KAZIMIERAS BAGDONAS

MULTIMODAL SECURITY SYSTEM FOR INTERNET OF THINGS COMMUNICATIONS

DOCTORAL DISSERTATION

Kaunas
2022

KAUNAS UNIVERSITY OF TECHNOLOGY

KAZIMIERAS BAGDONAS

MULTIMODAL SECURITY SYSTEM FOR INTERNET OF THINGS COMMUNICATIONS

Doctoral dissertation
Technological Sciences, Informatics Engineering (T 007)

2022, Kaunas

This doctoral dissertation was prepared during the period 2016–2021 at Kaunas University of Technology, Faculty of Informatics, Department Of Computer Sciences. The studies were supported by the Research Council of Lithuania. The doctoral right has been granted to Kaunas University of Technology together with Vilnius Gediminas Technical University.

Scientific supervisor:

Prof. dr. Algimantas VENČKAUSKAS (Kaunas University of Technology, Technology Sciences, Informatics Engineering, T 007)

Doctoral dissertation has been published in:
http://ktu.edu

Editor:

Dr. Armandas Rumšas (Publishing House *Technologija*)

KAUNO TECHNOLOGIJOS UNIVERSITETAS

KAZIMIERAS BAGDONAS

DAUGIAMODALI SAUGUMO SISTEMA DAIKTŲ INTERNETO KOMUNIKACIJAI

Daktaro disertacija
Technologijos mokslai, informatikos inžinerija (T 007)

2022, Kaunas

Disertacija rengta 2016–2021 metais Kauno technologijos universiteto Informatikos fakultete, Kompiuterių katedroje. Doktoranturos teisė Kauno technologijos universitetui suteikta kartu su Vilniaus Gedimino technikos universitetu. Mokslinius tyrimus rėmė Lietuvos mokslo taryba.

Mokslinis vadovas:
Prof. dr. Algimantas VENČKAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija, T 007)

Interneto svetainės, kurioje skelbiama disertacija, adresas:
http://ktu.edu

Redagavo:

Dr. Armandas Rumšas (Leidykla „Technologija")

Abstract

The emergence of Internet of Things (IoT) networks is promising to allow billions of devices to be connected in wireless *ad hoc* networks, thus providing various types of data to be generated, analyzed, and used, to create synergistic benefits that could not be obtained from isolated devices. The IoT architecture consists of low power and low computing devices and is further constrained by the limited bandwidth, thus cybersecurity solutions for IoT have to be designed and grounded with these limitations in mind. The fundamental cybersecurity tasks are object identification and authentication. More advanced cybersecurity possibilities and applications rely on these two being executed in the strongest possible way, which is often not applicable to IoT devices due to their limitations. An alternative to a single strong, but resource-intensive, the method is a multimodal solution that integrates two or more methods in conjunction to increase the overall security level.

In this thesis, we present a multimodal security system for IoT communication that shall integrate secure data streaming, a distributed software-based localization algorithm, and a power management control system for it, together with a novel multimodal localization data integration solution for object identification and authentication. Due to the limitations inherent in the IoT architecture, a set of methods have been developed to obtain the desired results. Round Trip Time (RTT) ranging measurements are used in a distributed localization algorithm for ad hoc networks that allows partial convergence of the network to generate localization solutions. A Hybrid Control System (HCS) is developed to manage power between communication, computation, and localization tasks, and it can function even with intermittent power sources, such as solar cells. A MAST-based multimodal identification and authentication method that can employ the geolocation solution of the End-Node, the geolocation information from the IoT Network Nodes (NN's) which provides measurements for the generation of said solution, and which combines it with asymmetric encryption. Finally, a lightweight secure streaming protocol for IoT is presented. The combination of these solutions creates a distributed software solution that could be deployed in IoT networks to obtain a multimodal security system for IoT objects.

Reziumė

Daiktų Interneto (DI) atsiradimas žada galimybę sujungti milijardus įrenginių į tinklus, teikiančius įvairiausius duomenis, kurių bendroje analizėje tikimasi išgauti sinergetinio efekto naudą, kuri nebūtų pasiekiama žvelgiant į izoliuotus įrenginius. DI susideda iš mažos galios ir mažų skaičiavimo pajėgumų įrenginių, su ribotu duomenų pralaidumu. DI kibernetinio saugumo sprendimai turi būti kūriami atsižvelgiant į šiuos apribojimus. Fundamentalūs kibernetinio saugumo uždaviniai yra objektų identifikavimas ir autentifikavimas. Pajėgios kompiuterinės sistemos geba šias užduotis realizuoti naudojant saugius, bet sudėtingus metodus, kurie ne visada yra prieinami DI įrenginiams. Alternatyva skaičiavimams intensyviems algoritmams yra kelių silpnesnių metodų panaudojimas multimodaliniame rėžime. Išmaniai panaudojus kelis nepriklausomus resursus, galima pasiekti analogišką saugumo laipsnį su paprastesniais algoritmais.

Šioje disertacijoje yra pristatomas multimodalinė DI objektų saugumo sistema skirta komunikacijai DI įrenginiams. Dėl DI architektūrinių apribojimų užduoties realizacijai prireikė keturių naujų sprendimų. Siūloma sistema integruoja naują, paskirstytą, programinį lokalizavimo algoritmą, jo energijos sąnaudų valdymui skirtą hibridinę kontrolės sistemą, naują saugų ir lengvą komunikavimo protokolą, bei naują multimodalinę saugumo schemą, naudojančią geolokacijos duomenis DI įrenginių identifikavimui ir autentifikavimui. Paskirstytas lokalizacijos algoritmas leidžia rasti lokalizacijos sprendimą dalinai konvergavusiuose tinkluose. Išvystyta hibridinės kontrolės sistema, skirta valdyti ir paskirstyti DI įrenginių energijos resursus tarp skaičiavimų, komunikavimo ir lokalizacijos užduočių taip, jog įrenginys galėtų veikti nesustodamas net ir su protarpiniais energijos šaltiniais, tokiais kaip Saulės baterijos. Merkelizuoto abstrakčios sintaksės medžio struktūra grįstas multimodalinis identifikavimo ir autentifikavimo algoritmas, integruojantis lokalizacijos informaciją ir asimetrinę kriptografiją suteikia galimybę apibrėžti teritoriją, kur buvimas jos rėžiuose, bei kaimyniniai DI mazgai yra naudojami kaip parametrai saugumo sprendime. Siūlomas metodas suteikia galimybę identifikuoti DI objektus panaudojant parašus sugeneruotus su privačiais raktais, ir integruoti geolokacijos modą pasinaudojant maišos algoritmais. Pabaigoje pristatomas lengvasvoris, saugus duomenų transliacijos protokolas. Šių metodų apjungimas sukuria paskirstytą programinį sprendimą, kuris yra skirtas DI objektų identifikavimo ir autentifikavimo užduočiai įvykdyti.

Acknowledgments

I wish to express gratitude to my supervisor Professor Dr. Algimantas Venčkauskas for their support, guidance, and assistance during my studies. I would like to thank my colleagues Prof. Dr. Egidijus Kazanavičius, Prof. Dr. Jevgenijus Toldinas, Prof. Dr. Agnius Liutkevičius, Dr. Stasys Maciulevičius, Dr. Gedeiminas Činčikas, and Dr. Rasa Brūzgienė for their valuable feedback.

I wish to thank Stasė and Pranas Kanapeckai for their consideration and the nudge. Finally, I want to express gratefulness to my family, especially Irma, for understanding, patience, and support.

Kazimieras Bagdonas
Kaunas, 2022

Contents

List of Figures

List of Tables

GLOSSARY

AoA	Angle of Arrival
APS	Absolute Positioning Solution
ASIC	Application Specific Integrated Circuit
AST	Abstract Syntax Trees
BPL	Battery Power Level
CA	Continuous Authentication
CPC	Constant Power Consumption
DTLS	Datagram TLS
EEH	Electromagnetic Energy Harvesting
EKF	Extended Kalman Filter
FL	Fuzzy Logic
FLC	Fuzzy Logic Controller
GNSS	Global Satellite Navigation Systems
GPS	Global Positioning System
HPCS	Hybrid Power Control System
HCS	Hybrid Control System
HMACs	Hash based message authentication codes
IN	Inertial Navigation
IoT	Internet of Things
IP	Input Power
Li-Fi	Low Energy, Light-Fidelity
LLS	Linearized Least Squares
LRF	Local Reference Frame
LSSP	Lightweight Secure Streaming Protocol
M2M	Machine-to-Machine
MAST	Merkelized Abstract Syntax Trees
MEO	Medium Earth Orbit
MLS	Multi-Level Steganography
MMIA	Multi-modal Identification and Authentication Method
MN	Mobile Node
NC	Network Convergence
NetEM	Network Emulation
NN	Network Node
PAL	Power Allocated for Localization
PID	Proportional Integral Derivative
PUF	Physical Unclonable Function
RES	Renewable Energy Sources
RFID	Radio-Frequency Identification
ROM	Read Only Memory
RSSI	Received Signal Strength Indication

RTP	Real-Time Transport Protocol
RTT	Round Trip Time
TCP	Transmission Control Protocol
TDoF	Time Difference of Flight
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
THE	Thermoelectric Energy Harvesting
TLS	Transport Layer Security
ToF	Time of Flight
TTSH	Two-Tier Signature-Hash
UDP	User Datagram Protocol
ULS	Ubiquitous Localization System
UN	User Node
VNN	Virtual Network Node

Introduction

1.1. PROBLEM FORMULATION

With the advent and proliferation of computers into industries and the personal lives of people, these devices have become significant in numerous ways. At the beginning of the digital revolution, computer systems were large in size and limited in numbers. The Internet itself was developed without security considerations for the data that it was transmitting. With the subsequent development of computer systems, the effect of Moore's law, and the proliferation of digital technology, computers became ubiquitous throughout the industry and society. Currently, a large part of human activities, ranging from personal to industrial, and even governmental functions, are being infused and enhanced with information technologies, and thus cybersecurity is being recognized as one of the preeminent concerns. The open nature of computer hardware, software, and networks is bringing forth new and substantial challenges for the verification and validation of communication and data. These challenges can be introduced into processes by either error, happenstance, or malicious intent. The ability to identify and authenticate objects is the first and crucial step to building reliability in any IT infrastructure. Be it a temperature sensor in a smart house, or a radiation detector in a nuclear reactor, data validity expectation is fundamental in vast numbers of applications.

Personal computers, laptops, smartphones, and tablets have become a part of personal and professional life for hundreds of millions of people. These devices are running complex operating systems that manage numerous applications simultaneously. Most identification and security functions are managed at the application and communication layers. With the emergence of Internet of Things (IoT) networks that are envisioned to be comprised of billions of devices connected in ad hoc networks, solutions for object identification, and authentication have become a complex endeavor. The nature of IoT devices limits the available power, computational resources, and the range of sensors that can be realistically employed. Furthermore, the disparate hardware architectures and configurations limit widespread solutions to software, instead of basing them on hardware augmentations.

A single mode identification and authentication method are susceptible to spoofing and thus pose a risk for security and data integrity. The ability to use a multimodal method for object identification and authentication can mitigate these risks. In the case

of IoT, where the number of devices is expected to be in orders of billions, manual verification would be practically impossible, thus dramatically reducing the reliability of the deployed systems. Further, more specific devices can be expected to perform their functions in specific geographical locations. Thus data verification can be compromised by the relocation of said devices outside the expected area of operations.

Currently, no security method has been developed which could provide a location-based multimodal object identification and authentication for IoT devices.

1.2. RELEVANCE OF THE WORK

Creating ad hoc IoT networks comprising millions or billions of devices that can provide data integrity and verification is a challenging task. Not only data can be subjected to spoofing, but network nodes can be relocated by external forces, rendering their measurements obsolete at best, and resulting in a malicious effect at worst. Creating a system that could generate a geolocation solution has always been a significant task. Global Navigation Satellite Systems can provide such functionality, but their integration may be unfeasible due to the unit cost, energy, or computational power limitations on IoT nodes. A widespread geolocation service via communication channels using off-the-shelf equipment has not yet been achieved. Not only because of the limitations imposed by IoT hardware, but also by the lack of universal localization solutions. The possibility to integrate identification and authentication methods with the location information would substantially enhance the reliability and security of the data on IoT networks.

1.3. OBJECT OF THE THESIS

The object of this research is a cybersecurity solution for the devices on ad hoc IoT networks.

1.4. AIM OF THE THESIS

The main aim of this work is to propose a software-based multimodal security system for Internet of Things communications that integrates localization, and streams data in a secure, low power, and low bandwidth solution.

1.5. TASKS OF THE THESIS

The main tasks of this thesis are:

1. Investigate the currently available localization methods for wireless communication, propose and evaluate a distributed ad hoc localization method for IoT network;

2. Investigate the presently available control methods and evaluate their suitability for IoT applications and propose and evaluate a control system for IoT device

power management in relation to the localization with wireless communication;

3. Investigate cryptographic methods and propose a lightweight multimodal solution for IoT object identification and authentication which would integrate the localization information;
4. Investigate IoT communication methods and propose a secure data protocol for data streaming from an IoT network node;
5. Implement and evaluate the proposed methods via computer simulations and/or experiments.

1.6. RESEARCH METHODOLOGY

The following research methodology has been employed to achieve the thesis objectives.

1. Comparative analysis of scientific literature has been used for the evaluation of localization methods, control systems, cryptographic methods, and communication protocols;
2. Quantitative Research has been used to develop and evaluate the proposed localization, control, identification and authentication, and secure communication methods;
3. Analytical Research has been used to evaluate localization, control, identification and authentication, and secure communication methods;
4. Applied Research has been used to evaluate and validate the proposed localization, control, identification and authentication, and secure communication methods.

1.7. SCIENTIFIC NOVELTY

The scientific novelty of this thesis can be summarized as:

1. A novel distributed software-based localization method has been proposed for IoT networks that can propagate localization solutions over the IoT *ad hoc* networks.
2. An adaptive hybrid control system for power management of wireless localization techniques for IoT network nodes has been developed that can ensure persistent localization functionality even for devices with intermittent power sources.
3. A secure and lightweight communication protocol for data streaming has been proposed for IoT applications, comparable to UDP in energy/bandwidth requirements, that provides identification, authentication, and data integrity/security features.

4. A novel MAST-based multimodal identification and authentication method for IoT devices has been proposed that integrates localization-based identification and authentication in a predefined geographical zone with additional parameters and computationally trivial verification.

1.8. PRACTICAL VALUE

The proposed multimodal security system for IoT communications evidence that:

1. The proposed distributed, software-based localization method can be deployed on any IoT devices that can obtain sufficient ranging measurement accuracy over the wireless communication channel.
2. The proposed adaptive power management system can be deployed to IoT devices that have persistent or intermittent power sources.
3. The proposed secure and lightweight communication protocol for data streaming can be employed in IoT devices with trivial firmware upgrades. It is applicable to use cases with bandwidth and power limitations, where the loss of data packets is not critical.
4. The proposed MAST-based identification and authentication method can be employed in multimodal security systems to achieve high compression and computationally trivial verification.

1.9. THESIS STATEMENTS

1. The proposed multimodal security system for IoT communications can significantly enhance the security and reliability of IoT over the existing designs.
2. The proposed distributed, software-based localization method is a feasible prospect for a ubiquitous IoT localization solution.
3. The proposed Hybrid control system for the IoT localization can ensure persistent localization functionality even with intermittent power sources and can prioritize measurements based on their quality and available power.
4. The proposed application of the Merkelized Abstract Syntax Tree to the identification and authentication of IoT devices significantly enhances security and reliability with a computationally trivial validation.
5. The proposed Lightweight Secure Streaming Protocol in M1 mode provides identification and authentication functionality to the IoT devices with comparable bandwidth and energy consumption to the UDP. LSSP provides additional functionality and security modes with moderate overheads in comparison to the state-of-the-art analogs.

1.10. SCIENTIFIC APPROVAL

All of the results presented in the thesis are original and correspond to two internationally referred "ISI Web of Science" scientific journal publications.

The experimental results were presented and discussed in three international conferences:

1. Bagdonas, Kazimieras; Jusas, Nerijus; Venčkauskas, Algimantas. *A converging distributed positioning algorithm for Internet-of-things*, Elektronika ir elektrotechnika. Kaunas : KTU. ISSN 1392-1215. eISSN 2029-5731. 2017, Vol. 23, iss. 6, p. 72-76. [Science Citation Index Expanded (Web of Science); Scopus; Computers & Applied Sciences Complete] Q3 (2017, Scopus Sources)]

2. Venčkauskas, Algimantas; Morkevičius, Nerijus; Bagdonas, Kazimieras; Damaševičius, Robertas; Maskeliūnas, Rytis. *A lightweight protocol for secure video streaming*, Sensors. Basel : MDPI AG. ISSN 1424- 8220. eISSN 1424-8220. 2018, vol. 18, iss. 5, art. no. 1554, p. 1-14. [Science Citation Index Expanded (Web of Science); Scopus; DOAJ] Q1 (2018, Scopus Sources)]

3. Bagdonas, Kazimieras; Venčkauskas, Algimantas. *Localization algorithm for identification of mobile objects in an Ad-Hoc Internet of Things network* 11th international workshop on data analysis methods for software systems, Druskininkai, Lithuania, November 28-30, 2019 / Lithuanian Computer Society, Vilnius University Institute of Data Science and Digital Technologies, Lithuanian Academy of Sciences. Vilnius : Vilnius University, 2019. ISBN 9786090703243. eISBN 9786090703250. p. 8.

4. Bagdonas, Kazimieras.; Venčkauskas, Algimantas. *Identification of dynamic parameters and velocity control of a moving IoT node using a single ranging measurement source* 10th international workshop on data analysis methods for software systems, Druskininkai, Lithuania, November 29 - December 1, 2018. Vilnius : Vilnius University, 2018. ISBN 9786090700433. p. 9.

5. Bagdonas, Kazimieras; Venčkauskas, Algimantas. *IoT mobile network Node's velocity estimation via curve fitting* 9th International workshop on data analysis methods for software systems, DAMSS : Druskininkai, Lithuania, November 30 - December 2, 2017 / Lithuanian Computer Society, Vilnius University, Institute of Data Science and Digital Technologies, Lithuanian Academy of Sciences. Vilnius : Vilnius University, 2017. ISBN 9789986680642. p. 6. DOI: 10.15388/DAMSS.2017.

1.11. THESIS ORGANIZATION

The thesis consists of 5 chapters:

Chapter 1 is an introduction providing a summary of the work's novelty, aims, and objectives. This includes a brief identification of the main problems in the IoT area and the motivation for the work. Chapter 2 is a review of the literature on the state-of-the-art of relevant topics associated with the thesis research object. Chapter 3 provides a theoretical background for the developed methods. Chapter 4 presents the developed methods. Chapter 5 delivers the Results obtained from the validation and evaluation of the proposed methods and discusses the proposed methods and obtained experimental results. Chapter 6 concludes the thesis where the proposed solutions and contributions are summarized.

Review of the Literature

This chapter provides the background and the state-of-the-art developments related to the thesis tasks. Section 2.1 presents the topics related to the IoT. It provides a general overview of the Internet of Things (IoT) philosophy and architecture, devices, and protocols. Section 2.2 presents the topics related to localization. This section focuses on Radio Frequency based localization methods and algorithms with the focus on IoT applications. Section 2.3 presents the topics related to the Control methods with the focus on Hybrid Control Systems (HCS). Section 2.4 comments on the topics related to the methods combining multiple modalities for cybersecurity purposes. Section 2.5 presents the topics related to the secure communication. Section 2.7 presents conclusions for the Chapter.

2.1. BACKGROUND ON THE INTERNET OF THINGS

Internet of Things

Internet of Things is an emerging infrastructure of sensors and computational devices which is expected to generate novel capabilities and opportunities for industrial, scientific, governmental and personal applications, (Ashton et al., 2009).

IoT encompasses categories of objects that are able to communicate through wireless channels and perform information processing. Typically, the IoT device is considered to be a representative of low power and computing capability class device. There are a number of IoT definitions, but, for the purpoceses of this thesis, a definition provided by (Whitmore et al., 2015) shall be used: "*A paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to achieve some objective.*" However, recent machine learning applications in self-driving automotive applications have seen a significant increase in IoT device computing capabilities (Sharma et al., 2022).

IoT is usually envisioned as a digital distributed network between billions of interconnected devices, (Dar et al., 2011). The vast number of Network Nodes (NN) is expected to generate a synergistic effect and enable the acquisition and processing of the actionable data. One of such possible synergistic effects is the possibility to achieve ubiquitous positioning solution (Zhang et al., 2016). With the increasing proliferation of interconnected devices, IoT itself is expected to evolve and gain functionality based

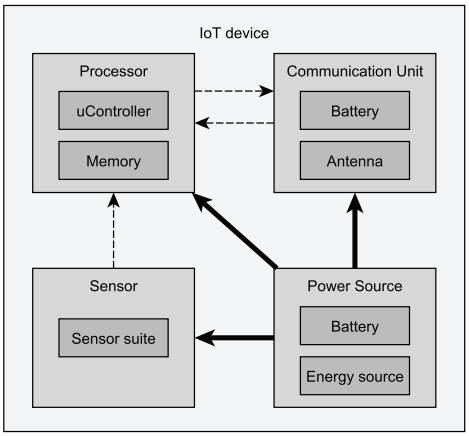

Figure 2.1.1: Typical structure of an IoT device

on the increasing computation capabilities and power efficiency through Moore's law.

Internet of Things Devices

A typical IoT device, as shown in Figure 2.1.1, consists of four main parts: a μController, sensors, a battery and a communication module. The μController contains software in a Read-only-memory (ROM) module and is capable of performing somewhat complex computations. Complexity of computations is more bounded by the available energy to the IoT device, rather than by the limitations of the μController as IoT devices are expected to operate for extended periods of time. Sensors in IoT devices are limited by the available energy, the processing power of the μController and the data throughput of the communication unit. Communication in the IoT network is usually assumed to be of the wireless variety, and thus must by facilitated by a wireless communication module. The final part of the IoT device is a battery. While the battery technology has been advancing, it is doing so at a significantly lower pace in comparison to the computing capabilities provided by Moore's law. Due to this fact, energy harvesting, either from ambient or renewable sources, is often considered in order to extend the operational capabilities of IoT devices.

A different class of even more simplified IoT devices without the μController has been in consideration and is referred to as chipless IoT devices (Preradovic et al., 2009). Currently, chipless IoT devices, are mostly implemented as passive RFID tags that can harvest energy from the incoming signals and generate a response. Such IoT devices have been used in localization applications, yet they lack the required functionality and flexibility for ubiquitous localization.

Additionally, intermediate architecture in the network is being presented to improve the IoT capabilities by moving substantially more powerful devices and distributing them among the IoT nodes. Such architecture is referred to as Fog comput-

ing. The Fog-Nodes not only have significantly more conditional power that is used to process the information collected from the local IoT devices, but we have substantially more energy and thus can increase the productivity in between the local IoT nodes.

Wireless Communication Between Internet of Things Devices

Communication between IoT devices is constrained by a number of limitations. The most significant is power, (Al-Sarawi et al., 2017). Every packet that is transmitted or received and processed by the IoT device consumes power, (Carvalho Silva et al., 2017). If an IoT device does not have capability to replenish its power reserves, its operational capacity in time is limited. A number of low power communication protocols are employed in IoT networks, with varying capabilities. Trade-offs between the data rate and the communication range are a typical consideration. Further communication protocols with less data overhead are used in order to preserve energy. This approach introduces a trade-off between the data reliability and the power consumption. Communication protocols employed by IoT devices are: Bluetooth, Bluetooth Low Energy, Light-Fidelity (Li-Fi), Near-field communication, Wi-Fi, ZigBee, Z-Wave, LTE, 5G, LPWAN, etc. As IoT as a technology is only at the beginning stage of its deployment, radical improvements in the hardware and software are expected. With an increased number of devices being deployed in the world, a synergistic effect can be obtained with the sheer number and proximity of IoT devices. IoT optimized transmission algorithms will emerge to take advantage of exponentially increasing permutations for the data transmission within the IoT. The ability to balance the amount of data that is being retransmitted through the node while taking into consideration the available power and the location of the node will increase the efficiency of the network.

Authentication and Identification in Internet of Things

Identification is the ability to distinguish a unique device. Authentication is the ability to verify the identity of the device. These two capabilities are fundamental in the cybersecurity domain and are used in conjunction, (Grassi et al., 2020).

Internet of Things devices are increasing at an exponential rate, entering a variety of previously untapped fields and becoming part of human life, (Husamuddin et al., 2017), (Chen et al., 2017). Such interconnection with individual people and high integration with other economical endeavors makes Internet of Things devices the newest and most vulnerable part of digital ecology. Security issues related to Internet of Things devices can be distinguished into two major categories: Security services and Security vulnerabilities in IoT architecture.

Security of the services describes human and IoT interaction where security is aimed at a specific target, (Abomhara et al., 2015). Security services is a major and potentially life-threatening threat due to the fact that increasingly more and more complex and capable devices are becoming part of IoT, e.g., self-driving vehicles, home automation, home security, home monitoring, etc. The main IoT security concerns can be categorized as: authentication, authorization, integrity, confidentiality, non-repudiation, availability, and privacy, (El-Hajj et al., 2019). These concerns cover

personal and private data, the access and control of personal and private spaces, data integrity and process control, (Hernandez et al., 2014).

Security challenges in IoT layers must be able to manage the typical cybersecurity threats with significantly lower resources and capabilities, (Mahmoud et al., 2015). Perceptually dangerous threats, such as node capture, denial of service, denial of sleep, distributed denial of service, reply attack, mass node authentication, routing threads must be handled by IoT systems, (Airehrour et al., 2016), (Mukherjee, 2015). Network layer security must be able to handle routing attacks, Man-in-the-Middle, eavesdropping and denial of service. The application layer security must ensure data accessibility and authentication, data privacy and identity, and the ability to deal with Big data.

The most common approaches towards the authentication of IoT devices include solutions that use hash, cryptographic algorithms, physical or biometric data, such as fingerprints, retinal scans, etc., or behavioral information, such as gait analysis, keystroke dynamics, etc., (El-Hajj et al., 2019). Token-based authentication that is based on data or credentials can also be employed, (Chae et al., 2015), (Blazquez et al., 2015). Different types of authentication procedures can be integrated in order to authenticate IoT network participants. Procedures can include one-way, two-way, or three-way authentication strategies. The authentication architecture can be centralized or distributed, hierarchical or flat. The IoT layer, where authentication procedures are applied, can be distinguished into perception, network, and application layers, (Kothmayr et al., 2013). Finally, hardware-based solutions for IoT authentication can be implicit or explicit. In the case of implicit physical characteristics, all the hardware is employed to generate an authentication solution. In the explicit case, Trusted Platform Modules or specialized hardware chips can be used to store or generate keys for authentication.

IoT is comprised of devices of varying complexity, starting with chip-less passive nodes, (Tuyls et al., 2006), self driving vehicles, (Tangade et al., 2016), which are of significant monitoring value and significant potential for harm resulting from malicious activities; in the model, entire systems interconnect multiple IoT devices into a single complex system. An even larger scale can be reached with wireless sensor networks and mobile network applications that can span over vast areas and are susceptible to malevolent mass data gathering, such as precision tracking of individuals over large areas, (Chan et al., 2014).

2.2. LOCALIZATION TECHNIQUES

Localization is an act of defining an object's location in relation to a specific reference frame, (Kramer et al., 1993). The reference frame can be relative, local, global, on the scale of a star system, or even a galaxy or the universe. Currently, accurate positioning solutions can be obtained via satellite base positioning systems, such as GPS, Galileo, Glonass and BeiDou, (Jin, 2012). A supplementary and less accurate solution can be obtained from mobile communication networks, (Otsason et

al., 2005), however, there is no reliable and widely available positioning solution for indoor environments, (Greßmann et al., 2010). These indoor environments include warehouses, urban canyons, and even subterranean spaces and tunnel systems, such as metros.

In relation to IoT devices, we are usually concerned with relative, local and global reference frames. Historically, localization was performed with triangulation techniques, but, with the advance of artificial satellites, trilateration technique has been dominating in the last half of century. While triangulation, or localization with Angle of Arrival (AoA) requires the distance and angular information, trilateration can be performed with only distances. In practice distances are estimated from the Time of Flight (ToF) of the signal between two points. AoA techniques require more complex antennas for localization in RF, while ToF requires either high precision clocks or accurate time synchronization, (Kramer et al., 1993). All of these requirements introduce additional cost onto IoT devices in the form of complexity and specific hardware, however, benefits from localization are great and thus are being actively pursued by academy and industry.

Received Signal Strength Indication

Received signal strength indication (RSSI) was one of the earliest techniques to be used in low cost localization over communication networks, (Sugano et al., 2006). RSSI is a significantly non-linear measurement, and is highly affected by interference/obstruction, however, basic presence measurements can be employed, and, if a significant amount of independent measurements can be performed, localization can be achieved to a satisfactory level.

Radio-Frequency Identification Tag Based Localization

Radio-frequency identification (RFID) is a device consisting of a radio transponder (and an optional digital logic) that is used for object identification, (Bouet et al., 2008). RFID tags are designed for low cost and disposability. In the localization context, RFID tags can be employed as reference points for a device to localize itself if the locations of those points that are known. Due to the simplistic nature of RFID tags, localization with them is usually performed in the proximity mode, and its functionality is constrained by the RFID technology.

Timing Based Localization

Timing based localization is realized by measuring the Time of Flight (ToF) of the RF signal, (Groves, 2015). It can be based on signal pulses, carrier wave phase observation, data packets, etc. In order to accurately measure the ToF, the networked devices must by synchronized. If such synchronization is not possible, either Time Difference of Flight (TDoF) or Round Trip Time (RTT) can be measured. In the context of IoT timing based localization, RTT measurements look to be the most promising, with the trade-off of higher overall power consumption, as each measurement requires a request and a response to be transmitted over the network in order to obtain a single

measurement. RTT measurements also require a sufficiently accurate clock to be used in an IoT device. As RF signals propagate through the medium at the speed similar to the speed of light in vacuum (c = 299792458m/s), 1m ranging accuracy corresponds to the timing measurement resolution of 3.3ns. Such timing resolution requires clock speeds grater than 300MHz. While in current IoT devices such clock speeds are not usually employed, the Moore's law and the advances in the Application Specific Integrated Circuit (ASIC) design and manufacturing allow us to extrapolate such standards for the future. Additionally, employment of advance algorithms for data gathering and processing allows us to reduce these requirements further, thus bringing the possibility of ToF localization for IoT devices as a possibility.

It is noteworthy that ToF measurements can be derived from standard communication packets propagating through the IoT network, without the need for overhead communication. While deliberate measurements can produce consistent results, measurements of opportunity can be sufficient in a densely populated IoT network.

Localization solution accuracy is also a function of the available network nodes to communicate with and the geometry of their positions in relation to the node. In the case of favorable geometry, the number of the required independent measurements decreases and vice versa.

Indoor Localization

Throughout the ages, localization and navigation have been very useful and important endeavors. Only with advancements in the timekeeping technology, sufficiently accurate longitudinal navigation was achieved and enabled global trade networks. In the modern times, positioning and navigation challenges are being solved by Global Navigation Satellite Systems (GNSS). Systems like Global Positioning System (GPS), GLONASS, Galileo, BeiDou can provide a global positioning solution as long as receivers are able to acquire signals from satellites orbiting in Medium Earth Orbit (MEO). Due to the on-board power constrains and the long distance between satellites and receivers, the signal strength is insufficient to perform positioning in indoor environments. In order to overcome this limitation, a local hardware is deployed, or signals of opportunity are employed to augment the GNSS solution. Such arrangements are prohibitively expensive and complex for ubiquitous deployment. A certain success can be achieved by employing communication networks such as GSM in order to aid the GNSS solution. However, if GNSS signals are not available at all, the desirable accuracy and precision is difficult to achieve. This problem is exaggerated if even GSM signals are not available, e.g., in underground tunnel systems. There is a vision where IoT devices, numbering in millions or billions, interconnected via wireless communication, could fulfill such a task, however, a number of challenges and issues remain unresolved.

The initial research into indoor localization with Radio Frequency (RF) communication equipment, such as Wi-Fi access points, has proposed to utilize the Received Signal Strength Indicator (RSSI). While RSSI is able to provide proximity de-

tection, indoor localization and navigation is challenging due to the high variance in the measured signal. Additionally, the Time of Arrival (ToA), Time Difference of arrival (TDoA), Angle of Arrival (AoA) methods have been employed, (Liu et al., 2007). The initial approaches relied on the prior knowledge of the geolocational distribution of networks as well as on extensive profiling of network parameters, such as RSSI fingerprint mapping. While such approaches can be employed in a limited area, they are hard to scale up in order to achieve the ubiquitous localization solution. As IoT devices employ various communication standards, such as Wi-Fi ZigBee, Bluetooth, etc., with different power levels and different maximum communication ranges, the creation of true ad hoc localization solutions in the IoT network is made more difficult when relying on signal strength measurements. The most universal ranging method in such a case is based on timing. Timing-based measurements can be used in a number of different ways, depending on all hardware capabilities and the power availability, (Obeidat et al., 2021). Timing measurements accuracy depends on hardware clocks that can be constructed by using quartz crystals or even atomic clocks. There is exponential relationship between the accuracy of the clock and its cost. In the case of IoT, there are severe restrictions both on the measurement accuracy performed by the hardware, and the available energy to perform these measurements is severely restricted. Due to these limitations, IoT indoor localization remains a challenging endeavor. Additional impacts on the quality of positioning solution are the geometric distribution of the network nodes in space, (Yang et al., 2009), the signal noise level and the limited computational power to process these measurements with advanced methods.

Radio Frequency based Indoor Localization

In general, the localization positioning solutions in ad hoc networks and subsequently in IoT can be distinguished by the level of accuracy and decentralization they are capable of achieving. A sufficiently accurate and fully distributed and decentralized IoT localization solution would provide an enabling impetus form a number of Machine-to-Machine (M2M) applications, (Verma et al., 2016). Additionally, the accuracy is influenced by both the employed measurement technique and algorithms, (Savvides et al., 2001) used to compute a positioning solution. The most prevalent measurement techniques are:

- Time of Arrival (ToA): requires synchronization of all clocks among the network nodes in order to perform accurate ranging measurements.

- Round Trip Time (RTT): requires high timing resolution and standardized packet processing time. Due to the current IoT hardware and software setups, it is unable to provide predictable delay estimation for packet processing time.

- Angle of Arrival (AoA): requires a specific antenna and the front-end design in order to differentiate the direction of the incoming RF signals.

- Received Signal Strength Indicator (RSSI): highly susceptible to noise and environmental factors.

When evaluating the pros and cons of different types of ranging measurements, range estimation derived from the RTT timing information is the most universal, requires no additional hardware to be added to the IoT devices, however, it requires hardware to be adapted to perform more precise timing measurements. Such a development is feasible and likely once IoT devices have become disseminated in vast numbers in all environments. The utility of ubiquitous localization is sufficient motivation for them to be included in the designs. Once the solution space converges on the RTT as a standard way to perform ranging measurements, the integration of different devices in a vast ad hoc network will become feasible. IoT hardware with alternative measurement methods is also being developed, (Bagdonas et al., 2009) that can overcome the low timing resolution of the RTT measurements.

The most basic positioning algorithm based on range estimation is trilateration, (Murphy et al., 1995). In order to obtain a trilateration solution in 3D space, full ranging measurements are used. The most basic trilateration algorithm cannot employ additional measurements to enhance its solution. A more mathematically and computationally advanced approach is to use the Linearized Least Squares (LLS) algorithm. The computational complexity of LSS grows exponentially with the number of the included measurements. The performance of different positioning algorithms has been extensively studied, (Shang et al., 2004), (Macagnano et al., 2014), and the growing consensus is focused on the distributed implementations, (Rabaey et al., 2002). The distributed nature of these algorithms is more suited for the expected scale in the spirit of the IoT networks, (Gubbi et al., 2013). Distributed algorithms have been analyzed extensively in relation to their complexity and positioning errors, (Wymeersch et al., 2009), (Mao et al., 2007), (Niculescu et al., 2004), (Etiabi et al., 2020), (Kumar et al., 2020).

The arrival of new generations of low power wireless communication technologies promises to expand the capabilities of IoT devices. The positioning techniques for IoT devices with an overview of error sources and error mitigation techniques are presented by (Li et al., 2020) and (Khan et al., 2021). A comprehensive overview of the state-of-the-art localization technologies for IoT is presented by (Asaad et al., 2022), where the authors make prediction that the incorporation of location information into the IoT communication network will increase with the IoT adoption and proliferation.

2.3. POWER MANAGEMENT IN INTERNET OF THINGS DEVICES

Communication between IoT devices is constrained by a number of limitations. The most significant is power, (Al-Sarawi et al., 2017). Every packet that is transmitted or received and processed by the IoT device consumes power, (Carvalho Silva et al., 2017). If an IoT device does not have capability to replenish its power reserves, its operational capacity in time is limited. A number of low power communication protocols

are employed in IoT networks with varying capabilities. Trade-offs between the data rate and the communication range are a typical consideration. Further communication protocols with less data overhead are used in order to preserve energy. This approach introduces a trade-off between data reliability and power consumption. The communication protocols employed by IoT devices are: Bluetooth, Bluetooth Low Energy, Light-Fidelity (Li-Fi), Near-field communication, Wi-Fi, ZigBee, Z-Wave, LTE, 5G, LPWAN, etc. Since IoT as a technology is only at the initial stage of its deployment, radical improvements in the hardware and software are expected. With an increased number of devices being deployed in the world, a synergistic effect can be obtained with the sheer number and proximity of IoT devices. IoT optimized transmission algorithms will emerge to take advantage of the exponentially increasing permutations for the data transmission bath within the IoT. The ability to balance the amount of data that is being retransmitted through the node taking into consideration the available power and location will increase the efficiency of the network.

Digital Control Systems

A control system is a hardware or software implementation of an algorithm that manages the device to operate in a desired performance envelope, (Branicky et al., 1998), (Goodwin et al., 2001). In the case of IoT, power consumption, due to its limited suply in IoT devices, is a critical parameter that must be taken into careful consideration, (Barot et al., 2020). The most significant power consumption in IoT devices is typically wireless communication. Energy consumption optimization will become more relevant as the IoT networks are expected to expand at an exponential rate, (Sundhari et al., 2020). Dependent on the data rate, it can be orders of magnitude higher in comparison to data processing or data acquisition. The power management issue is also affected by the communication channel, and, with the introduction of 6G technologies, IoT networks will have to manage this issue, (Khan et al., 2020). For the localization task, power consumption is a function of requirements - the localization solution frequency, the power required to obtain a single localization solution and localization accuracy, which are directly influenced by the number of network nodes that a device must communicate. While the traditional control systems were designed to react to a step impulse on the input, such a complex task requires a more advanced approach. One of the possible realizations of a power control system for an IoT localization node is the Hybrid Control System (HCS) with distinct parts for distinct parameters.

Kalman Filters

Kalman filter is a discreet optimal mathematical estimator for linear systems that is extensively used either to indirectly estimate measurements, filter Gaussian noise, or estimate the state of the system. Kalman filters have become ubiquitous in the positioning and localization tasks, as they do not require the storage of historical measurement data to perform estimation and are relatively economical in the computing sense, (Welch et al., 1995). In the context of IoT localization, the Kalman filter is well

suited for the localization solution estimation, especially if an insufficient number of measurements is obtained at any given point in time. Recently, Kalman filters have been proposed for numerous applications, starting from the measurement accuracy improvement, (Zhuang et al., 2019), low-power centimeter-level indoor IoT localization, (Zhuang et al., 2019), energy harvesting in IoT networks, (Yao et al., 2020a), to the control of energy efficient communication schemes for IoT, (Huang et al., 2019).

Kalman filter is based on linear algebra and requires several complex mathematical operations to be performed in order to obtain their state estimate. The higher the number of states are present in the state vector, the more computationally demanding do these operations, like matrix inversions, become. While the modern Kalman filters may consist of hundreds or sometimes thousands of states that are estimated at the sampling rate, in order to be in line with the capabilities of IoT, the number of states in the Kalman filter should be minimized. The access to the hardware implemented accelerators in the form of ASIC or a programmable micro FPGA could be possible if the provided performance and economic economical benefits outweighed the cost of development and manufacturing to be included in the IoT μControllers of IoT devices, (Zhang et al., 2019).

Fuzzy Logic

In the control theory, Fuzzy Logic (FL) refers to the type of controller that uses rules defined in fuzzy logic, (Klir et al., 1995). Usually, rules are expressed in IF-THEN rules, referring to the input and output, and then, in the deffuzification step, a continuous function is computed. This function is then used to determine the value of the output. In the context of IoT localization, the IoT localization Fuzzy logic controller is well suited to select the measurement sampling frequency and the number of the observed nodes in relation to the accuracy and power consumption. Recently, Fuzzy Logic controllers have been applied to the security architecture for IoT, (Zahra et al., 2020), the detection of DoS attacks, (Haripriya et al., 2019), a countermeasure approach to risk management in the IoT, (Kotenko et al., 2015), and generalized Fuzzy Logic based frameworks for IoT systems, (Zoican et al., 2021). Similarly to the Kalman filter, the ability to accelerate the computation of fuzzy logic functions with a programmable or a dedicated accelerator is a potential route to provide enhanced performance and capabilities to IoT devices.

2.4. MULTIMODAL SECURITY SOLUTIONS

As the edge computing-based designs for IoT security, (Sha et al., 2020) presents the contemporary efforts at software based approaches and concludes that, while tremendous research interests have been sparked, it still remains a significant challenge. Some solutions like (Nabusoba et al., 2020) use GSM messaging for authentication and authorization. The majority of multimodal security systems like (A Hassen et al., 2020), (Olazabal et al., 2019) and (Majeed et al., 2022) use biometric data and attempt to employ the blockchain technology, yet no scalable security solution for IoT

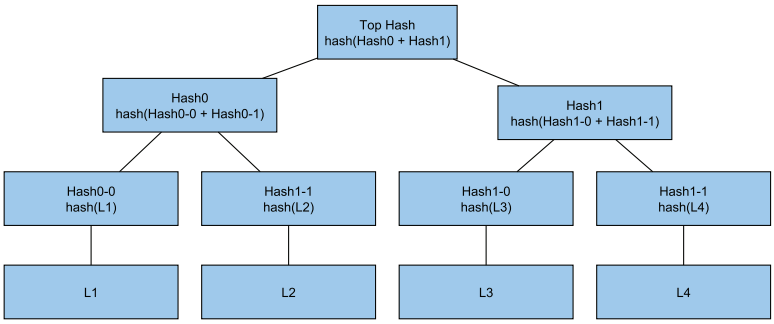

Figure 2.4.1: Merkel Tree Structure

communication has been proposed.

MAST

A of edge computing-based designs for IoT security, (Sha et al., 2020) presents contemporary efforts at software based approaches and concludes that, while tremendous research interests have been sparked, it still remains a significant challenge. Some solutions like (Nabusoba et al., 2020) use GSM messaging for the authentication and authorization. The majority of multimodal security systems, like (A Hassen et al., 2020), (Olazabal et al., 2019) and (Majeed et al., 2022) use biometric data and make attempts to employ the blockchain technology, yet no scalable security solution for IoT communication has been proposed.

Cryptografic signatures

Cryptografic signatures are a well established technology that is widely used in digital communication. They provide high confidence for identification and authentication. The most widely used digital signature algorithms are Rivest–Shamir–Adleman, (RSA) (Rivest et al., 1978), Digital Signature Algorithm (DSA), (Kerry et al., 2013), Elliptic Curve Digital Signature Algorithm (ECDSA), (Johnson et al., 2001). Digital signatures can have a varying level of security dependent on the algorithm, the amount of data that is being allocated for it, and the implementation of the algorithm, (Jansma et al., 2004). Different systems must balance these parameters in order to achieve the desired balance of performance and security.

Schnorr signature is an algorithm known for its simplicity which generates cryptographic signatures, (Schnorr, 1991), (Seurin, 2012). By using an agreed upon cryptographic hash function $H : 0, 1* \rightarrow \mathbb{Z}_q$ users are able to sign and verify information with private and public keys. The key generation is such that x is selected from the allowed list, and the public verification key is generated $y = g^x$. To sign a message M, a random k is selected from the allowed list, $r = g^k$, $e = H(r||M)$, where $||$ denotes concatenation and r is a bit string, $s = k - xe$. The pair (s, e) is the signature.

In order to verify the signature, let $r_v = g^s y^e$ and let $e_v = H(r_v||M)$. If $e_v == e$, then the signature is considered to be verified.

Currently, Schnorr Signatures are being investigated as an tool for confidential transactions in the Bitcoin network for implementation of smart contracts, (Yu, 2020) and (Chan et al., 2021). The application of Schnorr Signatures has also been introduced to the IoT context, (Ma, 2020) and (Agarwal et al., 2020), where IoT and private transactions on Blockchains can be enabled by them. Additionally, Schnorr Signatures are investigated as a tool to create secure and anonymous communication in IoT networks, (Hamouid et al., 2021).

2.5. INTERNET OF THINGS DATA STREAMING

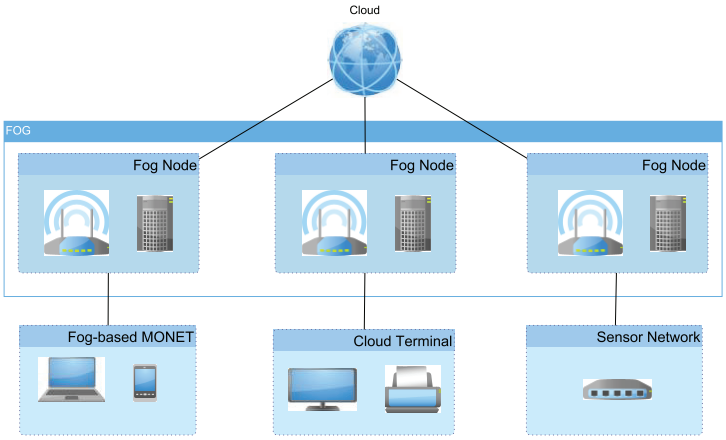

Figure 2.5.1: Architecture of Fog computing, consisting of three layers

In comparison to the traditional computer networks and architectures, Internet of Things (IoT) introduces additional challenges that arise out of constraints of its architecture, and the contemporary cloud and hosting models cannot address them adequately on their own, (Sicari et al., 2015; Venčkauskas et al., 2016). These challenges, ranked by the order of significance, include (i) rigorous requirements for latency, (ii) significant constraints on the available bandwidth for the network, (iii) computer power and resource constraints, (iv) consistent connectivity to the Internet and persistent services, (v) existing and normal cybersecurity challenges. As reported in (Miessler, 2014) by HP Fortify, 70% of the most frequently used IoT devices contain security vulnerabilities that have not been detected or removed after deduction. In order to deal with these challenges regarding the technology and cybersecurity, novel architecture for IoT is required. One such approach to mitigate vulnerabilities is for computing, (Bonomi et al., 2012). Fog computing seeks to distribute computing, storage, control, and network functionality in closer proximity to the end-user devices. Fog computing can be represented as a triple layer hierarchical architecture: Cloud-Fog-

End Devices 2.5.1

Depending on the application, both IoT and Fog computing can be categorized in these essential groups: smart cities, environmental sensing, management of smart homes and buildings, security and healthcare, and surveillance, (Stojmenovic et al., 2016). The challenges and possible solutions for full computing in these domains were thoroughly researched in papers by Stojmenovic, Roman, Tran et al., (Stojmenovic et al., 2016; Roman et al., 2018; Tran et al., 2016; Rahman et al., 2018). A non-extensive list of challenges for the *Fog-End Device* layer are: intrusion detection, privacy, network security, rogue Fog-Nodes, authentication, access control, security of data in storage, and security of sensitive or private data during the computation in the Fog-Node.

The contemporary solutions for cybersecurity that have been developed for Internet are designed to protect enterprise networks, consumer grade electronics, and data centers; they are mainly designed to provide a perimeter-based focus protection. Due to the nature of our computing architecture, this existing security approach is no longer viable in order to provide a comparable security level.

If these existing security practices are to be applied to full computing architecture, they could be adequately employed at the *Fog-Cloud* layer. The application of security practices for the *End Device-Fog Node* layer is difficult due to the limitations of the end device computed capabilities, the available energy for these devices, the environment is distributed and heterogeneous, and the available bandwidth of wireless communications is significantly limited. For the *End Device-Fog Node* layer, the most common cybersecurity issues are the inadequate software protection, insufficient or nonexistent communication encryption, insufficient or nonexistent authorization, and significant privacy concerns.

A substantial portion of IoT and computing systems employ the benefit from the capability to stream the data from the end devices to the nodes of the fall or directly to the cloud. Devices then generate data streams are typically video cameras, vehicles, smart phones, smart sensors, controls, portable and wearable devices, etc., (Yang, 2017). In order to secure such data streams, three essential cybersecurity goals must be achieved: authentication, integration, confidentiality, (Usman et al., 2016). In order to successfully achieve these goals, especially for the computing *End Device-Fog Node* layer, novel approaches must be introduced in order to address the limited computer capabilities, limited available power, and constraints on the network's bandwidth.

One of the major applications for IoT devices is real-time wireless video sensing. In recent time, it has become a major research topic due to the sensitive privacy issues it can introduce, (Costa et al., 2014; Hamoudy et al., 2017). The devices that are capable of video data streaming include surveillance and security cameras, house monitors, transit vehicles, smart traffic cameras, etc. In general, the streaming of video data is a popular application form of IoT devices, because it is creating significant added value. However, streaming of video data over IoT is inherently unsecure and contains a significant number of security threats. Challenges to address these security threats

are very difficult because it is hard to evaluate different requirements which include: privacy and confidentiality; limited power available for devices; nonrepudiation (including timestamping); low delivery latency due to a real-time content requirement; limited network bandwidth; content broadcast capabilities; continuous authentication (CA) of the data stream source and content with limited computation; and ability to securely resume the transmission of data streaming after the interruption of transmission, (Sicari et al., 2015), (Hamoudy et al., 2017), (Winkler et al., 2014).

Secure Internet of Things Data Streaming

In order to ensure the security of data streams, several methods can be employed. The most widely adopted ones are cryptography, covert channels, digital watermarking, and steganography. Dependent on the requirements, these technologies can be realized in alternative TCP/IP layers of the protocol stack.

Various transport protocols are used to implement the streaming of data strategies. (Fairhurst et al., 2017) proposes broader protocols which can be used as an inspiration for creating atypical transfer services: the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Real-Time Transport Protocol (RTP), Transport Layer Security (TLS), Datagram TLS (DTLS), and others. A significant number of services has been conducted in order to study and analyze the reliability, consumption of power, bandwidth efficiency, and the security of the protocols, (Rajaboina et al., 2016; Gopinath et al., 2013; Pakanati et al., 2015; Xylomenos et al., 1999; Giannoulis et al., 2009; Suárez-Albela et al., 2017). Analysis of the MQTT and CoAP lightweight protocols, conducted by De Caro et al., (De Caro et al., 2013), focused on the design for a highly constrained resource environments. General analysis of technologies for IoT data streaming has been presented by (Herrero, 2020).

The Qualitative and quantitative comparison of these protocols has revealed that CoAP is more efficient due to it being designed on top of the UDP protocol. Because of the nature of the video streaming percentage, off packet loss can be tolerated. This percentage depends on the various requirements inherent in the application and technology that is being used for implementation.

Numerous cryptographic schemes and methods of authentication are based on the hash-chain method. A Multicasting scheme, based on a message recovery signature scheme, has been proposed by Yang et al. (Yang et al., 2014) as a source authentication. This proposed scheme provides confidentiality, multicast source integrity, authentication, and also provides a sequence number for the packet, so that video streaming could be displayed in the correct sequence. This scheme has an inherent drawback of providing less tolerance, but it suffers from significantly increased added information for each packet that is effectively doubling the amount of useful information being streamed. A two-tier signature-hash (TTSH) has been proposed by Wang et al. (Wang et al., 2013) for stream authentication in order to improve the quality of video data. It is achieved by the reduction of the authentication dependence overhead while protecting its integrity. Significant gains can be achieved by using the TTSH

scheme in both the video quality of the authenticated video stream and the overall energy efficiency of the transmission. A Timed Efficient Stream Loss-Tolerant Authentication (TESLA) broadcast authentication scheme has been proposed by Perrig et al. (Perrig et al., 2001). The authentication of the source of the data stream is achieved by TESLA by using time and key series. The drawbacks of the TESLA scheme are the difficulty in adopting it for real-time data streaming, and the inability to provide repudiation of the source. The cryptographic keys are expected to be used for a period of time, thus time synchronization between the sender and the receiver must be achieved. Because the ability to check the incoming packets is only valid during the next period, the delayed datastream can be lost. In our previous work, we have proposed the employment of an energy-efficient SSL protocol, (Venckauskas et al., 2015) that is able to provide the most effective ratio between the security of the transmitted data and the energy being used for transmission.

The authentication of datastreams based on the clustering technique has been proposed by Usman et al. (Usman et al., 2016). This data streaming technique maintains the quality of the transmitted data and authenticates the data streams with significant energy efficiency improvements. It achieves authentication into the step scheme (1) node authentication, and (2) secure transmission of the data stream through data authentication. The authentication of data packets is based on crypto-hash tags. These crypto-hash tags chain data packets in a sequence - the subsequent data packet is chained to the previous one. Actually, the usage of crypto-hash tags increases the amount of data being transferred significantly and increases the energy consumption by about 20%. A covert channel adapted to various application protocols and networks has been proposed by Wendzel et al. (Wendzel et al., 2015). These covert channels provide authentication functionality for data sources and content and can be implemented on different TCP/IP protocol stack layers, (Degraaf et al., 2005; Xie et al., 2015; Islam et al., 2017). A hidden payload in covert channels contains protocol headers, the so-called micro-protocols, in order to enhance the properties of the network covert channels. The addition of such protocol headers enables the introduction of fundamental features, such as dynamic routing, simultaneous connections, reliability, proxy capabilities, or session management for network covert channels. In addition, such features enhance communication and make it stealthier and more adaptive. An overview and categorization of micro-protocols has been provided by Wendzel et al.. (Wendzel et al., 2014). An authentication method of an identity has been proposed by Xie et al. (Xie et al., 2015) that is based on the reverse usage of the network covert channel. Xie et al. (Xie et al., 2015) proposed an identity authentication method based on the reverse usage of the network covert channel, where identity tags are being transmitted as packet intervals in order to exploit the data carrier. The FTP platform has been used to validate this method by the authors. However, this method suffers from a decreased data rate by 28—47%, as it has been shown by experimentation, depending on the channel noise. An authentication technique that employs geolocation information of IoT nodes by using a covert channel has been proposed by Islam et al. (Islam et al.,

2017). This technique is based on the Physical Unclonable Function (PUF) and the ICMP covert channel. A novel hybrid cryptosystem for secure video data streaming for IoT applications has been presented by (Alarifi et al., 2020), and an incorporation of blockchain state channels for IoT devices was developed by (Jeong et al., 2022).

Deep hiding techniques, based on steganography methods that can be applied to any existing network, have been proposed by Frączek et al.. (Fraczek et al., 2011) in order to reduce the deductibility even further. In the paper, five different deep hiding types of techniques were presented. The techniques include Steganogram Scattering, Multi-Level Steganography (MLS) Steganogram Hopping, Inter-Protocol Steganography, and Carrier Modifications Camouflage. Deductibility properties of the existing methods can be reused by employing these methods. These methods can be used in various combinations while using different steganographic methods, scattering the data in between a number of sending hosts, employing different carrying network protocols, etc. Frączek et al. additionally introduced the idea of multilevel steganography (MLS) that is discussed further in their work (Frączek et al., 2012). MLS simultaneously employs two or more different steganographic methods. The lower-level MLS method is wrapped up by the upper-level MLS and uses it as a carrier. For this reason, the lower-level steganography method is significantly harder to detect or identify even if the upper-level steganography method is detected. Various scenarios are proposed by the authors in which MLS can be applied. The more secure lower-level method is employed to transmit critical information such as integrity, encryption keys or authentication information for the data that is being transmitted by the upper level less secure method. Parameter changes for the upper level can also be transmitted via the lower-level method in order to decrease the chances of detection (e.g., taking advantage of Steganogram Hopping by transmitting updated parameters through the lower-level in order to change the upper-level method). An embedded watermark at the beginning of the datastream sequence is a method proposed by Kesavan Gopal (Kesavan Gopal, 2010). It employs a unique identifier for a device or the user-defined payload. While being semi-fragile by nature, this method is protocol independent, has high attack resistance, and low packet losses through transmission.

2.6. CRITERIA FOR THE SYSTEM

Criteria for Localization Solution

The review of the state-of-the-art scientific literature has revealed many proposed localization algorithms for the IoT. A selection of publications has been made and investigated as listed bellow.

A1 – (Mpeis et al., 2020)

A2 – (Safavi et al., 2018)

A3 – (Aernouts et al., 2020)

A4 – (Lin et al., 2016)

A5 – (Guo et al., 2019)

Localization methods have been evaluated by their achieved *Accuracy*, level of algorithms *Distribution*, are they a *Software* solution, are they able to *converge partially in zones*, do they require *a priori information* to achieve localization solution, and can they integrate external solutions, such as GNSS, seamlessly. The results of the comparative analysis for localization algorithms are summed up in Table 2.1, where an empty cell represents the lack of feature, *YES* represents active functionality. From the comparison of different IoT localization algorithms, we can conclude that steady research progress has been made over recent years and localization problem is actively being researched. The lack of dominant approach indicates the need for further development.

Table 2.1: Criteria evaluation for localization algorithms

	A1	A2	A3	A4	A5
Accuracy	$\approx$ 2 m	$\approx$ 2 m		$\approx$ 2.5 m	1.435 m
Distributed algorithm		Yes	2–15		Yes
Software solution	Yes	Yes		Yes	Yes
Zone convergence	Yes	Yes		Yes	Yes
No *a priori* data		Yes	Yes		
Integration of external solutions			Yes		Yes

Criteria for Power Management System

The review of the state-of-the-art scientific literature has revealed a number of proposed power management systems for the IoT. A selection of publications has been made and investigated.

B1 – (Mayer et al., 2020)

B2 – (Chen et al., 2018)

B3 – (Yao et al., 2020b)

Table 2.2: Criteria evaluation for power management systems

	B1	B2	B3
Adaptive	Yes	Yes	Yes
Intermittent power sources	Yes		
Ability to distribute power between between functions		Yes	Yes
Localization over communication channel			

The evaluation criteria for power management systems have been selected: *Adaptive*, *Intermittent power sources*, and the *Ability to distribute power between between functions*. Power management is a crucial aspect of IoT. Most of power management systems are tailored to specific applications. Though there are systems proposed for communication power management, no system as of yet has been proposed for localization tasks over communication channel.

Multimodal IoT security solutions

The review of the state-of-the-art scientific literature has revealed several multimodal IoT security solution propositions. A selection of publications has been made and investigated as listed bellow.

D1 – (Olazabal et al., 2019)

D2 – (A Hassen et al., 2020)

The evaluation criteria for multimodal IoT security solutions have been selected as follows: *multi-modality* - ability to integrate multiple modes for increased security, *parameter compression* - ability to compress parameters such that transmission over IoT would be feasible, *scalable number of parameters* - ability to increase or decrease the number of used modes, and *trivial validation* - ability to validate the security solution with a trivial amount of computation. From the review of the state-of-the-art publications, we can conclude that multimodal IoT security solutions are only recently being introduced into the IoT. No proposition of multimodal solution with a scalable amount of parameters was found.

Table 2.3: Criteria evaluation for localization solution multimodal security solutions

	D1	D2
Multi-modality	Yes	Yes
Parameter compression		Yes
Scalable number of parameters		
Trivial validation		Yes

Criteria for communication protocol

The review of the state-of-the-art scientific literature has revealed a large number solutions of proposed IoT communication protocols. A selection of publications has been made and investigated as listed bellow.

C1 – (Mahmood et al., 2018)

C2 – (Abbasinezhad-Mood et al., 2018)

C3 – (Glissa et al., 2019)

C4 – (Kim et al., 2019)

C5 – (Luo et al., 2020)

C6 – (Oh et al., 2021)

The evaluation criteria for lightweight IoT communication protocols have been selected: *Confidentiality* – capability to encrypt the data, *Integrity* – capability to validate the received information, *Authentication* – capability to authenticate the source of the transmitted data, *Privacy* – capability to mask the identity of the transmission source, and *Key exchange* – necessity for the devices involved in the transmission to exchange cryptographic keys. The comparison of the analyzed protocols is summarised in Table 2.4, where an empty cell represents the lack of feature, *YES* represents active functionality, and the *X* represents issues or drawbacks. From the comparison of different IoT communication protocols, we can conclude that steady research progress has been made over recent years and lightweight secure IoT communication protocols are being actively improved.

Table 2.4: Criteria evaluation for communication protocol

	C1	C2	C3	C4	C5	C6
Confidentiality			Yes	Yes	Yes	Yes
Integrity		X	Yes		Yes	Yes
Authentication	Yes	Yes	Yes		Yes	Yes
Privacy	Yes	Yes	Yes	Yes	Yes	Yes
No key exchange	X					

2.7. CONCLUSION OF THE OVERVIEW

After analysis of the published scientific works, it was concluded that IoT object identification and authentication is a relevant field for research with numerous scientific papers being published. The current state of the field is active, and numerous publications are being made on specific aspects of IoT security. What was found lacking was the research into the creation of more generalizable solutions. Comparative analysis of scientific literature has been conducted, and relevant tools and methods have been selected in order to fulfill the aim of the thesis. Various approaches to use multimodality in IoT security methods exist, however, none of them incorporates localization information, considers the power management, data integrity and encryption in a systematic fashion. For these reasons, we can conclude that the chosen problem is relevant and worth further research. After the analysis of the currently available literature and solutions, sets of criteria have been developed for each part of the Multimodal Security System for IoT communications.

Theory Framework

In this chapter, theoretical developments required for the development of a multimodal security system for IoT communications are presented. Section 3.1 presents the creation of the ubiquitous, distributed localization algorithm that is required to generate localization solutions in the IoT network. Section 3.2 presents the creation of a hybrid control system designed to manage the power consumption of the Edge-Node by allocating it to computation, communication and localization tasks. The HCS is designed to work with intermittent power sources and to ensure the continuous performance of the Edge-Node. Section 3.3 presents the Merkelized Abstract Syntax Tree (MAST) that is used to create the multimodal identification and authentication method. Section 3.4 presents the Lightweight Secure Communication Protocol that is used to communicate over the IoT network. Section 3.5 provides the conclusions for the chapter.

3.1. UBIQUITOUS LOCALIZATION SYSTEM

In order to create a versatile ad hoc localization algorithm for IoT, let our network be comprised of three types of network nodes that possess the capability to perform ranging measurements, perform localization communication and store local and absolute positioning solutions. The localization method presented in this section has been published in the journal publication (Bagdonas et al., 2017) and is based on previous work presented in international conference proceedings (Bagdonas et al., 2009) and (Bagdonas et al., 2008).

- A Network Node (NN) is a stationary IoT node. It can send and receive data, and perform RTT measurements with other nodes that are in its communication range.
- A User Node (UN) is a mobile IoT node that can move in any direction, has ability to send and receive data, and perform RTT measurements with other nodes that are in its communication range.
- A Local Reference Frame (LRF) is a set of a minimum of 4 interconnected NNs. None of the three NNs may lie on a straight line, and the fourth NN must be located outside the plane defined by the positions of the former NNs. Such a conjunction of NNs forms a different tetrahedron in three dimensions.

- An Absolute Positioning Solution (APS) is a positioning solution independent and external to LRFs in the IoT network. APS can be obtained directly from NNs, provided by GNSS, NN if it has relevant technological capabilities, or indirectly through ranging UNs and the incorporation of UNs APS coordinates into the IoT localization algorithm.

- A Virtual Network Node (VNN) is a UN with this new solution obtained by performing ranging measurements with one or more LRFs. Such VNN can contain APS ordinance provided by an independent UN feature. VNN is used to relate two or more overlapping LRFs and subsequently propagate the APS solution through IoT networks.

- Network Convergence (NC) is a state when two or more overlapping LRFs are merged, and an APS solution is generated. Such NC can occur locally or be a full IoT subnetwork event, where the coordinates of NNs in LRF are replaced by their APS coordinates. Once NC has been achieved, the IoT positioning solution converts to an APS augmentation/substitution solution and is fully compatible with the other APS system.

In order to obtain a three-dimensional solution, a minimum of four IoT NNs must be in direct contact with each other in order to form a LRF. Communication between these nodes provides both a possibility to perform direct ranging measurements and allows the exchange of information. In order to initialize the localization algorithm, each NN must perform communication with all available NNs. RTT measurements of the performed and ranging estimation is obtained. Such a collection of measurements produces dual results on both ends of the communication and ranging measurements. The obtained measurements are thus exchanged pairwise, and the obtained average value is used by both of the NNs. With repeated measurements over time, the accuracy can be increased, and the variance can be reduced in the ranging estimate. The effectiveness of such averaging reduces the effectiveness with a number of samples acquired, however, a more advanced mathematical approach would yield a significant improvement and an increase in the ranging resolution of the measurement.

Each NN aggregates the obtained ranging measurements in the internal database containing the IDs of the neighboring NNs and the associated range estimate. Each individual NN creates its own LRF and is designated as its zero point NN_0 with coordinates $x_0 = 0$, $y_0 = 0$ and $z_0 = 0$. Ranging measurements between NNs in LRF are defined as ρ_{ij}, where i and j represent the indexes of the NNs inside a specific LRF, where index i represents the origin node, and the index j represents the connected node for RTT measurement. Each NN can and usually belongs to multiple LRFs, and their reference indexes are different for each individual LRF as shown in Figure 3.1.1.

Once the ranging measurements have been obtained for each individual NN and databases populated with the averaged ranging estimates, these databases are shared in between the NN. After this stage, each individual node correlates the obtained measurements and performs search through the existing database in order to identify such

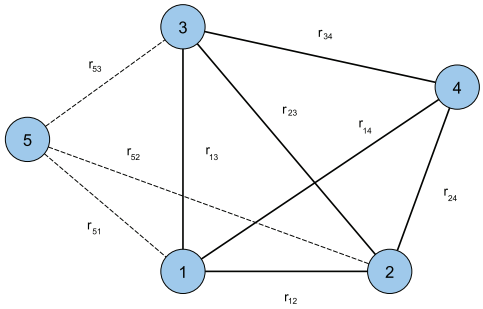

Figure 3.1.1: Formation of tetrahedrons for NN 1

connecting NNs that at least a single tetrahedron LRF can be formed. In case multiple tetrahedrons can be formed, LRFs are merged if tetrahedrons share NNs.

After the search, all duplicates are removed thus ensuring that only unique tetrahedrons are contained in the databases. Each tetrahedron originates on the host node such that coordinates assigned to it are $x_0 = 0$, $y_0 = 0$ and $z_0 = 0$. For each LRF, the trilateration algorithm is applied. The first neighboring NN is assigned such coordinates that it is placed on the LRF's X axis: $x_1 = \rho_1$,$y_1 = 0$,$z_1 = 0$. The coordinates of the second and the third neighboring NNs are computed by using the Equations 3.1 through 3.6, where:

x_i is the i'th nodes coordinate on the x axis in the LRF
y_i is the i'th nodes coordinate on the y axis in the LRF
z_i is the i'th nodes coordinate on the z axis in the LRF
ρ_{ij} is the range between the i'th and the j'th nodes

$$x_2 = \frac{\rho_{12}^2 - \rho_{01}^2}{-2\rho_{01}} \tag{3.1}$$

$$y_2 = \sqrt{\rho_{02}^2 - x_2^2} \tag{3.2}$$

$$z_2 = 0; \tag{3.3}$$

$$x_3 = \frac{\rho_{03}^2 - \rho_{13}^2 + x_2^2}{-2x_2} \tag{3.4}$$

$$y_3 = \frac{\rho_{13}^2 - \rho_{23}^2 + x_2^2 + z_2^2}{2y_2} - \frac{x_2 * x_3}{y_2} \tag{3.5}$$

$$z_3 = \sqrt{\rho_{03}^2 - x_4^2 - y_4^2}; \tag{3.6}$$

When the coordinates of all NNs in the tetrahedron have been computed, they are combined in a LRF by computing the rotation matrixes between two tetrahedrons

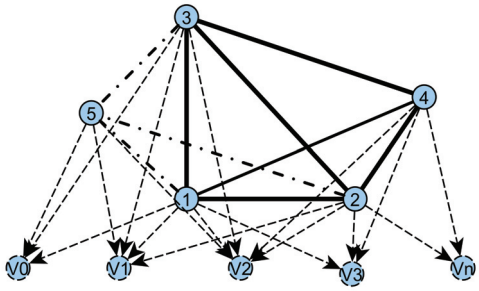

Figure 3.1.2: Observation of the VNN over its trajectory

and converting the coordinates into unified LRF comprising of all unique tetrahedrons that the host NN was able to form with the neighboring NNs. The computation of rotation matrixes involves the Linearized Least Squares (LLS) algorithm as no analytical model can be applied due to noisy measurements. The size of matrixes involved in the computation of LLS solution is constrained to 3x3 thus it does not amount to significant computational requirements for each individual node.

Once this stage is complete, the network is populated with overlapping LRFs. The orientation of each individual LRF is random and does not correlate with its neighbors. Further aggregation of LRF is not advisable as errors from ranging measurements propagate into rotation matrixes, and the positioning error significantly increases with the increase of the distance between the host NN and the nodes being aggregated into LRF. Every connected neighboring LRF is ensured to share mutual nodes, thus the transition of the positioning solution between two neighboring LRFs is possible. The continuous positioning solution between unconverged LRFs is obtained through the fact that neighboring LRFs have a significant overlapping. Once UN enters such an overlapping zone, its position is computed in both LRFs in parallel.

During the transition of UN through a LRF, a set of VNN_i is created, where $i = 0 : n$. As VNNs are created with each successful set of ranging measurements, positioning solutions from all overlapping LRFs that have performed their measurement point in space can be directly matched. In the case that UV does not possess the independent measurement capability, the feature can be successfully applied if the linear motion of the UV is assumed. Additionally, with the sampling rate being sufficiently high in relation to UV's movement speed, a linearization assumption can be adopted, such that the trajectory of the UV is interpreted as linear for the time equal to the measurement period. In case two LRF's are connected via less than 3 mutual nodes, or have NN in between them that did not have a possibility to form their own LRF, continual localization could be enabled by creating VN or external independent means, such as Inertial Navigation (IN).

Node Specific Positioning

When a User Node (UN) enters an area where it can obtain at least 3 ranging measurements to 3 distinct NN of a LRF, a trilateration algorithm can be performed and a solution for its relative position inside LRF can be obtained. If UN is capable of higher computational performance, the LLS algorithm can be employed to achieve higher accuracy, since more measurements can be employed in the calculation of a positioning solution.

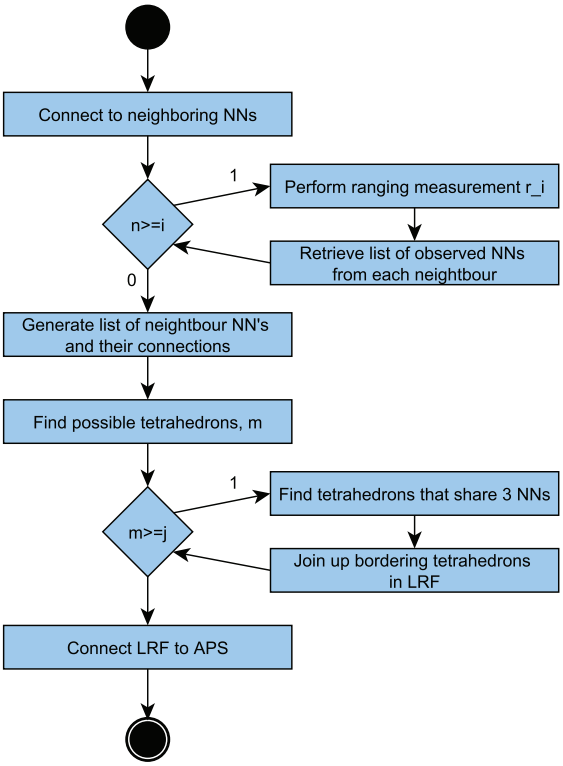

Figure 3.1.3: Localization algorithm

In the case a UN has an independent positioning solution, its results can be transferred to LRF. Each individual measurement is then treated as a VNN, as represented in Figure 3.1.2, where V_0 represents the estimated position of UN at measurement time t_0, V_1 represents the estimated position at measurement time t_1, etc. If the nature of such an independent positioning solution provides only relative UN positional changes (e.g., inertial navigation), it can be used to augment the ranging solution inside LRF. If the independent UN's positioning solution is able to provide the absolute coordinates (e.g., from GNSS), such VNN is incorporated into LRF. In order to translate NNs coordinates from LRF to APS, NN must have connections to three VNNs or NNs with the APS solution. The required three VNNs or NNs must not be positioned on a line.

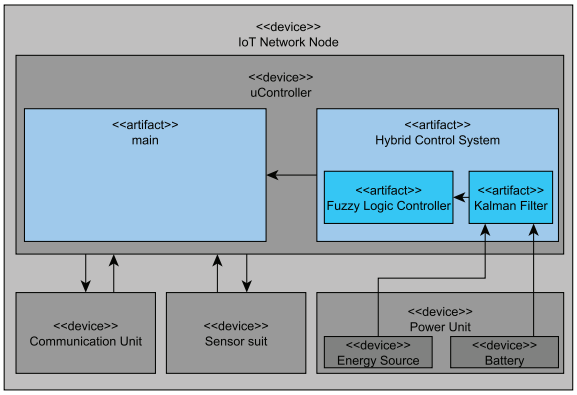

Figure 3.2.1: Proposed Hybrid IoT Localization Control System

Once the sufficient amount of measurements has been collected, LRF can be migrated to the absolute coordinate system as each of its NN is connected to at least three other NN. LRF is then considered to be fully converged. The quality of the positioning solution can further be augmented with additional measurements and observations of higher geometrical quality. Figure 3.1.3 represents the localization algorithm.

Convergence of the Network

When LRF obtains a positioning solution for its nodes in the absolute positioning system, the solution can be migrated to the neighboring LRF. Such migration can be achieved because neighboring LRFs share a number of NN. If at least 3 NN of LRF obtain coordinates in the absolute positioning system, the transition from local coordinates to the absolute ones can be obtained with the rotation matrix by computing the rotation LRF around its origin. Such an approach avoids the pitfall of drastic error accumulation when LRFs are being conjoined with only relative positions derived from ranging estimations. If the neighboring LRF shares less than the required 3 NN, o a neighboring NN does not have a sufficient number of its own neighbors to form LRF, and the introduction of VNN is insufficient to meet this requirement, NNs coordinates in the absolute positioning system can be approximated. This approximation can be further enhanced with either new VNN being provided by a new UN, or by having a connection to a different adjacent LRF that has converged to the absolute positioning system.

3.2. HYBRID POWER CONTROL SYSTEM

For the IoT localization task, the following Hybrid Control system is proposed. A PID controller is designed to control the IoT devices power consumption. It takes data from the power source module as the remaining power in the battery, the input power from the renewable power source and power consumption level from the

μController as shown in Figure 3.2.1. The output is provided to the Fuzzy Logic Controller (FLC) for integration. A Kalman filter module receives measurements from the Processor and estimates the localization solution for time t. It provides accuracy estimation to FLC as an input. FLC evaluates the power consumption, the localization solution accuracy, and, based on these inputs, decides on the number of network nodes to communicate with and the sampling rate. The elements in the Hybrid control system are summarized below.

1. Kalman Filter - to control the IoT device's power consumption
2. Fuzzy Logic - to determine the number of network nodes ranging measurements which are performed based on available power and controlled by ranging measurement variance levels

The proposed architecture is capable of adapting to the changing accuracy requirements and the changing levels of the available power. Dependant on the rules defined in FLC, a priority to the localization solution accuracy or the duration of operational time can be prioritized. Additional rules can easily be introduced to define specific operation modes for the IoT localization device based on the time of day, the time of year, or other parameters.

Kalman Filter Design

Kalman filter is an optimal linear estimator that is able to work with with the data that is used with the Gaussian and white noise. Kalman filter is described by a system dynamic model that comprises the state vector X_t and the state transition matrix A, and a measurement model that is comprised of the observation vector u_t and the observation transition matrix H. State vector contains the states that the Kalman filter tries to estimate. The states are not necessarily directly observed by measurements. The state transition matrix is derived from the state transition equations which describe how each individual element of the state vector changes from time moment t to time moment $t + 1$. As Kalman is a linear estimator, state transition equations must be linear. If the equations that describe the transition of states are not linear, they can be substituted with a simplified model, or a more advanced estimator, such as Extended Kalman Filter (EKF), can be employed, though EKF is no longer an optimal estimator. A comprehensive explanation of Kalman filters can be found throughout the literature, however, this work has been based on the control theory book *Kalman Filtering Theory and Practice* (Grewal et al., 2014). In this chapter, only the original work associated with the creation and application of a specific Kalman filter shall be presented.

In our case, the task is to manage the power consumption of an IoT NN such that continual operation can be maintained. We assume that our device is capable of directly measuring the battery power level and the power input from the solar power supply. Due to the nature of solar power generation which is dependent on the latitudinal location of the device on the surface of the Earth, the time of year and the

time of day, the equation that describes the maximum power generation from a solar power generator is not continuous and nonlinear. In order to simplify the computational burden for the IoT device, this nonlinear equation is transformed into a set of linear equations. Solar power generation is additionally infused with the noise that subtracts from its maximal power input value at any given time all day, on any day of the year, and at any given latitude.

The modeled IoT NN has a Constant Power Consumption (CPC) that is necessary to maintain its operation. For the sake of this design, we assume CPC to be constant.

State Equations and State Vector

State vector is defined by Equation 3.7.

$$x_t = \begin{bmatrix} PAL_t & BPL_t & IP_t & \delta BPL & \delta IP & CPC \end{bmatrix} \tag{3.7}$$

where:

PAL_t – Power allocated for localization
BPL_t – Battery Power Level
IP_t – Input Power
δBPL_t – Change in the battery power level
δIP – Change in the input power level
CPC – Constant Power Consumption

PAL_t is the amount of power that the filter assigns for the localization task. This power budget is then distributed between the number of nodes that the localization task is being conducted with. Dependent on the sampling frequency of the ranging measurements and the power allocated for the communication channel, the number of samples obtained from the assigned lower budget can vary for each NN. BPL_t is the total available energy being stored in the battery. Because NN operation is mandated to work in perpetuity, KF must evaluate the available energy in relation to the general power consumption and the power input from the solar power generator. IP_t is the power input from the solar power generator which is directly measured by the NN. δBPL_t is the estimated change in the battery power level. This change takes into account CPC, PAL_t and IP_t. δIP is the expected change in the generated power from the solar power generator. State transition Equations are described further, see 3.8, 3.9, 3.10, 3.11, 3.12.

$$PAL_{t+1} = IP_t - CPD_t - dBPL_t \tag{3.8}$$
$$BPL_{t+1} = BPL_t + \delta BPL_t \tag{3.9}$$
$$IP_{t+1} = IP_t + \delta IP_t \tag{3.10}$$
$$\delta BPL_{t+1} = \delta BPL_t \tag{3.11}$$
$$\delta IP_t = SMPR * \delta IP_t \tag{3.12}$$
$$CPD_{t+1} = CPD_t \tag{3.13}$$

By using the transition equations, we can generate matrix A such that Equation 3.15 would be true, where x_{t+1} is the estimate of the connector at time $t+1$, A is this the transition matrix, and x_t is a state vector at time t.

State transition matrix

$$A = \begin{bmatrix} 0 & 0 & 1 & -1 & 0 & -1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.14}$$

$$x_{t+1} = A \times x_t \tag{3.15}$$

Measurement Vector and Measurement Sensitivity Matrix

Measurement vector 3.16 directly measures the battery power level BPL_t, the solar power generator's input IP_t, and the difference between the internal models of power consumption and the and observed values through measurements. δIP_t represents the difference between the linear solar power generation model that is defined by the parameters of the time of sunset, the time of sunrise, and the value generated at noon. These parameters depend on the time of the year and the NN location on the surface of the planet. δBPL_t describes the difference between the expected bowel reserves in the battery and the value obtained from direct measurements.

From this description we can write a measurement sensitivity Matrix H 3.17 such that ensures relation between the measurement vector and the state vector as defined in Equation 3.18, where u_t is a measurement vector.

$$u_t = \begin{bmatrix} BPL_t & IP_t & \delta IP_t & \delta BPL_t \end{bmatrix} \tag{3.16}$$

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.17}$$

$$u_t = H \times x(t) \tag{3.18}$$

δBPL_t is modeled linearly. BPL_t value starts at a 50% power level and declines to 4% of the maximum capacity at the moment of sunrise. After that, BPL_t is modeled linearly to increase to 100% of the power capacity at the moment of sunset. After sunset, BPL_t decreases linearly to 50% at the moment of midnight as described by Equations 3.19, 3.20, 3.21.

$$\delta BPL_t = \frac{BPL_{sr} - BPL_{in}}{t_{sr} - t_{st}}, t \in t < t_{sr} \tag{3.19}$$

$$\delta BPL_t = \frac{BPL_{ss} - BPL_{sr}}{t_{ss} - t_{sr}}, t \in t_{ss} < t < t_{sr} \tag{3.20}$$

$$\delta BPL_t = \frac{BPL_{mn} - BPL_{ss}}{t_{mn} - t_{ss}}, t \in t > t_{ss} \tag{3.21}$$

Where:

BPL_{in} is the Battery Power Level at the beginning of the day

BPL_{sr} is the Battery Power Level at sunrise

BPL_{ss} is the Battery Power Level at sunset

BPL_{mn} is the Battery Power Level at midnight, t_{st} is the beginning of simulation

$t_{st}$is the time of sunrise as a function of the day of the year and the location of NN

t_{sr} is the time of sunrise as a function of the day of the year and the location of NN

t_{ss} is the time of sunset as a function of the day of the year and the location of NN

t_{mn} is midnight.

δIP_t the linear model for change in power. It is defined by Equations 3.22, 3.23, 3.24, 3.25. It takes the power input to values from a nonlinear model at the sunrise, noon, and sunset moments, and it computes linear trajectories between these points.

$$\delta IP_t = 0, t \in t < t_{sr} \tag{3.22}$$

$$\delta IP_t = \frac{IP_{ss} - IP_{sr}}{t_{zn} - t_{sr}}, t \in t_{ss} < t < t_{ss} \tag{3.23}$$

$$\delta IP_t = \frac{IP_{ss} - IP_{sr}}{t_{ss} - t_{zn}}, t \in t_{ss} < t < t_{ss} \tag{3.24}$$

$$\delta IP_t = 0, t \in t > t_{ss} \tag{3.25}$$

Where IP_{sr} is Power Input at sunrise, IP_{zn} is Power Input at noon, IP_{ss} is Power Input at sunset, t_{sr} is the time of sunrise, t_{zn} is the time of midday, and t_{ss} is the time of sunset.

Fuzzy Logic Controller

Fuzzy logic is a type of logic that can operate on variables whose values are represented as real numbers, in contrast to Boolean logic, whose variables can only be a 0 or a 1. Fuzzy logic allows the application of the decision-making mechanism which operates on non-numerically defined rules. For this application, a Fuzzy Logic Controller is proposed to control the number of NNs that the system performs the ranging task. Additionally, the logic controller determines the number of NNs to communicate from three groups, described by the variance level in their ranging measurements. The goal is to allocate the available power in such a way that a) a reliably accurate localization solution can be obtained and b) the available excess power is used for the reduction of variance in the measurements associated with specific NN. Figure 3.2.2 shows the IO of the Fuzzy Logic Controller.

Fuzzy Logic Controller has six inputs and four outputs.

- IN_PAL – provides the amount of the available powerful localization task.
- IN_nNN – provides the number of the observable NNs.
- IN_avgV – provides the average variance level in ranging measurements with all observed NNs.
- $IN\_nNN\_Low\_V$ – provides the number of NNs whose ranging measurements are categorized as having the low variance level.
- $IN\_nNN\_Avg\_V$ – provides the number of NNs whose ranging measurements are categorized as having the average variance level.
- $IN\_nNN\_High\_V$ – provides the number of NNs whose ranging measurements are categorized as having the high variance level.

The functions for these input are specified in Table 3.1.
The proposed Fuzzy Logic Controller has four outputs.

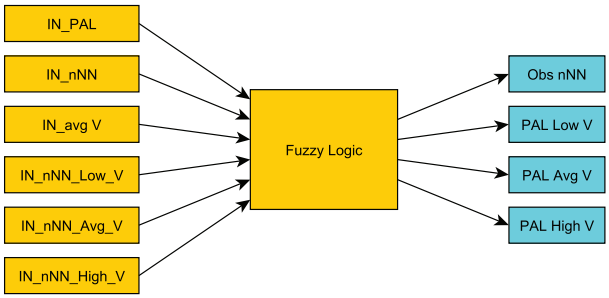

Figure 3.2.2: Fuzzy logic IO

Table 3.1: Parameters of Input Membership Function for Fuzzy Logic Block

Variable	Function	Range	P1	P2	P3
IN_PAL	Low_PAL	[0 1]	-0.41	0	0.1
	Med_PAL	[0 1]	0.05	0.15	0.3
	High_PAL	[0 1]	0.2	1	1.42
IN_nNN	Low_nNN	[0 26]	-10.84	0	6
	Avg_nNN	[0 26]	4	8	14
	High_nNN	[0 26]	10	26	36
IN_avg_V	Low_V	[0 1]	-0.42	0	0.42
	Avg_V	[0 1]	0.08	0.5	0.91
	High_V	[0 1]	0.58	1	1.42
IN_nNN_Low_V	Low_n	[0 26]	-10.83	0	4
	Avg_n	[0 26]	2	5	15
	High_n	[0 26]	10	26	36.83
IN_nNN_Avg_V	Low_n	[0 26]	-10.83	0	4
	Avg_n	[0 26]	2	5	15
	High_n	[0 26]	10	26	36.83
IN_nNN_High_V	Low_n	[0 26]	-10.83	0	4
	Avg_n	[0 26]	2	5	15
	High_n	[0 26]	10	26	36.83

Table 3.2: Parameters of Output Membership Function for Fuzzy Logic Block

Variable	Function	Range	P1	P2	P3
OUT_nNN	OUT_Low_nNN	[0 26]	-10.83	0	4
	OUT_Avg_nNN	[0 26]	2	6	10
	OUT_High_nNN	[0 26]	8	26	36.83
OUT_Low_PAL	OUT_Low_PAL_LOW	[0 1]	-0.42	0	0.05
	OUT_Low_PAL_AVG	[0 1]	0.02	0.1	0.2
	OUT_Low_PAL_High	[0 1]	0.15	1	1.42
OUT_Avg_PAL	OUT_Avg_PAL_LOW	[0 1]	-0.42	0	0.05
	OUT_Avg_PAL_AVG	[0 1]	0.02	0.1	0.2
	OUT_Avg_PAL_High	[0 1]	0.15	1	1.42
OUT_High_PAL	OUT_High_PAL_LOW	[0 1]	-0.42	0	0.05
	OUT_High_PAL_AVG	[0 1]	0.02	0.1	0.2
	OUT_High_PAL_High	[0 1]	0.15	1	1.42

- Obs_nNN – determines the number of NNs that will be used for the localization task.
- PAL_Low_V – determines the amount of energy that will be allocated for low variance NNs.
- PAL_Avg_V – determines the amount of energy that will be allocated for average variance NNs.
- PAL_High_V – determines the amount of energy that will be allocated for high variance NNs.

Functions for these outputs are specified in Table 3.2.

The rules for the Fuzzy Logic Controller are defined below. The goal of these rules is to manage the power in such a way that at least four NNs from the set of the low variance would be used for the localization task. If no such NNs are being observed, then the energy is allocated to the average variance group. If there are no NNs, or the number of available NNs is insufficient in the average variance group, then the energy is allocated to high variance NNs. If more than four high variance NNs are present, and sufficient energy is available, then this energy is assigned to high variance NNs.

```
"IN__PAL==High_PAL | IN_nNN==Low_nNN | IN_avg_V==Low_V |
    IN_nNN_Low_V==Low_n | IN_nNN_Avg_V==Low_n | IN_nNN_High_V==
    Low_n => OUT_Low_PAL=OUT_Low_PAL_LOW, OUT_Avg_PAL=
    OUT_Avg_PAL_AVG, OUT_High_PAL=OUT_High_PAL_HIGH (1)"

"IN__PAL==Med_PAL | IN_nNN==Avg_nNN | IN_avg_V==Avg_V |
    IN_nNN_Low_V==Avg_n | IN_nNN_Avg_V==Avg_n | IN_nNN_High_V==
    Avg_n => OUT_Low_PAL=OUT_Low_PAL_AVG, OUT_Avg_PAL=
```

```
    OUT_Avg_PAL_AVG, OUT_High_PAL=OUT_High_PAL_AVG (1)"

"IN__PAL==High_PAL | IN_nNN==High_nNN | IN_avg_V==High_V |
    IN_nNN_Low_V==High_n | IN_nNN_Avg_V==High_n | IN_nNN_High_V
    ==High_n => OUT_Low_PAL=OUT_Low_PAL_High, OUT_Avg_PAL=
    OUT_Avg_PAL_AVG, OUT_High_PAL=OUT_High_PAL_LOW (1)"

"IN__PAL==Low_PAL | IN_nNN==Low_nNN | IN_avg_V==High_V |
    IN_nNN_Low_V==High_n | IN_nNN_Avg_V==Low_n | IN_nNN_High_V
    ==Low_n => OUT_nNN=OUT_Low_nNN (1)"

"IN__PAL==Med_PAL | IN_nNN==Avg_nNN | IN_avg_V==Avg_V |
    IN_nNN_Low_V==Avg_n | IN_nNN_Avg_V==Avg_n | IN_nNN_High_V==
    Avg_n => OUT_nNN=OUT_Avg_nNN (1)"

"IN__PAL==High_PAL | IN_nNN==High_nNN | IN_avg_V==Low_V |
    IN_nNN_Low_V==Low_n | IN_nNN_Avg_V==Avg_n | IN_nNN_High_V==
    High_n => OUT_nNN=OUT_Avg_nNN (1)"
```

3.3. MULTIMODAL IDENTIFICATION AND AUTHENTICATION METHOD WITH GEOLOCATION DATA INTEGRATION

Hashing of Geolocation Data with Variable Precision

Geolocation information can be expressed in numerous global and local coordinate standards, such as Latitude and Longitude, Earth-centered, Earth-fixed, UTM, UPS, local tangent plane, etc. For the purpose of this work, we shall consider geolocation information to be expressed in the latitude and longitude as integer numbers, with the highest bits designated for degrees, subsequent value referring to the minute, then, the second, and, lastly arc seconds. Dependent on the precision of the localization algorithm and method, we expect the accuracy resolution of 1m. Let longitude be expressed as $Y \in \mathbb{Z}$ and latitude be expressed as $X \in \mathbb{Z}$. The area A on the spheroid can be then defined by using X and Y by applying the Floor function. The Floor function is realized by zeroing out the predefined number of the least significant bits for each coordinate. The more bits are eliminated from the coordinates, the greater area is defined by X and Y. The system falters if the coordinates correspond to the Equator or the Prime Meridian. In order to overcome this limitation, additional bits are introduced to specify the exact number of bits that have been eliminated. These bits are appended at the end of the X and Y coordinates. The number of the bits eliminated from X and Y can differ; thus, a rectangular area on the surface of the spheroid can be defined. X and Y with the eliminated bits shall be considered the geometric center of the area A, and the width and the height of the area will be equal to the maximum length at a specific longitude and latitude expressed by the eliminated information from the coordinates.

In order to verify if a new set of coordinates X_t, Y_t are within the area A, they

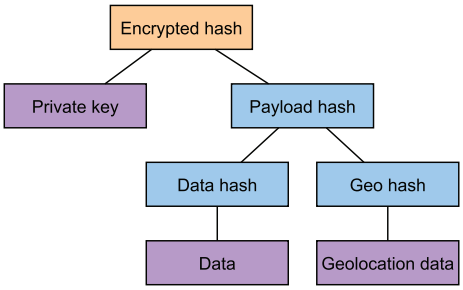

Figure 3.3.1: MMIA1: Merkel Tree Structure

are xor'ed with the original coordinates X and Y starting from the most significant bit, up to the first bit that has been eliminated.

$$X_{chk} = X(MSB\ RMB) \oplus X_t(MSB : RMB) \tag{3.26}$$

$$Y_{chk} = Y(MSB\ RMB) \oplus Y_t(MSB : RMB) \tag{3.27}$$

Where:

X_{chk} is the result of the X coordinate validations. If $X_{chk} = 0$, then UN is within the boundaries of the proscribed valid geographic zone.

Y_{chk} is the result of the X coordinate validations. If $Y_{chk} = 0$, then UN is within the boundaries of the proscribed valid geographic zone.

X is the center coordinate for the proscribed valid geographic zone.

Y is the center coordinate for the proscribed valid geographic zone.

MSB is the Most Significant Bit number, $MSB > 0$.

RMB is the number of masked bits, $RMB < MSB$.

X_t is the X coordinate for the localization solution obtained by UN at time t.

Y_t is the Y coordinate for the localization solution obtained by UN at time t.

If both X_{chk} and X_{chk} are equal to zero, then the coordinates X_t, Y_t lie within the proscribed valid geographic zone A, and the parameter is considered as valid.

In order to use such a function in practice, the Floor function must be implemented before the hash function is applied to the geolocation data. For this operation to be successful, the Fog-Node must communicate the number of bits RMB that have to be zeroed out from the coordinates of its obtained geolocation solution. Once this parameter has been defined, it can be used until the new one is provided by the Fog-Node. If the Floor function is applied before the hash function, the Fog-Node can verify the MAST tree without receiving the exact geolocation solution from the Edge-Node.

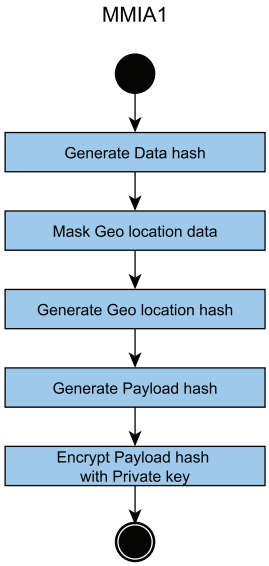

Figure 3.3.2: MMIA1: Algorithm for generation of encrypted Payload hash

Proposed Multimodal Identification MAST Tree

We propose two versions of the Multimodal Identification and Authentication Method (MMIA). The first version MMIA1 is represented in Figure 3.3.1 with the *Encrypted hash* at its root.

The MAST tree represented in Figure 3.3.1 shows the structure of MMIA1. It is generated by using hashing and asymmetric encryption functions. The *Payload hash* is generated by hashing together the hashes of the data that is being transmitted and the geolocation data. Before hashing, the *Geolocation data* is floored to the specified accuracy by the Fog-Node. The floor function provides the aliasing effect that is used in order to simplify the verification that the transmitting Edge-Node is within the geographical boundary defined by the minimum resolution of defined accuracy. Once the *Payload hash* has been generated, it is then encrypted by using the *Private key* of the Edge-Node. Encryption provides authentication functionality to the system.

Algorithm for MMIA1: Generation of the Encrypted Hash

Further, the algorithm for generating an *Encrypted hash* for the secure Edge-Node device by using the MMIA1 algorithm is described in detail:

1. A predetermined hash function must be applied to the data D in order to generate a hash D_h that is intended to be transmitted to the Fog-Node. The output of the

hash function will be denoted as dh_i.

$$D_h = h(D) \tag{3.28}$$

2. The coordinates of a localization solution C_X and C_Y are masked by clearing the predetermined number of bits by starting with the least significat bit. This is achieved by constructing a mask number m, where the value of individual bits is determined by Equation 3.29. The number of bits to clear is defined by the Fog-Node and represented as N_m. Each coordinate is bitwise multiplied with the mask number m.

$$m_i = 1 : i \geq N_m; 0 : i < N_m; \tag{3.29}$$

$$C_X^M(i) = C_x * m_i, i = n \ldots 0 \tag{3.30}$$

$$C_Y^M(i) = C_y * m_i, i = n \ldots 0 \tag{3.31}$$

3. The obtained masked coordinates C_X^M and C_Y^M are then concatenated to form masked geolocation information data G^M

$$G^M = C_X^M || C_Y^M \tag{3.32}$$

4. A predetermined hash function must be applied to the geolocation information data G^M. The output of the hash function will be denoted as G_h^M.

$$G_h^M = h(G^M) \tag{3.33}$$

5. Payload hash P_h is generated by applying the hash function to the concatenated Data and Geolocation hashes.

$$P_h = D_h || G_h^M \tag{3.34}$$

6. The obtained Payload hash P_h is then encrypted by using the private key K_{PR} of the Edge-Node to obtain the encrypted hash value EH_h that can then be transmitted to the Fog-Node.

$$EH_h = E(P_h, K_{PR}) \tag{3.35}$$

Algorithm for MMIA1 Authentication

Further, the algorithm for the identification and authentication of a received encrypted hash by a Fog-Node device is described in detail:

1. The received EH_h is decrypted with the Edge-Nodes public hey K_{PB} in order to obtain the Payload hash as shown in Equation 3.36.

$$P_h = D(EH_h, K_{PB}) \tag{3.36}$$

2. The geolocation hash value is created following the same steps as defined in Equations 3.29, 3.30, 3.31, 3.32 and 3.33.

3. Data hash D_h is computed by applying the hash function to the data segment of the message as defined in Equation 3.28, and the recreated payload hash is recreated as defined in Equation 3.34

4. The decrypted payload is then xor'ed with the recreated payload hash. If the result is equal to zero, the integrity of the received data and the geographic origin of the data can be considered as valid.

Figure 3.3.2 represents the algorithm for the creation of Encrypted Payload hash for MMIA1.

The MAST tree represented in Figure 3.3.3 shows the structure of MMIA2. It is generated by using hashing and asymmetric encryption functions. The *Root hash* is generated by hashing together the *Payload hash* and *NN 0 hash*. *Payload hash* has the identical structure to that of the *Root hash* defined in the MMIA1 version of the algorithm. It provides the function of verifying the integrity of the transmitted data and the geographic condition set by the Fog-Node. The *Root hash* is obtained by hashing the said *Payload hash* with the *NN 0 hash*. The *NN 0 hash* represents the root hash of the hash tree that contains the ID hashes and the hashes of the floored geolocation data for each *NN* that was used to generate the geolocation solution for the Edge-Node. In order to verify the *NN 0 hash*, the Fog-Node must have the geolocation information of each *NN* used in the generation of the Edge-Node geolocation solution, and the Edge-Node must append the ID's of the *NNs* that were used to generate its geolocation information, to the data it is transmitting. The ID's of the *NNs* must be appended in the exact sequence that they were used to generate the *NN 0 hash* tree. The obtained *Root hash* is then subsequently encrypted by using the *Private key* of the Edge-Node.

In both proposed algorithms, once the Fog-Node has decrypted the *Payload hash* for *MMIA1* or the *Root hash* for *MMIA2*, it can recreate and verify the MAST trees by using only the geolocation condition it has communicated to the Edge-Node and the recieved ID's of *NNs*. The verification step can be sped up by storing the precomputed values for each NN_ihash in the Fog-Node, where $i \subseteq 1...m$ and m is the number of the observed NN.

Algorithm for MMIA2: Generation of the Encrypted Hash

Further, the algorithm for generating an *Encrypted hash* for the secure Edge-Node device using the MMIA2 algorithm is described in detail:

1. A predetermined hash function must be applied to the data D in order to generate a hash D_h that is intended to be transmitted to the Fog-node. The output of the hash function will be denoted as dh_i.

$$D_h = h(D) \tag{3.37}$$

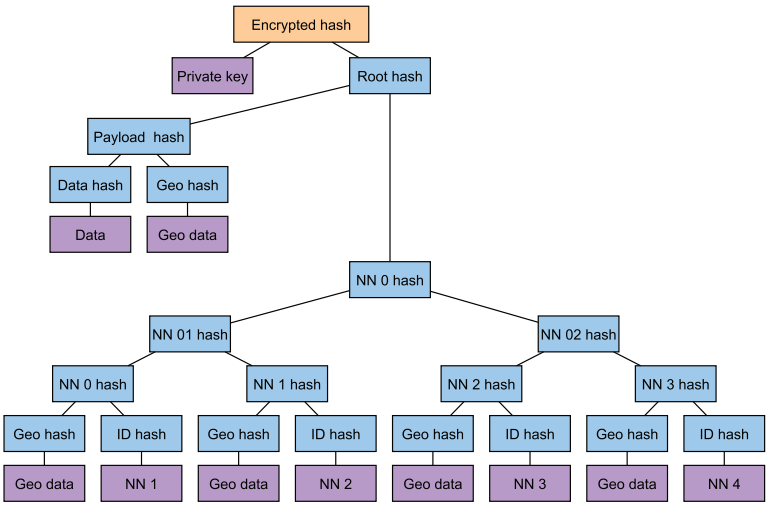

Figure 3.3.3: MMIA2: Merkel Tree Structure

2. The coordinates of a localization solution C_X and C_Y are masked by clearing the predetermined number of bits by starting with the least significat bit. This is achieved by constructing a mask number m, where the value of individual bits is determined by Equation 3.38. The number of bits to clear is defined by the Fog-Node and represented as N_m. Each coordinate is bitwise multiplied with the mask number m.

$$m_i = 1 : i \geq N_m; 0 : i < N_m; \tag{3.38}$$

$$C_X^M(i) = C_x * m_i, i = n \ldots 0 \tag{3.39}$$

$$C_Y^M(i) = C_y * m_i, i = n \ldots 0 \tag{3.40}$$

3. The obtained masked coordinates C_X^M and C_Y^M are then concatenated to form a masked geolocation information data G^M

$$G^M = C_X^M || C_Y^M \tag{3.41}$$

4. A predetermined hash function must be applied to the geolocation information data G^M. The output of the hash function shall be denoted as G_h^M.

$$G_h^M = h(G^M) \tag{3.42}$$

5. Payload hash P_h is generated by applying the hash function to the concatenated Data and Geolocation hashes.

$$P_h = D_h || G_h^M \tag{3.43}$$

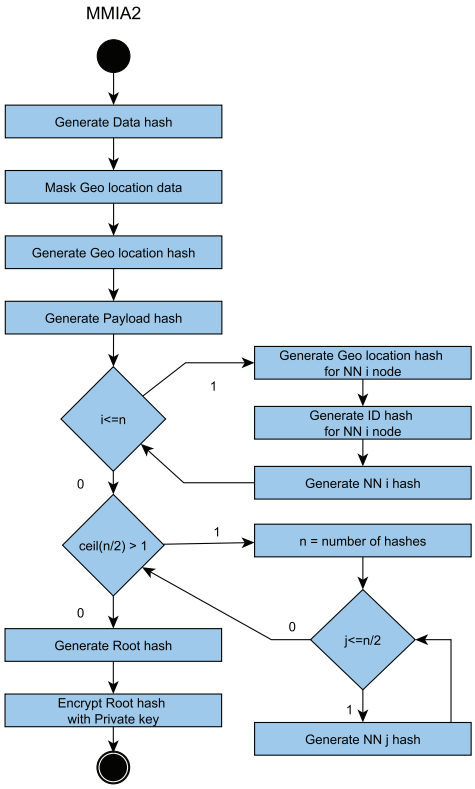

Figure 3.3.4: MMIA2: Algorithm for the generation of encrypted Root hash

6. Each NN that was involved in the generation of the localization solution on the Edge-Node side provides its own geolocation data to the Edge-Node. This data is subsequently reused to generate Geo hash G_h^i for each individual NN as shown in Equation 3.44, where N is the number of NNs that have been used to generate the localization solution.

$$G_h^i = h(G^i), i = 1, 2 \dots N \tag{3.44}$$

7. The ID of each individual NN that was involved in the generation of the localization solution on the Edge-Node side, its ID is amended to the data segment of the message that is being transferred to the Fog-Node and forms part of the message. Each ID is subsequently used to generate the ID hash.

$$ID_h^i = h(ID^i), i = 1, 2 \dots N \tag{3.45}$$

8. For each individual NN that was involved in the generation of the localization solution on the Edge-Node side, their geolocation data hash G_h^i and ID hash

ID_h^i is concatenated and hashed into a single $NN_h^i h$ value.

$$NN_h^i h = h(G_h^i || ID^i), i = 1, 2 \dots N \tag{3.46}$$

9. The generated $NN_h^i h$ values are then concatenated pairwise to form the next layer of the binary hash tree. If the number of NNs is odd, the last remaining hash value NN_h^N is hashed alone.

$$NN_h^{ij} = h(NN_h^i h || NN_h^j h), i = 1, 3 \dots N, j = i + 1 \tag{3.47}$$

10. Step 9 is repeated recursively until the number of the hash values is equal to 1. This value is then denoted as NN_h^0.

11. The value of the Payload hash P_h is then concatenated with the value of NN_h^0 and hashed to form a Root hash for the MAST tree.

$$Root_h = h(P_h || NN_h^0) \tag{3.48}$$

12. The obtained Root hash of the MAST tree is subsequently encrypted by using the private key of the Edge-Node.

$$EH_h = E(P_h, Root_h) \tag{3.49}$$

Algorithm for MMIA2 Authentication

Further, the algorithm for the identification and authentication of a received encrypted hash by a Fog-Node device is described in detail:

1. The received EH_h is decrypted with the Edge-Nodes public hey K_{PB} in order to obtain the original Root hash. D in Equation 3.50 refers to the decryption function.

$$Root_h = D(EH_h, K_{PB}) \tag{3.50}$$

2. The geolocation hash value is created by following the same steps as defined in Equations 3.38, 3.39, 3.40, 3.41 and 3.42.

3. Data hash D_h is computed by applying the hash function to the data segment of the message as defined in Equation 3.37, and the recreated payload hash P_h is recreated as defined in Equation 3.43.

4. For each ID that was appended to the original message, Geo hash G_h^i, ID hash ID_h^i and NN_{hh}^i hash values are computed by using Equations 3.44, 3.45 and 3.46. The geolocation data is obtained in the internal database of the Fog-Node or can be requested to be transmitted by the NN^i Edge-Node.

5. Through the recursive process, the generated NN^i hashes are concatenated pairwise and hashed into higher stems of the binary hash tree. Once only a single hash value remains, it is denoted as NN_h^0.

6. The computed hash values of payload hash P_h and NN_h^0 are concatenated, and the Root hash value of the MAST tree is computed.

7. The computed Root hash is xor'ed with the $Root_h$ value obtained from Equation 3.50. If the result of this operation equals to 0, the identification and authentication of the Edge-Node, the Edge-Node geolocation and integrity of the data are verified. Additionally, the reliability of the NNs that have been used by the Edge-Node to obtain the geolocation solution have been verified.

Figure 3.3.4 represents the algorithm for the creation of the Encrypted Root hash for MMIA2.

The differences between the proposed MMIA1 and MMIA2 versions of the identification and authentication algorithms are that MMIA1 requires significantly fewer computations of hash functions, thus it is more suitable for computationally less capable devices or where security requirements are lower. The MMIA2 version has additional parameters integrated into the Root hash, namely, the ID's and the location data of each neighboring NN that was used to generate the localization solution. These additional parameters enable the possibility to whitelist or blacklist certain NNs if they are deemed trustworthy, or conversely, to blacklist certain NNs and allow the possibility for the Fog-Node to filter out the data packets that have a localization solution that is based on the measurements from these NNs.

3.4. LIGHTWEIGHT SECURE STREAMING PROTOCOL

In order to enable data streaming in scenarios where a slight amount of packet loss is tolerated, e.g., data streaming in low bandwidth networks and resource constrained devices, we propose a lightweight secure streaming protocol (LSSP) to be used in the data streaming applications between the devices of the End-device and Fog-End layers. The protocol that is presented in this section has previously been published in the journal publication (Venčkauskas et al., 2018).

The protocol is described by the following name properties:

- Authenticated data streaming without the establishment of connection.
- Separate operational modes, designed for the protocol to enable different levels of security: sender's authentication, data integrity and authentication, confidentiality of the transmitted data, and robustness to partial loss of the data in transit.
- The ability to resume security properties even after interactions in the datastream with no additional data being transmitted in between the sender and the receiver, or additional steps from either of the involved devices.

- Elimination of the data overhead due to the fact that all the introduced security data is embedded within the headers within the modified UDP packets. The data inside the UDP packets remains unmodified by the protocol.

- Multicasting and broadcasting is supported by the protocol in the data stream.

- Secure and simple hash, symmetric encryption and HMACs functions are underlying the technology that enables the proposed protocols. These functions can be easily realized in the Fog-End devices.

The following techniques are used to realize the proposed protocol:

1. Modified packets from the UDP transport header, (Zander et al., 2007), are employed to transmit the streaming of data from the end device to the Fog-Node. Security checks and the reordering of the data packets are conducted by using the information embedded in the header fields of the UDP packet.

2. Continuous authentication, (Xie et al., 2015), between the streaming device and the device receiving the data stream is based on the authenticator of the end device, (Venčkauskas et al., 2012). Hash based message authentication codes (HMACs), time stamps and secure hash functions are employed to achieve this functionality.

3. Time-stamping and employment of secret keys is used to ensure the data confidentiality.

4. Checksums, ("Performance of checksums and CRCs over real data", 1998), and inclusion of redundant data, like error correction codes, (Ishengoma, 2014; Reed et al., 1960; Hamming, 1950), can be employed to enhance the robustness of the datastream in nonideal network environments in order to reduce the amount of packet loss.

To achieve efficient and flexible secure communication in the proposed protocol, we define three security modes:

- Mode 1 – authentication of the data source.

- Mode 2 – authentication of the data source and the integrity of the content.

- Mode 3 – authentication of the data source, the integrity of the content and confidentiality features.

Modified UDP for Secure Data Streaming

In order to achieve features that have been envisioned for the protocol, we propose the lightweight secure streaming protocol (LSSP) that is created by modifying the standard UDP packets with additional authentication information which is included inside the UDP packet headers. The structure of the original UDP packet is not disturbed, however, the functionality of some fields is altered. The required information for source authentication (data stream authenticators and dynamic devices) is generated from hashing the device's secure identifier and the time stamp. The generated authentication information is then separated and distributed among the headers of the UDP packets. Due to the design of the UDP protocol, no guarantee of packet delivery, ordering information, or avoiding the transmission of duplicate packets is present, we have included the numbers of data segments and packets in LSSP. Additional authentication information can be restored by employing error correction codes. These error correction codes for authentication information only restore the lost authentication information, and do not restore the transmitted data from the stream.

By adding the message authentication code digest to the transmitted data, authentication and data integrity is achieved. This digest is computed at the transmitting device using a secure device identifier (sid) and secure hash functions (h). Because the available UDP header space is limited, data stream packets are distributed among data segments s_i. We assign a sequence number for each individual segment with a sequence number $i = 0, 1, ...$

The type of the code algorithm that is being used to generate the message authentication code influences the length of the segments, and is distributed in n packets. The additional redundancy information is added to the datastream in order to enable the error correction. In a similar fashion, each data packet $p_{i,j}$, $j = 0, 1, ...n - 1$ that belongs to the same data segment si is sorted and allocated a sequence number i.

Each packet that is transmitted contains within it a segment number i, and the back number j, which defines its place in the segment. These numbers are added into the altered UDP header. At the reception device, packet numbers are used to arrange the received packets in the segment, and segment numbers are used to identify different segments within the datastream.

Figure 3.4.1 represents the modified UDP packet structure. This approach is based on the concept of covert channel micro-protocols. The modified UDP packet header remains unchanged only in its destination port field when comparing to the original UDP packet header, (Zander et al., 2007). The source port's first byte is fragmented into two 4-bit nibbles, first of which is used to store the segment number i, and the packet's sequence the number j, is being stored inside the second nibble. The second byte of the source port, the checksum fields and the packet length are used to store five bytes of the authentication data.

In case authentication is being computed by using the HMAC-SHA1 algorithm, the size of the data segment is determined by $n = 4 + 1$ data packets. The size of the digest based on SHA1 is only 160 bits which can be contained within four headers of

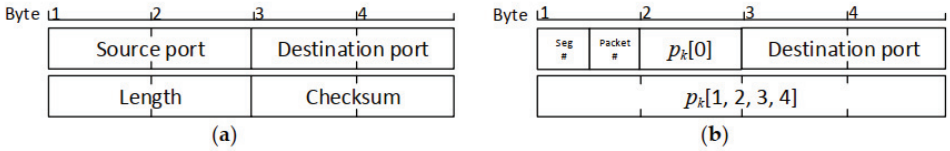

Figure 3.4.1: Comparison of a standard User Datagram Protocol (UDP) packet (**a**) and a modified UDP packet (**b**) containing authentication data and segment and packet numbers.

the UDP packets, with one more package required for the addition of the checksum generated by the XOR error correction code. The selection of UDP header fields was based on the following assumptions:

1. The source port is not an important field as the sending device is identified by the destination port and authenticated by using a different method;
2. The length of the UDP data is essentially a redundant field as the length of the data could be calculated from the IP header information;
3. The checksum field is not compulsory in the UDP header, moreover, data integrity is checked in the data link layer. Additionally, data integrity could be checked in the LSSP protocol.

Free modification of some UDP header fields could lead to some issues in complex networks using routers, firewalls, etc., but the primary target of the LSSP protocol is communications between Fog-Nodes and end devices where only OSI Level 2 network infrastructure devices are used. Our observations show that modified UDP header fields do not cause any additional issues in the OS (Windows and Linux) network stack as long as low level network libraries are being used (e.g., libpcap, winpcap (team, [n.d.]), etc.).

Generation of Secure Device Identifiers and Registration of End Devices

The first step of the protocol is the registration of the new Fog-End device at the Fog-Node and the generation of the secure device identifier (sid) which is known only to the end device that streams the data, and one (or more) of the Fog-Nodes which receives data and checks its security properties. The secure device identifier is transferred to the Fog-Nodes by using a secure channel and is stored in the Fog-Node. In order to register a new Fog-End device at the Fog-Node, an initial secure channel must first be established. Since initial wireless interfaces are potentially insecure, an alternative secure communications channel is required. A direct wired connection between two components, e.g., using USB or ethernet, could provide sufficient protection. We propose using a wired connection for the registration of the end device and wireless connection for further communications.

Authentication information (encryption keys in LSSP) is generated from the secure device identifier (sid). Therefore, this identifier must be unclonable, of good quality, generated truly randomly, contain sufficient entropy, be of a sufficient length, and not be stored on the end device. For this purpose, physical unclonable functions (PUF), (Hamming, 1950), are used, but a PUF is usually realized on special hardware. We have developed a secret encryption key generation algorithm by using the signature of the embedded system, (Venčkauskas et al., 2012). The proposed method effectively generates high-quality keys without any additional hardware and infrastructure cost, which is vital for devices with limited resources. We propose to use this algorithm for generating secure device identifiers.

Further, the algorithm for generating a secure device identifier (sid) by using the signature of the end devices is described in detail:

1. Create the set of signatures of the components of the end device $ES = es_i, i = 1, ..., n$. The signature is created by applying the string concatenation of the Vendor ID (cv_i), Type ID (ct_i), Model ID (cm_i), and Serial Number (csn_i):

$$es_i = cv_i||ct_i||cm_i||csn_i \tag{3.51}$$

   In steps 2–6, a subset of the component signatures is created. These signatures shall be used for computing the end device signature.

2. Calculate the device's embedded program header hash $ph = h(pk||psn)$.

3. Create the $n \times m$ matrix $MH = mh_{ij}$ from the bytes of the device's embedded program header hash $mh_{ij} = eb(ph, (i-1) \times j + i)$, where n is the number of the end device's signatures, and $m = eb(ph, n)modn$.

4. Calculate the sum s_j of the column elements in the matrix MH, $s_j = \Sigma_{i=1}^{n} mh_{ij}, j = 1, ..., m$.

5. Create the index array of the component signatures $IND = ind_j$, where $ind_j = s_j modn$ and delete repetitive indices, $ind_j \neg ind_i, \forall i \in 1...j-1$.

6. Create the subset of the component signatures $\widetilde{ES} \subseteq ES, \widetilde{es_i} = es_j$, where $j = ind_k, \forall ind_k \in IND, k = 1, ..., m$, from which the end device signature will be created.

7. Create the signature of the end device $ss_i = sign(\widetilde{ES})$.

8. Generate the secret device identifier $sid = fsid(ss, salt, iteration\_count, key\_length)$, where $salt = eb(ph, n)modn$, $iteration\_count = count(\widetilde{ES})$.

LSSP Mode 1: Source Authentication

In order to facilitate the authentication of the data source for the data stream, the headers of the all data packets include a segment message of the authentication code digest and a digest of an error correction code for the data segment.

The transmitted UDP headers contain segment and packet ID numbers. These numbers are subsequently used to arrange the received packets in the sequence of the digest's fragments. These digest's fragments are distributed among the different packets of the same segment. The transmitting device is not required to perform any modifications or computations on the data that is being transmitted.

The value of the digest is independent of the data content; the authentication of the data source is updated by performing the following calculation:

1. $mac1_i = HMAC(sid, ts||i)$, where sid is the secure identifier of the source, ts is the current timestamp, and i is the number of the transmitted segment.

2. The digest is divided into fragments $p_k = submac(mac1_i)$, where $k = 1...m, m = lenght(mac1_i)/5$.

3. We calculate the $mac1_i$ error correction code: $ecc_i = fecc(p_1...p_k)$, where $fecc$ is the chosen error correcting function.

4. We insert p_k and ecc_i into the UDP headers. After the insertion, the packets are ready to be transmitted to the receiver.

In order for the data streams source to be authenticated, the receiving device has to collect all the digest fragments of the p_k from the same segment as aggregate $mac1_i$. In case not all of the packets have been received, they can be restored by employing the error correction code. The receiving device also has to compute its own version of the corresponding function in order to obtain $mac1_r$. The data authentication is successful if both values are identical.

LSSP Mode 2: Source and Content Authentication

The following procedure to provide authentication for the source and the content has to be observed at the sending node:

1. A novel authentication key k_i must be generated for each new segment s_i in the stream by using equation $k_i = H(sid||ts||i)$, where i is the segment's number in the transmission, the timestamp is represented by ts, and sid is the source secure identifier.

2. Once all of the segment's data fragments have been aggregated, $HMAC$ digest can be computed by using all the data that is included in the packets by using the k_i key; the concatenation of the data $mac2 = HMAC(ki, data)$ is performed when all the data packets have been included in the data segment.

3. The fragmentation of the digest is performed by using $p_k = submac(mac1_i)$, where $k = 1...m, m = lenght(mac1_i)/5$.

4. The error correction code for $mac1_i$ is computed with $ecci = fecc(p_1...p_k)$, where $fecc$ is the desired correction function.

5. After the UDP headers have been updated with the p_k and ecc_i, the data segment can be transmitted via the data stream for the receiver.

The receiving device has to collect all the data packets that comprise a segment of data. Once all of the data packets have been collected, $mac2_s$ digest value can be restored by extracting data from the headers of the corresponding packets. In case a packet was lost during the transmission of the data, the error correction code can be employed to restore the specific missing fragments.

The receiver's $mac2_r$ digest version is calculated from the obtained key k_i values by using data that was received from the stream. If the sender's $mac2_s$ value corresponds to the receiver's value $mac2_r$ then the sender's identity has been authenticated, and the data integrity has been verified. In such a case, data packets are left unmodified in the whole data segment

LSSP Mode 3: Source Authentication, Content Authentication, and Confidentiality

In order to further enhance this variation the proposed protocol, it is possible to use symmetric encryption which increases the security properties and ensures the confidentiality of the data. Content integrity and source authentication is ensured by using the identical procedure as in Mode 2 version of the algorithm. The enhancement is achieved by the usage of symmetrical cipher encrypting of all the data (e.g., AES) in the CBC mode after the computation of the digest.

A data packet is independently encrypted in the sending device with the initialization vector iv_j, $j = 0, 1, ..., n-1$ and the secret encryption key ek_i. All the packets share the same encryption key for the i-th segment. The secret encryption key is generated by using the following equation: $ek_i = H(sid||jj||ts||jj||i)$, where sid is the secure identifier of the source, ts is the current timestamp, and H is the same secure hash function as used for the HMAC calculations. In case the length of the resulting secret key is too great for the chosen encryption algorithm, the secret key is then trimmed to fit the requirements of the encryption algorithm in use. A sufficiently secure hash function must be chosen in order to introduce a sufficiently lengthy result of the hash function in order to generate a sufficiently secure encryption key. In case AES256 is chosen for encryption, then, in order to achieve the required security level, at least the SHA256 algorithm should be employed to perform HMAC calculations.

In the CBC encryption mode, the employed initialization vector must be different for every individual data packet and has to be computed by using the following Equation:

$$iv_j = H(sid||i||j) \tag{3.52}$$

Such a protocol for security parameter derivation ensures that the receiving party is able to decrypt the data even in the presence of data loss inside the segment. The lost packets can be reconstructed only if sufficient error correction data is available. The reconstruction of the full segment is impossible.

If required, the resilience to the data loss can be increased with the introduction of tropical modifications by introducing redundant error correction information with additional data packets. If such an introduction is conducted, it is required to calculate the error correction code for those data packets.

3.5. CONCLUSIONS OF THE THEORY FRAMEWORK

In this chapter, constituent parts of an IoT multimodal identification and authentication method have been presented. A method to perform localization in a LRF and the propagation of the absolute positioning solution throughout the network has been described. The proposed method is able to generate localization solutions in ad hoc IoT networks without a priori data, and propagate the absolute positioning solution through the network. In zones where there is an insufficient amount of NNs, or zones that are disjointed from the wider network, the proposed algorithm is able to use LRFs for relative positioning.

A hybrid control system designed to ensure continuous functionality of IoT devices by the allocation of power over time to different functionalities has been specified. The proposed HPCS is able to work with intermittent power sources such as Solar power collectors. HPCS is able to maintain device functionality throughout the 24 hour daily and yearly cycles, while adjusting to the latitude of the UN.

A multimodal identification and authentication method that can integrate the verification of geolocation solutions has been defined. The proposed method uses hash functions to aggregate such parameters as payload data, localization data, the IDs of the neighboring NNs and their location data that can be used to increase the number of parameters. Additionally, the inclusion of neighboring NNs IDs enables whitelisting functionality.

A lightweight secure communication protocol for IoT data streaming was introduced. LSSP is a modified UDP protocol that uses handshake–free identification and authentication and has the capacity to include data encryption, as well as multicast and broadcast functionality. The proposed protocol is designed for applications where packet loss is not critical and it can be adjusted to work in three different modes dependent on the user's needs and capabilities.

The combination of these presented methods creates a multimodal security solution for IoT communications that fulfills the aim of the thesis.

Methods

This chapter describes the experimental setups created to test and validate the proposed methods. Section 4.1 describes the simulation created to validate the distributed localization algorithm. Section 4.2 presents the parameters of the HCS and the simulation setup to test the design. Section 4.3 outlines the validation of the multimodal identification and authentication method. Section 4.4 comments on the experimental setup created to test and validate the Secure Lightweight Communication Protocol. Section 4.5 provides conclusions for the Methods chapter.

4.1. SIMULATION SETUP FOR VERIFICATION OF THE DISTRIBUTE LOCALIZATION ALGORITHM

A simulation has been performed in the MATLAB environment. A set of 100 nodes was randomly distributed in a volume of $30m$ by $10m$ by $5m$ as represented in Figure 4.1.1. A maximum communication distance has been introduced, and computed ranges were subjected to 2% random noise of ranges estimation via RTT for a communication range of $5m$.

When the simulation is initialized, no positioning information is present in the network. First, LRFs are created for each NN. In the actual implementation of the algorithm, this step would not be instantaneous as the ranging estimates would be collected and distributed in the P2P manner. Given that the immobility of the NN individual ranging estimates would form the natural communication and data relay between NNs in an ad hoc network, precision could be increased by averaging the measurements over a period of time. Once the ranging information has been obtained, each node creates an individual database. For the purposes of simulation, the database has been aggregated in a single structure. While, in actuality, the duration of the formation of each individual LRF can vary, for simulation purposes we compute all LRFs at t_0. The computed LRFs are not aligned in the absolute positioning system and are randomly orientated. With their orientation being dependent on the first two nodes, they managed to form a tetrahedron.

Once LRFs have been computed, simulated UNs are released to the simulated environment. The UN movement is simulated over time with the sampling rate of 1s as a discreet set of ranging measurements with equal constraints as the ones applied to NN. Each UN is moving in a linear trajectory at a speed of 1m/s. VNs are created only if 3 ranging measurements are performed with individual LRFs. If UN is in an

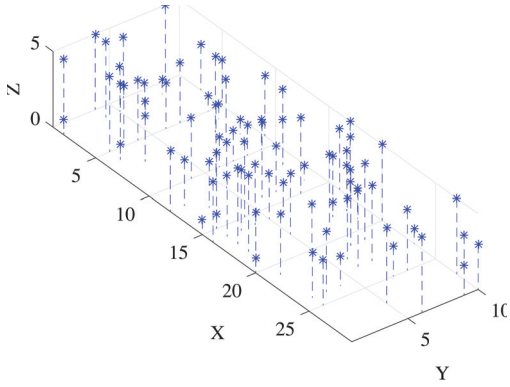

Figure 4.1.1: NNs of a simulated network

overlapping zone between two or more LRFs and has at least 3 ranging measurements with each individual LRF, VN obtains positioning solutions in all LRFs. Once UNs have finished their routes, the network's status is investigated in relation to the NN positioning accuracy and LRF convergence to the absolute positioning system.

The evaluation of the algorithm's performance has been recorded in over 100 simulations. Such a sample size has been chosen to average out the geometric influence of the positioning solution from the random nature of NN locations. Additionally, UN trajectories have also been randomized.

4.2. SIMULATION SETUP FOR VERIFICATION OF THE HYBRID CONTROL SYSTEM

To validate the proposed Hybrid Control System, a MATLAB simulation has been conducted. The simulation generates the number of available NNs and assigns the initial variance level to each individual NN. Throughout the simulation, a random set of these NNs is provided as available to the Hybrid Control System. The simulation emulates solar power generation dependent on the longitude, day of the year, time of day, and noise level parameters.

To validate the proposed Hybrid Control System, it is evaluated on the ability to maintain functionality throughout the 24 hour cycle while minimizing the downtime, maximizing the localization accuracy, and avoiding over-saturation of the battery with power.

A 24-hour simulation period is divided into 864 samples, each constituting 100 seconds of the entire sampling period. At each sampling, the Kalman Filter generates an estimate of the available powerful localization task, and the Fuzzy Logic Controller manages connections with individual NNs. The constant Power Consumption is set at such a value that, without power being allocated to localization, the IoT node would be able to perform its background tasks for two days if starting with a full battery and receiving no power from the solar power generator.

4.3. SIMULATION SETUP FOR THE VERIFICATION OF THE MULTIMODAL IDENTIFICATION AND AUTHENTICATION METHOD

To verify the proposed multimodal identification and authentication algorithm, a simulation has been designed in MATLAB. The simulation consists of MNs with assigned private keys and geolocation static coordinates. A mobile MN is simulated to traverse the geolocation where a specific area of interest is designated. The designated zone is unknown to the MN and is only verified by the receiver of the data transmitted by MN. The MN is continuously transmitting data at the present constant sampling rate that is signed with the proposed multimodal identification hash tree. The sampling rate has to be sufficiently low to allow all the complications to be performed within the MN.

The hash tree includes a public key from the MN that is being used to generate the *Top hash* together with the hash of the payload. This key is constant and does not need to be recomputed. The *Payload hash* is generated by hashing ID and geolocation hashes. The *ID hash* is generated by hashing together the *Data hash* in the public key of the sender. If MN is the origin of the data, its own public key is used in this step. The *Data hash* is generated by hashing the data that is being transmitted.

The Geolocation hash is generated by hashing together *Geo hash* which is obtained by hashing the coordinates of the MN, and the public keys of the NNs that have been used to compute the geolocation data.

During the simulation, we investigate various scenarios where illegal hashes are included in the generation of the *Top hash*. First, we investigate the ability to specify the geographic location, and then the investigation of illegal NNs being included in the generation of geolocation data is conducted.

4.4. EXPERIMENTAL SETUP FOR VERIFICATION OF THE LIGHTWEIGHT SECURE STREAMING PROTOCOL

Qualitative Analysis

The proposed protocol provides additional advantages in comparison to DTLS, such as the simplified registration of new devices for the streaming session. The DTLS protocol employs the handshake procedure, during which, the authentication between the client and the server is established. The handshake procedure employs x.509 certificates. To use the DTLS protocol, x.509 certificates must be generated, signed, and transmitted to all the nodes in the network. The generation of x.509 certificates requires stringent management, storage, and revocation of all these certificates that have been issued in the network.

No special stages are required to establish new connections when using the LSSP protocol between the client and the server. In case the employed version of the protocol is the M1 - the simplest variation, no data overhead is introduced into the packets transmitted over the network, thus ensuring zero traffic overhead for the authentication of the data.

Additionally, the handshake procedure that is employed by the DTLS, requires a

significant time to conclude. The duration of the handshake procedure is dependent on the quality of the network. In case a significant data loss is present, the duration of the handshake procedure is extended significantly. Furthermore, the hedging procedure requires bidirectional communication between the client and the server, thus increasing the traffic in the network further. This network congestion can be negatively impacted if the handshake procedure has to be repeated periodically. The data fields in the DTLS packets as additional protocol and security data are embedded within. This additional data adds to the overall traffic increase.

As the DTLS protocol employs the timing information, long interruptions in the data streaming session incur additional handshake procedures to be executed. The LSSP protocol does not suffer from such a drawback as the resumption of the streaming session does not require any additional actions. The receiver can automatically perform the source authentication right after the reception of the first whole segment has been concluded.

Because the DTLS protocol is based on the point-to-point architecture, it cannot be effectively used for multicasting data to numerous receivers at the same time. If such functionality is required, individual connections have to be established with each receiver. This effectively prohibits DTLS from being employed in multicast data streaming applications for computing due to the power and bandwidth limitations. The proposed LSSP does not suffer from such drawbacks and thus can be efficiently employed in situations where multicasting is required. As LSSP does not employ any handshake techniques, it can also be used for broadcasting applications as no acknowledgment from or communication with the receivers is required.

The proposed LSSP protocol also has advantages over DTLS in the situations of data loss in a noisy network environment because the DTLS protocol does not include any mechanism to deal with errors or delivery failures in such conditions. DTLS ensures data integrity only during the handshake stage if the packet is lost in the lower UDP/IP stack levels. Higher resistance to the data loss incurred due to errors appearing in the lower network stack layer can be handled by the LSSP protocol with the usage of ECC to authenticate data for the payload.

The drawbacks that are introduced by the LSSP protocol, in comparison to the standard UDP or the DTLS protocols, include the increased memory requirements on the transmission device, as the segment data must be aggregated fully inside the memory to ensure the required conditions for the data authentication and the ECC. Depending on the length of the used codes digests, this memory overhead can be impacted negatively. In case HMAC-SHA1 is employed, then the buffer has to be increased five times in comparison to the standard requirements for the UDP transmissions.

The requirement to aggregate all those segments of data introduces additional latency to the datastream over the network, as the calculations can only be computed once all segments of data have been loaded into the memory. The effect on the latency is bigger if the ‘slow’ data stream is used. Increased latency mitigation can be achieved by the reduction of the packet size.

Performance Analysis

A streaming client and a receiving client have been created to evaluate the performance characteristics of the proposed method. An embedded Raspberry Pi computer (Model B, revision 2, BCM2835 CPU, 512 MB RAM) running *Raspbian GNU/Linux 9 (stretch)* was used to implement the 'End Device' prototype. The results have been obtained by performing measurements at the sending device. A standard Windows 10 PC has been used as a receiving party for the data stream. The Java programming language has been used to implement the LSSP protocol. Open source security libraries from the Bouncy Castle (Bouncy Castle Inc., 2018) have been integrated into the implementation. jnetpcap java library (Technologies, 2018) have been employed to gain access to the UDP packet headers. libpcap (team, [n.d.]) and winpcap system libraries have been used to gain interface to the low level. Tests involving DTLS were implemented in the Java native DTLS protocol provided by the Bouncy Castle (*Legion of the Bouncy Castle Inc. Java (D)TLS API and JSSE Provider. User Guide.* 2018).

4.5. CONCLUSIONS FOR THE METHODS CHAPTER

This chapter presents the tools that have been used to verify the validity of the proposed multimodal authentication and identification method for IoT objects. A combination of quantitative, analytic, and applied research has been chosen to validate the functionalities of the methods. Simulation validation has been created for the localization algorithm as the base technology of the range estimation by using communication packets in RTT is still not developed enough for practical experimentation with the desired measurement accuracy. Because of this limitation, the HPCS has also been validated through mathematical simulation by using the MATLAB environment. The LSSP communication protocol has been tested by using practical equipment, directly measuring the power consumption, data throughput and computational requirements have been estimated. The MMIA identification and authentication method have been validated in the MATLAB environment by investigating the ability to define the geographic zone and a blacklist of NNs.

Results and Discussion

The Results chapter presents the obtained results from the testing and verification experiments and discusses the proposed methods, and the achieved experimental results are presented. Section 5.1 presents the results obtained from the simulation designed to verify the distributed localization algorithm. Section 5.2 presents the results obtained from the verification of the Hybrid Control System. Section 5.3 presents the verification results of the multimodal identification and authentication algorithm. Section 5.4 presents the results of the experimental testing performed to validate and investigate the performance of the Lightweight Secure Streaming Protocol. Section 5.5 discusses the obtained results for the distributed localization algorithm. Section 5.6 discusses the achieved results in relation to the power management of the IoT node. Section 5.7 discusses the obtained results for the lightweight secure streaming protocol. Section 5.8 discusses the obtained results for the multimodal identification and authentication algorithm. Section 5.9 discusses the integration of the presented methods into the Multimodal Security System for Internet of Things Communication. Section 5.10 discusses the future improvements and additional research that could be performed to advance the developed methods and solutions. Section 5.11 provides conclusions for the Results chapter.

5.1. RESULTS OF THE DISTRIBUTED LOCALIZATION ALGORITHM VERIFICATION

Figure 5.1.1 shows the distribution of the number of connections for NNs in the simulated network. Higher connectivity produces a consistent UN positioning solution due to the overlapping LRF and enables faster network convergence. Nodes with a connection number lower than 3 are unable to form a LRF. Figure 5.1.2 shows the average positioning error for randomly generated UNs moving on a linear trajectory through the network. UNs cleared the network's coverage area in under 14 steps. During each step, VNN was created if LRF was present. The positioning error in the initial simulation steps is significantly higher due to unfavorable geometry as UN enters the simulated network and has NN located only in front of it. As the UN moves further through the simulated space, it enters the network and becomes surrounded by NN. Having NN located around the UN produces a higher accuracy positioning solution.

After the simulation was performed, 26% of NN achieved convergence. Al-

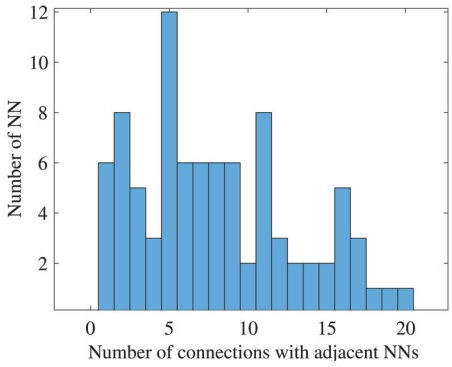

Figure 5.1.1: Distribution of connectivity between the nodes of a simulated a network.

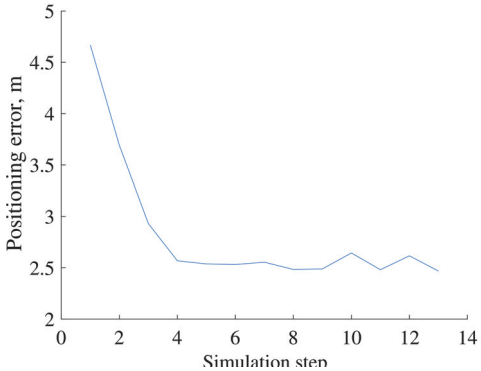

Figure 5.1.2: Average positioning error for all simulated UNs during their crossing through the simulated network.

though full network convergence has not been achieved, it is noteworthy that only with 3 UN having APS functionality and following a random straight line path, the local NC occurred in four zones. Additional iterations improve the network's convergence level and positioning accuracy significantly as presented in Table 5.1. Full network convergence has not been achieved as NN on the fringe of the network has not been able to form LRFs.

Table 5.1: Summary of the simulation results for the distributed localization algorithms.

Number of iterations	NC level, %	Average positioning error, m
1	26	2.8
2	63	2.2
4	70	1.9
8	74	1.9

5.2. RESULTS OF HYBRID CONTROL SYSTEM POWER MANAGEMENT FOR LOCALIZATION FUNCTIONALITY VERIFICATION

Here, the results of the simulation investigating the performance of the HCS are presented and analyzed to validate the proposed hybrid control system design.

Figure 5.2.1 shows the number of available NNs at each sample time in blue dots and represents the amount of used NNs as instructed by a Fuzzy Logic Controller in the red stars. This number is generated randomly assigning from the pool of the available NNs. A specific NN can appear, disappear, and then reappear throughout the simulation. Each NN is identified by its ID and thus can be categorized easily within the range of the available NNs. NNs are sorted by variance levels, and the Fuzzy Logic Controller chooses randomly several NNs dependent on the available power from each group.

Figure 5.2.2 shows the histogram of how many times each NN has been used for the localization task. As the measurements are being conducted with individual NNs, the ranging measurements of the variance level yield a decrease over time, thus a specific NN can move in between different sets of NNs.

Figure 5.2.3 shows the estimated change in battery power from the linear model in a blue dash-dot line and the simulated change in battery power level in a blue straight line.

Figure 5.2.4 shows the power input from the solar power generator in the green dashed line, the power assigned for localization in the red straight line, and the change in the battery power level in the blue dash-dot line.

Figure 5.2.5 shows the linear estimate model for the Battery Power Level BPL_{Proj} over the simulation period and the obtained Battery Power Level BPL as managed by the Kalman Filter.

Figure 5.2.6 shows how the variance level of individual NN changes over time as the Hybrid Control System allocates power to perform ranging measurements with it. In this simulation, the change in the variance of the ranging measurements is modeled as a logarithmic function of the total accumulated power. While this model does not capture all the nuances of the aggregated accuracy over the average results, it is used for illustration purposes.

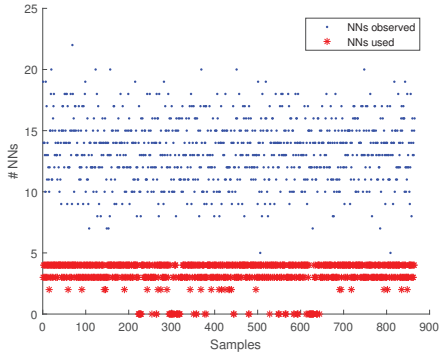

Figure 5.2.1: Number of observed NNs by the Edge-Node and the number of NNs assigned for localization measurements by the Fuzzy Logic controller.

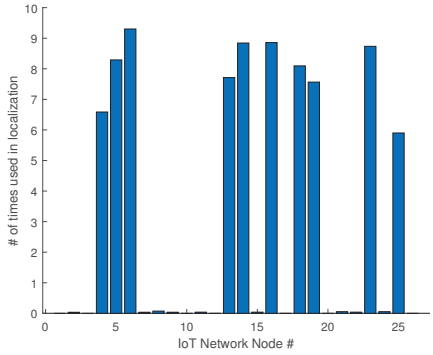

Figure 5.2.2: Number of times individual NNs have been used for localization measurements as assigned by the Fuzzy Logic Controller

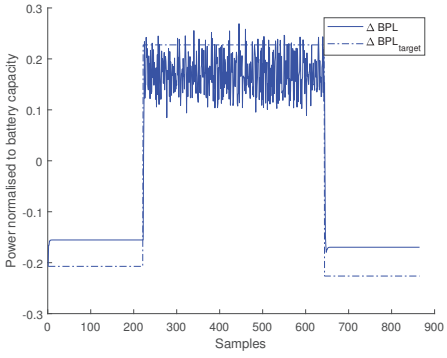

Figure 5.2.3: Total power consumption as managed by Kalman Filter over the simulated 24h period.

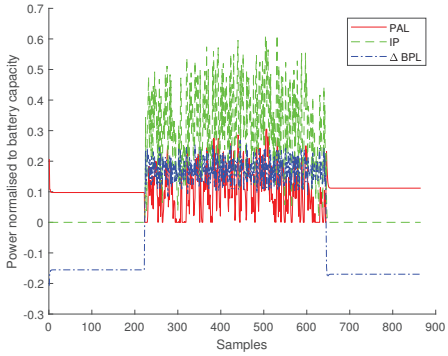

Figure 5.2.4: Power inputs into Kalman filter. PAL – Power Allocated to Localization, IP – Input Power, ΔBPL – change in Battery Power Level.

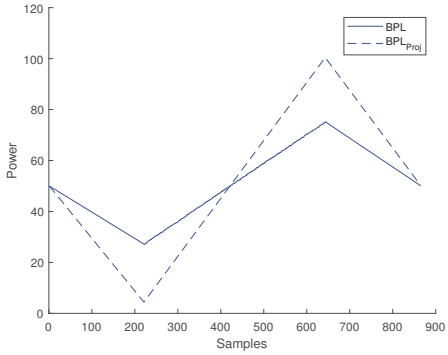

Figure 5.2.5: The battery power level over the simulated 24h period as managed by Kalman Filter.

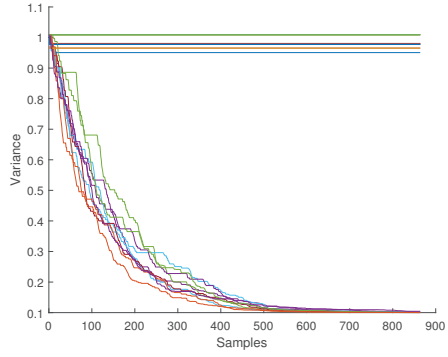

Figure 5.2.6: The change in RTT ranging solution variance for individual NNs produced by the averaging of measurements.

5.3. RESULTS OF MULTIMODAL IDENTIFICATION AND AUTHENTICATION METHOD VERIFICATION

Figure 5.3.1 shows the results of the Multimodal Identification and Authentication Method Verification simulation. The blue line represents the trajectory of the MN, the green stars represent the valid NNs, and the red stars represent the invalid NNs to be used for localization. The black cross represents the designated geolocation from which the data is expected. The red square represents the accuracy constraints. The data that is transmitted from within the area of the square is to be considered valid, and the data that is transmitted outside of the designated area is to be rejected.

Figure 5.3.2 shows the number of illegal NNs detected in the signature transmitted by the source. The data containing a localization solution based on the range measurements from illegal NNs is thus rejected as invalid.

Figure 5.3.3 shows the status of the signature (accepted or rejected) based on whether the data packet was transmitted from within the determined geographic zone and based on whether the localization data was generated with the ranging measurements from the accepted NNs. X here represents the number of the sample in the sequence, and the Y axis represents the number of the detected NNs which are not in the white list of the approved NNs. The white list in the simulation is arbitrary and is created for illustrative purposes.

5.4. RESULTS OF LIGHTWEIGHT SECURE DATA STREAMING PROTOCOL VERIFICATION

The comparison of the performance between the six analyzed protocols in respect to the sequential transfer of 10 MB of data with respect to the transmission duration when using different packet lengths is presented in Figure 5.4.1.

Independent of the length of the transmitted packet, the UDP protocol provides the fastest transmission times among the analyzed protocols. The performance of the M1 version of the LSSP protocol is very similar to the UDP results. The main difference is that M1 additionally transmits data source authentication functionality which is lacking in UDP. The slight difference between these two protocols can be explained by the higher computational requirements imposed by M1's calculations required to be performed on the transmitting device.

However, the total amount of bids that is transmitted via wireless channels is equivalent in both UDP and M1 cases, the only effective difference between these two protocols being a longer processing time on the transmitter's side to perform the required computations before sending packets out. This difference can be observed in the figure as a difference in the transmission time of 0.5 s was registered while transmitting in the $M1$ protocol 10 MB of data in data packets of 512 B size.

A viable comparison between the DTLS2 and $M2$ protocols, both of which can provide similar levels of performance and have similar data and source authentication properties, can be used as a benchmark to evaluate the performance of the proposed

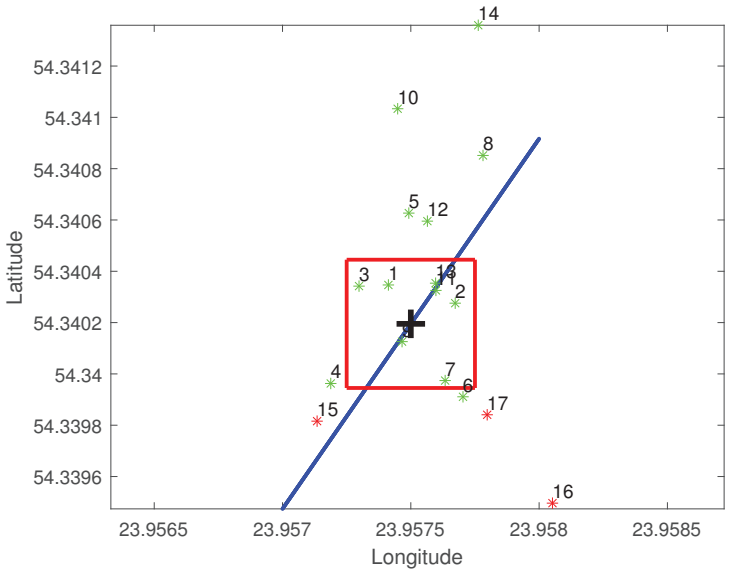

Figure 5.3.1: Simulated scenario of a MN traversing the designated zone.

protocol.

$M3$ is slower than DTLS3 because an additional data packet containing ECC information for data is sent in each data protocol.

The NetEM (Network Emulation) tool has been used to evaluate how the methods are performing in real-life networks. The NetEM tool provides the capability to emulate different conditions and falls off the network functionality. We employed NetEM as developed by (Hemminger et al., 2005) on the transmission device (Raspberry Pi) to simulate random packet loss in the hardware of the network. At the reception, we sought to collect all the available data packets. The missing data packets, if possible, were recovered or restored. Figure 5.4.2 illustrates the results obtained from this experiment.

To evaluate the proposed method's level of energy efficiency, the total energy consumption of that dreaming device has been measured while 10MB of data has been streamed in 256 B packets. The training device consists of a Raspberry Pi computer and a USB WiFi adapter connected to it. The obtained results are represented in Figure 5.4.3.

The power consumption of the Wi-Fi module was measured by the arrangement shown in Figure 5.4.4.

A Digitus Wireless 150N USB adapter has been used to measure the energy consumption of the transmission unit by using a current shunt and a bench multimeter. Energy consumption measurements have been conducted by using a standard Windows 10 PC during the experiments of data transmission. The power consumed by the USB Wi-Fi adapter has not been included in the computation.

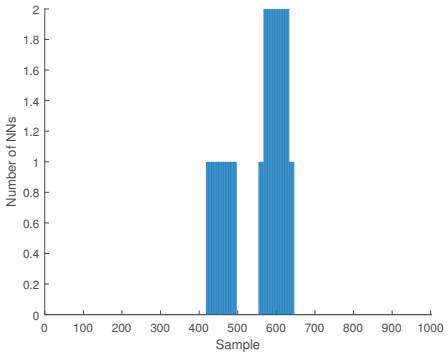

Figure 5.3.2: Illegal NNs detected in localization solution.

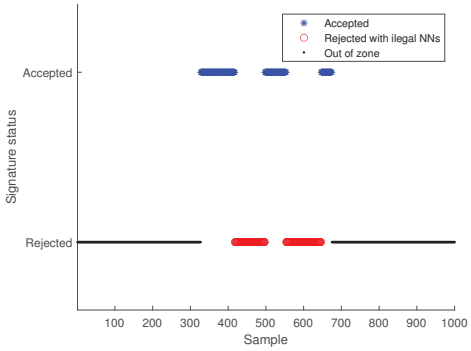

Figure 5.3.3: Illegal NNs detected in localization solution.

The implementations of LSSP and the corresponding DTLS protocols using identical cybersecurity algorithms have been realized with the native Java cryptographic libraries. This step was taken to ensure the validity of the comparison between the different protocols while still providing an identical level of security for the transmitted data. The goal of this experiment was to measure and evaluate the difference in energy consumption between the different protocols while using empirical measurements.

To compare all the protocols under investigation, 10 K of data has been transmitted from the streaming device, and packets have been received by using the Wireshark software at the server device. The total amount of the data that was transmitted over wireless channels has then been computed. Figure 5.4.5 illustrates the obtained results.

This chart considers only the packets that were transferred from the transmission device and ignores the handshake packets that have been employed by the DTLS protocol, that has been transmitted from the server back to their transmission device.

When comparing the obtained results, we can indemnify that LSSP $M1$ modification does not introduce additional data to the transmission and is equivalent to the

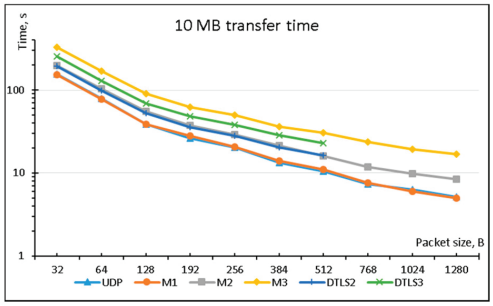

Figure 5.4.1: Time required to transfer 10 MB of data for each of analyzed protocols.

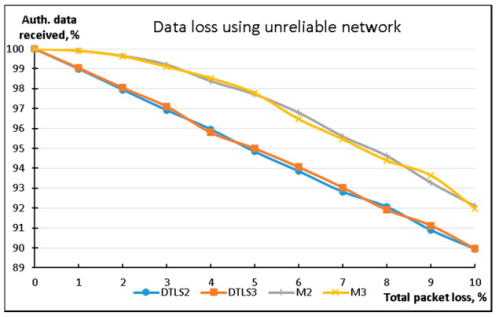

Figure 5.4.2: Experimental results of practical performance in sub optimal network infrastructure.

standard UDP protocol. The additional packets introduced in the LSSP $M2$ and $M3$ modes are used to transmit ECC information for the data that the overhead amounts to 25% in comparison to the $M1$ version of all standard UDP transmissions. The $DTLS2$ and $DTLS3$ versions of the protocol perform the handshaking function (label - DTLS-HS) and introduce the overhead data related to the DTLS protocol in each transmitted packet of data (label - DTLS)

5.5. DISCUSSION ON THE LOCALIZATION RESEARCH

The results presented in the simulation section are a proof-of-concept for an algorithm to study the possibility of LRFs utilization for the positioning purpose inside the IoT network. The simulation has validated the concept of the translation of coordinates between LRFs to achieve a continuous positioning solution for UN. For future work, a comparative analysis between the proposed and centralized positioning algorithms is planned to assess the power and bandwidth requirements for the proposed algorithm. The network did not achieve 100% convergence due to the facts that a), not all randomly placed NN could form LRF and thus could not obtain coordinates relative to other NNs, and b) trajectories of the UNs were linear and not evenly distributed

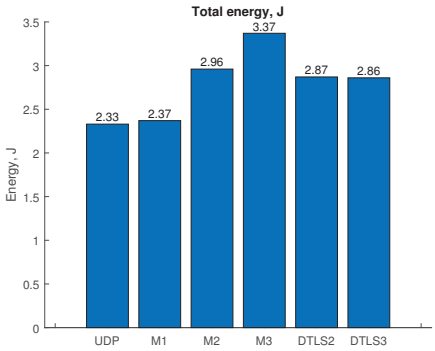

Figure 5.4.3: Experimental results of the energy consumption test.

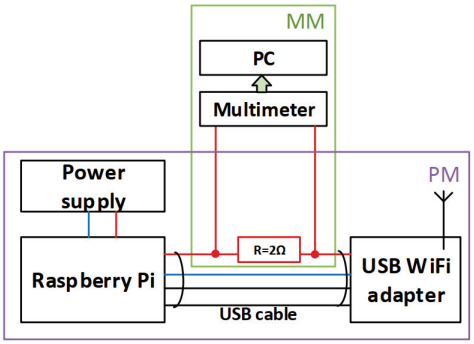

Figure 5.4.4: A setup for power consumption measurements.

throughout the network due to the random nature of their origin and the direction of movement. An actual IoT positioning system would not be limited to several UN appearances, thus the performed simulation presents only a limited view of the system's performance, however, we have simplified it by omitting influences on accuracy from varying noise levels, signal multipath, packet loss and movement of NN, thus such simulation more accurately represents a snapshot of the network convergence, rather than its full functionality. The proposed algorithm would best be deployed in an indoor environment densely populated with IoT NNs. Real-life applications range from localization tasks in industrial environments such as warehouses to indoor/urban canyon settings where GNSS signals are obstructed or outright undetectable.

In real-life applications, such an algorithm would be operational over long periods, gathering additional data from VNNs and improving its positioning solution. The investigation of such influences is reserved for future studies.

The future work also includes the integration of independent measurements in UN, such as inertial navigation, GNSS, and a magnetometer to investigate the possible enhancing effects of these independent measurements and their fusion in a prototype

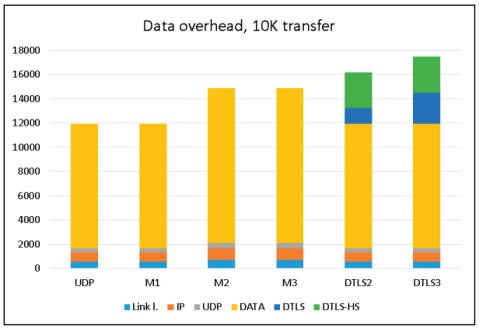

Figure 5.4.5: Experimental results for the comparison of data overhead.

system that will be deployed to evaluate the real-life performance in a noisy environment, to estimate the power consumption and the necessary throughput to achieve seamless positioning for moving UN.

In this thesis, a multimodal identification and authentication method with localization data for the objects of the Internet of Things has been proposed. Localization is realized by employing the RTT ranging measurements. Tetrahedral reference frames comprised of IoT network nodes are used to create local positioning solutions. Virtual network nodes are used to propagate the absolute positioning solution between the local reference frames and achieve network convergence. Sustained operation is achieved by a hybrid control system comprised of a Kalman filter and a Fuzzy logic controller, while adaptively managing power usage for localization and communication tasks. Multiple modes for object identification and authentication are transmitted as a root of a Multimodal hash Tree via a lightweight, secure streaming protocol. The obtained results show that a multimodal object identification and authentication method for IoT objects with localization information can be realized within the envelope of the already existing IoT devices.

5.6. DISCUSSION ON THE POWER MANAGEMENT OF INTERNET OF THINGS DEVICE FOR LOCALIZATION TASKS

This thesis covers the relevant technologies for power management for IoT devices with persistent localization functionality. Technologies related to power generation, localization, and power control have been overviewed and summarized. From the collected material we can perceive some possible permutations of these technologies that can be selected for specific environmental and functional IoT device parameters. A Hybrid Control System consisting of a Kalman filter and a Fuzzy Logic Controller has been designed and stimulated. From the obtained results we can see that the hybrid control system can adapt to the noisy power input signal and distribute power resources to the specified rules.

Figure 5.2.5 shows that the Hybrid Control System can manage the battery power

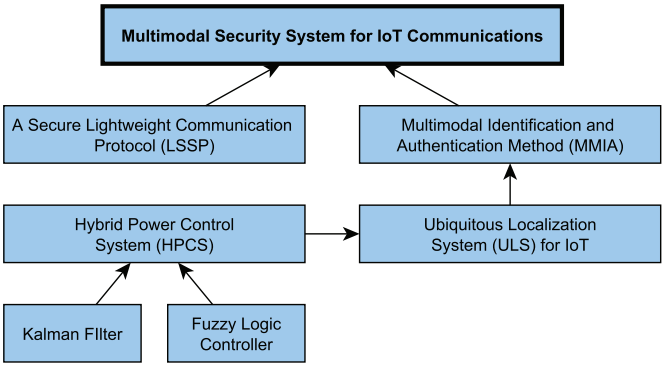

Figure 5.7.1: Relationships between proposed Solutions.

even if the provided power level is noisy and significantly lower than expected from the linear model employed by the Kalman filter.

Figure 5.2.6 represents the estimated improvement in arranging the measurement accuracy. The change in the estimated ranging measurements variance is modeled as a logarithmic function of the total accumulated power. While this model does not capture all the nuances of aggregated accuracy over average results, it is used for illustration purposes.

The designed Hybrid Control System relies on linear models and low dimension matrixes. To compute the Kalman filter estimate, the matrix inversion and multiplication computations must be performed. As the sample rate is set at a $100s$ period, even low computing power IoT devices are capable of performing such computations. Fuzzy logic is also suitable for embedded systems as the outputs are generated from the predetermined linear functions of the inputs.

5.7. DISCUSSION ON LIGHTWEIGHT SECURE STREAMING PROTOCOL

In this thesis, a new lightweight secure streaming protocol (LSSP) for the Fog computing *Fog Node-End Device* layer has been proposed and analyzed. This method is aimed at applications operating at low bandwidth, low resource, packet loss tolerant applications, such as data or video data streaming.

The introduced protocol employs a covert channel-inspired data transmission using UDP packets with authentication information of the data source being included in the headers of the UDP packet. Three different modes of practical implementation were investigated. In the first mode, only the data source authentication information has been used. The second mode integrates both data source authentication and the authentication of the content. The third mode, on top of data source authentication, introduces content data confidentiality. In situations where the network conditions are not ideal, and probable data loss is extensive, the introduction of more redundancy by increasing the number of data packets can be implemented to achieve an increase in the

reliability of the transfer data. Multicasting and broadcasting obligations are suitable for the proposed protocol. Special stages are not a requirement for the network session to be established between the server and the client. The proposed protocol is resilient to the data packet losses introduced by transmission over the network infrastructure.

From the obtained experimental results we can conclude that the proposed protocol operating in Mode 1 modification with the data source authentication functionality has comparable energy consumption characteristics, data overhead, and performance to the UDP protocol.

The introduction of redundant ECC packets into the Mode 2 and Mode 3 variance of the protocol increases the reliability of the data transfer in comparison to the DTLS protocol. The security properties of the proposed protocol and DTLS are comparable. Additionally, the proposed protocol has a lower bandwidth overhead in comparison to DTLS in cases where new connections are required to be frequently re-established. The DTLS protocol suffers from complex handshake procedures and reduces its bandwidth efficiency. In cases when additional ECC packets are being transmitted in the LSSP article protocol, the impact is less severe than that in the DTLS case.

5.8. DISCUSSION ON MULTIMODAL IDENTIFICATION AND AUTHENTICATION METHOD FOR INTERNET OF THINGS DEVICES

The coupling of the standard object identification and authentication methods, such as private keys with the geolocation information, creates an opportunity to have smart authentication methods that can validate not only the transmitter of the data but also some additional parameters, such as the location where the measurements were obtained and the sources were used to generate the geolocation solution. The employment of the Multimodal Identification and Authentication Method and the cryptographic keys of their neighboring IoT nodes, with their geolocation information, can be integrated to achieve even more robust authentication methodologies.

5.9. DISCUSSION ON INTEGRATION OF PROPOSED SOLUTIONS

Figure 5.7.1 depicts the relationship between the proposed solutions and the way they integrate to form a multimodal security system for IoT communications. The software-based Ubiquitous Localization System is enabled by the Hybrid Power Control System. Due to the high power requirements of packet-based ranged measurements, this activity must be managed in IoT devices. The application of the Kalman Filter and a Fuzzy Logic Controller enables persistent localization within the available power consumption and input levels.

As a software solution, the Ubiquitous Localization System (ULS) is designed to enable a variety of IoT devices to take advantage of such functionality. While the packet-based RTT range measurement technology is beyond the scope of this thesis, the proliferation and progression of IoT devices allow us to infer that such capabilities will become available in the near future. The exploitation of LRFs and VNNs

enables the proposed ULS to provide limited functionality even in these areas of the IoT network that does not have an absolute positioning solution.

The Multimodal Identification and Authentication Method uses the localization solution provided by the ULS in MMIA1 mode, and, by employing variable masking of the least significant bits of the UNs coordinates, enables the definition of the geographic zone, from which the received data packets are interpreted as valid. Additionally, the MMIA2 mode can exploit the IDs and the location of the neighboring NNs as an additional security factor. MMIA2 introduces additional computational and memory requirements at the UNs and ends up in hashing those values to form the Root hash, however, they can be reused in whole or in part for subsequent data packets.

The proposed Secure Lightweight Communication Protocol by itself contains identification and authentication features with the optional data encryption in the M3 mode. It is created to generate a secure singlecast, multicast, or broadcast communication in scenarios with limited power and bandwidth resources. When coupled together with MMIA, they form the proposed Multimodal Security System for IoT Communications.

5.10. FUTURE WORKS

The obtained results from the validation of the distributed localization algorithm are promising. The network convergence level on average exceeded 70% with only 4 traversals via random linear trajectories. The average positioning error decreased below $2m$. We can conclude that the residual error is mainly influenced by the noise in the ranging measurements and the sub-optimal geometry in the randomly generated placements of the NNs. Due to the current limitations of hardware and methods, sufficiently precise RTT ranging measurements cannot be realized with off-the-shelf IoT equipment. Future works for the development of advanced measurement processing are envisioned to fill this gap. The proposed localization method does not include any kinematic prediction model. A possible future improvement is the application of a linear or extended Kalman filter at a cost of increased computational complexity. The benefits of such an upgrade need to be weighed against the requirements for computing and power resources.

A hybrid control system has been tested over a number of simulations. It was able to manage the power resources adequately and maintain functionality throughout the parameter envelope. If the power input levels were reduced below the functional threshold, localization functionality could only be maintained if the ranging measurement with different NNs could be spread out through the samples and integrated over time into a single solution. Such functionality was investigated but is beyond the scope of the thesis. The Fuzzy Logic controller tended to prefer NNs with the lowest variance level in the ranging measurements and prioritized them over others. The creation of a more flexible rule-set focused on developing alternative ranging sources when there is available power is an obvious possible improvement.

The multimodal IoT object identification and authentication method have suc-

cessfully achieved the required functionality. Possible enhancements for the method include asymmetrical encryption of the NNs IDs to increase the level of privacy. Alternatively, privacy-preserving authentication methods could be investigated.

LSSP has been proposed in three modes of increasing functionality and, with it, associated overhead in power and compute consumption. Investigation into more advanced cryptographic methods might be warranted to trade-off between these costs and introduce additional functionality such as privacy-preserving authentication.

5.11. CONCLUSIONS FOR THE RESULTS AND DISCUSSION CHAPTER

To conclude the results and discussion chapter, we refer back to the criteria that have been established in Chapter 2. The proposed Multimodal Security System for IoT Communications is suited for extensive deployment. For it to achieve its full potential, as many as possible IoT devices should incorporate it into the firmware.

Fulfillment of the localization solution criteria

Distributed algorithm – the proposed algorithm has been shown to enable the convergence of the simulated three-dimensional ad hoc IoT network. The convergence level improves over time with the additional iterations where mobile UNs traverse the area. We conclude that the criteria of distribution have been satisfied.

Software solution – the localization and the convergence of the network has been realized by using the simulated communication between IoT nodes, thus we conclude that the proposed solution does not require additional hardware, given if packet based RRT ranging measurements are available.

Zone convergence – during the simulation, the increase in network convergence over the subsequent iterations reveals that additional zones of the network can converge to the absolute positioning solution and provide localization functionality without the requirement of full network convergence. We consider zone convergence criteria to be fulfilled.

No *a priori* data – validation of the algorithm has been conducted without any prior localization information for the NNs, thus we consider this criterion to be fulfilled and the algorithm to be capable to function in *ad hoc* networks.

Integration of external solutions – network convergence from LRFs to the absolute positioning solution demonstrated that the integration of external positioning solutions such as GNSS is feasible. We consider this criterion to be fulfilled.

When comparatively analyzing the proposed localization algorithm with the published alternatives, that have been presented in Table 2.1 we can conclude that it satisfies distributed architecture, software solution, ability to converge in zones, and the lack of *a priori* data to achieve localization solution. The estimated accuracy is in on par with alternative ToA-based localization solutions and is mainly influenced by the

accuracy of the ranging measurements. It is noteworthy to mention that the proposed localization algorithm has been published in 2017 and developments in the field of IoT localization have been advancing.

Fulfillment of the Power Management System criteria

Adaptive – during the validation, the HCS has demonstrated the capability to adjust to both noisy power inputs and achieve persistent functionality over the 24h window, with the remaining power level at the end of the period equal to that of the start of the period. This demonstrates that the adaptability criterion is fulfilled.

Intermittent power sources – the designed HCS was able to manage power usage in accordance with the provided Solar power input model. We consider this criterion to be fulfilled.

Can distribute power to the most beneficial measurements – HCS was able to select the appropriate number of NNs for localization tasks and managed to direct the allocated energy resources towards the measurements with the lowest variance, while at the same time improving their estimate through the averaging of multiple measurements. We consider this criterion to be fulfilled.

When comparatively analyzing the proposed power management system with the published alternatives, that have been presented in Table 2.2 we can conclude that typically power control systems are designed for specific applications, and management of power for localization over communication channel was yet to be proposed.

Fulfillment of the identification and authentication criteria

Identification and authentication – the proposed MMIA method integrates encryption with an asymmetric cryptographic key and UNs localization information. Identification via the combination of a digital signature and the location data synergizes into a more robust security solution. We consider this criterion to be fulfilled.

Integration of the geographic zone – the size of the geographic area by masking the least significant bits of the coordinates ensures that the output of the SHA256 hash function is identical within that zone. We consider this criterion to be fulfilled.

Integration of encryption – the echolocation and digital signature parameters are protected by using the asymmetric encryption, and the private key is not transmitted over the IoT network. We consider this criterion to be fulfilled.

Scalable secondary parameters – the ability to add the hashed values of the neighboring NNs IDs and their location data provides an increased number of parameters and enables whitelisting/blacklisting of NNs by their reliability and trustworthiness. We consider this criterion to be fulfilled.

When comparatively analyzing the proposed multimodal security solution with

the published alternatives, that have been presented in Table 2.3 we can conclude that the multimodal approach has recently been adopted in IoT research, however, the most common approach is the incorporation of a couple of fixed parameters, without the ability to scale. In this context, the multimodal security solution with MAST has significantly more functionality as it can incorporate a varying number of parameters in MMIA2 mode.

Fulfillment of the communication protocol criteria

Multicasting/Broadcasting – the proposed LSSP protocol uses a modified UDP header and can provide source authentication without the need for a handshake, thus we consider the criteria for multicasting and broadcasting modes to be fulfilled.

Distinct modes – the proposed method has been implemented and tested in three distinct modes, with differing requirements and capabilities. We consider this criterion to be fulfilled.

Identification and authentication – LSSP mode 1 provides device identification and authentication through the digital signature. We consider this criterion to be fulfilled.

Data encryption – LSSP mode 3 provides data encryption capability. We consider this criterion to be fulfilled.

When comparatively analyzing the proposed LSSP with the published alternatives, that have been presented in Table 2.4 we can conclude that LSSP satisfies 4 out of 5 criteria, namely: Confidentiality, Integrity, Authentication, and absence of key exchange. It is noteworthy to mention that LSSP has been published in 2018 and developments in the field of lightweight secure IoT protocols have been advancing.

Conclusions

This chapter provides conclusions in relation to the body of work that has been conducted for this PhD thesis.

1. A distributed localization method based on RTT ranging measurements for ad hoc IoT networks has been created. The distributed nature of the method allows it to be deployed seamlessly with no prior knowledge of the IoT network's node's location. During the validation in simulation, it has been shown that it can operate with full or partial network convergence, where pockets of the network obtain the absolute positioning solution, while those isolated or lacking sufficient connectivity operate in the local reference frame mode. With 8 iterations of pass-through with linear trajectories, the simulated network has achieved 74% convergence level and an average positioning error of $1.9m$. The introduction of virtual network nodes allows the propagation of the absolute positioning solution over time with the measurements of opportunity.

2. A specialized hybrid control system has been developed to manage power consumption for localization and communication tasks. The validation of the system shows that it can distribute the available power based on the expected power input, the current battery level, and the quality and number of the available RTT measurements. The proposed Kalman filter can distribute power over the $24h$ window with 50% battery reserves remaining to be used for the next day. The Fuzzy Logic Controller on average selected 4 NNs for ranging measurements with their ranging estimate variance being reduced to an average $0.1m$. over 900 samples.

3. Two versions of the Multimodal Identification and Authentication Method: *MMIA1* and *MMIA2* have been proposed. *MMIA1* provides identification and authentication via a digital signature and the geolocation root hash of a MAST tree. It can be obtained by the application of the hashing function three times and a single application of the encryption function on the generated hash. *MMIA2* additionally includes IDs and geolocation hashes of the IoT network nodes that have been used in obtaining localization solutions. Both proposed variants of the method result in the same sized root hash, however, the second variant requires additional hashing calculation on the part of the IoT network node. During the

validation phase, *MMIA2* has successfully eliminated samples that used undesirable NNs for the geolocation solution generation 100% of the time.

4. A lightweight secure streaming protocol has been designed and proposed to be employed for data streaming from IoT devices. Three security modes were defined. Mode 1 provides the authentication of the data source. Mode 2 adds data integrity. Mode 3 adds confidentiality features. Through empirical experimentation, it has been shown that the M1 protocol has a comparative performance to the UDP protocol with the bonus of authentication functionality, with the $0.5s$ difference in the transmission time due to the processing requirements, and it requires a modest 2% increase in the total power. The proposed M2 protocol in comparison to DTLS2 provides similar performance and similar source authentication properties and requires a 3% increase in the total power over the DTLS2. The proposed M3 protocol is slower in comparison to DTLS3 due to additional data packets containing ECC information. M3 protocol requires additional 18% total energy in comparison to DTLS3. Since LSSP was published in 2018, IoT security has increasingly come into the focus of the research community, and improvements have been made as detailed in section 5.11. Nonetheless, LSSP stands as a viable choice due to its set of features and performance.

5. The combination of the proposed methods provides a set of solutions that can be combined into a practical localization-based multimodal security system for IoT. At this stage, the limiting factor is the accuracy of the RTT ranging measurements that can be achieved with the current methods and hardware. Additional research into the possible solutions to enhance the available measurement accuracy is required, but it is beyond the scope of this thesis.

Bibliography

A HASSEN, Oday; A ABDULHUSSEIN, Ansam; M DARWISH, Saad; OTHMAN, Zulaiha Ali; TIUN, Sabrina; A LOTFY, Yasmin, 2020. Towards a secure signature scheme based on multimodal biometric technology: application for IOT Blockchain network. *Symmetry*. Vol. 12, no. 10, p. 1699.

ABBASINEZHAD-MOOD, Dariush; NIKOOGHADAM, Morteza, 2018. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems*. Vol. 84, pp. 47–57.

ABOMHARA, Mohamed; KØIEN, Geir M, 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pp. 65–88.

AERNOUTS, Michiel; LEMIC, Filip; MOONS, Bart; FAMAEY, Jeroen; HOEBEKE, Jeroen; WEYN, Maarten; BERKVENS, Rafael, 2020. A multimodal localization framework design for iot applications. *Sensors*. Vol. 20, no. 16, p. 4622.

AGARWAL, Vidushi; PAL, Sujata, 2020. Blockchain meets IoT: a scalable architecture for security and maintenance. In: *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, pp. 53–61.

AIREHROUR, David; GUTIERREZ, Jairo; RAY, Sayan Kumar, 2016. Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. In: *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, pp. 115–120.

AL-SARAWI, Shadi; ANBAR, Mohammed; ALIEYAN, Kamal; ALZUBAIDI, Mahmood, 2017. Internet of Things (IoT) communication protocols. In: *2017 8th International conference on information technology (ICIT)*. IEEE, pp. 685–690.

ALARIFI, Abdulaziz; SANKAR, Syam; ALTAMEEM, Torki; JITHIN, K. C.; AMOON, Mohammed; EL-SHAFAI, Walid, 2020. A Novel Hybrid Cryptosystem for Secure Streaming of High Efficiency H.265 Compressed Videos in IoT Multimedia Applications. *IEEE Access*. Vol. 8, pp. 128548–128573. Available from DOI: 10.1109/ACCESS.2020.3008644.

ASAAD, Safar M; MAGHDID, Halgurd S, 2022. A Comprehensive Review of Indoor/Outdoor Localization Solutions in IoT era: Research Challenges and Future Perspectives. *Computer Networks*, p. 109041.

ASHTON, Kevin et al., 2009. That 'internet of things' thing. *RFID journal*. Vol. 22, no. 7, pp. 97–114.

BAGDONAS, Kazimieras; BORRE, Kai, 2008. Ubiquitous WiFi/GNSS positioning system-TOA based distance estimation. In: *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pp. 1773–1779.

BAGDONAS, Kazimieras; JUSAS, Nerijus; VENCKAUSKAS, Algimantas, 2017. A Converging Distributed Positioning Algorithm for Internet-of-Things. *Elektronika ir Elektrotechnika*. Vol. 23, no. 6, pp. 72–76.

BAGDONAS, Kazimieras; SCHIØLER, Henrik; BORRE, Kai, 2009. Range estimation for indoor positioning via drifting clocks. In: *Proceedings of the 22nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2009)*, pp. 516–526.

BAROT, Virendra; KAPADIA, Viral; PANDYA, Sharnil, 2020. QoS enabled IoT based low cost air quality monitoring system with power consumption optimization. *Cybernetics and Information Technologies*. Vol. 20, no. 2, pp. 122–140.

BLAZQUEZ, Alberto; TSIATSIS, Vlasios; VANDIKAS, Konstantinos, 2015. Performance evaluation of openid connect for an iot information marketplace. In: *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, pp. 1–6.

BONOMI, Flavio; MILITO, Rodolfo; ZHU, Jiang; ADDEPALLI, Sateesh, 2012. Fog computing and its role in the internet of things. In: *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13–16.

BOUET, Mathieu; DOS SANTOS, Aldri L, 2008. RFID tags: Positioning principles and localization techniques. In: *2008 1st IFIP Wireless Days*. Ieee, pp. 1–5.

BOUNCY CASTLE INC., Legion of the, 2018. *BC-FJA (Bouncy Castle FIPS Java API) User Guide*. [`https://downloads.bouncycastle.org/fips-java/BC-FJA-SecurityPolicy-1.0.0.pdf`]. Accessed: 2018-03-08.

BRANICKY, Michael S; BORKAR, Vivek S; MITTER, Sanjoy K, 1998. A unified framework for hybrid control: Model and optimal control theory. *IEEE transactions on automatic control*. Vol. 43, no. 1, pp. 31–45.

CARVALHO SILVA, Jonathan de; RODRIGUES, Joel JPC; ALBERTI, Antonio M; SOLIC, Petar; AQUINO, Andre LL, 2017. LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities. In: *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*. IEEE, pp. 1–6.

CHAE, Cheol-Joo; CHOI, Kwang-Nam; CHOI, Kiseok; YAE, Yong-Hee; SHIN, YounJu, 2015. The extended authentication protocol using e-mail authentication in OAuth 2.0 protocol for secure granting of user access. *Journal of Internet Computing and Services*. Vol. 16, no. 1, pp. 21–28.

CHAN, Aldar C-F; ZHOU, Jianying, 2014. Cyber–physical device authentication for the smart grid electric vehicle ecosystem. *IEEE Journal on Selected Areas in Communications*. Vol. 32, no. 7, pp. 1509–1517.

CHAN, Wai Kok; CHIN, Ji-Jian; GOH, Vik Tor, 2021. Bitcoin Addresses. Scaling, Migration and Payment Perspectives.

CHEN, Liang; THOMBRE, Sarang; JÄRVINEN, Kimmo; LOHAN, Elena Simona; ALÉN-SAVIKKO, Anette; LEPPÄKOSKI, Helena; BHUIYAN, M Zahidul H; BU-PASHA, Shakila; FERRARA, Giorgia Nunzia; HONKALA, Salomon, et al., 2017. Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access*. Vol. 5, pp. 8956–8977.

CHEN, Xi; MA, Ming; LIU, Anfeng, 2018. Dynamic power management and adaptive packet size selection for IoT in e-Healthcare. *Computers & Electrical Engineering*. Vol. 65, pp. 357–375.

COSTA, Daniel G; SILVA, Ivanovitch; GUEDES, Luiz Affonso; VASQUES, Francisco; PORTUGAL, Paulo, 2014. Availability issues in wireless visual sensor networks. *Sensors*. Vol. 14, no. 2, pp. 2795–2821.

DAR, Kashif; TAHERKORDI, Amirhosein; ROUVOY, Romain; ELIASSEN, Frank, 2011. Adaptable service composition for very-large-scale internet of things systems. In: *Proceedings of the 8th Middleware Doctoral Symposium*, pp. 1–6.

DE CARO, Niccolò; COLITTI, Walter; STEENHAUT, Kris; MANGINO, Giuseppe; REALI, Gianluca, 2013. Comparison of two lightweight protocols for smartphone-based sensing. In: *2013 IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*. IEEE, pp. 1–6.

DEGRAAF, Rennie; AYCOCK, John; JACOBSON, Michael, 2005. Improved port knocking with strong authentication. In: *21st Annual Computer Security Applications Conference (ACSAC'05)*. IEEE, 10–pp.

EL-HAJJ, Mohammed; FADLALLAH, Ahmad; CHAMOUN, Maroun; SERHROUCHNI, Ahmed, 2019. A survey of internet of things (IoT) authentication schemes. *Sensors*. Vol. 19, no. 5, p. 1141.

ETIABI, Yaya; AMHOUD, El Mehdi; SABIR, Essaid, 2020. A distributed and collaborative localization algorithm for internet of things environments. In: *Proceedings of the 18th International Conference on Advances in Mobile Computing & Multimedia*, pp. 114–118.

FAIRHURST, Gorry; TRAMMELL, Brian; KÜHLEWIND, Mirja, 2017. Services provided by IETF transport protocols and congestion control mechanisms. *RFC Series*. Vol. 8095.

FRACZEK, Wojciech; MAZURCZYK, Wojciech; SZCZYPIORSKI, Krzysztof, 2011. How hidden can be even more hidden? In: *2011 Third International Conference on Multimedia Information Networking and Security*. IEEE, pp. 581–585.

FRĄCZEK, Wojciech; MAZURCZYK, Wojciech; SZCZYPIORSKI, Krzysztof, 2012. Multi-level steganography: Improving hidden communication in networks. *Journal of Universal Computer Science (J. UCS)*. Vol. 18, no. 14, pp. 1967–1986.

GIANNOULIS, S; ANTONOPOULOS, C; TOPALIS, E; ATHANASOPOULOS, A; PRAYATI, A; KOUBIAS, S, 2009. TCP vs. UDP performance evaluation for CBR traffic on wireless multihop networks. *Simulation*. Vol. 14, p. 43.

GLISSA, Ghada; MEDDEB, Aref, 2019. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*. Vol. 82, pp. 100–112.

GOODWIN, Graham C; GRAEBE, Stefan F; SALGADO, Mario E, et al., 2001. *Control system design*. Upper Saddle River, NJ: Prentice Hall.

GOPINATH, T; KUMAR, AS Rathan; SHARMA, Rinki, 2013. Performance evaluation of TCP and UDP over wireless ad-hoc networks with varying traffic loads. In: *2013 International Conference on Communication Systems and Network Technologies*. IEEE, pp. 281–285.

GRASSI, Paul; GARCIA, Michael; FENTON, James, 2020. *Digital identity guidelines*. Tech. rep. National Institute of Standards and Technology.

GRESSMANN, Björn; KLIMEK, Helge; TURAU, Volker, 2010. Towards ubiquitous indoor location based services and indoor navigation. In: *2010 7th Workshop on Positioning, Navigation and Communication*. IEEE, pp. 107–112.

GREWAL, Mohinder S; ANDREWS, Angus P, 2014. *Kalman filtering: Theory and Practice with MATLAB*. John Wiley & Sons.

GROVES, Paul D, 2015. Principles of GNSS, inertial, and multisensor integrated navigation systems, [Book review]. *IEEE Aerospace and Electronic Systems Magazine*. Vol. 30, no. 2, pp. 26–27.

GUBBI, Jayavardhana; BUYYA, Rajkumar; MARUSIC, Slaven; PALANISWAMI, Marimuthu, 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*. Vol. 29, no. 7, pp. 1645–1660.

GUO, Guangyi; CHEN, Ruizhi; YE, Feng; PENG, Xuesheng; LIU, Zuoya; PAN, Yuanjin, 2019. Indoor smartphone localization: A hybrid WiFi RTT-RSS ranging approach. *IEEE Access*. Vol. 7, pp. 176767–176781.

HAMMING, Richard W, 1950. Error detecting and error correcting codes. *The Bell system technical journal*. Vol. 29, no. 2, pp. 147–160.

HAMOUDY, Mina A; QUTQUT, Mahmoud H; ALMASALHA, Fadi, 2017. Video security in Internet of things: an overview. *IJCSNS*. Vol. 17, no. 8, p. 199.

HAMOUID, Khaled; OMAR, Mawloud; ADI, Kamel, 2021. A Privacy-Preserving Authentication Model Based on Anonymous Certificates in IoT. In: *2021 Wireless Days (WD)*. IEEE, pp. 1–6.

HARIPRIYA, AP; KULOTHUNGAN, K, 2019. Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP Journal on Wireless Communications and Networking*. Vol. 2019, no. 1, pp. 1–15.

HEMMINGER, Stephen et al., 2005. Network emulation with NetEm. In: *Linux conf au*. Citeseer. Vol. 5, p. 2005.

HERNANDEZ, Grant; ARIAS, Orlando; BUENTELLO, Daniel; JIN, Yier, 2014. Smart nest thermostat: A smart spy in your home. *Black Hat USA*.

HERRERO, Rolando, 2020. Analysis of IoT mechanisms for media streaming. *Internet of Things*. Vol. 9, p. 100168.

HUANG, Yanqiu; YU, Wanli; DING, Enjie; GARCIA-ORTIZ, Alberto, 2019. EPKF: Energy efficient communication schemes based on Kalman filter for IoT. *IEEE Internet of Things Journal*. Vol. 6, no. 4, pp. 6201–6211.

HUSAMUDDIN, Md; QAYYUM, Mohammed, 2017. Internet of Things: A study on security and privacy threats. In: *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. IEEE, pp. 93–97.

ISHENGOMA, Fredrick R, 2014. The art of data hiding with reed-solomon error correcting codes. *arXiv preprint arXiv:1411.4790*.

ISLAM, Md Nazmul; PATIL, Vinay C; KUNDU, Sandip, 2017. Determining proximal geolocation of IoT edge devices via covert channel. In: *2017 18th International Symposium on Quality Electronic Design (ISQED)*. IEEE, pp. 196–202.

JANSMA, Nicholas; ARRENDONDO, Brandon, 2004. Performance comparison of elliptic curve and rsa digital signatures. *nicj. net/files*.

JEONG, Min-Hyuk; KIM, Sang-Kyun, 2022. Video Streaming Based on Blockchain State Channel with IoT Camera. *Journal of Web Engineering*, pp. 661–676.

JIN, Shuanggen, 2012. *Global navigation satellite systems: signal, theory and applications*. BoD–Books on Demand.

JOHNSON, Don; MENEZES, Alfred; VANSTONE, Scott, 2001. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*. Vol. 1, no. 1, pp. 36–63.

KERRY, Cameron F; DIRECTOR, Charles Romine, 2013. FIPS PUB 186-4 federal information processing standards publication digital signature standard (DSS).

KESAVAN GOPAL, DMM, 2010. Watermarking of digital video stream for source authentication. *IJCSI Int. J. Comput. Sci*, p. 7.

KHAN, Fasih Ullah; AWAIS, Muhammad; RASHEED, Muhammad Babar; MASOOD, Bilal; GHADI, Yazeed, 2021. A Comparison of Wireless Standards in IoT for Indoor Localization Using LoPy. *IEEE Access*. Vol. 9, pp. 65925–65933.

KHAN, Wali Ullah; JAMEEL, Furqan; JAMSHED, Muhammad Ali; PERVAIZ, Haris; KHAN, Shafiullah; LIU, Ju, 2020. Efficient power allocation for NOMA-enabled IoT networks in 6G era. *Physical Communication*. Vol. 39, p. 101043.

KIM, Jongkil; CAMTEPE, Seyit; SUSILO, Willy; NEPAL, Surya; BAEK, Joonsang, 2019. Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing. In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 55–66.

KLIR, George; YUAN, Bo, 1995. *Fuzzy sets and fuzzy logic*. Vol. 4. Prentice hall New Jersey.

KOTENKO, Igor; SAENKO, Igor; AGEEV, Sergey, 2015. Countermeasure security risks management in the internet of things based on fuzzy logic inference. In: *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE. Vol. 1, pp. 654–659.

KOTHMAYR, Thomas; SCHMITT, Corinna; HU, Wen; BRÜNIG, Michael; CARLE, Georg, 2013. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*. Vol. 11, no. 8, pp. 2710–2723.

KRAMER, Bernhard; MACKINNON, Angus, 1993. Localization: theory and experiment. *Reports on Progress in Physics*. Vol. 56, no. 12, p. 1469.

KUMAR, Sudhir; DAS, Sajal K., 2020. Target Detection and Localization Methods Using Compartmental Model for Internet of Things. *IEEE Transactions on Mobile Computing*. Vol. 19, no. 9, pp. 2234–2249. Available from DOI: 10.1109/TMC.2019.2921537.

Legion of the Bouncy Castle Inc. Java (D)TLS API and JSSE Provider. User Guide. 2018 [https://downloads.bouncycastle.org/fips-java/BC-FJA-(D)TLSUserGuide-1.0.3.pdf]. Accessed: 2018-03-08.

LI, You; ZHUANG, Yuan; HU, Xin; GAO, Zhouzheng; HU, Jia; CHEN, Long; HE, Zhe; PEI, Ling; CHEN, Kejie; WANG, Maosong, et al., 2020. Toward location-enabled IoT (LE-IoT): IoT positioning techniques, error sources, and error mitigation. *IEEE Internet of Things Journal*. Vol. 8, no. 6, pp. 4035–4062.

LIN, Kai; CHEN, Min; DENG, Jing; HASSAN, Mohammad Mehedi; FORTINO, Giancarlo, 2016. Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings. *IEEE Transactions on Automation Science and Engineering*. Vol. 13, no. 3, pp. 1294–1307.

LIU, Hui; DARABI, Houshang; BANERJEE, Pat; LIU, Jing, 2007. Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. Vol. 37, no. 6, pp. 1067–1080.

LUO, Xi; YIN, Lihua; LI, Chao; WANG, Chonghua; FANG, Fuyang; ZHU, Chunsheng; TIAN, Zhihong, 2020. A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access*. Vol. 8, pp. 67192–67204.

MA, Tianchen, 2020. White-box Schnorr Signature for Internet of Things Security. In: *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*. IEEE, pp. 1939–1942.

MACAGNANO, Davide; DESTINO, Giuseppe; ABREU, Giuseppe, 2014. Indoor positioning: A key enabling technology for IoT applications. In: *2014 IEEE World Forum on Internet of Things (WF-IoT)*. IEEE, pp. 117–118.

MAHMOOD, Khalid; CHAUDHRY, Shehzad Ashraf; NAQVI, Husnain; KUMARI, Saru; LI, Xiong; SANGAIAH, Arun Kumar, 2018. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*. Vol. 81, pp. 557–565.

MAHMOUD, Rwan; YOUSUF, Tasneem; ALOUL, Fadi; ZUALKERNAN, Imran, 2015. Internet of things (IoT) security: Current status, challenges and prospective measures. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 336–341.

MAJEED, Russel R; ALKHAFAJI, Sarmad KD, 2022. ECG classification system based on multi-domain features approach coupled with least square support vector machine (LS-SVM). *Computer Methods in Biomechanics and Biomedical Engineering*, pp. 1–8.

MAO, Guoqiang; FIDAN, Barış; ANDERSON, Brian DO, 2007. Wireless sensor network localization techniques. *Computer networks*. Vol. 51, no. 10, pp. 2529–2553.

MAYER, Philipp; MAGNO, Michele; BENINI, Luca, 2020. Smart power unit—mW-to-nW power management and control for self-sustainable IoT devices. *IEEE Transactions on Power Electronics*. Vol. 36, no. 5, pp. 5700–5710.

MIESSLER, Daniel, 2014. HP study reveals 70 percent of internet of things devices vulnerable to attack. *Retrieved June*. Vol. 30, p. 2015.

MPEIS, Paschalis; ROUSSEL, Thierry; KUMAR, Manish; COSTA, Constantinos; LAOUDIASDENIS, Christos; CAPOT-RAY, Denis; ZEINALIPOUR-YAZTI, Demetrios, 2020. The anyplace 4.0 IoT localization architecture. In: *2020 21st IEEE International Conference on Mobile Data Management (MDM)*. IEEE, pp. 218–225.

MUKHERJEE, Amitav, 2015. Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*. Vol. 103, no. 10, pp. 1747–1761.

MURPHY, William; HEREMAN, Willy, 1995. Determination of a position in three dimensions using trilateration and approximate distances. *Department of Mathematical and Computer Sciences, Colorado School of Mines, Golden, Colorado, MCS-95*. Vol. 7, p. 19.

NABUSOBA, Joan; OTIENO, Calvins; CHERUIYOT, Wilson, 2020. MAAMSIC: Multimodal Authentication and Authorization Model for Security of IoT Communication via GSM Messaging in Sub-Saharan Africa. In: *International Conference on Soft Computing and Pattern Recognition*. Springer, pp. 911–920.

NICULESCU, Dragoş; NATH, Badri, 2004. Error characteristics of ad hoc positioning systems (APS). In: *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pp. 20–30.

OBEIDAT, Huthaifa; SHUAIEB, Wafa; OBEIDAT, Omar; ABD-ALHAMEED, Raed, 2021. A review of indoor localization techniques and wireless technologies. *Wireless Personal Communications*, pp. 1–39.

OH, JiHyeon; YU, SungJin; LEE, JoonYoung; SON, SeungHwan; KIM, MyeongHyun; PARK, YoungHo, 2021. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors*. Vol. 21, no. 4, p. 1488.

OLAZABAL, Oscar; GOFMAN, Mikhail; BAI, Yu; CHOI, Yoonsuk; SANDICO, Noel; MITRA, Sinjini; PHAM, Kevin, 2019. Multimodal biometrics for enhanced iot security. In: *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. IEEE, pp. 0886–0893.

OTSASON, Veljo; VARSHAVSKY, Alex; LAMARCA, Anthony; DE LARA, Eyal, 2005. Accurate GSM indoor localization. In: *International conference on ubiquitous computing*. Springer, pp. 141–158.

PAKANATI, Chennareddy; PADMAVATHAMMA, M; REDDY, N Ramanjaneya, 2015. Performance comparison of tcp, udp, and tfrc in wired networks. In: *2015 IEEE International Conference on Computational Intelligence & Communication Technology*. IEEE, pp. 257–263.

Performance of checksums and CRCs over real data, 1998. *IEEE/ACM Transactions on Networking*. Vol. 6, no. 5, pp. 529–543.

PERRIG, Adrian; CANETTI, Ran; SONG, Dawn; TYGAR, J Doug, 2001. Efficient and secure source authentication for multicast. In: *Network and Distributed System Security Symposium, NDSS*. Vol. 1, pp. 35–46.

PRERADOVIC, Stevan; BALBIN, Isaac; KARMAKAR, Nemai Chandra; SWIEGERS, Gerhard F, 2009. Multiresonator-based chipless RFID system for low-cost item tracking. *IEEE Transactions on Microwave Theory and Techniques*. Vol. 57, no. 5, pp. 1411–1419.

RABAEY, C Savarese J; LANGENDOEN, Koen, et al., 2002. Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In: *USENIX technical annual conference*, pp. 317–327.

RAHMAN, Abdur; ROY, Shanto; KAISER, M Shamim; ISLAM, Md. Shahidul, 2018. A Lightweight Multi-tier S-MQTT Framework to Secure Communication between low-end IoT Nodes. In: *2018 5th International Conference on Networking, Systems and Security (NSysS)*, pp. 1–6. Available from DOI: 10.1109/NSysS.2018.8631379.

RAJABOINA, RajaSekhar; REDDY, P Chenna; KUMAR, Raja Ashok; VENKATRAMANA, Nangil, 2016. Performance comparison of TCP, UDP and TFRC in static wireless environment. *International Journal of Information and Computer Security*. Vol. 8, no. 2, pp. 158–180.

REED, Irving S; SOLOMON, Gustave, 1960. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*. Vol. 8, no. 2, pp. 300–304.

RIVEST, Ronald L; SHAMIR, Adi; ADLEMAN, Leonard, 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. Vol. 21, no. 2, pp. 120–126.

ROMAN, Rodrigo; LOPEZ, Javier; MAMBO, Masahiro, 2018. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*. Vol. 78, pp. 680–698.

SAFAVI, Sam; KHAN, Usman A; KAR, Soummya; MOURA, José MF, 2018. Distributed localization: A linear theory. *Proceedings of the IEEE*. Vol. 106, no. 7, pp. 1204–1223.

SAVVIDES, Andreas; HAN, Chih-Chieh; STRIVASTAVA, Mani B, 2001. Dynamic fine-grained localization in ad-hoc networks of sensors. In: *Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 166–179.

SCHNORR, Claus-Peter, 1991. Efficient signature generation by smart cards. *Journal of cryptology*. Vol. 4, no. 3, pp. 161–174.

SEURIN, Yannick, 2012. On the exact security of schnorr-type signatures in the random oracle model. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, pp. 554–571.

SHA, Kewei; YANG, T Andrew; WEI, Wei; DAVARI, Sadegh, 2020. A survey of edge computing-based designs for IoT security. *Digital Communications and Networks*. Vol. 6, no. 2, pp. 195–202.

SHANG, Yi; SHI, Hongchi; AHMED, Ahmed A, 2004. Performance study of localization methods for ad-hoc sensor networks. In: *2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE Cat. No. 04EX975)*. IEEE, pp. 184–193.

SHARMA, Neerav; GARG, Rahul Dev, 2022. Cost reduction for advanced driver assistance systems through hardware downscaling and deep learning. *Systems Engineering*. Vol. 25, no. 2, pp. 133–143.

SICARI, Sabrina; RIZZARDI, Alessandra; GRIECO, Luigi Alfredo; COEN-PORISINI, Alberto, 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*. Vol. 76, pp. 146–164.

STOJMENOVIC, Ivan; WEN, Sheng; HUANG, Xinyi; LUAN, Hao, 2016. An overview of fog computing and its security issues. *Concurrency and Computation: Practice and Experience*. Vol. 28, no. 10, pp. 2991–3005.

SUÁREZ-ALBELA, Manuel; FERNÁNDEZ-CARAMÉS, Tiago M; FRAGA-LAMAS, Paula; CASTEDO, Luis, 2017. A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications. *Sensors*. Vol. 17, no. 9, p. 1978.

SUGANO, Masashi; KAWAZOE, Tomonori; OHTA, Yoshikazu; MURATA, Masayuki, 2006. Indoor Localization System using RSSI Measurement of Wireless Sensor Network based on ZigBee Standard. *Wireless and Optical Communications*. Vol. 538, pp. 1–6.

SUNDHARI, RP Meenaakshi; JAIKUMAR, K, 2020. IoT assisted Hierarchical Computation Strategic Making (HCSM) and Dynamic Stochastic Optimization Technique (DSOT) for energy optimization in wireless sensor networks for smart city monitoring. *Computer Communications*. Vol. 150, pp. 226–234.

TANGADE, Shrikant; MANVI, Sunilkumar S, 2016. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In: *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, pp. 1–6.

TEAM, The Tcpdump, [n.d.]. *Tcpdump & Libpcap*. [`http://www.tcpdump.org/`]. Accessed: 2018-03-08.

TECHNOLOGIES, Sly, 2018. *jNetPcap API*. [`http://jnetpcap.com`]. Accessed: 2018-03-08.

TRAN, An Thien; PALACIOS, Ricardo Colomo, 2016. A Systematic Literature Review of Fog Computing. In: *Norsk konferanse for organisasjoners bruk at IT*. Vol. 24.

TUYLS, Pim; BATINA, Lejla, 2006. RFID-tags for anti-counterfeiting. In: *Cryptographers' track at the RSA conference*. Springer, pp. 115–131.

USMAN, Muhammad; JAN, Mian Ahmad; HE, Xiangjian; NANDA, Priyadarsi, 2016. Data sharing in secure multimedia wireless sensor networks. In: *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, pp. 590–597.

VENCKAUSKAS, Algimantas; JUSAS, Nerijus; KAZANAVICIUS, Egidijus; STUIKYS, Vytautas, 2015. An energy efficient protocol for the internet of things. *Journal of Electrical Engineering*. Vol. 66, no. 1, p. 47.

VENČKAUSKAS, Algimantas; JUSAS, Nerijus; MIKUCKIENĖ, Irena; MACIULEVIČIUS, Stasys, 2012. Generation of the secret encryption key using the signature of the embedded system. *Information technology and control*. Vol. 41, no. 4, pp. 368–375.

VENČKAUSKAS, Algimantas; MORKEVICIUS, Nerijus; BAGDONAS, Kazimieras; DAMAŠEVIČIUS, Robertas; MASKELIŪNAS, Rytis, 2018. A lightweight protocol for secure video streaming. *Sensors*. Vol. 18, no. 5, p. 1554.

VENČKAUSKAS, Algimantas; ŠTUIKYS, Vytautas; JUSAS, Nerijus; BURBAITĖ, Renata, 2016. Model-driven approach for body area network application development. *Sensors*. Vol. 16, no. 5, p. 670.

VERMA, Pawan Kumar; VERMA, Rajesh; PRAKASH, Arun; AGRAWAL, Ashish; NAIK, Kshirasagar; TRIPATHI, Rajeev; ALSABAAN, Maazen; KHALIFA, Tarek; ABDELKADER, Tamer; ABOGHARAF, Abdulhakim, 2016. Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications*. Vol. 66, pp. 83–105.

WANG, Wei; WANG, Chunqiu; ZHAO, Min, 2013. Resource optimized TTSH-URA for multimedia stream authentication in swallowable-capsule-based wireless body sensor networks. *IEEE journal of biomedical and health informatics*. Vol. 18, no. 2, pp. 404–410.

WELCH, Greg; BISHOP, Gary, et al., 1995. *An introduction to the Kalman filter*. Citeseer.

WENDZEL, Steffen; KELLER, Jörg, 2014. Hidden and under control. *annals of telecommunications-annales des télécommunications*. Vol. 69, no. 7, pp. 417–430.

WENDZEL, Steffen; ZANDER, Sebastian; FECHNER, Bernhard; HERDIN, Christian, 2015. Pattern-based survey and categorization of network covert channel techniques. *ACM Computing Surveys (CSUR)*. Vol. 47, no. 3, pp. 1–26.

WHITMORE, Andrew; AGARWAL, Anurag; DA XU, Li, 2015. The Internet of Things—A survey of topics and trends. *Information systems frontiers*. Vol. 17, no. 2, pp. 261–274.

WINKLER, Thomas; RINNER, Bernhard, 2014. Security and privacy protection in visual sensor networks: A survey. *ACM Computing Surveys (CSUR)*. Vol. 47, no. 1, pp. 1–42.

WYMEERSCH, Henk; LIEN, Jaime; WIN, Moe Z, 2009. Cooperative localization in wireless networks. *Proceedings of the IEEE*. Vol. 97, no. 2, pp. 427–450.

XIE, Haijiang; ZHAO, Jizhong, 2015. A lightweight identity authentication method by exploiting network covert channel. *Peer-to-Peer Networking and Applications*. Vol. 8, no. 6, pp. 1038–1047.

XYLOMENOS, George; POLYZOS, George C, 1999. TCP and UDP performance over a wireless LAN. In: *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320)*. IEEE. Vol. 2, pp. 439–446.

YANG, Jen-Ho; LIN, Iuon-Chang, 2014. A source authentication scheme based on message recovery digital signature for multicast. *International Journal of Communication Systems*. Vol. 27, no. 11, pp. 2616–2627.

YANG, Shusen, 2017. IoT stream processing and analytics in the fog. *IEEE Communications Magazine*. Vol. 55, no. 8, pp. 21–27.

YANG, Zheng; LIU, Yunhao, 2009. Quality of trilateration: Confidence-based iterative localization. *IEEE Transactions on parallel and distributed systems*. Vol. 21, no. 5, pp. 631–640.

YAO, Hu; MUQING, Wu, 2020a. Kalman filtering based adaptive transfer in energy harvesting IoT networks. *IEEE Access*. Vol. 8, pp. 92332–92341.

YAO, Jingjing; ANSARI, Nirwan, 2020b. Enhancing federated learning in fog-aided IoT by CPU frequency and wireless power control. *IEEE Internet of Things Journal*. Vol. 8, no. 5, pp. 3438–3445.

YU, Gary, 2020. Simple Schnorr signature with Pedersen commitment as key. *Cryptology ePrint Archive*.

ZAHRA, Syed Rameem; CHISHTI, Mohammad Ahsan, 2020. Fuzzy logic and fog based secure architecture for internet of things (flfsiot). *Journal of ambient intelligence and humanized computing*, pp. 1–25.

ZANDER, Sebastian; ARMITAGE, Grenville; BRANCH, Philip, 2007. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials*. Vol. 9, no. 3, pp. 44–57.

ZHANG, Daqiang; HE, Zongjian; QIAN, Yuming; WAN, Jiafu; LI, Di; ZHAO, Shengjie, 2016. Revisiting unknown RFID tag identification in large-scale internet of things. *IEEE Wireless Communications*. Vol. 23, no. 5, pp. 24–29.

ZHANG, You-Sheng; CHEN, Tsung-Hsuan; CHIOU, Yih-Shyh; CHEN, Shih-Lun; CHEN, Wei-Ting; LIN, Yang-Ke; WEN, Fu-Jung; LIN, Ting-Lan, 2019. Design and Implementation of Real-Time Localization Algorithms Based on FPGA for Positioning and Tracking. In: *2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*. IEEE, pp. 446–448.

ZHUANG, Yuan; WANG, Qin; SHI, Min; CAO, Pan; QI, Longning; YANG, Jun, 2019. Low-power centimeter-level localization for indoor mobile robots based on ensemble Kalman smoother using received signal strength. *IEEE Internet of Things Journal*. Vol. 6, no. 4, pp. 6513–6522.

ZOICAN, Sorin; ZOICAN, Roxana; GALATCHI, Dan, 2021. Fuzzy Logic Framework for Internet of Things Systems Implementation. In: *2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*. IEEE, pp. 223–236.

SL 344. 2022-07-22, 14 leidyb. apsk. l. Tiražas 14 egz. Užsakymas 145.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas