ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

ΨΗΦΙΑΚΑ ΚΥΚΛΩΜΑΤΑ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ ΣΥΝΔΕΔΕΜΕΝΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΔΗΜΗΤΡΙΟΣ Γ. ΜΥΡΙΔΑΚΗΣ

ΕΠΙΒΛΕΠΩΝ

ΑΝΑΠ. ΚΑΘΗΓΗΤΗΣ ΑΘΑΝΑΣΙΟΣ ΚΑΚΑΡΟΥΝΤΑΣ

ΛΑΜΙΑ, ΙΟΥΛΙΟΣ 2021

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE AND BIOMEDICAL INFORMATICS

DIGITAL CIRCUITS AND SYSTEMS TO ENHANCE SECURITY IN SMART DEVICES CONNECTED TO THE INTERNET

DOCTORAL THESIS

DIMITRIOS G. MYRIDAKIS

SUPERVISOR

ASSOCIATE PROFESSOR ATHANASIOS KAKAROUNTAS

LAMIA, JULY 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

ΨΗΦΙΑΚΑ ΚΥΚΛΩΜΑΤΑ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ ΣΥΝΔΕΔΕΜΕΝΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΔΗΜΗΤΡΙΟΣ Γ. ΜΥΡΙΔΑΚΗΣ

ΕΠΙΒΛΕΠΩΝ

ΑΝΑΠ. ΚΑΘΗΓΗΤΗΣ ΑΘΑΝΑΣΙΟΣ ΚΑΚΑΡΟΥΝΤΑΣ

ΛΑΜΙΑ, ΙΟΥΛΙΟΣ 2021

ΨΗΦΙΑΚΑ ΚΥΚΛΩΜΑΤΑ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ ΣΥΝΔΕΔΕΜΕΝΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΔΗΜΗΤΡΙΟΣ Γ. ΜΥΡΙΔΑΚΗΣ

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

Αναγνωστόπουλος Ιωάννης, Καθηγητής του Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας

Κακαρούντας Αθανάσιος, Αν. Καθηγητής Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας (Επιβλέπων)

Κουφοπαύλου Οδυσσέας, Καθηγητής του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών

Σταμούλης Γεώργιος, Καθηγητής του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Τασουλής Σωτήριος, Επ. Καθηγητής του Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας

Κίτσος Παρασκευάς, Αν. Καθηγητής του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Πελοποννήσου

Δασυγένης Μηνάς, Επ. Καθηγητής του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Δυτικής Μακεδονίας

ΛΑΜΙΑ, ΙΟΥΛΙΟΣ 2021

……..

Δημήτριος Γ. Μυριδάκης

Αφιερωμένη με πολύ αγάπη στην οικογένειά μου!

Ευχαριστίες

Μέσα από το παρόν κείμενο θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους αυτούς που με βοήθησαν ώστε να ολοκληρώσω, έστω και κάτω από δύσκολες περιστάσεις, την παρούσα διδακτορική διατριβή. Αρχικά θα ήθελα να εκφράσω τις ευχαριστίες στον επιβλέποντά μου, Αναπληρωτή Καθηγητή του τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική του Πανεπιστημίου Θεσσαλίας κ. Κακαρούντα Αθανάσιο, ο οποίος στάθηκε δίπλα μου όλο αυτό το διάστημα αρωγός, με την καθοδήγησή αλλά και την ενθάρρυνσή του, παίζοντας καθοριστικό ρόλο στην ολοκλήρωση της διδακτορικής μου διατριβής. Στάθηκα ιδιαίτερα τυχερός που γνώρισα έναν τέτοιο άνθρωπο, καθώς η συνεργασία μας σε όλα τα επίπεδα δε θα σταματήσει εδώ. Επίσης, θα ήθελα να ευχαριστήσω τους ακαδημαϊκούς του Πανεπιστημίου Θεσσαλίας, οι οποίοι με τις απαντήσεις τους, στα όποια ερωτήματα και απορίες ειδικού ενδιαφέροντος τους έθετα, μου προσέφεραν πολύτιμη βοήθεια. Επίσης τους ερευνητές από τα NOKIA Bell Labs με τους οποίους υπήρξε μία άριστη συνεργασία. Θα ήταν παράληψή μου να μην ευχαριστήσω για την αγαστή συνεργασία και όχι μόνο, την ερευνητική ομάδα του κ. Κακαρούντα Αθανασίου, της οποίας είμαι μέλος, καθώς θα ήθελα να αναφερθώ με ιδιαίτερη μνεία στους συνσυγγραφείς μου κ. Σπαθούλα Γεώργιο, κ. Παπαφωτίκα Στέφανο και κ. Μυριδάκη Παύλο. Κλείνοντας, θα ήθελα να εκφράσω τη βαθιά ευγνωμοσύνη μου στη μητέρα και τα αδέρφια μου που με ενθάρρυναν όλο αυτό το διάστημα, αλλά κυρίως στη γυναίκα και τις κόρες μου, οι οποίοι έδειξαν με την ανοχή τους μεγάλη συμπαράσταση αλλά συνάμα και ενθάρρυνση, καθώς τους στέρησα σύζυγο και πατέρα όλο αυτό το διάστημα.

Περίληψη

Στόχοι

Η συνεχής αύξηση του αριθμού των συσκευών Internet of Things (IoT) και η ένταξή τους σε δημόσιες και ιδιωτικές υποδομές έχει εισαγάγει νέες εφαρμογές στην αγορά και την καθημερινή μας ζωή. Ταυτόχρονα, αυτές οι συσκευές δημιουργούν μία πιθανή απειλή για την προσωπική και τη δημόσια ασφάλεια. Αυτό μπορεί εύκολα να γίνει κατανοητό είτε λόγω της ευαισθησίας των συλλεγόμενων δεδομένων, είτε λόγω της αξιοπιστίας της λειτουργίας των συσκευών. Λαμβάνοντας υπόψη ότι οι περισσότερες συσκευές IoT έχουν χαμηλό κόστος και χρησιμοποιούνται για διάφορες εργασίες, όπως παρακολούθηση ατόμων ή έλεγχος περιβαλλοντικών συνθηκών εσωτερικού χώρου, ο παράγοντας της ασφαλείας πρέπει να ενισχυθεί.

Η παρούσα διδακτορική διατριβή παρουσιάζει αποτελέσματα από τη συσχέτιση των φυσικών χαρακτηριστικών, όπως η παροχή του ρεύματος μίας έξυπνης συσκευής, με τα λειτουργικά χαρακτηριστικά της, προκειμένου να ανιχνευθεί μία κατασκευαστική ή λειτουργική ανωμαλία. Η ιδέα αυτή προέκυψε από το γεγονός ότι οι περισσότερες από τις διαθέσιμες έξυπνες συσκευές στην αγορά, που συνδέονται με το Διαδίκτυο, δημιουργώντας το λεγόμενο Διαδίκτυο των Πραγμάτων (ΔτΠ), είναι συσκευές ειδικής εφαρμογής με περιορισμένη λειτουργικότητα. Ζητήματα σχετικά με εφαρμογές διαδικτύου, που απαιτούν λύσεις, είναι η ασφάλεια, η διαθεσιμότητα και η αξιοπιστία. Η έρευνα αυτή εκμεταλλεύεται την απόκλιση (είτε αύξηση ή μείωση) της παροχής του ρεύματος. Αυτό μπορεί να θεωρηθεί ως παράπλευρη παρακολούθηση λειτουργίας της συσκευής, δεδομένου ότι η απόκλιση του ρεύματος σηματοδοτεί ότι ένας πόρος καταναλώνει περισσότερη ισχύ από την αναμενόμενη. Με αυτόν τον τρόπο επιτυγχάνεται η αξιοποίηση της τεχνικής επίθεσης πλαϊνών καναλιών, για την προστασία έξυπνων συσκευών χαμηλού κόστους. Στοχεύει στην επέκταση του συνόλου δεδομένων που παρέχονται σε Intrusion Detection Systems (IDS) προκειμένου να επιτευχθεί μεγαλύτερη ακρίβεια στην ανίχνευση ανωμαλιών. Έτσι, μαζί με τα τυπικά δεδομένα που παρέχονται σε ένα IDS, όπως η κυκλοφορία δικτύου, μεταβιβαζόμενα πακέτα, χρήση CPU κ.λπ., προτείνεται να συμπεριληφθούν πληροφορίες σχετικά με τη φυσική κατάσταση της συσκευής και τη συμπεριφορά της, όπως η κατανάλωση ισχύος, η παροχή του ρεύματος, η εκπεμπόμενη θερμότητα,

κ.λπ. Η ευαισθησία της τυπικής λειτουργίας μίας έξυπνης συσκευής όσον αφορά τη λειτουργία και τη λειτουργικότητα πιθανό να αποδειχθεί πολύτιμη, καθώς οποιαδήποτε απόκλιση μπορεί να προειδοποιήσει για μία κατασκευαστική ή λειτουργική ανωμαλία.

Μεθοδολογία

Για την επίτευξη των δηλωθέντων στόχων της παρούσας διδακτορικής διατριβής επιλέχθηκαν οι ακόλουθες μέθοδοι: επισκόπηση βιβλιογραφίας για την υπάρχουσα τεχνολογία, καθορισμός εφαρμογών και τεχνολογιών επικοινωνίας που χρησιμοποιούνται σε ένα σενάριο επιθέσεων IoT συσκευών, μελέτη τεχνολογίας μικροελεγκτών, σχεδιασμός και προσομοίωση, πειραματικές μετρήσεις χρόνου εκτέλεσης και ανίχνευσης επιθέσεων και τέλος ανάλυση των αποτελεσμάτων. Μία μεθοδολογία που συσχετίζει την παροχή του ρεύματος μίας έξυπνης συσκευής με τα λειτουργικά χαρακτηριστικά της, προκειμένου να ανιχνεύσει μία κατασκευαστική ή λειτουργική ανωμαλία σε συσκευές IoT.

Αποτελέσματα

Αποδεικνύεται ότι η παρατήρηση της τυπικής λειτουργίας μίας έξυπνης συσκευής μέσω λειτουργικών παραμέτρων (όπως η παροχή ρεύματος) μπορεί να προσφέρει πολύτιμους δείκτες ασφαλείας, καθώς οποιαδήποτε απόκλιση από τα κανονικά όρια μπορεί να αποτελεί ένδειξη παραβίασης ασφαλείας ή λειτουργικής ανωμαλίας. Η διδακτορική διατριβή προσφέρει τα αποτελέσματα από έξι (6) πειράματα που αποδεικνύουν αυτή την υπόθεση και συμβάλλουν σε μία ολιστική προσέγγιση ασφάλειας για την εποχή του ΔτΠ. Τα αποτελέσματα παρουσιάζουν 100% ανίχνευση επίθεσης σε πραγματικό χρόνο και είναι η πρώτη φορά που παρουσιάζεται μία λύση ασφαλείας χαμηλού κόστους κατάλληλη για κάθε τύπο συσκευής στόχου στη διεθνή βιβλιογραφία.

Συμπεράσματα

Η επέκταση των παραμέτρων που παρακολουθούνται για τα ζητήματα της ασφάλειας που αντιμετωπίζουν τα Intrusion Detection Systems (IDS) αναμένεται να ενσωματωθεί σύντομα σε μεγάλα συστήματα. Η παρούσα διατριβή παρουσιάζει τη βάση για αυτό το είδος επέκτασης των παραμέτρων που θα παρέχει πρόσθετες

μετρήσεις για την προστασία κρίσιμων υποδομών IoT, προσπαθώντας να αντιμετωπίσει τόσο την αξιοπιστία όσο και τα ζητήματα ασφάλειας με βάση τη βιοϊσοδυναμία των συσκευών IoT για τη διασφάλισή τους, εξετάζοντας την «υγεία» της ίδιας της συσκευής.

Λέξεις κλειδιά: παρακολούθηση ρεύματος, ανίχνευση ανωμαλιών, ασφάλεια, διαδίκτυο των πραγμάτων, ασφάλεια υλικού, έξυπνη συσκευή, φυσικά χαρακτηριστικά, συστήματα ανίχνευσης εισβολής.

Abstract

Objectives

The continuous increase in number of Internet of Things (IoT) devices and their integration into public and private infrastructure has introduced new applications to the market and our daily lives. At the same time, these devices pose a potential threat to personal and public safety. This can be easily understood either due to the sensitivity of the data collected or due to the reliability of the operation of the devices. Taking into consideration that most of the IoT devices are low cost and used for a variety of tasks, such as monitoring people or controlling indoor environmental conditions, the safety factor needs to be strengthened.

This doctoral thesis presents the results from the correlation of physical characteristics, such as the power supply of a smart device, with its functional characteristics, in order to detect a structural or functional anomaly. The idea came from the fact that most of the smart devices are available on the market, which are connected to IoT, are special application devices with limited functionality. Issues which are related to the web applications that require solutions are security, availability and reliability. This research takes advantage of the deviation (either increase or decrease) of the power supply. This can be considered as an ancillary monitoring of the operation of the device, since the current deviation signals that a resource consumes more power than expected. In this way, the utilization of the side channel attack technique is achieved, for the protection of smart low-cost devices. Its aim is to extend the data set provided in an IDS in order to achieve greater accuracy in anomaly detection. Thus, in addition to the standard data provided in IDS, such as network traffic, transferable packets, CPU usage, etc., it is recommended to include information about the physical condition and behavior of the device, such as power consumption, power supply, heat emitted, etc. The sensitivity of the standard operation of a smart device in terms of function and functionality may prove to be valuable, as any deviation can warn of a structural or functional abnormality.

Methodology

The following methods were selected to achieve the stated objectives of this doctoral thesis: literature review of existing technology, definition of applications and communication technologies used in an IoT device attack scenario, study of microcontroller technology, design and simulation, experiments and experiments attacks and finally analysis of the results. A methodology which is correlated the power supply of a smart device with its functional characteristics in order to detect a structural or functional anomaly in IoT devices.

Results

It turns out that observing the normal operation of a smart device through functional parameters (such as power supply) can provide valuable safety indicators, as any deviation from the normal limits can be a sign of a security breach or functional malfunction. The doctoral thesis offers the results of six (6) experiments that prove this hypothesis and contribute to a holistic security approach for the IoT era. The results show 100% real-time attack detection and are the first time a low-cost security solution suitable for any type of target device has been introduced in the international literature.

Conclusions

The extension of the monitored parameters for security issues addressed by an IDS is expected to be integrated into large systems soon. This doctoral thesis presents the basis for this kind of expansion of parameters that provides additional measurements for the protection of critical IoT infrastructure, trying to cope with both the reliability and security issues based on the bioequivalence of IoT devices to safeguard them by looking at the "Health" of the device itself.

Keywords: current monitoring, anomaly detection, security, internet of things, hardware security, smart device, physical characteristics, intrusion detection systems.

Δημοσιεύσεις

A Power Dissipation Monitoring Circuit for Intrusion Detection and Botnet Prevention on IoT Devices, Dimitrios Myridakis, Paul Myridakis, Athanasios Kakarountas, Computation 2021, 9(2), 19; DOI: 10.3390/computation9020019. (SJR Q2: 0.34)

Enhancing Security on IoT Devices via Machine Learning on Conditional Power Dissipation, Dimitrios Myridakis, Stefanos Papafotikas, Konstantinos Kalovrektis, Athanasios Kakarountas, Electronics 2020, *9*(11), 1799; DOI: 10.3390/electronics9111799. (I.F. 2.412)

Smart Devices Security Enhancement via Power Supply Monitoring, Myridakis, D.; Spathoulas, G.; Kakarountas, A.; Schinianakis, D., Future Internet 2020, *12*, 48. DOI: 10.3390/fi12030048. (SJR Q2: 0.39)

Κεφάλαια σε Βιβλία

Mimicking Biometrics on Smart devices and its application in IoT Security for Health systems, Dimitrios Myridakis, Georgios Spathoulas, Athanasios Kakarountas, Dimitris Schoinianakis and Joachim Lueken, Internet of Things and Information & Communication Technology for Healthcare Applications" in EAI/Springer Innovations in Communications and Computing Book series. DOI: 10.1007/978-3-030-42934-8.

Πρακτικά Συνεδρίων

Intrusion Detection and Botnet Prevention Circuit for IoT Devices, Dimitrios Myridakis, Paul Myridakis, Athanasios Kakarountas, SEEDA CECNSM 2020 (5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference) Corfu, Greece, September 2020. DOI: 10.1109/seeda-cecnsm49515.2020.9221789.

Monitoring Supply Current Thresholds for Smart Device's Security Enhancement, Dimitrios Myridakis, Georgios Spathoulas, Athanasios Kakarountas, Dimitris Schoinianakis and Joachim Lueken, (DCOSS) 1st International Workshop on Security and Reliability of IoT Systems (SecRIoT), Santorini, Jun 2019. DOI: 10.1109/DCOSS.2019.00058.

Anomaly detection in IoT devices via monitoring of supply current, Dimitrios Myridakis, Georgios Spathoulas, Athanasios Kakarountas, Dimitris Schoinianakis and Joachim Lueken, 8th International Conference on Consumer Electronics - Berlin -ICCE, Berlin, Sep 2018. DOI: 10.1109/ICCE-Berlin.2018.8576178.
"2018 ICCE BERLIN OUTSTANDING PAPERS AWARDS"

Supply Current Monitoring for Anomaly Detection on IoT Devices, Dimitrios Myridakis, Georgios Spathoulas and Athanasios Kakarountas (Short paper), 21st Pan-Hellenic Conference on Informatics PCI, Dep. of Computer Science and Engineering, Larisa Sep 2017. DOI: 10.1145/3139367.3139423.

Διακρίσεις

Υποτροφία & Χρηματοδότηση Έρευνας "Internet of Things Security (IoT Security)", NOKIA Bell Labs, κωδικός ΕΛΚΕ Πανεπιστημίου Θεσσαλίας: 5419.

Επισήμανση του Άρθρου «Smart Devices Security Enhancement via Power Supply Monitoring», Future Internet 2020, 12, 48, στην κύρια σελίδα του περιοδικού, εξώφυλλο.

2018 ICCE BERLIN OUTSTANDING PAPERS AWARDS, 2018 IEEE International Conference on Consumer Electronics-Berlin, Berlin.

Περιεχόμενα

Κατάλογος εικόνων

Κατάλογος Πινάκων

Ακρωνύμια

APTs	Advanced Persistent Threats
BP	Blood Pressure
CPU	Central Processing Unit
C&C	Command and Control
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
EoL	End-of-Life
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IDS	Intrusion Detection System
M2M	Machine to Machine
ML	Machine Learning

MTBF	Mean Time Between Failures
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
OEE	Overall Equipment Efficiency
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
PUFs	Physical Unclonable Functions
PCA	Principle Component Analysis
PWM	Pulse Width Modulation
RFID	Radio Frequency IDentification
RIP	Routing Information Protocol
ROI	Return-on-Investment
RUL	Remaining Useful Life
SSH	Secure Shell
SSL	Secure Sockets Layer

SEU	Single Event Upset
SCADA	Supervisory Control And Data Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TQM	Total Quality Management
UDP	User Datagram Protocol
WSN	Wireless Sensor Network
ΔτΠ	Διαδίκτυο των Πραγμάτων
ΗΚΓ	ΗλεκτροΚαρδιοΓραφήμα

1 ΕΙΣΑΓΩΓΗ

1.1 Ασφάλεια στις IoT συσκευές

Ο συνεχώς αυξανόμενος αριθμός έξυπνων συσκευών, που εισάγεται κάθε χρόνο στην αγορά των ηλεκτρονικών ειδών ευρείας κατανάλωσης, έχει προκαλέσει αρκετούς προβληματισμούς στους προγραμματιστές και στους κατασκευαστές. Το πιο σημαντικό μέλημα είναι η αύξηση των έξυπνων συσκευών που συνδέονται με το Internet of Thinks. Αυτή η συνεχώς αυξανόμενη αγορά του IoT, αν και γεμάτη ευκαιρίες για καινοτόμα προϊόντα, εισάγει καταναλωτικά προϊόντα, που αναπτύχθηκαν ως λύσεις βασισμένες σε Η/Υ με περιορισμένα χαρακτηριστικά. Επιπλέον, έχουν αυξήσει σημαντικά τις απαιτήσεις σε τηλεπικοινωνιακές υποδομές υψηλής ρυθμαπόδοσης (throughput), αυξάνοντας όμως παράλληλα τους κινδύνους που σχετίζονται με ηλεκτρονικές επιθέσεις. Ο κύριος λόγος είναι η δημιουργία έξυπνων συσκευών που περιλαμβάνουν μόνο τα στοιχειώδη χαρακτηριστικά για την επεξεργασία δεδομένων και τη δικτύωση, δίχως την ενσωμάτωση μηχανισμών ασφαλείας (π.χ. κρυπτογραφία, firewall κ.ο.κ.).

Αυτή όμως η δυνατότητα επικοινωνίας με τον καθένα και οτιδήποτε στον κόσμο, έχει αλλάξει ριζικά τις πτυχές της ιδιωτικότητας, της ασφάλειας και της ελευθερίας των συσκευών IoT, αυξάνοντας σημαντικά το πλήθος των δεδομένων που ανταλλάσσονται, τόσο ανάμεσα στα επιμέρους ιδιωτικά δίκτυα όσο και μέσω του διαδικτύου. Πολλά από τα δεδομένα που ανταλλάσσονται χαρακτηρίζονται ως ευαίσθητα δεδομένα, οπότε τίθεται το θέμα της ασφάλειας της πληροφορίας που μεταδίδεται μέσω του διαδικτύου. Καθώς όλο και περισσότερο η πληροφορία γίνεται διαθέσιμη σε ηλεκτρονική μορφή μέσω διαφόρων αισθητήρων και συσκευών του ΔτΠ, η έννοια της ύπαρξης ενός προηγμένου εχθρού, ο οποίος συνεχώς στοχοποιεί την εύκολη πληροφορία αυτή, με στόχο την απόκτηση δεδομένων, είναι αναπόφευκτη. Οι κακόβουλοι χρήστες του διαδικτύου (hackers) επιδιώκουν να υποκλέψουν τέτοιου είδους πληροφορίες (ευαίσθητα δεδομένα). Σε άλλες περιπτώσεις προσπαθούν απλώς να παρακωλύσουν την παροχή υπηρεσιών με σκοπό να βλάψουν τον πάροχο της υπηρεσίας για λογαριασμό ενός τρίτου ή με σκοπό να ζητήσουν λύτρα από το θύμα. Παρατηρείται λοιπόν μία διαρκής αύξηση των

επιθέσεων σε αυτές τις «έξυπνες συσκευές» και ιδιαίτερα αυτές που είναι στοχευμένες και προηγμένες (Advanced Persistent Threats), οι οποίες θεωρούνται ως η σημαντικότερη απειλή για την ασφάλεια των πληροφοριών και των συστημάτων που τις υποστηρίζουν. Επιπρόσθετα επιτυχείς επιθέσεις που στοχεύουν σε IoT συσκευές, προκαλούν προβλήματα ασφάλειας και θέτουν νέες προκλήσεις. Αυτές οι επιτυχημένες επιθέσεις προερχόμενες από τα botnets που κατοικούν σε εξειδικευμένες συσκευές IoT αυξάνονται σημαντικά σε αριθμό και η βαρύτητα των ζημιών που προκαλούν είναι παρόμοια με αυτή ενός πολέμου. Αυτό εγείρει και άλλα σημαντικά ζητήματα ασφαλείας, καθώς και νέες προκλήσεις. Τα θέματα ασφάλειας αφορούν την προσωπική ασφάλεια των πολιτών, την ασφάλειά του εξοπλισμού τους, καθώς και την προστασία άλλων ψηφιακών υποδομών, από μία πιθανή επίθεση botnet. Από την άλλη πλευρά, υπάρχουν προκλήσεις στην αντιμετώπιση επιτυχημένων επιθέσεων παραβιασμένων συσκευών IoT, που προέρχονται από botnets. Ο αριθμός των επιθέσεων αυξάνεται εκθετικά κάθε χρόνο, σε αναλογία με τα τρωτά σημεία που εκμεταλλεύονται και τις περισσότερες φορές με απρόβλεπτα αποτελέσματα. Τα χαρακτηριστικά των επιθέσεων ποικίλλουν σημαντικά από επίθεση σε επίθεση και από καιρό σε καιρό. Οι προειδοποιήσεις για τη σοβαρότητα των επιθέσεων δείχνουν ότι υπάρχει ανάγκη για λύσεις που να αντιμετωπίζουν τις επιθέσεις από τη γέννησή τους.

Επιπλέον, ακολουθώντας πρωτόκολλα παρόμοια με την εξάπλωση πανδημίας ενός βιολογικού ιού, υπάρχει η ανάγκη καραντίνας μολυσμένων συσκευών IoT, απαγορεύοντας έτσι την εξάπλωση του ιού και επομένως τον σχηματισμό του botnet. Αν και στη σύγχρονη αγορά υπάρχει ένας σημαντικός αριθμός τεχνολογικών λύσεων για την ασφάλεια των συστημάτων, η συνεχώς αυξανόμενη ευφυΐα των επιτιθέμενων και η ταυτόχρονη αδυναμία των αμυνόμενων δημιουργεί μία κατάσταση ανασφάλειας και περιορισμένης αποτελεσματικότητας στον εντοπισμό των επιθέσεων. Ωστόσο, αυτό είναι δύσκολο, καθώς δεν υπάρχει προηγούμενη γνώση ενός νέου ιού ή τα τρωτά σημεία μίας έξυπνης συσκευής. Τέλος, δεδομένου ότι υπάρχει φυσική πρόσβαση σε έξυπνες συσκευές, υπάρχει ακόμη και η απειλή της αλλαγής λογισμικού, αλλάζοντας π.χ. την κάρτα μνήμης της συσκευής. Συνεπώς οι τεχνικοί της ασφάλειας υπολογιστικών συστημάτων αλλά και οι ερευνητές, αντιμετωπίζουν όλο και πιο συχνά ένα ευρύ φάσμα από ασυνήθιστα κακόβουλα γεγονότα. Καλούνται να ανιχνεύσουν αυτές τις ανωμαλίες όταν συμβαίνουν και στην συνέχεια να τις

κατηγοριοποιήσουν ώστε να διαλέξουν την κατάλληλη μέθοδο αντιμετώπισης. Η πρωταρχική πρόκληση στην αυτοματοποιημένη ανίχνευση και στην κατηγοριοποίηση των ανωμαλιών είναι ότι οι ανωμαλίες αυτές αποτελούν ένα μεγάλο εύρος γεγονότων, από κατάχρηση ενός δικτύου (DoS, DDoS attacks, network scans) σε ασυνήθιστη συμπεριφορά των χρηστών του δικτύου ακόμη και σε νέα άγνωστα γεγονότα. Οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) αποτελούν έναν συνήθη τύπο επίθεσης εξαιτίας της διαθεσιμότητας δωρεάν εργαλείων και φθηνών διαδικτυακών υπηρεσιών που επιτρέπουν σε οποιονδήποτε με πρόσβαση στο Internet να ξεκινήσει μία επίθεση. Αυτό έχει οδηγήσει σε έντονη αύξηση, της συχνότητας, του μεγέθους και της πολυπλοκότητας των επιθέσεων, τα τελευταία χρόνια. Χαρακτηριστική είναι η δημοσίευση της εταιρίας Arbor Networks, η οποία δείχνει μία συνεχή κλιμάκωση τόσο στο μέγεθος όσο και στη συχνότητα των επιθέσεων [1].

1.2 Σκοπός και στόχος

Το θέμα της παρούσας διατριβής είναι στην αιχμή του δόρατος της έρευνας που πραγματοποιείται στο πεδίο της τεχνολογίας που αφορά το IoT και συγκεκριμένα στο επίπεδο του υλικού και της ασφάλειας που πρέπει να προσφέρει στη συσκευή και στο δίκτυο.

Ως στόχοι της διδακτορικής διατριβής θέτονται: 1) η μελέτη της συμπεριφοράς ενός κυκλώματος όταν υφίσταται επίθεση, 2) η ανάπτυξη ενός απλού κυκλώματος για τη συσχέτιση της συμπεριφοράς με το ρεύμα τροφοδοσίας, 3) η δημιουργία μιας αρχιτεκτονικής [2] για την επίτευξη προσαρμοσμένης ανίχνευσης μέσω της παρακολούθησης πλήθους φυσικών παραμέτρων, 4) η ανάπτυξη μεθοδολογίας για το σχεδιασμό μιας αυτόνομης έξυπνης συσκευής [3] χαμηλού κόστους για τον εντοπισμό μιας επίθεσης μέσω της κατανάλωσης ενέργειας αξιοποιώντας αλγόριθμο μηχανικής μάθησης, και 5) η ανάπτυξη και δοκιμή μιας πρότυπης συσκευής για την ασφαλή δικτύωση των έξυπνων IoT συσκευών [4].

Η παρούσα διδακτορική διατριβή παρουσιάζει μία νέα ιδέα για τον εντοπισμό μίας ανωμαλίας που δημιουργείται από επιθέσεις ιών σε συσκευή IoT ή από βλάβες στην ηλεκτρονική συσκευή. Αξιοποιεί μαθήματα που αντλήθηκαν από την τεχνική

επίθεσης πλευρικού καναλιού και συγκεκριμένα την ανάλυση ισχύος κατά την εκτέλεση κώδικα [5]. Αυτό σημαίνει ότι η ανάλυση ισχύος μπορεί να χρησιμεύσει ως μοναδική υπογραφή του εκτελούμενου κώδικα. Δεδομένου ότι μία συσκευή IoT εκτελεί συνήθως μόνο μία και σαφώς καθορισμένη εργασία, η συμπεριφορά (λειτουργία) του εκτελούμενου κώδικα μπορεί εύκολα να αναλυθεί [6]. Επιπλέον, δεδομένου ότι αυτή η συμπεριφορά ορίζεται από τα στοιχεία επεξεργασίας της συσκευής που χρησιμοποιούνται από τον εκτελεσμένο κώδικα, τότε η συνολική κατανάλωση ισχύος κατά τη διάρκεια της κανονικής λειτουργίας, ποικίλλει σε ένα σαφές εύρος. Έτσι, κατά τη διάρκεια της κανονικής λειτουργίας, περιμένουμε ότι η κατανάλωση ισχύος της συσκευής θα βρεθεί σε αυτό το ασφαλές εύρος. Λαμβάνοντας υπόψη ότι οι συσκευές IoT μπορεί να έχουν πολλαπλούς τρόπους λειτουργίας (π.χ. κανονική λειτουργία, ενημέρωση, κατάσταση αναστολής κ.λπ.), είναι δυνατόν να επεκταθεί το ασφαλές εύρος για να περιλαμβάνει πολλές περιοχές, σχηματίζοντας συστάδες λειτουργίας. Έτσι, οποιαδήποτε απόκλιση ισχύος προκαλείται είτε με αυξημένη κίνηση στο δίκτυο είτε με εσωτερική ανωμαλία (Trojan hardware ή software virus) αναμένεται να εντοπιστεί.

1.3 Ερευνητικά ερωτήματα

Εκτός από τα ζητήματα ασφαλείας που αναφέρθηκαν προηγουμένως, υπάρχει η ανάγκη παρακολούθησης της φυσιολογικής λειτουργίας του εξοπλισμού μας. Αυτό περιλαμβάνει το χρόνο λειτουργίας, την κατανάλωση ισχύος και πολλά άλλα. Είναι επιθυμητό να εντοπιστεί οποιαδήποτε ανωμαλία εγκαίρως, προκειμένου να αποφευχθεί κάποια μόνιμη καταστροφή του εξοπλισμού μας. Μπορεί να δημιουργηθούν ζητήματα όπως η ηλεκτρονική γήρανση, η φυσική υποβάθμιση των υλικών κ.λπ., παρουσιάζοντας σημαντική διαφορά στα χαρακτηριστικά της λειτουργίας χωρίς να είναι εμφανής σε εύθετο χρόνο.

1.4 Πεδίο διατριβής

Στο πλαίσιο της διδακτορικής διατριβής, διεξήχθη μελέτη λειτουργίας των συσκευών IoT, καθώς και των νέων ειδών επιθέσεων σε αυτές. Αναλύθηκαν οι απαιτήσεις που

έπρεπε να ικανοποιούνται, προκειμένου να επιτυγχάνεται η ασφάλεια (security) όπως αυτή επιβάλλεται από τις σύγχρονες απαιτήσεις των συσκευών IoT. Η αντιμετώπιση των νέων ειδών επιθέσεων στις IoT συσκευές, αποτέλεσε ένα ακόμη σημαντικό μέρος του πεδίου της διατριβής. Ως κύριες εφαρμογές μελετήθηκαν εκείνες που παρουσίαζαν συνάφεια με τα επιστημονικά πεδία που θεραπεύει το Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, όπως η Βιοϊατρική και οι Ιατρικές εφαρμογές, αλλά και ευρύτερα των τηλεπικοινωνιών.

Η σχεδίαση κυκλωμάτων και συστημάτων (υλικού/λογισμικού) βάσει νέων τεχνικών/τεχνολογιών, η βιομιμητική και το White Hacking, αποτέλεσαν βασικό μέρος της διατριβής. Επιπλέον μελετήθηκαν οι περιπτώσεις ενσωμάτωσης κακόβουλου υλικού (Trojan hardware) είτε ως περιπτώσεις αλλοίωσης του επιπέδου ασφάλειας (security και safety), είτε ως μέθοδοι ανίχνευσης ύποπτης συμπεριφοράς. Τέλος, αξιοποιήθηκαν τεχνικές που βασίζονται σε φυσικά χαρακτηριστικά των συστημάτων, όπως η κατανάλωση ενέργειας, καθώς και αλγόριθμοι Μηχανικής Μάθησης (ML) σε edge computing, παρουσιάζοντας ένα ενοποιημένο μοντέλο ανώμαλης συμπεριφοράς. Οι προαναφερόμενες τεχνικές, αποτελούν την αιχμή της έρευνας και έχουν ευρεία αποδοχή σε σύγχρονες εφαρμογές.

1.5 Αναμενόμενο αποτέλεσμα

Με την ολοκλήρωση της διδακτορικής διατριβής, έχουν αναπτυχθεί συστήματα κατάλληλα για την ενίσχυση της ασφάλειας σε IoT συσκευές, τα οποία ενσωματώνονται σε έξυπνες συσκευές αυξάνοντας την πληροφορία που παρέχεται στους IDS, ενώ είναι δυνατή η ανίχνευση ύποπτης συμπεριφοράς με αυτόνομο τρόπο. Τα πλεονεκτήματα των τεχνικών που χρησιμοποιούνται σε αυτή τη διατριβή, σε συνδυασμό με την εκμετάλλευση των φυσικών χαρακτηριστικών των συσκευών IoT, εισάγουν μία νέα μέθοδο για την ανίχνευση εισβολής σε μία συσκευή IoT. Η καινοτομία βρίσκεται στο γεγονός ότι ένα εξωτερικό κύκλωμα, είναι ικανό να ανιχνεύει απόπειρες εισβολής χωρίς προηγούμενη γνώση της συσκευής IoT υπό παρακολούθηση ή της λειτουργικότητάς της, ενώ δεν απαιτείται η ενσωμάτωση σε κάθε IoT συσκευή που ελέγχει. Επιπλέον, είναι μία χαμηλού κόστους, μικρού μεγέθους και υπολογιστικά δίκαιη λύση για την ενίσχυση της ασφάλειας σε συσκευές

IoT που βρίσκονται στα νοικοκυριά, οι οποίες είναι ευάλωτες σε επιθέσεις λόγω της έλλειψης επαγγελματικού συστήματος εντοπισμού εισβολής (IDS) σε ένα σπίτι ή ενσωματωμένων μηχανισμών ασφαλείας στην ίδια τη συσκευή.

Η συμβολή αυτής της διατριβής συνοψίζεται στα ακόλουθα:

- Πρότυπη υλοποίηση χαμηλού κόστους, μικρού μεγέθους ενσωματωμένου συστήματος, για την παρακολούθηση εξωτερικά, άγνωστων συσκευών IoT, με δυνατότητα μάθησης στον τομέα της λειτουργίας.
- Βελτίωση της ασφάλειας για συσκευές IoT έναντι DDoS και παρόμοιων επιθέσεων, χωρίς την ανάγκη IDS που βασίζεται σε cloud.
- Μίμηση των βιομετρικών χαρακτηριστικών που επιτρέπουν την επέκταση των δεδομένων που συλλέγονται από εξωτερικά IDS (όταν είναι συνδεδεμένα), παρόμοια με εκείνη της κατάστασης παρακολούθησης που εφαρμόζεται στη βιομηχανία.
- Δε βασίζεται σε κανόνες δικτύου ή/και μοτίβα ιών, προσφέροντας μία πιο ισχυρή ασφάλεια για επιθέσεις άγνωστης φύσης.
- Η ενοποίηση των παραπάνω σε μία αρχιτεκτονική εισάγει για πρώτη φορά στον τομέα των ενσωματωμένων συστημάτων και κατ' επέκταση στην επιστημονική βιβλιογραφία, μία νέα γενιά αυτοελεγχόμενων συστημάτων της ίδιας τους της «υγείας».

1.6 Περίγραμμα διατριβής

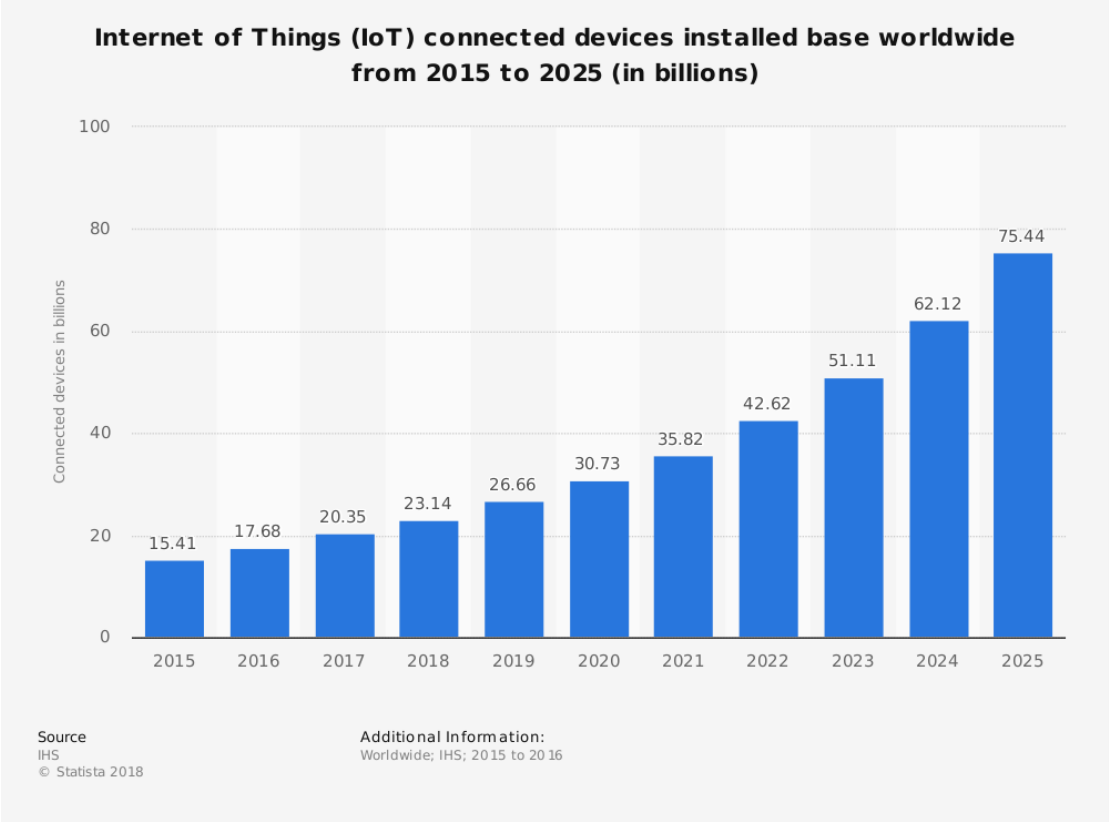
Μετά την εισαγωγή του πρώτου κεφαλαίου που αφορά στην ασφάλεια των IoT συσκευών, το σκοπό και το στόχο της διατριβής, τα ερευνητικά ερωτήματα στο πεδίο της, αλλά και τα αποτελέσματα αυτής, στο δεύτερο κεφάλαιο αναλύονται το Διαδίκτυο των Πραγμάτων και οι εφαρμογές του σε διάφορους τομείς. Δίνεται ιδιαίτερη έμφαση στην ανάλυση της ασφάλειάς του και παρατίθενται ορισμένα παραδείγματα επιθέσεων. Στο τρίτο κεφάλαιο γίνεται μία επισκόπηση της έρευνας επάνω στην ασφάλεια των IoT συσκευών. Το τέταρτο κεφάλαιο επικεντρώνεται στην ασφάλεια μέσω παρακολούθησης φυσικών παραμέτρων «βιομιμητισμός», ενώ στο πέμπτο κεφάλαιο παρουσιάζονται η μεθοδολογία και οι τεχνολογίες που

αξιοποιήθηκαν στην παρούσα διατριβή, καθώς αναλύονται εκτενώς τα πειράματα που διεξήχθησαν για την έρευνα με τα αποτελέσματά τους. Η διατριβή κλείνει με το έκτο κεφάλαιο το οποίο περιλαμβάνει τα συμπεράσματα που προέκυψαν από την παραπάνω έρευνα, ενώ παράλληλα αναφέρει και μελλοντική εργασία.

2 ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΚΑΙ ΟΙ ΕΦΑΡΜΟΓΕΣ ΤΟΥ

2.1 Internet of Things (IoT)

Το Internet of Things (IoT) είναι ένα νέο παράδειγμα που κερδίζει γρήγορα έδαφος στο σενάριο των σύγχρονων ασύρματων τηλεπικοινωνιών. Πρωτοεμφανίστηκε το 1999 αλλά τα τελευταία χρόνια γνωρίζει ραγδαία ανάπτυξη. Αυτό συνεπάγεται με έναν τεράστιο αριθμό ετερογενών συσκευών, ο οποίος αναμένεται να ξεπεράσει τα 75 δισεκατομμύρια έως το 2025 (Εικόνα 1). Αυτές οι συσκευές μπορεί να είναι οικιακές συσκευές, κάμερες παρακολούθησης, οχήματα, αισθητήρες κ.ά., που λειτουργούν ως μέρος του οικιακού αυτοματισμού, της έξυπνης πόλης, του έξυπνου δικτύου, της έξυπνης γεωργίας, του έξυπνου συστήματος μεταφοράς, της έξυπνης υγείας κ.λπ. Τρία βασικά στοιχεία: ασύρματα δίκτυα αισθητήρων (WSN), επικοινωνία μεταξύ μηχανών (M2M), αναγνώριση RF (RFID) και εποπτικός έλεγχος με απόκτηση δεδομένων (SCADA), θεωρούνται μέρος του Διαδικτύου των Πραγμάτων [7, 8]. Θα είναι σε θέση να ενσωματώνει απρόσκοπτα μεγάλο αριθμό αυτών των διαφορετικών συσκευών, τεχνολογιών επιπέδου συνδέσμων και υπηρεσιών που ενδέχεται να εμπλέκονται σε ένα τέτοιο σύστημα; Τώρα το IoT υπερβαίνει την επικοινωνία M2M και υπόσχεται μία τεχνολογική επανάσταση, αλλά για να λειτουργήσει καλά, όλες οι συσκευές πρέπει να μιλούν την ίδια γλώσσα. Είναι ένα μεγάλο έργο που αντιμετωπίζει όμως πολλά ζητήματα ασφάλειας.



Εικόνα 1: Συνδεδεμένες συσκευές IoT [Πηγή: www.statista.com]

2.2 Γιατί είναι σημαντικό το Internet of Things;

Μπορεί να εκπλαγεί κανείς αν μάθει πόσα πράγματα είναι συνδεδεμένα με το Διαδίκτυο και πόσα οικονομικά οφέλη που μπορεί να αποκομίσει από την ανάλυση των data streams. Ακολουθούν μερικά παραδείγματα του Internet of Things σε διάφορους κλάδους.

2.2.1 Βιομηχανικές και ιδιωτικές εφαρμογές

Αρχίζοντας από τις έξυπνες λύσεις μεταφοράς, όπου εκεί συναντάμε εφαρμογές οι οποίες επιταχύνουν την ροή της κυκλοφορίας, μειώνουν την κατανάλωση καυσίμων, προτεραιοποιούν τα προγράμματα επισκευής οχημάτων και το σημαντικότερο σώζουν ζωές. Συνεχίζοντας έπειτα στα έξυπνα ηλεκτρικά δίκτυα (Smart Electric Grids), βλέπουμε εφαρμογές οι οποίες συνδέουν αποτελεσματικότερα τις

ανανεώσιμες πηγές ενέργειας, βελτιώνοντας την αξιοπιστία του συστήματος και φυσικά οι χρεώσεις των καταναλωτών γίνονται με βάσει τις μικρότερες προσαυξήσεις. Περνώντας στις μηχανές αισθητήρων παρακολούθησης, βλέπουμε να διενεργούν διαγνώσεις και να προβλέπουν τα θέματα συντήρησης που εκκρεμούν, βραχυπρόθεσμα stock-out αποθεμάτων, θέτοντας προτεραιοποιήσεις στα προγράμματα του υπεύθυνου προσωπικού για τις επισκευές ώστε να καλύψουν αποτελεσματικότερα τις ανάγκες επισκευής εξοπλισμού αλλά και περιφερειακές ανάγκες. Τα Data-driven συστήματα είναι χτισμένα σε υποδομές των «έξυπνων πόλεων» καθιστώντας ευκολότερο για τους δήμους να «τρέχουν» τις διαδικασίες διαχείρισης αποθεμάτων, την επιβολή του νόμου καθώς και άλλα προγράμματα, πιο αποτελεσματικά.

Αλλά αναλογιζόμενοι και σε προσωπικό επίπεδο, θα δούμε τη χρήση του IoT σε συνδεδεμένες συσκευές οι οποίες χαράζουν τη δική τους πορεία τόσο στον κόσμο των επιχειρήσεων όσο και στη μαζική αγορά. Σκεφτείτε, σας τελειώνει το γάλα. Καθώς γυρνάτε από τη δουλειά στο σπίτι, λαμβάνετε αυτόματα μία ειδοποίηση από το ψυγείο σας που σας υπενθυμίζει να σταματήσετε στο κατάστημα για γάλα. Επίσης το σύστημα ασφαλείας του σπιτιού σας, που ήδη σας επιτρέπει να ελέγχετε από απόσταση τις κλειδαριές και τους θερμοστάτες σας ή μπορεί να ρυθμίσετε το κλιματιστικό ώστε να «δροσίσει» το σπίτι σας και να ανοίξει τα παράθυρα, με βάση τις προτιμήσεις σας.

2.2.2 Εφαρμογές Υγείας

Ένας άλλος πολύ σημαντικός κλάδος όπου βρίσκει εφαρμογή το IoT, είναι αυτός της Υγείας. Εφαρμογές της υγείας που χρησιμοποιούν smartphones, όπου ο πολλαπλασιασμός τους στην καθημερινότητα, μας έχει δώσει πρόσβαση στην ανάπτυξη των ελεγχόμενων αισθητήρων από αυτά, επισημαίνοντας το ρόλο τους ως οδηγού για το IoT. Διάφορα προϊόντα υλικού και λογισμικού έχουν σχεδιαστεί για να κάνουν τα smartphones μία ευέλικτη συσκευή υγειονομικής περίθαλψης. Μία εκτεταμένη ανασκόπηση των εφαρμογών υγειονομικής περίθαλψης για τα smartphones παρέχεται στην [9], συμπεριλαμβανομένης μίας συζήτησης σχετικά με τις εφαρμογές για τους ασθενείς και τις γενικές εφαρμογές υγειονομικής περίθαλψης,

καθώς και για την ιατρική εκπαίδευση, την κατάρτιση, τις εφαρμογές αναζήτησης πληροφοριών και άλλες (συλλογικά αναφερόμενες ως βοηθητικές εφαρμογές). Πέραν των παραπάνω, είναι πολλές οι πρόσφατες εφαρμογές smartphone που εξυπηρετούν παρόμοιους σκοπούς [10-13]. Επιπλέον υπάρχουν και οι επικείμενες λύσεις υγειονομικής περίθαλψης. Παρά το γεγονός ότι είναι διαθέσιμη μία πληθώρα φορητών ιατρικών συσκευών, δεν είναι ξεκαθαρισμένη η ένταξή τους στο Διαδίκτυο. Προβλέπεται ότι είναι μόνο θέμα χρόνου αυτές οι ιατρικές συσκευές να εξοπλιστούν με τη λειτουργικότητα του IoT. Οι εφαρμογές, οι συσκευές και άλλες υπηρεσίες υγειονομικής περίθαλψης αυξάνονται σε αριθμό καθώς αυξάνεται η ζήτηση για υπηρεσίες IoT σε όλο τον κόσμο. Ορισμένες περιοχές υγειονομικής περίθαλψης για τις οποίες είναι επικείμενη η ενσωμάτωση με IoT, περιλαμβάνουν λοιμώξεις του δέρματος, ανακοπή, ανίχνευση αιμοσφαιρίνης, θεραπεία καρκίνου, ανώμαλη ανάπτυξη κυττάρων, οφθαλμικές διαταραχές και απομακρυσμένο έλεγχο [14-16]. Οι περισσότερες συσκευές σήμερα, είναι φορητές διαγνωστικές συσκευές με συμβατική συνδεσιμότητα. Επίσης πολλοί ερευνητές έχουν εργαστεί για την ανάπτυξη έξυπνων αναπηρικών αμαξιδίων, πλήρως αυτοματοποιημένα για άτομα με ειδικές ανάγκες. Ένα αξιοσημείωτο παράδειγμα ανάπτυξης αναπηρικών αμαξιδίων είναι η έξυπνη αναπηρική πολυθρόνα που σχεδιάστηκε από το τμήμα IoT της Intel [17]. Αυτή η εξέλιξη δείχνει ότι τα τυποποιημένα «πράγματα» μπορούν να εξελίσσονται σε έξυπνες μηχανές με βαθμό αυτοματοποίησης. Αυτή η συσκευή μπορεί να παρακολουθεί ζωτικές λειτουργίες του ατόμου που κάθεται στην καρέκλα και να συλλέγει δεδομένα περιβάλλοντος του χρήστη, επιτρέποντας την αξιολόγηση της προσβασιμότητας μίας τοποθεσίας. Στη διαχείριση φαρμάκων υπάρχει το πρόβλημα μη συμμόρφωσης στον τομέα της φαρμακευτικής αγωγής, που αποτελεί σοβαρή απειλή για τη δημόσια υγεία και μπορεί να προκαλέσει τεράστιες οικονομικές απώλειες παγκοσμίως. Για να αντιμετωπιστεί αυτό το ζήτημα, το IoT υπόσχεται μερικές λύσεις. Για παράδειγμα, μία έξυπνη μέθοδος συσκευασίας για τα κουτιά φαρμάκων και τη διαχείριση φαρμάκων με βάση το Διαδίκτυο προτείνεται στο [18]. Δεδομένου ότι η ιατρική και η φυσική αποκατάσταση μπορούν να ενισχύσουν και να αποκαταστήσουν τη λειτουργική ικανότητα και την ποιότητα ζωής των ατόμων με κάποια σωματική βλάβη ή αναπηρία, αντιπροσωπεύουν έναν ζωτικό κλάδο της ιατρικής. Το IoT έχει τη δυνατότητα να ενισχύσει προβλήματα αποκατάστασης που συνδέονται με τη γήρανση του πληθυσμού και την έλλειψη εμπειρογνωμόνων στον

τομέα της υγείας. Τυπικά παραδείγματα συστημάτων αποκατάστασης περιλαμβάνουν μία οντολογική βάση, αυτοματοποιημένη μέθοδο σχεδιασμού για έξυπνα συστήματα αποκατάστασης βασισμένα στο IoT, όπως προτείνεται στο έγγραφο [19]. Τα συστήματα αποκατάστασης που βασίζονται στο IoT, όπως ένα ολοκληρωμένο σύστημα εφαρμογής για τις φυλακές [20], αποκατάσταση ημικρανίας [21], το ιατρικό σύστημα αποκατάστασης μίας έξυπνης πόλης [22] και ένα σύστημα εκμάθησης γλωσσών για τον παιδικό αυτισμό [23] υπογραμμίζουν τις ατελείωτες δυνατότητες σε αυτόν τον τομέα.

Η παλμική οξυμετρία είναι κατάλληλη για τη μη επεμβατική, συνεχόμενη παρακολούθηση κορεσμού του οξυγόνου του αίματος. Η ενσωμάτωση τεχνολογίας του IoT με παλμική οξυμετρία είναι χρήσιμη για τις εφαρμογές υγειονομικής περίθαλψης. Μία έρευνα σχετικά με τις υπηρεσίες υγειονομικής περίθαλψης που βασίζονται στο CoAP αναλύει το δυναμικό της παλμικής οξυμετρίας με βάση το IoT [24]. Αυτή η συσκευή μπορεί να χρησιμοποιηθεί για να παρακολουθεί συνεχώς την υγεία του ασθενούς μέσω ενός δικτύου IoT. Ένα σύστημα οξυμέτρου για εφαρμογές τηλεϊατρικής περιγράφεται στο [25]. Μία άλλη σημαντική εφαρμογή είναι αυτή της παρακολούθησης της πίεσης του αίματος. Η εργασία στο [26] εξετάζει τον τρόπο λειτουργίας μίας συσκευής BP Bringing με ένα κινητό της Apple, ενώ μία υπολογιστική συσκευή για τη συλλογή και μετάδοση δεδομένων της BP προτείνεται στο [27]. Ο συνδυασμός ενός κινητού τηλεφώνου KIT και παρακολούθησης της αρτηριακής πίεσης με δυνατότητα NFC KIT (BP) δοκιμάζεται στην [28], ως μέρος μίας παρακολούθησης BP που βασίζεται σε IoT. Η παρακολούθηση του ηλεκτροκαρδιογραφήματος (ΗΚΓ), είναι ακόμα μία από τις εφαρμογές που εκμεταλλεύεται το IoT και έχει τη δυνατότητα να δώσει πληροφορίες και μπορούν να χρησιμοποιηθούν στο μέγιστο βαθμό [29]. Αρκετές μελέτες έχουν συζητήσει ρητά την παρακολούθηση ΗΚΓ βασισμένη στο IoT [30-33]. Η [34] εισάγει ένα καινοτόμο σύστημα παρακολούθησης ΗΚΓ που βασίζεται σε IoT. Τα δεδομένα ΗΚΓ συλλέγονται χρησιμοποιώντας ένα φορητό κόμβο παρακολούθησης και μεταδίδονται απευθείας στο cloud του IoT χρησιμοποιώντας Wi-Fi. Τόσο τα πρωτόκολλα HTTP όσο και το MQTT χρησιμοποιούνται στο cloud του IoT για να παρέχουν έγκαιρα οπτικά τα δεδομένα ΗΚΓ στους χρήστες και να ανιχνεύουν μη φυσιολογικά δεδομένα που θα μπορούσαν να υποδεικνύουν καρδιακή δυσλειτουργία σε πραγματικό χρόνο. Τέλος η ανίχνευση στάθμης της γλυκόζης είναι μία από τις καταλυτικές εφαρμογές

στα συστήματα IoT. Ο σακχαρώδης διαβήτης είναι μία μεταβολική ασθένεια που χαρακτηρίζεται από αύξηση του σακχάρου στο αίμα (υπεργλυκαιμία) και τη διαταραχή της γλυκόζης στο μεταβολισμό, είτε ως αποτέλεσμα μειωμένης έκκρισης ινσουλίνης ή λόγω της μειωμένης ευαισθησίας των κυττάρων του σώματος στην ινσουλίνη. Η [35] μελετάει τη σκοπιμότητα της επεμβατικής και συνεχούς παρακολούθησης της γλυκόζης (CGM) σε σύστημα που βασίζεται στην προσέγγιση του IoT. Το μοντέλο χρησιμότητας στο [36] αντιμετωπίζει δυναμικά τα οφέλη από τη χρήση του m-IoT σε μη επεμβατική ανίχνευση της στάθμης της γλυκόζης, σε μία αρχιτεκτονική για τη διαχείριση του διαβήτη. Οι υπηρεσίες υγειονομικής περίθαλψης με βάση το IoT αναμένεται να μειώσουν το κόστος, να αυξήσουν την ποιότητα της ζωής, καθώς αναμένεται να εμπλουτίσουν την εμπειρία του χρήστη. Από την πλευρά των παρόχων υγειονομικής περίθαλψης, το IoT έχει τη δυνατότητα να προσδιορίσει σωστά τους βέλτιστους χρόνους για την ανανέωση προμηθειών για διάφορες συσκευές για την ομαλή και συνεχή λειτουργία τους. Επιπλέον, το IoT προβλέπει τον αποτελεσματικό προγραμματισμό των περιορισμένων πόρων εξασφαλίζοντας το καλύτερο δυνατό για τη χρήση και την εξυπηρέτηση περισσότερων ασθενών.

2.3 Ανοιχτά ζητήματα ασφάλειας στο Internet of Things

2.3.1 Ανάλυση της Ασφάλειας

Είναι πολλά τα οφέλη τα οποία προσφέρει η τεχνολογία του IoT, αλλά συνάμα πολλοί και οι περιορισμοί για τις συσκευές του, εμποδίζοντας την πλήρη υιοθέτησή τους στους παραπάνω κλάδους. Η διαλειτουργικότητα και η ασφάλεια επηρεάζονται ιδιαίτερα από τέτοιους περιορισμούς [26]. Δεδομένου ότι η αρχιτεκτονική του συστήματος δεν είναι καλά καθορισμένη, ο περιορισμός και η ακεραιότητα των δεδομένων καθώς και η ευρωστία του συνολικού συστήματος δεν είναι εγγυημένα. Ακόμη αν και το IoT παρέχει τα πρωτόκολλα για τη διατήρηση των πληροφοριών, εγείρονται διάφορα θέματα. Για παράδειγμα, είναι αμφίβολο αν οι τεχνολογίες και οι πρακτικές του Διαδικτύου όπως πρωτόκολλα TCP/IP & OSI ή όπως πρωτόκολλα IEEE 802.3 ή IEEE 802.11 ισχύουν για το IoT. Αυτές οι ανησυχίες οφείλονται στο γεγονός ότι οι συσκευές IoT δεν ακολουθούν τις ίδιες πρακτικές εφαρμογής πρωτοκόλλου και αφορούν συγκεκριμένες αρχιτεκτονικές, υπολογιστικές

δυνατότητες και απαιτήσεις διασύνδεσης. Ως αποτέλεσμα, η ασφάλεια πρέπει να αντιμετωπιστεί πιο αποτελεσματικά. Για να κατανοήσουμε το μέγεθος του προβλήματος, πρέπει να έχουμε μία πλήρη εικόνα για το πώς το σύστημα IoT είναι εγκλωβισμένο και χρησιμοποιείται από τα πρωτόκολλα και τις τεχνολογίες που το εφαρμόζουν. Η στοίβα του πρωτοκόλλου OSI (ISO/IEC7498-1) αποτελεί την ιδανική εκκίνηση, δεδομένου ότι μπορούμε να τοποθετήσουμε κάθε τεχνολογία στο επίπεδό της και να την μελετήσουμε γενικά, αλλά και από την άποψη της ασφάλειας ειδικότερα. Για παράδειγμα, οι τεχνολογίες που βασίζονται στα πρότυπα IEEE 802.15.4 και IEEE 802.15.1 καλύπτουν το Φυσικό Επίπεδο (Physical Layer) και το Επίπεδο Ζεύξης Δεδομένων (Data Link Layer). Ουσιαστικά, με τον κατάλληλο εξοπλισμό, μπορεί κανείς να παρακολουθήσει τα δεδομένα που εισέρχονται ή εξέρχονται από τη συσκευή IoT. Όσον αφορά το δεύτερο επίπεδο Data Link, με μία πολύ κοινή επίθεση όπως η MAC Spoofing, ο επιτιθέμενος δεν αποκτά μόνο φυσική πρόσβαση στο δικτυακό του στόχο, αλλά μπορεί να αλλάξει ή να κρύψει τη φυσική διεύθυνση του συστήματός του, έτσι ώστε να μη γίνεται εύκολα αντιληπτός. Ωστόσο, εάν η στοίβα πρωτοκόλλου που χρησιμοποιείται δεν εκμεταλλεύεται τις MAC διευθύνσεις, μπορεί χρησιμοποιώντας μία εφαρμογή ανάλυσης πρωτοκόλλων να καταγράψει τα πλαίσια που ανταλλάσσονται. Πρόκειται για μία επίθεση διπλής όψης, δεδομένου ότι θα μπορούσε κατ’ αρχήν να έχει πρόσβαση στο περιεχόμενό του στόχου, αν δεν είναι κρυπτογραφημένο και ταυτόχρονα να παρεμβαίνει στο πρωτόκολλο με την αποστολή παρόμοιων πλαισίων [37]. Στα υψηλότερα επίπεδα, όπως το Επίπεδο Δικτύου (Network Layer) συναντάμε τις επίσης πολύ συνηθισμένες επιθέσεις και ειδικά όταν χρησιμοποιείτε το ευρέως διαδεδομένο IP: IP Spoofing, Routing (RIP) Attacks, Ping Flood (ICMP Flood), Ping of Death Attack, Packet Sniffing, Teardrop Attack [38]. Προχωρώντας στο Επίπεδο Μεταφοράς (Transport Layer) βρίσκουμε επιθέσεις σε πρωτόκολλα όπως TCP και UDP: TCP Sequence number prediction attack, TCP SYN flood, TCP reset attack, UDP flood attack, Smurf attack κ.λπ. [39]. Στο Επίπεδο Συνόδου (Session Layer) έχουμε επιθέσεις Session hijacking στις υπάρχουσες συνδέσεις του Επιπέδου Μεταφοράς, όπως οι επιθέσεις Man-In-The-Middle, Blind hijacking, κ.λπ. [40]. Στο Επίπεδο Παρουσίασης (Presentation Layer), έχουμε επιθέσεις σχετικά με τον τρόπο που τα δεδομένα παραδίδονται σε εφαρμογές του τελικού χρήστη. Σε αυτό το επίπεδο, η κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων συνήθως γίνεται μέσω των

πρωτοκόλλων SSL και TLS. Επιθέσεις που ισχύουν σε αυτή την κατηγορία είναι οι επιθέσεις Session Layer: SSL stripping, STARTTLS command injection attack, Beast, Padding Oracle Attacks, Compression attacks, Certificates attacks. [41]. Τέλος, στο Επίπεδο Εφαρμογής (Application Layer) οι επιθέσεις που συναντάμε σχετίζονται με την εφαρμογή του τελικού χρήστη όπως για παράδειγμα η επίθεση FTP bounce σε εφαρμογές FTP, η επίθεση SSH brute force σε εφαρμογές SSH, η επίθεση HTTP Input validation [42], η επίθεση SQL injection [43], η επίθεση Cross Site Request Forgery [44] και η επίθεση XSS.

Το Secure Shell (SSH) είναι ένα πρωτόκολλο για ασφαλή απομακρυσμένη σύνδεση, άλλα και ασφαλή υπηρεσίες δικτύου μέσω ενός μη ασφαλούς δικτύου. Αποτελείται από τρία βασικά στοιχεία [45]:

1. Το Πρωτόκολλο Επιπέδου Μεταφοράς (Transport Layer Protocol) το οποίο παρέχει τον έλεγχο της ταυτότητας του διακομιστή, την ακεραιότητα των δεδομένων και εμπιστευτικότητα στις συναλλαγές. Μπορεί επίσης να εφαρμόζει συμπίεση δεδομένων καθώς εκτελείται τυπικά μέσω σύνδεσης TCP/IP.
2. Το Πρωτόκολλο Ελέγχου Ταυτότητας Χρήστη (User Authentication Protocol) πιστοποιεί το αναγνωριστικό του χρήστη/πελάτη στο διακομιστή και τρέχει πάνω από το Πρωτόκολλο Επιπέδου Μεταφοράς.
3. Το Πρωτόκολλο Σύνδεσης (Connection Protocol) πολυπλέκει το κρυπτογραφημένο φυσικό κανάλι σε πολλά λογικά κανάλια και τρέχει μέσω του Πρωτόκολλο Ελέγχου Ταυτότητας Χρήστη.

2.3.2 Παραδείγματα επιθέσεων

Η προαναφερθείσα ανάλυση δεν εφαρμόζεται πολύ καλά στα συστήματα IoT και πόσο δε στα συστήματα υγειονομικής περίθαλψης, επιτρέποντας ενδιάμεσες επιθέσεις, εισβολείς, καθώς και πρόσβαση σε πληροφορίες υγείας που με τη σειρά τους πλήττουν την ιδιωτικότητα, την ασφάλεια και την αξιοπιστία ολόκληρου του συστήματος IoT. Οι οργανώσεις υγειονομικής περίθαλψης γίνονται στόχος ολοένα και περισσότερο από hackers και αυτό οφείλεται στο χρυσωρυχείο προσωπικών δεδομένων που κατέχουν. Η φράση του όρκου του Ιπποκράτη, «Πρώτον, μην κάνετε

κακό», αναφέρεται συνήθως μεταξύ των ιατρικών επαγγελματιών, ώστε να αντικατοπτρίζει τη μέγιστη σημασία που αποδίδεται στην περίθαλψη των ασθενών. Το συναίσθημα είναι σαφές: πάνω απ' όλα, ένας επαγγελματίας υγείας πρέπει να εξετάζει την ευημερία των ασθενών. Το 2020, η «ευημερία» έχει εξελιχθεί ώστε να περιλαμβάνει ανησυχίες για την προστασία της ιδιωτικής ζωής στον κυβερνοχώρο. Κατά τη συζήτηση αυτών των δυνητικών προβλημάτων, πρέπει να σκεφτούμε τη σημασία των IoT εφαρμογών και τι επιπτώσεις μπορεί να έχει μία επίθεση που θα αλλάξει ή θα αφαιρέσει δεδομένα.

Μία πιθανή πραγματική επίδραση στον κόσμο από αυτές τις επιθέσεις μπορεί να είναι και ουσιαστική όπως η WannaCry και NotPeyta επιθέσεις ransomware του 2017 [46]. Οι Cyberattackers έχουν τώρα τη δυνατότητα να αποκτήσουν πρόσβαση, να κλέψουν και να πουλήσουν πληροφορίες ασθενούς στον dark web. Πέρα από αυτό όμως, έχουν την ικανότητα να κλείνουν την πρόσβαση σε κρίσιμα συστήματα και αρχεία ασθενών ενός νοσοκομείου, κάνοντας την αποτελεσματική περίθαλψη των ασθενών σχεδόν αδύνατη. Ένα τυπικό παράδειγμα θα μπορούσε να είναι ένα σύστημα συσκευών που παρακολουθεί τον ασθενή (π.χ. σάκχαρο, πίεση, θερμοκρασία, παλμό κ.λπ.) και στέλνει τα δεδομένα αυτά σε ένα σύστημα καταγραφής/παρακολούθησης εντός ενός νοσοκομείου ή ενός παρόμοιου συστήματος που είναι εγκατεστημένο σε ιατρείο. Πόσο ασφαλής είναι αυτή η μετάδοση; Πόσο αξιόπιστο; Αν κάνουμε ένα βήμα περαιτέρω, ας θεωρήσουμε μία αντίστοιχη συσκευή που ελέγχει τη ροή φαρμάκων ενδοφλέβια για να ρυθμίσει το σάκχαρο στον ασθενή. Τι γίνεται αν δεν χορηγηθεί η σωστή ποσότητα; Σε ένα άλλο όχι τόσο επικίνδυνο παράδειγμα αξίζει να αναφέρουμε την περίπτωση επίθεσης στο σύστημα smart IoT λαμπτήρων "Hue" της εταιρείας Philips [47]. Στην περίπτωση αυτή η Smart Hub λύση της Philips που χρησιμοποιούσε μη κρυπτογραφημένη επικοινωνία ήταν επιρρεπής σε εξαναγκασμένη αναβάθμιση του δικτύου με μολυσμένο firmware, το οποίο έκανε τους κόμβους να είναι υπό τον έλεγχο του επιτιθέμενου χωρίς δυνατότητα διόρθωσης. Τέλος, άλλο ένα παράδειγμα είναι αυτό της κυβερνοεπίθεσης τον Οκτώβρη του 2016, η μεγαλύτερη που έχει καταγραφεί ποτέ στην ιστορία, υποστηρίζουν ειδικοί σε θέματα της ασφάλειας στο Διαδίκτυο. Στην επίθεση χρησιμοποιήθηκε ένα μόνο «όπλο», το botnet Mirai, το οποίο κατάφερε να θέσει εκτός λειτουργίας χιλιάδες ιστοσελίδες ταυτόχρονα.

Ποιά είναι τα πρωτόκολλα τα οποία χρησιμοποιούνται και πώς προστατεύονται από τις επιθέσεις; Η χρήση των ήδη γνωστών και των ευρέως διαδεδομένων τεχνολογιών έχουν το πλεονέκτημα ότι, οποιαδήποτε γνωστή ευπάθεια μπορεί να ισχύει επίσης και για συσκευές IoT, αλλά θα μπορούσαν να υπάρχουν πολλές άλλες, που να σχετίζονται με τις συγκεκριμένες συσκευές. Υπάρχουν επίσης τεχνολογίες και πρωτόκολλα που έχουν δημιουργηθεί αποκλειστικά για IoT και τις συσκευές που το διαμορφώνουν, όπως τα πρότυπα πρωτόκολλα IEEE 802.15.4 ή τα ZigBee's. Μία εξαιρετική προστασία για την αντιμετώπιση των εγγενών τρωτών σημείων και των ιδιόμορφων αυτών πρωτοκόλλων και συσκευών. Με την αυξανόμενη υιοθέτηση ιατρικών συσκευών και συσκευών IoT, η έκταση για επιθέσεις υγειονομικής περίθαλψης γίνεται ακόμη μεγαλύτερη. Το πρόβλημα έχει επιδεινωθεί περαιτέρω, με το περιορισμένο προσωπικό στον τομέα της ασφάλειας του κυβερνοχώρου και τους περιορισμούς στον προϋπολογισμό για την ασφάλειά του (κυβερνοχώρου). Προκειμένου να επιτευχθεί ισχυρή απόδοση σε ένα σύστημα IoT, έχουν γίνει διάφορες προσεγγίσεις [48]. Οι τεχνολογίες πληροφοριών και επικοινωνιών των προγραμματιστών, κάνουν ευκολότερο το έργο για τους ερευνητές και τους μηχανικούς, ώστε να συνειδητοποιήσουν ότι το σύστημα είναι πιστοποιημένο για όλες τις εφαρμογές. Στην πραγματικότητα, εξετάζοντας την εμπιστευτικότητα και ευαισθησία των ιατρικών δεδομένων, ένα σύστημα υγειονομικής περίθαλψης πρέπει να πληροί προηγμένο έλεγχο πρόσβασης και διαδικασίες με αυστηρές απαιτήσεις ασφάλειας και ποιότητας δεδομένων [49]. Η εργασία [50] στοχεύει στην ενσωμάτωση της τεχνολογίας της τεχνητής νοημοσύνης, όπως τα νευρωνικά δίκτυα και τα ευφυή συστήματα, σε ένα ασφαλές σύστημα παρακολούθησης της υγειονομικής περίθαλψης. Αυτό θα επιτρέψει στο σύστημα να λειτουργήσει ως «έξυπνο μοντέλο υγειονομικής περίθαλψης» που λαμβάνει αποφάσεις από μόνο του και δίνει προτεραιότητα στις παραμέτρους υγείας που συλλέχθηκαν από τους αισθητήρες κόμβους. Στην [51], οι συγγραφείς προτείνουν μία αρχιτεκτονική ελέγχου πρόσβασης για περιορισμένους πόρους υγειονομικής περίθαλψης IoT. Η προσέγγιση βασίζεται σε μία πολιτική που παρέχει λεπτομερή πρόσβαση σε εξουσιοδοτημένους χρήστες υπηρεσιών, προστατεύοντας παράλληλα πολύτιμους πόρους από μη εξουσιοδοτημένη πρόσβαση, ενώ η [52] προτείνει ένα υβριδικό μοντέλο ασφάλειας για τη διασφάλιση δεδομένων διάγνωσης σε ιατρικές εικόνες. Η σημασία της ασφάλειας IoT σε γενικές γραμμές είναι αρκετά εμφανής στη διεθνή σκηνή τυποποίησης, πολιτικής χάραξης και

κοινοπραξιών. Μία ενδιαφέρουσα εκτεταμένη έκθεση, με τίτλο «Key Fun Suggestions for Fun in the Critical Information Infrastructure to Identification Key IoT Cyber Security Recommendations», δημοσιεύθηκε τον Νοέμβριο του 2017 από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[53].

3 ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΕΡΕΥΝΑΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ IoT ΣΥΣΚΕΥΩΝ

3.1 Θεωρητικό πλαίσιο

Υπάρχει ένας σημαντικός αριθμός ερευνητικών εργασιών που παρουσιάστηκαν τα τελευταία χρόνια για συσκευές IoT και θέματα σχετικά με τη λειτουργία τους. Τα πιο σημαντικά ζητήματα, τα οποία και έχουν εμπνεύσει αυτή τη διατριβή, είναι η αξιοπιστία και η ασφάλεια (φυσική προστασία και ακεραιότητα των δεομένων/προγραμμάτων) της συσκευής. Η αξιοπιστία σχετίζεται άμεσα με τις φυσικές παραμέτρους του προϊόντος που ορίζονται από το περιβάλλον λειτουργίας, τη γήρανση υλικού, το μέσο χρόνο πριν την αποτυχία (MTBF, Mean Time Before Failure), τη διαδικασία κατασκευής (γνήσια ή πλαστά) [54] και την κατάστασή του (αναμονή, δυσλειτουργία, κ.λπ.) [55]. Παρόλο που το ζήτημα της αξιοπιστίας είναι κρίσιμο για πολλές εφαρμογές, οι ερευνητές συνεχίζουν να το μελετούν κυρίως υπό εργαστηριακές συνθήκες ή βάσει θεωρίας. Η αξιοπιστία ωστόσο είναι εξαιρετικά επιρρεπής στις συνθήκες λειτουργίας και πρέπει να διερευνηθεί περαιτέρω [56]. Ιδιαίτερο ενδιαφέρον ως μελέτη περίπτωσης είναι η διερεύνηση παρόμοιων (ή πανομοιότυπων) έξυπνων συσκευών που λειτουργούν κάτω από διαφορετικές συνθήκες (είτε χαρακτηρίζονται κανονικές είτε χαρακτηρίζονται ως ακραίες) και τον υπολογισμό της υποβάθμισης της αξιοπιστίας (ως μέτρηση) βάσει του μέσου χρόνου πριν από την αποτυχία (MTBF) για κάθε περιβάλλον. Ωστόσο, εκτός από αυτή τη μελέτη περίπτωσης, η οποία είναι χαρακτηριστική για τις αναμενόμενες συνθήκες λειτουργίας, υπάρχουν περιπτώσεις όπου το υλικό δε λειτουργεί όπως αναμενόταν. Τέτοιες περιπτώσεις περιλαμβάνουν το αποτέλεσμα ενός Trojan hardware ή μίας επίθεσης πλαϊνών καναλιών. Παίρνοντας μαθήματα από άλλους κλάδους όπως η δοκιμή κυκλωμάτων, η αρχή της ανώμαλης λειτουργίας μοιάζει με το αποτέλεσμα του Single Event Upset (SEU) [57]. Έτσι, πολλές ανώμαλες λειτουργίες υλικού μπορεί να χαρακτηριστούν ως αποκλίσεις της κανονικής λειτουργίας.

Όσον αφορά το ζήτημα της ασφάλειας, η πρόσφατη αύξηση της χρήσης ετερογενών υπολογιστικών συσκευών [58] έχει καταστήσει πολύ πιο δύσκολη την προστασία των υπολογιστικών υποδομών από κάθε είδους κινδύνους, όπως επιθέσεις στον κυβερνοχώρο, δυσλειτουργίες ή διαρροές απορρήτου [59-66]. Ενώ οι υπολογιστικές

συσκευές είχαν το ίδιο μέγεθος, παρόμοιους πόρους και εγκατεστημένα συγκεκριμένα λειτουργικά συστήματα, ήταν εφικτή η παρακολούθηση της λειτουργίας τους και η σύγκρισή τους με τα προκαθορισμένα κανονικά πρότυπα χρήσης. Σήμερα όμως, η ποικιλία των συσκευών IoT μαζί με τις συρρικνωμένες δυνατότητες επεξεργασίας, έχουν κάνει την προστασία τους ένα δύσκολο εγχείρημα. Πολλά από τα πρόσφατα προβλήματα ασφάλειας στον κυβερνοχώρο συνδέονται άμεσα ή έμμεσα με αυτή τη δραματική αλλαγή στην πρωτοφανή εναλλαγή με τη μορφή συσκευών που χρησιμοποιούνται. Ανάλογα με το λογισμικό μίας συσκευής IoT, ο εντοπισμός εκτέλεσης κακόβουλου κώδικα ή το αποτέλεσμα μίας επίθεσης, είναι διαφορετικά.

Το Botnet είναι ένα σύνολο μολυσμένων μηχανημάτων (bots) που ελέγχεται μέσω εξυπηρετητών (servers) Command and Control (C&C) από τους επιτιθέμενους. Η συχνότητα εμφάνισης του εν λόγω κακόβουλου λογισμικού, καθώς και το επίπεδο πολυπλοκότητάς του αυξάνεται κάθε χρόνο. Τα πλήγματα από αυτού του είδους κακόβουλου λογισμικού μπορούν να πάρουν πολλές σοβαρές μορφές συμπεριλαμβανομένης της απώλειας σημαντικών δεδομένων ή χρημάτων. Οι συσκευές IoT χρησιμοποιήθηκαν πρόσφατα για να δημιουργήσουν τεράστια bot δίκτυα και να εκτελέσουν κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS attack), το μέγεθος των οποίων είναι μεγαλύτερο από εκείνο οποιασδήποτε παρόμοιας επίθεσης στο παρελθόν [61, 62], καθώς και τα ανεπαρκή μέτρα ασφαλείας που συνήθως εφαρμόζουν οι κατασκευαστές σε αυτές τις συσκευές προσφέρουν στους εγκληματίες του κυβερνοχώρου νέες ευκαιρίες όσον αφορά τη δημιουργία μεγάλων και αποτελεσματικών δικτύων bot.

Επιπλέον, η απόκτηση φυσικών δεδομένων που επεξεργάζονται από αυτές τις συσκευές συνιστά σημαντική απειλή για την ιδιωτικότητα των χρηστών [63, 64]. Οι συσκευές IoT, εγκατεστημένες στην εργασία ή ακόμα και σε δημόσιους χώρους, παρακολουθούν και αποθηκεύουν δεδομένα σχετικά με τις δραστηριότητες που συμβαίνουν στον χώρο παρατήρησής τους. Στην πράξη, μία συσκευή IoT συλλέγει δεδομένα σχετικά με τη δραστηριότητα των ανθρώπων που βρίσκονται σε αυτούς τους χώρους, μερικές φορές ακόμη και χωρίς τη συγκατάθεσή τους ή ακόμη και εν αγνοία τους. Η παρακολούθηση, η αποθήκευση, η επεξεργασία ή ακόμα και η

αξιοποίηση αυτών των δεδομένων, έχει σοβαρές επιπτώσεις στην ιδιωτική ζωή για τους εμπλεκόμενους.

Η αγορά, για την παραγωγή συσκευών IoT, φαίνεται να έχει αυξηθεί εκθετικά και πολλοί νέοι πωλητές διαφορετικών μεγεθών, προσπαθούν να κατασκευάσουν συσκευές IoT, διεκδικώντας ένα μερίδιο αυτής της αγοράς. Αυτό έχει άμεσες επιπτώσεις στη μέση ποιότητα και τις ιδιότητες των νέων παραγόμενων συσκευών IoT. Σε μία αγορά φθηνών συσκευών, αλλά με μεγάλη παραγωγή, οι πωλητές επιλέγουν συνήθως το πιο ανταγωνιστικό προϊόν, δηλαδή το χαμηλότερο κόστος και το μικρότερο χρονικό διάστημα για την αγορά. Έτσι, η ασφάλεια δεν είναι ο σημαντικότερος παράγοντας για τέτοιες συσκευές χαμηλού κόστους. Αυτό οδηγεί στην εισαγωγή της αγοράς, λιγότερο ασφαλών προϊόντων ή των εναλλακτικών τους λύσεων, λόγω της ανάγκης χαμηλού κόστους. Επιπλέον, εξαιτίας των λιγότερο γνωστών κατασκευαστών που δημιούργησαν τέτοιες συσκευές ή τμήματα αυτών, δημιουργήθηκε αυξημένος κίνδυνος κακόβουλου υλικού [65, 66].

Ένας άλλος σημαντικός παράγοντας που εντείνει το πρόβλημα είναι ότι ένα σημαντικό ποσοστό των συσκευών IoT που χρησιμοποιούνται ήδη, ειδικά σε βιομηχανικές εγκαταστάσεις, είναι συσκευές που δε σχεδιάστηκαν με συνδεσιμότητα στο Διαδίκτυο. Οι αλλαγές στις απαιτήσεις ή οι λόγοι ευκολίας χρήσης ανάγκασαν τους ανθρώπους να συνδέσουν τέτοιες εγκαταστάσεις στο Διαδίκτυο. Το πιο συνηθισμένο σενάριο σε αυτές τις περιπτώσεις είναι ότι αυτές οι συσκευές δεν έχουν επαναδιαμορφωθεί για να προστατευθούν [67]. Αυτό συμβαίνει είτε λόγω ανεπαρκούς συνειδητοποίησης της ασφάλειας, είτε λόγω του γεγονότος ότι οι συγκεκριμένες συσκευές απλώς δεν μπορούν να επαναδιαμορφωθούν. Αυτό έχει οδηγήσει σε σημαντικές παραβιάσεις της βιομηχανικής ασφάλειας [68]. Στην [62] αναλύονται τα βασικά χαρακτηριστικά των κακόβουλων προγραμμάτων του διαδικτύου που οργανώνουν ομαδικές και συντονισμένες επιθέσεις DDOS, ενώ στην [69] παρουσιάζονται άλλου τύπου επιθέσεις οι οποίες μπορούν να γίνουν σε συσκευές του IoT όπως οι Φυσικές Επιθέσεις: Node Jamming, Physical Damage, Node Tampering, Social Engineering, Malicious Node Injection, Sleep Deprivation Attack, Malicious Code Injection on the Node, οι Επιθέσεις Δικτύου: Traffic Analysis Attacks, RFID Spoofing, RFID Cloning, RFID Unauthorized Access, Man In the Middle Attack, Denial of Service, Sinkhole Attack, Routing Information Attacks,

Sybil Attack, οι Επιθέσεις Λογισμικού: Virus and Worms, Malicious Scripts, Spyware and Adware, Trojan Horse, Denial of Service ή ακόμη και Επιθέσεις Κρυπτοανάλυσης: Man In The Middle Attack, Side Channel Attacks, Cryptanalysis Attacks. Επίσης πρόσφατες έρευνες όπως η [70] έχουν δείξει τη δυνατότητα των δούρειων ίππων σε επίπεδο υλικού, κακόβουλα εξαρτήματα ή ακόμη και ακολουθίες εντολών κατά την ενεργοποίησή τους να παρακάμπτουν τα συστήματα ασφαλείας.

Σήμερα είναι μία κοινή αντίληψη ότι στην εποχή του ΔτΠ, οι μεγάλες ανησυχίες για τους σχεδιαστές και κατασκευαστές συσκευών IoT, στρέφονται στην αξιοπιστία και την ασφάλεια [59, 71-73]. Αυτή η κρισιμότητα υπαγορεύεται περαιτέρω από τον αυξανόμενο αριθμό συσκευών που εισάγονται στην αγορά κάθε χρόνο, καθώς και από το γεγονός ότι αυτές οι συσκευές είναι τυπικά «για ειδικές λειτουργίες», που σημαίνει ότι παρουσιάζουν περιορισμένη λειτουργικότητα και υπολογιστικούς πόρους. Συνεπώς οι τεχνικοί της ασφάλειας υπολογιστικών συστημάτων αλλά και οι ερευνητές, αντιμετωπίζουν όλο και πιο συχνά ένα ευρύ φάσμα από ασυνήθιστα κακόβουλα γεγονότα και καλούνται να ανιχνεύσουν αυτές τις ανωμαλίες όταν συμβαίνουν και στην συνέχεια να τις κατηγοριοποιήσουν ώστε να διαλέξουν την κατάλληλη μέθοδο αντιμετώπισης. Η πρώτη μέθοδος ανίχνευσης ανωμαλιών για την ανίχνευση εισβολής προτάθηκε σχεδόν πριν από 40 χρόνια [74]. Υπάρχουν πολλές έρευνες, άρθρα ανασκόπησης, καθώς και βιβλία σχετικά με αυτό το ευρύ θέμα. Ένα εκτενές εύρος ερευνών επί τεχνικών ανίχνευσης ανωμαλιών βρίσκεται σε πολλά βιβλία [75-78]. Σε άλλες έρευνες, οι συγγραφείς προσεγγίζουν σφαιρικά αλλά και πιο γενικά το θέμα της ανίχνευσης ανωμαλιών [79, 80]. Σε αρκετά άρθρα ανασκόπησης περιγράφονται διάφορες μέθοδοι ανίχνευσης ανωμαλιών δικτύου. Στην [81] παρουσιάζεται ένα εργαλείο για την ανάλυση των πτυχών ασφαλείας των κατανεμημένων προγραμμάτων IoT και την προστασία τους από επιθέσεις υπερχείλισης του buffer, ενώ η [82] προτείνει ένα πολυπλατφορμικό σύστημα ανίχνευσης ανωμαλίας που υποστηρίζει ετερογενείς συσκευές. Άλλη μία έρευνα [83] παρουσιάζει την επισκόπηση ενός συστήματος ανίχνευσης κατανεμημένων εσωτερικών ανωμαλιών για το IoT, όπου κάθε κόμβος παρακολουθεί τους γείτονές του και αν εντοπιστεί μη φυσιολογική συμπεριφορά, ο κόμβος παρακολούθησης θα μπλοκάρει τα πακέτα από τον κόμβο που συμπεριφέρεται μη φυσιολογικά στο στρώμα ζεύξης δεδομένων και θα αναφέρει στον γονικό κόμβο του. Λόγω της ετερογένειας των έξυπνων συσκευών του IoT, παρατηρούμε πλέων πως οι

υπάρχουσες τεχνικές ανίχνευσης ύποπτης συμπεριφοράς ή επιθέσεων, δεν είναι αποτελεσματικές ή δε μπορούν να εφαρμοστούν δεδομένης της τεράστιας κλίμακας αυτών των συσκευών και των διαφορετικών τύπων που έχει αναπτύξει ο κάθε κατασκευαστής [84]. Από τις πιο αποτελεσματικές μεθόδους ανίχνευσης ανωμαλιών δικτύου είναι οι PCA (Principle Component Analysis) [85, 86], ανάλυση wavelet [87, 88], μαρκοβιανά μοντέλα (markovian models) [89], συσταδοποίηση (clustering) [90], ιστογράμματα [91] και εντροπία [92, 93].

Σήμερα, παρόλο που ένα μεγάλο μέρος της επιστημονικής κοινότητας ασχολείται με το θέμα της ανίχνευσης ανωμαλιών δικτύου, το πρόβλημα της εύρεσης μίας γενικής μεθόδου για ένα ευρύ φάσμα ανωμαλιών δικτύου εξακολουθεί να παραμένει άλυτο. Τα ευρέως διαθέσιμα συστήματα που χρησιμοποιούνται για την ανίχνευση εισβολής είναι αναποτελεσματικά ενάντια σε ένα σύγχρονο κακόβουλο λογισμικό (malware). Τέτοια συστήματα, ως επί το πλείστων, χρησιμοποιούν τεχνικές που βασίζονται στα χαρακτηριστικά των επιθέσεων ή αλλιώς στις υπογραφές τους (misuse-based techniques ή signature-based techniques). Η παραπάνω προσέγγιση παρουσιάζει ελλείψεις [94, 95]. Οι υπογραφές περιγράφουν μόνο παράνομα μοτίβα στην κίνηση δικτύου, οπότε απαιτείται γνώση των μοτίβων αυτών εκ των προτέρων [96]. Ως αποτέλεσμα, οι λύσεις που βασίζονται στις υπογραφές δεν μπορούν να αντιμετωπίσουν νέες τεχνικές επιθέσεων και επιθέσεις που δεν είναι ακόμη γνωστές, ονομαζόμενες και ως επιθέσεις μηδενικής ημέρας (0day attacks) [97]. Επιπλέον, δεν είναι σε θέση να εντοπίσουν μία συγκεκριμένη επίθεση μέχρι ένας κανόνας για την αντίστοιχη ευπάθεια να έχει δημιουργηθεί, δοκιμαστεί, κυκλοφορήσει και να αναπτυχθεί, το οποίο συνήθως απαιτεί ένα μεγάλο χρονικό διάστημα.

Επίσης, άλλη μία κατηγορία επιθέσεων που απλά αγνοεί τις μαθηματικές ιδιότητες ενός κρυπτογραφικού συστήματος και εστιάζει στη φυσική εφαρμογή του στο υλικό, είναι αυτή των επιθέσεων πλαϊνών καναλιών, οι οποίες συνήθως αναφέρονται ως SCA. Πιο συγκεκριμένα, τα κρυπτογραφικά συστήματα διαρρέουν συνήθως πληροφορίες σχετικά με την εσωτερική διαδικασία υπολογισμού. Στην πράξη, αυτό σημαίνει ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν διάφορες τεχνικές για να εξαγάγουν βασικές και άλλες μυστικές πληροφορίες από τη συσκευή [98]. Ουσιαστικά, οι επιθέσεις πλαϊνών καναλιών παρακολουθούν την κατανάλωση ενέργειας και τις ηλεκτρομαγνητικές εκπομπές ενώ μία συσκευή εκτελεί

κρυπτογραφικές λειτουργίες. Οι επιθέσεις πλαϊνών καναλιών που πραγματοποιούνται κατά ηλεκτρονικών συσκευών και συστημάτων, είναι φθηνές και σχετικά απλές ως προς την εκτέλεση. Αυτό σημαίνει ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν διάφορες τεχνικές πλαϊνών καναλιών για τη συλλογή δεδομένων και την εξαγωγή κρυφών κρυπτογραφικών κλειδιών. Ως εκ τούτου, μία διαφορετική προσέγγιση των τεχνικών ανίχνευσης ανωμαλιών δικτύου κρίνεται απαραίτητη ως μία πιθανή λύση για τη συμπλήρωση των λύσεων που προσφέρουν οι λοιπές τεχνικές.

Αυτό έχει οδηγήσει τους επιστήμονες αλλά και τις εταιρίες, τα τελευταία χρόνια, να αναζητήσουν νέους τρόπους ανίχνευσης, αντιμετώπισης και προστασίας των έξυπνων συσκευών από τις επιθέσεις. Συγκεκριμένα, είναι μία κοινή προσέγγιση για τον εντοπισμό ύποπτης συμπεριφοράς μέσω διαφόρων μετρήσιμων παραμέτρων όπως στην [99] που αφορά στην ανίχνευση επιθέσεων DDoS μέσω Machine Learning τεχνικών για τον έλεγχο ρυθμού μετάδοσης πακέτων, το μέγεθος πακέτου κ.ά.. Στην [100] παρουσιάζεται μία μέθοδος για την ανίχνευση ανώμαλων σε λειτουργίες οικιακών συσκευών IoT, οι οποίες μπορούν να μάθουν ακολουθίες συμπεριφοράς χρηστών σύμφωνα με συνθήκες όπως, ώρα της ημέρας, θερμοκρασία και υγρασία. Όταν φτάσει μία εντολή λειτουργίας, η μέθοδος συγκρίνει την τρέχουσα ακολουθία με τις ακολουθίες που έχουν μάθει για την τρέχουσα κατάσταση. Εάν οι αλληλουχίες δεν ταιριάζουν, η λειτουργία θεωρείται ανώμαλη. Ακόμη μία προσέγγιση που χρησιμοποιεί τεχνικές συσταδοποίησης των χαρακτηριστικών Machine Learning, βασισμένη σε συστήματα ανίχνευσης και χρήση παραμέτρων για τη σωστή εκπαίδευση του συστήματος συναντάμε στην [101]. Στην [102], προτάθηκαν δύο προσεγγίσεις που περιλαμβάνουν βαθιά αυτοματοποιημένα μοντέλα κωδικοποιητή για την ανάλυση χρονοσειρών που συλλέγονται από ανιχνευτές βαρυτικών κυμάτων και παρέχουν μία ετικέτα ταξινόμησης (θόρυβος ή πραγματικό σήμα). Η εργασία [103] επικεντρώνεται στην ανίχνευση απροσδόκητων δεδομένων αισθητήρα που προκύπτουν είτε από το ίδιο το σύστημα αισθητήρων είτε από το ελεγχόμενο περιβάλλον. Προτείνεται μία νέα προσέγγιση για την αυτόματη ανίχνευση ανωμαλιών σε ετερογενή δίκτυα αισθητήρων που βασίζονται σε προηγμένη ανάλυση δεδομένων με ανάλυση δεδομένων cloud. Η πρώτη εκμεταλλεύεται έναν τεχνητό αλγόριθμο νευρωνικού δικτύου χωρίς επίβλεψη, ενώ η ανάλυση δεδομένων cloud εκμεταλλεύεται τον αλγόριθμο επεξεργασίας πολλαπλών παραμέτρων από απόσταση. Τα αποτελέσματα της έρευνας στην [104] αντιπροσωπεύουν μία προσπάθεια

διερεύνησης ανωμαλιών σε ένα σενάριο πολλαπλών IoT (MIoT). Αρχικά, προτείνει ένα νέο μεθοδολογικό πλαίσιο που μπορεί να κάνει τη μελλοντική έρευνα σε αυτόν τον τομέα ευκολότερη, συνεκτική και ομοιόμορφη. Στη συνέχεια, στο πλαίσιο της ανίχνευσης ανωμαλιών σε ένα MIoT, ορίζει το λεγόμενο «πρόβλημα προς τα εμπρός» και το «αντίστροφο πρόβλημα». Ο στόχος της εργασίας [105] είναι να διερευνήσει την καταλληλότητα προσεγγίσεων βαθιάς μάθησης για ένα σύστημα ανίχνευσης εισβολής που βασίζεται σε ανωμαλίες. Σε αυτή την εργασία, τα ανεπτυγμένα μοντέλα ανίχνευσης ανωμαλιών βασίζονται σε διαφορετικές δομές deep neural network, συμπεριλαμβανομένων των συνελικτικών νευρωνικών δικτύων (convolutional neural networks), των αυτοκωδικοποιούμενων (autoencoders) και των επαναλαμβανόμενων νευρωνικών δικτύων (recurrent neural networks).

Τα έργα που παρουσιάστηκαν στο παρελθόν εξακολουθούν να επικεντρώνονται σε λύσεις δικτύου και στη διαθεσιμότητα υψηλής ισχύος υπολογισμού του συστήματος που ενσωματώνει το ML και άλλους μηχανισμούς για τον εντοπισμό ανωμαλιών ή/και ανίχνευσης εισβολής. Αυτό σημαίνει ότι οι προτεινόμενες λύσεις είναι δαπανηρές, απαιτώντας ειδικό εξοπλισμό για την υλοποίησή τους, το οποίο σε καμία περίπτωση δεν είναι χαμηλού κόστους. Η επιθυμία εξεύρεσης λύσης χαμηλού κόστους και χαμηλής υπολογιστικής ισχύος δεν ικανοποιείται, κάτι που είναι απαραίτητο για καταναλωτικά προϊόντα που στοχεύουν τη χρήση στο σπίτι.

Οι [6, 106-108] από τους Μυριδάκης Δ. κ.ά. μελετάνε φυσικά χαρακτηριστικά όπως η παροχή του ρεύματος και εξάγουν πληροφορίες που σε συνδυασμό με κατώφλια ή εύρη τιμών εντοπίζουν ανωμαλίες στις συσκευές IoT. Αυτές είναι οι πρώτες προσπάθειες για την εφαρμογή ενός αυτόνομου συστήματος ικανού να παρέχει βελτιωμένη ασφάλεια με χαμηλό κόστος. Ωστόσο, δε διαθέτουν την ενσωμάτωση αλγορίθμων ML και έναν ισχυρό τρόπο ανίχνευσης εισβολής, χωρίς να γνωρίζουν τη λειτουργία της συσκευής στόχου IoT.

Σε αυτό το σημείο αξίζει να επισημάνουμε ότι η Ενσωματωμένη Μηχανική Μάθηση (Embedded Machine Learning), δεν είναι μία απλή τεχνολογία, αλλά αντιθέτως, παρέχει τη δυνατότητα για καλύτερα επιχειρηματικά αποτελέσματα και βελτιώσεις στις βασικές γραμμές των επιχειρήσεων σε πολλούς και διαφορετικούς τομείς, με αποδεδειγμένη απόδοση επένδυσης σύμφωνα όπως αναφέρεται στο [109]. Στις περισσότερες περιπτώσεις, οι επιχειρήσεις επεξεργάζονται δεδομένα IoT σε edge

clusters ή στο cloud, παρά σε edge devices και microcontrollers. Η έλευση της Ενσωματωμένης Μηχανικής Μάθησης (Embedded Machine Learning) και του TinyML, αντιστρέφει αυτό το παράδειγμα, ωθώντας τη νοημοσύνη των εφαρμογών στα edge δίκτυα IoT. Ορισμένα από τα σημαντικά οφέλη είναι:

- Η σημαντική εξοικονόμηση πόρων εύρους ζώνης, ενέργειας και αποθήκευσης.
- Ευκαιρίες για ταχύτερη και χαμηλή καθυστέρηση (low-latency) επεξεργασίας δεδομένων.
- Διευκόλυνση εφαρμογών ελέγχου σε πραγματικό χρόνο και ενίσχυση των έγκαιρων αποφάσεων.
- Χρησιμοποίηση μεγάλων ποσοτήτων δεδομένων από μη συνδεδεμένες συσκευές.

Τα παραπάνω οφέλη είναι απτά και έχουν σαφή επιχειρηματική συνάφεια. Η ικανότητα των επιχειρήσεων να χρησιμοποιούν περισσότερα δεδομένα και διαδικασίες στην άκρη του δικτύου, επιτρέπει νέες αποδοτικές δραστηριότητες στις επιχειρήσεις, μεταφράζοντας άμεσα σε χρηματικά οφέλη και βελτιώνοντας τις εταιρικές γραμμές. Η ενσωματωμένη μηχανική μάθηση δεν είναι ούτε μία νέα διαφημιστική εκστρατεία ούτε μία άσκηση μηχανικής για χάκερ και υπολογιστές. Είναι ένα πρόγραμμα αλλαγής παιχνιδιών στον χώρο υπολογιστών της Τεχνητής Νοημοσύνης και του Διαδικτύου των πραγμάτων, που μπορεί να αυξήσει την παραγωγικότητα της επιχείρησης. Ο καλύτερος μάρτυρας για αυτό είναι ο σημαντικός αριθμός περιπτώσεων χρήσης ROI (Return-on-Investment), που δημιουργείται επί του παρόντος από βιομηχανικές επιχειρήσεις παγκοσμίως. Παραδείγματα τα οποία παρουσιάζουν ένα αντιπροσωπευτικό σύνολο τέτοιων περιπτώσεων χρήσης έχουν όπως παρακάτω:

3.1.1 Ευφυής Διαχείριση Περιουσιακών Στοιχείων και Βιομηχανική Συντήρηση

Οι περισσότερες βιομηχανικές επιχειρήσεις διατηρούν τα περιουσιακά τους στοιχεία βάσει μίας προσέγγισης προληπτικής συντήρησης. Το τελευταίο εξαρτάται από τη συντήρηση ή την αντικατάσταση σε τακτά χρονικά διαστήματα περιουσιακών στοιχείων, όπως μηχανήματα και εργαλεία. Αυτά τα διαστήματα υπαγορεύονται από το ονομαστικό τους EoL (End-of-Life), το οποίο παρέχεται από τον OEM (Original

Equipment Manufacturer). Αυτή η προσέγγιση βοηθά στην αποφυγή καταστροφικών διακοπών παραγωγής, καθώς τα περιουσιακά στοιχεία διατηρούνται συνήθως πριν καταρρεύσουν. Ωστόσο, η προληπτική συντήρηση οδηγεί σε μη βέλτιστη χρήση ακριβών περιουσιακών στοιχείων, δεδομένου ότι τα περιουσιακά στοιχεία αντικαθίστανται πάντα πολύ πριν από το EoL.

Η έλευση της 4ης Βιομηχανικής Επανάστασης (Industry 4.0) και του Βιομηχανικού Διαδικτύου των πραγμάτων επιτρέπει στις βιομηχανικές επιχειρήσεις να εφαρμόζουν την παρακολούθηση των περιουσιακών τους στοιχείων βάσει συνθηκών. Αξιοποιώντας ψηφιακά δεδομένα από αισθητήρες (π.χ. αισθητήρες δόνησης, αισθητήρες θερμοκρασίας, θερμικές εικόνες) και συστήματα διαχείρισης περιουσιακών στοιχείων (π.χ. δεδομένα ποιότητας προϊόντος, ανάλυση λαδιού), οι επιχειρήσεις μπορούν σήμερα να λαμβάνουν πληροφορίες σε πραγματικό χρόνο σχετικά με την κατάσταση των βιομηχανικών περιουσιακών στοιχείων, όπως εργαλεία και μηχανήματα [110] Επιπλέον, χρησιμοποιώντας αλγόριθμους μηχανικής εκμάθησης, μπορούν επίσης να αντλήσουν προγνωστικά στοιχεία σχετικά με την υπολειπόμενη ωφέλιμη ζωή RUL (Remaining Useful Life) των στοιχείων τους. Σε αρκετές περιπτώσεις, αξιόπιστες εκτιμήσεις RUL επιτρέπουν στις βιομηχανικές επιχειρήσεις να μετατρέψουν την προληπτική συντήρηση σε προγνωστική συντήρηση [111]. Η προληπτική συντήρηση είναι το απόλυτο όραμα της λειτουργίας συντήρησης και επισκευής, η οποία οδηγεί στην καλύτερη δυνατή συνολική απόδοση εξοπλισμού OEE (Overall Equipment Efficiency). Η παρακολούθηση βάσει συνθηκών και η προγνωστική συντήρηση βοηθούν τις επιχειρήσεις να βελτιώσουν τη χρήση των περιουσιακών τους στοιχείων, να μειώσουν το χρόνο διακοπής της παραγωγής, να εξαλείψουν τα απόβλητα λόγω βλάβης του εξοπλισμού και να προγραμματίσουν εργασίες συντήρησης σε βέλτιστο χρόνο. Η προληπτική συντήρηση θεωρείται ως μία από τις «δολοφονικές εφαρμογές» της 4ης βιομηχανικής επανάστασης (Industry 4.0): Έχει απτή απόδοση επένδυσης (ROI) και εφαρμόζεται σε όλους σχεδόν τους βιομηχανικούς τομείς, όπως για παράδειγμα βιομηχανία, ενέργεια, κατασκευές, έξυπνα κτίρια, πετρέλαιο, φυσικό αέριο και εξόρυξη.

Οι περισσότερες προβλέψεις συντήρησης τελευταίας τεχνολογίας μεταφέρουν και αναλύουν δεδομένα στο cloud. Αυτή η προσέγγιση εξοικονομεί ενέργεια αλλά παρουσιάζει περιορισμούς στη λειτουργία της. Για παράδειγμα, η πρόβλεψη μίας

αποτυχίας που βασίζεται σε ανάλυση μηχανικής μάθησης η οποία βασίζεται σε cloud δεν είναι πάντα αρκετά γρήγορη για να επιτρέψει κατάλληλες διορθωτικές ή προληπτικές ενέργειες. Η ενσωματωμένη μηχανική μάθηση προσθέτει σημαντική αξία στη συμβατική πρόβλεψη συντήρησης και παρακολούθησης συνθηκών: Παράγει πληροφορίες σε πραγματικό χρόνο και επιτρέπει αποφάσεις σε πραγματικό χρόνο. Η εκτέλεση της μηχανικής μάθησης απευθείας σε συσκευές συλλογής δεδομένων ή μικροελεγκτές μέσα στο μηχάνημα, επιτρέπει στις βιομηχανικές επιχειρήσεις να αντλούν έγκαιρες και ακριβείς πληροφορίες σχετικά με την κατάσταση των διαφόρων περιουσιακών στοιχείων.

Η βιομηχανική συντήρηση σε πραγματικό χρόνο με βάση την ενσωματωμένη μηχανική μάθηση είναι επίσης μία εξαιρετική περίπτωση χρήσης για OEMs. Συγκεκριμένα, οι OEM μπορούν να βελτιώσουν τα μηχανήματά τους με έξυπνες λειτουργίες ανίχνευσης βλαβών και ανωμαλιών, αξιοποιώντας τη μηχανική μάθηση μέσα στα προϊόντα τους. Μπορούν συνεπώς να παρέχουν τέτοιες λειτουργίες πληροφοριών ως υπηρεσία στους πελάτες τους για να επιτρέψουν νέα επιχειρηματικά μοντέλα όπως η Συντήρηση ως Υπηρεσία (Maintenance-as-a-Service). Συνολικά, η Ενσωματωμένη Μηχανική Μάθηση βελτιώνει την αποτελεσματικότητα των προηγμένων εφαρμογών Προληπτικής Συντήρησης (Predictive Maintenance) με τρόπους που αυξάνουν τη χρήση των στοιχείων και βελτιστοποιούν τα παράθυρα των υπηρεσιών τους.

3.1.2 Διαχείριση Ποιότητας (Quality Management) και Κατασκευή Μηδενικών Ελαττωμάτων (Zero-Defect Manufacturing)

Η Μηχανική Μάθηση άνοιξε πρόσφατα νέους ορίζοντες στη διαχείριση ποιότητας για εργασίες κατασκευής και παραγωγής. Συγκεκριμένα, ενδυναμώνει την έννοια της προγνωστικής ποιότητας [112] δηλαδή, την ικανότητα πρόβλεψης ζητημάτων ποιότητας πριν εμφανιστούν. Σε αυτήν την κατεύθυνση, οι τεχνικές μηχανικής μάθησης, συμπεριλαμβανομένης της βαθιάς μάθησης (deep learning) εφαρμόζονται σε μεγάλο όγκο δεδομένων από γραμμές παραγωγής. Ο στόχος των αλγορίθμων είναι να εντοπίζει προληπτικά συνθήκες ή μοτίβα που οδηγούν σε ελαττωματικά προϊόντα. Με βάση αυτά τα μοτίβα, οι διαχειριστές εγκαταστάσεων μπορούν να λάβουν διορθωτικά μέτρα που αποτρέπουν την εμφάνιση του ελαττώματος. Επιπλέον, οι τεχνικές μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση

των προτύπων που σχετίζονται με τη βελτιστοποίηση άλλων παραμέτρων, όπως το κόστος και η περιβαλλοντική απόδοση.

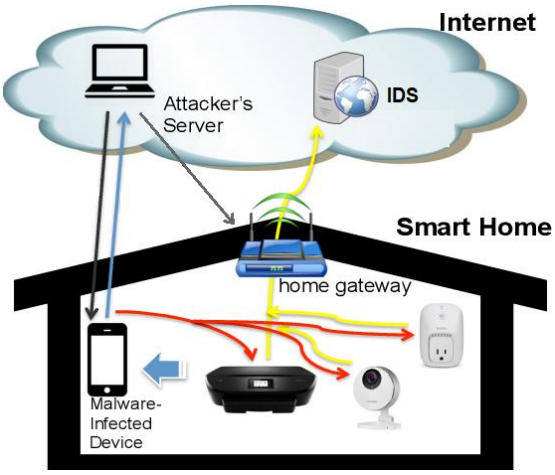
Η ενσωματωμένη μηχανική εκμάθηση προσθέτει σημαντική αξία στις παραπάνω περιπτώσεις χρήσης ποιότητας διαχείρισης. Συγκεκριμένα, παρέχει τα μέσα για την εξαγωγή προγνωστικών πληροφοριών σχετικά με πιθανά ελαττώματα με βάση την επεξεργασία δεδομένων μέσα στον εξοπλισμό. Αυτές οι πληροφορίες μπορούν να συνδυαστούν με πληροφορίες από το cloud analytics για τον προσδιορισμό διαδικασιών και παραμέτρων ελέγχου που οδηγούν σε προβλήματα ποιότητας. Ομοίως, μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση πολλαπλών παραμέτρων ταυτόχρονα, οδηγώντας σε Zero Defect Manufacturing [113]. Έτσι, η ενσωματωμένη μηχανική μάθηση εξοπλίζει τους διαχειριστές εγκαταστάσεων και τους μηχανικούς ποιότητας με ένα νέο κύμα πληροφοριών σε πραγματικό χρόνο, σε επίπεδο περιουσιακών στοιχείων σχετικά με τα ελαττώματα, που συμπληρώνει τις υπάρχουσες γνώσεις σχετικά με τα προβλήματα διαχείρισης ποιότητας. Ως εκ τούτου, επιτρέπει στις επιχειρήσεις να υπερέχουν στην εφαρμογή των στρατηγικών διαχείρισης ποιότητας, όπως η Total Quality Management (TQM) [114]. Συνολικά, οι βιομηχανικές επιχειρήσεις μπορούν να αξιοποιήσουν την ενσωματωμένη μηχανική εκμάθηση για να συμπληρώσουν τις υπάρχουσες γνώσεις τους σχετικά με τη διαχείριση ποιότητας, προκειμένου να βελτιώσουν την ποιότητα των προϊόντων, μειώνοντας παράλληλα τους χρόνους και το κόστος παραγωγής.

Η προσέγγιση της παρούσας διδακτορικής διατριβής, βασίζεται σε φυσικά μετρήσιμα χαρακτηριστικά (όπως η ένταση του ρεύματος) για την ανίχνευση ανωμαλιών, που προκαλούνται σε συσκευές IoT με σκοπό την κυρίευσή τους και τη χρησιμοποίησή τους. Λαμβάνοντας υπόψη ότι τέτοιες συσκευές έχουν περιορισμούς από πλευράς λειτουργικότητας και λειτουργικών χαρακτηριστικών, αναμένεται ότι οποιαδήποτε απόκλιση από την κανονική λειτουργία έχει ως αποτέλεσμα ανάλογη απόκλιση για την καταναλισκόμενη ισχύ. Η παραπάνω προσέγγιση αποτελεί μία αποτελεσματική μέθοδο για την ανίχνευση επιθέσεων όπως έχουν δείξει οι [6, 106-108] που λαμβάνει υπόψη την εξαγωγή πληροφοριών από την ένταση του ρεύματος, ανάλογα με την περίπτωση, για τον εντοπισμό λειτουργικών ανωμαλιών των συσκευών IoT. Εισάγει μία νέα μέθοδο για την ανίχνευση εισβολής σε μία συσκευή IoT, παρακολουθώντας παράπλευρες φυσικές επιδράσεις, όπως η κατανάλωση ισχύος. Βασιζόμενη στην

τεχνική επίθεσης πλευρικού καναλιού, αυτή η έρευνα συσχετίζει επιτυχώς οποιαδήποτε αύξηση κυκλοφορίας του δικτύου και του φορτίου των συσκευών, με την υπερβολική ισχύ σε κατάσταση ηρεμίας που προέκυψε από μία κακόβουλη προσπάθεια πρόσβασης στη συσκευή IoT. Πιο συγκεκριμένα, αξιοποιεί την τεχνική της ανάλυσης ισχύος της επίθεσης SCA [5], και ενσωματώνει Machine-Learning Clustering. Παρέχει ένα φάσμα δυνατοτήτων ανάλυσης ισχύος σε πραγματικό χρόνο και συνδυάζει τις αναλύσεις με τη μηχανική μάθηση και αναλύσεις κατωφλίων με δυνατότητα κλιμάκωσης για την ανίχνευση ύποπτης συμπεριφοράς συσκευών που συνδέονται στο Διαδίκτυο. Η καινοτομία βρίσκεται στο γεγονός ότι ένα εξωτερικό κύκλωμα, είναι ικανό να ανιχνεύει ανώμαλη λειτουργία ή λειτουργικότητά, χωρίς προηγούμενη γνώση της υπό παρακολούθησης συσκευής IoT, εισάγοντας έτσι για πρώτη φορά μία λύση ασφαλείας κατάλληλη για κάθε τύπο συσκευής στόχου, στη διεθνή βιβλιογραφία.

3.2 Πεδίο εφαρμογής

Προκειμένου να γίνει κατανοητό το πρόβλημα το οποίο επιλύει η διατριβή, ορίζεται παρακάτω η τοπολογία της επικοινωνίας των συσκευών οικιακών IoT δίχως βλάβη της γενικότητας με το Διαδίκτυο. Παρατηρούμε ότι προκειμένου να είναι ασφαλής η επικοινωνία, απαιτείται η παρεμβολή μονάδων υλικού Firewall και IDS. Αυτή όμως δεν είναι η περίπτωση για την πλειοψηφία των οικιακών δικτύων, με αποτέλεσμα να είναι σχεδόν αδύνατη η προστασία με τις τυπικές ρυθμίσεις των συσκευών.



Εικόνα 2: Υπόδειγμα σύνδεσης

4 ΑΣΦΑΛΕΙΑ ΜΕ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΦΥΣΙΚΩΝ ΠΑΡΑΜΕΤΡΩΝ «ΒΙΟΜΙΜΗΤΙΣΜΟΣ»

4.1 Θεωρητικό πλαίσιο

4.1.1 Βιομιμητισμός ορισμός και προέλευσή

Ο Βιομιμητισμός ή αλλιώς Βιομιμητική, είναι μία λέξη της οποίας η προέλευσή έρχεται από και αρχαία ελληνικά χρόνια «βίος (bios) και μίμησις (mīmēsis)». Η παραπάνω λέξη αφορά στη μίμηση μοντέλων, συστημάτων καθώς και στοιχείων της φύσης με σκοπό την επίλυση σύνθετων ανθρώπινων προβλημάτων. Η βιομιμητική στην ουσία είναι η έννοια μελέτης της φύσης και της εξέλιξης, προς εφεύρεση, πιο βιώσιμων σχεδίων, προϊόντων και τεχνολογιών για τους ανθρώπους. Αποτελεί μία προσέγγιση στην καινοτομία που επιδιώκει βιώσιμες λύσεις στις προκλήσεις που αντιμετωπίζουν οι άνθρωποι, αντιγράφοντας διαδικασίες και στρατηγικές της φύσης. Η καινοτομία των ανθρώπων πολύ συχνά εμπνέεται από τη φύση, καθώς η φύση λειτουργεί αποτελεσματικά και με βιώσιμο τρόπο.

4.1.2 Παραδείγματα βιομιμητισμού

Υπάρχει μία πλούσια ιστορία σχεδιασμού εμπνευσμένη από τη φύση. Ένα από τα πρώτα παραδείγματα είναι το τεχνητό νευρωνικό δίκτυο (artificial neural network) το οποίο αναπτύχθηκε από τους Warren McCulloch και Walter Pitts το 1943 για να μιμηθεί τη νευρωνική συμπεριφορά [115]. Στα τέλη της δεκαετίας του 1950, ο Otto Schmitt επινόησε τον όρο «Βιομιμητική» (Biomimetics) και εστίασε την έρευνά του στη μίμηση της ηλεκτρικής δραστηριότητας ενός νεύρου [116]. Ο όρος «Βιονικά» (Bionics) επινοήθηκε από τον Jack Steele το 1960 για να περιγράψει ένα τρόπο επίλυσης προβλημάτων μηχανικής χρησιμοποιώντας τη βιολογία. Το 1997, η Janine Benyus επινόησε τον όρο Biomimicry για να περιγράψει την καινοτομία εμπνευσμένη από τη φύση, σε ένα βιβλίο που έφερε τη βιομιμητικότητα στην πρώτη γραμμή του πράσινου σχεδιασμού [117].

4.1.3 Φυσικά χαρακτηριστικά – παράμετροι Συσκευών «Biometrics»

Μέρος του βιομιμητισμού είναι η ανάλυση των στοιχείων του υποκειμένου. Η μέθοδος της ανάλυσης ονομάζεται βιομετρία. Στις μέρες η βιομετρική τεχνολογία ακούγεται όλο και περισσότερο. Ο όρος προέρχεται από τη βιομετρία, που είναι η επιστήμη καταγραφής των ιδιαίτερων χαρακτηριστικών του ανθρώπινου σώματος (χρώμα ματιών, ύψος, δακτυλικά αποτυπώματα κ.ά.) καθώς και της συμπεριφοράς του (βάδισμα, ρυθμός πληκτρολόγησης, ρυθμός ομιλίας κ.α.), και η αξιοποίηση αυτών των δεδομένων. Πρωτοπόρος αυτής της τεχνολογίας υπήρξε ο Ben Miller, που εισήγαγε και τον αντίστοιχο όρο, το 1987. Σύμφωνα μάλιστα με τον ακριβή ορισμό του Miller, η βιομετρική τεχνολογία είναι ένα σύνολο μεθόδων, που έχουν τη δυνατότητα αναγνώρισης ή ταυτοποίησης ενός ζωντανού οργανισμού, βάσει των φυσικών χαρακτηριστικών του ή ορισμένων χαρακτηριστικών της συμπεριφοράς του [118]. Τα βιομετρικά συστήματα αναγνώρισης έχουν τη δυνατότητα καταγραφής αυτών των χαρακτηριστικών και την αξιοποίηση των ψηφιακών δεδομένων, που προκύπτουν έπειτα από επεξεργασία, προκειμένου να πραγματοποιήσουν ταυτοποίηση ενός προσώπου. Κάθε μέρα ακούμε και διαβάζουμε, για κυβερνήσεις που χρησιμοποιούν αναγνώριση προσώπου για θεώρηση και έκδοση διαβατηρίων, τράπεζες οι οποίες υιοθετούν φωνητική αναγνώριση για έλεγχο ταυτότητας χρηστών και αυτοκίνητα που χρησιμοποιούν τεχνολογίες δακτυλικών αποτυπωμάτων για την αύξηση αποτελεσματικότερης λειτουργίας. Ακολουθούν ενδεικτικά παραδείγματα τα οποία έχουν συνεισφέρει στην τεχνολογική επανάσταση της βιομετρίας.

- **Πρόσβαση τηλεφώνου με δακτυλικό αποτύπωμα (Fingerprint)**

Η πρόσβαση στο λειτουργικό σύστημα των σύγχρονων έξυπνων συσκευών τηλεφωνίας με τη χρήση μιας βιομετρικής μεθόδου είναι ιδιαίτερα συχνή. Η αξιοποίηση του δακτυλικού αποτυπώματος είναι το πρώτο παράδειγμα σύνθετης βιομετρικής τεχνολογίας που υιοθετήθηκε τόσο πρόθυμα. Σύμφωνα με έκθεση γνωστής εταιρίας τεχνολογίας, περισσότερα από 900 εκατομμύρια κινητά τηλέφωνα χρησιμοποιούνται επί του παρόντος σε όλο τον κόσμο, πράγμα που σημαίνει ότι εκατομμύρια άνθρωποι αποκτούν πρόσβαση σε αυτά τοποθετώντας το δάκτυλό τους στον ειδικό ενσωματωμένο αισθητήρα. Η έρευνα στο αντικείμενο είναι πλέον ώριμη και αξιοποιεί αλγορίθμους μηχανικής μάθησης, οι οποίοι είναι ικανοί με μικρό

αριθμό δειγματοληψιών να είναι σε θέση να αναγνωρίσουν σε μεγάλο ποσοστό ακρίβειας το δακτυλικό αποτύπωμα του υποκειμένου.

Προχωρώντας ακόμη περισσότερο στη βιομετρική, πλέον επιτρέπεται και το ξεκλείδωμα των smartphone με αναγνώριση προσώπου, γνωστή και ως Face ID, εμπλουτίζοντας τη βιομετρική βιομηχανία.

- **Μεγάλες βάσεις δεδομένων με ανθρώπινα βιομετρικά στοιχεία**

Το Ομοσπονδιακό Γραφείο Ερευνών των ΗΠΑ (FBI) έχει συσσωρεύσει μία τεράστια βιομετρική βάση δεδομένων για όλα τα πράγματα που αφορούν τους Αμερικανούς πολίτες, από διάφορους τύπους βιομετρικών στοιχείων, όπως δακτυλικά αποτυπώματα, φωτογραφίες για αναγνώριση προσώπου, μοτίβα ίριδας, έως και δεδομένα αναγνώρισης βαδίσματος. Το FBI συλλέγει τα δεδομένα του από διάφορες κυβερνητικές και ιδιωτικές πηγές επιβολής του νόμου, χρησιμοποιώντας τα δεδομένα για την πρόληψη του εγκλήματος, την άδεια μετανάστευσης και την ασφάλεια.

Όμως η μεγαλύτερη ανθρώπινη βιομετρική βάση δεδομένων ανήκει στην Ινδία και ονομάζεται Aadhaar. Με την υποστήριξη της κυβέρνησης, έχει εξελιχθεί σε μία πιο εκτεταμένη βιομετρική βάση δεδομένων με δεδομένα ταυτότητας περισσότερων από ενός δισεκατομμυρίου ανθρώπων σε λιγότερο από δέκα χρόνια. Αυτό το σύστημα χρησιμοποιείται συχνά και στην εκπαίδευση. Το Aadhaar είναι ένα εξαιρετικό παράδειγμα για το πώς τα Big Data και τα βιομετρικά στοιχεία μπορούν να ωφελήσουν μία χώρα.

Στην Ελλάδα πρόκειται να εκδοθούν συσκευές, οι οποίες θα δίνουν στους αστυνομικούς τη δυνατότητα να πραγματοποιήσουν αναγνώριση προσώπου σε πραγματικό χρόνο και αναγνώριση δακτυλικών αποτυπωμάτων, ενώ βρίσκονται σε εξωτερική υπηρεσία. Το σχέδιο διάδοσης της νέας τεχνολογίας αποτελεί μέρος του έργου «Smart Policing», που ανακοινώθηκε το 2017 και στοχεύει στον εντοπισμό και την επαλήθευση της ταυτότητας των πολιτών που σταματά για έλεγχο η αστυνομία.

Επί του παρόντος, οι πολίτες που δεν είναι σε θέση να παράσχουν έγγραφα ταυτοποίησης σε έλεγχο της αστυνομίας, πρέπει να μεταφερθούν στο πλησιέστερο αστυνομικό τμήμα για την ταυτοποίησή τους. Εφαρμόζοντας την αναγνώριση προσώπου σε πραγματικό χρόνο, οι νέες συσκευές θα κάνουν την ταυτοποίηση των

πολιτών πιο γρήγορη και αποτελεσματική. Οι συσκευές, οι οποίες έχουν παρόμοια εμφάνιση με τα «έξυπνα» τηλέφωνα, θα συνδέονται με 20 διαφορετικά databases που ανήκουν σε διεθνείς και εθνικές αρχές, όπως το Ελληνικό Υπουργείο Μεταφορών, το Υπουργείο Εξωτερικών, η Europol, το FBI και η Interpol.

- **Έλεγχος διαβατηρίων με σάρωση ίριδας ματιών**

Η σάρωση της ίριδας των ματιών χρησιμοποιείται σε όλα τα μεγάλα αεροδρόμια ανά τον κόσμο εδώ και αρκετά χρόνια. Υπάρχει ένα σύστημα στο οποίο μπορεί οποιοσδήποτε εφόσον συμφωνήσει να σαρώσει τα μάτια του. Τα στοιχεία του εν συνεχεία αποθηκεύονται σε μία διεθνή βάση δεδομένων. Το πλεονέκτημα είναι ότι, αντί να περιμένει σε μία μεγάλη ουρά διαβατηρίων, απλά περπατάει σε ένα περίπτερο και κοιτάει μία κάμερα. Το λογισμικό στη συνέχεια σαρώνει την ίριδα και ταιριάζει τα δεδομένα των ματιών του με τις πληροφορίες που είναι αποθηκευμένες στη βάση δεδομένων.

- **Μετανάστευση και πολιτογράφηση**

Το Σύστημα Υπηρεσιών Μετανάστευσης και Πολιτογράφησης (INSPASS) είναι εγκατεστημένο σε όλα τα μεγάλα αεροδρόμια των ΗΠΑ. Χρησιμοποιεί τεχνολογία επαλήθευσης γεωμετρίας χεριών μειώνοντας σημαντικά το χρόνο επεξεργασίας της μετανάστευσης. Το αεροδρόμιο Ben Gurion του Τελ Αβίβ στο Ισραήλ, επίσης χρησιμοποιεί κιόσκι εισόδου Express Card, το οποίο είναι εξοπλισμένο με την τεχνολογία της γεωμετρίας χεριών για την ασφάλεια και το μεταναστευτικό.

- **Βιομετρία στην οδήγηση**

Υπολογίζεται ότι πάνω από δύο εκατομμύρια αυτοκίνητα στο Ηνωμένο Βασίλειο χρησιμοποιούν βιομετρική τεχνολογία για να ξεκλειδώσουν τα αυτοκίνητά τους και να ξεκινήσουν τους κινητήρες τους. Οι κατασκευαστές αυτοκινήτων χρησιμοποιούν αναγνώριση φωνής μέσω Bluetooth για να εξατομικεύσουν συστήματα ψυχαγωγίας και έχουν αναγνώριση δακτυλικών αποτυπωμάτων στις λαβές των θυρών καθώς και σε μέρη όπου το παραδοσιακό κλειδί θα εισαχθεί για να ξεκλειδώσει το όχημα.

- **Διαδικτυακή ταυτοποίηση τραπεζών**

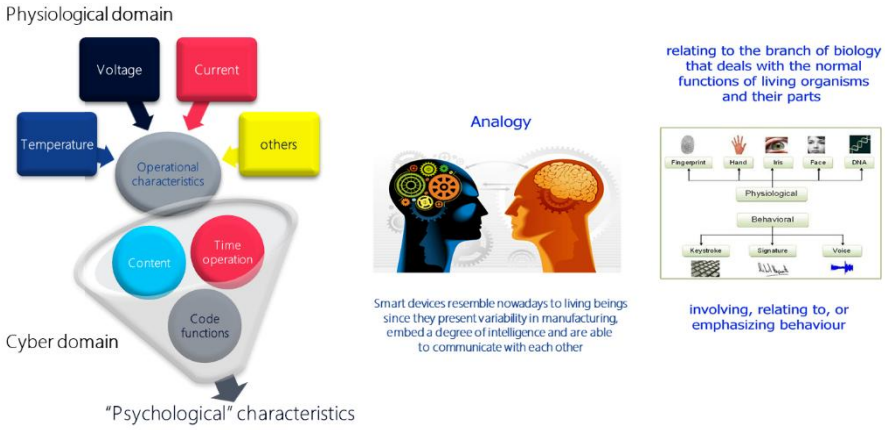
Οι πελάτες των τραπεζών μπορούν πλέον να χρησιμοποιούν την τεχνολογία δακτυλικών αποτυπωμάτων και αναγνώρισης προσώπου για να συνδεθούν στους διαδικτυακούς τραπεζικούς λογαριασμούς τους, αισθανόμενοι την αύξηση της ασφάλειας των πληρωμών. Ακολουθώντας αυτά τα βήματα της βιοτεχνολογίας, αντικαταστάθηκε το παλιό σύστημα που βασίζονταν στον κωδικό πρόσβασης και υιοθετήθηκε η τεχνολογία αναγνώρισης δακτυλικών αποτυπωμάτων και για εφαρμογές mobile banking. Οι πελάτες των χρηματοπιστωτικών ιδρυμάτων, μπορούν πλέον να επαληθεύουν τις μεταφορές χρημάτων χρησιμοποιώντας τον ενσωματωμένο αισθητήρα δακτυλικών αποτυπωμάτων στις συσκευές τους Android ή iOS.

4.1.4 Η λειτουργία μίας IoT συσκευής

Στις μέρες μας, η Εποχή της Πληροφορίας υποχωρεί στην Εποχή της Βιολογίας, καθώς υπέροχες ιδέες προκύπτουν από την απλή παρατήρηση του ζωντανού κόσμου. Μία από αυτές τις λύσεις που εμπνέονται από τη φύση, ενέπνευσε και την παρούσα διατριβή. Το τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική θεραπεύει παρόμοια προβλήματα, καθόσον συνδυάζει την Επιστήμη της Πληροφορικής με τη Βιολογία. Η ιδέα έρχεται να παρομοιάσει μία «έξυπνη συσκευή», ως ένα ζωντανό οργανισμό, ένα έμβιο ον, ώστε να εντοπίσει τυχόν «ιώσεις» που θα βλάψουν αυτή τη συσκευή. Ο παραλληλισμός αυτός, μας δίνει τη δυνατότητα να μελετήσουμε τη συσκευή σε άλλο επίπεδο και να εξάγουμε χρήσιμα συμπεράσματα προς όφελος της επιστημονικής κοινότητας αλλά και γενικότερα της ευρύτερης κοινωνίας, καθώς και να αξιοποιήσουμε τεχνικές άλλων επιστημονικών πεδίων.

Η υπόθεση είναι ότι, όπως ένας υγιής ανθρώπινος οργανισμός έχει συγκεκριμένη συμπεριφορά, έτσι και μία «υγιή έξυπνη συσκευή», έχει τη δική της συγκεκριμένη λειτουργική συμπεριφορά, εφ’ εξής φυσιολογική/κανονική συμπεριφορά. Στην περίπτωση που ο ανθρώπινος οργανισμός μολυνθεί από κάποιο ιό, παρουσιάζει εμφανή συμπτώματα όπως: βήχας, αύξηση θερμοκρασίας σώματος (πυρετός), φτέρνισμα κ.λπ. Καθώς τα παραπάνω απαιτούν επιπλέον ενέργεια, ταυτόχρονα αλλάζει και η συμπεριφορά του και ενεργοποιείτε το ανοσοποιητικό του σύστημα. Αντίστοιχα και στην περίπτωση που η «έξυπνη συσκευή» μολυνθεί από κάποιον ιό, παρουσιάζει ορισμένα συμπτώματα – ανωμαλίες, εφ εξής μη φυσιολογική/ανώμαλη

συμπεριφορά. Η λειτουργική της συμπεριφορά αναμένεται ότι θα αλλάξει καθώς απαιτείτε επιπλέον ενέργεια ως αποτέλεσμα της επίθεσης και έτσι ενεργοποιείται ο μηχανισμός της άμυνάς της.



Εικόνα 3: Σύλληψη ιδέας

Στην παραπάνω Εικόνα, φαίνεται η αναλογία της λειτουργίας μιας συσκευής, η οποία επηρεάζεται από τις εισόδους της (φυσικό επίπεδο – φυσιολογικές εισόδους) και τη συμπεριφορά της (εγγενής κώδικας), με τη βιομετρία στον άνθρωπο. Κάθε διαταραχή μπορεί να οφείλεται σε πλήθος παραγόντων, όπως μια δικτυακή επίθεση, το ακατάλληλο περιβάλλον λειτουργίας, μια βλάβη κ.ο.κ. Όσο πιο απλή η λειτουργία της συσκευής (μετρημένη σε processes) τόσο πιο εύκολη η αναγνώριση της αιτίας. Η προσέγγιση είναι συμπτωματολογική και επιτρέπει την ανίχνευση μιας μη αναμενόμενης συμπεριφοράς με την εμφάνισή της, σε αντίθεση με τις υπάρχουσες προσεγγίσεις οι οποίες βασίζονται σε προχαρακτηρισμένες τιμές (κατώφλι ή εύρος τιμών). Οι μέθοδοι που ενέπνευσαν αυτή την προσέγγιση είναι η Ανάλυση Ισχύος (Power Analysis - PA), η Διαφορική Ανάλυση Ισχύος (Differential Power Analysis - DPA) αλλά και η δοκιμή λειτουργίας μέσω ρεύματος (current based testing – π.χ. IDDQ [2]). Σε όλες τις προαναφερθείσες περιπτώσεις η προσέγγιση αφορά μια συσκευή που λειτουργεί ορθά και μέσω των προαναφερθέντων προσεγγίσεων εξάγουμε συμπεράσματα για τη λειτουργία που επιτελούν. Η προτεινόμενη προσέγγιση είναι η αντίθετη, δηλαδή η εφαρμογή μιας παραλλαγής τους για την ανίχνευση μιας μη αναγνωρίσιμης λειτουργίας.

4.1.5 Μέθοδοι εξαγωγής πληροφορίας για τη λειτουργία

- **Κατώφλι**

Η λέξη κατώφλι χρησιμοποιείται σε πάρα πολλές περιπτώσεις και σε διάφορες επιστήμες, όπως στη φυσική, στη βιολογία και στην ψυχολογία, για να υποδηλώσει τον ελάχιστο βαθμό έντασης τον οποίο πρέπει να φτάσουν διάφοροι τύποι φυσικής, χημικής ή ψυχοφυσικής ενέργειας, ώστε να καταστεί δυνατή η εκδήλωση ορισμένων φαινομένων.

Υπάρχουν διάφοροι τύποι κατωφλιού, ανάλογοι είτε με τους διάφορους τύπους ερεθισμάτων είτε με τα αποτελέσματά τους. Ο όρος κατώφλι υποδηλώνει την ελάχιστη ένταση ερεθίσματος που είναι αναγκαία για να προκληθεί κάποια αντίληψη του ερεθίσματος αυτού. Η ένταση αυτή, που ονομάζεται απόλυτο κατώφλι, αντιστοιχεί προς το όριο που χωρίζει τα αντιληπτά ερεθίσματα (υπεροριακά ή άνω του κατωφλίου) από εκείνα που δεν είναι αντιληπτά (υποοριακά ή κάτω του κατωφλίου). Ένα πολύ αδύνατο σήμα, για παράδειγμα (ώστε να μη γίνεται αντιληπτό), είναι κάτω από το απόλυτο κατώφλι. Αντίθετα, διαφορικό κατώφλι είναι η ελάχιστη μεταβολή έντασης που απαιτείται για να κάνει αντιληπτή τη διαφορά ανάμεσα σε δύο ερεθίσματα.

- **Όρια**

Η μέθοδος των ορίων περιοχών, έχει ως στόχο να ορίζει τη μέγιστη και την ελάχιστη τιμή, χρησιμοποιώντας ορισμένες μετρήσεις. Το φυσικό χαρακτηριστικό το οποίο χρησιμοποιείται στην παρούσα διατριβή προς μέτρηση, είναι η τάση του ρεύματος.

Για να καταστεί δυνατό να αξιοποιηθεί κατά το μέγιστο η πληροφορία που προκύπτει από το παραπάνω φυσικό χαρακτηριστικό, πραγματοποιείται βελτίωση της αναλογίας σήματος προς θόρυβο (SNR ή S/N) με έναν αλγόριθμο κινούμενου παραθύρου για την εξομάλυνση των αποκλίσεων του σήματος. Με αυτόν τον τρόπο, οι αιχμές οι οποίες μπορεί να προκύψουν κατά τις μετρήσεις, εξαλείφονται όταν εμφανίζονται (σπάνια), ενώ διατηρείται μία συχνότερη εμφάνιση αιχμών κατά την περίπτωση ανίχνευσης ανωμαλίας.

Αυτή η τεχνική εξομάλυνσης σημάτων ονομάζεται κινούμενος μέσος όρος. Από την αρχική ακολουθία δεδομένων [y_1, y_2, ..., y_N], δημιουργήθηκε μία αντίστοιχη ομαλή ακολουθία δεδομένων. Το εξομαλυσμένο σημείο $(y_k)_s$ είναι ο μέσος όρος ενός περιττού αριθμού 2n +1 (n = 1, 2, 3, ..) των μη επεξεργασμένων ακολουθιών δεδομένων y_{k-n}, y_{k-n+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+n-1}, y_{k+n}, δηλαδή:

$$(y_k)_s = \sum_{i=-n}^{i=n} y_{k+i}/(2n+1) \quad (1)$$

Ο αριθμός 2n + 1 είναι το πλάτος του παραθύρου. Όσο μεγαλύτερο είναι το πλάτος του παραθύρου, τόσο πιο έντονη η εξομάλυνση. Το SNR μπορεί να βελτιωθεί περαιτέρω αυξάνοντας το πλάτος του παραθύρου ή με το πέρασμα πολλαπλών παραθύρων (εξομάλυνση σε ήδη εξομαλυσμένα σημεία). Κατά τη διάρκεια μέσης επεξεργασίας κινούμενων παραθύρων, πραγματοποιείται επίσης υπολογισμός αιχμών, συγκρίνοντας την τιμή y_k με τα όρια $y_{thres.max}$ και $y_{thres.min}$. Αν υποθέτουμε ότι η ακίδα είναι θετική, δηλαδή το σήμα ανεβαίνει, τότε το sp_k ορίζεται σε 1 μόνο για την περίπτωση αυτή το y_k είναι μεγαλύτερο από το $y_{thres.max}$. Το sp_k είναι επίσης ρυθμισμένο στο 1 σε περίπτωση που η ακίδα είναι αρνητική, δηλαδή το σήμα είναι φθίνον και το y_k είναι μικρότερο από $y_{thres.min}$. Στη συνέχεια, το τελικό πλήθος των αιχμών υπολογίζεται σε ένα παράθυρο χρόνου με περιττό αριθμό δειγμάτων, π.χ. 2m+1, όπου m » n.

$$sp_k = \begin{cases} 1 & if\ y_k > y_{thres.max}\ and\ y_k - y_{k-1} > 0, \\ 1 & if\ y_k < y_{thres.min}\ and\ y_k - y_{k-1} < 0, \\ 0 & if\ otherwise \end{cases} \quad (2)$$

όπου το δείγμα k-th έχει τιμή y_k, η οποία συγκρίνεται με το κατάλληλο όριο $y_{thres.max}$ ή $y_{thres.min}$, αντίστοιχα, στην προηγούμενη τιμή του. Ο υπολογισμός πραγματοποιείται για 2m + 1 δείγματα y_{k-m}, y_{k-m+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+m-1}, y_{k+m}, όπου m » n. Στη συνέχεια, μία πρόχειρη εκτίμηση των αναγνωρισμένων αιχμών στα διαδοχικά δείγματα 2m+1 εκτελούνται με την ακόλουθη εξίσωση:

$$spikes = \sum_{i=-m}^{i=m} sp_{k+i} \quad (3)$$

Η επιλογή των m, n, $y_{thres.max}$ και $y_{thres.min}$ στην παρούσα διατριβή θεωρήθηκε ως πληροφορία που δόθηκε από τον κατασκευαστή της συσκευής IoT. Η τυπική τιμή για το m είναι 5000 και για το n είναι 20. Τα όρια που ορίστηκαν για το συναγερμό επιλέχθηκε να είναι 50 προκειμένου να αποφευχθούν αρνητικά θετικά λόγω τυχαίων αιχμών που προέρχονται από το ενεργειακό δίκτυο.

- **Πρότυπο (Pattern)**

Ένα πρότυπο (pattern) είναι μία κανονικότητα στον κόσμο ή σε αφηρημένες έννοιες. Αν για παράδειγμα μιλάμε για βιβλία ή ταινίες, η περιγραφή ενός είδους θα ήταν ένα πρότυπο. Προκειμένου η μηχανή να αναζητήσει μοτίβα δεδομένων, θα πρέπει να τα προεπεξεργαστεί και να τα μετατρέψει σε μορφή που ο υπολογιστής μπορεί να κατανοήσει. Εν συνεχεία, ο ερευνητής μπορεί να χρησιμοποιήσει αλγόριθμους ταξινόμησης, παλινδρόμησης ή ομαδοποίησης ανάλογα με τις διαθέσιμες πληροφορίες που σχετίζονται με το πρόβλημα, ώστε να πάρει πολύτιμα αποτελέσματα. Ένας από τους αλγορίθμους που χρησιμοποιήθηκε στην παρούσα διατριβή, είναι ο αλγόριθμος ομαδοποίησης. Ένας αλγόριθμος μη εποπτευόμενης μάθησης, όπου χωρίζει τα δεδομένα σε έναν αριθμό συστάδων με βάση την ομοιότητα των χαρακτηριστικών. Με αυτό τον τρόπο επιτυγχάνεται η ταξινόμηση των λειτουργιών μίας έξυπνης συσκευής και δημιουργείται το πρότυπο της κανονικής της λειτουργίας.

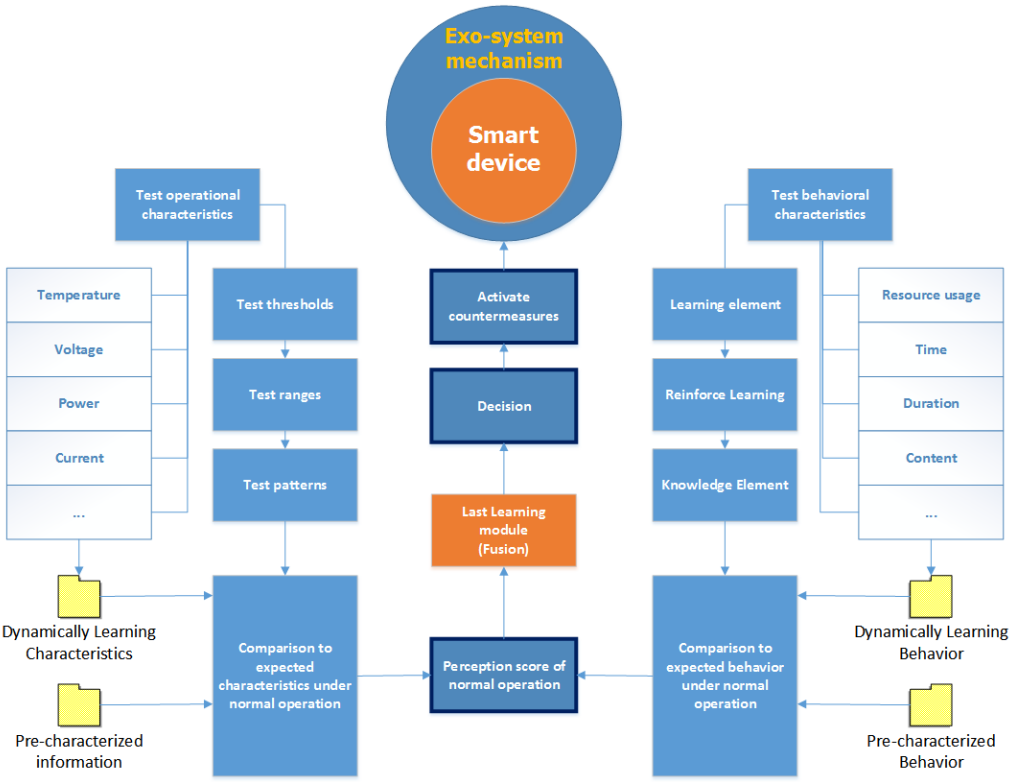
- **Συμπεράσματα**

Η υπόθεση που γίνεται σε αυτή τη διατριβή είναι ότι οποιαδήποτε συσκευή έχει τα δικά της φυσικά χαρακτηριστικά λειτουργίας, τα οποία καταναλώνουν μία προκαθορισμένη ποσότητα ισχύος. Έτσι, όταν συμβαίνει μία επίθεση ή παρατηρείται ανώμαλη συμπεριφορά, η μέτρηση του ρεύματος εντοπίζει ένα διαφορετικό προφίλ λειτουργίας (υπερβολική χρήση των πόρων επικοινωνίας και επεξεργασίας). Ένα άλλο αξιοσημείωτο γεγονός το οποίο πρέπει να αναφερθεί, είναι οι περιβαλλοντικές συνθήκες οι οποίες διαφέρουν ανά τον κόσμο. Η κάθε έξυπνη συσκευή πιθανόν να έχει τη δική της συμπεριφορά αναλόγως των περιβαλλοντικών συνθηκών. Άλλο ένα κενό που έρχεται να καλύψει η παρούσα διατριβή, καθώς ο παραπάνω τρόπος προτυποποίησης που αναφέρθηκε, αφορά σε κάθε συσκευή ξεχωριστά.

Η δυναμική απόκριση σε μη μοντελοποιημένες συμπεριφορές και η προσαρμοστικότητα της συσκευής για την ανίχνευση οποιαδήποτε επίθεσης, είναι ορισμένα από τα χαρακτηριστικά τα οποία μπορούν να ξεχωρίσουν αυτή τη διατριβή.

4.2 Προτεινόμενη Αρχιτεκτονική

Η αρχιτεκτονική του προτεινόμενου συστήματος είναι αυτή που φαίνεται στο παρακάτω σχήμα.



Εικόνα 4: Αρχιτεκτονική Συστήματος

Ένα ηλεκτρονικό κύκλωμα τοποθετείται σε κάθε συσκευή υπό παρακολούθηση, για την οποία αναλύονται τόσο η φυσιολογική λειτουργία όσο και η συμπεριφορά. Ως φυσιολογική λειτουργία γίνεται αναφορά στις εισόδους του, οι οποίες αφορούν φυσικά μεγέθη όπως ρεύμα, θερμοκρασία κατανάλωση κλπ τα οποία συλλέγονται με κατάλληλους αισθητήρες. Υπάρχει η δυνατότητα προχαρακτηρισμού από τον κατασκευαστή ή η δημιουργία ενός σετ εκμάθησης. Ως φυσιολογική συμπεριφορά αναφέρεται η λειτουργία που οφείλεται στην εκτέλεση του εγγενούς κώδικα και αφορά παραμέτρους όπως ο χρόνος, η δικτυακή κίνηση, η αξιοποίηση πόρων κλπ.

Και σε αυτή την περίπτωση είναι υποθετικά δυνατός ο προχαρακτηρισμός ή η δυναμική εκμάθηση.

Η απόκλιση από την αναμενόμενη λειτουργία, αντιμετωπίζεται ως σύμπτωμα, το οποίο μελετάται στη συνέχεια. Εφόσον επιμένει τότε αναγνωρίζεται μια συστηματική προσπάθεια αλλαγής της λειτουργίας οπότε και ενεργοποιείται το πρωτόκολλο αντιμετώπισης. Σε περίπτωση που δεν επαναλαμβάνεται η περίεργη συμπεριφορά, τότε αντιμετωπίζεται ως τυχαίο γεγονός και αγνοείται.

Ως βασικό πρωτόκολλο αντιμετώπισης επιλέχτηκε ο αποκλεισμός δια της αποσύνδεσης από την παροχή ρεύματος. Το προτεινόμενο σύστημα παρακολούθησης τοποθετείται inline (σε σειρά) όπως τα ups, οπότε απομονώνει τη συσκευή υπό παρακολούθηση. Το πρωτόκολλο είναι ίδιο με αυτό της πανδημίας, καθώς η επίδραση ενός botnet σε ένα δίκτυο έχει ακριβώς αυτή την εξάπλωση.

5 ΠΕΙΡΑΜΑΤΑ

5.1 Μεθοδολογία και Τεχνολογία Πειραμάτων

5.1.1 Μέθοδοι

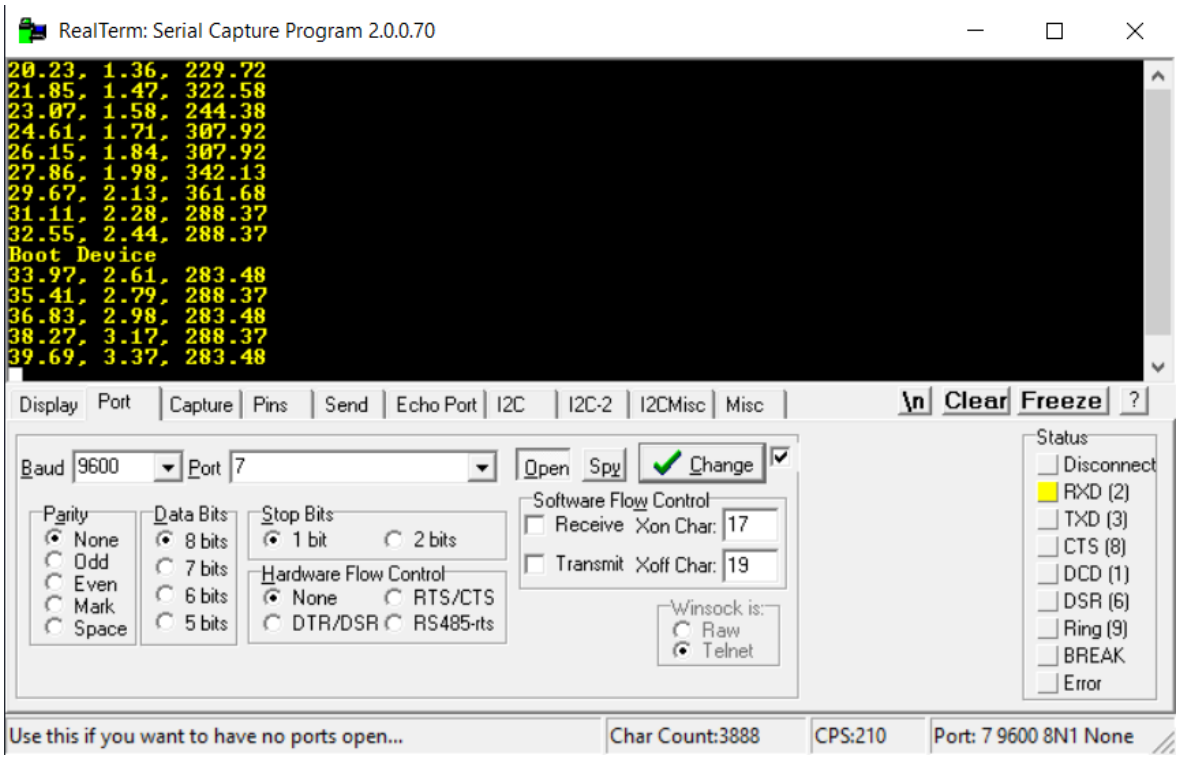
Για τον καθορισμό κοινών εφαρμογών και τεχνολογιών επικοινωνίας που χρησιμοποιούνται από τις συσκευές IoT, καθώς και των απαιτήσεων για τις τεχνολογίες ασύρματης επικοινωνίας και ασφάλειας αυτών, αναλύθηκε το υπόβαθρο και σχετικά έργα, που σηματοδοτούν την αιχμή του δόρατος του Διαδικτύου των Πραγμάτων. Η σύγκριση τεχνολογιών ασύρματης επικοινωνίας χαμηλής ισχύος, χαμηλού εύρους ζώνης σχετίζονται με την ασφάλεια, την απόδοση και την κατανάλωση ενέργειας των περιορισμένων συσκευών IoT.

Παρουσιάζεται μία τεχνολογική μελέτη μικροελεγκτών, με το σχεδιασμό του κυκλώματος, τη μοντελοποίηση συστήματος IDS βασισμένο σε μικροελεγκτή με διαχείριση λειτουργίας εκπαιδεύσεως και τέλος η αυτοματοποιημένη ανίχνευση εισβολής. Πειράματα με μικροελεγκτές για τον προσδιορισμό του χρόνου εκτέλεσης και την ανίχνευση των εισβολών σε πραγματικό χρόνο. Προσομοίωση και μετρήσεις της εντάσεως του ρεύματος στο χρόνο εκτέλεσης, χρησιμοποιώντας το παρακάτω υλικό και λογισμικό των πειραμάτων καθώς και εργαστηριακό εξοπλισμό, (ψηφιακό πολύμετρο, αισθητήρες, κ.λπ.) κατά τη μετάδοση των δεδομένων σε διαφορετικά επίπεδα ασφάλειας (χωρίς ή με κρυπτογράφηση). Ανάλυση των αποτελεσμάτων για διερεύνηση συσχέτισης μεταξύ ασφάλειας, εντάσεως ρεύματος και απόδοσης του συστήματος. Διερεύνηση αλγορίθμων μηχανικής μάθησης για την απόδοση του βέλτιστου αποτελέσματος καθώς και την αυτοματοποίηση του συστήματος.

5.1.2 Λογισμικό πρόγραμμα RealTerm

Για τη λήψη και τον εντοπισμό σφαλμάτων των ροών δεδομένων στη σειριακή επικοινωνία χρειαζόμαστε λογισμικό παρακολούθησης, το οποίο ονομάζεται σειριακό τερματικό. Για να είμαστε λίγο πιο ακριβείς, τα σειριακά τερματικά είναι εργαλεία λογισμικού που χρησιμοποιούνται για αναπτυξιακούς σκοπούς και εντοπισμό σφαλμάτων. Είναι χρήσιμα για την αποστολή και λήψη δεδομένων που

αποστέλλονται από πρωτόκολλα σειριακής επικοινωνίας, κυρίως RS-232 ή UART. Ένα από αυτά τα προγράμματα που χρησιμοποιήθηκε και στην παρούσα διδακτορική διατριβή είναι το RealTerm (Εικόνα 5). Μπορεί να χρησιμοποιηθεί για παρακολούθηση, έλεγχο και προβολή σειριακών δεδομένων. Το όνομα «τερματικό» προέρχεται από παλαιότερο τερματικό υπολογιστή που χρησιμοποιήθηκε για την εισαγωγή και ανάκτηση δεδομένων. Το παρόν λογισμικό τερματικού μιμείται την ίδια εμπειρία. Το RealTerm είναι πλούσιο σε χαρακτηριστικά, καθώς μπορεί να εμφανίσει δεδομένα σε διαφορετικές μορφές, όπως ASCII, ANSI, Hex, ακέραιος (8 bit και 16 bit), Binary, Nibble και float. Μόλις ο χρήστης εξοικειωθεί με τη διεπαφή RealTerm, χρησιμοποιεί αυτό το εργαλείο για όλους τους σκοπούς εντοπισμού σφαλμάτων. Έχει επιλογές όπως, λήψη δεδομένων σε αρχείο, αποθήκευση ως hex, καθώς και τη δυνατότητα να προσθέσει χρονικές σημάνσεις σε διαφορετικές μορφές. Μπορεί να στείλει συμβολοσειρές δεδομένων σε διαφορετικές μορφές και διαφορετικούς χαρακτήρες στο τέλος της γραμμής, οι οποίοι δύναται να προστεθούν εύκολα. Το RealTerm είναι ένα πρόγραμμα λογισμικού ανοιχτού κώδικα και διατίθεται δωρεάν για χρήση και διανομή.



Εικόνα 5: Περιβάλλον RealTerm

5.1.3 Λογισμικό πρόγραμμα Kst Plot

Το Kst Plot (Εικόνα 6) είναι από τα γρηγορότερα εργαλεία σχεδίασης, σετ δεδομένων σε πραγματικό χρόνο, καθώς διαθέτει ενσωματωμένη λειτουργία ανάλυσης δεδομένων. Το Kst Plot περιέχει πολλές ισχυρές ενσωματωμένες δυνατότητες και μπορεί να επεκταθεί με διάφορες προσθήκες και επεκτάσεις. Το Kst Plot έχει άδεια χρήσης βάσει της GPL και διατίθεται ελεύθερα για όλους. Επιπλέον, από την έκδοση 2.0.x είναι διαθέσιμο στα λειτουργικά συστήματα: Microsoft Windows, Linux, Mac OSX.

5.1.3.1 Χαρακτηριστικά του Kst Plot:

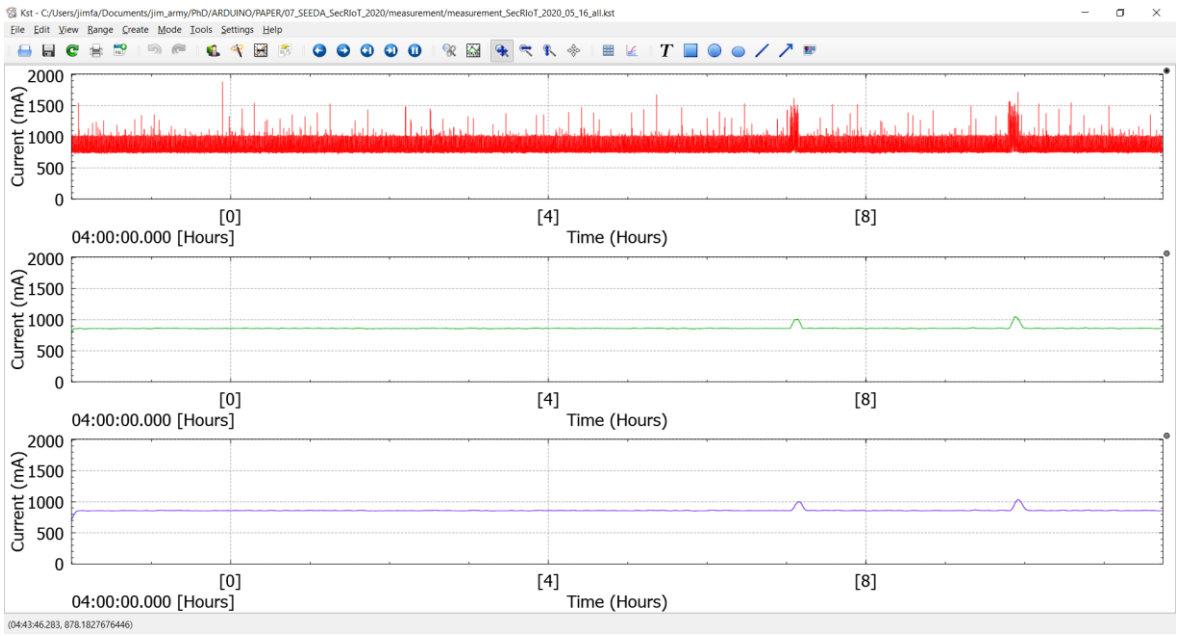
Τα χαρακτηριστικά του περιλαμβάνουν:

- Σχεδίαση «ροής» δεδομένων σε πραγματικό χρόνο.
- Χειρισμός γραφήματος με πληκτρολόγιο και ποντίκι.
- Υποστήριξη από προσθήκες και επεκτάσεις.
- Πλήθος επιλογών ενσωματωμένων λειτουργιών σχεδίασης και χειρισμού δεδομένων, όπως ιστογράμματα, εξισώσεις και φάσματα ισχύος.
- Δυνατότητες χαρτογράφησης χρωμάτων και χαρτογράφησης περιγράμματος για τρισδιάστατα δεδομένα, καθώς και υποστήριξη μήτρας και εικόνας.
- Ενσωματωμένες δυνατότητες φιλτραρίσματος και τοποθέτησης καμπυλών.
- Φιλική διεπαφή γραμμής εντολών.
- Γραφικό περιβάλλον εργασίας χρήστη με μη τυπικούς διαλόγους για βελτιστοποιημένη ροή εργασίας.
- Υποστήριξη πολλών δημοφιλών μορφών δεδομένων.
- Πολλαπλές καρτέλες.
- Εκτεταμένα αντικείμενα σχολιασμού παρόμοια με εφαρμογές γραφικών διανυσμάτων.
- Εξαγωγή υψηλής ποιότητας σε bitmap ή διανυσματικές μορφές.
- Πλήρως σενάριο σε python (beta διατίθεται σε linux).

5.1.3.2 Αρχιτεκτονική προσθηκών

Το Kst Plot βασίζεται σε αρχιτεκτονική plugin:

Οι πηγές δεδομένων είναι προσθήκες που παρέχουν υποστήριξη για νέους τύπους αρχείων. Τα πρόσθετα μπορούν εύκολα να προστεθούν για οποιονδήποτε τύπο λειτουργίας, συμπεριλαμβανομένων των προσθηκών προσαρμογής και φίλτρου. Για την επέκταση του μεγάλου αριθμού προσθηκών που βασίζονται στο GSL και έχουν ήδη διανεμηθεί με το Kst Plot, χρειάζεται εξατομικευμένη περίπτωση ανάπτυξης.



Εικόνα 6: Περιβάλλον KST Plot

5.2 Πείραμα 1ο

Σε αυτό το πείραμα, χρησιμοποιήθηκε μία εμπορική κάμερα IP. Η κάμερα είναι μία πιο περίπλοκη συσκευή που επέτρεψε τον πειραματισμό σε διάφορες συνθήκες, όπως η ροή ενός βίντεο μίας ακίνητης εικόνας, η ροή ενός βίντεο με συνεχείς και έντονες αλλαγές στις εικόνες λήψης ή ακόμη και κίνηση της ίδιας της κάμερας. Για να αποδείξουμε την ιδέα, ορίσαμε ως στόχο τον έλεγχο των αποκλίσεων της κανονικής λειτουργίας. Οποιαδήποτε απόκλιση είναι μία προειδοποίηση για την παρουσία μίας ανωμαλίας. Η κανονική λειτουργία αναφέρεται εφεξής ως κανονικό προφίλ της συσκευής.

5.2.1 Ρύθμιση πειραμάτων

Προκειμένου να εφαρμοστεί η προτεινόμενη ρύθμιση, χρησιμοποιήσαμε έναν μικροελεγκτή Arduino Uno, ο οποίος παρακολουθεί την παροχή του ρεύματος (ένταση ισχύος) της συσκευής στόχου. Η συσκευή Arduino Uno παρεμβάλλεται μεταξύ του τροφοδοτικού και της συσκευής που πρέπει να παρακολουθείται. Η συνδεσμολογία έχει ως εξής:

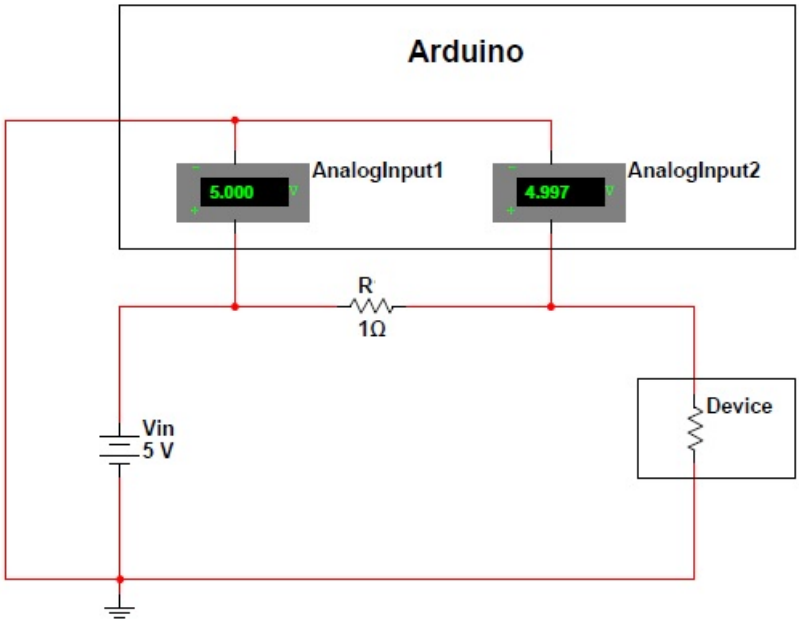
- Αρχικά, ο μικροελεγκτής Arduino Uno είναι συνδεδεμένος σε έναν προσωπικό υπολογιστή. Ο κώδικας που έχει αναπτυχθεί για το σκοπό παρακολούθησης της εντάσεως του ρεύματος, φορτώνεται στη μνήμη του Arduino Uno. Το Arduino Uno βασίζεται σε μικροεπεξεργαστή AVR.
- Το κύκλωμα παρακολούθησης έχει υλοποιηθεί σε διάτρητη πλακέτα. Περιλαμβάνει μικρή αντίσταση του 1 Ohm, που χρησιμοποιείται για λόγους ακρίβειας στη βαθμονόμηση. Η αντίσταση βρίσκεται μεταξύ των δύο εισόδων του μικροελεγκτή για να μετρηθεί η ένταση. Η ένταση ισχύος μπορεί να υπολογιστεί μέσω της μέτρησης της τάσης στα δύο σημεία εισόδου, σύμφωνα με τον ακόλουθο τύπο:

$$I = \frac{V2 - V1}{R} \quad (4)$$

όπου V1 και V2 είναι οι δύο τάσεις αναφοράς όπως απεικονίζονται στην Εικόνα 7, και R είναι η αντίσταση 1 Ohm.

Στη συνέχεια, δύο αναλογικές είσοδοι του Arduino Uno, δηλαδή το A4 και το A5, είναι συνδεδεμένες στο κύκλωμα μέσω της διάτρητης πλακέτας, προκειμένου να συλλεχθούν οι μετρήσεις του ρεύματος. Η είσοδος A4 συνδέεται με το σημείο πριν από την αντίσταση, ενώ η είσοδος A5 μετρά την τάση στο άλλο άκρο της αντιστάσεως. Για την αποφυγή βραχυκυκλώματος ή άλλων επικίνδυνων καταστάσεων που μπορεί να προκύψουν εξαιτίας συσκευών που παρουσιάζουν δυσλειτουργία, η γείωση της διάτρητης πλακέτας συνδέεται με τη γείωση Arduino Uno (GND).

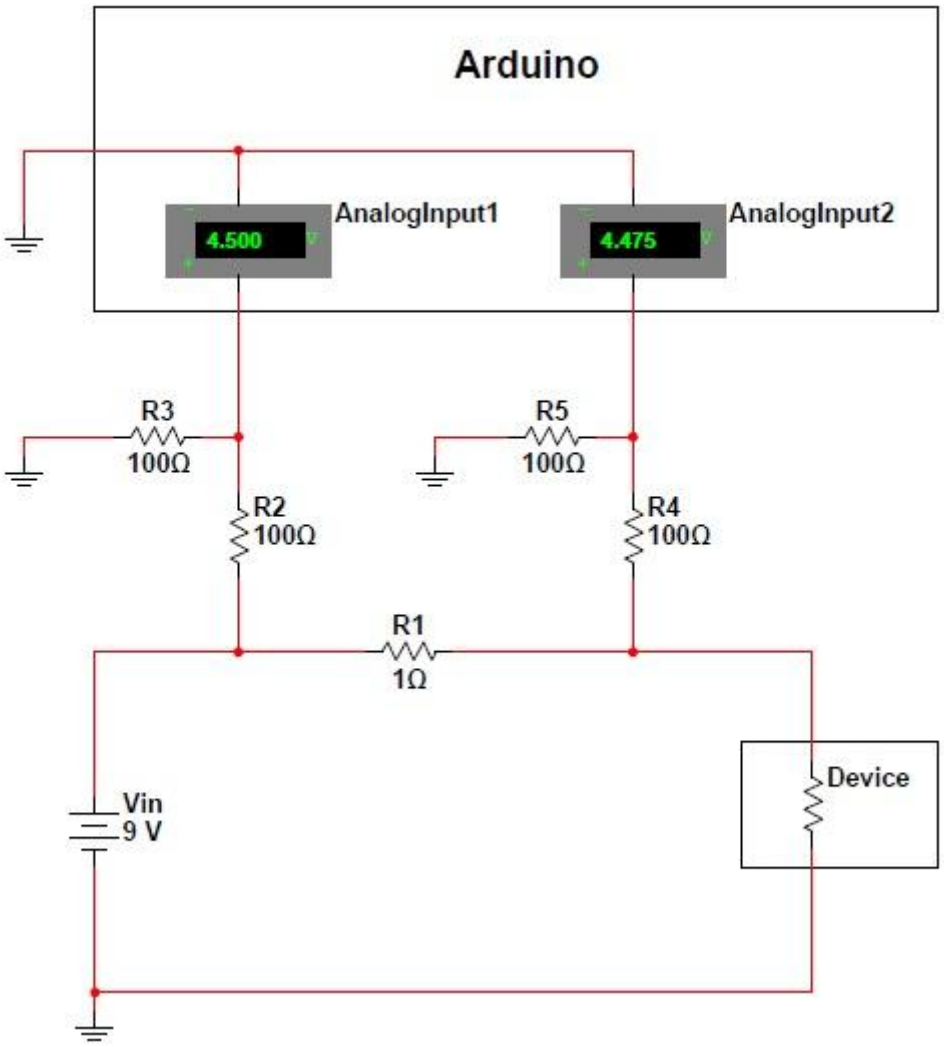
Τέλος, η συσκευή που παρακολουθείται συνδέεται σειριακά με την αντίσταση. Το κύκλωμα ολοκληρώνεται με τη σύνδεση τροφοδοσίας DC 5V στην παροχή του ρεύματος.



Εικόνα 7: Κανονικό Κύκλωμα

Για την περίπτωση που η συσκευή έχει υψηλότερη τάση ισχύος από 5 Volts (επομένως η είσοδος στο κύκλωμα είναι μεγαλύτερη από 5V), προσαρμόστηκε το κύκλωμα αναλογικής εισόδου του μικροελεγκτή Arduino Uno, και αυτό διότι δεν μπορεί να υπερισχύσει του ανώτατου ορίου 5V. Σε αυτή την περίπτωση σχεδιάστηκε μία νέα διάταξη για την αντιμετώπιση αυτών των χαρακτηριστικών του κυκλώματος.

Η νέα διάταξη του κυκλώματος αποτελείται από τέσσερις πρόσθετες αντιστάσεις 100 Ohm, οι οποίες συνθέτουν δύο διαιρέτες τάσης. Ο πρώτος διαιρέτης εφαρμόζεται στον πρώτο ακροδέκτη εισόδου A4 του κυκλώματος, πριν από την αντίσταση. Ο δεύτερος εφαρμόζεται μετά την αντίσταση, στον δεύτερο ακροδέκτη εισόδου A5 του κυκλώματος. Το αποτέλεσμα αυτής της ρύθμισης είναι η μείωση κατά το ήμισυ των δύο μετρήσεων των αναλογικών εισόδων του Arduino Uno. Η εγκατάσταση υψηλής τάσης της συσκευής παρακολούθησης απεικονίζεται στην Εικόνα 8.



Εικόνα 8: Κύκλωμα Υψηλής Τάσης

5.2.2 Μελέτη περιπτώσεων

Αυτή η μελέτη περίπτωσης IP κάμερας θεωρήθηκε ως σενάριο έξι πιθανών καταστάσεων, οι οποίες προσομοιώθηκαν και πραγματεύονται ακολούθως:

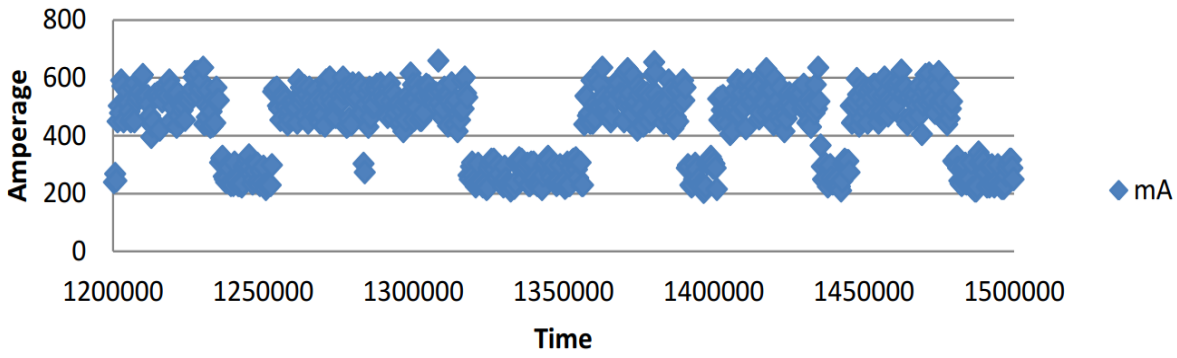
Στατική εικόνα: Σε αυτό το σενάριο, η IP κάμερα μεταδίδει μία στατική εικόνα και δεν υπάρχει πρόσθετη δραστηριότητα δικτύου. Η μέση ένταση είναι 284.38 mA.

Στατική εικόνα και DoS: Σε αυτό το σενάριο, η IP κάμερα μεταδίδει ροές ακίνητης εικόνας, ενώ επιχειρείται εναντίον της, επίθεση DoS. Ο μέσος όρος η ένταση είναι 296.89 mA.

Γρήγορη αλλαγή εικόνων: Σε αυτό το σενάριο, τοποθετούνται διάφορες εικόνες γρήγορα μπροστά από την κάμερα. Η μέση ένταση ήταν 277.60mA.

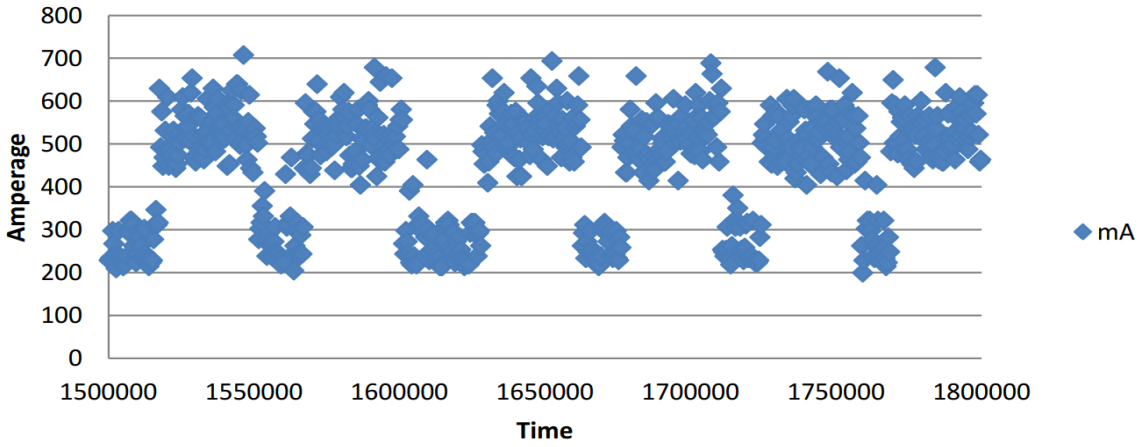
Γρήγορη αλλαγή εικόνων και DoS: Σε αυτό το σενάριο, μία επίθεση DoS επιχειρήθηκε κατά της IP κάμερας όπως το προηγούμενο σενάριο. Η μέση ένταση ήταν 288.65mA.

Σενάριο κίνησης κάμερας IP: Σε αυτό το σενάριο, υπήρχε μετακίνηση της IP κάμερας. Η μέση ένταση ήταν 434.29 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 9.



Εικόνα 9: Σενάριο κίνησης IP κάμερας

Σενάριο κίνησης κάμερας IP και DoS: Σε αυτό το σενάριο, το σενάριο κίνησης επαναλήφθηκε, ενώ μία επίθεση DoS επιχειρήθηκε ενάντια στην κάμερα IP. Η μέση ένταση ήταν 443.28μA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 10.



Εικόνα 10: Σενάριο κίνησης IP κάμερας με επίθεση DoS

Σενάριο	Κανονική	DoS	Προσαύξηση
IP κάμερα - ακίνητη εικόνα	284.38	296.8	4.37 %
IP κάμερα - εναλλασσόμενες εικόνες	277.6	288.65	3.98 %
IP κάμερα – κίνηση	434.29	443.28	2.07 %

Πίνακας 1: Μέση Ένταση (mA) των εξεταζόμενων σεναρίων 1ου πειράματος

Στον Πίνακα 1 απεικονίζονται οι τιμές για τη μέση ένταση κάθε ενός από τα σενάρια που εξετάστηκαν. Το τελευταίο έδειξε ότι υπάρχει πράγματι απόκλιση εντάσεως του ρεύματος όταν υπάρχει επίθεση DoS.

5.2.3 Συζήτηση αποτελεσμάτων

5.2.3.1 Αξιολόγηση της μέτρησης ισχύος

Για να αξιολογηθεί η εγκυρότητα των μετρήσεων, ενσωματώθηκε ένα ψηφιακό πολύμετρο για τη μέτρηση της τάσης στα ίδια σημεία. Στη συνέχεια ολοκληρώθηκαν οι συνδέσεις και οι απαραίτητες δοκιμές (ισχύς, κ.λπ.) και επαναλήφθηκαν οι ίδιες μετρήσεις με τη χρήση της προσαρμοσμένης εγκατάστασης παρακολούθησης. Τα αποτελέσματα δεν είχαν παρατηρήσιμες αποκλίσεις από αυτές του ψηφιακού πολύμετρου.

5.2.3.2 Δραστηριότητα δικτύου

Προκειμένου να αποδειχθεί ότι η παρατήρηση της δραστηριότητας δικτύου της συσκευής είναι εφικτή, εκτελέσθηκε μία Denial of Service (DoS) επίθεση. Χρησιμοποιήθηκε δέσμη ενεργειών που εκτελεί την εντολή ping (ping ip -t -l 5000) έναντι της διεύθυνσης IP της συσκευής στόχου.

Αυτό το σενάριο επαναλήφθηκε για δέκα φορές, ενώ το μέγεθος των πακέτων δεδομένων ρυθμίστηκε σε 5000 byte. Τέλος, προκειμένου να αναλυθούν δεδομένα και να αντληθούν συμπεράσματα από τις μετρήσεις, αποθηκεύτηκαν σε ένα αρχείο

καταγραφής. Οι μετρήσεις αναφέρονται σε δύο διαφορετικά σενάρια, συμπεριλαμβανομένης ή όχι της δραστηριότητας δικτύου που παράγεται από το προαναφερόμενο σενάριο.

5.2.4 Συμπεράσματα

Σε αυτό το πείραμα η απόκλιση της εντάσεως του ρεύματος συσχετίστηκε με ζητήματα αξιοπιστίας και ασφάλειας που σχετίζονταν άμεσα με συσκευές IoT και απέδειξε ότι μπορεί να εντοπιστεί ανωμαλία. Το μειονέκτημά του βρίσκεται στις μικρές αποκλίσεις (σε ποσοστό επί τοις εκατό), ωστόσο αυτό μπορεί να ξεπεραστεί με τη χρήση ειδικών φίλτρων για τον εντοπισμό αιχμών και μικρο-ρευμάτων. Η κύρια συμβολή αυτού του πειράματος είναι ότι εισάγει μία νέα τεχνική για την ανίχνευση ανωμαλιών, σε μία μη συμπτωματική προσέγγιση για την ανίχνευση της ίδιας της αιτίας.

5.3 Πείραμα 2ο

Αυτό το πείραμα παρουσιάζει μία μεθοδολογία που συσχετίζει την ένταση του ρεύματος τροφοδοσίας μίας έξυπνης συσκευής με τα λειτουργικά χαρακτηριστικά της, προκειμένου να ανιχνεύσει μία κατασκευαστική ανωμαλία ή ανωμαλία ασφαλείας σε συσκευές IoT. Αποδεικνύεται ότι η συνειδητοποίηση της τυπικής λειτουργίας μίας έξυπνης συσκευής μέσω λειτουργικών παραμέτρων (όπως η παροχή ρεύματος) μπορεί να προσφέρει πολύτιμους δείκτες ασφαλείας, καθώς οποιαδήποτε απόκλιση από τα κανονικά επιχειρησιακά όρια, μπορεί να αποτελεί ένδειξη παραβίασης ασφαλείας ή λειτουργικής ανωμαλίας.

Όπως έχει ήδη εξηγηθεί, η κύρια μεθοδολογία που παρουσιάζεται σε αυτή τη διατριβή περιλαμβάνει τη συσχέτιση των λειτουργικών φυσικών δεδομένων με την κατανάλωση ενέργειας, ως μέσο για την εξαγωγή συμπερασμάτων σχετικά με τη δραστηριότητα του δικτύου της συσκευής. Έχει διαμορφωθεί μία συσκευή ως ενδιάμεσος παρατηρητής μεταξύ της συσκευής που βρίσκεται υπό παρακολούθηση και της τροφοδοσίας αυτής. Αυτή η προσέγγιση είναι ρεαλιστική, αφού όλες οι συσκευές προσφέρουν πρόσβαση στο τροφοδοτικό τους. Το προτεινόμενο σύστημα μπορεί τελικά να χρησιμοποιηθεί για την ανίχνευση επιθέσεων κατά της συσκευής.

5.3.1 Ρύθμιση πειραμάτων

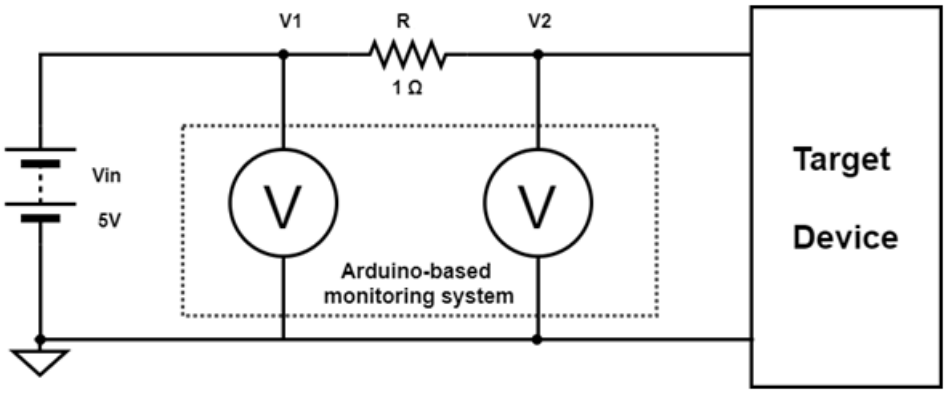
5.3.1.1 Κανονική ρύθμιση

Όπως έχει ήδη εξηγηθεί στην παρουσιαζόμενη μεθοδολογία, χρησιμοποιήθηκε μικροελεγκτής χαμηλού κόστους για την παρακολούθηση εντάσεως του ρεύματος της στοχευόμενης συσκευής. Η πλακέτα που ενσωματώνει τον μικροελεγκτή πρέπει να παρεμβάλλεται μεταξύ του τροφοδοτικού και της συσκευής που παρακολουθείται.

- Αρχικά, η πλακέτα συνδέεται με έναν προσωπικό υπολογιστή. Ο κώδικας φορτώνεται στη μνήμη του συστήματος (ενσωματωμένη επίσης στην πλακέτα).
- Η πλακέτα περιλαμβάνει επιπλέον κυκλώματα για τη μέτρηση της έντασης του ρεύματος. Συγκεκριμένα, περιλαμβάνει μία αντίσταση 1 Ohm που

χρησιμοποιείται για τον υπολογισμό της απόκλισης εντάσεως του ρεύματος κατά τη διάρκεια της κανονικής λειτουργίας, βάσει του νόμου του Ohm. Η τελευταία αντίσταση βρίσκεται ανάμεσα σε δύο αναλογικές εισόδους (συνδεδεμένες μέσω μετατροπέα A/D στον μικροελεγκτή) προκειμένου να μετρηθεί το ρεύμα. Η ένταση του ρεύματος μπορεί να υπολογιστεί σύμφωνα με τον τύπο της εξίσωσης (4).

- Όπου V1 και V2 είναι οι δύο τάσεις αναφοράς και R1 είναι η αντίσταση 1 Ohm, όπως απεικονίζονται στην Εικόνα 11: Διάταξη κυκλώματος της συσκευής παρακολούθησης.
- Δύο αναλογικές είσοδοι συνδέονται στο κύκλωμα, που αντιστοιχούν στις δύο τάσεις αναφοράς V1 και V2 αντίστοιχα (Εικόνα 11), προκειμένου να μετρηθεί η τάση στον κόμβο.
- Τέλος, η συσκευή στόχος συνδέεται σειριακά με την αντίσταση. Το κύκλωμα ολοκληρώνεται με τη σύνδεση μίας τροφοδοσίας DC 5V στην είσοδο ισχύος της συσκευής στόχου.



Εικόνα 11: Διάταξη κυκλώματος της συσκευής παρακολούθησης

5.3.2 Μελέτη περιπτώσεων

Δύο εφαρμογές θεωρήθηκαν ότι αποδεικνύουν την έννοια, δηλαδή την ανίχνευση ανωμαλιών σχετικά με την ασφάλεια μέσω της παρακολούθησης εντάσεως του ρεύματος. Η πρώτη εφαρμογή είναι ένας αισθητήρας υγρασίας και θερμοκρασίας, που χρησιμοποιεί προσαρμοσμένο υλικό ειδικά σχεδιασμένο για αυτό το σκοπό. Αποτελείται από έναν μικροελεγκτή Arduino Uno (μία πλακέτα που λειτουργεί

αυτόνομα) μαζί με τους απαιτούμενους αισθητήρες. Η δεύτερη εφαρμογή βασίζεται σε μία εμπορικά διαθέσιμη κάμερα IP για την επιτήρηση εσωτερικών και εξωτερικών χώρων. Και στις δύο περιπτώσεις η ένταση του ρεύματος των συσκευών παρατηρήθηκε για χρονικό διάστημα 5 λεπτών με ρυθμό δειγματοληψίας ένα (1) δείγμα ανά χιλιοστό του δευτερολέπτου. Σύμφωνα με τα πειράματά μας, επαληθεύσαμε ότι αυτό είναι ένα επαρκές χρονικό πλαίσιο για την ανίχνευση μίας ανωμαλίας, με βάση το προφίλ λειτουργίας και το φορτίο κίνησης δικτύου.

5.3.2.1 Συσκευή προσαρμοσμένου θερμομέτρου

Στην πρώτη μελέτη περίπτωσης, μία συσκευή θερμόμετρου υλοποιήθηκε χρησιμοποιώντας έναν μικροελεγκτή Arduino Uno, με μία ενσωματωμένη επέκταση WiFi Shield [119] και έναν αισθητήρα DHT-22 [120]. Ο μικροελεγκτής συνδέονταν με το τοπικό ασύρματο δίκτυο μέσω του WiFi Shield. Ο κώδικας που έτρεχε στη συσκευή, συνέλλεγε τις τιμές που επέστρεφε ο αισθητήρας ανά 10 δευτερόλεπτα. Όταν ήταν συνδεδεμένο στο δίκτυο, μετέδιδε τα δεδομένα. Στη συνέχεια, εμφάνιζε τη θερμοκρασία και την υγρασία του περιβάλλοντος [121].

Για τη σύνδεση του αισθητήρα DHT-22 στο Arduino Uno, χρησιμοποιήθηκαν τρεις από τις τέσσερις ακίδες του αισθητήρα. Ο πρώτος ακροδέκτης DHT-22 συνδέθηκε με την έξοδο 5V του Arduino Uno για παροχή ρεύματος. Ο δεύτερος ακροδέκτης χρησιμοποιήθηκε για τη μεταφορά δεδομένων στο Arduino Uno μέσω της ψηφιακής θύρας εισόδου του (ψηφιακό pin2). Τέλος, ο τέταρτος ακροδέκτης, ο οποίος είναι η γείωση του αισθητήρα, συνδέονταν με τη γείωση του μικροελεγκτή (GND).

Για την τροφοδοσία της συσκευής χρησιμοποιήθηκε barrel jack 2.1 mm, καθώς:

- Η πλακέτα μπορεί να λειτουργήσει υπό εξωτερικές συνθήκες ισχύος 6V - 20V, ενώ η προτεινόμενη παροχή του είναι μεταξύ 7V και 12V.
- Εάν η τροφοδοσία της πλακέτας είναι μικρότερη από 7V, η παροχή εξόδου 5V που παρέχεται στο DHT-22, μπορεί να μην είναι επαρκής και στην περίπτωση αυτή η εφαρμογή καθίσταται ασταθής.

Η τροφοδοσία της πλακέτας με 12V, μπορεί να οδηγήσει σε υπερθέρμανση του σταθεροποιητή και πιθανώς να προκαλέσει βλάβη στην πλακέτα. Έτσι, ο μετασχηματιστής που χρησιμοποιήθηκε ήταν ρυθμιζόμενος 12V και η πραγματική του απόδοση ήταν 8.18V (μετρημένος με ψηφιακό πολύμετρο στις απολήξεις του τροφοδοτικού). Με αυτό τον τρόπο το Arduino Uno μαζί με τον αισθητήρα τροφοδοτούνταν σωστά, αλλά με συνέπεια, η τάση εισόδου στο κύκλωμα να είναι 8.18V και ταυτόχρονα η απαίτηση της ισχύος της τάσης, όσον αφορά τις μετρήσεις και των δύο εισόδων της συσκευής Arduino Uno μέχρι 5V.

5.3.2.2 Εμπορική κάμερα IP

Στη δεύτερη μελέτη περίπτωσης, χρησιμοποιήθηκε μία εμπορική κάμερα IP. Καθώς η κάμερα είναι μία πιο περίπλοκη συσκευή, επέτρεπε να πειραματιστούμε σε διάφορες συνθήκες, όπως η ροή ενός βίντεο μίας στατικής εικόνας, η ροή ενός βίντεο με συνεχείς και έντονες αλλαγές στις εικόνες λήψης ή ακόμα και κίνηση της κάμερας. Η κάμερα τροφοδοτήθηκε με συνεχές ρεύμα 5V, μέσω barrel jack 2.1mm.

5.3.3 Συζήτηση αποτελεσμάτων

5.3.3.1 Αξιολόγηση της μέτρησης ισχύος

Για να αξιολογηθεί η εγκυρότητα των μετρήσεων, ενσωματώθηκε ένα ψηφιακό πολύμετρο για τη μέτρηση της τάσης στα ίδια σημεία. Στη συνέχεια ολοκληρώθηκαν οι συνδέσεις και οι απαραίτητες δοκιμές (ισχύς, κ.λπ.) και επαναλήφθηκαν οι ίδιες μετρήσεις με τη χρήση της προσαρμοσμένης εγκατάστασης παρακολούθησης. Τα αποτελέσματα δεν είχαν παρατηρήσιμες αποκλίσεις από αυτές του ψηφιακού πολύμετρου.

5.3.3.2 Δραστηριότητα δικτύου

Προκειμένου να αποδειχθεί ότι η παρατήρηση της δραστηριότητας δικτύου της συσκευής είναι εφικτή, εκτελέσθηκε μία Denial of Service (DoS) επίθεση.

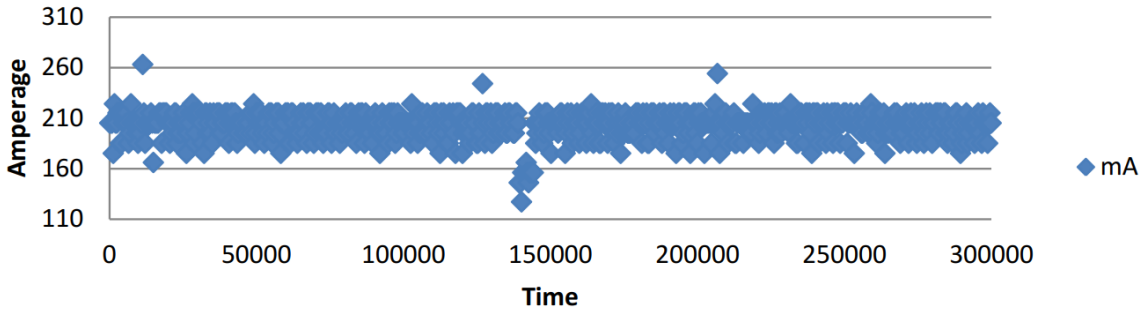
Χρησιμοποιήθηκε δέσμη ενεργειών που εκτελεί την εντολή ping (ping ip -t -l 5000) έναντι της διεύθυνσης IP της συσκευής στόχου.

Αυτό το σενάριο επαναλήφθηκε για δέκα φορές, ενώ το μέγεθος των πακέτων δεδομένων ρυθμίστηκε σε 5000 byte. Τέλος, προκειμένου να αναλυθούν δεδομένα και να αντληθούν συμπεράσματα από τις μετρήσεις, αποθηκεύτηκαν σε ένα αρχείο καταγραφής. Οι μετρήσεις αναφέρονται σε δύο διαφορετικά σενάρια, συμπεριλαμβανομένης ή όχι της δραστηριότητας δικτύου που παράγεται από το προαναφερόμενο σενάριο.

5.3.3.3 Αποτελέσματα μελέτης περίπτωσης συσκευής προσαρμοσμένου θερμόμετρου

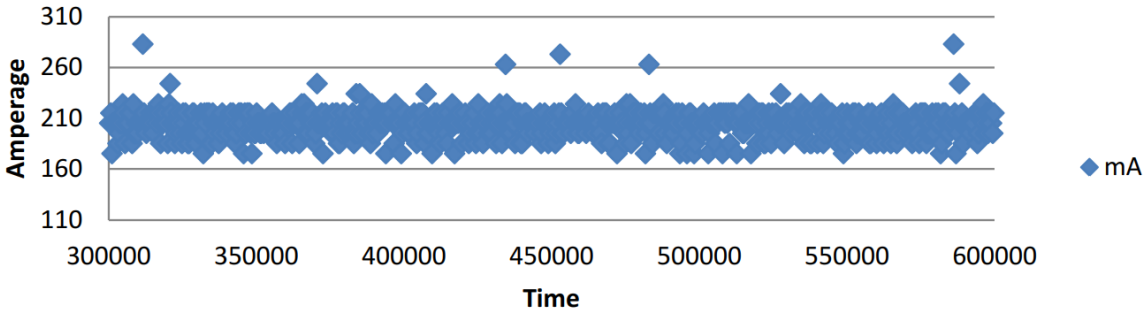
Όσον αφορά την προσαρμοσμένη συσκευή θερμόμετρου εξετάστηκαν δύο προφίλ/σενάρια:

Κανονικό προφίλ: Σε αυτό το σενάριο, η συσκευή θερμόμετρου Arduino Uno πραγματοποίησε κανονικά τη λήψη θερμοκρασίας και της υγρασίας του δωματίου. Κανένας παράγοντας εξωτερικού περιβάλλοντος δεν υπερέβη τα φυσιολογικά χαρακτηριστικά ούτε επιτελέστηκε επίθεση, προκειμένου να υπάρξει ένα προφίλ της έντασης ισχύος σε κανονικές συνθήκες λειτουργίας για λόγους σύγκρισης. Η μέση τιμή της έντασης ήταν 202.54 mA. Οι μετρήσεις απεικονίζονται στην Εικόνα 12.



Εικόνα 12: Θερμόμετρο - Κανονικό προφίλ

Προφίλ ανωμαλίας: Σε αυτό το σενάριο μία επίθεση DoS εκτελέστηκε έναντι της συσκευής θερμόμετρου Arduino Uno, ενώ εκτελούσε την κανονική λειτουργία της, συλλέγοντας δεδομένα θερμοκρασίας και υγρασίας. Οι μετρήσεις σχετικά με την ένταση ισχύος πραγματοποιήθηκαν για να παρακολουθήσουν τη δραστηριότητα δικτύου της συσκευής. Η μέση τιμή της έντασης ήταν 204.29 mA. Οι μετρήσεις παρουσιάζονται στην Εικόνα 13.

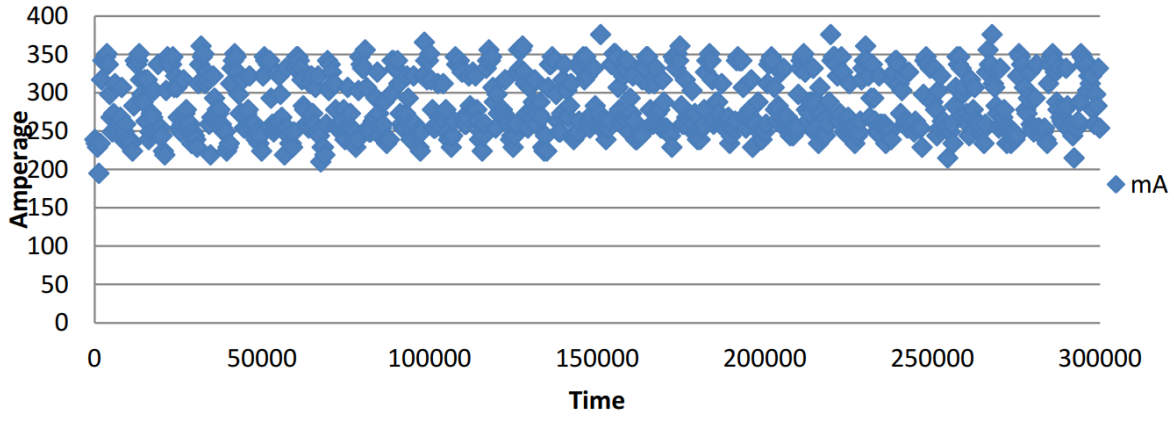


Εικόνα 13: Θερμόμετρο - με επίθεση DoS

5.3.3.4 Αποτελέσματα μελέτης περίπτωσης IP κάμερας

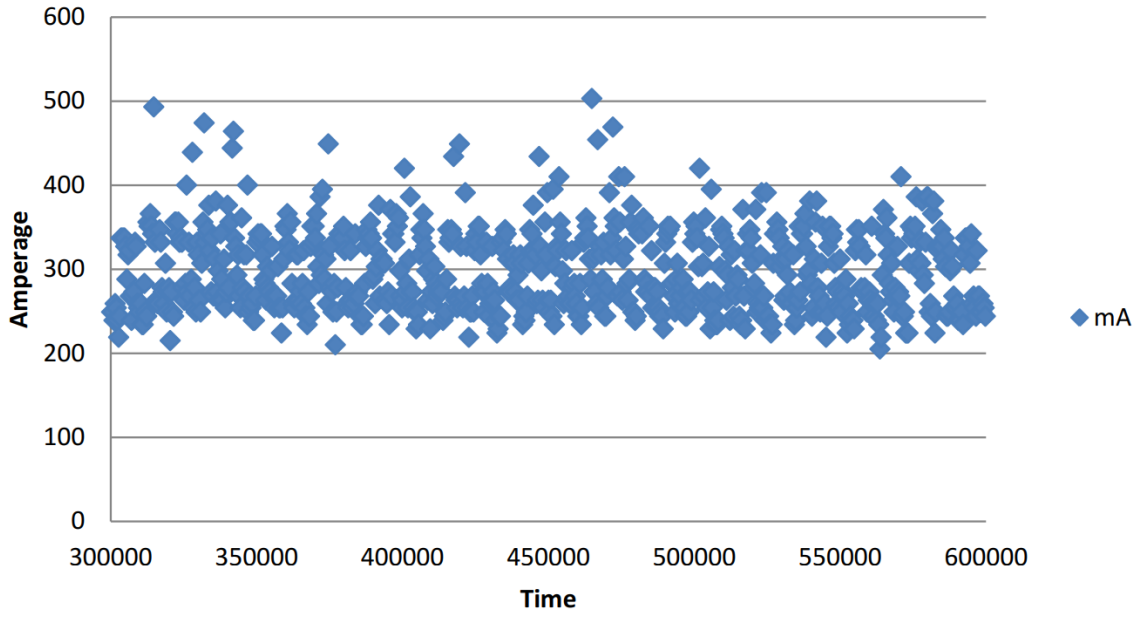
Σχετικά με την προσαρμοσμένη συσκευή κάμερας IP προσομοιώθηκαν έξι καταστάσεις:

Στατική εικόνα: Σε αυτό το σενάριο, η IP κάμερα μεταδίδει μία ακίνητη εικόνα και δεν υπάρχει επιπλέον δραστηριότητα δικτύου. Η μέση ένταση είναι 284.38 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 14.



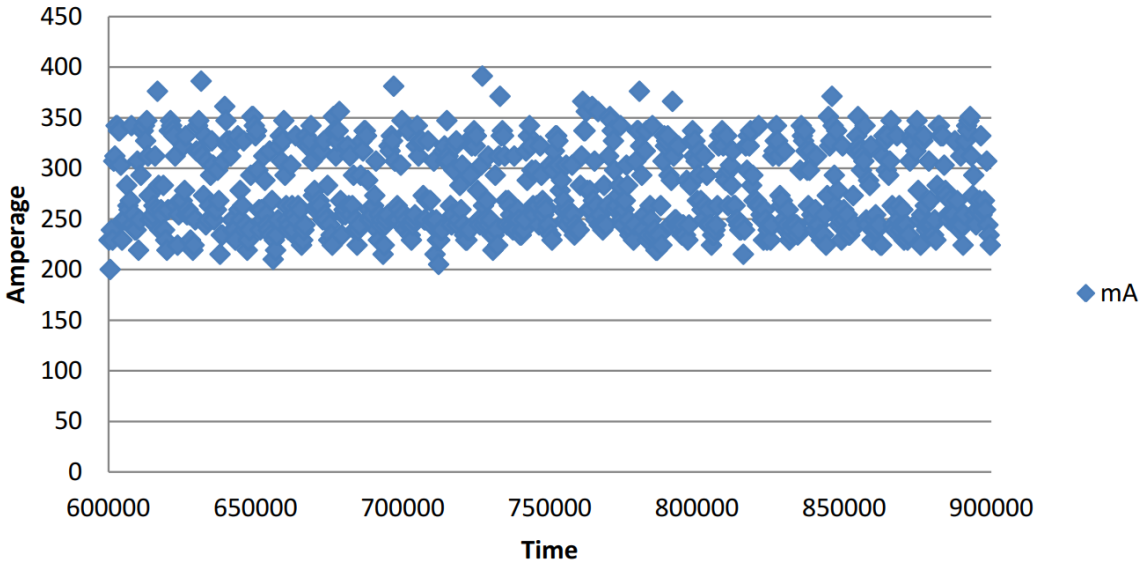
Εικόνα 14: Στατική εικόνα

Στατική εικόνα με επίθεση DoS: Σε αυτό το σενάριο, στην IP κάμερα ρέει μία στατική εικόνα, ενώ επιχειρείται μία επίθεση DOS. Η μέση ένταση είναι 296.89 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 15.



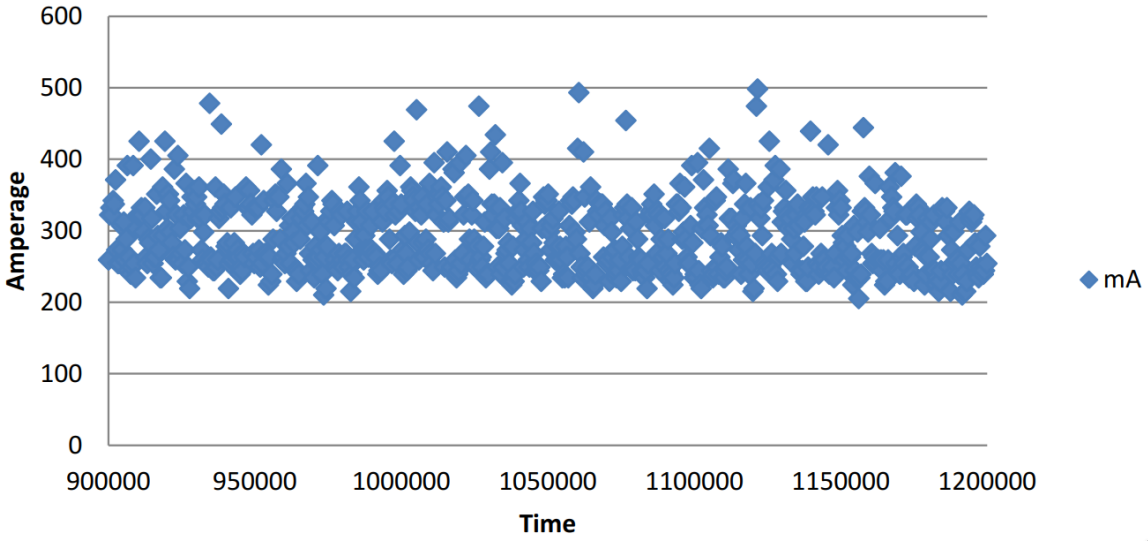
Εικόνα 15: Στατική εικόνα με επίθεση DoS

Γρήγορη εναλλαγή εικόνων: Σε αυτό το σενάριο, διάφορες εικόνες τοποθετούνται γρήγορα μπροστά από την κάμερα, προκειμένου να ενεργοποιηθεί η αλλαγή λειτουργίας. Η μέση ένταση ήταν 277.60 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 16.



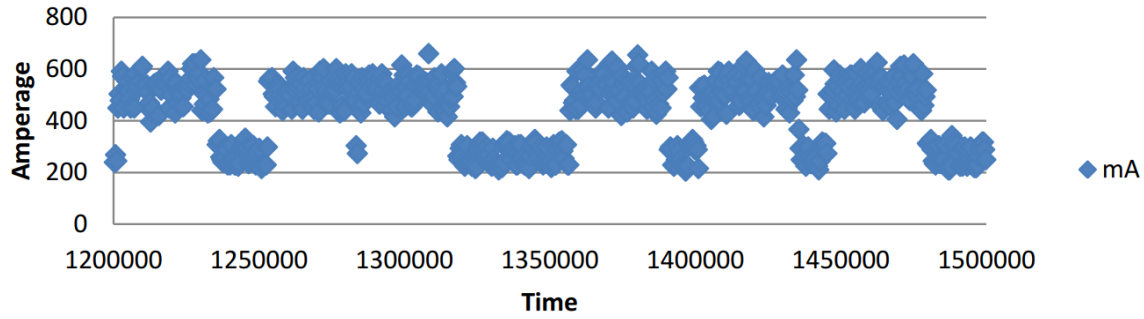
Εικόνα 16: Γρήγορη εναλλαγή εικόνων

Γρήγορη αλλαγή εικόνων με επίθεση DoS: Σε αυτό το σενάριο, συνεχίστηκε η γρήγορη εναλλαγή εικόνων μπροστά από την κάμερα IP, ενώ επιχειρήθηκε επίθεση DoS κατά της κάμερας IP. Η μέση ένταση ήταν 288.65 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 17.



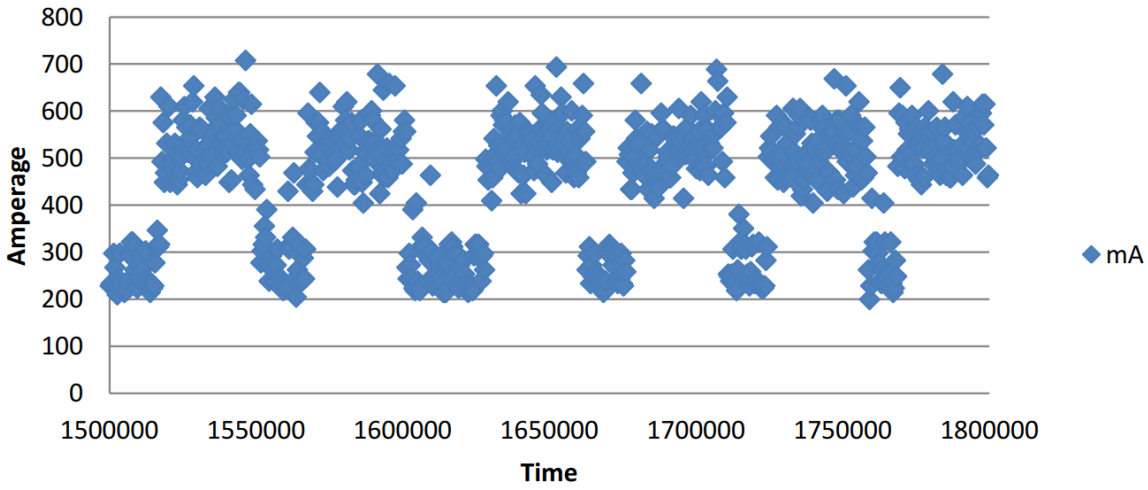
Εικόνα 17: Γρήγορη εναλλαγή εικόνων με επίθεση DoS

Σενάριο κίνησης IP κάμερας: Σε αυτό το σενάριο παρουσιάστηκε έντονη κίνηση μπροστά από την κάμερα. Η μέση ένταση ήταν 434.29 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 18.



Εικόνα 18: Σενάριο κίνησης IP κάμερας

Σενάριο κίνησης IP κάμερας και επίθεση DoS: Σε αυτό το σενάριο, το σενάριο κίνησης επαναλήφθηκε, ενώ επιχειρήθηκε επίθεση DoS κατά της κάμερας IP. Η μέση ένταση ήταν 443.28 mA. Το γράφημα μετρήσεων παρουσιάζεται στην Εικόνα 19.



Εικόνα 19: Σενάριο κίνησης IP κάμερας με επίθεση DoS

Στον Πίνακα 2 απεικονίζονται οι τιμές μέσης εντάσεως για κάθε ένα από τα εξεταζόμενα σενάρια. Τα προαναφερθέντα γραφήματα και ο Πίνακας 2, απεικονίζουν σαφώς ότι υπάρχει απόκλιση της εντάσεως του ρεύματος υπό την παρουσία μίας επίθεσης DoS. Θεωρώντας ότι η απόδοση της προσομοιωμένης επίθεσης DoS ήταν πολύ περιορισμένη, μπορούμε να συμπεράνουμε ότι ακόμη και με

απλά εξωτερικά κυκλώματα ήταν δυνατή η ανίχνευση των αποκλίσεων καθώς και η ανίχνευση της επιθέσεως.

Σενάριο	Κανονική	DoS	Προσαύξηση
Θερμόμετρο	202.54	204.29	0.86 %
IP κάμερα - ακίνητη εικόνα	284.38	296.8	4.37 %
IP κάμερα - εναλλασσόμενες εικόνες	277.6	288.65	3.98 %
IP κάμερα – κίνηση	434.29	443.28	2.07 %

Πίνακας 2: Μέση ένταση (mA) για τα εξεταζόμενα σενάρια 2ου πειράματος

5.3.4 Συμπεράσματα

Σε αυτό το πείραμα παρουσιάστηκε μία νέα τεχνική που βασίζεται στην παρακολούθηση φυσικών παραμέτρων για την ανίχνευση ανωμαλιών σε μία συσκευή IoT. Η απόκλιση της εντάσεως του ρεύματος συσχετίστηκε με την κατάσταση ασφαλείας των δύο συσκευών IoT και αποδείχθηκε ότι μία επίθεση DoS μπορεί να εντοπιστεί μέσω της παρακολούθησης εντάσεως του ρεύματος. Ενώ έχουν χρησιμοποιηθεί μόνο οι μέσες τιμές, η προσέγγιση που παρουσιάστηκε ανίχνευσε με επιτυχία, υψηλή δραστηριότητα δικτύου, παρακολουθώντας μόνο την ένταση του ρεύματος.

5.4 Πείραμα 3ο

Η κύρια ιδέα του παρόντος πειράματος επικεντρώθηκε στην παρακολούθηση της έντασης του ρεύματος, προκειμένου να ανιχνευθεί μία κατασκευαστική ή λειτουργική ανωμαλία των συσκευών IoT. Λαμβάνοντας υπόψη ότι τέτοιες συσκευές είναι περιορισμένες από άποψη λειτουργικότητας και λειτουργικών χαρακτηριστικών, αναμένεται ότι τυχόν αποκλίσεις από την κανονική λειτουργία θα οδηγήσουν σε ανάλογες αποκλίσεις όσον αφορά την κατανάλωση ισχύος.

Η παρακολούθηση της παροχής του ρεύματος μίας συσκευής IoT, παράλληλα και χωρίς να επηρεάζεται η λειτουργία της συσκευής, μπορεί να αποτελέσει μία καλή ένδειξη, σχετικά με την πιθανότητα λειτουργίας της συσκευής με μη φυσιολογικό τρόπο. Αναμένεται ότι οι αποκλίσεις στο δίκτυο ή στη δραστηριότητα της συσκευής IoT, θα προκαλέσουν ανάλογες αποκλίσεις όσον αφορά την ένταση του ρεύματος.

Σε αυτό το πείραμα, δημιουργήθηκε μία συσκευή ως ενδιάμεσος παρατηρητής μεταξύ της συσκευής που θέλουμε να παρακολουθήσουμε και της τροφοδοσίας της. Αυτή η προσέγγιση είναι ρεαλιστική, καθώς όλες οι συσκευές προσφέρουν πρόσβαση στην τροφοδοσία τους. Το προτεινόμενο σύστημα μπορεί τελικά να χρησιμοποιηθεί, προκειμένου να εντοπιστούν προβλήματα αξιοπιστίας και επιθέσεις σχετιζόμενες με την ασφάλεια κατά της συσκευής.

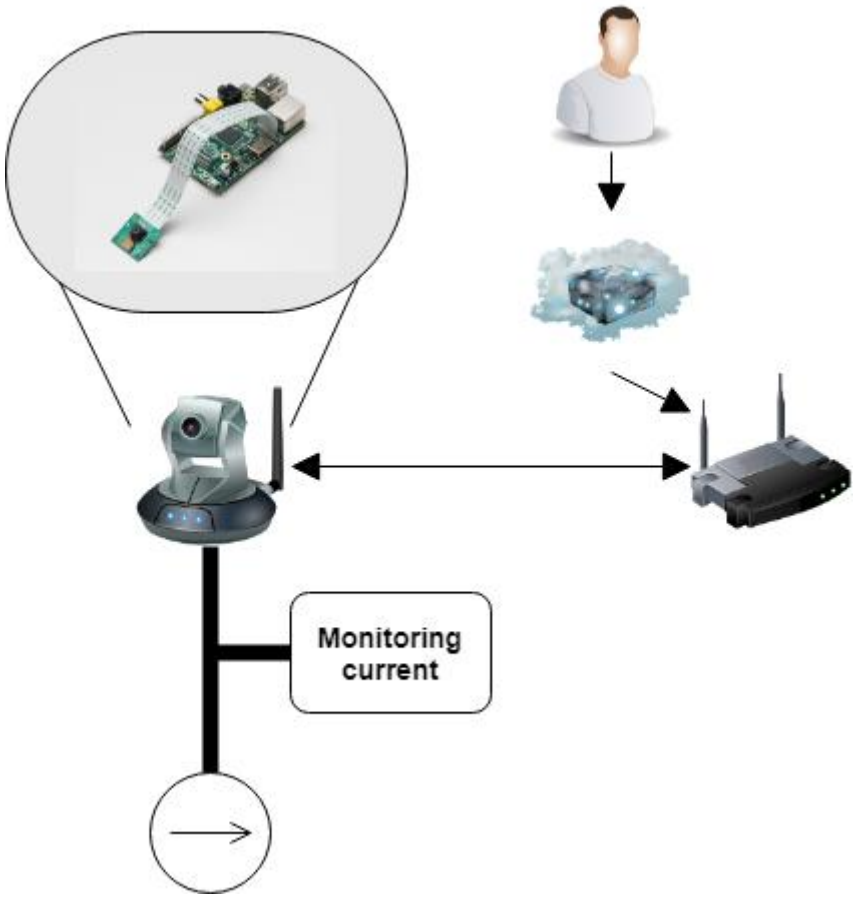
5.4.1 Ρύθμιση πειραμάτων

Προκειμένου να υλοποιηθεί η προτεινόμενη ρύθμιση, δημιουργήθηκε ως συσκευή στόχου μία προσαρμοσμένη κάμερα IP σε έναν κατάλληλο προγραμματισμένο μικροϋπολογιστή για τους σκοπούς μας και χρησιμοποιήθηκε ένας μικροελεγκτής χαμηλού κόστους για την παρακολούθηση της έντασης ισχύος της. Η συσκευή μικροελεγκτή παρεμβλήθηκε μεταξύ της τροφοδοσίας και της συσκευής παρακολούθησης. Η διάταξη έχει ως εξής:

- Αρχικά, ο μικροελεγκτής είναι συνδεδεμένος σε έναν προσωπικό υπολογιστή. Ο κώδικας που έχει αναπτυχθεί για το σκοπό παρακολούθησης της έντασης του ρεύματος, συντάσσεται και φορτώνεται στη μνήμη.

- Το κύκλωμα παρακολούθησης περιλαμβάνει αντίσταση 1 Ohm, που χρησιμοποιείται για λόγους ακρίβειας. Η αντίσταση βρίσκεται μεταξύ των δύο εισόδων του μικροελεγκτή για να μετρηθεί η ένταση. Η ένταση ισχύος μπορεί να υπολογιστεί μέσω της μέτρησης της τάσης στα δύο σημεία εισόδου, σύμφωνα με τον τύπο της εξίσωσης (4).

Δύο αναλογικές είσοδοι του μικροελεγκτή, συνδέονται στο κύκλωμα (Εικόνα 20), προκειμένου να συλλεχθούν οι μετρήσεις ισχύος. Η πρώτη είσοδος συνδέεται στο σημείο πριν από την αντίσταση, ενώ η δεύτερη χρησιμοποιείται για την μέτρηση της τάσης στο άλλο άκρο της αντιστάσεως. Για να αποφύγετε βραχυκύκλωμα ή άλλες επικίνδυνες καταστάσεις, οι οποίες μπορεί να προκύψουν εξαιτίας συσκευών που παρουσιάζουν δυσλειτουργία, συνδέουμε την τάση γείωσης με τη γείωση του μικροελεγκτή (GND).



Εικόνα 20: Διάταξη συσκευής

Τέλος, η συσκευή που παρακολουθείται συνδέεται σειριακά με την αντίσταση. Το κύκλωμα ολοκληρώνεται με τη σύνδεση τροφοδοσίας DC 5V στην παροχή του ρεύματος.

5.4.2 Μελέτη περιπτώσεων

Προκειμένου να αποδειχθεί η έννοια του πειράματος αυτού, ορίσαμε ως στόχο να ανιχνεύσουμε αποκλίσεις της κανονικής λειτουργίας μίας συσκευής, παρακολουθώντας ειδικά τις αποκλίσεις της έντασης του ρεύματος. Κάθε τέτοια απόκλιση αποτελεί προειδοποίηση για την ύπαρξη ανωμαλίας. Η κανονική λειτουργία θα αναφέρεται στη συνέχεια ως κανονικό προφίλ της συσκευής. Η μελέτη διεξήχθη ως μέρος του αντίκτυπου μίας ανωμαλίας στην αξιοπιστία και την ασφάλεια. Συγκεκριμένα, στο πείραμα χρησιμοποιήθηκε προσαρμοσμένο υλικό, αποτελούμενο από ένα μικροεπεξεργαστή Raspberry Pi, μαζί με απαιτούμενο αισθητήρα (8MP Camera Board - Έκδοση 2), για τη δημιουργία μίας κάμερας IP, για εσωτερική και εξωτερική χρήση. Ο μικροϋπολογιστής προγραμματίστηκε σύμφωνα με τις ερευνητικές ανάγκες για να λειτουργήσει ως πραγματική κάμερα IP σε πραγματικό κόσμο. Έδινε τη δυνατότητα στον χρήστη να συνδέεται στη συσκευή και να παρακολουθεί σε πραγματικό χρόνο τη ροή του βίντεο της κάμερας. Η κάμερα τροφοδοτήθηκε με ρεύμα της τάξεως των DC 5V, μέσω του τροφοδοτικού της. Η λειτουργία της συσκευής άλλαζε σκόπιμα κατά τη διάρκεια της φάσης παρακολούθησης, προκειμένου να προσομοιωθούν οι συνθήκες του πραγματικού κόσμου. Η προσαρμοσμένη κάμερα τοποθετήθηκε σε περιβάλλον γραφείου, υπό συνθήκες όπως, δραστηριότητα στο οπτικό πεδίο της κάμερας, το επίπεδο φωτισμού ή η απαίτηση για συνεχόμενη ροή βίντεο, καθώς χαρακτηρίζονταν από σημαντικές αλλαγές καθ’ όλη τη διάρκεια της ημέρας.

5.4.2.1 Συσκευή προσαρμοσμένης IP κάμερας

Προκειμένου να αποδειχθεί ότι είναι εφικτή η παρατήρηση της μη φυσιολογικής δραστηριότητας δικτύου της συσκευής, χρησιμοποιήθηκε μία επίθεση Denial of Service (DoS), μέσω της χρήσης του hping3.

Χρησιμοποιήθηκαν δύο διαφορετικές περίοδοι παρακολούθησης. Κατά τη διάρκεια της πρώτης περιόδου, η οποία διήρκεσε για μία εβδομάδα, η κάμερα λειτουργούσε κανονικά χωρίς να εκτελείται καμία επίθεση εναντίον της. Η δεύτερη περίοδος παρακολούθησης διήρκεσε 24 ώρες και κατά τη διάρκεια αυτών εκτελέστηκαν τρεις διαφορετικές επιθέσεις DoS κατά της κάμερας. Οι τρεις επιθέσεις έχουν με τη σειρά τους όπως στο ακόλουθο χρονοδιάγραμμα:

- Η πρώτη επίθεση ήταν μεταξύ 18:10 και 18:20.
- Η δεύτερη επίθεση ήταν μεταξύ 02:50 και 03:10.
- Τέλος, η τρίτη επίθεση έγινε μεταξύ 09:35 και 10:50

5.4.3 Συζήτηση αποτελεσμάτων

5.4.3.1 Αξιολόγηση της εγκυρότητας της μέτρησης

Για να μπορέσει να αξιολογηθεί η εγκυρότητα των μετρήσεων, ενσωματώθηκε ένα ψηφιακό πολύμετρο για τη μέτρηση της τάσης στα ίδια σημεία. Στη συνέχεια ολοκληρώθηκαν οι συνδέσεις και οι απαραίτητες δοκιμές (ισχύς, κ.λπ.), καθώς επαναλήφθηκαν οι ίδιες μετρήσεις με τη χρήση της προσαρμοσμένης εγκατάστασης παρακολούθησης. Τα αποτελέσματα δεν είχαν παρατηρήσιμες αποκλίσεις από αυτές του ψηφιακού πολύμετρου.

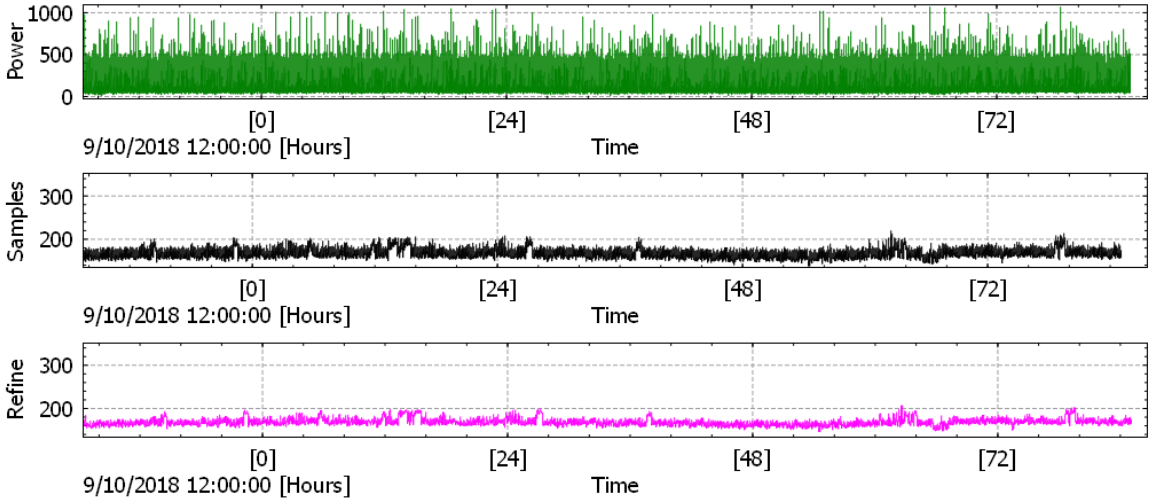
5.4.3.2 Αποτελέσματα μελέτης περίπτωσης συσκευής προσαρμοσμένης IP κάμερας

Ο μικροϋπολογιστής Raspberry Pi (IP Camera), μαζί με το μικροελεγκτή Arduino Uno (monitoring circuit), τοποθετήθηκαν σε ένα περίβλημα εικονικής κάμερας για να παραχθεί μία συσκευή άμεσα χρησιμοποιούμενη.

Όσον αφορά την Μελέτη Περίπτωσης εξετάστηκαν δύο προφίλ/σενάρια:

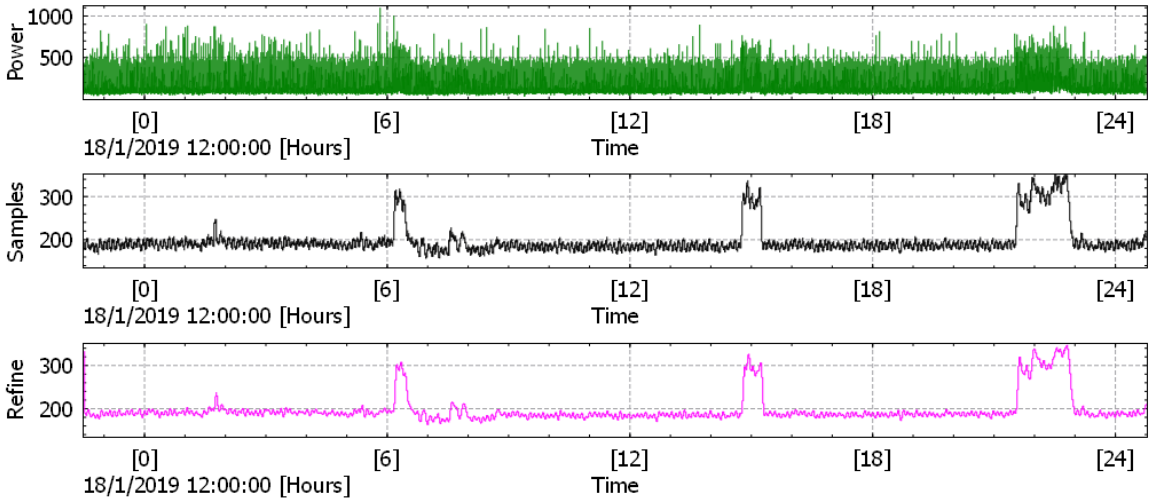
Κανονικό προφίλ: Σε αυτό το σενάριο, η συσκευή μικροϋπολογιστών, πραγματοποίησε κανονικά τη λήψη. Κανένας παράγοντας εξωτερικού περιβάλλοντος δεν υπερέβη τα φυσιολογικά χαρακτηριστικά, ούτε επιτελέστηκε επίθεση,

προκειμένου να υπάρξει ένα προφίλ της έντασης ισχύος σε κανονικές συνθήκες λειτουργίας για λόγους σύγκρισης. Παρουσιάζονται οι μετρήσεις για αυτό το προφίλ (Κανονικό), οι οποίες απεικονίζονται σε τρία γραφήματα, με το χρόνο σε ώρες στον οριζόντιο άξονά τους. Στο διάγραμμα που ονομάζεται «Power», εμφανίζεται το ρεύμα της συσκευής. Η Εικόνα 21 παρουσιάζει δείγματα των μετρήσεων έντασης ρεύματος στα οποία έχει εφαρμοστεί ένα φίλτρο εξομάλυνσης (Samples) και τέλος το βελτιωμένο διάγραμμα (Refine) εμφανίζει τα ήδη φιλτραρισμένα δείγματα που διέρχονται από ένα δεύτερο φίλτρο για το καλύτερο αποτέλεσμα.



Εικόνα 21: Μετρήσεις Κανονικού Προφίλ

Προφίλ ανωμαλίας: Σε αυτό το σενάριο μία επίθεση DoS εκτελέστηκε κατά της συσκευής, ενώ εκτελούσε την κανονική της λειτουργία, συλλέγοντας δεδομένα. Οι μετρήσεις σχετικά με την ένταση ισχύος, έγιναν για να παρακολουθήσουν τη δραστηριότητα του δικτύου της συσκευής. Στην Εικόνα 22 εμφανίζονται οι μετρήσεις για αυτό το προφίλ (Ανωμαλίας), τις οποίες παρουσιάζουν τα τρία διαγράμματα αντίστοιχα, όπως στην προηγούμενη παράγραφο.



Εικόνα 22: Μετρήσεις Προφίλ Ανωμαλίας

Τα ανωτέρω παρουσιαζόμενα στοιχεία, έδειξαν ότι υπάρχει πράγματι απόκλιση της εντάσεως του ρεύματος όταν πραγματοποιείτε μία επίθεση DoS. Λαμβάνοντας υπόψη ότι τα χαρακτηριστικά της επίθεσης DoS ήταν ρεαλιστικά και ότι υπήρξε μία επίθεση, μπορεί να ειπωθεί ότι ακόμη και ένα απλό εξωτερικό κύκλωμα είναι σε θέση να αισθανθεί αποκλίσεις και να ανιχνεύσει την ανωμαλία. Αναμένεται να μετρήσει ακόμα μεγαλύτερες αποκλίσεις υπό φυσιολογική επίθεση botnet και έτσι να ενεργοποιήσει μία ασφαλή λειτουργία για την έξυπνη συσκευή.

5.4.4 Συμπεράσματα

Σε αυτό το πείραμα η απόκλιση της εντάσεως του ρεύματος, συσχετίστηκε με θέματα αξιοπιστίας και ασφάλειας των συσκευών IoT και αποδείχθηκε ότι μπορεί να ανιχνευθεί μία ανωμαλία. Η κύρια συμβολή αυτής της εργασίας είναι ότι εισάγει μία νέα τεχνική για την ανίχνευση ανωμαλιών σε μία συμπτωματική προσέγγιση, αντί για την ανίχνευση της ίδιας της αιτίας.

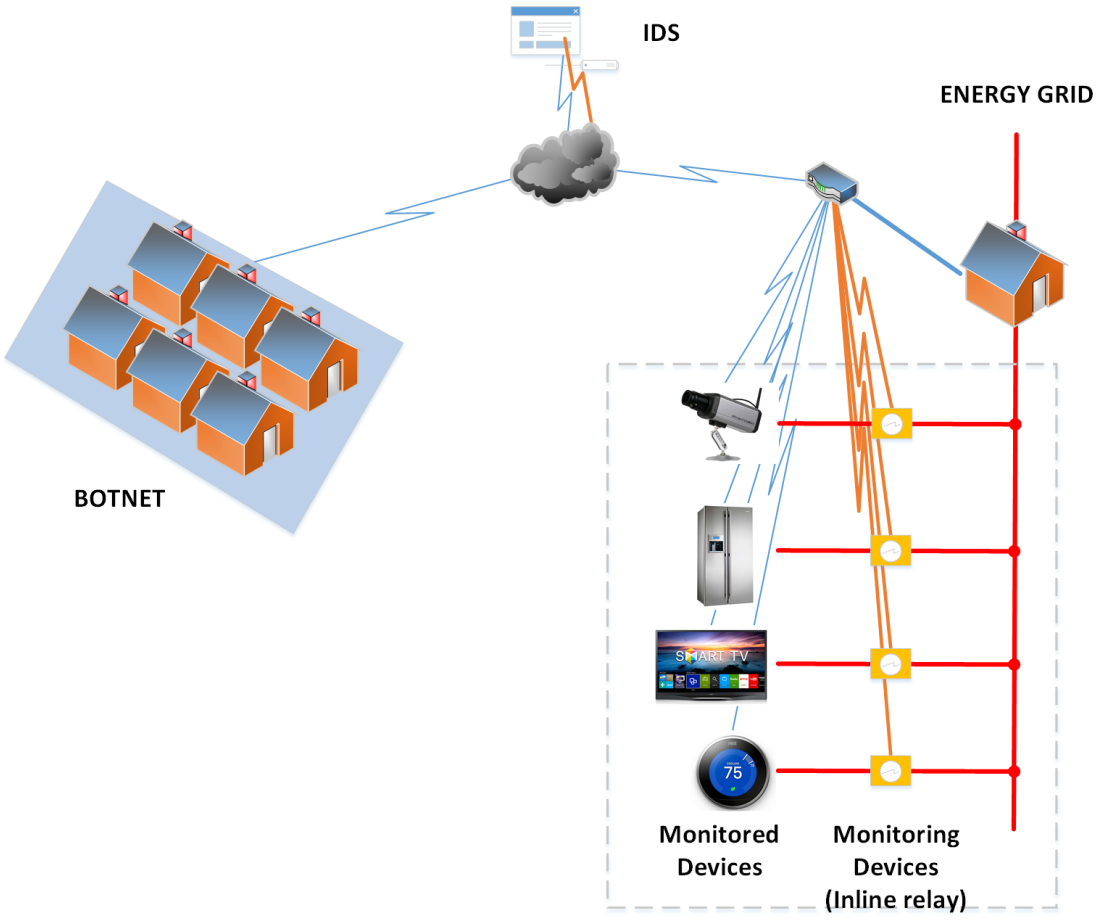
5.5 Πείραμα 4ο

Η κύρια ιδέα του παρόντος πειράματος ήταν η παρακολούθηση του ρεύματος τροφοδοσίας για την ανίχνευση μη φυσιολογικής λειτουργίας συσκευών IoT. Η ιδέα βασίζεται στο γεγονός ότι, οποιαδήποτε λειτουργία μίας ηλεκτρικής ή και ηλεκτρονικής συσκευής, χαρακτηρίζεται από την κατανάλωσή της. Επιπλέον, λαμβάνοντας υπόψη την ισχύ του ρεύματος, η κατανάλωση εξαρτάται από τα χαρακτηριστικά εισόδου και μπορεί να συναχθεί το συμπέρασμα ότι ένα σύστημα που εκτελεί μία συγκεκριμένη λειτουργία, ορίζεται σε ένα χαρακτηριστικό εύρος κατανάλωσης ισχύος. Θεωρώντας ότι οι συσκευές IoT είναι περιορισμένες όσον αφορά τη λειτουργικότητα και τα λειτουργικά χαρακτηριστικά, αναμένεται ότι οποιεσδήποτε αποκλίσεις από την κανονική λειτουργία θα οδηγήσουν σε ανάλογες αποκλίσεις σχετικά με την κατανάλωση ισχύος. Έτσι, τυχόν κακόβουλη ενέργεια κατά της συσκευής IoT, αναμένεται να εντοπιστεί μέσω της κατανάλωσης ενέργειας, απόκλιση που προκαλείται από την πηγή κακόβουλης επίθεσης.

Η συμβολή αυτού του πειράματος είναι η εισαγωγή ενός εξωτερικού μηχανισμού στις συσκευές IoT, που έχει γενική χρήση και είναι εύκολα προσαρμόσιμο σε οποιαδήποτε συσκευή IoT. Αυτός ο μηχανισμός είναι ένα σύστημα παρακολούθησης παροχής ρεύματος, ειδικά σχεδιασμένο για τη συσκευή στόχο, αναλύοντας τη συμπεριφορά ηλεκτρικού ρεύματος της συσκευής, χωρίς να επηρεάζεται η λειτουργία της. Αυτό μπορεί να παρέχει μία καλή ένδειξη, σχετικά με τη δυνατότητα ότι η συσκευή λειτουργεί με ανώμαλο τρόπο. Αναμένεται ότι οι αποκλίσεις στο δίκτυο ή τη δραστηριότητα επεξεργασίας της συσκευής IoT θα προκαλέσει ανάλογες αποκλίσεις σχετικά με την κατανάλωση ενέργειας. Η ηλεκτρική συμπεριφορά της συσκευής IoT αποθηκεύεται στο εξωτερικό σύστημα παρακολούθησης, οπότε οποιαδήποτε επίδραση από κακόβουλη επίθεση στη συσκευή IoT ενδέχεται να μην μπορεί να καλυφθεί από τον εισβολέα. Τα όρια ενεργοποιούν τον εντοπισμό της επίθεσης για την παραβίαση της κανονικής λειτουργίας. Σε όλο αυτό το πείραμα, ο προ-χαρακτηρισμός και τα κανονικά όρια λειτουργίας της εντάσεως του ρεύματος θέτονται από το χρήστη. Δημιουργήθηκε μία συσκευή ως ενδιάμεσος παρατηρητής μεταξύ της συσκευής που παρατηρήθηκε και την τροφοδοσία αυτής. Αυτή η προσέγγιση είναι ρεαλιστική αφού όλες οι συσκευές προσφέρουν πρόσβαση στη τροφοδοσία τους. Το προτεινόμενο σύστημα μπορεί τελικά να χρησιμοποιηθεί για τον

εντοπισμό προβλημάτων αξιοπιστίας και ειδικά με την ασφάλεια επιθέσεων κατά της συσκευής.

Η τοπολογία μίας τελικής λύσης παρουσιάζεται στην Εικόνα 23, όπου οποιοδήποτε σπίτι είναι συνδεδεμένο στο Διαδίκτυο μπορεί να χρησιμοποιήσει τις υπηρεσίες ενός παρόχου IDS. Μέχρι σήμερα, ένα botnet έξυπνων συσκευών επιτίθεται είτε στο IDS είτε στη συσκευή στόχο. Το δεύτερο σενάριο βρίσκεται στο πεδίο αυτού του πειράματος. Κάθε έξυπνη συσκευή είναι συνδεδεμένη στο δίκτυο ενέργειας (τροφοδοσία) μέσω των προτεινόμενων συσκευών παρακολούθησης και στο Διαδίκτυο μέσω του δρομολογητή. Οποιαδήποτε απόκλιση από την αναμενόμενη λειτουργία αναφέρεται στο IDS και ταυτόχρονα, μπορούν να ενεργοποιηθούν ασφαλής διαδικασίες, με βάση τις πολιτικές ασφαλείας. Σε αυτό το πείραμα, η έρευνα επικεντρώθηκε μόνο στην ανίχνευση ανωμαλιών.



Εικόνα 23: Τοπολογία των συσκευών παρακολούθησης σε ένα νοικοκυριό

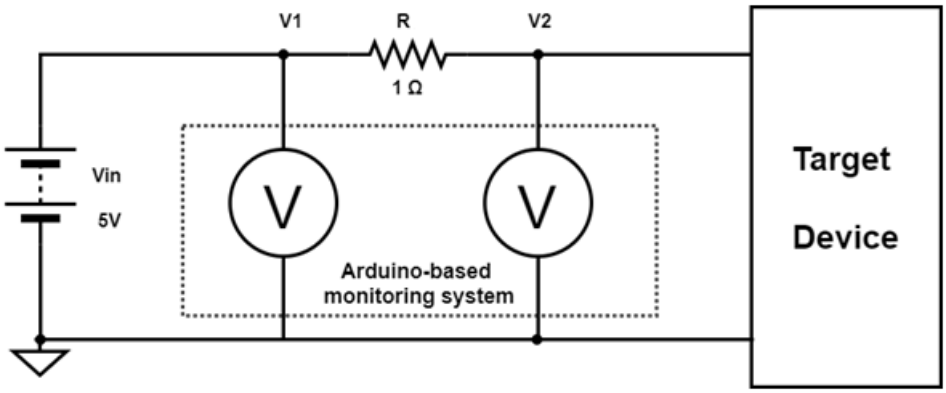
5.5.1 Ρύθμιση πειραμάτων

Προκειμένου να εφαρμοστεί η προτεινόμενη ρύθμιση, κατασκευάστηκε ως συσκευή στόχου μία προσαρμοσμένη κάμερα IP και χρησιμοποιήθηκε ένας μικροελεγκτής χαμηλού κόστους για την παρακολούθηση της έντασης ενέργειας της συσκευής στόχου.

Η συσκευή στόχου (κάμερα IP), βασίστηκε σε ένα προγραμματιζόμενο μικροϋπολογιστή κατάλληλο για το δικό μας σκοπό. Η συσκευή μικροελεγκτή παρεμβάλλονταν μεταξύ της τροφοδοσίας και της συσκευής παρακολούθησης, ως εξής:

- Το κύκλωμα παρακολούθησης περιλαμβάνει αντίσταση 1 Ohm, που χρησιμοποιείται για λόγους ακρίβειας. Η αντίσταση βρίσκεται μεταξύ των δύο εισόδων του μικροελεγκτή για να μετρηθεί η ένταση. Η ένταση ισχύος μπορεί να υπολογιστεί μέσω της μέτρησης της τάσης στα δύο σημεία εισόδου, σύμφωνα με τον τύπο της εξίσωσης (4).

- Δύο αναλογικές είσοδοι του μικροελεγκτή συνδέονται στο κύκλωμα (Εικόνα 24) για τη συλλογή των μετρήσεων ισχύος. Η πρώτη είσοδος συνδέεται με το σημείο πριν από την αντίσταση ενώ η δεύτερη χρησιμοποιείται για τη μέτρηση της τάσης στο άλλο άκρο της αντίστασης.
- Τέλος, η συσκευή προς παρακολούθηση συνδέεται σειριακά στην αντίσταση. Το κύκλωμα ολοκληρώνεται συνδέοντας ένα τροφοδοτικό συνεχές ρεύματος (DC) 5V στην παροχή του ρεύματος.



Εικόνα 24: Κύκλωμα συσκευής παρακολούθησης

Επιπλέον, βελτιώθηκε η αναλογία σήματος προς θόρυβο (SNR ή S/N) με μία τεχνική λογισμικού. Η συσκευή παρακολούθησης μπορεί να προγραμματιστεί εύκολα και έτσι, χρησιμοποιήθηκε ένας αλγόριθμος κινούμενου παραθύρου εξομαλύνοντας τις αποκλίσεις σήματος. Με αυτόν τον τρόπο οι αιχμές μπορούν να εξαλειφθούν όταν αυτές συμβαίνουν, έστω και σπάνια, ενώ περισσότερο διατηρείται η συχνή εμφάνιση αιχμών για ανίχνευση ανωμαλιών. Αυτή η τεχνική εξομάλυνσης σημάτων ονομάζεται κινούμενος μέσος όρος. Από την αρχική ακολουθία δεδομένων $[y_1, y_2, ..., y_N]$, δημιουργήσαμε μία αντίστοιχη ομαλή ακολουθία δεδομένων. Το εξομαλυσμένο σημείο $(y_k)_s$ είναι ο μέσος όρος ενός περιττού αριθμού 2n + 1 (n = 1, 2, 3, ...) των πρωτογενών ακολουθιών δεδομένων y_{k-n}, y_{k-n+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+n-1}, y_{k+n}, σύμφωνα με την εξίσωση (1).

Ο αριθμός 2n + 1 είναι το πλάτος του παραθύρου. Όσο μεγαλύτερο είναι το πλάτος του παραθύρου, τόσο πιο έντονη η εξομάλυνση. Το SNR μπορεί να βελτιωθεί περαιτέρω αυξάνοντας το πλάτος του παραθύρου ή με το πέρασμα πολλαπλών παραθύρων (εξομάλυνση σε ήδη εξομαλυσμένα σημεία). Κατά τη μέση επεξεργασία κινούμενων παραθύρων, διεξάγεται επίσης υπολογισμός αιχμής, συγκρίνοντας την τιμή y_k με τα όρια $y_{thres.max}$ και $y_{thres.min}$. Αν υποθέτουμε ότι η ακίδα είναι θετική, δηλαδή το σήμα ανεβαίνει, τότε το sp_k ορίζεται σε 1 μόνο για την περίπτωση αυτή το y_k είναι μεγαλύτερο από το $y_{thres.max}$. Το sp_k είναι επίσης ρυθμισμένο στο 1 σε περίπτωση που η ακίδα είναι αρνητική, δηλαδή το σήμα είναι φθίνον και το y_k είναι μικρότερο από $y_{thres.min}$. Στη συνέχεια, ο τελικός πληθυσμός των αιχμών υπολογίζεται σε ένα παράθυρο χρόνου με περιττό αριθμό δειγμάτων, π.χ. 2m + 1, όπου m » n.

Στην εξίσωση (2) το δείγμα k-th έχει τιμή y_k, η οποία συγκρίνεται με το κατάλληλο όριο $y_{thres.max}$ ή $y_{thres.min}$ αντίστοιχα, στην προηγούμενη τιμή του. Ο υπολογισμός πραγματοποιείται για 2m + 1 δείγματα y_{k-m}, y_{k-m+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+m-1}, y_{k+m}, όπου m » n. Στη συνέχεια, μία πρόχειρη εκτίμηση των αναγνωρισμένων αιχμών στα διαδοχικά δείγματα 2m + 1 εκτελούνται με την εξίσωση (3).

Η επιλογή των m, n, $y_{thres.max}$ και $y_{thres.min}$ σε αυτό το πείραμα θεωρήθηκε ως πληροφορία που δόθηκε από τον κατασκευαστή της συσκευής IoT. Η τυπική τιμή για το m είναι 5000 και για το n είναι 20. Τα όρια που ορίστηκαν για το συναγερμό, επιλέχθηκε να είναι 50, προκειμένου να αποφευχθούν αρνητικά θετικά, λόγω τυχαίων αιχμών που προέρχονται από το ενεργειακό δίκτυο.

5.5.2 Μελέτη περιπτώσεων

Για να αποδείξουμε την ιδέα αυτού του πειράματος, θέσαμε ως στόχο να ανιχνεύσουμε ανωμαλίες λειτουργίας μίας συσκευής, παρακολουθώντας τις αποκλίσεις της παροχής του ρεύματος. Οποιαδήποτε απόκλιση είναι μία προειδοποίηση για την παρουσία πιθανής ανωμαλίας. Ο παράγοντας ανίχνευσης αποτελεί παραβίαση των κανονικών ορίων λειτουργίας για μία επιλεγμένη χρονική περίοδο. Η αναμενόμενη λειτουργία θα αναφέρεται στη συνέχεια ως το κανονικό προφίλ της συσκευής.

Εξετάστηκαν τρία σενάρια για να ελεγχθούν διάφοροι τύποι ανώμαλων λειτουργιών που συμβαίνουν από κακόβουλες επιθέσεις. Το πρώτο σενάριο προϋποθέτει μία μέτρηση προσαρμοσμένου έξυπνου θερμομέτρου θερμοκρασίας και υγρασίας σε ένα σπίτι. Η ανώμαλη λειτουργία προσομοιώνεται αντικαθιστώντας τον αισθητήρα με ένα από τα κατεστραμμένα υλικά που ελήφθη από το εργαστήριό μας (το οποίο υποθετικά καταστράφηκε από έναν εισβολέα - φυσική επίθεση στο σύστημα). Το αναμενόμενο αποτέλεσμα θα πρέπει να παρουσιάζει συστηματικό σφάλμα με την πάροδο του χρόνου. Τα όρια του ρεύματος, μετρήθηκαν για κανονική λειτουργία στο εύρος θερμοκρασίας 10 ^oC – 30 ^oC. Ο κατεστραμμένος αισθητήρας που επιλέχθηκε ήταν μόνιμα κολλημένος στο 1 παρουσιάζοντας σφάλματα σε αρκετά bit εξόδου. Το δεύτερο σενάριο προϋποθέτει μία προσαρμοσμένη έξυπνη κάμερα ασφαλείας

εγκατεστημένη σε ένα σπίτι. Μία επίθεση πραγματοποιήθηκε μέσω του δικτύου, προσπαθώντας να πάρει τον έλεγχο της συσκευής με προσομοίωση σε μία επίθεση bot. Το τρίτο σενάριο προϋποθέτει φυσική πρόσβαση σε μία κάμερα (φυσική επίθεση με αντικατάσταση του εξοπλισμού με μολυσμένο) και αλλαγή της κάρτας μνήμης με μία άλλη η οποία είχε προεγκατεστημένο μολυσμένο κώδικα. Προκειμένου να αποδειχθεί ότι η ανίχνευση ανωμαλιών είναι εφικτή, ακολουθήθηκαν οι παρακάτω ρυθμίσεις.

5.5.2.1 Έξυπνο θερμόμετρο

Για το πρώτο σενάριο, το έξυπνο θερμόμετρο, το οποίο αποτελείται από έναν μικροελεγκτή Arduino Uno Rev3 με μία ενσωματωμένη ασπίδα Wi-Fi και έναν αισθητήρα DHT 22 για τη μέτρηση της θερμοκρασίας και της υγρασίας του σπιτιού, τοποθετήθηκαν μέσα σε ένα σπίτι. Λήφθηκαν μέτρα για την εξάλειψη όλων των πηγών φθοράς από το περιβάλλον του σπιτιού.

5.5.2.2 Κάμερα IP με DoS επίθεση

Για το δεύτερο σενάριο, μία επίθεση άρνησης υπηρεσίας (DoS) χρησιμοποιήθηκε με τη χρήση του hping3 στη συσκευή στόχου (κάμερα IP), η οποία αποτελείται από έναν μικροελεγκτή Raspberry Pi 3 B+ και μία πλακέτα κάμερας RMP 8MP έκδοση 2. Χρησιμοποιήθηκαν δύο διαφορετικές περίοδοι παρακολούθησης. Κατά τη διάρκεια της πρώτης περιόδου, η οποία διήρκεσε μία εβδομάδα, η κάμερα λειτουργούσε κανονικά χωρίς να εκτελεστεί καμία επίθεση εναντίον της. Η δεύτερη περίοδος παρακολούθησης διήρκεσε 24 ώρες και κατά τη διάρκεια αυτής της περιόδου, εκτελέστηκαν τρεις διαφορετικές προσπάθειες DoS ενάντια στην κάμερα. Οι τρεις επιθέσεις πραγματοποιήθηκαν σύμφωνα με το ακόλουθο χρονοδιάγραμμα:

- Η πρώτη επίθεση ήταν μεταξύ 06:00 και 07:00.
- Η δεύτερη επίθεση ήταν μεταξύ 14:30 και 15:30.
- Τέλος, η τρίτη επίθεση πραγματοποιήθηκε μεταξύ 21:30 και 23:00.

5.5.2.3 Κάμερα IP με μολυσμένο κώδικα

Για το τρίτο σενάριο, ακολουθήσαμε την ίδια ρύθμιση με εκείνη του πρώτου σεναρίου, δηλαδή, ελεγχόμενες εξωτερικές συνθήκες, χωρίς πηγές φυσικών επιδράσεων. Η διαφορά βρίσκεται μόνο στο μολυσμένο λογισμικό που εκτελείται στο ίδιο υλικό.

Για όλα τα σενάρια και τα πειράματα, η δειγματοληψία της εντάσεως του ρεύματος ήταν η περίοδος των 100 ms. Αυτό προήλθε από τη συχνότητα λειτουργίας των συσκευών IoT.

5.5.3 Συζήτηση αποτελεσμάτων

5.5.3.1 Αξιολόγηση εγκυρότητας μέτρησης

Προκειμένου να αξιολογηθεί η εγκυρότητα των μετρήσεων, ενσωματώθηκε ένα ψηφιακό πολύμετρο για τη μέτρηση της τάσης και της παροχής του ρεύματος στα ίδια σημεία. Οι δοκιμές επαναλήφθηκαν και οι μετρήσεις που αποκτήθηκαν από το ψηφιακό πολύμετρο συγκρίθηκαν με αυτές της προσαρμοσμένης ρύθμισης. Τα αποτελέσματα είχαν αμελητέες αποκλίσεις από αυτές του ψηφιακού πολύμετρου, όπως αναμενόταν στα όρια λάθους του οργάνου.

5.5.3.2 Αποτελέσματα σεναρίων

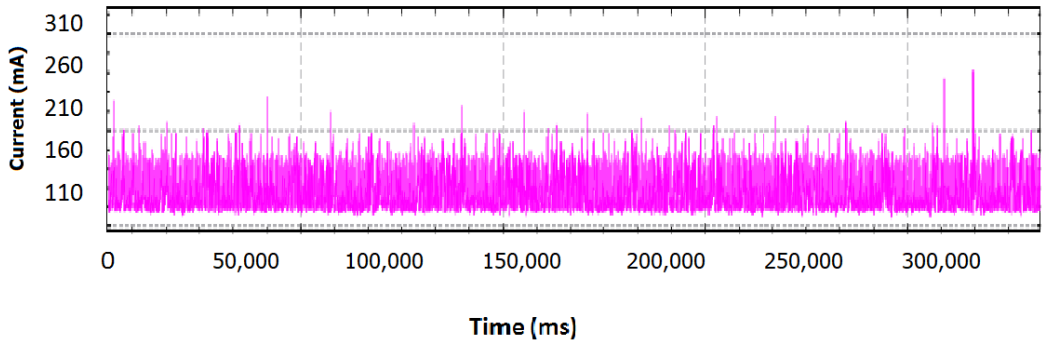
Σε αυτήν την ενότητα, απεικονίζονται τα αποτελέσματα που αποκτήθηκαν από τις συσκευές κατά τη διάρκεια των πειραμάτων. Η ώρα και η περίοδος των δειγμάτων είναι επαρκής για να παρουσιάσει τα αποτελέσματα της ανιχνευμένης ανωμαλίας. Χρησιμοποιώντας απλούς κανόνες ορίων ή εύρους τιμών, η ανίχνευση ανωμαλιών επιτυγχάνεται μόνο με μία φυσική παράμετρο λειτουργίας, δηλαδή την ένταση του ρεύματος τροφοδοσίας. Παρουσιάζεται μία ανάλυση των αποτελεσμάτων και των τιμών για κάθε ένα σενάριο ξεχωριστά στις ακόλουθες ενότητες.

5.5.3.2.1 Πρώτο σενάριο - Έξυπνο θερμόμετρο

Για το πρώτο σενάριο, σχετικά με το έξυπνο θερμόμετρο, η συσκευή εκτέλεσε την κανονική της λειτουργία καταγράφοντας τη θερμοκρασία και την υγρασία δωματίου. Όσον αφορά το πρώτο σενάριο, δύο προφίλ εξετάστηκαν:

Κανονικό προφίλ

Σε αυτό το προφίλ λειτουργίας, κανένας εξωτερικός περιβαλλοντικός παράγοντας δεν υπερέβη τα κανονικά χαρακτηριστικά και δεν πραγματοποιήθηκε καμία επίθεση, προκειμένου να υπάρχει αναφορά του προφίλ υπό φυσιολογικές συνθήκες καθώς και μη βεβλαμένος εξοπλισμός. Στην Εικόνα 25, απεικονίζεται η ένταση του ρεύματος που μετρήθηκε κατά τη διάρκεια 350 δευτερολέπτων.

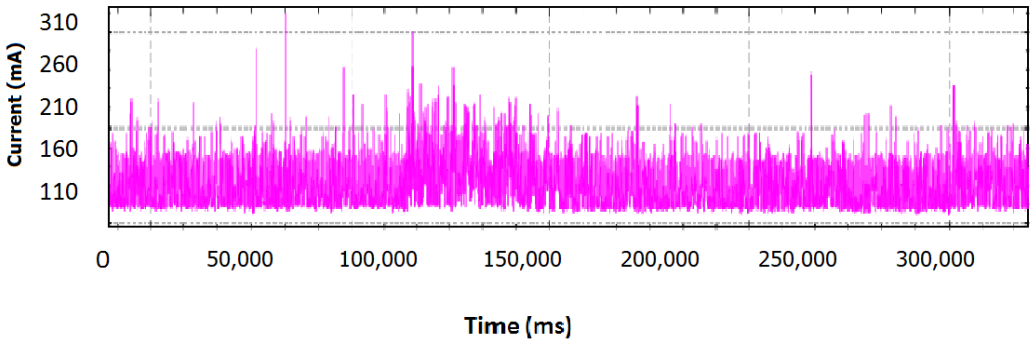


Εικόνα 25: Κανονικό προφίλ έξυπνου θερμομέτρου

Προφίλ Ανωμαλίας

Σε αυτό το προφίλ λειτουργίας, ο αισθητήρας αφαιρέθηκε και αντικαταστάθηκε με ένα κατεστραμμένο. Οι ληφθείσες τιμές για 350 δευτερόλεπτα, παρουσιάζουν στην Εικόνα 26 την ύπαρξη μίας αξιοσημείωτης διακύμανσης της μετρούμενης ισχύος του ρεύματος. Αυτό συμβαίνει λόγω των βλαβών στοίβας-στο-1 του κατεστραμμένου αισθητήρα, δημιουργώντας μεγαλύτερη απορρόφηση ισχύος από την προτεινόμενη στον ADC (Μετατροπέας Αναλογικού σε Ψηφιακό) της συσκευής παρακολούθησης. Αξιοποιώντας αυτό, βρίσκοντας και λαμβάνοντας υπόψη τον αριθμό των ακίδων, ο μηχανισμός παρακολούθησης μπορεί να ανιχνεύσει αποτελεσματικά μία τέτοια συμπεριφορά. Πρέπει να σημειωθεί ότι, αυτή η ανίχνευση είναι εφικτή μόνο εάν η στοίβα-στο-1 έχει σίγουρα βλάβη επηρεάζοντας την κατανάλωση ισχύος και ο

αριθμός των αιχμών που υπερβαίνουν τα όρια είναι αρκετά υψηλός, για να προσδιοριστεί μία απόκλιση σε λειτουργία.



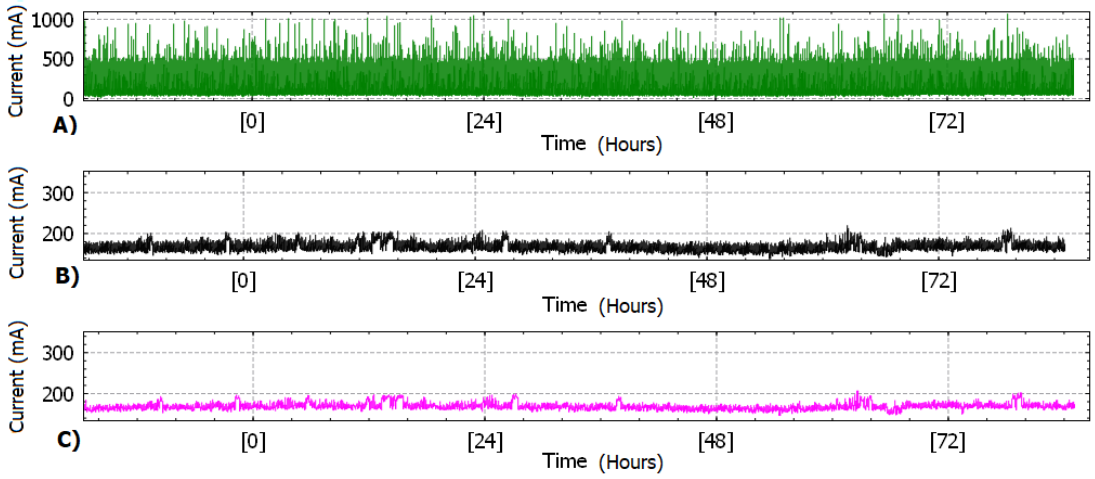
Εικόνα 26: Έξυπνο θερμόμετρο με κατεστραμμένο αισθητήρα

5.5.3.2.2 Δεύτερο σενάριο — Κάμερα IP με DoS επίθεση

Ένα Raspberry Pi (IP Camera), μαζί με ένα Arduino Uno (κύκλωμα παρακολούθησης), τοποθετήθηκαν σε ένα περίβλημα εικονικής κάμερας για την παραγωγή ενός ολοκληρωμένου προϊόντος. Όσον αφορά το δεύτερο σενάριο, δύο προφίλ εξετάστηκαν ξανά.

Κανονικό προφίλ

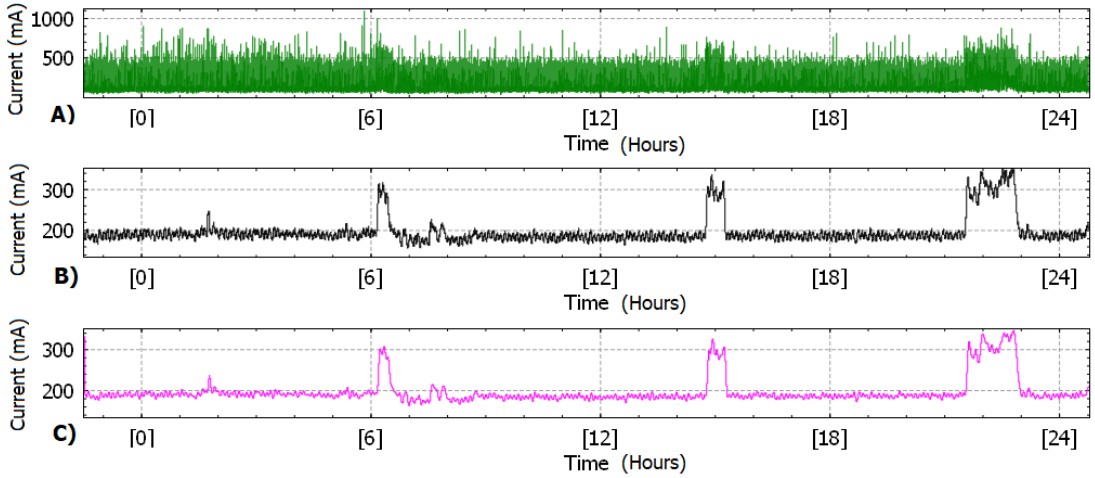
Σε αυτό το σενάριο, η μικροηλεκτρονική συσκευή πραγματοποίησε περιοδική καταγραφή των τρεχουσών τιμών. Κανένας εξωτερικός παράγοντας περιβάλλοντος δεν ξεπέρασε τα κανονικά χαρακτηριστικά και δεν πραγματοποιήθηκε καμία επίθεση, προκειμένου να δημιουργηθεί ένα βασικό προφίλ της έντασης ισχύος υπό κανονικές συνθήκες λειτουργίας για λόγους σύγκρισης. Αυτό το προφίλ (Κανονικό) απεικονίζεται στην Εικόνα 27, εμφανίζοντας τρία γραφήματα, όπου στον οριζόντιο άξονα παρουσιάζεται ο χρόνος (ώρες). Στην Εικόνα 27^{A} η ένταση του ρεύματος της συσκευής εμφανίζεται όπως λαμβάνεται από το εξωτερικό κύκλωμα. Στην Εικόνα 27^{B} εφαρμόστηκε το φίλτρο εξομάλυνσης, όπου διακρίνονται οι διακυμάνσεις ισχύος, και τέλος στην Εικόνα 27^{C}, εμφανίζονται τα ήδη φιλτραρισμένα δείγματα που διέρχονται από ένα δεύτερο φίλτρο για το καλύτερο αποτέλεσμα.



Εικόνα 27: Μετρήσεις κατά τη λειτουργία χωρίς επιθέσεις (Κανονικό προφίλ)

Προφίλ Ανωμαλίας

Σε αυτό το σενάριο, μία επίθεση DoS πραγματοποιήθηκε κατά της συσκευής, ενώ η λειτουργία της εκτελέστηκε κανονικά (συλλογή δεδομένων). Ελήφθησαν μετρήσεις σχετικά με την ένταση του ρεύματος προκειμένου παρατηρηθεί η δραστηριότητα δικτύου της συσκευής και οι τιμές απεικονίζονται στην Εικόνα 28.



Εικόνα 28: Μετρήσεις κατά τη λειτουργία με επίθεση (Προφίλ ανωμαλίας)

Στην Εικόνα 28[A], υπάρχει πράγματι μία απόκλιση (αιχμές) της εντάσεως του ρεύματος όταν υπάρχει επίθεση DoS. Λαμβάνοντας υπόψη ότι τα χαρακτηριστικά της επίθεσης DoS ήταν ρεαλιστικά, μπορεί να ειπωθεί ότι ακόμη και με ένα απλό εξωτερικό σύστημα παρακολούθησης, είναι δυνατόν να ανιχνευθεί μία λειτουργική

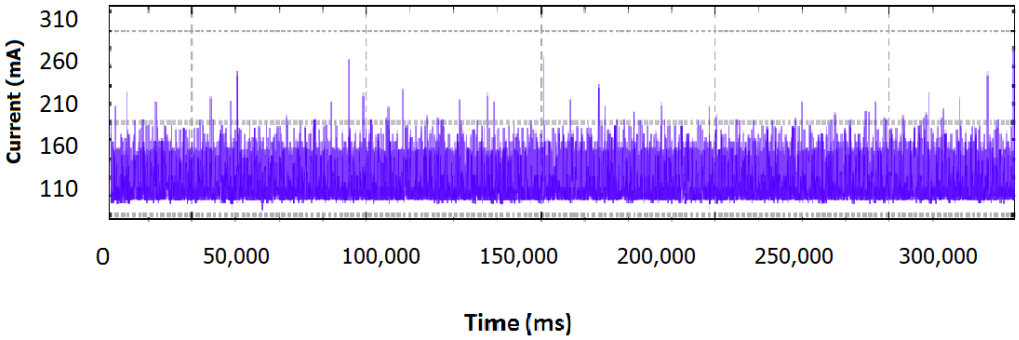
ανωμαλία. Αναμένεται να μετρήσει ακόμη μεγαλύτερες αποκλίσεις κάτω από μία μαζική επίθεση botnet και έτσι να ενεργοποιηθεί μία ασφαλή λειτουργία για την έξυπνη συσκευή. Ακόμη και εφαρμόζοντας το φίλτρο εξομάλυνσης, όπως φαίνεται στην Εικόνα 28^{B} και Εικόνα 28^{C} (πρώτη και δεύτερη εφαρμογή φίλτρου αντίστοιχα), ο αριθμός των αιχμών, όπως υπολογίζεται με την εξίσωση (3), βρίσκεται ψηλά.

5.5.3.2.3 Τρίτο σενάριο — Κάμερα IP με μολυσμένο κώδικα

Για το τελευταίο σενάριο, χρησιμοποιήθηκε μία κάμερα IP (εκμετάλλευση του εξοπλισμού του δεύτερου σεναρίου, για λόγους ασφαλείας). Αυτό το σενάριο προϋποθέτει ότι υπάρχει φυσική πρόσβαση στον εξοπλισμό και ότι η επίθεση είναι η αντικατάσταση της κάρτας μνήμης με μία άλλη με εγκατεστημένο μολυσμένο κώδικα. Πιο συγκεκριμένα, ο κώδικας κακόβουλου λογισμικού που προστέθηκε στην κάρτα της κάμερας ήταν ο mirai. Αυτό είναι ένα αντίγραφο του αρχικού λειτουργικού συστήματος και του κώδικα εφαρμογής, συμπεριλαμβανομένου ωστόσο και του Δούρειου ίππου. Αυτό το σενάριο αποδεικνύει ότι το εξωτερικό σύστημα παρακολούθησης θα ανιχνεύσει μία μη φυσιολογική συμπεριφορά ακόμη και αν δεν υπάρχει επίθεση στο δίκτυο, αλλά μάλλον μία σιωπηρή κακόβουλη επίθεση, δηλαδή η αλλαγή του υπάρχων εξοπλισμού με μία μολυσμένη κάρτα. Και πάλι, δύο προφίλ εξετάστηκαν για αυτό το σενάριο.

Κανονικό προφίλ

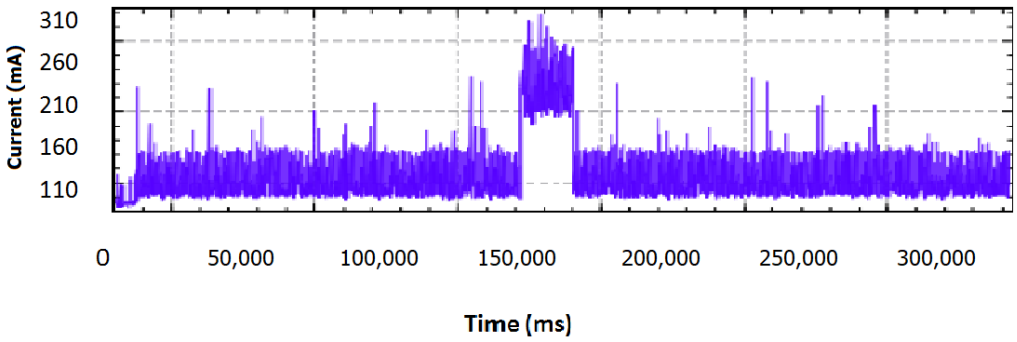
Σε αυτό το προφίλ λειτουργίας, κανένας εξωτερικός περιβαλλοντικός παράγοντας δεν υπερέβη τα κανονικά χαρακτηριστικά και δεν πραγματοποιήθηκε καμία επίθεση, προκειμένου να δημιουργηθεί ένα προφίλ φυσιολογικών συνθηκών για τιμές αναφοράς. Τα δείγματα της εντάσεως του ρεύματος ήταν για 350 δευτερόλεπτα και απεικονίζονται στην Εικόνα 29.



Εικόνα 29: Κανονικό προφίλ κάμερας IP

Προφίλ Ανωμαλίας

Σε αυτό το προφίλ λειτουργίας, η κάρτα μνήμης αφαιρέθηκε και αντικαταστάθηκε με μολυσμένη. Οι ληφθείσες τιμές αποδεικνύουν ότι υπάρχει μία υπολογίσιμη διακύμανση στο ρεύμα που μετρήσαμε. Η ενεργοποίηση του κακόβουλου κώδικα είχε ως αποτέλεσμα την υπερβολική κατανάλωση ενέργειας, η οποία απεικονίζεται στην Εικόνα 30. Και πάλι ο αριθμός των αιχμών είναι υψηλός και υπολογίστηκε με την εξίσωση (3), καθώς η αξιοσημείωτη απόκλιση ανιχνεύεται πολύ εύκολα.



Εικόνα 30: Κάμερα IP με μολυσμένο κώδικα εφαρμογής

5.5.4 Συμπεράσματα

Αυτό το πείραμα, εισάγει μία λύση για την παρακολούθηση συσκευών IoT, εκμεταλλευόμενο χαρακτηριστικά που παρουσιάζουν οι επιθέσεις πλευρικού

καναλιού. Η ιδέα βασίζεται στο γεγονός ότι οι κατασκευαστές δεν παρέχουν μηχανισμούς ασφαλείας ή μέτρα προστασίας από τους χάκερ στα προϊόντα IoT τους, κυρίως λόγω του χαμηλού κόστους τους. Ωστόσο, αυτό οδηγεί σε μία κρίσιμη αύξηση του πεδίου της ασφαλείας που πρέπει να προστατευτεί. Επιτυχείς επιθέσεις σε συσκευές IoT ανακοινώνονται καθημερινά, αλλά οι κύριες ενέργειες για την ασφάλεια των συσκευών IoT βρίσκονται κυρίως σε εμπορικά Συστήματα Ανίχνευσης Εισβολής (IDS). Επιπλέον, οι επιθέσεις έχουν γίνει πιο εξελιγμένες και μπορούν να καλυφθούν, ώστε να μη γίνουν αντιληπτές από τα IDS.

Η ιδέα ακολουθεί την υπόθεση ότι οποιαδήποτε πρόσθετη επεξεργασία δεδομένων θα οδηγήσει σε αύξηση της κατανάλωσης ισχύος. Έτσι, αναπτύχθηκε ένας μηχανισμός παρακολούθησης, χρησιμοποιώντας ένα απλό κύκλωμα και έναν μικροελεγκτή ικανό να εκτελεί απλούς υπολογισμούς τοποθετημένος μεταξύ του βύσματος τροφοδοσίας και της συσκευής IoT. Η συνεχής παρακολούθηση της παροχής του ρεύματος για μία συσκευή με ρητά καθορισμένη λειτουργία, ενδέχεται να αποκαλύψει σημαντικές πληροφορίες και να επεκτείνει τα δεδομένα για την κατάσταση της συσκευής IoT. Το τελευταίο είναι σημαντικό για το σύγχρονο IDS και ακολουθεί γενικά βιο-εμπνευσμένες προσεγγίσεις για την ανίχνευση της ανωμαλίας. Ως εκ τούτου, η παροχή του ρεύματος, παρακολουθήθηκε αξιοποιώντας τις γνώσεις που αποκτήθηκαν από την τεχνική της επίθεσης των πλαϊνών καναλιών. Η απόκλιση του παρακολουθούμενου ρεύματος συσχετίστηκε με ζητήματα ασφάλειας και αξιοπιστίας των συσκευών IoT και αποδείχθηκε ότι μία ανωμαλία μπορεί να ανιχνευθεί με μη τυπικές μεθόδους.

Η κύρια συμβολή αυτού του πειράματος είναι ότι εισήγαγε μία νέα τεχνική για τον εντοπισμό λειτουργικών ανωμαλιών των έξυπνων συσκευών, σε μία μη συμπτωματική προσέγγιση για τον προσδιορισμό της ίδιας της αιτίας. Αυτό επιτρέπει την έγκαιρη ανίχνευση ανωμαλιών, τη μείωση εξάρτησης της ασφάλειας από τη συσκευή στόχο IoT και την αύξηση των δεδομένων που μπορεί να συσχετιστούν με ένα νέο είδος botnet. Αναμένεται να επεκταθεί η παρακολούθηση των παραμέτρων για ζητήματα ασφαλείας που αντιμετωπίζει το IDS και να ενσωματωθεί σύντομα σε μεγάλα συστήματα. Η μέθοδος που παρουσιάζεται είναι η βάση για αυτόν τον τύπο παραμέτρου, επέκταση που θα παρέχει πρόσθετες μετρήσεις για την προστασία κρίσιμων υποδομών IoT. Τέλος, αν και η τεχνική έχει αξιοπρεπή απόδοση σχετικά με

την αξιοπιστία του εξοπλισμού (σε αντίθεση με την επίθεση στο δίκτυο και τη φυσική επίθεση), μπορεί να χρησιμοποιηθεί ως μέσο για τον εντοπισμό Trojan υλικού ή πλαστών IP.

5.6 Πείραμα 5ο

Η ανάγκη για ασφαλείς και αξιόπιστες συσκευές έχει γίνει το κύριο ερώτημα στην αγορά του Internet of Things σήμερα. Αυτό το πείραμα στοχεύει στην εισαγωγή ενός κυκλώματος, συνδεδεμένου σε σειρά με την τροφοδοσία της συσκευής, καθώς και στην ανάλυση της συμπεριφοράς αυτής. Το κύκλωμα ανίχνευσης λειτουργεί σε πραγματικό χρόνο (Real Time detection), δηλαδή συλλέγει την πληροφορία με την ανάγνωση των τιμών της εντάσεως του ρεύματος από τη συσκευή και την επεξεργάζεται για την ανίχνευση μη φυσιολογικών δραστηριοτήτων. Αξιοποιώντας τεχνικές επίθεσης πλευρικού καναλιού, το κύκλωμα ανιχνεύει οποιαδήποτε ανωμαλία, πέραν της αναμενόμενης λειτουργίας και θέτει σε καραντίνα τη συσκευή υπό παρακολούθηση. Το κύκλωμα αναλύεται και απεικονίζεται σε μία απλή υλοποίηση. Τα αποτελέσματα της δοκιμής του κυκλώματος έδειξαν εξαιρετική απόδοση στην ανίχνευση εισβολής, με επιτυχία 100%.

Η λειτουργία της συσκευής ανίχνευσης DoS επιθέσεων, βασίζεται στη συμπεριφορά της συσκευής στόχου (IoT συσκευή) και ειδικότερα στην παρακολούθηση της έντασης του ρεύματος. Πιο συγκεκριμένα, είναι αναγκαίο να οριστεί η φυσιολογική συμπεριφορά της συσκευής από το διαχειριστή. Καθορίζονται δηλαδή κανόνες φυσιολογικής και μη φυσιολογικής συμπεριφοράς. Η διαδικασία αυτή είναι εύκολη, δεδομένου ότι οι συσκευές αυτές αν και «έξυπνες» έχουν περιορισμένες δυνατότητες. Αποτέλεσμα του παραπάνω είναι να υπάρχουν μικρές διακυμάνσεις και να μπορεί να μοντελοποιηθεί εύκολα.

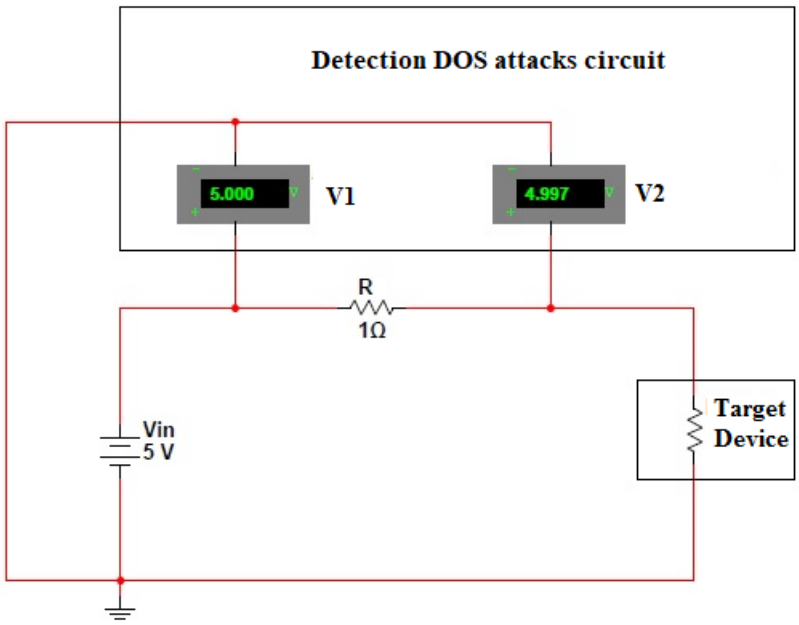
5.6.1 Ρύθμιση πειραμάτων

Για την υλοποίηση του παρόντος πειράματος χρειάστηκε να δημιουργήσουμε μία κάμερα IP ως συσκευή στόχου, στην οποία πραγματοποιήθηκαν οι DoS επιθέσεις ώστε να αποδειχθεί το σενάριο. Η συσκευή αυτή αποτελούνταν από έναν μικροϋπολογιστή και μία κάμερα.

Το κύκλωμα ανίχνευσης DoS επιθέσεων, ήταν ένα κατασκευασμένο αυτόνομο κύκλωμα. Αποτελούνταν από μία υπολογιστική πλατφόρμα, μία πλακέτα με μικροελεγκτή, θύρες εισόδου/εξόδου και γείωση. Προγραμματίστηκε κατάλληλα

και τοποθετήθηκε ανάμεσα στη συσκευή στόχο και στην παροχή του ρεύματος. Η λογική του βασίζεται στις αποκλίσεις εντάσεως του ρεύματος της συσκευής στόχου σε σχέση με την κανονική της λειτουργία. Μεταξύ της πρώτης και της δεύτερης μετρήσεως παρεμβάλλονταν μία αντίσταση του 1 Ohm, ώστε να μας αποδώσει την ένταση του ρεύματος μέσω της εξίσωσης (4).

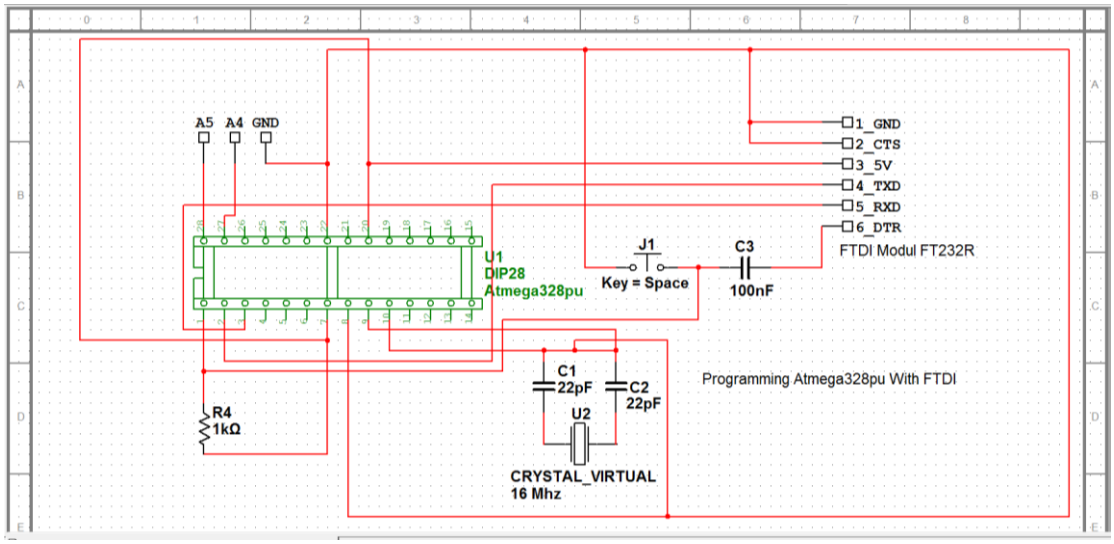
Η διάταξη του κυκλώματος φαίνεται στην Εικόνα 31.



Εικόνα 31: Διάταξη Κυκλώματος

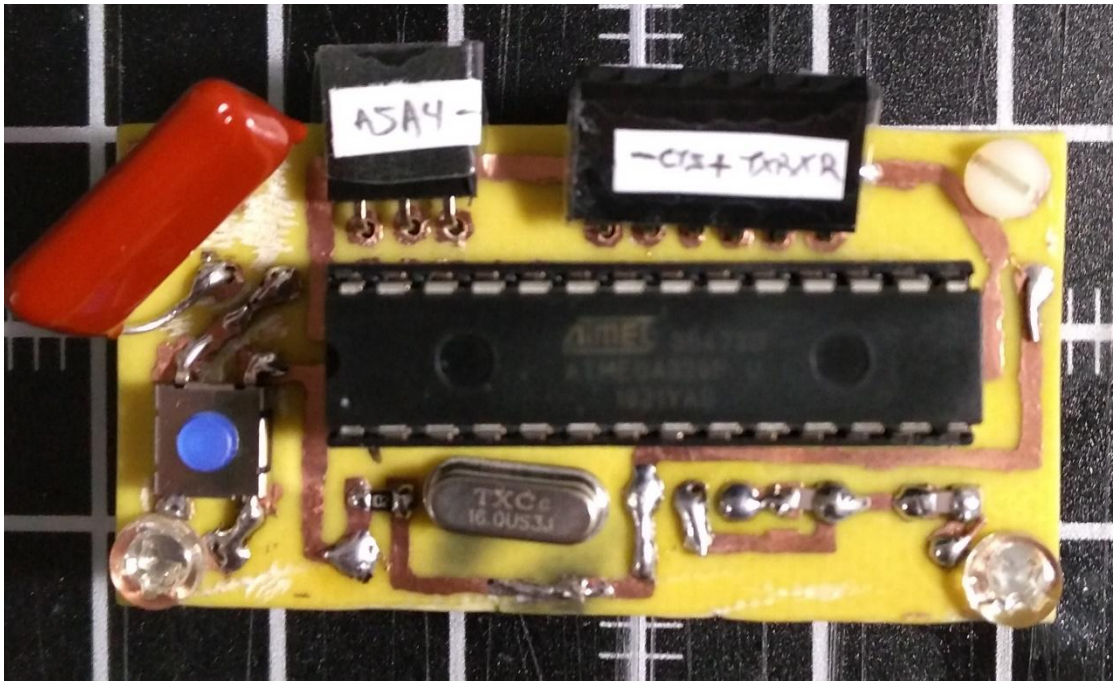
Αρχικά έγινε ο σχεδιασμός σε πλατφόρμα, για τη δημιουργία του αρχικού προγραμματισμού μέσω ISP και συγκεκριμένα για τον μικροελεγκτή ATmega328P-PU. Εν συνεχεία ο σχεδιασμός με τα παρακάτω υλικά μετατράπηκε σε υλοποίηση. Για το κύκλωμά χρησιμοποιήθηκε ο microcontroller ATmega328P-PU, καθώς επίσης ένα DIP Socket 28 pin και ένας κρυσταλλικός ταλαντωτής 16 MHz. Επίσης μία αντίσταση 220 Ohm, δύο κεραμικοί πυκνωτές 22 pF και ένας κεραμικός πυκνωτής 100 nF. Για την επανεκκίνησή του κυκλώματος χρησιμοποιήθηκε ένα Tact Switch και τέλος κατάλληλα υλικά κόλλησης/σύνδεσης τα οποία ένωσαν τα παραπάνω σε μία πλακέτα χαλκού 2 επιπέδων 55*28 mm. Επιπλέον προστέθηκε ένα FTDI Module για

καλύτερη λειτουργικότητα, το οποίο ήταν ρυθμισμένο στα 5 Volt. Η ψηφιακή σχεδίαση του παραπάνω κυκλώματος φαίνεται στην Εικόνα 32.



Εικόνα 32: Κύκλωμα προσομοίωσης

Και το τελικό αποτέλεσμα του κυκλώματος παρουσιάζεται στην Εικόνα 33.



Εικόνα 33: Κύκλωμα ανίχνευσης DoS

Επιπρόσθετα για να εξομαλυνθούν οι μετρήσεις μας και να αποφευχθεί ο θόρυβο (spikes) που μπορεί να δημιουργείται από άλλους παράγοντες, εφαρμόσθηκαν φίλτρα, προγραμματίζοντας το λογισμικό μας. Αυτή η τεχνική εξομάλυνσης σημάτων

ονομάζεται κινούμενος μέσος όρος. Από την αρχική ακολουθία δεδομένων [y_1, y_2, ..., y_N], δημιουργήθηκε μία αντίστοιχη ομαλή ακολουθία δεδομένων. Το εξομαλυσμένο σημείο $(y_k)_s$ είναι ο μέσος όρος ενός περιττού αριθμού 2n +1 (n = 1, 2, 3, ..) των πρωτογενών ακολουθιών δεδομένων y_{k-n}, y_{k-n+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+n-1}, y_{k+n}, εξίσωση (1).

5.6.2 Μελέτη περιπτώσεων

Προκειμένου να αποδειχθεί το πείραμα, υλοποιήθηκε μία IP κάμερα ως συσκευή στόχου, η οποία βασίστηκε σε έναν micro-controller Raspberry Pi 3 B+ καθώς και μία RPI 8MP camera board version 2. Η παραπάνω συσκευή (IP κάμερα) είχε τοποθετηθεί σε κύρια είσοδο σπιτιού εσωτερικού χώρου, με σκοπό τη ρεαλιστική απεικόνιση της κίνησης κατά τη διάρκεια μίας ημέρας (24 ώρες). Στην IP κάμερα πραγματοποιήθηκαν DoS επιθέσεις σε δύο φάσεις της ημέρας:

- Η πρώτη επίθεση πραγματοποιήθηκε μεταξύ 13:30 και 14:00.
- Ενώ η δεύτερη επίθεση πραγματοποιήθηκε μεταξύ 18:30 και 19:00.

Η διάρκεια και το μέγεθός ήταν τέτοιου βαθμού, ώστε να αποδειχθεί το πείραμα (εντοπισμός DoS επίθεσης) χωρίς να σταματήσει η λειτουργία της συσκευής. Σε περίπτωση επίθεσης μεγαλύτερης εντάσεως, τα αποτελέσματα ήταν κλείσιμο της κάμερας (άρνηση παροχής υπηρεσιών).

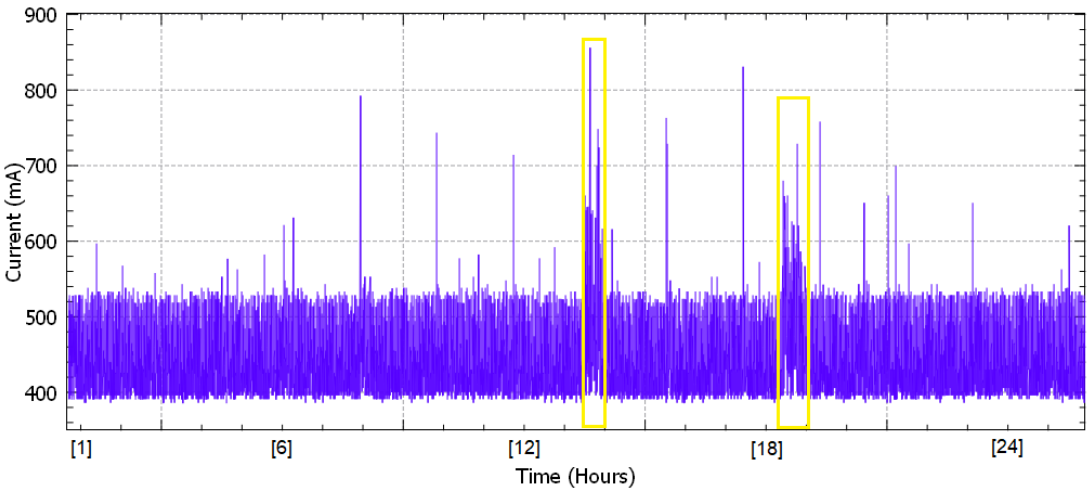
Ο ρυθμός της δειγματοληψίας των τιμών ήταν 100 ms, ώστε η ανταπόκριση του κυκλώματος στην ανίχνευση της DoS επίθεσης να είναι άμεση (real time), όπως παρουσιάζεται και στα διαγράμματα των αποτελεσμάτων Εικόνα 34, Εικόνα 35 και Εικόνα 36.

Επίσης για την εγκυρότητα των μετρήσεων χρησιμοποιήθηκε ψηφιακό πολύμετρο, στις δύο εισόδους των τιμών, τα αποτελέσματα του οποίου δεν είχαν παρατηρήσιμες αποκλίσεις από τις μετρήσεις του κυκλώματός.

5.6.3 Συζήτηση αποτελεσμάτων

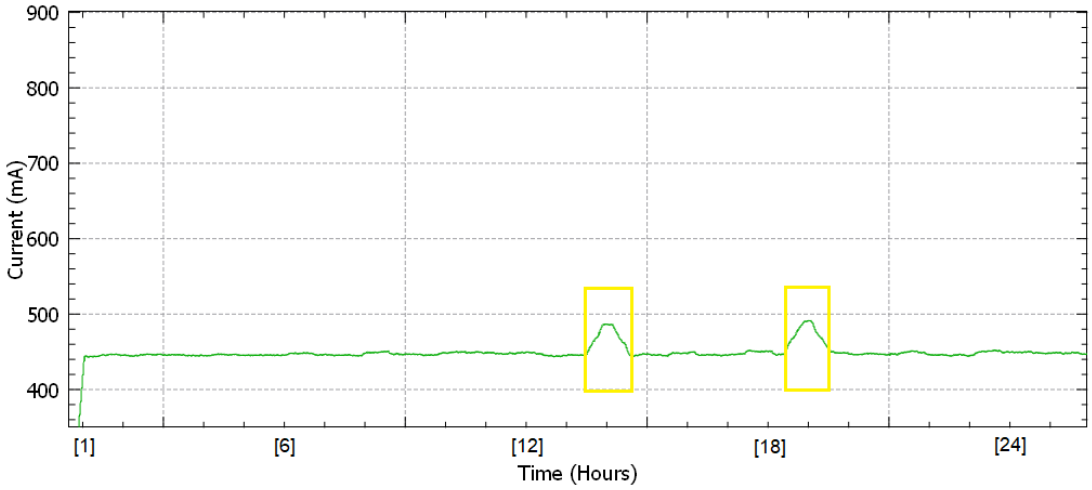
Σε αυτή την ενότητα παρουσιάζονται τα αποτελέσματα του παραπάνω πειράματος, τα οποία αποκτήθηκαν από τις συσκευές. Η ανίχνευση της DoS επίθεσης, επιτυγχάνεται μόνο μέσω της φυσικής παραμέτρου που μελετήθηκε, δηλαδή της παροχής του ρεύματος.

Στο διάγραμμα που παρουσιάζεται στην Εικόνα 34 βλέπουμε την ένταση του ρεύματος της IoT συσκευής (κάμερα IP) όπως αυτή λαμβάνεται από το κύκλωμά ανίχνευσης DoS επιθέσεων. Παρατηρούμε ότι η διακύμανση σε πολλές φάσεις ξεπερνά στιγμιαία τα όρια της φυσιολογικής συμπεριφοράς της κάμερας (spikes). Αυτό μπορεί να οφείλεται σε αστάθμητους παράγοντες όπως για παράδειγμα κάποια αυξομείωση της τάσεως του ρεύματος, μίας και οι τιμές που μετράμε είναι φυσικά χαρακτηριστικά. Παρόλα αυτά όμως οι δύο επιθέσεις που εκτελέστηκαν κατά τη διάρκεια της ημέρας (24 ώρες) όπως αναφέρεται και στην ενότητα 5.6.2 Μελέτη περιπτώσεων, είναι οφθαλμοφανές ότι εντοπίστηκαν και παρουσιάζονται στο διάγραμμα της εικόνας εντός του κίτρινου πλαισίου.

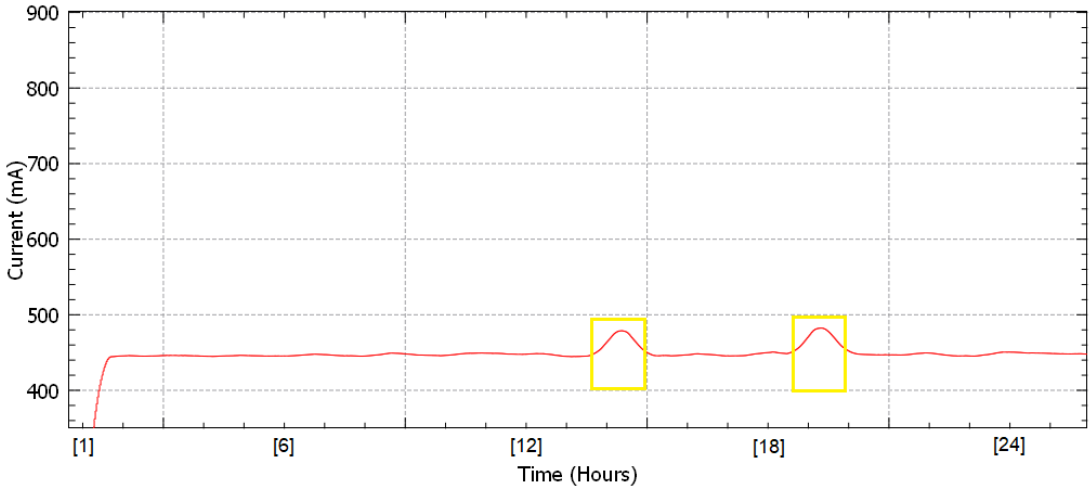


Εικόνα 34: Μετρήσεις Ρεύματος

Για να μπορέσουμε όμως να αποφύγουμε τις τυχόν λανθασμένες μετρήσεις λόγω των spikes, όπως αναφέραμε και στην ενότητα 5.6.1 Ρύθμιση πειραμάτων, χρησιμοποιήσαμε λογισμικά φίλτρα σε σειρά, εξαλείφοντας τον παράγοντα αυτό και τα αποτελέσματα παρουσιάζονται στα διαγράμματα των Εικόνα 35 και Εικόνα 36.



Εικόνα 35: Μετρήσεις ρεύματος με χρήση 1ου φίλτρου



Εικόνα 36: Μετρήσεις ρεύματος με χρήση 2ου φίλτρου

Τέλος, παρατηρούμε ότι η τελική τιμή η οποία απεικονίζεται στη γραφική παράσταση της Εικόνα 36, μας αποδίδει ξεκάθαρα την ανίχνευση της DoS επίθεσης και στις δύο φάσεις της ημέρας, χωρίς την παρεμπόδιση των spikes.

5.6.4 Συμπεράσματα

Αυτό το πείραμα αποσκοπούσε στην εισαγωγή ενός κυκλώματος συνδεδεμένου με το τροφοδοτικό μίας συσκευής και την ανάλυση της συμπεριφοράς αυτής. Η κατανάλωση ισχύος υπολογίζεται σε σχέση με το ρεύμα και την παροχή τάσης σε κάθε περίπτωση, μετά από φιλτράρισμα των ηλεκτρικών σημάτων για την

απομάκρυνση του θορύβου. Εκμεταλλευόμενοι τις τεχνικές επίθεσης πλευρικού καναλιού, το κύκλωμα ανιχνεύει οποιαδήποτε ανωμαλία της αναμενόμενης λειτουργίας παρακολουθώντας την υπερβολική κατανάλωση ισχύος. Το σήμα ανίχνευσης μπορεί να χρησιμοποιηθεί για τη ρύθμιση της συσκευής που βρίσκεται υπό παρακολούθηση, θέτοντάς την σε καραντίνα και έτσι αποτρέπει την εισβολή ή τη συμπερίληψη της συσκευής σε ένα botnet. Το κύκλωμα ανίχνευσης λειτουργεί σε πραγματικό χρόνο (Real Time detection), δηλαδή συλλέγει την πληροφορία με την ανάγνωση των τιμών της εντάσεως του ρεύματος από τη συσκευή και την επεξεργάζεται για την ανίχνευση μη φυσιολογικών δραστηριοτήτων. Τα αποτελέσματα της δοκιμής του κυκλώματος έδειξαν εξαιρετική απόδοση στην ανίχνευση εισβολής, με επιτυχία 100%.

5.7 Πείραμα 6ο

Αυτό το πείραμα παρουσιάζει την εκμετάλλευση της τεχνικής επίθεσης των πλαϊνών καναλιών (SCA), για την προστασία έξυπνων συσκευών χαμηλού κόστους, αξιοποιώντας τα χαρακτηριστικά της παροχής του ρεύματος. Επίσης, για βέλτιστο αποτέλεσμα ενσωματώνει έναν αλγόριθμο βασισμένο στην μηχανική μάθηση (ML) για την ανίχνευση εισβολής (ID). Το σύστημα είναι πρωτότυπο και χρησιμοποιεί τον αλγόριθμο K-Means Clustering με επιτηρούμενη εκπαίδευση. Τα αποτελέσματα αυτού του πειράματος έδειξαν επιτυχή ανίχνευση ύποπτης συμπεριφοράς έξυπνων συσκευών IoT.

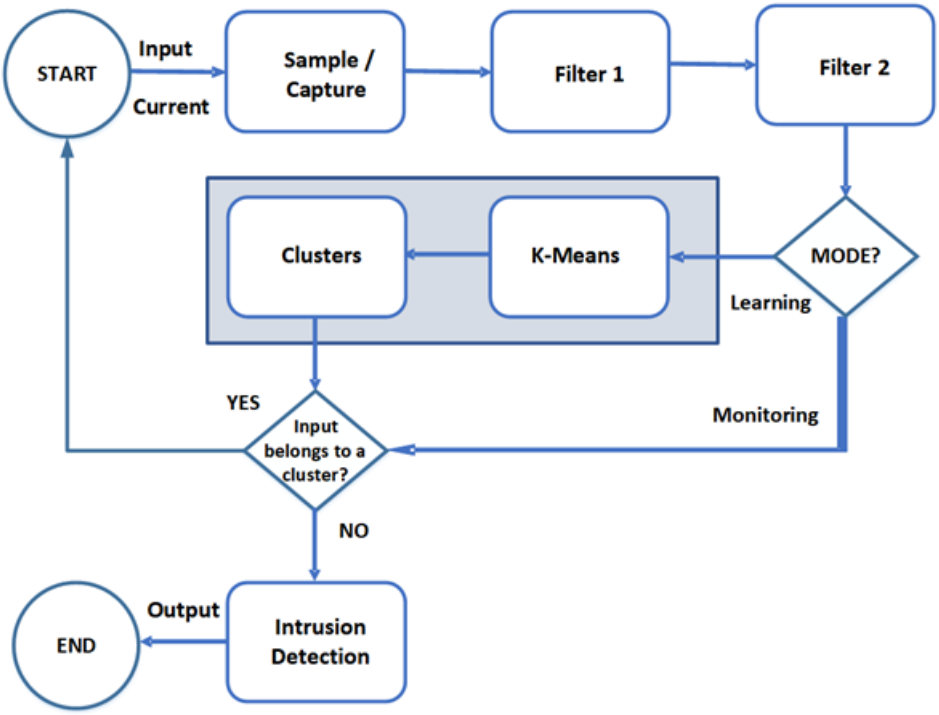
5.7.1 Ρύθμιση πειραμάτων

Τα ολοκληρωμένα κυκλώματα κατασκευάζονται από πληθώρα τρανζίστορ, τα οποία λειτουργούν ως διακόπτες ελεγχόμενης τάσης. Το ρεύμα ρέει κατά μήκος του υποστρώματος του τρανζίστορ όταν το φορτίο εφαρμόζεται ή αφαιρείται από την πύλη. Το ρεύμα αυτό φορτίζει τις πύλες άλλων τρανζίστορ, διαρρέει καλώδια και άλλα φορτία του κυκλώματος. Οποιαδήποτε πρόσθετο ηλεκτρικό φορτίο, καταναλώνει ενέργεια και παράγει ηλεκτρομαγνητική ακτινοβολία, οι οποίες είναι και οι δύο εξωτερικά ανιχνεύσιμες. Η ανάπτυξη του συστήματος Side-Channel Monitor Device, βασίστηκε στην γνωστή τεχνική της SCA και επικεντρώνεται στην παρακολούθηση της τροφοδοσίας, εξάγοντας χρήσιμες πληροφορίες για την ανίχνευση ύποπτης συμπεριφοράς, σε συσκευές συνδεδεμένες στο Διαδίκτυο. Η υπόθεση που γίνεται σε αυτό το πείραμα είναι ότι, οποιαδήποτε ηλεκτρική ή ηλεκτρονική συσκευή έχει τα δικά της φυσικά χαρακτηριστικά, τα οποία σύμφωνα με την αναμενόμενη λειτουργία, καταναλώνουν μία προκαθορισμένη ποσότητα ισχύος. Έτσι, όταν συμβαίνει μία επίθεση ή ύποπτη συμπεριφορά, τότε παρατηρείται ένα διαφορετικό προφίλ λειτουργίας που επηρεάζει την κατανάλωση της ισχύος (υπερβολική χρήση των πόρων επικοινωνίας και επεξεργασίας).

Αυτό το πείραμα εισάγει μία καινοτόμο ψηφιακή συσκευή στον τομέα της ασφάλειας του IoT, η οποία προσαρμόζεται εύκολα σε οποιαδήποτε συσκευή IoT ως ένας εξωτερικός μηχανισμός ή αλλιώς ως ένα «έξυπνο κέλυφος», εφεξής «SmartShell». Η

λειτουργία του βασίζεται στην τεχνική επίθεσης SCA, όπως αναφέρθηκε παραπάνω, και παρακολουθεί την παροχή ρεύματος αναλύοντας τη συμπεριφορά της συσκευής. Αξιοποιώντας τον αλγόριθμο k-Means Clustering που είναι ενσωματωμένος στον κώδικά της, μπορεί να εκπαιδευτεί για να ανιχνεύσει ύποπτη συμπεριφορά. Ένα άλλο πλεονέκτημα αυτής της συσκευής είναι η διαλειτουργικότητά της, καθώς μπορεί να εφαρμοστεί και να εκπαιδευτεί με οποιαδήποτε λειτουργία χαρακτηριστικών της συσκευής IoT, ενώ συνδέεται μεταξύ του τροφοδοτικού και της ίδιας της συσκευής. Επιπλέον, λειτουργεί χωρίς την υποστήριξη Server υψηλής υπολογιστικής ισχύος, προσφέροντας αυτονομία λειτουργίας ακόμα και όταν η DDoS είναι επιτυχής.

Η ροή εργασιών του προτεινόμενου συστήματος απεικονίζεται στην Εικόνα 37. Αρχικά γίνεται δειγματοληψία της εισόδου και στη συνέχεια χρησιμοποιώντας φίλτρα για την εξομάλυνση των αιχμών και την ακρίβεια της κυματομορφής, το σήμα είναι διαθέσιμο για χρήση από τον μηχανισμό ανίχνευσης εισβολής. Το SmartShell έχει δύο τρόπους λειτουργίας, και συγκεκριμένα την «Training Mode» και την «Monitoring Mode». Στην περίπτωση της πρώτης σύνδεσης του SmartShell με την ενσωματωμένη συσκευή IoT, η κατάσταση «Training Mode» λειτουργεί για μεγάλο χρονικό διάστημα. Περισσότερες λεπτομέρειες για τη Λειτουργία «Training Mode» παρέχονται στην ακόλουθη υποενότητα. Σε αυτήν τη λειτουργία το SmartShell παρακολουθεί την κανονική λειτουργία και τους τρόπους λειτουργίας της συσκευής IoT δημιουργώντας τις συστάδες της κανονικής λειτουργίας. Έτσι, στη συνέχεια, κατά τη διάρκεια της λειτουργίας «Monitoring Mode», το SmartShell δειγματίζει το ρεύμα τροφοδοσίας και ελέγχει εάν η είσοδος ταιριάζει σε μία από τις αναγνωρισμένες συστάδες. Εάν δεν ταιριάζει, τότε παράγεται ένα σήμα ανίχνευσης εισβολής, προκαλώντας μία αποτυχημένη ασφαλή λειτουργία (δηλαδή, τερματισμός λειτουργίας). Σε περίπτωση που η είσοδος ανήκει σε μία από τις συστάδες κανονικής λειτουργίας, τότε το SmartShell επαναλαμβάνει τον κύκλο παρακολούθησης.

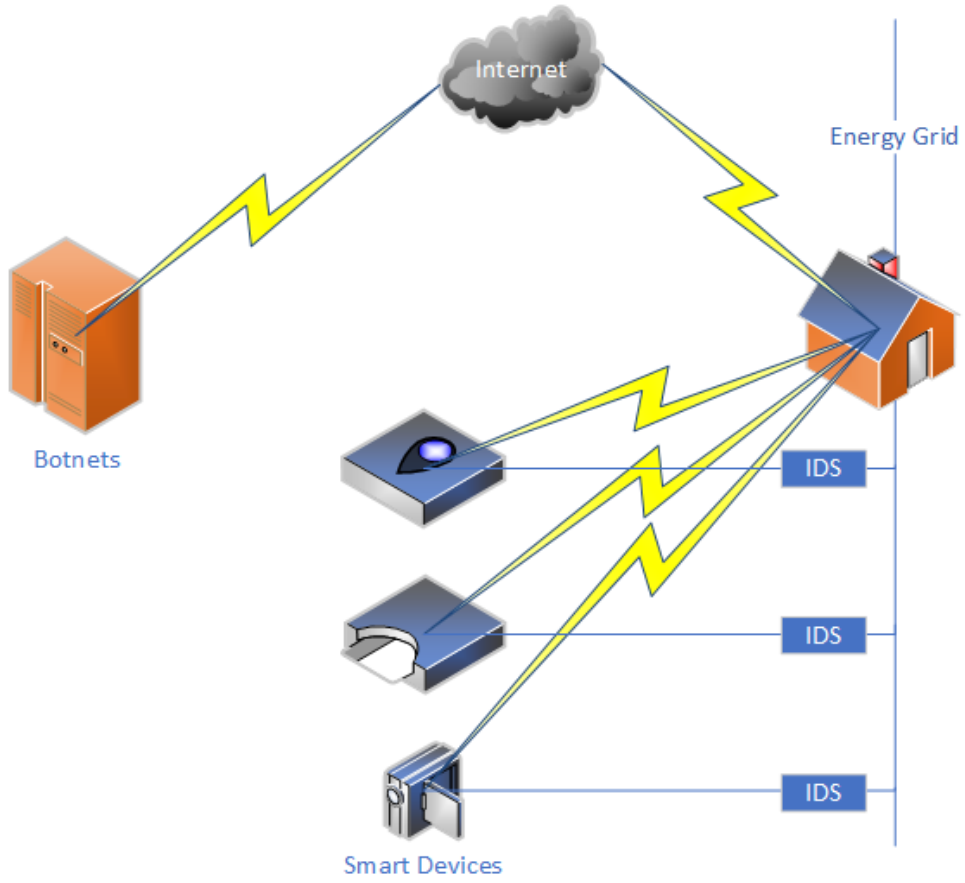


Εικόνα 37: Ροή εργασιών της διαδικασίας που συμβαίνει στη συσκευή Smart Shell

Στην Εικόνα 38, οι έξυπνες συσκευές συνδέονται στο δίκτυο τροφοδοσίας (τροφοδοσία) μέσω της προτεινόμενης συσκευής SmartShell. Η τοπολογία δείχνει την επεκτασιμότητα της προτεινόμενης λύσης, επιτρέποντας την προστασία θεωρητικά άπειρου αριθμού συσκευών IoT. Οι συσκευές IoT συνδέονται στο Διαδίκτυο μέσω του δρομολογητή ISP που είναι εγκατεστημένος στο σπίτι. Τα botnets επιτίθενται σε αυτό το δίκτυο συσκευών, πραγματοποιώντας εξελιγμένες επιθέσεις, οι οποίες συνήθως δεν εντοπίζονται λόγω της απουσίας εγκατεστημένου ειδικού υλικού ασφαλείας στο σπίτι (π.χ. Hardware firewalls, IDS). Η παρουσία των SmartShells επιτρέπει την αυτόνομη λειτουργία αποτρέποντας την εξάπλωση ενός bot στις οικιακές συσκευές. Ένα ισχυρό χαρακτηριστικό αυτής της λύσης είναι ότι κάθε SmartShell εκπαιδεύεται με βάση τη λειτουργικότητα της συνδεδεμένης συσκευής IoT, προσφέροντας έναν εξελιγμένο μηχανισμό παρακολούθησης.

Αυτή η προσέγγιση επιτρέπει την αυτόνομη λειτουργία του SmartShell για κάθε συσκευή IoT, αν και μπορεί να επιτευχθεί επέκταση της λειτουργικότητάς του, μέσω μίας εσωτερικής πύλης που μεταδίδει μετρήσεις ρεύματος σε ένα IDS που βασίζεται

σε cloud. Αυτό θα αύξανε περαιτέρω την ασφάλεια, εάν ο ιδιοκτήτης του σπιτιού έχει τις πηγές για να χρησιμοποιήσει μία τέτοια υπηρεσία. Μία σημείωση που πρέπει να γίνει είναι ότι το SmartShell είναι σε θέση να επικοινωνεί με την πύλη μέσω διαφορετικού καναλιού επικοινωνίας από αυτό των συσκευών IoT (π.χ. Bluetooth) μόνο σε λειτουργία μετάδοσης, καθιστώντας το μη διαθέσιμο σε επιθέσεις. Τέλος, ένα παράλληλο όφελος από τη μετάδοση των μετρήσεων του ρεύματος σε ένα IDS που βασίζεται σε cloud θα αύξανε σημαντικά την ενημέρωση για άγνωστους τύπους επιθέσεων στο μέλλον.

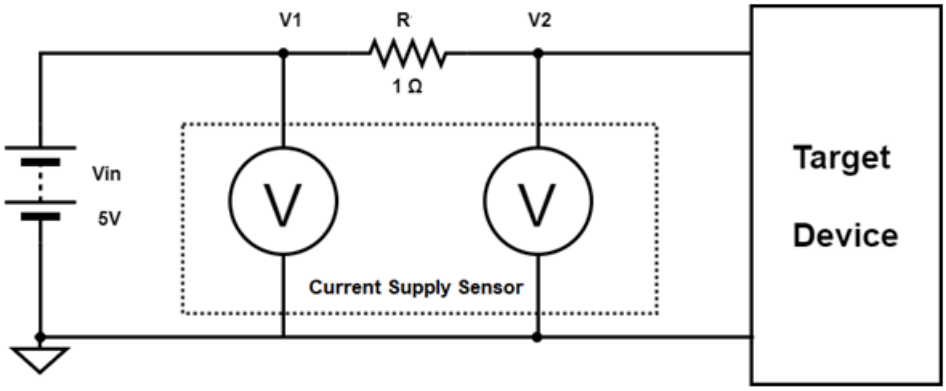


Εικόνα 38: Τοπολογία των συσκευών παρακολούθησης σε ένα νοικοκυριό

5.7.2 Μελέτη περιπτώσεων

5.7.2.1 Υλοποίηση του SmartShell

Το SmartShell βασίζεται σε έναν χαμηλού κόστους χαμηλής ισχύος μικροελεγκτή (ATmega 2560) που παρακολουθεί συνεχώς την παροχή του ρεύματος της συσκευής. Για να επιτευχθεί αυτό, αναπτύσσεται ένας αισθητήρας παροχής ρεύματος, όπως απεικονίζεται στην Εικόνα 39.



Εικόνα 39: Κύκλωμα συσκευής παρακολούθησης

Συγκεκριμένα, η διάταξη του ηλεκτρικού κυκλώματος περιγράφεται λεπτομερώς ως εξής:

- Το κύκλωμα παρακολούθησης περιλαμβάνει μία αντίσταση 1 Ohm ή και μικρότερη αντίσταση που χρησιμοποιείται για λόγους ακρίβειας. Η αντίσταση βρίσκεται μεταξύ των δύο εισόδων του μικροελεγκτή για τη μέτρηση της έντασης. Η ένταση ισχύος μπορεί να υπολογιστεί μέσω της μέτρησης της τάσης στα δύο σημεία εισόδου σύμφωνα με την εξίσωση (4).

- όπου V1 και V2 είναι οι δύο τάσεις αναφοράς, όπως απεικονίζονται στην Εικόνα 39 και το R είναι η αντίσταση 1 Ohm.
- Οι δύο αναλογικές είσοδοι του μικροελεγκτή συνδέονται στο κύκλωμα (Εικόνα 39) για τη συλλογή των μετρήσεων ισχύος. Η πρώτη είσοδος συνδέεται στο σημείο πριν από την αντίσταση ενώ η δεύτερη χρησιμοποιείται για τη μέτρηση της τάσης στο άλλο άκρο της αντίστασης.

- Η συσκευή προς παρακολούθηση συνδέεται σειριακά στην αντίσταση. Το κύκλωμα ολοκληρώνεται συνδέοντας την παροχή συνεχούς ρεύματος (DC) 5V για την τροφοδοσία.
- Τα ληφθέντα δεδομένα που σχετίζονται με την παροχή ηλεκτρικού ρεύματος αποθηκεύονται σε ένα buffer (μνήμη του μικροελεγκτή).
- Τέλος, με βάση τα ληφθέντα δεδομένα, ο αλγόριθμος εκπαίδευσης δημιουργεί προφίλ διαφορετικών τρόπων λειτουργίας. Μετά την εκπαίδευση, οποιαδήποτε απόκλιση από αυτά, επιτρέπει στο SmartShell να ανιχνεύει ανώμαλη λειτουργία.

Αν και η υλοποίηση του υλικού είναι εύκολη και απλή, απαιτούνται περαιτέρω ενέργειες. Η βελτίωση της αναλογίας σήματος προς θόρυβο (SNR ή S/N) με μία τεχνική λογισμικού ήταν απαραίτητη ενέργεια, αξιοποιώντας τις δυνατότητες προγραμματισμού του μικροελεγκτή του SmartShell. Έτσι, ένας αλγόριθμος κινούμενου παραθύρου χρησιμοποιήθηκε για την εξομάλυνση των αποκλίσεων του σήματος. Με αυτόν τον τρόπο, οι αιχμές μπορούν να εξαλειφθούν όταν εμφανίζονται σπάνια, ενώ διατηρείται μία συχνότερη εμφάνιση αιχμών για ανίχνευση ανώμαλης λειτουργίας.

Αυτή η τεχνική εξομάλυνσης σημάτων ονομάζεται κινούμενος μέσος όρος. Από την αρχική ακολουθία δεδομένων $[y_1, y_2, ..., y_N]$, δημιουργήσαμε μία αντίστοιχη ομαλή ακολουθία δεδομένων. Το εξομαλυσμένο σημείο $(y_k)_s$ είναι ο μέσος όρος ενός περιττού αριθμού 2n +1 (n = 1, 2, 3, ..) των μη επεξεργασμένων ακολουθιών δεδομένων y_{k-n}, y_{k-n+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+n-1}, y_{k+n}, σύμφωνα με την εξίσωση (1).

Ο αριθμός 2n + 1 είναι το πλάτος του παραθύρου. Όσο μεγαλύτερο είναι το πλάτος του παραθύρου, τόσο πιο έντονη η εξομάλυνση. Το SNR μπορεί να βελτιωθεί περαιτέρω αυξάνοντας το πλάτος του παραθύρου ή με το πέρασμα πολλαπλών παραθύρων (εξομάλυνση σε ήδη εξομαλυσμένα σημεία). Κατά τη διάρκεια μέσης επεξεργασίας κινούμενων παραθύρων, πραγματοποιείται επίσης υπολογισμός αιχμών, συγκρίνοντας την τιμή y_k με τα όρια $y_{thres.max}$ και $y_{thres.min}$. Αν υποθέτουμε ότι η ακίδα είναι θετική, δηλαδή το σήμα ανεβαίνει, τότε το sp_k ορίζεται σε 1 μόνο για την περίπτωση αυτή το y_k είναι μεγαλύτερο από το $y_{thres.max}$. Το sp_k είναι επίσης ρυθμισμένο στο 1 σε περίπτωση που η ακίδα είναι αρνητική, δηλαδή το σήμα είναι φθίνον και το y_k είναι

μικρότερο από $y_{thres.min}$. Στη συνέχεια, το τελικό πλήθος των αιχμών υπολογίζεται σε ένα παράθυρο χρόνου με περιττό αριθμό δειγμάτων, π.χ. 2m+1, όπου m »n.

Στην εξίσωση (2) το δείγμα k-th έχει τιμή y_k, η οποία συγκρίνεται με το κατάλληλο όριο $y_{thres.max}$ ή $y_{thres.min}$ αντίστοιχα, στην προηγούμενη τιμή του. Ο υπολογισμός πραγματοποιείται για 2m + 1 δείγματα y_{k-m}, y_{k-m+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+m-1}, y_{k+m}, όπου m » n. Στη συνέχεια, μία πρόχειρη εκτίμηση των αναγνωρισμένων αιχμών στα διαδοχικά δείγματα 2m + 1 εκτελούνται με την εξίσωση (3).

Η επιλογή των m, n, $y_{thres.max}$ και $y_{thres.min}$ σε αυτό το πείραμα θεωρήθηκε ως πληροφορία που δόθηκε από τον κατασκευαστή της συσκευής IoT. Η τυπική τιμή για το m είναι 5000 και για το n είναι 20. Τα όρια που ορίστηκαν για το συναγερμό, επιλέχθηκε να είναι 50, προκειμένου να αποφευχθούν αρνητικά θετικά, λόγω τυχαίων αιχμών που προέρχονται από το ενεργειακό δίκτυο.

5.7.2.2 Υλοποίηση αλγορίθμου εκπαίδευσης

Η επιλογή του αλγορίθμου k-Means Clustering για αυτό το πείραμα έγινε λόγω της απλότητας και της ικανότητας να είναι γρήγορος και αποτελεσματικός, ακόμη και όταν εκτελείται σε μικρούς επεξεργαστές με χαμηλές δυνατότητες. Επιπλέον, το μικρό αποτύπωμα μνήμης επιτρέπει την ενσωμάτωσή του σε έναν μικροελεγκτή χαμηλού κόστους και χαμηλής ισχύος, όπως αυτός του SmartShell. Αυτό είχε ως αποτέλεσμα τη σταθερή εκπαίδευση του συστήματος μέσω της δημιουργίας διαφορετικών συστάδων και ελάχιστη αλληλεπίδραση από το χρήστη.

Ο αλγόριθμος εκπαίδευσης (k-Means Clustering Algorithm) έχει δύο εισόδους:

- Το σετ εκπαίδευσης (αρχικοποίηση συστάδων), το οποίο περιέχει τα δεδομένα εκπαίδευσης της κατανάλωσης του ρεύματος των συσκευών IoT, καταγράφεται εφόσον ο χρήστης το θέτει σε κατάσταση εκπαίδευσης.
- Η τιμή k, όπου k είναι ο αριθμός συστάδων που πρόκειται να δημιουργήσει ο αλγόριθμος. Αυτή η τιμή ορίζεται από το χρήστη και αντιπροσωπεύει τους διαφορετικούς τρόπους λειτουργίας της συσκευής IoT, όπου η συσκευή έχει

διαφορετική κατανάλωση ρεύματος. Για παράδειγμα, εάν μία συσκευή IoT έχει 2 λειτουργίες (αναμονή και μετάδοση) το k πρέπει να είναι 2.

Τα βήματα που ακολουθεί ο αλγόριθμος k-Means Clustering είναι 6:

1. Ταξινομεί το σετ εκπαίδευσης με αύξουσα σειρά.
2. Ορίζει τυχαία k κέντρα βάρους (centroids) στο σετ εκπαίδευσης.
3. Δημιουργεί συστάδες δεδομένων που βρίσκονται πιο κοντά στα κέντρα βάρους.
4. Υπολογίζει τη μέση τιμή κάθε συστάδας και μετακινεί τα κέντρα βάρους εκεί.
5. Επαναλαμβάνει τα βήματα 3 και 4.
6. Τελειώνει όταν οι προηγούμενες μέσες τιμές είναι ίδιες με τις τελευταίες.

Δεδομένου ότι τα κέντρα βάρους ρυθμίζονται τυχαία στην αρχή του αλγορίθμου, είναι πιθανό ο αλγόριθμος να δημιουργήσει λάθος συστάδες. Για να εξαλειφθεί αυτή η πιθανότητα, ο αλγόριθμος πρέπει να εκτελείται επανειλημμένα (βήματα 1-6) για αρκετές εκατοντάδες φορές. Κάθε φορά μετά το βήμα 6, το σύστημα συγκρίνει τη συνολική μεταβολή των συστάδων που έχουν παραχθεί με την προηγούμενη ελάχιστη συνολική μεταβολή που έχει βρεθεί και αποθηκεύει τις συστάδες με τη μικρότερη.

Ένα άλλο χαρακτηριστικό που έχουμε προσθέσει στον αλγόριθμο k-Means Clustering είναι να ρυθμίσουμε τα κέντρα βάρους στο σετ εκπαίδευσης χειροκίνητα για πρώτη φορά, ένα στην αρχή, ένα στο τέλος και τα υπόλοιπα σε θέσεις με βήματα μετά το πρώτο centroid $s = (ts_{Last} - ts_{First})/k - 1$, αφού το σύνολο δεδομένων είναι μονοδιάστατο, όπου ts_{Last} και ts_{First} είναι το τελευταίο και το πρώτο σετ τιμών εκπαίδευσης. Για παράδειγμα, εάν έχουμε ένα σετ εκπαίδευσης σε mA:

$$ts = [3,4,5,7,9,11,42,43,44,49,52,55,558,94,95,96,99,100] \; και \; k = 3$$

τα κέντρα βάρους για την πρώτη φορά θα ρυθμιστούν στις ακόλουθες θέσεις [|]:

$$ts = [|3,4,5,7,9,11,42,43,44,49,|52,55,58,94,95,96,99,|100].$$

το οποίο δημιουργεί τις περισσότερες φορές συστάδες με τη μικρότερη συνολική μεταβολή, αλλά ακόμα και αν αποτύχει, θα εκτελεστεί ρυθμίζοντας τυχαία κέντρα βάρους μερικές εκατοντάδες φορές. Η έξοδος του αλγόριθμου k-Means Clustering είναι τα δημιουργημένα k Clusters και το σύστημα αποθηκεύει min και max για κάθε

ένα, τα οποία είναι τα κατώφλια που χρησιμοποιούνται από τον αλγόριθμο Intrusion Detection.

5.7.2.3 Υλοποίηση αλγορίθμου ανίχνευσης εισβολής

Ο αλγόριθμος ανίχνευσης εισβολής (Intrusion Detection) επιλέχθηκε να είναι απλός, καθώς αυτή η εργασία στοχεύει να χρησιμεύσει ως βάση για τα αυτόνομα συστήματα που ενσωματώνουν δυνατότητες ML και είναι χαμηλού κόστους και μικρού μεγέθους. Αυτή η απαίτηση επιβάλλει σημαντικούς περιορισμούς τόσο στη χωρητικότητα μνήμης όσο και στην υπολογιστική ισχύ.

Δεδομένου ότι τα σήματα εισόδου έχουν υποστεί προεπεξεργασία προκειμένου να απομακρυνθούν τα περιττά spikes και να εξομαλυνθεί η κυματομορφή, αναμένεται να παρατηρηθούν διαδοχικές αιχμές και περιοχές υψηλής δραστηριότητας όταν πραγματοποιείται εισβολή. Έτσι, ένα κινούμενο παράθυρο στη χρονική σειρά μετρά πόσες φορές μετρήθηκε αυτή η δραστηριότητα. Αυτό πραγματοποιείται συγκρίνοντας κάθε είσοδο με τις ελάχιστες και μέγιστες τιμές κάθε συστάδας. Σε μία δεδομένη σύντομη χρονική περίοδο, η εμφάνιση πέντε τιμών εκτός εύρους θεωρείται ύποπτη και ενεργοποιείται μία προειδοποίηση. Κάθε προειδοποίηση έχει Time-to-Live (TTL), όπου μετά αφαιρείται. Η παρουσία τριών διαδοχικών προειδοποιήσεων σε μία δεδομένη χρονική περίοδο ενεργοποιεί έναν εντοπισμό εισβολής και το SmartShell ενεργοποιεί μία διαδικασία ασφαλείας.

Παρόλο που υπάρχει μία ποικιλία ενεργειών που πρέπει να εκτελεστούν μετά από εντοπισμό εισβολής, καθώς ο σκοπός αυτού του πειράματος είναι να αποτρέψει τη δημιουργία botnets, η προεπιλεγμένη διαδικασία ασφαλείας περιλαμβάνει την απενεργοποίηση της συσκευής στόχου IoT. Δεδομένου ότι υπήρχε εντοπισμός εισβολής και το SmartShell λειτουργεί αυτόνομα, χωρίς γνώση του δικτύου των συσκευών IoT, επιλέχθηκε η προεπιλεγμένη διαδικασία, ακολουθώντας πρωτόκολλα παρόμοια με την εξάπλωση πανδημίας ενός βιολογικού ιού, όπου υπάρχει η ανάγκη καραντίνας μολυσμένων συσκευών IoT, απαγορεύοντας έτσι την εξάπλωση του ιού και επομένως το σχηματισμό botnets. Όπως προαναφέρθηκε, αυτό το πείραμα είναι βιο-εμπνευσμένο που μιμείται την ανίχνευση μίας απροσδόκητης λειτουργίας, καθώς

και την ενεργοποίηση του βασικού πρωτοκόλλου για τέτοιες καταστάσεις, που είναι το lockdown. Με αυτόν τον τρόπο, η μολυσμένη συσκευή IoT δεν θα είναι σε θέση να μολύνει καμία άλλη, καθώς έχει αφαιρεθεί από το δίκτυο. Αν και αυτή η διαδικασία εγείρει ερωτήματα σχετικά με τον έλεγχο που αποκτά το SmartShell, σε γενικές γραμμές είναι η ίδια προσέγγιση που ακολουθείται από εξελιγμένο IDS σε βιομηχανικό περιβάλλον.

5.7.3 Συζήτηση αποτελεσμάτων

Σε αυτήν την ενότητα, δοκιμάζεται η προτεινόμενη λύση. Η ακόλουθη εγκατάσταση εξετάζεται για την εκτέλεση των δοκιμών ανίχνευσης εισβολής.

1. Μία προσαρμοσμένη ψηφιακή κάμερα παρακολούθησης IP χρησιμεύει ως IoT συσκευή στόχος, έχοντας προγραμματιστεί κατάλληλα για τη μετάδοση βίντεο που λήφθηκε μέσω Διαδικτύου (συνδεδεμένη με WiFi).
2. Το SmartShell, παρεμβάλλεται στη σύνδεση, ανάμεσα στο τροφοδοτικό και την «IoT συσκευή υπό προστασία»

Η προσαρμοσμένη κάμερα παρακολούθησης IP αποτελείται από έναν μικροελεγκτή Raspberry Pi 3 B + και μία πλακέτα κάμερα RPI 8MP έκδοση 2. Αυτή είναι η συσκευή IoT στην οποία στόχευαν οι επιθέσεις. Οι επιθέσεις πραγματοποιήθηκαν στη συσκευή στόχο από εξωτερικές συσκευές και σε αυτήν την περίπτωση με ένα κινητό τηλέφωνο μέσω της εφαρμογής Termux, το οποίο είναι διαθέσιμο σε οποιονδήποτε και μπορεί να χρησιμοποιηθεί εύκολα για επιθέσεις DoS, όταν κάποιος βρίσκεται κοντά στο οικιακό δίκτυο. Η τεχνική της επίθεσης ήταν DoS Attack και πραγματοποιήθηκε με το εργαλείο Hummer, στην IP της συσκευής στόχου και πιο συγκεκριμένα στην πόρτα 8554. Πολλά πακέτα πλημμυρίζουν το κανάλι επικοινωνίας για να εκτελέσουν επιτυχώς την επίθεση DoS.

Για λόγους πειραμάτων, ο χρήστης μπορεί να τροποποιήσει και να αλλάξει το χρόνο εκκίνησης της συσκευής, καθώς και το χρόνο εκπαίδευσής της καθώς και τον αριθμό των συστάδων που πρόκειται να δημιουργηθούν. Στο μέλλον αυτό αναμένεται να ρυθμίζεται δυναμικά από τον αλγόριθμο εκπαίδευσης. Στο παρόν πείραμα, οι χρόνοι των παραπάνω καταστάσεων ήταν 5 λεπτά για τη λειτουργία «Boot Device», 1920

λεπτά (32 ώρες) για τη λειτουργία «Training» και $k = 3$. Το ποσοστό δειγματοληψίας της συσκευής ανίχνευσης SmartShell ήταν 100 ms και αυτό για την πληροφόρηση σε πραγματικό χρόνο σχετικά με την επίθεση.

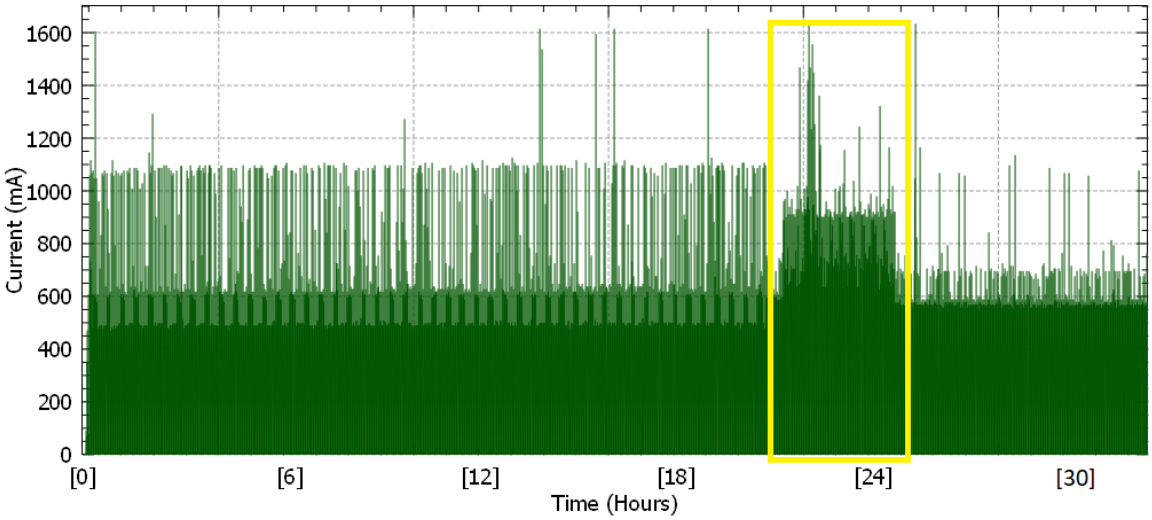
Στην Εικόνα 40 απεικονίζεται ένα παράδειγμα της κατανάλωσης ισχύος της στοχευμένης έξυπνης συσκευής (κάμερα web) σε διαφορετικές λειτουργίες (Εκκίνηση, Αναμονή, Μετάδοση, Κίνηση). Κατά την εκκίνηση της έξυπνης συσκευής, η κατανάλωση ισχύος δεν είναι σταθερή και δεν θα πρέπει να συμπεριληφθεί στον αλγόριθμο εκπαίδευσης ή ανίχνευσης εισβολής. Η εκπαίδευση ή η λειτουργία ανίχνευσης εισβολής μπορεί να ξεκινήσει όταν ολοκληρωθεί η εκκίνηση της συσκευής. Ενώ το σύστημα βρίσκεται σε κατάσταση εκπαίδευσης δημιουργεί διαφορετικές συστάδες δεδομένων για τις διαφορετικές λειτουργίες της έξυπνης συσκευής IoT, όπως φαίνεται στην Εικόνα 40: Αναμονή (Stand By) 24-38mA, Μετάδοση (Broadcasting) 58-72mA και Κίνηση (Movement) 102- 116mA.

Εικόνα 40: Κατανάλωση ρεύματος web κάμερας και δημιουργία συστάδων

Αυτές οι συστάδες χρησιμοποιούνται από τον αλγόριθμο ανίχνευσης εισβολής ενώ ελέγχουν σε πραγματικό χρόνο την κατανάλωση ισχύος της συσκευής IoT. Εάν η τιμή κατανάλωσης ισχύος της συσκευής IoT δε βρίσκεται μεταξύ του κατώτερου και ανώτερου ορίου (κατωφλίων) των δημιουργημένων συστάδων, το σύστημα εντοπίζει μία δυσλειτουργία ή μία επίθεση στην συσκευή IoT.

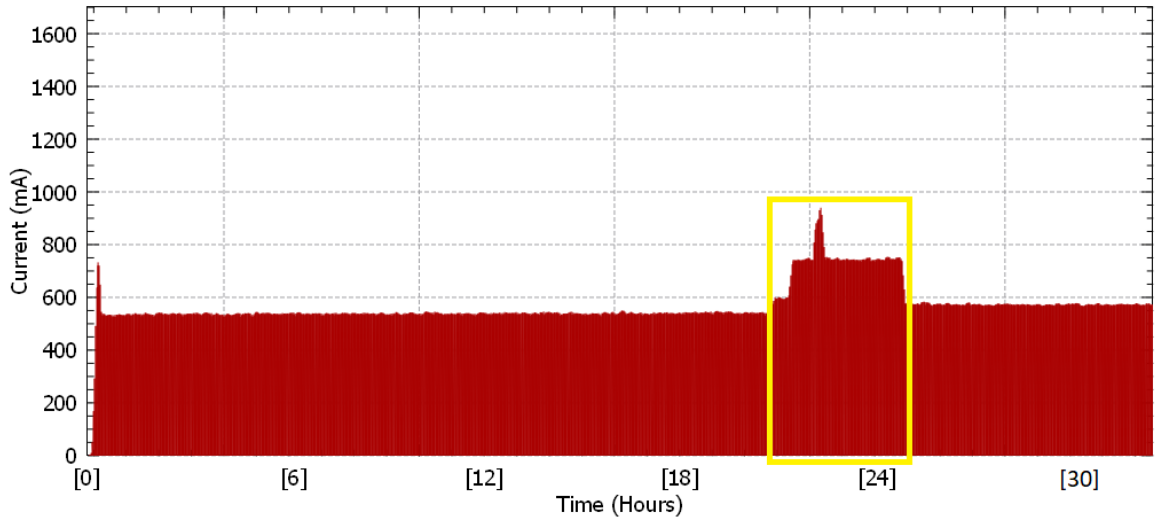
Πρέπει να τονιστεί ότι αναμένεται να έχει διαφορετικά αποτελέσματα για πανομοιότυπες συσκευές εγκατεστημένες σε τοποθεσίες με διαφορετικές συνθήκες (π.χ. εσωτερικούς ή εξωτερικούς χώρους) ή ακόμη και στην ίδια συσκευή IoT όταν εγκαθίσταται σε διαφορετικές τοποθεσίες με διαφορετική ποιότητα ισχύος. Αυτό εξηγεί την αναγκαιότητα της ποιοτικής ανάλυσης της εισόδου, σε αντίθεση με την προηγούμενη ποσοτική ανάλυση που πραγματοποιήθηκε από τα [6, 106, 107], το οποίο είναι επιρρεπές στα χαρακτηριστικά του δικτύου ισχύος στην περιοχή.

Στην Εικόνα 41 απεικονίζονται οι μετρήσεις του ρεύματος τροφοδοσίας κατά τη διάρκεια του πειράματος (32 ώρες), χωρίς τη χρήση οποιουδήποτε φίλτρου (υλικό ή λογισμικό). Ως αποτέλεσμα, υπάρχει πολύς θόρυβος στο σήμα (spikes), που επηρεάζει την ανίχνευση της επίθεσης, η οποία μπορεί να παρατηρηθεί εντός του κίτρινου πλαισίου.



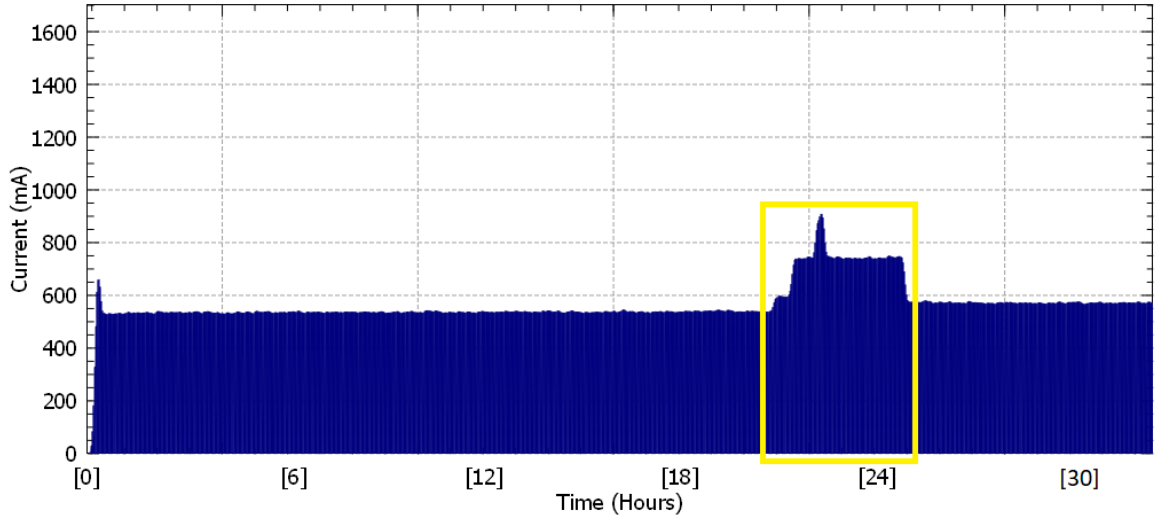
Εικόνα 41: Μετρήσεις χωρίς χρήση λογισμικού φίλτρου

Ωστόσο, μετά την εφαρμογή του πρώτου λογισμικού φίλτρου, όπως παρατηρείται στην Εικόνα 42, οι τιμές που λαμβάνονται είναι απαλλαγμένες από το θόρυβο και η μορφή του σήματος είναι πλέον κατάλληλη για τον αλγόριθμο ML που θα εκπαιδευτεί. Το φίλτρο αφαίρεσε τυχαίες αιχμές που δεν είχαν καμία αξία στην ανάλυση του ρεύματος τροφοδοσίας.



Εικόνα 42: Μετρήσεις εφαρμόζοντας το πρώτο λογισμικό φίλτρο

Τέλος, για να εξαλειφθεί κάθε πιθανότητα εμφάνισης ψευδώς θετικής ένδειξης επίθεσης, εφαρμόστηκε και ένα δεύτερο φίλτρο λογισμικού για περαιτέρω εξομάλυνση του σήματος. Τα αποτελέσματα των μετρήσεων παρουσιάζονται στην Εικόνα 43, όπου η ανίχνευση της επίθεσης διακρίνεται εντός του κίτρινου πλαισίου.

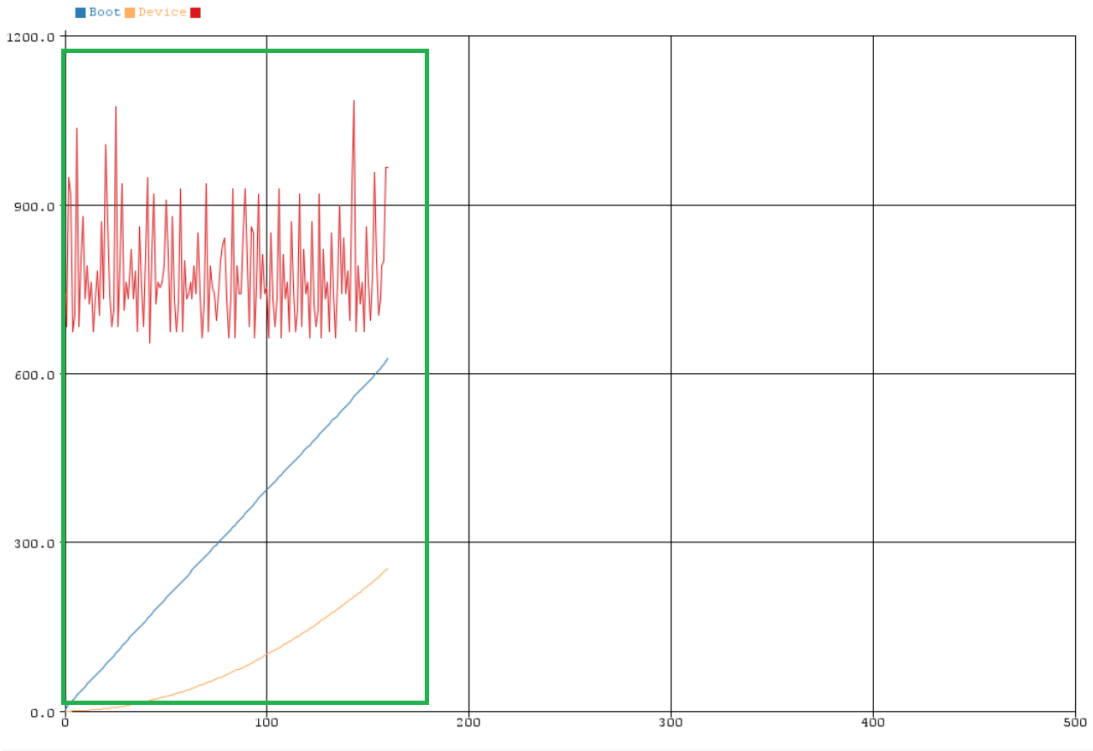


Εικόνα 43: Μετρήσεις εφαρμόζοντας το δεύτερο λογισμικό φίλτρο

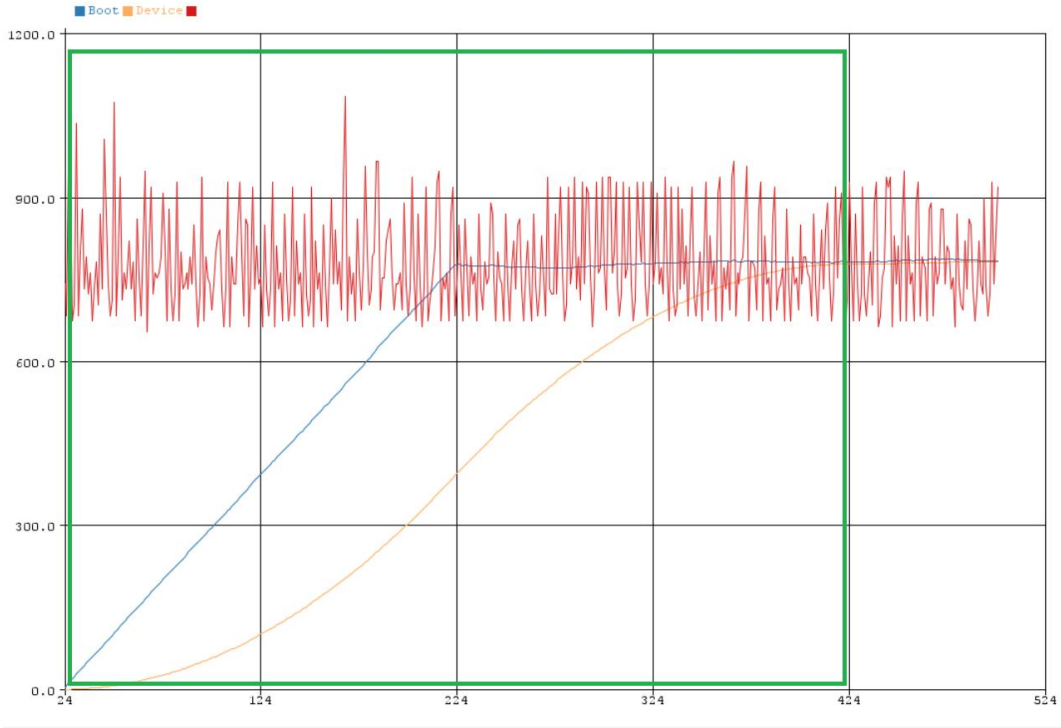
Η συσκευή SmartShell είχε τέσσερις τρόπους λειτουργίας που αναλύονται παρακάτω, όπως προκύπτει από τον αλγόριθμο ML. Η κόκκινη γραμμή στα διαγράμματα απεικονίζει την ένταση του ρεύματος, ενώ η μπλε και κίτρινη απεικονίζουν τις τιμές από το πρώτο και το δεύτερο λογισμικό φίλτρο αντίστοιχα, τα οποία αναφέρθηκαν

παραπάνω. Επιπλέον, στο επάνω αριστερό μέρος των εικόνων, εμφανίζεται η τρέχουσα λειτουργία της συσκευής SmartShell.

Κάθε συσκευή IoT όταν εκκινεί, χρησιμοποιεί πολλούς πόρους, με αποτέλεσμα η ένταση του ρεύματος να είναι μεγαλύτερη από την κανονική λειτουργία της. Έτσι, επιλέχθηκε ένας αρχικός χρόνος αδράνειας (5 λεπτά) ώστε να ξεκινήσει η κάμερα IP, χωρίς να ξεκινήσει η εκπαίδευσή της. Η παραπάνω λειτουργία ονομάζεται «Boot Device» και παρουσιάζεται στην Εικόνα 44 και Εικόνα 45. Παρατηρήθηκε ότι η κάμερα από ένα σημείο και μετά, αρχίζει να παρουσιάζει μία φυσιολογική συμπεριφορά (βλ. Εικόνα 45, μετά το πράσινο πλαίσιο), καθώς οι τιμές συγκλίνουν.

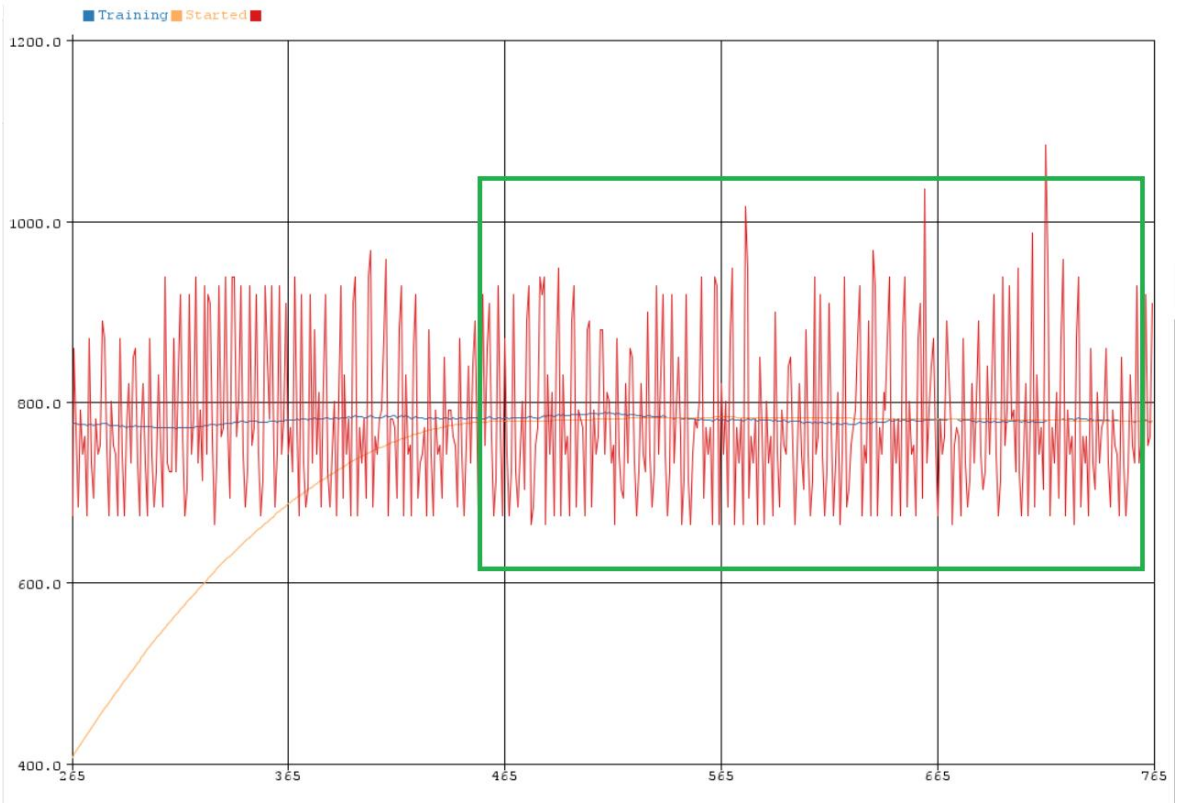


Εικόνα 44: Κατάσταση εκκίνησης συσκευής 1

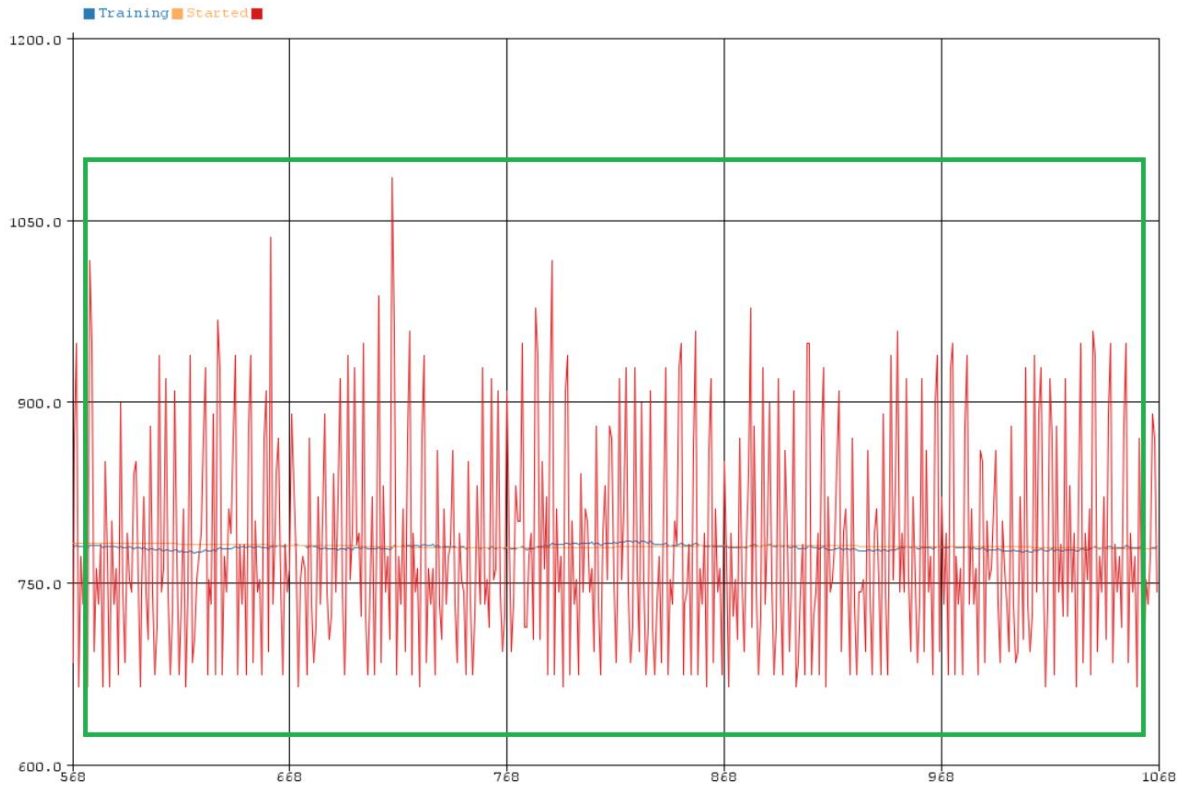


Εικόνα 45: Κατάσταση εκκίνησης συσκευής 2

Στη συνέχεια, η συσκευή εφόσον ολοκληρώσει το χρόνο εκκίνησης, ξεκινά την εκπαίδευση και αυτό απεικονίζεται στην Εικόνα 46 μέσα στο πράσινο πλαίσιο. Κατά τη διάρκεια της εκπαίδευσης, μελετώνται η λειτουργικότητα και οι συνθήκες της συσκευής στόχου (π.χ. κάμερα IP). Για παράδειγμα, λήψη ακίνητης εικόνας, λήψη κινούμενης εικόνας, λήψη εικόνας κατά τη διάρκεια της ημέρας ή της νύχτας, αναμονή και πολλά άλλα. Τέλος, δημιουργεί τις συστάδες που αντιστοιχούν στους τρόπους λειτουργίας της στοχευμένης συσκευής IoT. Για λόγους παρουσίασης, οι συστάδες ορίζονται σε δύο από τον χρήστη για το παρόν πείραμα. Αυτή η λειτουργία ονομάζεται «Training Started» και εμφανίζεται στην Εικόνα 46 και Εικόνα 47.

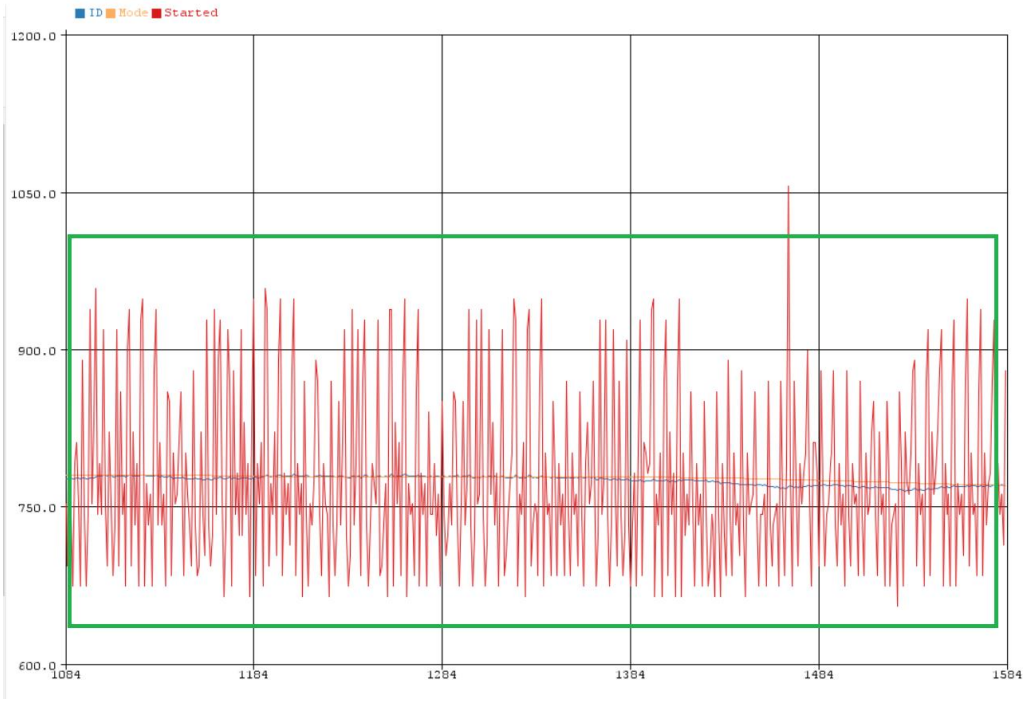


Εικόνα 46: Κατάσταση εκπαίδευσης 1

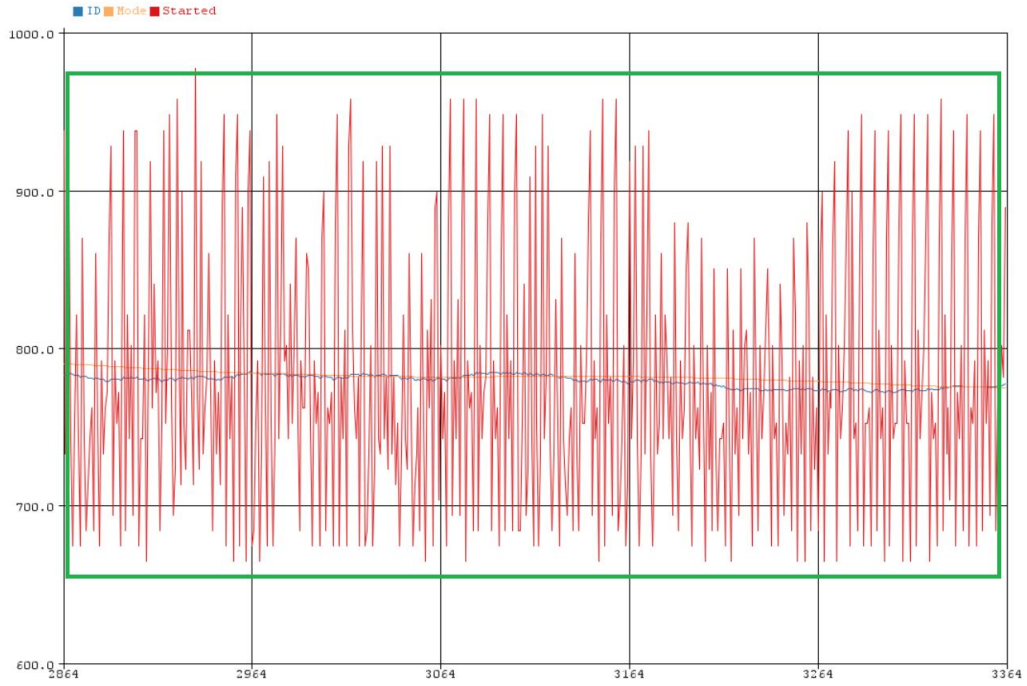


Εικόνα 47: Κατάσταση εκπαίδευσης 2

Εν συνεχεία, η συσκευή εφόσον έχει ολοκληρώσει τον κύκλο εκπαίδευσης, τοποθετείται σε κατάσταση μόνιμης λειτουργίας ανίχνευσης εισβολής, κατά τη διάρκεια της οποίας η συσκευή ανιχνεύει τυχόν επιθέσεις που γίνονται στην κάμερα. Αυτή η λειτουργία ονομάζεται «ID Mode Started» και παρουσιάζεται στην Εικόνα 48 και Εικόνα 49.



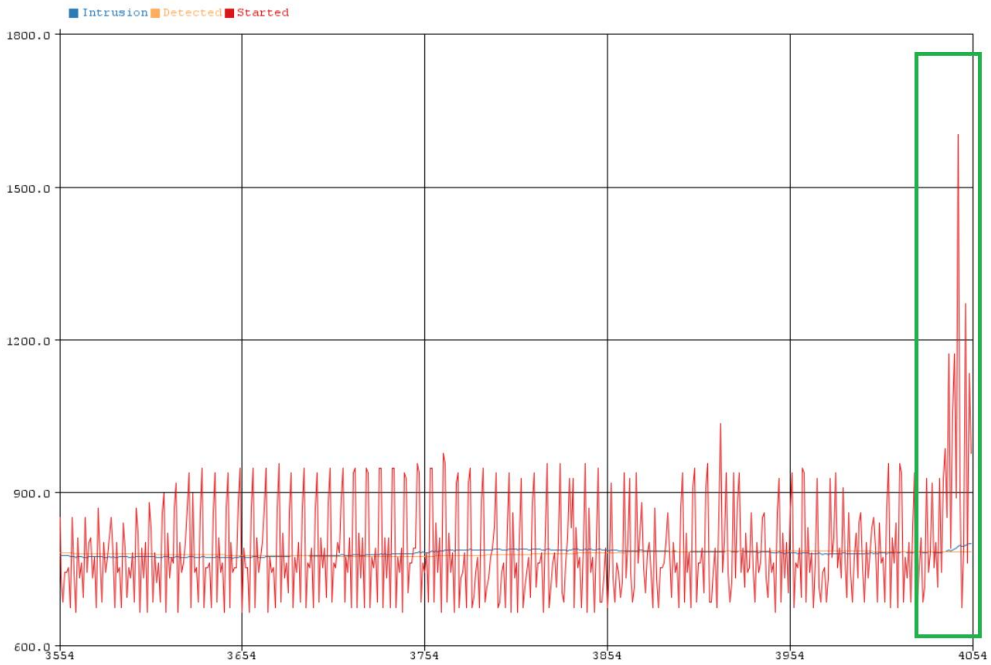
Εικόνα 48: Κατάσταση ανίχνευσης εισβολής 1



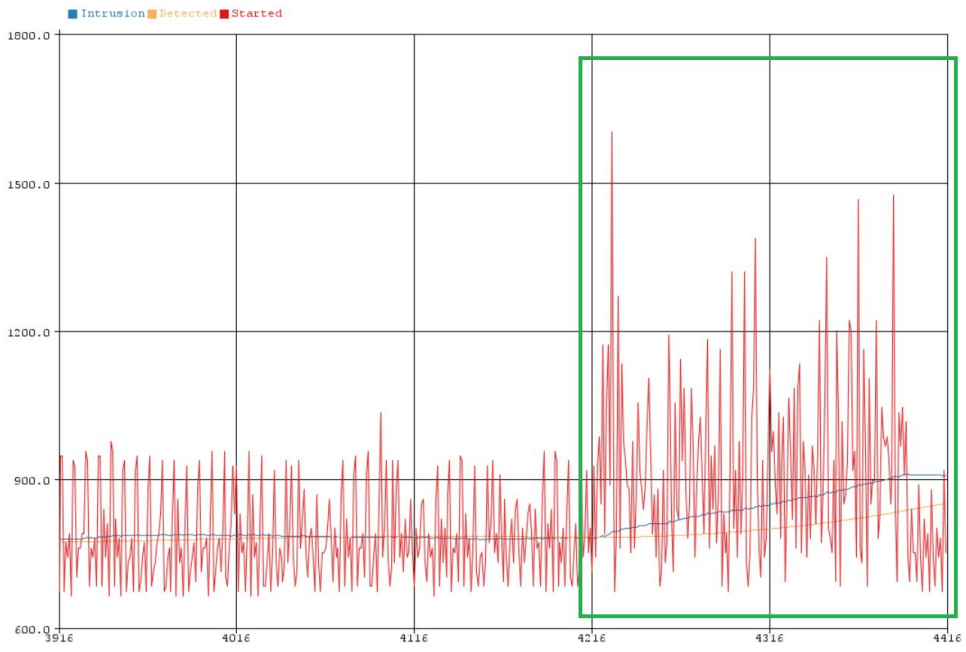
Εικόνα 49: Κατάσταση ανίχνευσης εισβολής 2

Τέλος, στην Εικόνα 50 και εντός του πράσινου πλαισίου, παρατηρείται χαρακτηριστικά η ανίχνευση της επίθεσης σε πολύ μικρό χρονικό διάστημα (ανίχνευση σε πραγματικό χρόνο) από τη συσκευή, καθώς ο ρυθμός δειγματοληψίας

όπως αναφέρεται παραπάνω είναι 100ms. Κατά τη διάρκεια ανίχνευσης της επίθεσης, το σύστημα ενημερώνεται, εμφανίζοντας ένα μήνυμα «Intrusion Detected Started» όπως φαίνεται στην Εικόνα 50 και Εικόνα 51, επάνω και αριστερά. Αυτή η λειτουργία της συσκευής ονομάζεται «Intrusion Detected Started».

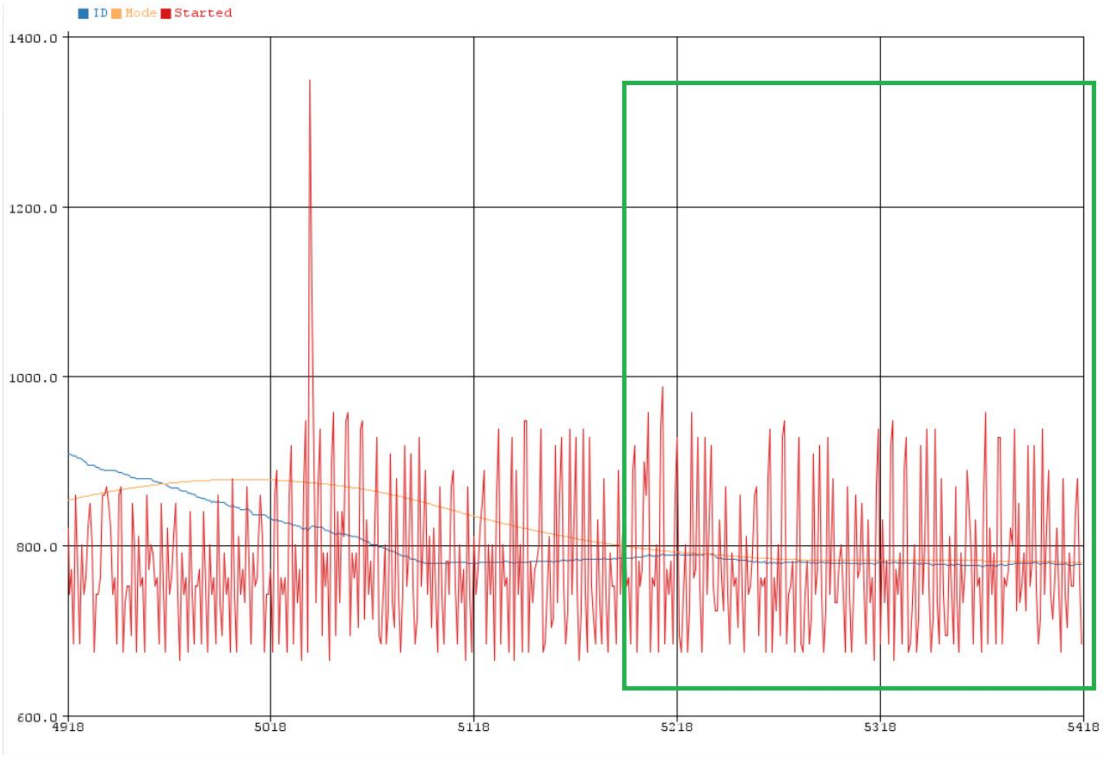


Εικόνα 50 Ανίχνευση εισβολής 1

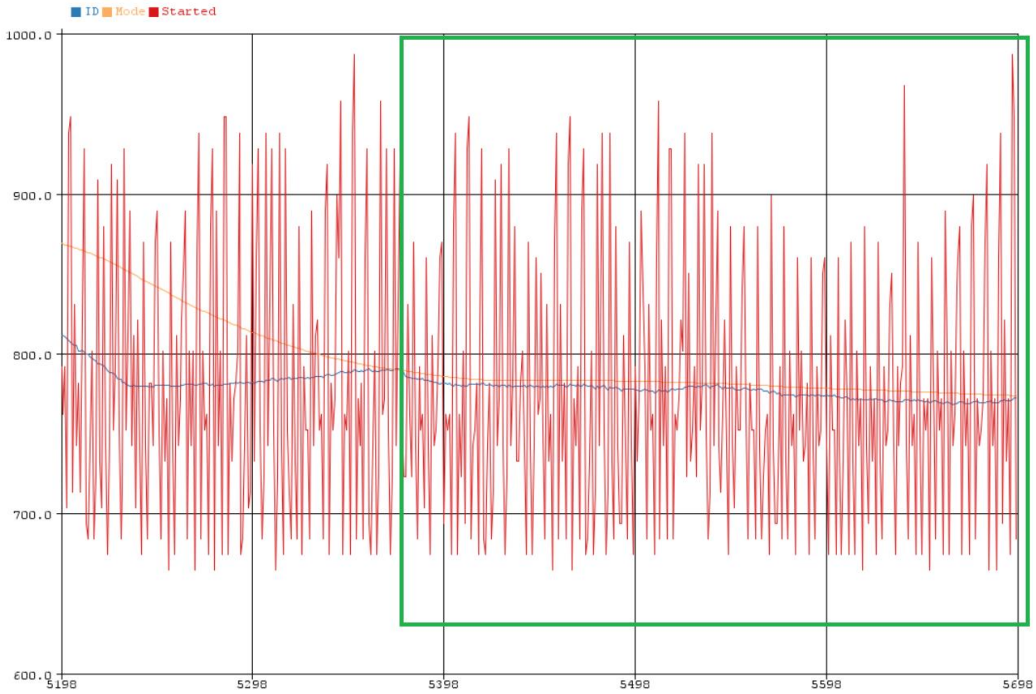


Εικόνα 51: Ανίχνευση εισβολής 2

Στην Εικόνα 52 και Εικόνα 53 εμφανίζεται η άμεση απόκριση του συστήματος της συσκευής, στην επαναφορά της στο «ID Mode Started», μετά την επίθεση. Αυτό είναι εύκολα αντιληπτό, καθώς εντός του πράσινου πλαισίου απεικονίζεται η ανίχνευση της φυσιολογικής συμπεριφοράς της συσκευής. Ταυτόχρονα, το μήνυμα με την τρέχουσα κατάσταση της συσκευής εμφανίζεται στο επάνω αριστερό μέρος των εικόνων.



Εικόνα 52: Κατάσταση ανίχνευσης εισβολής μετά την επίθεση 1



Εικόνα 53: Κατάσταση ανίχνευσης εισβολής μετά την επίθεση 2

Συνοψίζοντας λοιπόν τη λειτουργία της συσκευής ανίχνευσης «SmartShell», παρατηρήθηκαν τέσσερις τρόποι λειτουργίας, όπως παρακάτω:

1. Η λειτουργία «Boot Device», στην οποία η Smart Shell περιμένει την εκκίνηση της κάμερας IP, χωρίς να ξεκινήσει η εκπαίδευση ή ο εντοπισμός εισβολής.

2. Η λειτουργία «Training Started», στην οποία η Smart Shell εκπαιδεύτηκε στις λειτουργίες της κάμερας (π.χ. συνεχής ροή κίνησης, αναμονή, μετάδοση κ.λπ.) και δημιούργησε τα διάφορα σύνολα αυτών των λειτουργιών που πρόκειται να χρησιμοποιηθούν από τον αλγόριθμο Ανίχνευσης Εισβολής.

3. Η λειτουργία «ID Mode Started», στην οποία η συσκευή, ακόμη και μετά την ολοκλήρωση της εκπαίδευσης, εντοπίζει τυχόν επιθέσεις που πρόκειται να γίνουν στην κάμερα, με βάση την προηγούμενη εκπαίδευση.

4. Και τέλος, η λειτουργία «Intrusion Detected Started», στην οποία εντοπίστηκαν οι επιθέσεις και το σύστημα ενημερώθηκε παρουσιάζοντας ένα μήνυμα.

Η προτεινόμενη λύση είναι αυτόνομη και ενεργοποιεί πρωτόκολλα ασφαλείας μετά τον εντοπισμό εισβολής. Δεδομένου ότι αυτή είναι η πρώτη συσκευή του είδους της (ενσωμάτωση αλγορίθμου ML), δεν είναι απαραίτητο να γίνει σύγκριση με παρόμοιες λύσεις, αν και ενσωματώνουν αλγόριθμο ML για την ανίχνευση της εισβολής. Επιπλέον, παρόλο που δεν υπάρχουν σύνολα δεδομένων για το σκοπό αυτό, στον Πίνακα 3 η προτεινόμενη εργασία συγκρίνεται με τις μόνες παρόμοιες εφαρμογές κατά τη διάρκεια 3 διαφορετικών τύπων επιθέσεων. Επίθεση DoS όπως περιγράφηκε προηγουμένως, επίθεση mirai και επίθεση zero-day. Στις παρενθέσεις παρέχεται το ποσοστό ψευδώς θετικής ανίχνευσης. Οι μετρήσεις για τις υπαίθριες εγκαταστάσεις πραγματοποιήθηκαν κατά τη διάρκεια του καλοκαιριού, καθώς δεν υπάρχουν διαθέσιμα δεδομένα για τις υπόλοιπες εποχές.

Προκειμένου να επισημανθούν τα επιπλέον πλεονεκτήματα της προτεινόμενης λύσης, εξετάστηκαν περαιτέρω οι εγκαταστάσεις του SmartShell σε διάφορα περιβάλλοντα. Για τις ανταγωνιστικές υλοποιήσεις θεωρήσαμε προ-διαμορφωμένες, καθώς δεν υπάρχει δυνατότητα εκπαίδευσης.

Work	DoS (in)	mirai (in)	zero-day (in)	DoS (out)	mirai (out)	zero-day (out)
[9]	95(2)	100(2)	100(2)	81(22)	100(15)	69(40)
[10]	96(2)	100(2)	100(1)	83(17)	100(15)	70(22)
[30]	96(2)	100(1)	100(1)	84(15)	100(13)	72(20)
[12]	98(2)	100(1)	100(1)	86(12)	100(11)	**75(20)**
This work	**100(0)**	**100(0)**	0(100)	**100(1)**	**100(2)**	0(100)
Mod. work	**100(0)**	**100(0)**	**100(1)**	**100(1)**	**100(2)**	72(20)

Πίνακας 3: Σύγκριση εργασιών ανίχνευσης εισβολής από αυτόνομα ενσωματωμένα συστήματα. Οι αριθμοί αντιστοιχούν στο ποσοστό της αληθώς θετικής ανίχνευσης εισβολής και σε παρένθεση το αντίστοιχο ποσοστό ψευδώς θετικής ανίχνευσης.

Όπως μπορεί να παρατηρηθεί στον Πίνακα 3, η προτεινόμενη λύση παρουσίασε την καλύτερη βαθμολογία σε σύγκριση με τις ανταγωνιστικές. Το κύριο μειονέκτημα του προτεινόμενου συστήματος εντοπίστηκε σε μία επίθεση zero-day, στην οποία η ακολουθία εκκίνησης είναι μέρος της επίθεσης και κατά τη διάρκεια αυτής της χρονικής περιόδου το σύστημα παραμένει αδρανές, καθώς δεν έχει προκαθορισμένες

ελάχιστες και μέγιστες τιμές για τις συστάδες. Μετά την εφαρμογή προκαθορισμένων τιμών παρόμοιες με αυτές που περιγράφονται στο [107], η τροποποιημένη έκδοση του προτεινόμενου πειράματος παρουσιάζει επαρκή ανίχνευση εισβολής. Όλα τα έργα παρουσίασαν υψηλή βαθμολογία στην επίθεση mirai, καθώς προκαλεί υψηλή δραστηριότητα. Στην επίθεση DoS τα αποτελέσματα ήταν δίκαια, καθώς η δραστηριότητα μπορεί να ελεγχθεί. Στην επίθεση zero-day το τροποποιημένο προτεινόμενο έργο παρουσιάζει δίκαια αποτελέσματα. Όπως ήταν αναμενόμενο, τα αποτελέσματα μετρήσεων των πειραμάτων που βασίστηκαν σε διαφορετικές εγκαταστάσεις, έδειξαν ότι η μοντελοποίηση της ισχύος του ρεύματος σε ένα ελεγχόμενο περιβάλλον (π.χ. εσωτερικό) είναι κοντά στο θεωρητικό μοντέλο (π.χ. εργαστηριακές συνθήκες), σε αντίθεση με τα αποτελέσματα σε εξωτερικό περιβάλλον, που έχουν σημαντικές αποκλίσεις λόγω των συνθηκών (π.χ. θερμοκρασία) [122] και της ποιότητας τροφοδοσίας κατά τη διάρκεια μίας σεζόν [123].

5.7.4 Συμπεράσματα

Σε αυτό το πείραμα, παρουσιάστηκε ένα αυτόνομο σύστημα παρακολούθησης ρεύματος που εκμεταλλεύεται την τεχνική της SCA, το οποίο μπορεί να χρησιμοποιηθεί για την έξυπνη προστασία έξυπνων συσκευών, μέσω εντοπισμού ύποπτης συμπεριφοράς, ενσωματώνοντας έναν αλγόριθμο ML για ανίχνευση εισβολής. Το σύστημα εκμεταλλεύεται χαρακτηριστικά της παροχής του ρεύματος, για το βέλτιστο αποτέλεσμα. Το προτεινόμενο σύστημα είναι πρωτότυπο και χρησιμοποιεί τον αλγόριθμο *k*-Means Clustering με εκπαίδευση χωρίς επίβλεψη. Τα αποτελέσματα αυτού του πειράματος έδειξαν επιτυχημένη ανίχνευση, απεικόνιση και αναφορά των επιθέσεων σε έξυπνες συσκευές IoT σε πραγματικό χρόνο. Τα αποτελέσματα απεικόνισαν την ισχυρή ανίχνευση εισβολής που διενεργήθηκε από την προτεινόμενη λύση σε αντίθεση με ανταγωνιστικές αυτόνομες εφαρμογές χαμηλού κόστους και μικρού μεγέθους. Ένα μειονέκτημα της προτεινόμενης λύσης είναι η αρχική κατάσταση αδράνειας κατά την ακολουθία εκκίνησης, η οποία μπορεί να χρησιμοποιηθεί για την επίθεση της υπό προστασία συσκευής IoT.

Επειδή αυτή είναι η πρώτη συσκευή του είδους της και λόγω της έλλειψης σημείων αναφοράς, σκοπός είναι να χρησιμοποιηθεί ως βασικό κύκλωμα, ώστε να δημιουργηθούν σύνολα δεδομένων για μελλοντικά έργα, τα οποία πρόκειται να συγκριθούν με την παρούσα λύση. Έτσι, από τεχνική άποψη, δεν υπάρχουν σύνολα δεδομένων και άλλες ανταγωνιστικές συσκευές, που να επιτρέπουν τη σύγκριση αυτή τη στιγμή. Επιπλέον, υπάρχουν σημαντικές δυνατότητες για μελλοντική εργασία σε τομείς όπως, security και privacy, η προσθήκη και ο συνδυασμός πρόσθετων φυσικών χαρακτηριστικών των συσκευών, ή ακόμη και η βελτίωση της ίδιας της συσκευής με την αυτόματη ανίχνευση της τιμής *k*.

6 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ

Είναι αναμφίβολο ότι πρέπει να γίνουν ακόμη σημαντικά βήματα στον τομέα της ασφάλειας αλλά και της ασφαλής υποδομής του IoT. Όσον αφορά τα κρίσιμα συστήματα, όπως για παράδειγμα του κλάδου της υγειονομικής περίθαλψης, οι συσκευές που χρησιμοποιούνται προσφέρουν ένα ευρύ ερευνητικό φάσμα για την ανάπτυξη αποτελεσματικών μηχανισμών ασφάλειας και απορρήτου των ευαίσθητων δεδομένων, για την προστασίας της ιδιωτικής ζωής. Ακόμη και σε αυτό το πλαίσιο, έχουμε εξετάσει και αποδείξει ότι με την παρακολούθηση έμμεσων χαρακτηριστικών των συσκευών IoT, είναι δυνατόν να αντλήσουμε ασφαλή αποτελέσματα ως προς το εάν η συσκευή δέχεται επίθεση ενεργοποιώντας τους αντίστοιχους μηχανισμούς προστασίας.

Η παρούσα διδακτορική διατριβή εισηγήθηκε μια αρχιτεκτονική ενός συστήματος ικανού να παρακολουθήσει την υγεία μιας έξυπνης συσκευής IoT ως προς την αξιοπιστία τους και την ασφάλειά τους. Το σύστημα τοποθετείται εξωτερικά επιτρέποντας την υιοθέτησή του στο σύνολο των συσκευών IoT ενώ η προσέγγιση σχεδίασης και υλοποίησης βασίστηκε σε παραμέτρους κόστους και σχεδιαστικής απλότητας. Αξιοποιώντας χαρακτηριστικά λειτουργίας, όπως είναι το ρεύμα τροφοδοσίας, ήταν δυνατή η δημιουργία μετρικών καλής λειτουργίας (αναμενόμενης εναλλακτική – normal operation) και μετρικών ανώμαλης συμπεριφοράς (anomaly). Παρόλο που στα πειράματά μας εξετάσαμε απλά σενάρια για διάφορες καθημερινές εφαρμογές, η προσέγγιση είναι ίδια για όλες σχεδόν τις συσκευές IoT. Έχουμε εξετάσει και αποδείξει ότι με την παρακολούθηση έμμεσων χαρακτηριστικών των συσκευών IoT, είναι δυνατόν να αντλήσουμε ασφαλή αποτελέσματα ως προς το εάν η συσκευή δέχεται επίθεση ενεργοποιώντας τους αντίστοιχους μηχανισμούς προστασίας. Τελικά, η παρούσα διατριβή προσπαθεί να αντιμετωπίσει τόσο την αξιοπιστία όσο και τα ζητήματα ασφάλειας με βάση τη βιοϊσοδυναμία των συσκευών του IoT, εξετάζοντας την «υγεία» της ίδιας της συσκευής.

Στη συνέχεια προτάθηκε μεθοδολογία ενσωμάτωσης σε μια συσκευή χαμηλού κόστους και χαμηλής υπολογιστικής ισχύος, μηχανισμού μηχανικής μάθησης προκειμένου να είναι δυνατή η ανίχνευση της ανωμαλίας (anomaly detection), για οποιοδήποτε τρόπο λειτουργίας (operation mode) και κάτω από οποιεσδήποτε

συνθήκες, καθώς από την παρατήρηση προέκυψε πώς η ίδια συσκευή μπορεί να παρουσιάζει διαφορετικό προφίλ λειτουργίας αν τοποθετηθεί σε εσωτερικό ή εξωτερικό χώρο, αν οι μετρήσεις γίνονται την άνοιξη ή το χειμώνα κ.ο.κ. Συνεπώς αυτό έκανε περισσότερο επιτακτική την αξιοποίηση μηχανισμού μηχανικής μάθησης μη επιβλεπόμενου προκειμένου να λαμβάνονται υπόψη όλα τα χαρακτηριστικά λειτουργίας και συμπεριφοράς, σε κάθε περιβάλλον λειτουργίας. Η προτεινόμενη λύση είναι γενική και έχει εφαρμογή επίσης σε κάθε συσκευή IoT και δεν χρειάζεται διαφορετική σχεδίαση αλλά είναι αυτόματα προσαρμοζόμενη. Τα αποτελέσματα έδειξαν ότι εφαρμόζοντας ένα απλό πρωτόκολλο αντιμετώπισης, όπως της απομόνωσης (lockdown), η αντιμετώπιση της δημιουργίας ενός botnet είναι επιτυχής επιτυγχάνοντας υψηλά επίπεδα θετικών αληθών αναγνωρίσεων επίθεσης.

Η μελλοντική εργασία περιλαμβάνει την ενίσχυση των δυνατοτήτων παρακολούθησης με την εφαρμογή και τον πειραματισμό, μετρήσεων υπό μία ποικιλία φυσικών χαρακτηριστικών, καθώς και πιθανή δημιουργία του κυκλώματος σε ολοκληρωμένο. Αυτή η διδακτορική διατριβή είναι η αρχή για την ανάπτυξη ενός ολοκληρωμένου συστήματος που χρησιμοποιεί τεχνολογία VLSI, για την εισαγωγή εξωτερικών συστημάτων ασφαλείας σε οικιακές συσκευές και συσκευές IoT. Η επέκταση των παραμέτρων που παρακολουθούνται για τα ζητήματα της ασφάλειας που αντιμετωπίζουν τα Συστήματα Ανίχνευσης Εισβολής (IDS) αναμένεται να ενσωματωθεί σύντομα σε μεγάλα συστήματα.

Η κύρια συνεισφορά της παρούσας διατριβή είναι η δυνατότητα επέκτασης των παραμέτρων ανάλυσης για την αντιμετώπιση μιας επαυξημένης επιφάνειας επίθεσης όπως αυτή των συσκευών IoT, αξιοποιώντας τα φυσικά χαρακτηριστικά λειτουργίας τους ως επιπλέον παραμέτρους. Στο μέλλον θα είναι δυνατή η ενσωμάτωση πολύπλοκων ευφυών τεχνολογιών σε συσκευές ειδικού σκοπού για αυτό το λόγο, αξιοποιώντας ως βάση την παρούσα διδακτορική διατριβή. Επιπλέον χαρακτηριστικά είναι η ενσωμάτωση της αυτοεπίγνωση της κατάστασης λειτουργίας του συστήματος ώστε να είναι δυνατή η online ανάλυση στο πεδίο του χρόνου, όπως ανάλυση της σταθερότητας και της ασφάλειας. Τέλος, αντικείμενο μελέτης είναι τα πρωτόκολλα αντιμετώπισης, όπως κάποιο σύστημα αυτοθεραπείας ή αντεπίθεσης.

Βιβλιογραφία

[2] P. K. Lala, *Self-checking and fault-tolerant digital design*: Morgan Kaufmann, 2001.

[3] N. Sklavos, "On the hardware implementation cost of crypto-processors architectures," *Information Security Journal: A Global Perspective,* vol. 19, pp. 53-60, 2010.

[4] Y. Agarwal and A. K. Dey, "Toward building a safe, secure, and easy-to-use internet of things infrastructure," *Computer,* pp. 88-91, 2016.

[5] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu, "On code execution tracking via power side-channel," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 1019-1031.

[6] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schoinianakis, and J. Lueken, "Anomaly detection in iot devices via monitoring of supply current," in *2018 IEEE 8th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)*, 2018, pp. 1-4.

[7] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of things journal,* vol. 3, pp. 70-95, 2015.

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks,* vol. 54, pp. 2787-2805, 2010.

[9] A. S. M. Mosa, I. Yoo, and L. Sheets, "A systematic review of healthcare applications for smartphones," *BMC medical informatics and decision making,* vol. 12, p. 67, 2012.

[14] V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, 2011, pp. 1-6.

[15] E. Gayat, A. Bodin, C. Sportiello, M. Boisson, J.-F. Dreyfus, E. Mathieu, *et al.*, "Performance evaluation of a noninvasive hemoglobin monitoring device," *Annals of emergency medicine,* vol. 57, pp. 330-333, 2011.

[16] M. Pesta, J. Fichtl, V. Kulda, O. Topolcan, and V. Treska, "Monitoring of circulating tumor cells in patients undergoing surgery for hepatic metastases from colorectal cancer," *Anticancer research,* vol. 33, pp. 2239-2243, 2013.

[18] Z. Pang, J. Tian, and Q. Chen, "Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things," in *16th International Conference on Advanced Communication Technology*, 2014, pp. 352-360.

[19] Y. J. Fan and Y. H. Yin, "Member, IEEE, Li Da Xu, Senior Member, IEEE, Yan Zeng, and Fan Wu," IoT-Based Smart Rehabilitation System"," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 10, 2014.

[20] M. I. Bhat, S. Ahmad, A. Amin, and S. Ashraf, "e-Health with internet of things," *Int. J. Comput. Sci. Mob. Comput*, vol. 6, pp. 357-362, 2017.

[21] Z. Guangnan and L. Penghui, "IoT (Internet of Things) control system facing rehabilitation training of hemiplegic patients," *Chinese Patent*, vol. 202, p. 045, 2012.

[22] Y. Yue-Hong, F. Wu, F. Y. Jie, L. Jian, X. Chao, and Z. Yi, "Remote medical rehabilitation system in smart city," *Chinese Patent*, vol. 103, p. 880, 2014.

[23] S. Liang, Y. Zilong, S. Hai, and M. Trinidad, "Childhood autism language training system and Internet-of-Things-based centralized training center," *Chinese Patent*, vol. 102, p. 661, 2011.

[24] H. A. Khattak, M. Ruta, and E. E. Di Sciascio, "CoAP-based healthcare sensor networks: A survey," in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*, 2014, pp. 499-503.

[25] E. C. Larson, M. Goel, M. Redfield, G. Boriello, M. Rosenfeld, and S. N. Patel, "Tracking lung function on any phone," in *Proceedings of the 3rd ACM Symposium on Computing for Development*, 2013, pp. 1-2.

[26] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, *et al.*, "Internet of Things in healthcare: Interoperatibility and security issues," in *2012 IEEE international conference on communications (ICC)*, 2012, pp. 6121-6125.

[27] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678-708, 2015.

[28] A. Dohr, R. Modre-Opsrian, and M. Drobics, "Dieter Hayn in Guenter Schreier. The internet of things for ambient assisted living," in *2010 Seventh International Conference on Information Technology: New Generations. Institute of Electrical & Electronics Engineers (IEEE)*, 2010.

[29] B. J. Drew, R. M. Califf, M. Funk, E. S. Kaufman, M. W. Krucoff, M. M. Laks, *et al.*, "Practice standards for electrocardiographic monitoring in hospital settings: an American Heart Association scientific statement from the Councils on Cardiovascular Nursing, Clinical Cardiology, and Cardiovascular Disease in the Young: endorsed by the International Society of Computerized Electrocardiology and the American Association of Critical-Care Nurses," *Circulation*, vol. 110, pp. 2721-2746, 2004.

[30] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, *et al.*, "Health monitoring and management using Internet-of-Things (IoT)

sensing with cloud-based processing: Opportunities and challenges," in *2015 IEEE International Conference on Services Computing*, 2015, pp. 285-292.

[31] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192-202, 2016.

[32] M. Marudhapandi, D. Ramkumar, R. Ramkumar, S. Jeevanandham, and N. Suguna, "Wearable ECG Monitoring System and Data Analysis," 2019.

[33] A. Rahman, T. Rahman, N. H. Ghani, S. Hossain, and J. Uddin, "IoT based patient monitoring system using ECG sensor," in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 2019, pp. 378-382.

[34] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An IoT-cloud based wearable ECG monitoring system for smart healthcare," *Journal of medical systems*, vol. 40, p. 286, 2016.

[35] T. N. Gia, M. Ali, I. B. Dhaou, A. M. Rahmani, T. Westerlund, P. Liljeberg, *et al.*, "IoT-based continuous glucose monitoring system: A feasibility study," *Procedia Computer Science*, vol. 109, pp. 327-334, 2017.

[36] R. S. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2011, pp. 5264-5266.

[37] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE network*, vol. 20, pp. 41-47, 2006.

[38] A. H. Alqahtani and M. Iftikhar, "TCP/IP attacks, defenses and security tools," *International Journal of Science and Modern Engineering (IJISME)*, vol. 1, pp. 42-47, 2013.

[39] G. Yang, M. Gerla, and M. Sanadidi, "Defense against low-rate TCP-targeted denial-of-service attacks," in *Proceedings. ISCC 2004. Ninth International Symposium on Computers And Communications (IEEE Cat. No. 04TH8769)*, 2004, pp. 345-350.

[40] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, "One-time cookies: Preventing session hijacking attacks with stateless authentication tokens," *ACM Transactions on Internet Technology (TOIT)*, vol. 12, pp. 1-24, 2012.

[41] R. Holz, Y. Sheffer, and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)," *Request for Comments*, vol. 7457, 2019.

[42] H. Beitollahi and G. Deconinck, "Tackling application-layer DDoS attacks," *Procedia Computer Science*, vol. 10, pp. 432-441, 2012.

[43] J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," in *13th Pacific Rim international symposium on dependable computing (PRDC 2007)*, 2007, pp. 365-372.

[44] P. De Ryck, L. Desmet, W. Joosen, and F. Piessens, "Automatic and precise client-side protection against CSRF attacks," in *European Symposium on Research in Computer Security*, 2011, pp. 100-116.

[45] T. Ylonen and C. Lonvick, "The secure shell (SSH) protocol architecture," ed: RFC 4251, January, 2006.

[46] S. Mansfield-Devine, "Ransomware: the most popular form of attack," *Computer Fraud & Security*, vol. 2017, pp. 15-20, 2017.

[47] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 195-212.

[48] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Computer Networks*, 2019.

[49] S. Sicari, A. Rizzardi, L. Grieco, G. Piro, and A. Coen-Porisini, "A policy enforcement framework for Internet of Things applications in the smart health," *Smart Health*, vol. 3, pp. 39-74, 2017.

[50] H. A. El Zouka and M. M. Hosni, "Secure IoT communications for smart healthcare monitoring system," *Internet of Things*, p. 100036, 2019.

[51] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Policy-based access control for constrained healthcare resources in the context of the Internet of Things," *Journal of Network and Computer Applications*, vol. 139, pp. 57-74, 2019.

[52] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *Ieee Access*, vol. 6, pp. 20596-20608, 2018.

[54] P. Kitsos, N. Sklavos, and A. G. Voyiatzis, "Ring oscillators and hardware Trojan detection," in *Hardware Security and Trust*, ed: Springer, 2017, pp. 169-187.

[55] G. Keramidas, N. Voros, and M. Hübner, *Components and Services for IoT Platforms*: Springer, 2016.

[56] D. J. Smith, *Reliability, maintainability and risk: practical methods for engineers*: Butterworth-Heinemann, 2017.

[57] K. Morgan, M. Caffrey, P. Graham, E. Johnson, B. Pratt, and M. Wirthlin, "SEU-induced persistent error propagation in FPGAs," *IEEE Transactions on Nuclear Science*, vol. 52, pp. 2438-2445, 2005.

[58] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, pp. 1645-1660, 2013.

[59] P. Wang, S. Chaudhry, L. Li, S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Research*, 2016.

[60] Y. Lee and D. Kim, "Threats analysis, requirements and considerations for secure Internet of Things," *International Journal of Smart Home*, vol. 9, pp. 191-198, 2015.

[61] R. Dobbins and S. Bjarnason, "Mirai iot botnet description and ddos attack mitigation," *Arbor Threat Intelligence*, vol. 28, 2016.

[62] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," *arXiv preprint arXiv:1702.03681*, 2017.

[63] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Security and Communication Networks*, vol. 7, pp. 2728-2742, 2014.

[64] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things," *IEEE Cloud Computing*, vol. 3, pp. 36-45, 2016.

[65] S. Moein, T. A. Gulliver, F. Gebali, and A. Alkandari, "A new characterization of hardware trojans," *IEEE Access*, vol. 4, pp. 2721-2731, 2016.

[66] H. Li, Q. Liu, and J. Zhang, "A survey of hardware Trojan threat and defense," *Integration*, vol. 55, pp. 426-437, 2016.

[67] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6.

[68] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, pp. 49-51, 2011.

[69] D. Sopori, T. Pawar, M. Patil, and R. Ravindran, "Internet of things: security threats," *Int. J. Adv. Res. Comput. Eng. Technol.(IJARCET)*, vol. 6, pp. 263-267, 2017.

[70] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *2016 IEEE symposium on security and privacy (SP)*, 2016, pp. 18-37.

[71] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 2546-2590, 2016.

[72] D. DiMase, Z. A. Collier, J. Carlson, R. B. Gray Jr, and I. Linkov, "Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems," *Risk Analysis,* vol. 36, pp. 1834-1843, 2016.

[73] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent transportation systems,* vol. 16, pp. 546-556, 2014.

[74] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering,* pp. 222-232, 1987.

[75] I. H. Witten and E. Frank, "Data mining: practical machine learning tools and techniques with Java implementations," *Acm Sigmod Record,* vol. 31, pp. 76-77, 2002.

[76] T. Hastie, R. Tibshirani, and J. Friedman, *The elements of statistical learning: data mining, inference, and prediction*: Springer Science & Business Media, 2009.

[77] D. K. Bhattacharyya and J. K. Kalita, *Network anomaly detection: A machine learning perspective*: Crc Press, 2013.

[78] C. C. Aggarwal, *Outlier Analysis*, 1 ed.: Springer-Verlag New York, 2013.

[79] V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial intelligence review,* vol. 22, pp. 85-126, 2004.

[80] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR),* vol. 41, pp. 1-58, 2009.

[81] F. A. Teixeira, F. M. Pereira, H.-C. Wong, J. M. Nogueira, and L. B. Oliveira, "SIoT: Securing Internet of Things through distributed systems analysis," *Future Generation Computer Systems,* vol. 92, pp. 1172-1186, 2019.

[82] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, and R. Budiarto, "Anomaly detection and monitoring in Internet of Things communication," in *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2016, pp. 1-4.

[83] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, 2016, pp. 319-320.

[84] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 756-767.

[85] L. Huang, X. Nguyen, M. Garofalakis, M. I. Jordan, A. Joseph, and N. Taft, "In-network PCA and anomaly detection," in *Advances in Neural Information Processing Systems*, 2007, pp. 617-624.

[86] M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," MIAMI UNIV CORAL GABLES FL DEPT OF ELECTRICAL AND COMPUTER ENGINEERING2003.

[87] W. Lu and A. A. Ghorbani, "Network anomaly detection based on wavelet analysis," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, pp. 1-16, 2008.

[88] W. Lu, M. Tavallaee, and A. A. Ghorbani, "Detecting network anomalies using different wavelet basis functions," in *6th Annual Communication Networks and Services Research Conference (cnsr 2008)*, 2008, pp. 149-156.

[89] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the Markov-chain model for cyber-attack detection," *IEEE Transactions on Reliability*, vol. 53, pp. 116-123, 2004.

[90] I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised clustering approach for network anomaly detection," in *International conference on networked digital technologies*, 2012, pp. 135-145.

[91] A. Kind, M. P. Stoecklin, and X. Dimitropoulos, "Histogram-based traffic anomaly detection," *IEEE Transactions on Network and Service Management*, vol. 6, pp. 110-121, 2009.

[92] B. M. Tellenbach, "Detection, classification and visualization of anomalies using generalized entropy metrics," ETH Zurich, 2012.

[93] F. Iglesias and T. Zseby, "Entropy-based characterization of internet background radiation," *Entropy*, vol. 17, pp. 74-101, 2015.

[94] C.-Y. Ho, Y.-C. Lai, I.-W. Chen, F.-Y. Wang, and W.-H. Tai, "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems," *IEEE Communications Magazine*, vol. 50, pp. 146-154, 2012.

[95] P. Bereziński, B. Jasiul, and M. Szpyrka, "An entropy-based network anomaly detection method," *Entropy*, vol. 17, pp. 2367-2408, 2015.

[96] Z. Li, A. Das, and J. Zhou, "Usaid: Unifying signature-based and anomaly-based intrusion detection," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, 2005, pp. 702-712.

[97] T.-H. Cheng, Y.-D. Lin, Y.-C. Lai, and P.-C. Lin, "Evasion techniques: Sneaking through your intrusion detection/prevention systems," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 1011-1020, 2011.

[98] Y. Zhou and D. Feng, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing," *IACR Cryptology ePrint Archive*, vol. 2005, 2005.

[99] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, 2018, pp. 29-35.

[100] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly Detection in Smart Home Operation From User Behaviors and Home Conditions," *IEEE Transactions on Consumer Electronics*, vol. 66, pp. 183-192, 2020.

[101] S. Muller, J. Lancrenon, C. Harpes, Y. Le Traon, S. Gombault, and J.-M. Bonnin, "A training-resistant anomaly detection system," *Computers & Security*, vol. 76, pp. 1-11, 2018.

[102] R. Corizzo, M. Ceci, E. Zdravevski, and N. Japkowicz, "Scalable auto-encoders for gravitational waves detection from time series data," *Expert Systems with Applications*, p. 113378, 2020.

[103] F. Cauteruccio, G. Fortino, A. Guerrieri, A. Liotta, D. C. Mocanu, C. Perra, *et al.*, "Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance," *Information Fusion*, vol. 52, pp. 13-30, 2019.

[104] F. Cauteruccio, L. Cinelli, E. Corradini, G. Terracina, D. Ursino, L. Virgili, *et al.*, "A framework for anomaly detection and classification in Multiple IoT scenarios," *Future Generation Computer Systems*, vol. 114, pp. 322-335.

[105] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018.

[106] D. Myridakis, G. Spathoulas, and A. Kakarountas, "Supply Current Monitoring for Anomaly Detection on IoT Devices," in *Proceedings of the 21st Pan-Hellenic Conference on Informatics*, 2017, pp. 1-2.

[107] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schinianakis, and J. Lueken, "Monitoring Supply Current Thresholds for Smart Device's Security Enhancement," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 224-227.

[108] D. Myridakis, G. Spathoulas, A. Kakarountas, and D. Schinianakis, "Smart Devices Security Enhancement via Power Supply Monitoring," *Future Internet*, vol. 12, p. 48, 2020.

[110] W. Zhang, D. Yang, and H. Wang, "Data-driven methods for predictive maintenance of industrial equipment: a survey," *IEEE Systems Journal*, vol. 13, pp. 2213-2227, 2019.

[111] M. Compare, P. Baraldi, and E. Zio, "Challenges to IoT-enabled predictive maintenance for industry 4.0," *IEEE Internet of Things Journal*, vol. 7, pp. 4585-4597, 2019.

[112] Y. Bai, Z. Sun, J. Deng, L. Li, J. Long, and C. Li, "Manufacturing quality prediction using intelligent learning approaches: A comparative study," *Sustainability*, vol. 10, pp. 1-15, 2017.

[113] R. J. Eleftheriadis and O. Myklebust, "A quality pathway to digitalization in manufacturing thru zero defect manufacturing practices," in *6th International Workshop of Advanced Manufacturing and Automation*, 2016, pp. 187-191.

[114] F. Talib and Z. Rahman, "Total quality management practices in manufacturing and service industries: a comparative study," *International Journal of Advanced Operations Management*, vol. 4, pp. 155-176, 2012.

[115] W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The bulletin of mathematical biophysics*, vol. 5, pp. 115-133, 1943.

[116] J. M. Harkness, "In Appreciation¶ A Lifetime of Connections: Otto Herbert Schmitt, 1913-1998," *Physics in Perspective*, vol. 4, pp. 456-490, 2002.

[117] J. Benyus, "Innovation inspired by nature: biomimicry," *New York: William Morrow & Co*, 1997.

[118] B. Miller, "Vital signs of identity [biometrics]," *IEEE spectrum*, vol. 31, pp. 22-30, 1994.

[122] M. Malewski, D. M. Cowell, and S. Freear, "Review of battery powered embedded systems design for mission-critical low-power applications," *International Journal of Electronics*, vol. 105, pp. 893-909, 2018.

[123] P. Lezhnyuk, V. Komar, S. Kravchuk, and D. Sobchuk, "Mathematical modeling of operation quality of electric grid with renewable sources of electric energy," in *2017 International Conference on Modern Electrical and Energy Systems (MEES)*, 2017, pp. 324-327.

Ηλεκτρονική Βιβλιογραφία

[1] Helpnetsecurity. (2020, 10-05). *https://www.helpnetsecurity.com/2016/07/19/ddos-attacks-escalate/*. Available: https://www.helpnetsecurity.com/2016/07/19/ddos-attacks-escalate/

[10] Imedicalapps. (2019, 10-06). *Imedicalapps*. Available: http://www.imedicalapps.com/2014/01/diagnose-app-evidencebased-clinical-decision/

[11] Prognosisapp. (2019, 10-06). *Prognosisapp*. Available: http://www.prognosisapp.com

[12] Apple. (2019, 10-06). *Apple*. Available: https://www.apple.com/itunes/charts/

[13] Medicaljoyworks. (2019, 10-06). *Medicaljoyworks*. Available: http://www.medicaljoyworks.com/

[17] Intel. (2019, 10-06). *Intel*. Available: http://www.intel.co.kr/content/www/kr/ko/internet-of-things/videos/dr-hawkingsconnected-wheelchair-video.html

[53] Enisa. (2019, 10-06). *Baseline Security Recommendationsfor IoT*. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendationsfor-iot/(2019)

[109] J. Soldatos. (2021, 24-02). *Embedded Machine Learning Applications With Proven ROI*. Available: https://www.wevolver.com/article/embedded-machine-learning-applications-with-proven-roi

[119] Arduino. (2017, 05-10). *Arduino*. Available: https://www.arduino.cc/

[120] Adafruit. (2017, 05-10). *DHT22 temperature-humidity sensor*. Available: https://www.adafruit.com/product/385

[121] Thingworx. (2017, 05-10). *Thingworx platform*. Available: https://www.thingworx.com