Use of Narrow Band Technologies in Smart Home

Major Project Report

Submitted in fulfillment of the requirements
for the degree of

Master of Technology
in
Electronics & Communication Engineering
(Embedded Systems)

By

Yash Patel

(22MECE06)

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A+' GRADE

Electronics & Communication Engineering Department
Institute of Technology
Nirma University
Ahmedabad-382 481

May 2024

Use of Narrow Band Technologies in Smart Home

Major Project Report

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology

in

Electronics & Communication Engineering

By

Yash Patel
(22MECE06)

Under the guidance of

External Project Guide:

Jitendra Vairagade

Principal Engineer/ Manager

NXP India Pvt. Ltd.,

Pune.

Internal Project Guide:

Dr. Bhupendra Fataniya

Assistant Professor, EC Department,

Institute of Technology,

Nirma University, Ahmedabad.

Electronics & Communication Engineering Department

Institute of Technology-Nirma University

Ahmedabad-382 481

May 2024

Declaration

This is to certify that

a. The thesis comprises my original work towards the degree of Master of Technology in Embedded Systems at Nirma University and has not been submitted elsewhere for a degree.

b. Due acknowledgement has been made in the text to all other material used.

- Yash Patel
22MECE06

Disclaimer

"The content of this paper does not represent the technology,opinions,beliefs, or positions of NXP India Pvt. Ltd.,its employees,vendors, customers, or associates."

Certificate

This is to certify that the Major Project entitled **"Use of Narrow Band Technologies in Smart Home"** submitted by **Yash Patel (22MECE06)**, towards the partial fulfilment of the requirements for the degree of Master of Technology in Embedded Systems, Nirma University, Ahmedabad is the record of work carried out by him under our supervision and guidance. In our opinion, the submitted work has reached the level required for being accepted for examination. The results embodied in this major project, to the best of our knowledge, haven't been submitted to any other university or institution for the award of any degree or diploma.

Date: Place: Ahmedabad

Dr. Bhupendra Fataniya

Internal Guide & Assi. Professor (ECE)
Institute of Technology
Nirma University,
Ahmedabad 382 481

Dr. N. P. Gajjar

PG Coordinator (Embedded Systems)
Institute of Technology
Nirma University,
Ahmedabad 382 481

Dr. Usha Mehta

Professor & HoD, EC
Institute of Technology
Nirma University,
Ahmedabad 382 481

Director

School of Technology
Institute of Technology
Nirma University,
Ahmedabad 382 481

Date : 17 May, 2024

To Whomsoever It May Concern

Ongoing Internship Certificate

This is to certify that **Mr. Patel Yash Harishbhai (Emp ID: 13984659)**, is undergoing an internship at **NXP India Pvt. Ltd., Pune.** He started the internship on **17 July, 2023** on the **project titled: Use of Narrow Band Technologies in Smart Home under the guidance of Jitendra Vairagade.**

Under the company's Intellectual Proprietary rights clause any disclosure of scripts or software programs written during the Internship tenure which are subjected to be used under project are strictly private and confidential and cannot be disclosed to any person outside the company.

For NXP INDIA Pvt Ltd

Manish Subodh
HR Manager

Acknowledgement

It gives me immense pleasure to express gratitude to **Dr. Bhupendra Fataniya**, Assistant Professor, EC Department, Institute of Technology, Nirma University for his valuable guidance and continual encouragement throughout this work.

The chain of my gratitude would be incomplete if I forgot to thank the first cause of this chain, **Dr. Usha Mehta**, Hon'ble Head and **Dr. N.P Gajjar**, PG Coordinator of Embedded Systems, EC Department Institute of Technology, Nirma University for her kind support and providing basic infrastructure, a healthy research environment and for providing this exhilarating opportunity and continual support in reaching a higher goal.

It is a pleasure to be associated with NXP India Pvt. Ltd., and I would like to thank the entire staff. I am grateful to **Jitendra Vairagade**, Team Manager, NXP Semiconductor and Other Team members, for their valuable guidance and continual encouragement throughout this work. The appreciation and continual support imparted have been a great motivation for me in reaching a higher goal. Their guidance has triggered and nourished the intellectual maturity that I will benefit from, for a long time to come.

A special thank you is expressed wholeheartedly to Dr Rajesh N. Patel, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout this work. I would also thank the Institution and all faculty members of the Electronics and Communication Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Yash Patel

22MECE06

Contents

Declaration iii

Disclaimer iv

Certificate v

Acknowledgement vii

Abstract xiii

1 Introduction 1

1.1 Company Profile 1

1.2 Mission and Vision 2

1.3 Products and Services 2

1.4 Problem Statement 2

1.5 Objective 3

1.6 Approach 3

1.7 Scope of Work 3

1.8 Outline of Thesis 5

2 Literature Survey 6

3 Narrow-Band Technology 8

3.1 Introduction 8

3.2 Narrow Band Signal 10

3.3 Various Technology for the smart Home Automation 10

4 Open Thread **12**
4.1 Overview 12
4.2 Introduction 13
4.2.1 General Characteristics 13
4.3 IEEE 802.15.4 PHY/MAC 14
4.4 No Single Point of Failure 15
4.5 Thread Device Types and Roles 16
4.5.1 Routing Full Thread Devices 16
4.5.2 Non-Routing Full Thread Devices 16
4.5.3 Non-Routing Minimal Thread Devices 17
4.5.4 Border Router 17
4.6 Network Topology 18
4.6.1 Mesh Networks 18
4.6.2 MLE (Mesh Link Establishment) Messages 19
4.7 Adding a new device to a Thread Network 20
4.7.1 Discovery 20
4.7.2 Commissioning 21
4.7.3 Attaching 21

5 ZigBee **22**
5.1 Overview 22
5.2 General Characteristics 23
5.3 Network Node Types 23
5.3.1 Coordinator 24
5.3.2 Router 24
5.3.3 End Devices 24
5.4 Network Topology 25
5.5 ZigBee Profiles 26

6 Networking Experiments and Results **27**
6.1 Results of First Phase 27
6.2 Results of Final Phase 31

7 Conclusion **37**

References **38**

List of Tables

4.1 Device Limits 18

6.1 Experiment Values 29
6.2 Hop Wise Finding 35
6.3 Payload wise Findings 36
6.4 Distance Wise Findings 36

List of Figures

4.1 Overview of Thread Specification 14
4.2 Role of Thread Border Router 18
4.3 Basic Thread Network Topology and Devices 19
4.4 Router Eligible End Device (REED) with Thread Network Credentials attaching to a Parent Router 21

6.1 Result1 29
6.2 Result2 30
6.3 Result3 30
6.4 Result4 30
6.5 Setup to Perform Experiments 34

Abstract

This project aims to explore and analyze the utilization of narrow-band technologies in the context of smart home systems. The increasing complexity and diversity of smart home devices necessitate efficient communication protocols to enhance connectivity and streamline interactions. Narrow-band technologies, characterized by their narrow frequency range and low power consumption, emerge as promising solutions to address these challenges.

Energy efficiency is a critical aspect of smart homes, and the project will investigate how narrow-band technologies contribute to reduced power consumption in connected devices. By optimizing energy usage, we aim to enhance the overall sustainability and longevity of smart home systems.

Moreover, the research will address the security and privacy implications associated with implementing narrow-band technologies. Understanding potential vulnerabilities and developing robust security measures are crucial components of creating a trustworthy and resilient smart home environment.

The insights gained from this project will inform the design and implementation of future smart home systems, providing a foundation for more efficient, secure, and interconnected living spaces. As the Internet of Things continues to evolve, the integration of narrow-band technologies holds the potential to redefine the landscape of smart home technology, offering users a more seamless and reliable experience.

Chapter 1

Introduction

In an era where connectivity is the cornerstone of technological advancements, the integration of narrow-band technology into Smart Home systems emerges as a transformative leap forward. This technology offers a spectrum of compelling motivations, driving us to explore its application within the realm of intelligent home solutions.

Moreover, the adoption of narrow-band technology introduces a paradigm shift in the scalability and deployment of smart devices. It's suitability for supporting a multitude of connected devices within a smart home ecosystem promotes a cohesive and integrated user experience. This scalability paves the way for the creation of innovative applications, enhancing the overall intelligence and responsiveness of the home environment.

1.1 Company Profile

NXP Semiconductors, headquartered in Eindhoven, Netherlands, is a leading global semiconductor manufacturer with a rich history dating back to its founding in 1953. Specializing in high-performance mixed-signal electronics, NXP plays a pivotal role in shaping the future of connectivity, security, and mobility. The company's diverse portfolio encompasses a wide range of products, including microcontrollers, secure identification solutions, and automotive semiconductor solutions. NXP is at the forefront of innovation, driving advancements in areas such as the Internet of Things (IoT), edge computing, and secure connectivity. With a commitment to sustainability, NXP emphasizes responsible business practices and is dedicated to creating technologies that not only enhance efficiency but also contribute to a more sustainable and connected world.

1.2 Mission and Vision

The mission of the company is to build solutions, not just products that enhance the capabilities of people, organizations, and the world at large. NXP builds design purpose-built, rigorously tested technologies that enable devices to sense, think, connect, and act intelligently to improve people's daily lives. NXP debuts i.MX applications processor with a dedicated neural processing unit for advanced machine learning at the edge and also introduces S32G networking processor unlocking the value of vehicle data.

1.3 Products and Services

NXP has given so many products in the market like multi-core SoCs and the ARM-based processors and microcontrollers, power architecture processors, Additional MPU/MCU Architectures, Automotive processors, Wireless products such as MiGLO, Sigfox LPWAN network, Matter and RF products and Security authentication products.

1.4 Problem Statement

The integration of reliable technology in Smart Home Automation systems is imperative for ensuring seamless, efficient, and secure operations. However, a critical challenge emerges with the existence of a single point of failure within the architecture. This vulnerability poses a substantial risk to the entire smart home ecosystem, as the failure of a central component can disrupt the functionality of interconnected devices, compromising user experience, security, and overall system dependability. Addressing this issue is paramount to achieving a robust and resilient Smart Home Automation infrastructure that can withstand potential failures and provide users with a consistently reliable and secure living environment.

1.5 Objective

To determine performance, robustness, and scalability among wireless protocols and derive the latency, range, and max device support along with Cost and power consumption.

1.6 Approach

One approach to providing free licensed, low-cost, and low-power wireless connectivity with high efficiency is by utilizing open-source protocols like Open Thread, ZigBee, or LoRa. These protocols are designed for low-power, long-range communication, making them suitable for various IoT applications. Additionally, leveraging unlicensed frequency bands, such as the 2.4 GHz ISM band, can contribute to cost-effectiveness.

Implementing mesh networking can enhance coverage and reliability without a centralized infrastructure. Open-source software and hardware solutions, like OpenThread for ZigBee or The Things Network for LoRa, enable community-driven development, reducing costs and promoting accessibility.

1.7 Scope of Work

A wireless technology involves exploring the vast landscape of connectivity options that enable communication without physical cables. Technologies such as Wi-Fi, Bluetooth, ZigBee, and NFC have become integral parts of our daily lives, connecting devices seamlessly.

1. Wi-Fi, known for its high-speed data transfer over local networks, is prevalent in homes and businesses.
2. Bluetooth facilitates short-range wireless communication between devices like smartphones, headphones, and speakers.
3. ZigBee, on the other hand, is designed for low-power, low-data-rate applications in home automation and IoT devices.
4. NFC (Near Field Communication) allows contactless data exchange between devices

within close proximity.
As technology continues to advance, the search for and cataloging of wireless technologies remain crucial for understanding the evolving landscape of interconnected devices.
To compare wireless technologies for the best suitable use for our application in terms of scalability, efficiency, feasibility, compatibility, interoperability, and reliability.
Exploring case studies in wireless technologies, particularly OpenThread and ZigBee, offers valuable insights into their diverse applications. OpenThread, an open-source implementation of the Thread networking protocol, has found success in creating robust and scalable mesh networks for smart homes and industrial IoT applications. Case studies highlight its efficiency in handling low-power devices and maintaining reliable communication. Examining real-world scenarios reveals ZigBee's efficacy in building energy-efficient solutions and enabling seamless connectivity among devices. By delving into these case studies, one gains a deeper understanding of how OpenThread and ZigBee contribute to the evolution of wireless technology, shaping the landscape of the Internet of Things.

Through a comprehensive exploration of case studies in wireless technologies like OpenThread and ZigBee, we can pave the way for designing a prototype that ensures a cohesive integration of numerous elements. By synthesizing the strengths and lessons learned from these case studies, our prototype can leverage OpenThread's robust mesh networking capabilities and ZigBee's efficiency in short-range communication. This synthesis aims to create a holistic solution that addresses the challenges posed by diverse devices within a network. The prototype would prioritize seamless connectivity, power performance, and reliability, drawing inspiration from the successful implementations highlighted in the case studies. This iterative approach, grounded in real-world examples, enhances the probability of making a well-rounded and effective wireless technology prototype that caters to the intricate demands of modern connectivity ecosystems.

1.8 Outline of Thesis

This report has six chapters, each explaining a different part of the project. Chapter 1 describes the introductory part. Chapter 2 looks at details of narrowband technology and narrowband signal and also about the various technologies for smart home automation. Chapter 3 covers open thread technology which which is one of the wireless technologies. Chapter 4 highlights ZigBee which is also one of the wireless technology. Chapter 5 explains the work done on these wireless technologies in NXP Semiconductor. The last chapter gives a final reflection on the internship, concluding the report.

Chapter 2

Literature Survey

ZigBee and OpenThread are wireless communication protocols commonly employed in the realm of IoT (Internet of Things) to facilitate low-power, short-range communication between devices. This literature review aims to explore the key characteristics, applications, and comparisons between ZigBee and OpenThread. The growing demand for Internet of Things (IoT) applications has resulted in a huge amount of data that requires the use of big data analytics. The integration of big data analytics into IoT-based smart cities as well as advanced smart home applications can greatly benefit from the development of wireless communication protocols, with the Thread protocol emerging as a promising alternative. The thread is based on IEEE 802.15.4 and has advanced features such as meshing, IPv6 support and multiple gateways that provide no single point of failure. The author of [1] presents a low-cost mesh design and evaluation using a Raspberry Pi, an nRF52840 dongle, and OpenThread 1.2 (ie, an open source software implementation of the Thread protocol stack).

The paper [2] presents an extension of the Internet subnet by connecting resource-constrained nodes (e.g., embedded sensors and actuators) over multiple wireless hops. This is necessary to support the Internet of Things (IoT) of the future. RPL, the IPv6 routing standard for low-capacity and lossy networks, attempted to achieve this goal, but was not widely adopted in practice. Basically, this paper provides a comparative analysis of the technical aspects of RPL and Thread based on their specifications and explains why using Thread instead of RPL might make sense for the Internet in the future. In particular, the main differences between RPL and Thread are their respective scopes and multihop network architectures, which lead to Thread's unique design and advantages over RPL.

Article written by system engineer [3] provides information about how automation is even more important nowadays for both residential, commercial, and industrial domains. It provides a significant amount of details related to ZigBee and open thread, their application based on need and their characteristics, factors for selection of technology, etc. While author in [4] introduced the development of ZigBee technology for the applications, where low cost, low data rate, and more battery life were the main requirements. Paper [6, 7] indicates the performance analysis review of ZigBee and open-thread wireless technology which gives a basic overview of how technology will be used in different environments for smart home applications and how networking for the IOT applications will be best implemented using these technologies.

The author of [8] gives a brief look at how ZigBee effectively delivers solutions for a variety of areas including consumer electronic device control, energy management, and efficient home and commercial building automation as well as industrial plant management.

Other links in the references chapter show the information on wireless technology and how people have difficulties developing applications based on those technologies and solutions for the issues for development and also illustrate the characteristics of various technologies.

Chapter 3

Narrow-Band Technology

3.1 Introduction

Narrowband technology refers to communication methods that operate within a narrow range of frequencies. This technology is crucial in various fields, including telecommunications, radio, and wireless systems. In the context of wireless communication, narrowband technologies have specific characteristics that differentiate them from broadband technologies.

Key aspects of narrowband technology:

Frequency Range : Narrowband technologies utilize a small portion of the radio frequency spectrum, often working within a limited bandwidth. This restricted spectrum allocation allows for more efficient and focused transmission of data.

Low Data Rate : Compared to broadband technologies that can transmit large volumes of data at high speeds, narrowband technologies typically handle lower data rates. They are optimized for transmitting smaller amounts of data but excel in maintaining connectivity over longer distances.

Efficiency : Narrowband technologies are designed for efficiency in terms of power consumption and spectral usage. By utilizing a smaller frequency range, they can transmit signals more effectively, which can be advantageous for applications where conserving battery power is crucial, such as in IoT devices.

Applications : Narrowband technology finds extensive use in various applications, including but not limited to telecommunications, IoT (Internet of Things), smart home devices, industrial automation, and remote monitoring systems. For example, in smart homes, narrowband technologies like ZigBee or Z-Wave enable smart devices to communicate efficiently, creating interconnected systems for automation and control.

Interoperability: Many narrowband technologies used in home automation are designed to be interoperable, meaning devices from different manufacturers can communicate with each other. This is important for creating a seamless smart home experience where devices can work together regardless of their brand or type.

Interference Mitigation : The focused nature of narrowband signals makes them less susceptible to interference from other signals operating on different frequencies. This characteristic is particularly beneficial in environments with high radio frequency interference.

Long-Range Communication : Narrowband technologies can often provide long-range communication capabilities due to their ability to maintain signal integrity over extended distances.

Security : Some narrowband technologies offer enhanced security features, including encryption and secure communication protocols, ensuring data privacy and integrity.
In essence, narrowband technology optimizes the use of limited frequency ranges for effective, reliable, and often long-range communication while ensuring efficient power consumption, making it a preferred choice for various wireless communication applications in different sectors.

3.2 Narrow Band Signal

Narrowband signals are signals that use a narrow frequency range or have a small bandwidth. In the audio spectrum, narrowband sounds are sounds that use a narrow range of frequencies. In a telephone, narrowband is usually considered to cover the frequencies of 300-3400 Hz, or the audio band.

In radio communications, a narrowband channel is a channel where the message bandwidth does not significantly exceed the coherent bandwidth of the channel.

Narrowband in wired channel analysis means that the channel under consideration is narrow enough that its frequency response can be kept flat. The message bandwidth is therefore less than the link bandwidth of the channel. In other words, no channel has perfectly uniform fading, but the analysis of many aspects of wireless systems is greatly simplified if uniform fading can be assumed.

3.3 Various Technology for the smart Home Automation

Here are a few examples of narrowband technologies commonly used in smart home automation:

ZigBee : ZigBee is a wireless communication protocol used for creating personal area networks with small, low-power digital radios. It's often used in smart home devices like smart bulbs, smart plugs, and sensors due to its low power consumption and ability to create mesh networks.

Z-Wave : Z-Wave is another wireless communication protocol designed specifically for smart home devices. It operates on low-power radio waves and allows devices to communicate with each other. Z-Wave is known for its interoperability among various brands of smart home products.

Thread : Thread is an IP-based wireless protocol that provides reliable, secure, and low-power connectivity for smart home devices. It's designed to create robust mesh networks, allowing devices like thermostats, lights, and locks to communicate seamlessly.

Bluetooth Low Energy (BLE) : BLE is a wireless technology that's widely used in smart home devices due to its low power consumption. It allows for short-range communication between devices, such as connecting smartphones to smart locks or sensors.

LoRaWAN : LoRaWAN (Long Range Wide Area Network) is a wireless technology used for long-range communication in smart home applications. It's suitable for low-power, battery-operated devices transmitting small amounts of data over long distances.

In a nutshell, These technologies enable smart home devices to communicate effectively, providing users with interconnected and efficient home automation solutions. OpenThread is an open-source implementation of the Thread networking protocol. Nest has released OpenThread to make the technology used in Nest products more broadly available to developers to accelerate the development of products for the connected home. A detailed explanation is given in the following chapter.

Chapter 4

Open Thread

4.1 Overview

Open Thread is an open-source, low-power wireless mesh networking protocol developed by Nest, a subsidiary of Google (now part of the Matter protocol). It is specifically designed for connecting Internet of Things (IoT) devices in a reliable, secure, and power-efficient manner. Open Thread is based on the IEEE 802.15.4 standard and operates in the 2.4 GHz frequency band. As it provides IP connectivity, its deployment is anticipated in various IOT fields e.g., home automation, building automation, wireless sensor networks, etc.

This protocol facilitates the creation of robust and self-healing mesh networks, allowing IoT devices to communicate with each other and with the Internet. Open Thread's key features include low latency, scalability, support for thousands of devices, and seamless interoperability. It implements various security mechanisms, including encryption and authentication, ensuring data privacy and network integrity.

Open Thread enables devices to form decentralized networks, promoting flexibility and resilience. Its open-source nature encourages collaboration and innovation within the IoT ecosystem, fostering the development of diverse applications across smart homes, industrial automation, healthcare, and more.

With its focus on low power consumption, high reliability, and flexibility, Open Thread has become a fundamental technology driving the expansion of interconnected IoT devices and smart environments, contributing significantly to the evolution of the IoT landscape. The general characteristics of the Thread stack and network are presented below.

4.2 Introduction

The Internet of Things (IoT) aims to transform people's lives through smart homes and businesses. At home, the goal is a network of connected devices, lighting, air conditioning, security and entertainment systems, all of which together make consumers' lives more comfortable and satisfying. In commercial buildings, IoT aims to improve the efficiency, functionality, automation and security of buildings such as offices, healthcare facilities, hotels and schools.

4.2.1 General Characteristics

The Thread Specification is an open standard for reliable, cost-effective, low-power, secure, and wireless IPv6 communication. It is designed specifically for connected home and business applications where an IP-based network is desired and multiple application layers can be used on the same network.

- The general characteristics of the Thread stack and network are as follows:
- Simple network layout, deployment and operation - Simple protocols for building, connecting and maintaining fiber networks allow systems to self-determine and resolve routing issues as they arise.
- Secure – Devices do not join the Thread Network unless authorized and all communications are encrypted and secure.
- Small and large networks - Networks can range from a few devices to hundreds of devices communicating seamlessly. The Threaded network layer is designed to optimize network performance based on expected usage. The Thread Domains feature allows multiple networks to work together seamlessly.

• Range – Typical networked devices provide enough range to cover the floor of a typical home or building. Spread spectrum technology is used in the physical layer to achieve good interference tolerance.

• No single point of failure – The stack is designed to provide secure and reliable operations even with the failure or loss of individual devices.

• Low power – End Devices can typically operate for several years on AA type batteries using suitable duty cycles.

This figure 4.1 illustrates an overview of the Thread Specification.

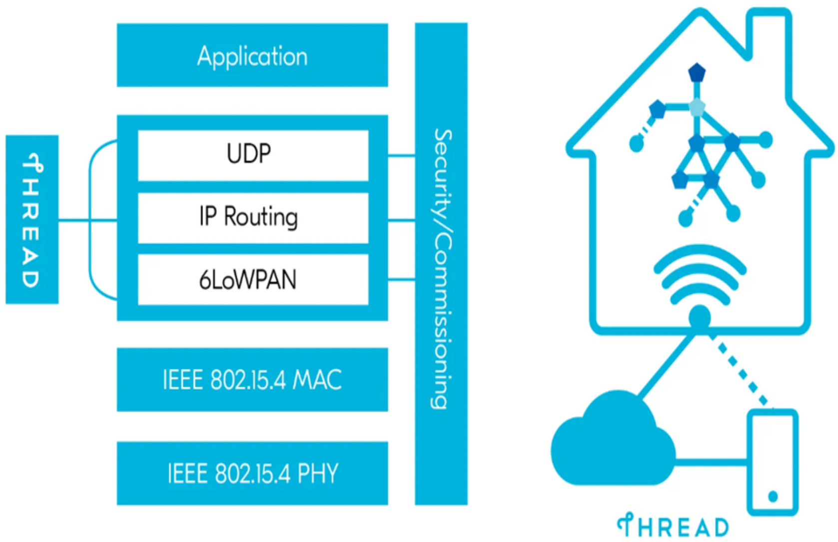

Figure 4.1: Overview of Thread Specification

4.3 IEEE 802.15.4 PHY/MAC

The thread specification uses the PHY (Physical) and MAC (Media Access Control) layers of IEEE 802.15.4 [IEEE802154] for link-layer communication, operating at 250 kbps in the 2.4 GHz band. The thread uses the IEEE 802.15.4-2006 and IEEE 802.15.4-2015 versions of the specifications. The thread specification is based on the IEEE 802.15.4 standard, which provides reliable message transmission between individual devices in a thread at the link level. IEEE 802.15.4 provides a CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance) mechanisms that allows multiple fiber devices to use the shared 2.4 GHz bandwidth by waiting for a free channel before transmitting. IEEE 802.15.4 uses link-layer acknowledgements and retries, which enable reliable transmission of individual messages. Encryption, authentication, and replay protection are also available to ensure secure communication. Routines are defined as low-power devices that collect messages buffered by always-on nodes. IEEE 802.15.4 is a widely used, well-tested protocol that the Thread specification relies on to provide reliable end-to-end communication.

4.4 No Single Point of Failure

In a system of devices using a thread stack, none of these devices represent a single point of failure. Although there are several devices in the system that perform special functions, the structure of the thread is such that they can be replaced without affecting the continuous communication in the Thread Network. For example, a child's Sleepy End Device needs a parent router to communicate, so a parent represents a single point of failure in its communication. However, the Sleepy End Device can choose another parent router if its parent router is not available. Therefore, this transition should not be visible to the user. Although a mesh network is not designed for a single point of failure, certain topologies have single devices without backup capabilities. For example, in the network part of a thread with one Border Router, it is not possible to switch to an alternate Border Router if the Border Router loses power. A router can assume the role of leader in certain threaded operations. This manager must make decisions about the network portion of the thread. For example, a Principal assigns router addresses and allows new router requests. A driver is selected, and if the driver fails, another router becomes the driver. It is this self-contained operation that ensures there are no single points of failure. The Roles of Router and Border Router can both be in the same thread at the same time.

4.5 Thread Device Types and Roles

There are two types of thread devices in the specification: Full Thread Device (FTD) and Minimum Thread Device (MTD). MTD has the lowest requirements for device hardware (such as memory capacity) and power consumption, while FTD is the most versatile in a thread network. These roles are explained in more detail in the following sections.

4.5.1 Routing Full Thread Devices

Router

A Thread Router provides routing services to Thread Devices in the network. Routers also provide connectivity and security services for devices trying to join the network. Routers are not designed to sleep. Routers can downgrade their functionality and become REEDs (Router-eligible End Devices).

Leader

The Leader is an additional role of one Router in a Thread network. The Leader is an elected role of one Router, which takes certain decisions in the Thread network such as allowing REEDs to upgrade to Routers. If the Leader of a Thread Network fails, another Router will be dynamically selected to resume the role. All Routers have the necessary Thread Network Information to seamlessly assume this role.

4.5.2 Non-Routing Full Thread Devices

Router-Eligible End Device (REED)

REEDs have the capability to become Routers but due to the network topology or conditions are not acting as Routers. The Thread Network manages REEDs becoming Routers through the Leader, without user interaction.

Full End Device (FED)

FEDs are end devices like REEDs, however, they do not have the capability to be a Router, so they will never become a Routing Thread Device or Leader.

4.5.3 Non-Routing Minimal Thread Devices

Minimal End Device (MED)

Minimal-end devices (MEDs) communicate only through their Parent Router and cannot forward messages to other devices. A MED has its radio turned on, even when idle.

Sleepy End Device (SED)

Sleepy End Devices (SEDs) communicate only through their Parent Router and cannot forward messages to other devices. A SED has its radio turned off during idle periods and wakes periodically to communicate with its parent.

Synchronized Sleepy End Device (SSED)

Synchronized Sleepy End Devices (SSEDs) communicate only through their Parent Router and cannot forward messages to other devices. An SSED has its radio is turned off during idle periods and wakes periodically to listen for messages from its parent at scheduled intervals.

4.5.4 Border Router

A Border Router is the role of a Thread Device that provides connectivity from the Thread Network to adjacent networks on other physical layers (for example, Wi-Fi or Ethernet). Border Routers provide services for devices within the Thread Network, including routing services for off-network operations. There may be several Border Routers in one Thread Network. Any FTD can provide Border Router services, even if the device is not acting as a Router in the Thread Network.

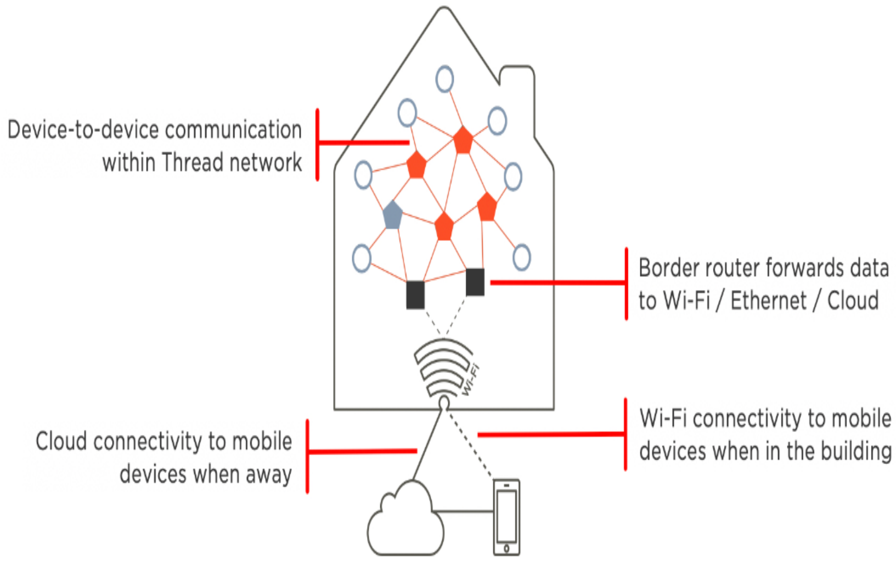

Figure 4.2: Role of Thread Border Router

4.6 Network Topology

The Thread Specification enables full mesh connectivity between all Routers in a Thread Network.

The actual topology is based on the number of Routers in the Thread Network. If there is only one Router, then a basic star topology with a single Router is formed. If there is more than one Router then a mesh topology is automatically formed. Figure 4.3 illustrates the basic topology of a Thread Network and the types of devices.

Table 4.1: Device Limits

Role	**Limit**
Leader	1
Router	32
End Device	511 per Router

4.6.1 Mesh Networks

Mesh networks make wireless systems more reliable by allowing radios to forward messages to other radios. For example, if a node cannot send a message directly to another node,

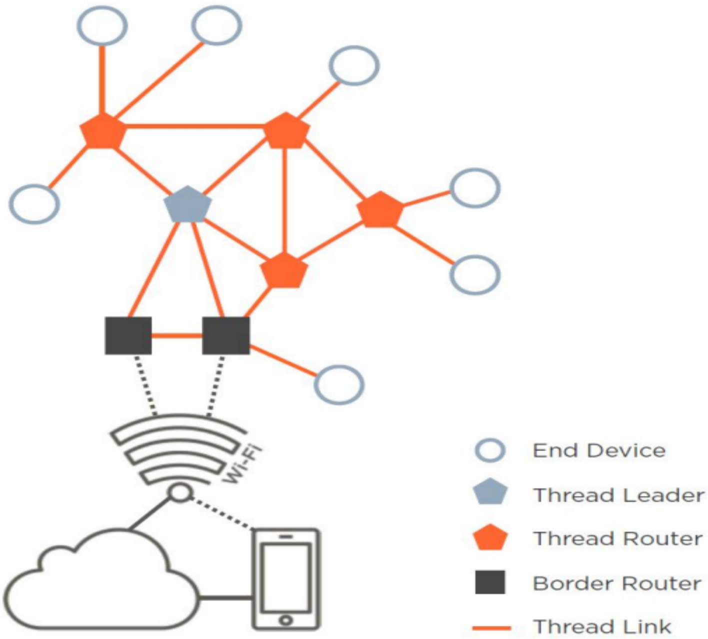

Figure 4.3: Basic Thread Network Topology and Devices

the mesh network forwards the message through one or more intermediary nodes. If an individual link fails, messages can be forwarded along an alternate path. As discussed in the Routing and Network Connectivity section below, the nature of the Thread Network is that all Router nodes maintain routes and connectivity with each other so the mesh is constantly maintained and connected. There is a limit of 32 active Routers in the Thread Network. However, 64 Router addresses are used to allow recycling of Router addresses. In a Thread mesh network, the end devices do not route for other devices. These devices communicate via a Parent Router that handles the routing operations for its Child devices.

4.6.2 MLE (Mesh Link Establishment) Messages

MLE messages are used for establishing and configuring secure radio links, detecting neighboring devices, and maintaining routing costs between devices in the Thread Network. MLE messages are transported using single-hop link-local unicast and multicast between Thread Devices. MLE messages are used for identifying, configuring, and securing links to neighboring devices as the topology and physical environment change. MLE is also used to distribute configuration values that are shared across the Thread Network such as the channel and the Personal Area Network ID. These messages are forwarded with controlled flooding as specified by Multicast Protocol for Low-power and Lossy Networks (MPL). MLE messages also ensure asymmetric link costs are considered when establishing routing costs between two devices. Asymmetric link qualities are common in IEEE 802.15.4 networks. To ensure two-way messaging is reliable, Thread Devices consider bidirectional link quality.

4.7 Adding a new device to a Thread Network

There are three phases a new device must go through before it can participate in a Thread Network:

1. Discovery
2. Commissioning
3. Attaching

Once attached, a device is fully participating in the Thread Network and can exchange application layer information with other devices and services within and beyond the Thread Network.

4.7.1 Discovery

Before a Thread Device can participate in a Thread Network, it must first discover and establish contact with a Joiner Router for commissioning. The joining device iterates through all channels issues an MLE Discovery Request on each channel, and waits for MLE Discovery Responses. The Discovery Response contains a payload including the network name and steering data, to steer devices into joining the Thread Network where they are expected. Once a device has discovered the Thread Network, it uses a link-local channel to the Joiner Router to establish a connection to the commissioning application and perform commissioning.

Discovery and commissioning are only required for the very first attachment of a Thread Device to a Thread Network. Every Thread device stores the Network Credentials in non-volatile memory for subsequent attachments.

4.7.2 Commissioning

Thread Commissioning is the process of authenticating a new device and providing it with the Network Credentials. For this, an authenticated DTLS session is established between a joining Thread Device and a commissioning application on a smartphone, tablet, or webpage. This session is used to securely authenticate the Joiner. If this process is successful, the Joiner Router securely provides the Joiner with the Thread Network Credentials, so that it can attach to the Thread Network.

4.7.3 Attaching

A detached Thread Device with Network Credentials will periodically attempt to attach to a Thread Network by multicasting MLE Parent Requests to nearby Routers and REEDs. If required, a REED will, upon hearing the parent request, upgrade to a Router role to support the connectivity of the newly attached Thread Device. The attaching Thread Device and the Thread Router then use MLE Messages to configure a secure link and provision IPv6 addresses. A Thread Device will always attach as an End Device, and can upgrade to a Router later by requesting a Router ID from the Leader. This attachment process is illustrated in Figure 4.4.

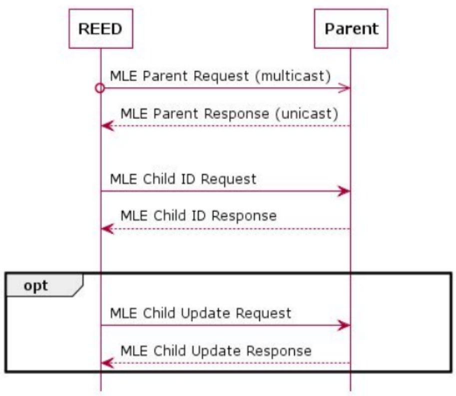

Figure 4.4: Router Eligible End Device (REED) with Thread Network Credentials attaching to a Parent Router

Chapter 5

ZigBee

5.1 Overview

ZigBee is a wireless communication technology designed for low-power, short-range applications, ideal for smart home devices, industrial automation, and sensor networks. It operates on the IEEE 802.15.4 standard, using low energy and providing secure data transfer over short distances. ZigBee networks can support multiple devices, forming a mesh network where each device can communicate with others, enabling efficient and reliable data transmission.

ZigBee aims to enable products and services to work together through standardization and testing. ZigBee is designed with backward and forward compatibility in mind. ZigBee supports sleepy end devices, allowing for long-lasting battery-powered applications. Network devices such as light bulbs are mostly used for routing. ZigBee networks can contain more than a thousand devices simultaneously.

ZigBee network function based on a mesh topology, allowing devices to form connections with one another. Each device can act as a router, passing data through the network until it reaches its intended destination. This mesh architecture enhances reliability and extends the range of communication.

5.2 General Characteristics

ZigBee is intended as a cost-effective and low-power solution. It is targeted to several markets including home automation, building automation, sensor networks, smart energy, and personal health care monitoring.

The general characteristics of a ZigBee network are as follows:

• Low power – Devices can typically operate for several years on AA-type batteries using suitable duty cycles. With extremely careful design and special battery technologies, some ZigBee devices such as gas meters can achieve 20 years of battery life.

• Low data rate – The 2.4 GHz band supports a radio data rate of 250 kbps. Actual sustainable traffic through the network is lower than this theoretical radio capacity. As such, ZigBee is better used for sampling and monitoring applications or basic control applications. See AN1138: ZigBee Mesh Network Performance and AN1142: Mesh Network Performance Comparison.

• Small and large networks – ZigBee networks vary from several devices to thousands of devices communicating seamlessly. The networking layer is designed with several different data transfer mechanisms (types of routing) to optimize the network operation based on the expected use.

• Range – Typical devices provide sufficient range to cover a normal home. Readily available designs with power amplifiers extend the range substantially. A distributed spread spectrum is used at the physical layer to be more immune to interference.

• Simple network installation, start and operation – The ZigBee standard supports several network topologies. The simple protocols for forming and joining networks allow systems to self-configure and fix routing problems as they occur.

5.3 Network Node Types

The ZigBee specification supports at most one coordinator, multiple routers, and multiple end devices within a single network. These node types are described in the following sections.

5.3.1 Coordinator

The ZigBee Coordinator (ZC) is responsible for forming a centralized network. A coordinator is a router with additional features that uses a hard network address of 0x0000. ZigBee coordination functions include selecting a suitable channel after scanning available channels and selecting an extended PAN ID Once the network is formed, the coordinator acts as a router.

The coordinator also has additional tasks, such as acting as a trust center or network manager. The Trust Center manages network security settings and access rights. Network management monitors and corrects network problems such as PAN ID conflicts or channel changes due to interference. These choices are up to the application developer and in some cases are made by the application layer used, such as ZigBee 3.0.

Only a network coordinator can be designated as a centralized trust center for security purposes when starting a network.

5.3.2 Router

ZigBee routers are the core of network topology. They provide routing services to connected devices. A router is the connection of its subnodes to the network. ZigBee routers are designed so that their radio is always on. The router stores the messages in its terminals. This means they are mostly connected because they never sleep. The number of routers in a ZigBee network is not limited. Unlike terminals, routers are not designed to sleep and should generally remain on until the network is established.

5.3.3 End Devices

ZigBee End Devices (ZEDs) are leaf nodes. ZigBee End Devices (ZEDs) are connected to only one other device, their router. ZED can be a sleepy or sleepy terminal. Devices with a sleepy head are designed for low-energy work. In most cases, the device is in sleep mode.

When they are awake, they retrieve messages stored on their parent router. Sleeping terminals always receive power, but do not yet forward or store messages to other devices. They communicate only through their master nodes and, unlike router devices, cannot forward messages intended for other nodes. Depending on the network stack, end devices can be of several types:

Sleepy end power down their radio when idle, and thus conserve resources. However, they must poll their parent node to receive incoming messages and acknowledgments; no data is sent to the sleepy end device until the end device requests it. Sleepy end devices are also sometimes known as rx-off-when-idle devices. This is a standard ZigBee device type.

Non-sleepy end devices do not route messages for other devices but they remain powered during operation. These devices are known as Rx-on-when-idle devices. This is a standard ZigBee device type.

5.4 Network Topology

The ZigBee network layer (NWK) supports star and mesh topologies. In a star topology, the network is controlled by one single device called the ZigBee coordinator. The ZigBee coordinator is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator In mesh topologies, the ZigBee coordinator is responsible for starting the network and choosing certain key network parameters, but the network may be extended through the use of ZigBee routers. Mesh networks allow full peer-to-peer communication. ZigBee routers in mesh networks do not currently emit regular IEEE Std 802.15.4 beacons.

There are two types of networks:

1. Centralized Network: Centralized networks the role of the Trust Center acts as gatekeeper to determine when and who is authorized to join the network.

2. Distributed Network: In a distributed network router forms the network and allows other devices to join in the network.

5.5 ZigBee Profiles

Before ZigBee 3.0, application profiles, or simply profiles, sat on top of the basic ZigBee stack. These were developed to specify the OTA messages required for device interoperability. A given application profile could be certified on either the ZigBee or ZigBee PRO stack. Now, ZigBee 3.0 has introduced an all-encompassing application layer specification for defining OTA behavior for all ZigBee applications.

The following are the application profile groups that existed before ZigBee 3.0:

- Home Automation (HA) – Devices for typical residential and small commercial installations.
- Smart Energy (SE) – For utility meter reading and interaction with household devices.
- Commercial Building Automation (CBA) – Devices for large commercial buildings and networks.
- Telecom Application (TA) – Wireless applications within the telecom area.
- Health Care (HC) – Monitoring of personal health in the home or hospital environment.
- Retail – Monitoring and information delivery in a retail environment.
- ZigBee Light Link – Wireless control of LED lighting systems.

Chapter 6

Networking Experiments and Results

The implementation of the project is divided into two stages:

1.Initial Phase: The first(Initial) phase is basically the trial phase where open thread networking was implemented on a lesser number of devices and its various attributes such as scalability, reliability, and performance were observed.
2.Final Phase: In this phase, A large network of around 150 devices was built, and the same characteristics of a network were analyzed.

6.1 Results of First Phase

In the realm of home automation systems, optimizing performance is crucial for seamless functionality. When comparing OpenThread and ZigBee protocols, performance analysis involves evaluating key metrics such as latency, packet loss, and range. Latency measures the delay in data transmission while minimizing packet loss to ensure data integrity. The range signifies the effective coverage area for connected devices. OpenThread, an open-source implementation of the Thread networking protocol, may offer advantages in terms of flexibility and community support. ZigBee, known for its low power consumption, might excel in scenarios requiring energy efficiency. Tailoring the choice between OpenThread and ZigBee to specific home automation needs can enhance overall system performance by striking a balance between latency, packet loss, and range considerations.

Based on the study of various wireless technologies, the conclusion was made that for our application of smart home automation, open thread and ZigBee both are the best suitable for this application. So here comes to verify the development of it. To verify it, a testing process is performed.

The first and foremost step needed is test setup. Test setup refers to the arrangement and configuration of the equipment used for conducting the tests. It involves specifying how the devices are connected, the network configurations, and any additional components that contribute to the testing process. So here two different experiments were performed with different setups.
Experiment 1: This experiment was conducted with a setup involving a lower number of devices.
Experiment 2: This involved a different setup where a higher number of devices were utilized.

Testing protocols should be defined for testing because here testing protocols refer to specific procedures, methods, and standards followed during the testing process. Some aspects that can be considered are standard compliance, testing procedures, data collection methods, performance metrics, test cases, and controlled variables. In both experiments, the primary action taken was to perform "pinging" from one device to another. This process helped in measuring the time taken by data bytes to travel from one node (device) to another and then return to the original node. This round trip time was measured to understand the latency or delay in data transmission between the devices in each setup. The data collected from these experiments could potentially help in understanding network efficiency, performance bottlenecks, or how network congestion might vary concerning the number of devices involved in data transmission within a network setup. The selection of channels was based on the interference. Network stability is checked by doing multiple runs. Devices were pinged and monitored the data and packet values. Scripts using

Python language are developed for the process such as recording the time and fetching the values from the reports means parsing the data from the log files.

Here the table for the experiment is shown below table 6.1

Table 6.1: Experiment Values

Experiment	Devices	Time Taken
Small Network	5-7	10s
Big Network	20-25	20s
Ping Small Network	5	30s
Ping ig	10-15	35s

Latency and time taken is directly proportional to the number of devices connected in the network. Some experimental results are presented in the figure 6.1, 6.2, 6.3 and 6.4.

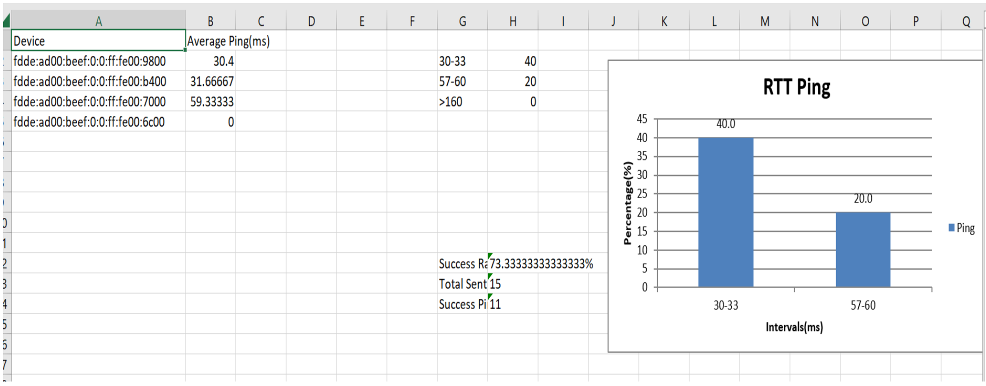

Figure 6.1: Result1

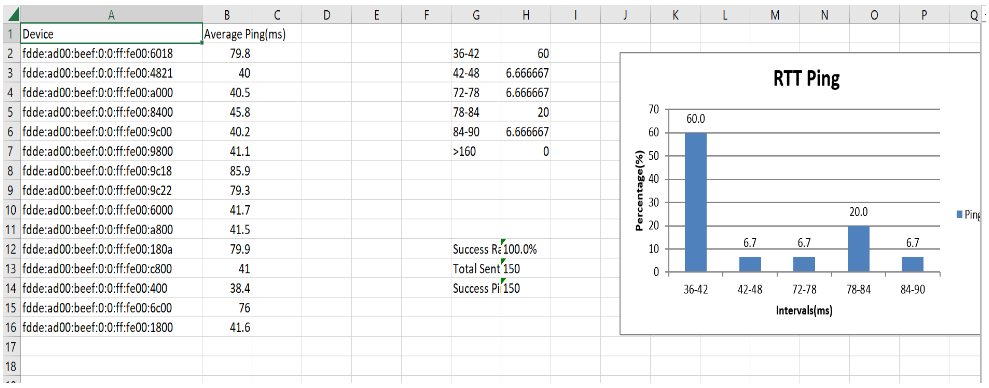

Figure 6.2: Result2

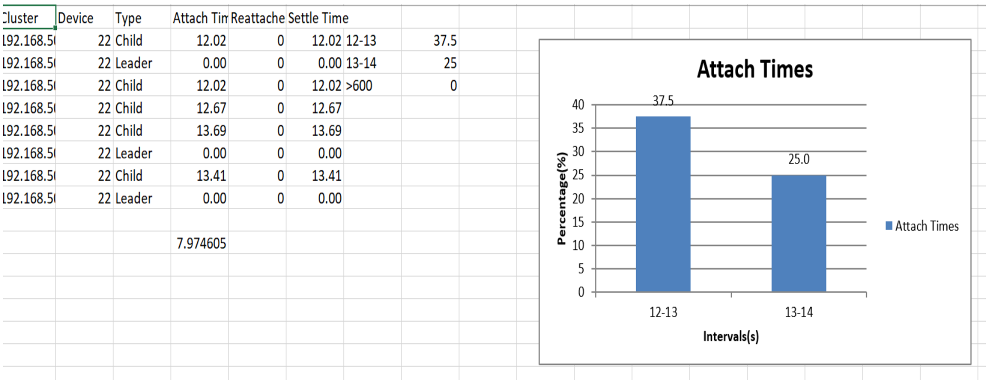

Figure 6.3: Result3

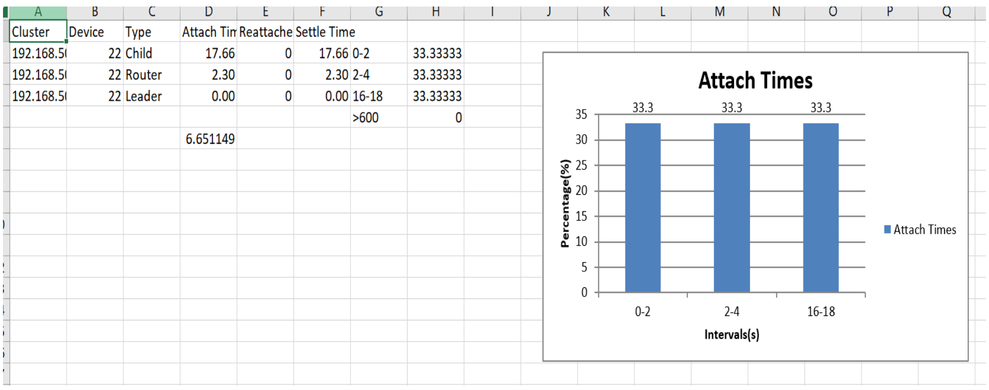

Figure 6.4: Result4

6.2 Results of Final Phase

In large and diverse networks, spanning various environments from smart homes to industrial settings, the complexities of managing power consumption become paramount. ZigBee and Open Thread protocols appear as crucial players, each offering nuanced approaches to ensuring low-power operation in these complex ecosystems. ZigBee, built upon the IEEE 802.15.4 standard, inherently prioritizes energy efficiency by employing techniques like low-duty cycle operation, allowing devices to conserve power during periods of inactivity. Moreover, ZigBee's use of low-power wake-up mechanisms enables devices to remain in a low-power state minimizing overall energy consumption. This capability is particularly helpful in scenarios where devices are deployed in remote or battery-powered environments, such as smart sensors in agricultural fields or industrial equipment checking systems.

However, Open Thread, as an open-source implementation of the Thread protocol, also emphasizes energy efficiency. Leveraging IPv6 (Internet Protocol Version 6) and 6LoWPAN technologies, Open Thread perfects communication protocols to minimize overhead and reduce power consumption without sacrificing reliability or performance. Through features like low-power listening and adaptive synchronization, Open Thread enables devices to synchronize their communication schedules dynamically, allowing them to sleep for longer periods and conserve energy while supporting network responsiveness. This adaptability is especially beneficial in large-scale deployments where devices may be used in diverse environments with fluctuating network conditions and traffic patterns.

ZigBee and Open Thread protocols stand for sophisticated solutions for achieving low-power operation in large and diverse network environments. Their nuanced approaches to energy efficiency, coupled with robust network management features, make them indispensable tools for enabling sustainable and reliable IoT deployments across various industries and applications.
The steps followed to implement this setup and perform the experiment are described below.

1. Hardware Setup:

• Use NXP's SoCs (system on chip) and chipsets for creating the network.

• Bring up all boards with required files and configurations.

• Install the required software and drivers on each board.

2. Network Connection:

• Connect the boards to an Access Point (AP) for Internet access.

• Ensure remote access to the boards for management and monitoring purposes.

3. Deployment:

• Distribute the boards to distinct locations within the office area to simulate real-world scenarios.

4. Network Configuration:

• Create an Open Thread network on the boards.

• Appoint one board as the leader and configure the rest as routers.

• Ensure all boards are connected in a mesh network topology.

5. End Device Addition:

• Add several end devices to the network.

• Ensure all end devices are connected through the AP for network access.

6. Network Scaling:

• Gradually increase the number of devices in the network, up to the target size of 150 devices.

• Test the network's performance and stability at each stage.

7. Testing and Monitoring:

• Conduct thorough testing of the network's functionality, performance, and reliability.

• Check the network using proper tools to find and address any issues that arise.

8. Data Collection and Analysis:

• Collect data on network performance, including throughput, latency, and packet loss.

• Analyze the data to evaluate the network's performance under various conditions and loads.

The setup consists of an array of clusters distributed through a building floor. Each cluster contains multiple development boards connected via serial to an NXP's SoCs with Wi-Fi enabled to report processing and network activity to a Central Server. The Wi-Fi network was configured on Channel 3 while the Thread network was settled on Channel 20.
Below figure shows the experiment setup for final phase.

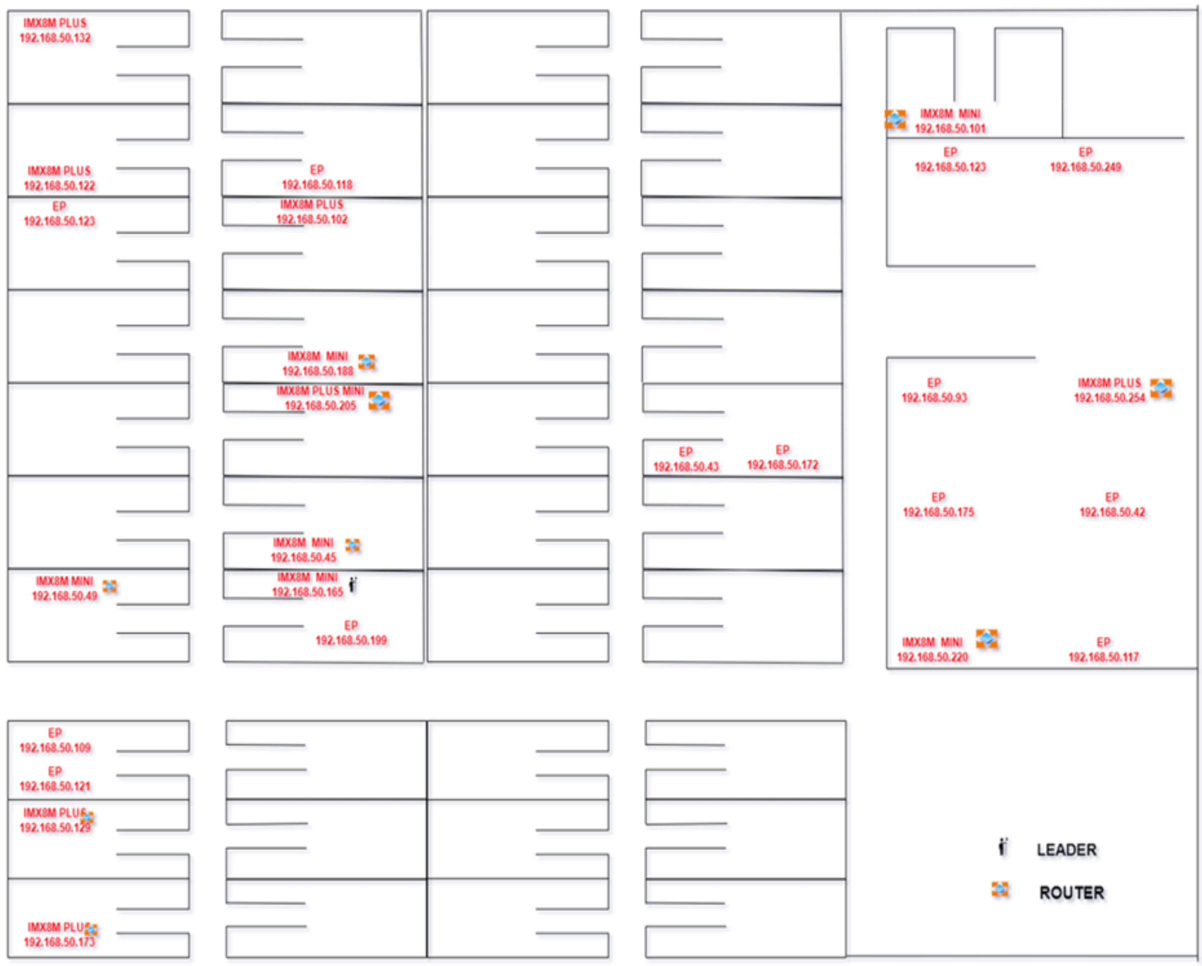

Figure 6.5: Setup to Perform Experiments

Various findings from the experiments are presented below.

1. Hop Wise Findings: There was a noticeable increase in RTT (Round Trip Time) as the number of hops in the network increased. This is a common phenomenon in multi-hop networks, where each additional hop introduces additional latency.

• The increase in RTT can be attributed to the fact that messages are transmitted from hop to hop in a multi-hop network. Each intermediate node in the path introduces a certain amount of delay, resulting in an overall increase in RTT.

• Larger networks with more hops are likely to experience higher RTT compared to smaller networks with fewer hops. The results obtained from this experiment is shown in table 6.2.

Table 6.2: Hop Wise Finding

Hop Wise					
SN	**Device Role**	**Ping Type**	**Ping Hop**	**RTT**	**Pay Load**
1	Router	OT MLE	1	128.66	105
2	Router	OT MLE	2	142	105
3	Router	OT MLE	3	165	105
4	Child	OT MLE	1	118	105
5	Child	OT MLE	2	165	105
6	Child	OT MLE	3	192.33	105

2. Payload wise Findings:

• When the payload size was higher, messages were fragmented into smaller packets. This is a widespread practice in network communication, especially when dealing with large data payloads that cannot be transmitted in a single packet.

• The results showed that as the payload size increased, the RTT also increased. This can be attributed to the fact that larger payloads require more time to send, especially when messages are fragmented into smaller packets. The results of this experiment are presented in table 6.3.

Table 6.3: Payload wise Findings

Payload Wise					
SN	**Device Role**	**Ping Type**	**Ping Hop**	**RTT**	**Pay Load**
1	Router	OT MLE	1	42.66	50
2	Router	OT MLE	1	102	100
3	Router	OT MLE	1	170.66	250
4	Router	OT MLE	2	78	50
5	Router	OT MLE	2	172.33	100
6	Router	OT MLE	2	212.33	250
7	Router	OT MLE	3	105	50
8	Router	OT MLE	3	172.33	100
9	Router	OT MLE	3	211.66	150

3. Distance Wise Findings:

• There was a clear increase in RTT as the distance between nodes in the network increased. This is a fundamental characteristic of network communication, where longer distances require more time for data to travel.

• As the distance increased, messages were routed through more intermediate devices. Each additional device introduces a certain amount of delay, contributing to the overall increase in RTT. The results are shown in table 6.4.

Table 6.4: Distance Wise Findings

Diatance Wise						
SN	**Device Role**	**Ping Type**	**Ping Hop**	**RTT**	**Pay Load**	**Dist (ft)**
1	Router	OT MLE	1	67.333	100	∼10
2	Child	OT MLE	2	114	100	∼10
3	Router	OT MLE	3	135	100	∼50-100
4	Router	OT MLE	3	183	100	∼<100

Chapter 7

Conclusion

In conclusion, our large network testing setup using NXP's SoCs and chipsets has offered valuable insights into the scalability, performance, and reliability of Open Thread networks. By carefully planning and executing the setup, we were able to create a network of up to 150 devices distributed across separate locations in the office area.

Through comprehensive testing and monitoring, we evaluated the network's functionality and performance under various conditions. The data collected on throughput, latency, and packet loss has provided a detailed picture of the network's behaviour and capabilities.

Our findings show that the company's SoCs and chipsets are well-suited for large network deployments, proving robustness and stability. However, further optimization and fine-tuning may be needed to achieve the best performance in real-world scenarios.

Overall, this large network testing has been a valuable learning experience, highlighting the importance of meticulous planning, thorough testing, and continuous monitoring in ensuring the success of complex network deployments. Our documented method and findings will serve as a valuable resource for future network testing endeavours, providing a roadmap for achieving reliable and scalable network solutions using the company's technology.

References

[1] Moustafa M. Nasralla , Haleem Farman, Nikumani Choudhury, “Performance Evaluation of an IEEE 802.15.4-Based ThreadNetwork for Efficient Internet of Things Communications inSmart Cities”, Appl. Sci. 2023, 13, 7745. https://doi.org/10.3390/app13137745.

[2] Hyung-Sin Kim, Sam Kumar, and David E. Culler, “Thread/OpenThread: A Compromise in Low-Power Wireless Multihop Network Architecture for the Internet of Things”, IEEE Communications Magazine • July 2019 0163-6804/19/$25.00 © 2019 IEEE.

[3] Roberto Sandre, Systems Engineer, Texas Instruments, “Thread and Zigbee for home and building automation”, March 2018.

[4] Tarek Elarabi, Vishal Deep, Chashamdeep Kaur Rai, “Design and Simulation of State-of-Art ZigBee Transmitter for IoT Wireless Devices”, 2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT).

[5] Mahesh Pawaskar, Sonia Aneesh, Disha Sharma, Pooja Sawale, Rashmi Sharma, Ashish Sharma, ”IoT enabled Smart Dustbin using Zigbee Network”, 2021 International Conference on Advances in Computing, Communication, and Control (ICAC3), 978-1-6654-2634-3/21/$31.00 ©2021 IEEE — DOI: 10.1109/ICAC353642.2021.9697275

[6] Ashwini Shamsundar, ”Modeling and Performance Evaluation of the Thread Protocol”,Delft University of Technology,2017.

[7] Rakesh Das, Jitendranath Bera, ”ZigBee based Small-World Home Area Networking for Decentralized Monitoring and Control of Smart Appliances ”, 2021 5th International Conference on Smart Grid and Smart Cities (ICSGSC) — 978-1-6654-0134-0/21/$31.00 ©2021 IEEE — DOI: 10.1109/ICSGSC52434.2021.9490482.

[8] D. M. Han and J. H. Lim, ”Design and implementation of smart home energy management systems based on ZigBee”, IEEE Trans. Consum. Electron., 2010.

[9] https://www.threadgroup.org ZigBee Alliance, 2015, [online] Available: http://www.zigbee.org.

[10] ”IEEE 802.15.4–2003 Standard”, [online] Available: http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.

[11] https://openthread.io

[12] Thread Group, ”Thread 1.1.1 Specification”, Feb. 2017.

[13] Boca Raton, ZigBee Network Protocols and Applications FL CRC Press 2014.

[14] J. Li, X. Zhu, N. Tang and J. Sui, ”Study on zigbee network architectureand routing algorithm”, 2010 2nd International Conference on Signal Processing Systems, vol. 2, pp. V2-389, 2010.

[15] T. Winter et al., “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” IETF RFC 6550, Mar. 2012.

[16] S. Farahani, ”ZigBee wireless networks and transceivers”, newnes, 2011.