1862
RIGA TECHNICAL UNIVERSITY

Daniils Aleksandrovs-Moisejs

ASSESSMENT OF WIRELESS NETWORK THROUGHPUT AND CYBERSECURITY IN INTERNET OF THINGS SYSTEMS

Summary of the Doctoral Thesis

RTU Press
Riga 2025

RIGA TECHNICAL UNIVERSITY
Faculty of Computer Science, Information Technology and Energy
Institute of Photonics, Electronics and Telecommunications

Daniils Aleksandrovs-Moisejs
Doctoral Student of the Study Programme "Telecommunications"

ASSESSMENT OF WIRELESS NETWORK THROUGHPUT AND CYBERSECURITY IN INTERNET OF THINGS SYSTEMS

Summary of the Doctoral Thesis

Scientific supervisor
Associate Professor Dr. sc. ing.
ALEKSANDRS IPATOVS

RTU Press
Riga 2025

Aleksandrovs-Moisejs, D. Assessment of Wireless Network Throughput and Cybersecurity in Internet of Things Systems. Summary of the Doctoral Thesis. - Riga: RTU Press, 2025. 52 p.

Published in accordance with the decision of the Promotion Council “P-08” of 27 June 2025, Minutes No. 41.

Cover picture from www.shutterstock.com.

https://doi.org/10.7250/9789934372186
ISBN 978-9934-37-218-6 (pdf)

DOCTORAL THESIS PROPOSED TO RIGA TECHNICAL UNIVERSITY FOR PROMOTION TO THE SCIENTIFIC DEGREE OF DOCTOR OF SCIENCE

To be granted the scientific degree of Doctor of Science (PhD), the present Doctoral Thesis has been submitted for defence at the open meeting of RTU Promotion Council on 21 November 2025 10:00 a.m. at the Faculty of Computer Science, Information Technology and Energy of Riga Technical University, Āzenes iela 12, Room 201.

OFFICIAL REVIEWERS

Associate Professor Dr. sc. ing. Andis Supe,
Riga Technical University (RTU)

Professor Dr. sc. ing. Rafael Asorey Cacheda,
Polytechnic University of Cartagena (UPCT), Spain

Professor Dr. ing. Habil. Mehmet Ercan Altinsoy,
Dresden University of Technology (TUD), Germany

DECLARATION OF ACADEMIC INTEGRITY

I hereby declare that the Doctoral Thesis submitted for review to Riga Technical University for promotion to the scientific degree of Doctor of Science (PhD) is my own. I confirm that this Doctoral Thesis has not been submitted to any other university for promotion to a scientific degree.

Daniils Aleksandrovs-Moisejs …………………………… (signature)

Date: ………………………

The Doctoral Thesis has been written in Latvian. It consists of an Introduction, five chapters, Conclusions, 57 figures, 22 tables, and two appendices; the total number of pages is 177, including appendices. The Bibliography contains 146 titles.

ANNOTATION

The global tendencies of IEEE 802.11 and IEEE 802.15.4 wireless or sensor networks have been rapidly deployed in a variety of lifestyle applications, including IoT, smart home systems and critical infrastructures such as industrial, scientific and medical (ISM) sectors. Such networks provide a convenient and flexible environment for data transmission, but using IoT devices is associated with several security and performance issues. The IEEE 802.15.4 standard is the basis for protocols such as Zigbee and has been developed for operation in low-power sensor networks, enabling data transmission in limited environmental conditions. However, low power consumption and low throughput make 802.15.4 networks a little vulnerable to PHY and MAC attacks such as packet injection and denial of service attacks.

The Thesis is focused on cybersecurity and throughput aspects of IEEE 802.15.4 networks, focusing on the analysis of attacks and methods to counteract them. The study includes an experimental evaluation of the throughput of the Zigbee network based on Shannon's theorem, taking into account the factors such as overhead, probability of successful packet transmission and channel utilisation rate. The statistical modelling method based on the Nakagami distribution was used to assess the impact of interference and attacks on the network. The experiments analysed network attacks such as packet injection, DoS attacks, and signal jamming. For network protection, the CC2531 packet monitor module was used, and attack blocking techniques using additional monitoring devices and RF interference generation were used.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

A
AES – Advanced Encryption Standard
AI – Artificial Intelligence
AMQP – Advanced Message Queuing Protocol
AP – Access Point

B
BMS – Building Management System
BPSK – Binary Phase Shift Keying

C
CoAP – Constrained Application Protocol
CRC – Cyclic Redundancy Check
CRR – Critical Response Rate
CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

D
DDoS – Distributed Denial of Service
DoS – Denial of Service
DSSS – Direct Sequence Spread Spectrum

F
FOTA – Firmware Over-The-Air
FHSS – Frequency Hopping Spread Spectrum

G
GPIO – General Purpose Input/Output

H
HTTP – Hypertext Transfer Protocol

I
IaaS – Infrastructure as a Service
IDS – Intrusion Detection System
IEEE – Institute of Electrical and Electronics Engineers
IoT – Internet of Things
ISM – Industrial, Science and Medical
IT – Information Technology
IPS – Intrusion Prevention System

L
LAN – Local Area Network
LLC – Logical Link Control
LoRaWAN – Long Range Wide Area Network
LQI – Link Quality Indicator

M
MAC – Media Access Control
MAE – Mean Absolute Error
MIMO – Multiple Input Multiple Output
ML – Machine Learning
MQTT – Message Queuing Telemetry Transport

O
OAuth – Open Authorization
OFDM – Orthogonal Frequency Division Multiplexing
OFDMA – Orthogonal Frequency Division Multiple Access
OLS – Ordinary Least Squares
OSI – Open Systems Interconnection

P
PHY – Physical Layer

Q
QAM – Quadrature Amplitude Modulation
QoS – Quality of Service

R
RADIUS – Remote Authentication Dial-In User Service
RBAC – Role-Based Access Control
RF – Radio Frequency
RMSE – Root Mean Square Deviation
RSA – Rivest-Shamir-Adleman
RSSI – Received Signal Strength Indicator

S
SDR – Software-Defined Radio
SSH – Secure Shell
SNR – Signal-to-Noise Ratio
SSL – Secure Sockets Layer
SZTK – Student scientific conference

T
TCP/IP – Transmission Control Protocol/Internet Protocol
TLS – Transport Layer Security

U

URH – Universal Radio Hacker
USB – Universal Serial Bus

V

VLAN – Virtual Local Area Network

W

WLAN – Wireless Local Area Network
WI-FI – Wireless Fidelity
WPA2 – Wi-Fi Protected Access 2
WPA3 – Wi-Fi Protected Access 3

GENERAL DESCRIPTION OF THE DOCTORAL THESIS

Topicality of the Research

Nowadays, smart home technologies and building management systems (BMS) are being implemented in private flats and industrial environments, providing central control over electricity, lighting, heating, water supply, home security and other essential smart functions. Modern systems such as the Internet of Things (IoT) and BMS offer extensive opportunities for home automation and remote management [1]–[3].

While management solutions are rapidly progressing, the security aspects of modern smart systems are often neglected. Smart systems users often assume that a complex password or channel encryption using TLS is a better way to secure the system. Systems can be compromised not only externally but also internally in the network. In such cases, it is better to use network bridges with implemented VLANs or a firewall with fine-grained access control [4].

Particularly alarming is the presence of "backdoors", which are frequently identified in low-cost, mass-produced IoT devices. These may be made into software when they are manufactured, or they may be unexpected user-controlled "backdoors" that have not been disabled for remote access (e.g. SSH), enabled, non-existent encryption protocols, or even enabled with default modes set. In cybersecurity science, a "backdoor" refers to any vulnerability that allows authentication bypass and unauthorised access to the system without the owner's acceptance [5]–[7].

User forgetfulness is also a common source of threat when users connect from unsecured devices, use weak passwords, or click on malicious links, thereby introducing viruses and spyware into the network. If the organisation's firewall lacks properly configured access rules, there is an estimated 50–70 % probability that the system will become infected.

Therefore, information security must not only be considered as a technical problem but also as one of organisational design and user activity. Knowledge of fundamental security principles – confidentiality, integrity, and availability (CIA Triad) and using multi-layered protection mechanisms such as logical (encryption, authentication and firewalls), physical (device and access controls), and administrative (security policies, rules and staff training) [8].

The relevance of the Doctoral Thesis is grounded in the need to design and evaluate practical defence mechanisms for IoT networks, particularly within Zigbee protocol environments, which are often popularised by low-cost devices with minimal security standards. Networks must not only work effectively but also demonstrate the ability to withstand multiple forms of cyber attacks, like packet injection or signal jamming, which can interrupt the functionality of the system [3], [9], [10].

Aim and Tasks of the Doctoral Thesis

Based on the analysis of security and throughput issues in IoT networks, **the aim of the Doctoral Thesis** was defined – to theoretically study IoT network performance and cybersecurity policy aspects and potential threat types, and to experimentally construct a Zigbee-based IoT testbed, analysing its vulnerabilities using Python programming, specialised security testing equipment and the Nakagami distribution model.

To achieve the aim brought into focus, the following **basic tasks** had to be performed:

1. To carry out the performance of modern wireless IoT standards, fundamental principles and performance characteristics of the IEEE 802.15.4 standard and to assess the related cybersecurity aspects.
2. To design an experimental hybrid IoT operational testbed, enabling a defined number of Zigbee devices to analyse their activity and to evaluate network performance based on built-in solutions.
3. To check a performance analysis of the IEEE 802.15.4-based network architecture and its devices within the experimental setup, using packet monitoring tools and a custom-developed Python launch script for analysing network packets.
4. To research vulnerabilities of the IEEE 802.15.4 standard and perform analysis of RSSI and throughput under injected network scenarios using RZUSBSTICK and a Python-based vulnerability simulation script.
5. To analyse attacks against IEEE 802.15.4 standard-based networks and develop multiple countermeasure strategies based on CC2531 packet monitoring and HackRF One frequency modulation tools.
6. To use the Nakagami distribution and its parameters to compare RSSI and throughput in accordance with Shannon’s theorem and to evaluate the attitude of the IEEE 802.15.4-based network testbed under normal and vulnerability conditions.
7. To perform a simulation of the IEEE 802.15.4 standard in the controlled environment using the Python programming platform, based on acquired experimental data, in order to compare original and modified results with cybersecurity and performance indicators.

8. To evaluate the obtained results, draw an appropriate conclusion and propose potential improvements for enhancing cybersecurity within the IEEE 802.15.4 standard framework.

Methodology of the Research

To achieve the defined basic tasks in developing the Doctoral Thesis and scientifically evaluate the identified issues, experimental measurements of the hybrid network testbed were conducted and programmed, taking into account cybersecurity policies. The testbed's environment included equipment and devices such as RZUSBstick, CC2531 with the Killerbee library, HackRF One, various Zigbee-based modules, Raspberry Pi microcontrollers and Kali Linux working environment, as well as the Python programming language. The packet analyser program Wireshark was used for Zigbee data packet analysis, while both wired and wireless (IEEE 802.15.4) networks were created and tested in various attack and defence scenarios. This approach enables an effective evaluation of the manipulation between IoT devices, identification of potential security vulnerabilities, and the development of applicable defence mechanisms.

Mathematical calculations were performed using Python mathematical libraries (matplotlib, scipy), while the statistics of experimental measurement results were conducted in the Excel program.

For the successful completion of the experiments, the Python scripts used for Zigbee network monitoring, attacks and countermeasures implementation are available in the public GitHub repository: https://github.com/DannyAlmois/PhD_IoT_Zigbee_Cybersecurity.

Research Results and Scientific Novelty

Acquisitions of the Doctoral Thesis

1. To examine the network recovery processes during defence activation, a polynomial and a hybrid trend model were employed. The obtained results demonstrated that linear trends are incapable of showing recovery dynamics due to the unreliable capacity of packet injection and attack behaviour. Squared and three-dimensional polynomial equations, as well as a hybrid model that accumulated external factors, were used to better show fluctuations during recovery.
2. A comprehensive evaluation of IEEE 802.15.4 networks under various types of attack was conducted using customised software and freshly developed Python-based scripts.

An innovative countermeasure approach based on dynamic monitoring and adaptive interference was introduced, using CC2531 and SDR modules to detect specific packet types or IEEE 802.15.4 network anomalies. This enhanced the network resilience up to 60–95 %, depending on the attack type, and reduced throughput recovery time by as much as 30 %.

3. An attack simulation model was created to emulate jamming, packet injection and DoS vulnerability scenarios with up to 30 virtual Zigbee devices. The simulation model proved a countermeasure detection with an accuracy of 95 % in comparison to real-world testing, providing a useful resource for assessing defensive measures and planning for future research.
4. Using the Nakagami distribution with fixed parameters ($m = 0.8$; $\Omega = 0.3$) to simulate signal degradation in an indoor IEEE 802.15.4 multi-path propagation environment. Despite the fixed parameters, it still managed to demonstrate the decrease in the signal and increase in the packet loss probability when under attack, indicating the susceptibility of the network to different types of attacks in smart home and IoT scenarios.

Main Conclusions of the Doctoral Thesis

1. The development of an integrated WLAN and IoT communication system based on Raspberry Pi and RaspBee II, Zigbee device router, proved to be both technically and economically justified. This approach allowed for easy SSH-based remote access and efficient network management without requiring complicated infrastructure.
2. Various defence mechanisms were developed, including malicious packet disruption, adaptive data stream filtering, and channel-level network monitoring. All of these mechanisms reinstated some level of network throughput after attacks and provided reliable communication despite ongoing attacks.
3. The implementation of security mechanisms showed high effectiveness against different types of attack. 94.83 % of effectiveness in real environments and 85.14 % in simulations were indicative that the network displayed the most resistance to packet injection attacks.
4. In respect of jamming attacks, the defence was successful 60.11 % for the real network and 78.05 % for simulations, thereby authenticating the success of the signal filter and interference-based attack protection mechanism.

5. Denial-of-service (DoS) attacks were the hardest to defend against. For example, the mitigation was only 47.75 % effective in physical networks, while 93.33 % was in simulation environments. These differences showed how hardware constraints and external noise factors affected real tests.
6. A comparison of protection results between real and simulated environments showed significant differences. Simulations did not have limitations of real tests execution by media, making mitigation much more effective; it was able to hone in on detection and block from signal jamming and DoS attacks that were overtly complex in real tests.
7. The Nakagami distribution with fixed parameters allowed for a better understanding of changes in signal behaviour in different threat scenarios. It could easily model signal instability and increase the probability of packet loss due to jitter, particularly with respect to interference conditions.
8. The simulation framework that operated from an underlying Python architecture was developed to model the attack behaviour and test the effectiveness of defences. The simulated network's performance metrics had a 95 % agreement with testing metrics of the physical test devices, giving a much finer level of detail not physically attainable with the delays and zeroing out of the network without any devices. Information patterns in the network congested with adversarial traffic could be explored with a simulation.
9. The evaluation of the network performance while being attacked suggested that throughput dropped by 40–60 % during DoS and jamming attack scenarios. In fact, attackers achieved pseudo-recovery time without undertaking any countermeasures, which extended to 30 %. The forecasting is performed in conjunction with polynomial and hybrid trend models; thus, we were limited to the forecasting of the recovering dynamics of only $R^2 = 0.96$, to optimise post-attack mitigations.

Theses to be Defended in the Doctoral Thesis

1. One of the attack strategies related to an IoT hybrid network can purposely decrease signal strength (*RSSI*) to an approximate level of –90 dBm and quite severely disrupt several aspects of network performance. This type of attack can be detected and countered with an effectiveness of 90 % or more by a defence module utilising HackRF One.

2. Using a CC2531 monitoring module on Zigbee channel 15 (2.425 GHz), it is feasible to identify signal (*RSSI*) level changes and packet flow disruptions caused by defined attacks, leading to partial network paralysis and disturbances with the order of transmission.
3. The assumption of signal attenuation being modelled from a Nakagami distribution in the enclosed space will predict the strength of the signal (*RSSI*) to be more than 20 % higher than the RSSI value recorded from the experiment.

Approbation of the Research Results

The main results of the Doctoral Thesis have been presented at three international scientific conferences and two SZTK events, as well as published in one scientific journal and two conference proceedings.

Publications in scientific journals

Aleksandrovs-Moisejs, D., Ipatovs, A., Grabs, E., Rjazanovs, D. Evaluation of a Long-Distance IEEE 802.11ah Wireless Technology in Linux Using Docker Containers. Elektronika ir elektrotechnika = Electronics and Electrical Engineering, 2022, Vol. 28, No. 3, pp. 71–77.

Publications in full-text conference proceedings

1. **Aleksandrovs-Moisejs, D**., Ipatovs, A., Grabs, E., Rjazanovs, D., Siņuks, I. Arduino-Based Temperature Sensor Organization and Design. In: 2023 Photonics & Electromagnetics Research Symposium (PIERS 2023): Proceedings, Czech Republic, Prague, 3–6 July 2023.
2. **Aleksandrovs-Moisejs, D.,** Grabs, E., Chen, T., Beļinskis, R., Bogdanovs, N., Kārkliņš, T., Klūga, J., Stetjuha, M., Ipatovs, A. Arduino-based Implementation and Design of Modern Temperature Measurements Sensor Environments. In: 2024 Photonics & Electromagnetics Research Symposium (PIERS 2024): Proceedings, China, Chengdu, 21–25 April 2024.

Scope and Structure of the Doctoral Thesis

The total number of pages of the Doctoral Thesis is 176. It contains five chapters, conclusions, bibliography, and two appendices.

The introduction of Chapter 1 presents modern wireless networks and architectures, operational principles and characteristics of IEEE standards, with a particular focus on IEEE 802.11 and IEEE 802.15.4 networks, their functionalities, topology types, protocols, and integration ways within the IoT ecosystem. Chapter 1 also examines the major vulnerabilities in the PHY, MAC and LLC layers, as well as common security issues affecting these networks.

Chapter 2 provides an examination of the attack types that use WLAN in IEEE 802.11/802.15.4 networks, including DoS, packet injection and signal jamming attacks. It describes the operational principles, the implementation, and the impact on network performance, in terms of RSSI, and how the throughput is affected. The chapter assesses existing detection and mitigation methods and considers various mitigation methods to see how effective the countermeasures are.

Chapter 3 discusses the experimental procedures related to the study, including the test network architecture, hardware and software, equipment tools (RZUSBStick, CC2531 and HackRF One), monitoring tools based on Wireshark and the launching scripts, which were personally used to execute DoS, signal jamming and packet injection attacks. The modelling parameters used for the Python programming environment are also indicated, as well as the experiment methodology from which the original and modified (Nakagami) RSSIs were measured and throughput was calculated (based on the suggested Shannon theorem, using empirical evidence).

The comprehensive analysis of the collected data is provided in Chapter 4, evaluating the impact of attacks on connection quality, throughput, and network stability, and also comparing results from real and simulated Zigbee environments. Comparative analysis of different attack types and their effects is included, with special attention to the use of the Nakagami distribution for modelling signal degradation and evaluating network reliability under stress conditions.

Chapter 5 describes the developed methods for protecting the IoT network against DoS, jamming and packet injection attacks. It introduces approaches for detecting malicious packets, including MAC address-based filtering, dynamic channel jamming, and adaptive blocking techniques. Also covered are polynomial trend algorithms to predict how networks will recover after attacks and suggestions to enhance resilience, assessing the ways in which the suggested systems performed in both realistic and simulated settings.

The main conclusions of the research are summarised at the end of the Doctoral Thesis. Conclusions highlight the core findings and contributions of the study, while also outlining some directions for future research in the field of IoT and cybersecurity. The conclusions emphasise the practical relevance of the developed methods and their application within IoT networks, particularly in Zigbee-based environments. Lists of comprehensive bibliography, the results of experimental measurements and Python codes are included in the appendices.

CONTENT OF THE DOCTORAL THESIS

Chapter 1

This chapter of the Doctoral Thesis provides an assessment of the IEEE 802.11 and IEEE 802.15.4 hybrid network, examining its core mechanisms and protocols.

At the beginning of the chapter, the hybrid testbed is established by integrating two wireless data technologies, enabling simultaneous support for both standards. The IEEE 802.11 standard is implemented in its IEEE 802.11ax version at the 5 GHz frequency band, reducing the risk of interference while usable in parallel with IEEE 802.15.4. IEEE 802.11 is the foundation of traditional internet connections and remote access (e.g. SSH). By contrast, IEEE 802.15.4 as a standard is used as the basis for home automation solutions, using the Zigbee protocol at the 2.4 GHz frequency band. It is in this network that various types of cyberattacks can be tested, and the behaviour of the network and the resilience of the mitigation security mechanisms against any cyber threats can be analysed.

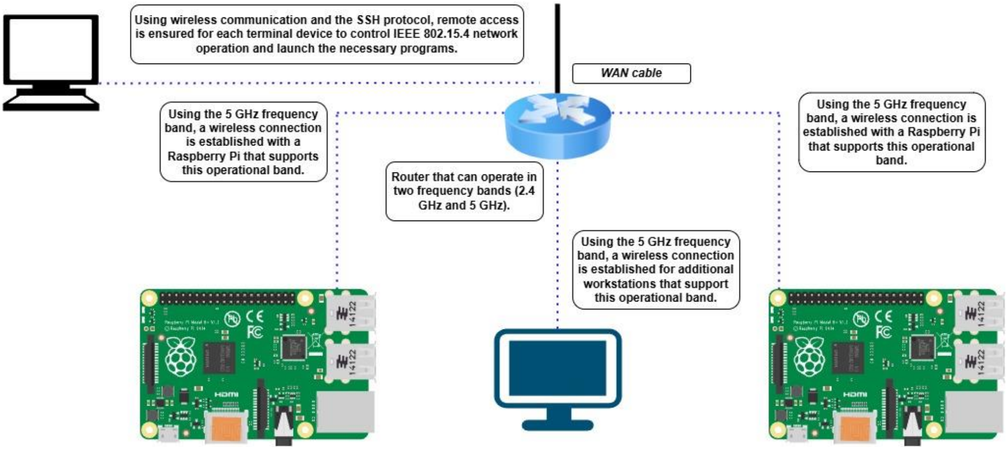
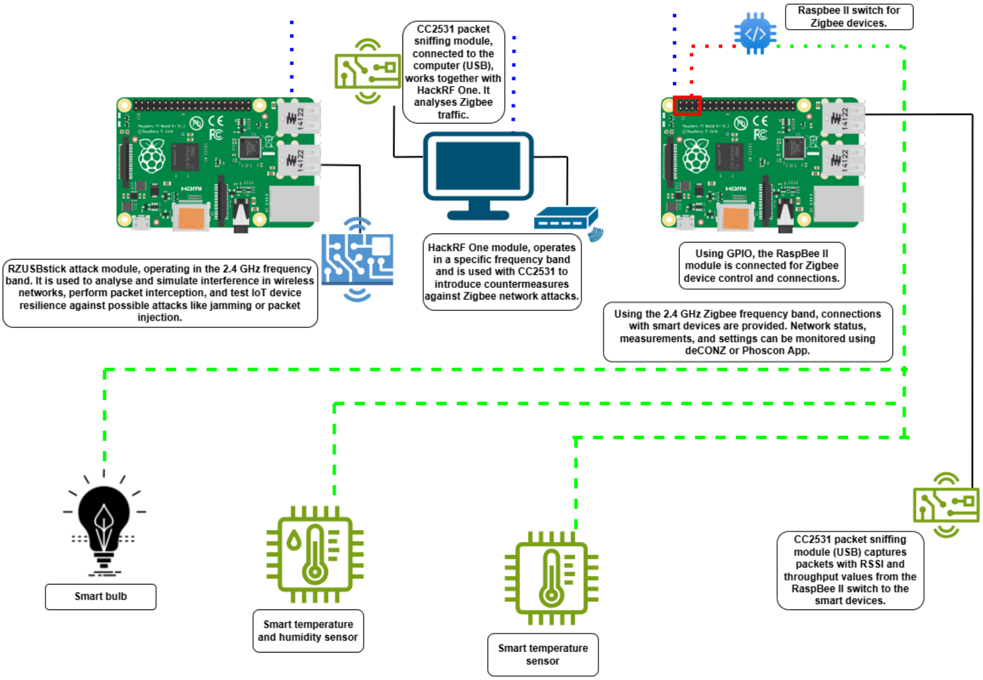

Using wireless communication and the SSH protocol, remote access is ensured for each terminal device to control IEEE 802.15.4 network operation and launch the necessary programs.
WAN cable
Using the 5 GHz frequency band, a wireless connection is established with a Raspberry Pi that supports this operational band.
Router that can operate in two frequency bands (2.4 GHz and 5 GHz).
Using the 5 GHz frequency band, a wireless connection is established with a Raspberry Pi that supports this operational band.
Using the 5 GHz frequency band, a wireless connection is established for additional workstations that support this operational band.

Fig. 1. Experimental wireless IEEE 802.11 network architecture scheme for IEEE 802.15.4 communication control.



Raspbee II switch for Zigbee devices.

CC2531 packet sniffing module, connected to the computer (USB), works together with HackRF One. It analyses Zigbee traffic.

RZUSBstick attack module, operating in the 2.4 GHz frequency band. It is used to analyse and simulate interference in wireless networks, perform packet interception, and test IoT device resilience against possible attacks like jamming or packet injection.

HackRF One module, operates in a specific frequency band and is used with CC2531 to introduce countermeasures against Zigbee network attacks.

Using GPIO, the RaspBee II module is connected for Zigbee device control and connections.

Using the 2.4 GHz Zigbee frequency band, connections with smart devices are provided. Network status, measurements, and settings can be monitored using deCONZ or Phoscon App.

CC2531 packet sniffing module (USB) captures packets with RSSI and throughput values from the RaspBee II switch to the smart devices.

Fig. 2. Experimental Zigbee network architecture with attack, defence mechanisms and smart devices.

Section 1.1 provides an overview of the IEEE 802.11 (Wi-Fi) standard, which is widely used in home and office network environments. It enables data to be transmitted across many frequency bands – 2.4 GHz, 5 GHz, 6 GHz and 60 GHz – making it viable for both mobility and high-throughput usages. The standard has developed through various degrees since its inception in 1997, culminating in a number of versions (from 802.11a to 802.11ax or Wi-Fi 6), benefitting from improved performance and scalability [11], [12].

The key performance attributes are throughput, latency and interference. The 2.4 GHz frequency band provides a larger coverage area, but is susceptible to interference. The 5 GHz and 6 GHz frequency bands deliver higher transmission speeds at a lower degree of interference, but have a shorter coverage area [11].

The IEEE 802.11 standard associates the physical layer (PHY), data link layer with MAC and LLC sublayers, and integrated security mechanisms that ensure efficient and secure communication in wireless networks.

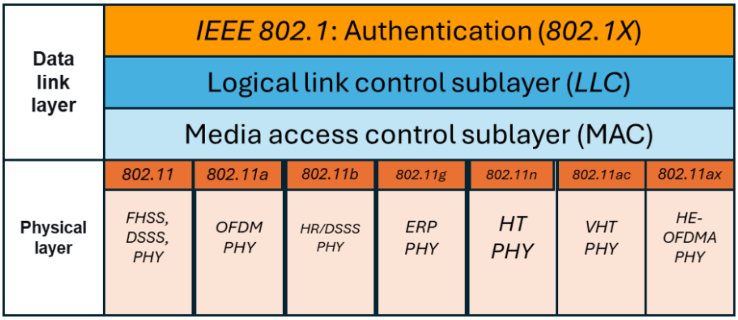


Fig. 3. IEEE 802.11 standard operating stack [13].

The **physical layer** allows the physical transfer of data using radio waves, operating in the 2.4 GHz, 5 GHz and 6 GHz frequency bands. Different modulation techniques are used, including DSSS and FHSS in previous standard versions and OFDM, QAM, MIMO and OFDMA technologies for the latest standard that radically enhances throughput and interference resilience [14]–[16].

The **MAC sublayer** is responsible for managing access to the shared transmission medium with the help of the CSMA/CA algorithm. The sublayer manages the packet flow during the packet transmission and prevents packet collisions while providing QoS and reliable packet delivery mechanisms [17].

The **LLC sublayer** provides a logical link control between the data link and network layers. LLC handles flow control, addressing, error detection and correction mechanisms (e.g. CRC), and a function for facilitating the interface between the MAC sublayer and the higher layer network protocols within the OSI model [17].

Security mechanisms in the IEEE 802.11 standard include a variety of layers of protection from authentication to encryption of the data. Earlier implementations used WEP, which is now widely deemed insecure. Today’s standards employ WPA2 and WPA3 secure protocols.

- **WPA2** specifications employ the Advanced Encryption Standard (AES) with a 128-bit key to protect communication utilising a four-way handshake mechanism.
- **WPA3** includes enhanced authentication with simultaneous authentication of equals (SAE), which provides both protection against weak password (brute force) attacks and forward secrecy to enhance the data protected on public networks [18]–[20].

Both protocols include measures to mitigate replay attacks and denial-of-service (DoS) attacks. Furthermore, authentication can be enhanced utilising the 802.1X protocol and

RADIUS servers, which offer centralised user management and multi-factor authentication capabilities.

In Section 1.2, the architecture and applications of wireless IoT networks are examined. IoT devices function via a communication framework that it would evaluate to be somewhat basic in form. The cloud infrastructure, which is described as a centralised facility, is the system within which the data that has been collected by the IoT devices is stored, processed, and analysed. The communication network does the work of establishing a connection to the IoT devices, which relay their information to the cloud structure via the Internet. This communication network is either a wired infrastructure or wireless. The communication between the devices and the Internet is made by the IoT gateway or hubs. Next are the physical devices, such as smart sensors and numerous other types of devices, that connect to the communication network, collect and record information regarding the environment. The environment can vary greatly, from an apartment or a building to a street or a city. User applications mean that the software or interfaces that allow users the ability to interact with the IoT devices and view, visualise and manage the data. Every IoT device receives data from its operating environment and transmits it to the cloud for additional processing for storage via an external network. Users can interact with the devices and the data through dedicated applications [2], [21], [23].

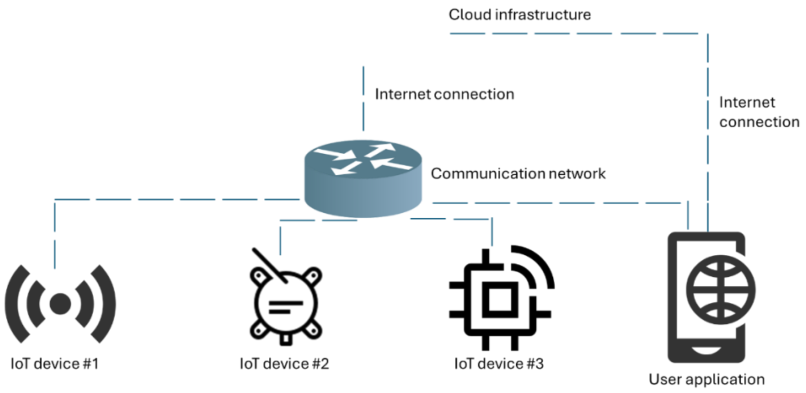


Fig. 4. IoT network architecture.

In **Section 1.3,** the most significant IoT protocols, along with their use cases, are summarised. The protocols are classified by their purpose: data transfer and network management. Message transfer protocols include MQTT, CoAP and AMQP, which are used for sending data from IoT devices to servers and for transferring messages. The use of MQTT is great for low-bandwidth networks. CoAP is a lighter alternative to HTTP for constrained environments, and AMQP provides comprehensive functionality for more complex messaging. The communication system for wireless means, such as Zigbee and LoRaWAN, describes the data transfer technologies, as well as the network topologies. Protocols will depend on the requirements for the application – volume of data, transmission range, latency and use of energy [2], [22], [25].

In **Section 1.4,** the physical and data link layer operational principles of the IEEE 802.15.4 standard, emphasising their importance in IoT network design, are examined. The IEEE 802.15.4 is used as the foundational aspect for many low-power wireless protocols, including Zigbee and Thread. The **physical layer** utilises DSSS modulation and provides some operating options in the 2.4 GHz ISM band, with other regions allowed to operate in the 868/915 MHz bands. These physical layer characteristics provide good coverage with better resistance to interference [24], [26]–[28].

The **data link layer** in the IEEE 802.15.4 standard provides the implementation of data frame access using the CSMA/CA method, supports synchronisation using beacon technology that is provided as part of the MAC layer, and allows for a number of network topologies, including hierarchical and mesh connections [27].

Security in the IEEE 802.15.4 standard is a vital aspect of networks. The standard utilises AES-128 encryption to provide data confidentiality, integrity and authentication. The security mechanisms act against unauthorised access and eavesdropping attacks. Additionally, some implementations of reputation systems and network monitoring systems are used to enhance the security level [29].

It is noted that IEEE 802.15.4 is especially viable for devices with constrained resources because of the low power consumption, low data rates and reliability needed for smart sensors, monitoring equipment and other IoT devices.

Section 1.5 contains a theoretical analysis of the performance differences between IEEE 802.11 and IEEE 802.15.4 networks, based on scientific literature and technical specifications of both standards. IEEE 802.11 (Wi-Fi) networks are high-throughput networks (with a maximum throughput of 9.6 Gbit/s) that fit any application that heavily utilises data streaming, such as viewing video. However, these networks typically incur higher costs in terms of power consumption, have higher interference variables, and are less suitable for battery-constrained wireless devices in low-power applications. For RSSI, typical values would range from −30 dBm to −50 dBm, and IEEE 802.11 would not utilise LQI as a measurement parameter [30], [33].

Conversely, IEEE 802.15.4 networks, which support sensors and low-throughput devices, enable a transmission rate of 250 kbit/s, less power consumption, and better resilience to interference. The RSSI level is similar, from –30 dBm to –50 dBm, and LQI values of 0 to 255, while higher values have a better indication of signal strength. The comparison shows that if you have high data rate and low latency applications, the IEEE 802.11 standard is preferred; on the other hand, if the application is an energy-efficient and sustainable system, like an environmental monitoring system or an automation solution, then the IEEE 802.15.4 standard is a better solution. It will depend on the specific application requirements regarding data rate, power consumption and coverage area as to which protocol will be preferred [31].

Section 1.6 describes the experimental hybrid network, which combines devices based on IEEE 802.11 and IEEE 802.15.4 standards to evaluate their interoperability and network performance in testbed usage scenarios. As mentioned, the hybrid testbed includes two Raspberry Pi devices. One of them is used for Zigbee coordinator (Raspbee II module), which is connected to the GPIO interface and a CC2531 sniffer adapter with Killerbee firmware for monitoring IEEE 802.15.4 data packets. This configuration allows the examination of RSSI, throughput, and data packets in real time using custom Python launch scripts [34], [35].

The second Raspberry Pi acted as the attacker node and was used with the RZUSBStick, connected to a programmed KillerBee library that was capable of performing DoS attacks, packet injection and signal jamming. There were also other defensive means like a Kali Linux workstation, a HackRF One device, and another CC2531 module for attack detection and neutralisation [34], [36].

The experiments concentrated on the analysis of the data flow, synchronisation issues, interference effects, and connectivity reliabilities of each of the protocols. It was observed that while IEEE 802.11 offered high transmission speed, IEEE 802.15.4 provides relative stability and energy efficiency. It is fair to say that a hybrid of the two network protocols can offer sufficient characteristics for the secure and flexible IoT system of the future.

Chapter 2

Section 2.1 provides a general overview of the concept and historical development of cybersecurity, as well as today's information technology landscape. It examines not only the responsibilities of cybersecurity engineers but also offers an overview of Cyber Resilience Review (CRR), which includes both preventive and responsive measures in the face of cyber threats. Additionally, the human factor is emphasised as a crucial element in maintaining security, along with highlighting the importance of collaboration between various security stakeholders [37], [38].

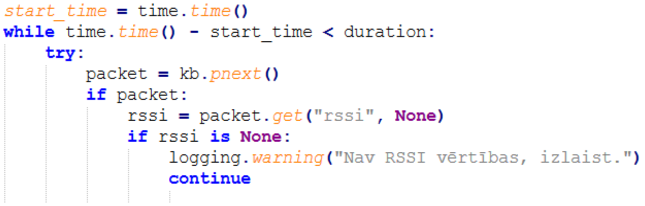
Section 2.2 examines various types of cybersecurity breaches through examples while evaluating their effects on IT infrastructure and service availability. The Section also examines threat sources, including external and internal threats, as well as their targets, typical vulnerabilities and the evolution of attack motivations.

Several significant virus attack examples are described:

- **Ransomware** is a type of virus, which is designed to encrypt data or block access to files. The user loses the capability to open documents or open essential applications on the computer. This type of malware provides some instructions on how to make a payment to decrypt the data. As a result, the IT systems of many organisations have been compromised by viruses such as WannaCry or Petya, where users lose full access to their computers.
- **Viruses** have the ability to infect files, spread within infrastructure, and replicate their executable code into other files or applications.
- **A Trojan horse** is a cyberattack in which malicious code is disguised as legitimate software or files.
- **A botnet is** a maliciously controlled network, which consists of malware-infected devices such as computers, routers, IP cameras, IoT devices and other network nodes [39].

Sections 2.3 and **2.4** are focused on the security challenges of IoT networks with special reference to the IEEE 802.15.4 standard. The author discusses the security features of the IEEE 802.15.4 standard, especially the encryption of data using TLS/SSL and AES or RSA algorithms. Authentication mechanisms such as OAuth, OpenID, 2F, RBAC and security update policies are also discussed. The risks are described in detail – wireless connection vulnerabilities such as man-in-the-middle (MitM) attacks, jamming and other attack types. Default credentials and insufficient device protection are highlighted as significant security issues. A systematic approach to ensuring network security is presented, including physical device protection and the use of intrusion detection and prevention systems (IDS/IPS) [9]–[10], [39]–[42].

Section 2.5 describes in detail the IEEE 802.15.4 standard security analysis and attack testing approach through the use of the Zigbee protocol. The Doctoral Thesis focuses on the practical value of vulnerability detection and the tools needed to build different attack scenarios using hardware devices and open-source software. The equipment used is described, including the CC2531 module, the Killerbee library, as well as a Python code element for extracting RSSI data [34], [35].



```
start_time = time.time()
while time.time() - start_time < duration:
    try:
        packet = kb.pnext()
        if packet:
            rssi = packet.get("rssi", None)
            if rssi is None:
                logging.warning("Nav RSSI vērtības, izlaist.")
                continue
```

Fig. 5. Example of RSSI value processing package from Killerbee.

During the Doctoral Thesis, different types of attacks were analysed.

- **Packet injection:** During the development of the Doctoral Thesis, additional attack packets were generated and initialised to resemble regular and legitimate traffic, but with lower RSSI values, characteristic of weaker or more distant sources. This was done to visually and functionally mimic normal IEEE 802.15.4 network behaviour while testing the network’s ability to recognise and process such traffic. This method enabled the identification of whether the network could effectively detect anomalies, such as irregularities in RSSI values that may pollute the traffic or render it inoperable.
- **DoS attack:** In the course of the research, additional attack packets were generated to intentionally overload the network by exceeding the normal packet transmission frequency allowed by the IEEE 802.15.4 standard. These packets were initialised with specific headers and parameters designed to mimic legitimate network behaviour, allowing for the assessment of the network’s ability to detect and process such malicious traffic.
- **Jamming attack:** As part of the Doctoral Thesis, deliberate signal interference was introduced into the network to block IEEE 802.15.4 communication. The signal jamming scenarios were simulated by analysing the network’s reaction to prolonged

periods of missing data, as well as sudden changes in signal strength (RSSI), which may indicate the presence of a potential attack.

The Doctoral Thesis also describes the use of HackRF One and CC2531 for attack detection and the implementation of protection scenarios through an adaptive jamming mechanism. A detailed overview is provided on how signal strength is measured and how data flow is analysed across various scenarios.

Chapter 3

Section 3.1 provides an overview of the technical specifications of wireless communications devices that would be needed for the Doctoral Thesis's experimental part, while **Subsection 3.1.1** presents both theoretical and practical evaluation of Zigbee network throughput based on Shannon's theorem and an empirically adjusted throughput model. The analysis considers influencing factors such as the limited channel bandwidth (2 MHz), the presence of signal interference, protocol overhead, and the operation of the CSMA/CA mechanism [35], [43]–[46].

The theoretical maximum transmission throughput of the Zigbee standard reaches up to 250 kbit/s, but testbed conditions reduce this to 120 kbit/s due to noise floor levels, SNR, packet transmission success probability, channel utilisation coefficient and other parameters.

The defined Formulas (3.1)–(3.4) included the packet success probability coefficient (P_{success}) and channel utilisation coefficient (*Duty_Cycle)* for integration. The SNR calculation used RSSI minus the assumed –95 dBm noise floor value. The transmission efficiency criteria relied on measurable parameters that exist in practice [46]–[56].

$$C = C_{\text{THEORETICAL}} \times (1 - OVERHEAD) \times P_{\text{success}} \times Duty\,Cycle\,, \tag{3.1}$$

where

C – maximum achievable throughput (kbit/s);
$C_{THEORETICAL}$ – theoretical Zigbee throughput (250 kbit/s);
OVERHEAD – protocol overhead (0.4 = 40 %);
P_{success} – probability coefficient of successful packet transmission;
Duty_Cycle – coefficient of channel utilisation [46], [56].

$$SNR = RSSI - NOISE\_FLOOR, \tag{3.2}$$

where

SNR – signal-to-noise ratio (dB);

$RSSI$ – received signal strength indicator (dBm);

$NOISE\_FLOOR$ – noise floor level (dBm).

$$P_{\text{success}} = \left(0.1, \left(1.0, \frac{SNR}{MAX\_SNR}\right)\right), \tag{3.3}$$

where

P_{success} – probability coefficient of successful packet transmission;

SNR – signal-to-noise ratio;

MAX_SNR – maximum signal-to-noise ratio.

$$Duty\_Cycle = \left(0.1, \left(0.8, \frac{SNR}{MAX\_SNR}\right)\right), \tag{3.4}$$

where

$Duty\_Cycle$ – coefficient of channel utilisation;

SNR – signal-to-noise ratio;

MAX_SNR – maximum signal-to-noise ratio.

The author chooses 40 dB as the *MAX_SNR* value because it stems from practical measurements that consider the wireless Zigbee network limitations. This parameter affects those calculations of both the packet transmission success probability and the channel utilisation coefficients. Zigbee networks function within the 2.4 GHz frequency range, which faces major interference from Wi-Fi and Bluetooth systems. The value of 40 dB stands as a reliable empirical measurement for upcoming measurement activities according to [47] and [51].

The packet transmission success probability remains at 10 % when the SNR is low, but increases to 100 % at its maximum value. The channel utilisation coefficient remains below 80 % even when SNR reaches its highest point, because CSMA/CA and network load restrictions limit transmission duration. The results validate the requirement to optimise network operation in particular application environments that prioritise energy efficiency. The research findings establish a foundation for designing IoT systems that meet specific infrastructure requirements.

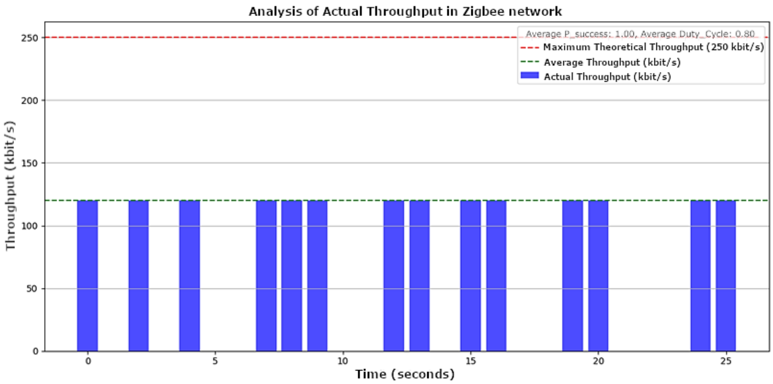


Fig. 6. Analysis graph of Zigbee network actual throughput.

Subsection **3.1.2** describes the distribution of RSSI in a wireless Zigbee network evaluated using the Nakagami distribution, which provides a more accurate representation of complex multipath propagation environments compared to traditional Rayleigh and Rician models [52], [53].

The Nakagami distribution was used in the Doctoral Thesis to model signal propagation in wireless networks and to assess its impact on network performance. The following probability density function is used to model the RSSI values.

$$F \sim Gamma\left(m, \frac{m}{\omega}\right), \tag{3.5}$$

where m is a shape parameter, and ω is a scale parameter.

Expression (3.5) is used to produce Nakagami distribution data, which helps modify RSSI readings and create realistic wireless network signal fluctuations. The randomly generated data receive their distribution characteristics through a probability density function (PDF), which is defined in Expression (3.6) [52]–[54].

$$f(x) = \frac{2m^{m}}{\Gamma(m)\omega} m_{x^{2m-1}e^{-\frac{m}{\omega}x^{2}},\ x>0}{}^{,} \tag{3.6}$$

where m is a shape parameter, ω = E[R^2] is a scale parameter, and Γ(m) is gamma distribution.

Using signal modulation calculations with Expressions (3.5) and (3.6) using the Nakagami distribution parameters $m = 0.8$ and $\omega = 0.3$, which were derived from experimentally obtained RSSI value (–85 dBm), which indicates a weak, unstable connection under non-line-of-sight (NLOS) conditions. Analysis of the experimental data shows that RSSI values in Zigbee networks also depend on obstacles in the environment and the effects of multipath reflection. Modified versions of RSSI values and network throughput were calculated by taking into consideration the effect of the Nakagami distribution. The results confirm that implementing this process allows for more realistic modelling of testbed environmental effects on network performance, which is important in designing IoT systems [52]–[54].

This is especially useful for assessing signal strength and throughput of a Zigbee network based on the Nakagami distribution. In Expression (3.7), the modified RSSI signal strength is calculated using real measured RSSI values from the Killerbee software and tools, and the modified throughput can be calculated from these modified RSSI values using Expressions (3.1)–(3.4) [47]–[56].

$$RSSImod = RSSIorig + 10 \times \log10(F), \tag{3.7}$$

where $RSSI_{orig}$ is the measured original $RSSI$ value, and F is a gamma distribution.

By applying the logarithmic correction of Expression (3.7), the value of *RSSI* considers random fluctuation of signal power due to multipath propagation effects (e.g. reflections, diffraction and scattering). Additionally, the *RSSI* value is a more practical value of random variations and demonstrates some of the uncertainty associated with situational complex environments such as buildings and urban areas.

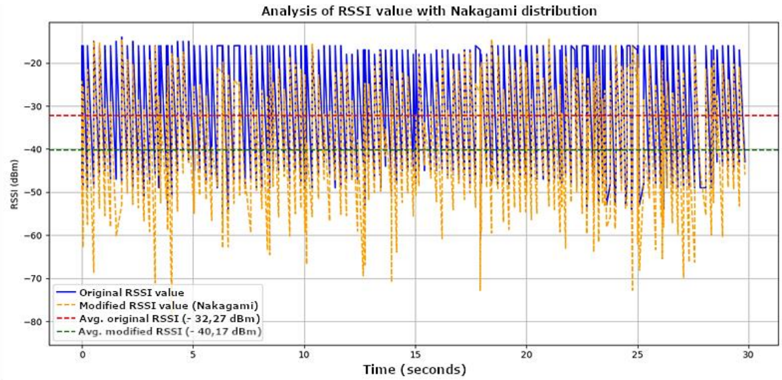


Fig. 7. *RSSI* value due to the Nakagami distribution.

In **Section 3.2,** the Zigbee network performance was analysed using Python-based launch scripts and Killerbee firmware tools. Furthermore, the modified *RSSI* value, which was constructed from the Nakagami distribution, was to be analysed a little more closely in order to retain a closer representation of the propagation characteristics in a real environment. The real throughput and modified throughput (Nakagami) performance, in addition to signal strength performance, would be analysed for study purposes across all compromises and counter measurements respectively [55].

The experimental part included three attack types: packet injection, DoS attack and signal jamming. Different injection time frequencies (0.25 and 0.5 seconds) were used. The experimental part was completed, observing the behaviour of the original and modified RSSI values and throughput (original and modified) value metrics.

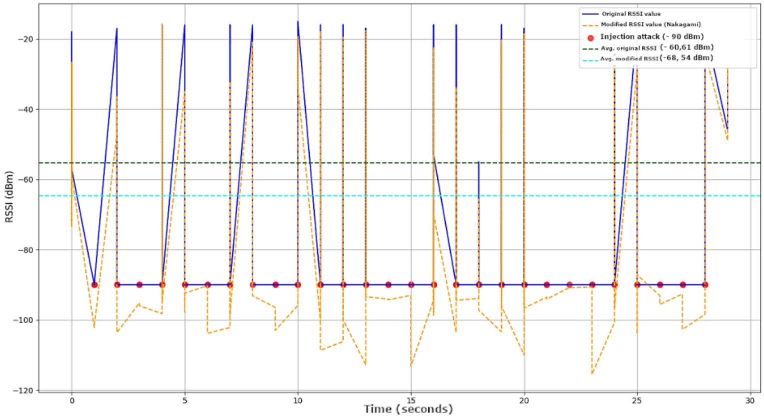


Fig. 8. *RSSI* analysis during a packet injection attack with a sending frequency of 0.25 seconds.

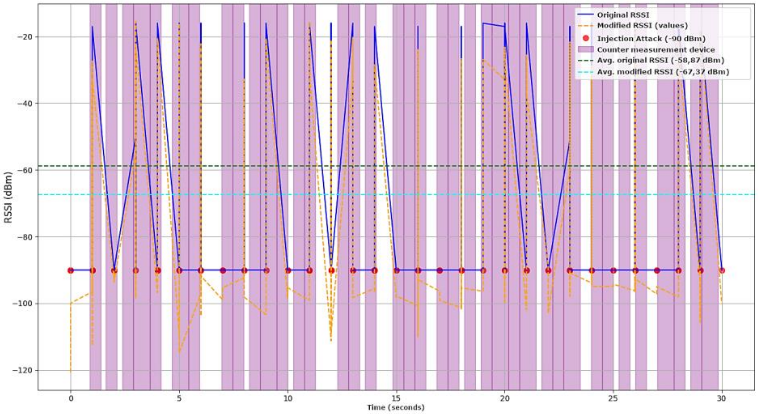


Fig. 9. *RSSI* analysis during a packet injection attack with a countermeasure device, with a sending frequency of 0.25 seconds.

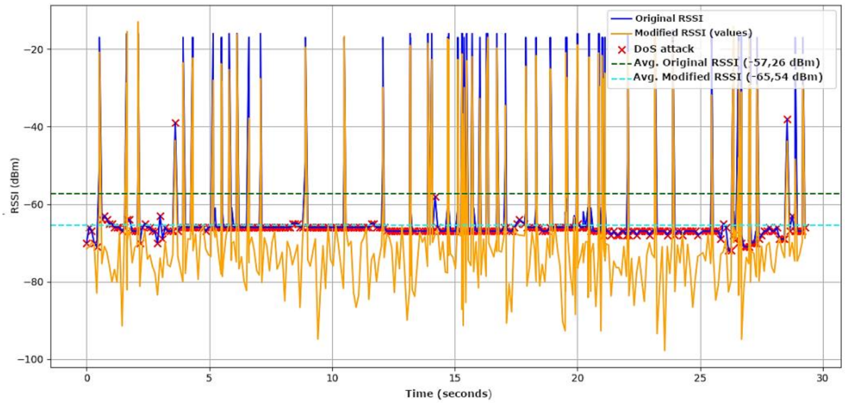


Fig. 10. *RSSI* analysis during a DoS attack.

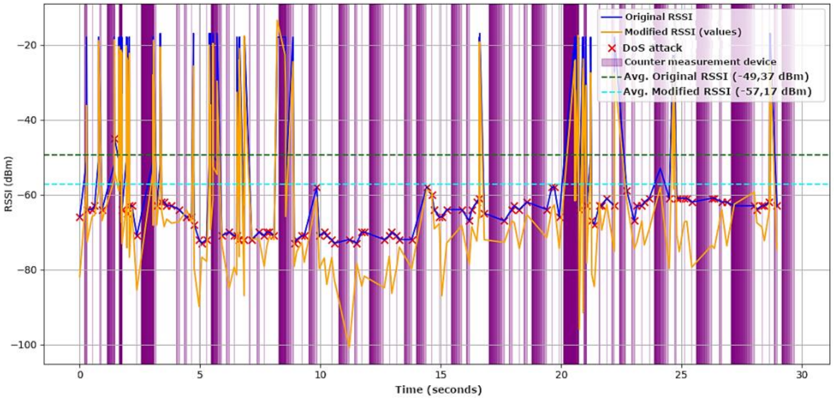


Fig. 11. *RSSI* analysis during a DoS attack and a countermeasure device.

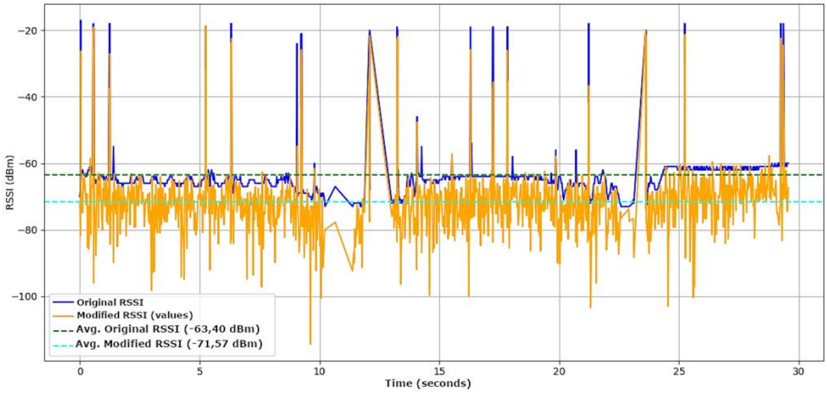


Fig. 12. *RSSI* analysis during a signal jamming attack.

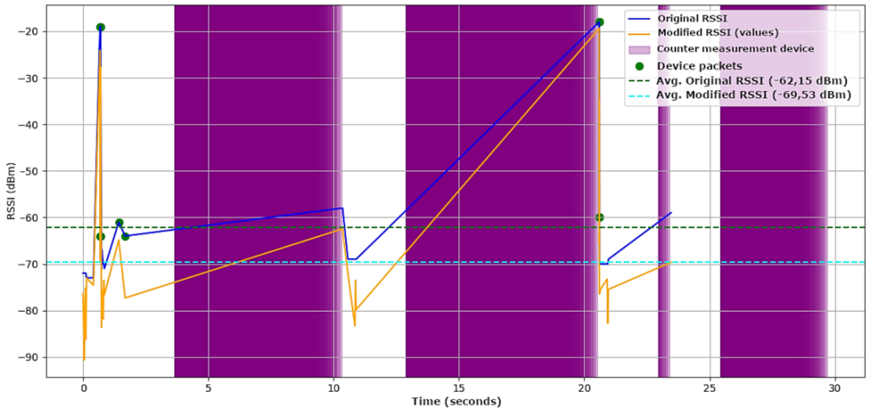


Fig. 13. *RSSI* analysis during a signal jamming attack and a countermeasure device.

The experimental part's findings show that packet injection attacks employing lower *RSSI* values of –90 dBm affect the Zigbee *RSSI* and throughput significantly, but cannot completely cease the network. Due to the longer measured time of 60–120 seconds, there is more fluctuation in the values for both *RSSI* and throughput (original and modified). It is especially significant when packet injection is occurring more frequently. DoS attacks using higher-frequency Zigbee packet traffic in the form of a DoS attack every 0.1 seconds had lower throughput, but there was still some flexibility in the network. The *RSSI* value was relatively stable, and although messages (packets) were being sent from one device to another, they were being sent at a lower throughput (it took longer to send a packet). Signal jamming attacks conducted at the highest frequency of 0.02 seconds resulted in rapid fluctuations of *RSSI* values and a lower original and modified throughput of the Zigbee network, demonstrating significant levels of channel or overload, indicating clear instability of the channel.

In order to combat the above-described attack interference, the CC2531 monitoring module and HackRF One countermeasure module were used, which could detect particularly harmful packets and stop any further delivery of those packets. It was shown that suppression of injection packets can maintain up to 99 % effectiveness, with stable throughput and only minor *RSSI* fluctuations. With DoS attacks, it was possible to reach throughput levels of around 85 % of normal, which is considered a significant accomplishment in terms of network resilience, and selective interference generation helped maintain that throughput. During jamming of signals, Zigbee self-adaptive technology (*RSSI* analysis, data signal recovery and filtering) helped counteract interference, allowing for improved quality in communication, particularly in long-term measurements.

This includes graphs that analyse the original *RSSI* and throughput and the modified measurements, which serve as visualisation of observed network behaviour under attack and countermeasure events. The valuable characteristics of adaptive networks were clearly illustrated, given the capability to maintain high efficiency in complex operational conditions. Given the ability to assess modified throughput through the use of real empirical models, it was possible to objectively assess the damaging impact that interference can have on the use of a Zigbee network and provide indications as to how the network may behave in certain future scenarios, making it an effective consideration when analysing the security of IoT infrastructure [46], [49], [50], [52], [60].

Chapter 4

Section 4.1 describes the additional (simulated) step – implementation of a simulation based on an ideal Zigbee network model, the ability to find and compare throughputs and *RSSI* readings to the previous results from the physical space and experimentation, as referred to earlier in this Doctoral Thesis. The site's expectation is to assess network performance under the best possible circumstances (external threats, such as packet injection, DoS or jamming, do not exist). Within the section, differences were noted between the simulated and physical results [56], [57].

Furthermore, in **Section 4.1,** a new metric is proposed, Recovery Value, which is a method that provides a numerical evaluation of the network's capacity to resume regular functioning following an attack. The efficiency evaluation is executed by expressing mathematical relationships between *RSSI* and throughput values before and after the implementation of avoidance measures [47], [48], [56].

In **Section 4.2,** a comparative analysis of the behaviour of the Zigbee network in the real environment to the behaviour of the Python simulation environment has been created. The focus of the comparative analysis was on investigating the performance of attack and defence mechanisms. This type of comparative analysis was useful for framework interference prevalent in the testbed and for determining how well the simulation environment represents practical purposes.

The simulated environment was controlled, all parameters were reproducible across tests; however, it cannot reflect the dynamic, multifactorial environment we see in IoT environments. For real IoT networks, there are aspects that we cannot control, such as the physical placement of devices, the electromagnetic conditions surrounding the devices and other unforeseen interferences. Due to this, the fluctuations in *RSSI* and throughput do not translate directly from the simulated networks to a real environment.

Table 1

Comparison of Average RSSI in the Real Network and Simulation. Types of Attacks and the Impact of Protection

	Real network performance				Simulation network performance			
Type of attack	**Avg. original RSSI value [dBm]**	**Avg. modified RSSI value [dBm]**	**Avg. recovered original RSSI value [dBm]**	**Avg. recovered modified RSSI value [dBm]**	**Avg. original RSSI value [dBm]**	**Avg. modified RSSI value [dBm]**	**Avg. recovered original RSSI value [dBm]**	**Avg. recovered modified RSSI value [dBm]**
Packet injection	–56.63	–65.46	–49.93	–58.75	–51.90	–58.77	–42.21	–49.15
DoS attack	–49.37	–57.17	–44.87	–51.77	–59.30	–67.84	–59.95	–69.70
Signal jamming	–62.15	–69.53	–57.85	–63.46	–53.88	–59.93	–47.18	–52.94

Table 2

Comparison of Average Throughput in a Real Network and in Simulation. Types of Attacks and the Impact of Protection

	Real network performance				Simulation network performance			
Type of attack	**Avg. original throughput value [kbit/s]**	**Avg. modified throughput value [kbit/s]**	**Avg. recovered original throughput [kbit/s]**	**Avg. recovered modified throughput [kbit/s]**	**Avg. original throughput value [kbit/s]**	**Avg. modified throughput value [kbit/s]**	**Avg. recovered original throughput [kbit/s]**	**Avg. recovered modified throughput [kbit/s]**
Packet injection	73.42	63.55	80.86	70.45	91.25	89.37	114.57	113.31
DoS attack	96.02	73.38	105.04	85.48	94.40	68.05	94.42	64.76
Signal jamming	74.51	50.08	82.25	60.16	87.83	83.75	104.33	101.97

As observed, the average recovered *RSSI* of the packet injection attacks under real network conditions was noticeably higher than in the simulation (–49.93 dBm compared to 42.21 dBm in the simulation). Throughput measures also illustrated that compared to the loading effects in the simulation, real testbed network conditions performed far better in an adaptive manner. For reference, in the case of a signal jamming attack, the throughput of the real network increased from 74.51 kbit/s to 82.25 kbit/s when the jamming protection mechanisms were subsequently implemented, illustrating that these real testing environments could adapt.

Table 3

Percentage of Successful Countermeasures in Real and Simulation Environments

	Effectiveness of countermeasures in real network [%]	Effectiveness of countermeasures in simulation [%]
Packet injection attack	94.83 %	85.14 %
DoS attack	47.75 %	93.33 %
Signal jamming attack	60.11 %	78.05 %

In contrast, in the case of denial-of-service attacks, the simulation showed a greater effectiveness of countermeasures (see Table 3) – 93.33 % of countermeasures percentage compared with only 47.75 % in the real network. This difference was likely due to latency in real environments and the inability to identify all of the DoS packets during real testing.

Table 4

RSSI Error Analysis for Experimental and Simulation Data (Original *RSSI* Values)

Type of attack	*MAE* orig. *RSSI*, *dBm*	*RMSE* orig. *RSSI*, *dBm*
Packet injection	33.33	40.01
DoS attack	19.99	25.74
Signal jamming attack	21.87	23.85

Table 5

RSSI Error Analysis for Experimental and Simulation Data (Modified RSSI Values)

Type of attack	*MAE* mod. *RSSI, dBm*	*RMSE* mod. *RSSI, dBm*
Packet injection	34.31	40.9
DoS attack	21.97	28.51
Signal jamming attack	23.69	28.10

RSSI error analysis between the simulation and real experimental setup identified that the largest differences occurred during the packet injection attacks (MAE ≈ 33.33 dBm, RMSE ≈ 40.01 dBm). The DoS attack error was smaller (MAE ≈ 19.99 dBm), which demonstrates that the simulation model had a more consistent accuracy performance in these instances [58], [59].

To summarise, this Section demonstrates that both environments and network simulations have their interpretations. The real network displayed great adaptability in an open environment to adapt to a packet injection attack, and simulations allowed for finding the best parameters while still allowing defence to be tested with falsified data and environment. With both environments or simulations combined, we can find more dependable and secure IoT solutions in future studies.

Chapter 5

Chapter 5 provides a thorough examination of IoT network management, security and performance optimisation aspects. These aspects examined current topics of concern in IoT networks, implementable solutions and the latest innovations that support network security and operational efficiencies in real-time situations. An expanding number of united devices and amounts of transferred data create new realms of concerns. Some of the most pressing concerns are monitoring and update management, the importance of security regulations and legislation, network traffic and throughput optimisation, and finally, the use of machine learning (ML) and artificial intelligence (AI) as it pertains to aspects of cybersecurity solutions.

Section 5.1 considers issues with device range, protocol differences and limited resources, with a focus on FOTA, which allows updates to occur remotely while still supporting authentication and data integrity.

Section 5.2 discusses regulations and legal considerations regarding security, and **Section 5.3** looks at network optimisation through edge computing, with lower latencies and more efficient data processing with filtering at source, for example, an IoT gateway.

Section 5.4 focuses on the role of ML and AI with respect to network security. In particular, anomaly detection, neural network models, and security orchestration, automation, and response (SOAR) are the basis for proactive defence models [60].

Section 5.5 explores network segmentation and micro-segmentation, which combine to restrict the spread of certain types of cyberattacks and provide application-level access control, which can be very helpful in IoT environments with large numbers of devices [61], [62].

Section 5.6 underlines the importance of a unified approach for managing performance and security. The importance of QoS is emphasised with respect to data flow prioritisation, coupled with an understanding of network stability during critical information transfer. QoS technologies allow limiting the impact of non-critical processes on the network and the alignment of resources to more important tasks [63].

Section 5.7 extensively explores IoT network behaviour in the presence of cyber threats, with a focus on mathematical modelling techniques used to describe changes in RSSI and changes in the throughput of the network during various attack types. It is noted that non-linear regression and hybrid models are crucial in accurately predicting behaviours and interpreting the dynamics faced within networks. In an experiment, it was determined that traditional regression was unable to capture the chaotic shifts in performance during the impacts of attacks [64].

Polynomial regression was harnessed to describe the overall changes in *RSSI* and throughput under the assumption that changes can be described using n-order polynomials:

$$y(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{5.1}$$

where

a_n, a_{n-1},…, a_0 – polynomial coefficients that determine the shape of the function using ordinary least squares (OLS);

x – normalised time ($x \in [0, 1]$);

$y(x)$ – estimated value (*RSSI* or throughput) [64], [65].

The coefficients a_i had been found using the OLS method, which aims to minimise the error function E that estimates the difference between the actual data y_i and polynomial $y(x_i)$:

$$E = \sum_{i=1}^{N} \left(y_i - y(x_i)\right)^2, \tag{5.2}$$

where N is the number of data points.

To determine the coefficients, the matrix form is used:

$$Y = XA + \epsilon, \tag{5.3}$$

where

Y – the vector of observed values (measurements);

X – the design matrix (containing powers of input variables);

A – the vector of unknown coefficients;

ϵ – noise and measurement errors.

The coefficients are calculated using the normal equation:

$$A = (X^T X)^{-1} X^T Y. \tag{5.4}$$

This means that each a_i is estimated by minimising the error between observed and predicted data.

The hybrid model is made by averaging between polynomial regression and cubic spline interpolation. This allows for smoothing the data while preserving the trends in throughput, while filtering the effects of noise in the network and *RSSI* measurements. Depending on the degree of the polynomial, a least squares polynomial fit may be quadratic, cubic, or of the fifth order with a bias towards approximation [64]–[66].

The cubic spline is defined as

$$S(x) = \sum_{i=1}^{m} b_i B_i(x), \tag{5.5}$$

where

$B_i(x)$ – the basis spline functions;

b_i – the coefficients calculated to ensure a smooth interpolation of the curve;

m – the number of spline nodes.

The spline coefficients are obtained by minimising the following error function:

$$E = \sum_{i=1}^{N} \left(y_i - S(x_i)\right)^2 + \lambda \int \left(S''(x)\right)^2 dx, \tag{5.6}$$

where λ is the regularisation parameter that controls the smoothness of the spline [64].

The higher-order polynomial, cubic spline and hybrid methods provide a good balance between accuracy and smoothness and have the added benefit of filtering out error and highlighting important trends, like the drastic drop in throughput during a DoS attack and jamming attack, or the subsequent recovery period after defence mechanisms are triggered.

In other words, the use of polynomial and spline methods will allow us to isolate the moments of attack while modelling the way the network would have naturally responded, even noting the recovery period after each excursion. Of note, the models were validated through R^2, where the higher-order models exhibited much higher correlations with actual data, as opposed to the classical method.

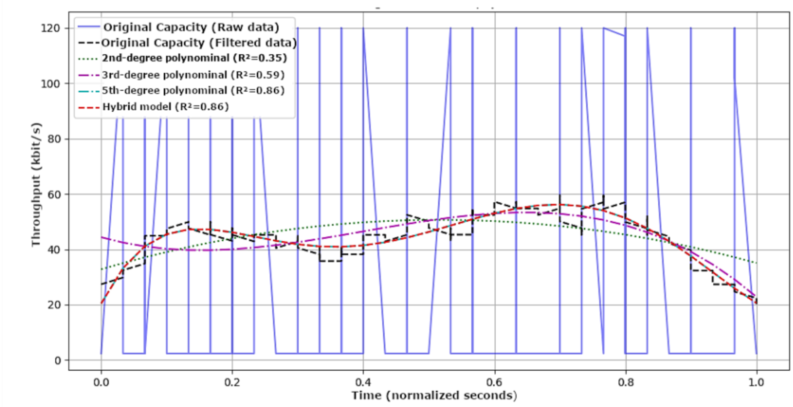


Fig. 14. Analysis of changes in network throughput. Original data, packet sending frequency – 0.25 seconds with polynomial and hybrid models during packet injection.

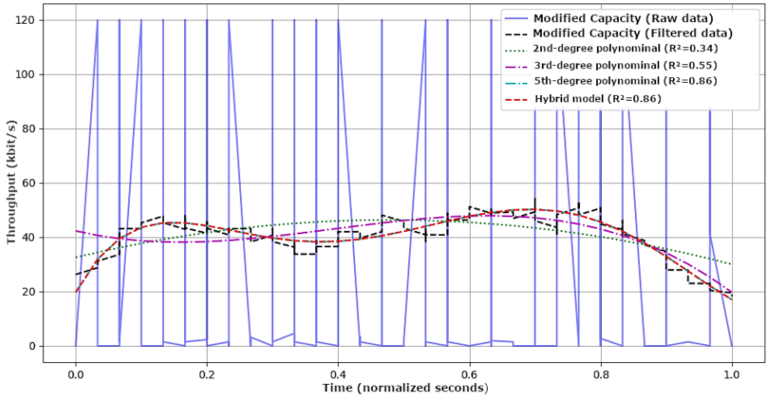
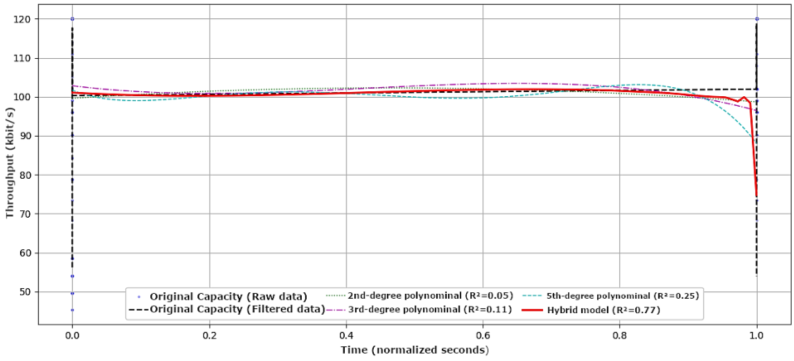
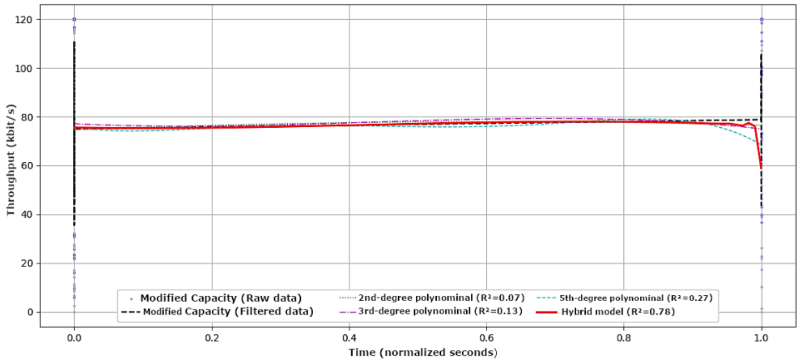


Fig. 15. Analysis of changes in network throughput. Modified data, packet sending frequency – 0.25 seconds with polynomial and hybrid models during packet injection.

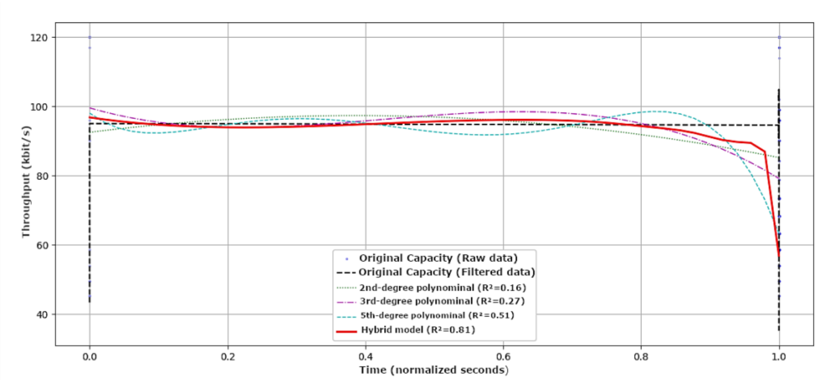


a)

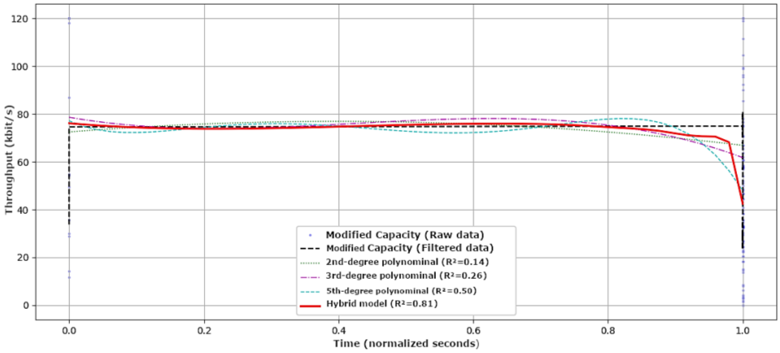


b)

Fig. 16. Analysis of changes in network throughput: a) – original data; b) – modified data with polynomial and hybrid models during DoS attack.



a)



b)

Fig. 17. Analysis of changes in network throughput: a) – original data; b) – modified data with polynomial and hybrid models during signal jamming attack.

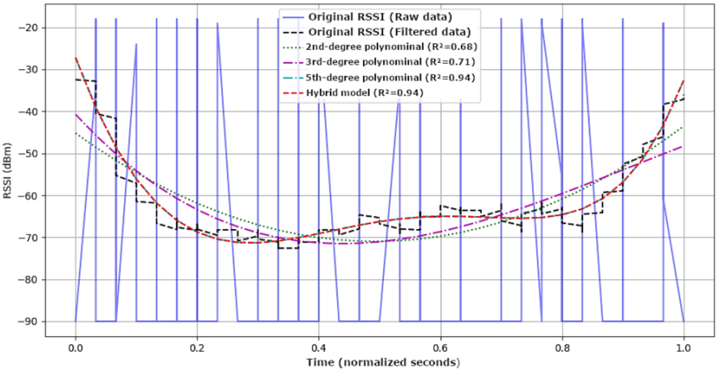


Fig. 18. Analysis of changes in *RSSI*. Original data, packet sending frequency – 0.25 seconds with polynomial and hybrid models during packet injection.

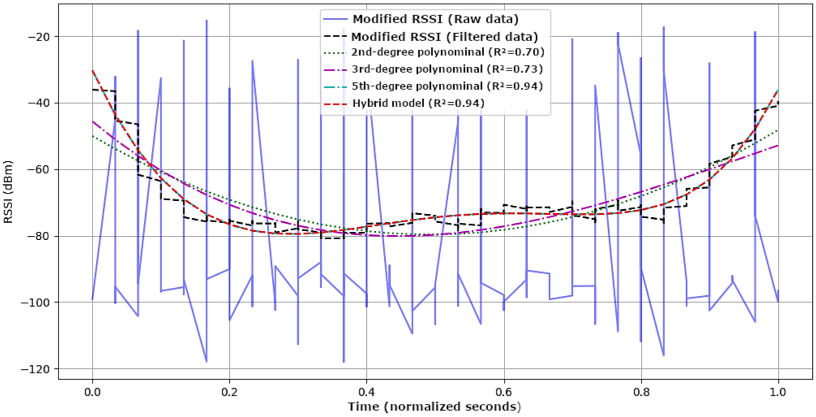
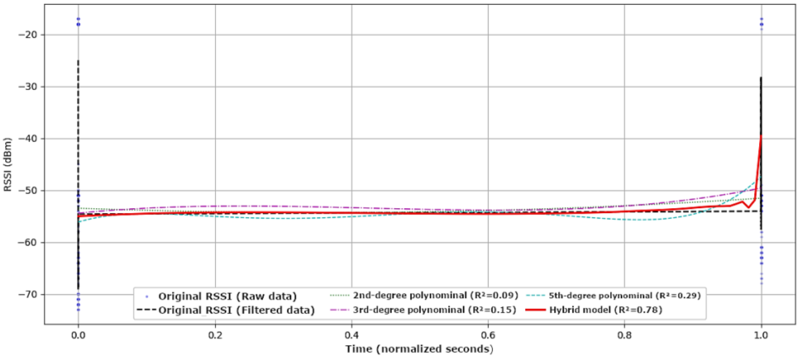
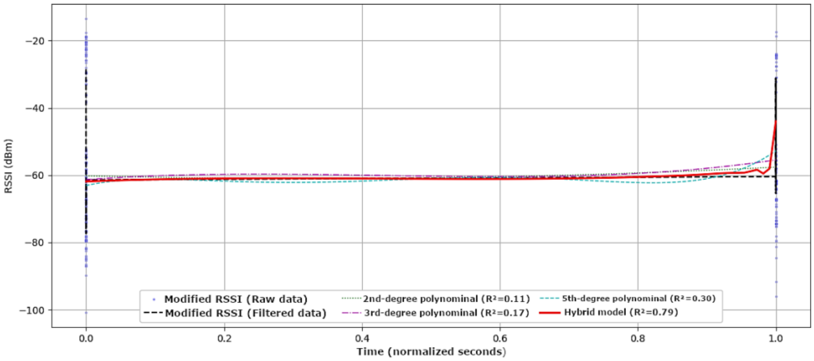


Fig. 19. Analysis of changes in *RSSI*. Modified data, packet sending frequency – 0.25 seconds with polynomial and hybrid models during packet injection.

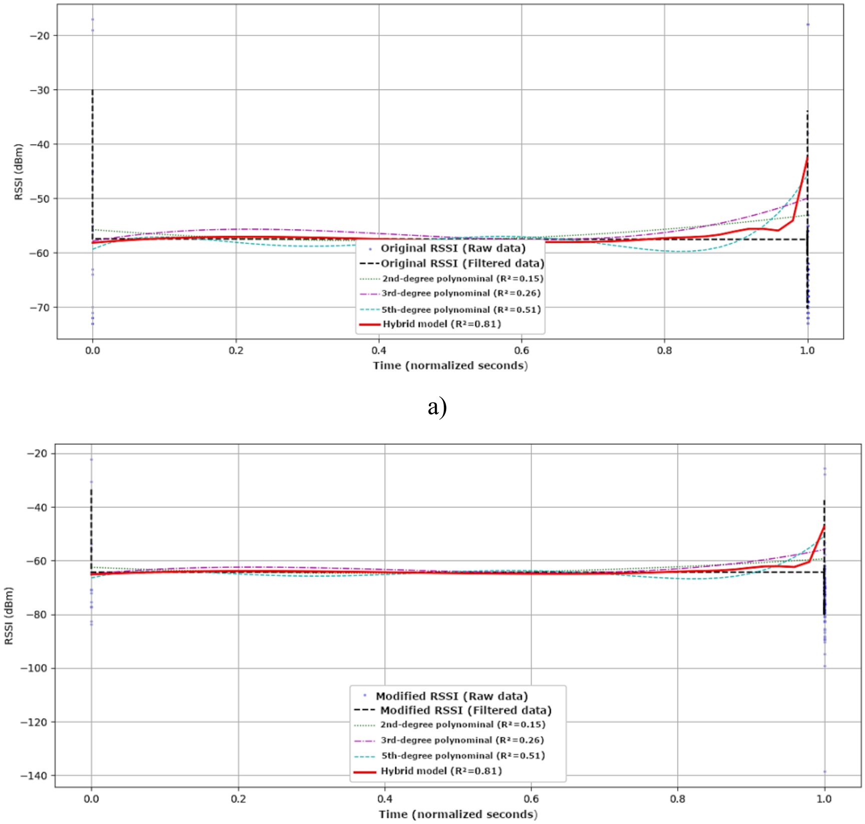


a)



b)

Fig. 20. Analysis of changes in *RSSI*: a) – original data; b) – modified data with polynomial and hybrid models during DoS attack.



a)

b)

Fig. 21. Analysis of changes in *RSSI*: a) – original data; b) – modified data with polynomial and hybrid models during signal jamming attack.

The analysis demonstrates that variations in the values of the *RSSI* and throughput indicators can be useful for automated attack detection systems. This allows for the development of dynamic defences that change with the changes in load on the network and the type of interference. It was determined that hybrid models are optimal in achieving a good balance of fitting data and filtering out noise, which can be particularly useful for detecting IoT network attacks and measuring its recovery. The conclusion of Chapter 5 of the Thesis proposes an original, mathematically rigorous approach for assessing the security of IoT networks, which may be used as a starting point for developing automated defence in different application scenarios in the future.

SUMMARY OF THE DOCTORAL THESIS

The **goal of the Doctoral Thesis** was to carry out an extensive investigation of the security of wireless communication networks, more specifically, a hybrid network based on IEEE 802.11 and IEEE 802.15.4 standards, their vulnerabilities and the proposal of some defence mechanisms that could potentially guarantee the stability and security of the network from a myriad of cyber threat conditions. Specifically, it aimed to develop and evaluate methods for the effective protection against attacks on IEEE 802.15.4 wireless networks. Examples of these attacks included DoS, signal jamming and packet injection. The study also considered network throughput, RSSI and recovery after attacks.

C**hapter 1** examines the IEEE 802.11 and IEEE 802.15.4 standards with particular focus on the use of these standards in IoT networks. The IEEE 802.15.4 standard is typically used in Zigbee networks and is designed for low throughput and narrow-bandwidth communication, which is interesting for IoT devices. It has lower energy usage, which allows a longer operation time, but also has vulnerabilities because of the limited security, and these devices are susceptible to attacks such as DoS and jamming. The findings also outline vulnerabilities related specifically to many IEEE 802.11 standards, for example, WPA2 and WPA3 encryption vulnerabilities are still open to attacks, which still pose a significant threat to Wi-Fi networks. The overall findings suggest that IEEE 802.15.4 networks are vulnerable to a wider variety of attacks due to their resource-constrained conditions and their use of the 2.4 GHz frequency band, while IEEE 802.11 standards pose a higher data rate but are also limited by vulnerabilities to security.

Chapter 2 provides a comprehensive exploration of the types of network attacks and how they can affect the viability of IEEE 802.11 and IEEE 802.15.4 networks. The chapter describes the types of attacks and the importance of wireless network operation, including DoS attacks, packet injection, etc., and elaborates on which parts of the network throughput and overall network service stability were affected. The chapter also describes protection mechanisms relevant to both IEEE 802.11 and IEEE 802.15.4 networks that aim to defend against varying types of attacks. The conclusions laid out in the chapter describe which attacks were selected for the testbed, provide insight into their primary mechanisms and highlight the impacts.

Chapter 3 provides a detailed overview of the experimental setup and technologies used to examine RSSI, throughput and security. Several devices were tested in the experimental part, including the RZUSBStick (acting as the attack transmitter), CC2531 IEEE 802.15.4 network packet sniffer module and HackRF One SDR universal tool to implement countermeasures. Also, calculations were conducted on throughput using an empirical model arising from Shannon's theorem (i.e., a theoretical limit based on real testing packet transmissions). The purpose of the model calculations was to estimate the maximum theoretical throughput (the maximum expected throughput, limited only by theoretical packet transmission parameters). The calculations yielded a theoretical throughput that can be as high as 250 kbit/s, but the primary throughput limitations were reduced to an operational level of approximately 120 kbit/s (the resultant throughput is highly dependent upon the real testbed location, environmental setups and factors worsening). The Nakagami distribution was also employed in a model to study an understanding of signal quality variations due to variations with different levels of network load. The fixed Nakagami parameter (m = 0.8, Ω = 0.3) allowed analytics as to the impacts of throughput due to signal strength analyses, which contributed to understanding network behaviour under interference. The experimental findings illustrated that we observed significant levels of degraded network performance and throughput as DoS attacks create continual interference, such that the user experience was congested, whereby any legitimate activity was not possible. The effectiveness of the protection for the IEEE 802.15.4 network was only 47.75 %, which increasingly signifies the complexity in real-world environments and external factors that would create outside power to exacerbate the effectiveness of DoS attacks (which, moreover, did not completely paralyse the network, but degraded its performance). The other attacks provide some or diminished signals of jammers, given that they created some interference, causing the likelihood of interference on signal quality. However, because the primary attack regarding throughput was related to the network's overall support (i.e., performance diminished, requiring alternate throughputs, which takes into account congestion to 50.08 kbit/s), the effectiveness of protection measures was 60.11 %, which is also demonstrably better than observed during the DoS attacks. Finally, the packet injection attack was detected, and protection was used to block only over 94.83 % of true positives with the introductory use of more sophisticated methods, packet filtering and authentication.

Chapter 4 presents an analysis of the experimental outcomes by contrasting those obtained in an actual environment with those obtained in a simulation environment with Python. It was analysed that protection mechanisms perform substantially better in simulation environments, which do not have external disturbances (i.e., physical layer limitations on the hardware or radio medium, etc.). It was determined that in actual environments, the DoS and jamming attacks impacted the percentage of overall throughput for the network. The effective countermeasures, such as dynamic frequency shifting and packet filtering practices, resulted in impacts being reduced by approximately 40–60 %. In simulation settings, the protection efficiency for DoS attacks was 93.33 %, for jamming attacks 78.05 %, but for packet injection, it was under the performance for actual networks at 85.14 %.

Chapter 5 provides further evaluation of both additional performance and protection measures for IEEE 802.15.4 to improve network operations, which includes micro-segmentation, QoS and VLAN in IEEE 802.11 networks, and their indirect interaction in IoT systems. Polynomial regression models were used to identify and predict the network post-attack recovery performance. For example, network performance was back to 85 % of its throughput just after 30 seconds, following a DoS attack using regression-based forecasting. This included the successful application of polynomial regression models for predicting and improving network recovery. The polynomial regression models were used to identify faster dynamic recovery stabilisation patterns and provide an acceptable rate of accuracy (96 %) for estimating completion time, significantly enhancing network security and performance in response to other attacks. These mechanisms allowed for identifying improved network security and performance timelines.

The conducted study clearly indicated that IEEE 802.15.4 networks are susceptible to attack, and the use of strong protection mechanisms greatly enhances security and reliability within the network. The study demonstrated that both DoS and jamming attacks are the most difficult types of attacks to detect, as they damage the network through the physical layer and disrupt signal transmission and the ability of the network to function. Packet injection attacks were shown to be the most blocked attack type, primarily because the packet filtering mechanisms protected unauthorised packet transmission through the network.

The Nakagami distribution was used to model the *RSSI* variation across all tests and at different distances and conditions of attack, allowing for a realistic analysis of signal quality and proving useful for investigating network behaviour during attacks. Additionally, the created simulation environment provided a secure area to examine the different attacks and protection mechanisms before applying them in the real tests, and allowed for the improvement of network protection methods and the evaluation of their effectiveness.

There is an important practical element to this study due to the mechanisms for protection that can be close to implementation in several IoT and Zigbee networks, which will greatly enhance the security and reliability of the network. There is value in being able to develop such mechanisms to suit smart homes and networks in industry, as there is a high requirement for security to protect digital information and ensure the reliability of the network.

In the future, this approach has several opportunities to be continued in several directions. One direction would be to incorporate ML algorithms into the experiments to enhance the effect of attacks being predicted and detected, so that threats are diminished before impacting network operations. It would also be fascinating to test on larger networks with more than 100 IoT devices to see how protected or unprotected networks perform in more complex environments. Testing the protection mechanisms in a hybrid network where both IEEE 802.11 and IEEE 802.15.4 standards can be used concurrently would be pertinent, considering that numerous modern IoT infrastructures are designed as hybrids.

Comparative Analysis with Traditional Network Security Solutions

By using the comparison with the most commonly referenced sources in network security, it can be established that the author has proposed an innovative method for protection in Zigbee networks. While in the sources primarily focus on general network security in nature, authentication, access control, and cryptography algorithms security, the Thesis focuses on the security analysis of specific hybrid networks IEEE 802.11 and IEEE 802.15.4 against actual attack scenarios, specifically attacks relevant to Zigbee environments [67], [68].

Overall, the primary contribution of the Thesis is an approach for experimentally verifying the handling of packet injection, DoS, and jamming attacks in Zigbee networks, which have not been adequately examined in previous studies. The experiments carried out in this study were conducted to see various attack techniques and remedies, and a variety of experiments were considered – this included selective blocking of packets on the network, adaptive jamming based on packet headers or other types of attributes, and network recovery modelling.

Experimental analysis was done using real hardware and software, along with mathematical models, using a low-level network protocol and software. This was performed to provide a much better prediction of how a network would behave after an attack occurs.

BIBLIOGRAPHY

[1] Neuron Team. “KNX Protocol: The Basics and Its Possibilities with IoT”. Emqx.com. https://www.emqx.com/en/blog/knx-protocol (accessed Nov. 10, 2023).

[2] Shashkina, V. “IoT solution architecture: an overview of components & design tips.” Itrexgroup.com. https://itrexgroup.com/blog/iot-architecture-components-design-tips/ (accessed Aug. 31, 2022).

[3] AVSystem. “IoT Protocols & Standards Guide – Protocols of the Internet of Things.” Avsystem.com. https://avsystem.com/blog/iot/iot-protocols-and-standards (accessed Jul. 6, 2024).

[4] TDT BMS. “How a battery management system (BMS) works and its role in different sectors.” https://www.tdtbms.com/ru/news/-how-a-battery-management-system-bms-works-and-its-importance-across-industries.html (accessed Aug. 8, 2024).

[5] Toulas, B. “Bleeping Computer Chinese cyberspies use new SSH backdoor in network device hacks.” Bleepingcomputer.com. https://www.bleepingcomputer.com/news/security/chinese-cyberspies-use-new-ssh-backdoor-in-network-device-hacks/ (accessed Feb. 4, 2025)

[6] Shaikh, R. A. “Backdoor uncovered in China-made patient monitors – Contec CMS8000 raises questions about healthcare device security.” Tomhardware.com. https://www.tomshardware.com/tech-industry/cyber-security/backdoor-uncovered-in-china-made-patient-monitors-contec-cms8000-raises-questions-about-healthcare-device-security (accessed Feb. 1, 2025)

[7] Yiming Li, Yong Jiang, Zhifeng Li, Shu-Tao Xia, “Backdoor Learning: A Survey”, 2020, p. 17.

[8] PIRIT. “Information Security.” Pirit.biz. https://pirit.biz/reshenija/informacionnaja-bezopasnost (accessed Apr. 12, 2019)

[9] Payatu Security. “Zigbee Security 101: Architecture and Security Issues.” Payatu.com. https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/ (accessed Feb. 11, 2023)

[10] Kudelski Security. “Zigbee Security Basics: Part 3.” Research.kudelskisecurity.com. https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/ (accessed Nov. 21, 2017)

[11] Ancāns, A. “Research and Improvement of the Performance of Road Transport Wireless Communication Networks”, RTU Press, 2021, 175 p.

[12] Saliga, S. V. “An introduction to IEEE 802.11 wireless LANs”, IEEE Xplore, 2000, 10 p.

[13] Tektronix. “Wi-Fi Overview: 802.11 Physical Layer and Transmitter Measurements// Tektronix.” Tek.com. https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements (accessed 2017).

[14] Sharma, P., Singh, G. “Comparison of Wi-Fi IEEE 802.11 Standards Relating to Media Access Control Protocols”, International Journal of Computer Science and Information Security, 2016, 7 pp.

[15] Kurnaz, C., Engiz, B. K., Kose, U. “Investigating the effect of number of users on signal strength level and throughput for Wi-Fi system”, IEEE, 2017, 4 p.

[16] Song, X., Wu, M., Jermaine, C., Ranka, S. “Using support vector machines for anomalous change detection”, Proceedings of the 3rd IEEE International Conference on Data Mining (ICDM 2003), 2003, pp. 626–629.

[17] Banerjee, S., Sharan, A. “WiFi-LSTMs: A deep learning approach for WiFi-based human activity recognition”, IEEE Access, 2021, Vol. 9.

[18] NetSpot. “Wireless Security Protocols: WEP, WPA, WPA2, and WPA3.” Netspotapp.com. https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html

[19] HFCL. “WPA2 vs WPA3: Key Difference in Wi-Fi Security Protocols.” HFCL.com. https://io.hfcl.com/blog/wpa2-vs-wpa3/ (accessed May 7, 2024)

[20] Cisco Meraki. “WPA3 Encryption and Configuration Guide.” Meraki.com. https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide (accessed Apr. 15, 2025)

[21] Telecommunication Standardization Sector of ITU, “Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks, Next Generation Network – Frameworks and Functional Architecture Models, Overview of the Internet of Things”, 2012.

[22] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. “Internet of Things: A General Overview between Architectures, Protocols and Applications,” IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, pp. 2347–2376, Oct. 2015, DOI: 10.1109/COMST.2015.2444095.

[23] **Aleksandrovs-Moisejs, D.,** Ipatovs, A., Grabs, E., Rjazanovs, D., Sinuks, I. “Arduino-based temperature sensor organization and design,” 2023 Photonics & Electromagnetics Research Symposium (PIERS), Aug. 2023, DOI: 10.1109/PIERS59004.2023.10221361

[24] Sethi, B. K. “Your complete guide to IoT protocols and standards in 2022 for support secure data exchange.” Kellton.com. https://www.kellton.com/kellton-tech-blog/your-complete-guide-to-iot-protocols-and-Standards-2022 (accessed Mar. 15, 2022).

[25] NetworkLessons. “IoT Standards and Protocols.” NetworkLessons.com. https://networklessons.com/cisco/evolving-technologies/iot-standards-and-protocols

[26] Allerin. “Six Types of IoT Network Protocols” Allerin.com https://www.allerin.com/blog/six-types-of-iot-network-protocols

[27] Frenzel, L. “What’s the Difference Between IEEE 802.15.4 and Zigbee Wireless?” Electronicdesign.com. https://www.electronicdesign.com/technologies/communications/wireless/article/21796046/whats-the-difference-between-ieee-802154-and-zigbee-wireless (accessed Mar. 22, 2013).

[28] GeeksforGeeks. “Introduction of IEEE 802.15.4 Technology” GeeksforGeeks.org https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/ (accessed Feb. 22, 2023)

[29] Saleem, S., Ullah, S., Kwak, K. S. “A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks”, Graduate School of Information & Communication Engineering, Jan. 2011, p. 13.

[30] Goldoni, E., Savioli, A., Risi, M., Gamba, P. “Experimental analysis of RSSI-based indoor localization with 802.15.4”, IEEE Xplore, May 2010, p. 8.

[31] Delsing, J., Eliasson, J., Leijon, V. “Latency and Packet Loss of an Interferred 802.15.4 Channel in an Industrial Environment”, SensorComm 2010, July 2010, p. 9.

[32] Latre, B., De Mil, P., Moerman, I., Dierdonck, N. V., Dhoedt, B., Demeester, P. “Maximum Throughput and Minimum Delay in IEEE 802.15.4”, Mobile Ad-hoc and Sensor Networks, First International Conference, MSN 2005, Dec. 2005, p. 12.

[33] Shu, F., Sakurai, T., Zukerman, M., Vu, H. “Packet loss analysis of the IEEE 802.15.4 MAC without acknowledgments”, IEEE Communications Letters, Jan. 2007, p. 4.

[34] Hacking Land. “KillerBee – IEEE 802.15.4/ZigBee Security Research Toolkit” Hacking.land. https://www.hacking.land/2018/07/killerbee-ieee-802154zigbee-security.html?m=1 (accessed Jul. 2018).

[35] River Loop Security. “KillerBee Project Overview” RiverLoopSecurity.com. https://riverloopsecurity.com/projects/killerbee/

[36] "AVR2016: RZRaven Hardware User's Guide", Microchip Documentation, https://manualzz.com/doc/19793759/avr2016--rzraven-hardware-user-s-guide-8-bit-microcontrol

[37] Microsoft. "What is Information Security (InfoSec)?" Microsoft Security, 2024.

[38] Sousa de Araujo, M., Souza Machado, B. A., Passos, F. U., "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance", Progress and Research in Cybersecurity and Data Privacy, Mar. 2024, p. 16.

[39] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. "DDoS in the IoT: Mirai and Other Botnets", ResearchGate, Jan. 2017, p. 6, DOI: 10.1109/MC.2017.201

[40] Mazhar T., Talpur, D. B., Al Shloul, T., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., Hamam, H. "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence", MDPI Intelligent Neural Systems for Solving Real Problems, Apr. 2023, p. 30.

[41] Singh, J., Rani, S., Kumar, V. "Role-Based Access Control (RBAC) enabled secure and efficient data processing framework for IoT networks," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 16, No. 2, Aug. 2024. pp. 19–32.

[42] Security Scorecard. "Cybersecurity for the Internet of Things (IoT)" SecurityScorecard.com. https://securityscorecard.com/blog/cybersecurity-for-the-internet-of-things-iot/ (accessed Feb. 8, 2024).

[43] Texas Instruments: CC2531 Datasheet, Texas Instruments. – https://www.ti.com/lit/ds/symlink/cc2531.pdf

[44] Adafruit. Great Scott Gadgets HackRF One – Software Defined Radio. https://www.adafruit.com/product/3583

[45] MetaGeek. "Zigbee and Wi-Fi Coexistence" MetaGeek.com. 2024. https://www.metageek.com/training/resources/zigbee-wifi-coexistence/ (accessed 2024).

[46] NS2Project. "How to Calculate Network Channel Capacity in NS2" NS2Project.com. https://www.ns2project.com/how-to-calculate-network-channel-capacity-in-ns2/ (accessed 2024).

[47] Haque, K. F., Abdelgawad, A., Yelamarthi K. "Comprehensive Performance Analysis of Zigbee Communication: An Experimental Approach with XBee S2C Module", MDPI Reliability Analysis of Wireless Sensor Network, Apr. 2022, p. 23.

[48] Lanzisera, S., Mehta, A. M., Pister, K. S. J. "Reducing Average Power in Wireless Sensor Networks Through Data Rate Adaptation", Communications, 2009. ICC '09. IEEE International Conference, Jul. 2009, p. 6.

[49] Rupareliya, K. “Top 6 Factors to Consider When Designing the IoT Infrastructure”, Spiceworks.com. https://www.spiceworks.com/tech/iot/guest-article/factors-to-consider-when-designing-the-iot-infrastructure/ (accessed Sept. 20, 2021).

[50] Burchfield, T. R., Venkatesan, S., Weiner, D. “Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations.”, MobiusConsulting.com., 2007, p. 13.

[51] Goyal, M., Prakash, S., Xie, W., Bashir, Y., Hosseini, S. H., Durresi, A. “Evaluating the Impact of Signal to Noise Ratio on IEEE 802.15.4 PHY-level Packet Loss Rate”, The 13th International Conference on Network-Based Information Systems, NBiS 2010, 2010, pp. 279–284.

[52] Di Marco, P., Fischione, C., Santucci, F., Johansson, K. H. “Modeling IEEE 802.15.4 Networks over Fading Channels”, IEEE Transactions on Wireless Communications, Sept. 2012, p. 30.

[53] Bandur, D., Jaksic, B., Raicevic, A., Popovic, B., Bandur, M. “Performance Analysis of an IEEE 802.15.4 Network Operating Under κ–μ Fading, Interference and AWGN”, Iranian Journal of Science and Technology, Transactions of Electrical Engineering, Vol. 44, Mar. 2020, pp. 1549–1557.

[54] Molisch, A. F., Balakrishnan, K., Cassioli, D., Chong, C-C., Emami, S., Fort, A., Karedal, J., Kunisch, J., Schantz, H., Schuster, U., Siwiak, K. “Channel Model Final Report for IEEE 802.15.4a”, IEEE Communications, Jan. 2004, p. 40.

[55] Carnegie Mellon University. Zigator: Security Analysis of Zigbee Networks. https://mews.sv.cmu.edu/research/zigator

[56] Lopez-Vilos, N., Valencia-Cordero, C., Azurdia-Meza, C., Montejo-Sanchez, S., Mafra, S. B. “Performance Analysis of the IEEE 802.15.4 Protocol for Smart Environments under Jamming Attacks”, MDPI Cyber Security in IoT Era, Jun. 2021, p. 26.

[57] Khanji, S., Iqbal, F., Hung, P. C. K. “ZigBee Security Vulnerabilities: Exploration and Evaluating”, The 10th International Conference on Information and Communication Systems 2019, Jul. 2019, p. 6.

[58] Rajawat, A. S., Mohammed, O., Shaw, R. N., Ghosh, A. “Applications of AI and IoT in Renewable Energy,” Chapter 6 – Renewable energy system for industrial internet of things model using fusion-AI, 2022, pp. 107–128.

[59] StatisticsHowTo. “Root Mean Square Error (RMSE) Calculation.” Statisticshowto.com. https://www.statisticshowto.com/probability-and-statistics/regression-analysis/rmse-root-mean-square-error/

[60] Rapid7. “What is Security Orchestration, Automation, and Response (SOAR)?” Rapid7.com. https://www.rapid7.com/fundamentals/what-is-soar/

[61] Varga, P., Plosz, S., Soos, G., Hegedus, C. “Security threats and issues in automation IoT”, 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Jul. 2017.

[62] Al-Ofeishat, H. A., Alshorman, R. “Build a Secure Network Using Segmentation and Micro-segmentation Techniques”, International Journal of Computing and Digital Systems, Jul. 2024, pp.1499–1508.

[63] UC Berkeley. Quality of Service in Wireless Networks. UC Berkeley Lecture Notes. https://people.eecs.berkeley.edu/~istoica/classes/cs268/06/notes/13-QoSx2.pdf

[64] Scikit-learn. Polynomial Regression for Signal Analysis // Scikit-learn Documentation.

[65] Fletcher, S. J. “Data Assimilation for the Geosciences”, Chapter 10 – Introduction to Semi-Lagrangian Advection Methods, 2017, pp. 361–441.

[66] Hodges, L. “Methods in Experimental Physics”, Vol. 28, Common Univariate Distributions, 1994, pp. 35–61.

[67] Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2011.

[68] Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2010.

Daniils Aleksandrovs-Moisejs was born in Riga in 1997. He obtained his Academic Bachelor's degree in Electrical Science (2019) and an Academic Master's degree in Telecommunications (2021) from Riga Technical University. Since 2020, he has been an IT specialist at the Hospital of Traumatology and Orthopaedics. He is a researcher and lecturer at the Institute of Photonics, Electronics and Telecommunications of the RTU Faculty of Computer Science, Information Technology and Energy. His research areas include network reliability, wireless communication networks, and wired/wireless sensor networks.