Veikko Markkanen

SHARING SECURITY INFORMATION BETWEEN RESOURCE CONSTRAINED NETWORK NODES

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

ACKNOWLEDGEMENT

The research was supported by Business Finland (grant number 8365/31/2022) and the University of Jyväskylä

ABSTRACT

Markkanen, Veikko
Sharing Security Information Between Resource Constrained Network Nodes
Jyväskylä: University of Jyväskylä, 2024, 76 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

Challenges in resource constrained IoT networks are driven by the miniaturization of purpose-specific hardware and the imperative for cost-efficiency. These characteristics make traditional security solutions, which focus on securing individual devices, unrealistic. Instead, decentralized solutions that leverage the collective resources of a network must be considered. For these solutions, key enablers include self-configuration, scalability, resilience to extreme dynamics, and the overall sustainability and reliability of the network, suggesting the ad hoc paradigm, an attractive foundation for development. Therefore, the objective of this master's thesis is to examine the feasibility of ad hoc networking in providing a reliable communication framework for sharing security information between resource constrained devices.

The research consists of the examination of major challenges in resource constrained IoT systems and exploration of promising solutions from academic literature. It details various categories of ad hoc networking, key standards, and routing protocols. Additionally, a simulation artifact was developed to assess the feasibility of using ad hoc networking to distribute security information among resource constrained devices across different network sizes. The findings indicate that ad hoc networking is an efficient and scalable framework for sharing security information in terms of throughput, latency, and the overall reliability of the introduced security functionality. The key factors affecting these values could be identified as the physical topology of the network and the availability of existing routes between nodes. Furthermore, the alignment of ad hoc networking with academically proposed solutions was affirmed.

The results from this thesis can provide a reference base for further steps in validating ad hoc networking as a suitable communication framework upon which more complex, decentralized security functionalities can be implemented.

Keywords: IoT security, Internet of Things, IoT, ad hoc networking, distributed computing, network simulation

TIIVISTELMÄ

Markkanen, Veikko
Sharing Security Information Between Resource Constrained Network Nodes
Jyväskylä: Jyväskylän yliopisto, 2024, 76 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Resurssivajeisten IoT-verkkojen turvallisuushaasteet juontavat juurensa tarkasti rajattuun tehtävään suunniteltujen laitteiden optimoinnista kustannustehokkuutta varten. Tässä ympäristössä laitteiden suojaaminen perinteisin, yksittäiseen laitteeseen keskittyvin menetelmin, ei ole realistista. Vastuu kyberturvasta tulisi hajauttaa verkon kollektiivisia resursseja hyödyntäen. Hajautettujen menetelmien ytimessä on laitteiden kyky muodostaa autonomisia, skaalautuvia, ja kestäviä verkkoja, joiden rakentamiseksi ad hoc -verkkoteknologia tarjoaa hedelmällisen perustan. Näin ollen, tämän pro gradu -tutkimuksen tavoitteena on kartoittaa ad hoc -verkkoteknologian soveltuvuutta turvallisuustiedon jakamiseen resurssivajeesta kärsivien laitteiden kesken.

Tutkimus koostuu IoT-verkoille tyypillisten haasteiden tunnistamisesta, sekä akateemisessa kirjallisuudessa esitettyjen ratkaisujen käsittelystä. Se erittelee ad hoc -verkkojen kategoriat, keskeisiä standardeja sekä reititysprotokollia ja tutkii niiden soveltuvuutta IoT-ympäristössä. Lisäksi tutkimuksessa kehitettiin simulaatioartefakti, jolla arvioitiin ad hoc -verkkoteknologian kykyä jakaa turvallisuustietoa erikokoisissa IoT-sensoriverkoissa. Tulokset osoittivat ad hoc -verkkoteknologian tukevan turvallisuustiedon tehokasta ja skaalautuvaa jakamista, kapasiteetin, viiveen ja toimintavarmuuden näkökulmista. Verkon fyysinen topologia ja reittien olemassaolo tunnistettiin merkittäväksi tekijöiksi suorituskyvyn kannalta.

Tämän tutkimuksen tulokset tarjoavat pohjan ad hoc -verkkoteknologian validoimiseksi viitekehyksenä, jonka päälle voidaan toteuttaa monimutkaisempia, hajautettuja turvallisuustoiminnallisuuksia.

Asiasanat: esineiden internet, IoT, IoT kyberturva, ad hoc verkkoteknologia, verkkosimulointi, hajautetut teknologiat

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1 Introduction

1.1 Navigating the IoT landscape

Internet of things (IoT) has effectively changed the way we live, work, and communicate in various key industry sectors. It continues to display unprecedented opportunities for individuals and businesses alike, providing capabilities such as real time health monitoring, urbanization management, and industrial automatization (Cano et al. 2018). This technology is based on the pervasive presence of various wireless technologies around us like tags, sensors, actuators, and mobile phones (Abdmeziem et al. 2016). These heterogeneous devices seamlessly embed computing and communications creating an ecosystem of smart gadgets that envelope the user almost imperceptibly. Consequently, increasing the risks inherent to technological integration. Furthermore, academic and industry research has shown that IoT systems are among the most vulnerable in the world (Schiller et al. 2023; Bitdefender 2023).

The dependence on IoT systems for technical and economic success has set actors vulnerable to hostile cyber actions and other serious cyber threats (Skouloudi et al. 2020). With the steady invasion of IoT devices and networks, there is a growing security need to support this area. According to the work of Alqaravi et al. (2023) main concerns include the susceptibility of sophisticated attacks on IoT networks capable of crippling the critical services provided by these devices, altering sensitive data collected and transported by IoT devices or by taking control over the systems altogether.

While securing IoT is becoming a prime concern for the industry, several issues exist to prevent the consolidation of IoT security (Frustaci et al. 2017). Many of these challenges are related to the limited scalability of IoT networks and resource constrained nature of the devices themselves. Another major concern is that all of the security challenges and threats of each network technology are passed by default onto the IoT systems, and there are additional security threats that arise from the coexistence and collaboration of heterogenous devices and technologies. These factors render traditional security solutions incompatible within IoT networks. To realistically improve the security of smart devices, decentralized, smart solutions must be considered. Proposed solutions, highlight automated distribution of responsibilities and cooperative decision-making, while minimizing human intervention and single points of failure.

A key factor within the proposed solutions is the nodes' ability to establish and maintain decentralized, light weight, scalable and highly dynamic networks which enables reliable communication between the nodes of the network to achieve a common goal. This must be done without jeopardizing the confidentiality, availability, and integrity (CIA) of the regular functioning of the network. For such a solution, the ad hoc paradigm, combined with recent technological advancements, presents attractive foundations for development.

1.2 Overview of research framework

This research explores solutions in the realm of IoT security. The main research question for this work can be summarized as:

- Can we share and deliver security information to enable cooperative decision-making between resource constrained network nodes based on ad hoc networking?

This question delves into the potential of ad hoc networking to create a reliable communication framework for IoT devices with resource limitations. Three supporting research questions are investigated to dissect the primary query:

1. What are the key challenges in resource constrained IoT networks?
2. What type of solutions have been identified as promising advances for these challenges?
3. Which of the key challenges for consolidating IoT security can we improve on via ad hoc networking?

A dual-method approach is employed to answer these questions. Firstly, a literature review is conducted to establish theoretical framework. It examines the current state of IoT, its integration challenges, and growth trajectories. This includes a focus on security concerns, privacy, and the evolving threat landscape for smart devices – factors that critically impact the realization of IoT vision. The review then delves into IoT networking – its key components, prevailing wireless communication technologies, architectures, and general requirements, along with the design challenges these elements present. Special attention is given to addressing IoT's unique needs and ad hoc networking as a potential solution for some of these challenges.

The latter part of the research transitions into an empirical study using the design science framework, where network simulator 3 (ns3) plays a pivotal role. Here, the feasibility of using an ad hoc network for information transmission among IoT nodes is tested via simulation artefact. The simulation aims to assess whether such a network can facilitate cooperative communication and decision making among IoT devices while maintaining their essential functions like sensing and data transmission.

1.3 Structure

This master's thesis is structured into eight chapters. Following introduction, the second chapter provides a general background on the state of IoT integration, - security, and the enabling wireless technologies. Third chapter explains the current design challenges for IoT networks, and research directions. Fourth chapter delves into ad hoc networks, their routing, related protocols, and standards. The fifth chapter details empirical research framework used in this work to demonstrate transferring security related traffic within ad hoc network. Analysis of results is found in chapter six, then followed by discussion and conclusion.

2 Background and Context

The purpose of this chapter is to overview the basic components for this research. These are the concepts of modern internet of things, security, and wireless communication technologies for IoT. Understanding this context enables the further examination of challenges unique to IoT network, as well as the proposed wireless networking solutions to combat some of these challenges.

2.1 Internet of Things

International Telecommunication Union (ITU) (2005) described the Internet of Things as follows: from anytime, anyplace, connectivity for anything. According to ITU's vision, connections would multiply and create an entirely new dynamic network of networks – an Internet of Things.

Since then, IoT has become one of the most important technologies of the century. We can connect everyday objects such as kitchen appliances, light bulbs, fitness trackers, baby monitors, to the Internet via embedded devices, where seamless communication is possible between people, processes, and things. Currently, according to the IoT Analytics (2023), there are over 14.3 billion active IoT endpoints, and this number is expected to grow up to 29 billion IoT connections by 2025.

Schiller et al. (2022) trace the rapid proliferation of IoT devices to a confluence of technological advancements and evolving consumer demands. Key drivers include the miniaturization of powerful and energy-efficient electronics, advancements in wireless communication technologies, and the increasing accessibility of cloud computing resources. These factors have made it feasible to embed intelligence and connectivity into a broad array of devices, from household appliances to industrial equipment (Cano et al. 2018). Furthermore, the consumer appetite for smart, interconnected devices that offer enhanced convenience, improved efficiency, and personalized experiences has significantly fuelled this expansion, to the point of dependency on large-scale IoT systems.

As an inevitable result, deployments of large-scale and secure IoT systems have become critical. Within an autonomous IoT network, sensors and devices need to communicate with each other in a distributed way. This requires a mechanism by which different nodes can agree upon the validity of any communicated data. However, there are many design challenges associated with the deployment of IoT devices. According to the work of Frustaci et al. (2017) and Mocnej et al. (2018), few of these challenges are related to scalability and high latency due to a centralized network architecture and limitations related to secure transmission of private and confidential information. Due to the massive number of devices that can belong to several users, data ownership of users' needs to be ensured, so that they can exercise complete control over what data they want to share with others (Sobin 2020). Apart from these, challenges include the computational power and energy required by security algorithms, which is not available in the average resource constrained IoT devices and the lack of reliability in the IoT network (Schiller et al. 2021; Silva et al. 2018).

2.2 IoT security

Alqarawi et al. (2022) refer security on IoT as the degree of protection of, or resilience to, IoT applications and infrastructure. IoT is exceptionally prone to disruptions. Smart devices generally rely on external resources for security and resilience, with several applications left unattended in various real-world conditions. The devices introduce minimal security controls for the points of connection they create from the internal network. This place un-feasible burden of responsibility for existing security measures. Breaching internal networks through compromised IoT nodes trivialize capturing and misusing other devices, within the breached network segment. Common factors preventing the consolidation of IoT security are listed below, with recent work validating and adding to the previous research.

Factors preventing the consolidation of IoT security (Borgia 2014; Silva et al. 2018; Schiller et al. 2022):

- Very large attack surface
- Low device resources
- Systems are complex
- Standards are fragmented
- IoT is often deployed on legacy infrastructure
- There are contradicting security viewpoints and requirements
- Low cost of devices does not allow security
- Usability and functionality are valued above security
- Lack of skills in IoT cyber security
- Update mechanisms are complicated
- Liability on security incidents
- Physical vulnerability due to widespread deployment

To solve these challenges, a reliable communication framework is required to support decentralized, secure, and supervised architecture, where the processing load of security related tasks is intelligently divided among the nodes of the network. Failing to do so would result in deteriorating of the IoT vision (Frustaci et al. 2017).

2.3 Wireless communication

In wireless communication technology, a transmitter and receiver antennae are connected with certain shape for wireless communication. The transmitter modulates the signal onto the carrier wave, which is captured by the receiver antenna. The receiver then performs analog-to-digital conversion, translating the signal into a format that can be understood and used by the receiving device. This process eliminates the need for physical wires, offering flexibility in device manufacturing, deployment, and movement (Paliwal et al 2022).

Wireless communication methods such as Wi-Fi, Bluetooth, and cellular networks are key enablers in the realm of IoT. As highlighted by Sikimić et al. (2020), by removing the need for physical connection, wireless communication enables IoT devices to connect and communicate seamlessly with ubiquity. It also allows devices to be placed in locations where wiring would be impractical or impossible. This flexibility and mobility make it easier to deploy IoT solutions across any domain, while also reducing installation and maintenance costs (Borgia 2014).

According to Abdmeziem et al. (2016) salient advantage of wireless communication within the IoT domain is its capability to expedite and streamline data transfer. This allows IoT devices to transmit data instantaneously, fostering rapid decision-making and timely interventions. Abdmeziem et al. list various applications such as smart home systems, industrial automation, healthcare monitoring, and transportation infrastructures, where the attribute is of significant importance. The immediacy and efficiency of data transfer via wireless means enable effective functioning of these sectors, ensuring they operate with heightened responsiveness and agility.

Another critical aspect of wireless communication technologies in IoT is their scalability and flexibility (Gupta et al. 2017). These technologies enable IoT networks to adapt to changing demands and conditions by easily integrating new devices, accommodating different protocols, and expanding operational ranges (Khan et al. 2018). This adaptability is crucial for maintaining dynamic and responsive IoT systems, which must evolve with technological advancements and shifting user requirements.

Central to the deployment of IoT systems is the efficient management of power. As highlighted by Mahmoud et al. (2016), wireless communication technologies are meticulously engineered to optimize power usage. This optimization ensures that IoT devices can function over prolonged periods without the necessity for frequent battery replacements or power interventions. The low power consumption characteristic of these technologies is particularly beneficial for IoT applications that necessitate continuous, uninterrupted operation without fixed infrastructure. In scenarios where device longevity and minimal maintenance are crucial, wireless communication stands as a significant advantage, making it the ideal choice for a multitude of IoT applications.

3 Resource constrained IoT devices

This chapter reviews the main challenges and their proposed solutions from academic literature, in relation to resource constrained IoT systems. The aim of the chapter is to build an understanding of the various challenges which contribute to the unique characteristics of the IoT networks. Recognizing these challenges support examining further networking solutions, and their applicability within resource constrained IoT networks.

For challenges stemming from the general structure of IoT networks, foundational theory for this chapter is provided by Silva et al. (2018) in their study: "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges". Silva et al. compile the main challenges as availability, performance, security, reliability, scalability, and mobility related. They also highlight the absence of a universal definition for the architecture as another challenge. Similar themes are explored by Abdmeziem et al (2016), in "Architecting the internet of things: state of the art". Their research compares different architectures for the Internet of Things emphasizing the need for a standard architecture. Other distinctive challenges in this work include distributivity and resource scarcity. Another major challenge is explored in the works of Wang et al. (2017). They identify power consumption as root issue for most of the challenges regarding IoT, in their work: The Design Challenges of IoT: From System Technologies to Ultra-Low Power Circuits. Several research align with energy as a major issue. In particular, Taleb et al. (2022), combine the energy constrain with device placement to highlight finding the optimal position in common IoT environments as yet another overachieving challenge. Other distinctive features of resource constrained IoT networks are combined and compared to a larger theoretical foundation. Majority of the examined research highlight possible solutions for the challenges presented. These include optimization of key functionalities, advanced security algorithms, machine learning, standardization, and distributed architectures among others (Gupta et al. 2017; Saleem et al. 2018; Fu et al. 2019; Gamatie et al. 2019; Hassija et al. 2019; Schizas et al. 2022; Schiller et al. 2022; Yu et al. 2023).

3.1 Challenges in resource constrained IoT environments

Market forces have played a major role in creating an ecosystem of resource constrained IoT devices. The archetype of an ideal IoT device today is compact, lightweight, cost-effective, and capable of fulfilling its designated function upon immediate deployment. This list effectively excludes numerous attributes, the lack of which directly impacts the overall reliability of IoT networks. In general, these challenges can be broadly categorized into networking, device, and system design related. Overarching these considerations is the pervasive issue of security, a concern magnified by the IoT's expanding scale and the growing dependence on the constant availability and connectivity of these devices. Delving into these topics, uncovers the obstacles and opportunities that define the contemporary IoT landscape.

Networking challenges: In the realm of wireless communication, a foundational prerequisite for performance is the 'link budget margin'. As described by Wang et al. (2017), the term refers to the strength of the signal that is being sent out by the transmitter, and how well the receiver can pick up that signal. As the signal strength and receiver sensitivity are impacted by a variety of interventions, calculating the optimal use of energy is considered a major challenge.

Within resource constrained IoT networks this issue becomes particularly prevalent. IoT devices are commonly dispersed across wide areas. This means there is variety in proximity among transmissions and receptions. For example, Paliwal et al. (2022) notes that, location, population, and flora are well-known variables impacting signal propagation characteristics and network parameters. According to their work, the attenuation of radio waves is increased by flora, environmental vegetation, and humidity. Paliwal et al. divide IoT application areas into rural and urban. Within rural environments, the distance between devices is commonly higher, leaving more room for distance based deuterating of signals. Weather conditions are also of elevated importance. In metropolitan areas however, physical obstruction such as buildings, mobility related issues such as node movement, and population related issues such as noise and network congestion complicate optimizing power usage. Since the devices inherently have limited memory, processing power, and battery life, communication often represents the most significant energy expenditure (Triantafyllou et al. 2018). This means that in addition to managing transmission power, optimizing the time spent during transmission, reception, and data processing pose major challenges. Effective management of these factors is critical for the sustainability of IoT systems, as outlined by Sobin (2020).

Routing in IoT networks is about finding the best path between source and destination. According to Trintafyllou et al. (2018) this involves matching the traffic pattern of its deployment area and be mindful of the power required to function. The dynamic nature of IoT devices – including mobility, devices going offline, or new devices joining the network – adds layers of complexity to routing algorithms within IoT networks. Ensuring efficient data transfer while accommodating these fluctuations is a major challenge, particularly, when there are other considerations like limited range, the density of devices and data, memory, and processing power (Devi et al. 2019). The route loss constraint, including attenuation is also affected by various weather conditions and locales, such as whether the device is inside, outside, on the open, or within proximity of other physical objects. IoT systems must be capable of managing such mobility, ensuring uninterrupted service during movement, transitions between coverage areas, and handovers. Other factors affecting availability may include software glitches, hardware failures, human errors, or a combination thereof (Paliwal et al. 2022).

Borgia (2014) highlights bandwidth constraints and the management of wireless spectrum as another dimension of complexity for densely populated IoT environments. Bandwidth constraint is a major challenge due to the lower capacity of wireless links. Elaborating on the subject in more recent work, Paliwal et al. (2022), note that wireless links are prone to fading, noise, and interference conditions, all of which contribute to a lower throughput jeopardizing the confidentiality, integrity, and availability requirements set by modern services. Furthermore, both commercial and industial systems require low end-to-end latencies, typically under 10 ms, between the sensing devices and the control nodes. This requirement is also threatened by interference from numerous devices and various environmental factos, as discussed by Chiang & Zhang (2016).

The 2.4GHz Industrial, Scientific, and Medical (ISM) band, for example, is heavily congested with various technologies like WiFi, Bluetooth, and ZigBee (Silva et al. 2018). Meanwhile, newer standards such as LoRa, SigFox, and NB-IoT are emerging in the sub-GHz band. These technologies, while conserving bandwidth and energy, come with their own set of challenges, such as smaller maximum transmission unit (MTU) sizes and lower transmission rates (Mahmoud et al. 2016). Additionally, the cost of deploying, maintaining, and operating these networks is a significant consideration, driving research towards cost-effective strategies and low-cost technologies. The coexistence and orchestration of these diverse standards are imperative to ensure the quality of service.

Interoperability is another critical issue in IoT, since various types of devices need to be connected seamlessly. For effective IoT functionality, it is crucial that services are compatible with all device types, achieved through adherence to standardized protocols at the network and application levels. Nevertheless, achieving full interoperability is complex due to diverse hardware platforms, varying communication protocols, and inconsistent interpretations of similar protocols (Ahmed et al. 2019).

Scalability is intertwined with interoperability, as the network must accommodate the integration of new devices and services without compromising existing operations. As noted by Silva et al. (2018), this is further complicated by the need for effective data management, as the rapid proliferation of IoT devices generates vast amounts of data that require efficient processing and transmission, generating reliance on external storage and processing services.

As IoT networks increasingly rely on cloud computing for data processing and storage, cloud related issues of security and privacy become paramount. Hassija et al. (2019) note that the external processing and storage of data open up vulnerabilities to attacks and breaches. Furthermore, the centralization inherent in cloud-based solutions introduces single points of failure, along with latency and cost challenges.

Aligning with the work of Hassija et al. Ahmed et al. (2019) highlight IoT as a major source of big data. Therefore, external storage and computing solutions for these systems are becoming increasingly costly and challenging to integrate. The transfer of extensive amounts of data creates latency issues, bandwidth constraints, while also introducing a single point of failure into the system. Reliance on external services risks the availability and consistency of the cloud services, which can also be affected by network failures, outages, or disruptions, which affect the performance and responsiveness of IoT devices and applications (Ahmed et al. 2019). Furthermore, Burhan et al. (2018) focus on security and privacy concerns regarding external processing and storing of personal data. According to their work, users send private information to fulfil their tasks. When such private data leaves the local network, there are many opportunities for attackers to access it.

Hardware constraints: Security and privacy issues are prominent concerns in the IoT domain. IoT endpoints are commonly optimized for cost and battery life and tend to treat security as a secondary consideration. Several attacks have demonstrated the ability to breach IoT systems via vulnerabilities due to outdated or simply insufficient security measures. The problem is accurately described by Alquarawi et al. (2023), who state that there is a plethora of literature focusing on securing IoT, yet the devices are still getting hacked. The inherent limitations of these systems, such as restricted computational power, minimal memory, and constrained energy resources, significantly increase their vulnerability to various security threats (Babu et al. 2024).

One of the primary challenges in resource constrained IoT systems is the limited computational power of the devices. These devices often lack the capability to implement complex encryption algorithms and advanced security protocols, which are essential for safeguarding data against unauthorized access and ensuring the integrity of communications. According to Schiller et al. (2022) This limitation not only makes the devices susceptible to various forms of cyber-attacks but also hinders the implementation of robust authentication mechanisms, leaving the systems vulnerable to unauthorized access and control. This is the result of optimizing the cost and performance of a device for a specific purpose, while other substantial considerations would be needed.

Additionally, Schiller et al. note the minimal memory available in these devices as another significant challenge. The constraint on memory limits the amount of data that can be stored and processed, such as encryption keys and security logs. This limitation hampers the ability of the system to maintain historical data, which is often crucial for identifying and analysing security breaches and patterns of attacks. Furthermore, the restricted memory capacity obstructs the implementation of sophisticated security software and firmware updates, which are vital for addressing known vulnerabilities and enhancing the system's security posture.

The energy constraints of IoT devices further compound the security and performance related challenges. As examined by Trintafyllou et al. (2018) security operations, including data encryption, decryption, and transmission of secure signals, are inherently energy intensive. In resource-constrained environments, where preserving battery life is a critical concern, there is often a tradeoff between implementing robust security measures and maintaining efficient energy consumption. This trade-off leads to scenarios where security measures are either scaled down or overlooked entirely in favour of prolonging the device's operational life, thereby making the system more susceptible to various types of threats (Frustaci et al. 2018).

Furthermore, a prevalent issue in the IoT domain, particularly with more affordable devices, is the lack of comprehensive lifecycle support. As alluded by Frustaci et al. (2018), many devices are manufactured and shipped without necessary security patches and continue to operate without receiving any updates. This practice leaves the devices perpetually vulnerable to known exploits and security flaws. The absence of regular updates and patches, especially in a landscape where new vulnerabilities are continually being discovered, poses a severe risk to the integrity and security of the entire IoT ecosystem (Alqarawi et al. 2023).

System design challenges: The typical deployment scenarios of IoT devices in diverse and often uncontrolled environments add to the challenges. Devices operating in harsh conditions, rural areas, or within congested perimeter, face networking challenges, as well as issues in conserving energy (Paliwal et al. 2018). Devices operating in public or physically insecure spaces are at a higher risk of physical tampering, leading to compromised security (Zakaret et al. 2022). In such scenarios, the inability to physically safeguard the devices, coupled with their limited on-device security capabilities, presents a significant challenge in ensuring the overall security of the IoT system (Schiller et al. 2022).

A significant challenge arises from the integration of numerous heterogeneous devices within IoT networks. According to Silva et al. (2018), this diversity introduces a plethora of potential entry points for attackers, each with its unique vulnerabilities. The variety in connectivity, operating systems, firmware, and hardware among these devices means that securing each node becomes a highly individualized task. In such a landscape, an attacker only needs to exploit the weakest link to compromise the entire network. This heterogeneity also complicates the process of implementing uniform security measures, as each device may require a different approach to security, depending on its specific capabilities and limitations, as noted by Schiller et al. (2022).

Another critical challenge is the lack of standardization in security protocols and the absence of a common architectural framework in IoT systems (Agrawal et al. 2023). This lack of standardization results in inconsistent security practices and makes the deployment of universal security solutions nearly impossible. Without common standards, manufacturers may not prioritize security, particularly in the case of low-cost devices, leading to a wide variance in the security posture across different IoT products (Frustaci et al. 2018). This inconsistency not only complicates the task of securing IoT networks but also makes it challenging to ensure compatibility and secure interoperability between devices from different manufacturers.

Additionally, system scalability must be considered. Scalability is the ability of a system to adapt to changes in the environment and meet the evolved responsibilities in the future. With the growing idea of IoT, lack of scalability is a major cause of poor performance and often necessitates the reengineering of the whole system. It is a desirable attribute for any system, with the premises of growing amount of work. As IoT systems generate, store, and process more data, there is a clear need for novel, approaches to manage this increase efficiently and reliably. The contradiction is clear to the current centralized means, which are limited by computational bottlenecks, fault tolerance and cost among others (Hassija et al. 2019). However, achieving scalability in the scope of IoT is met with challenges on multiple fronts. Gupta et al. (2017) survey these challenges and emphasise the need for accountability. They state that there must be protocols that accommodate and remotely identify each and every "thing" in the internet of things, which becomes a daunting tasks with numerous heterogenous devices. Furthermore, a network of these things must tolerate failure and remain operational without complete deployment, allowing for gradual rollouts and changes along the way. A particular concern highlighted by Schiller et al. (2022) is the security landscape for resource constrained IoT environments. As the number of responsibilities and ultimately, the connected devices grow, scaling security measures to accommodate this growth without compromising on performance or energy efficiency becomes increasingly challenging. Ensuring that security protocols are both lightweight and robust enough to be effective across a large and diverse network of devices is yet another significant challenge (Krishna et al. 2021). In essence, the main concern for scaling up IoT systems, is the ability to adhere to the known best practises in the face of increased complexity.

3.2 Solutions

The security and sustainability of resource constrained IoT systems is a multifaceted issue, compounded by the heterogeneity of devices, the lack of lifecycle support and standardization, and the challenges of scalability. These factors, combined with the inherent limitations of IoT devices in terms of computational power, memory, and energy resources, create a complex landscape that requires comprehensive and adaptive solutions. Addressing these challenges is crucial for ensuring the security and resilience of IoT networks, especially given their growing prevalence and importance in various sectors. Gratifyingly, a plethora of advances can be identified from both academic and industry research. While it is beyond the scope of this chapter to encompass all such advancements comprehensively, the focus will be on elucidating some of the frequently discussed or promising approaches.

Standardization: Standards have played a key role for the advancement of society, technology, and economy. At best, they can be thought of as the collective understanding of the latest, and best guidelines for a specific industry. Compliance with recognized standards not only enhance market access for developers and retailers, but the benefits encompass savings in research and development, in addition to increased consumer trust as well. In their report on Economic benefits of standards, International Organization for Standardization (ISO) displays several case studies where the value of standards is estimated at several percentages of sales revenue for most of the companies involved (ISO. 2014). While it is argued that standards commonly fail to adhere to specific context, for the wider spectrum of IoT security, the need for industry regulation has been recognized and acted upon.

Very recently a turning point in the evolving landscape of the IoT cybersecurity was met with advances in regulations by the public regulatory agencies, like the EU, the US, and the UK. The main goal for these regulatory bodies is twofold: To enhance IoT cybersecurity for enabling connected devices to become more resilient against cyber threats, and to safeguard personal information within the IoT realm. They way which these approaches aim to achieve their goals are by introducing voluntary certification schemes for manufacturers, but also through legal obligations for device manufacturers and providers to meet cybersecurity standards from the outset. Key legislative approaches include information sharing with users, conformity assessment procedures for digital products, and improved handling of vulnerabilities among others (european-cyber-resilience-act.com. 2023). If successful, these approaches would significantly work towards unifying cybersecurity across the market.

Elsewhere both the industry and academic communities have continued to drive collaboration, develop guidelines, and create standards together with the governmental regulatory bodies. Recent research by Saleem et al. (2018) encompass these efforts in a structural manner. Their work follows close collaboration between industry professionals and academics, experienced in supervising implementation and auditing standards such as ISO27001 and legislations including General Data Protection Regulation (GDPR) and Data Protection Act 1998 to propose IoT Security Framework (IoTSFW). IoTSFW can be considered a valuable contribution especially for its cross disciplinary nature. Creating actionable guidelines encompassing wide range of industries, organizations and other suitable infrastructures is a daunting, but necessary task.

Integrated sensing strategies: With resource scarcity identified as the key challenge in IoT networks, different sensing strategies have emerged as potential solution for many real-world applications. Continuous sensing, storing, processing, and transmitting data cost energy. In their research Fu et al. (2018) contrast this to the rarity, randomness, and transitory nature of events within many of the application domains for wireless sensors. They propose an event triggered sensing scheme for wireless structural health monitoring system, which makes use of filtering mechanisms to eliminate noise, impact detecting module to become active only when certain thresholds are met, and local processing capabilities for ensuring responsiveness. The approach requires hardware design solutions and processing power, but the combination of modules, and event-triggered sensing achieved consumption of only a twelfth of what an always on system consumed during idle periods highlighting a significant extension of battery life. Several event-triggered sensing schemes have achieved similar results as highlighted by Yu et al. (2023).

Another sensing strategy aims to reduce costs and increase reliability by incorporating the measurement of various metrics to gather multimeric data. It enables IoT networks to address more complex and comprehensive issues closer to the source of data while also reducing the number of sensors required. A recent protype was created by Sarwar et al. (2020). They introduced a sensor which achieved detailed structural information gathering though vibration or strain triggered sensing, combining both multimeric, and event-triggered sensing. Further advances in wireless sensor systems, particularly in monitoring roads and railroad infrastructure, have been demonstrated by Sim & Park (2017) and Taher et al. (2022). These studies successfully merged different metrics to achieve more accurate calculations of structural integrity under different conditions.

Fog computing: Fog/edge computing has emerged as one of the most promising research directions for IoT. The paradigm concerns locating computing resources among a data source or a cloud or other files centre. Hassija et al. (2019) describe fog computing as decentralized means of analysing and computing to store and process time-sensitive data efficiently and quickly. They also highlight enhanced security and resilience against data breaches, as less data travels through vulnerable communications.

The obvious comparison of fog computing is to be drawn between the current de facto architecture, cloud computing. Varghese et al. (2020) observed the performance of a fog computing model in a scenario involving online gaming. They demonstrated a 20 % decrease in latency using edge nodes for processing user needs instead of the typical cloud environment, in addition to 90 % decreased traffic between the edge and the cloud server. In their work, Sarkar et al. (2016) modelled a theoretical fog computing architecture and analysed its performance in the context of IoT applications. Their research displayed similar results in terms of reduced latency, but also highlight a 40.48 % reduction in mean energy consumption. The finding was attributed to overall advantages in energy dissipation due to the fog computing architecture's ability to process data closer to the source, rather than transmitting all data to distant cloud servers for processing.

Most of the academic work has considered fog computing as an extension of the cloud computing framework. To exist somewhere between the edge and the cloud. Yet, advances have been made towards integrating more computing capabilities for devices at the very edge of the network. This change is driven by the vast number of devices and data generated by them. It is expected that the cloud ecosystem will be unable to facilitate the future IoT systems. However, the edge computing approach within the embedded domain is severely limited by memory, energy, and processing power. To overcome these challenges, several proposals have been made.

One of such approaches involve systems consisting of various processing elements for meeting both performance and power-efficiency requirements. In their work, Gamatie et al. (2019) prototype new heterogenous multicore architecture for the embedded domain based on low power technology. An average of 22 % of energy gain was observed in contrast to reference design measured on FPGA prototypes. Limitations for Gamatie et al. (2019) include complexity and memory strain.

In their work Chen et al. (2018) presented a manufacturing scenario, where they compared self-organized task allocation mechanism based on edge computing to a centralized, cloud based, task scheduling mechanism. The former achieved significantly reduced service delay and bandwidth optimization. These benefits relied on Raspberry Pi devices, which were observed to have enough processing power to perform cloud services including, data fusion and cooperation with working partners, at the networks edge. Additionally, as highlighted by the work of Hoang & Spencer (2022) there is still considerable optimization to be achieved via more efficient algorithms in terms of efficiency and processing speeds. They managed up to 100 000 times faster processing of raw measurement data via on-board reference-free displacement algorithm in comparison to traditional methods. While most of these challenges come down to the cost of implementation, the work of Chen et al. (2018) serves as a reminder that even limited resources deployed at the network edge will bolster the service quality in IoT based use cases.

Scalability and Interoperability: An IoT system must be capable of supporting a vast number of heterogenous devices, features, and users. To overcome this challenge, several techniques were identified by Gupta et al. (2017) in their survey of the field. Notable findings involve refactored data pipelines to accommodate the increased amount of data, and scaling in various directions to efficiently distribute resources and tasks between otherwise overloaded devices. Ren et al. (2017) narrow down their search of scalability solutions to systems requiring real-time and context aware service provisioning. Drawing on the concept of edge computing, they prototype a system architecture where services for smart wearables are dynamically provisioned from an edge-server, contrasting the traditional cloud-based approach. Observed results involved reduced latency up to 86 percent, and up to 91 percent of reduced energy consumption in contrast to a cloud-based approach, where the applications are downloaded directly on the devices. In particular, the efficient offloading of app downloading and data processing to the edge of the network were deemed major advances towards more scalable IoT systems.

Of particular emphasis in much of the research involving scalability is the need for built-in capabilities for bootloaders, security keys, and other features to eliminate human interaction (Gupta et al. 2017). This idea can be extended towards self-healing and self-configuration capabilities that have been debated for over a decade, but only recently, have the devices received enough capabilities to realistically tap into this potential. Notably, through the emergence of more powerful MCU's and microprocessors, improvements in wireless connectivity and interoperability achieved through standards and regulation, as noted by Agrawal et al. (2023). These capabilities have been prototyped in numerous scenarios such as those involving smart cities environments and emergency rescue as surveyed by Quy et al. (2022a) and Ahmed et al. (2017).

Machine learning: Machine learning solutions have been met with extremely high expectations across the industry. Unsurprisingly, machine learning has been observed an attractive solution in numerous applications within the context of IoT as well. Particularly, solutions that can alleviate the strain of frequent data access and transmissions to cloud or other central locations, as the volume of data generated by the IoT system increase are high in demand (Schizas et al. 2022). At the forefront of such solutions exist TinyML.

TinyML is a concept for combining computationally restricted embedded systems, with machine learning, to deploy intelligent algorithms on IoT nodes. According to Sanchez-Iborra & Skarmeta (2020) TinyML aims to facilitate on-device data processing, pattern recognition, and decision-making, while consuming minimal energy. The idea relies on the processing model of common IoT devices. They are left idle for most of the time. This means they have latent processing capabilities, proposed to be leveraged by machine learning algorithms. On the other hand, it is recognized by Sanches-Iborra & Skarmeta (2020), that transmitting data is far costlier than the actual processing done in the devices due to the simplicity of operations. This suggest that major optimizations would be achieved if the data could be processed locally. The concept is closely related to edge computing, thus reaping benefits from both ends.

Despite these advances, the deployment of machine learning solutions raises questions including the scalability and sustainability of ML models across the heterogeneity of IoT devices. Addressing these challenges present further topics of academic and industrial efforts. Some active directions with promising results involve data compression for memory and power management (Signoretti 2021), and secure and improved machine learning models for decentralized model training (Ficco et al. 2024; Li et al. 2020). Adding to these advances, popular lightweight frameworks such as TensorFlow Lite for Microcontrollers are being actively developed to dispatch machine learning models on various architectures (David et al. 2021).

Advances in security: The severity of IoT failures and the loose security practises of the industry from past years make up a bad combination. Recognized by the academic world, industry, and governmental entities, securing the IoT ecosystem is now a prime concern. While many of the previously discussed advances have security applications, there exist a multitude of approaches directly for securing the devices from various threats they face (Schiller et al. 2022).

Particularly interesting direction for securing these devices are various types of previously overlooked physical security modules. These modules add a layer of protection for the data transmitted or processed within IoT systems. Sidhu et al. (2019) specify key injection, where each device is given a unique electronic identity by injecting a semiconductor chip with unique identity in each device, as a method which strengthens authentication significantly. In such solutions, the integrity of key injection process is of extreme importance and can be achieved via hardware security modules that can create, secure, and manage these keys. Another type of physical security solution is the Secure Element (SE) technology. Zakaret et al. (2022) refer to SE as a dedicated hardware chip designed to securely store and manage digital keys and credentials, such as cryptographic keys, in a protected environment. In principle, it provides a high level of security for digital transactions and data by isolating sensitive information from potential threats and vulnerabilities found in the broader device or network. Furthermore, several sources have identified SE technology as essential for blockchain based security solutions in the IoT domain (Schiller et al. 2022). Another component similar to SE, is the ARM TrustZone, which has emerged as a hardware mechanism for creating an isolated Trusted Execution Environment for applications to run securely (Pinto & Santos 2019).

Security algorithms refer to security software running in the same network or within the IoT devices themselves. Such advances have primarily focused on improving authentication, trust, and integrity of the communication channel among IoT devices. These topics of interests are frequently paired with encryption techniques optimized for resource-constrained devices and intrusion detection systems tailored for the embedded IoT domain (Schiller et al. 2022). Notable contributions include the work of Maitra et al. (2019) who surveyed the performance of popular IoT encryption algorithms. They highlight Advanced Encryption System (AES-256) and eXtended Tiny Encryption Algorithm (XTEA). AES-256 was observed more powerful of the two, providing ample security to sensitive data, for devices built on 16 and 32-bit architectures. However, many embedded systems operate on 8-bit architectures with less memory and power at their disposal. XTEA was observed as the more feasible solution for such systems, reaching 60 times the power efficiency and only a seventh of the program memory in comparison to AES run on the same devices. Although XTEA is not on par with AES security wise, the added protection narrows the window of opportunity for various attacks. These findings emphasise the need for consideration of the whole system architecture and the services it is required to provide, when designing security.

Network Intrusion Detection Systems (NIDS) are a popular topic of interest and a primary tool for combating network intrusions and various types of attacks. However, adapting these systems for IoT networks has been met with significant challenges such as the possibility of a novel attack, the vast number of agents required for the IDS to function, and the diverse communication patterns that introduce additional traffic and routes to be monitored. To efficiently extend these systems for the IoT domain novel approaches area required. One such approach is the Hybrid Intrusion Detection System proposed by Khraisat et al. (2019). In essence, they combine lightweight versions of Signature based Intrusion Detection (SIDS) with Anomaly based Intrusion Detection (AIDS) through stacking ensemble method. The hybrid approach was tested on the Bot-IoT dataset and achieved a detection rate of 99.7% in contrast to around 93% by the standalone IDS's. Khraisat et al. leave the impact on energy consumption unresolved. In their survey, Gyamfi & Jurcut (2022) focus on this element among others and define multi access edge computing and machine learning as the future directions for NIDS design. They aim to resolve resource constraints via enabling IoT nodes to operate a lightweight binary based NIDS, which forwards intrusions to a more in-depth analysis performed on a platform located at the networks edge. The training of both models is located on cloud servers. Both of these works serve as reference and guidelines for developing NIDS for IoT systems, but equally highlight that there is still a lack of effort in designing a truly decentralized, practical approach to detect attacks in real environments.

To conclude, blockchain technology presents another promising approach to addressing security challenges within IoT networks by leveraging its decentralized nature for secure, transparent transactions and automated agreements through smart contracts, which are essentially digital rules shared across multiple devices. This integration aims to enhance device authentication, data integrity, and resistance against attacks by removing centralized vulnerabilities and ensuring privacy protection. However, challenges persist, notably in block generation consistency and scalability due to the diverse capabilities of IoT devices and the volume of transactions (Hassija et al, 2019; Mezquita et al. 2019). Future improvements in blockchain are essential for its effective application in IoT security, focusing on optimizing consensus mechanisms and network scalability to accommodate the vast number of interconnected devices. As highlighted by Xu et al. (2021), the synergy between blockchain and IoT holds the potential to advance security paradigms, despite existing computational and storage challenges that need addressing to fully harness blockchain's capabilities for IoT security.

4 Ad hoc-based IoT networks

This chapter delves into ad hoc networking and its applicability within the context of IoT. Here are explored the main categories, protocols, and associated standards of ad hoc networks. This chapter plays a crucial role as it defines the theoretical basis for the role and sustainability of ad hoc networking in IoT systems.

The general understanding of ad hoc networks within this work particularly builds on the work of Ramanathan & Redi (2002): "A brief overview of ad hoc networks: challenges and directions". This study presents an early view of networks formed for a specific purpose, principles that are still applicable today. Routing in ad hoc networks is covered in numerous studies, but the work of Roy & Deb (2018) "Performance comparison of routing protocols in mobile ad hoc networks" provides a clear understanding of the most significant protocols. Bhatia & Dharma (2016) also address ad hoc routing protocols, basing their evaluations on simulations of protocol performance. A broader and less-known range of routing protocols for ad hoc networks is discussed by Alotaibi, E., & Mukherjee, B. (2012) in their study: "A survey on routing algorithms for wireless ad-hoc and mesh networks". The most recent theoretical foundation for addressing ad hoc networks is formed by Agraval et al. (2023) in "Classification and comparison of ad hoc networks: A review" and Boulaiche (2020) in: Survey of secure routing protocols for wireless ad hoc networks. The transition of ad hoc networks into the IoT context is addressed by Reina et al. (2013) in their study "The role of ad hoc networks in the Internet of Things", Munisha & Gill (2019) in "Mobile Ad Hoc Networks and routing protocols in IoT enabled smart environment: A review", and Cano et al. (2018) in "Evolution of IoT: An industry perspective". Cano et al. (2018), also discuss standards relevant to ad hoc networking.

4.1 Overview

Wireless networks have evolved significantly in terms of their organization and management. According to Hernandez et al. (2014) this evolution is driven by the diverse requirements of the various deployment scenarios they serve. The foundational experiments by the Wireless Ethernet Compatibility Alliance (WECA) in the late 1990s marked the beginning of this journey, and since then, the application areas and use cases for wireless communications have expanded considerably.

Currently, most wireless networks operate in what is known as 'Infrastructure Mode'. This mode relies on Access Points (APs) and a fixed, wired backbone network, facilitating communication from a source device to a destination. However, this traditional structure can be limiting in scenarios where the installation of intermediate systems like APs, base stations, routers, or switches is unfeasible or impractical (Rubinstein et al. 2006). For such cases, 'Infrastructure-less Mode', or ad hoc networking, offers a viable alternative.

In his overview of ad hoc networking, Remondo (2011) states the typical purpose of a network terminal as to function as an end system. This means running applications, acting as a source of information, and receiving data as the destination of intended data traffic. In ad hoc networks, terminals also function as intermediate systems. This quality enables nodes to route and forward information to other nodes independently, without the need for a centralized administrator, thus providing greater flexibility (Agrawal et al. 2023). Communication over intermediate network nodes exceeds the limits of physical transmission range between the source and the destination. It is why wireless ad hoc networks are considered multi-hop wireless networks.

Rubinstein et al. (2006) define the ad hoc mode as an operational setting for 802.11 radios, primarily functioning at the Physical and Data link layers (Layer 1 and 2) of the OSI Model, with an emphasis on its application in Wireless Local Area Networks (WLAN). Beyond WLAN's, ad hoc networks are commonly deployed in various networking scenarios including local (LAN) and personal area networks (PAN). As stated by Remondo (2011), although the research on ad hoc networking is not restricted to certain technologies, it has primarily assumed Bluetooth or IEEE 802.11 to be the underlying technologies. In recent years, some change has been observed, due to the emergence of competing technologies (Cilfone et al. 2019).

According to a survey by Boukerche et al. (2011), the main body of academic research on ad hoc networking has historically focused on routing. There is a broad consensus that routing is closely related to the functioning of the network on a multitude of communication layers, and it remains a core function for optimizing network performance in relation to several key parameters such as sustainability, throughput, latency, scalability, and robustness (Quy et al. 2022b). More recently, comparable interest has been resurfacing in different applications of ad hoc networks within the IoT context. Truly decentralized systems bolstering unrestricted connectivity and operating at high levels of cost-efficiency have been proposed as an attractive ground for developing future IoT systems (Reina et al. 2013; Agrawal et al. 2023). This surge of interest underscores the potential of ad hoc networking as one of the key technologies for overcoming challenges posed by the expanding IoT landscape.

4.2 Core access network standards for ad hoc networks

Institute of Electrical and Electronics Engineers (IEEE) is the leading developer of industry standards in a broad range of technologies. Among others, IEEE standards provide the basis for wireless networking, and are the words most widely used wireless computer networking standards. Within this chapter are examined some of the main wireless standards and technologies for ad hoc networking. Particularly, the focus is on IEEE 802 family of standards for local area networks, personal area networks, and metropolitan area networks. These standards are created and maintained by the IEEE LAN/MAN Standards Committee.

4.2.1 IEEE 802.11 (WLAN & WiFi)

IEEE 802.11 is a part of the IEEE 802 set of technical standards for wireless local area networks (WLAN). It defines medium access control (MAC) and physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations within a local area. The IEEE 802.11 standard defines infrastructure-based and infrastructure-less as the two operational modes for Wireless LANs. From here on, this chapter focus on the infrastructure-less or Ad hoc mode of operation (IEEE 2003; Anastasi et al. 2004; Remondo 2011).

When operating in this mode, stations are considered to from an Independent Basic Service Set (IBSS), which is synonymous to an ad hoc network. After the synchronization stage, any station within the transmission radios of any other station can start communicating. This approach excludes the need for an Access Point (AP), while preserving wireless internet connectivity, should one of the stations bolster a connection to the wired network. As Anastasi et al. (2004) highlight, in a pure ad hoc networking environment, the user's devices constitute the network. This setup necessitates significant cooperation among devices to fulfil networking functionalities typically provided by infrastructure.

The 802.11 specify Distributed Coordination Function (DCF) which is the fundamental MAC technique for when there are no AP available and individual 802.11 nodes must contend with each other for access to the media. DFC provides the basic access methods of the 802.11 MAC protocol and is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme.

According to DCF before initiating a transmission, a station must sense the channel to determine whether any other stations is transmitting. If the medium is found to be idle for a specific interval called Distributed InterFrame Space (DIFS), the station finishes the transmission. If the medium detects transmitting activity during this period, the transmission is rescheduled after the end of the ongoing event. On top of the re-scheduled time is added a random interval called backoff time. Backoff time is used to initialize backoff timer, which decreases for as long as the channel is sensed as idle. A station can only transmit its frame after the backoff timer has reached zero.

Independent of the sensing mechanisms introduced, it is possible that two or more stations sense the channel as idle and start transmitting simultaneously. Such a scenario would result in a collision at the receiving node, which in essence means the corruption and loss of transmitted data. Therefore, 802.11 standard employs an immediate positive acknowledgement scheme. The scheme involves the transmission of an acknowledgement frame (ACK) after a time interval called the Short InterFrame Space (SIFS). ACK is only transmitted after a successful reception effectively highlighting whether the initial transmission was successful. This knowledge enables the source to reschedule transmitting lost frames if needed.

The 802.11 also specifies Cyclic Redundancy Check (CRC) algorithm to be used for error detection within the frames themselves. The process involves both the calculation of the CRC value before transmission and its comparison with the Frame Check Sequence (FCS) at the receiver to detect any errors. If an erroneous frame is detected (the CRC does not match the FCS value) the station is required to stay idle for Extended InterFrame Space (EIFS) interval, before reactivating the backoff algorithm. DCF relies on EIFS whenever the physical layer indicates to the MAC that a frame transmission was begun and did not result in the correct reception of a complete MAC frame with a correct Frame Check Sequence (FCS) value. Upon receiving a complete frame during the EIFS resynchronizes the station to the actual busy/idle state of the medium, so the EIFS is terminated, and normal medium access continues following reception of that frame.

IEEE 802.11 technology provided fertile grounds to implement single-hop ad hoc networks due to its straightforward deployment. When compatible stations are within common transmission range they can communicate. The initial single-hop coverage has since been extended upon via multi-hop ad hoc networking. These mechanisms, operating at the network layer, are commonly deployed at nodes to enable them to forward packets towards the intended destination and extending the range of the network beyond a single node’s transmission radius. The 802.11 set of standards remains a popular Layer 1 and Layer 2 solution for ad hoc and other forms of wireless networking due to its rapid commercial evolution and functional maturity (Rao et al. 2015).

IEEE 802.11a/b/g/n/ac/ax: While not exclusively designed for ad hoc networks, these amendments to the original 802.11 provide a wide range of data rates, improved frequency usage, and efficiency that are beneficial for ad hoc networking over short to medium distances. They offer various physical layer improvements that increase bandwidth, reduce interference, and improve signal reliability. The latest accepted evolution of the standard is 802.11ax. 802.11ax supports maximum theoretical data rate of 9.6 Gbps. It operates on 2.4, 5, and 6 GHz frequencies (1-7.125 GHz), and supports channel widths of 20/40/80/160 MHz. The standard focus on surpassing its predecessors by ensuring faster connections, optimizing spectrum usage, enhancing reliability, and improving power efficiency (Rao et al. 2015; Mahmoud 2016; Qureshi & Asghar 2023).

IEEE 802.11s: The IEEE 802.11s amendment specifically addresses the implementation of mesh networking, a type of ad hoc networking, capabilities within WLANs. It defines the architecture and protocols that enable wireless devices to establish, maintain, and participate in a mesh network. Mesh networking allows for direct, peer-to-peer communication among two or more network nodes, facilitating data forwarding and routing across the network in a decentralized manner. This amendment incorporates features for path selection, mesh peering, and forwarding protocols to ensure efficient and reliable connectivity across the network. It also supports self-forming and self-healing capabilities, allowing the network to dynamically adjust to the addition or failure of nodes without requiring manual reconfiguration. By extending the core 802.11 standard to include mesh networking, IEEE 802.11s offers a scalable and flexible solution for extending WLAN coverage and enhancing connectivity in a variety of deployment scenarios. 802.11s inherently depends on one of 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, or 802.11ax to carry the actual traffic (IEEE 2011).

IEEE 802.11p: In 1999, the Federal Communications Commission (FCC) allocated a 75 MHz Dedicated Short Range Communication (DSRC) band centred at 5.9 GHz (5.85 – 5.925 GHz) for vehicular communications (Xie et. al, 2017). The 802.11p amendment was created to provide standardized access to the DSRC band. It extends its predecessors (mainly 802.11a) PHY and MAC layer specifications to meet the requirements of high mobility introduced by Vehicular Ad hoc Networks (VANET), particularly to enhance road travel and transportation efficiency. Improvements centre around faster and more efficient communication between vehicles. Also, improvements to communication time are considered. The main difference between 802.11a and 802.11p is that the latter proposes to use 10MHz frequency bandwidth, to make the signal more robust against fading and increase the tolerance for multipath propagation effects of signals in vehicular environment. Among proposed applications for the amendment are toll collection, vehicle safety services, and commerce transaction via cars (Qiu et. al, 2017).

4.2.2 IEEE 802.15 (Bluetooth & ZigBee)

The IEEE 802.15 working group on Wireless Specialty Networks (WSN) is also a part of the IEEE 802 standards committee. It focuses on the development of open consensus standards addressing wireless networking for the IoT. Among notable contributions for ad hoc networking, are 802.15.1 Bluetooth and 802.15.4 ZigBee (Mahmoud 2016).

Bluetooth: Bluetooth is a short-range wireless technology that is used for transmitting data between fixed and mobile devices and building Personal Area Networks (PAN) within the ISM band from 2.4 to 2.485 GHz. Designed for low power consumption and cost, the original Bluetooth facilitates communication up to 10 meters. Later versions extend this up to 400 meters. The maximum data rate for the latest version (Bluetooth 5) is 2 mbps. Bluetooth uses Frequency-Hopping Spread Spectrum to minimize interference and enhance communication robustness (Bisdikian 2001).

The standard supports ad hoc networking through piconets, where a master device communicates with up to seven active slaves, with the possibility of forming scatternets for larger network configurations. It specifies PHY and MAC layer protocols for efficient secure communication, incorporating device discovery, pairing, and encryption (Remodo 2011).

With Bluetooth Low Energy (BLE) and Bluetooth Mesh, the standard has expanded further into IoT applications, offering energy-efficient communication and support for large-scale networks. BLE optimizes power usage and connection efficiency, while Bluetooth Mesh enables many-to-many communication suitable for smart environments and industrial applications (Yin et al. 2019).

ZigBee: ZigBee is a low-power, low-data rate wireless communication technology that is widely used for creating Personal Area Networks (PANs) within the ISM band from 2.4 GHz. It is designed for energy efficiency and reliability over short to medium distances. The maximum data rate for ZigBee is 250 kbits. ZigBee employs the IEEE 802.15.4 standard at the Physical (PHY) and Media Access Control (MAC) layers and supports multi-hop mesh networking by defining a coordinator for managing the network topology. The protocol is optimized for low bandwidth needs and can support thousands of nodes in a single network (Mahmoud 2016).

ZigBee 3.0 unifies the previous ZigBee versions into a single, comprehensive standard that improves interoperability and user experience. Support for 800 MHz for Europe and 900 MHz for USA and Australia were also added. This evolution enhances its application in diverse environments, from smart homes to industrial automation (Digi International 2024).

4.2.3 LoRa

LoRa is a physical layer specification developed by Semtech, focusing on achieving power-efficient communications over long distances. It is based on Chirp Spread Spectrum (CSS) technology with integrated Forward Error Correction (FEC). By optimizing CSS, LoRa achieves extremely low power consumption and long-distance communication capabilities. This makes it particularly suitable for Internet of Things (IoT) applications where devices are dispersed over vast areas and operate at low data rates. LoRa operates in the Sub-GHz bands of ISM, such as 433, 868 MHz in Europe and 915 MHz in USA (Bor et al. 2016).

The LoRa physical layer can be used with any MAC layer, however, LoRaWAN is commonly associated as the specification for the MAC and application layers. Due to LoRaWAN operating the network in a star topology, adapting LoRa to modern IoT scenarios involving ad hoc characteristics, efficient multi-hop protocols are required to support LoRa at the MAC layer. Examples of which are proposed by Bor et al. (2016) and Tran et al. (2022).

4.3 Categories

Agrawal et al. (2023) survey the state of academic research on ad hoc networking through the past years highlighting 2010's as the most frequent years of interest in the subject. More importantly, the interest has resurfaced nearing 2023. This is closely attributed to the technological atmosphere, which highlights mobility and ubiquity as common characteristics of the market. As discussed in the previous chapter there is now a need to be online anytime and everywhere. This sets a pool of requirements for smart devices, for many of which, ad hoc networking is proving an attractive means of connectivity.

4.3.1 Wireless sensor networks

Wireless sensor networks are a type of network which facilitates relaying sensor data from the physical environment to a central location for analysis and action. The wireless sensors are dispersed in a sensor field and are connected via wireless communication medium. For the most applications of WSN, the network is formed in an ad hoc manner where sensor nodes can organize themselves with no prior coordination (Ketshabetswe et al. 2019; Agrawal et al. 2023).

Within a WSN, a single sensor node is a lightweight unit equipped with processing unit, storage, and transceiver module (Ketshabetswe et al. 2019). Commonly, they host one to several sensory units for collecting data from their surroundings and are also equipped with analog-to-digital converter. Sensor nodes measure the fluctuation of conditions within their vicinity, convert them into relative electric signals which are processes via the node's processor. Via its transceiver, the node can wirelessly transmit the data produced by its processor to other nodes or/and to a selected sink point. Wireless sensors are typically battery powered.

According to Kandris et al. (2019) the collaborative use of a sufficient amount of sensor nodes enables WSN to perform simultaneous data acquirement of ambient information at several points of interest positioned over wide areas. As described by Yu et al. (2024), enabled by continuous technological development, these devices host increasingly powerful sensing, processing, and communicative capabilities despite the cost-effective nature and their small size. The advances have brought forth an ever-growing range of applications of different types for WSN. Some of which include battlefield surveillance, environmental monitoring, disaster detection and rescue, precise and intelligent agriculture, medicine and health care, environment-friendly buildings, traffic control, and object tracking (Kandris et al. 2019; Ketshabetswe et al. 2019).

Despite its growing popularity, Paliwal & Saraswat (2022) note that several of the challenges related to IoT networking are particularly prevalent in the case of WSN. These include the limitations within the power source, memory capacity, transmission bandwidth, topological routing, and data aggregation (Farsi et al. 2018). Even within the realm of resource limited IoT devices, sensors in wireless sensor networks face especially stringent constraints. This is primarily due to their compact physical size, which limits manufacturers' ability to incorporate larger memory, more powerful processors, extensive antennae, or long-lasting batteries without introducing extensive costs (Schiller. et al. 2022; Kethabetswe et al. 2019, Farsi et al. 2018).

4.3.2 Wireless mesh networks

Wireless mesh networks (WMN) have garnered growing interest as a prominent research topic within the academic community due to their easy implementation, dynamically self-organized, self-configured and adaptive nature. WMN's possess profound capabilities of extending the limits of broadband connectivity to traditionally costly or inefficient scenarios. In their research, Taleb et al. (2022) list various applications of wireless mesh networking. Some of which include broadband home networking, education, healthcare, corporate networks, industrial automation, disaster management, military, and rescue operations, even in the most rural areas.

Cayiri et al. (2009) describe WMNs as comprising radio networks set up in a mesh topology. The common architecture consists of mesh clients, mesh routers, and gateways. Mesh routers provide the clients with mesh routing functions. These devices also serve as network extenders and relay data to other mesh routers (Caputo 2010). Some of them serve as gateways, to provide the network with access to a central backbone network, like the internet. Others may serve as access points to provide various clients access to the network. Users connect to the mesh network via APs with a variety of connected devices such as laptops, mobile phones, and smart televisions (Afanasyev et al. 2010).

As described by Agrawal et al. (2023), in mesh networking the devices are connected in a way, that most nodes have multiple paths to other nodes. This creates many routes for information between pairs of users, increasing the overall resilience of the network if a node or connection fails. The traffic originated by clients uses multihop capabilities reaching the wireless backhaul communication system created by the mesh routers. The mesh routers relay information using wireless radio links reaching the routers acting as gateways, which connect the mesh network to a backbone network (Cayiri et al. 2009). There are no limitations on the type of backbone network, meaning WMN's work can leverage both wired and wireless networks for providing connectivity within the network (Zhou-Kangas 2014).

While one of the main advantages of WMN's is their cost-effective implementation, the performance of WMS's is particularly dependant on the accurate placement of the participating routers and gateways. Taleb et al. (2022) surveyed the importance of node placement in WMN's and found the poor placement resulting in interferences and congestion causing low throughput, considerable packet loss, and high delays significantly hindering the performance of the WMN's. They describe the problem as NP-hard, increasing the computational time exponentially in relation to problem size.

4.3.3 Mobile ad hoc networks

In their research Agrawal et al. (2023) note that in recent years there has been a leap in wireless communication systems involving independent mobile users. Users have moved from traditional fixed location computing to always requiring connectivity. This has been seen as setting a stage for Mobile ad hoc networks (MANET). According to Hernandez et al. (2014), MANET is formed spontaneously by multiple mobile devices such as smartphones, vehicles or drones connecting to a self-established and maintained network. These devices collaboratively establish a network without the need for a pre-existing communication infrastructure or centralized administration. Each node in MANET acts as a routing device to propagate data packets to other devices, considerably reducing the human intervention in the functioning of the network (Bang et al. 2013; Eltahlawy et al. 2023).

MANET's have gained academic prominence due to their diverse application domains as highlighted by Bang et al. (2013). Key applications include emergency response communication systems, temporary network setups for conferences or meetings, military operations in inaccessible or hostile terrains, and vehicular networks for traffic monitoring. Their ability to form and operate autonomously makes MANETs ideal for scenarios where mobility is involved and traditional network infrastructure is unavailable, impractical, or expensive to deploy (Ahmed et al. 2017). Furthermore, this operational flexibility simplifies the integration of various systems and applications, saving significant development time and resources. Similar to WSNs and WMNs, but with added dynamic due to node mobility, MANETs enable a diverse pool of resources to communicate seamlessly, enhancing the system's adaptability and responsiveness to different events (Quy et al. 2022b).

MANETs operate on the principle of multi-hop routing. In this setup, data packets are passed from one mobile node to another until they reach their destination. This multi-hop data transmission method ensures that nodes located beyond the direct wireless transmission range can still communicate. As noted by Quy et al. (2022a) and Bang et al (2013), this method significantly enhances the timely access to different services, as well as the flexibility and range of the network but also introduces challenges in routing protocols due to the dynamic topology of the network.

The performance and reliability of MANETs are closely linked to the mobility patterns of the nodes. As these nodes are free to move, the network topology is subject to constant change, which poses challenges in maintaining stable communication links (Agrawal et al. 2023). According to studies by Eltahlawy et al. (2023), this high degree of mobility leads to frequent network partitioning, route changes, and the need for robust and adaptive routing protocols. The study also points out the crucial role of efficient routing algorithms in mitigating packet loss, reducing latency, and maintaining network coherence in MANET environments.

Additionally, MANETs face challenges such as interference, noise, and signal fading, which become more complex to manage when scaling up (Eltahlawy et al. 2023). Interference can occur when there is excessive traffic over the network's capacity, leading to congested data paths and degraded network performance. Noise, an inherent issue in wireless communication, can distort signal integrity, while signal fading becomes a concern when a hop within the MANET becomes too long or crowded, resulting in weakened signal strength and reduced data throughput (Ahmed et al. 2017).

Security in MANETs is another area of significant concern, as the open medium and decentralized nature of these networks make them vulnerable to various security threats (Rubinstein et al. 2006). The absence of a fixed infrastructure complicates the implementation of traditional security mechanisms. As a result, research in MANETs also focus on developing security protocols that can safeguard against threats like eavesdropping, spoofing, and denial-of-service attacks, as elaborated by Ahmed et al. (2017). However, it is also noted, that means to do so require computational capacity, and applications, typical mobile devices do not necessarily possess (Paliwal & Saraswat 2022).

In conclusion, while MANETs offer remarkable flexibility and adaptability for dynamic networking environments, their effectiveness is contingent upon sophisticated routing strategies, robust security protocols, and efficient management of inherent challenges such as node mobility, interference, noise, and signal fading. Ongoing research in this field continues to explore innovative solutions to optimize the performance and security of these self-organizing wireless networks, with careful consideration for the overall cost of these systems.

4.4 Ad hoc routing

A critical aspect of ad hoc networking occurs at the Network Layer (Layer 3) of the OSI Model. Here, the transmission of data packets between nodes in an ad hoc network involves dynamic routing protocols (Silva et al. 2018). According to Hernandez et al. (2014), the function of a routing protocol in Ad hoc network is to achieve efficient communication with minimal time and consumption of network resources. These protocols are designed to adhere to the network's constantly changing topology, accommodating the movement, addition, or departure of nodes within the network. They aim to provide best response time, shortest delay, and highest throughput while minimizing costs. For the scope of this research, we will limit the focus on the so-called de-facto ad hoc routing protocols, which have facilitated most academic and industrial interest. These can be divided as table-driven and source-initiated protocols (Boukerche et al. 2011).

4.4.1 Source-initiated protocols (reactive)

Source-initiated routing, also referred to as reactive routing protocols, represent a class of routing protocols where the route is created only when there is an explicit request for it (Boukerche et al. 2011). The route is created through a mechanism which involves flooding the network with route request packets, starting from the source node's immediate neighbours, and progressively expanding to each subsequent node until the destination is reached. The process is completed when a route to destination is discovered, or all possible routing options have been explored. Once the route is established, it is sustained through maintenance procedure until the destination becomes inaccessible due to a link rupture, or the route is no longer needed (Rubinstein 2006).

For the network nodes, reactive routing is a fast, yet lightweight method, reducing the memory consumption significantly, by only initiating route discovery process when required to. However, the flooding mechanism introduces several inconveniences from the networks' performance perspective. Rubinstein (2006) observe frequent redundancy issues, contention, and collisions as the main problems related to reactive routing. They state that, in a typical ad hoc network, there are low-bandwidth links, and power limited terminals, which make these networks more suspectable to extensive control traffic occurring at specific time.

Ad hoc on demand distance vector routing: Ad hoc on demand distance vector (AODV) was developed by Perkins et al. (2003) as an improvement to Destination-Sequenced Distance-Vector (DSDV) and is one of the most widely studied source-initiated routing protocols. AODV is designed to for use in networks requiring quick adaptation to dynamic link conditions and it features low processing and memory overhead, low utilization, and determines unicast routes to destinations within the network. AODV establish routes between nodes only as needed, rather than maintaining complete network routing tables at each participating node. This approach minimizes the routing overhead for large networks with dynamic topologies, making it suitable for mobile ad hoc networks. AODV enables response to link ruptures and changes in a timely manner (Perkins et al. 2003).

Key features of AODV include the use of destination sequence numbers to ensure loop-free and up-to-date routes, and a route discovery process initiated by broadcasting Route Request (RREQ) packets. When a node requires a route to a destination, it broadcasts an RREQ. This request is propagated by neighbours until it reaches the destination or a node with a valid route. The route is then established in reverse, using Route Reply (RREP) packets (Perkins et al. 2003).

In research comparing ad hoc routing protocols, AODV has achieved consistently high scores, prompting it as the de-facto routing protocol for dynamic ad hoc networks. Notable works by Ade & Tijare (2012) and Gangwar & Kumar (2012) attribute this success to its ability to maintain connection by periodic exchange of information. However, some drawbacks have also been identified. Boulaiche (2020) note that AODV routing protocol is designed for networks where each node can be trusted. This requires additional authentication mechanisms or segmented environments to secure networks and can be considered a weakness. Devi & Gill (2019) consider preserving the freshness of sequence numbers as another challenge. In case changes happen in the network, and there are no periodic updates in immediate vicinity, the new node may have a better route to one or several destinations. However, before a node becomes a target or a source, it is not involved in any routing action leaving the potential best route inaccessible. Further issues include overhead introduced by a multitude of RREP packets in response to a single RREQ, the periodic updates each node perform for local connectivity, related power consumption, and the lack of multicasting capabilities, which have since emerged together with numerous security functions as extensions to the original AODV protocol (Alotaibi & Mukherjee 2012; Roy & Deb 2018; Boulaiche 2020).

Dynamic Source Routing (DSR): DSR is a prominent routing protocol designed for use in wireless ad hoc networks. It is generally considered effective with relatively small number of nodes, or low mobility. Like AODV it establishes routes only when they are needed for data transmission (Ade & Tijare 2010). The route discovery process in DSR involves broadcasting a route request (RREQ), which contains the source and destination addresses, as well as an initially empty list of nodes that the packet has traversed. The RREQ propagates through network with each node appending their addresses within the record. Upon reaching the destination, or a node with a route to the destination, a route reply is generated and sent back to the source node using the path recorded in the RREQ. Unlike AODV, DSR utilizes source routing and contains the complete route for each packet within the packet header. Link breakages are handled through route error messages, which are echoed back from the point of rupture. Another key feature of DSR involves route caches at each node, which are leveraged to decide on whether to initiate a route request or not (Johnson et al. 2007; Roy & Deb 2018).

When comparing on-demand routing protocols, Perkins et al. (2001) observe DSR to be more efficient in scenarios where routes are relatively stable or in smaller networks. This is attributed to caching and source routing characteristics. Each node can learn route information from packet headers, decreasing the need to initiate new route requests. This generates less control overhead. However, in many cases, ad hoc networks are not stale, and can contain several nodes. In such a scenario DSR scales up poorly. The routing overhead carried within each packet becomes heavy impacting the performance of the network. Path length correlates directly to the size of the packet headers. Node movement on the other hand reduces the efficiency of caching mechanisms. Roy & Dep (2018) highlight similar issues with the DSR protocol, notably its significant routing overhead that, while reducing the frequency of route discoveries, demands considerably more processing resources than many comparable protocols. As the number of nodes increases, the potential for accumulating stale or unused paths also rises, which can occupy valuable space and resources. Furthermore, the requirement to store and manage extensive routing caches quickly becomes a resource drain when nodes with low resources are considered. Like AODV, the original DSR does not involve multicasting capabilities (Johnson et al. 2007).

4.4.2 Table-driven protocols (proactive)

Table driven or proactive routing is based on routing tables maintained at each participating node. Table driven routing is comparable to classic internet routing. In such a network, participating nodes share routing information during specific intervals regardless of the actual communication built on top of it. Proactive routing requires each node to respond to changes in network topology by propagating update messages through the network in order to maintain a consistent network state (Rubinstein et al. 2006; Roy & Deb 2018).

According to Agrawal et al. (2023) proactive routing produce low latency routes, which save both time and resources during the actual communication requests. However, Rubinstein et al. (2006) note that this method of routing introduces significant amount of control traffic in highly dynamic networks, impacting the overall burden of the network. In a wireless setting this should be avoided.

Destination-Sequenced Distance-Vector: Perkins & Bahgwat (1994) introduced DSDV as a table-driven routing scheme for mobile ad hoc networks. Like many other distance-vector routing protocols, it is based on the Bellman-Ford algorithm, where each node will maintain a routing table for its neighbouring nodes (Kurniawan et al. 2020). The core functions of the protocol are described by Boukerche et al. (2011) as nodes maintaining routing table entries for each possible destination along with their associated distance from the source in hop counts, sequence numbers, which are maintained for each entry to avoid routing loop problem and stale routes, and requiring nodes to send periodic routing updates to all neighbouring nodes, which can also be triggered by any change within the network topology.

Generally, DSDV is considered effective in scenarios involving low node counts and static topologies (Rubinstein 2008). Having up to date routes maintained at each node reduces routing overhead and latency. These dynamics shift as the topological changes become more frequent the number of incremental packets transmitted by DSDV also increase. With every change, DSDV necessitates the generation of a new sequence number for the updated routes to be accepted and propagated through the network (Roy & Deb 2018). When nodes move, leave, or join the network frequently, the requirement for new sequence numbers can lead to delays in achieving network convergence. The delay is further exacerbated in large networks. Furthermore, with energy constraints and bandwidth becoming increasingly pressing issues, DSDV is criticised for regular updates of routing tables which use battery power and bandwidth even when the network is idle (Quy et al. 2022a).

Optimized Link State Routing (OLSR): Among de-facto ad hoc routing protocols is also Optimized Link-State Routing protocol. OLSR was designed by Clausen et al. (2003) as an optimization of the classical link-state algorithm, tailored for the requirements of mobile ad hoc networks. Boukerche et al. (2011) centre these contributions to the introduction of multipoint relays (MPR's). The mechanics of OLSR involve each node selecting a subset of its neighbours in way that a broadcast message, rebroadcasted by these nodes, will reach all nodes 2-hops away from source. The selected one hop neighbours are designated as MPR's for the source. Information to define these relations are acquired through each node broadcasting periodic hello messages. Compared to traditional flooding mechanism, when routing information needs to access each device within the network, this task is only performed by the MPR's, using shortest path algorithm. The generation of link state information also relies on these nodes, significantly decreasing the need for control messages in dense networks.

OLSR has been compared to other ad hoc routing protocols and experimental results have shown it effective in large and dense networks and in those involving moderate mobility (Quy et al. 2022a; Kurniawan et al. 2020); These results are attributed to MPR's and reduced need for retransmissions when flooding the network. Furthermore, when the number of nodes increase, more optimizations can be achieved. The periodic broadcasting of hello messages increases resilience in networks where reliable transmission of control messages is difficult to achieve.

Comparing different ad hoc routing protocols, Hassanawi et al. (2012) discovered several drawbacks for OLSR. Notably, it's efficiency is limited to network nodes properties when scaling up. Like DSDV, it maintains routing table for all possible routes which becomes increasingly resource intensive when scaling up the network. Another issue is related to mobility related control messages. Due to nodes moving, the optimal routes change frequently, which introduces control traffic and delay in rediscovering broken links.

5 Research framework

In this chapter, the research framework is detailed. The chapter introduces means to study wireless networks, the use of Network Simulator 3, the principles of design science research, and the application of these principles in this research.

5.1 Means to study wireless networks

Studying wireless networks can be done by taking measurements from physical network devices and analysing them. However, in developmental research this is unrealistic. Instead, Gomez et al. (2023), in their review of common ways to study wireless networks, highlight three methods: testbeds, emulations and computer simulations of wireless networks.

Gomez et al. (2023) describe testbed as a platform based on the immersion of system components in a virtual environment. The main advantage of a testbed is the ability to replicate actual system components within a controlled testing environment. Testbeds provide realism and scale depending on the available resources. However, real equipment is often costly and unavailable for experimenting purposes. For large scale experiments, testing environment proves another challenge, as environmental variables are usually uncontrollable.

Computer simulations are used to study various issues in wireless networks including signal processing in the physical layer, medium access in the link layer, routing at the network layer, protocol issues in the transport layer and design considerations in the application layer. According to Breslau et al. (2000), they are based on numerical models that represent the behaviour of network components. The main advantages of computer simulations are cost efficiency, scalability, and replicability (Patel et al. 2019; Gomez et al. 2023). With computer simulations, network scenarios can be construed and modified with lower costs and the results can be achieved in a shorter time period. This advantage allows the easier analysis on the networks with different assumptions. The main disadvantage is the lack of trust in results, which may stem from oversimplifying real-world scenarios or inquieted modelling of the simulated environment. Computer simulations consist of three main components: a model of the simulated networks, the simulation of the network activities and the analysis of the results (Gomez et al. 2023).

Emulators leverage software primitives of the Operating System (OS) to mimic the functioning of switches, links, servers, and packets in a real network. Unlike simulators, emulators run with real code and use the actual protocol stack available in the OS. This allows for continuous event processing and makes emulators a practical tool for testing code that will later be deployed in real-world scenarios. However, the accuracy of emulators may decrease as the complexity of the network topology increases, and their performance is often limited by the hardware resources of the host device (Patel et al. 2019; Gomez et al. 2023).

For the scope of this research, computer simulation was designed as the ideal choice.

5.2 Network Simulator 3

Network simulator 3 (NS3) is a discrete-event network simulator for internet systems, primarily used for research and educational purposes. It is an open-source tool under the licence of GNU GPLv2 and maintained by an active community. NS3 excels in creating realistic simulation models, which can be integrated with actual networks, making it ideal for real-time network emulation. It supports various wireless and IP network models like Wi-Fi, LTE, Mesh, and routing protocols such as OLSR and AODV. NS-3's core facilitates research across a wide spectrum of IP and non-IP networks and includes a real-time scheduler, enhancing its capability for simulation-in-the-loop scenarios. This allows for interactions with real systems, such as transmitting and receiving packets on actual network devices and serving as a connective framework for adding link effects between virtual machines (nsnam.org 2023).

The main advantage of using NS3 to simulate IoT networking related elements is the ability to measure the performance of our chosen architecture when scaling up and introducing IoT related events and constraints, along with applying security traffic in addition to regular IoT traffic within the network. NS3 is restricted by its ability to support application layer functionality, which hinders using IoT related communication protocols such as http(s), CoAPP, MQTT in simulations. However, regarding communication at higher layers, simply referring to dummy traffic at this point is expected to prove useful.

When utilizing NS3 for network simulations, it is crucial to understand a few core concepts. The tool uses abstractions, to make simulated environments more manageable and representative of real-world scenarios. These abstractions include the following key components:

1. **Nodes**: In NS-3, nodes are basic entities that represent devices like computers, routers, or switches in a network. Each node can host various network interfaces and run multiple applications.
2. **Network Devices and Channels**: Network devices (like Wi-Fi adapters, Ethernet ports) are attached to nodes and facilitate communication. Channels represent the medium through which these devices communicate, such as a wireless channel for Wi-Fi or a cable for Ethernet.
3. **Applications and Traffic Generation**: NS-3 allows the creation of various types of network traffic through its application models. These can range from basic traffic generators to more complex application behaviours. For IoT simulations, one can model the behaviour of IoT devices sending periodic updates or responding to events.
4. **Protocols and Models**: NS-3 includes a wide range of protocol implementations and models for different layers of the network stack. It supports standard IP protocols, as well as specialized protocols for different network types. While it may have limitations with some recent amendments and application-layer IoT protocols, it provides extensive support for the basic lower-layer protocols, crucial for network research.
5. **Mobility Models**: These models simulate the movement of mobile nodes. In IoT scenarios, this can represent mobile sensors or devices changing their location over time.
6. **Energy Models**: Particularly relevant for IoT, energy models in NS-3 allow for the simulation of battery consumption and power management strategies in devices.
7. **Statistics and Data Collection**: NS-3 provides tools for collecting and analysing data from simulations. This includes packet tracing, throughput measurements, delay, and loss statistics, which are critical for evaluating the performance of network architectures.

In practical network environments, host-computers come with added or built in NIC's. In ns3 however, nodes represent the host machines, with network devices attached to them. These network devices require several configurations: they must be assigned MAC addresses, installed on nodes, configured for protocol stacks, and connected to communication channels. In a complex simulation system, the volume of these connections become tedious. Since connecting network devices to nodes, devices to channels, assigning IP addresses, etc, are common tasks when simulating networks NS3 provides a set of topology helpers. These utilities are designed to streamline the process of network setup in simulations, providing an efficient means to manage the extensive configurations required in detailed network models (nsnam.org).

5.3 Design science research

Design science is a research paradigm focusing on the development and validation of prescriptive knowledge (Hevner 2004). In the case of this study, it serves to aid in the development and validation of a computer simulation of an IoT network based on ad hoc networking. Through designing and testing this simulation, we can better understand the suitability of the chosen network technology in improving IoT network resilience and security.

In 2007, Peffers et al. conducted a review of the influential works regarding design science research. In their work, they outlined a six-step approach for a commonly accepted framework to conduct studies based on design science principles. The consensus approach highlighted the following tasks:

1. Problem identification and motivation
2. Defining the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

The empirical section for this thesis is built on the steps described above in the following manner:

1. Problem identification and motivation: Several issues exist to prevent the consolidation of IoT security (Schiller et al. 2022). Few of these challenges are related to the limited scalability and resource constrained nature of the IoT devices. Another major concern is that all of the security challenges and threats of each network technology are passed by default onto the IoT systems, and there are additional security threats that arise from the coexistence and collaboration of heterogeneous devices and technologies. These factors render traditional security solutions incompatible within IoT networks. Therefore, setting up satisfactory security controls for modern, complex IoT systems is a system design problem.

All tough common security threats have been observed to predominantly focus on denial of service, signals from threat intelligence and risk management research indicate extreme dynamic for the situation (Krishna et al. 2021)

2 Define the objectives for a solution: The proposed solutions should move away from conventional methods towards decentralized, intelligent security strategies that require minimal human intervention. Overcoming the limitations set by IoT's unique conditions can be solved by enabling nodes to distribute responsibilities automatically and make smart decisions, thereby minimizing the potential for a single point of failure and enhance the overall security of IoT system.

A key factor within the proposed solutions is the nodes' ability to establish and maintain decentralized, light weight, scalable and highly dynamic networks which enables intelligent and reliable communication between the nodes of the network to achieve a common goal.

3. Design and development: Within the scope of this research, an artefact in the form of network simulation is created. The simulation will examine the functionality of ad hoc networking as basis for security traffic between IoT nodes, avoiding interference with the original functionality of the IoT network.

In practise, the artefact introduces a security event within the simulated IoT network requiring cooperation between network nodes. The participating nodes must react by establishing means of communications amongst each other, distribute information and reach a consensus conclusion regarding the event.

4 and 5 Demonstration and Evaluation: The performance of the ad hoc network will be validated through running the simulation against a set of parameters. These parameters encompass throughput of received data, end-to-end delay, and the successful completion rate of the designated security task. Moreover, the practical functionality of the simulation itself will serve as a crucial metric. The outcomes of the simulation will address the central question: Can ad hoc networking be utilized for reliable dissemination of security-related information among nodes with limited computational resources?

6 Communication: Communication will centre around publishing this research.

5.4 Simulation artifact

This is the setup for a simple IoT-sensor network, in which resource constrained network nodes distribute security information amongst each other to perform security related-tasks. These tasks are invoked when a sink node depletes its resources and cannot perform its regular duties, prompting the selection of a successor for these responsibilities. The primary focus for this work is to examine the feasibility of autonomous, decentralized means of handling security events, via resource constrained systems based on ad hoc networking.

The simulation creates an ad hoc wireless network with applications to generate security related traffic, and regular IoT traffic, both of which will be received and forwarded via UDP sockets and processed by each network node by custom packet handling functions. The security traffic forms its own overlay solution and is identified by tagging related packets. Each of the nodes of the network are configured for Wi-Fi ad hoc mode and use Ad hoc on demand Distance Vector (AODV) protocol for route discovery. There is no central management in the system, and the decision-making is based on the nodes collective understanding of security related information. The distribution of security information is divided into three approaches—broadcasting, unicasting, and a hybrid method. This is done to evaluate trade-offs in terms of scalability, reliability, and efficiency. Each method provides different advantages and challenges in the context of network performance and security posture. In all three scenarios nodes other than the sink are responsible for transmitting regular data in a set interval. In addition to this, the sink is responsible for broadcasting unspecified management information in a more sparce interval. The described traffic has a dual purpose of mimicking typical WSN behaviour and introducing stress into the network.

A - Reliance on broadcasting: The initiator (sink-node) broadcasts a request for assistance, marked with a unique tag to categorize it as a type of security event. Upon receiving this request, nodes evaluate their potential to serve as candidates for the event. Eligible nodes then prepare a key-value pair of their node ID and current battery level, based on local data. The request is then forwarded. Nodes that cannot become candidates simply forward the request. Having completed the set up, candidate nodes initiate an update sequence, where they broadcast their key-value pairs in a multi-hop fashion and update their values upon learning of a node with a higher battery level. Once the sequence is complete, AODV is used to inform the sink about the most suitable candidate, as determined by the collective data. The sink then assesses the candidates' "votes" and delegates responsibilities to the chosen node. Upon confirmation, the selected candidate acknowledges its new duties. The primary advantage of this approach is that it reduces the computational load on the sink, which only needs to process the voting outcomes. However, the downside is that broadcasting can consume significant bandwidth and increase traffic volume, potentially becoming unmanageable as the system scales up.

B – Reliance on AODV: The second scenario excludes broadcasting and relies solely on AODV. The sink node is considered to know the addresses of all potential candidates, which enables it to directly contact each node from a loop. Upon receiving the alert, nodes initiate a pair of key values containing their current battery level and ID. At this point, candidates directly unicast their values back to the sink node who requested help. The source is now responsible for determining the successor by comparing value pairs it has received. Upon reaching a conclusion, the node responds to the most suitable candidate, which in turn, will acknowledge its updated responsibilities. The main promise of the approach involves less traffic introduced into the network, crucial for a resource constrained context. On the other hand, performance might suffer from inefficient means of reaching candidate nodes, in addition to leaving the responsibility of interpreting the received information to the sink.

C – Hybrid means of communication: The third scenario combines both broadcasting and unicasting, due to lack of multicasting capabilities in the base-AODV protocol implementation within NS3. The initial alert is broadcasted in a multi-hop manner like the first case, but the actual processing of the event follows the second scenario, relying on unicasting. This scenario is expected to strike a balance between coverage and network load. Like the second scenario, processing favours network performance over sink.

Tables 1 and 2 outline the set of configuration parameters and input variables used across all simulation runs. These parameters establish the baseline environment and conditions under which the simulations are conducted. The main examination parameters are total throughput, average end-to-end delay, and the overall success rate of the designated security tasks.

Configuration parameters:

wifiPHY	802.11a	
wifiMac	AdhocWifiMac	
IP protocol	IPv4	
IP address space	10.0.0.0, 255.0.0.0	
Routing protocol	AODV	
Communication protocol	UDP	
Propagation loss model	Log Distance (exponent of 3)	
Propagation delay model	Constat (speed of light)	
Error rate model	YansErrorRateModel	
Frequency Band	5	GHz
Channel width	20	MHz
Channel number	36	
Rate control	ConstantRateMobilityModel	
Data rate	6	mbps
Control rate	6	mbps
RTS/CTS	Enabled	
Mobility model	ConstantPosition	
Grid width	5	nodes
Step y	10 + 40	m
Step x	10 + 40	m
Energy drain	0.017	A
Initial energy	15000	J

Table 1. Configuration parameters

Input variables:

Number of nodes	10, 25, 50, 75, 100
Number of security events	10
Number of dummy packets	1000, 1000
Number of regular packets	1000, 1000

Size of regular packets	508, 1400	bytes
Size of management packets	508	bytes
Size of security related packets	< 50	bytes
Simulation time	300	s
Security event interval	20	s
Security events start time	60	s
Management packet interval	90, 60	s
Regular packet interval	1, 0.5	s

Table 2. Input variables

6 Analysis of results

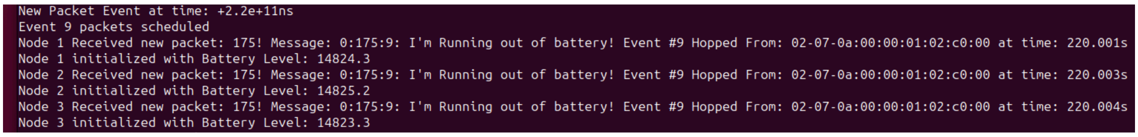
In this chapter, network performance is analysed based on the handling of the security events, total throughput, and average end-to-end latency.

6.1 Handling of the security event

The perceived success in handling security events is defined by two values: event coverage and result. Coverage refers to the percentage of responses the sink receives from all potential responses. This value is influenced by the detection rate of unique security packets and describes the degree of collective intelligence achievable. Result, on the other hand, is a simple evaluation of whether the system successfully identified and selected the most suitable candidate from among the responders. It is the most important metric, for assessing the functionality of the distributed security protocols. A security event is considered complete even in the case of a single response, however, such low coverage indicates sever issues in network performance.

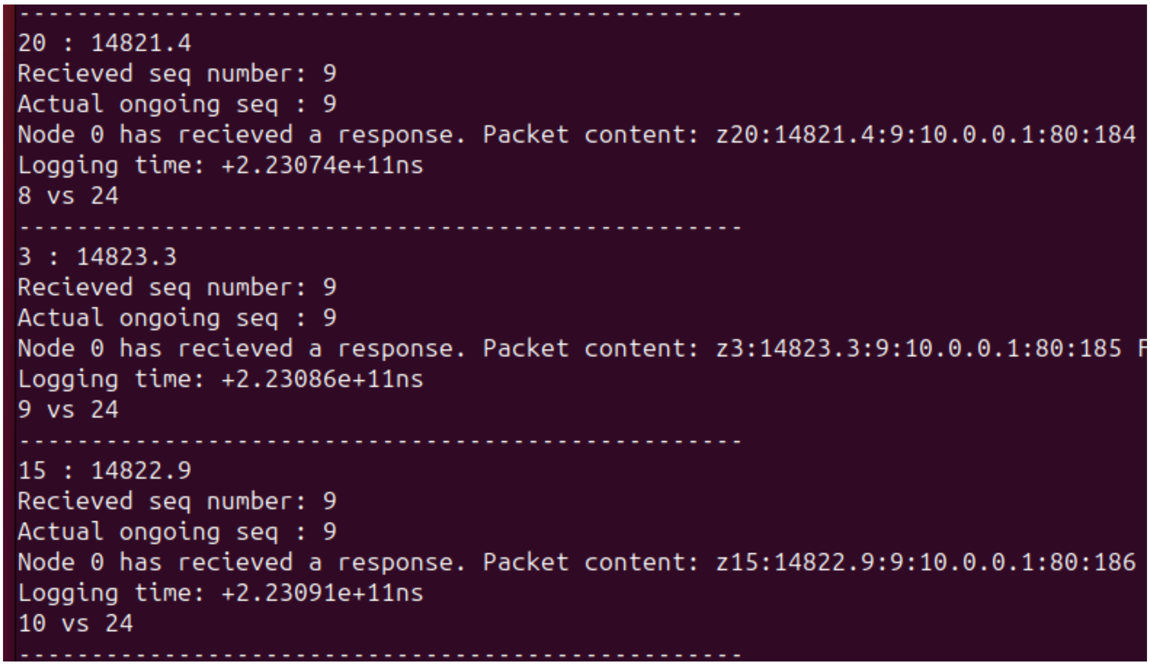
6.1.1 Result

Across all examined node counts, security events concluded with the most suitable candidate as the successor. These results were consistent for all approaches to distributing security information. The consistency was observed despite variations in coverage, throughput, or latency, indicating significant potential for ad hoc networking as a viable framework for distributed, computationally restricted systems, where security events are handled in an autonomous manner. Figures 1 to 3 depict key stages of the simulated process leading to the confirmation of the correct successor for B and C. Figures 4 to 7 depict key stages for A.



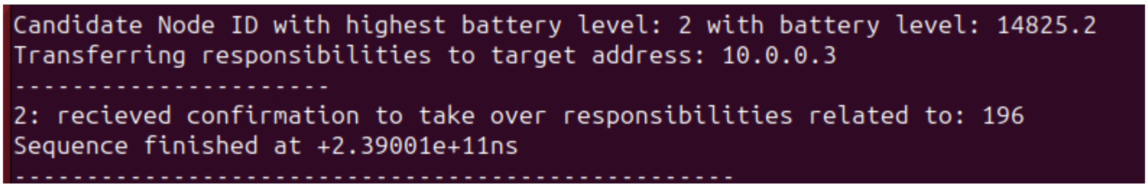
```
New Packet Event at time: +2.2e+11ns
Event 9 packets scheduled
Node 1 Received new packet: 175! Message: 0:175:9: I'm Running out of battery! Event #9 Hopped From: 02-07-0a:00:00:01:02:c0:00 at time: 220.001s
Node 1 initialized with Battery Level: 14824.3
Node 2 Received new packet: 175! Message: 0:175:9: I'm Running out of battery! Event #9 Hopped From: 02-07-0a:00:00:01:02:c0:00 at time: 220.003s
Node 2 initialized with Battery Level: 14825.2
Node 3 Received new packet: 175! Message: 0:175:9: I'm Running out of battery! Event #9 Hopped From: 02-07-0a:00:00:01:02:c0:00 at time: 220.004s
Node 3 initialized with Battery Level: 14823.3
```

Figure 1. The sink invokes a new security event prompting responses from available nodes



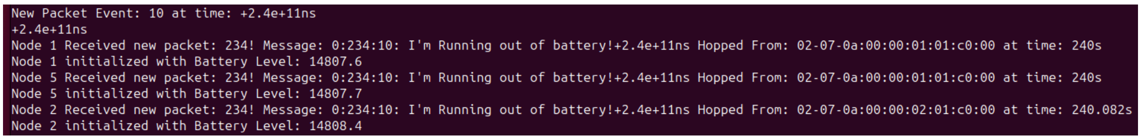
```
-------------------------------------------------
20 : 14821.4
Recieved seq number: 9
Actual ongoing seq : 9
Node 0 has recieved a response. Packet content: z20:14821.4:9:10.0.0.1:80:184
Logging time: +2.23074e+11ns
8 vs 24
-------------------------------------------------
3 : 14823.3
Recieved seq number: 9
Actual ongoing seq : 9
Node 0 has recieved a response. Packet content: z3:14823.3:9:10.0.0.1:80:185 F
Logging time: +2.23086e+11ns
9 vs 24
-------------------------------------------------
15 : 14822.9
Recieved seq number: 9
Actual ongoing seq : 9
Node 0 has recieved a response. Packet content: z15:14822.9:9:10.0.0.1:80:186
Logging time: +2.23091e+11ns
10 vs 24
-------------------------------------------------
```

Figure 2. Nodes responding to the alert



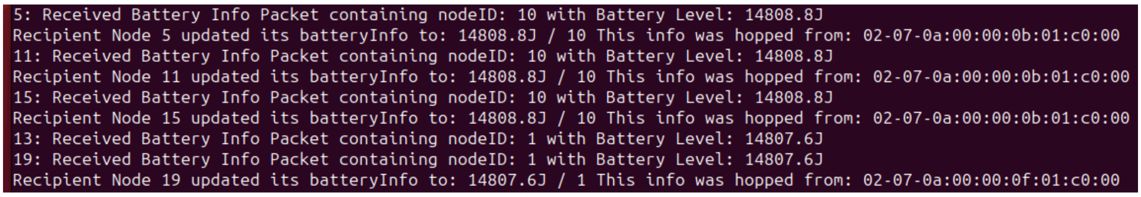
```
Candidate Node ID with highest battery level: 2 with battery level: 14825.2
Transferring responsibilities to target address: 10.0.0.3
----------------------
2: recieved confirmation to take over responsibilities related to: 196
Sequence finished at +2.39001e+11ns
-------------------------------------------------
```

Figure 3. For B and C, the sink evaluates the energy levels and signals to transmit responsibilities accordingly



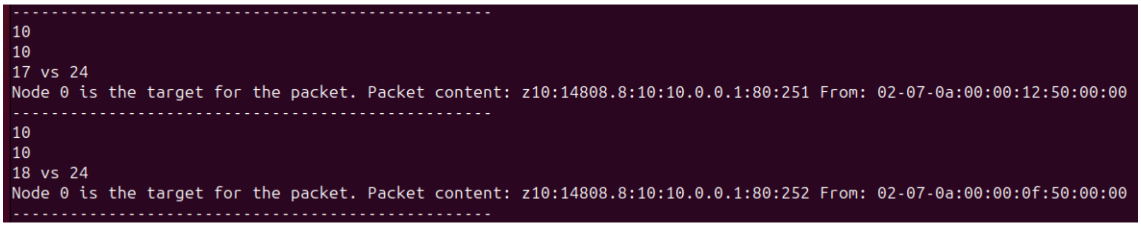
```
New Packet Event: 10 at time: +2.4e+11ns
+2.4e+11ns
Node 1 Received new packet: 234! Message: 0:234:10: I'm Running out of battery!+2.4e+11ns Hopped From: 02-07-0a:00:00:01:01:c0:00 at time: 240s
Node 1 initialized with Battery Level: 14807.6
Node 5 Received new packet: 234! Message: 0:234:10: I'm Running out of battery!+2.4e+11ns Hopped From: 02-07-0a:00:00:01:01:c0:00 at time: 240s
Node 5 initialized with Battery Level: 14807.7
Node 2 Received new packet: 234! Message: 0:234:10: I'm Running out of battery!+2.4e+11ns Hopped From: 02-07-0a:00:00:02:01:c0:00 at time: 240.082s
Node 2 initialized with Battery Level: 14808.4
```

Figure 4. The sink invokes a new security event prompting a response



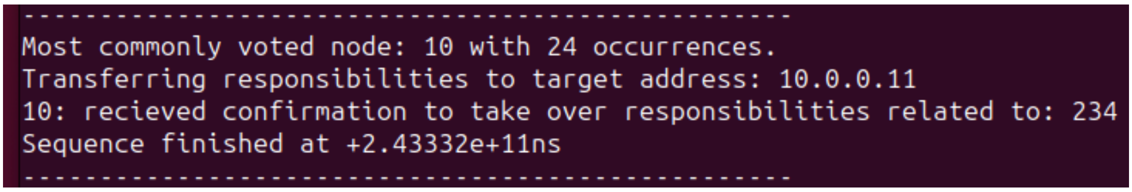
```
5: Received Battery Info Packet containing nodeID: 10 with Battery Level: 14808.8J
Recipient Node 5 updated its batteryInfo to: 14808.8J / 10 This info was hopped from: 02-07-0a:00:00:0b:01:c0:00
11: Received Battery Info Packet containing nodeID: 10 with Battery Level: 14808.8J
Recipient Node 11 updated its batteryInfo to: 14808.8J / 10 This info was hopped from: 02-07-0a:00:00:0b:01:c0:00
15: Received Battery Info Packet containing nodeID: 10 with Battery Level: 14808.8J
Recipient Node 15 updated its batteryInfo to: 14808.8J / 10 This info was hopped from: 02-07-0a:00:00:0b:01:c0:00
13: Received Battery Info Packet containing nodeID: 1 with Battery Level: 14807.6J
19: Received Battery Info Packet containing nodeID: 1 with Battery Level: 14807.6J
Recipient Node 19 updated its batteryInfo to: 14807.6J / 1 This info was hopped from: 02-07-0a:00:00:0f:01:c0:00
```

Figure 5. Nodes trade and update their knowledge on the highest energy level



```
-------------------------------------------------
10
10
17 vs 24
Node 0 is the target for the packet. Packet content: z10:14808.8:10:10.0.0.1:80:251 From: 02-07-0a:00:00:12:50:00:00
-------------------------------------------------
10
10
18 vs 24
Node 0 is the target for the packet. Packet content: z10:14808.8:10:10.0.0.1:80:252 From: 02-07-0a:00:00:0f:50:00:00
-------------------------------------------------
```

Figure 6. Sink node receives votes for the best candidate



```
-------------------------------------------------
Most commonly voted node: 10 with 24 occurrences.
Transferring responsibilities to target address: 10.0.0.11
10: recieved confirmation to take over responsibilities related to: 234
Sequence finished at +2.43332e+11ns
-------------------------------------------------
```

Figure 7. The sink evaluates vote count and signals to transmit responsibilities accordingly

While these results affirm the security protocol’s functionality as described in 5.4, subsequent analysis of metrics such as coverage, throughput, and latency will further determine the practicality of implementing these approaches in real-world network settings.

6.1.2 Coverage

Figure 8 present coverage in comparison to the size of the network. Both approaches leveraging broadcasting reached highly sufficient coverage across all node counts, with A experiencing slight deuteration of coverage when scaling up. C on the other hand maintained perfect coverage across all node counts. These results indicate high reliability in distributing the modelled security information within the network. B on the other hand displayed significant deuteration of coverage dropping down to 53 % at 50 nodes. Examining packet capture logs at nodes the loss of coverage centres around nodes furthest from the sink indicating distance, and the number of hops to have a significant influence in the case of unicasting security information. While not obvious, the slight downward trend of A is also a reason for concern. The modelled security traffic is extremely light. Increasing the size of this traffic via adding more complex security tasks, is likely to aggravate the displayed decline in a rapid fashion. For A, distance and the number of hops did not appear as significant, indicating the high amount of traffic generated by the security packet handling mechanisms as the main cause.

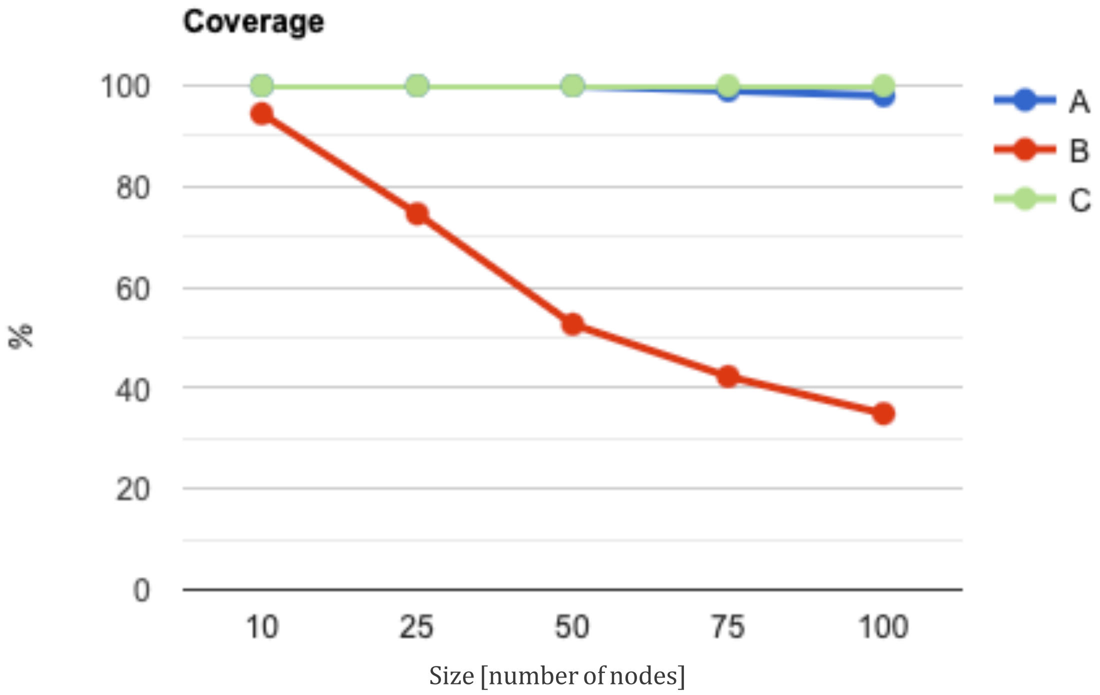


Figure 8. Coverage

A significant factor in coverage is packet delivery ratio (PDR). However, PDR cannot be uniformly measured across the scenarios. This is because broadcasting in a multi-hop manner involves significantly more instances of receptions than sending or forwarding events leading to challenges in quantifying packet delivery success rates. Therefore, instead of calculating PDR, the detection rate of unique security related packets is examined. This calculation involves logging each time a unique security packet is sent or forwarded, and received, enabling the comparison of the unique packets sent, and the cumulative number of unique packets seen by participating nodes. This effectively discards all duplicates of the same packet and highlights the likelihood at which a node receives at least one copy of a certain packet. The results of this comparison are presented in figure 9.

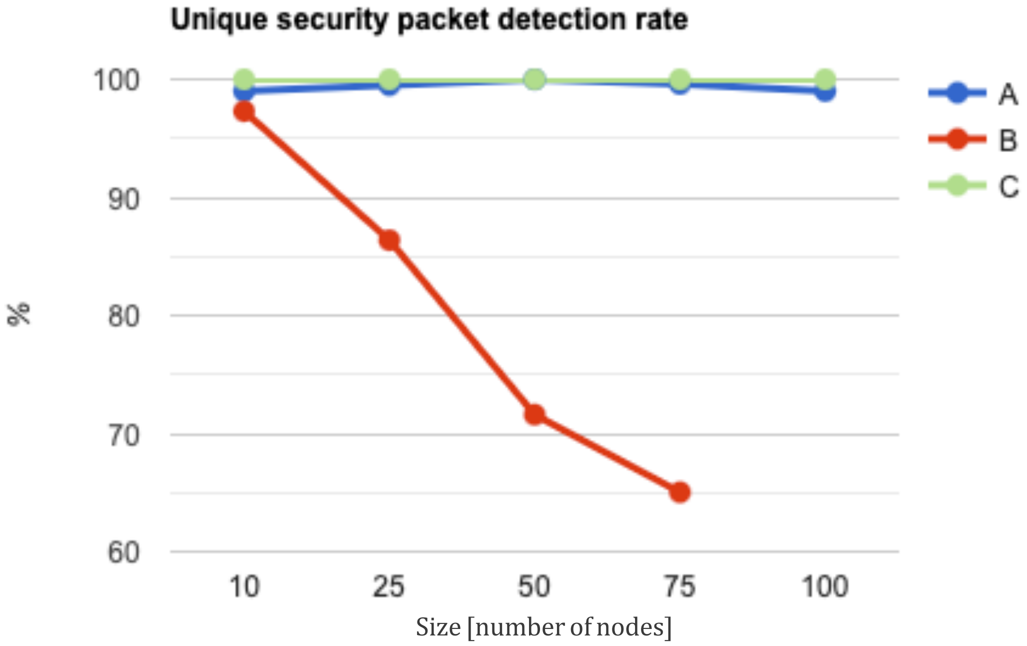


Figure 9. Detection rate of sent unique security packets

In figure 9 the overall trend mirrors that of coverage. B faces significant deuteration of detection rate when scaling up, eventually falling to 65 %. The reasons for this are twofold: First in the case of individually contacting each candidate, the time slot reserved for such functionality is likely to increasingly overlap with response traffic and the regular sensory data directed for the sink, overwhelming the node, and causing a significant point of congestion. Second, due to the nature of unicast traffic, processing security traffic may eventually lead to breaking past the overall thresholds set for a security event, rendering yet unfinished security traffic outdated. The reason why detection rate for B is slightly higher than coverage, is that the detection rate measures responses in relation to initial alerts received, while coverage compares them to the expected total. These results indicate significantly higher success in detecting responses over initial alerts. A response should not be sent if the alert has not been detected.

For A analysing the detection rate is more complex. While extremely shallow, the detection rate displays a curve. This indicates that scaling up the network to a point benefits the overall performance. The reason for such behaviour is linked to the multi-hop broadcasting mechanism. Adding more nodes, creates additional routes for traffic to reach each destination, ensuring that even if a single packet is lost, a copy of the same packet is likely to be received later. Due to the speed of broadcast traffic passing any thresholds is less likely. The downward curve, however, indicates that the amount of traffic eventually overwhelms the benefits gained from multiple routes. The fact why slight deuteration of unique packets at lower node counts does not impact coverage, is due to these packets being lost during the update sequence, which is exclusive to A. Losing packets during the update sequence only impacts the knowledge a single node has of other nodes, which is corrected by the voting mechanism.

Finally, C displays perfect detection rates of all unique packets sent. This is likely due to security event handling mechanism avoiding both major issues displayed by A and B. In C, the initial alert is effectively distributed via multihop broadcast mechanism, while the response traffic relies on uncasting. This balances the communication load placed on the sink, while also keeping overall security traffic at moderate, when comparing to the other two scenarios.

6.2 Average end-to-end latency

Average end-to-end latency measures the time it takes for a security related data packet to travel from the source to the destination across a network. It is calculated with the following formula:

$$Average\ End - to - End\ Latency = \frac{\sum(Latency\ of\ each\ packet)}{Number\ of\ packets}$$

Measuring average end-to-end latency is curial for defining the responsiveness of the target system. For time critical communications similar to the simulated security traffic, latencies below 10 ms can be considered sufficient. In table 3, the simulation results on average delay vs. the number of nodes across all scenarios are presented.

Average End-to-End Latency:

Size	A	B	C	Unit
10	0.213225	10.5155	0.8702	ms
25	0.225917	196.429	1.68635	ms
50	0.2313	1162.65	2.95754	ms
75	0.253825	2345.05	4.68113	ms
100	0.270981	N/A	6.73868	ms

Table 3. Average End-to-End Latency

Generally, the average end-to-end latency increases with more nodes introduced into the network. This trend is particularly apparent in B, where all communication is facilitated by AODV. A reaches extremely low latencies, operating below 0.1 ms on average even at 100 nodes. C also reaches sufficient latencies, peaking at 6.7 ms for 100 nodes. B however, experienced significant performance loss starting at 50 nodes, eventually averaging delays of 2.35 seconds at 75 nodes.

The significant delay in B is attributed to the functioning of the AODV routing protocol. Within B, the dissemination of the initial alert for security event is performed by the sink via individually contacting each of the candidate nodes. Due to long intervals between security events, there are no valid routes stored in the sink for each of the candidates whenever a new security event is initiated. This forces AODV to perform significant amount of route discovery. The resulting routing overhead is further increased with more nodes added to the network, which is significantly reflected in the rapid deuteration of the overall performance in B. These results are contrasted by A, which leverages multi-hop broadcasting for both the dissemination of the initial alert and the security information between candidates. Broadcasting avoids the overhead of route discovery in addition to RTS/CTS negotiations, ACK's and several other controls. It enables simultaneous message delivery to all nodes within range, reducing collisions and protocol complexity. While also leveraging unicasts for response traffic, the excessive broadcasting in A influence the average end-to-end latency in a significant manner. C combines elements from both approaches. It also leverages multi-hop broadcasting to disseminate the initial alert, but excludes any further broadcasting, and relies on direct responses from each of the candidate nodes. Even so, the resulting latencies are extremely low. The achieved latency can be attributed to two major factors: first the routing related load is distributed between candidate nodes. Unlike the initial alert, each of the candidate nodes are required to find a single route to the destination. Second, some routing information on the sink node is already present at candidate nodes due to regular traffic. The reason why C is slightly slower than A, is the number of broadcasts sent, which influences the average latency. Overall, the latencies in A and C can be considered highly sufficient for transmitting time critical information. That being said, the regular traffic targeting the sink node favours low latencies. It is expected that initiating the security event from a node other than the sink, would meet slightly higher latencies in all scenarios, while the overall trend would remain consistent.

6.3 Throughput

Total throughput represents the cumulative amount of data successfully transmitted across the network over a given period. It is calculated with the following formula:

$$Throughput = \frac{Total\ Data\ Transferred}{Total\ Time\ Taken}$$

Measuring total throughput across different node counts enables the observation and analysis of network performance under varying conditions. Variation in total throughput is in essence a measure of scalability for both, the size and complexity of tasks. The theoretical maximum throughput for a single link is set by the NS3 ConstantRateWifiManager at 6 Mbps. However, considering the restricted nature of the simulated environment, the actual throughput should remain significantly below the theoretical maximum. Particularly, for security related traffic, ensuring moderate consumption of bandwidth while preserving high success rate is essential. In table 4 the simulation results on total-, and security related throughputs vs. number of nodes are compared between scenarios. The behaviour of total throughput is further highlighted in figure 10.

Total Throughput and Security-Related Throughput:

	A) Broadcasted consensus		B) Reliance on AODV		C) Hybrid approach		
Size	Total Throughput	Sec. Throughput	Total Throughput	Sec. Throughput	Total Throughput	Sec. Throughput	Unit
10	39042	1301	37905	164	38110	369	bps
25	110012	9604	94781	375	101522	1114	bps
50	240511	37893	178026	591	204975	2358	bps
75	389403	87299	240300	822	305698	3580	bps
100	549246	150527	N/A	N/A	403612	4758	bps

Table 4. Total throughput and security-related throughput

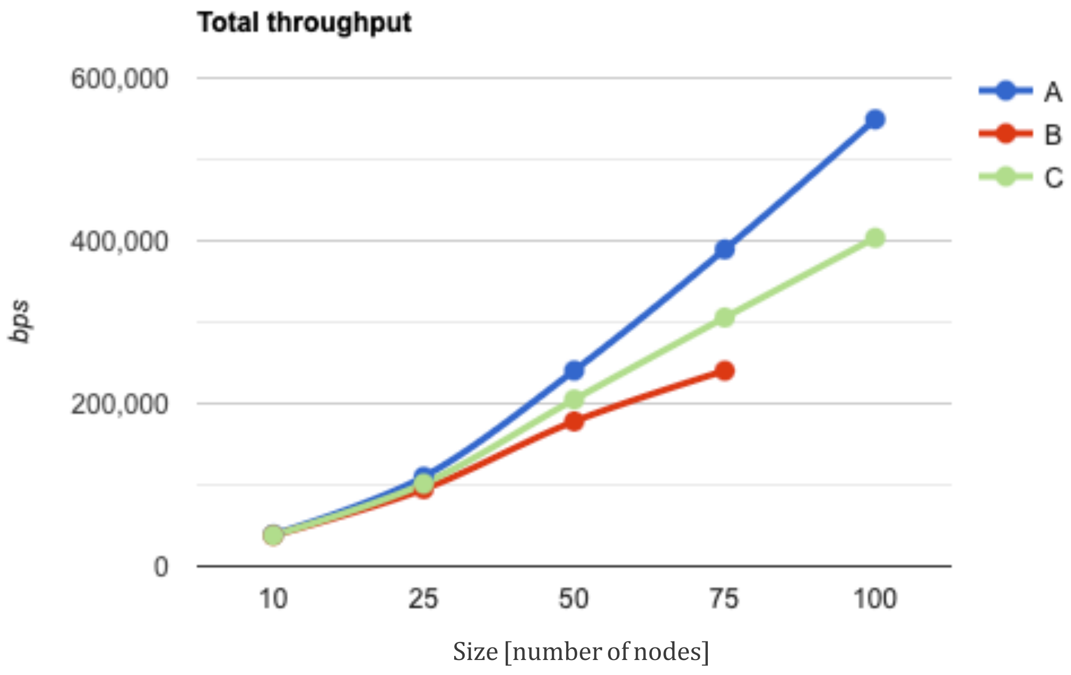


Figure 10. Total throughput

From table 4 we can observe steady increase in throughput across different node counts for A and C. A sees consistently highest values reaching 549246 bps at 100 nodes. C comes relatively close reaching 403612 bps at 100 nodes. B however, was unable to withstand 100 nodes, and reached a throughput of 240300 bps on 75 nodes. Focusing on regular traffic, A and C reach comparable values across all node counts, while B fell behind approximately 20 % at 75 nodes. Consequently, both A and C achieve high success rate of the security event, with minimal impact on regular traffic across all node counts. The deteriorating throughput in B indicates sever scalability issues, which impact both regular and security traffic. Due to the configuration of the baseline environment the observed variation is attributed to the handling of security traffic within each scenario. This factor is further illustrated by figure 11, which highlights the relative utilization rate of security traffic or the portion of security related traffic, from total throughput.

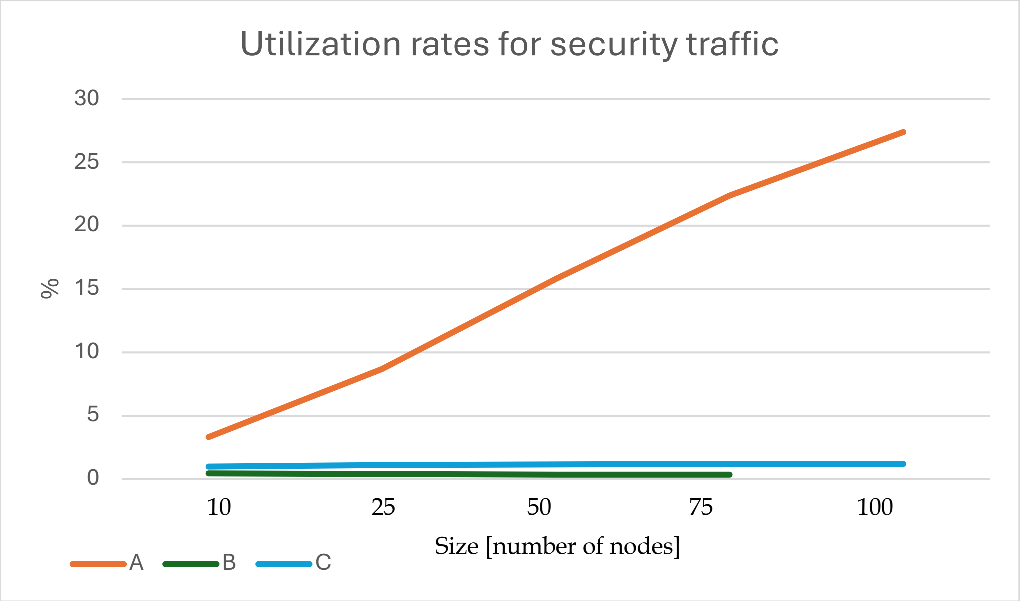


Figure 11. Utilization rate of security traffic

From Figure 11. It becomes obvious that the number of nodes has a significant impact on the portion of security traffic in A. The result is expected, as distributing information via multi-hop broadcasting becomes an increasingly challenging task with more participants. Contrasting the utilization rates at 100 nodes between A and C it becomes clear that excessive broadcasting is an unsustainable mechanism. With significant increase in security related packets sent across all node counts, the time nodes are required to spend transmitting or receiving increases in A, which has significant implications on the battery lifetime of each unit. In addition, with more traffic, the likelihood of collisions, congestion, packet loss, and other types of instability increase, eventually leading to a reduced total throughput. On the other hand, both B and C display a stark contrast with steady consumption of network resources across all node counts. However, while the portion of security traffic stays consistent, the complexity of reaching all candidates become more difficult. As clearly highlighted in terms of latency and total throughput, B experiences significant deterioration of performance when scaling up. In the case of throughput, the issue is congestion at the sink node. The sink is already the destination for the sensory data sent by each node. In the case of B it is also responsible for contacting each of the candidates. The result is that B is in constant state of transmission and receiving, which leads to 20% reduction in total throughput compared to C. Furthermore, as highlighted by the average delay, this state of congestion spans over 20 seconds which is the maximum timeframe for a single security event. In terms of throughput, C appears most reliable.

6.4 Summary of simulation results

The simulation revealed several insights into the behaviour of wireless sensor networks (WSNs) within an ad hoc networking framework.

Ad Hoc Networking Considerations:

- Throughput: In WSN context, the network displayed more than sufficient throughput, predominantly around the sink node. This suggests that even complex and heavier traffic patterns could be accommodated.
- Latency: Latencies significantly depended on the availability of existing routes. This proves proper tuning of routing protocols to the specific network context essential. When appropriately configured, latency did not compromise the delivery of time-critical services.
- Routing Dynamics: Regular traffic facilitated up to date routes for reaching the sink. However, the sink experienced challenges in reaching out to other nodes, requiring considerable route discovery for each of the events. In addition, due to links becoming congested, the optimal routes changed, which introduced control traffic and potential delay in rediscovering broken links. Mobility is expected to exacerbate these effects.
- Mobility and AODV: The mobility of nodes impacted the effectiveness of the base AODV routing protocol. With constant positions, frequent route updates (every 3 seconds) were unnecessary, suggesting that less frequent updates would have sufficed, depending on node mobility.
- Topology: The physical topology of the network markedly influenced performance. More nodes created more routes, and thus higher reliability. Scaling up in size would eventually overrun these benefits due to the amount of data directed at the sink.
- Reliability: In the case of an urgent task requiring cooperation between network nodes, the ad hoc paradigm was proven a valid solution for reaching the necessary help in a self-organized way, without relying on any existing infrastructure. This “service” was available despite some links missing.

- Scalability: The simulated network was tested in various node counts up to 100 nodes, with the promise of further scaling. The results indicate significant and foremost easy scaling of the entire network.
- Management: Setting up and scaling up the network required no additional configuration highlighting the self-configuring and self-maintaining nature of ad hoc networks. When a device was configured for ad hoc mode operation, adding it, was fast and straightforward, leading to significantly reduced management load, working extremely well in tandem with the autonomous, decentralized handling of security events simulated.

Approach-Specific Considerations:

- Scenario A: Showed high coverage and extremely low latencies due to extensive broadcasting, which, while fast, resulted in a high duplication rate of packets. The intense broadcasting demonstrated potential for handling more frequent and complex security traffic but raised concerns about sustainability in a resource-constrained system. The collective intelligence approach in Scenario A led to a deeper exchange of information among nodes, though the feasibility of broadcasting this information in real-world setting is questionable. For this approach, introducing a hop counter, which decrease after each rebroadcast could prove significant improvement.
- Scenario B: Managed a balanced load with relatively low coverage, which was sufficient for the simulation's tasks. The approach was efficient for tasks requiring localized responses, making it suitable for operations where proximity is crucial. However, the higher delays observed could hinder mission-critical applications, suggesting a need to explore alternative routing protocols or configurations.
- Scenario C: Achieved the highest coverage with low latencies and adequate throughput, placing minimal strain on resources. The strategy of using initial broadcasts to alert nodes, followed by direct responses, proved effective. Regular traffic facilitated the establishment of responsive routes. Yet, reliance on broadcasting may only be practical in controlled settings and does not address security concerns like authentication and encryption, which require further investigation.

The simulation underscored the potential of ad hoc networking in distributing security responsibilities among IoT nodes, even under constraints. Each scenario highlighted different strengths and weaknesses, offering valuable insights into how ad hoc networking could be leveraged for security tasks in IoT environments. Further studies are needed to address unresolved issues such as secure authentication and the practical implementation of encryption in such networks. In terms of collective intelligence, A displayed depth, albeit in a simple form, via reaching consensus between candidates, which came costly, while B and C relied on smart decision making based on the collective information gathered from individual network nodes. Based on the achieved results, following studies should focus on enhancing the distribution of security information and decision making in C, to enable experimentation with more complex security tasks, requiring the collective intelligence of multiple network nodes. Such approach could involve more recent routing protocols, and the introduction and fuzzification of additional variables.

Limitations: The limitations for the simulation artifact must also be considered. The simulation artifact is a simplified representation of a real-world application. Improvements are required in terms of realism and generalization of the model. The environment used, leverages a static grid layout. This reflects the nature of WSN's, but it does not account for depth, which has potential impact on distances. In addition, the simulation parameters set up a favourable environment for communications. Different topologies, mobility -, propagation loss -, and delay models should be experimented with to generalize results across more categories of IoT networks. Also, the controlled environment consists of nodes which are trusted. This is also a basic assumption for AODV routing protocol (Perkins et al. 2003). The scenario does not consider for potential adversarial impact on the network. Furthermore, the baseline environment is using widely popular, but outdated standards and protocols for most operations. For example, the WiFi 802.11a could be replaced with more recent amendments and future work should also consider experimenting with other low-level protocols like ZigBee and Bluetooth Low Energy. The same applies for routing, where AODV was used in default settings. Changing some of the defaults would have significant potential in improving functionality within the network, especially when a protocol designed for mobile networks is used in a static context. Different Ad hoc routing protocols should also be considered, and their effects compared. Future work would also benefit from extending the analysis with detailed experimentation of the expected system lifetime. Energy consumption should be monitored in detail and compared with traditional means of handling security events. Finally, extending the model with more complex security functionality and diversity in the way these events are detected, initiated, and handled is critical for working towards applicable solutions and the consolidation of IoT security.

7 Discussion

Challenges in resource constrained IoT environments are rooted in miniaturisation of hardware designed for a certain purpose. This concept, shaped by market forces that aspire for maximum efficiency at minimum cost, result in various challenges which impact the overarching concept of IoT security. These challenges encompass device related issues like lack of power and support for the expected lifecycle. They involve concern for network performance over wireless medium, impacting the timely availability of systems and the data they generate. There are also system related challenges, like the variation among devices themselves and the operational environment they are deployed on.

In response to these challenges, academic literature has identified numerous promising advances. For example, fog computing, novel sensing strategies, advanced security algorithms, and standardization efforts help address the limitations imposed by resource scarcity. The direction of identified solutions emphasise local processing capabilities, reduce the power consumption needed for constant connectivity, and prompt advanced security features and compliance with security standards, thus mitigating the impact of limited resources on reliability, device functionality and network performance.

Ad hoc networking, with its inherent benefits, aligns well with these identified solutions. The decentralized nature of ad hoc networks mitigates the need for any central infrastructure, which can be resource-intensive and restrictive. This model supports efficient data transmission by reducing distance and hops between network segments required to convey information, aligning with time critical events, and the energy-efficient strategies essential in IoT environments. It inherently supports distribution of processing capabilities among peers, allowing real-time data handling and decision-making, which improves response times and reduces the load on the network. Moreover, the flexibility and scalability of ad hoc networks allow for the dynamic inclusion and reconfiguration of devices without extensive overhead or reprogramming, which is crucial in managing the heterogeneous nature of IoT devices and their varied capabilities.

Further, ad hoc networking brings additional benefits that, while not directly reflected in the discussed solutions, are valuable to resource constrained IoT networks. For instance, the capability for rapid deployment and self-configuration of ad hoc networks is particularly beneficial in extending connectivity. The routing requirements of modern IoT systems involve various dynamics such as nodes requiring constant connectivity, joining, or leaving the network or going offline, which are built into ad hoc routing protocols. Additionally, the resilience of ad hoc networks to node failures and other interruptions enhances system reliability and service availability, as the network can continue to function effectively even when individual links fail or are powered down to conserve energy. Also, most ad hoc networks operate using standard protocols such as 802.11 or 802.15.4. This means that as long as the device supports the necessary protocol, it can participate in the network. In addition, the devices operate in peer-to-peer mode, which enables any device to communicate directly with other devices in the network, while also introducing minimal interference, and thus conserve bandwidth.

This alignment is further validated via the developed simulation artefact. The artifact demonstrated highly sufficient network performance for security traffic in terms of latency and throughput. Additionally, the work displayed the feasibility of autonomous, decentralized means of handling simple security events via resource-constrained systems based on ad hoc networking akin to local processing. The decentralized approach also leveraged the collective knowledge of the participating nodes, reducing the reliance on any central management entity or human intervention, suggesting potential for building more complex security overlays on top of the ad hoc mode of operation.

The promise of this approach scales extremely well with the recent changes in standardization, forcing manufactures to incorporate security functionality into their devices. Rather than a complete redesign of their products, changing the mode of operation, and enabling local processing of security related tasks based on efficient distribution of security functionality, has significant promise in achieving the level of security required by standards. Not as a product of individuals secured, but as the collective pool of resources from the network.

However, several considerations exist before applying ad hoc networking in a practical setting. While ad hoc networking support local processing of data, conserving energy otherwise used for data transmission outside the local network, these benefits must be balanced with the energy requirements each node has when participating in routing and maintenance activity in ad hoc networks. Therefore, further research is required to compare the energy drain of the two methods. Also, more work is required to identify and examine ad hoc routing protocols best suited for IoT networks. Specifically, there is a need to optimize control traffic and the re-discovery of broken links, as the traffic patterns and nodes moving cause optimal routes to change frequently. Another limiting factor is the open and decentralized nature of ad hoc networks which makes them suspectable to various security threats, including man-in-the-middle attacks, eavesdropping, and node replication attacks. Although ad hoc networking enables development of novel security solutions, the challenges stemming from the lack of centralized authority must be carefully considered and accounted for. In the simulation artefact for example, the baseline environment is expected to be controlled, and each of the nodes trusted. Real world applicability requires foremost features for ensuring trust among the participating nodes. Other concerns involve the cost of systems capable of sophisticated security functionalities, careful consideration for node placement and the physical topology of the networks for establishing successful coverage, in addition to overcoming the physical constraints of these devices.

8 Conclusion

In conclusion, this work has highlighted ad hoc networking as a suitable communication framework for light weight, scalable and dynamic networks, which enables decentralized communication between the nodes of the network to achieve a common goal. It shows that while individually securing each of the resource constrained devices is not realistic, by relying on the collective resources from a network of such devices, the overall reliability of the system can be improved. Key factors identified from the simulation artifact that affect these results are the physical topology of the network and the availability of existing routes between nodes. However, the practicality of this approach relies on technical advancements and the careful consideration for security and sustainability. Future research is required to validate the practical approaches and to accurately capture the potential of the ad hoc mode of operation, for distributed handling of security events among the nodes of the network.

REFERENCES

A. Kurniawan, P. Kristalina and M. Z. S. Hadi. (2020) "Performance Analysis of Routing Protocols AODV, OLSR and DSDV on MANET using NS3," *2020 International Electronics Symposium (IES)*, Surabaya, Indonesia, pp. 199-206. https://doi.org/10.1109/IES50839.2020.9231690

Abdmeziem, M. R., Tandjaoui, D., & Romdhani, I. (2016). Architecting the internet of things: state of the art. *Robots and Sensor Clouds*, 55-75. https://doi.org/10.1007/978-3-319-22168-7_3

Aboubakar, M, Mounir K, and Pierre Roux. (2021) "A review of IoT network management: Current status and perspectives." *Journal of King Saud University-Computer and Information Sciences* 34.7: 4163-4176.

Ade, S. A., & Tijare, P. A. (2010). Performance comparison of AODV, DSDV, OLSR, and DSR routing protocols in mobile ad hoc networks. *International Journal of Information Technology and Knowledge Management, 2*(2), 545-548.

Afanasyev, M., Chen, T., Voelker, G. M., & Snoeren, A. C. (2010). Usage patterns in an urban WiFi network. *IEEE/ACM Transactions on Networking*, *18*(5), 1359-1372. https://doi.org/10.1109/TNET.2010.2040087.

Agrawal, R., Faujdar, N., Romero, C. A. T., Sharma, O., Abdulsahib, G. M., Khalaf, O. I., ... & Ghoneim, O. A. (2023). Classification and comparison of ad hoc networks: A review. *Egyptian Informatics Journal*, *24*(1), 1-25. https://doi.org/10.1016/j.eij.2022.10.004

Ahmed Gad-Elrab Ahmed, A. (2019). Benefits and Challenges of Internet of Things for Telecommunication Networks. IntechOpen. https://doi.org/10.5772/intechopen.81891

Ahmed, D. E. M., & Khalifa, O. O. (2017). An overview of MANETs: applications, characteristics, challenges and recent issues. https://www.ijeat.org/wp-content/uploads/papers/v6i4/D4927046417.pdf

Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer networks*, *56*(2), 940-965. https://doi.org/10.1016/j.comnet.2011.10.011

Alqarawi, G., Alkhalifah, B., Alharbi, N., & El Khediri, S. (2023). Internet-of-things security and vulnerabilities: case study. *Journal of Applied Security Research*, *18*(3), 559-575. https://doi.org/10.1080/19361610.2022.2031841

Anastasi, G., Conti, M., & Gregori, E. (2004). IEEE 802.11 ad hoc networks: Protocols, performance, and open issues. *Mobile Ad hoc networking*, 69-116. https://doi.org/10.1002/0471656895.ch3

Babu, C. S., Saltonya, M. S., Ganapathi, S., & Gunasekar, A. (2024). AIoT Revolution: Transforming Networking Productivity for the Digital Age. In *Artificial Intelligence of Things (AIoT) for Productivity and Organizational Transition* (pp. 108-143). IGI Global. https://doi.org/10.4018/979-8-3693-0993-3.ch005

Bhagya Nathali Silva, Murad Khan & Kijun Han (2018) Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges, IETE Technical Review, 35:2, 205-220, https://doi.org/10.1080/02564602.2016.1276416

Bhatia, D., & Sharma, D. P. (2016). A comparative analysis of proactive, reactive and hybrid routing protocols over open source network simulator in mobile ad hoc network. *International Journal of Applied Engineering Research*, *11*(6), 3885-3896. https://www.researchgate.net/publication/301679418_A

Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. *IEEE Communications magazine*, *39*(12), 86-94. https://doi.org/10.1109/35.968817

Bitdefender. (2023). *2023 IoT Security Landscape Report*. Retrieved from https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

Bor, M. C., Vidler, J., & Roedig, U. (2016). LoRa for the Internet of Things. In *Ewsn* (Vol. 16, pp. 361-366). https://core.ac.uk/download/pdf/42415697.pdf

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer networks*, *55*(13), 3032-3080. https://doi.org/10.1109/ACCESS.2019.2902072

Boulaiche, M. (2020). Survey of secure routing protocols for wireless ad hoc networks. *Wireless Personal Communications*, *114*(1), 483-517. https://doi.org/10.1007/s11277-020-07376-1

Breslau, L., Estrin, D., Fall, K., Floyd, S., Heidemann, J., Helmy, A., ... & Yu, H. (2000). Advances in network simulation. *Computer*, *33*(5), 59-67. https://doi.org/10.1109/2.841785

Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796. https://doi.org/10.3390/s18092796

Cano, J.; Berrios, V.; Garcia, B.; Toh, C. (2018). Evolution of iot: An industry PErsPEctivE. IEEE Internet of Things Magazine. 1(2):2-7. https://doi.org/10.1109/IOTM.2019.1900002

Caputo, C. (2014). Wireless Network Video. In Digital Video Surveillance and Security. https://doi.org/10.1016/B978-0-12-420042-5.00005-8

Chen, B., Wan, J., Celesti, A., Li, D., Abbas, H., & Zhang, Q. (2018). Edge computing in IoT-based manufacturing. *IEEE Communications Magazine*, *56*(9), 103-109. https://doi.org/10.1109/MCOM.2018.1701231

Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of things journal*, *3*(6), 854-864. https://doi.org/10.1109/JIOT.2016.2584538

Cilfone, A., Davoli, L., Belli, L., & Ferrari, G. (2019). Wireless mesh networking: An IoT-oriented perspective survey on relevant technologies. *Future internet*, *11*(4), 99. https://doi.org/10.3390/fi11040099

Clausen, T., & Jacquet, P. (2003). RFC3626: Optimized link state routing protocol (OLSR). https://doi.org/10.17487/RFC3626

David, R., Duke, J., Jain, A., Janapa Reddi, V., Jeffries, N., Li, J., ... & Rhodes, R. (2021). Tensorflow lite micro: Embedded machine learning for tinyml systems. *Proceedings of Machine Learning and Systems*, *3*, 800-811. https://doi.org/10.48550/arXiv.2010.08678

Devi, M., & Gill, N. S. (2019). Mobile ad hoc networks and routing protocols in IoT enabled. *J. Eng. Appl. Sci*, *14*(3), 802-811. https://doi.org/10.36478/jeasci.2019.802.811

Digi International. (n.d.). Zigbee wireless standard. Retrieved May 3, 2024. https://fr.digi.com/solutions/by-technology/zigbee-wireless-standard

Eltahlawy, A. M., Aslan, H. K., Abdallah, E. G., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). A Survey on Parameters Affecting MANET Performance. *Electronics*, *12*(9), 1956. https://doi.org/10.3390/electronics12091956

European Cyber Resilience Act. (n.d.). Retrieved May 3, 2024, https://www.european-cyber-resilience-act.com

Farsi, M., Elhosseini, M. A., Badawy, M., Ali, H. A., & Eldin, H. Z. (2019). Deployment techniques in wireless sensor networks, coverage and connectivity: A survey. *Ieee Access*, *7*, 28940-28954. https://doi.org/10.1109/ACCESS.2019.2902072

Ficco, M., Guerriero, A., Milite, E., Palmieri, F., Pietrantuono, R., & Russo, S. (2024). Federated learning for IoT devices: Enhancing TinyML with onboard training. *Information Fusion*, *104*, 102189. https://doi.org/10.1016/j.inffus.2023.102189

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, *5*(4), 2483-2495. https://doi.org/10.1109/JIOT.2017.2767291

Fu, H., Khodaei, Z. S., & Aliabadi, M. F. (2018). An event-triggered energy-efficient wireless structural health monitoring system for impact detection in composite airframes. *IEEE Internet of Things Journal*, *6*(1), 1183-1192. https://doi.org/10.1109/JIOT.2018.2867722

Gamatie, A., Devic, G., Sassatelli, G., Bernabovi, S., Naudin, P., & Chapman, M. (2019). Towards energy-efficient heterogeneous multicore architectures for edge computing. *IEEE Access*, *7*, 49474-49491. https://doi.org/10.1109/ACCESS.2019.2910932

Gomez, J., Kfoury, E. F., Crichigno, J., & Srivastava, G. (2023). A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, *237*, 110054. https://doi.org/10.1016/j.comnet.2023.110054

Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in internet of things: features, techniques and research challenges. *Int. J. Comput. Intell. Res*, *13*(7), 1617-1627. https://www.academia.edu/download/88799654/ijcirv13n7_06.pdf

Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. *Sensors*, *22*(10), 3744. https://doi.org/10.3390/s22103744

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721-82743. https://doi.org/10.1109/ACCESS.2019.2924045

Hassnawi, L. A., Ahmad, R. B., Yahya, A., Aljunid, S. A., & Elshaikh, M. (2012). Performance analysis of various routing protocols for motorway surveillance system cameras' network. *International Journal of Computer Science Issues (IJCSI)*, *9*(2), 7. https://www.researchgate.net/publication/235047709

Hernandez-Jayo, U., Mammu, A. S. K., & De-la Iglesia, I. (2014). Reliable communication in cooperative ad hoc networks. *Contemporary Issues in Wireless Communications*. https://doi.org/10.5772/59041

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105. https://doi.org/10.2307/25148625

Hoang, T., & Spencer Jr, B. F. (2022). Autonomous wireless smart sensor for monitoring of railroad bridges. University of Illinois. https://hdl.handle.net/2142/114403

IEEE 802 LMSC. (n. d.). Retrieved May 3, 2024, Ieee802.org

Institute of Electrical and Electronics Engineers. (2003). IEEE standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (ANSI/IEEE Std 802.11, 1999 Edition (R2003)). https://doi.org/10.1109/IEEESTD.2003.95617

Institute of Electrical and Electronics Engineers. (2020). Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)* , vol., no., pp.1-4379, 26 Feb. 2021, https://doi.org/10.1109/IEEESTD.2021.9363693

International Telecommunication Union. (2005) ITU Internet Report 2005: The Internet of Things, International Telecommunication Union. https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

IoT Analytics. (2023). https://iot-analytics.com/number-connected-iot-devices/

Ishmael, J., Bury, S., Pezaros, D., & Race, N. (2008). Deploying rural community wireless mesh networks. *IEEE Internet Computing*, *12*(4), 22-29. https://doi.org/10.1109/MIC.2008.76

ISO. (2014). Economic benefits of standards. https://www.iso.org/publication/PUB100403.html

Johnson, D., Hu, Y. C., & Maltz, D. (2007). RFC 4728: The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. https://dl.acm.org/doi/abs/10.17487/rfc4728

Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: an up-to-date survey. *Applied system innovation*, *3*(1), 14. https://doi.org/10.3390/asi3010014

Ketshabetswe, L., Zungeru, A., Mangwala, M., Chuma, J., & Sigweni, B. (2019). Communication protocols for wireless sensor networks: A survey and comparison. Botswana International University of Science and Technology. https://doi.org/10.1016/j.heliyon.2019.e01591

Khan, R., & Tariq, A. (2018). A Survey on Wired and Wireless Network. *Lahore Garrison University Research Journal of Computer Science and Information Technology*, *2*(3), 19-28. https://doi.org/10.54692/lgurjcsit.2018.020350

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics*, *8*(11), 1210. https://doi.org/10.3390/electronics8111210

Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., & Bizon, N. (2021). State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability*, *13*(16), 9463. https://www.mdpi.com/2071-1050/13/16/9463

Lee, J. H., Park, M. -S., & Shah, S. C. "Wi-Fi direct based mobile ad hoc network," 2017 2nd International Conference on Computer and Communication Systems (ICCCS), Krakow, Poland, 2017, pp. 116-120. https://doi.org/10.1109/CCOMS.2017.8075279

Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*, *149*, 106854. https://doi.org/10.1016/j.cie.2020.106854

Mahmoud, M. S., & Mohamad, A. A. (2016). A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications. University of Embu. http://dx.doi.org/10.4236/ait.2016.62002

Maitra, S., Richards, D., Abdelgawad, A., & Yelamarthi, K. (2019, March). Performance evaluation of IoT encryption algorithms: memory, timing, and energy. In *2019 IEEE sensors applications symposium (SAS)* (pp. 1-6). IEEE. https://doi.org/10.1109/SAS.2019.8706017

Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., Corchado, J. M., & AETiC, A. (2019). Blockchain technology in IoT systems: review of the challenges. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516-0281. https://doi.org/*10.33166/AETiC.2019.05.003*

Mocnej, J., Seah, W. K., Pekar, A., & Zolotova, I. (2018). Decentralised IoT architecture for efficient resources utilisation. *IFAC-PapersOnLine*, *51*(6), 168-173. https://doi.org/10.1016/j.ifacol.2018.07.148

Nsnam.org. (2023). https://www.nsnam.org

nycmesh.net. (n.d.) NYC Mesh. Retrieved May 6. 2024. https://www.nycmesh.net

OPAL. (n.d.) Decentralized Battle Management. Retrieved May 6. 2024. https://www.iai.co.il/p/opal

Paliwal, M., & Saraswat, P. (2022). IoT and Wireless Communications: An Overview. *International Journal of Innovative Research in Computer Science & Technology*, *10*(1), 92-96. https://doi.org/10.55524/ijircst.2022.10.1.16

Patel, N. D., Mehtre, B. M., & Wankar, R. (2019). Simulators, emulators, and test-beds for internet of things: A comparison. In *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 139-145). IEEE. https://doi.org/10.1109/I-SMAC47947.2019.9032519

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM computer communication review*, *24*(4), 234-244. https://doi.org/10.1145/190809.190336

Perkins, C. E., Royer, E. M., Das, S. R., & Marina, M. K. (2001). Performance comparison of two on-demand routing protocols for ad hoc networks. *IEEE Personal communications*, *8*(1), 16-28. https://doi.org/10.1109/98.904895

Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, https://www.rfc-editor.org/info/rfc3561

Pinto, S., & Santos, N. (2019). Demystifying arm trustzone: A comprehensive survey. *ACM computing surveys (CSUR)*, *51*(6), 1-36. https://doi.org/10.1145/3291047

Qiu, H. J. F., Ho, I. W.-H., Tse, C. K., & Xie, Y. (2017). A methodology for studying 802.11p VANET broadcasting performance with practical vehicle distribution. *Intelligent Assistive Technology and Systems Lab, University of Toronto; Department of Electronic and Information Engineering, The Hong Kong Polytechnic University*. https://arxiv.org/pdf/1410.3978.pdf

Qureshi, I. A., & Asghar, S. (2023). A systematic review of the IEEE-802.11 standard's enhancements and limitations. *Wireless Personal Communications*, *131*(4), 2539-2572. https://doi.org/10.1007/s11277-023-10553-7

Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022b). Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wireless Personal Communications*, *125*(4), 3501-3525. https://doi.org/10.1007/s11277-022-09722-x

Quy, V. K., Nam, V. H., Linh, D. M., Ban, N. T., & Han, N. D. (2022a). Communication solutions for vehicle ad-hoc network in smart cities environment: A comprehensive survey. *Wireless Personal Communications*, *122*(3), 2791-2815. https://doi.org/10.1007/s11277-021-09030-w

Ramanathan, R., & Redi, J. (2002). A brief overview of ad hoc networks: challenges and directions. *IEEE communications Magazine*, *40*(5), 20-22. https://doi.org/10.1109/MCOM.2002.1006968

Rao, K. P. K., & Kalaiarasi, K. (2015). A Survey on IEEE Standards for Mobile Ad Hoc Networks. *IOSR Journal of Engineering*, *5*(02), 55-64. https://www.iosrjen.org/Papers/vol5_issue2%20(part-2)/I05225564.pdf

Reina, D. G., Toral, S. L., Barrero, F., Bessis, N., & Asimakopoulou, E. (2013). The role of ad hoc networks in the internet of things: A case scenario for smart environments. *Internet of things and inter-cooperative computational technologies for collective intelligence*, 89-113. https://doi.org/10.1007/978-3-642-34952-2_4

Remondo, D. (2011). Wireless ad hoc networks: an overview. *Network Performance Engineering: A Handbook on Convergent Multi-Service Networks and Next Generation Internet*, 746-766. https://doi.org/10.1007/978-3-642-02742-0_31

Ren, J., Guo, H., Xu, C., & Zhang, Y. (2017). Serving at the edge: A scalable IoT architecture based on transparent computing. *IEEE Network*, *31*(5), 96-105. https://doi.org/10.1109/MNET.2017.1700030

Rong, C., Cayiri, E. (2009). Wireless Network Security. In Computer and Information Security Handbook. https://doi.org/10.1016/B978-0-12-374354-1.00011-X

Roy, A., Deb, T. (2018). Performance Comparison of Routing Protocols in Mobile Ad Hoc Networks. In: Mandal, J., Saha, G., Kandar, D., Maji, A. (eds) Proceedings of the International Conference on Computing and Communication Systems. Lecture Notes in Networks and Systems, vol 24. Springer, Singapore. https://doi.org/10.1007/978-981-10-6890-4_4

Rubinstein, M. G., Moraes, I. M., Campista, M. E. M., Costa, L. H. M., & Duarte, O. C. M. (2006, August). A survey on wireless ad hoc networks. In *IFIP International Conference on Mobile and Wireless Communication Networks* (pp. 1-33). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-34736-3_1

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018, June). IoT standardisation: Challenges, perspectives and solution. In *Proceedings of the 2nd international conference on future networks and distributed systems* (pp. 1-9). https://doi.org/10.1145/3231053.3231103

Sanchez-Iborra, R., & Skarmeta, A. F. (2020). Tinyml-enabled frugal smart objects: Challenges and opportunities. *IEEE Circuits and Systems Magazine*, *20*(3), 4-18. https://doi.org/10.1109/MCAS.2020.3005467

Sarkar, S., & Misra, S. (2016). Theoretical modelling of fog computing: a green computing paradigm to support IoT applications. *Iet Networks*, *5*(2), 23-29. https://doi.org/10.1049/iet-net.2015.0034

Sarwar, M. Z., Saleem, M. R., Park, J. W., Moon, D. S., & Kim, D. J. (2020). Multimetric event-driven system for long-term wireless sensor operation for SHM applications. *IEEE Sensors Journal*, *20*(10), 5350-5359. https://doi.org/10.1109/JSEN.2020.2970710

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. *Future Internet*, *14*(12), 363. https://doi.org/10.3390/fi14120363

Sharif, A., Li, J. P., & Saleem, M. A. (2018). Internet of things enabled vehicular and ad hoc networks for smart city traffic monitoring and controlling: a review. *International Journal of Advanced Networking and Applications*, *10*(3), 3833-3842. https://www.proquest.com/scholarly-journals/internet-things-enabled-vehicular-ad-hoc-networks/docview/2139475061/se-2

Sidhu, S., Mohd, B. J., & Hayajneh, T. (2019). Hardware security in IoT devices with emphasis on hardware trojans. *Journal of Sensor and Actuator Networks*, *8*(3), 42. **https://doi.org/10.3390/jsan8030042**

Signoretti, G.; Silva, M.; Andrade, P.; Silva, I.; Sisinni, E.; Ferrari, P. An Evolving TinyML Compression Algorithm for IoT Environments Based on Data Eccentricity. *Sensors*; 2021; *21*, 4153. https://dx.doi.org/10.3390/s21124153

Sikimić, M., Amović, M., Vujović, V., Suknović, B., & Manjak, D. (2020). An overview of wireless technologies for IoT network. In *2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-6). IEEE. https://doi.org/10.1109/INFOTEH48170.2020.9066337.

Silva, B. N., Khan, M., & Han, K. (2018). Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Technical review*, *35*(2), 205-220. https://doi.org/10.1080/02564602.2016.1276416

Sim, S. H., & Park, J. W. (2017). Stability assessment method for railroad bridges using acceleration and strain in combination. International Association of Structural Engineering and Mechanics. https://doi.org/10.1016/j.asej.2023.102521

Skouloudi, C., Malatras, A., Naydenov, R., & Dede, G. (2020). *Guidelines for Securing the Internet of Things*. ENISA. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Sobin, C. C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications*, *112*(3), 1383-1429. https://doi.org/10.1007/s11277-020-07108-5

Taleb, S. M., Meraihi, Y., Gabis, A. B., Mirjalili, S., & Ramdane-Cherif, A. (2022). Nodes placement in wireless mesh networks using optimization approaches: a survey. *Neural Computing and Applications*, *34*(7), 5283-5319. https://doi.org/10.1007/s00521-022-06941-y

Tran, H. P., Jung, W. S., Yoo, D. S., & Oh, H. (2022). Design and implementation of a multi-hop real-time LoRa protocol for dynamic LoRa networks. *Sensors*, *22*(9), 3518. https://doi.org/10.3390/s22093518

Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. *Wireless communications and mobile computing, 2018.* https://doi.org/10.1155/2018/5349894

Varghese, B., Wang, N., Nikolopoulos, D. S., & Buyya, R. (2020). Feasibility of fog computing. *Handbook of Integration of Cloud Computing, Cyber Physical Systems and Internet of Things*, 127-146. https://doi.org/10.1007/978-3-030-43795-4_5

Xi, Z. "The comparison of decentralized and centralized structure of network communication in different application fields." *2019 International Conference on Management Science and Industrial Economy (MSIE 2019)*. Atlantis Press, 2020. https://doi.org/10.2991/msie-19.2020.10

Xie, Y., Ho, I. W. H., & Magsino, E. R. (2017). The modeling and cross-layer optimization of 802.11 p VANET unicast. *IEEE access*, *6*, 171-186. https://doi.org/10.1109/ACCESS.2017.2761788

Xu, L. Da., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, *8*(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Yin, J., Yang, Z., Cao, H., Liu, T., Zhou, Z., & Wu, C. (2019). A survey on Bluetooth 5.0 and mesh: New milestones of IoT. *ACM Transactions on Sensor Networks (TOSN)*, *15*(3), 1-29. https://ink.library.smu.edu.sg/sis_research/4540

Yu, X., Fu, Y., Li, J., Mao, J., Hoang, T., & Wang, H. (2023). Recent advances in wireless sensor networks for structural health monitoring of civil infrastructure. *Journal of Infrastructure Intelligence and Resilience*, 100066. https://doi.org/10.1016/j.iintel.2023.100066

Yu, X., Fu, Y., Li, J., Mao, J., Hoang, T., & Wang, H. (2024). Recent advances in wireless sensor networks for structural health monitoring of civil infrastructure. *Journal of Infrastructure Intelligence and Resilience, 3*(1), 100066. https://doi.org/10.1016/j.iintel.2023.100066

Zakaret, C., Peladarinos, N., Cheimaras, V., Tserepas, E., Papageorgas, P., Aillerie, M., & Agavanakis, K. (2022). Blockchain and secure element, a hybrid approach for secure energy smart meter gateways. *Sensors*, *22*(24), 9664. https://doi.org/10.3390/s22249664

Zhou-Kangas, Y. “MODELING AND ANALYSING THE PERFORMANCE OF A WIRELSS MESH NETWORK.” (2014) University of Jyväskylä. http://urn.fi/URN:NBN:fi:jyu-201406041925