security and Privacy, 8: e70016.

[72] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) IoT Botnets." arXiv, Feb. 13, 2017. Accessed: Nov. 27, 2023. [Online]. Available:

[73] "Yandex Pummeled by Potent Meris DDoS Botnet." Accessed: Feb. 29, 2024. [Online].

[74] "What is recursive DNS?," Cloudflare. Accessed: Feb. 29, 2024. [Online]. Available:https://www.cloudflare.com/learning/dns/what-is-recursive-dns/

[75] "Stuxnet explained:The first known cyberweapon," CSO Online. Accessed: Mar.01, 2024. [Online]. Available: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[76] Bin Hulayyil, S., & Li, S. (2023). Ripple20 Vulnerabilities Detection Using a Featureless Deep Learning Model. Proceedings of the International Conference on Cybersecurity and Privacy, 1–10.

[77] Gelgi, M., Guan, Y., Arunachala, S., Rao, M. S. S., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques. Sensors, 24(11), 3571.

[78] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.

[79] Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.

[80] Gilchrist, A. (2016). Industry 4.0: The Industrial Internet of Things. Apress.

[81] Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). Industrial Control Systems Security: Challenges and Solutions. Computers & Security, 68, 1-10.

[82] Qin, J., Liu, Y., & Grosvenor, R. (2016). A Categorical Framework of Manufacturing for Industry 4.0 and Beyond. Procedia CIRP, 52, 173-178.

[83] Li, L., Zhang, Q., & Wang, B. (2019). *IoT-Based Precision Agriculture for Crop Monitoring*. IEEE Internet of Things Journal, 6(2), 1357-1364.

[84] Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). *Big Data in Smart Farming – A review*. Agricultural Systems, 153, 69-80.

[85] Suryawanshi, A. B., & Patil, M. P. (2020). *Smart Irrigation System Using IoT*. International Journal of Innovative Technology and Exploring Engineering, 9(1), 333-336.

[86] Patel, D., & Thakkar, H. (2021). IoT Based Automated Irrigation System. International Journal of Computer Applications, 174(25), 34-38.

[87] Kamilaris, A., & Prenafeta-Boldú, F. X. (2018). Deep learning in agriculture: A survey. Computers and Electronics in Agriculture, 147, 70-90.

[88] Zhang, C., & Zhang, X. (2019). Crop Disease Monitoring System Based on IoT and Image Processing. Journal of Ambient Intelligence and Humanized Computing, 10(5), 2017-2029.

[89] Ruiz-Garcia, L., Lunadei, L., Barreiro, P., & Robla, J. I. (2009). A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends. Sensors, 9(6), 4728-4750.

[90] Kamilaris, A., Kartakoullis, A., & Prenafeta-Boldú, F. X. (2017). A review on the practice of big data analysis in agriculture. Computers and Electronics in Agriculture, 143, 23-37.

[91] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22–32.

[92] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645–1660.

[93] Mukherjee, M., & Pal, S. (2018). IoT Based Smart Waste Management System for Smart Cities. International Journal of Computer Applications, 182(30), 1-6.

[94] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context Aware Computing for The Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 16(1), 414–454.

[95] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A Review of Internet of Things for Smart Home: Challenges and Solutions. Journal of Cleaner Production, 140, 1454-1464.

[96] Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. Computer, 44(9), 51–58.

[97] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Information centric networking for the internet of things: Challenges and opportunities," IEEE Network, vol. 30, no. 2, pp. 92-100, 2016.

[98] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13–16, 2012.

[99] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," RFC 7252, 2014.

[100] J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 527–537, 2015.

[101] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[102] Riahi, A., Laurent, M., & Fernandez, J. M. (2018). Lightweight cryptography for the Internet of Things: A comprehensive review. Sensors, 18(10), 3301.

[103] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190.

[104] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC), 1-6.

[105] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516.

[106] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing and Communications Workshops (PerCom Workshops), 1-6.

[107] Lotfollahi, M., Shirabad, J. B., & Shirani, A. (2020). Deep learning for IoT security: A survey. Journal of Network and Computer Applications, 148, 102452.

[108] Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

[109] Nguyen, G., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Federated learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658.

[110] Kairouz, P., McMahan, H. B., Avent, B., et al. (2019). Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977.

[111] Zhang, J., et al. (2022). "5G and IoT: Enabling Technologies and Challenges." IEEE Communications Surveys & Tutorials, 24(1), 100-122.

[112] Chen, M., et al. (2023). "6G Networks for IoT: Future Perspectives and Challenges." IEEE Internet of Things Journal, 10(5), 4500-4514.

[113] Singh, K., & Kumar, P. (2021). "Artificial Intelligence in IoT: Applications and Research Directions." Journal of Network and Computer Applications, 176, 102892.

[114] Li, Y., et al. (2022). "Machine Learning for IoT Data Analytics: A Survey." ACM Computing Surveys, 55(3), 1-34.

[115] Dutta, S., & Goyal, N. (2021). "Security and Privacy in IoT: A Comprehensive Survey." Computers & Security, 109, 102384.

[116] Casino, F., et al. (2020). "Blockchain Applications for IoT Security: A Survey." Computer Networks, 173, 107121.

[117] Shi, W., et al. (2016). "Edge Computing: Vision and Challenges." IEEE Internet of Things Journal, 3(5), 637-646.

[118] Bonomi, F., et al. (2012). "Fog Computing and Its Role in the Internet of Things." Proceedings of the MCC Workshop on Mobile Cloud Computing, 13-16.

[119] Al-Fuqaha, A., et al. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[120] Perera, C., et al. (2017). "Sustainable IoT for Smart Cities: Opportunities and Challenges." IEEE Communications Magazine, 55(9), 92-99.

[121] Bakhsh ST, Alghamdi S, Alsemmeari RA, Hassan SR. An adaptive intrusion detection and prevention system for Internet of Things. International Journal of Distributed Sensor Networks. 2019;15(11). doi:10.1177/1550147719888109

[122] Afrah Gueriani, Hamza Kheddar, Ahmed Cherif Mazari (2024) “Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey”

[123] Shalini Subramani, M. Selvi (2023) ”Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks”

[124] Mahjoub, C., Hamdi, M., Alkanhel, R.I. (2024) et al. “An adversarial environment reinforcement learning-driven intrusion detection algorithm for Internet of Things. J Wireless Com Network”

[125] Tianbo Gu, Allaukik Abhishek, Hao Fu, Huanle Zhang, Debraj Basu, Prasant Mohapatra (2020) “Towards Learning-automation IoT Attack Detection through Reinforcement Learning”

[126] Balega, M., Farag, W., Wu, X.-W., Ezekiel, S., Good, Z. (2024) “Enhancing IoT Security: Optimizing Anomaly Detection through Machine Learning”

[127] Chongqi Guan, Heting Liu, Guohong Cao, Sencun Zhu, Thomas La Porta (2023) “HoneyIoT: Adaptive High-Interaction Honeypot for IoT Devices Through Reinforcement Learning”

[128] Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, Benjamin C.M. Fung, Saja Al Mamoori (2023) “Deep learning-enabled anomaly detection for IoT systems”

[129] Hanan Hindy, Ethan Bayne, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Xavier Bellekens (2020) “Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)”

[130] Sheikh Tahir Bakhsh et al., "An adaptive intrusion detection and prevention system for Internet of Things", International Journal of Distributed Sensor Networks, 2019.

[131] Pietro Spadaccino and Francesca Cuomo, "Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing and Machine Learning", arXiv preprint arXiv:2012.01174, 2020.

[132] A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity, 2021.

[133] Pietro Spadaccino and Francesca Cuomo, "Intrusion detection systems for IoT: Opportunities and challenges offered by edge computing", ITU Journal on Future and Evolving Technologies, 2022.

[134] Khawla Shalabi et al., "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review", Procedia Computer Science, 2024.

[135] A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity, 2021.

[136] Gu, T., et al. (2020). "Towards Learning-automation IoT Attack Detection through Reinforcement Learning." arXiv:2006.15826.

[137] Pokhrel, S., et al. (2021). "IoT Security: Botnet detection in IoT using Machine learning." arXiv:2104.02231.

[138] Rey, V., et al. (2021). "Federated Learning for Malware Detection in IoT Devices." arXiv:2104.09994.

[139] Gökçe Karacayılmaz & Harun Artuner (2024) "A novel approach detection for IIoT attacks via artificial intelligence." Cluster Computing.

[140] Petar Radanliev, David De Roure, Carsten Maple, Jason R. C. Nurse, Razvan Nicolescu, Uchenna Ani (2024) "AI security and cyber risk in IoT systems." Frontiers in Big Data.

[141] Yan Lin Aung, Ivan Christian, Ye Dong, Xiaodong Ye, Sudipta Chattopadhyay, Jianying Zhou (2025) "Generative AI for Internet of Things Security: Challenges and Opportunities." arXiv:2502.08886.

[142] Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics 2022, 11, 198. https://doi.org/10.3390/electronics11020198

[143] Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. arXiv preprint arXiv:2502.11470.

[144] Kumar, P., & Singh, R. (2023). A novel hybrid autoencoder and modified particle swarm optimization for intrusion detection in IoT. Frontiers in Computer Science, 15.

[145] Zhang, Y., & Li, X. (2023). Real-time detection method of edge IoT proxy network intrusion based on PSO-ELM. Proceedings of the 2023 International Conference on Artificial Intelligence, Systems and Network Security.

[146] Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., & Bhushan, B. (2022). A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. Sustainability, 14(19), 12828.

[147] Songma, S., Netharn, W., & Lorpunmanee, S. (2024). Extending Network Intrusion Detection with Enhanced Particle Swarm Optimization Techniques. arXiv preprint arXiv:2408.07729.

[148] Li, J., & Wang, H. (2021). A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization and Convolutional Neural Network. Information Sciences, 579, 1-14.

[149] Hussain, M., & Khan, S. (2023). Hybridized bio-inspired intrusion detection system for Internet of Things. Frontiers in Big Data, 6.

[150] A. Khraisat, A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, no. 1, p. 18, 2021.

[151] S. Zhao, et al., "E-GraphSAGE: Graph Neural Network for Network Intrusion Detection," arXiv preprint arXiv:2103.16329, 2021.

[152] A. Gueriani, H. Kheddar, A. C. Mazari, "Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey," arXiv preprint arXiv:2405.20038, 2024.

[153] Y. Wei, M. Shangguan, "A review of deep learning based intrusion detection systems," Highlights in Science, Engineering and Technology, vol. 56, pp. 188-199, 2023.

[154] A. Aljawarneh, et al., "Deep reinforcement learning-based IoT intrusion detection system," Computer Networks, vol. 182, 2020, 107482.

[155] S. Lin, et al., "Deep Q-learning for IoT network security and denial of service attack prevention," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6247–6257, 2020.

[156] F. A. Gers, et al., "Reinforcement learning for adversarial detection in IoT," Sensors, vol. 20, no. 18, 2020, 5237.

[157] J. Chen, et al., "Multi-agent reinforcement learning for cooperative intrusion detection in IoT networks," IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2041–2052, 2021.

[158] R. Han, et al., "Model-based reinforcement learning for IoT security: A survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 259–282, 2022.

[159] Zhou, J., Liu, Y., Fu, X., & Liu, Y. (2019) “Anomaly Detection in IoT Communication Network Based on Spectral Analysis and Hurst Exponent“ Applied Sciences, 9(24), 5319.

[160] Golomb, T., Mirsky, Y., & Elovici, Y. (2018). CIoTA: Collaborative IoT Anomaly Detection via Blockchain. arXiv preprint arXiv:1803.03807.

[161] Marco Arazzi, Serena Nicolazzo & Antonino Nocera (2025) “A Fully Privacy-Preserving Solution for Anomaly Detection in IoT using Federated Learning and Homomorphic Encryption. Information Systems Frontiers.”

[162] Sharma, A., Kalra, S., Choudhary, R., & Chaudhary, R. (2022) “Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security" Complex & Intelligent Systems, 8, 3251–3274.

[163] Ma, X., Tang, H., Li, L., & Wang, X. (2023) “A Fully Privacy-Preserving Solution for Anomaly Detection in IoT using Federated Learning and Homomorphic Encryption” Information Systems Frontiers.

[164] Gaur, M., Chauhan, H., & Alazab, M. (2023). “Analysis of the Cryptographic Algorithms in IoT Communications: Security, Performance and Challenges.” Information Systems Frontiers.

[165] Bernstein, D. J. (2008). “ChaCha, a variant of Salsa20. Workshop Record of the SASC”, 8.

[166] Gaur, M., Chauhan, H., & Alazab, M. (2023). Analysis of the Cryptographic Algorithms in IoT Communications: Security, Performance and Challenges. Information Systems Frontiers.

[167] Hankerson, D., Menezes, A., & Vanstone, S. (2004). “Guide to Elliptic Curve Cryptography”. Springer.

[168] Gayathri R, Usharani S, Mahdal M, Vezhavendhan R, Vincent R, Rajesh M, Elangovan M. (2023) “Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques”. Sensors (Basel).

[169] Pedro Manso, Jose Moura, Carlos Serrao (2021) “SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks”

[170] Aashma Uprety, Danda B. Rawat (2021) “Reinforcement Learning for IoT Security: A Comprehensive Survey”

[171] Nader Karmous, Yassmine Ben Dhiab, Mohamed Ould-Elhassen Aoueileyine, Neji Youssef, Ridha Bouallegue, Anis Yazidi (2024) “Deep learning approaches for protecting IoT devices in smart homes from MitM attacks”

[172] Liu, C., Tan, R., Wu, Y. et al. Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity 7, 20 (2024).

[173] Sebestyen, H.; Popescu, D.E.; Zmaranda, R.D. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. Computers 2025, 14, 61.

[174] Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. IoT 2021, 2, 163-186.

[175] Alkasassbeh, M. (2023). "Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques." Sensors, 23(3), 1708.

[176] Al-Naymat, G., Al-kasassbeh, M., & Al-Hawari, E. (2018). "Exploiting SNMP-MIB Data to Detect Network Anomalies using Machine Learning Techniques."

[177] Alkasassbeh, M. (2023). "The Critical Role of SNMP in Enabling Network Security." ResearchGate.

[178] Wani, M. A., et al. (2021). "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)." CAAI Transactions on Intelligence Technology.

[179] Nguyen, T. T., et al. (2020). "DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking." Electronics, 9(9), 1533.

[180] Luo K. A distributed SDN-based intrusion detection system for IoT using optimized forests. PLoS One. 2023

[181] Kamali Poorazad, S., Benzaïd, C., & Taleb, T. (2023). "Blockchain and Deep Learning-Based IDS for Securing SDN-Enabled Industrial IoT Environments." arXiv preprint arXiv:2401.00468.

[182] Ain Shams Engineering Journal (2023). "Securing IoT and SDN systems using deep-learning based automatic intrusion detection."

[183] Jamshidia, S., Nikanjama, A., Nafia, K. W., Khomha, F., & Rastab, R. (2025). Application of Deep Reinforcement Learning for Intrusion Detection in Internet of Things: A Systematic Review.

[184] A novel reinforcement learning-based hybrid intrusion detection system on fog-to-cloud computing. The Journal of Supercomputing, 80, 26088–26110 (2024).

[185] Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. Sensors, 25(7), 2056.

[186] Alam, M. M., Jahan, I., & Wang, W. (2024). IoTWarden: A Deep Reinforcement Learning Based Real-time Defense System to Mitigate Trigger-action IoT Attacks. arXiv preprint arXiv:2401.08141.

[187] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[188] M. A. Ferrag, L. Maglaras, A. Ahmim, H. Janicke, and J. Jiang, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 58, 2021.

[189] Y. Kim, S. Cho, and H. Kim, "Deep learning-based anomaly detection for IoT devices," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6037–6046, 2019.

[190] W. Lin, X. Guo, and W. Shi, "CNN based network intrusion detection system for IoT," Security and Communication Networks, vol. 2018, 2018.

[191] M. Lotfollahi, M. Shirali Hossein Zade, M. S. Jazi, and R. Sadeghi, "Deep learning approach for network intrusion detection in IoT," IEEE Access, vol. 7, pp. 172140–172150, 2019.

[192] H. Xiao, Y. Xiao, and M. Van der Schaar, "Autoencoder-based anomaly detection for IoT networks," IEEE Transactions on Network Science and Engineering, vol. 7, no. 3, pp. 1476–1486, 2020.

[193] M. A. Ferrag, L. Maglaras, and H. Janicke, "Deep learning-based intrusion detection for IoT security: A review," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1675, 2020.

[194] M. Zolanvari et al., "Deep learning for IoT security: A survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020.

[195] N. Javaid, A. Mahmood, and A. Anpalagan, "Resource-constrained deep learning models for IoT," Sensors, vol. 21, no. 11, 2021.

[196] J. Zhang, P. Wang, and Z. Wang, "Challenges in training deep learning models for IoT cybersecurity," IEEE Network, vol. 34, no. 6, pp. 156–161, 2020.

[197] A. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," arXiv preprint arXiv:1702.08608, 2017.

[198] S. J. Pan, Q. Yang, "A survey on transfer learning," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 10, pp. 1345-1359, 2010.

[199] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology.

[200] Sultana, S., Ahsan, M., & Islam, M. (2021). "Lightweight Zero Trust Architecture for IoT Environments." IEEE Internet of Things Journal, 8(7), 5708-5720.

[201] Modi, C., Patel, D., Borisaniya, B., Patel, H., & Rajarajan, M. (2017). "Micro-segmentation for IoT Security: Architecture and Challenges." IEEE Communications Magazine, 55(9), 70-75.

[202] Kim, J., & Feamster, N. (2018). "Improving Network Security through Micro-Segmentation in Dynamic IoT Environments." ACM SIGCOMM Computer Communication Review, 48(1), 27-34.

[203] Sharma et al., (2020) "Ensemble Learning Approach for IoT Network Intrusion Detection" IEEE Internet of Things Journal

[204] Nguyen et al., 2019 “Robust IoT Intrusion Detection Using Ensemble Learning and Feature Selection" Computer Networks

[205] Khan et al., 2021 "Adaptive Ensemble Learning for Secure IoT Networks" Journal: Sensors

[206] Alazab et al., 2020 "Detecting IoT Botnet Attacks Using Ensemble Machine Learning Models" Future Generation Computer Systems

[207] Singh et al., 2021 "IoT Security: Machine Learning and Ensemble Techniques for Anomaly Detection" IEEE Communications Surveys & Tutorials

[208] Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80-84.

[209] Zolanvari, M., Badiei, S., Dehghantanha, A., Choo, K.-K. R., & Parizi, R. M. (2019). A Systematic Review on Security and Privacy in the Internet of Things: Current Status, Challenges, and Future Directions. IEEE Internet of Things Journal, 6(5), 8186-8202.

[210] Santos, R. L. T., & Barros, R. C. (2020). Egress filtering to mitigate IoT botnets attacks. 2019 IEEE 14th International Conference on Availability, Reliability and Security (ARES), 1-8.

[211] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for Secure Egress Filtering and Network Traffic Control in IoT Environments. IEEE Internet of Things Journal, 7(9), 8700-8713.

[212] Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.

[213] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhu, H. (2017). Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, 1093–1110.

[214] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[215] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

[216] Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44.

[217] Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy (SP), 636-654.

[218] Zhang, Y., Deng, R. H., & Liu, J. K. (2018). Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594-1605.

[219] Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251-279.

[220] Antonakakis, M., et al. (2017). "Understanding the Mirai Botnet." USENIX Security Symposium, pp. 1093–1110.

[221] Kolias, C., et al. (2017). "DDoS in the IoT: Mirai and Other Botnets." Computer, vol. 50, no. 7, pp. 80-84.

[222] Mikhaylov, K., et al. (2019). "Firmware updates for IoT devices: Challenges and solutions." IEEE Communications Surveys & Tutorials, 21(3), 2249-2273.

[223] Nguyen, T. T., & Armitage, G. (2008). "A survey of techniques for Internet traffic classification using machine learning." IEEE Communications Surveys & Tutorials, 10(4), 56-76.

[224] Behal, S., et al. (2020). "DDoS attack mitigation using network filtering techniques." Journal of Network and Computer Applications, 154, 102544.

[225] Christidis, K., & Devetsikiotis, M. (2016). "Blockchains and smart contracts for the Internet of Things." IEEE Access, 4, 2292-2303.

[226] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). "Security and privacy challenges in industrial Internet of Things." Proceedings of the 52nd Annual Design Automation Conference, 54.

[227] Antonakakis, M., et al. (2017). "Understanding the BrickerBot Attack." IEEE Security & Privacy, 15(5), 58-65.

[228] Kolias, C., et al. (2017). "DDoS and PDoS in the IoT: Analysis and Defense Mechanisms." Computer, vol. 50, no. 7, pp. 80-84.

[229] Azmoodeh, A., Dehghantanha, A., & Choo, K-K. R. (2018). "Detecting IoT malware using deep learning." IEEE Access, 6, 25719-25729.

[230] Doshi, R., Apthorpe, N., & Feamster, N. (2018). "Machine learning DDoS detection for consumer IoT devices." IEEE Security and Privacy Workshops, pp. 29-35.

[231] Roman, R., Zhou, J., & Lopez, J. (2013). "On the Features and Challenges of Security and Privacy in Distributed Internet of Things." Computer Networks, 57(10), 2266-2279.

[232] Fu, K., & Blum, J. (2018). "VPNFilter: Analysis and Mitigation of a Multistage IoT Malware." IEEE Security & Privacy, 16(5), 40-47.

[233] Kolias, C., et al. (2017). "DDoS and malware threats in IoT: Detection and mitigation." Computer, 50(7), 80-84.

[234] Sun, K., Yu, F. R., & Zhao, L. (2018). "IoT Security and Privacy: Architecture, Challenges and Solutions." IEEE Communications Magazine, 56(7), 20-26.

[235] Kolias, C., et al. (2017). "DDoS and Botnet Threats in IoT: Detection and Prevention." Computer, 50(7), 80-84.

[236] Doshi, R., Apthorpe, N., & Feamster, N. (2018). "Machine Learning for IoT Botnet Detection." IEEE Security and Privacy Workshops, pp. 29-35.

[237] I. Butun, P. Osterberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” IEEE Commun. Surv. Tutor

[238] P. Pongle and G. Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT,” in 2015 International Conference on Pervasive Computing (ICPC), Pune, India: IEEE, Jan. 2015, pp. 1–6.

[239] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, “IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges,” IEEE Access

[240] A. E. Omolara et al., “The internet of things security: A survey encompassing unexplored areas and new insights,” Comput. Secur., vol. 112, p. 102494, Jan. 2022

[241] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” IEEE Commun. Surv. Tutor., vol. 21, no. 3, pp.

[242] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, vol. 7, pp. 82721– 82743, 2019

[243] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey,” J. Netw. Comput. Appl., vol. 161, p. 102630, Jul. 2020

[244] S. Duangphasuk, P. Duangphasuk, and C. Thammarat, “Review of Internet of Things (IoT): Security Issue and Solution,” in 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI- CON), Phuket, Thailand: IEEE, Jun. 2020, pp. 559–562.

[245] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey,” Sensors, vol. 18, no. 9, p. 2796, Aug. 2018,

[246] Y. Chahid, M. Benabdellah, and A. Azizi, “Internet of Things Protocols Comparison, Architecture, Vulnerabilities and Security: State of the art,” in Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems, Larache Morocco: ACM, Nov. 2017, pp. 1–6.

[247] A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Gener. Comput. Syst., vol. 108, pp. 909–920, Jul. 2020

[248] I. Butun, P. Osterberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” IEEE Commun. Surv. Tutor., vol. 22, no. 1, pp. 616–644, 2020.

[249] A. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” IEEE Trans. Emerg. Top. Comput., vol. 5, no. 4, pp. 586–602, Oct. 2017

[250] H. Akram, D. Konstantas, and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, 2018

[251] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” IEEE Commun. Surv. Tutor., vol. 21, no. 3, pp. 2702–2733, 2019

[252] M. A. Amanullah et al., “Deep learning and big data technologies for IoT security,” Comput. Commun., vol. 151, pp. 495–517, Feb. 2020

[253] G. Glissa, A. Rachedi, and A. Meddeb, “A Secure Routing Protocol Based on RPL for Internet of Things,” in 2016 IEEE Global Communications Conference (GLOBECOM)

[254] Khan, M. A., & Salah, K. (2023). A Comprehensive Survey of IoT Firmware Vulnerabilities and Binary Analysis Techniques. Sensors, 23(22), 7080.

[255] Pawar, P. S., & Kotecha, K. (2019). A Survey on Secure Firmware Update Mechanisms for IoT. ACM Computing Surveys, 52(4), Article 72. ACM.

[256] Perumal, T., et al. (2023). Secure Firmware Updates: Challenges and Solutions for Embedded and IoT Systems. Journal of Cybersecurity and Privacy, 3(1), 88–105.

[257] Rajput, A. R., et al. (2023). Security Challenges and AI-Based Solutions in IoT: A Survey. Sensors, 23(7), 3593. PMC.

[258] Khan, R. A., et al. (2023). A Systematic Review of IoT Vulnerabilities and Security Mechanisms. Applied Sciences, 15(6), 3036. MDPI.

[259] Guan, C., Liu, H., Cao, G., Zhu, S., & La Porta, T. (2023). HoneyIoT: Adaptive High-Interaction Honeypot for IoT Devices Through Reinforcement Learning.

[260] Mfogo, V. S., Zemkoho, A., Njilla, L., Nkenlifack, M., & Kamhoua, C. (2023). AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices.

[261] Dowling, S., Schukat, M., & Barrett, E. (2020). New framework for adaptive and agile honeypots. ETRI Journal, 42(6), 965-975.

[262] Touch, S., Colin, J.-N. (2022) "A Comparison of an Adaptive Self-Guarded Honeypot with Conventional Honeypots." Appl. Sci.

[263] Guarnizo, J. D., Tambe, A., Bhunia, S. S., Ochoa, M., Tippenhauer, N., Shabtai, A., & Elovici, Y. (2017). SIPHON: Towards Scalable High-Interaction Physical Honeypots.

[264] Wang, M., Santillan, J., & Kuipers, F. (2018). ThingPot: an interactive Internet-of-Things honeypot.

[265] Armin Ziaie Tabari, Xinming Ou. (2020) "A Multi-phased Multi-faceted IoT Honeypot Ecosystem"

[266] Naoto Watanabe, Taku Yamazaki, Takumi Miyoshi, Ryo Yamamoto, Masataka Nakahara, Norihiro Okui, Ayumu Kubota (2024) "Self-adaptive Traffic Anomaly Detection System for IoT Smart Home Environments"

[267] Yavuz, E., & Moustafa, N. (2021). Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. Applied Sciences

[268] Marchal, S., Miettinen, M., Nguyen, T. D., & Asokan, N. (2018). DÏoT: A Federated Self-learning Anomaly Detection System for IoT.

[269] Doshi, R., Apthorpe, N., & Feamster, N. (2021). Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT. arXiv preprint arXiv:2109.02544.

[270] Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., & Sivaraman, V. (2019). An Adaptive Intrusion Detection and Prevention System for Internet of Things. International Journal of Distributed Sensor Networks

[271] Shentong Mo, Russ Salakhutdinov, Louis-Philippe Morency, Paul Pu Liang (2024) "IoT-LM: Large Multisensory Language Models for the Internet of Things"

[272] Miada Almasre, Alanoud Subahi (2024) "Create a Realistic IoT Dataset Using Conditional Generative Adversarial Network"

[273] Hanan Hindy, Ethan Bayne, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Xavier Bellekens (2024) “Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)”

[274] Attila Frankó, Gergely Hollósi, Dániel Ficzere, Pal Varga (2022) “Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability”

[275] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, “AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning,” in 2019 IEEE 9th Annual

[276] Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA: IEEE, Jan. 2019, pp. 0305–0310.

[277] M. Bensalem, S. K. Singh, and A. Jukan, “On Detecting and Preventing Jamming Attacks with Machine Learning in Optical Networks,” in 2019 IEEE Global Communications Conference (GLOBECOM), Dec. 2019, pp. 1–6.

[278] M. Hasan, Md. M.Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” Internet Things, vol. 7, p. 100059, Sep. 2019.

[279] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, “Toward a Lightweight Intrusion Detection System for the Internet of Things,” IEEE Access, vol. 7, pp. 42450–42471, 2019.

[280] R.-F. Liao et al., “Security Enhancement for Mobile Edge Computing Through Physical Layer Authentication,” IEEE Access, vol. 7, pp. 116390–116401, 2019.

[281] G. Thamilarasu and S. Chawla, “Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things”, Sensors, vol. 19, no. 9, Art. no. 9, Jan. 2019.

[282] D. Wang, X. Wang, Y. Zhang, and L. Jin, “Detection of power grid disturbances and cyber-attacks based on machine learning,” J. Inf. Secur. Appl., vol. 46, pp. 42–52, Jun. 2019.

[283] Y. Zhang, P. Li, and X. Wang, “Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network,” IEEE Access, vol. 7, pp. 31711–31722, 2019.

[284] Q. Abu Al-Haija and S. Zein-Sabatto, “An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks,” Electronics, vol. 9, no. 12, p. 2152, Dec. 2020.

[285] M. Al-kasassbeh, M. A. Abbadi, and A. M. Al-Bustanji, “LightGBM Algorithm for Malware Detection,” in Intelligent Computing, K. Arai, S. Kapoor, and R. Bhatia, Eds., in Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2020, pp. 391–403.

[286] A. Amouri, V. T. Alaparthy, and S. D. Morgera, “A Machine Learning Based Intrusion Detection System for Mobile Internet of Things,” Sensors, vol. 20, no. 2, Art. no. 2, Jan. 2020.

[287] Y. Arjoune, F. Salahdine, Md. S. Islam, E. Ghribi, and N. Kaabouch, “A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication,” in 2020 International Conference on Information Networking (ICOIN), Jan. 2020, pp. 459–464.

[288] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, “A Machine Learning Security Framework for Iot Systems,” IEEE Access, vol. 8, pp. 114066–114077, 2020,

[289] Y.-W. Chen, J.-P. Sheu, Y.-C. Kuo, and N. Van Cuong, “Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning,” in 2020 European Conference on Networks and Communications (EuCNC), Jun. 2020, pp. 122–127.

[290] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, “Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning With One-Class SVM and K-Means Clustering,” IEEE Wirel. Commun. Lett., vol. 9, no. 2, pp. 139–142, Feb. 2020.

[291] F.Khalid, S. R. Hasan, S. Zia, O. Hasan, F. Awwad, and M. Shafique, “MacLeR: Machine Learning-Based Runtime Hardware Trojan Detection in Resource-Constrained IoT Edge Devices,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 39, no. 11, pp. 3748–3761, Nov. 2020.

[292] L. Peng, J. Zhang, M. Liu, and A. Hu, “Deep Learning Based RF Fingerprint Identification Using Differential Constellation Trace Figure,” IEEE Trans. Veh. Technol., vol. 69, no. 1, pp. 1091-1095, Jan 2020.

[293] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, “Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques,” Int. J.Environ. Res. Public. Health, vol. 17, no. 24, p. 9347, Dec. 2020.

[294] J. Roldán, J. Boubeta-Puig, J. Luis Martínez, and G. Ortiz, “Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks,” Expert Syst. Appl., vol. 149, p. 113251, Jul. 2020.

[295] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, “An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic,” IEEE Internet Things J., vol. 7, no. 9, pp. 8852–8859, Sep. 2020.

[296] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city,” Future Gener. Comput. Syst., vol. 107, pp. 433–442, Jun. 2020.

[297] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, and T. Huang, “A real-time and ubiquitous network attack detection based on deep belief network and support vector machine,” IEEECAA J. Autom. Sin., vol. 7, no. 3, pp. 790–799, May 2020.

[298] A. R. Gad, A. A. Nashat, and T. M. Barkat, “Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset,” IEEE Access, vol. 9, pp. 142206– 142217, 2021.

[299] Z. Lv, L. Qiao, J. Li, and H. Song, “Deep-Learning-Enabled Security Issues in the Internet of Things,” IEEE Internet Things J., vol. 8, no. 12, pp. 9531–9538, Jun. 2021.

[300] I. H. Sarker, “CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks,” Internet Things, vol. 14, p. 100393, Jun. 2021.

[301] S. Rachmadi, S. Mandala, and D. Oktaria, “Detection of DoS Attack using AdaBoost Algorithm on IoT System,” in 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia: IEEE, Oct. 2021, pp. 28–33.

[302] I. Ullah and Q. H. Mahmoud, “Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks,” IEEE Access, vol. 9, pp. 103906–103926, 2021.

[303] K. Yang, S. Kpotufe, and N. Feamster, “An Efficient One-Class SVM for Anomaly Detection in the Internet of Things.” arXiv, Apr. 22, 2021.

[304] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, “Stacked recurrent neural network for botnet detection in smart homes,” Comput. Electr. Eng., vol. 92, p. 107039, Jun. 2021.

[305] S. Pokhrel, R. Abbas, and B. Aryal, “IoT Security: Botnet detection in IoT using Machine learning.” arXiv, Apr. 05, 2021. Accessed: Mar. 03, 2024. [Online].

[306] B. Lahasan and H. Samma, “Optimized Deep Autoencoder Model for Internet of Things Intruder Detection,” IEEE Access, vol. 10, pp. 8434–8448, 2022.

[307] J. Liu, J. Bai, H. Li, and B. Sun, “Improved LSTM-Based Abnormal Stream Data Detection and Correction System for Internet of Things,” IEEE Trans. Ind. Inform., vol. 18, no. 2, pp. 1282–1290, Feb. 2022.

[308] O. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, “A machine learning based framework for IoT device identification and abnormal traffic detection,” Trans. Emerg. Telecommun. Technol., vol. 33, no. 3, p. e3743, 2022.

[309] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, “An improved anomaly detection model for IoT security using decision tree and gradient boosting,” J. Supercomput., vol. 79, no.3, pp. 3392-3411, Feb. 2023.

[310] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, “Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT),” IEEE Internet Things J., vol. 5, no. 3, pp. 1505–1515, Jun. 2018.

[311] L. Mainetti, L. Patrono, and A. Vilei, “Evolution of wireless sensor networks towards the Internet of Things: A survey”.

[312] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. Costa, and B. Walke, “The IEEE 802.11 universe,” IEEE Commun. Mag., vol. 48, no. 1, pp. 62–70, Jan. 2010.

[313] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment. Berkeley, CA: Apress, 2020.

[314] “Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions,” p. 3465, 2023.

[315] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” J. Electr. Comput. Eng., vol. 2017, pp. 1–25, 2017.

[316] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia: IEEE, Nov. 2015, pp. 1–6.

[317] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,” Future Gener. Comput. Syst., vol. 100, pp. 779–796, Nov. 2019.

[318] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada: IEEE, Jul. 2009, pp. 1–6.

[319] Y. Meidan et al., “N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018.

[320] “IoT-23 Dataset: A labeled dataset of Malware and Benign IoT Traffic.,” Stratosphere IPS. Accessed: Apr. 19, 2024. [Online].

[321] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning,” IEEE Access, vol. 10, pp. 40281–40306, 2022.

[322] S. García, M. Grill, J. Stiborek, and A. Zunino, “An empirical comparison of botnet detection methods,” Comput. Secur., vol. 45, pp. 100–123, Sep. 2014.

[323] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, “Characterization of Encrypted and VPN Traffic using Time-related Features” in Proceedings of the 2nd International Conference on Information Systems Security and Privacy, Rome, Italy: SCITEPRESS – Science and Technology Publications, 2016, pp. 407-414.

[324] A. Habibi Lashkari, G. Draper Gil, M. S. I. Mamun, and A. A. Ghorbani, “Characterization of Tor Traffic using Time based Features:,” in Proceedings of the 3rd International Conference

on Information Systems Security and Privacy, Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 253-262.

[325] A. Habibi Lashkari, G. Kaur, and A. Rahali, “DIDarknet: A Contemporary Approach to Detect and Characterize the Darknet Traffic using Deep Image Learning,” in Proceedings of the 2020 10th International Conference on Communication and Network Security, in ICCNS ’20. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 1-13.

[326] Z. Ahmad et al., “Anomaly Detection Using Deep Neural Network for IoT Architecture,” Appl. Sci., vol. 11, no. 15, Art. no. 15, Jan. 2021.

[327] R. Panigrahi and S. Borah, “A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems,” Int. J. Eng. Technol., vol. 7, pp. 479–482, Jan. 2018.