An Investigation Framework for Internet of Things Spatial Modelling and Forensic Reconstruction

A thesis submitted to

Auckland University of Technology

in fulfilment of the requirements

for the degree of

Doctor of Philosophy in Computer Science

Supervisors

Dr Alastair Nisbet

Dr Mahsa Mohaghegh

Rijo Jacob

2024

Abstract

Internet-enabled Things, equipped with sensors and utilised for various applications, are a complex type of digital device that has become considerably more prevalent over the last decade. Coming in a variety of form factors to suit different physical environments, this digital device type has caused the lines that traditionally separated a physical scene from a digital scene to blur. Though often resource-constrained, Things are a valuable source of digital evidence in investigations. Whilst the data generated depends on the role of a device for an application, the data may be stored across multiple platforms, including any locally available storage. Forensic examination of Things collected from an evidential scene may yield valuable evidence for the forensic investigator.

However, identifying Things at the scene of a forensic examination is difficult. The conventional procedure of search and seizure applicable for identifying digital devices is more suited for device types, such as USB sticks, mobile phones and computers, which are immediately distinguishable as digital devices because of their external appearance. Most Things, however, are not immediately distinguishable due to physical similarities to ordinary physical objects. Therefore, investigators searching for digital devices may overlook various Things and leave those devices behind. Additionally, identifying Things by applying the search and seizure procedure risks inadvertently tampering with the scene, as actions that investigators take to search for digital devices at the evidential scene may trigger changes to the state of one or more sensor-equipped devices.

This research attempts to fill this significant gap in investigative procedures by providing a framework that will enable investigators to search an evidential scene much better prepared to identify Things. An approach that will also give investigators the greatest possibility to obtain forensic evidence of the various Things at the scene, including their locations, is to capture and examine the real-time communications of Things for the number and locations of active Things. With every active Thing located prior to entry, investigators will be able to search for digital devices and avoid leaving an unknown number of Things at the evidential scene unaccounted for. With evidence of the locations obtained in the form of communications before entering a scene, investigators will be able to justify the actions involved to search the locations for the sensor-equipped devices. However, there are several challenges to this approach.

Consider a domestic residence as an example of a scene that investigators monitor for some time to obtain evidence of the location of every active Thing. Communications that yield forensic evidence will need to be obtained without entering a scene and without using any fixed monitoring infrastructure, both because that may not be possible and to avoid tampering with the evidential scene inadvertently. This research, hence, provides a framework that is specifically suited for forensic investigators to locate and track the active Things at the evidential scene whilst obtaining evidence suitable for forensic purposes. As one of the principal objectives of capturing communications is to obtain location evidence, this research examines how location accuracy is affected by the distance and the number of locations from which communications are captured. Whilst the framework developed is primarily suited for investigative purposes, the framework may be utilised in any of many other scenarios, where monitoring network traffic of Things to locate them is required.

Table of Contents

List of Figures

List of Tables

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a University or other institution of higher learning.

Rijo Jacob

14 May 2024

Publications

1. Jacob, R., & Nisbet, A. (2022). Designing a Forensic Investigation Framework for IoT Monitoring and Modelling. *Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 42-43,* 265-271.

2. Jacob, R., & Nisbet, A. (2022). A forensic investigation framework for Internet of Things monitoring. *Forensic Science International: Digital Investigation, 42-43,* 301482. https://doi.org/10.1016/j.fsidi.2022.301482

Acknowledgements

I am forever grateful to Rabbi Hillel who said, “If I am not for me, who will be for me? And when I am for myself alone, what am I? And if not now, then when?”.

Thank you Dr Alastair Nisbet for your mentorship, guidance and unwavering support throughout. I am indebted to you for your earnest dedication to excellence.

My sincere thanks to Dr Mahsa Mohaghegh and to everyone in Faculty who became a part of my journey with their support.

I cannot begin to express my gratitude to my family.

Abbreviations and Acronyms

3-D	Three-Dimensional
ACK	Acknowledgement
AI	Artificial Intelligence
AL	Always Listening
BLE	Bluetooth Low-Energy
CoT	Core of Trust
CNN	Convolutional Neural Network
DCoC	Digital Chain of Custody
DCoC-IoT	Digital Chains of Custody in IoT
DCTF	Differential Constellation Trace Figure
DL	Deep Learning
DW	Digital Witness
FEMS	Forensics Edge Management System
FFD	Full Function Device
FL	Frequently Listening
FSAC	Forensic State Acquisition Controller
FSAIoT	Forensic State Acquisition from Internet of Things
GPS	Global Positioning System
HAN	Home Area Network
IAT	Inter Arrival Time

IMU	Inertial Measurement Unit
IoT	Internet of Things
LAN	Local Area Network
LEA	Law Enforcement Agencies
LF	Low Frequency
MAC	Medium Access Control
ML	Machine Learning
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
OSI	Open Systems Interconnection
PAN	Personal Area Network
PCR	Platform Configuration Register
PHR	Physical Header
PHY	Physical Layer
PPDU	Physical Protocol Data Unit
PSDU	Physical Service Data Unit
RF	Radio Frequency
RFD	Reduced Function Device
RFF	Radio Frequency Fingerprint
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator

RSS	Radio Signal Strength
RTLS	Real-time Location Tracking system
SAIL	Situation-Aware Indoor Localisation
SE	Secure Element
SHR	Synchronization Header
SNR	Signal-to-Noise Ratio
TPM	Trusted Platform Module
US	United States
UWB	Ultra-Wide Band
VLC	Visible Light Communication
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

Chapter 1

INTRODUCTION

1.1 Background

Over the years, Internet of Things (IoT) technologies have vastly improved. The advancements have enabled various applications that utilise physical objects equipped with computing and communication technologies, which are a complex digital device type known as Things (Gubbi, Buyya, Marusic, & Palaniswami, 2013). In 2023, the number of connected Things surpassed 16 billion (Christian, 2024). Whilst the number of IoT connections surpassed non-IoT connections in 2020 (Lueth, 2020), the prevalence of Things in physical environments has blurred the lines that traditionally separated a physical scene from the digital scene for forensic investigations.

Unlike their ordinary counterparts, connected Things generate voluminous data that may provide vital forensic evidence. However, the forensic identification of Things with the conventional search and seizure procedure applicable to digital devices has been difficult (Quick & Choo, 2018). Digital forensic investigators may overlook and leave Things behind at the scene. Practical difficulties for the forensic process of identification arise from the rapid introduction and growing variety of Internet-enabled Things. A growing challenge for the process of identification is the likeness of Internet-enabled Things to their ordinary counterparts.

Despite the pervasiveness of Things having significant implications for securing a digital scene, the field of digital forensics has yet to advance sufficiently for the identification of Internet-enabled Things. The alternative means of identification from the Device Fingerprinting and Indoor Localisation areas are not suited for forensic

investigators to identify Internet-enabled Things at the evidential scene. To accomplish the task of forensic identification, notwithstanding the challenges to identify potentially numerous and a large variety of Things, forensic investigators need monitoring and modelling capability. This will enable investigators to enter an evidential scene much better prepared to collect both known and unknown Things in the shortest possible timeframe.

1.2 Problem Statement

Radio signals' monitoring ahead of searching an evidential scene for Things has significant benefits for forensic investigators. Passive monitoring of the Radio Frequencies (RFs), specifically the RFs that Things occupy, will inform the Internet-enabled Things' count, type and location. Forensic evidence of every active Thing within a network may begin with information gathered in the form of communications through monitoring of the RFs, which provides investigators a suitable basis to launch a search for a finite number of Things. Forensic evidence of the location of every active Thing may also be obtained in the form of communications through monitoring. Location evidence provides investigators a suitable basis to search for Things at specific locations. Furthermore, as entering a scene with sensor-equipped Things to search for digital devices risks inadvertently tampering with the scene, location evidence will enable investigators to justify the actions taken at the evidential scene to collect the located Things.

With improvements in IoT technologies transparently embedding information and systems into the surroundings of physical environments, investigators and law enforcement agencies (LEAs) may urgently need monitoring and modelling capability to be able to identify and collect Things for forensic examination in a laboratory

setting. However, any evidence of Things and their locations for forensic purposes will need to be obtained by investigators without inadvertently tampering with the evidential scene. This requirement imposes constraints for monitoring a scene. Monitoring can neither be carried out after entering a scene nor can utilise any fixed monitoring infrastructure. Monitoring and modelling capability, hence, requires a framework that is suited for forensic investigators to harness the communications between Things for IoT spatial modelling.

With the aim to contribute to the readiness of forensic investigators to identify Internet-enabled Things, this work further examines the challenges involved in obtaining forensic evidence of Things in the form of communications and develops a framework that investigators may utilise to determine the count and locations of Things.

The following overarching question identifies the central problem that this work attempts to solve:

What is an effective forensic reconstruction framework to ascertain the number and locations of Internet-enabled Things by harnessing the wireless communications between Things ahead of searching an evidential scene for Things?

1.3 Scope of Research

Analysis of the various capabilities that a system requires for monitoring and modelling Things narrowed the scope of this research to the following sub-questions.

1) ***How can the wireless communications of a heterogeneous IoT environment be observed to enable the accurate modelling of Things?***

2) ***How can the wireless communications of a heterogeneous IoT environment be analysed to map the logical topologies of Things?***
3) ***How can the wireless communications of a heterogeneous IoT environment be utilised to determine the locations of Things?***

The three sub-questions were identified by constructing a model of the system to locate and track Things from the radio signals of an IoT environment. The model consisted of three processes, where a process of observing the communications between Things initially collects the communications required for accurate modelling of an IoT environment. This is followed by a process of analysing the communications which has a focus on building the logical topologies of operating IoT platforms. The framework also includes a process of utilising the communications observed and analysed to determine the location of every active Thing.

1.4 Research Approaches

The inquiry into observing the communications between Things was based on the expectation that transmissions from every active Thing are not required to discover all active Things in an IoT environment, regardless of the network topology. This line of inquiry required data from various configurations of Things to be analysed. As empirical tests required the deployment of numerous Things, a logical alternative was to generate simulations that mimic real-world scenarios. A custom-built IoT simulator was, hence, utilised for the inquiry. An empirical approach was applied for the inquiry into utilising the communications between Things. This inquiry expected the monitorable range of wireless communications between Things to vary. Experiments involved a selection of Things, both mains and battery-powered. The inquiry into analysing the communications between Things expected that the type of every active

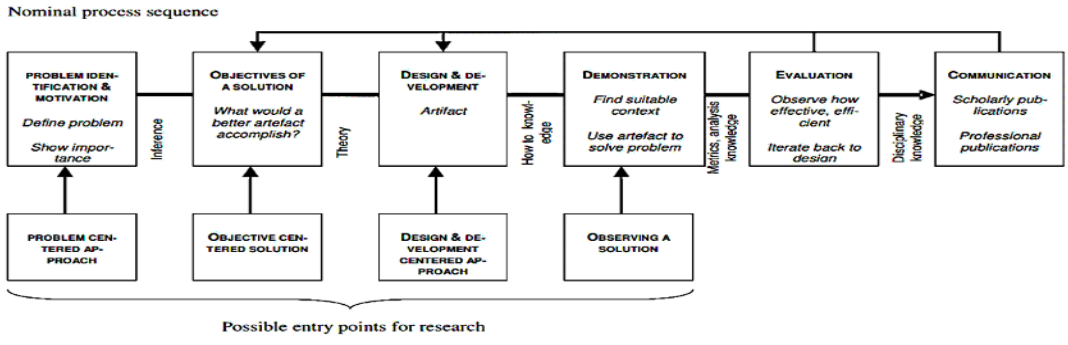
Thing may be determined from the data embedded in their wireless transmissions. This inquiry also involved empirical tests of a selection of Things.

1.5 Research Methodology and Phases

According to Novikov and Novikov (2013), a research project that aims to construct a certain system under the constraints of time, resources and scope requires a suitable research methodology to be incorporated. Digital Forensics is a relatively new scientific field that has yet to standardise research methodologies. The work of Montasari, Carpenter, and Hill (2019), which underscores the absence of formal methodologies that are suitable for research studies in Digital Forensics, recommends the Design Science methodology as an alternative for the design, development and evaluation of digital forensics artefacts. However, the Design Science methodology of Pfeffers et al. (2006) is not suited for research projects with an intent to identify and fill a gap in research that satisfies an immediate need. Figure 1.1 identifies the four possible entry points of the Design Science research methodology.

Figure 1.1

Entry Points of Design Science Research Methodology

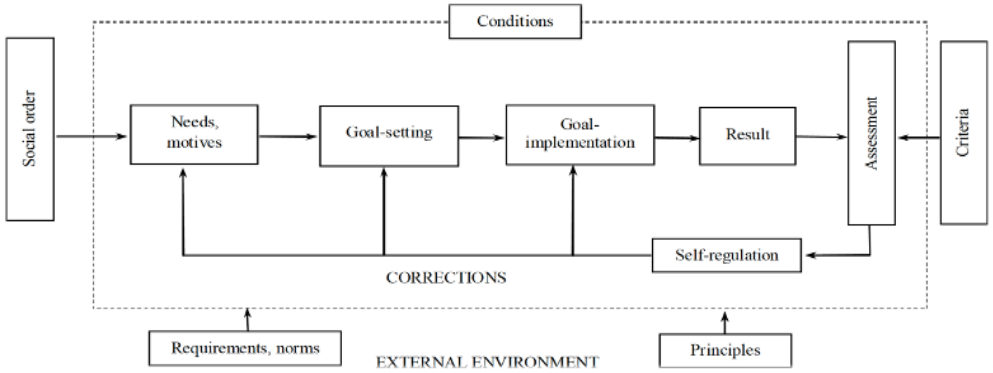


Note. From *"The Design Science Research Process: A Model for Producing and Presenting Information Systems Research,"* by K. Pfeffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen and J. Bragge, 2006, *First International Conference on Design Science Research in Information Systems and Technology*, (10.48550/arXiv.2006.02763). In the public domain.

For a suitable research process, this research adopted the basic structural components of any scientific activity, which is explained in the work of Novikov and Novikov (2013). Figure 1.2 shows the basic structural components, which cover the process of stating needs via motives.

Figure 1.2

Structural Components of an Activity



Note. From *"Research methodology: From philosophy of science to research design,"* by A. M. Novikov and D. A. Novikov, 2013. Copyright 2018 by Elsevier B.V.

The initial phase of this research, which involved a systematic review of the literature, determined the aim of this research. The goal-setting phase that followed defined the goals of this research. This phase identified a gap in research and narrowed the scope of this research. That was followed by preparations for goal implementation, including procurement and setup of hardware and software required for data collection. The results phase, which reviewed and analysed the data collected through the goal implementation phase, generated the data required for the assessment phase of this research.

1.6 Research Contribution

This research contributes a forensic investigation framework for IoT-based digital investigations, where forensic investigators may capture real-time communications of

a heterogeneous IoT environment and obtain forensic evidence of the various Things in operation at an evidential scene. By providing a framework for harnessing wireless communications, this research brings to the fore wireless communications of Things as a forensically significant data source. The recommended approach, which is suited for IoT environments where multiple IoT platforms and heterogeneous IoT communication technologies operate, covers the methods, including hardware and software, applicable for observing, analysing and utilising communications of an IoT environment. Furthermore, several models are defined to assist the implementation of the various methods to systematically capture real-time network traffic for accurate modelling, analyse communications to determine the number of Things and utilise communications to determine the location of every active Thing.

1.7 Thesis Structure

The remainder of this thesis is structured and organised using 8 chapters. The focus of each chapter is briefly described below.

Chapter 2, titled Forensic Identification of Things, reviews the methods that exist to identify Things. The review is followed by a discussion of the limitations of the methods.

Chapter 3 is titled Literature Review. This chapter focuses on IoT mesh networking solutions and networking standards, including IEEE 802.15.4 and ITU-T G.9959, that enable robust wireless communications where other traditional wireless technologies are less suitable. This chapter briefly discusses the origin and notions of the term “Internet of Things”, the various types of Things and the market for Things.

Chapter 4, titled Research Design, covers the design of research. This chapter describes a model of the system for monitoring and modelling Things constructed after considering the challenges for forensic investigators to leverage wireless communications at wireless digital scenes. This chapter also explains the applicable criteria for evaluation of the model. Furthermore, this chapter covers the implementation plan, including research methods, data collection, data analysis and solution definition.

Chapters 5, 6 and 7 cover the analysis of the data collected to assess the various aspects of wireless communications between Things that form the evaluation criteria. Each chapter focuses on a distinct aspect and covers the data collected, reviewed and analysed to study that aspect.

Chapter 8, titled Discussion, is the penultimate chapter of this thesis. In this chapter, a forensic investigation framework that enables spatial modelling of an IoT environment is defined using the results covered in Chapters 5, 6 and 7. This chapter also provides an appraisal of the model of the system for harnessing wireless communications based on the findings of the empirical and simulation experiments.

Chapter 9, which is titled Conclusions and Future Research, is the final chapter and initially provides the conclusion of this thesis. This chapter also provides directions for future research to build on the contributions of this work.

Chapter 2

FORENSIC IDENTIFICATION OF THINGS

2.1 Introduction

The need for forensic methods and tools that are suitable for IoT infrastructures has drawn the interest of digital forensics and cyber security researchers to contribute to developing IoT forensics as a branch of digital forensics. This has led to the development of methods suitable for the extraction of digital evidence from IoT specific evidence sources, including cloud-based infrastructures. Researchers have also developed new processes that provide for quickly analysing significantly large volumes of data as well as reducing the storage costs for digital investigations. Ongoing research, however, is yet to develop an alternative or alternatives suitable for forensic identification of Things.

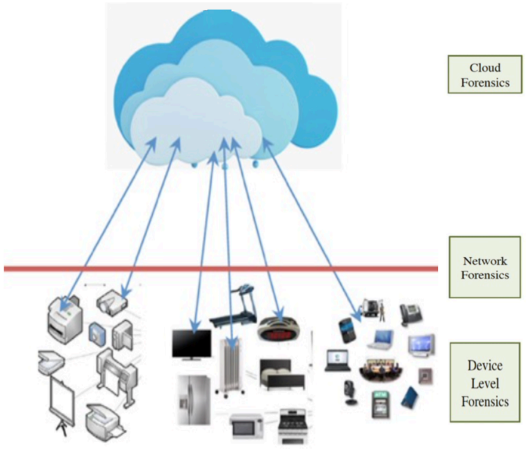
Whilst Internet-enabled Things are increasingly replacing ordinary things and augmenting non-IoT devices in physical environments for various IoT applications and services, researchers have explored various methods to identify Things, including through non-IoT devices, Digital Chains of Custody, Device Fingerprinting and Indoor localisation. This chapter provides a thorough assessment of the various methods from the perspective of forensic investigators and law enforcement agencies. The methods are classified as either forensics-incorporated or forensics-unincorporated. This classification of the methods is used to distinguish the methods based on the requirements considered for development. The methods developed by considering the requirements of forensic investigations are categorised as forensics-incorporated methods. The methods which are primarily suited for purposes other than forensic investigations are categorised as forensics-unincorporated methods.

2.2 IoT Forensics

Though numerous cloud-based platforms may be potential sources for forensic artefacts in IoT-based digital investigations (MacDermott, Baker, Buck, Iqbal, & Shi, 2020), the work of Zawoad and Hasan (2015) earlier pointed out that a cloud forensics scheme's one of many forensics schemes that underpins IoT forensics. Whilst the researchers described IoT forensics as another branch of digital forensics, the researchers defined IoT forensics as a combination of device, network and cloud forensics schemes. According to the researchers, the scope of the processes of identification, collection, organisation and presentation for IoT forensics spans IoT infrastructures, which includes cloud-based platforms, networks and devices as shown in Figure 2.1.

Figure 2.1

IoT Forensics



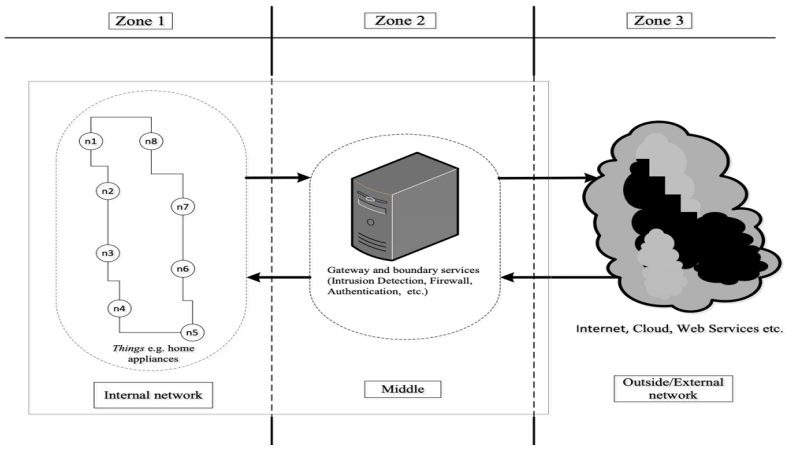
Note. Adapted from *"FAIoT: Towards building a forensics aware eco system for the Internet of Things,"* by S. Zawoad and R. Hasan, 2015, *IEEE International Conference on Services Computing,* 10.1109/SCC.2015.46. Copyright 2016 by Elsevier B.V.

To systematically approach IoT-based digital investigations, the work of Oriwoh, Jazani, Epiphaniou, and Sant (2013) recommends the application of the 1-2-3 Zones approach, which is a zone-based method. The 1-2-3 Zones approach identifies 3

zones, namely, Zone 1, Zone 2 and Zone 3, that investigators are to focus on in any IoT-based digital investigation. Zone 1 consists of Things that constitute the internal network as shown in Figure 2.2. Zone 2 consists of gateway and boundary services. Zone 3 consists of the services, including Cloud and Web Services, outside of an internal network.

Figure 2.2

IoT-based Investigation Zones



Note. From *"Internet of Things Forensics: Challenges and approaches,"* by E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, 2013, *9th International Conference on Collaborative Computing: Networking, Applications and Worksharing,* (10.4108/icst.collaboratecom.2013.254159). Copyright 2013 by ICST.

2.3 Challenges for Identifying Things

In the work of Quick and Choo (2018), the researchers underscore that securing an internal network for IoT-based digital investigations is problematic. One of the most pressing concerns is the increasingly challenging task of identifying Things. Quick and Choo (2018) further point out that there are two main challenges for identification of the IoT digital evidence sources within an internal network. One of the challenges is the rapid introduction of new Things to IoT markets which requires forensic investigators to familiarise and catalogue the new IoT devices that are introduced by IoT manufacturers. The other challenge is the physical similarity of IoT devices to

familiar physical objects, which makes them indistinguishable from ordinary physical objects.

To augment the conventional procedure of search and seizure for the identification of IoT devices, Quick and Choo (2018) argue for quicker analysis of the structured and unstructured data from all other evidence sources at a digital scene. However, the identification of digital devices through the conventional search and seizure procedure risks non-compliance with the ACPO principle of digital evidence that no action by investigators should alter data (Williams, 2011). This is because the actions that forensic investigators take during a field search are potential triggers for changes to the state of IoT devices with sensors.

2.4 Forensics-incorporated Alternatives to Identify IoT Devices

Researchers have explored several frameworks and methods to identify IoT devices for forensic purposes. However, the methods recommended to identify IoT devices have challenges and limitations for implementation by forensic investigators and LEAs. This section provides a review and assessment of the forensics-incorporated solutions.

2.4.1 Automated Internal IoT Forensics

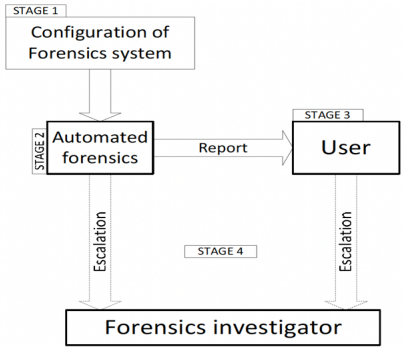
2.4.1.1 Autonomous Forensics Service

In Oriwoh and Sant (2013), the researchers proposed the idea of automated forensics in IoT environments. The researchers pointed out that IoT-based digital investigations within Home IoT environments require intelligent and adaptable solutions that are suited for a dynamic and pervasive network model. The researchers further pointed out the need for a security and forensics solution that is more manageable by the end-user of a Home IoT environment. With the aim to enable autonomous forensics

capability in IoT environments, Oriwoh and Sant (2013) introduced the design of the Forensics Edge Management System (FEMS). Figure 2.3 shows the forensics model.

Figure 2.3

FEMS Model



Note. From *"The forensics edge management system: A concept and design,"* by E. Oriwoh and P. Sant, 2013, *10th International Conference on Ubiquitous Intelligence and Computing and 10th International Conference on Autonomic and Trusted Computing,* 10.1109/UIC-ATC.2013.71. Copyright 2013 by IEEE.

With the device owner as a part of the process, the FEMS model is designed to integrate into an IoT environment and provide for a robust, autonomous solution that is capable of carrying out a preliminary forensic investigation. The design of FEMS provides for an autonomous forensics service which covers network monitoring, data logging, timeline creation as well as presentation of investigations reports in a format that is understandable by humans. FEMS goes into the forensics mode and associated activities begin as a response to an event that triggers an alarm based on a set threshold. Any data that is logged after observing an event is treated as data having forensic relevance.

The next stage of the forensics mode involves parsing, compressing, and differentiating the data captured following an event to intelligently make decisions about that event. Following the analysis of data, a timeline of the events that occurred

during a crime is generated. The analysis of data also provides the basis for escalation of incidents, which the user may choose to override. The forensics mode concludes with a clear report of the analysis and the decisions, which informs users without expertise in forensics and assists further investigations. The design of FEMS also provides for security services such as basic monitoring to detect anomalies, data logging, intrusion detection and prevention and threshold establishment for a safe and secure state of the IoT environment as per user requirements and preferences.

Oriwoh and Sant (2013) underscores the flexibility of the FEMS model which allows for implementations to use a stand-alone device for integrating the system into personal networks. With a stand-alone implementation, however, the operation of FEMS within personal networks is confined to the link between a switch and the Internet router. To expand the access of the system beyond a switch and into the internal network, the alternative of incorporating FEMS into a gateway device is recommended. The expanded access of the system, however, is limited to the data flowing directly between internal network entities and the Internet gateway.

2.4.1.2 Implementation Challenges

The FEMS model assumes sufficient storage for the autonomous forensics service to be able to inspect real-time data flowing through an internal network and retain relevant data following specific events. Network data, however, can quickly outgrow available and affordable storage. Also, as FEMS provides for collecting and processing data having forensic value from the perception, network, and application layers of an IoT environment, integration of cloud storage to implement the system is likely to increase bandwidth needs. The continuous operation of FEMS within personal networks for automated forensics, hence, is a challenge.

2.4.1.3 Implementation Limitations

Although the FEMS model provides for escalation of issues to relevant authorities, even when users are physically away from home, the design is not aimed at the specific needs of LEAs. As the design is suited for the needs of IoT device owners, access to network data collected from across the three different layers of an IoT environment by the FEMS implementation will require elevated privileges. The model proposed by Oriwoh and Sant (2013), therefore, is useful for limited scenarios of cyber-crimes.

2.4.2 IoT Devices in Digital Chains of Custody

2.4.2.1 Digital Witnesses

Researchers have explored a Digital Chain of Custody (DCoC) scheme to mainly provide more flexibility to the traditional evidence handling approach (Prayudi & Azhari, 2015). The work of Nieto, Roman, and Lopez (2016) introduced a new "digital witnessing" approach to deploy Digital Chains of Custody in IoT (DCoC-IoT) for the purpose of evidence management in IoT environments. The researchers argued for IoT devices as collaborators of a new DCoC scheme that utilises mobile devices and personal networks of IoT environments to replace humans and remove human involvement for evidence management. The researchers envisaged IoT devices as a "digital witness", which is a container of digital evidence that is also able to collaborate in the management of digital evidence from both the technological and legal standpoints.

Nieto et al. (2016) derived the critical components of the DCoC-IoT scheme, which is required for digital devices to be able to acquire, store and transmit evidence to an authorised entity, by referring to several standards. The guidelines and standards

utilised to develop the requirements include UNE 71505, UNE 71506, ISO/IEC 27037, ISO/IEC 27042 and the ISO/IEC 30121. As the DCoC-IoT is a scheme for IoT devices to testify against malicious activities, implementation of the DCoC-IoT scheme requires technologies that provide for security guarantees. Hardware security devices that Nieto et al. (2016) identified as being suitable included Trusted Platform Module [TPM] v2.0 and secure elements (SEs), which provide for employing a secure communication channel and for storing keys and hashes.

The main criterion that Nieto et al. (2016) defined for a device to qualify as a digital witness (DW) requires that the device makes use of a core of trust (CoT) to implement a trusted execution environment as well as to store and protect the proof of integrity of digital evidence. Nieto et al. (2016) note that TPMs, which provide for a CoT, is useful to validate the integrity of software components and as a tamper-resistant chip. In Han, Shin, Park, and Kim (2018), the researchers point out that TPMs are widely deployed in devices utilised by enterprises and government systems for the need of trusted platforms. In addition to integrating a master key and a cryptographic processor, TPMs allow third-party applications to store hashes in platform configuration registers (PCRs).

Although the integration of multiple hardware security devices will affect both the design and affordability of IoT devices, the DCoC-IoT scheme requires that a DW also utilises secure hardware that will allow the device to be identified as part of a DCoC. As both SIM cards and electronic identity cards have provisions for this requirement, Nieto et al. (2016) recommend that IoT devices store a private key locally for digital signature operations. The scheme also requires that the public and private key pairs are owned by the owner of the devices. Such a link between key

pairs and the identity of a specific individual, however, introduces the need for consent from device owners. So, although Nieto et al. (2016) intended a DCoC scheme that does not require the intervention of device owners, the scheme requires users to authorise the procedures for which a personal device will be utilised.

2.4.2.2 Key Dependencies

The work of Nieto, Rios, and Lopez (2018), which extended the privacy capabilities of the DW approach to encourage the collaboration of citizens, recommended for personal IoT devices to be prepared by their users. The preparation step involves installing what is referred to as the PRoFIT software before an investigation begins. According to the researchers, the role of PRoFIT is to aid citizens in privacy and forensics related decisions and subsequent phases of an investigation. The installation of PRoFIT software to prepare every personal device that is required for evidence management, however, depends on the level of interactions allowed by manufacturers between the device and its user. Further, the privacy enhanced DW approach expects every citizen to cooperate with relevant authorities and authorise the use of all personal devices for evidence management.

2.4.2.3 Pre- and Post-Implementation Challenges

The work of Nieto, Rios, and Lopez (2017) identified potential solutions to enable anonymity with certain restrictions and to mitigate some of the privacy problems associated with the DW approach. This includes the crowds-like protocol, direct anonymous attestation protocol, anonymous routing protocol such as AASR, HAWK mechanism for transactional privacy and protocols such as homomorphic encryption. A crowds-like protocol is suggested for DWs to form anonymous links sufficient to transmit messages to an authorised entity, which will need to know the identity of the

DWs forming the group and involved in the transmission of evidence. An anonymous routing protocol is suggested to anonymise the identity of the DWs involved in the discovery of the optimal route to the final entity, known as the Official Collection Point. However, implementing the different schemes for privacy guarantees requires significant resources, which are not available to many IoT devices.

The criterion of a CoT for digital witnessing and the requirement of SEs to implement a DCoC also increase the challenges for forensic investigators in IoT environments. The work of Han et al. (2018) identified flaws in TMP v2.0 that allow an adversary to reset TPM and forge PCRs. The researchers also note that countermeasures involving hardware specific firmware updates will take a considerable amount of time to be applied. Similar flaws have also been found in SEs such as in a SIM card. In 2019, researchers at the AdaptiveMobile Security discovered a security vulnerability in SIM cards that was exploited for more than 2 years by a sophisticated attacker. The vulnerability and associated exploits, codenamed the Simjacker (McDaid, 2019), allowed the delivery and execution of spyware that instructs the SIM card to retrieve data and execute commands. Thus, the implementation of the DCoC-IoT scheme will require forensic investigators to additionally check the potentially numerous security hardware for any signs of tampering and therefore having forensic implications.

2.4.3 Internal IoT Events Reconstruction

2.4.3.1 IoT Device State Acquisition

Researchers have argued for the monitoring and logging of changes to the state of IoT devices as these sources of digital evidence have considerably increased the complexities of evidence acquisition. In the work of Meffert, Clark, Baggili, and Breitinger (2017), which proposed a generalised framework for data collection from

IoT devices, the researchers introduced a new Forensic State Acquisition from Internet of Things (FSAIoT) framework. As IoT devices mostly utilise limited long-term storage, the FSAIoT has a focus on the logs that update device state for the acquisition and analysis of IoT devices. The FSAIoT framework is designed for collecting data from both the internal network and services of the outside network.

As there are technical challenges for obtaining historical records from IoT devices, the FSAIoT framework involves the deployment of a centralised Forensic State Acquisition Controller (FSAC) device in IoT environments for state acquisition. The role of the FSAC device, when compared to the forensics service provided by FEMS in an IoT environment, is limited. For state acquisition of IoT devices, the controller device makes use of three modes. The different modes are controller to IoT devices, controller to hub and controller to cloud. An implementation of the framework, however, requires the FSAC device to establish connections that enable the three modes to acquire state information from IoT devices, the hub and the cloud service supporting the IoT environment.

2.4.3.2 Acquisition Limitation

A proof-of-concept implementation of the FSAIoT framework, which combined OpenHAB and Insteon devices, involved manual configuration of the connection information to enable the binding of Insteon devices at run time. Acquiring state information of the devices utilised information located on the actual device that identifies each target device. The FSAC device, as a non-Insteon device, gained limited terminal access to the Insteon Hub. The controller to hub mode utilised authentication credentials that were located on the hub. The controller to cloud mode, which involved the linking of the FSAC device to an online account, also required

certain codes that were found on the actual hub. The FSAIoT framework is, hence, applicable when authentication credentials and other device specific information of the devices at a scene is known to the investigator.

2.4.4 Internal IoT Evidence Sources Discovery

2.4.4.1 Big Digital Forensic Data Analysis

Researchers have argued for quicker analysis of the disparate data from identifiable sources of digital evidence at the evidential scene to discover the overlooked IoT devices. Building on the work of Quick and Choo (2016) that introduced the approach of data reduction by selective imaging, Quick and Choo (2018) developed certain processes to work through larger volumes of digital forensic evidence, referred to as big digital forensic data. The researchers combined the processes of data reduction and quick analysis, along with automated data extraction to improve the time that is required to analyse significantly large volumes of data.

The process of data reduction is based on imaging specific types of files and data, including, the registry, document files, spreadsheets, email, browsing history, communications and pictures. The data volume reduction process retains information in the native source format with metadata, which enables processing of the data subsets by software such as EnCase, NUIX and Access Data FTK, which are widely utilised for forensic purposes. The process of feature extraction has a focus on pseudo-unique data identifiers. Email addresses, email message identifiers, cookies and credit card numbers are a few examples of pseudo-unique data identifiers. The process of analysis focuses on correlating features extracted from datasets that span disparate devices and different cases.

2.4.4.2 Implementation Challenges

The effectiveness of the processes of data reduction and quick analysis depends on the locations of potential evidence sources and possible connections. Legal and jurisdiction issues are likely to hinder access to cloud-based evidence sources. Another challenge for the method is to obtain permission to gain access to networks with which a potential evidence source has interacted. The effectiveness of the method also depends on the availability of forensically relevant information. The time that data is available for the process of extraction before being over-written is an issue with cloud-based evidence sources. The growing use of data encryption and anti-forensic techniques also adds to the complexities for processing evidence from IoT and non-IoT devices (MacDermott et al., 2020).

2.5 Forensics-unincorporated Alternatives to Identify IoT Devices

Other areas of research with a focus on IoT device identification are “indoor localisation and tracking” and “device fingerprinting”. Both areas have emerged as key for the development of IoT applications useful for healthcare, energy management, security management, home automation and industrial automation. Various methods and techniques that provide for a range of use-cases already exist. However, the techniques are not suited for the forensic identification process. This section provides a review and assessment of some of the recent work that has advanced indoor localisation and device fingerprinting for IoT scenarios.

2.5.1 Device Tracking in Indoor IoT Environments

The area of indoor localisation has made significant progress to enable location-based services in indoor spaces. The main objective of research in this area has been to develop a solution that estimates and predicts the location of an object or an

individual within indoor spaces (Ngamakeur, Yongchareon, S., & Rehman, 2020). However, developing a single technique of indoor localisation, similar to the Global Positioning System (GPS), which has enabled location-based services in outdoor environments, has been a challenge. This is mainly due to the diverse localisation requirements of the wide range of indoor applications across domains which are enabled by IoT technologies (Chowdhury, Elkin, Devabhaktuni, Rawat, & Oluoch, 2016).

With a focus on the challenges within smaller geographical areas and multi-resident environments such as office buildings, hospitals and care facilities, researchers have developed a selection of indoor localisation techniques to provide for different scenarios. More recent studies have focused on techniques suitable for indoor localisation of sensor deployments in Wireless Sensor Networks (WSNs) to enable location-based services in IoT environments (Chowdhury et al., 2016). Some studies explored device-free methods to provide geographically meaningful data for different kinds of applications across areas such as home automation and eHealth. The studies that developed device-free approaches for indoor localisation have a focus on enabling location-based services without the need for users to carry devices (Ngamakeur et al., 2020).

2.5.1.1 Overview of Indoor Localisation

The work of Zafari, Gkelias, and Leung (2019) defined indoor localisation as the process of obtaining the location of a device or user in an indoor space. With the proliferation of smartphones and wearables in indoor settings, the localisation and tracking of devices has also been referred to as the localisation and tracking of end-users. Zafari et al. (2019) broadly classified the many different systems that exist for

indoor localisation and tracking into three different categories. Their survey differentiated most of the existing localisation systems as either device-based or monitor-based. However, Zafari et al. (2019) also observed the emergence of a third category of solutions, that of proximity-based systems.

In device-based localisation systems, anchor nodes or reference nodes are utilised as a basis to find the relative location of a device. These are systems designed for updates on the current location of a user to enable navigation. In contrast, monitor-based localisation systems utilise reference nodes to passively find the position of a device. Such systems provide for tracking the movement of users using their device locations to enable various kinds of services. Proximity-based localisation systems have a focus on estimating the distance between a device or user and a point of interest to find the relative distance between two objects. There is growing interest in this type of localisation, which offers a more reliable and cost-effective alternative for context-aware services (Zafari et al., 2019).

The survey of Zafari et al. (2019) further classified the localisation systems into two main categories based on the wireless technology used. Both categories of systems have made use of a wide range of technologies, including Wireless Fidelity (Wi-Fi), ultra-wide band (UWB), acoustics, Radio Frequency Identification (RFID), Bluetooth Low-Energy (BLE) and visible light. However, Zafari et al. (2019) point out that the many different services being built on IoT platforms are more likely to benefit from indoor localisation systems that make use of both short and long-range IoT technologies. A number of challenges exist for the development and adoption of indoor localisation techniques that will improve location-based services and localisation services to users. Some of the known challenges are multipath effects and

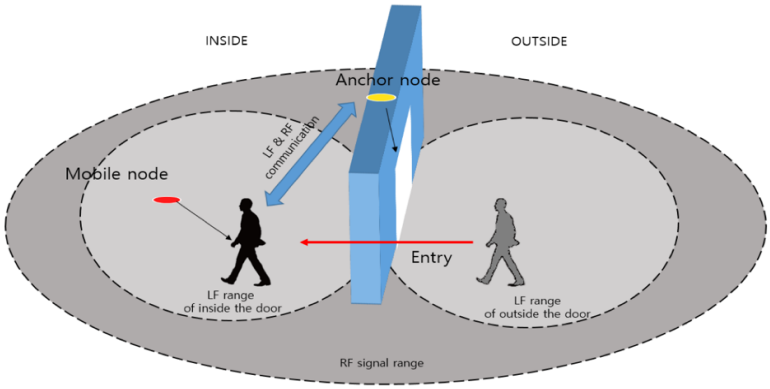
noise, privacy and security, standardisation and cost, radio environment and energy efficiency.

2.5.1.2 Location Awareness

The work of Park, Kim, and Kang (2018) argued for the need of various location-based services that depend on the current location of a user. The researchers observed that most of the techniques available for location awareness are not suitable for practical implementation in indoor environments. Although previous studies improved location precision, Park et al. (2018) found the studies to have developed techniques that overlooked the need for real-time indoor localisation of devices which operate on power from limited battery capacity. The researchers also found several techniques required many wireless beacon nodes for location awareness, without consideration of the costs of initial installation and maintenance. For a more suitable solution in indoor environments, Park et al. (2018) introduced the hybrid situation-aware indoor localisation (SAIL) system, which is shown in Figure 2.4.

Figure 2.4

SAIL System



Note. From *"A situation-aware indoor localization (SAIL) system using a LF and RF hybrid approach,"* by J. K. Park, J. Kim, S. J. Kang, 2018, *Sensors,18*(11), p.5. Copyright 2018 by Elsevier B.V.

The SAIL system is mainly designed to work with limited battery capacity devices such as wearable devices and mobile tags. The proposed system leverages the high transmittance to obstacles characteristic of low frequency (LF) and low-power requirement of BLE to reduce the complexity and power requirements for real-time indoor localisation. Combining LF and BLE 4.0, the system requires fewer anchor nodes initially and provides for a cost-effective solution for implementation in large buildings. The system is designed for detecting mobile devices as nodes pass through an entrance location and for determining the position of a device within an indoor environment.

To recognise whether a node is entering or leaving a room, the system calculates the distance from the entrance location and the direction of movement. The hybrid SAIL system consists of two components, a mobile node and an anchor node, to recognise when a user passes through a particular location by observing the mobile node. The system expects the mobile node to be attached to a user and the anchor node to be mounted at a specific access location. The system requires the LF transmitter to be a part of the anchor node and the receiver to be with the mobile node. The anchor node, which is installed at the entrance, uses two LF antennas to cover the two sides of an entrance.

The SAIL system recognises and monitors the indoor location of a node using the received signal strength indicator (RSSI) of LF signals and the BLE signals between anchor nodes. The mobile node of the hybrid SAIL system, which receives LF signal from an anchor node, recognises whether the current situation is entry or exit. The RSSI values of the LF signals received by the mobile node are compared to determine the distance to the entrance location. The information obtained by the mobile node is

transmitted to the anchor node, which communicates with other anchor nodes in nearby locations over BLE. The anchor nodes form a distributed computing environment, which enables the SAIL system to expand the recognition range. As the anchor nodes of a distributed network synchronise and monitor the information received from a mobile node, the area corresponding to the location of the mobile node is activated.

An evaluation of the performance of the hybrid SAIL system showed that the system is applicable as a real-time situation-aware indoor localisation system. The system, utilising one anchor for every entry location, accurately recognised both the direction of travel and the indoor location of a mobile node. The maximum average localisation error was found to be less than 50cm. The system also performed well when mobile nodes congested in a specific area. The time to determine user location did not increase significantly as the number of nodes increased from 5 to 20. The difference in the average time to determine user location was less than 0.5 seconds between the two node settings. According to Park et al. (2018), however, the design of the hybrid SAIL system is best suited for location-based services and applications such as patient monitoring and mobile asset management.

2.5.1.3 Device Tracking

The work of Rashid, Louis, and Fiawoyife (2019) argued for improving user interaction with wireless appliances in smart home environments through real-time tracking of IoT device locations. The researchers pointed out that user interaction in the home IoT context has many drawbacks. Smart home control typically involves user interfaces which are complex and cumbersome. Amongst the different interfaces, voice and gesture interfaces considerably lack reliability. There is also the requirement that users must have prior knowledge of an environment to be able to

control it. Through their study, Rashid et al. (2019) introduced a point-and-click framework for users to be able to intuitively control the potentially numerous electrical fixtures in a smart built environment. The system architecture consists of the following four components –

1) *UWB Real-time Location Tracking System (RTLS)*
2) *User with a hand-held clicker*
3) *Electrical control system*
4) *Building Information Model-based virtual environment*

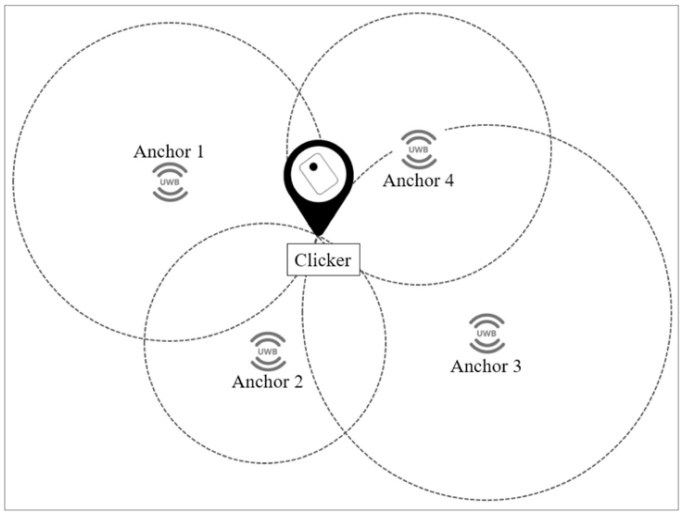
Communications between the different components, which uses a UWB wireless system, enables user interactions with the smart environment to be realised. The hand-held clicker transmits contextual information, including position and orientation, to the virtual environment to update the position and orientation of the virtual representation of the clicker. The virtual environment provides for deciphering the intent of a user to determine the appliance of interest. The virtual environment identifies the relay switch corresponding to the appliance and updates the clicker, which sends a command to the relay switch upon the click of a push-button that is mounted on the clicker.

The point-and-click functionality is enabled by a UWB-based indoor positioning system and an inertial measurement unit (IMU). Coupling the indoor positioning system and the IMU generates requisite contextual information of the user with respect to the built environment when a pointing action is performed by the user. The information retrieved is fed into a building information model-based virtual environment which then determines the appliance of interest to the user. The system uses two kinds of modules, namely, anchors and a tag. Implementation of the system

requires 5 of these modules, including 4 anchors and a single tag. Figure 2.5 shows the UWB-based localisation system which enables tracking the location and orientation of a handheld clicker in an indoor environment.

Figure 2.5

UWB-based Positioning System



Note. From *"Wireless electric appliance control for smart buildings using indoor location tracking and BIM-based virtual environments,"* by K. M. Rashid, J. Louis and K. K. Fiawoyife, 2019, *Automation in Construction,* 10.1016/j.autcon.2019.01.005. Copyright 2019 by Elsevier B.V.

The anchors, which must be mounted within a built environment, provide for reference points. The position of each anchor is determined and registered using the virtual environment. The tag, however, is implemented through the clicker that also has a 3-axis accelerometer and 3-axis gyroscope. The two instruments provide orientation information related to the clicker. The RTLS determines the location of a tag by using what has been referred to as the multilateration technique, which is also used by GPS. The technique involves determining the point of intersection of circles where the anchors form the centre and the distance from the tag forms the radius. The time difference between the UWB signals that are sent and received provides for calculating the linear distance between every anchor and the tag.

Although testing of the UWB-based positioning system showed that the framework is effective for radiolocating the low-power IoT devices in indoor environments, the work of Farnham (2019) highlighted that the design of UWB-based techniques generally overlooks the challenges for practical implementation. The researchers point out that the UWB technique, though robust against multipath effects of indoor environments, requires additional power as it involves high-bandwidth transmission between multiple access points within range. Despite the power constraints of many commodity IoT devices, Rashid et al. (2019) explored the UWB technique with the aim to extend the utility of Building Information Model to the operation phase of an environment and the integration of Building Information Model with IoT and smart devices.

2.5.1.4 Radio Environment Mapping

In the work of Farnham (2019), the researchers argued for the need of many IoT scenarios that require accurate real-time indoor location of low-power commodity devices, such as smart watches or asset tags. Radiolocation of low-power commodity devices enables applications such as asset tracking in domains, including, health, retail and industry. Another important application is geo-fencing in factories where there are autonomous robots alongside human personnel. However, the radiolocation of commodity devices in indoor environments is a difficult problem due to multipath radio propagation and as the movement of objects and people causes dynamic variations. Farnham (2019) noted that low-power commodity devices lack indoor localisation capabilities. The researchers further noted that existing techniques for indoor localisation require special hardware and involve surveying, both of which involves considerable expenses for the end-user.

To reduce the complexity and power requirements, which increases with the number of anchor nodes required for more accurate localisation, Farnham (2019) recommends exploiting existing Wi-Fi infrastructure with the Angle of Arrival estimation capability. The proposed approach requires two Wi-Fi access points, with not more than 4 antennas, to operate within the range of commodity devices. The radio transmissions of the commodity devices are utilised to generate awareness of the impact of environmental changes without high power consumption. The proposed approach, unlike some conventional approaches which combines Time of Arrival and Angle of Arrival techniques, involves selective use of Angle of Arrival capabilities. The approach also provides for adaptively taking radio measurements as compatible devices move around.

The radio transmissions obtained by the Wi-Fi access points are processed to obtain accurate representations of the radio spatial environment (Farnham, 2019). Spatial interpolation, which enables the estimation of radio signal strength (RSS) at locations for which measurements are not available, provides for mapping the radio environment with minimal measurements. Farnham (2019) recommends radio environment mapping to eliminate the unfeasible candidates and to locate transmitters which does not support sounding packets for localisation based on Angle of Arrival. Radio mapping also provides for a way to detect non-line of sight scenarios. Farnham (2019) underscores that the use of radio environment maps, which are repositories of the radio measurements and predictions, enables the inferences about a dynamic environment using standard radio infrastructure to be exploited for optimising the process of localisation.

The radio maps provide a way for the localisation approach to adapt the measurement frequency, reduce the number of measurements required and lower the computational cost. The radio maps, which are obtained by exploiting Angle of Arrival triangulation, provide a basis for fingerprint-based subsequent localisation of commodity device transmitters. Updates to predictions about an environment involve comparing the RSS measure with indirect radio propagation models. This, however, requires statistical or empirical models suitable for predicting the spatial distribution. The indirect radio map formation significantly reduces the number of complex calculations that is required as devices move in an environment.

Experiments utilised two 802.11n Wi-Fi access points, each of which has an Intel 5300 radio with 3 dipole antenna elements. The channel state information and RSS of the responses to sounding requests are used for calculating the Angle of Arrival of the beamforming sounding packets from Wi-Fi devices. The measurements are interpolated in the next step to form the radio path loss map. The results showed a 36% increase in localisation accuracy compared to fixed measurement frequency approach. For the same accuracy as the fixed measurement frequency approach, adaptive localisation reduced the power consumption by a factor of 20. The experiments in an indoor test scenario mainly showed that the adaptive localisation approach provides for accurate localisation without the need for expensive surveys or training of Artificial Intelligence (AI) techniques to recognise a wide range of scenarios.

However, the adaptive localisation approach is not designed for highly dynamic environments where the applications will need to adapt to changes frequently. Farnham (2019) noted that the power consumption will increase significantly if the

approach is implemented for dynamic scenarios. More measurements and calculations will also increase resource utilisation on access points, which is likely to affect the operation of a network. Implementation of the approach is also not suited for indoor environments where the IoT platforms utilise new and improved low-power wireless communication technologies such as Zigbee, Z-Wave. Although Farnham (2019) developed the adaptive localisation approach for low-power IoT device localisation within complex radio environments, the design of the approach limits the processing of responses to sounding packets which are received by Wi-Fi access points to the responses from compatible devices.

2.5.1.5 Localisation using Photodiodes

The work of Shao, Khreishah, and Khalil (2020) argued for improving indoor localisation that is based on Visible Light Communication (VLC) by eliminating the need for computation at the device through a real-time backward channel from devices to a controller. VLC-based indoor localisation, which utilises ubiquitous lighting infrastructure, aims to provide high accuracy localisation without causing any interruption to RF-based devices. VLC-based localisation involves capturing light from fluorescent lamps or LEDs and leveraging information such as the optical signals strength, angle-of-arrival, the polarization and light distribution patterns. Light, with its properties of dominant line-of-sight signals and the incidence angle sensitive propagation path loss, has enabled locating devices capable of sensing light.

In the work of Shao, Khreishah, and Khalil (2018), however, the researchers pointed out that VLC-based localisation is not suitable for location-based services in IoT environments. The researchers observed that most VLC-based approaches require location and orientation information to be transmitted to a server, which affects real-

time tracking of devices. The researchers further observed that the approaches require sensing and computation at the device, which adds significant workload on resource-constrained IoT devices. To address the aforementioned problems, Shao et al. (2020) recommended using the retroreflector-based visible light localisation system.

Retroreflector-based visible light localisation was originally introduced in 2018 through the work of Shao et al. (2018). Unlike other VLC approaches, the retroreflector-based visible light localisation approach is designed to operate without the need for any additional uplink RF channel. Other design considerations of the system, also referred to as RETRO by Shao et al. (2018), were immediate feedback, minimum latency and the capability to work with any single unmodified light source. To enable the localisation of IoT devices without computation at the device, both Shao et al. (2018) and Shao et al. (2020) argued using a retroreflector device, which will reflect light back to its source with negligible scattering.

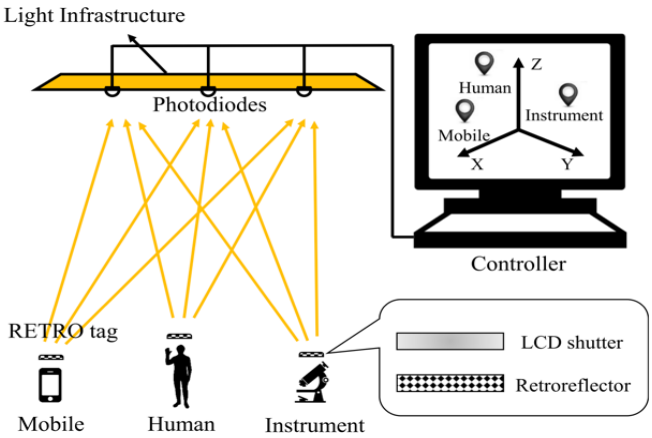
Implementation of RETRO involves small light sensors such as photodiodes to be mounted on infrastructural lamps. The retroreflector device, which is both small and lightweight, and the photodiodes together provides for an almost zero-delay backward channel from IoT devices to a controller device. The system also requires an LCD shutter to cover the front of the retroreflector for a unique signal frequency that distinguishes the reflected light of different IoT devices. The controller utilises the signal strength of the retroreflected optical signals to determine the location and orientation of an IoT device from its RETRO tag.

To evaluate the localisation and orientation accuracy of the RETRO system, signal amplitude measurements utilised a commercially available corner-cube retroreflector and a photodiode. The results obtained with a single photodiode are applied to a

realistic system, where a LED panel is used as light source and photodiodes are placed every 20cm. The photodiode with the largest output signal amplitude and 4 other photodiodes around it are selected by the controller for localisation. Using 5 photodiodes for their RSSI based localisation algorithm, the location error was found to be less than 2cm in most cases. The system also performed well in terms of orientation accuracy, with an orientation error of less than a degree. Figure 2.6 shows the RETRO system.

Figure 2.6

RETRO System



Note. From *"Enabling Real-Time Indoor Tracking of IoT Devices Through Visible Light Retroreflection,"* by S. Shao, A. Khreishah, I. Khalil, 2020, *IEEE Transactions on Mobile Computing, 19*(4), p. 837. Copyright 2002-2012 by IEEE.

A wide-scale implementation of the RETRO system requires an overhaul of both the manufacturing procedures and existing lighting infrastructure. In particular, the wiring process will need to be adapted to ensure that the size of the photodiodes is significantly less than the front face of the retroreflector (Shao et al., 2020). There is also the requirement of a specific type of light source. Shao et al. (2020) noted that the received optical power will not be comparable to the area of the light source when the light source is irregular. The accuracy of the RSSI-based algorithm depends on both the light emission pattern and the accuracy of modelling the light distribution.

The design of the solution is not suited for every type of lamp that may be utilised for indoor illumination.

According to Shao et al. (2020), the RETRO system is also not suited for the localisation of fast-moving objects. This requires the system to dynamically adapt the localisation algorithm to minimise the time required to run as the speed of object varies. However, the most significant drawback of the system is the localisation capacity, which is limited by the maximum modulation frequency. In theory, increasing the modulation frequency will enable a greater number of devices to be tracked simultaneously. As the output signal amplitude will decrease with increase in modulation frequency, Shao et al. (2020) recommend increasing the reflecting area of devices utilizing the higher modulation frequency. A larger reflecting area is required to guarantee the reliability of the retroreflected signal. Implementation of the system in an indoor environment, therefore, will require expensive surveys involving experts to understand the application scenarios and assess the installation requirements.

2.5.1.6 Limitations of Indoor Localisation Methods

Studies have utilised different combinations of techniques and technologies to develop localisation methods that provide for a wide range of location-based services in IoT environments. Though researchers have been successful in adapting techniques such as multilateration for new methods which are more suitable for IoT scenarios, the techniques and technologies utilised also limited the applicability of the solutions. In particular, the solutions developed for indoor localisation do not provide for ad-hoc implementation needs, such as to facilitate the work of forensic investigators during a field search activity in indoor IoT environments. Selecting the most suitable system or combination of systems suitable for an indoor environment requires reasonable

knowledge of the target environment. Selection and implementation will vary depending on factors such as the number of users, number of target devices, entry and exit points and available infrastructure.

Setting up and configuring systems such as SAIL and RETRO for the identification of IoT devices through indoor localisation services also requires knowledge of the current location of devices and their specific types. The requirement of prior knowledge of an environment introduces the need to survey a target indoor environment. The solutions further require hardware, such as anchor nodes or retroreflectors, to be integrated into existing infrastructure to be able to gather and process information pertaining to a specific location. Ad-hoc implementation of one or more indoor IoT localisation systems for IoT digital investigations, thus, risks tampering with the digital scene. Some systems also require users to carry additional hardware to enable tracking, which makes such solutions impracticable for forensic investigations.

Furthermore, the interaction between indoor localisation services and hardware installations such as anchor nodes requires applicable software to run on target devices. To enable localisation services, therefore, recommended software will need to be installed and configured on the actual devices prior to activation of localisation services. This introduces the need for remote installation and activation of software on target devices, which requires investigators to identify the IoT platform and be able to gain access to the different platforms. The ability to install and enable new services remotely, however, will vary between platforms and depend on available storage, which is often very limited in IoT devices unlike many other digital devices. Future work in this area, therefore, needs to consider the limitations of existing localisation

solutions for ad-hoc implementations and develop solutions that provide for forensic investigation purposes.

2.5.2 Individuality in IoT Device Behaviours

Researchers have been arguing for IoT device behaviour fingerprinting using deep learning methods (Aneja, Aneja, & Islam, 2018; M. Liu, Han, Liu, & Peng, 2021). Sánchez, Valero, Celdrán, G., and Pérez (2021) surveyed the work advancing IoT device behaviour fingerprinting within the area of behaviour data science. Researchers have been tapping into the potential of IoT device behavioural patterns for the challenge of optimization of devices and system performance in different scenarios. Advancements in device behaviour fingerprinting techniques has provided for significantly improving the limitations of traditional solutions for IoT device identification.

Traditional solutions have been mostly built on approaches such as names and labels, which are susceptible to modification or duplication in large environments where the number of devices increases significantly over time. Traditional solutions also involve multiple levels of granularity, which further adds to the complexities for management in IoT environments. Research and development of device identification through device behaviour fingerprints has focused on three levels of granularity. Sánchez et al. (2021) identified “type”, “model” and “individual” as the different categories of the granularity found amongst various studies. The requirement of a device type provides for the different types of devices to be detected. The requirement of a device model provides for the different models to be identified based on common hardware and software. Device fingerprints also provide for differentiating ‘individual’ physical

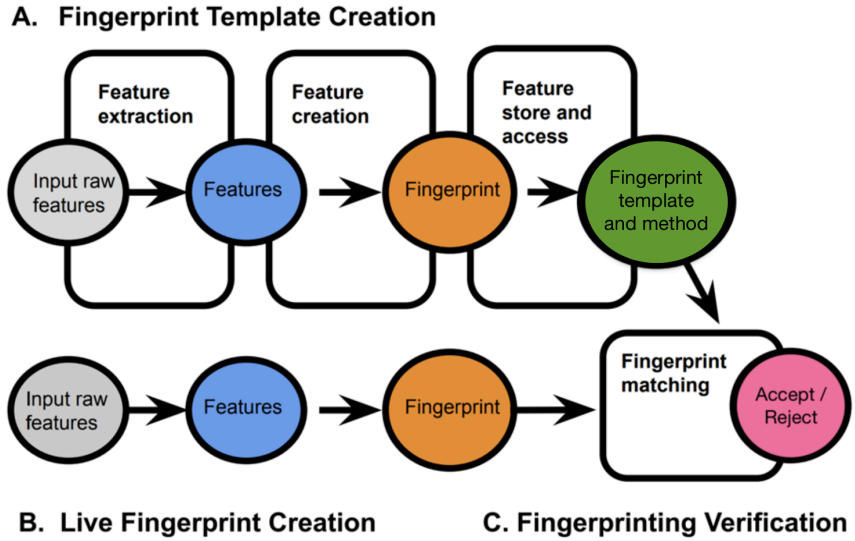
devices from the minor differences between identical physical devices (Sánchez et al., 2021).

2.5.2.1 Overview of Device Fingerprinting

The workflow of the device fingerprinting process starts with fingerprint template creation (Yadav, Feraudo, Arief, Shahandashti, & Vassilakis, 2020). This step is followed by live fingerprint creation and fingerprint verification, which is shown in Figure 2.7.

Figure 2.7

IoT Device Fingerprinting Process



Note. Adapted from *"Position paper: A systematic framework for categorising IoT device fingerprinting mechanisms,"* by P. Yadav, A. Feraudo, B. Arief, S. F. Shahandashti and V. G. Vassilakis, 2020, *2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things,* p. 65. Copyright 2020 by Elsevier B.V.

For the device fingerprinting process to be effective in target scenarios, the fingerprints of devices must be unique as well as impossible or very difficult to forge. It is also necessary for the fingerprints of devices to be built on features that are stable across a wide range of environmental conditions (Xu, Zheng, Saad, & Han, 2015).

The work of Yadav et al. (2020) identified many different approaches amongst the work to develop IoT device fingerprinting. The researchers further identified the different combinations of approaches that are applied for IoT device fingerprinting.

Amongst the different approaches, Yadav et al. (2020) found that most of the mechanisms that are developed utilised a passive approach in which a target is observed without any interaction. An active approach, in contrast to the passive approach, involves sending traffic with the aim to elicit responses from a target. The responses from a target provide for the information required to develop an identification pattern. Other popular approaches include a static approach and a combination of static and dynamic approaches. Static approaches rely on features that do not change over the time whereas the dynamic approach relies on features that typically change over time such as the inter-arrival time associated with data flow. From the combinations of approaches, the least popular has been the combination of active and static approaches. A few other approaches which have been combined are Medium Access Control (MAC), Network or Application layer for fingerprinting input features and device type, class or unique for fingerprinting output.

2.5.2.2 AI-based Device Fingerprinting

In Sánchez et al. (2021), the researchers point out a shift in the techniques used for processing and evaluating IoT device fingerprints from Statistical approaches to AI. This has led to the dominance of Machine Learning (ML) and Deep Learning (DL) techniques in device behaviour fingerprinting. The work of Yadav et al. (2020) identified the important features of an IoT device fingerprinting mechanism through a survey of the different approaches that studies have combined. The researchers found

most of the fingerprinting mechanisms that exists for IoT device identification to have combined 7 different approaches.

A classification of existing mechanisms based on 7 logical categories found that most of the existing mechanisms combined the passive approach along with AI. For the mechanisms that used AI, studies mainly combined the Network layer for fingerprinting input features. Few studies have also combined MAC and Application layers along with the Network layer for fingerprinting input features. Yadav et al. (2020) also found 1 study, from the 31 papers that were surveyed, to have utilised the MAC layer alone. For the fingerprinting output, however, the approach of most of the existing fingerprinting mechanisms were based on device class.

Yadav et al. (2020) compared ML-based fingerprinting with rule-based approaches developed for device fingerprinting. The researchers point out that the criteria of fingerprinting in rule-based fingerprinting are structured mathematically through if-then-else rules. The ML models, which have been created using different input features, have been trained using two different learning methods. Yadav et al. (2020) found that the development of ML-based fingerprinting mechanisms has utilised supervised and unsupervised learning. Amongst the two methods, supervised ML-based fingerprinting requires advance knowledge of the classification of the learning data and therefore, makes use of labelled data. In contrast, unsupervised ML-based fingerprinting involves the classification of unlabelled data by inference.

2.5.2.3 Fingerprinting Identical Devices

In the work of Jafari, Omotere, Adesina, Wu, and Qian (2018), the researchers utilise three different DL models for the identification of IoT devices from amongst devices of a single manufacturer. The study utilised six Zigbee certified devices which are

identical and generated large datasets of RF traces using a USRP based testbed to learn the characteristics of the different devices from the RF data. The study also makes use of RF data having a wide range of signal-to-noise ratio to be able to guarantee resilience in a variety of RF communication channel conditions. Experiments carried out showed that DL methods are suitable for analysing RF signals to distinguish IoT devices. However, the different DL models are primarily considered with the aim of developing a physical layer authentication method for IoT environments with the RF fingerprints of wireless IoT devices.

2.5.2.4 Inter Arrival Time Fingerprinting

In Aneja et al. (2018), the researchers developed a Convolutional Neural Network (CNN) for the identification of IoT devices based on the Inter Arrival Time (IAT), which is the time between two consecutive network packets that are received. The researchers point out that previous research has utilised statistical techniques for analysing IAT to generate device fingerprints required to differentiate devices. Their study utilised two Apple devices to obtain packets required to plot graphs of 100 IATS for the different devices. The resulting images of the graphs are processed for extracting device fingerprint features and to determine which of the selected devices can be differentiated. However, the researchers developed the CNN with the aim of providing a more efficient method of processing packets that are received by router devices for the identification of devices which are internal to a network. The technique, therefore, is suited for implementation in a Wireless Local Area Network (WLAN) environment and for the identification of a select number of non-IoT devices.

2.5.2.5 Differential Constellation Trace Figure Fingerprinting

In Peng, Zhang, Liu, and Hu (2019), the researchers developed a CNN for the identification of IoT devices. The study utilised 54 Zigbee certified devices and extracted Radio Frequency Fingerprint (RFF) features through a differential constellation trace figure (DCTF), which is a two-dimensional representation of the differential relationship of signal time series. The researchers also make use of RF data having different signal-to-noise ratios (SNRs). Classification of the 54 selected devices using CNN-DCTF showed the model to be suitable for identification across SNR levels of 15dB and 30dB. However, the proposed CNN-DCTF DL model is recommended as an alternative to existing RFF methods and developed for a terminal authentication method that has low complexity and high identification accuracy.

2.5.2.6 Lightweight Convolutional Neural Network for Fingerprinting

The work of Qing, Wang, Guo, and Yang (2020) argued for network traffic based multi-class classification for IoT device identification. The study recommends a new CNN model that is developed by removing unnecessary fully-connected layers and adopting the more efficient separable convolution over regular convolution. Simulations of the new CNN based identification showed lower computational complexity with a slight performance loss compared to other CNN based device type identification. The new network traffic and DL-based system, which is lightweight in terms of computational complexity and model size, is recommended as an alternative to other DL-based methods that are less suitable for IoT device type identification because of high computational complexity and larger model sizes. However, training of the recommended light-weight DL-based system requires the network layer traffic of target IoT environments.

2.5.2.7 Zero-Bias Deep Learning for Fingerprinting

The work of Liu et al. (2020) proposed an enhanced DL framework to utilise physical layer signals of IoT devices for their identification. The assumption for this work was that every wireless signal transmitter has a radiometric fingerprint that is likely to reflect in the demodulated signals. Experiments using real data from automatic dependant surveillance-broadcast showed the DL framework, which combines a zero-bias dense layer, to be effective. However, the study recommends the zero-bias dense layer for deep neural networks to jointly verify the identity of devices to be able to report on unknown IoT devices, which has been a challenge to accomplish using DL. The researchers built on this framework and argued for non-cryptographic device verification over cryptographic device verification to avoid the risk of identity spoofing attacks in IoT environments through the disclosure of security keys.

2.5.2.8 Bi-directional Fingerprinting

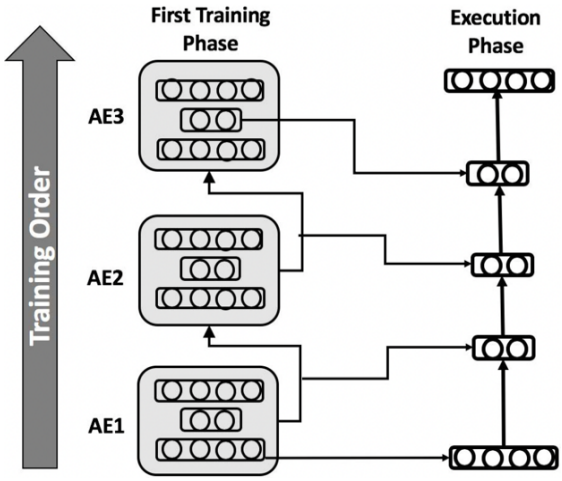
In Liu et al. (2021), the researchers proposed a new bidirectional IoT device identification method. The study developed an autoencoder-based RFF reciprocal conversion network to be able to predict the downlink RFF with samples of downlink signal data acquired from the uplink. The study builds on the work already done on RFF with a focus on what is described in Liu et al. (2021) as unilateral IoT device identification in one of two communication directions. Evaluations of the downlink identification network showed high accuracy of IoT device identification. However, the researchers exploit the inherent reciprocity in the RFFs of the two-way communications for IoT devices of a network to be able to identify the downlink. The proposed method enables IoT devices to offload the learning process from a device to the base station and reduces the computational complexity for IoT devices with hardware insufficiencies.

2.5.2.9 Probabilistic Fingerprinting

The work of Ortiz, Crawford, and Le (2019) presented a completely different technique for modelling device behaviour using network traffic. The researchers observed that previous studies have not provided for the identification of unseen devices and that designing techniques which provide high-accuracy identification requires a rich set of labelled network traffic. Their study introduced a probabilistic framework for device identification, the design of which aims to provide for a more suitable IoT fingerprinting mechanism to verify and discover IoT devices. Implementation of the framework involves stacked autoencoders as shown in Figure 2.8.

Figure 2.8

Stacked Autoencoders



Note. From *"DeviceMien: Network device behavior modeling for identifying unknown IoT devices,"* by J. Ortiz, C. Crawford and F. Le, 2019, *International Conference on Internet of Things Design and Implementation,* 10.1145/3302505.3310073. Copyright 2022 by Elsevier B.V.

Every autoencoder is trained in sequence, where the output of the n^{th} encoder is utilised as an input for training the $n^{th}+1$ encoder. The training phase of the fingerprinting mechanism recommended by Ortiz et al. (2019) requires pre-processed TCP-flow of the target devices for training a deep LSTM-autoencoder network. The

LSTM autoencoder is able to learn a set of representative features. The stacked autoencoders automatically learn the features of the traffic generated by devices as well as the classes of observed traffic. The mechanism also implements a Bayesian hyper-parameter tuning framework to separate the features from the data into discernible classes. The next phase of the mechanism involves a classifier which classifies all TCP-flow samples.

Ortiz et al. (2019) underscore that a distribution of the traffic classes is useful to probabilistically model devices. The researchers argued that probabilistic matching using known device behaviours will enable meaningful feedback in device identification, including for unseen devices. To generate the distribution for each device, all the TCP-flow samples are fed into an encoder. The output vectors of the encoder are taken as input by the classifier to assign a class label and classify the TCP-flow samples of every device. The classifier is further used to generate a distribution of all the traffic classes. In the next step, the distribution is transformed as a multinomial distribution with a Dirichlet prior.

For evaluation of the approach proposed in the work of Ortiz et al. (2019), the researchers collected at least 170,000 flows from a publicly available data source and more than 4 million samples from a private lab, each with a wide range of devices. The researchers separated the devices of the two independent sources into two main classes, namely, IoT and non-IoT devices. Over 20 IoT devices were amongst the devices at the publicly available data source, which was based in the University of New South Wales (UNSW Australia, 2017). The second source, a private lab based in North America, consisted of 72 IoT devices. The private lab utilised more than 1 instance of certain device types such as Google Chromecast, SonosPlay and

SmartThings hub. Device types such as Amazon Echo and Withings Aura were amongst the devices of both sources.

Experimental implementation found that the technique is suitable for the identification of devices with 50 or more samples. Experiments also found the technique to infer the class of previously unknown devices. These results, however, are not valid for the identification of IoT devices. Most of the devices which are identified as IoT devices in the work of Ortiz et al. (2019) are not designed for Internet-based applications where the number of connected devices grows significantly over time. Devices such as Amazon Echo, Google Chromecast and Amcrest Wi-Fi camera have all adopted the Wi-Fi standard for networking and communications. Whilst the devices require considerably high power and bandwidth to operate, the deployment of such devices in physical environments will be limited to non-IoT platforms.

2.5.2.10 Limitations of Fingerprinting Solutions

The differences in the wireless communications of digital devices have been exploited by researchers for developing IoT device fingerprinting mechanisms that mainly enable non-cryptographic identification of devices. The different techniques, which are primarily aimed at mitigating security risks in an IoT environment, also provide for detecting rogue devices and malicious changes to a network (Salman, Elhajj, Chehab, & Kayssi, 2019). In Y. Liu et al. (2020), the researchers underscore that the zero-bias layer developed for IoT device fingerprinting may also be generalised for virus detection or intrusion detection. Kotak and Elovici (2020) add that device fingerprinting using deep learning, which enables the verification of permitted IoT devices, is also useful for organisations that have adopted the Bring Your Own

Device policy. However, the AI-based fingerprinting techniques, which provide for IoT device identification in a range of scenarios, are not designed and developed with consideration of the challenges encountered by forensic investigators.

Although known and unknown IoT devices at a digital scene have forensic relevance, most studies have not considered the requirement of differentiating the unknown devices at the type and individual levels for developing the new AI models. Though most studies have combined a variety of approaches together with AI to improve device identification, the fingerprinting mechanisms recommended have been exclusively tested and evaluated for differentiating between known device types or individual devices. Thus, the existing AI-based fingerprinting mechanisms, although capable of detecting any unknown devices through differentiation of known devices, do not provide for differentiating the unknown devices. Apart from not being able to learn and differentiate unknown devices, most of the recommended AI models have been evaluated using a select few devices. The AI techniques are also not designed with a consideration for the interpretation of all the different layers involved, which is necessary for the work of forensic investigators. Similar requirements related to storage, security and privacy have also not been considered for the development of the AI models.

2.6 Conclusion

Studies have developed and improved various forensics-incorporated and forensics-unincorporated methods for the identification of Things. However, the techniques and technologies utilised for the methods limit the applicability of the solutions for identification by forensic investigators and LEAs. Despite the efforts and contributions of researchers over the years, practical challenges for investigators and

LEAs to accomplish the task of identifying Things at a wireless digital scene persists. This led to the conclusion that developing a framework that fills the gap in investigative procedures to identify Things is a necessary and worthwhile undertaking.

Chapter 3

LITERATURE REVIEW

3.1 Introduction

This chapter presents a review of the main networking solutions that are utilised for IoT applications. Following an appraisal of the evolution of Things, a survey of the networking solutions that enabled IoT applications involving a growing number of Things identified several widely deployed solutions. This chapter also identifies and reviews the communication technologies which underpin the networking solutions that enable Things to connect and communicate for Internet-based applications.

3.2 Internet of Things

3.2.1 The Origin

In 1999, MIT established the Auto-ID Centre to build a connected physical world, where information about things can be harvested and shared through the Internet. (Thiesse & Michahelles, 2006). The goal was to provide for linking the supply chain to corporate information systems and facilitate the creation of value chains built on the lifecycle of products (Sundmaeker, Guillemin, Friess, & Woelfflé, 2010; Thiesse & Michahelles, 2006). This MIT initiative significantly advanced automatic identification using Radio Frequency (Thiesse & Michahelles, 2006). This is considered by many to be an update of the technology that was manipulated by the Germans in World War II to identify their aircraft from allied and enemy aircraft (IEEE, 2015). The idea to create an “Internet of Things” by equipping physical objects with RFID tags led to the general acceptance and use of the term Internet of Things since the early 2000’s (Ashton, 2009).

Though the Auto-ID Center has since been attributed with the origin of the term Internet of Things, an earlier reference to the term was made in 1997 by the International Telecommunication Union (IEEE, 2015). Over the last two decades, however, researchers have worked towards a more inclusive vision for the Internet of Things (Gubbi et al., 2013; Sundmaeker et al., 2010). This has resulted in significant developments in different areas which has also progressed the realisation of a "smart environment" (Weiser, 1991), where the objects of the physical world are interconnected seamlessly. Although challenging, as pointed out in the work of Vermesan et al. (2016), the research community has had a focus on the development of a smart world, with the IoT providing for a ubiquitous information and communications infrastructure (Caceres & Friday, 2012).

Whilst cloud computing emerged as a critical technology to support a growing ubiquitous computing infrastructure, efforts to develop the environment envisaged in the work of Weiser (1991) converged WSNs, distributed computing and the Internet (Gubbi et al., 2013). Advancements in microelectromechanical systems and wireless communications enabled the adaptation of embedded sensors to suit a variety of miniature devices (Gubbi et al., 2013). This provided for the need of various domains to be able to utilise real-time data from their respective environments. Progress in the development of WSN technologies also enabled the interconnection of the heterogeneous miniature devices utilised in different domains, including the Industrial Internet domain (Gubbi et al., 2013).

3.2.2 Notions

According to Cisco IBSG (2011), however, the IoT came into existence between 2008 and 2009 as the World Wide Web evolved into a "social" web where people

connected, communicated and shared information with family and friends. It was estimated in 2010 that the market for IoT had generated as much as USD 30 billion for China's IoT industry in revenues (Business Wire, 2011). A loose collection of disparate networks which had emerged when the backbone infrastructure for the consumer Internet extended to business and industrial networks led to the notion of disparate networks coming together to form the Internet of Things (Cisco IBSG, 2011). The high number of digital devices that connected to the Internet during the late 2000s also contributed to this notion of the existence of the Internet of Things (Cisco IBSG, 2011).

Cisco IBSG (2011) also anticipated IoT to further evolve to become a "a network of networks" wherein diverse networks across different sectors are connected through increased security, analytics and management capabilities. However, the work of Sundmaeker et al. (2010) pointed out that the connected objects in various domains had merely formed what are Intranets of Things and mainly exchanged information within the environments where processes are controlled. Although the Internet expanded into enterprise and consumer assets, technology vendors had not been able to fully explore and exploit the potential of an expanded Internet (Vermesan et al., 2013).

According to Vermesan et al. (2014), several wired and wireless communication technologies such as Ethernet, Wi-Fi and Z-Wave, which are also supported by a strong technology alliance, had to be adapted for the specific needs of IoT applications, including energy efficiency, reliability and security. The IERC (2011) earlier argued for the technologies underpinning the Internet to be suited to enable people, data and things to connect seamlessly. In IERC (2011), the European Research Cluster on IoT envisaged the emergence of a new Internet-like structure

wherein uniquely identifiable objects interconnects and transforms the physical world into a knowledge system. Sundmaeker et al. (2010) also expected the IoT to be sufficiently open, complex and uncertain to transform the connected physical objects into “real actors of the Internet”.

3.2.3 Creating of Open, Global Network

Since the ARPANET, the Internet has mostly standardised on IP through continuous development and improvement (Cisco IBSG, 2011). Over the last decade, however, the Internet has been transforming into a new virtual space from where physical objects can interact and seamlessly respond to changes in the surroundings in a well-coordinated manner (Čolaković & Hadžialić, 2018). In Vermesan et al. (2013) and Vermesan et al. (2016), the researchers offer an explanation for the ongoing transformation of the Internet. Their work pointed out that the concept of IoT has evolved into a multidisciplinary domain, wherein Internet technology, devices and people have been converging (Vermesan et al., 2016).

Through the work of Vermesan et al. (2013) and Vermesan et al. (2016), the European Research Cluster on IoT draws focus to the creating of the open, global network as Business and Industrial Internet, Consumer, Business and Industrial Internet customer converge. The researchers at the European Research Cluster on IoT observed that IoT has been forging as a complete ecosystem for business innovation, reusability and interoperability through the open, global network that is created. Data, people and things will all be connected by the open, global network and new Internet-based applications and services will make use of the interaction and cooperation between a variety of things. For the IoT applications to make use of “intelligent”

things, however, the open, global network will additionally require the cloud to support with analytical intelligence (Vermesan et al., 2016; Vermesan et al., 2013).

As the concept of IoT allowed for pervasive presence of things, the markets for sensors, semiconductor, cloud computing and ubiquitous communication technologies expanded further (Vermesan et al., 2013). The possibilities to address the future challenges of societal trends through things interacting and cooperating in an Internet-like structure presented significant development opportunities for these different markets (Vermesan et al., 2013). Innovations in technology and applications markets have since enabled advanced computing to be weaved into physical objects for new generation intelligent systems. The work of Li et al. (2020) observed that computing has become an integral and invisible part of many different physical environments through the adoption of IoT in various sectors, including smart cities and other cyber-physical systems.

The growth in the deployment and presence of connected physical objects (Li et al., 2020) reflects the vision discussed in Weiser (1991) that of a physical world where software and hardware would be found everywhere without being noticeable. As ordinary objects are reimagined with advanced computing and communication technologies for a pervasive presence in 'smart and intelligent' environments of a variety of things, physical environments are increasingly characterised by intelligent devices, systems as well as decision-making (Acharjya, Geetha, & Sanyal, 2017; Gubbi et al., 2013; Vermesan et al., 2013). Areas such as spectrum sensing, transmission resource allocation are currently being developed by the research community to enable cognition of scenario and environments (Li et al., 2020). It is

expected that on-going developments will lead to intelligent cognition capability for IoT in the future.

3.2.4 An Equivocal Term

Although several enabling technologies have advanced an open and global network spanning every major economic sector, there is no standardised definition in literature as yet for the term "Internet of Things". Following are some of the definitions by key stakeholders of the IoT paradigm -

1. *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" (IERC, 2014).*

2. *"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (IoT-GSI, 2012).*

The Internet of Things has also been described as-

1. *"A network of items - each embedded with sensors - which are connected to the Internet" (IEEE, 2015).*

2. *"A network of interconnected objects that not only harvests information from the environment and interacts with the physical world, but also uses existing Internet standards to provide services for information transfer, analytics, applications and communications" (Gubbi et al., 2013).*

3. *"A pervasive presence of a variety of things or objects, such as RFID tags, sensors, actuators, and mobile phones, which through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals" (Giusto, Iera, Morabito, & Atzori, 2010).*

4. *"A network that is available anywhere, anytime, by anything and anyone" (ITU, 2005).*

3.3 Things

3.3.1 Expanded Term

Since the "Internet of PCs", which emerged in 2010 before moving towards the "Internet of Things", advancements in technology have enabled a broad array of physical objects which are capable of sensing and transmitting data to other similar physical objects connected through wired and wireless connections (Sundmaeker et al., 2010). In Gubbi et al. (2013), the researchers noted that what had been fundamentally Things had changed with the evolution of the concept of IoT. As IoT gained recognition as one of the key enablers of the next industrial revolution (Sundmaeker et al., 2010) and with initiatives such as the CASAGRAS project in 2008 recognising the importance of IoT for future economic growth and sustainability, researchers sought to bring clarity for the term based on the more inclusive concept of IoT which considers a pervasive presence of a variety of things in diverse environments.

In the work of Sundmaeker et al. (2010), the European Research Cluster on IoT defined Things as physical or virtual entities that interact and communicate with other Things and with the environment, react autonomously to events of the physical world and influence through processes that trigger specific actions, and which provide for

new services as active participants in business, information and social processes. The European Research Cluster on IoT further predicted that Things will vary depending on the domain of application. Whilst a more inclusive IoT extended the application domains to areas from intelligent buildings to independent living to automotive, the original goal of enabling computers to sense information without human intervention expanded beyond the type of physical objects within the supply chain context, where IoT had initially been of significance.

From basic sensors to a plethora of digital devices, a myriad of physical objects with computing and communication capabilities have progressively entered different domains over the last two decades. By 2008, sensors that could pick high-frequency electrical current from ingestible event markers, heart rate, body movement and other physiological parameters were already going through trials in patients. Technology that could collect data about patients were also being developed (Chorost, 2008). Major IT vendors like Cisco and HP initiated long-term projects, such as Planetary Skin, Central Nervous System for the Earth and Smart Dust, having the potential to add trillions of sensors to the environment (Cisco IBSG, 2011). During the late 2000s, a selection of sophisticated new devices that are diverse in functionalities rapidly entered consumer markets before business markets (Leclercq-Vandelannoitte, 2015).

With the globalization of mobile communications, smaller, smarter and more affordable new devices from smartphones to tablets having built-in communication capabilities increasingly connected to the Internet and exchanged information from virtually anywhere at anytime (Cisco IBSG, 2011). By 2009, the Internet additionally connected 27 million smart category mobile devices with GPS capability and mobile communication networks (Dixit, Ojanpera, Nee, & Prasad, 2011). By 2012,

advancements in WSN technologies such as WirelessHART and ISA100.11a enabled the transition of what had been collectively referred to as smart category devices in the industrial domain. The high cost of installation that is involved in the deployment of technology, such as measurement instruments and final control elements using wired technology, significantly limited its use before devices that used wireless technology emerged (Nixon, 2012).

Apart from being utilised for new devices with low-powered sensors and mobile sensors, WirelessHART also provided for environmental health and safety monitoring (Nixon, 2012). As advancements in WSN technologies enabled the interconnection of miniature devices equipped with sensors for applications in environmental, infrastructure and traffic monitoring (Gubbi et al., 2013), half of all the Internet connections in 2013 were estimated to be various Things (Vermesan et al., 2013). By 2015, wearables such as fitness trackers and smart watches, which integrated nanoelectronics, organic electronics, sensors, actuators, visualisation and communication technology, were being designed for systems involving body-mounted devices, clothes and fabric. Companies such as Google and Volvo worked to develop self-driven vehicles using automotive vision for a smart mobility future, where there would be computer-controlled vehicles (Vermesan et al., 2015).

3.3.2 Types of Things

Two main categories of Things have emerged in recent years, namely, consumer IoT and Industrial IoT devices (CBI, 2020). Whilst some of them are domain specific, an estimated 60% of the devices are cross-industry devices with use in multiple domains (CBI, 2020). There are also intermediary devices, which are typically more resourceful. Intermediary devices are typically utilised as gateways that provide for

connecting sensor devices and for edge processing of data (Milenkovic, 2020). Manufacturing, construction, healthcare, transportation and aerospace industries have also been using "digital twins" alongside Things and aside from the multitude of devices with built-in sensors that are connectable from the IoT ecosystem (Farsi, Daneshkhah, Hosseinian-Far, & Jahankhani, 2020).

Digital Twin, a term borrowed from NASA (Glaessgen & Stargel, 2012), refers to "a synchronised cyber representation and replica that mirror the states and behaviours of a physical Thing" (Milenkovic, 2020). Digital twins are enhanced with AI and software analytics to perform simulations using real-time sensor data from different environments and predict the behaviour of the physical counterpart (Kaur, Mishra, & Maheshwari, 2020). Digital twins have enabled predictive maintenance without the need for cloud-hosted services to access the physical assets (Kaur et al., 2020). As cloud-based proxy devices of physical assets, digital twins bring several benefits for cloud-based applications, including improved availability, faster access, bandwidth and power savings (Milenkovic, 2020). According to Cooney (2016), Gartner estimated millions of digital twins to represent Things by 2021.

3.3.3 Market for Things

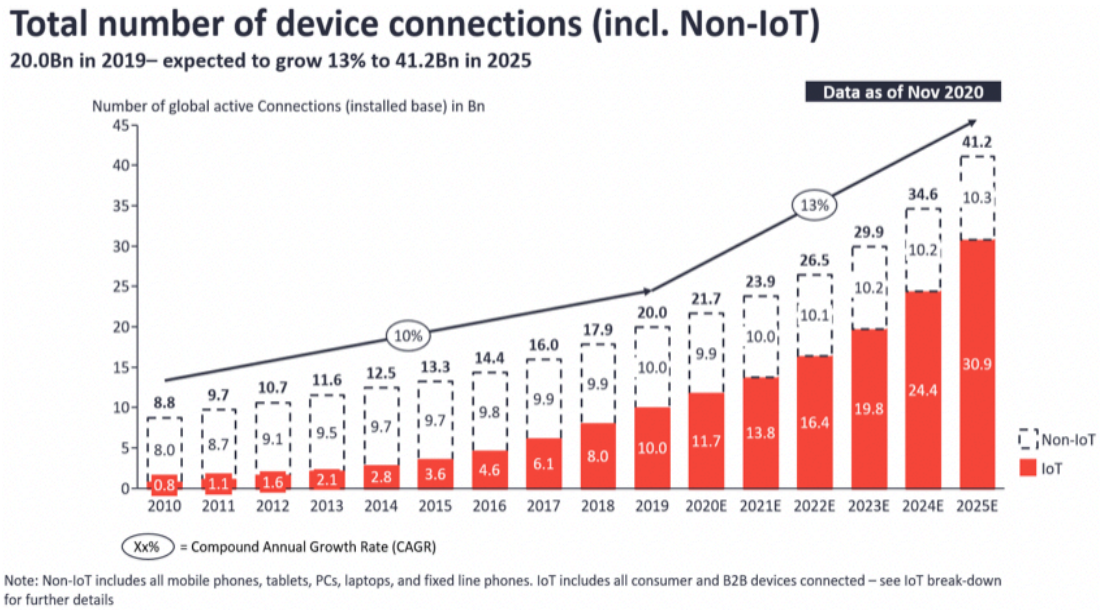
The market insights obtained and published by Lueth (2020) estimated that Internet-connected Things exceeded non-IoT connections, which comprised mobile phones, computers, tablets and laptops, at the end of 2020 by 4%. Consumer, manufacturing, utilities, retail and transportation sectors have all been moving ahead with the adoption of Things. Whilst advancements in IoT technologies enabled the replacement of smart devices of the industrial domain, Hatler (2017) estimated over 33 million industrial IoT devices to be in use for industrial applications by 2021. It

was also estimated that many of the industrial IoT devices will be used for short-range systems (Hatler, 2017). The market for consumer IoT devices, however, has been stronger compared to the market for industrial IoT devices. In 2020, industrial IoT devices accounted for 37% of all IoT devices (CBI, 2020).

Figure 3.1 compares the growth of IoT connections and non-IoT connections between 2010 and 2025 (Lueth, 2020).

Figure 3.1

IoT Surpassed Non-IoT Connections in 2020



Note. From *"State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time,"* by K. L. Lueth, 2020, (https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/). In the public domain.

Whilst consumer IoT devices accounted for 63% of the 12 billion active connections in 2020, over 45 billion consumer IoT devices are expected to be connected by 2025 (CBI, 2020; NZ IoT Alliance, 2020). In Europe, the third-largest IoT market following Asia-Pacific and North America, the market for IoT solutions is expected to grow 15.7% year on year until 2025 (CBI, 2020). KPN, the Dutch Telco, has covered

the Netherlands in a wireless IoT network to monitor various environments by connecting sensors. Many other nations are also building wireless network grids that will facilitate the delivery of IoT applications and enable users to select and subscribe through service providers (Juskalian, 2016).

SigFox, a leading service provider for IoT, already has coverage for at least 1.1 billion people across 70 countries, including Australia, New Zealand, Central America, Europe and the Middle East (Sigfox, 2020). Some cities have also partnered with IoT service providers to build IoT laboratories in exchange for the benefits of IoT solutions (NZ IoT Alliance, 2020). The shift in the paradigm of Internet-based applications has also been advancing the use of technology in the healthcare sector and enabling this crucial service sector to explore solutions suitable for the more desirable and convenient home-centric services (Silva, Khan, & Han, 2018). In Europe, healthcare applications are also integrated with big data, artificial intelligence and robotics to improve the delivery of health services (CBI, 2020).

3.4 Consumer IoT Mesh Networking Solutions

3.4.1 Z-Wave

3.4.1.1 Overview

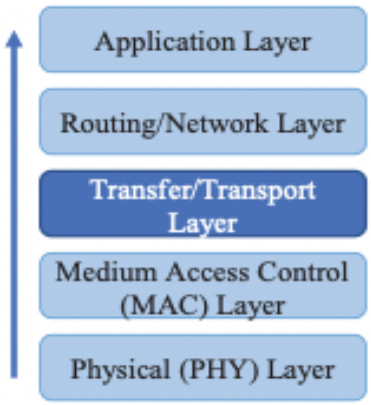
Z-Wave is an RF-based communications technology available for wireless IoT applications in residential and light commercial environments (Gomez & Paradells, 2010). This wireless communications protocol was introduced by Zensys in 1999 and designed for residential automation applications. The Danish company, based in Copenhagen, targeted the Z-Wave protocol for the low-cost and reliable home area network market (Hersent, Boswarthick, & Elloumi, 2011). Since its inception, the wireless communications protocol has been deployed for applications such as status

reading, monitoring and control of lighting, ambient temperature and security. According to Z-Wave Alliance (2022), Z-Wave technology is the market leader in wireless control and is deployed in over 100 million products sold worldwide.

The design of the Z-Wave protocol by Zensys allows for communications between devices without power constraints and devices with power constraints (Hersent et al., 2011). The wireless communications protocol stack constitutes 5 layers, namely, the physical layer, medium access control layer, transfer layer, routing layer and the application layer (Babun et al., 2020). Figure 3.2 shows the organisation of the different layers that form the Z-Wave protocol stack. The design of the protocol also allows for applications to build and operate over a mesh network. The protocol builds a routing table which ensures that every node has a valid path through select nodes to other nodes in a network. Radio signals from a source are relayed to destination by nodes without power constraints (Hersent et al., 2011).

Figure 3.2

Z-Wave Protocol Stack



Note. Adapted from *"Z-IoT: Passive device-class fingerprinting of zigbee and z-wave iot devices,"* by L. Babun, H. Aksu, L. Ryan, K. Akkaya, E. S. Bentley, E. S. and A. S. Uluagac, 2020, *Proceedings of the 2020 IEEE International Conference on Communications,* p. 2. Copyright 2020 by IEEE.

3.4.1.2 Z-Wave Device Types

Z-Wave technology differentiates different network devices as either controllers or slaves. Amongst the two types of nodes, a controller node maintains the full topology of a network and calculates the routes to reach any node of the network. Z-Wave networks deploy two types of controllers, namely, primary controller and secondary controller. A primary controller is responsible for maintaining the complete network topology map and calculating routes. A secondary controller receives copies of the node list and routes from the primary controller of a network and takes the role of the primary controller when a primary controller is not available. The Z-Wave protocol also allows for node inclusions at reduced radio power, which has enabled first-generation Z-Wave networks to deploy battery-powered devices as portable controllers (Hersent et al., 2011).

In contrast to controller nodes, slaves do not maintain the network topology. Further, a slave node does not calculate routes and has no topology map. However, a slave node acts as repeater on a network and provides for routing commands from other nodes of a network. Though Z-Wave requires that repeaters are mains-powered, the protocol allows for battery-powered nodes to operate as routing slaves. Like slaves, routing slaves do not calculate routes but have a limited knowledge of the network topology. Routing slaves store static routes to send unsolicited messages to up to 5 other nodes of a network. For a routing slave to optionally perform as a repeater, the slave node must be mains-powered (Hersent et al., 2011).

3.4.1.3 Z-Wave Inter-Node Communications Security

To enable broader application of IoT devices, the design of the Z-Wave protocol has allowed for securely transferring data between the nodes of a network. The

implementation of security, however, had been optional until recently. Z-Wave protocol does not employ any security solution at the medium access control and routing layers. The protocol provides security for Z-Wave applications through a Z-Wave Application Security Layer in transport layer, the implementation of which involves a security command class. The first-generation security solution provided confidentiality and message integrity to Z-Wave network communications through encryption of outgoing messages and a message authentication code (Hersent et al., 2011; Silicon Labs, 2018b).

Features of the first-generation security solution included end-to-end security on an application level, a single network-wide key, AES symmetric block cipher algorithm and 128-bit key length. However, vulnerabilities and shortcomings of the first-generation security solution led to an update of the security specifications for Z-Wave applications. The Z-Wave Plus framework update, which facilitates the implementation of robust new Z-Wave products, provides an improved security solution for applications. The new second-generation security solution employs a security command class that is different to the security command class defined for the first-generation security solution (Silicon Labs, 2018a, 2018b).

The updated security layer specifications refer to the original security command class as S0 and to the new security command classes as S2, where S2 stands for Security 2. Key features of the S2 command class-based security solution are stronger key exchange, stronger authentication, support for multicast and lower communication overhead. The S2 security solution requires every device to be assigned with a unique 40 digits device-specific key, which enables the validation of device identity. In

comparison to the S0 based security layer, the S2 security layer offers both a secure inclusion process and encrypted communications (Silicon Labs, 2018a, 2018b).

3.4.2 Zigbee

3.4.2.1 Overview

Zigbee, which is a popular RF-based technology, has been widely deployed for IoT applications since its release in 2005. The Zigbee wireless protocol was originally developed by Ember Corporation to provide for the need of a networking solution that will enable IoT applications with many nodes. However, the first specification of the Zigbee protocol was released by the Zigbee Alliance, an alliance of several companies which was formed in 2002 to support the development of a multi-vendor mesh networking solution that guarantees interoperability of multi-vendor products for IoT applications. In 2008, the Zigbee Alliance had more than 200 members with different rights, including promoters, participants and adopters. Since its inception, the Zigbee Alliance has released several enhanced versions of the Zigbee protocol through revised specifications such as Zigbee 2006 and Zigbee Pro (Chew, 2019).

Zigbee 3.0, which is a newer version built on Zigbee Pro, further improved the interoperability which allows various applications such as home automation, health care and lighting to share a network. The Zigbee Pro specification added support for more nodes and hops through source routing, multicasting and enhanced security for a secure operating environment. In comparison to the Open Systems Interconnection (OSI) model, the Zigbee protocol stack has a different structure. Zigbee specification has defined 4 main layers, namely, application, network, medium-access control and physical. The Zigbee network layer protocol, which enables mesh routing, provides for the need of IoT applications to operate in a more robust and resilient network. In

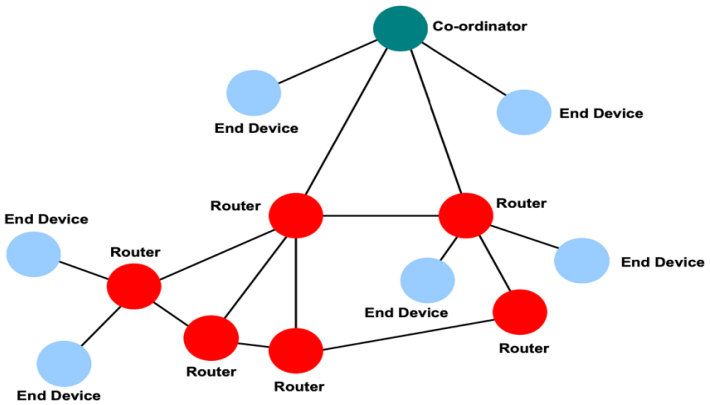
addition to routing, the Zigbee network layer handles network discovery and network management in a Zigbee network (Chew, 2019; Hersent et al., 2011; Kambourakis et al., 2020).

3.4.2.2 Zigbee Device Types

The Zigbee protocol specification allows for three different logical device roles in a network. The different device roles are the Co-ordinator, Router and End Device. The Zigbee Co-ordinator node handles network coordination and acts as the bridge to connect to other networks. Both Router and End-Device nodes must associate with either a Co-ordinator node or a Router node that is within radio range. Whilst extending a network, Router nodes give flexibility and efficiency for inter-node communications between End Device nodes and a Co-ordinator node that is outside radio range. The operation of a Zigbee network requires that both the Coordinator and Router nodes are continuously powered, without the need to go to sleep (Kambourakis et al., 2020; NXP, 2018). Figure 3.3 shows a Zigbee network with all the three device types.

Figure 3.3

A Zigbee Network



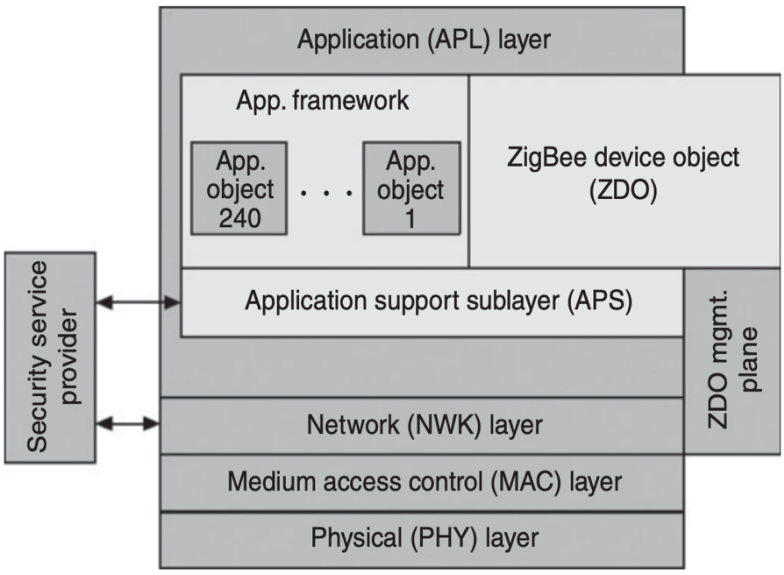
Note. From *"Zigbee 3.0 stack user guide,"* by NXP, 2018, (https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf). In the public domain.

3.4.2.3 Zigbee Inter-Node Communications Security

Some of the ideal applications using Zigbee include home automation, lighting control, meter reading, hospital patient monitoring, environmental control and industrial automation. To suit a wide range of applications in both commercial and domestic environments, the design of the Zigbee protocol stack has allowed for implementing secure Zigbee networks. Furthermore, Zigbee technology offers privacy for the communications between the nodes of a network. Zigbee protocol includes security features, such as access control lists, key-based encryption of network communications and frame counters, that enable measures to prevent intrusion of a network by malicious entities. The security services, which span two levels, are provided at the network and the application levels as shown in Figure 3.4. The key-based security for network communications utilises a 128-based AES-based encryption system (NXP, 2018).

Figure 3.4

Zigbee Protocol Security Levels



Note. From *The Wireless Internet of Things: A Guide to the Lower Layers,* by D. Chew, 2019, IEEE Press. Copyright 2019 by John Wiley & Sons, Inc.

Zigbee PRO security uses a 128-bit AES-based encryption system to encrypt network communications. The encryption of communications either involves the same key for all the nodes of a network or an individual key that is applied for communications between two specific nodes. The nodes of a Zigbee network may use keys that are pre-configured, commissioned during the installation of a system or distributed by a trust centre node that manages encryption keys whilst implementing security policies. The Co-ordinator of a Zigbee network is nominated by default as the trust centre node in a centralised security model. In a distributed security model where a trust centre is not used, the Router nodes of a Zigbee network manage security keys and security policies (Hersent et al., 2011; NXP, 2018).

3.4.3 Thread

3.4.3.1 Overview

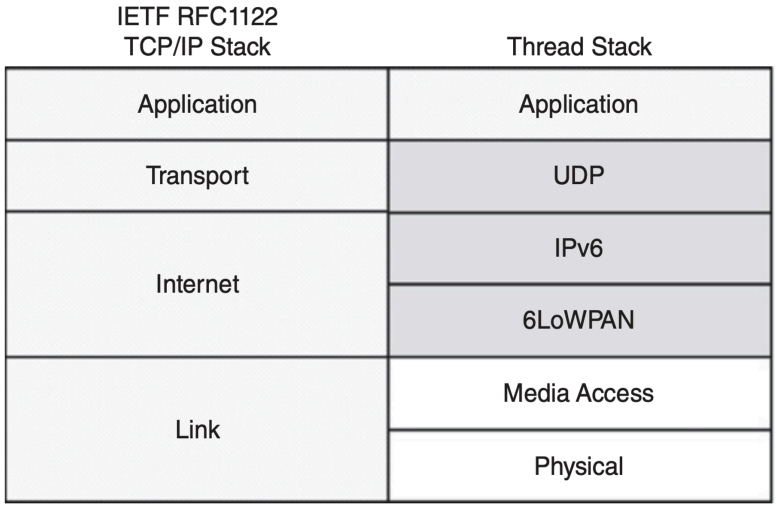
Thread, which is a relatively new wireless technology, added to the growing list of technologies that enable communication between power-constrained devices for various IoT applications. The RF-based technology, which was developed by Google Inc's Nest Labs to standardise the connectivity and communications of gadgets from different manufacturers, offers a different mesh networking solution for IoT applications. Like the Zigbee protocol, the Thread protocol is maintained and supported by the Thread Group. The industry group was formed in 2014 by Nest Labs and industry partners such as Samsung Electronics, ARM Holdings Plc, Yale Locks and Silicon Labs to encourage manufacturers of consumer gadgets to deploy Thread for IoT applications. At the time of writing, the growing list of members of the Thread Group also includes Amazon, Legrand, LG, Salto, SmartThings, Schneider Electric, Siemens, Orange and Osram (Thread Group, 2022a; Unwala, Taqvi, & Lu, 2018).

According to OpenThread (2022a) and Thread Group (2022b), the Thread protocol is a low-power and low-latency wireless mesh networking protocol that enables reliable and secure end-to-end communication between thousands of IoT devices. Thread offers manufacturers of products with the flexibility to implement multiple application layers on the same mesh network and provide for diverse use cases. Thread is also suited for the seamless integration of devices with larger IP networks. With an IPv6 over 6LoWPAN layer, Thread supports IoT applications on IPv6-based mesh networks. The IP foundation of Thread technology enables network operations without gateways, removing this potential single point of failure and reducing associated infrastructure investment for both connected homes and commercial buildings.

Figure 3.5, which is adapted from the work of Chew (2019), provides a comparison between the TCP/IP stack and the Thread protocol stack.

Figure 3.5

A Comparison between TCP/IP Stack and Thread Stack



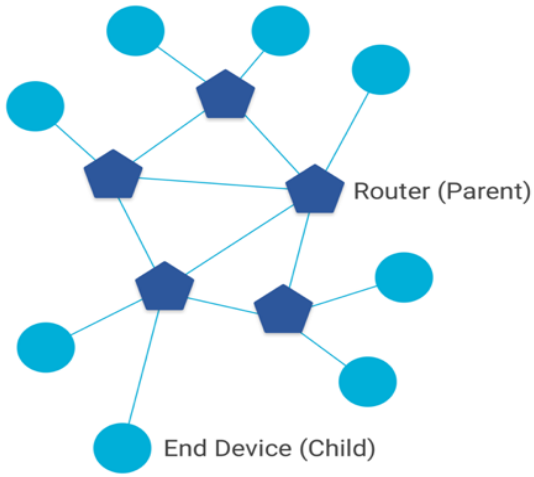
Note. Adapted from *The Wireless Internet of Things: A Guide to the Lower Layers,* by D. Chew, 2019, IEEE Press. Copyright 2019 by John Wiley & Sons, Inc.

3.4.3.2 Thread Device Types

Thread technology differentiates the nodes of a network as either a Router node or an End Device node. There are also different types of Router nodes and End Device nodes. Amongst the two main types of nodes, Thread Router nodes provide secure commissioning services to new devices joining a network. Amongst the different End Device types, a Router Eligible End Device node optionally acts as a Router to provide secure commissioning services when a Router node is not within the range of a new device trying to join a network. The three other End Device types are a Full End Device, a Minimal End Device and a Sleepy End Device. The different types of End Device nodes associate and communicate with a Router node, whereby a Router node becomes parent to one or more End Device child node, as shown in Figure 3.6 (OpenThread, 2022b; Thread Group, 2017).

Figure 3.6

Thread Parent and Child Nodes



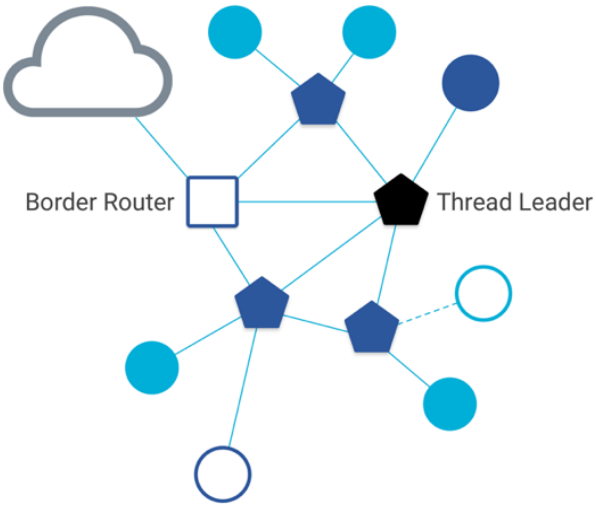
Note. From *"Thread Primer,"* by OpenThread, 2022, (https://www.openthread.io/guides/thread-primer). In the public domain.

The Router nodes must keep their transceiver enabled and forward packets for other devices that operate in a network. Whilst End Device nodes have no forwarding role,

the transceiver on all End Device nodes, except the Sleepy End Device type, is never disabled. Amongst the different End Device types, the Minimal End Device and Sleepy End Device do not subscribe to an all-routers multicast address. The Router, Router Eligible End Device and Full End Device, all of which subscribe to an all-routers multicast address, maintain the IPv6 address mappings of a Thread network. Furthermore, Thread technology requires that the Router nodes are managed by a single Router, which is dynamically self-elected as the Thread Leader. In addition to serving as a Leader, Router nodes serve as Border Routers for the external connectivity of a Thread network, as shown in Figure 3.7 (OpenThread, 2022b; Thread Group, 2017).

Figure 3.7

Thread Leader and Border Router



Note. From *"Thread Primer,"* by OpenThread, 2022, (https://www.openthread.io/guides/thread-primer). In the public domain.

3.4.3.3 Thread Inter-Node Communications Security

The design of the Thread protocol has also allowed for protecting information exchanged between the nodes of a mesh network. Thread technology offers confidentiality, authenticity and integrity for device communications with security

services applied to the Transport and Link layers. The security services provide for access control, replay protection and non-repudiation to prevent impersonation, message spoofing, tampering and other generic attacks. Security is implemented by encrypting runtime communications twice with two separate keys at the different layers where security services are applied. Thread employs DTLS encryption for messages encapsulated at the Transport layer and AES-CCM encryption at the Link layer (Kambourakis et al., 2020; Thread Group, 2017; Unwala et al., 2018).

The inter-node communications of a Thread network are encrypted using 128-bit encryption keys. Both the keys required are derived from a single Master Key, which is a network-wide key that is generated and securely distributed by the Leader node of a Thread network. Every node that joins a Thread network receives the Master Key from one of the Router nodes of that network. The key pair is generated by a Thread node using the SHA-based HMAC algorithm that is described in IETF RFC 6234. From the 256-bit output of the secure hash algorithm, the upper 16 bytes is used for link-layer encryption and the lower 16 bytes is used for transport-layer encryption. Furthermore, Thread implements hop-by-hop encryption for the security of 6LoWPAN headers to protect forwarding and routing operations (Kambourakis et al., 2020; Thread Group, 2017; Unwala et al., 2018).

3.5 Short-range Sensor Networks

As the concept of IoT evolved and expanded the scope of Things, researchers also pointed out that Sensor Networks have a key role in future communication and networking systems such as the IoT (Buratti, Verdone, & Ferrari, 2011). Over the years, many researchers have contributed to this important field of research from various perspectives. The main aim of the researchers has been to enable a large

number of small objects that mainly utilise sensing capabilities to collaborate and form a system that is both diverse and powerful (Buratti et al., 2011). The efforts by researchers have contributed to the development of a variety of Sensor Network radio technologies which are applicable for use in different geographical areas. Two radio technologies that are available for implementation of Sensor Networks in small geographical areas are the IEEE 802.15.4 and the ITU-T Recommendation G.9959.

3.5.1 IEEE 802.15.4

As wireless technologies that are suitable for the industrial domain emerged, Nixon (2012) observed that many smart devices developed with wireless communication capabilities for industrial applications operated in the 2.4GHz ISM radio band utilising IEEE 802.15.4 compatible DSSS radios. By providing for low data-rate wireless connectivity amongst fixed and mobile devices in challenging environments, the IEEE 802.15.4 radio technology enabled applications that require simple, low-cost communication networks (Bhat, 2011). The IEEE 802.15.4 radio technology has been utilised for two different industrial wireless standards, the International standard IEC62591-1, also known as WirelessHART, and the US standard ANSI/ISA100.11a-2011, also known as ISA100.11a (Nixon, 2012).

Since its inception in 2003, the IEEE 802.15.4 radio technology has also provided for developing and improving a variety of mesh networking standards, including Zigbee, Thread and DigiMesh. As Wi-Fi and BLE technologies are relatively less suitable for applications involving a growing number of inexpensive devices in small geographic areas, the more scalable mesh networking technologies have been enabling a variety of wireless IoT applications (Li et al., 2020). So, the mostly licence-free spectrum has increasingly been shared for wireless personal networking. In contrast to the data rate

of 11Mbps that is supported by Wi-Fi, the mesh networking technologies support reliable, low-latency transmission at data rates greater than 100kbps and less than 500 kbps. There is, however, growing interest amongst researchers to enable Things and sensors to share the 4G and 5G licensed spectra that will meet the growing bandwidth needs of some IoT applications but reduce occupancy of license-free spectrums (Li et al., 2020).

Table 3.1 shows the spectrum shared with wireless personal networking technologies.

Table 3.1

Shared Spectrum

Wireless Technology Type	Technology Name	Max Range	Max Bandwidth/ Data Throughput	Operating Life (Battery)	Module Cost	Spectrum/ Operating Frequency	Spectrum License
WPAN	ANT+	30m	1 Mbps	Days	$1 - $15	2.4 GHz	unlicensed
	Bluetooth 4.0 LE	50m	24 Mbps	Hours	$1 - $15	2.4 GHz	unlicensed
	RFID	Passive: 10m Active: 100m	100 Kbps	Passive Tags: n/a Active Tags: years	Passive: <$1-$5 Active: $5-$25	120-150 kHz; 12.56 MHz, 433 MHz, ISM bands (868 MHz, 900 MHz), 2.5-5.8 GHz	unlicensed
	NFC	10cm	424 Kbps	n/a	<$1	13.56 MHz	unlicensed
	802.15.4g	200m	200 Kbps	Up to 4 years	$1-$15	2.4 GHz	unlicensed
	ZigBee	10-100 meters	250 Kbps	up to two years	$1 - $15	2.4GHz/ 900Mhz (915 MHz, 868 MHz)	unlicensed
WLAN	Wi-Fi	300m	250 Mbps (802.11n); 54 Mbps (802.11a/g); 11 Mbps (802.11b); 1Gbps (802.11ac)	4-8 hours(com) 50 hours (idle)	$10+	2.4GHz/5GHz	unlicensed
	Wi-Fi (802.11ah)	up to 1000m	100 kbps (802.11ah)			Sub-1 GHz ISM bands - Europe (863-868.6 MHz); Japan (950.8 MHz - 957.6z MHz); Korea (917-923.5 MHz); USA (902-928 MHz)	unlicensed

Note. Adapted from *Harnessing the Internet of Things for Global Development*, by ITU and Cisco (2016), https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf. In the public domain.

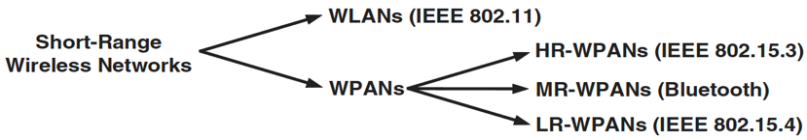
3.5.1.1 Low-Rate Wireless Personal Area Networks

The work of Buratti et al. (2011), which includes a detailed explanation of the IEEE 802.15.4 technical standard, described IEEE 802.15.4 as the de-facto standard for Low-Rate Sensor Networks. Typical characteristics of Sensor Networks assumed for

the IEEE 802.15.4 standard are numerous devices, battery-powered devices, star and mesh topologies, low bandwidth, small packet sizes, varying address lengths, unknown node positions, high unreliability, as well as long idle periods (IoT6, 2014; Langendoen, 2008). The IEEE 802.15.4 is mainly recommended as a low data-rate alternative to other short-range communication technologies, such as IEEE 802.15.1 or the Bluetooth technology as shown in Figure 3.8, which has enabled Wireless Personal Area Networks (WPANs) with little or no infrastructure (Farahani, 2008; IEEE, 2020).

Figure 3.8

Short-range Communication Standards



Note. From *Zigbee Wireless Networks and Transceivers* (p. 4), by S. Farahani, 2008, Newnes.

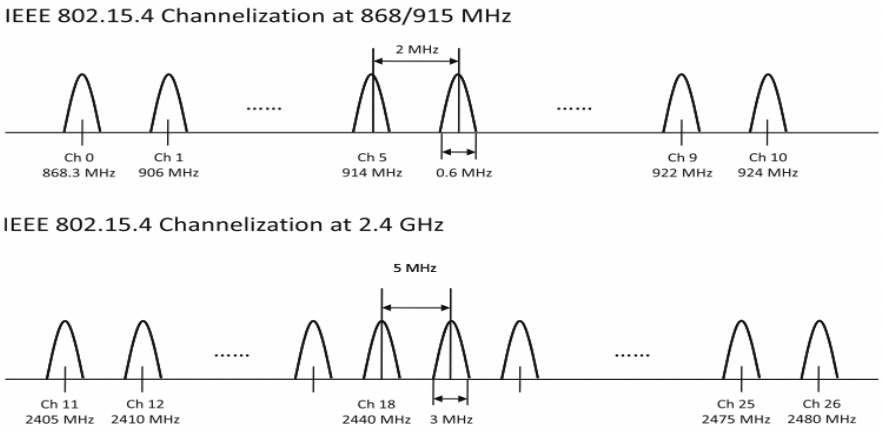
In addition to providing for low data-rate, short-range transmissions, IEEE 802.15.4 provides for ultra-low power consumption to guarantee long battery lifetime (IEEE, 2020). The IEEE 802.15.4 standard also provides for an ultra-low complexity, ultra-low cost radio technology, which is desirable to applications involving a growing number of devices (IEEE, 2020). The standard, which is a part of the 802.15 family of standards, is mainly suited for applications having relaxed throughput and latency requirements (Buratti et al., 2011). The aim of the IEEE 802.15.4 standard, however, is to standardise the lower layers of the OSI model whilst enabling wireless connectivity amongst inexpensive devices. The standard, therefore, defines the specifications for the bottom layers, the physical layer (PHY) and the MAC sub-layer.

3.5.1.2 802.15.4 Radio Data Rates and Range Options

With multiple PHYs defined for the PHY specification, the IEEE 802.15.4 standard has support for Sensor Networks in a variety of frequency bands. The PHY specification includes support for the 868MHz, 915MHz and 2.4GHz frequency bands to enable low-rate wireless connectivity across the mostly unlicensed spectrum in different regions. Across the three frequency bands, the standard specifies 27 half-duplex channels and allows a raw data rate of up to 250kbps with the option to scale down the data rate to suit applications with requirements of 20kbps or less. Amongst the three bands, the 868MHz band, for which a minimum of -92dBm RF sensitivity is specified, provides for up to 20kbps data rate. This band has a single channel, as shown in Figure 3.9, with an ideal transmission range of 1km (Buratti et al., 2011; IEEE, 2020).

Figure 3.9

27 Channels across 868MHz, 915MHz and 2.4GHz Bands



Note. From *Sensor networks with IEEE 802.15. 4 systems: distributed processing, MAC, and connectivity,* by C. Buratti, R. Verdone and G. Ferrari, 2013, Springer. Copyright 2011 by Springer-Verlag Berlin Heidelberg.

The 915MHz band, for which a minimum of -92dBm RF sensitivity is specified, also has an ideal transmission range of approximately 1km. This band, however, supports up to 40kbps data rate across 10 channels. The 2.4GHz band has a slightly different

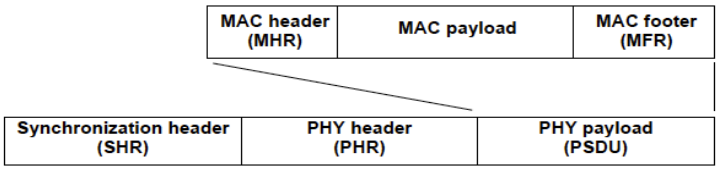
requirement of -85dBm or better RF sensitivity. This band supports up to 250kbps data rate across 16 channels. This band, however, has a much less ideal transmission range of approximately 200m, the computation of which considered a compliant device as capable of transmitting at -3dBm. Buratti et al. (2011) point out that the true or actual transmission range is much lower than the ideal transmission range due to real-world propagation impairments arising from wave reflection, diffraction and scattering.

3.5.1.3 802.15.4 Radiocommunications Structure

The IEEE 802.15.4 PHY layer specification requires that transmissions between IEEE 802.15.4 compatible devices, each forming a Physical Protocol Data Unit (PPDU), are organised as frames. The frame structure, however, will vary depending on the purpose of transmission. Regardless of the frame structure, every PPDU combines a Synchronization Header (SHR), a Physical Header (PHR) and a Physical Service Data Unit (PSDU) or Physical payload, as shown in Figure 3.10. A PSDU is essentially the MAC Payload Data Unit or the MAC layer frames generated by combining a MAC Header, MAC Footer and a MAC Service Data Unit (MSDU) or MAC payload. To reduce the complexity, however, the IEEE 802.15.4 standard limits the transmission frame structures to four possible types for every PPDU (Buratti et al., 2011; IEEE, 2020).

Figure 3.10

Schematic View of IEEE 802.15.4 PPDU



Note. From *"802.14.5-2020 - IEEE standard for low-rate wireless networks,"* by IEEE, 2020. In the public domain.

The standard provides for sufficiently robust transmission in noisy channels between inexpensive devices with beacon frames, data frames, acknowledgement (ACK) frames and MAC command frames. Amongst the pre-defined purposes of transmission, the optional confirmation of successful frame reception is enabled by ACK frames. The IEEE 802.15.4 standard provides for the transfer of data through data frames. The IEEE 802.15.4 radio technology also utilises MAC peer entity control transfers and beacon messages, the transmission of which is enabled by the MAC command frame and beacon frame, respectively. The design of the frame structures, except the ACK frame structure, has provision for a MAC payload. The PHY payload, therefore, may vary but not exceed 127 bytes. Furthermore, the standard requires the SHR and PHR of every PPDU to be 5 bytes and 1 byte, respectively (Buratti et al., 2011; IEEE, 2020).

3.5.1.4 802.15.4 Peer MAC entities, Topologies and Channel Access

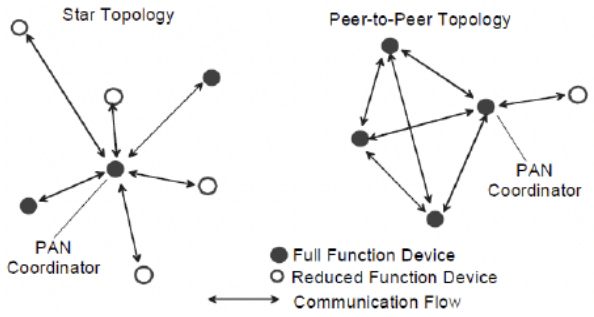
The IEEE 802.15.4 radio technology provides for both star and peer-to-peer operation with capabilities such as unique 64-bit extended address or allocated 16-bit short address, full acknowledged protocol, and energy detection. The standard differentiates IEEE 802.15.4 compliant devices as either a Full Function Device (FFD) or a Reduced Function Device (RFD), where the FFD is capable of all the services defined by the IEEE 802.15.4 MAC specification compared to the RFD which provides for limited services. The standard further differentiates IEEE 802.15.4 compliant devices as a Personal Area Network (PAN) coordinator, a coordinator or a device. PAN coordinators and coordinators are always FFDs. However, FFDs are not always PAN coordinators and coordinators. RFDs, though, always constitute devices (Buratti et al., 2011; IEEE, 2020).

The IEEE 802.15.4 WPAN requires two or more IEEE 802.15.4 compliant devices to communicate on the same channel. Regardless of the topology adopted, every IEEE 802.15.4 WPAN requires a PAN coordinator to serve as the primary controller of the PAN. Though the IEEE 802.15.4 radio technology provides for connectivity amongst mainly battery-powered FFDs and RFDs, mains-powered FFDs are preferred for PAN coordinators. The PAN coordinator selects a unique identifier for the PAN established by it. The PAN coordinator is also responsible for assigning unique short addresses to the other FFDs and RFDs joining a PAN with extended address. Communications between devices of a PAN using the short addresses are enabled by the unique PAN identifier, which also enables transmissions between independent networks (Buratti et al., 2011; IEEE, 2020).

To allow Sensor Networks to adopt either star or peer-to-peer topology, the IEEE 802.15.4 radio technology enables links to be formed around a single FFD and between any FFD and any other FFD that is within transmission range, as shown in Figure 3.11.

Figure 3.11

Star and Peer-to-Peer Topologies



Note. From *"802.15.4-2020 - IEEE standard for low-rate wireless networks,"* by IEEE, 2020. In the public domain.

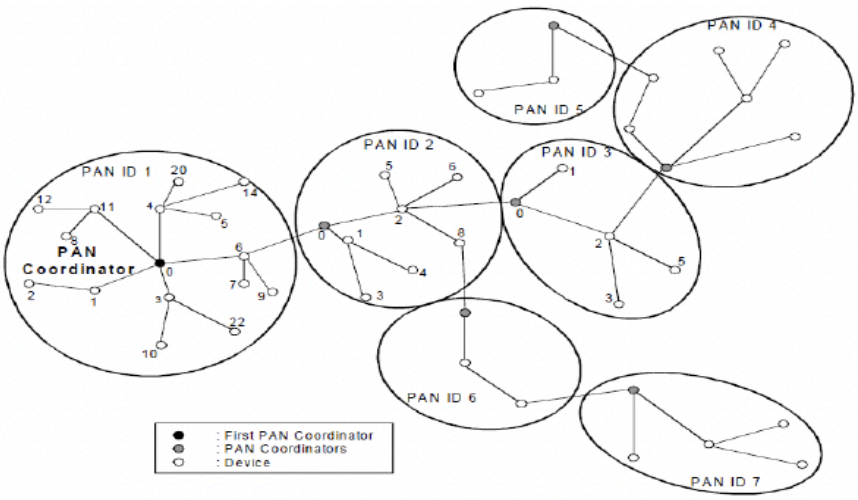
A peer-to-peer network, which enables multiple hops to route messages between devices within range of each other, is especially beneficial for more complex network

formations such as a mesh network. The IEEE 802.15.4 radio technology also enables Sensor Networks to form a cluster tree, which is a special case of a peer-to-peer network, where most of the devices are FFDs and RFDs connect as a leaf device at the end of a branch (Buratti et al., 2011; IEEE, 2020).

IEEE 802.15.4 compliant devices may form a single cluster network structure, which is the simplest form of a cluster tree network, where all the FFDs behave as coordinators. Where there are multiple neighbouring clusters, the devices across adjacent clusters of a cluster may join a growing mesh of clusters to form a large multi-cluster network structure, as shown in Figure 3.12. Though a multi-cluster structure increases message latency, the mesh of multiple neighbouring clusters significantly increases coverage area. The IEEE 802.15.4 MAC enables functions such as PAN association and disassociation, network beacon generation, a reliable link between two peer MAC entities, ACK frame generation and channel access employing CSMA-CA (Buratti et al., 2011; IEEE, 2020).

Figure 3.12

A Mesh of Multiple Neighbouring Clusters



Note. From *"802.15.4-2020 - IEEE standard for low-rate wireless networks,"* by IEEE, 2020. In the public domain.

The IEEE 802.15.4 radio technology enables two different modes of channel access with CSMA-CA, namely, beacon-enabled and non-beacon enabled. In Sensor Networks implementing non-beacon enabled access mechanism, the MAC sub layer shall employ the unslotted version of the CSMA/CA protocol for transmitting data or MAC command frames. For Sensor Networks implementing the beacon-enabled access mechanism, the MAC sub-layer employs the slotted version of the CSMA-CA algorithm. This, however, requires the WPAN coordinator to transmit beacons periodically and bound the channel time through a superframe structure that has an active and inactive portion. During the inactive portion, the WPAN coordinator will be able to enter a sleep (low power) mode (Buratti et al., 2011; IEEE, 2020).

3.5.2 ITU-T G.9959

The G.9959 recommendation, which the ITU Telecommunication Standardisation Sector issued for in-premises access networks, has been available and updated since 2012. According to ITU-T (2015), the ITU-T issued the G.9959 recommendation with a view to standardising sensor device communications on a worldwide basis. In the G.9959 recommendation, the ITU-T has defined the specifications for short-range narrow-band digital radio communication transceivers, which are useful for wireless IoT applications involving mostly small form-factor devices (ITU-T, 2015). Since its first release in 2012, the G.9559 recommendation has enabled the interoperability of several wireless IoT hardware (Chew, 2019). With the G.9959 recommendation, the ITU-T mainly offered a narrow-band sensor networking standard which allowed for mesh topology network operations.

The main purpose of the G.9959 recommendation, however, has been to decouple the layers that the proprietary Z-Wave protocol; utilised for a variety of smart home

products since 2003; implemented to enable low-rate data transmissions. Revisions to the original G.9959 recommendation, including the 2015 revision, do not limit the network formations to mesh topology. The specifications covered by the G.9959 recommendation have allowed for different network topologies, like the specifications covered by IEEE 802.15.4 technical standard. Furthermore, the G.9959 recommendation of the ITU-T has been targeted at the home automation sector, identifying this sector as the main area for which the specifications have been defined. (Chew, 2019).

3.5.2.1 Narrow-band Short-Range Sensor Networks

The main characteristics of short-range sensor networks which are assumed for the ITU-T G.9959 specifications are very similar to the characteristics which are assumed for the IEEE 802.15.4 specifications. The G.9959 recommendation is also suited for numerous devices, battery powered devices, mesh formations, low bandwidth, small packet sizes, unknown node positions, high unreliability, as well as long idle periods. In contrast to IEEE 802.15.4 radio technology, however, the ITU-T G.9959 radio technology has provided for a narrow band alternative to low-rate, short-range communication technologies. In addition to providing for narrow band, short-range communication transceivers, the ITU-T G.9959 specifications have been defined with a focus on low-power, low-bandwidth control networks. The G.9959 recommendation specifies that the maximum power level at the input of a compatible receiver, which has been referred to as the receiver saturation power level, must be in decibels comparable to 1 milliwatt (ITU-T, 2015).

Whilst the ITU-T G.9959 recommendation mainly pertains to the lower layers of the Z-Wave protocol, the specifications mostly conform to the OSI model. Similar to the

IEEE 802.15.4 standard, the ITU-T G.9959 recommendation for short-range, narrow-band transceivers has mainly defined the PHY and MAC layer specifications. The MAC layer of the G.9959 recommendation provides for on-demand communications and acknowledged communications in a low-cost control network. Other responsibilities of the MAC layer include handling domain identification, node identification, collision avoidance and backoff algorithms, transmission error and support for battery operation. Furthermore, the MAC layer specifies a 32-bit identifier to uniquely identify individual domains and an 8-bit short address to uniquely identify nodes within a given domain (Chew, 2019; ITU-T, 2015).

The PHY layer specifications of the G.9959 recommendation define the data transfer rates and a frame format that is suited for low-power, low-bandwidth control networks. Outgoing data is inserted into a physical RF frame format at the PHY layer. The layer is also responsible for extracting and forwarding of incoming data from the RF frame structure to the upper layers. In addition to forwarding for the upper layers, the PHY layer handles tasks such as the activation and deactivation of a radio transceiver, data transmission and reception, clear channel assessment and frequency selection. In contrast to the IEEE 802.15.4 PHY layer, the G.9959 PHY specification also provides for a multi-channel operation. This involves the assignment of RF profiles to physical channels (ITU-T, 2015).

3.5.2.2 G.9959 Radio Data Rates and Range Options

In comparison to the IEEE 802.15.4 standard, which has support for both sub-GHz and super-GHz transceivers, the ITU-T G.9959 recommendation has support for sub-GHz transceivers only (ITU-T, 2015). Though the ITU-T G.9959 PHY specification does not define specific regional frequencies, ITU-T G.9959 compliant radio

communication transceivers generally operate in 868MHz and 915MHz ISM bands (Herrero, 2022). The sub-GHz band operation enables G.9959 transceivers to offer applications superior range performance in indoor environments where there are walls and other obstacles (Silicon Labs, n.d.). The transceivers conforming to the G.9959 recommendation also rely on other regional specific bands for operation, which varies based on local licensing and regulations (Herrero, 2022).

When compared to the 2.4GHz band, operating at sub-GHz bands provides G.9959 radios with superior propagation characteristics (Chew, 2019; Silicon Labs, n.d.). Sub-GHz bands, which enable easier transmissions, also improve the transmission efficiency of G.9959 radios (Silicon Labs, n.d.). Sub-GHz bands are a quieter spectrum when compared to the more congested 2.4GHz ISM band, where radio signals from various sources, including Wi-Fi devices, Bluetooth devices and microwave, crowd and collide (Chew, 2019; Silicon Labs, n.d.). Across the supported license-free RF bands, G.9959 recommendation allows for compatible RF transceivers to operate in a one, two or three channel configuration. In contrast to IEEE 802.15.4 transceivers, wireless communications using G.9959 transceivers may occur over one or more channels and at one or more data rates (ITU-T, 2015).

The G.9959 PHY layer specification requires that each channel is assigned a unique RF profile, which will vary depending on the RF profiles designated for a region. An RF profile may have one or more data rates defined for use over a specific radio channel (ITU-T, 2015). To allow more than one transmission rate, regardless of the RF band, G.9959 radio technology supports physical layer configuration changes (Herrero, 2022). Unlike IEEE 802.15.4 PHY specification, where the data rate varies based on the RF band, the G.9959 PHY specification has defined up to three different

data rates for use in a given radio channel (ITU-T, 2015). The data rates of 40kbps and 100kbps are applicable to both mains-powered and battery-powered nodes. A lower data rate option of 9.6kbps is also available to mains-powered devices.

Table 3.2 shows the minimum receiver sensitivity that is specified for each of the three applicable data rates.

Table 3.2

G.9959 Receiver Sensitivity

Data Rate	Minimum Receiver Sensitivity
9.6kbps	-95dBm
40kbps	-92dBm
100kbps	-89dBm

Note. Adapted from *Recommendation ITU-T G.9959*, by ITU-T (2015). In the public domain.

Whilst the operational range of the G.9959 transceivers depends on several factors of a given environment, the ITU-T G.9959 recommendation does not specify the ideal transmission range for compliant sub-GHz transceivers (Chew, 2019). The work of Chew (2019), however, argues that the ITU-T G.9959 recommendation allows for a typical range of 30 metres when the operating environment is indoor. Chew (2019) explains that whilst Z-Wave technology conforms to the ITU-T G.9959 recommendation, the typical operating range provided by Z-Wave technology corresponds to the typical operating range of G.9959 radio technology. Chew (2019) further notes that the typical range of G.9959 radio technology increases to 100 metres when the operating environment is outdoor.

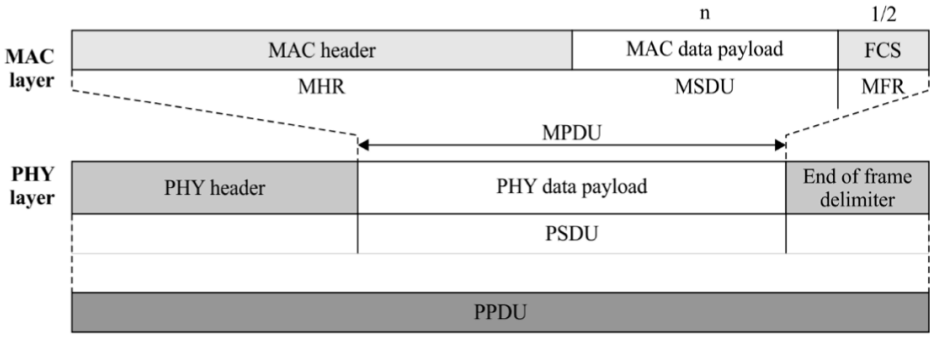
3.5.2.3 G.9959 Radiocommunications Structure

Similar to IEEE 802.15.4 PHY, the G.9959 PHY organises transmissions over the physical radio channel as frames, each of which constitutes a G.9959 PPDU. The

structure of a G.9959 PPDU, in contrast to IEEE 802.15.4 PPDU, combines a Start Header, a G.9959 PSDU and an End Header. The G.9959 PSDU is essentially the data that is passed to the PHY layer from the MAC layer or the G.9959 MAC Protocol Data Unit (MPDU), as shown in Figure 3.13. The G.9959 PSDU may vary in size to support the different data rates but not exceed 170 bytes, which is the maximum size specified for the highest data rate of 100kbps. The general format of the G.9959 MPDU consists of a MAC Header, a MSDU and a MAC Footer. However, a number of variations of the MPDU format have been defined by the G.9959 recommendation. The structure of a frame that is received by the G.9959 PHY, therefore, will vary depending on the format of the MPDU (ITU-T, 2015).

Figure 3.13

Schematic View of G.9959 PPDU



Note. From *"Recommendation ITU-T G.9959,"* by ITU-T, 2015. In the public domain.

The G.9959 MAC, which ensures the robustness of transmission through mechanisms such as frame acknowledgement and retransmission, may pass a singlecast MPDU, a multicast MPDU or an acknowledgement MPDU to the PHY layer as a PSDU. The 3 possible MPDUs shall use one of two formats defined for each MPDU. The specific format that is applicable depends on the operating channel configuration. The format that is applicable for the one channel configuration is also the format applicable for the two channel configuration. Amongst the 3 MPDUs, singlecast MPDUs and the

acknowledgement MPDUs will have a similar format. The G.9959 recommendation specifies a zero-byte length MAC data payload for acknowledgement MPDUs, which enables the confirmation of successful reception and validation of an MPDU upon request for frame acknowledgement (ITU-T, 2015).

Singlecast MPDUs and acknowledgement MPDUs formats will both include 3 identifier fields, namely, HomeID, Source Node ID and Destination Node ID. In contrast, multicast MPDUs format will only include 2 identifier fields, namely, HomeID and Source Node ID. The Destination Node ID field is replaced by a dedicated "multicast addressing bitmask" with which the multicast header identifies the different destination nodes. In addition to singlecast, multicast and acknowledge frames, a G.9959 MAC entity receives two other frame types for forwarding to higher entities, namely, routed frames and beam frames. The MPDU format of a beam frame has a beam tag field, replacing the HomeID field that is specified for the general MPDU format, which distinguishes a beam frame (ITU-T, 2015).

3.5.2.4 Peer MAC entities, Topologies and Channel Access

Like IEEE 802.15.4 radio technology, the ITU-T G.9959 radio technology supports both star and peer-to-peer operations. The key features of G.9959 technology include channel access, frame validation and a distinct MAC layer interface that exchanges MPDUs with the MAC layer instead of MSDUs as per the OSI reference stack. Further, G.9959 technology allows two modes of operation for compliant radios, always listening (AL) or frequently listening (FL). A G.9959 node may also alternate between the two specified modes of operation. In AL mode, the receiver of a G.9959 node stays on for the entire period of operation. In FL mode, however, the receiver of a G.9959 switches between on and off states at regular intervals. Though the FL mode

offers significant energy savings, this mode suffers from increased transmission latency due to its lower receiver duty cycle (ITU-T, 2015).

The FL mode of operation is specified for battery-powered nodes that are required to be reachable at any time. Battery-powered nodes that spend most of their operational life in sleep mode and wake up to poll other nodes for pending messages, however, are to use the AL mode to receive frames. Battery-powered devices that use the FL mode for a more responsive behaviour wake up to detect a beam from the incoming messages. Consecutively transmitted beam frames enable battery-powered devices to detect a beam within a short span of time before either staying awake or returning to sleep immediately, which depends on the HomeID hash value. The back-to-back transmission of beam frames, however, varies depending on the beam type. The G.9959 recommendation specifies two beam types, namely, the fragmented beam and the continuous beam (ITU-T, 2015).

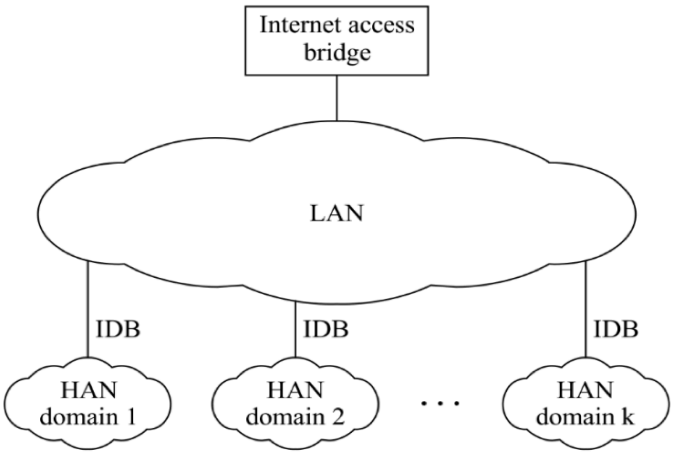
The format of a fragmented beam comprises beam fragments, each comprising several beam frames. The duration of each beam fragment will be in the range of 110-115ms. The G.9959 recommendation has also specified that every beam fragment following a beam fragment must start 190-200ms from the start of the previous fragment. A continuous beam, in contrast, is a series of beam frames, where a long continuous beam lasts for a maximum of 1160ms and a short continuous beam lasts for a maximum of 300ms. The G.9959 recommendation also specifies that a compliant network requires two different types of nodes, namely, a Domain Master and an Endpoint node. The different nodes allow a G.9959 network to be divided into logical domains, where two or more physical nodes communicate over the same medium. Every G.9959 domain requires a Domain Master, which is a node with

extended management capabilities, to handle the operations of that domain. The domain master also provides for the registration and maintenance of the registered nodes. Including the domain master, however, a domain may connect up to 232 nodes (ITU-T, 2015).

Whilst a node belongs to only one domain, all the nodes are allocated an 8-bit NodeID identifier that is unique by the domain master during node registration. Communications between the nodes of a domain using the NodeIDs are enabled by a unique 32-bit HomeID identifier, which also limits the number of possible domains. The nodes of different domains interconnected by a Local Area Network (LAN) infrastructure may also communicate. Although the nodes of a domain may receive the transmissions from nodes of overlapping domains, the communication between the nodes of overlapping domains requires inter-domain bridges or IDBs. A generic LAN interconnected G.9959 network, which comprises multiple Home Area Network (HAN) domains, is shown in Figure 3.14. Each domain represents a set of G.9959 devices (ITU-T, 2015).

Figure 3.14

Generic G.9959 Network Architecture

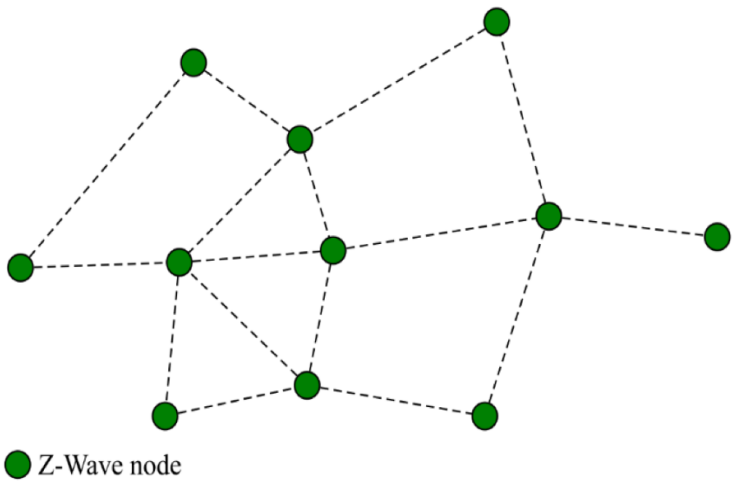


Note. From *"Recommendation ITU-T G.9959,"* by ITU-T, 2015. In the public domain.

Like IEEE 802.15.4 technology, ITU-T G.9959 technology is also suited for WSN applications. The technology allows any two devices within range to send and receive messages, enabling the routing of messages from any device to any other device on the network through multiple hops. Although the network layer specification is not defined as part of the standard, the specifications cite Z-Wave routing protocol for a model of the higher layer and to explain the complex network formations that G.9959 technology is suited for. Depending on the higher layer, therefore, G.9959 technology allows compliant devices to operate in a mesh network topology which is useful to applications that require a redundant and more reliable network. A G.9959 mesh network, which implements Z-Wave routing protocol, is illustrated in Figure 3.15 (ITU-T, 2015).

Figure 3.15

G.9959 Mesh Topology Network



Note. From *"Recommendation ITU-T G.9959,"* by ITU-T, 2015. In the public domain.

The ITU-T G.9959 radio technology relies on CSMA-CA technique for channel access control. The MAC layer requests the PHY layer for channel status to avoid RF collisions before transmitting and retransmitting. If the channel is busy for a pre-

defined period, the MAC layer indicates to the network layer that the transmission has failed. When the validation of a transmission is required, failure to receive an acknowledgement MPDU will also indicate that the transmission attempt failed. However, the originator node will attempt to retransmit the frame and wait for an acknowledgement MPDU up to a pre-defined number of times. The node waits before retransmitting for a duration that is calculated from within a specified range. The random delay, also known as the random backoff period, prevents the G.9959 nodes retransmitting at the same time (ITU-T, 2015).

3.6 Conclusion

The IEEE 802.15.4 and the ITU-T G.9959 have underpinned the development and improvement of several mesh networking technologies, such as Zigbee and Z-Wave. Both the IEEE 802.15.4 and the ITU-T G.9959 have been suited for implementation of Sensor Networks in small geographical areas. As the efforts to realise a “smart environment” converged WSNs, distributed computing and the Internet, the more scalable mesh networking technologies enabled Internet-based applications that involve a growing number of inexpensive devices. The rapid surge of inexpensive devices in recent years leads to the conclusion that more Internet-based applications are utilising the new and improved Sensor Network radio technologies, replacing Wi-Fi and Bluetooth. The diverse range of mesh networking technologies that already exist presents an opportunity to reconstruct Sensor Networks from real-time communications. As investigators may not be able to use any fixed hardware, however, a simple framework requiring minimal hardware that may be quickly deployed is required. Other challenges for reconstruction of Sensor Networks, such as the opportunities for portable devices to move around, also have to be considered for system design in order to develop an effective forensic reconstruction framework.

Chapter 4

RESEARCH DESIGN

4.1 Introduction

The approach of modelling and reconstruction of an IoT devices' network by capturing real-time communications between IoT devices, which suitably enables identification of every IoT device that forms an IoT environment, has not been explored to sufficiently advance the field of digital forensics for IoT device identification. This chapter presents the design of the system that leverages the diversity in IoT communication technologies for modelling an IoT device environment. The challenges for monitoring and modelling an IoT device environment are discussed and a model of the system with capabilities that are desirable is defined. In this chapter, the criteria for evaluation of the envisaged system are also identified and explained. Furthermore, the research methods and data collection phases are described.

4.2 Research Problem

Problem clarification narrowed the gap in research to the lack of knowledge for harnessing the wireless communications between Things of an IoT environment to ascertain the number and locations of active Internet-enabled Things ahead of a field search activity by investigators to identify Things.

The following question is formulated to identify the central research problem and indicates the direction of inquiry of this study –

What is an effective forensic reconstruction framework to ascertain the number and locations of Internet-enabled Things by harnessing the wireless

communications between Things ahead of searching an evidential scene for Things?

Decomposition of this question distinguished the different areas of significance to the central problem and defined the goals of this study. The following logically ordered sub-questions represent the design of the system of knowledge for which this study is undertaken–

1) ***How can the wireless communications of a heterogeneous IoT environment be observed to enable the accurate modelling of Things?***
2) ***How can the wireless communications of a heterogeneous IoT environment be analysed to map the logical topologies of Things?***
3) ***How can the wireless communications of a heterogeneous IoT environment be utilised to determine the locations of Things?***

4.3 IoT Monitoring and Modelling System – A Model

A system for IoT monitoring requires several capabilities to enable forensic identification of Things by forensic investigators and LEAs. An effective monitoring system must have the capability to discover, determine and locate potentially numerous and a large variety of IoT devices in the shortest possible time. To be applicable in diverse, highly dynamic, and complex settings, however, it is also crucial that the system for IoT monitoring is relatively straightforward to implement and is suited for prolonged periods of monitoring. Several challenges are considered to develop a model of the IoT monitoring system that is effective for digital forensic investigations and law enforcement purposes. The model constructed has also considered potential risks for monitoring an IoT environment with the goal of ascertaining the low-energy wireless sensing deployments prior to the entry to a

scene. Each of the three core capabilities that are required for a system of IoT monitoring is explained below.

4.3.1 Key Capabilities

4.3.1.1 Discover IoT Technologies

One of the main challenges considered for the design of the system for monitoring IoT devices is that a target environment is likely to operate multiple, heterogeneous IoT platforms. A target environment is, therefore, likely to operate heterogenous IoT communication technologies, which are built on the low-power, reliable and Internet-enabled communications stacks developed by the IEEE and the IETF to standardise low-rate, short-range communications (Granjal, Monteiro, & Silva, 2015). The other challenge considered for the design is that the locations neighbouring a target are likely to utilise IoT technologies, including technologies similar to those already operating within the target. An effective monitoring solution, hence, must be capable of discovering and identifying the heterogeneous wireless sensor networking technologies that co-exist and operate within a specific location.

The capability to discover the IoT technologies that are operating is also key to determine and deploy resources appropriate for monitoring a location. The capability to discover the IoT technologies operating within a specific target, however, depends on the capability of the system for IoT monitoring to differentiate the IoT networks that operate within a target location from those around a target location. This requires that the system allows for surveying all neighbouring locations around a target prior to surveying a specific target. Following a survey of the neighbouring locations, the system should enable forensic investigators and LEAs to specifically omit the channels and networks that operate outside of the target. This is especially significant

when the communications of IoT devices outside a target are obtainable within the perimeter of the target.

4.3.1.2 Determine IoT Device Number and Type

An effective solution must also provide for determining the number and types of IoT devices within a location. Advancements in short-range radio technologies have enabled low data-rate wireless connectivity with fixed and mobile devices in challenging environments (Bhat, 2011). Additionally, the short-range radio technologies enable IoT devices to operate in one of three possible topologies, including star, mesh or a mesh of clusters, which will vary depending on the different IoT applications for which the two device types are utilised.

The main challenge in designing a system that will allow forensic investigators to determine the number and type of IoT devices present is that the overlapping communications between IoT devices are likely to be obscured. With new and improved IoT communication technologies such as Z-Wave Plus having a focus on security and privacy, network layer packets are increasingly unintelligible for monitoring purposes. Hence, a system for IoT monitoring that is built on network layer data will soon become obsolete and irrelevant in scenarios where more secure IoT technologies are in operation.

A more suitable alternative is for the system to rely on logical topology information which is typically embedded into communications in an intelligible format for the purpose of network management and control. The information embedded, however, varies from one technology to another. As network management and control is not standardised across the different IoT technologies that are available, determining the

number and type of devices requires correlation of the information utilised by a specific technology for network management and control.

4.3.1.3 Locate IoT Devices

In addition to the requirements of discovering IoT technologies and determining the type of IoT devices, it is fundamental for an effective monitoring solution to provide for locating the different devices within a target location. The main challenge for this requirement, however, is the opportunities for portable and mobile devices to be moved around a location or be turned on and off both manually and automatically. The design of the solution, therefore, should be suited for continuous operation and extended monitoring of IoT devices. This will allow forensic investigators and LEAs to locate IoT devices and track any changes to the last known location of a device. A system that allows for tracking the latest location of IoT devices will enable investigators to search and account for all the IoT devices at the scene.

The other challenge for this requirement is that there may be unknown interferences within an environment that cause attenuation of radio signals. There may also be interferences in neighbouring locations that affect the strength of radio signals. This requires that a system for monitoring IoT devices allows for estimating the interferences in and around a target environment. However, accounting for all the known and unknown interferences that affect radio signals is not practical for forensic investigators and LEAs. This requires forensic investigators to undertake extensive survey and assessment of the interferences, including those that exist within an environment. Also, surveying a target carries some risk of inadvertently tampering with a scene.

A more suitable alternative for the system to provide for locating IoT devices is to rely on relative data generated about a specific device. This requires the system to allow for simultaneous monitoring from multiple locations. The locations for simultaneous monitoring should be, wherever possible, such that there are overlaps in monitored areas. The system should further allow for the relative data generated for devices within a specific target to be combined and processed. Depending on the number of locations from where a device is monitored, a method of trilateration or multilateration may be applied. The relative information from multiple monitoring locations, whenever this is available, is useful to improve the accuracy of device location provided by the system.

4.3.2 Ancillary Design Considerations

It is desirable that the system provides for determining and locating as many IoT devices within the least possible time. Such a system minimises the delay to enter and search a scene for IoT devices. It is further desirable that a system for IoT monitoring provides for discovering and determining the devices from the peripheries of an IoT environment. This is because monitoring from a reasonable distance to the target may not be possible. Furthermore, it is desirable that the system is not built on any fixed hardware but instead utilises hardware and software which can be carried and deployed quickly by LEAs when required. This will allow LEAs to monitor a target from select positions, depending on the constraints of a location, without relying on permanent surveillance infrastructure or ad-hoc installation of monitoring hardware, both of which may not be possible.

4.3.3 Key Features of the Model

A model of the system for IoT monitoring is constructed for the different possible scenarios and challenges that forensic investigators and LEAs are likely to encounter prior to entry to a scene. The design of the system has a focus on modelling low-rate, short-range wireless sensing deployments and tracking the IoT device locations from radio signals. The design of the system is, therefore, suited for monitoring and tracking both fixed and mobile IoT devices regardless of the topology formed. The design is also suited for monitoring and tracking of IoT devices regardless of the topology formed by the heterogeneous devices of a target environment.

The design of the system is structured to enable investigators to systematically proceed to map an internal IoT devices' network before securing a target wireless digital scene. In all, there are three distinct stages that allow a step-by-step reconstruction of the wireless sensing deployments. The design has also allowed for additional information pertaining to a target, such as wall types and floor layout, to be incorporated by LEAs. Contextual information, which is typically maintained by relevant authorities, is useful to improve the accuracy of the locations. Where such information is not available, investigators may proceed to estimate the location of devices, albeit with less accuracy.

Whilst a 3-stage model for IoT monitoring is lightweight, the design of the system is suited for continuous operation. With a design that does not require LEAs to install specialised equipment within a premise like other solutions developed for the identification of IoT devices, the model of the IoT monitoring system has allowed for adjustments required to adapt to the challenges on the ground. With a design that is mostly built on low-cost hardware and software, both of which are widely available,

implementing the solution does not depend on sophisticated new hardware and software. The design is also suited to enable LEAs to target a specific location without risking detection by an adversary.

With a design that does not require any pre-requisite infrastructure to be available on-premises for monitoring a target environment, the system has allowed for forensic investigators and LEAs to have sufficient control to make ad-hoc changes to deployment when needed. The structure of the system allows for a “blinded” approach, which may be necessary following an operational threat assessment by LEAs. A limited operation of the framework, whereby LEAs may quickly gather information and locate the IoT devices of an internal network, involves passing over the second stage of the system without fully processing the information that is collected to proceed to the third step of the process.

Additionally, the structure of the system allows for an early termination of the 3-stage reconstruction process. Within the 3-stage model of the system is an ultra-lightweight system involving 2 out of the 3 stages. The 2-stage system presents forensic investigators and LEAs with a basic option that may be implemented for surveying and mapping a target IoT environment. If the objective of monitoring an environment is not to locate the IoT devices but to estimate the number of devices within a premise as quickly as possible, then the full option need not be implemented. Completing stages 1 and 2 will be sufficient to generate a map of the internal IoT devices’ network. Furthermore, the basic option also allows for monitoring a target from multiple locations simultaneously without having to select locations having overlaps between the monitored areas.

4.3.4 Locate and Track IoT Devices

The three stages combined to locate and track IoT devices from their wireless communications are explained below.

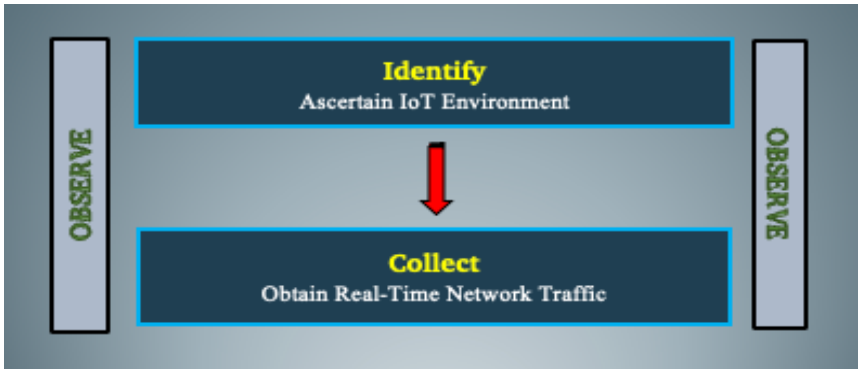
4.3.4.1 Initiation Stage - Observing IoT Device Communications

From an overall design point of view, the first stage of the modelling process provides for sensing and obtaining the IoT device communications from locations bordering a target environment. This stage involves a method to ascertain an IoT environment at a wireless digital scene and to identify the low-rate, short-range wireless technologies in operation. The method, involving a selection of hardware and software identified as suitable to sense traffic on radio channels, provides the basis for proceeding through to modelling of low-energy sensor platforms. The detection step also identifies the different radio frequencies that are occupied by IoT devices and the channels that are available for new networks to operate. The output of this method provides greater clarity of the details required for the next step of the reconstruction process.

Figure 4.1 shows the two sub-processes that this stage of the modelling process combines.

Figure 4.1

Stage 1 of Locating and Tracking IoT Devices



The structure of this sub-system also includes a method for obtaining real-time network traffic from a heterogeneous IoT environment composed of multiple low-energy sensor platforms to generate the data required for accurate modelling. Communications of the heterogeneous IoT devices at a location are to be collected by resources identified as suitable for the purpose of capturing the disparate traffic from the peripheries of a location. The method provides for determining the deployment strategy that is unique for the constraints of different locations. The deployment strategy identifies the number of radio modules required to capture the traffic simultaneously from locations surrounding a target. The communications captured at this step provides for the data required to examine the messages of the wireless sensing platforms.

4.3.4.2 Intermediate Stage - Analysing IoT Device Communications

This second sub-system involves two separate methods that determines the data paths of IoT device networks. This step of the sensor platforms modelling process involves a method of extraction that examines the traffic captured through the previous step specifically for the network management and control data. The method generates the real-time logical network data required for a targeted analysis of the IoT device connections. The method involves selective processing of communications through the deconstruction of traffic that is obtainable from heterogeneous sensor platforms. The data that has been extracted from the communications is further processed through the next step of the reconstruction process.

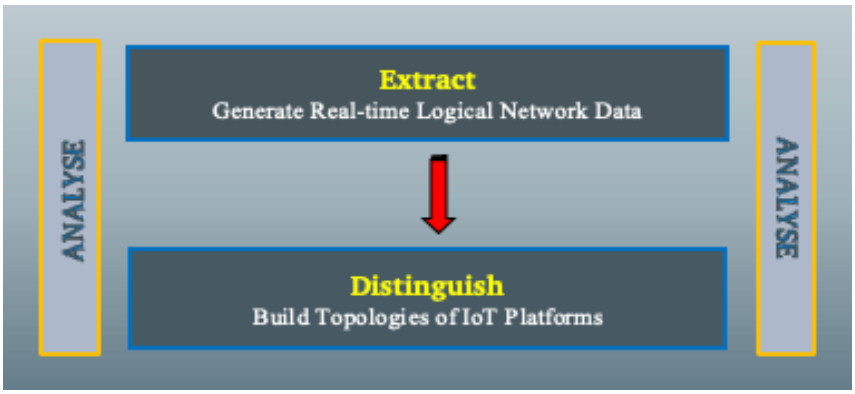
The second step of the analysis stage builds the logical topologies formed by the nodes of heterogeneous low-energy wireless sensing platforms. This involves a method of distinguishing the unique datalinks that generate the traffic obtainable from

a target location. The method focuses on the information that devices of a target network utilise for communicating with other devices that is part of the same network. This includes features that are unique to a network such as the addressing schemes and network identification information that helps different deployments to also share the frequency with other similar networks. The method also identifies the different information required to describe a target network from real-time network management and control data that is embedded in the low-rate traffic.

Figure 4.2 shows the two sub-processes that this stage of the modelling process combines.

Figure 4.2

Stage 2 of Locating and Tracking IoT Devices



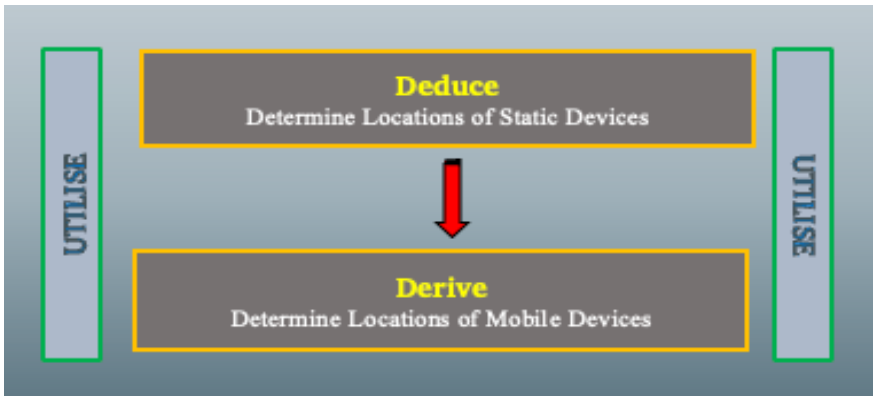
4.3.4.3 Final Stage - Utilising IoT Device Communications

This stage of the modelling process further utilises the low-rate, short-range radio signals to determine the locations of the various nodes connected by heterogeneous low-energy wireless sensing platforms. This initially involves a method of deduction that utilises the locations of the monitoring nodes deployed according to the constraints of a specific location. The locations of the radio modules deployed for monitoring the communications originating from the static sources are examined to determine the location of each static device, relative to monitoring nodes.

The output of the previous step provides an arrangement of the different static sources that are observed by each monitoring node. Merging the projections generate an arrangement of the different static sources relative to multiple monitoring nodes, wherever this is available. This stage of the modelling process also combines two sub-processes as shown in Figure 4.3. The final step of the modelling process derives the locations of the mobile devices relative to the static devices connected by a low-energy wireless sensing platform. The method involves examining the different datalinks that are formed between the nodes.

Figure 4.3

Stage 3 of Locating and Tracking IoT Devices



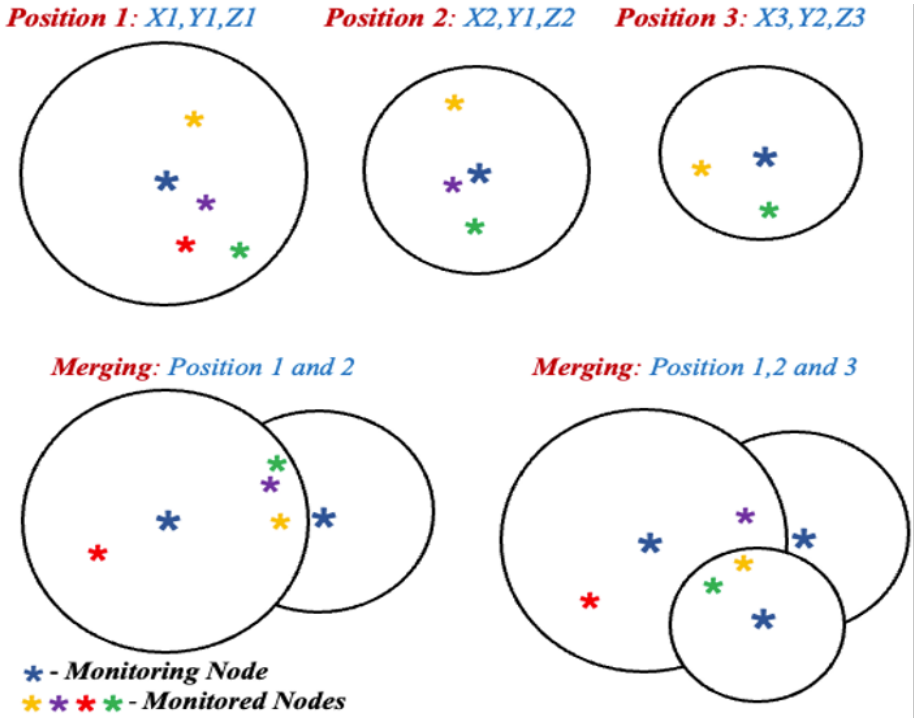
The derivation method initially identifies the destinations of signals captured from static sources, the locations of which were initially deduced. The locations of the radio modules that were deployed for monitoring the communications from the mobile devices are thereafter examined to determine locations of the mobile devices relative to each monitoring node. That generates an arrangement of the mobile devices that are observed by each monitoring node. Merging the projections generate an arrangement of the mobile devices relative to multiple monitoring nodes, wherever this is available.

Next, the monitorable range of the static sources is incorporated to derive the locations of the mobile destination nodes relative to static source nodes. Where there is more than one static device, the location of a mobile device relative to every static device is derived separately before being merged. This further improves the location accuracy of located mobile devices through a projection of the mobile devices that is relative to static devices.

Figure 4.4 illustrates the reconstruction of an internal IoT devices' network at this 3rd stage of the modelling process.

Figure 4.4

Reconstruction of Internal IoT Devices' Network



For illustration purposes, a total of 3 monitoring nodes are shown to have detected several nodes within a target from 3 different positions around it. The relative positions of the 3 monitoring nodes in a 3-dimensional (3-D) space are identified through cartesian coordinates, where X, Y and Z correspond to one of the three axes

that are pair-wise perpendicular and share a common originating point. Whilst X and Y axes are horizontally oriented, the Z-axis is vertically oriented. The variations that are applied to the positions of the monitored nodes show how the different projections generated using data from 3 different monitoring nodes enable the mapping of wireless sensing deployments for a given point in time.

4.3.5 Assessment Criteria

The effectiveness of the model that is explained in section 4.3.4 depends on the effectiveness of each of the three stages of the model. To validate the model, therefore, each of the three different stages must be validated separately. This necessitates the assessment of three different aspects of IoT devices, each of which corresponds to one of the three stages of the model for monitoring IoT devices. The three aspects which have been identified as the core criteria to evaluate the model are monitorability, traceability and discoverability of IoT devices. Each of the three criteria that is being referred to here is explained below.

4.3.5.1 Monitorability of IoT devices

This criterion of assessment corresponds to the last stage of the modelling process which is mainly concerned with determining the locations of static and mobile IoT devices operating within a target. The criterion refers to the monitorability aspect of the low-rate, short-range radios that are utilised by IoT devices of low-energy wireless sensing platforms. To be able to assess the model for IoT monitoring based on the monitorability aspect of IoT devices, the possibility of monitoring both fixed and mobile IoT devices from locations outside and away from the indoor environments that the devices operate must be investigated. That requires empirical tests combining a range of IoT devices with a variety of wall types. A study into the monitorability of IoT devices also uncovers the main factors that affect the monitorability of IoT

devices. Understanding the extent to which the different factors influence the monitorability of IoT devices is required to construct a guide that is useful to forensic investigators and law enforcement agencies.

4.3.5.2 Traceability of IoT devices

This criterion of assessment corresponds to the intermediate stage of the modelling process which is mainly concerned with building the topology based on datalinks that are formed between IoT devices. The criterion refers to the traceability aspect of the low-rate, short-range radio signals to datalinks of a wireless sensing platform. To be able to assess the model for IoT monitoring based on the traceability aspect of IoT devices, the commonalities and differences in network management and control communications of IoT devices must be explored. That requires empirical tests combining a range of IoT devices which connect and communicate using different short-range communication technologies. A study into the traceability of IoT devices also uncovers the factors that affect the traceability of communications to datalinks. Understanding of the different factors that affect the traceability of IoT devices is required to construct a guide that is suitable to both forensic investigators and law enforcement agencies.

4.3.5.3 Discoverability of IoT devices

This criterion corresponds to the initialisation stage of the modelling process which is mainly concerned with collecting wireless communications between the IoT devices operating within a specific location. The criterion refers to the discoverability aspect of IoT devices from the short-range radio signals that are obtainable from the external peripheries of low-rate, short-range wireless communication environments. To be able to assess the model of the IoT monitoring system based on the discoverability aspect

of IoT devices, the possibility of discovering IoT devices before the nodes of an indoor IoT environment are all monitorable must be explored. That requires empirical experiments involving large-scale deployment of IoT nodes in a variety of indoor physical environments. Simulations experiments, relatively, are more suited to generate data from scenarios that involve many IoT devices. A study into the discoverability aspect also uncovers the different factors that affect the chances of discovering IoT devices from the peripheries of an IoT environment.

4.4 Implementation Plan

4.4.1 Research Methods

To evaluate the model of the system explained in section 4.3.4, this study generates the data required through simulation and empirical approaches. Simulation experiments require an IoT simulator to run tests and collect data from both star and mesh networks. As most of the simulators available for IoT research implement either IEEE 802.15.4 or LoRaWAN (Chernyshev, Baig, Bello, & Zeadally, 2018), simulation experiments utilise a new purpose-built IoT simulator suited for the mobility and scalability needs of this study. The MATLAB-based IoT simulator utilises new and improved MATLAB libraries to generate 3-D simulations. To configure the purpose-built IoT simulator to run 3-D simulation experiments that mimic real-world scenarios, empirical experiments to study IoT monitorability precede the simulation experiments. Findings of the study into IoT monitorability inform the study into IoT discoverability. A combination of both sensor and actuator devices that are widely available in the market provides for collecting data iteratively through both empirical and simulation approaches.

4.4.2 Data Collection

This study generates the required data over three phases. The focus of each phase is briefly described below.

a) Phase 1. The principal objective of the initial phase of data collection is to obtain the data required to study the monitorability of IoT devices from the communications that are obtainable from within IoT environments. This phase, therefore, combines a selection of widely available IoT devices with a selection of wall types widely used for the construction of indoor environments. To obtain the target data, the selected IoT devices are monitored from a range of distances to every wall type selected. To monitor and capture packets, this phase utilises suitable hardware and software. The packets captured are interpreted and filtered to determine the change in rate of periodic communications as the monitoring distance increases. The data obtained from the selected IoT devices form the basis of the study into the monitorability of IoT device communications.

b) Phase 2. The next phase of data collection obtains data required to study the traceability of IoT devices from the communications that are obtainable from within IoT environments. This phase, therefore, involves a selection of widely available IoT devices. To obtain the target data, network packets of the selected IoT devices are monitored and captured utilising suitable hardware and software. This is followed by the interpretation of the packets captured. Next, the interpreted network packets are inspected to ascertain the frame types employed by the IoT devices for communications with peer MAC entities. The data related to the frame types employed by the selected IoT devices form the basis of the study into the traceability of IoT device communications.

c) Phase 3. The final phase focuses on the data required to study the discoverability of IoT devices from the communications that are obtainable from within IoT environments. As the mesh networking solutions enable both star and mesh network topologies, this phase involves simulations of both star and mesh networks. To ensure that simulations generated mimic real-world scenarios, the number of devices and the distances between devices that form datalinks are randomised. Further, the findings of the study into monitorability and traceability of IoT devices are also incorporated. To obtain target data, the effect of changes to monitoring distance on the configuration of devices that may be discovered is observed. The data obtained for different monitoring distances, related to the percentage of devices that may be discovered, form the basis of the study into the discoverability of IoT device communications.

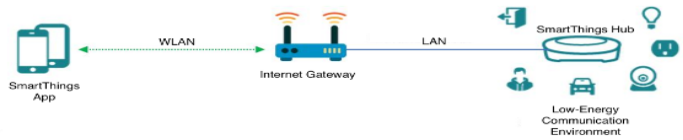
4.4.3 Testbed

The empirical phases require a testbed that consists of several IoT devices, stand-alone radios and a variety of wall types. Each of the different components required for a fit-for-purpose testbed was determined through the setup of a staging environment and a pilot study of IoT monitorability. The pilot study involved several sensing devices that are compatible to work with the widely available SmartThings platform developed by Samsung. The SmartThings platform, which supports IoT applications involving a growing number of low-energy sensing devices, connects compatible IoT devices to a hub that supports two mesh networking communication technologies. The SmartThings platform also supports automated setup and control of compatible devices through a proprietary mobile application. A staging network for the pilot study was formed using widely available Zigbee certified wireless sensing devices and a SmartThings hub, which also acted as the gateway for the local sensor network

to access the Internet. The hub connected to the Internet over LAN, which isolated the hub from the WLAN that shared a common Internet gateway as shown in Figure 4.5.

Figure 4.5

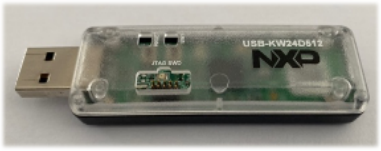
Staging Network with SmartThings Devices



The Zigbee certified devices selected and used for the pilot study consisted of a device with motion sensor and a device with door open/close and vibration sensors. As the staging network of Zigbee devices operated, the communications between devices were observed with a stand-alone radio module suited for sensing and obtaining IEEE 802.15.4 radio transmissions. From amongst the available stand-alone radio modules, a Kinetis USB-KW24D512 development board, shown in Figure 4.6, was set up to perform as an outdoor, mobile monitoring node. This model featured the KW2xD Wireless Microcontroller with integrated IEEE 802.15.4 radio that operates at 2.4 GHz and -102 dBM receiver sensitivity.

Figure 4.6

Kinetis USB-KW24D512



In comparison to other solutions from Texas Instruments and Nordic, the NXP Kinetis module together with the Kinetis Protocol Analyser Adapter having PCAP support in Wireshark enables quicker filtering and analysis of captured packets. Wireshark network packet analyser enabled examination of the packets captured from the different monitoring locations by the Kinetis USB. An Intel Compute Stick powered

by Cygnett Power Bank, as shown in Figure 4.7, enabled the use of the Kinetis module as an outdoor, mobile monitoring node.

Figure 4.7

Kinetis USB-KW24D512 as Outdoor, Mobile Monitoring Node

To obtain data required for a pilot study of IoT monitorability, communications of the Zigbee devices that formed the staging network were monitored from several locations away from the wall. Initially, the communications were monitored and captured from an external location that is 3m away from wall. The distance of monitoring location to wall iteratively increased every 2mins by 5m until communications from the devices were no longer obtainable. Communications of the devices were observed from across a selection of wall types, including brick exterior, internal dry wall or GIB board, Garage door, Single-pane Window, Double-Glazed Window and Obscure Glass Window.

A preliminary examination of periodic communications was carried out by filtering and auditing the captured packets using Wireshark to determine the percentage loss in periodic communications as the monitoring node moved away from monitored nodes. Following the analysis of communications between Zigbee devices, results of which

are covered in Section 5.3.1, a Vera Edge hub to interconnect Z-Wave compliant devices was setup alongside the SmartThings hub. Like SmartThings, Vera is a widely available platform, which allows configuration and control of compliant IoT devices through a mobile application. Following the setup; from amongst the stand-alone Z-Wave radio modules that were tested, Silicon Labs Z-Wave UZB was found to have support for sensing, capture and interpretation of communications between Z-Wave devices. Figure 4.8 shows the Z-Wave UZB that was identified as suitable for the requirements of this study.

Figure 4.8

Z-Wave UZB

The pilot study, which was based on several Zigbee devices, identified that several more devices are required for a robust study into IoT monitorability. The staging network, which utilised two IoT platforms, identified that several more devices and multiple IoT platforms with support for IEEE 802.15.4 and ITU-T G.9959 radio technology are required to obtain communications required for a robust study into IoT traceability. Additional IoT platforms and devices required for the testbed were accordingly selected. The pilot study, which involved a selection of wall types, also identified the different wall types required for a robust study into the monitorability of IoT devices. Furthermore, the pilot study and staging setup found and repurposed stand-alone radio modules, with a USB dongle form factor and support for a network packet analyser, suitable for the empirical phases.

Table 4.1 lists the IoT device models that formed the staging network and enabled the identification of different hardware and software components required for the testbed.

Table 4.1

Staging Network Devices

IoT Device Model Name	Technology	Device Power Source	Application
Samsung SmartThings Hub	Zigbee, Z-Wave	Mains	WSN Gateway
Vera Edge Smart Home Controller	Z-Wave	Mains	WSN Gateway
Aeotec Multipurpose Sensor	Zigbee	Battery	Sensor Node
SmartThings Motion Sensor	Zigbee	Battery	Sensor Node
Aeotec Switch (Non-USB)	Z-Wave	Mains	Actuator Node
Aeotec Multi-Sensor	Z-Wave	Battery	Sensor Node

4.4.4 Data Analysis

A robust analysis of the data collected through empirical and simulation approaches is required for the assessment of monitorability, traceability and discoverability characteristics of low-rate, short-range IoT device communications. Initially, the analysis phase examines the data collected through the first phase of data collection, which is described in section 4.4.2. The objective is to find the emerging patterns in relation to the monitorability of IoT devices. Analysis, therefore, has a focus on the percentage loss in periodic communications of IoT devices as the distance of monitoring location to wall increased. Further, the results of the analysis of IoT monitorability form the basis of the answers to following questions.

1) *What is the monitorable range of mains-powered IoT devices with integrated low-rate, short-range radio?*

2) *What is the monitorable range of battery-powered IoT devices with integrated low-rate, short-range radio?*

The next stage examines the data related to frame types obtained through the second phase of data collection, which is described in section 4.4.2. The various frame types employed by IoT devices for communications with peer MAC entities are consolidated and analysed to identify the commonalities and differences in structured network management and control communications. The results of the analysis of IoT traceability form the basis of answers to the following questions.

1) *What percentage of the 802.15.4 frame types employed for communications with peer MAC entities does the mains-powered, static IoT devices account for?*
2) *What percentage of the 802.15.4 frame types employed for communications with peer MAC entities does the battery-powered, mobile IoT devices account for?*
3) *What percentage of the 802.15.4 frame types employed for communications with peer MAC entities does the mains-powered, static IoT devices and the battery-powered, mobile IoT devices commonly account for?*
4) *What percentage of the G.9959 frame types employed for communications with peer MAC entities does the mains-powered, static IoT devices account for?*
5) *What percentage of the G.9959 frame types employed for communications with peer MAC entities does the battery-powered, mobile IoT devices account for?*
6) *What percentage of the G.9959 frame types employed for communications with peer MAC entities does the mains-powered, static IoT devices and the battery-powered, mobile IoT devices commonly account for?*

The final stage of the analysis phase examines the data collected through the third phase of data collection, which is described in section 4.4.2. Initially, the monitoring

distances from which every IoT device may be discovered across star and mesh networks are identified. Thereafter, analysis has a focus on the configuration of IoT devices that may be monitored across the monitoring distances from which every IoT device may be discovered. The results of the analysis of IoT discoverability form the basis of answers to the following questions.

1) *What is the smallest configuration of IoT devices that enables 100% discovery of IoT devices in star configuration?*
2) *What is the smallest configuration of IoT devices that enables 100% discovery of IoT devices in mesh configuration?*
3) *What is the farthest radius limit of indoor environments from where the smallest configuration of IoT devices that enables 100% discovery may be monitored?*
4) *What is the nearest radius limit of indoor environments from where the smallest configuration of IoT devices that enables 100% discovery may be monitored?*

4.4.5 Solution Definition

The findings of the monitorability, traceability and discoverability assessments are utilised for an assessment of the model of the system explained in section 4.3.4. The objective is to validate the concept of harnessing IoT device communications for forensic purposes based on the following hypotheses.

H1: The forensic investigator can observe and analyse the wireless communications between IoT devices ahead of searching an evidential scene to definitively determine the number and types of IoT devices that operate at the scene.

H2: The forensic investigator can utilise the wireless communications between IoT devices that are observed ahead of searching an evidential scene to accurately locate the different types of IoT devices that operate at the scene.

The step that follows utilises the results obtained through simulation and empirical experiments to define the methods applicable to monitor radio signals of IoT devices as well as accurately log and locate IoT devices within a location. The following additional questions, formulated based on the model of the system, guide the development of specific methods useful to forensic investigators encountering an IoT rich digital scene.

1) *What is a framework for forensic investigators and law enforcement agencies to –*
    a. *Distinguish the low-rate, short-range IoT technologies that operate within a specific physical environment from the peripheries of the target?*
    b. *Determine the operating channels of the low-rate, short-range IoT technologies within a target physical environment?*
    c. *Capture low-rate communications of IoT devices to generate data required for an accurate modelling?*
2) *What is a framework for forensic investigators and law enforcement agencies to –*
    a. *Extract the network management and control data from the low-rate communications between peer MAC entities?*
    b. *Determine the type and power-source of a device with extracted network management and control data?*
    c. *Map the logical topologies of wireless sensing platforms connecting IoT devices?*
3) *What is a framework for forensic investigators and law enforcement agencies to –*
    a. *Determine the locations of the static IoT devices within a physical environment?*
    b. *Determine the locations of the mobile IoT devices within a physical environment?*

Combining the methods applicable, the final step defines the framework for harnessing IoT device communications to ascertain the IoT specific deployments of a target. The framework constructed, complete with the main processes, supporting processes, specific procedures and the tools required for a range of scenarios, forms the recommended solution for the research problem covered in section 4.2.

4.5 Conclusion

Whilst the diversity in communication technologies created the opportunity to generate valuable insights from the radio signals of a physical environment, analysis of the challenges for harnessing the communications between Things led to the conclusion that an effective solution requires a system that discovers, determines and locates Things. A model of the envisaged system, hence, combines the processes of collecting communications between Things, building logical topologies and determining the location of every active Thing. The underlying principles of the design of the system are three discrete aspects of the communications between Things, namely, monitorability, traceability and discoverability. Simulation and empirical experiments, hence, inform the development of methods to monitor the communications between Things as well as accurately log and locate Things within a location.

Chapter 5

IoT MONITORABILITY FINDINGS

5.1 Introduction

In this chapter, the data generated to study the monitorability of IoT devices is reviewed and discussed. The results and findings of the study into IoT monitorability are presented following a review of the data generated. To generate data suitable for the study into IoT monitorability, several widely available IoT devices with integrated radio were paired with a range of wall types and observed using stand-alone radio module. The devices were iteratively observed from a range of distances to the selected wall types to capture communications and generate data suitable to understand the factors that influence the monitorability of IoT devices. The data generated was further analysed to understand the monitorable range of IoT devices and the rate of monitorable transmissions.

5.2 Monitorability Study Data

The data required to study the monitorability of IoT devices was generated by observing 8 IoT devices, each of which utilised an integrated radio for wireless communications. The data generated was entirely based on IoT device communications which were transmitted by the 8 selected IoT devices across 7 selected wall materials. A selection of 4 mains-powered and 4 battery-powered devices was used to obtain data from both mains-powered and battery-powered IoT devices. The wall materials selected and paired to obtain data were wall types typically utilised to build indoor environments.

Table 5.1 shows the 7 selected wall types paired with IoT devices to obtain data.

Table 5.1

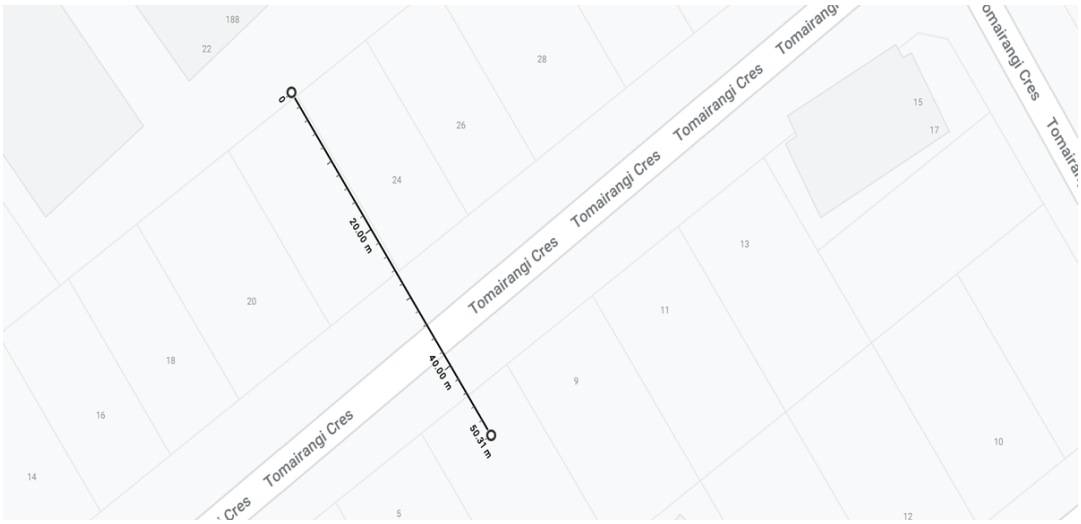
Wall Types Selected

Wall Types
Brick Exterior Cladding
Colorsteel Garage Door
Single-Pane Window
Double-Glazed Window
Obscure Glass Window
Metal Roof
Internal Dry Wall (GIB Board)

To build on the pilot study data generated using few IoT devices, details of which are covered in Section 5.3.1, communications of the larger sample of IoT devices were also observed and captured from locations within 0-10m, within 45-55m to the selected external wall types. All locations suitable to observe and capture communications from were determined using Google Maps that allows to measure paths from a certain location. Figure 5.1 shows the Google Maps view of a selected location that is within 45-55m to a selected wall type.

Figure 5.1

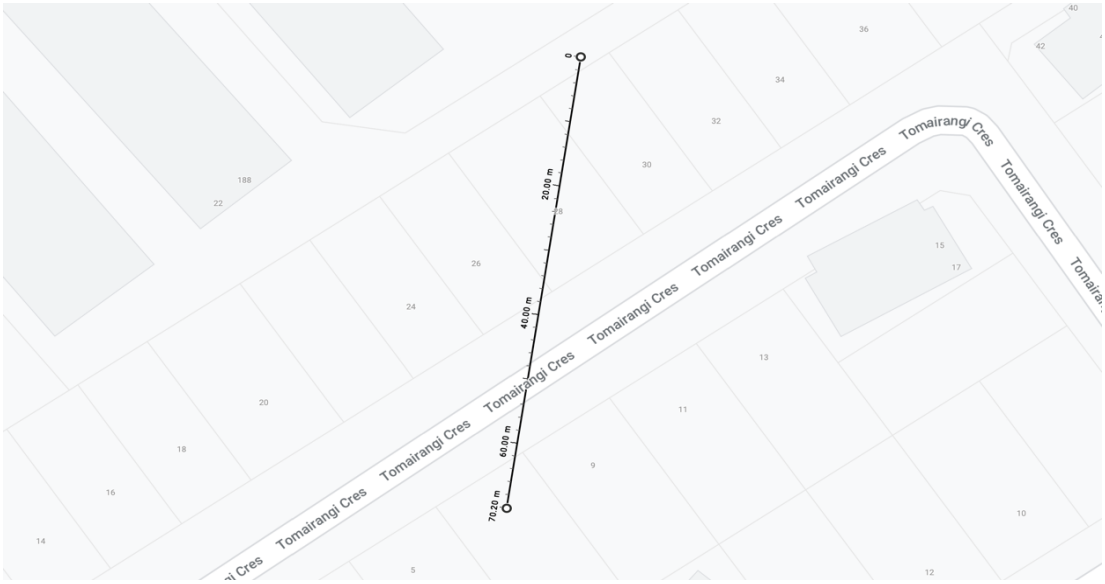
Location within 45-55m to Wall



Additionally, communications of the selected 8 IoT devices were captured from a location that is within 65-75m to the selected external wall types. Figure 5.2 shows the Google Maps view of a location that is within 65-75m to a selected wall type.

Figure 5.2

Location within 65-75m to Wall



Amongst the selected ranges, communications obtained from locations within 0-10m to selected external wall types were utilised to generate baseline data related to monitorable communications. The baseline data generated was utilised to compare the data obtained for locations within 45-55m and 65-75m to external wall. To generate data that supplements the data generated during the pilot study, the communications of each IoT device were captured for 2 consecutive minutes iteratively from different distances to every wall type selected. Next, the captured communications were interpreted using Wireshark packet analyser.

Then, the periodic broadcasts from the mains-powered devices and periodic data requests from the battery-powered devices amongst the communications captured every 40 seconds were audited. An audit of the periodic communications captured

every 40 seconds from 3 different ranges to 7 different wall types generated a dataset of 3 values for each of the 3 distance ranges to the 7 different wall types. The average of every dataset obtained was further computed, which generated data suitable for analysis. The data generated from the communications of 8 IoT devices was catalogued prior to analysis. The data obtained for the 8 IoT devices across 7 wall materials is organised based on the wall type and reviewed below.

5.2.1 Brick Exterior

Data obtained for each of the 8 IoT devices across Brick Exterior cladding showed a decrease in monitorable periodic communications as the distance to wall increased from 0-10m to 65-75m. Data showed the periodic communications from all 8 IoT devices remained monitorable when the distance to wall increased from 0-10m to 45-55m. However, the monitorable periodic communications were fewer across the devices when the distance to wall increased from 0-10m to 45-55m. In contrast, there were no monitorable periodic communications from any of the 8 IoT devices when the distance to wall increased from 0-10m to 65-75m. The data in respect of periodic communications of IoT devices obtained by observing transmissions from across Brick Exterior wall is tabulated in Table 5.2.

Table 5.2

Monitorable Communications across Brick Exterior

Brick Exterior	0-10m	45-55m	65-75m
SmartThings Hub	5	3	0
Philips Hue Hub	5	3	0
Philips Light Bulb - 01	4	2	0
Philips Light Bulb - 02	4	2	0
Aeotec Multipurpose Sensor	6	2	0
SmartThings Motion Sensor	6	2	0
Philips Indoor Motion Sensor	7	2	0
Philips Outdoor Motion Sensor	6	2	0

5.2.2 Internal Dry Wall or GIB Board

Data obtained for each of the 8 IoT devices across Internal Dry Wall showed a decrease in monitorable periodic communications as the distance to wall increased from 0-10m to 65-75m. Whilst the periodic communications from all 8 IoT devices remained monitorable when the distance to wall increased from 0-10m to 45-55m, data showed a decrease in monitorable periodic communications from 5 out of 8 devices. 4 out of the 5 devices that showed a decrease in monitorable periodic communications were sensor devices, all of which were powered by battery. In contrast to the decrease in monitorable periodic communications when the distance increased to 45-55m, there were no monitorable periodic communications from any of the devices when the distance to wall increased from 0-10m to 65-75m.

Table 5.3 presents the data in respect of periodic communications of IoT devices obtained by observing transmissions from across Internal Dry Wall.

Table 5.3

Monitorable Communications across Internal Dry Wall

Internal Dry Wall	0-10m	45-55m	65-75m
SmartThings Hub	5	5	0
Philips Hue Hub	5	5	0
Philips Light Bulb - 01	5	4	0
Philips Light Bulb - 02	5	5	0
Aeotec Multipurpose Sensor	6	5	0
SmartThings Motion Sensor	6	4	0
Philips Indoor Motion Sensor	5	4	0
Philips Outdoor Motion Sensor	6	4	0

5.2.3 Colorsteel Garage Door

Data obtained for each of the 8 IoT devices across Garage Door showed a decrease in monitorable periodic communications as the distance to Garage Door increased from 0-10m to 65-75m. The periodic communications were fewer but remained

monitorable for all devices when the distance to Garage Door increased to 45-55m. Data showed the decrease to be more pronounced amongst the battery-powered sensor devices. In contrast, there were no monitorable periodic communications from any of the 8 IoT devices when the distance to Garage Door increased to 65-75m.

Table 5.4 presents the data in respect of periodic communications of IoT devices obtained by observing transmissions from across Garage Door.

Table 5.4

Monitorable Communications across Garage Door

Garage Door	0-10m	45-55m	65-75m
SmartThings Hub	5	4	0
Philips Hue Hub	5	4	0
Philips Light Bulb - 01	6	5	0
Philips Light Bulb - 02	6	5	0
Aeotec Multipurpose Sensor	9	1	0
SmartThings Motion Sensor	9	5	0
Philips Indoor Motion Sensor	8	1	0
Philips Outdoor Motion Sensor	8	2	0

5.2.4 Single-Pane Window

Table 5.5 presents the data in respect of periodic communications of IoT devices obtained by observing transmissions from across Single-Pane Window.

Table 5.5

Monitorable Communications across Single-Pane Window

Single-Pane Window	0-10m	45-55m	65-75m
SmartThings Hub	5	5	0
Philips Hue Hub	9	9	0
Philips Light Bulb - 01	10	9	0
Philips Light Bulb - 02	10	10	0
Aeotec Multipurpose Sensor	6	4	0
SmartThings Motion Sensor	6	4	0
Philips Indoor Motion Sensor	5	2	0
Philips Outdoor Motion Sensor	5	2	0

Data obtained for each of the 8 IoT devices across Single-Pane Window showed a decrease in monitorable periodic communications as the distance to Single-Pane Window increased from 0-10m to 65-75m. Whilst the periodic communications from all 8 IoT devices remained monitorable when the distance to Single-Pane Window increased from 0-10m to 45-55m, data showed a decrease in monitorable periodic communications from 5 out of 8 devices. 4 out of the 5 devices with fewer monitorable periodic communications were battery-powered sensor devices. 1 mains-powered device amongst the 4 mains-powered devices also showed a decrease in periodic monitorable communications when the distance to Single-Pane Window increased from 0-10m to 45-55m. However, there were no monitorable periodic communications from any of the mains-powered devices when the distance to Single-Pane Window increased from 0-10m to 65-75m. Like the mains-powered devices, there were no monitorable periodic communications from any of the battery-powered devices when the distance to Single-Pane Window increased from 0-10m to 65-75m.

5.2.5 Double-Glazed Window

Table 5.6 presents the data in respect of periodic communications of IoT devices obtained by observing transmissions from across Double-Glazed Window.

Table 5.6

Monitorable Communications across Double-Glazed Window

Double-Glazed Window	0-10m	45-55m	65-75m
SmartThings Hub	5	3	0
Philips Hue Hub	5	3	0
Philips Light Bulb - 01	5	3	0
Philips Light Bulb - 02	4	2	0
Aeotec Multipurpose Sensor	6	0	0
SmartThings Motion Sensor	6	1	0
Philips Indoor Motion Sensor	6	0	0
Philips Outdoor Motion Sensor	6	3	0

Data obtained for each of the 8 IoT devices across Double-Glazed Window showed a decrease in monitorable periodic communications as the distance to wall increased from 0-10m to 65-75m. The periodic communications remained monitorable for 6 out of the 8 devices when the distance to Double-Glazed Window increased from 0-10m to 45-55m. Compared to battery-powered sensor devices, data showed a less pronounced decrease in monitorable periodic communications across mains-powered devices when the distance to Double-Glazed Window increased from 0-10m to 45-55m. However, there were no monitorable periodic communications from any of the IoT devices when the distance to Double-Glazed Window increased from 0-10m to 65-75m.

5.2.6 Obscure Glass Window

Table 5.7 presents the data generated about periodic communications of IoT devices obtained by observing transmissions from across Obscure Glass Window.

Table 5.7

Monitorable Communications across Obscure Glass Window

Obscure Window	0-10m	45-55m	65-75m
SmartThings Hub	5	5	0
Philips Hue Hub	5	4	0
Philips Light Bulb - 01	4	3	0
Philips Light Bulb - 02	4	3	0
Aeotec Multipurpose Sensor	6	4	0
SmartThings Motion Sensor	6	4	0
Philips Indoor Motion Sensor	4	2	0
Philips Outdoor Motion Sensor	4	1	0

Data obtained for the 8 IoT devices across Obscure Glass Window showed a decrease in monitorable periodic communications as the distance to Obscure Glass Window increased from 0-10m to 65-75m. Whilst periodic communications remained monitorable when the distance to wall increased from 0-10m to 45-55m, data showed

the monitorable periodic communications did not decrease for 1 mains-powered IoT device out of 4 similar devices. As the distance to Obscure Glass Window increased from 0-10m to 65-75m, however, there were no monitorable periodic communications from any of the mains-powered devices. There were no monitorable periodic communications from any of the battery-powered devices either.

5.2.7 Metal Roof

Table 5.8 presents the data generated about periodic communications of IoT devices obtained by observing transmissions from across Metal Roof.

Table 5.8

Monitorable Communications across Metal Roof

Metal Roof	0-10m	45-55m	65-75m
SmartThings Hub	15	10	0
Philips Hue Hub	16	11	0
Philips Light Bulb - 01	17	12	0
Philips Light Bulb - 02	15	10	0
Aeotec Multipurpose Sensor	10	0	0
SmartThings Motion Sensor	11	0	0
Philips Indoor Motion Sensor	12	1	0
Philips Outdoor Motion Sensor	12	4	0

Data obtained for each of the 8 IoT devices across Metal Roof showed a decrease in monitorable periodic communications as the distance to Metal Roof increased from 0-10m to 65-75m. The monitorable periodic communications were fewer for all devices when the distance to Metal Roof increased from 0-10m to 45-55m. Data showed the decrease to be more pronounced amongst the battery-powered sensor devices than the mains-powered devices. There were no monitorable periodic communications from 2 out of the 4 battery-powered IoT devices. In contrast, periodic communications remained monitorable from all 4 mains-powered devices. When the distance to Metal

Roof increased from 0-10m to 65-75m, there were no monitorable periodic communications from any of the 8 IoT devices.

5.3 Monitorability Study Results

5.3.1 Pilot Study Results

Table 5.9 shows the average of monitorable communications obtained from within 10m and from within 55m to 6 wall types for 3 IoT devices that were selected for the pilot study. Changes in average monitorable communications of at least 40% are also highlighted for each device.

Table 5.9

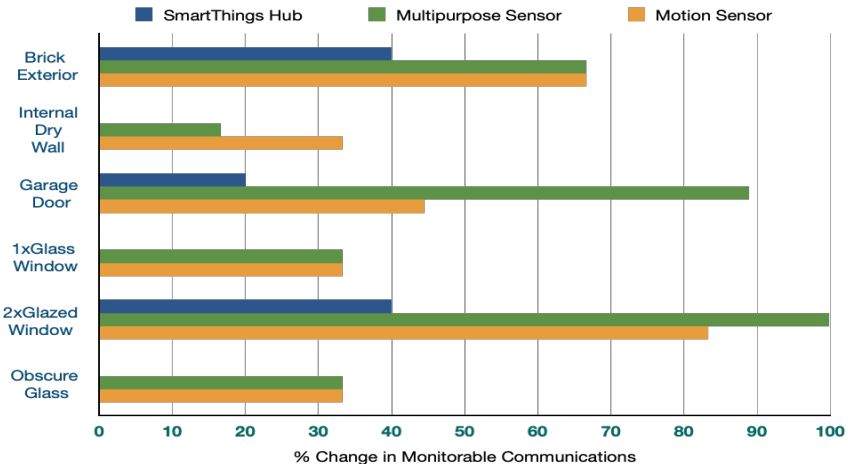
Monitorable Communications Comparison

Wall Types	SmartThings Hub		Multipurpose Sensor		Motion Sensor	
	0-10m	45-55m	0-10m	45-55m	0-10m	45-55m
Brick Exterior	5	3	6	2	6	2
Internal Dry Wall	5	5	6	5	6	4
Garage Door	5	4	9	1	9	5
Single-Pane Window	5	5	6	4	6	4
Double-Glazed Window	5	3	6	0	6	1
Obscure Glass Window	5	5	6	4	6	4

Figure 5.3 shows the percentage changes in average number of monitorable communications across all three devices for the 6 different wall types.

Figure 5.3

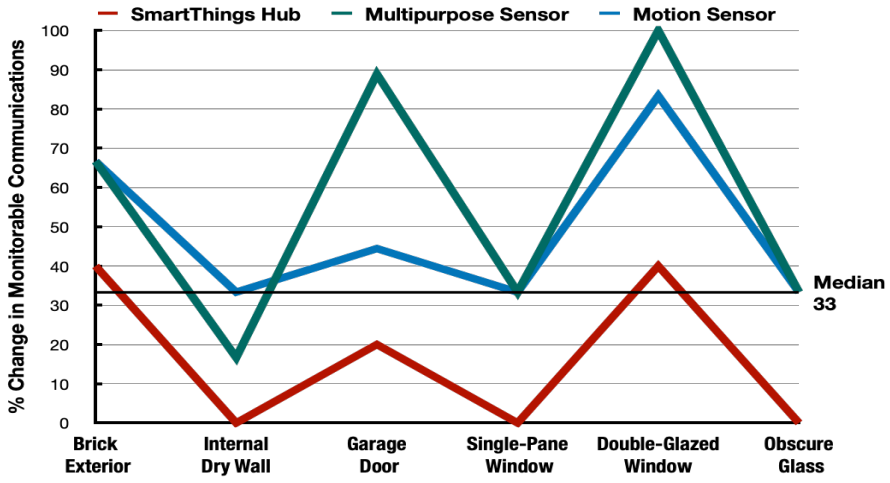
Percentage Change in Monitorable Communications



The view of percentage changes in monitorable communications points out that 2 out of 6 wall types, i.e. a third of all wall types used for testing, affected monitorable communications from the three devices by at least 40%. The wall types that affected the monitorable periodic communications by 40% or more are insulated brick exterior and double-glazed window. The median of the percentage changes in average number of monitorable communications across all three devices for 6 wall types is 33%. Figure 5.4 highlights the median of the percentage changes in average number of monitorable communications across all three devices for 6 wall types and distinguishes the 3 wall types that affected the average values most as the distance of monitoring increased.

Figure 5.4

Median of the Percentage Changes in Monitorable Communications



A comparison between the percentage changes in average number of monitorable communications and the median of the percentage changes point out that both insulated brick exterior and double-glazed window considerably affected the monitorable periodic communications of all 3 devices. Amongst the 3 devices, the monitorable communications of both battery-powered devices were also considerably affected by colorsteel garage door.

Figure 5.5 shows the average number of periodic communications from the multipurpose sensor that is monitorable within 10m and within 55m to 6 different wall types. The mean of the periodic communications monitorable within 10m and within 55m to wall is 7 and 3, respectively.

Figure 5.5

Monitorable Communications of Multipurpose Sensor

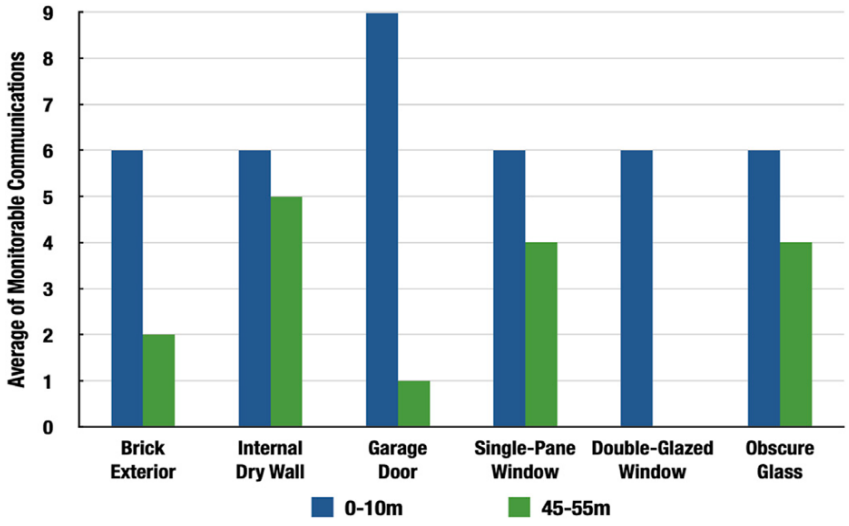
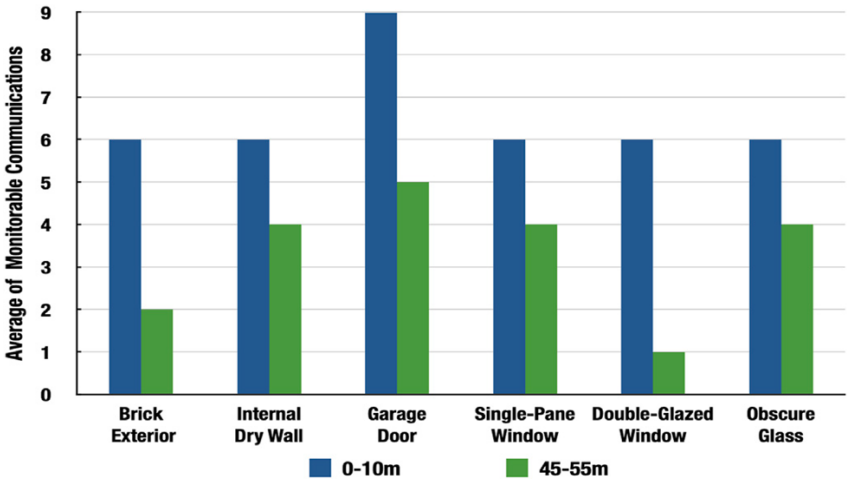


Figure 5.6 shows the average number of periodic communications from the motion sensor that is monitorable within 10m and within 55m to 6 different wall types.

Figure 5.6

Monitorable Communications of Motion Sensor

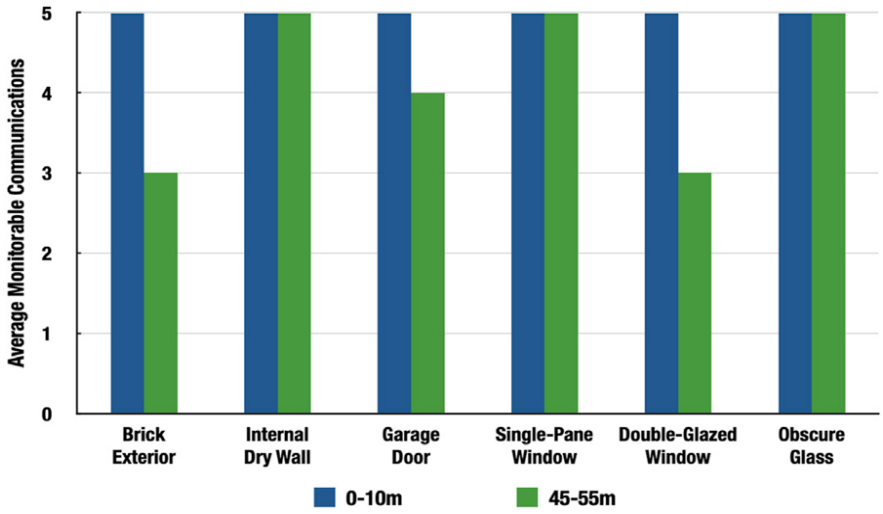


The mean of the periodic communications monitorable within 10m and within 55m to wall is 7 and 3, respectively. The change in average number of monitorable data requests, as the monitoring radio moved away from the different wall types, is remarkable amongst the battery-powered devices. The monitorable data requests from both the sensor nodes decreased by over 65% after the monitoring radio was redeployed from within 10m to brick cladding exterior to within 55m. For the double-glazed window, the monitorable data requests decreased by over 80%. For the colorsteel sectional garage door, however, the monitorable data requests showed a decrease of over 80% for only one sensor node. For 5 wall types, out of the 6 wall types, the monitorable data requests decreased by at least 33% as the monitoring radio moved approximately 50m away from the different walls.

Figure 5.7 shows the average number of periodic communications from the hub device that is monitorable within 10m and within 55m to 6 different wall types. The mean of the periodic communications monitorable within 10m and within 55m to wall is 5 and 4, respectively.

Figure 5.7

Monitorable Communications of SmartThings Hub



In contrast to the results of the battery-powered devices, the average number of monitorable broadcasts from the mains-powered hub remained the same for 3 out of 6 wall types as the monitoring radio moved approximately 50m away from the walls. There were no changes amongst the average number of broadcasts monitorable from within 10m distance and within 55m distance to internal dry wall, single pane window and obscure glass window. The average number of monitorable broadcasts showed a decrease of 40%, as the monitoring radio moved approximately 50m away, for brick exterior and double-glazed windows. Still, the decrease was 20% or less for 4 out of 6 wall types after the monitoring radio was redeployed from within 10m to within 55m distance to the different walls.

The differences in the results suggested that the monitorable range of IoT devices with integrated IEEE 802.15.4 radio depends on two factors, specifically, the power source of the device and the type of wall behind which a device is placed. Amongst the findings is also that the monitorable range of sensor devices with integrated IEEE 802.15.4 radio is relatively less compared to a network controller device interconnecting the sensor devices. The differences in the results between the monitorable data requests and broadcasts across 6 different wall types suggested that the battery powered sensor devices have a limited monitorable range of approximately 45m from most wall types. Though the mean of monitorable periodic communications is significantly less for within 55m to external wall, a mean of 3 indicates that battery powered radios transmit signals that are monitorable from 45m at least once every 40 seconds.

5.3.2 Detailed Study Results

The results of the detailed study into IoT monitorability, which utilised a larger sample of IoT devices to find the monitorable range of IoT devices that operate either on battery or mains power source, builds on the pilot study results. Based on the findings of the pilot study, the data obtained for the larger sample of mains-powered IoT devices and battery-powered IoT devices were separately analysed. The data obtained for the two IoT device types were also analysed to find the rate of monitorable periodic communications from the two IoT device types.

5.3.2.1 Mains-Powered IoT devices

Table 5.10 shows the average number of periodic communications monitorable from within 0-10m, 45-55m and 65-75m ranges for the 4 mains-powered IoT devices. Changes in average monitorable communications of at least 40% are also highlighted for each device.

Table 5.10

Comparison of Periodic Communications from Mains-Powered Devices

Wall Types	SmartThings Hub			Philips Hue Hub			Philips Light Bulb - 01			Philips Light Bulb - 02		
	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m
Brick Exterior	5	3	0	5	3	0	4	2	0	4	2	0
Internal Dry Wall	5	5	0	5	5	0	5	4	0	5	5	0
Garage Door	5	4	0	5	4	0	6	5	0	6	5	0
Single-Pane Window	5	5	0	9	9	0	10	9	0	10	10	0
Double-Glazed Window	5	3	0	5	3	0	5	3	0	4	2	0
Obscure Glass Window	5	5	0	5	4	0	4	3	0	4	3	0
Metal Roof	15	10	0	16	11	0	17	12	0	15	10	0

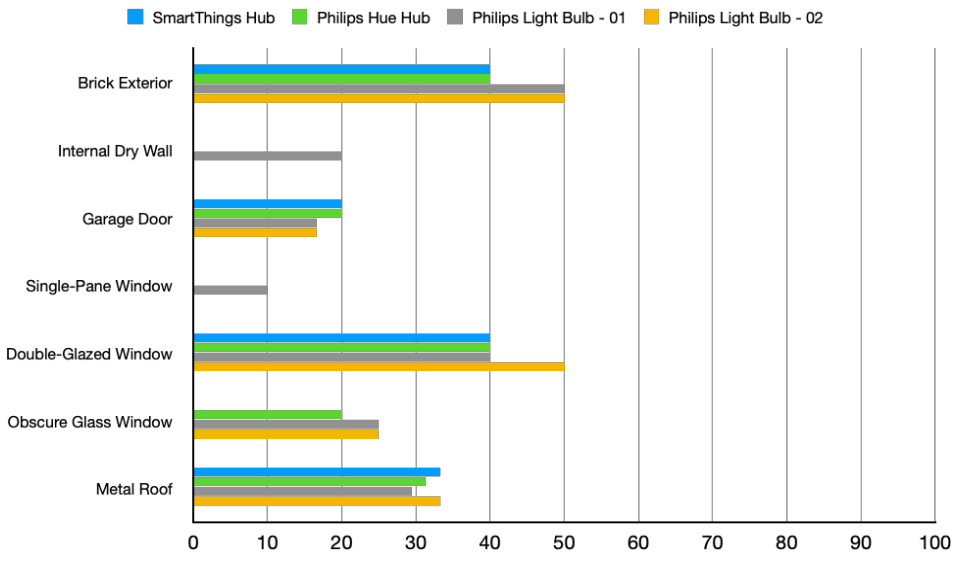
The data obtained showed there were no periodic communications from any of the 4 mains-powered devices when observed from locations within 65 to 75m to 7 different

wall types. In contrast, there were periodic communications when the 4 mains-powered devices were observed from locations within 45 to 55m to the different wall types. The data obtained for the 45 to 55m range, however, showed the monitorable communications varied. Further, the average number of monitorable periodic communications varied for the 4 devices across all wall types. Data also showed monitorable periodic communications from within 0 to 10m range varied. The monitorable periodic communications varied for the mains-powered devices across all 7 wall types.

The variations in monitorable periodic communications from the 4 mains-powered IoT devices were analysed further using graphical view of the data obtained. A graphical representation of the data enabled comparison of the periodic communications monitorable from within 0-10m and 45-55m ranges to the 7 different wall types. Figure 5.8 shows the percentage change to the average number of monitorable periodic communications as the distance to walls increased from within 10m range to within 45-55m range for each of the 4 mains-powered IoT devices.

Figure 5.8

Percentage Change in Periodic Communications of Mains-Powered Devices



This view shows 2 out of the 7 wall types, which is less than a third of all the wall types that were used, affected the monitorable communications of all 4 devices tested by at least 40%. The 2 wall types that appeared to have affected the monitorable periodic communications most are insulated brick exterior and double-glazed window. The loss in monitorable periodic communications effected by both insulated brick exterior and double-glazed window was 50%. Whilst the loss in monitorable periodic communications for all 4 devices was mostly less than 40% across the 7 wall types, the loss in periodic communications effected was less than 30% by 4 out of 7 wall types, which is more than half of all wall types. Furthermore, the loss in monitorable periodic communications effected was between 10% and 20% for 3 wall types, including single-pane window, garage door and internal dry wall.

Generally, the patterns in data that emerged for the pairing of 4 mains-powered devices with 7 wall types are similar to the patterns in data that emerged for the pairing of 1 mains-powered IoT device with 6 wall types during pilot study. Compared to the differences between periodic communications monitorable approximately 10m away and approximately 50m away from the 7 wall types, the differences between periodic communications monitorable approximately 10m away and approximately 70m away from the 7 wall types are more pronounced across all 4 mains-powered devices. The pattern of data obtained for locations approximately 70m away from the 7 wall types, which is highlighted in Table 5.10, suggest that periodic communications of mains-powered devices are not monitorable 70m away. However, the differences between the periodic communications monitorable approximately 70m away and approximately 50m away from the 7 wall types for all 4 mains-powered devices suggest that the monitorable range of periodic communications from mains-powered devices is approximately 60m.

5.3.2.2 Battery-Powered IoT Devices

A detailed study of battery-powered IoT devices followed the study of mains-powered IoT devices. Table 5.11 shows the average number of periodic communications monitorable from within 0-10m, 45-55m and 65-75m for the 4 battery-powered IoT devices. Changes in average monitorable communications of at least 40% are also highlighted for each battery-powered device.

Table 5.11

Comparison of Periodic Communications from Battery-Powered Devices

Wall Types	Aeotec Multipurpose Sensor			SmartThings Motion Sensor			Philips Indoor Motion Sensor			Philips Outdoor Motion Sensor		
	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m	0-10m	45-55m	65-75m
Brick Exterior	6	2	0	6	2	0	7	2	0	6	2	0
Internal Dry Wall	6	5	0	6	4	0	5	4	0	6	4	0
Garage Door	9	1	0	9	5	0	8	1	0	8	2	0
Single-Pane Window	6	4	0	6	4	0	5	2	0	5	2	0
Double-Glazed Window	6	0	0	6	1	0	6	0	0	6	3	0
Obscure Glass Window	6	4	0	6	4	0	4	2	0	4	1	0
Metal Roof	10	0	0	11	0	0	12	1	0	12	4	0

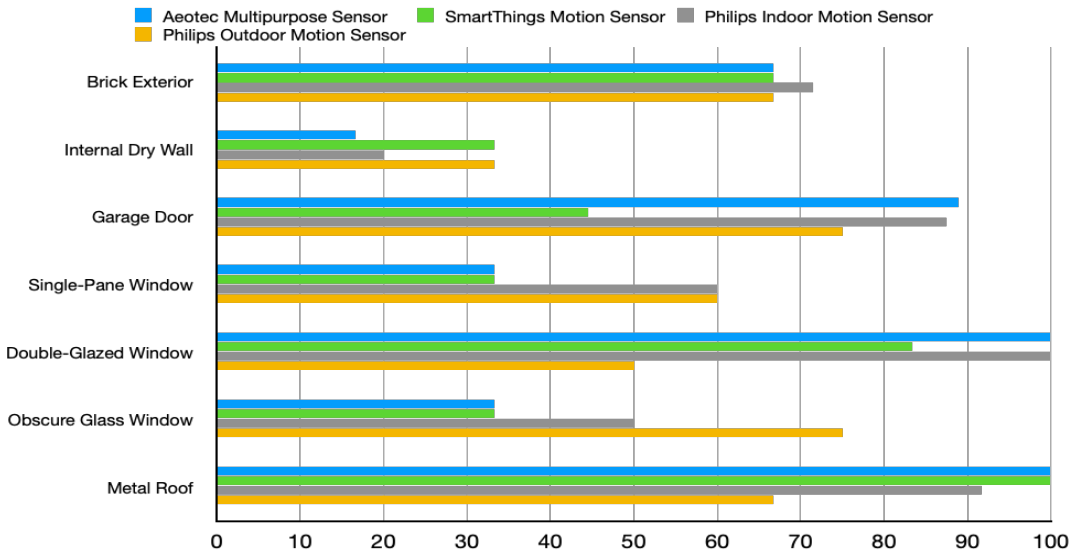
Like the data obtained for the 4 mains-powered devices, the data obtained for the battery-powered devices showed there were no periodic communications from any of the 4 battery-powered devices when observed from locations within 65 to 75m to 7 different wall types. However, there were periodic communications when the 4 battery-powered devices were observed from locations within 45 to 55m to the different wall types. The data obtained for the 45 to 55m range also showed the monitorable communications varied for the 4 devices across all 7 wall types. Data also showed monitorable periodic communications from within 0 to 10m range

varied. The monitorable periodic communications varied for the battery-powered devices across all 7 wall types.

The variations in monitorable periodic communications from the 4 battery-powered IoT devices were analysed further using graphical view of the data obtained. A graphical representation of the data enabled comparison of the periodic communications monitorable from within 0-10m and 45-55m ranges to the 7 different wall types. Figure 5.9 shows the percentage change to the average number of monitorable periodic communications as the distance to walls increased from within 10m range to within 45-55m range for each of the 4 battery-powered IoT devices.

Figure 5.9

Percentage Change in Periodic Communications of Battery-Powered Devices



This view shows the loss in periodic communications for all 4 devices was at least 30% across 6 out of the 7 wall types. 4 out of those 6 wall types, which is more than half of all the wall types used, appear to have affected monitorable communications from the 4 devices by at least 40%. The 4 wall types that appear to have affected the monitorable periodic communications relatively more are brick exterior, garage door,

double-glazed window and metal roof. 3 out of those 4 wall types appear to have affected the monitorable communications from all 4 devices by at least 50%. Amongst the 4 wall types, brick exterior and metal roof appear to have affected the monitorable communications from all 4 devices by at least 60%. Double-glazed window and metal roof appear to have effected the highest possible loss in monitorable periodic communications.

The patterns in data that emerged for the pairing of 4 battery-powered devices with 7 wall types are similar to the patterns in data that emerged for the pairing of 2 battery-powered devices with 6 wall types during the pilot study. In contrast to the patterns that emerged for the battery-powered devices, the pattern of data obtained for locations approximately 70m away from the 7 wall types for all 4 battery-powered devices, which is highlighted in Table 5.11, suggests that periodic communications are not monitorable 70m away. However, as the pilot study results suggested, the differences between the periodic communications obtained approximately 50m away and approximately 10m away from the 7 wall types for all 4 battery-powered devices suggest that the monitorable range of periodic communications from battery-powered devices is approximately 45m.

5.3.3 Additional Results

5.3.3.1 Mains-Powered IoT devices

The data in respect of periodic communications that was generated for the 4 mains-powered devices using the communications captured from locations approximately 50m away was further analysed to determine the rate of monitorable transmissions from mains-powered IoT devices. This analysis involved the computation of mean value of the data obtained for each of the 4 mains-powered devices. The mean and

standard deviation of the data obtained for each of the 4 mains-powered devices is shown in Table 5.12.

Table 5.12

Mean of Monitorable Periodic Communications across Mains-powered Devices

Wall Types	SmartThings Hub	Philips Hue Hub	Philips Light Bulb - 01	Philips Light Bulb - 02
Brick Exterior	*3*	*3*	*2*	*2*
Internal Dry Wall	5	5	4	5
Garage Door	4	4	5	5
Single-Pane Window	5	9	9	10
Double-Glazed Window	*3*	*3*	*3*	*2*
Obscure Glass Window	5	4	3	3
Metal Roof	10	11	12	10
Mean (Standard Deviation)	**5 (+/-2.38)**	**5.57 (+/-3.15)**	**5.42 (+/-3.69)**	**5.28 (+/-3.45)**

The high standard deviation in data across all 4 mains-powered devices suggests that the type of wall that surrounds mains-powered IoT devices with integrated radio has an impact on the rate of monitorable radio signals. For 2 out of 4 mains-powered devices, 86% of the data appeared to be within +/- one standard deviation of the mean. For both the other mains-powered devices, 71% of the data obtained appeared to be within +/- one standard deviation of the mean. The mean values of the 4 mains-powered devices, which varied between 5 and 5.57, are comparable to the mean value of the pilot study data. Importantly, the mean values imply that mains-powered radios transmit signals that are monitorable from 60m at least once every 40 seconds, regardless of the wall type.

5.3.3.2 Battery-Powered IoT devices

The data generated for the 4 battery-powered devices using communications captured from locations approximately 50m away was also analysed to determine the rate of

monitorable transmissions from battery-powered IoT devices. Accordingly, further analysis of the data involved the computation of mean value of the data obtained for each of the 4 battery-powered devices. The mean and standard deviation of the data obtained for each of the 4 battery-powered devices is shown in Table 5.13.

Table 5.13

Mean of Monitorable Periodic Communications across Battery-powered Devices

Wall Types	*Aeotec Multipurpose Sensor*	*SmartThings Motion Sensor*	*Philips Indoor Motion Sensor*	*Philips Outdoor Motion Sensor*
Brick Exterior	2	2	2	2
Internal Dry Wall	5	4	4	4
Garage Door	1	5	1	2
Single-Pane Window	4	4	2	2
Double-Glazed Window	0	1	0	3
Obscure Glass Window	4	4	2	1
Metal Roof	0	0	1	4
Mean (Standard Deviation)	**2.28 (+/-2.05)**	**2.85 (+/-1.86)**	**1.71 (+/-1.25)**	**2.57 (+/-1.13)**

The high standard deviation in data across 3 out of 4 battery-powered devices suggests that the type of wall that surrounds battery-powered IoT devices with integrated radio has an impact on the rate of monitorable radio signals. For 2 out of 4 battery-powered devices, 71% of the data appeared to be within +/- one standard deviation of the mean. For both the other battery-powered devices, 57% of the data obtained appeared to be within +/- one standard deviation of the mean. The mean values of the 4 battery-powered devices, which varied between 1.71 and 2.85, are comparable to the mean values of the pilot study data. Importantly, the mean values imply that battery-powered radios transmit signals that are monitorable from 45m at least once every 40 seconds, regardless of the wall type.

5.4 Conclusion

This chapter reviewed and discussed the communications of IoT devices that were monitored and captured to study the monitorability of IoT devices. To generate the data required for the study, 8 IoT devices were iteratively monitored from various distances. Experiments utilised 7 wall types to determine the factors that influence the monitorability of IoT devices, the monitorable range of periodic communications and the rate of monitorable transmissions. The study into the monitorability of IoT devices from radio communications found that the monitorable range of IoT devices depends on the power source and wall type. The study, which analysed the communications of mains and battery-powered IoT devices with integrated IEEE 802.15.4 radio, found mains-powered IoT devices transmit periodic communications monitorable from as far as 60m to a variety wall types at least once every 40 seconds. Further, the study found battery-powered IoT devices transmit periodic communications monitorable from as far as 45m to a variety wall types at least once every 40 seconds.

Chapter 6

IoT TRACEABILITY FINDINGS

6.1 Introduction

In this chapter, the data obtained for the study of IoT devices traceability is reviewed and discussed. The study of IoT devices traceability examined network management and control communications that IoT devices with integrated radio employ to communicate with other devices of an internal IoT devices' network. Like the study into IoT monitorability, the study into traceability is entirely based on wireless communications between IoT devices. For data collection, a selection of IoT platforms and devices were setup and observed. From amongst the communications captured, network management and control communications were examined to understand the commonalities and differences in communications of IoT devices. The results formed the basis of the findings related to the specific details of IoT devices that may be traced from wireless communications of node pairs that form datalinks.

6.2 Traceability Study Data

Three IoT platforms connected the IoT devices selected for the study into IoT traceability. The selection of platforms included Samsung SmartThings, Vera Edge and Philips Hue. Amongst the platforms, Samsung SmartThings included support for both Zigbee and Z-Wave based sensor networks. The Vera Edge platform, which supports Z-Wave technology, provided for a second Z-Wave network. The Philips Hue platform, which supports Zigbee technology, provided for a second Zigbee network. The setup of all three IoT platforms utilised a hub that connected to the Internet gateway and acted as the network controller. The SmartThings hub acted as the network controller for a Zigbee network and a Z-Wave network simultaneously.

Whilst connected to the Internet, the hub of each platform enabled setup and configuration of compatible sensor and actuator devices. A selection of sensor and actuator devices that are widely available for the selected IoT platforms was setup to obtain data for all device types. To be able to generate the data required, communications between the nodes connected by each of the 3 IoT platforms were iteratively observed. Table 6.1 lists the selection of IoT devices along with other information, including supported technology, device type and power source.

Table 6.1

Selection of Devices for IoT Traceability Study

IoT Device	Technology	Node Type	Device Type	Power Source
SmartThings Hub	Zigbee, Z-Wave	Sink	Static	Mains
Vera Edge Hub	Z-Wave	Sink	Static	Mains
Philips Hue Hub	Zigbee	Sink	Static	Mains
Aeotec Multipurpose Sensor	Zigbee	Sensor	Mobile	Battery
Philips Motion Sensor	Zigbee	Sensor	Mobile	Battery
Philips Hue Bulb - 01	Zigbee	Actuator	Static	Mains
Philips Hue Bulb - 02	Zigbee	Actuator	Static	Mains
Aeotec Multi-Sensor	Z-Wave	Sensor	Mobile	Battery
Aeotec Window Sensor	Z-Wave	Sensor	Mobile	Battery
Aeotec Switch - 01	Z-Wave	Actuator	Static	Mains
Aeotec Switch - 02	Z-Wave	Actuator	Static	Mains

From amongst the communications between the different node types that were captured over several iterations, network management and control communications between the nodes were targeted for inspection. Initially, the network management and control communications between nodes of the two Zigbee platforms were interpreted and separated from the packets captured. Subsequently, the network management and control communications between nodes of the two Z-Wave platforms were interpreted and separated from the packets captured. Next, samples of

the network management and control communications obtained from the testbed of Zigbee and Z-Wave networks were examined. That involved the audit of address types embedded in transmissions captured as the nodes communicated with peer MAC entities. The audit of the address types generated the data required to analyse and understand the commonalities and differences in network management and control communications of IoT devices. Data obtained for each IoT device is catalogued and reviewed below.

6.2.1 Sink Nodes

6.2.1.1 Zigbee

Samples of the communications captured from the static SmartThings Hub showed the Zigbee sink node to have employed two 802.15.4 applications for network management and control. Inspection of the communications showed the SmartThings Hub non-periodically transmitted 802.15.4 Data and periodically transmitted 802.15.4 Beacon. Inspection of the 802.15.4 applications, which the SmartThings Hub employed to operate in a Zigbee network, showed the non-periodic transmissions of 802.15.4 Data to have embedded identifiers to identify the network, source and destination. The periodic transmissions of 802.15.4 Beacon by the SmartThings Hub, in contrast, embedded identifiers to identify the network and source.

Table 6.2 lists the 802.15.4 applications and the identifiers that the static SmartThings Hub utilised to operate as the sink device of a Zigbee network.

Table 6.2

802.15.4 Applications and Identifiers of SmartThings Hub

802.15.4 Application	Frequency	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Beacon	Periodic	Yes	Yes	No

Further inspection of the communications showed the periodically transmitted 802.15.4 Beacon utilised the superframe specification field to identify the node as a "PAN coordinator" device. Like the communications from the static SmartThings Hub, samples of the communications captured from the static Philips Hue Hub showed the Zigbee sink node to have employed two 802.15.4 applications for network management and control. Inspection of the communications showed the Philips Hue hub, to operate in a Zigbee network, non-periodically transmitted 802.15.4 Data and periodically transmitted 802.15.4 Beacon.

The non-periodic transmissions of 802.15.4 Data embedded the identifiers to identify the network, source and destination. In contrast, the periodic transmissions of 802.15.4 Beacon embedded identifiers to identify the network and source. Like the 802.15.4 Beacon periodically transmitted by the SmartThings Hub, the 802.15.4 Beacon periodically transmitted by the Philips Hue Hub included the superframe specification field. However, the 802.15.4 Beacon periodically transmitted by the Philips Hue Hub did not identify the node as a "PAN coordinator" device. Table 6.3 lists the 802.15.4 applications and the identifiers that the static Philips Hue Hub utilised to operate as the sink device of a Zigbee network. The 802.15.4 Beacon transmitted by the Philips Hue Hub device is distinguished from the 802.15.4 Beacon transmitted by the SmartThings Hub device using the "Type 2" label.

Table 6.3

802.15.4 Applications and Identifiers of Philips Hue Hub

802.15.4 Application	Type	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Beacon (Type 2)	Periodic	Yes	Yes	No

6.2.1.2 Z-Wave

Samples of the communications captured from the static SmartThings hub showed the Z-Wave sink node to have employed two G.9959 applications for network management and control. Inspection of the communications showed the SmartThings Hub, to operate in a Z-Wave network, non-periodically transmitted G.9959 Wake Up No Information and non-periodically transmitted G.9959 Acknowledgement. Inspection of the G.9959 applications employed by the SmartThings Hub showed the non-periodic transmissions of G.9959 Wake Up No Information and the non-periodic transmissions of G.9959 Acknowledgement embedded identifiers to identify network, source and destination. Table 6.4 lists the G.9959 applications and the identifiers that the static SmartThings Hub utilised to operate as the sink device of a Z-Wave network.

Table 6.4

G.9959 Applications and Identifiers of SmartThings Hub

G.9959 Application	Type	Network ID	Source ID	Destination ID
Wake Up No More Information	Non-Periodic	Yes	Yes	Yes
Acknowledgement	Non-Periodic	Yes	Yes	Yes

Table 6.5 lists the G.9959 applications and the identifiers that the static Vera Edge Hub utilised to operate as the sink device of a Z-Wave network.

Table 6.5

G.9959 Applications and Identifiers of Vera Edge Hub

G.9959 Application	Type	Network ID	Source ID	Destination ID
Wake Up No More Information	Non-Periodic	Yes	Yes	Yes
Acknowledgement	Non-Periodic	Yes	Yes	Yes

Like the communications from the static SmartThings hub, samples of the communications captured from the static Vera Edge Hub showed the Z-Wave sink

node to have employed two G.9959 applications for network management and control. To operate in a Z-Wave network, the Vera Edge Hub non-periodically transmitted G.9959 Wake Up No Information and non-periodically transmitted G.9959 Acknowledgement. Inspection of the G.9959 applications employed by the Vera Edge Hub showed the non-periodic transmissions of G.9959 Wake Up No Information and the non-periodic transmissions of G.9959 Acknowledgement embedded identifiers to identify network, source and destination.

6.2.2 Sensor Nodes

6.2.2.1 Zigbee

Samples of the communications captured from the mobile Aeotec Multipurpose Sensor showed the Zigbee sensor node to have employed two 802.15.4 applications for network management and control. To operate in a Zigbee network, Aeotec Multipurpose Sensor periodically transmitted 802.15.4 Command and non-periodically transmitted 802.15.4 Data. Both the periodic transmissions of 802.15.4 Command and the non-periodic transmissions of 802.15.4 Data by the Aeotec Multipurpose Sensor embedded identifiers to identify the network, source and destination.

Table 6.6 lists the 802.15.4 applications and the identifiers that the mobile Aeotec Multipurpose Sensor utilised to operate in a Zigbee network.

Table 6.6

802.15.4 Applications and Identifiers of Aeotec Multipurpose Sensor

802.15.4 Application	Type	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Command	Periodic	Yes	Yes	Yes

Like the samples of the communications from the Aeotec Multipurpose Sensor, samples of the communications from the mobile Philips Motion Sensor showed the Zigbee sensor node to have employed two 802.15.4 applications for network management and control. The Philips Motion Sensor also periodically transmitted 802.15.4 Command and non-periodically transmitted 802.15.4 Data to operate in a Zigbee network. Both the periodic transmissions of 802.15.4 Command and the non-periodic transmissions 802.15.4 Data by the Philips Motion Sensor embedded the identifiers to identify network, source and destination.

Table 6.7 lists the 802.15.4 applications and the identifiers that the mobile Philips Motion Sensor utilised to operate in a Zigbee network.

Table 6.7

802.15.4 Applications and Identifiers of Philips Motion Sensor

802.15.4 Application	Type	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Command	Periodic	Yes	Yes	Yes

6.2.2.2 Z-Wave

Table 6.8 lists the G.9959 applications and the identifiers that the mobile Aeotec Multi-Sensor utilised during operation.

Table 6.8

G.9959 Applications and Identifiers of Aeotec Multi-Sensor

G.9959 Application	Type	Network ID	Source ID	Destination ID
Wake Up Notification	Periodic	Yes	Yes	Yes
Acknowledgement	Non-Periodic	Yes	Yes	Yes

Samples of the communications captured from the mobile Aeotec Multi-Sensor showed the Z-Wave sensor node to have employed two G.9959 applications for

network management and control. To operate in a Z-Wave network, the Aeotec Multi-Sensor periodically transmitted G.9959 Wake Up Notification and non-periodically transmitted G.9959 Acknowledgement. Both the periodic transmissions of G.9959 Wake Up Notification and non-periodic transmissions of G.9959 Acknowledgement by the Aeotec Multi-Sensor embedded the identifiers that identify network, source and destination.

Like the samples of the communications from the Aeotec Multi-Sensor, samples of the communications from the mobile Aeotec Window Sensor showed the Z-Wave sensor node to have employed two G.9959 applications for network management and control. The Window Sensor also periodically transmitted G.9959 Wake Up Notification and non-periodically transmitted G.9959 Acknowledgement to operate in a Z-Wave network. Both the periodic transmissions of G.9959 Wake Up Notification and the non-periodic transmissions of G.9959 Acknowledgement by the Window Sensor embedded the identifiers that identify network, source and destination.

Table 6.9 lists the G.9959 applications and the identifiers that the mobile Aeotec Window Sensor utilised during operation.

Table 6.9

G.9959 Applications and Identifiers of Aeotec Window Sensor

G.9959 Application	Type	Network ID	Source ID	Destination ID
Wake Up Notification	Periodic	Yes	Yes	Yes
Acknowledgement	Non-Periodic	Yes	Yes	Yes

6.2.3 Actuator Nodes

6.2.3.1 Zigbee

Samples of the communications from one of the two static Philips Hue Bulbs showed the Zigbee actuator node to have employed two 802.15.4 applications for network

management and control. To operate in a Zigbee network, the Philips Hue Bulb non-periodically transmitted 802.15.4 Data and periodically transmitted 802.15.4 Beacon. Inspection of the 802.15.4 applications, which the Philips Hue Bulb employed, showed the non-periodic transmissions of 802.15.4 Data embedded the identifiers that identify network, source and destination. In contrast, the periodic transmissions of 802.15.4 Beacon by the Philips Hue bulb embedded network identifier and source identifier. Further inspection of communications showed the periodically transmitted 802.15.4 Beacon utilised the superframe specification field to identify the node as a non-PAN coordinator device.

Table 6.10 lists the different 802.15.4 applications and the identifiers that the static Philips Hue Bulb utilised to operate in a Zigbee network.

Table 6.10

802.15.4 Applications and Identifiers of Philips Hue Bulb - 01

802.15.4 Application	Type	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Beacon	Periodic	Yes	Yes	No

Samples of the communications from the second Philips Hue Bulb also showed the Zigbee actuator node to have employed two 802.15.4 applications for network management and control. Inspections of the communications showed the second Philips Hue Bulb also non-periodically transmitted 802.15.4 Data and periodically transmitted 802.15.4 Beacon to operate in a Zigbee network. Inspections of the 802.15.4 applications showed the non-periodic transmissions of 802.15.4 Data embedded the identifiers that identify network, source and destination. The periodic transmissions of 802.15.4 Beacon, however, embedded the identifiers to identify network and source.

Table 6.11 lists the different 802.15.4 applications and the identifiers that the second static Philips Hue Bulb utilised to operate in a Zigbee network.

Table 6.11

802.15.4 Applications and Identifiers of Philips Hue Bulb - 02

802.15.4 Application	Type	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Beacon	Periodic	Yes	Yes	No

Further inspection of communications showed the periodically transmitted 802.15.4 Beacon also included the superframe specification field. The 802.15.4 Beacon periodically transmitted by the Philips Hue Bulb also identified the actuator node as a non-PAN coordinator device.

6.2.3.2 Z-Wave

Samples of the communications from one of the two static Aeotec Switches showed the Z-Wave actuator node to have employed one G.9959 application for network management and control. To operate in a Z-Wave network, the Aeotec Switch non-periodically transmitted G.9959 Acknowledgement. The non-periodic transmissions of G.9959 Acknowledgement embedded identifiers to identify the network, source and destination.

Table 6.12 lists the G.9959 application and the identifiers that the static Aeotec Switch utilised to operate in a Z-Wave network.

Table 6.12

G.9959 Applications and Identifiers of Aeotec Switch - 01

G.9959 Application	Type	Network ID	Source ID	Destination ID
Acknowledgement	Non-Periodic	Yes	Yes	Yes

Table 6.13 lists the G.9959 application and the identifiers that the second static Aeotec Switch utilised to operate in a Z-Wave network.

Table 6.13

G.9959 Applications and Identifiers of Aeotec Switch - 02

G.9959 Application	Type	Network ID	Source ID	Destination ID
Acknowledgement	Non-Periodic	Yes	Yes	Yes

Samples of the communications from the second static Aeotec Switch device also showed the Z-Wave actuator node to have employed one G.9959 application for network management and control. Inspection of the communications showed the second Aeotec Switch also non-periodically transmitted G.9959 Acknowledgement to operate in a Z-Wave network. Further inspection showed the non-periodic transmissions of G.9959 Acknowledgement embedded the identifiers to identify the network, source and destination.

6.3 Traceability Study Results

In general, inspection of the communications captured from all three node types, including sink, sensor and actuator, showed every IoT device to have employed at least one 802.15.4 or G.9959 application with identifiers that identified the network, source and destination to communicate with peer MAC entities. Amongst the 3 node types, the sinks and actuators that operated in Zigbee networks also employed an 802.15.4 application without 3 identifiers. The 802.15.4 application that sink and actuator nodes additionally transmitted instead embedded 2 identifiers.

Following the review of 802.15.4 applications and G.9959 applications that IoT devices employ to operate and communicate, the commonalities and differences in network management and control communications of the sink, actuator and sensor

nodes were analysed. Analysis of the commonalities and differences in network management and control communications involved the collation and consolidation of 802.15.4 and G.9959 applications that featured in the communications between peer MAC entities of an IoT platform.

The consolidation of 802.15.4 and G.9959 applications that featured in the communications between peer MAC entities generated a view of the percentage of frame types that each device type accounted for. The frame types that featured amongst the transmissions of IoT devices with integrated 802.15.4 radio were initially analysed. Next, the frame types that featured amongst the transmissions of IoT devices with integrated G.9959 radio were analysed. The findings in respect of the IoT devices with integrated G.9959 radio were subsequently compared to the findings in respect of IoT devices with integrated 802.15.4 radio.

6.3.1 802.15.4 Radio Integrated Devices

The collation of 802.15.4 applications that featured amongst the selection of IoT devices showed the implementation of 802.15.4 Data application to be common and identical, with identical identifiers, across all mains-powered, static IoT devices and battery-powered, mobile IoT devices. Collation of the 802.15.4 applications also showed the implementation of 802.15.4 Command application to be common and identical, with identical identifiers, across all battery-powered, mobile devices. The 802.15.4 Command application, which feature across all battery-powered, mobile IoT devices, does not feature amongst the mains-powered, static IoT devices. The 802.15.4 Beacon application, which feature across all mains-powered, static IoT devices, does not feature amongst the battery-powered, mobile IoT devices.

Table 6.14 collates the 802.15.4 applications that the six IoT devices with integrated IEEE 802.15.4 radio utilised for communications with peer MAC entities.

Table 6.14

802.15.4 Applications of IoT Devices

IoT Device	Node Type	Power Source	Device Type	Frame Type 1	Frame Type 2
SmartThings Hub	Sink	Mains	Static	Beacon	Data
Philips Hue Hub	Sink	Mains	Static	Beacon (Type 2)	Data
Philips Hue Bulb – 01	Actuator	Mains	Static	Beacon	Data
Philips Hue Bulb - 02	Actuator	Mains	Static	Beacon	Data
Aeotec Multipurpose Sensor	Sensor	Battery	Mobile	Command	Data
Philips Motion Sensor	Sensor	Battery	Mobile	Command	Data

Unlike the identical implementation of the Command application by the battery-powered, mobile IoT devices, the implementation of the Beacon application is not identical across all mains-powered, static IoT devices. Two variants of the 802.15.4 Beacon application, with identical identifiers, feature across the mains-powered, static IoT devices. To analyse the commonalities and differences that were observed in network management and control communications of static and mobile IoT devices, the 802.15.4 applications of the 3 node types were consolidated. This involved the calculation of the percentage of 802.15.4 frame types that each device type accounted for and the percentage of 802.15.4 frame types that every device type commonly accounted for.

Table 6.15 shows the overall percentage of 802.15.4 frame types that each device type, mains-powered, static IoT devices and battery-powered, mobile IoT devices, accounted for. The table also shows the percentage of 802.15.4 frame types that the mains-powered, static IoT devices and the battery-powered, mobile devices amongst all node types commonly accounted for.

Table 6.15

Percentage of 802.15.4 Frame Types by Device and Node Type

Power Source, Device Type	Node Types	Overall %	% Common
Mains, Static	Sink, Actuator	66.67	33.33
Battery, Mobile	Sensor	66.67	33.33

This consolidated view of the 802.15.4 frame types that each of the 3 node types employed show both mains-powered, static IoT devices and battery-powered, mobile devices separately accounted for two-thirds of all 802.15.4 frame types employed by the 3 node types for communications with peer MAC entities. However, the view also points out that the mains-powered, static IoT devices and battery-powered, mobile devices commonly accounted for a third of all the 802.15.4 frame types employed by the 3 node types for communications with peer MAC entities. Exclusively, therefore, both mains-powered, static IoT devices and battery-powered, mobile devices accounted for a third of all the 802.15.4 frame types employed by the 3 node types for communications with peer MAC entities.

The results in respect of the IoT devices with integrated 802.15.4 radio suggest that the power source and usage type of an IoT device are traceable. The results in respect of the observed 802.15.4 frame transmissions suggest that Beacon frames signify a mains-powered, static source with integrated IEEE 802.15.4 radio. Additionally, Beacon frames with the superframe specification field identifying a “PAN Coordinator” device signify a mains-powered, static source that is a sink node.

Otherwise, the mains-powered, static source is either a sink or actuator node. Command frames signify a battery-powered, mobile source with integrated IEEE 802.15.4 that is a sensor node.

6.3.2 G.9959 Radio Integrated Devices

Table 6.16 collates the G.9959 applications that the six IoT devices with integrated G.9959 radio utilised for communications with peer MAC entities.

Table 6.16

G.9959 Applications of IoT Devices

IoT Device	Node Type	Power Source	Device Type	Frame Type 1	Frame Type 2
SmartThings Hub	Sink	Mains	Static	Wake Up No More Information	Acknowledgement
Vera Edge Hub	Sink	Mains	Static	Wake Up No More Information	Acknowledgement
Aeotec Switch - 01	Actuator	Mains	Static	-	Acknowledgement
Aeotec Switch - 02	Actuator	Mains	Static	-	Acknowledgement
Aeotec Multi-Sensor	Sensor	Battery	Mobile	Wake Up Notification	Acknowledgement
Window Sensor	Sensor	Battery	Mobile	Wake Up Notification	Acknowledgement

The collation of G.9959 applications that featured amongst the selection of IoT devices showed the implementation of G.9959 Acknowledgement application to be common and identical, with identical identifiers, across all mains-powered, static IoT devices and battery-powered, mobile IoT devices. Collation of G.9959 applications also showed the implementation of G.9959 Wake Up No More Information application by 2 out of 4 mains-powered, static IoT devices to be identical and to have utilised identical number of identifiers. The G.9959 Wake Up No More Information

application, which feature amongst the mains-powered, static IoT devices, does not feature amongst the battery-powered, mobile IoT devices.

The collated view of G.9959 applications that featured amongst the selection of IoT devices also showed the implementation of G.9959 Wake Up Notification application to be common and identical, with identical identifiers, across all battery-powered, mobile IoT devices. The G.9959 Wake Up Notification application, which feature across all battery-powered, mobile IoT devices, does not feature amongst the mains-powered, static IoT devices. To analyse the commonalities and differences that were observed in network management and control communications of static and mobile IoT devices, the G.9959 applications of the 3 node types were consolidated. This involved the calculation of the percentage of G.9959 frame types that each device type accounted for and the percentage of G.9959 frame types that every device type commonly accounted for.

Table 6.17 shows the overall percentage of G.9959 frame types that each device type, mains-powered, static IoT devices and battery-powered, mobile IoT devices, amongst the 3 node types accounted for. The table also shows the percentage of G.9959 frame types that the mains-powered, static IoT devices and the battery-powered, mobile devices amongst all node types commonly accounted for.

Table 6.17

Percentage of G.9959 Frame Types by Device and Node Type

Power Source, Device Type	Node Types	Overall %	% Common
Mains, Static	Sink	66.67	33.33
Mains, Static	Actuator	33.33	33.33
Battery, Mobile	Sensor	66.67	33.33

This consolidated view of the G.9959 frame types that each of the 3 node types employed show both mains-powered, static IoT devices and battery-powered, mobile

devices separately accounted for two-thirds of all G.9959 frame types employed by the 3 node types for communications with peer MAC entities. However, the view also points out that the mains-powered, static IoT devices and battery-powered, mobile devices commonly accounted for a third of all the G.9959 frame types employed by the 3 node types for communications with peer MAC entities. Exclusively, therefore, both mains-powered, static IoT devices and battery-powered, mobile devices accounted for a third of all the G.9959 frame types employed by the 3 node types for communications with peer MAC entities.

Supplementing the findings of the analysis of 802.15.4 applications, the results in respect of the IoT devices with integrated G.9959 radio also suggest that the power source and usage type of an IoT device are traceable. The results in respect of the observed G.9959 frame transmissions suggest that non-periodic Wake Up No More Information frames signify a mains-powered, static source with integrated ITU-T G.9959 radio that is a sink node. Periodic Wake Up Notification frames signify a battery-powered, mobile source with integrated G.9959 radio that is a sensor node. Additionally, the absence of non-periodic Wake Up No More information frames and periodic Wake Up Notification frames from a source that transmits non-periodic Acknowledgement frames signify a mains-powered, static source that is an actuator node.

6.4 Conclusion

This chapter reviewed and analysed the network management and control communications that IoT devices typically employed to study the traceability of IoT devices. Inspection of the communications between nodes of 3 IoT platforms showed the different IEEE 802.15.4 and ITU-T G.9959 applications that the nodes

implemented to communicate with peer MAC entities. Inspection of the communications also showed the different combinations of identifiers that transmissions embedded in an intelligible format for the purpose of network management and control. Analysis of the IEEE 802.15.4 and ITU-T G.9959 applications employed by IoT devices determined the commonalities and differences in communications of static and mobile IoT devices. The study, which examined network management and control communications of a variety of IoT devices that are available for various indoor applications, found that specifics of an IoT device, such as type, whether static or mobile, and power source, whether mains-powered or battery-powered, are distinguishable from the radio transmissions of node pairs that form an internal IoT devices' network.

Chapter 7

IoT DISCOVERABILITY FINDINGS

7.1 Introduction

This chapter covers the details and findings of the study into the discoverability aspect of IoT devices. The chapter includes a review of the data that was collected to study the discoverability of IoT devices from radio communications of an internal IoT devices' network. The review of data collected is followed by data analysis and the results obtained are discussed. To generate the data suitable to study IoT discoverability, experiments involved a MATLAB-based IoT network simulator, which was custom-built to simulate internal IoT devices' networks. The IoT network simulator provided for the need to be able to collect data from both star and mesh IoT networks. The data collected from simulated star and mesh IoT networks was examined to determine the iota (I), the smallest configuration of devices, from which 100% of the devices that constitute an internal IoT devices' network may be discovered through radio signals monitoring.

7.2 Discoverability Study Data

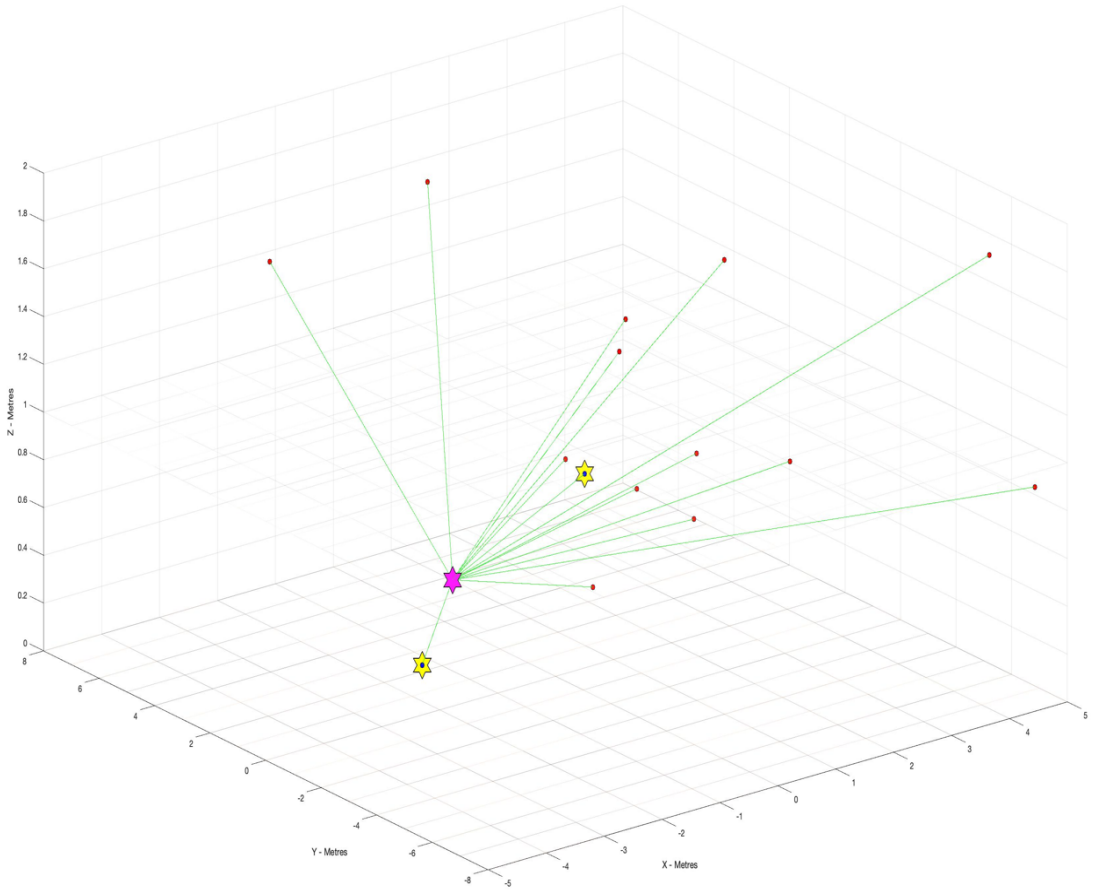
For every internal IoT devices' network that was simulated using the custom-built MATLAB-based IoT simulator, data was generated and obtained for a range of distances. To obtain data that corresponds to real-world scenarios, the IoT simulator incorporated the findings of the study into monitorability of IoT devices. Accordingly, mains-powered, static IoT devices were configured to have a maximum monitorable range of 60m and battery-powered simulations were configured to have a maximum monitorable range of 45m. Initial experiments carried out using the 3-D IoT simulator

involved the simulation of internal IoT devices' networks with nodes in star formation.

Figure 7.1 is the 3-D view generated by the IoT simulator for a star network scenario with 3 static IoT devices and 16 mobile IoT devices.

Figure 7.1

Simulation of Star Network with 3 Static and 16 Mobile IoT Devices



Subsequent experiments involved the simulation of internal IoT devices' networks with nodes in mesh formation. To collect the data required for a robust study into the discoverability aspect of IoT devices, the IoT simulator was configured to simulate internal IoT network formations using a different number of IoT devices for every simulation. The IoT simulator was also configured to randomise the distance between

the devices that formed datalinks in a formation. Furthermore, to generate data that corresponds to real-world scenarios, the IoT simulator confined the star and mesh formations of IoT devices generated to a grid that was scaled to match the floor area of homes built in NZ. All formations generated by the IoT simulator were confined to a floor area of 160sqm, which is marginally more than the 158sqm floor area of homes built in recent years (Stats NZ, 2020). The floor area was adjusted by 1% to improve readability of the grid.

The simulator further confined the star and mesh formations of IoT devices generated to a grid height scaled to represent 2m from the floor of a single-storied building. All distances for which data was obtained were selected based on the monitorability of IoT devices with 802.15.4 radio. For the simulator to generate data for the selected range of distances, estimations by the simulator considered all selected distances as relative to the centre of the 3-D grid that the IoT simulator utilised for plotting IoT devices. This also ensured the data obtained for each of the selected distances related to equidistant locations from the centre of a target environment.

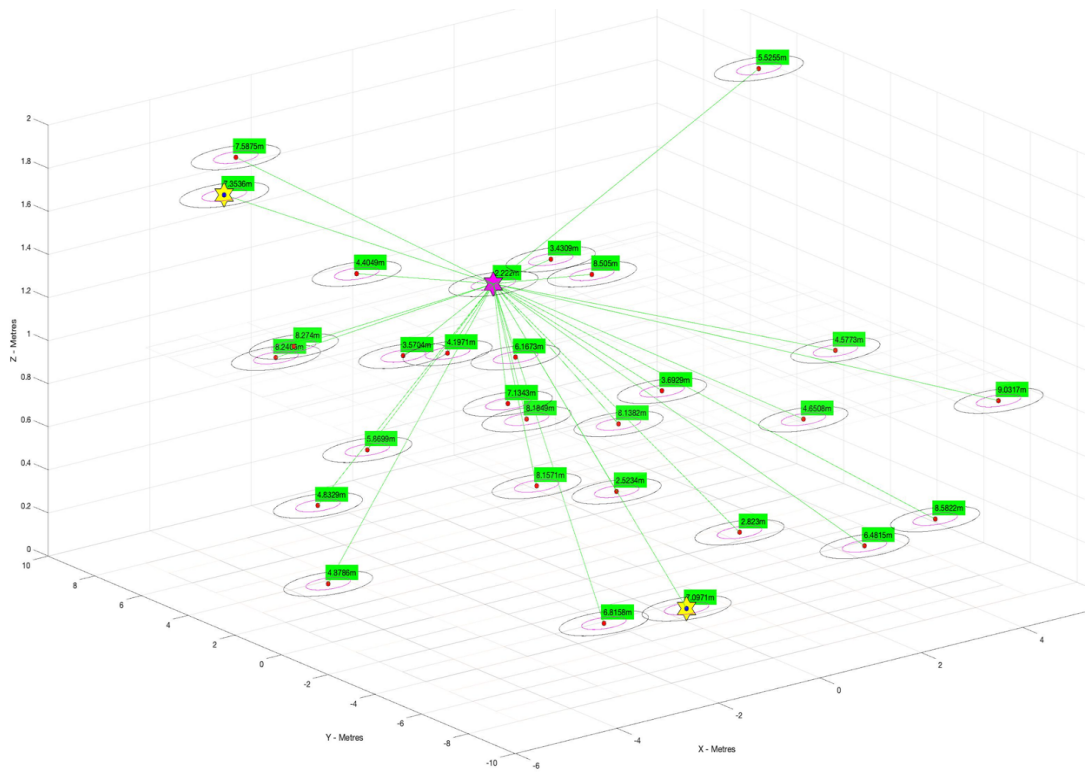
To generate data suitable for the study into IoT discoverability, the simulator primarily checked whether each of the selected distance is within monitorable range of the IoT devices that formed a network. For this, the simulator estimated relative distance of every IoT device from the centre of the target environment. To estimate the relative distance of every IoT device from the centre, the simulator computed the Euclidean distance between the Cartesian coordinates of the point at the centre of the 3-D grid and the Cartesian coordinates of every IoT device plotted on the grid. Then, the simulator factored the estimated relative distance of every IoT device to calculate

whether the selected distances are within monitorable range of the plotted IoT devices.

Figure 7.2 shows the relative distance of 3 static IoT devices and 26 mobile IoT devices from the centre of the grid utilised by the IoT simulator to simulate star and mesh formations of IoT devices. 1 out of the 3 static IoT devices present is represented by a magenta star to distinguish the PAN coordinator amongst them. The other static IoT devices present are represented by a yellow star. All mobile IoT devices are represented by red dots.

Figure 7.2

Relative Distance of 29 IoT Devices from Centre of Grid



The data obtained for the selected distances to every internal IoT network formation that was simulated was catalogued according to network topology and reviewed prior to analysis.

7.2.1 Star Topology

To obtain data specific to star networks, the 3-D IoT simulator was utilised to simulate 25 internal IoT devices' network scenarios, each with a different number of static and mobile IoT devices in star formation. The datalinks of a star network scenario spawned by the simulator were formed between one static device and all other static and mobile IoT devices of that scenario. Table 7.1 lists the total count of IoT devices and the specific configuration of IoT devices that each of the 25 star network scenarios comprised.

Table 7.1

IoT Devices Configuration of Star Network Scenarios

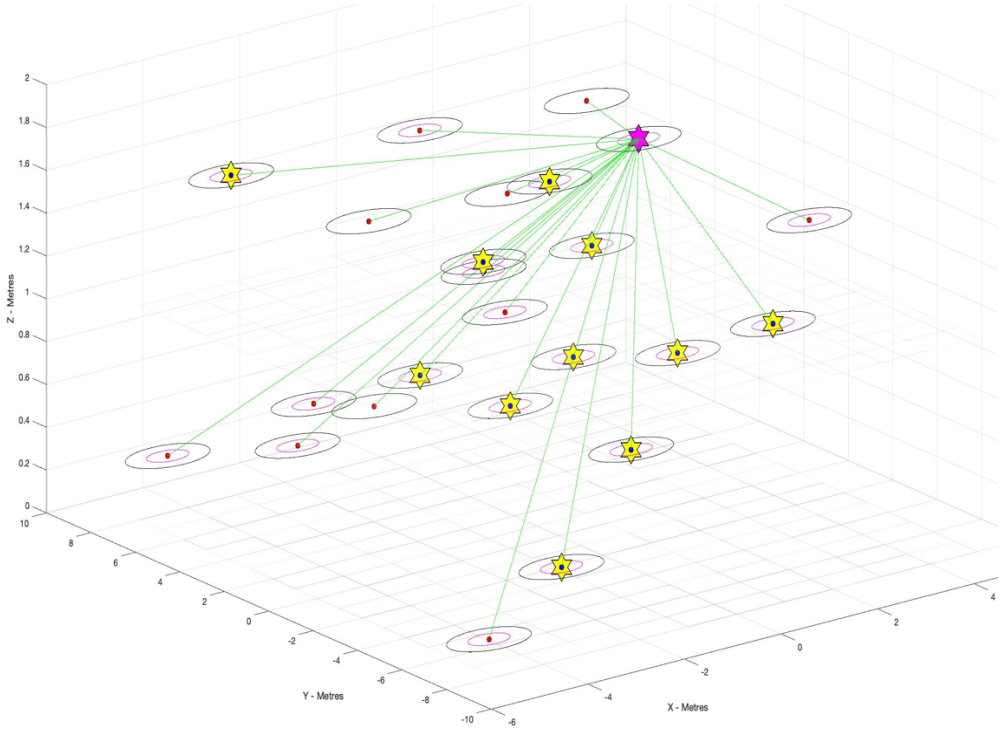
IoT Device Count	Total Static	Total Mobile
31	10	21
28	11	17
24	12	12
15	13	2
33	13	20
36	14	22
43	17	26
39	19	20
37	5	32
40	20	20
41	21	20
48	23	25
31	25	6
46	27	19
44	31	13
16	3	13
29	3	26
34	3	31
12	4	8
17	4	13
14	5	9
18	7	11
22	8	14
20	9	11
26	9	17

For each star network that was simulated, the simulator computed the number of IoT devices that may be monitored and the number of IoT devices that may be discovered for a range of distances. To identify the IoT devices of a star network that may be discovered, the simulator additionally factored the devices that formed datalinks with the devices that may be monitored. For every star network simulated, the IoT simulator obtained data for distances as near as 10m and as far as 70m, with a 10m difference between two consecutive distances. The simulator also generated visual representations of the data that was obtained for each scenario.

Figure 7.3 shows the image generated by the simulator for a star network scenario with 12 static and 12 mobile devices where the simulator computed the number of IoT devices that may be monitored and the number of IoT devices that may be discovered from 50m.

Figure 7.3

Image of Star Network Scenario with 24 IoT devices for 50m Range

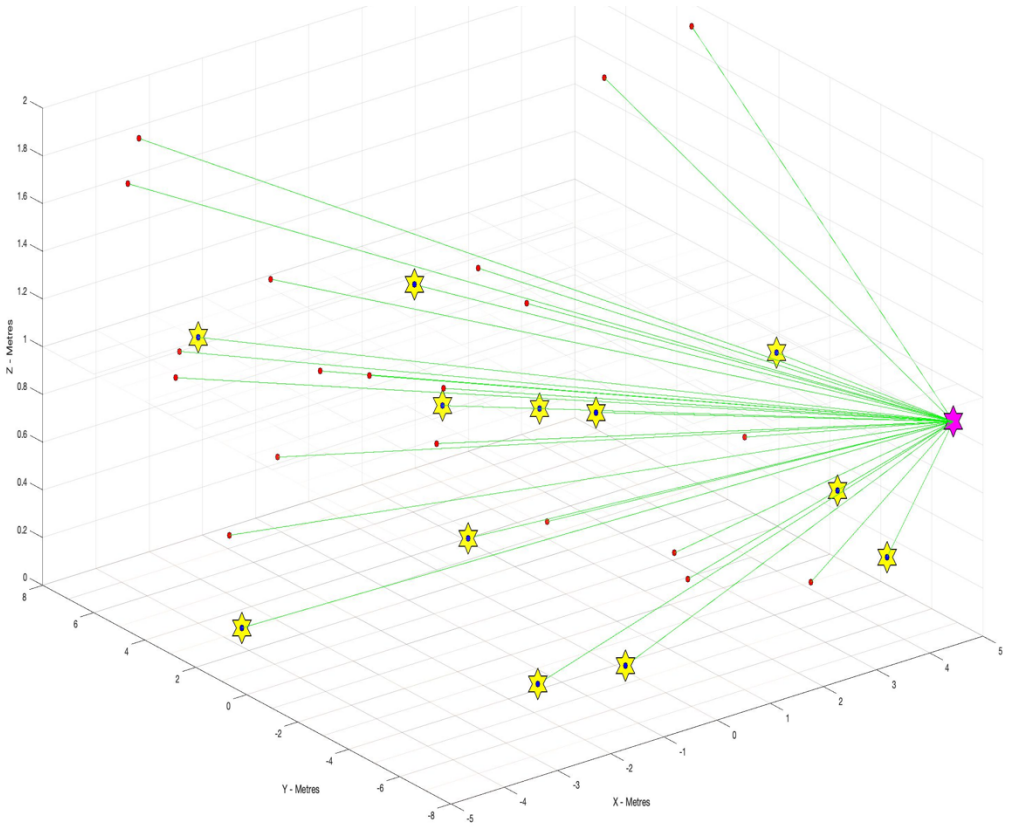


To differentiate the devices in each scenario, the generated images showed rings around devices. All devices that may be monitored and discovered were differentiated from the devices that may be discovered but not monitored. Devices that may be monitored and discovered were represented by 2 coloured rings whereas devices that may be discovered but not monitored were represented by a single ring.

Figure 7.4 shows the image generated by the simulator for a star network scenario with 13 static IoT devices and 20 mobile IoT devices where the simulator computed the number of IoT devices that may be monitored and the number of IoT devices that may be discovered from 70m. The image generated for this scenario shows no rings as no device may be discovered or monitored.

Figure 7.4

Image of Star Network Scenario with 33 IoT devices for 70m Range



Trends in data across the star network scenarios, each with a different configuration of IoT devices, showed that 100% of devices in star formation may be monitored and discovered from 10m range. Trends in data that the simulator obtained for ranges beyond 10m showed that 100% of devices in star formation may also be monitored and discovered from within and as far as 40m.

Table 7.2 compares the percentage of each device type that may be monitored from a 50m range.

Table 7.2

Star Network Configuration Discoverable from 50m Range

Static Devices	Mobile Devices	% Static in Range	% Mobile in Range	% Static Discoverable	% Mobile Discoverable
10	21	100	52.38	100	100
11	17	100	47.06	100	100
12	12	100	66.67	100	100
13	2	100	50.00	100	100
13	20	100	55.00	100	100
14	22	100	50.00	100	100
17	26	100	53.85	100	100
19	20	100	50.00	100	100
5	32	100	62.50	100	100
20	20	100	55.00	100	100
21	20	100	50.00	100	100
23	25	100	72.00	100	100
25	6	100	66.67	100	100
27	19	100	57.89	100	100
31	13	100	69.23	100	100
3	13	100	69.23	100	100
3	26	100	57.69	100	100
3	31	100	45.16	100	100
4	8	100	75.00	100	100
4	13	100	53.85	100	100
5	9	100	55.56	100	100
7	11	100	45.45	100	100
8	14	100	42.86	100	100
9	11	100	36.36	100	100
9	17	100	64.71	100	100

The table further compares the percentage of each device type that may be discovered from 50m range for each of the 25 star network scenarios simulated. Trends in data obtained for 50m range showed that 100% of devices in star formation may be discovered but not monitored. Data across the scenarios showed that 100% of the mobile IoT devices may be discovered but not monitored from 50m range.

Trends in data across the star network scenarios showed that 100% of devices in star formation may be discovered but not monitored from 60m range. Data showed that none of the mobile IoT devices of a star network, all of which may be discovered from 60m range, may be monitored from 60m range. Further, the trends in data across the star network scenarios showed that none of the IoT devices in star formation may be monitored or discovered from 70m range.

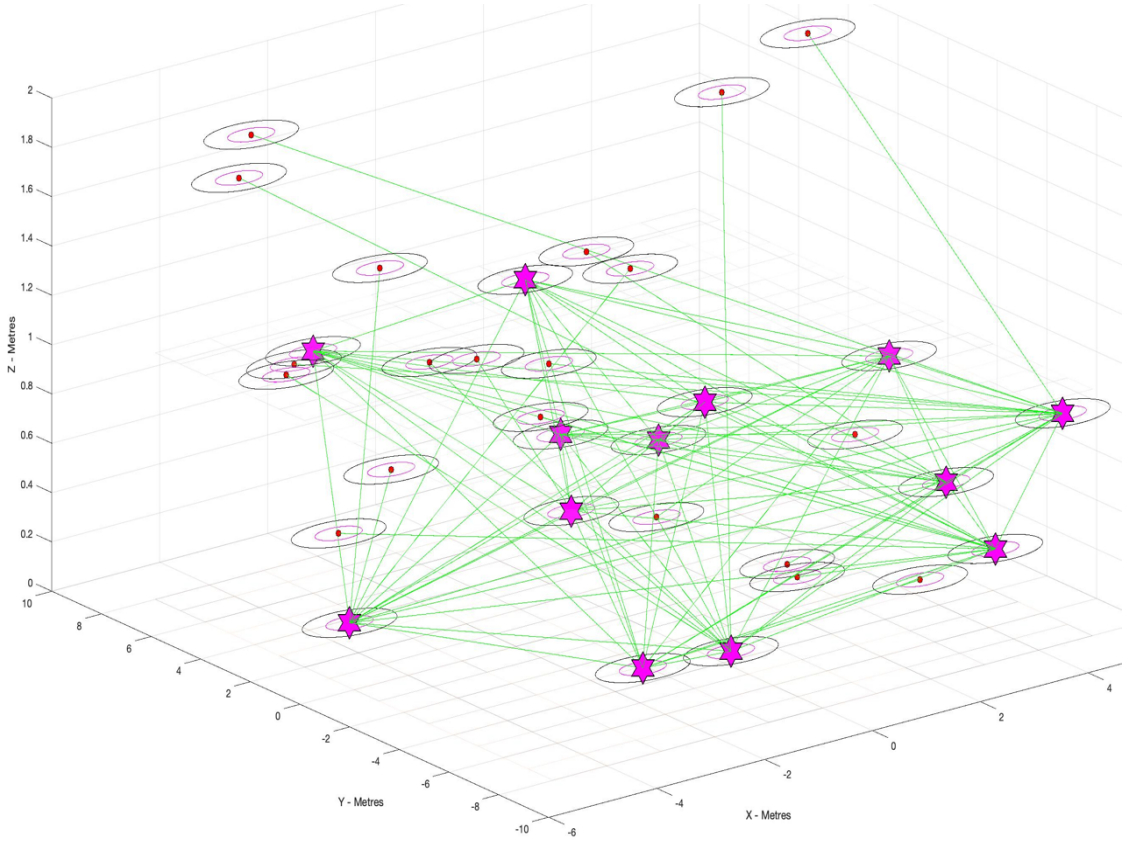
7.2.2 Mesh Topology

To obtain data specific to mesh networks, the 3-D IoT simulator was further utilised to simulate 25 mesh formations of IoT devices. The mesh scenarios spawned by the IoT simulator combined the same configuration of IoT devices that was combined for the simulated star scenarios. In contrast to the datalinks of the star network scenarios, the datalinks of every mesh network scenario spawned by the simulator were formed between all static devices and between the static and mobile IoT devices. For each mesh network scenario, the simulator computed the number of IoT devices that may be monitored and the number of IoT devices that may be discovered for distances as near as 10m and as far as 70m.

Figure 7.5 shows the image generated by the simulator for the mesh network scenario with 13 static IoT devices and 20 mobile IoT devices when observed from 40m range.

Figure 7.5

Image of Mesh Network Scenario with 33 IoT devices from 40m range



Trends in data across the mesh network scenarios showed that 100% of devices in mesh formation may be monitored and discovered from 10m range. Trends in data that the simulator obtained for ranges beyond 10m showed that 100% of devices in mesh formation may be monitored and discovered from within and as far as 40m.

Table 7.3 compares the percentage of each device type that may be monitored from a 50m range for each of the 25 mesh network scenarios simulated.

Table 7.3

Mesh Network Configuration Discoverable from 50m Range

Static Devices	Mobile Devices	% Static in Range	% Mobile in Range	% Static Discoverable	% Mobile Discoverable
10	21	100	52.38	100	100
11	17	100	47.06	100	100
12	12	100	66.67	100	100
13	2	100	50.00	100	100
13	20	100	55.00	100	100
14	22	100	50.00	100	100
17	26	100	53.85	100	100
19	20	100	50.00	100	100
5	32	100	62.50	100	100
20	20	100	55.00	100	100
21	20	100	50.00	100	100
23	25	100	72.00	100	100
25	6	100	66.67	100	100
27	19	100	57.89	100	100
31	13	100	69.23	100	100
3	13	100	69.23	100	100
3	26	100	57.69	100	100
3	31	100	45.16	100	100
4	8	100	75.00	100	100
4	13	100	53.85	100	100
5	9	100	55.56	100	100
7	11	100	45.45	100	100
8	14	100	42.86	100	100
9	11	100	36.36	100	100
9	17	100	64.71	100	100

The table further compares the percentage of each device type that may be discovered through radio signals of devices that may be monitored from 50m range. Trends in data across the mesh network scenarios showed that 100% of devices in mesh formation may be discovered but not monitored from 50m range. Data pointed out that 100% of the mobile IoT devices may be discovered but not monitored from 50m range. Trends in data across the mesh network scenarios showed that 100% of devices in mesh formation may be discovered but not monitored from 60m range. Data showed that none of the mobile devices of a mesh network, all of which may be

discovered from 60m range, may be monitored from 60m range. Further, the trends in data across the mesh network scenarios showed that none of the IoT devices in mesh formation may be monitored or discovered from 70m range.

7.3 Discoverability Study Results

7.3.1 Star Topology

Table 7.4 shows the data obtained for all simulated star networks with respect to the devices that may be discovered from ranges 10m to 70m.

Table 7.4

Star Network Devices Discoverable from 10m-70m Ranges

IoT Device Count	10m – 60m	70m
31	100%	0%
28	100%	0%
24	100%	0%
15	100%	0%
33	100%	0%
36	100%	0%
43	100%	0%
39	100%	0%
37	100%	0%
40	100%	0%
41	100%	0%
48	100%	0%
31	100%	0%
46	100%	0%
44	100%	0%
16	100%	0%
29	100%	0%
34	100%	0%
12	100%	0%
17	100%	0%
14	100%	0%
18	100%	0%
22	100%	0%
20	100%	0%
26	100%	0%

The data obtained for the 25 star network scenarios that corresponds to the IoT devices that may be discovered from 10m to 70m was collated for analysis. The data was analysed to determine the minimum configuration, the iota (I) configuration amongst all IoT devices in a star network, the radio signals of which will enable

100% discovery of the IoT devices is star formation. The trends in data indicated that none of the IoT devices in a star formation may be discovered from 70m range. The data, however, indicated 100% of the IoT devices in a star formation may be discovered through the radio signals of IoT devices that may be monitored from 10m to 60m ranges. So, the data obtained for 25 star networks that corresponds to the configuration of devices that may be monitored from 10m to 60m was examined.

Table 7.5 consolidates the data related to the configuration of IoT devices that was obtained for each scenario across 25 star networks. The configuration of IoT devices in star formation is represented by the percentage of static and mobile IoT devices.

Table 7.5

Star Network Configurations across 100% Discoverable Range

IoT Device Count	10-40m		50m		60m	
	% Static	% Mobile	% Static	% Mobile	% Static	% Mobile
31	100	100	100	52.38	100	0
28	100	100	100	47.06	100	0
24	100	100	100	66.67	100	0
15	100	100	100	50.00	100	0
33	100	100	100	55.00	100	0
36	100	100	100	50.00	100	0
43	100	100	100	53.85	100	0
39	100	100	100	50.00	100	0
37	100	100	100	62.50	100	0
40	100	100	100	55.00	100	0
41	100	100	100	50.00	100	0
48	100	100	100	72.00	100	0
31	100	100	100	66.67	100	0
46	100	100	100	57.89	100	0
44	100	100	100	69.23	100	0
16	100	100	100	69.23	100	0
29	100	100	100	57.69	100	0
34	100	100	100	45.16	100	0
12	100	100	100	75.00	100	0
17	100	100	100	53.85	100	0
14	100	100	100	55.56	100	0
18	100	100	100	45.45	100	0
22	100	100	100	42.86	100	0
20	100	100	100	36.36	100	0
26	100	100	100	64.71	100	0

Across all star network scenarios, data showed the configuration of a star network that may be monitored from 10m to 40m ranges as comparable to the actual configuration. The data, however, showed the configuration of a star network that may be monitored from 50m to 60m ranges as not comparable to the actual configuration.

Table 7.6 further shows the change in star network configurations that may be monitored as the distance increased.

Table 7.6

Change in Star Network Configurations across Discoverable Range

IoT Device Count	10-40m		50m		60m	
	% Static	% Mobile	% Static	% Mobile	% Static	% Mobile
31	-	-	-	47.62	-	100
28	-	-	-	52.94	-	100
24	-	-	-	33.33	-	100
15	-	-	-	50.00	-	100
33	-	-	-	45.00	-	100
36	-	-	-	50.00	-	100
43	-	-	-	46.15	-	100
39	-	-	-	50.00	-	100
37	-	-	-	37.50	-	100
40	-	-	-	45.00	-	100
41	-	-	-	50.00	-	100
48	-	-	-	28.00	-	100
31	-	-	-	33.33	-	100
46	-	-	-	42.11	-	100
44	-	-	-	30.77	-	100
16	-	-	-	30.77	-	100
29	-	-	-	42.31	-	100
34	-	-	-	54.84	-	100
12	-	-	-	25.00	-	100
17	-	-	-	46.15	-	100
14	-	-	-	44.44	-	100
18	-	-	-	54.55	-	100
22	-	-	-	57.14	-	100
20	-	-	-	63.64	-	100
26	-	-	-	35.29	-	100

This view points out that changes to the configuration of devices that may be monitored were due to the changes in percentage of mobile IoT devices that may be

monitored. Data across the star network scenarios show that the percentage of mobile IoT devices that may be observed increasingly decreased from 50m to 60m. Across all star network scenarios, the change in the percentage of mobile IoT devices that may be monitored from 60m range is more pronounced compared to the change in the percentage of mobile IoT devices that may be monitored from 50m range. Remarkably, data across the star network scenarios show an invariable decrease of 100% in the percentage of mobile IoT devices that may be monitored from 60m.

The results suggest that static nodes of a star network constitute the minimum configuration, the I, from which radio signals are required to discover every IoT device that constitutes an internal IoT devices' network. Although trends in data obtained showed 100% of IoT nodes in a star network may be discovered from ranges as near as 10m and as far as 60m, the analysis points out that radio signals of mobile IoT devices are not required to discover any of the static or mobile devices that constitute a star network. Whilst 100% of mobile IoT devices in a star network may be monitored from as near as 10m and as far 40m, decreases in mobile IoT devices that may be monitored did not appear to have any impact on the configuration of devices that may be discovered. The analysis points out that all static and mobile devices may be discovered when at least the static IoT devices may be monitored. The results further point out that a star network may be observed from as near as 50m and as far as 60m range to generate an accurate model, including all static and mobile IoT devices in star formation.

7.3.2 Mesh Topology

The steps followed to analyse the data obtained for the 25 star network scenarios were repeated to analyse the data obtained for the 25 mesh network scenarios. The data

obtained for the 25 mesh network scenarios that corresponds to the IoT devices that may be discovered from 10m to 70m was also analysed to determine the minimum configuration, the I, amongst all IoT devices in a mesh network, the radio signals of which will enable 100% discovery of the IoT devices in mesh formation.

Table 7.7 shows the data obtained for the mesh network scenarios that corresponds to the devices that may be discovered.

Table 7.7

Mesh Network Devices Discoverable from 10m-70m Ranges

IoT Device Count	10m – 60m	70m
31	100%	0%
28	100%	0%
24	100%	0%
15	100%	0%
33	100%	0%
36	100%	0%
43	100%	0%
39	100%	0%
37	100%	0%
40	100%	0%
41	100%	0%
48	100%	0%
31	100%	0%
46	100%	0%
44	100%	0%
16	100%	0%
29	100%	0%
34	100%	0%
12	100%	0%
17	100%	0%
14	100%	0%
18	100%	0%
22	100%	0%
20	100%	0%
26	100%	0%

The trends in data indicated that none of the IoT devices in a mesh formation may be discovered through the radio signals of IoT devices that may be monitored from 70m range. Data, however, indicated 100% of the IoT devices in a mesh formation may be

discovered through the radio signals of IoT devices that may be monitored from 10m to 60m ranges. So, the data obtained for 25 mesh networks that corresponds to the configuration of devices that may be monitored from 10m to 60m ranges was examined. Table 7.8 consolidates the data related to the configuration of IoT devices that was obtained for each scenario across 25 mesh networks. The configuration of IoT devices in mesh formation is represented by the percentage of static and mobile IoT devices.

Table 7.8

Mesh Network Configurations across 100% Discoverable Range

IoT Device Count	10-40m		50m		60m	
	% Static	% Mobile	% Static	% Mobile	% Static	% Mobile
31	100	100	100	52.38	100	0
28	100	100	100	47.06	100	0
24	100	100	100	66.67	100	0
15	100	100	100	50.00	100	0
33	100	100	100	55.00	100	0
36	100	100	100	50.00	100	0
43	100	100	100	53.85	100	0
39	100	100	100	50.00	100	0
37	100	100	100	62.50	100	0
40	100	100	100	55.00	100	0
41	100	100	100	50.00	100	0
48	100	100	100	72.00	100	0
31	100	100	100	66.67	100	0
46	100	100	100	57.89	100	0
44	100	100	100	69.23	100	0
16	100	100	100	69.23	100	0
29	100	100	100	57.69	100	0
34	100	100	100	45.16	100	0
12	100	100	100	75.00	100	0
17	100	100	100	53.85	100	0
14	100	100	100	55.56	100	0
18	100	100	100	45.45	100	0
22	100	100	100	42.86	100	0
20	100	100	100	36.36	100	0
26	100	100	100	64.71	100	0

Across all mesh network scenarios, data showed the configuration of a mesh network that may be monitored from 10m to 40m ranges as comparable to the actual

configuration. The data, however, showed the configuration of a mesh network that may be monitored from 50m to 60m ranges as not comparable to the actual configuration.

Table 7.9 further shows the change in mesh network configurations that may be monitored as the distance increased.

Table 7.9

Change in Mesh Network Configurations across Discoverable Range

IoT Device Count	10-40m		50m		60m	
	% Static	% Mobile	% Static	% Mobile	% Static	% Mobile
31	-	-	-	47.62	-	100
28	-	-	-	52.94	-	100
24	-	-	-	33.33	-	100
15	-	-	-	50.00	-	100
33	-	-	-	45.00	-	100
36	-	-	-	50.00	-	100
43	-	-	-	46.15	-	100
39	-	-	-	50.00	-	100
37	-	-	-	37.50	-	100
40	-	-	-	45.00	-	100
41	-	-	-	50.00	-	100
48	-	-	-	28.00	-	100
31	-	-	-	33.33	-	100
46	-	-	-	42.11	-	100
44	-	-	-	30.77	-	100
16	-	-	-	30.77	-	100
29	-	-	-	42.31	-	100
34	-	-	-	54.84	-	100
12	-	-	-	25.00	-	100
17	-	-	-	46.15	-	100
14	-	-	-	44.44	-	100
18	-	-	-	54.55	-	100
22	-	-	-	57.14	-	100
20	-	-	-	63.64	-	100
26	-	-	-	35.29	-	100

This view points out that changes to the configuration of IoT devices that may be monitored were due to the changes in the percentage of mobile IoT devices that may

be monitored. Data across the mesh network scenarios show that the percentage of mobile IoT devices that may be observed increasingly decreased from 50m to 60m. Across all mesh network scenarios, the change in the percentage of mobile IoT devices that may be monitored from 60m range is more pronounced compared to the change in the percentage of mobile IoT devices that may be monitored from 50m range. Remarkably, data across the mesh network scenarios show an invariable decrease of 100% in the percentage of mobile IoT devices that may be monitored from 60m.

The results suggest that static nodes of a mesh network constitute the minimum configuration, the I, from which radio signals are required to discover every IoT device that constitutes an internal IoT devices' network. Although trends in data obtained showed 100% of IoT nodes in a mesh network may be discovered from ranges as near as 10m and as far as 60m, the analysis points out that radio signals of mobile IoT devices are not required to discover any of the static or mobile devices that constitute a mesh network. Whilst 100% of mobile IoT devices in a mesh network may be monitored from as near as 10m and as far 40m, decreases in mobile IoT devices that may be monitored did not appear to have any impact on the configuration of devices that may be discovered. The analysis points out that all static and mobile devices may be discovered when at least the static IoT devices may be monitored. The results further point out that a mesh network may be observed from as near as 50m and as far as 60m range to generate an accurate model, including all static and mobile IoT devices in mesh formation.

7.4 Conclusion

This chapter covered the details of the study into discoverability of IoT devices, which examined star and mesh configurations of IoT devices. The study utilised a custom-built 3-D IoT simulator to generate star and mesh configurations of IoT devices and obtain data for ranges informed by IoT monitorability study. The data obtained using the simulator included percentage of static and mobile IoT devices that may be monitored and discovered from as near as 10m to as far as 70m. Analysis of the trends in data that correspond to the IoT devices that may be monitored and discovered determined the smallest configuration of IoT devices, the I, amongst all the IoT devices that will enable 100% discovery of the IoT devices of a network. The study found that the static devices of an internal IoT devices' network, where devices have formed datalinks in star or mesh formation, constitute the I of that network. The study which found that both static and mobile devices of an internal IoT devices' network may be discovered from the static devices, also found that every IoT device with 802.15.4 radio may be discovered from as near as 50m and as far as 60m from a target IoT environment.

Chapter 8

DISCUSSION

8.1 Introduction

The next stage of this work explored developing specific methods for the construction of a framework with which investigators may search for IoT devices after having obtained evidence of their locations. This initially involved an evaluation of the model of the approach to locate and track IoT devices, which is explained in Section 4.3.4, utilising the findings of the study into IoT monitorability, traceability and discoverability, covered in Chapters 5, 6 and 7 respectively. Following validation of the concept of harnessing the communications between IoT devices, the questions covered in Section 4.4.5 guided the development of several methods and models that investigators may apply in order to discover, determine and locate IoT devices. The results available from the study into IoT monitorability, traceability and discoverability primarily informed the development of applicable methods. Additional 3-D simulation experiments were carried out with the IoT simulator to support the development of applicable methods. The use of the IoT simulator was extended to understand if and how the distance and locations from which communications are captured will affect the accuracy with which locations of IoT devices may be determined. This chapter covers an appraisal of the model for monitoring and modelling IoT devices based on the criteria of evaluation, which is explained in Section 4.3.5. In this chapter, the methods and models required to systematically capture and examine radio signals of an IoT environment for spatial modelling are also defined. In all, the system defined for spatial modelling of an IoT environment from the radio signals of that environment consists of 3 stages.

8.2 Evaluation and Definition of IoT Monitoring and Modelling System

The effectiveness of the model for monitoring and modelling IoT devices, which is explained in Section 4.3.4, is discussed based on the findings of the assessment of aspects identified as the core criteria for evaluation. Each stage of the model for monitoring and modelling IoT devices is separately discussed as each of the three different aspects that form the criteria corresponds to a specific stage. Building on the results of the assessments of the three aspects, the discussion also covers the methods applicable for each stage of the monitoring and modelling system.

8.2.1 Initiation Stage – Observing IoT Device Communications

The criterion of assessment that corresponds to this stage of the modelling process is the discoverability of IoT devices, the study of which is covered in Chapter 7. The study into IoT discoverability, which explored the possibility of discovering IoT devices before the IoT devices are monitorable, analysed data obtained from star and mesh network scenarios. As expected, the study into IoT discoverability found that IoT nodes are discoverable for accurate modelling of a network provided that at least one node of every ad-hoc connection is monitorable. The trends in data obtained using a 3-D IoT simulator showed that 100% of the nodes of a network, where static and mobile devices have formed datalinks in star or mesh formation, may be discovered from radio signals if at least the static nodes of a network are monitored. However, trends in data obtained point out that the peripheries of a target IoT environment from where at least the static IoT devices may be monitored for an accurate modelling is limited to between 50m and 60m. Whilst the findings of the study of the discoverability aspect support observing IoT devices from the peripheries of an environment, this first stage of monitoring and modelling an IoT environment

requires a methodical approach. The following approach provides for sensing and obtaining communications between IoT devices of a target environment.

8.2.1.1 Ascertain Low-Rate Communications Environment

The recommended first step is to identify the low-rate, short-range wireless technologies. This step ascertains the presence of a low-rate wireless communications environment and provides the basis to continue with modelling of the target environment. The first step requires the setup and deployment of suitable modules to perform as outdoor, monitoring nodes. Amongst the modules available for Zigbee compliant platforms, the NXP Kinetis USB-KW24D512 performed well as an outdoor, mobile monitoring node. Amongst the modules available for Z-Wave compliant platforms, the Silicon Labs Z-Wave UZB module performed well as an outdoor, mobile monitoring node. For other IoT platforms, such as DigiMesh, modules suitable for the purpose of monitoring are required.

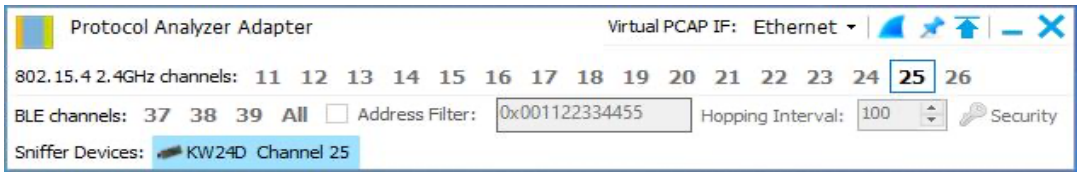
To identify the low-rate, short-range wireless technologies operating within a specific environment, deploy a compliant module to monitor the target environment initially from a location that is 5 to 10m away from target. The ID of every network detected from 5 to 10m away should be noted before moving the module further away. Monitor the target from two more locations further away to eliminate networks operating in locations neighbouring a target. For IEEE 802.15.4 platforms, where periodic communications of devices have a maximum monitorable range of 60m, the recommendation is to move the monitoring module to locations 35 to 45m away and 50m to 60m away. Then, the ID of every network detected from the two additional locations must be noted and compared with the IDs detected by the module 5 to 10m away from target. The ID of every network that the module detected from all 3

locations should then be noted. Some modules require the radio channel to be manually selected to enable the module to sense network traffic.

Figure 8.1 shows the manual selection of channel 25 using the NXP Kinetis Protocol Analyzer Adapter for NXP's Kinetis USB-KW24D512 module to monitor the specified channel for network traffic.

Figure 8.1

Channel Selection using NXP Kinetis Protocol Analyzer Adapter



Depending on the module in use, manual selection of radio channels must be repeated for every location the module is deployed to sense network traffic from all the channels available to IoT platforms for operation. The detection step will also identify the channels that are not in use. To identify IEEE 802.15.4 networks, the recommended duration of monitoring at each of the 3 monitoring locations is 40 seconds per channel. The duration specified is based on the findings of the study of IoT monitorability that is covered in Section 5.3.3. This method of ascertaining the low-rate communications environment also provides inputs required to continue with the reconstruction process.

8.2.1.2 Obtain Real-Time Low-rate Network Traffic

The next step of observing IoT device communications obtains the real-time traffic between mobile and static devices of a heterogeneous IoT environment. This step, therefore, requires that hardware and software resources which are suitable for the purpose of capturing the disparate traffic are deployed. Based on the results of the study of IoT discoverability covered in section 7.3, which showed that 100% of the

devices in an IoT environment may be discovered if the static devices of an environment are monitored from between 50m and 60m, a deployment strategy that is aimed at covering the static devices will obtain real-time traffic from a heterogeneous IoT environment and generate the data required to discover and locate IoT devices. For simultaneous monitoring of a target environment, this will require multiple outdoor, mobile modules to be deployed at the peripheries of a target environment to cover all the vantage points from where communications of static sources are detected.

However, the accuracy of the locations of static and mobile IoT devices will depend on the configuration of monitoring nodes that observe an IoT environment. This finding is based on further examination of the networks that were simulated to study IoT discoverability. To understand the factors that affect location accuracy, locations within internal IoT devices' networks from where nodes transmitted radio signals were observed from a select range of vantage points through further simulations. To obtain data that supports robust analysis, two combinations of monitoring nodes were utilised for every node across the star and mesh networks. The first combination utilised 2 monitoring nodes at certain distances across two perpendicular axes corresponding to each node. The second combination utilised 3 monitoring nodes at certain distances across three pair-wise perpendicular axes corresponding to each node.

The distances from which the nodes were observed to obtain data and study the factors that affect location accuracy were chosen based on the monitorability of IoT devices with integrated 802.15.4 radio. The scenarios simulated provided insight into the additional nodes around a target node that may be observed between the

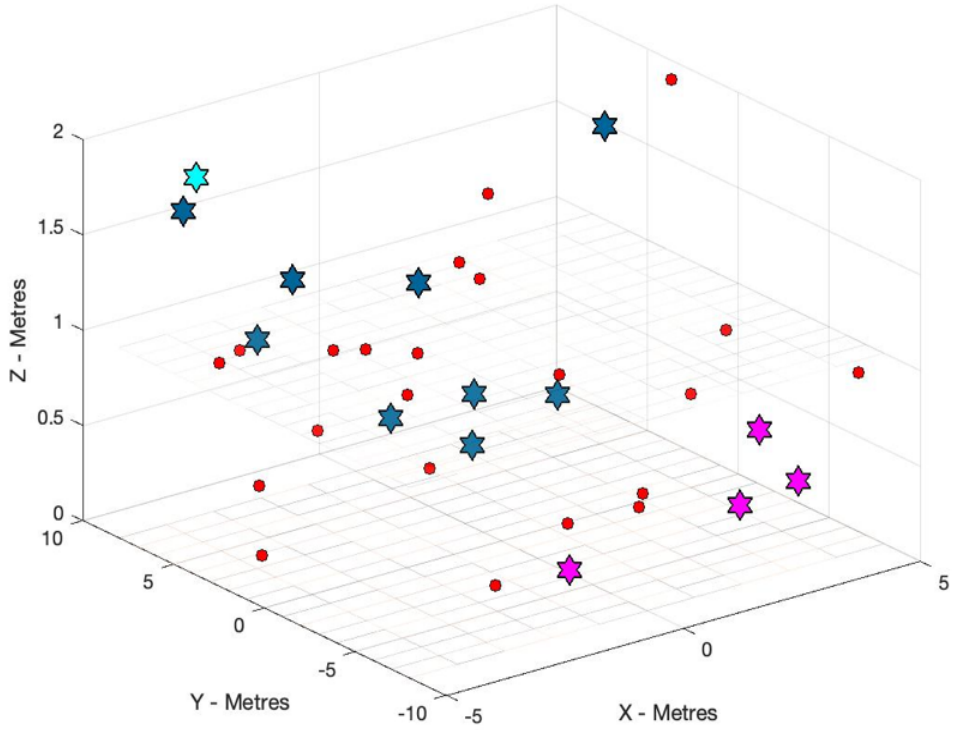
monitoring nodes and the additional nodes that may be commonly observed by the monitoring nodes from their different vantage points. From amongst the scenarios for which data was obtained, screenshots of a few are presented and explained. The following legend differentiates the nodes in each scenario.

- *Static Node - Target*
- *Static Node – Commonly Observed*
- *Static Node*
- *Mobile Node*

The scenarios presented pertain to an IoT environment that comprised of 36 IoT devices, including 14 static IoT devices. Figure 8.2 shows a scenario that utilised 2 monitoring nodes located 50m away from a static node across its X and Y axes.

Figure 8.2

Scenario of 2 Monitoring Nodes 50m away from Target

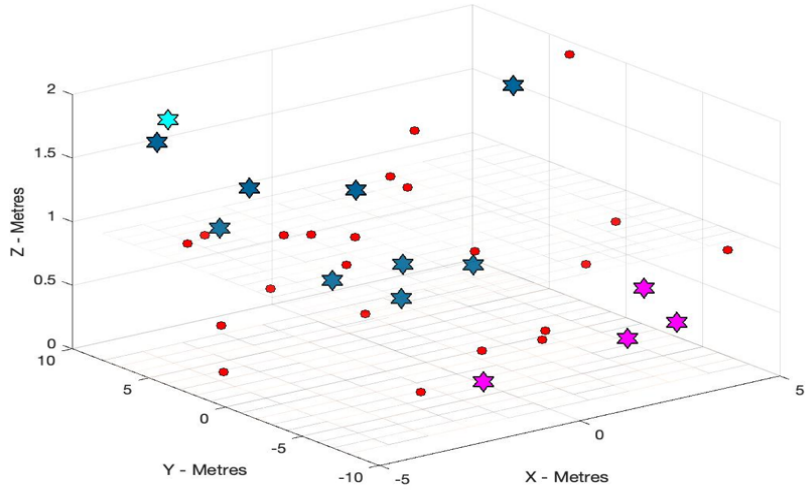


The image generated for this scenario show 9 static nodes are common amongst all the additional static nodes that may be monitored by each of the 2 monitoring nodes.

Figure 8.3 shows a scenario that utilised 3 monitoring nodes located 50m away from a static node across its X, Y and Z axes.

Figure 8.3

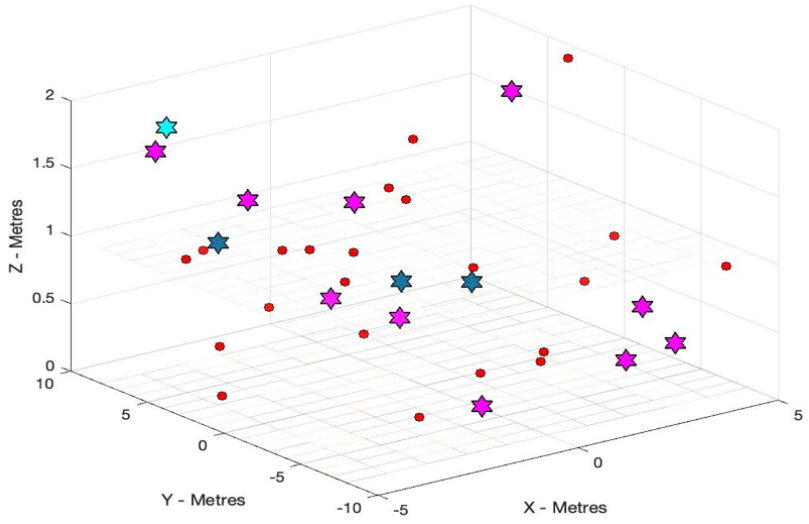
Scenario of 3 Monitoring Nodes 50m away from Target



The image generated for this scenario also show 9 static nodes are common amongst all the additional static nodes that may be monitored by each of the 3 monitoring nodes. Figure 8.4 shows a scenario that utilised 2 monitoring nodes located 60m away from a static node across its X and Y axes.

Figure 8.4

Scenario of 2 Monitoring Nodes 60m away from Target

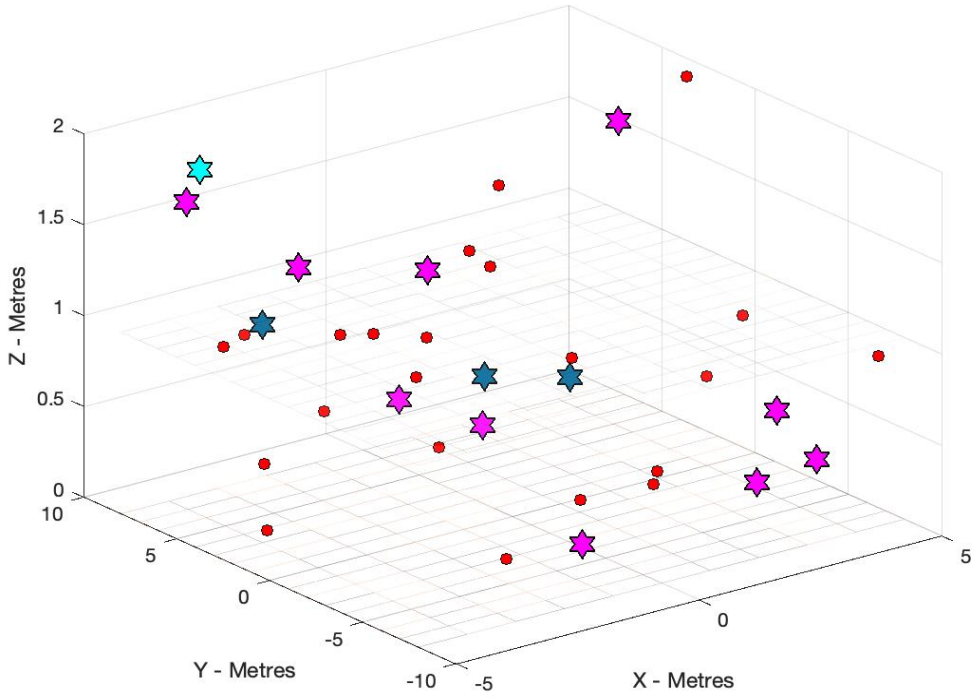


The image generated for this scenario show 3 static nodes as common amongst all the additional static nodes that may be monitored by each of the 2 monitoring nodes.

Figure 8.5 shows a scenario that utilised 3 monitoring nodes located 60m away from a static node across its X, Y and Z axes.

Figure 8.5

Scenario of 3 Monitoring Nodes 60m away from Target



The image generated for this scenario also show 3 static nodes as common amongst all the additional static nodes that may be monitored by each of the 3 monitoring nodes.

The data generated for every scenario that was simulated was catalogued according to the number of monitoring nodes and analysed.

Table 8.1 provides an insight into the additional nodes that may be observed by 2 monitoring nodes from equidistant vantage points across X and Y axes corresponding to a static node.

Table 8.1

Change in Additional Nodes Observed by 2 Nodes from 50 to 60m Range

Static Devices	Mobile Devices	Average of Additional Nodes in Common		Change
		50m	60m	
10	21	8.30	1.60	6.70
11	17	9.27	1.45	7.82
12	12	9.92	4.00	5.92
13	2	11.23	2.77	8.46
13	20	10.62	2.23	8.38
14	22	11.00	2.36	8.64
17	26	15.59	3.53	12.06
19	20	16.74	4.11	12.63
5	32	2.00	0.00	2.00
20	20	16.20	3.55	12.65
21	20	18.86	4.43	14.43
23	25	21.30	5.61	15.70
25	6	21.88	4.64	17.24
27	19	23.67	6.96	16.70
31	13	26.26	5.35	20.90
3	13	3.67	0.67	3.00
3	26	1.67	0.00	1.67
3	31	2.67	1.00	1.67
4	8	3.00	0.50	2.50
4	13	2.75	0.75	2.00
5	9	3.40	1.20	2.20
7	11	5.71	1.71	4.00
8	14	6.63	1.00	5.63
9	11	7.44	3.22	4.22
9	17	7.33	1.78	5.56
Median		**9.27**	**2.23**	**6.70**

Data obtained for vantage points 50m and 60m to every static node across 25 mesh networks was consolidated to analyse the change in additional nodes as the distance of monitoring increased. The median of the data that corresponds to the additional nodes that may be commonly observed by 2 monitoring nodes from vantage points 60m away showed up to 2 nodes in addition to the target static node. The median of the data that corresponds to the additional nodes that may be commonly observed by 2 monitoring nodes from vantage points 50m away showed up to 9 nodes in addition

to the target static node. The trends in data showed considerably more additional nodes may be observed by 2 nodes from a 50m range. The median of the data that corresponds to the change in additional nodes that may be observed suggests that the accuracy of static devices' locations is relatively better when observed with 2 monitoring nodes from vantage points 60m away across 2 perpendicular axes than from vantage points 50m away.

Table 8.2 provides an insight into the additional nodes that may be observed by 3 monitoring nodes from equidistant vantage points across X, Y and Z axes corresponding to a static node.

Table 8.2

Change in Additional Nodes Observed by 3 Nodes from 50 to 60m Range

Static Devices	Mobile Devices	Average of Additional Nodes in Common		Change
		50m	60m	
10	21	7.80	0.40	7.40
11	17	9.18	0.55	8.64
12	12	9.83	0.58	9.25
13	2	11.08	0.54	10.54
13	20	10.23	0.85	9.38
14	22	11.00	0.43	10.57
17	26	14.53	1.00	13.53
19	20	16.47	1.16	15.32
5	32	0.00	0.00	0.00
20	20	16.05	0.90	15.15
21	20	18.48	1.05	17.43
23	25	20.30	1.61	18.70
25	6	21.52	1.12	20.40
27	19	23.07	1.48	21.59
31	13	26.19	2.35	23.84
3	13	1.33	0.00	1.33
3	26	1.67	0.00	1.67
3	31	2.00	0.00	2.00
4	8	2.75	0.00	2.75
4	13	2.50	0.25	2.25
5	9	3.40	0.40	3.00
7	11	5.71	0.57	5.14
8	14	6.25	0.38	5.88
9	11	6.00	0.67	5.33
9	17	7.33	0.33	7.00
Median		**9.18**	**0.55**	**8.64**

Data obtained for vantage points 50m and 60m to every static node across 25 mesh networks was consolidated to analyse the changes. The median of the data that corresponds to the additional nodes that may be commonly observed by 3 monitoring nodes from vantage points 60m away showed up to 1 in addition to the target static node. The median of the data that corresponds to the additional nodes that may be commonly observed by 3 monitoring nodes from vantage points 50m away showed up to 9 additional nodes in addition to the target static node. The trends in data showed considerably more additional nodes may be observed by 3 nodes from a 50m range. The median of the data that corresponds to the change in additional nodes that may be observed suggests that the accuracy of static devices' locations is relatively better when observed by 3 monitoring nodes from vantage points 60m away across 3 pair-wise perpendicular axes than with 2 monitoring nodes from 2 perpendicular axes.

The median of the data that corresponds to the additional nodes that may be commonly observed by 2 monitoring nodes from vantage points 45m away showed up to 13 additional nodes than the target mobile node. The median of the data that corresponds to the additional nodes that may be commonly observed by 2 monitoring nodes from vantage points 35m away showed up to 28 additional nodes than the target mobile node change. The trends in data showed considerably more additional nodes may be observed by 2 nodes from a 35m range. The data related to additional nodes points out that a considerable number of static nodes are amongst the additional nodes observed. The median of the data that corresponds to the change in additional nodes that may be observed suggests that the accuracy of mobile devices' locations is relatively better when observed with 2 monitoring nodes from vantage points 45m away across 2 perpendicular axes than from vantage points 35m away.

Table 8.3 provides an insight into the additional nodes that may be observed by 2 monitoring nodes from equidistant vantage points across X and Y axes corresponding to a mobile node. Data obtained for vantage points 35m and 45m to every mobile node across 25 mesh networks was consolidated to analyse the change in additional nodes as the distance of monitoring increased.

Table 8.3

Change in Additional Nodes Observed by 2 Nodes from 35 to 45m Range

Static Devices	Mobile Devices	Average of Additional Nodes in Common		Change
		35m	45m	
10	21	28.10	13.48	14.62
11	17	25.65	14.18	11.47
12	12	21.67	14.92	6.75
13	2	14.00	12.50	1.50
13	20	30.55	16.25	14.30
14	22	33.68	18.50	15.18
17	26	39.65	22.00	17.65
19	20	36.70	23.55	13.15
5	32	28.16	6.66	21.50
20	20	37.05	23.85	13.20
21	20	38.60	25.50	13.10
23	25	44.32	28.68	15.64
25	6	29.17	25.50	3.67
27	19	43.79	30.58	13.21
31	13	41.77	33.38	8.38
3	13	13.38	5.31	8.08
3	26	25.04	7.85	17.19
3	31	30.35	7.81	22.55
4	8	10.00	5.88	4.13
4	13	15.38	6.54	8.85
5	9	12.67	6.78	5.89
7	11	15.82	8.27	7.55
8	14	19.57	10.07	9.50
9	11	18.73	11.09	7.64
9	17	23.00	11.88	11.12
Median		**28.10**	**13.48**	**11.47**

Table 8.4 provides an insight into the additional nodes that may be observed by 3 monitoring nodes from equidistant vantage points across X, Y and Z axes corresponding to a mobile node. Data obtained for vantage points 35m and 45m to every mobile node across 25 mesh networks was consolidated to analyse the changes.

Table 8.4

Change in Additional Nodes Observed by 3 Nodes from 35 to 45m Range

Static Devices	Mobile Devices	Average of Additional Nodes in Common		Change
		35m	45m	
10	21	28.10	10.86	17.24
11	17	25.65	11.59	14.06
12	12	21.67	12.92	8.75
13	2	14.00	12.50	1.50
13	20	30.55	13.75	16.80
14	22	33.68	15.64	18.05
17	26	39.65	18.50	21.15
19	20	36.70	20.50	16.20
5	32	28.16	2.41	25.75
20	20	37.05	20.85	16.20
21	20	38.60	22.45	16.15
23	25	44.32	24.28	20.04
25	6	29.17	24.67	4.50
27	19	43.79	27.79	16.00
31	13	41.77	31.38	10.38
3	13	13.38	3.38	10.00
3	26	25.04	4.19	20.85
3	31	30.35	4.52	25.84
4	8	10.00	4.25	5.75
4	13	15.38	5.00	10.38
5	9	12.67	5.67	7.00
7	11	15.82	7.18	8.64
8	14	19.57	8.43	11.14
9	11	18.73	9.27	9.45
9	17	23.00	9.88	13.12
Median		**28.10**	**11.59**	**14.06**

The median of the data that corresponds to the additional nodes that may be commonly observed by 3 monitoring nodes from vantage points 45m away showed up to 12 additional nodes than the target mobile node. The median of the data that

corresponds to the additional nodes that may be commonly observed by 3 monitoring nodes from vantage points 35m away showed up to 28 additional nodes than the target mobile node change. The trends in data showed considerably more additional nodes may be observed by 3 nodes from a 35m range. A closer look at the data related to additional nodes points out a considerable number of static nodes to be amongst the additional nodes observed. The median of the data related to the change in additional nodes that may be observed suggests that the accuracy of mobile devices' locations is relatively better when observed by 3 monitoring nodes from vantage points 45m away across 3 pair-wise perpendicular axes than with 2 monitoring nodes from 2 perpendicular axes.

Table 8.5 presents the recommended model for observing IoT devices, which is based on the results of additional simulation experiments carried out to understand the effect of changes to monitoring node configuration on the location accuracy of IoT devices.

Table 8.5

Model to Observe IoT Devices

Device Type	Monitoring Nodes	Deployment Technique	Deployment Range
Static	3	Pair-wise Perpendicular Axis	Expected Range
Mobile	3	Pair-wise Perpendicular Axis	Expected Range

Using this model to observe a target will generate the data required for an accurate modelling of a target environment. The model specifies the recommended number of monitoring nodes, the deployment technique and the distance of monitoring to observe an IoT environment. To generate data required for accurate modelling of static IoT devices, the recommended approach is to observe every potential location within a target using 3 monitoring nodes across pair-wise perpendicular axis from vantage points based on the expected monitorable range of static IoT devices. For

accurate modelling of mobile IoT devices, the recommended approach is to additionally observe every potential location within a target using 3 monitoring nodes across pair-wise perpendicular axis from vantage points based on the expected monitorable range of mobile IoT devices. The minimum duration of monitoring potential locations depends on the radio technology utilised by IoT platforms in operation. The recommended duration of monitoring every potential location for devices with integrated 802.15.4 radio is at least 40 seconds based on the findings covered in section 5.3.3.

8.2.2 Intermediate Stage – Analysing IoT Device Communications

The assessment criterion that corresponds to this stage of the modelling process is the traceability of IoT devices, the study of which is covered in Chapter 6. IEEE 802.15.4 and ITU-T G.9959 applications that are typically implemented by IoT devices to operate and communicate with peer MAC entities were studied by examining the commonalities and differences in network management and control communications of IoT devices. As expected, the study of the traceability aspect of IoT devices found that communications of IoT devices transmitted data required to trace radio signals from node pairs. Analysis of the communications showed both the type and power-source of an IoT device to be distinguishable from the data transmitted by node pairs.

Despite commonalities in network management and control communications, the communications of mains-powered, static IoT devices were found to be distinct compared to the communications of battery-powered, mobile IoT devices. The findings of the study of traceability aspect, thus, support the analysis of IoT device communications that were observed to determine the data paths of a heterogeneous

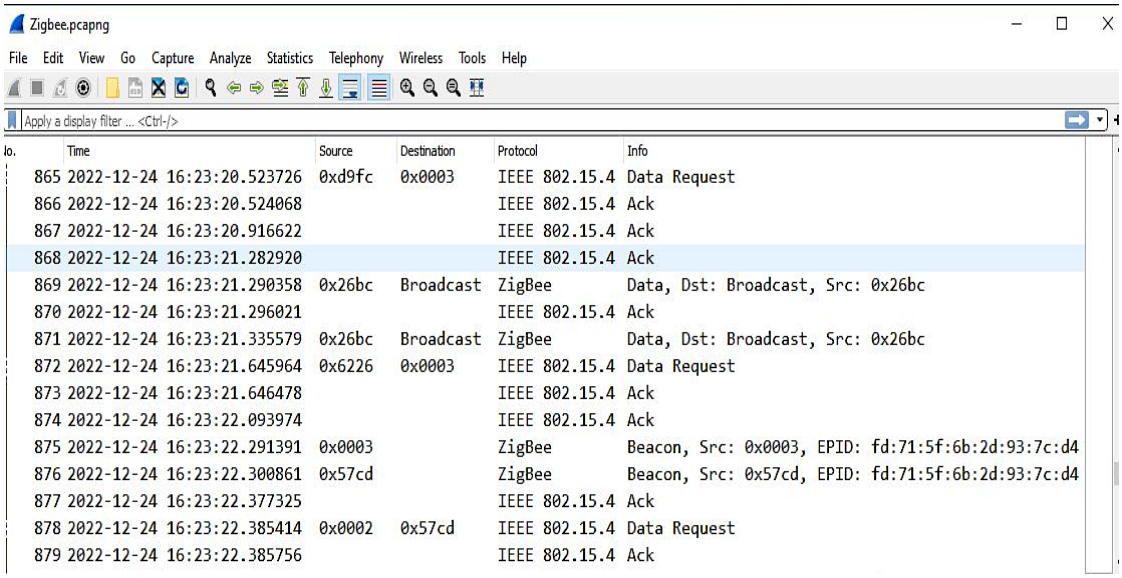
IoT environment. The analysis of IoT device communications to build a wireless sensing platforms topology, however, involves the systematic extraction of network management and control data from the communications observed. The following approach is, therefore, recommended for this stage of the process of IoT monitoring and modelling.

8.2.2.1 Generate Real-Time Logical Network Data

Logical network data is required to distinguish the datalinks that generated traffic. To generate the logical network data, network management and control communications should be extracted from the traffic captured. This requires running software suitable to open the packets captured and interpret the communications. A sample of the 802.15.4 frames captured by NXP's Kinetis USB-KW24D512 module and interpreted by Wireshark is shown in Figure 8.6.

Figure 8.6

Interpretation of Packets by Wireshark Packet Analyzer

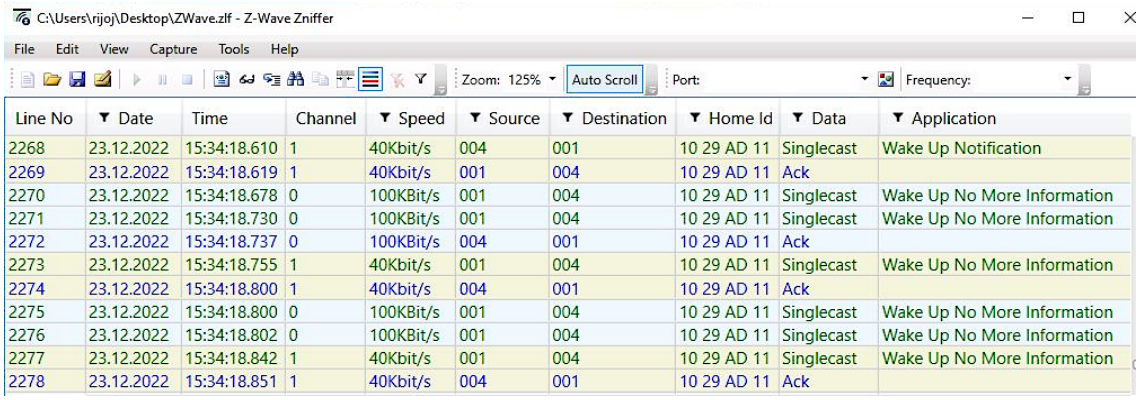


The G.9959 frames captured by Silicon Lab's Z-Wave UZB module requires Z-Wave Zniffer UI to be installed and configured.

Figure 8.7 shows a sample of the packets captured by Z-Wave UZB and interpreted by Z-Wave Zniffer UI.

Figure 8.7

Interpretation of Packets by Z-Wave Zniffer UI



Depending on the radio technology, applicable software must be utilised for the interpretation and separation of network management and control communications from each transmission source. From amongst the network management and control communications, technology-specific applications employed by each source should be identified and catalogued. Table 8.6 lists the 802.15.4 applications that the communications of all unique IoT communication sources may be inspected for.

Table 8.6

802.15.4 Applications to Trace IoT Devices

802.15.4 Application	Frequency	Network ID	Source ID	Destination ID
Data	Non-Periodic	Yes	Yes	Yes
Beacon (*Type 1: PAN Coordinator Identified*)	Periodic	Yes	Yes	No
Beacon (*Type 2: PAN Coordinator Unidentified*)	Periodic	Yes	Yes	No
Command	Periodic	Yes	Yes	Yes

Table 8.7 lists the G.9959 applications that the communications of all unique IoT communication sources may be inspected for.

Table 8.7

G.9959 Applications to Trace IoT Devices

G.9959 Application	Frequency	Network ID	Source ID	Destination ID
Wake Up No More Information	Non-Periodic	Yes	Yes	Yes
Wake Up Notification	Periodic	Yes	Yes	Yes
Acknowledgement	Non-Periodic	Yes	Yes	Yes

These tasks should be repeated until the applications employed by every source of network traffic are identified and catalogued. Where there are multiple networks that use the same radio technology, catalogue the sources and their technology-specific applications based on the network ID to differentiate the sources of a specific network. This method will generate data suitable for further processing.

8.2.2.2 Build Wireless Sensing Platforms Topology

The next step of analysing IoT device communications involves processing of the communications observed and catalogued to build the topology of every wireless sensing platform in operation. To generate the information that is required to build the topology of operating networks, technology-specific applications employed by the source nodes of every network in operation should be examined. Once every source node of a network is distinguished from the technology-specific applications, the node pairs that form the datalinks may be distinguished. This involves mapping the devices according to the source and destination addresses of communications. Further, the node pairs may be plotted to map the logical topology of a sensor network and to identify the node pairs that generated network traffic. Repeat these steps for a

heterogeneous IoT environment until all the nodes sending or receiving messages are identified and distinguished.

Table 8.8 presents a model to distinguish the type and power-source of sources that employ 802.15.4 applications. This model is based on the findings of the study into traceability of IoT devices with integrated 802.15.4 radio.

Table 8.8

802.15.4 Applications Based Model to Distinguish IoT Devices

802.15.4 Application	**Additional Information**	**Device Type**	**Power Source**	**Node Type**
Command	(Not Applicable)	Mobile	Battery-powered	Sensor
Beacon	*PAN Coordinator Identified*	Static	Mains-powered	Sink
Beacon (Type 2)	*PAN Coordinator Unidentified*	Static	Mains-powered	Sink or Actuator

Table 8.9 presents a model to distinguish the type and power-source of sources that employ G.9959 applications. This model is based on the findings of the study into traceability of IoT devices with integrated G.9959 radio.

Table 8.9

G.9959 Applications Based Model to Distinguish IoT Devices

G.9959 Application	**Additional Information**	**Device Type**	**Power Source**	**Node Type**
Wake Up No More Information	(Not Applicable)	Static	Mains-Powered	Sink
Wake Up Notification	(Not Applicable)	Mobile	Battery-powered	Sensor
Acknowledgement	No Other G.9959 Application	Static	Mains-powered	Actuator

8.2.3 Final Stage – Utilising IoT Device Communications

The criterion of assessment that corresponds to this stage of the modelling process is the monitorability of IoT devices, the study of which is covered in Chapter 5. The study examined the effects of power source and external walls to the transmission range of IoT devices. As expected, the study found that the transmission range of IoT devices through external walls that are commonly utilised for indoor environments will vary depending on the device power source. Compared to the periodic transmissions of battery-powered IoT devices, periodic transmissions of mains-powered IoT devices were found to have a greater transmission range. The transmission range of IoT devices, regardless of power source, also showed variations as the wall type changed.

However, the variations were minor across IoT devices powered by the same source. The results obtained for battery-powered IoT devices suggested that the transmissions of IoT devices have a limited range of approximately 45m. The results obtained for mains-powered IoT devices, however, suggested that transmissions of IoT devices have a range of approximately 60m. The findings of the study into the monitorability aspect support IoT device communications being utilised to determine the locations of IoT devices connected by IoT platforms. This, however, requires a 2-step approach of deducing the locations of static nodes and deriving the locations of mobile nodes. The following approach is, therefore, recommended for the final stage of the monitoring and modelling process.

8.2.3.1 Determine Locations of Static Nodes

The first phase of the approach determines the locations of static sources. As the communications of static nodes have a limited but greater monitorable range than battery-powered nodes, the locations of monitored static nodes may be deduced from

the locations of their monitoring nodes. The recommended first step is to catalogue the vantage points that monitoring nodes observed a target environment from and determine their X, Y and Z coordinates corresponding to the centre of the target. This will identify the nodes that monitored a target environment from a certain distance across each of the 3 axes.

Next, identify the monitoring nodes that observed locations within a target environment and captured communications of static sources from vantage points at expected monitorable range of static devices. If the number of static sources is yet to be ascertained, catalogue the static sources observed by each monitoring node to identify the unique sources. Next, based on the monitorable range of static sources, plot every static source observed by each monitoring node to generate an arrangement of the static sources corresponding to each monitoring node. Then, merge all the projections of every static source to determine the locations in 3-D space where the static sources may be located.

8.2.3.2 Determine Locations of Mobile Nodes

This phase of the modelling process derives the locations of mobile nodes relative to the static nodes that together form a low-energy wireless sensing platform. If the number of mobile nodes that form datalinks with static sources is yet to be ascertained, examine the communications of static sources that were located to discover mobile nodes and catalogue their identifier. Then, identify the monitoring nodes that observed locations within a target environment and captured communications of the mobile nodes from vantage points at expected monitorable range of mobile devices.

Subsequently, based on the monitorable range of mobile nodes, plot every mobile node observed by monitoring nodes. This will generate an arrangement of the mobile nodes corresponding to each monitoring node. Merge all the projections of every mobile node to determine the locations in 3-D space where the mobile nodes may be located. Then, incorporating the monitorable range of static sources, generate an arrangement of both mobile and static nodes that form datalinks. Using the 3-D coordinates of each static source, calculate the distance between the static nodes of an environment and the mobile nodes. This will generate a view of the mobile nodes relative to the static nodes of an IoT environment and identify the static node closest to every mobile node.

The actual locations of the static and mobile nodes, however, may vary from the locations determined by the methods of deduction and derivation. This is because the methods utilise expected monitorable range, which vary according to device power source, to determine the locations of the various devices observed by monitoring nodes. The data analysed for the study of IoT monitorability which tested 802.15.4 radio devices across seven wall types, however, showed that the monitorable communications from IoT devices varied across the wall types. The differences in monitorable communications across devices of the same type implies there are differences in monitorable range of IoT devices operating in the real-world.

To further improve the accuracy with which locations are determined, location estimates may additionally allow for the differences in monitorable range of a device operating within an indoor environment depending on the type of device. The data collected from the different device types tested for the study into monitorability show mobile devices to have a real-world monitorable range that is upto 10m more than the

expected range that is applicable for deriving their locations. Data obtained for static devices show a real-world monitorable range of upto 4m more than the expected range that is applicable for deducing their locations.

Table 8.10 presents a model to allow for the differences in the monitorable range of IoT devices across several wall types. This model is based on the data collected and analysed for the study into the monitorability of IoT devices.

Table 8.10

Model to Allow for Monitorable Range Differences in Location Estimates

Wall Types	Static IoT Device	Mobile IoT Device
Brick Exterior	Expected Range +4m	Expected Range +10m
Internal Dry Wall	Expected Range +4m	Expected Range +10m
Garage Door	Expected Range +4m	Expected Range +10m
Single-Pane Window	Expected Range +4m	Expected Range +10m
Double-Glazed Window	Expected Range +4m	Expected Range +10m
Obscure Glass Window	Expected Range +4m	Expected Range +10m
Metal Roof	Expected Range +4m	Expected Range +10m

This model to improve the location accuracy may be applied in conjunction with the layout of a target to further improve the location accuracy. For example, when the location of a mobile device that is across a brick wall is estimated to be 10m from its projected location based on the expected range, the absence of a room beyond 3m from the projected location would suggest that the actual location is not more than 3m from the projected location. This step may be repeated to factor in other wall types across which signals were observed.

Several real-world experiments that involved static and mobile IoT devices validated the model that is recommended to improve location accuracy. To carry out experiments in real-world settings, the site utilised for IoT monitorability and traceability study was revisited as this site was accessible and determined as suitable

for further experiments. As real-world experiments in a 3-D setting involve many challenges, including the selection of a site suitable for unmanned drone flights, operation of a drone adhering to local aviation rules applicable for non-certificated unmanned aircraft operators, experience to control a drone carrying payload above and near a target location, consent of inhabitants in nearby dwellings and lockdown periods to avoid hazards to people and property, all experiments carried out at the selected site utilised ground-based monitoring locations. Figure 8.8 shows the Google Maps satellite view of the location that was selected to carry out the location accuracy validation experiments.

Figure 8.8

Google Maps Satellite View of Location Testing Site

The red location pin that this view shows identify the site selected for experiments. The selected site is a residential area that is mostly surrounded by single-storied stand-alone dwellings and cars that are parked on roads. Several combinations of monitoring locations 60m and 45m away from the target were identified using Google

Maps. The identified locations were catalogued and utilised to iteratively monitor the target and capture packets from the IoT deployments, which varied from one scenario to another. The site was monitored without prior knowledge of the locations of IoT deployments within the site. The communications observed and analysed from the different scenarios are presented below.

Scenario 1

The first scenario involved two static and three mobile IoT devices within the target environment. The target site was monitored from locations approximately 60m away by following the catalogued combinations of two perpendicular locations.

Figure 8.9 shows a location approximately 60m away from where radio signals of both static devices were observed by a monitoring node along with another perpendicularly located monitoring node approximately 60m away.

Figure 8.9

Google Maps Satellite View of Monitoring Location 60m from Target

The aim of monitoring from locations 60m away was to locate any static devices in operation at the target site. Inspection of the packets captured by both the monitoring nodes from all catalogued locations showed two static devices to be in operation at the site. Further, both the devices were monitorable from two perpendicular locations, both approximately 60m away. The wall types that surrounded the room within the target across which the monitoring nodes captured packets of both devices included double-glazed window and brick exterior. Factoring the effect of the two wall types and the layout of the target, locations of the devices were determined to be between 60 and 63m from the first monitoring node and between 60 and 64m from the second monitoring node. Following this estimation of the locations of devices from locations of the monitoring nodes that captured packets from both static devices, the target was physically examined.

Upon physical examination of the target site based on the estimate from two monitoring nodes, two static devices were identified in a single room. One of the two static devices was identified approximately 63m away from the monitoring node that the device was estimated to be between 60 and 63m away. From the monitoring node that the monitored node was estimated to be between 60m and 64m away, the located static device was approximately 62m away. The second static device was identified approximately 62m away from the monitoring node that this device was estimated to be between 60 and 63m away. From the monitoring node that the monitored node was estimated to be between 60m and 64m away, the second static device was approximately 61m away.

Scenario 2

The second scenario involved two static and four mobile IoT devices within the target environment. The target site was monitored from locations approximately 60m away by following the catalogued combinations of two perpendicular locations. The aim of monitoring from locations 60m away was to locate any static devices in operation at the target site. Inspection of the packets captured by both the monitoring nodes from all catalogued locations showed two static devices to be in operation at this site. Both the static devices were monitorable from two perpendicular locations, each approximately 60m away. The wall types that surrounded the room within the target across which the monitoring nodes captured packets of both devices included garage door and brick exterior. Factoring the effect of the two wall types and the layout of the target, the locations of the two static devices were determined to be between 60 and 64m from the first monitoring node and between 60 and 64m from the second monitoring node.

Following this estimation of the locations of devices based on locations of the monitoring nodes that captured packets from the two devices, the target was physically examined. Upon physical examination of the target site based on the location estimate provided by the two monitoring nodes, two static devices were identified within the garage. One of the static devices was identified approximately 63m from both the monitoring nodes that captured communications from the device. The second static device was identified approximately 64m from both the monitoring nodes that captured communications from the device.

Scenario 3

The third scenario involved one static and four mobile IoT devices within the target environment. The target site was monitored from locations approximately 45m away by following the catalogued combinations of two perpendicular locations. In contrast to the first two scenarios, the aim of monitoring was to locate any mobile devices in operation at the target site. The packets captured by both the monitoring nodes were inspected to identify the number of mobile devices that are in operation at the site. Inspection of the packets that were captured by the monitoring nodes showed a total of four mobile devices to be in operation at this location. All four devices were monitorable from two perpendicular locations, both approximately 45m away.

Figure 8.10 shows a location 45m away from where radio signals of two out of the four mobile nodes were observed by a monitoring node along with another perpendicularly located monitoring node approximately 45m away.

Figure 8.10

Google Maps Satellite View of Monitoring Location 45m from Target

Based on the monitoring locations, the nodes were determined to operate in two different rooms within the site. The wall types that surrounded the rooms within the target across which the monitoring nodes captured packets of every device included double-glazed window, single-pane window and brick exterior. The locations of two out of four devices, which were determined to be in a single room, were determined to be between 45 and 55m from one of the two monitoring nodes. These two devices were estimated to be between 45 and 49m from the second monitoring node that captured communications from the devices. The other two devices, which were determined to be in a single room, were estimated to be between 45 and 49m from one of the two monitoring nodes that captured communications and between 45 and 50m from the second monitoring node that captured communications.

Following estimation of the locations of 4 mobile devices based on locations of the monitoring nodes that captured packets from all devices, the site was physically examined. Upon physical examination of the rooms based on the location estimate provided by the two monitoring nodes, all four mobile IoT devices were identified. One of the two mobile devices located within a single room was identified approximately 47m away from the monitoring node that the monitored nodes were estimated to be between 45 and 55m away. From the monitoring node that the monitored nodes were estimated to be between 45 and 49m, the first mobile device identified was approximately 46m away. The second mobile device was identified approximately 48m away from the monitoring node that the monitored nodes were estimated to be between 45 and 55m away.

The second device was approximately 46m away from the monitoring node that monitored nodes were estimated to be between 45 and 49m away. The third mobile

device was identified approximately 48m away from the monitoring node that the other two monitored nodes were estimated to be between 45 and 49m away. The third device was approximately 47m away from the monitoring node that the device was estimated to be between 45 and 50m away. The fourth mobile device was identified approximately 47m away from the monitoring node that this device was estimated to be between 45 and 49m away. The fourth device was approximately 46m away from the monitoring node that this device was estimated to be between 45 and 50m away.

Scenario 4

The fourth scenario involved two static and four mobile IoT devices where the static IoT devices operated in different rooms within the target environment. The target site was monitored from all catalogued locations approximately 60m away to obtain communications from any static device in operation. The aim of monitoring from locations 60m away was to locate any static devices in operation at the target site. The packets captured by both the monitoring nodes from different locations were inspected to identify the number of static devices in operation. Inspection of the packets showed that two static devices are in operation from two different rooms at the site. One of the two rooms within the target across which the monitoring nodes captured packets of a static device had brick exterior and double-glazed window. The other room from which monitoring nodes captured packets utilised single-pane window and brick exterior. Factoring the effect of the two wall types and the layout of the target, locations of both static devices were determined to be between 60 and 64m from one of the two monitoring nodes and between 60 and 63m from the other monitoring node.

Following estimation of the locations of the two static devices based on the locations of the monitoring nodes that captured packets from the two devices, the site was physically examined. The deployments were traced to the rooms from where communications of every static device were captured by two monitoring nodes. One of the two static devices was identified approximately 62m from the monitoring node that this device was estimated to be between 60 and 64m away. From the monitoring node that this device was estimated to be between 60 and 63m away, the device was approximately 63m away. The second static device identified was approximately 62m away from the monitoring node that this device was estimated to be between 60 and 64m away. The second static device was approximately 61m from the monitoring node that this device was estimated to be between 60 and 63m away.

Scenario 5

The fifth scenario involved two static and four mobile IoT devices. The target site was monitored from locations approximately 45m away by following the catalogued combinations of two perpendicular locations. The aim of monitoring from locations 45m away was to locate any mobile devices in operation at the target site. The packets that were captured by both monitoring nodes from various perpendicular locations were inspected to identify the number of mobile devices in operation. Inspection of the packets showed four mobile devices to be in operation at this location. Based on the monitoring locations, it was determined that the mobile devices operated in different rooms within the target site. The configuration of nodes that captured the packets of mobile nodes narrowed the location of each mobile device to rooms with different exterior walls. The wall types included brick exterior, single-pane window, double-glazed window and obscure window. Factoring the effect of the wall types and

the layout of the target, the locations of the mobile devices were estimated to be between 45 and 49m away from one of the two monitoring nodes that captured communications and between 45 and 48m from the other monitoring node.

Following estimation of the locations of the mobile devices from the locations of the monitoring nodes that captured packets, the site was physically examined. The rooms from where communications of every mobile device were captured by two monitoring nodes were traced. All mobile devices were identified approximately 46 to 47m away from the monitoring node that the devices were estimated to be between 45 and 49m away. From the monitoring node that the devices were estimated to be between 45 and 48m away, the mobile devices were identified approximately 47 to 48m away.

The actual location of static and mobile devices in all the scenarios were within the range estimated based on monitoring locations, wall types and the layout.

8.3 Guide for IoT Spatial Modelling and Forensic Reconstruction

Based on the results of the extensive empirical and simulation experiments to develop the system for IoT monitoring and modelling, the following sequence of steps is recommended to locate Things from their communications.

1. *Monitor the target environment iteratively from 3 locations. The locations for monitoring are to be selected based on the monitorable range of devices.*

   As mains-powered IoT devices with integrated IEEE 802.15.4 radio have a monitorable range of 60m, recommended locations to detect IEEE 802.15.4 based IoT platforms operating within a specific target are 5 to 10m away, 35 to 45m away and 50m to 60m away. The minimum recommended duration of monitoring

to detect IEEE 802.15.4 based IoT platforms is 40 seconds at each monitoring location.

2. *Note the network IDs from the communications obtained across all three locations. This will eliminate the networks and IoT technologies that are operating in locations neighbouring a specific target.*
3. *Identify locations around a target to monitor and discover all active IoT devices from the smallest configuration of devices.*
4. *Identify combinations of monitoring locations to monitor every potential location within a target where mains-powered and battery-powered IoT devices are in operation, according to their monitorable range. The first recommended deployment configuration is 3 monitoring nodes, where the nodes are pair-wise perpendicular and equidistant. Where this is not possible, the next recommended configuration is 2 equidistant monitoring nodes at perpendicular locations.*
5. *Deploy monitoring nodes at identified locations and observe the target to collect communications required for an accurate modelling.*

   The time to observe potential locations within a target depends on the technologies that are in operation. Where periodic communications are employed by all device types and where periodic communications are adequate to distinguish device type, power source and node type, the minimum time to monitor potential locations for a device type depends on the rate of monitorable transmissions from that device type. As an example, the recommended minimum duration is 40 seconds to observe IoT devices with integrated IEEE 802.15.4 radio. Where periodic communications are not employed by all device types, the locations may be monitored for extended duration to capture communications adequate for modelling.

6. *Extract network management and control communications from traffic captured.*
7. *Identify technology-specific applications employed by each network traffic source.*
8. *Catalogue the sources and their technology-specific applications based on the network ID to differentiate the communication sources of a specific network.*
9. *Distinguish the device type, power source and node type of each source from the technology-specific applications.*
10. *Identify and catalogue the locations from where each source was observed according to the recommended model for monitoring potential locations.*
11. *Plot each static source relative to the locations of monitoring nodes that observed the source based on the recommended model for monitoring potential locations.*
12. *Merge the projections of every static source to determine approximate locations of the static sources within a target IoT environment.*
13. *Plot every mobile node relative to the locations of monitoring nodes that observed the source based on the recommended model for monitoring potential locations.*
14. *Merge the projections of every mobile node to determine approximate locations of the mobile nodes within a target IoT environment.*
15. *Incorporate the distance between the static nodes of an environment and the mobile nodes. This will identify the static node closest to every mobile node.*
16. *Incorporate layout, if available, to further improve location estimate of every static and mobile node relative to the wall installations of the target.*
17. *Repeat steps 5 to 16 to identify any change in location of devices over time.*

8.4 Conclusion

An evaluation of the model for monitoring and modelling IoT devices, based on the findings of the study into IoT monitorability, traceability and discoverability, found the model to be effective. The findings based on simulation and empirical

experiments also informed the development of methods that are required for the spatial modelling of an IoT environment. As envisaged, the system for spatial modelling consists of 3 stages, that of observing, analysing and utilising communications between IoT devices.

Chapter 9

CONCLUSIONS AND FUTURE RESEARCH

9.1 Introduction

This work has explored the area of passively monitoring an IoT environment to accurately locate the various Things that are in operation because this capability will greatly assist forensic investigators to identify and collect Things from a scene of forensic examination. Building on the novel concept of harnessing wireless communications between Things from multiple monitoring nodes, this work developed a lightweight system for monitoring and modelling Things. The goal to develop a versatile system that enables both forensic investigators and LEAs to locate Things ahead of a field search activity initially prompted a preliminary inquiry into utilising the wireless communications between Things. This was followed by broader inquiries into utilising, analysing and observing wireless communications between Things. The inquiries involved a robust study of the monitorability, traceability and discoverability of Things from wireless communications.

The findings of the study into IoT monitorability, traceability and discoverability supported monitoring and modelling Things by combining the processes of observing, analysing and utilising wireless communications. The study into monitorability, traceability and discoverability of Things, which involved simulation and empirical experiments, also informed the construction of methods applicable for observing, analysing and utilising wireless communications. This final chapter covers the conclusions of the thesis, which is based on the work that was involved to design and develop a system that meets the needs of forensic investigators and LEAs in order to

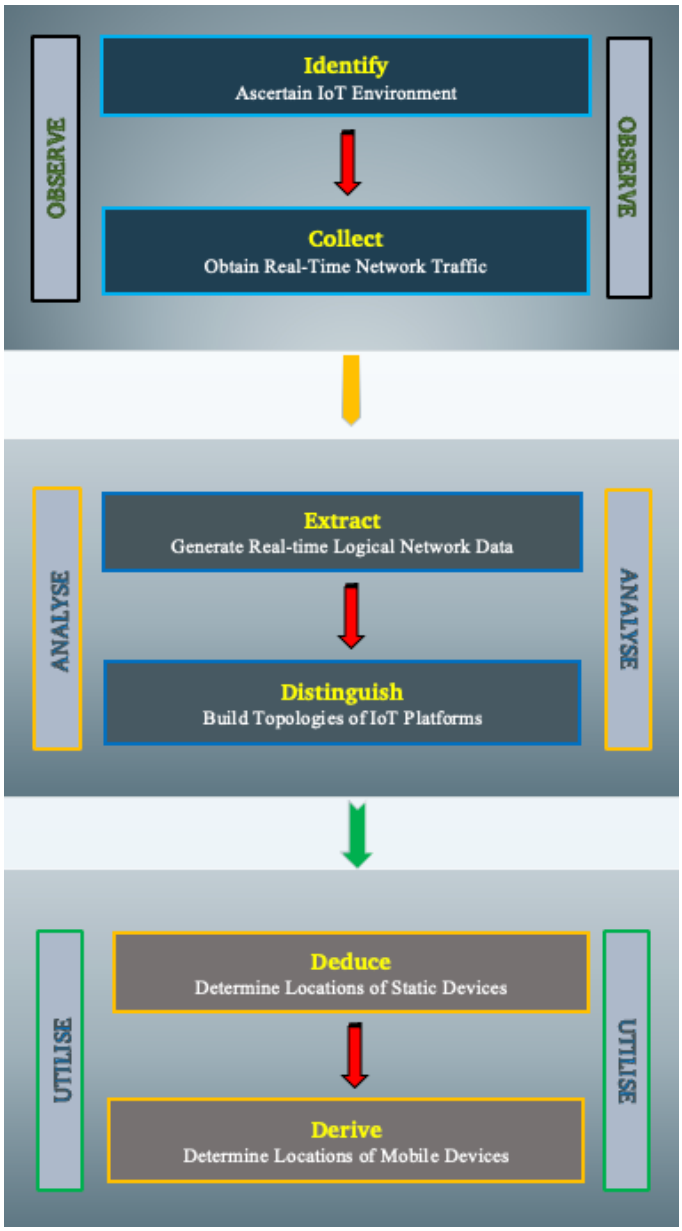
identify Things at a wireless digital scene. This chapter also provides suggestions for further research to build on the foundations of this work.

9.2 Conclusions

The system designed and developed for monitoring and modelling Things, which will enable forensic investigators and LEAs to locate and track Things of an IoT environment, is depicted in Figure 9.1.

Figure 9.1

System for Monitoring and Modelling Things



This system, which enables real-time reconstruction of IoT environments, is complex because there are many challenges to harnessing the communications between Things in order to accurately determine their locations prior to a field search activity by forensic investigators. Initially, the low-rate, short-range IoT technologies that operate within a specific physical environment are distinguished and the operating channels of the low-rate, short-range IoT technologies are determined before communications between Things are captured in order to generate the necessary data required for accurate modelling. These steps are recommended as multiple IoT platforms are likely to operate within a target IoT environment and as locations surrounding a target are likely to utilise technologies similar to those in operation within the target.

As network layer packets are increasingly unintelligible to provide enhanced security for communications, the system for IoT monitoring involves extraction and processing of network management and control messages embedded into communications in an intelligible format. The network management and control messages, which are not standardised across IoT technologies, depends on the technologies utilised by a target IoT environment. The recommendation, hence, is to extract the network management and control messages for every wireless sensing platform in operation. The subsequent step, which processes the network management and control messages, maps the logical topologies of operating platforms. As there are opportunities for battery-operated devices to be moved within a target IoT environment, the system is by design suited for continuous monitoring to generate a timeline and track changes to device locations.

As accounting for all the known and unknown interferences within and outside a target IoT environment that affect the strength of radio signals is difficult, the

recommendation is to determine the locations of Things operating within a target IoT environment using the locations from where monitoring deployments obtained real-time network traffic. A benefit of this novel system is that the methods involved are suited for investigators to obtain evidence of Things and their locations without inadvertently tampering with the scene. There is no requirement to enter a scene or use any fixed infrastructure to implement any stage of the system.

The various challenges and the capabilities that were considered for forensic investigators to harness the communications between IoT devices narrowed the scope of the problem studied to the following questions.

1) ***How can the wireless communications of a heterogeneous IoT environment be observed to enable the accurate modelling of Things?***
2) ***How can the wireless communications of a heterogeneous IoT environment be analysed to map the logical topologies of Things?***
3) ***How can the wireless communications of a heterogeneous IoT environment be utilised to determine the locations of Things?***

Developing this complex system for monitoring and modelling Things involved understanding three aspects of the communications between Things, namely, monitorability, traceability and discoverability. Understanding these discrete aspects of communications involved the investigation of low-rate, short-range transmissions. The investigations led to several findings that initially confirmed the following overarching hypotheses –

H1: The forensic investigator can observe and analyse the wireless communications between IoT devices ahead of searching an evidential scene to definitively determine the number and types of IoT devices that operate at the scene.

H2: The forensic investigator can utilise the wireless communications between IoT devices that are observed ahead of searching an evidential scene to accurately locate the different types of IoT devices that operate at the scene.

The findings of the study into IoT monitorability, traceability and discoverability that proved the hypotheses true also informed the construction of an effective forensic investigation framework for harnessing communications to locate Things. Amongst the findings of this work are the monitorable range of Things, the rate of monitorable transmissions, the types of devices that may be traced from the transmissions and the fewest number of monitoring devices that will enable a 100% discovery of the devices that operate within an IoT environment. The investigations also uncovered the factors that affect the monitorable range of Things, the traceability of transmissions to datalinks and the discovery of Things from the peripheries of a target IoT environment. Additional real-world experiments found the accuracy of location estimates is within 7% of the actual location. Importantly, the work carried out established that harnessing wireless communications between Things to locate Things and obtain location evidence is possible.

9.3 Future Research

Future studies may build on the system developed for IoT devices network monitoring and modelling to develop methods required to preserve and recreate the messages between Things that will otherwise be leaking from a wireless digital scene. Future studies may also build on the system for harnessing the wireless communications between Things to develop processes required to utilise the communications that may be logged to identify and assess the risks within a target location. The findings and results of this study may be referred to and utilised to

develop procedures factoring the time that is required to seize the Internet-enabled Things at a wireless digital scene.

It would be interesting to run further simulations and to develop alternative monitoring node deployment models. The alternatives will provide investigators with more deployment options to select from. It would also be interesting to run real-world experiments in a 3-D setting to identify the technologies that are best suited for implementation of the methods. Such experiments will also enable a comparison of the various technologies that may be utilised for implementation. Future work may implement the recommended methods in a variety of layouts to develop models that investigators may selectively apply depending on the layout of a target environment.

Future developments of low-rate, short-range wireless communication technologies may refer to this work for baseline measurement of the monitorable range of Things. The study into traceability identified that the traceability of Things varies between Zigbee and Z-Wave compliant devices. Improvements that narrow the differences in traceability of Things will reduce the complexities for the system for monitoring and modelling Things. The results of the traceability study may also be referred to for enhancements to IoT mesh networking technologies that will further differentiate the various sensors and actuators in operation.

Exaptation of the IoT monitoring and modelling system for locating Things that communicate using long-range radio technology will be beneficial to many other areas, including civilian search and rescue, farm animals search and rescue, military operations and security and surveillance operations. The methods and models that this work has contributed may also be applied as such in other scenarios where spatial modelling is required. As technology develops, future research may build on this

work to continually evolve the novel framework that fills the gap to locate Things from wireless communications prior to their identification at the scene. Continual enhancements to the framework will provide consistent guidance to forensic investigators, both in procedure and in ensuring adherence to a standard framework suitable for criminal and other investigations.

References

Acharjya, D. P., Geetha, M. K., & Sanyal, S. (Eds.). (2017). *Internet of Things: Novel advances and envisioned applications*. Springer.

Aneja, S., Aneja, N., & Islam, M. S. (2018). IoT device fingerprint using deep learning. *Proceedings of the 2018 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS),* 174-179. https://doi.org/10.1109/IOTAIS.2018.8600824

Ashton, K. (2009). *That 'Internet of Things' thing: In the real world, things matter more than idea.* Retrieved from http://www.rfidjournal.com/articles/view?4986

Babun, L., Aksu, H., Ryan, L., Akkaya, K., Bentley, E. S., & Uluagac, A. S. (2020). Z-IoT: Passive device-class fingerprinting of zigbee and z-wave iot devices. *Proceedings of the 2020 IEEE International Conference on Communications.* https://doi.org/10.1109/ICC40277.2020.9149285

Bhat, N. S. (2011). Design and implementation of IEEE 802.15.4 MAC protocol on FPGA. *Proceedings of the IJCA Innovative Conference on Embedded Systems, Mobile Communication and Computing, ICEMC2*(1), 1-5.

Buratti, C., Verdone, R., & Ferrari, G. (2011). *Sensor networks with IEEE 802.15. 4 systems: distributed processing, MAC, and connectivity*. Springer Science & Business Media.

Business Wire. (2011). *CCID Consulting: China's Internet-of-Things industry sees a landscape characterized by clustering in four regions.* Retrieved from http://www.businesswire.com/news/home/20111004005055/en/CCID-Consulting-Chinas-Internet-of-Things-Industry-Sees-Landscape#.VPWjqbOsWq4

Caceres, R., & Friday, A. (2012). Ubicomp systems at 20: Progress, opportunities, and challenges. *IEEE Pervasive Computing, 11,* 14-21. https://doi.org/10.1109/MPRV.2011.85

CBI. (2020). *The European market potential for integrated internet of things and big data services.* Retrieved from https://www.cbi.eu/market-information/outsourcing-itobpo/intergrated-internet-things/market-potential

Chernyshev, M., Baig, Z., Bello, O., & Zeadally, S. (2018). Internet of Things (IoT): Research, simulators, and testbeds. *IEEE Internet of Things Journal, 5*(3), 1637-1647. https://doi.org/10.1109/JIOT.2017.2786639

Chew, D. (2019). Protocols of the wireless Internet of Things. In E. Hossain (Ed.), *The wireless Internet of Things: A guide to the lower layers* (1st ed., pp. 21-45). John Wiley & Sons. https://doi.org/10.1002/9781119260608.ch2

Chorost, M. (2008). *The networked pill: A new information system records what pills do to the body.* MIT Technology Review. Retrieved from https://www.technologyreview.com/s/409773/the-networked-pill/

Chowdhury, T. J., Elkin, C., Devabhaktuni, V., Rawat, D. B., & Oluoch, J. (2016). Advances on localization techniques for wireless sensor networks: A survey. *Computer Networks, 110,* 284-305. https://doi.org/10.1016/j.comnet.2016.10.006

Christian, C. (2024). *IoT 2023 in review: The 10 most relevant IoT developments of the year.* Retrieved from https://iot-analytics.com/iot-2023-in-review/

Cisco IBSG. (2011). *The Internet of Things: How the next evolution of the Internet is changing everything.* Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144*, 17-39. https://doi.org/10.1016/j.comnet.2018.07.017

Cooney, M. (2016). *Gartner top 10 technology trends you should know for 2017.* Retrieved from https://www.networkworld.com/article/3132363/gartner-top-10-strategic-technology-trends-you-should-know-for-2017.html

Dixit, S., Ojanpera, T., Nee, R. v., & Prasad, R. (2011). Introduction to globalization of mobile and wireless communications: Today and in 2020. In D. S. Prasad R., van Nee R., Ojanpera T. (Eds.), *Globalization of Mobile and Wireless Communications* (pp. 1-18). Springer. https://doi.org/10.1007/978-94-007-0107-6_1

Farahani, S. (2008). ZigBee Basics. In S. Farahani (Ed.), *ZigBee Wireless Networks and Transceivers* (pp. 1-24). Newnes.

Farnham, T. (2019). Indoor localisation of IoT devices by dynamic radio environment mapping. *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 340-345. https://doi.org/10.1109/WF-IoT.2019.8767296

Farsi, M., Daneshkhah, A., Hosseinian-Far, A., & Jahankhani, H. (Eds.). (2020). *Digital twin technologies and smart cities*. Springer.

Giusto, D., Iera, A., Morabito, G., & Atzori, L. (2010). *The Internet of Things*: Springer.

Glaessgen, E., & Stargel, D. (2012). The digital twin paradigm for future NASA and U.S. air force vehicles. *Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference.* https://doi.org/10.2514/6.2012-1818

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine, 48*(6), 92-101. https://doi.org/10.1109/MCOM.2010.5473869

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communication Surveys & Tutorials, 17*(3). https://doi.org/10.1109/COMST.2015.2388550

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Han, S., Shin, W., Park, J.-H., & Kim, H. (2018). A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping. *Proceedings of the 27th USENIX Security Symposium*, 1229-1246.

Hatler, M. (2017). *Wireless sensor networks for IIoT.* Retrieved from https://www.smart-energy.com/magazine-article/wireless-sensor-network-tech-iiot/

Herrero, R. (2022). *Fundamentals of IoT communication technologies*: Springer International Publishing.

Hersent, O., Boswarthick, D., & Elloumi, O. (2011). *The Internet of Things: Key applications and protocols*. John Wiley & Sons.

IEEE. (2015). *Towards a definition of the Internet of Things (IoT)*. Retrieved from https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

IEEE. (2020). *802.14.5-2020 - IEEE standard for low-rate wireless networks.* https://ieeexplore.ieee.org/servlet/opac?punumber=9144689.

IERC. (2011). *Internet of Things: Pan European Research and Innovation Vision*. Retrieved from http://www.internet-of-things-research.eu/pdf/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011_web.pdf

IERC. (2014). *Internet of Things.* Retrieved from http://www.internet-of-things-research.eu/about_iot.htm

IoT6. (2014). *6LoWPAN.* Retrieved from https://iot6.eu/6lowpan

IoT-GSI. (2012). *Overview of the Internet of Things (*Recommendation ITU-T Y.2060). https://handle.itu.int/11.1002/1000/11559

ITU. (2005). *ITU Internet Reports 2005: The Internet of Things*. Retrieved from http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf

ITU, & Cisco. (2016). *Harnessing the Internet of Things for Global Development.* Retrieved from https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

ITU-T. (2015). *Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications* (Recommendation ITU-T G.9959). https://handle.itu.int/11.1002/1000/12399.

Jafari, H., Omotere, O., Adesina, D., Wu, H. H., & Qian, L. (2018). IoT devices fingerprinting using deep learning. *Proceedings of the 2018 IEEE Military Communications Conference (MILCOM)*. https://doi.org/10.1109/MILCOM.2018.8599826

Juskalian, R. (2016). *Europe Builds a Network for the Internet of Things. Will the Devices Follow?* MIT Technology Review. Retrieved November 19, 2020, from https://www.technologyreview.com/2016/07/19/158780/europe-builds-a-network-for-the-internet-of-things-will-the-devices-follow/

Kambourakis, G., Kolias, C., Geneiatakis, D., Karopoulos, G., Makrakis, G. M., & Kounelis, I. (2020). A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks. *Symmetry, 12*(4), 579. https://doi.org/10.3390/sym12040579

Kaur, M. J., Mishra, V. P., & Maheshwari, P. (2020). The convergence of digital twin, IoT, and machine learning: transforming data into action. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds.), *Digital twin technologies and smart cities* (pp. 3-17). Springer.

Kotak, J., & Elovici, Y. (2021). IoT device identification using deep learning. In Á. Herrero, C. Cambra, D. Urda, J. Sedano, H. Quintián, & E. Corchado (Eds.), *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)* (pp. 76-86). Springer. https://doi.org/10.1007/978-3-030-57805-3_8

Langendoen, K. (2008). Medium access control in wireless sensor networks. *Medium access control in wireless networks, 2,* 535-560.

Leclercq-Vandelannoitte, A. (2015). Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy, 36*(5), 18-24. https://doi.org/10.1108/JBS-08-2014-0100

Li, F., Lam, K. Y., Li, X., Sheng, Z., Hua, J., & Wang, L. (2020). Advances and emerging challenges in cognitive Internet of Things. *IEEE Transactions on Industrial Informatics, 16*(8), 5489-5496. https://doi.org/10.1109/TII.2019.2953246

Liu, M., Han, X., Liu, N., & Peng, L. (2021). Bidirectional IoT device identification based on radio frequency fingerprint reciprocity. *Proceedings of the ICC 2021-IEEE International Conference on Communications*, 1-6. https://doi.org/10.1109/ICC42927.2021.9500275

Liu, Y., Wang, J., Li, J., Song, H., Yang, T., Niu, S., & Ming, Z. (2020). Zero-bias deep learning for accurate identification of Internet-of-Things (IoT) devices. *IEEE Internet of Things Journal, 8*(4), 2627-2634. https://doi.org/10.1109/JIOT.2020.3018677

Lueth, K. L. (2020). *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time.* IoT Analytics. Retrieved from https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

MacDermott, Á., Baker, T., Buck, P., Iqbal, F., & Shi, Q. (2020). The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics. *International Journal of Digital Crime and Forensics (IJDCF), 12(1),* 1-13.

McDaid, C. (2019). *Simjacker – Next generation spying over mobile.* ENEA. Retrieved July 11, 2021, from https://blog.adaptivemobile.com/simjacker-next-generation-spying-over-mobile

Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017). Forensic state acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1-11. https://doi.org/10.1145/3098954.3104053

Milenkovic, M. (2020). *Internet of Things: Concepts and System Design*. Springer. https://doi.org/10.1007/978-3-030-41346-0

Montasari, R., Carpenter, V., & Hill, R. (2019). A road map for digital forensics research: A novel approach for establishing the design science research process in digital forensics. *International Journal of Electronic Security and Digital Forensics, 11*(2), 194-224.

Ngamakeur, K., Yongchareon, S., Y., J., & Rehman, S. U. (2020). A survey on device-free indoor localization and tracking in the multi-resident environment. *ACM Computing Surveys (CSUR), 53(4),* 1-29.

Nieto, A., Rios, R., & Lopez, J. (2017). Digital witness and privacy in IoT: Anonymous witnessing approach. *Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS*, 642-649. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.295

Nieto, A., Rios, R., & Lopez, J. (2018). IoT-Forensics meets privacy: Towards cooperative digital investigations. *Sensors, 18*(2), 492. https://doi.org/10.3390/s18020492

Nieto, A., Roman, R., & Lopez, J. (2016). Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices. *IEEE Network, 30*(6), 34-41. https://doi.org/10.1109/MNET.2016.1600087NM

Nixon, M. (2012). *A Comparison of WirelessHART vs. ISA100.11a.* Emerson. Retrieved from https://www.emerson.com/documents/automation/white-paper-a-comparison-of-wirelesshart-isa100-11a-en-42598.pdf

Novikov, A. M., & Novikov, D. A. (2013). *Research methodology : From philosophy of science to research design*. CRC Press.

NXP. (2018). *Zigbee 3.0 stack user guide* (JN-UG-3113). https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf

NZ IoT Alliance. (2020). *The Internet of Things: Accelerating a connected New Zealand.* Retrieved from https://iotalliance.org.nz/wp-content/uploads/sites/4/2018/09/Accelerating-a-Connected-New-Zealand-eBOOK.pdf

OpenThread. (2022a). OpenThread. Retrieved from https://www.openthread.io

OpenThread. (2022b). Thread Primer. Retrieved from https://www.openthread.io/guides/thread-primer

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 608-615.

Oriwoh, E., & Sant, P. (2013). The forensics edge management system: A concept and design. *Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 10th International Conference on Autonomic and Trusted Computing*, 544-550. https://doi.org/10.1109/UIC-ATC.2013.71

Ortiz, J., Crawford, C., & Le, F. (2019). DeviceMien: Network device behavior modeling for identifying unknown IoT devices. *Proceedings of the 2019 Internet of Things Design and Implementation*, 106-117. https://doi.org/10.1145/3302505.3310073

Park, J. K., Kim, J., & Kang, S. J. (2018). A situation-aware indoor localization (SAIL) system using a LF and RF hybrid approach. *Sensors, 18(11),* 3864. https://doi.org/10.3390/s18113864

Peng, L., Zhang, J., Liu, M., & Hu, A. (2019). Deep learning based RF fingerprint identification using differential constellation trace figure. *IEEE Transactions on Vehicular Technology, 69*(1), 1091-1095. https://doi.org/10.1109/TVT.2019.2950670

Pfeffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology,* 83-106.

Prayudi, Y., & Azhari, S. (2015). Digital chain of custody: State of the art. *International Journal of Computer Applications, 114*(5).

Qing, G., Wang, H., Guo, L., & Yang, J. (2020). Device type identification via network traffic and lightweight convolutional neural network for Internet of Things. *IEEE Access, 8*, 200219-200228. https://doi.org/10.1109/ACCESS.2020.3032469

Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing, 19,* 723-740.

Quick, D., & Choo, K. K. R. (2018). IoT Device Forensics and Data Reduction. *IEEE Access, 6,* 47566-47574.

Rashid, K. M., Louis, J., & Fiawoyife, K. K. (2019). Wireless electric appliance control for smart buildings using indoor location tracking and BIM-based virtual environments. *Automation in Construction, 101,* 48-58.

Salman, O., Elhajj, I. H., Chehab, A., & Kayssi, A. (2019). A machine learning based framework for IoT device identification and abnormal traffic detection. *Transactions on Emerging Telecommunications Technologies, 33*(3). https://doi.org/10.1002/ett.3743

Sánchez, P. M. S., Valero, J. M. J., Celdrán, A. H., Bovet, G., P., M. G., & Pérez, G. M. (2021). A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. *IEEE Communications Surveys & Tutorials, 23(2),* 1048-1077.

Shao, S., Khreishah, A., & Khalil, I. (2018). RETRO: Retroreflector based visible light indoor localization for real-time tracking of IoT devices. *Proceedings of*

the IEEE INFOCOM 2018-IEEE Conference on Computer Communications, 1025-1033. https://doi.org/10.1109/INFOCOM.2018.8485817

Shao, S., Khreishah, A., & Khalil, I. (2020). Enabling Real-Time Indoor Tracking of IoT Devices Through Visible Light Retroreflection. *IEEE Transactions on Mobile Computing, 19*(4), 836-851. https://doi.org/10.1109/TMC.2019.2901665

Sigfox. (2020). *Network Coverage.* Retrieved March 10, 2021, from https://www.sigfox.com/en/coverage

Silicon Labs. (2018a). *Z-Wave 500 Series SDK Contents v6.71.03.* Retrieved from https://www.silabs.com/documents/public/user-guides/INS12366%20-Instruction-Working-500-Series-Environment-User-Guide.pdf

Silicon Labs. (2018b). *Z-Wave Application Security Layer (S0).* Retrieved from https://www.silabs.com/wireless/z-wave/specification/security

Silicon Labs. (n.d.). *Key priorities for sub-GHz wireless deployment.* Retrieved from https://www.silabs.com/documents/public/white-papers/Key-Priorities-for-Sub-GHz-Wireless-Deployments.pdf

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

Stats NZ. (2020). *New homes around 20 percent smaller.* Retrieved from https://www.stats.govt.nz/news/new-homes-around-20-percent-smaller

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (Eds.). (2010). *Vision and challenges for realising the Internet of Things*. Publications Office of the European Union.

Thiesse, F., & Michahelles, F. (2006). An overview of EPC technology. *Sensor Review, 26*(2), 101-105. https://doi.org/10.1108/02602280610652677

Thread Group. (2017). *Thread 1.1.1 Specification.* Retrieved from https://www.threadgroup.org/technology/ourtechnology#specifications

Thread Group. (2022a). *Thread Group.* Retrieved from https://www.threadgroup.org/thread-group

Thread Group. (2022b). *Thread Group Support.* Retrieved from https://www.threadgroup.org/Support

UNSW Australia. (2017). Testbed Setup for IoT Data Collection. http://149.171.189.1

Unwala, I., Taqvi, Z., & Lu, J. (2018). Thread: An IoT protocol. *Proceedings of the 2018 IEEE Green Technologies Conference (GreenTech),* 161-167.

Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., . . . Baldini, G. (2014). Internet of Things strategic research and innovation agenda. In O. Vermesan & P. Friess (Eds.), *Internet of Things - From research and innovation to market deployment* (pp. 7-142). River Publishers.

Vermesan, O., Friess, P., Guillemin, P., Giaffreda, R., Grindvoll, H., Eisenhauer, M., . . . Tragos, E. Z. (2015). Internet of Things beyond the hype: Research, innovation and deployment. In O. Vermesan & P. Friess (Eds.), *Building the hyperconnected society* (Vol. 43). River Publishers.

Vermesan, O., Friess, P., Guillemin, P., Serrano, M., Bouraoui, M., Freire, L. P. r., . . . Wees, A. v. d. (2016). Internet of Things digital value chain connecting research, innovation and deployment. In O. Vermesan & P. Friess (Eds.), *Digitising the Industry Internet of Things connecting the physical, digital and virtual worlds* (Vol. 49). River Publishers.

Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., . . . Cousin, P. (2013). Internet of Things strategic research and innovation agenda. In O. Vermesan & P. Friess (Eds.), *Internet of Things : Converging technologies for smart environments and integrated ecosystems* (pp. 7-152). River Publishers.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American 265*(30), 94-104. https://doi.org/10.1109/MPRV.2002.993141

Williams, J. (2011). *ACPO Good Practice Guide for Digital Evidence*. Retrieved from https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf

Xu, Q., Zheng, R., Saad, W., & Han, Z. (2015). Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials 18*(1), 94–104. https://doi.org/10.1109/COMST.2015.2476338

Yadav, P., Feraudo, A., Arief, B., Shahandashti, S. F., & Vassilakis, V. G. (2020). Position paper: A systematic framework for categorising IoT device fingerprinting mechanisms. *Proceedings of the 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, 62-68. https://doi.org/10.1145/3417313.3429384

Z-Wave Alliance. (2022). *About Z-Wave Technology.* Retrieved from https://z-wavealliance.org/about_z-wave_technology/

Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials, 21*(3), 2568-2599. https://doi.org/10.1109/COMST.2019.2911558

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards building a forensics aware eco system for the Internet of Things. *Proceedings of the 2015 IEEE International Conference on Services Computing (SCC)*, 279-284. https://doi.org/10.1109/SCC.2015.46