MASTER

A study on the impact of transmission power on the message delivery latency in large ZigBee networks

Bangalore Lakshmana, S.

Award date:
2015

Department of Mathematics and Computer Science
System Architecture and Networking Group

A study on the impact of transmission power on the message delivery latency in large ZigBee networks

Master Thesis

Shashidhar Bangalore Lakshmana

Examination Committee:
Dr.ir. Pieter Cuijpers
Dr. Aly Aamer Syed
Dr. Majid Nabi

Eindhoven, August 2015

Abstract

The evolution of technology in daily life aims to reduce manual intervention in controlling complex machines, this is achieved through specially designed intelligent framework called as the automation system. The advent of internet technology into these control systems has paved way to be able to control the complex automation systems over the internet, which is a part of a phenomenon called as the Internet of Things (IoT). The concept of IoT has provided a platform for implementing large number of innovative ideas such as home automation, building automation, health care monitoring, smart agriculture, smart energy management etc. The ZigBee open standard is one of the many standards which delivers products/services capable of adapting to IoT, ZigBee focuses on devices operating in Low-Rate Wireless Personal Area Network; devices communicating over low data rates in a network of communication devices. In a network of hundreds of ZigBee devices, the ability to predict the performance of the network plays a crucial role in the process of designing efficient and reliable products. Therefore, a platform which enables researchers to make the process of predicting the behavior of large ZigBee networks is a need of the hour. The ZigBee devices are generally constrained by factors such as energy consumption, wherein transmission power of the devices is a major contributor for the total energy consumption and performance of the network. The focus of the thesis is to create a platform to simulate the behavior of large ZigBee networks and to evaluate the dependency of message latency in the network on transmission power. The platform is created using the NS-3 simulator, where the network layer of ZigBee devices is simulated using the IPv6 based AODV routing protocol and an adaptation 6LowPAN layer interfacing the IPv6 and 802.15.4 MAC. A number of experiments is conducted in a fixed grid topology to observe the changes in latency in communication of the network when the transmission power of devices are varied over a range of values. It is observed that the stability of latency of the network decreases with increase in transmission power, because, with increase in transmission power, the number of nodes within a range of one-hop increases. Some of the devices in this one-hop neighborhood could be just within the range of communication, an indication of poor connectivity. The AODV routing protocol decides routes based on number of hops to destination and does not take into account the quality of links. Thereby, a choice of poor quality links, increases the latency of communication in the network due to increase in number of retransmissions at the MAC layer. Though the trend of decrease in latency with increase in transmission power is evident from the experiments, but there is a certain degree of unpredictability over small changes in transmission power. To improve the performance of the network, it is proposed that either the right transmission power is determined to establish reliable links in the network or the routing protocol takes into consideration the link quality before establishing routes across the networks. The outcome of this project shows that there is a large scope for research to understand behavior of large ZigBee networks under different application scenarios.

Preface

The thesis is submitted in a partial fulfillment of the requirements for a Master's Degree in Embedded Systems for the author. It contains work done between February 2nd 2015 and July 31st 2015. The supervisor from the Technological University of Eindhoven is Dr. Ir. Pieter Cuijpers and the supervisor from the NXP Semiconductors, Eindhoven is Dr. Aly Syed. The thesis has been written solely by me, most of the text, with valuable feedback from the supervisors and I have done my best to provide references to the sources of information.

On Thursday 13th of November 2014, Pieter Cuijpers, Aly Syed and I had a discussion about the advancements in the ZigBee communication networks and the related work undertaken at the NXP Semiconductors. I was intrigued by the technology under development and was motivated to contribute to the company's work and for the research community of the world in the field of ZigBee devices. Eventually in the discussion we came into a consensus about the goals of my research for the internship at NXP Semiconductors, Eindhoven.

Writing this thesis has been hard and the 6 months have been a continuous learning process, testing the limits of my abilities at every instance and I strongly believe that I have learnt concepts which have broadened the horizons of my knowledge. I have dealt every obstacle head on with confidence and was successfully able to achieve my targets. During the course of writing the thesis I have encountered distinct subjects, I have tried to provide a broad perspective and scope of this research by combining different aspects of the behavior of large ZigBee networks. I have also strived to ensure that my research so far, triggers curiosity of fellow researchers from around the world and draw their attention to my inferences.

The thesis is written as a final thesis for the Master's degree in Embedded Systems, the text is mainly aimed to provide insight about a section of behavior of large ZigBee networks, throwing light over the certain intricate aspects about the functioning of the network. It is hoped that the observations made will be of interest to a large section of research community.

Acknowledgments

I would like to thank my supervisors, Dr. Ir. Pieter Cuijpers and Dr. Aly Syed, from the bottom of my heart, for their constant support, ideas, comments and invaluable pieces of knowledge that they have shared with me. They have always motivated me and cheered me up when everything almost seemed fruitless. It is their experience, knowledge and patience that was able to bring the best out of me and inspire me to complete the thesis successfully. I would like to convey my sincere thanks to my colleagues at NXP Semiconductors Eindhoven and the System Architecture and Networking group of the Technological University of Eindhoven for their indispensable support to help me in achieving the research goals. I would like to thank my parents B.S Lakshmana and Geetha, my brother Bhaskar and my sister-in-law Annapurna, for their constant moral support in completing my thesis.

Shashidhar Bangalore Lakshmana

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The world of technology, by designing innovative products helps in simplifying everyday life. The industries associated with these creations cannot work by themselves and depend on distinct organizations for assimilating the contributions from different services (can be a resource or a product) providers. In order to simplify the integration process, the technological companies, design standards based on a consensus. These standards can be a set of rules and regulations or guidelines for companies working towards a common goal. The Internet of Things [52], a phenomenon of bringing the world closer and connected through internet is one such common goal, many companies focus on creating application profiles such as the home automation system, health care, industrial automation, smart cities, smart lighting and many more. Every application profile has a consortium where the industries define the standards for their products, which shall be adhered by the service providers. In the aspect of Internet of Things, the ZigBee Alliance is a consortium of companies which define an open standard called as the ZigBee standard, where an open standard is a set of rules and regulations which are publicly available and can be used by any company with a little or no restrictions. The ZigBee alliance has drafted a large number of application profiles for the ZigBee devices, such as home automation, building automation, health care, smart energy, telecommunication systems and many more. The ZigBee devices are created specifically for low power, low data rate wireless communication networks, especially for the IoT based applications.

The current internet protocol, which is reaching maximum utilization, is the IPv4. The IoT is finding such widespread applications in the world, that the number of devices which shall be connected to the internet is expected to rise drastically in the near future. Therefore, the IPv4 version cannot support this enormously growing need for unique internet addresses. The newer internet version, the IPv6 is designed to be more robust, flexible, efficient and reliable form of communication over the internet. Therefore all the devices which are expected to be connected to the internet must be able to adapt and use the IPv6 version of the internet.

In a scenario where the internet version to be adapted is fairly new and the applications are wide spread, it is essential that the behavior of these devices be carefully observed and analyzed before adapting them into applications. With ZigBee playing an active role in the IoT applications, it is essential to understand behavior of ZigBee devices in a large networks under different circumstances of the desired applications, such as being able to predict the behavior in different environmental conditions of ZigBee networks in a building automation system. In order to be able to observe and analyze the framework of an application it is essential to setup the network with real nodes to judge the feasibility of application, because a network of real nodes provide reliable data about the application scenarios. This is advisable for a network of small number of nodes as it is economical to setup smaller networks of application. If the network consists of hundreds

of nodes, then it proves to be expensive to setup a physical network even before predicting the behavior. The network simulators can be used to understand the behavior of the communication networks by using mathematical models to reproduce different environmental conditions and run experimental simulations of various device frameworks. In a similar fashion, the network simulators can be used to replicate the ZigBee devices and large network of hundreds of nodes in different topology can be created to understand the behavior of these devices. The choice of network simulator to achieve the goals plays a crucial role.

Currently, there are large number of reliable network simulators [40] [30], for commercial, academic and research purpose, such as OMNET++, NetSim, NS-3 etc. Each of these simulators focus on different aspects of computer network simulations. The NS-3 network simulator is a complex, yet flexible, robust, reliable and efficient simulator. It was specifically designed for research and academic purposes. Based on certain comparisons, analysis and inferences, the NS-3 simulator is found to be suitable for network simulations related to large ZigBee networks. The network behavior can be analyzed in different perspectives such as performance, flexibility, robustness, customization etc. The performance of a network is basic and crucial aspect of a network. Therefore analyzing a network in terms of performance can be considered as the first step towards complete understanding of network.

The performance of a communication network can be measured using various performance metrics [17], such as latency, packet reception ratio, packet error rate, throughput, packet delivery ratio etc.The initial step should be to understand behavior of a large ZigBee network by focusing on a specific performance metric. Research has been done on ZigBee devices [27] [38] [19], but are minimum with respect to large ZigBee networks associated with IoT. The ZigBee devices are low power devices, generally battery operated and constrained by resources such as energy consumption, memory, computation speed etc. The communication range of a device is largely dependent on its transmission power and the transmission power is restricted by the energy available for the device through its source of power. Therefore, transmission power plays a crucial role in establishing and maintaining the network. It also has a direct impact on the performance of a network, based on the chosen metric to evaluate the performance. Thus, it can be inferred that transmission power, size of network and performance of network are largely interdependent and it is of high importance to understand the extent of this interdependency. Thus, this forms a crucial aspect for understanding the behavior of large ZigBee networks. The literature survey on the impact of transmission power control [26] [47] [48] [33] and link quality estimators [17], indicates that there are a large number of link quality estimators at our disposal and based on the user requirements and the application. The transmission power of a device also has a significant effect on the performance of a communication network and choosing the right transmission power for communication has direct impact on the performance of the network. Considering all the information it is essential to establish certain focused research goals for the master thesis.

1.2 Research goals

The Internet of Things and the association of ZigBee devices are fairly new and the applications are under constant evolution. In this process of evolution, the academic and industrial research must run coherently to create valuable products to the end users. The contribution of researchers from the academics provides new perspectives for the industries when manufacturing the products for the end user. In the case of ZigBee devices and its networks, the applications sought by the industries are widespread and require extensive research and in-depth understanding in order to innovate products for catering to the needs of consumers. The applications of ZigBee networks operate in different environmental conditions. Thereby it is required that the behavior of the devices can be predicted to fairly reliable extent under dynamic conditions (within and outside the network) and the device be able to adapt to such conditions. To understand the behavior, one must be able to recreate scenarios of application either by using the real devices or running

network simulations. The former method proves to be expensive, and the latter is feasible in all aspects from an academic perspective.

The performance of a ZigBee network being an essential evaluation criteria, can be established as the domain of research in this master thesis. As previously stated the transmission power of a device can have considerable impact on the performance of the network. Based on the extensive literature survey done on the impact of transmission power [47] [48] [33], the need for controlling transmission power and the use of different transmission power control algorithms [26], the results of the experiments conducted in the references prove that a transmission power control algorithm helps in obtaining better results in comparison to not using the algorithms. Thus, it can be inferred that it is essential to analyze the impact of the transmission power in the performance of ZigBee networks. Taking into consideration these aspects which require attention, the focus of this thesis can be stated as:

- To provide a platform to simulate and analyze the behavior of a large ZigBee network.
- Use the platform to understand the impact of transmission power on a performance metric; latency of the network.

The research focuses on setting up a platform using which an entire network of ZigBee devices can be simulated in a reliable simulation environment to obtain accurate information about the behavior of the network when subjected to changes in parameters; of the device itself and external to the device (environment of the network). This platform opens up paths to a large variety of domains of research of ZigBee networks. Many aspects of a communication network can be understood using this platform, such as impact of transmission power of devices, density of network, mobility in the network, different environmental conditions with large number of sources of interference etc. Using this platform, the thesis focuses on analyzing one of such aspects of performance in terms of latency of the network when subjected to changes in transmission power of the devices. To create the platform for the research and to achieve the set goals in a stipulated duration of time, requires thorough understanding of the available options, calculated planning and smart engineering approach.

1.3 The approach

The research goal is to create a platform to simulate ZigBee networks. In order to replicate ZigBee devices in a simulation environment, it is necessary to gain an overview of the ZigBee device architecture, following which a simulation platform can be established. After a brief understanding of the ZigBee architecture, it was evident that to create a simulation framework, recreating the ZigBee network layer is an important step. It is followed by the usage of 802.15.4 standard based MAC and PHY layers. On completing these two tasks, an environment to understand behavior of large ZigBee networks would be available. The first step, recreating ZigBee network layer requires use of an IPv6 based routing protocol, so that the devices in a ZigBee network be able to route messages within the network using IPv6 addresses. The IPv6 and 802.15.4 MAC layers cannot be used directly to run in harmony, due to a basic difference in frame size i.e the 802.15.4 MAC frame size is 127-bytes with the payload size as low as 72-bytes whereas the minimum frame size for standard IPv6 is 1280-bytes. This mismatch calls out loud for fragmentation of IPv6 packets before they can be compatible with 802.15.4 MAC layer, which is explained in detail in the subsequent chapter of 802.15.4 layer. The IETF 6LowPAN group solved this problem by creating an adaptation layer of 6LowPAN, which achieves compatibility between IPv6 and 802.15.4 MAC layers. Thus, to replicate ZigBee network layer, a 6LowPAN adaptation layer, in combination with IPv6 based routing protocol is necessary and the subsequent step is to use the 802.15.4 MAC and PHY layers. Therefore a network simulator must be chosen which can satisfy this requirement or atleast support implementation of the requirements.

The simulators available to be used are plenty [30] [40], NS-3 simulator is one such designed specifically for communication networks and has plenty of support to be used for simulating Wireless Sensor Network. The NS-3 simulator is an open source software, with an active support forum and largely used for academic and research purposes which makes it an eligible candidate for the purpose of this project. The NS-3 also satisfies the requirements that have been laid out for the project except for an IPv6 based routing protocol. Therefore, the first and foremost step in creating the platform to simulate large ZigBee networks, would be to implement this IPv6 based routing protocol in the chosen simulator NS-3. The ZigBee standard defines the use of AODV routing protocol in its mesh networks, and the NS-3 provides the AODV routing protocol which uses IPv4 addressing. Therefore, by implementing the AODV routing protocol which uses IPv6 addressing, all the requirements for the platform will be satisfied, considering the fact that NS-3 has implementations of 802.15.4 MAC and PHY layers.

The implementation of the routing protocol requires careful planning to ensure the tasks are completed successfully within the available time and have sufficient time to analyze the impact of transmission power on the latency of a large ZigBee network. The approach can be briefly explained with the following steps:

- Understanding the architecture of NS-3
- Understanding the IPv6 protocol
- Understanding the AODV routing protocol
- Implement AODV routing protocol to use IPv6 in NS-3
- Rigorous testing of the implemented routing protocol to ascertain functionality
- Combine 6LowPAN AODV and IPv6 to simulate ZigBee network layer
- Design basic to complex applications to understand the functioning of the implementation
- Analyze different parameters (network parameters and application parameters) associated in creating an application scenario and their impact on network behavior

All these steps shall be aimed towards achieving the research goal and to arouse inquisitiveness and discussion in the research community towards the behavior of large ZigBee networks.

1.4 Structure of Thesis

The following section describes the structure of the thesis report and provides an overview of the approach towards research goals. The Chapter 2 provides an overview of the ZigBee architecture and the protocol itself. This helps in understanding the domain of research which is required to know the bigger picture of the project. In Chapter 3 the IPv6 protocol is explained in detail, describing the need for IPv6, advantages over IPv4, features of IPv6; the robustness, reliability, efficiency and flexibility of the protocol. It also describes the Neighbor Discovery Protocol which is an important aspect to be understood when designing routing protocols for IPv6 as both share the common approach for neighbor discovery. The chapter also explains in detail the IPv6 addressing mechanism and how it differs from IPv4 which is very essential to design the required AODV routing protocol. In chapter 4, the Ad-hoc On demand Distance Vector routing protocol is described in detail, with proper reasoning for the choice of routing protocol made and its association with the ZigBee protocol. It also describes the implementation of AODV using IPv6 address in detail. The Appendix A provides information about the 6LowPAN in order to understand its role in the simulation of a ZigBee network and the process of header compression to bring about compatibility between IPv6 and 802.15.4 MAC. Appendix B helps in understanding the 802.15.4 MAC and PHY layers in brief. The 6LowPAN and 802.15.4 are not the focus of thesis, these are information

required to understand the overall structure of the protocol stack. In Chapter 5 background is laid to understand the simulation environment; NS-3 simulator. It describes in detail the architecture of NS-3 and the ZigBee network layer simulation framework and different mathematical models used to obtain reliable data out of experiments to be conducted. Information from these chapters establishes a strong base to understand the experiments conducted to achieve one of the research goals; to analyze the impact of transmission power devices on the performance of large ZigBee network in terms of latency. Chapter 6 provides details about the experiments conducted in the research, starting by stating a hypothesis followed by evaluation of the hypothesis through various experiments. The results are evaluated and set aside to draw conclusions on the observations. Chapter 7 explains in detail the conclusions drawn based on the observations and experimental evaluations. It also describes the challenges faced in the research and provides a detailed personal opinion about the scope of research. The possible future scope of the current research, the importance and contribution to the research community is explained in Chapter 8.

Chapter 2

ZigBee Standard

2.1 Introduction

The automation systems, operating on a wireless network, are driving the need for different data rates for communication. The network consists of a large number of distinct devices such as personal computers, mobile phones, tablets, sensor devices and many more, in which the parameters like energy conservation, security, interference, connectivity etc play an important role. Some applications demand low rate and low power consumption, whereas the others have devices externally powered thus energy consumption may not be hard constraint. In the year of 2000, IEEE New Standards Committee (NesCom) designed a new communication standard for the devices which would operate on low data rates, Low-Rate Wireless Personal Area Network (Lr-WPAN), called as 802.15.4 standards. In the year 2003, ZigBee Alliance introduced the ZigBee standard protocol. The ZigBee protocol is one of the major contributors towards IoT based applications in collaboration with Wireless Sensor Network (WSN) devices, which forms the basis of this master thesis.

The ZigBee Alliance consists of a group of companies working towards the development of a technical standard trademarked by the name ZigBee. The alliance publishes and maintains the ZigBee standard which provides application profiles to large number of OEMs vendors allowing them to manufacture inter-operable products to their customers. The alliance aims to establishing the ZigBee as a standard for low power wireless networks for sensing and controlling in the fields of consumer, industrial and commercial products. The ZigBee is a very low cost, very low power consumption, two way wireless communication standard. The list of application profiles included by the ZigBee standards includes some of the major domains such as Home Automation, Smart Energy, Telecommunication, Health Care, Building Automation and many more as shown in the figure 2.1, the image is taken from[10] .

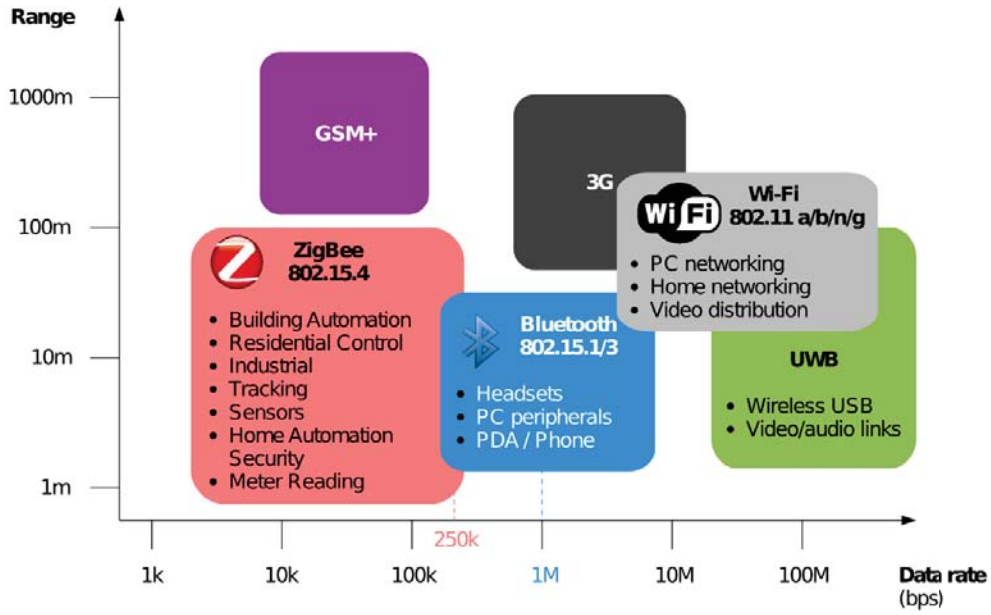

Figure 2.1: Wireless Standard Operating in the ISM Band

2.2 ZigBee Application Layer

The figure 2.2, figure is taken from [12], shows the ZigBee architecture describing every layer and sub-layer with its functionality and also the interface to the other adjoining layers.

* **Application Support Sub-layer (APS)** : The Application Support Sub-layer provides the necessary services for the application objects and the ZigBee Device Object to interact with the network layer for corresponding data and management services. A few of the services provided by the Application Support Sub-layer (APS) for data communication are request, confirm and response. The ZigBee APS also provides enhanced communication structures such as clusters, profiles or an endpoint that are software abstractions which help in distinctly identifying every application object.

  - Application object (endpoint) : The endpoint defines the possible input and output to the APS. Each device can have 240 objects. For example, a lighting application profile on a device will consist of number of switches to control the color of lighting. The input is the switch by itself which decides the color of the output light and the output will be the light bulb color status. The APS is also responsible for binding different tables, forwarding messages between these bound devices, defining and managing various group addresses, fragmentation and reassembly of the data packets. The binding tables are key to data communication over the network and these are stored in the coordinator and all the routers of the network.
  - Application Framework : The application framework is defined by the manufacturer based on the application objects. The framework creates an environment for data transfer by different application objects where each application uses its corresponding endpoint as an interface.
  - ZigBee Device Object (ZDO) : The ZigBee Device Object is responsible for the device management, consisting of functions such as:

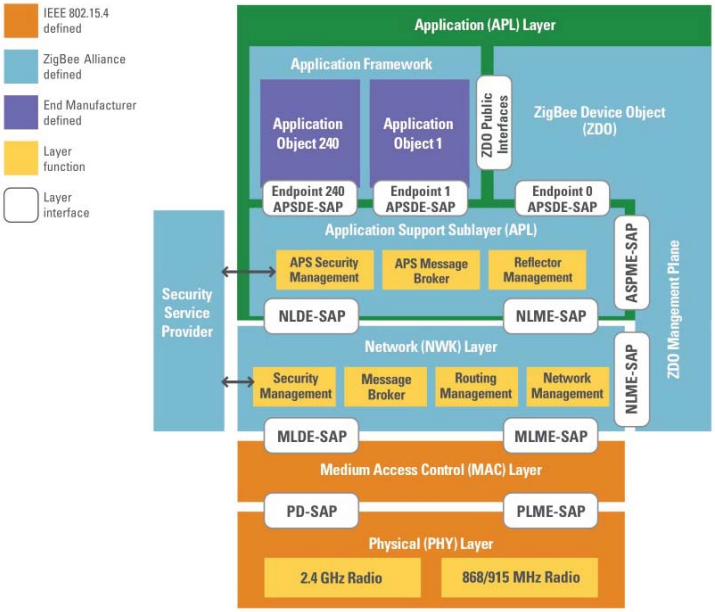

Figure 2.2: ZigBee Architecture

· initializing the APS and network layers
· defining the type of device and its corresponding operation
· security management
· binding device process management

- End node : Nodes are end devices as described in section 2.4, each end device can have multiple number of end points. Every end point can be associated with distinct application profile which can also be used to control many or a single device. Each device has a predefined communication profile which is in correspondence with application profile. For example, a simple remote control which can access many light switches in a house. The remote control is the end device, and three light switches are analogous to the end points.

2.3 ZigBee network layer

The ZigBee standard is associated with high level communication protocols which are used to create personal area networks. The ZigBee standard is in compliance with the 802.15.4 standards which define the Media Access Control (MAC) and Physical (PHY) layers. Furthermore, ZigBee builds upon the 802.15.4 standards defining the network layer specifications and provides a framework for application programming. The architecture is as shown in the figure 2.3 taken from [6].

- The ZigBee network layer provides services using two Service Access Point (SAP): The network data service, termed as Network Layer Data Entity (NLDE) SAP and the network management service, termed as Network Layer Management Entity (NLME) SAP. These services, NLDE and NLME, act as interface between the application and the MAC sub-layer through the MAC Common Part Sub-layer (MCPS)-SAP and MAC sub-Layer Management Entity (MLME)-SAP as shown in the figure 2.4, image taken from [16]. An implicit internal interface is available between the NLME and the NLDE which enables the NLME to use the network data services.

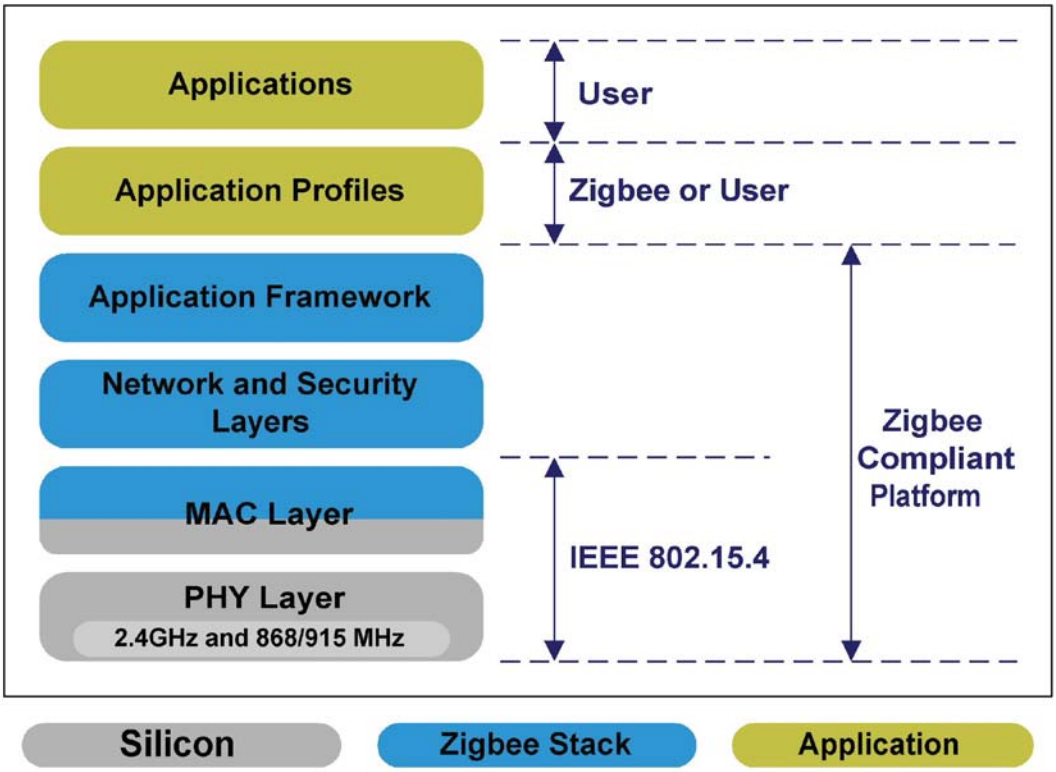

Figure 2.3: IEEE 802.15.4 and ZigBee working model

- The responsibilities of the ZigBee network layer via the the two SAPs: Network Layer Management Entity and the Network Layer Data Entity include the following:

* **Network Layer Management Entity (NLME)** : The NLME defines the process of successfully establishing a network. The NLME handles the requests and confirmation messages in the process of network discovery, network formation, device joining/leaving, router start, energy detection scan, network synchronization and route discovery. It takes care of the configuration of the stack, based on the required operation by the application. The NLME also handles the address assignment to the new devices which join the network.

* **Network Layer Data Entity (NLDE)** : The NLDE is responsible for the topology specific routing mechanisms. The transport of Application Protocol Data Unit (APDU) among the peer application entities is handled by the NLDE-SAP. It mainly consists of the data request, confirm and indication messages.

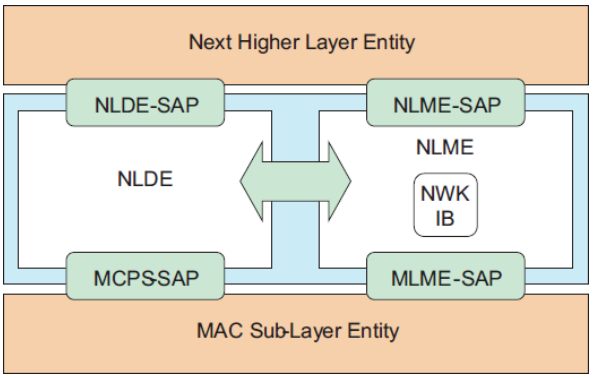

Figure 2.4: Network layer reference model

2.4 ZigBee devices

The ZigBee network layer defines three types of devices:

* **ZigBee coordinator** :The ZigBee coordinator is an Full Function Device (FFD). A coordinator is the one and only device whose presence is a basic requirement to establish a ZigBee network. The ZigBee networks are permitted to have one and only one coordinator for the whole network irrespective of the topology. In a star topology, the coordinator takes the position in the center, on the other hand, in tree and mesh topologies, it is situated at the root of the network like in tree or at random position as in mesh topology. The coordinator plays a vital role in the network establishment and system initialization. The zigbee coordinator detects the channel energy and selects an appropriate channel, the one on which least energy was detected, for the rest of the network. The coordinator is also responsible for choosing the devices that can join the network and assist in the process of network establishment. The coordinator can also function as a regular device and perform message routing, like in the star topology. In certain scenarios network can function even when the coordinator fails or switches off, but this is not possible if the coordinator was also part of the routing process, for example in the start topology. The coordinator also provides large number of services at the application layer, if these services are being used by the network, then it is essential that the coordinator is functional at all times. The ZigBee coordinator is also is the designated Trust Center, which is a repository for all the security keys.

* **ZigBee router** : A ZigBee router is an Full Function Device (FFD). An FFD has the ability to function like other regular end-devices and also possesses the ability to relay messages by allowing it to communicate with any other device within the same network or another network. The ZigBee routers are optional devices of a network which discover and associate themselves with other devices of the network i.e. either other ZigBee routers or a ZigBee coordinator. The ZigBee router is responsible for the local address allocation and de-allocation of the end-devices associated with itself. The address of the router serves as a reference for all the associated end-devices. The ZigBee router also participates in the multi-hop communication and mesh routing of messages. The ZigBee router is responsible for transmitting broadcast,multicast and unicast messages to the ZigBee end-devices. The ZigBee router also maintains a neighbor table containing a list of immediate neighbors of the router. The router has a specified routing protocol available, using which it makes the decision of choosing best possible route to a destination node at a particular instant of time, based on certain conditions that are routing protocol specific. The ZigBee router is used in tree and mesh topology to expand the network coverage. A router performs all functions of a coordinator, except establishing the network. In a star topology, these functions are

handled by a coordinator, thus router is not a mandatory device in this topology. In tree and mesh topology, routers can be placed in any extreme ends of the network as required by the application. The routers are usually not allowed to sleep and are generally externally powered devices.

* **ZigBee end-device** : The ZigBee end-device corresponds to a Reduced Function Device (RFD) of the IEEE 802.15.4. These are optional components of a network and are very simple devices which posses minimum required resources for communication. The ZigBee end-devices can communicate only with the other Full Function Device (FFD) and can never act as router/coordinator i.e it cannot allow other nodes to connect to a network through them. These end-devices discover and associate themselves with the ZigBee coordinators and/or ZigBee routers in the network. The ZigBee end-devices can be optimized for minimum power consumption. The end-devices operate on a low duty cycle, the power consumption is only during the transmission of the information and the parent device decides the sleep period of the end-device. Therefore, ZigBee architecture is designed to optimize the transmission time of an end-device to a low value and the power consumed during this transmission is low in comparison with other wireless devices. In a star topology, the end-devices are perimeter nodes whereas in tree or mesh topology they are the leaf nodes.

2.5 ZigBee network topologies

The ZigBee standard is compliant with the 802.15.4 standards in terms of the MAC and PHY layers. The 802.15.4 standards support start, tree, cluster tree and mesh topology whereas the ZigBee standard supports only the star, tree and mesh topology. The figure 2.5, image taken from

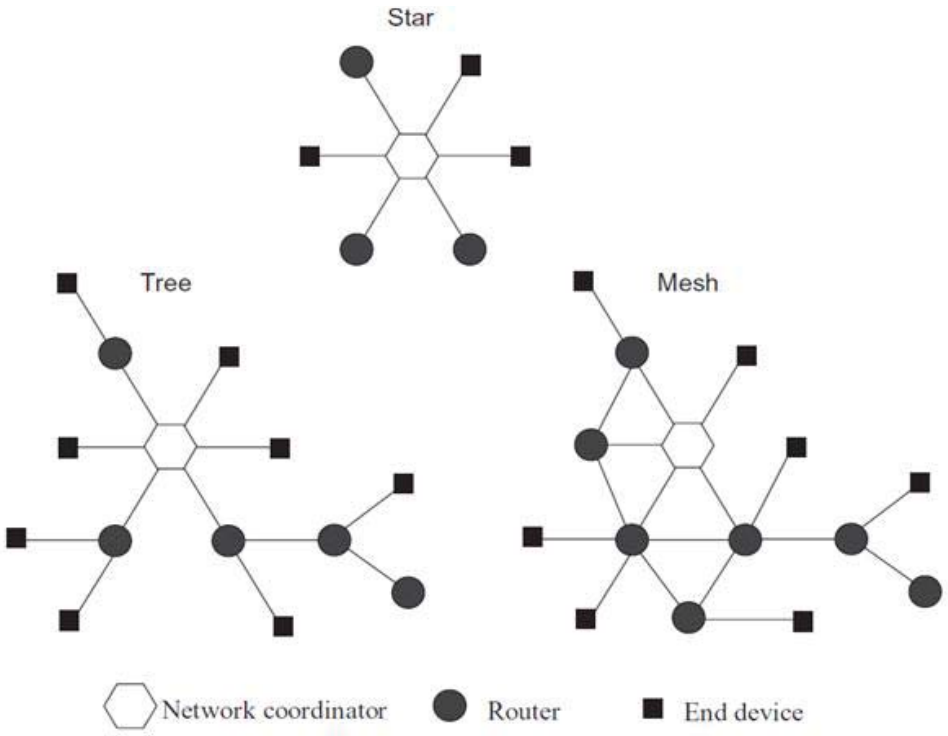

Figure 2.5: ZigBee network topologies.

[13], shows the three topology models supported by the ZigBee standards.

* **ZigBee star topology** : The ZigBee star topology consists of a number of end devices connected to a single coordinator as indicated in the figure 2.5. In this topology, the end devices communicate only with the coordinator i.e. any message addressed to other end devices must be sent to the coordinator, which determines the destination and forwards the packet.

  The major advantage of the start topology is that the end devices can send the packet to other end devices in just 2 hops through the coordinator. The topology is easy to implement due to the simplicity of its operation. It must also be noted that the messages are not boradcasted or multicasted, therefore the nodes not associated with the communication, do not receive any redundant packets.A new node has to only contact the coordinator directly, to join the network. Also, failure of one of the nodes in the network does not damage the links to other nodes, making it easy to isolate a faulty node and replace the node without disturbing the rest of the network.

  On the other hand, the coordinator acts as the single point of failure. Also, even if a destination end device is in the communication range of the source device, the source end device cannot communicate directly, the messages have to go through the coordinator, therefore increasing latency of overall communication. The performance of the network is dependent on the ability of the coordinator node as it is solely responsible for handling the traffic.

* **ZigBee tree topology** : The tree topology consists of a central coordinator and a large number of routers and end devices as shown in the figure 2.5. The function of the routers is to extend the network coverage by allowing more number of end devices to connect to the coordinator through them and thus join the network. The routers and coordinators are the only permitted devices to have children devices, the end devices just connect to their parent router or the coordinator.

  The key advantage with the tree topology is that the messages need not be flooded in the network. Every end devices is associated with a parent device and this parent child relationship is vital for communication in the network. The network is quite scalable depending on the capacity of the routers and coordinators.

  On the contrary, the drawbacks include the fact that, the tree topology is reliant on the dependability of the routers in the network, failure of which can disable communication with all the end device associated with the corresponding router. The possibility of accumulation of large number of devices with a single router can lead to performance degradation of the network.

* **ZigBee mesh topology** : The mesh topology is also referred to as the peer-to-peer network which consists of a single coordinator and a large number of routers and end devices as shown in the figure 2.5. The mesh topology forms a multi-hop network, in which the messages go through one or more nodes in the network to reach their destination node.

  The path to reach the destination is determined by the routing protocol installed on the nodes. If a path breaks due to any reason, then the multi hop network finds a new path to reach the destination. It is for the same reason that the mesh network is termed as a self healing network which is one of the major advantages of the mesh topology thus eliminating the dead zones. The range of the network can be increased just by adding new devices to the network, thus giving the flexibility to scale the network. Also, addition and deletion of a node from the network is quite simple and the nodes which have a path via the deleted node shall be informed about the removal of node or these nodes would eventually find a new path. The key advantage of the mesh topology lies in the face that, the nodes in the network can communicate with any other node in the same network through multi-hop paths.

  In comparison to other types of topology, mesh topology is much more complex due to

the additional overhead of a much complex routing algorithm. Since every node can connect to every other node in its communication range, thus there could be lot of redundant links stored in the routing table. Also, the network establishment and maintenance costs are higher than the other types of topology.

2.6 Summary

This chapter has provided a basic overview of the ZigBee architecture (section 2.2) and information about the ZigBee network layer (section 2.3 which is required to be able to create a simulation model of the ZigBee network layer in a network simulator. The chapter also provides details about the different types of ZigBee devices based on their role in a ZigBee network (section 2.4). These devices; Coordinator, Router and End device, play a crucial role in setting up and maintenance of the network. The allowed ZigBee topology styles are described in section 2.5, of which the mesh topology shall be used in the experimental section of the master thesis. A basic understanding of the ZigBee is sufficient to be able to evaluate the results obtained in the master thesis.

Chapter 3

Internet Protocol

3.1 Introduction

The internet was started as a means to exchange information among a small group of computers. This innovative idea became a widespread need with the growth of computer industry such that by the year 2020 it is expected to connect 4 billion people, over 25 billion embedded devices and intelligent systems generating over 4 trillion dollars of revenue with over 50 trillion giga bytes of data available to be analyzed and creating an opportunity for exceedingly 25 million internet applications[4]. This magnanimous growth of internet industry establishes a need for a revolution the operation of internet. The devices which use the internet require unique addresses in order to be accessible by rest of the devices without any problems of establishing wrong links of communication. The original version of the internet, the Internet Protocol version 4 (IPv4) uses 32-bit addressing which creates a pool of 4.3 billion devices which is not sufficient to meet the growing needs. The replacement internet protocol, the Internet Protocol version 6 (IPv6) uses 128-bit addresses, therefore, mathematically, creates 340 undecillion unique addresses. Thus allowing more number of devices to be connected to the internet using uniquely identified addresses, for many years to come.

3.2 Internet of Things (IoT)

The Internet of Things (IoT) is a term used to describe the scenario of connecting object, animal or people to the internet by providing unique identifiers to the devices attached on them and transfer specific information without any human-computer or human-human interaction. The application of IoT is widespread and has an impact on every day functionality of the modern world. To state, some of the large scale applications include: pet monitoring and controlling, embedded mobile applications, energy management, wireless networks, security, health care, building automation, smart homes/cities and many more. All these applications currently use the IPv4 but slowly drifting towards a much effective version of the internet, the IPv6.

The semi conductor industry has performed significant research to manufacture devices catering the various needs of the Internet of Things. The applications of IoT largely determine the design of specific devices. For instance, WirelessHart, DigiMesh, ISA100, WiMax, ZigBee and many more standards design devices for specific application profiles. The ZigBee has a large number of application profiles within itself, to state a few: home automation, building automation, telecommunication, health care, energy industry etc. All these application profiles have a significant scope to merge with the Internet of Things and the ZigBee alliance has been creating devices for the IoT for the past 12 years. Over the period of time technology companies are designing software solutions from the internet perspective, one of the most significant ones is the ZigBee Internet Protocol Specification, which was released by the ZigBee alliance in March 2013. ZigBee

Ip is the first open standard for an IPv6 based wireless mesh networking using the low power, low data rate and low cost devices. These specifications were designed with the sole purpose of adapting to the migration of internet technology using IPv6 from IPv4. The reasons for the shift from IPv4 to IPv6 are numerous, one of the main reason is the depletion of available IPv4 addresses due to which the needs of Internet of Things cannot be catered.

3.3 Migration of internet protocol version

IPv4 currently, is one of the most widely used internet versions to allow devices connect to the internet. The IPv4 uses 32-bit addresses which leaves out just over 4 billion unique addresses for the devices. Though these addresses are large in number, but is not sufficient to last forever. In the early 1990s a newer version called Ipv5 was developed, but a transition was not simple due to the widespread usage of the internet. Considering the shortage of addresses as the main reason to make a transition, the Internet Engineering Task Force formed a large number of groups to design a better version of internet protocol. In the year 1996 a series of standards were released by the IETF defining the Internet Protocol version 6 [25]. The IPv6 is not just an extension of IPv4, the process of communication is entirely different and is much more complex, stable and robust in nature [37] [46] [39].

* Higher routing efficiency : The fragmentation of the IPv6 packets is no longer mandatory, i.e. if large data packets have to transmitted, then in IPv4 these packets have to be fragmented due to its small sized length, but owing to large size of IPv6 packets which required fragmentation in IPv4 are no longer required to be fragmented. The fragmentation by itself was an intensive overhead process, thereby in comparison to IPv4 the network speed in IPv6 increases substantially. Adding to the routing efficiency is the flexibility to allocate address prefixes to the network, thereby allowing directed data flow in the IPv6.

* Quality of Service (QoS) : The IPv4 does not have the capability to differentiate between the delay sensitive data packets from a large scale data transfer, thereby requiring workarounds in order to implement the functionality. On the brighter side, IPv6 stores the information about the requirements of all data packets based on different applications that are delay sensitive, for instance, the video processing, Voice over Internet Protocol (VoIP), audio transmission etc. The structure of IPv6 is described in the section 3.4.3.

* Increased address space : The IPv4 uses NAT to extend the address space due to its limited address availability. On the contrary the IPv6 has extensively large address space thereby eliminating a complex functionality of NAT.

* Security : Security was always a concern in the IPv4, with enhanced security features forming an integral part of IPv6, it will be no more such a big concern.

* Stateless Address Auto Configuration (SLAAC) : Assigning IPv4 addresses and managing the same was a complex procedure, this has been overcome by the Stateless Address Auto Configuration in which the devices use Neighbor Discovery Protocol (NDP) via the ICMPv6 to assign and confirm unique addresses to themselves.

* Improved headers : The IPv4 header had many optional fields adding to the redundancy, this has been improved in the IPv6 headers which is much more robust as it handles these optional fields in a different manner described in the section 3.4. This simplification allows router to make routing decisions more efficiently and quickly.

* No broadcast : The IPv4 facilitates broadcast addresses, which is replaced by multicast group addresses in IPv6. This makes addressing more easier, as every user can focus on sending data to specific set of devices rather than broadcasting it over the internet. This reduces traffic, makes communication more directed and efficient. The IPv6 also supports addressing

called as Anycast address in which routers can send the data to the nearest device of the group, this is also a provision to improve efficiency of communication.

* Mobility : The IPv6 was designed keeping in mind the mobility of devices, using the IPv6 addressing, the devices can move around the globe and continue to use the same address which is taken into consideration by the auto IP configuration and extension headers.

* Extensibility : The flexibility of IPv6 is a commendable feature which allows the user to add more information to optional section, which is limited to 40 Bytes in IPv4 whereas in IPv6 it can be as large as the size of the packet itself.

3.4 Internet Protocol version 6 (IPv6)

3.4.1 Addressing format and types

* **Addressing format** : The IPv6 addresses [51] makes use of the hexadecimal number system. Hexadecimal number system uses radix (base) of 16 for defining the numbers. The system uses symbols 0-9 to represent numbers from zero to nine correspondingly and uses alphabet A-F to represent numbers from ten to fifteen correspondingly. To summarize, every digit in hexadecimal can represent a value between 0 and 15.

  • Addressing structure: An IPv6 address is 128-bits in length and is divided into eight 16-bit blocks where each block is represent by a 4-digit hexadecimal number separated by colon symbols, each hexadecimal digit representing a value between 0 and 15. For example: the following shows the binary format of the IPv6 address.

  0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

  Each block is converted into hexadecimal representation:

  2001:0000:3238:DFE1:0063:0000:0000:FEFB

  The IPv6 address is long even after conversion to hexadecimal representation. The standards set up by the IETF define the following rules to further shorten the IPv6 address representation if need be:

  Rule 1: Discard leading Zero(es): In block 5 of the above representation (0063), leading zeroes can be omitted. Therefore representation now looks like:

  2001:0000:3238:DFE1:63:0000:0000:FEFB

  Rule 2: If more than one consecutive blocks have only zeroes, omit them and replace it by double colon symbol (::). In our example, block 6 and 7 can be omitted and replaced with double colon as shown below.

  2001:0000:3238:DFE1:63::FEFB

  Consecutive blocks of zeroes can only be once replaced by ::, so if there are still other zeroes in the address, they can be shrunk to a single zero as shown below.

  2001:0:3238:DFE1:63::FEFB

• Interface identifier: The last 64-bits of the address is classified as a unique identifier for every device and this is termed as the interface identifier. Every device in the world is assigned a unique 48-bit MAC address. The interface identifier is generated by the EUI-64 format. In the EUI format the 48-bit MAC address is divided into two 24-bit halves and a hexadecimal value FFFE is squeezed in-between these halves. For instance, the figure 3.1 shows the process of EUI-64 format interface identifier generation. To convert the EUI-64 format into IPv6 interface identifier, the 7th most significant bit is complimented as shown in the figure 3.1, image taken from [5], where the modified EUI-64 represents the IPv6 interface identifier.

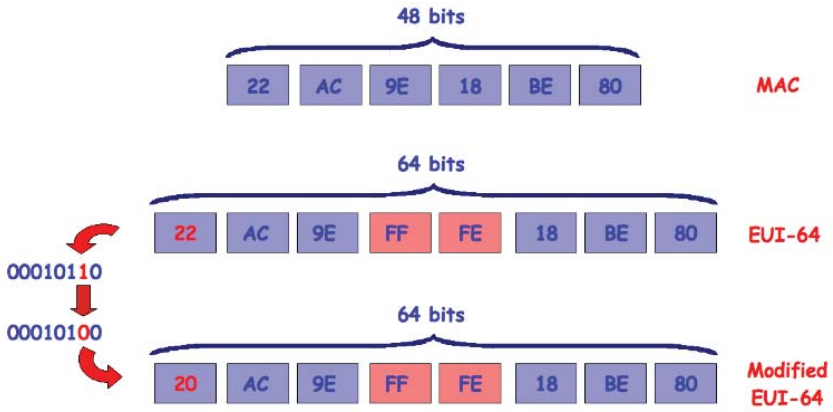

Figure 3.1: Generating EUI-64 format Interface Identifier

∗ **Address scope** : The figure 3.2, image taken from [9], shows the scope of IPv6 addresses assigned to a single device. All devices can have more than one interface and each interface will be defined by one or more of the scopes of addresses.

• **Global Address**: The global address is an unique identifier for the device at a global scope. Any device around the world can communicate with another device by addressing the packets to the global address of the intended recipient. This address is equivalent to the public address in the IPv4. The figure 3.3, image taken from [7], shows representation of global address.

Global Routing Prefix : The most significant 48-bits are termed as global routing prefix, where the three most significant bits are always 001. This global routing prefix is chosen by the service provider based on their norms and conditions.

• **Link Local Address**: The IPv6 auto configured address is the link local address, generated based on the MAC address of the device. In the link local address of a device, the first 10-bits are always assigned as 1111 1110 10 (FE80) and the next 54-bits are assigned with zeroes as shown in the figure 3.4, image taken from [7]. The link local address is used only by the devices on the same link. The link local address has a limited scope to just the particular link, therefore the routers do not forward messages to other networks which are addressed by the link local address. Thus two or more nodes on different networks can have the same link local address. The link local address is required for the IPv6 sublayer operations such as the NDP and some IPv6 protocols like the DHCPv6.

• **Unique Local Address**: The unique local address should be globally unique, but must be used only for local communication. The first 64-bits of a unique local address is subdivided into a prefix, local bit, global id and a subnet id. The 7-bit prefix is always set to 1111110 and the local bit is set to 1 indicating that the value was generated locally. The value 0 for the local bit has no functionality and is not defined, therefore the local bit is

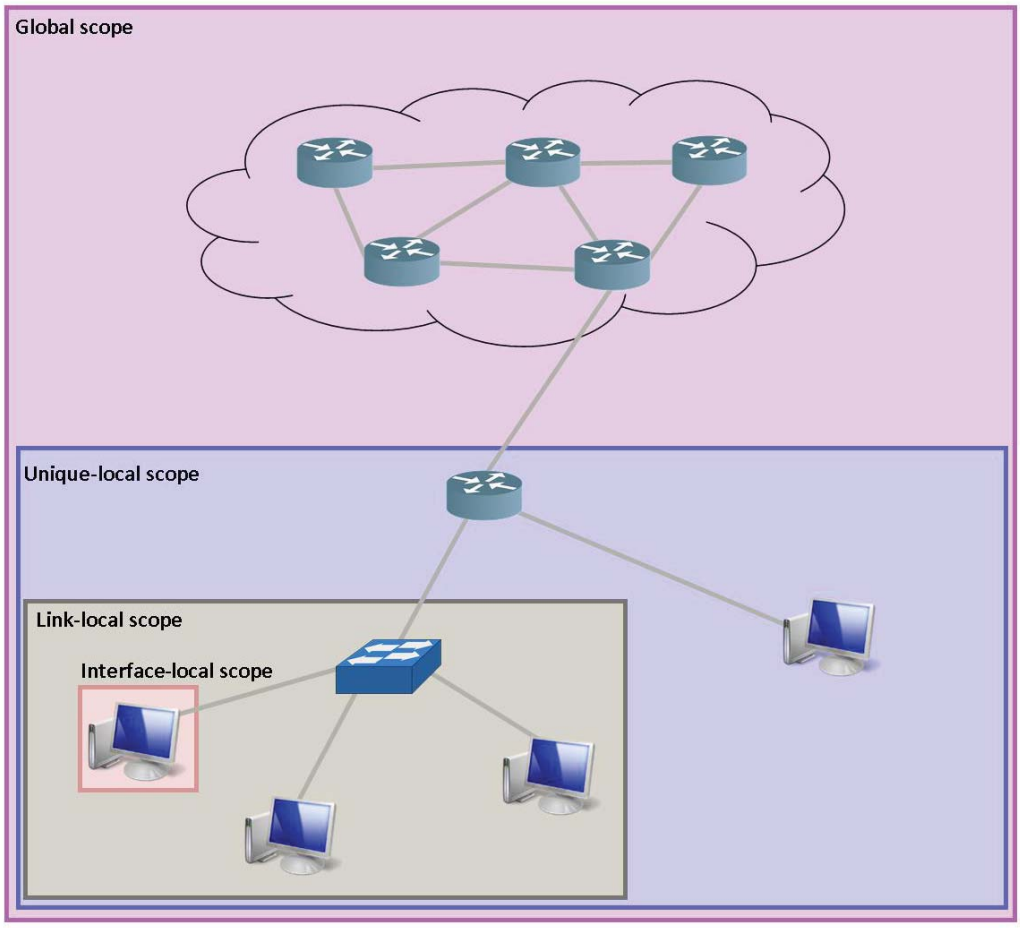

Figure 3.2: IPv6 scoped address architecture

always set as 1. Therefore the unique local address always starts with the value FD00 as shown in the figure 3.5.

∗ **Special addresses** : There are three unique addresses defined in the IPv6.

• **Unspecified address**: The unspecified address simply indicates that no valid address has been assigned to a device. The unspecified address is represented by ::/128 which is equivalent to 0:0:0:0:0:0:0:0/128.

• **Default route address**: In the condition where a device cannot find a route to forward a particular packet, the device sends the packet to the default route specified by the address ::/0. The default route generally points to another router where the process is repeated. This default router checks if a route exists to the destination, if not then it forwards the packet to its default router. The process is repeated till the packet reaches the destination or the hop limit exceeds and the packet is dropped. Every traversal to a default router is also accounted as one hop.

• **Loopback address**: The loopback address is a software loopback to the device itself. It has no hardware connection to the network and is generally used by the software engineers to test the device without actually sending the packets on the network and having to worry

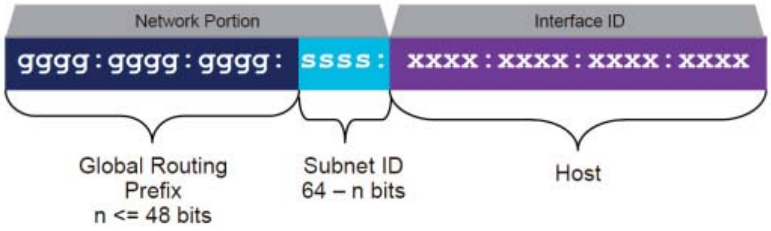

Figure 3.3: Global unicast address format in IPv6

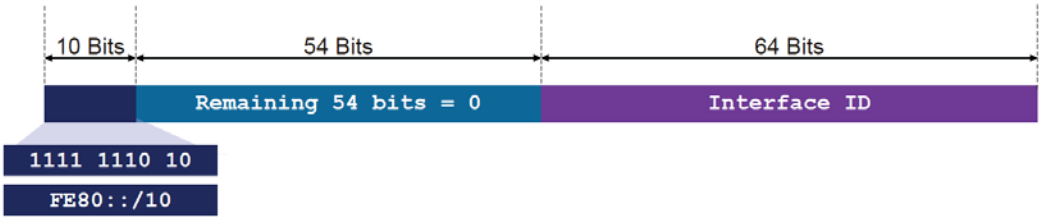

Figure 3.4: Link local address format in IPv6

about to broken or corrupted drivers and hardware. In the IPv6 the loopback address is defined as ::1/128 which is equivalent to 0:0:0:0:0:0:0:1/128.

* **Reserved addresses** : The IPv6 does not support broadcast address specifically, rather defines multicast groups which can be equivalent to a broadcast address. The table 3.1 shows some of the reserved IPv6 multicast addresses.

Table 3.1: Reserved IPv6 multi-cast addresses for routers and nodes

IPv6 Address	Scope
FF01::1	All nodes interface local
FF01::2	All routers interface local
FF02::1	All nodes in link local
FF02::2	All routers in link local
FF05::2	All routers in site local

These addresses are used by nodes to find other nodes and routers in their link local scope. The addresses are essential in the process of setting up of the network where the nodes communicate with their link local scope nodes to form their neighbor table entries and the routers on the link local scope are essential to confirm address selection of a node.

3.4.2 Addressing modes

The addressing mode [51] refers to the different ways by which a single device can be accessed, that implies the same device can be accessed by different addresses based on the scope of the address. The abstraction 'scope' in IPv6 addressing is classified into three types: Unicast, Multicast and Anycast address.

* **Unicast addressing** : The unicast address is an unique identification of the device in a network. When a packet is intended for a very specific user in the network, the Unicast address of the intended recepient is attached as the destination address of the packet, by this way the packet is delivered only to a specific device of the network. The figure 3.6 shows a depiction

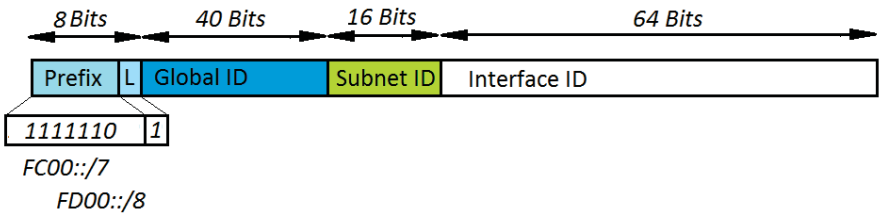

Figure 3.5: Unique local address format in IPv6

of how the unicast addressing works. As seen, many devices are in the network, but the packet is meant for a specific device and it is sent across network over a specific path with destination address as the intended recipient's unique unicast address.

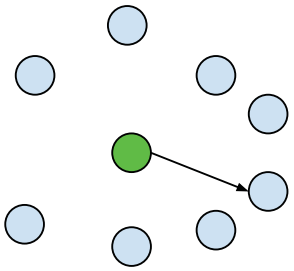

Figure 3.6: IPv6 Unicast addressing

∗ **Multicast addressing** : The multicast address is used to send the same packet to more than one device. All the devices part of the multicast group are assigned a multicast address, thus any packet sent with destination address as the defined multicast group address, is processed by all the devices part of the multicast group. IPv4 supports broadcast which is replaced by multicast address in IPv6. Theoretically the address can be defined as multicast but technically an address is assigned as "all nodes multicast group" which is equivalent to the IPv4 broadcast, in which all the nodes of the network are part of the group. The multicast addressing is done as shown in the figure 3.7.

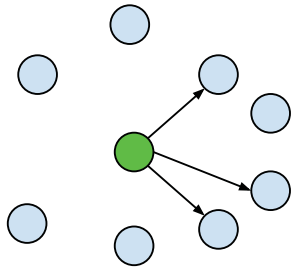

Figure 3.7: IPv6 Multicast addressing

∗ **Anycast addressing** : The anycast addressing has been introduced by the IPv6, the functionality of which is unavailable in the IPv4. In the anycast addressing mode, more than one device is assigned the same anycast address. When a device wants to communicate to this anycast address, then it sends the packet as a unicast message with the anycast address as the destination, thereby, the routing protocol makes a decision to send the packet

to the nearest device with the anycast address, where distance is measured by the cost of communication i.e the lesser cost closer the device and vice versa. The anycast addressing is depicted in the figure 3.8. Anycast addresses are designed to enable quick routing table updates. For example a router can send its routing table update to the anycast address of the routers, the nearby router processes it and sends it to another anycast address, thereby the group has regular routing table update.

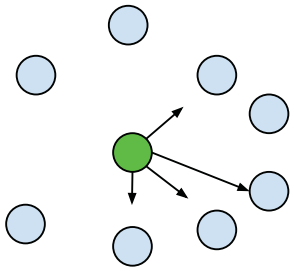

Figure 3.8: IPv6 Anycast addressing

3.4.3 IPv6 Headers

The IPv6 header [51] is one of the main differentiating factors between the two internet protocol versions, IPv4 and IPv6. Though the IPv6 address is 4 times larger than that of the IPv4 address, the IPv6 header is only twice the size of an IPv4 address. The IPv6 address has a, fixed header which contains all the information required for the router and an extension header which helps the router understand the packet handling process.

∗ **Fixed header** : The figure 3.9, image taken from [8], shows the structure of an IPv6 fixed header. The IPv6 fixed header consists of 8 distinct fields.

• **Version**(4-bits): This field represents the version of internet protocol used by the packet. For the IPv6, the version is 0110.

• **Traffic class**(8-bits): The traffic class field also known as the priority field, is split into two parts, the first 6-bits carry the type of service information. This field allows the source node to set different priorities to the packets which enables easier tracking of the packets generated by the same source node with different delivery priorities. This field helps the router in determining which packet has to get a higher delivery priority.

• **Flow label**(20-bits): The flow label is 20-bit entry which is used to sequence multiple packets of data. At the receiver or router, the node will know the sequence of arrived packets and helps in re-ordering them. For a default router handling, the flow label is set to a value of 0. The flow label was designed by keeping in mind the streams of data, such as audio and video. The routers must handle the data of same flow in a similar fashion. The handling information maybe specified within the same data packet or the router might look up for a routing protocol such as the RSVP. When a new flow arrives at the router, the data is cached and the other segments of data arriving with same flow information can be directed based on the cached information, this helps in faster and more efficient routing.

• **Payload length**(16-bits): The 16 bits of payload is used to store information about the amount of data the packet contains. The packet may consist of data from upper layers such as TCP and UDP. With 16-bits allotted in the total size, data size upto 65535 bytes can be indicated, but if the extension headers also contain the hop-by-hop extension, then the payload size might exceed the length of 65535 bytes. In case the payload itself exceeds the limit of 65535, then a new packet called a *Jumbogram*. When a *Jumbogram* packet

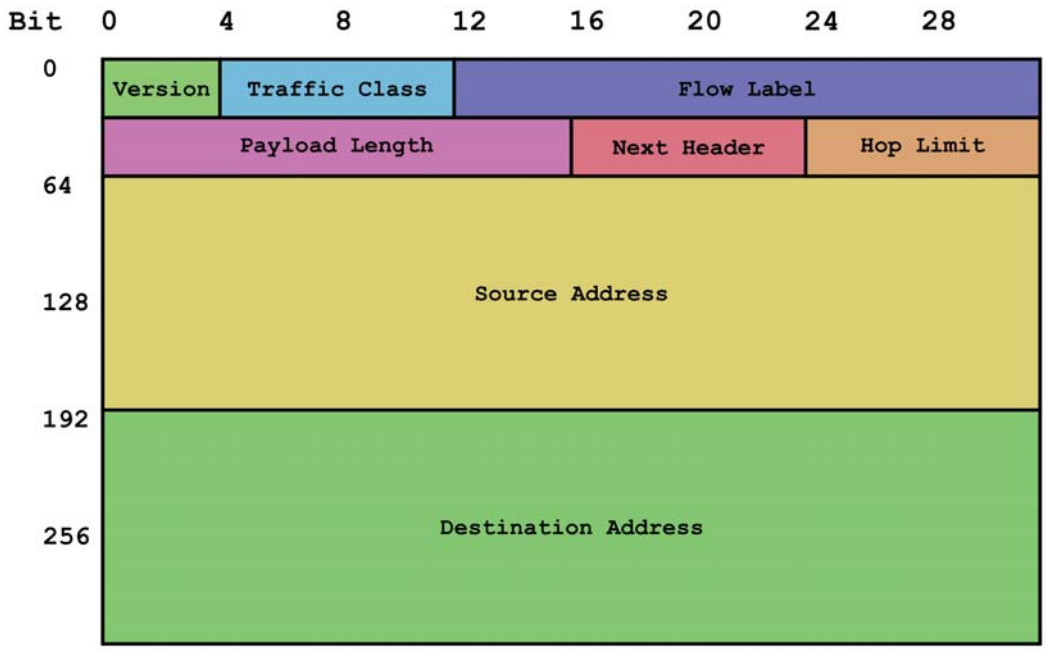

Figure 3.9: IPv6 fixed header format

is constructed, the payload length size is indicated as 0. The *Jumbograms* are used in supercomputer communication.

• **Next header**(8-bits): The next header field is used to indicate a presence or absence of extension headers as seen in the table 6.1. It also specifies the type of transport layer protocol used by the packet, generally, TCP, ICMPv6 or the UDP. The table 6.1 shows some of the values of next header field and their implications.

Table 3.2: Values of next header field

Value(in decimal)	Header
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
46	RSVP
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No next header
60	Destination Options Header

• **Hop limit**(8-bits): The hop limit field is mainly used for preventing infinite looping of a packet in the network. When a packet is created, this field is set to a maximum value of 255. Every node which receives this packet decrements the value by 1. When this value reaches 0, the packet is discarded and an ICMPv6 Time Exceeded message is generated.

• **Source address**(128-bits): This field indicates the IPv6 address of the node which generated the packet.

• **Destination address**(128-bits): This field indicates the IPv6 address of the intended recipient of the packet. If a routing extension header is present, then this field will indicate the address of the next router.

∗ **Extension header** : The IPv6 fixed header contains only the necessary information for a basic communication and routing. Other information, which may be sparsely used, are attached in the extension headers, where each extension header has an unique identifier. When extension headers are used, in the fixed header, a field is set to a certain value indicating the type of next extension header. If there are multiple extension headers then the next extension header will contain a value indicating the subsequent extension headers. The last one will contain a value of 59 which is a reference to no more extension headers. The table 3.3 shows the different extension header values and their brief description.

Table 3.3: Values of next header field

Extension header	Value(in decimal)	Description
Hop-by-Hop Options Header	0	Read by all devices in transit network
Routing header	43	Contains methods to support routing decision
Fragment Header	44	Contains parameters of data fragmentation
Encapsulating security payload header	50	Encryption information
Authentication Header	51	Information regarding the authenticity
Destination Options Header	60	Read by destination devices

The extension headers must be only in the sequence as indicated by the table 3.4. The extension headers are placed one after the other in a linked list format.

Table 3.4: Sequence of extention headers

Extension header
IPv6 Header
Hop-by-Hop Options Header
Destination Options Header
Routing header
Fragment Header
Authentication Header
Encapsulating security payload header
Destination Options Header
Upper Layer Header

3.4.4 Communication

The basic requirement for a device to communicate layer 3 messages is an unique IP address. In the IPv4 a device obtains its IP address by the DHCP or through manual configurations. Once the

IP address is confirmed, then in order to communicate with another node, following information is a mandatory requirement:

1. Source IP address
2. Source MAC address
3. Destination IP address
4. Destination MAC address

After the confirmation of address by DHCP or manual configuration, the source device has the 1st two data. The third information is provided by the higher layers or the routing protocol, but before sending the packet, it is essential to know the destination MAC address. In the IPv4, Address Resolution Protocol (ARP) takes care of obtaining the destination MAC address. The ARP sends a MAC level broadcast message requesting for the MAC address of the destination node, following which the destination node replies on a unicast message to the source node with its corresponding MAC address. In the end, all the 4 parameters are obtained to kick start the communication. On the contrary, the IPv6 does not required for the node to obtain the IP address using manual configuration or the DHCP, rather the IPv6 is designed to auto-configure the addresses. Also, IPv6 does not support broadcast messages which is replaced by multicasts. The Neighbor Discovery Protocol (NDP) takes care of all these processes using the ICMPv6 messages which acts as replacement and an enhancement to the ARP.

Neighbor Discovery Protocol (NDP) : The NDP [25] is an IPv6 communication protocol which is a replacement for the ARP in IPv4. This protocol helps in auto-configuration of IPv6 link local address. After a node has obtained a unique link local address, it joins a number of multicast groups in order to find a router, discover other nodes in the same network and associate itself with the global communication if necessary. All the communication between large number of nodes takes place on the multicast group. The NDP has following steps in the process of ascertaining a node's address:

• **Neighbor solicitation**: The first and foremost step in the process is to establish an IPv6 address for itself. This is done by either manual configuration, auto-configuration or the DHCPv6. After the device has assigned an address to itself, it should ensure that the same address is not utilized by other devices, therefore the device sends a group multiucast message to FF02::1 where all nodes in the same link local scope listen to the packet. If any node has already confirmed the same address then the device gets a reply, and thus a new address should be assigned. If not, then the address is confirmed and proceeds with the next step. If two nodes are trying to assign the same address, then they back off for a random amount of time. Since the back off is random, the device whose back off period expires the first, sends another neighbor solicitation message, upon which the address assignment gets confirmed the other node whose back off period was longer must create a new IPv6 address which is generally forced to be done by manual intervention.

• **Duplicate Address Detection (DAD)**: Once the Neighbor solicitation message has been dispatched, the device waits for certain duration of time for a response, a response for the message sent through its newly assigned address, soliciting if another node has already assigned the same address to itself. If the device does not get any reply during this duration of time, it is safe to assume that no other device possesses the same address and the address can be confirmed. This process is termed as Duplicate Address Detection and is very essential in the Neighbor Discovery Protocol.

• **Neighbor Advertisement**: Once the DAD process is completed, the device sets up its interface for the specific address and then sends out a message on the link local scope stating that it has assigned the specific address for itself, and everyone who is listening to the MAC multicast message can make a note of the IPv6 address of the device and in the future can communicate with the device on that specific address. This is an advertisement message

sent by the node, thus its called as neighbor advertisement. The above three steps ensure a device gets a link local address. In order to be accessible globally, the device requires a global unicast address which can be assigned only with the help of the router. Therefore, the device next should find a router in its link local scope and seek a global unicast address.

• **Router solicitation**: All the routers in the link local scope listen to packets on an address of FF02::2 which is an address for all routers multicast on link local scope as stated in the table 3.1. The devices seeking a global address, sends a message on this multicast group address soliciting a router in the link local scope. This helps the device in setting up its default gateway: a router to which the device unicasts all its packets if it does not know the route to a specific destination.In the case of failure of a default gateway the device solicits another router, following which it changes its default gateway to the new router.

• **Router advertisement**: On receiving a router solicitation message, the routers respond with a router advertisement to indicate their presence. The router advertisement will consist of a global unicast prefix, which is necessary for a device to assign a global address to itself. Therefore the device on a global network, will be identified by its router's prefix.

• **Redirect**: Sometimes, when a router receives a router solicitation message from a device, it knows that a better router is available for that particular device, therefore sends a redirect message to the device asking it to contact another router and set it as its default gateway.

• **Unicast communication**: Device to Device communication establishment requires the following information:

- Source MAC address
- Source IPv6 address
- Destination MAC address
- Destination IPv6 address

By the end of NDP, the source addresses, MAC and IPv6, are confirmed. The application specifies the IPv6 address of the destination node. The only unknown field is the destination MAC address.

Before understanding the process of obtaining the destination MAC address, its is essential to understand the solicited node multicast address generation process. Every device, on confirming its unicast address (either global or link local) or anycast address, it computes its own solicited node multicast address and joins the group, thereby responding to packets with destination address stated as its solicited node multicast address. The solicited node multicast address is calculated by taking lower order 24-bits of its unicast/anycast address and appending the prefix

FF02:0:0:0:0:1:FF00::/104

Resulting in a multicast address in the range

FF02:0:0:0:0:1:FF00:0000 to FF02:0:0:0:0:1:FFFF:FFFF

for instance, if the IPv6 address is

1234::12:123:12AA:BBCC

then the solicited node multicast address is calculated as

FF02::1:FFAA:BBCC

The MAC prefix of 33-33-FF is a reserved prefix for the MAC broadcasts. Therefore the sender device knows a MAC address on which the receiver is listening. This MAC address is calculated by appending a prefix of 33-33-FF to the lower 24 bits of the destination IPv6 address.

Now, in order to obtain the unicast MAC address of a destination node, the source node computes the destination node's solicited node multicast address. It then creates a packet with the destination address as the intended node's solicited node multicast address and sends it across with the MAC address as computed previously. The receiver is listening on this particular MAC address and the destination IPv6 address also matches with its solicited node multicast address. The packet contains the sender's IPv6 and MAC unicast address. Therefore destination replies with its own unicast MAC address attached in the packet which is received and processed by the sender. After processing this packet, the sender knows all the four required parameters and it is in a position to send intended data packets. This is the process of communication if a node does not know the receiver's unicast MAC address.

3.4.5 Subnetting

The IPv4 addresses defined a clear set of bits which can be used for creating subnet addresses. The subnet addresses in IPv4 are created using the netmasks, which allows one to use the host bits and created subnet bits. But, with increase in number of subnets, can lead to decrease in number of hosts per subnet as lesser number of address options are available to be chosen from. On the other hand IPv6 addresses use 128-bits, in which 16-bits are reserved for a subnet identifier as seen in the figure 3.3. Therefore, there are no bits sacrificed in order to form new subnets at the cost of host bits. These 16-bits provide 65535 unique subnet identifiers with each of them having 264 hosts, which in the entirety is a large amount and more than sufficient in many cases.

3.4.6 Routing protocols

Routing is the process by which a source node can speak to its intended destination node via multiple nodes and large number of possible routes to choose from. The routing protocol makes a decision of choosing the best route (based on certain
acrshortqos metrics). The routing protocols which were used by IPv4 are compatible with IPv6. The routing protocols can be classified based on the basis for functionality as:

* **Distance vector routing protocol** : The distance vector routing protocols rely upon certain link quality metrics to make a decision of best possible route. These metrics are hypothetically a measure of distance between two nodes. The distance vector routing protocols depend upon their immediate, i.e. the one hop neighbors, to find the best possible route from a source to destination. For example: RIPng, AODV etc.

* **Link state routing protocol** : The link state routing protocol, as name indicates, evaluates the state of a link and informs all its neighbors (generally periodically). The routing protocol is designed to make use of this link state information and decide the best possible route to a destination from a source node. Generally involves high overhead at the benefit of better reliability. For example: OSPF

The routing protocols, based on the scope, can be classified into two categories:

* **Interior routing protocol** : These routing protocols are used among the devices within a network boundary, such as used only by the routers in case of RIPng.

* **Exterior routing protocol** : These routing protocols are used to route or forward messages outside two or more autonomous systems. For example: BGP.

Protocols tuned to IPv6 The IPv4 routing protocol consists of a number of other smaller routing protocols designed for a specific purpose, such as the ICMP, DHCP and DNS. These protocols have been retained in the IPv6 but with some modifications.

- **ICMPv6**: The Internet Control Message Protocol version 6 is the upgraded version the ICMP used in IPv4, with small changes to accommodate the IPv6. The ICMPv6 is used for diagnostic messages, errors in packets, time outs, NDP etc.

- **DHCPv6**: The Dynamic Host Configuration Protocol version 6 is a replacement of the DHCP used in IPv4. The DHCP was responsible for address configuration in IPv4, whereas it is no longer required in IPv6 as the same functionality is carried out by the ICMPv6 messages. Nevertheless, the DHCPv6 can still be used to obtain this information. The DHCPv6 is extendable and can be used to include additional information of IPv6 which may not be present during address assignment.

- **DNS**: Though there is no new version of the DNS, but it has been configured to respond for IPv6 queries.

3.5 Summary

With the exponential rise in the internet usage, its only a matter of time before IPv4 becomes obsolete and the start of IPv6 domination. Many devices are being configured to make the best of the IPv6 while still retaining complete functionality of IPv4. The transition from IPv4 to IPv6 is expected to be smooth with a lot of facilities available to retain both the address and use tunneling, eventually migrating to the IPv6. The IPv6 is not just an extension of IPv4, it rather is a whole new different phenomenon which will create plenty of opportunities in the field of internet technology and its applications.

Chapter 4

Ad hoc On-Demand Distance Vector routing protocol

4.1 Introduction

There are a large number of distinct devices operating in the Internet of Things, the configurations of these devices are different and dependent on the type of application. These devices are connected to a network through wired or wireless technologies. The communication between the devices in a network may not be through direct one-to-one links. It is also possible that the network is further divided into subnets and devices are required to connect to two or more subnets and handle the traffic between them. The devices need to be able to reliably communicate among each other without a direct connection. The fact is that the devices used in the IoT applications are not necessarily powerful and static by position, there shall be applications where devices are of miniature size and are mobile in nature, such as patient monitoring systems, animal tracking etc. Considering all these possible conditions, it is essential that specific algorithms be designed to promote communication among the devices in the network. This calls for an efficient, dynamic and robust routing protocol at the network layer which takes into consideration a large number of constraints, that have been explained in the subsequent sections.

The Wireless Sensor Networks' generally consist of a large number of nodes, in order to establish communication between these nodes, a specific network topology has to be identified. The network topology forms a good base to introduce a routing algorithm to direct messages from one node to another. The routing algorithms interchangeably used with the routing protocols, determine the path for a message to move from a source node to a destination node. In WSNs, where there are large number of nodes situated in different environmental conditions, it is essential to improve the reliability of communication in the network. It is highly likely that in such a large network, for a node to communicate with another node, there could be multiple paths of communication, but each of the paths may instantaneously offer different link quality among the nodes themselves, due to, mobility, environmental conditions, hardware health, and many more reasons. Therefore, the routing protocol takes into consideration certain predetermined metrics, which give an estimate of link quality, and choose the best path to establish the communication. Thus it is of utmost importance to choose the appropriate routing protocol, based on the application requirements.

4.1.1 Challenges in network design

In the past few years, extensive research has been carried out on the Wireless Sensor Network [49][28][15] keeping in mind different aspects associated with it such as the environmental conditions, heterogeneity of devices within the network etc. Based on such factors, generic routing

protocols were designed, which can be customized based on the application requirement. Some of the major challenges in establishing a reliable Wireless Sensor Network include:

* **Node deployemnt** : The sensor nodes may be deployed in a static or random fashion. In case of minimum mobility of devices, generally, static routing is established where the path between two nodes are predefined. On the other hand, if the deployment is random, then the nodes try to find routes among themselves using a routing protocol. Generally, the communication ranges of these nodes are geographically small and cannot communicate with other nodes in the network directly through one-to-one links, therefore they rely on multi hop paths to establish communication between other nodes of the network.

* **Energy consumption** : The sensor nodes in a Wireless Sensor Network could be battery operated, in which case the energy consumption of the node plays a very important role. In the case of a power failure of a node, there could be ripple effects such as link breakage, loss of communication paths etc thereby disturbing the entire network setup. The routing protocol must be resilient and should be able to function even in dire circumstances of node failure in a Wireless Sensor Network.

* **Data transmission frequency** : The applications of the WSN might have different frequency of data communication. In some scenarios such as detection of forest fire, the messages are infrequent, but require a highly reliable route when there is a message to be sent. On the other hand, if the scenario is like sports training monitoring, then a loss of few messages within a span of a second may not make a huge difference where the message frequency is comparatively high. Therefore the routing protocol should ensure the reliability of network based on the message frequency in the application.

* **Heterogeneity of network** : A Wireless Sensor Network may consist of distinct devices. The data rates, communication range, energy consumption, memory and many other parameters may not be the same as that of other devices within the network. Sometimes, the network depends on the routing protocol to take into consideration such an heterogeneous network and perform efficient routing of messages.

* **Dynamics of network** : The devices in a Wireless Sensor Network could be mobile in nature, thus, the routing protocol should be robust and adaptive to ever changing conditions of the network and perform efficient routing. Additionally, the dynamics of network could be defined by the network traffic which can vary at short intervals due to unprecedented events in the network such as a sudden burst of messages in the network due to simultaneous activity in all the nodes. These dynamic network conditions make the design of routing protocol challenging.

* **Medium of transmission** : Under different environmental condition, transmission media in specific, the network conditions tend to change, which could have a direct impact on the efficiency of network. For example in sensor devices are placed on the cold mountains then the devices must be able to operated under extreme conditions of temperature changes, snow, rain etc, throughout the year, accessibility of the devices often is not an option, then the network conditions change drastically which should be taken into consideration by the routing protocol.

These are some of the major constraints which make the design of routing protocols for an application in Wireless Sensor Network, an uphill task.

4.1.2 Mobile Ad hoc Networking

In a large set of applications of WSNs, the devices can be perceived as mobile either with respect to position changes or change in environmental conditions thereby the links to other devices may change. Such networks that change their links with other devices dynamically, are termed as

Mobile Ad hoc Network (MANET). In such a scenario, the devices may be connected over a small sized network, or may communicate with other devices over the internet and require ad-hoc routing. The following are some of the types of MANETs [14][11]:

* **Vehicular Ad hoc Network (VANET)** : These are ad hoc networks inside a vehicle operating in highly dynamic environment due to, the mobility of vehicle, interference from external sources, vehicle to vehicle interference etc. The systems installed inside vehicle have to be very intelligent and efficient.

* **Smart Phone Ad hoc Network (SPAN)** : The SPAN are networks which generally use WiFi to connect with other devices, these networks are dynamic and require intelligent routing to keep the network connected. These networks work on the basis of peer to peer networking and there exists no single coordinator of the network, also the devices can join and leave as and when necessary.

* **Internet based Mobile Ad hoc Network (iMANET)** : The iMANET are ad hoc networks which connect a large number of mobile nodes with a static gateway node. The regular routing protocols are not applicable to the iMANET, special routing protocols have to be designed, based on the application requirements.

* **Military Mobile Ad hoc Network (M-MANET)** :These networks are mainly used for tactical battles in the military defense forces. They are designed to focus on security, reliability, longer range. They find applications in a large number of domains of the defense forces mainly in the infantry of an army.

As stated in the section 4.1, routing protocols can be designed based on the application requirement. The applications consists of a large number of domains, therefore, the routing protocols can be classified based on various categories [15][49][28]. Some of them include, routing based on: objective, architecture, transmission power, operational base, route selection, network structure, protocol operation, location based, data-centric, hierarchical, mobility, heterogeneity of network etc. In the MANET category, the routing protocols are classified on one of the parameters namely; route selection technique. Based on this technique, the routing protocols can be further classified into the following categories [18] :

* **Proactive routing protocols** : The proactive routing protocols [18][45][35] are also popularly known as table driven routing protocols. These routing protocols maintain active routes to all nodes in the network at all times using routing tables. The routing table entries contain a sequence number which indicate the freshness of the entry, the larger the sequence number, the more latest is the entry. To maintain these active routes, nodes periodically broadcast routing table information to other nodes in its vicinity, this way after a certain period of time, all the nodes will have updated their routing table for the entire network. The major advantage of the proactive routing protocols include:

  • Decrease in latency of communication, as active routes are available at all instances of time, therefore the nodes select the route and transfer their message, with a negligible delay between finding route and transferring data.

  • On a small network, these protocols are highly effective and provide high throughput.

  On the contrary, the drawbacks of such table driven routing protocols are:

  • A large overhead due to redundant routing table entries, which may or may not be used.

  • Increase in power consumption due to periodic sharing of routing table information.

  • Increase in network traffic due to the periodic broadcasts of information. The proactive routing protocols are preferred for small networks that have lesser energy consumption constraint and require lower latency. Some of the examples of proactive routing protocols are DSDV, OLSR etc.

∗ **Reactive routing protocols** : In the reactive routing protocols [18][45][35], the route to a specific node is calculated on demand. Therefore these are also termed as on-demand routing protocols. When a node wants to communicate with another node, and it does not have a route in its routing table, then it requests its immediate neighbor to provide a route. The request message is flooded throughout the network till a route is obtained. The routing entries are not stored forever, based on certain conditions, timers are set, on expiration of which a routing table entry is deleted. These routing protocols have advantages and disadvantages, based on the application requirement these can be balanced by customizing the protocol to a certain extent. The major advantages of the reactive routing protocols are:

• In comparison to proactive routing protocols, these have a smaller overheadm, as the messages are not broadcasted periodically.

• The amount of energy spent on transmission is reduced due to less periodic messages, also the nodes can sleep for longer duration of time.

• Memory usage is considerably reduced due elimination of redundant routes in the routing table.

Some of the shortcomings of the reactive routing protocols are:

• Whenever a node has to transmit a message to another specific node for the first time or when its route entry to the node has expired, then it has to wait for certain amount of time before a route is discovered. This amounts to some latency in communication.

• The route request messages are flooded in the network, which accounts to increase in network traffic.

• The routing table entries have to be carefully entered after considering a large number of link quality parameters, after which a reliable route can be established.

The reactive routing protocols are more suitable for low data rate, low power communication networks, which can accept some small degree of latency and have lower energy consumption. Some of the examples of reactive routing protocols include AODV, DSR.

4.2 Reactive Routing Protocols

4.2.1 DSR, DSDV and AODV

The reactive routing protocols are highly compatible with the low power and low rate data communication networks. A large number of reactive routing protocols are available which offer flexibility in customization of the protocol, based on the application requirements. Johnson and Maltz have introduced the DSR protocol[23][24] routing protocol which falls under the category of reactive routing protocols. The DSR protocol was designed for requirements of the multi hop ad hoc networks. The protocol is self organizing and self configuring, thus requiring minimal manual intervention. The DSR protocol allows more than one route between two devices allowing the user to choose the route based on the requirement such as load balancing, reduce energy consumption, higher throughput etc. The DSR ensures loop free routing, provides quick recovery of lost routes and operation of network containing unidirectional links. The DSR has less overhead in comparison to other MANET reactive routing protocols also performs route discovery less often. Though the performance is comparable to the other routing protocols, but it is slightly inferior for highly mobile nodes.

The Destination Sequence Distance Vector (DSDV)[21] is yet another reactive routing protocol catering to the needs of MANET. The DSDV allows devices to communicate with each other over multi hops in the absence of a base station like device. The routing information is broadcasted or multicasted periodically, where the period is estimated based on the arrival of first and the

best route to destinations, this way, redundant routes are not dispensed, rather reliable routes are communicated. The algorithm is carefully designed to estimate this period at an optimal value, in order to reduce the network traffic and also maintain reliable routes. The drawback is that, if the period is long, then the probability of sending data packets over stale links (unused for long durations of time) is high. Therefore a balance needs to be struck between a stale and a reliable route establishment. In the paper [21], Perkins and Bhagwat explain the methodology to strike this balance and also evaluate the performance of the DSDV routing protocol. They also explain the need for inclusion of layer 3 information in layer 2 operation for a reliable routing protocol. The authors also describe the settling time of the routing table entries to establish reliable routes, finally making a brief comparison of the DSDV with few other reactive routing protocols. In [36] authors compare the performance of DSDV and AODV, of which the Ad-hoc On demand Distance Vector routing protocol is described in the section 4.3.

The Ad-hoc On demand Distance Vector (AODV)[20] is a reactive routing protocol and as the name suggests it discovers the routes on demand. The AODV routing protocol is designed specially for the MANETs considering its ability to adapt to ever changing environmental conditions, also adaptable to mobile nodes network. The AODV is designed by combining features of DSR and DSDV, blending the advantages of two distinct protocols and forming a more reliable routing protocol for the MANETs.

4.2.2 ZigBee and AODV routing protocol

Some of the critical issues of many routing protocols, such as the looping and 'Bellman-Ford's counting to infinity' [34] are prevented in the careful design of the AODV routing protocol. The AODV is a descendant of the DSDV routing protocol, inheriting many properties but more robust and efficient in large aspects for instance in DSDV broadcasts every change in the network to every other node, which is not necessary in AODV to maintain active routes. When a new link is established in the network, all the nodes are informed about the new link in DSDV, whereas in AODV this is not required. Also, when a link breaks, then in DSDV all the nodes are informed about the breakage of link, on the contrary in AODV only the nodes affected with the link breakage are informed. Therefore, a lot of redundant communications are removed in AODV therefore reducing the overhead of communication and also the traffic in network. The AODV delivers a better performance than DSDV as proved in [36]. The ZigBee uses the AODV routing protocol as the networks where the ZigBee is used are dynamic in terms of device position and the network environment changes continuously, leading to changes in the links of the network. Such a case requires ad-hoc routing which is provided by the AODV.

The 802.15.4 ZigBee devices consist of two different addresses, a 16-bit (short) address which is assigned by the coordinator when a device joins the network and a 64-bit (long) address which is unique. The 16-bit address is unique only is a particular network. This address can change when the device leaves the network and joins the network of another coordinator. The 64-bit address is a permanent address which is assigned when the device is manufactured. It is necessary to know the 16-bit address of a device, as the data transmission uses the 16-bit addresses. The data can be addressed using both, 16-bit short address or the 64-bit long address. Data in ZigBee networks is a unicast to a specific device or is a broadcast to certain devices.

* **Broadcast transmissions** : In ZigBee, the broadcast transmissions aim to ensure that all the devices in the network receive the information, in order ascertain this, every device transmits a packet 3 times. The device also makes an entry in its broadcast table, where each entry lasts for 8 seconds. This way the protocol ensures that the transmissions are not endless. The stack also maintains a buffer space for the broadcast data as it is retransmitted a number of times. A large broadcast packet demands large buffer space, therefore the broadcast transmissions should be used intelligently.

* **Unicast transmissions** : The unicsat transmissions aim to deliver the packet to a single in-

tended device. In order to perform unicsat transmissions, the device must know the intended receiver's 16-bit address assigned by the coordinator when the device joined the network. There are two processes involved in the unicast transmissions

• Device discovery: The sender device broadcasts a message requesting for the 16-bit address of the intended receiver device. This broadcast transmission contains the 64-bit unique identifier of the receiver, the devices on receiving this broadcast transmission check for the 64-bit identifier and respond if the id matches with their own 64-bit address. In case of a match, the receiver responds with a message containing its 16-bit address across the network through the same path the request was received.

• Route discovery: The ZigBee uses mesh routing to establish a route between source and destination node. The mesh routing allows multiple hops across the network to allow a packet to reach from a source to destination. Only the ZigBee routers and coordinators can participate in the process of route discovery. This process involves a specific routing algorithm termed as Ad-hoc On demand Distance Vector (AODV). The routing protocol is described in the section 4.3.

The process of network discovery and route discovery together, can be performed at different layers of the ZigBee stack. In the thesis, the approach is to use the IPv6 in the network layer. ZigBee uses 802.15.4 standards for the MAC and PHY layer. The size of 802.15.4 MAC address is not compatible with the IPv6 address. Therefore an adaptation layer called the 6LowPAN is used to perform the header compression of IPv6 headers to make it compatible with the 802.15.4 MAC headers. As shown in the figure 4.1, the routing can be performed in two different ways, the first ones is called the route-over routing, and the second is termed as mesh-under routing [29][32][22].

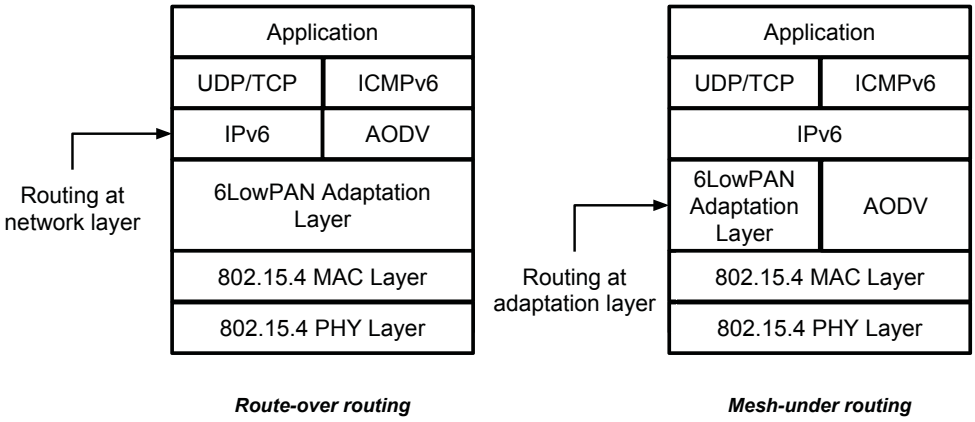

Figure 4.1: Route over and mesh under routing

∗ **Mesh-under routing** : The mesh-under routing technique performs routing over the 6LowPAN adaptation layer. It makes use of the MAC address or the 6LowPAN compressed headers to perform the routing. All fragments of an IP packet are routed to next hop to reach destination. The destination might receive different fragments of same IP packet from different routes.

∗ **Route-over routing** : The route-over routing technique uses the IPv6 stack to perform the routing. It uses the IPv6 addresses to identify different devices over the network. The 6LowPAN adaptation layer performs the header compression to make the IPv6 headers compatible with the MAC addresses. The fragments of IP packet are sent to next hop

neighbor, where the IP packet reconstruction takes place, following which the packet is forwarded to another next hop neighbor on route to the destination. This ensures that the fragments are reconstructed at every hop.

In mesh-under routing, if a fragment goes missing at the destination, the all fragments of the corresponding IP packet must be retransmitted from source to destination, which is additional overhead. Whereas, in route-over routing, the reconstruction of the IP packet takes place at every hop, thereby reducing the over head of a complete retransmission. As analysed in [32], the route over routing has far more benefits over the mesh under routing, mainly due to the prevention of collision thereby higher transmission probability. In our approach, we chose to use route over routing scheme as shown in figure 4.1, by using AODV routing protocol in the network layer.

4.3 The AODV routing protocol using IPv6

4.3.1 Introduction to AODV

The Ad-hoc On demand Distance Vector routing protocol[20] falls under the category of reactive routing protocols (see section 4.2). As the name indicates the routes are established in an Ad-Hoc fashion only when necessary, the routing protocol establishes multi-hop routes between a source and destination node. AODV does not maintain routes to nodes that have not been used for a certain duration of time, which is defined by a lifetime for every route, upon expiration of the lifetime, the route is deleted thereby reducing the size of the routing table. The AODV also facilitates passing information about broken links to all the affected nodes that were using the link in their routes.

4.3.2 AODV terminologies

The key terms required to understand the AODV routing protocols are described in brief here. The detail description is available in [41].

* Active route : An active route in a routing table entry which defines a valid route to particular destination. Only valid routes can be used to transmit data from source to destination node. A valid route is that route which is active and can be used for data communication.

* All nodes multicast address : The all nodes multicast is a IPv6 multicast group address. This multicast group consists of all the nodes which are in link-local scope. The all nodes multicast group address is (FF02::1)

* All routers multicast address : The all routers multicast address is the IPv6 multicast group address for all the routers in the link local scope.

* Destination : The destination address is IPv6 address of the intended recipient of a data packet. The destination address is supplied by the application through the IPv6 layer to the AODV routing protocol to provide a route to the specified address.

* Forwarding node : Any node which is not the intended recipient of a packet but forwards the packet/ or sends the packet to other nodes closer to the destination node is termed as a forwarding node.

* Forward route : The route established with the intention of sending packets from a source node to a destination node during the process of route discovery is called as a forward route.

* Invalid route : A route marked as invalid indicates that the routing table's lifetime has expired due to lack of activity over the route. Invalid routes should not be used to send data packets. The invalid routes indicate a previously alive route, thereby are kept to help in the process of route repair and also for future route requests.

* Originating node : A node that requests for a route to a specific destination is called as originating node.

* Reverse route : Upon reception of a route request and the receiver understands that the route request was intended to reach itself, it responds with a route reply message via the same path it received the route request. This path in which the route reply is sent is termed as reverse route.

* Sequence number : Sequence number indicates the freshness of information in the originating node. This number is incremented at different scenarios (as explained below), the higher the sequence number, the more fresh is the information. This is also used in preventing looping conditions in the AODV routing protocol. The following are cases in which the sequence number is modified:

  - Immediately before a node originates a route discovery, it MUST increment its own sequence number. This prevents conflicts with previously established reverse routes towards the originator of a RREQ.
  - Immediately before a destination node originates a RREP in response to a RREQ, it MUST update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.
  - The only other circumstance in which a node may change the destination sequence number in one of its route table entries is in response to a lost or expired link to the next hop towards that destination. The node determines which destinations use a particular next hop by consulting its routing table. In this case, for each destination that uses the next hop, the node increments the sequence number and marks the route as invalid.
  - A node may change the sequence number in the routing table entry of a destination only if:

    It is itself the destination node, and offers a new route to itself, or

    It receives an AODV message with new information about the sequence number for a destination node, or

    The path towards the destination node expires or breaks

  * Broken link: A link is said to be broken if no messages have been received in the link over a duration of time as defined by the timer ACTIVE_ROUTE_TIMEOUT.

4.3.3 AODV operation

In the approach to achieve the research goals of the project (as stated in the Chapter 1), the chosen routing mechanism is route-over routing, where the routing protocol operates at the network layer, see figure 4.1 for the stack architecture. The figure 4.2 shows the architectural design to simulate the behavior of a ZigBee network layer using the IPv6, AODV and the 6LowPAN modules. This is to pinpoint the functional layer of the AODV in the architecture. The IPv6 stack forms the network layer, and the AODV routing protocol uses the IPv6 addresses in routing mechanism. The Ad-hoc On demand Distance Vector routing protocol operates in two distinct phases, namely: Route discovery and route maintenance.

* **Route discovery** : The Ad-hoc On demand Distance Vector routing protocol uses two messages mainly; RREQ and RREP, to discover routes in a network. The advantage of AODV is that it is a self discovering routing protocol and requires minimum manual intervention. The routing table entry contains the following list of parameters:

  - Destination IPv6 address
  - Destination sequence number
  - Valid destination sequence number flag

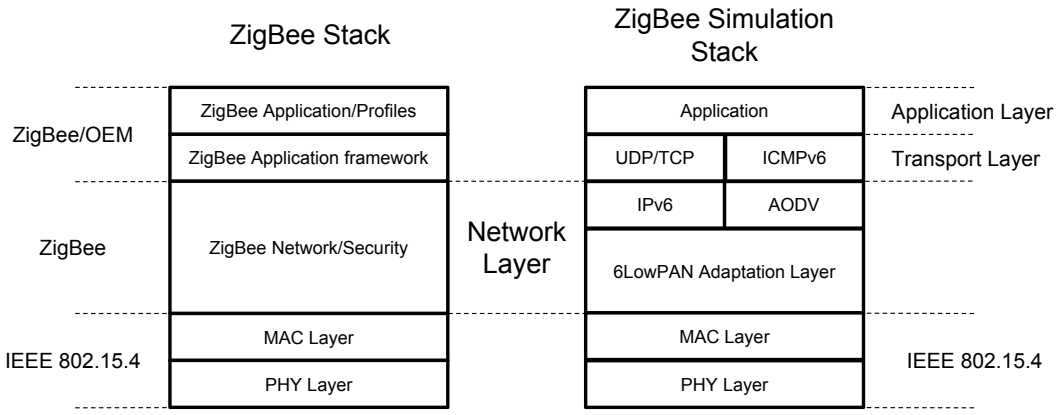

Figure 4.2: ZigBee network layer simulation architecture

- Network interface address
- Hop count
- Next hop
- Lifetime

When a node wants to send a data packet to another node, it looks up in its routing table to check if there is a route available to the specific destination node address. If it does not have a route to the destination address, then it sends a control message to all its one hop neighbors. In other words, these one hop neighbors in IPv6 are nothing but nodes in the link local scope. Therefore the source node sends a RREQ message to the all nodes multicast address (see section 4.3.2 for details). This is equivalent to broadcast address in IPv4. Every node in the link local scope receives the RREQ and begin to process it. The RREQ packet contains:

- source IPv6 address
- destination IPv6 address
- source node's latest sequence number
- destination node's sequence number
- multicast id

The multicast id, a counter value that indicates the number of times the RREQ message was sent for the same destination node with same sequence number, is incremented each time the source node uses the RREQ. The source IPv6 address and the multicast id form a unique identifier for the RREQ. The sequence numbers help in preventing looping of the messages. This is explained in detail in subsequent sections. The flowchart for the initiation of route discovery is shown in the figure 4.3. On receiving a RREQ message, the node first checks if it has a route to the original sender of the route request, called as origin node (see section 4.3.2). If it has an entry to origin, then it updates its routing table entries, if not, makes a new routing table entry. Then it checks if it has a routing table entry to the sender of RREQ, if yes, then updates routing table entry, if not, then creates a new routing table entry. The next step is to check if the node itself is the requested destination. It compares the destination address in the RREQ packet with its own addresses, if found matching, then it sends a RREP message to the sender of RREQ with the destination address of RREP as the origin of RREQ message. If it is found that it is not the destination, then it looks up in

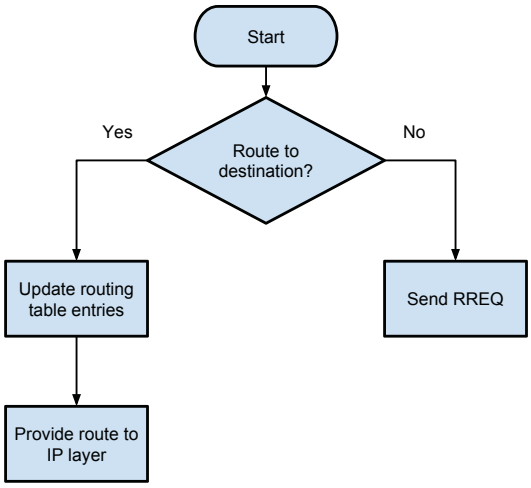

Figure 4.3: Initiation of route discovery by the RREQ messages

the routing table to check if it has a route to the destination. If route is found, then it sends a RREP to the sender of RREQ with the route to destination and appends the sequence number of the destination (from its routing table) in the RREP packet. Later, it checks if the gratuitous RREP is requested. The gratuitous RREP is a message which will be sent by this intermediate node to the actual destination node of the RREQ informing that it has sent the RREP to the origin node. If the node does not have a route to the destination, then it sends this RREQ to its immediate neighbors.

The flowchart for the handling of RREQ messages is shown in the figure 4.4. During the process of transmission and reception of the RREQ, a large number of nodes update their routing table and form routes to the source, destination and other nodes in the path of the control message. This process is termed as forward path establishment. The AODV routing protocol provides an extension technique to minimize communication overhead for data packets of small size. When the data packets are of low size, the data packets can be flooded with the RREQ message itself, therefore when the intended destination receives the RREQ message, it also has data packets in it, thus the data messages need not be sent again. This process is called as data flooding and the major advantage of this technique is its simplicity and higher efficiency if the data size is low. Whereas the process adds considerable overhead in the network and it significantly increases with small increase in the size of data packet.

The origin node may receive multiple RREP messages from different sources, but it chooses the one that arrived first and makes an entry in its routing table. The AODV routing protocol employs periodic messages called the 'Hello' messages, which are used to keep links active in a network. The Hello messages are constructed with following entries in a packet type RREP:

- Hoplimit is set as 1 indicating that the Hello message is only meant for 1 hop neighbors and should not be forwarded

- Destination address is set as the address of the sender of Hello message. This indicates to the receivers that the sender is in a single hop neighborhood and an immediate neighbor, and this is a sign of the hello message because the source and destination address of the packet is the same.

- Destination sequence number to be the latest sequence number of the source node.

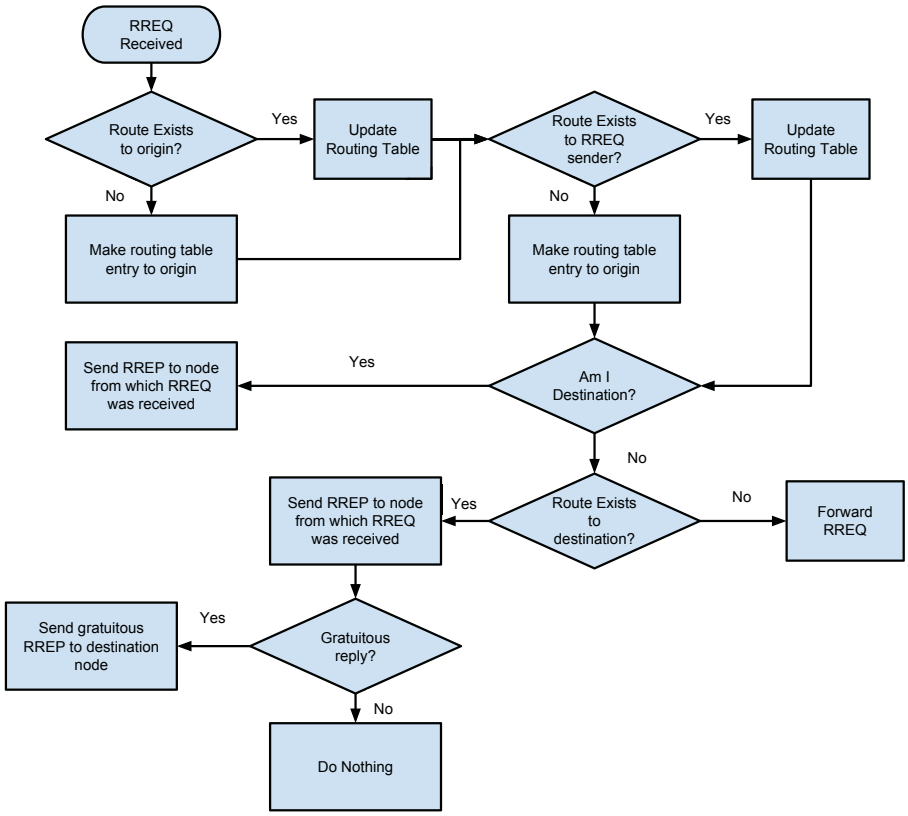

Figure 4.4: Flowchart indicating process of handling a RREQ message

Now, when a node receives a RREP message, it processes it to check if its an actual RREP or a Hello message. If the destination address and source address of a RREP message are same, then it indicates that it is a Hello message. On receiving a Hello message, it looks up in its routing table if there is a routing table entry. If there exists a routing table entry already, then it updates the routing table. If not, it creates a new routing table entry. In the case of the RREP message not being a Hello message, then it reads the packet and checks if it has a routing table entry to the destination of the RREQ message. If a route does not exist then it creates a routing table entry, if it exists, then it just updates the routing table entry. Next, it checks if the RREP message was meant to it. If the address of the source of RREP message matches with any of its addresses, then it means that the RREP message is meant for it. If that is true, then it updates its routing table and sends the packet in the AODV message queue. If the RREP message was not meant for itself, then it looks up in the routing table if a route exists to the origin of RREP message. It drops the packet if the route does not exist, but if a route exists then it updates the routing table and forwards the packet to the next hop on the route. During the process of a RREP message transmission from destination to origin node, all the intermediate nodes and destination node, setup or update their routing tables, this process is called as reverse path establishment. If the sender of RREP has requested for an acknowledgement then the receiver of RREP message replies with a RREPACK message.

Note: In a RREP message, the the origin refers to the actual sender of the RREQ message and the destination is the intended recipient of the RREQ message. The source address

could be the address of any intermediate node which is forwarding the packet and the next hop will be the address of the node which is an intermediate node in the route through which the RREP message should reach the origin node. The flow chart of handling a RREP message is shown in the figure

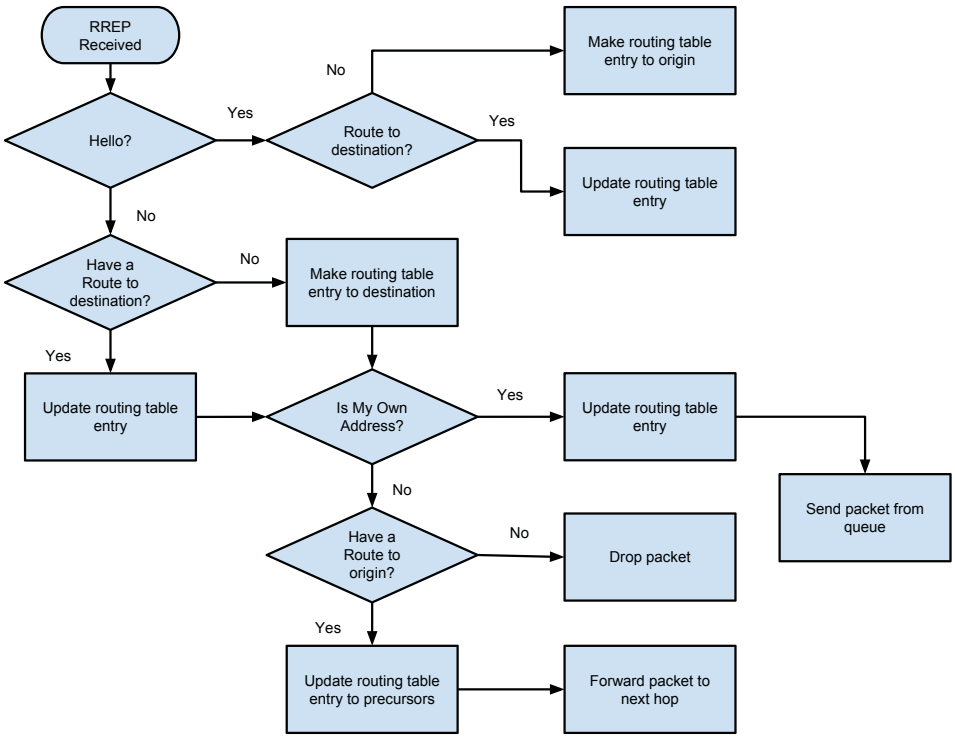

Figure 4.5: Flowchart indicating process of handling a RREP message

∗ **Route maintenance** : In the process of route discovery, forward and reverse path establishments, every routing table entry is assigned a lifetime (as per the user requirement). The lifetime is a timer, upon whose expiry, the route will be marked as invalid and will be no longer suitable for any data packet transmissions. Therefore, based on the application scenario, the AODV parameters have to be setup carefully. The lifetime known as ACTIVE_ROUTE_TIMEOUT is one such parameter. The timers play a vital role in the process of route maintenance. Whenever the route is used for any packet transfer i.e either control messages or data messages, the lifetime of the route is updated by resetting the timer to value whichever is maximum of current lifetime or the default value of ACTIVE_ROUTE_TIMEOUT.
In order to maintain routes, the links have to be active. The links are kept active by either exchange of Hello messages or any data packets, upon which the lifetime of route is extended, as previously stated. The links could break due to many reasons such as movement of the node, interference leads to packet losses etc. In such situations, the nodes which use a route with the specific broken link for their communication need to be informed about the inactive link. This is done using a control message called as the Route Error (RERR).

• Route Error (RERR) message: The RERR message is used to inform nodes about a link failure. Every node maintains a list of precursor nodes. This precursor list consists of all the nodes that are likely to use the node as their next hop in their route to another destination. Upon a link failure, the node sends a RERR message to all the nodes in its

precursor list. When a node receives the RERR message, then it invalidates the routing table entry which was using the node as a part of the route thereby setting distance to the destination theoretically as infinity. If the source node receives a RERR message and it requires a route to the destination then it can restart the route discovery process. When the RERR message is generated, then the sequence number of the destination is incremented so that all nodes know that it is the latest data about the link and the message should not be rejected.

• Sequence number: The sequence numbers are essential in maintaining a loop free network and avoiding the 'count to infinity' problem [34]. The forwarding nodes update their entry of sequence number only when sending a RREP message, and specifically in the case when

- The sequence number in routing table is invalid or
- The sequence number in the RREP message is higher then the already stored number or
- The sequence number is the same but the route was previously marked as inactive or
- The sequence number is the same but hop count is smaller

The nodes that send the RREQ message increment their sequence number before sending the control packet. The nodes that receive the RREQ message also increment their sequence number if the received RREQ message's sequence number is same as the one already stored in their entry.

Maintaining valid sequence number is essential for avoiding the looping problem in routing protocols. Consider the illustration as shown in the figure 4.6. There exists a route to

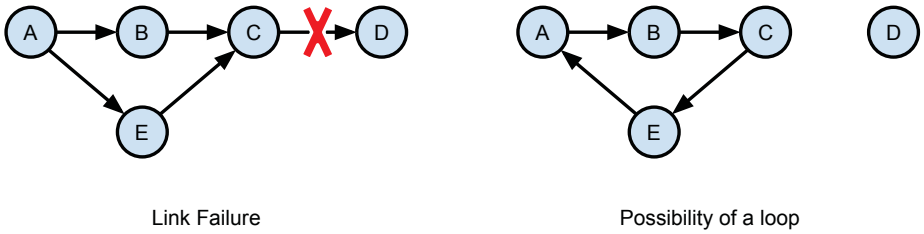

Figure 4.6: Illustration to shown how sequence numbers can be used to prevent looping problem

node D from node A via node B and node C. If the link between C and D breaks, node C will send a RERR message. Let us assume that the RERR message is lost and node A never received the RERR message. Therefore node A is unaware of the link failure between C and D. If node C begins a route discovery by sending a RREQ message and node A receives this RREQ message, then according to node A's routing table, the route to reach node D is through B and B thinks its through C. Therefore we would have a loop C-E-A-B-C as shown in figure 4.6. If sequence numbers were used, in which case C updates the sequence number for destination D and sends a RREQ message, but the entry to D in node A is stale in comparison to this sequence number, therefore node A will not respond to this sequence number thereby not replying with a RREP and thus the loop is prevented.

Summary of operation : The Ad-hoc On demand Distance Vector routing protocol is a flexible and robust routing protocol which has the ability to handle high traffic loads, large networks and relatively high mobility of the nodes in the network. Currently AODV does not include any security measures, it is under the assumption that all the nodes in the network can be trusted and there are no malicious nodes in the network. Also it is assumed that the higher layers (IPv6, transport or application) have certain security measures taken to prevent any

threat in the network. The design of this routing protocol aims to reduce the overhead of data traffic and eliminate redundant control traffic. The design also focuses on improving scalability and performance of the overall network.

4.3.4 AODV messages frame format

The Ad-hoc On demand Distance Vector routing protocol uses mainly 4 types of messages for route discover and route maintenance, namely; Route Reply (RREP), Route Request (RREQ), Route Error (RERR) and Route Reply Acknowledgment (RREPACK). The details of the frame formats of these messages which use the IPv6 addresses for identifying the nodes in the network is as described in the subsequent paragraphs.

∗ **RREQ frame format** : The Route Request frame format is as shown in the figure 4.7.

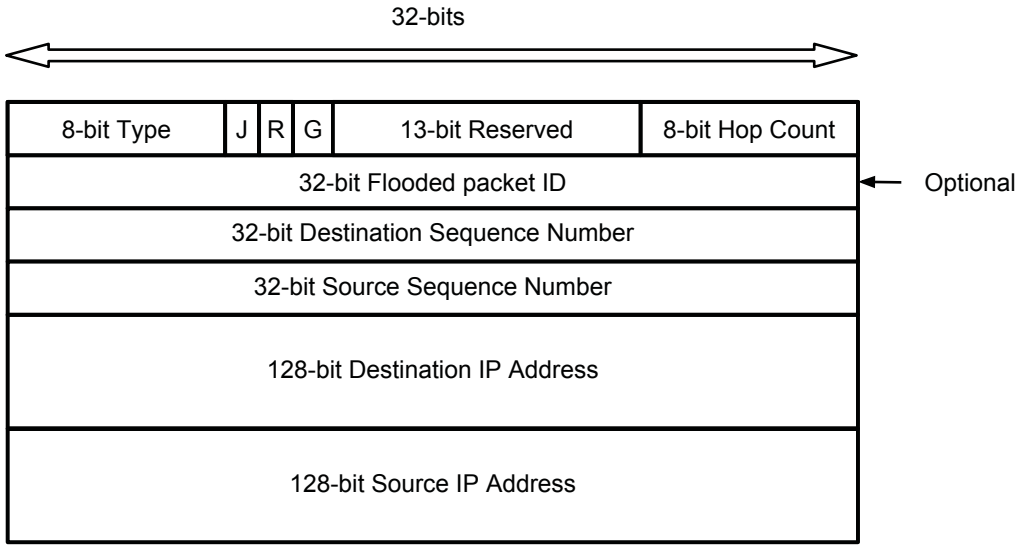

Figure 4.7: RREQ frame format in IPv6 version of AODV

- Type Id = 16: The frame consists of a 8-bit type id, which is used as an identifier to recognize the type of AODV message. On receiving an AODV message, the node checks the frame type, which will help in handling particular message.
- J: The join flag reserved for multicast addressing
- R: The repair flag reserved for multicast addressing
- G: The gratuitous reply flag, if this is set, then the gratuitous reply is requested by the RREQ message.
- Reserved: 13-bits are reserved for future use and are always set to 0 if unused.
- HopCount: An 8-bit HopCount indicates number of hops the message has taken to reach the destination at that point of time.
- Flooded packet ID: The 32-bit flooded packet ID is used when data flooding technique is used as described in section **??**.
- Destination sequence number: 32-bits
- Source sequence number: 32-bits
- Destination IP address: 128-bits

- Source IP address: 128-bits

∗ **RREP frame format** : The Route Reply frame format is as shown in the figure 4.8.

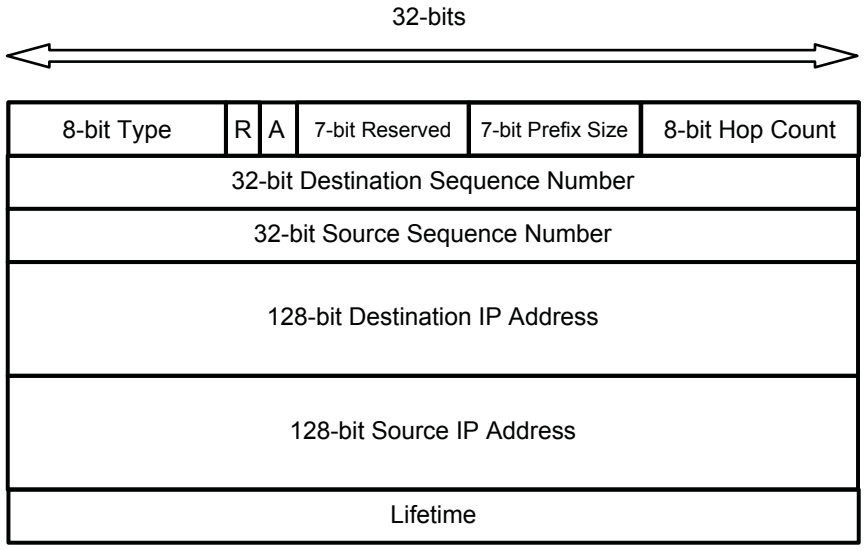

Figure 4.8: RREP frame format in IPv6 version of AODV

- Type Id = 17
- R: The repair flag reserved for multicast addressing
- A: The route reply acknowledgement flag. If this flag is set, then the sender is requesting for an acknowledgment on reception of the RREP
- Reserved: 7-bits are reserved for future use and are always set to 0 if unused.
- Prefix Size: 7-bits are reserved for prefixes which can be used to identify nodes using same routing prefixes, indicating that the next hop could be any node with the same prefix.
- HopCount: An 8-bit HopCount indicates number of hops the message has taken to reach the destination at that point of time.
- Destination sequence number: 32-bits
- Source sequence number: 32-bits
- Destination IP address: 128-bits
- Source IP address: 128-bits

∗ **RREPACK frame format** : The Route Reply Acknowledgment frame format is as shown in the figure 4.9.

- Type Id = 19
- Reserved: 8-bits are reserved for future use and are always set to 0 if unused.

∗ **RERR frame format** : The Route Error frame format is as shown in the figure 4.10.

- Type Id = 18
- N: The no delete flag is set to indicate that the link has been repaired and the route entry should not be deleted

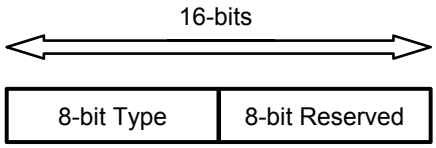

Figure 4.9: RREPACK frame format in IPv6 version of AODV

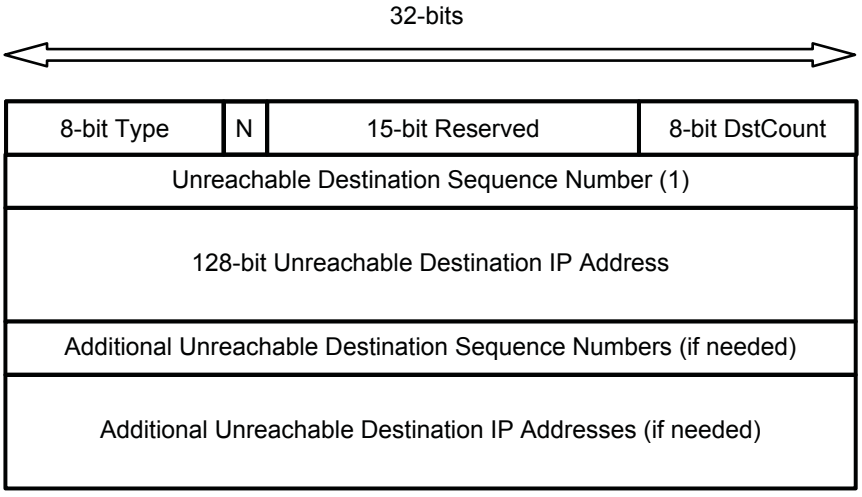

Figure 4.10: RERR frame format in IPv6 version of AODV

- Reserved: 15-bits are reserved for future use and are always set to 0 if unused.
- DstCount: An 8-bit DstCount indicates number of destinations that have been recognized as unreachable due to the link failure, this value must be atleast 1.
- Destination sequence number: 32-bits
- Destination IP address: 128-bits
- Additional unreachable destination sequence number: 32-bits only when needed else is zero.
- Additional unreachable destination IP address: 128-bits only when needed else is zero.

4.3.5 AODV using IPv6 miscellaneous information

The operation of AODV is same for both IPv4 and IPv6 versions, both versions use the same messages for route discovery and route maintenance. The notable difference being the size of the IP addresses and order of the frame parameters. The ICMP from IPv4 is replaced by the ICMPv6 process in IPv6. The AODV parameters and their default values remain the same for both IPv4 and IPv6. The small changes is that the hop limit field of the IPv6 header must be set to a value less than or equal to the NET_DIAMETER value of AODV. The NET_DIAMETER value specifies the maximum number of hops an AODV packet can take withing a network. The AODV provides a special extension of flooding the data to a specific destination which has not been used in the current design. The AODV does not take any security measures. If the application is prone to security attacks then the messages must be transmitted cryptographically across the network.

Chapter 5

ZigBee network layer simulation in NS-3

5.1 Introduction

In the field of communication and computer networking, the behavior of the network can be understood by physically creating the large network; which can turn out to be expensive based on the size and configuration of the network, also it is necessary to create a controlled environment consisting of different sources of interferences. The other option is to use program models, which replicate the behavior of the network by calculating the interaction between the network units and establish the network, using mathematical models or by observing the behavior from a production network. This can recreate the scenarios close to real time application, but will not be exactly the same, but helps in understanding the behavior of network to a large extent. This method of using mathematical formulas and calculating the behavior of the network is termed as *Network Simulation*. The network simulation also considers the environmental conditions of the physical network by adding certain attributes to reproduce the expected environmental conditions. A platform which is used to perform such network simulations are called as *Network Simulators*. The network simulators are designed with models of devices, applications, links, sources of interference, environmental conditions etc using which the performance of the network can be analyzed. A network simulator which is modeled using the accurate mathematical models, will behave as close to the real conditions as possible. The network simulators provide the flexibility for the user to customize their application and analyze the performance of the network at desired conditions. The term simulation is used to describe the process of reproducing a specific scenario in a network simulator. The commercial network simulators are driven by user friendly GUI, very few of them rely on the Command Line Interface (CLI). The simulators also provide visual aides and animations to project the close to real time scenario visually for the user. Generally, the network simulators create discrete event simulations, in which the processes/steps of simulations are stored as discrete events, which are executed one after the other, thereby triggering future events. The simulations are a complex set of processes which rely on a large number of parameters; network parameters which define the configuration of network and application parameters which define the application scenario. The impact of these parameters have to be carefully analyzed before reproducing a close to real life scenario and extracting reliable information out of the behavior of the network.

In the case of analysis of large ZigBee networks, using the hardware to create such networks proves to be expensive. Therefore, network simulators can be used to understand the large and dense ZigBee networks. In order to do this, a reliable, robust and flexible network simulator must be chosen. A large number of commercial network simulators are available at the disposal. For example, Opnet, NetSim, NS, OMNET++ [30] [40] etc. The Opnet and NetSim are proprietary

network simulators, where NetSim provides a reliable environment for simulating Wireless Sensor Network. Whereas the NS simulator and OMNET++ are open source software and both offer reliable simulations for the WSN. The NS simulator provides a set of larger complex simulation models in comparison to the OMNET++. The proprietary software is not preferred here for the academic research project due to cost constraints. Based on comparison between the NS and OMNET++ simulators, it is known that NS simulator provides a much robust environment and in-spite of the complex architecture the NS simulator is preferred here due to it reliability and flexibility. These facts make NS simulator the ideal choice to simulate a large ZigBee network. The latest version of the NS simulator is NS-3 which is an advanced network simulator. The subsequent sections help in understanding the network simulator, also provides information about the use of the simulator in simulating the behavior of large ZigBee networks. In the section 5.2 the basic architecture of NS-3 simulator is described, following which in section 5.3 the implementation of a model to simulate ZigBee network layer is explained. In section 5.4, the models which are used to recreate an environment of ZigBee networks are clearly explained. Thereby giving a clear understanding of the whole environment for the simulation and analysis of large ZigBee networks.

5.2 Architecture of NS-3

The NS-3 is a discrete event simulator used primarily for research and academic purpose. The NS-3 aims to create an open simulation platform for the networking research community. It focuses on creating the platform to simulate modern networking systems. Being an open source software, it encourages contribution to the community, peer contributions, peer reviews and discussions. The NS-3 is that network simulator in which the simulation core and models are implemented in C++. NS-3 is built as a library which may be statically or dynamically linked to a C++ main program that defines the simulation topology and starts the simulator. NS-3 also exports nearly all of its API to Python, allowing Python programs to import an "ns3" module in much the same way as the ns-3 library [42] is linked by executables in C++.

The NS-3 network simulator is a complex yet flexible and reliable network simulation platform. It is composed of a large number of abstract modules, which can be bound together to create a simulation environment and to observe the behavior of the network of sensor nodes. In this project we intend to use the IPv6 routing protocol to closely associate the applications with the IoT. The figure 5.1 shows some of the basic blocks required to create a network simulation of sensor nodes which use Ipv6RoutingProtocol. The environment contains the following abstract components [42] [43]

- **Node Container:** The number of nodes required for a simulation are created and placed into a logical container called as the node container. The node container technically holds pointers to the nodes, and any operation to a group of nodes can be performed by placing them under the same node container. The nodes consists of NetDevices, Interfaces and Sockets for communication.

- **NetDevice Container:** The NetDevice is logical equivalent of a real life network interface card. In NS-3 the netdevice is associated with the MAC and PHY layers. By installing the specific MAC and PHY protocols, the devices are assigned MAC addresses. Required netdevices can be placed under the common container called as the NetDevice container. The NetDevice container holds pointers to all the net devices associated with it.

- **Interface Containers:** The interfaces are of two types, IPv4 and IPv6. Each of these interfaces indicate the version of internet protocol which shall be used by the specific NetDevice. Therefore, for every NetDevice from the NetDevice container, an interface is added. Then based on the type of interface, corresponding addresses are added, i.e. IPv4 or IPv6 address. Then the interface is moved to a container of similar types i.e. the NetDevices using IPv4 interfaces can be moved into a single interface container and same applies to

IPv6 interfaces. A unique pair of interface pointer and the specific interface index is created which helps in identification of the interface. Interface index refers to the interface number on the NetDevice, as a NetDevice can have more than one interface associated with it. When the decision has to be made to choose a specific interface to communicate, then the Networking stack MUX (as seen in the figure 5.1) makes the decision based on the unique pair of interface pointer and interface index. The interface container consists of list of pointers to specific interfaces of a NetDevice associated with a particular node.

- **Helper functions:** The helper functions, as the name indicates are indeed useful in simplifying a lot of complex steps in creating a communication stack. The helper functions, assist in associating specific net device pointers with node pointers, assign MAC addresses, creating interfaces to specific NetDevice and assigning the IP addresses correspondingly, creating the unique pair of interface pointer and interface index etc. Most of the functionality is done automatically, but manual configuration is also at the disposal of the user, such as assigning manual MAC and IPv6 addresses.

These basic blocks are used to create a simulation environment. To create a ZigBee internet network layer simulation, it is essential to understand the structure of the NS-3 IP layer protocols and introduce the necessary AODV routing protocol in the right hierarchical position.

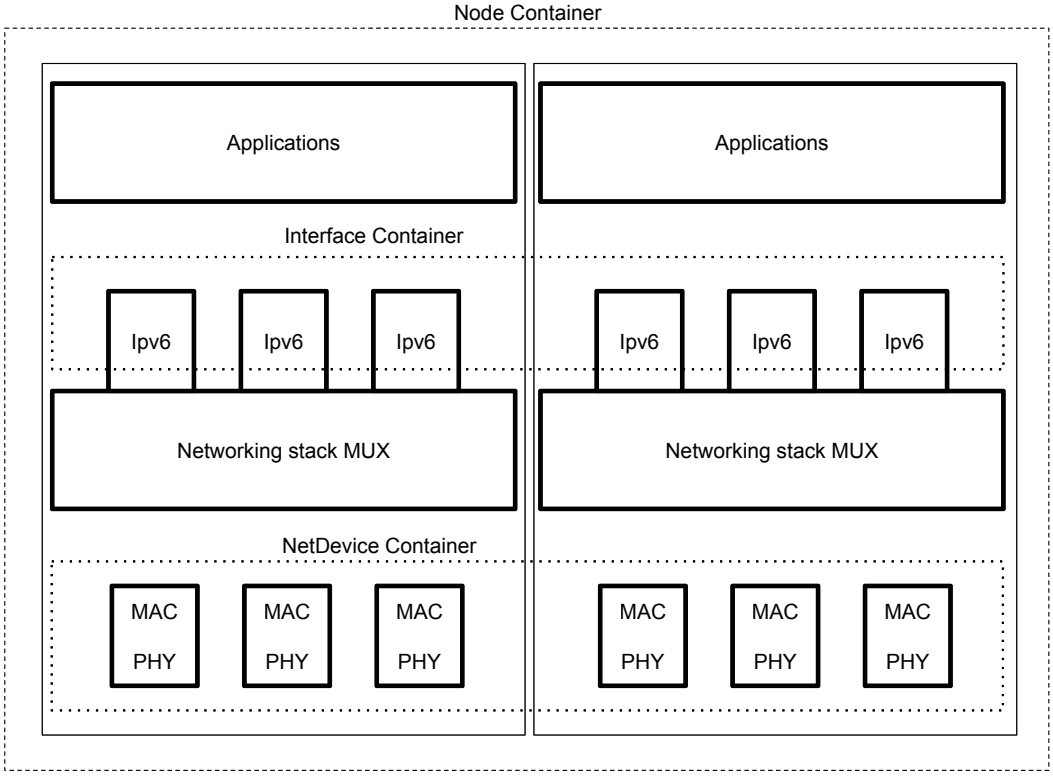

Figure 5.1: NS-3 simulation framework

5.3 ZigBee network layer

The platform to simulate a ZigBee network requires that the ZigBee network layer be simulated with appropriate modules. The figure 4.2 shows that the ZigBee network layer can be simulated

using the combination of IPv6 AODV and 6LowPAN sublayers and this is done using the NS-3 simulator. Therefore the stack as shown in figure 4.2, consists of an application, a transport layer (UDP), the network layer consisting of; IPv6, AODV and adaptation layer of 6LowPAN, the 802.15.4 MAC and PHY layers. This whole stack (as shown in figure 5.2) is used to simulate a large ZigBee network. As seen in the figure 5.2, the names shown in the stack correspond to NS-3 modules [44]. The research goal focuses on implementation of the AODV module which uses the IPv6 routing protocol. The figure 5.2 shows that the AODV is associated with the

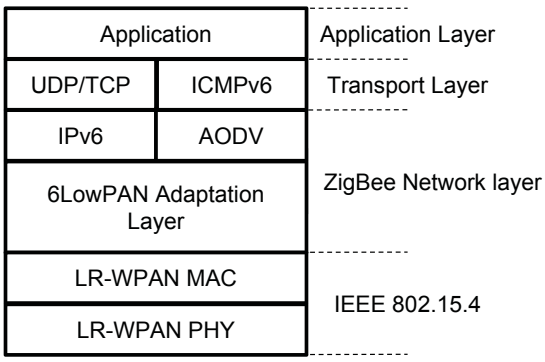

Figure 5.2: ZigBee network layer simulation in NS-3

IPv6 routing protocol. The IPv6 layer in the stack is interfaced with the upper and lower layers through certain APIs as shown in the figure 5.3. The application is defined in the user space. The kernel space is defined by the NS-3 modules. The Ipv6RoutingProtocol module controls the functions of the whole routing protocol, acting as interface between upper and lower layers. It makes direct contact with the transport layer, for example UDP as shown in the figure 5.3, through APIs. Specific functions such as the RouteOutput define the communication between two layers. The transport layer is directly bound to sockets which are defined in the application for communication. When the application has a packet to be routed to a destination node, then it requests the Ipv6RoutingProtocol to provide a route by calling the RouteOutput function. The Ipv6RoutingProtocol, using the AODV establishes a route to the desired destination and returns the route to the route. Using the route, via a bound socket the information is transferred to lower layers, which is explained in detail in the subsequent paragraphs. The Ipv6RoutingProtocol interfaces with the lower layers using the Ipv6L3Protocol, which is defined as a layer 3 protocol in NS-3. The layer 3 protocol is responsible for communicating with the lower layers; NetDevices as shown in the figure 5.3. The NetDevices are explained in detail in subsequent paragraphs, at this moment it is sufficient to know that the NetDevice class is responsible for controlling the MAC and PHY layers. Also as seen from the figure 5.3 the raw sockets in NS-3 bypass the normal TCP/UDP processing and connect the application with the IPv6 protocol directly. This is not used in the implementation of AODV. The routing of a packet which has just arrived at the node, in NS-3, is done by certain callback functions, namely:

- **Local Callback :** When the packet has to be routed within the node for a further processing, for example when the route is not available yet and the packet has to be queued till a route is available.
- **Multicast Forward Callback :** When the packet has to be multicasted to a list of nodes.
- **Unicast Forwards Callback :** When the packet has to be forwarded to a single node on the next hop.
- **Error Callback:** When there is an error in the packet or route and the packet has to be processed based on the type of error, the error callbacks identify the type of error and process

accordingly.

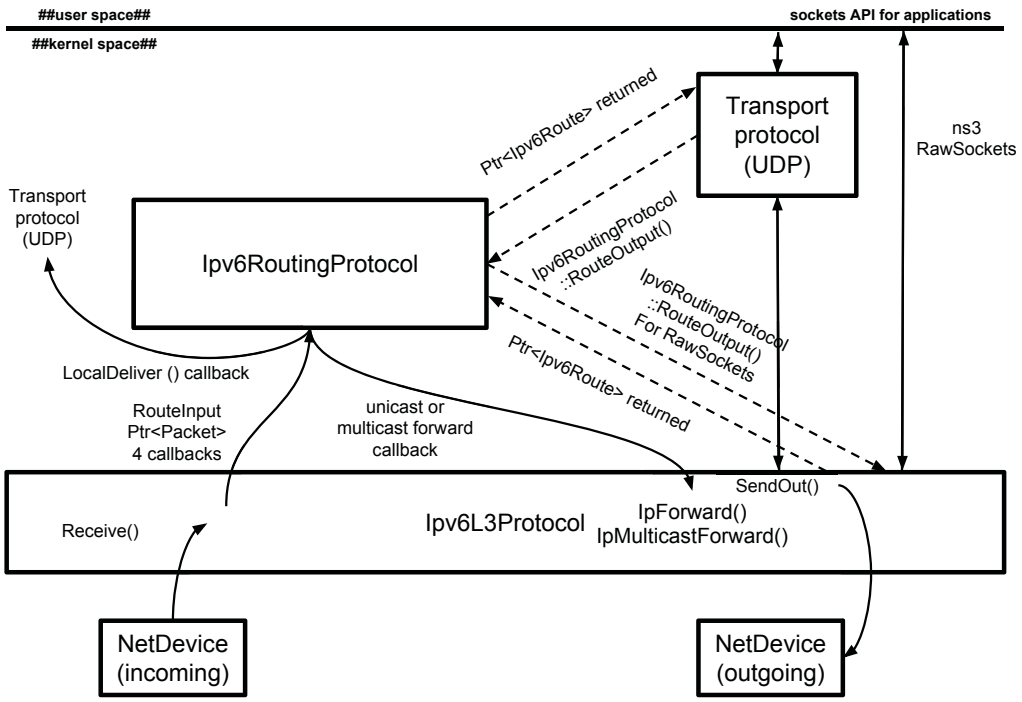

Figure 5.3: The APIs for communication between the IPv6 routing protocol with other upper and lower layers of the stack

The Ipv6RoutingProtocol in NS-3 has sub-functions which follow a hierarchy as shown in the figure 5.4. The Ipv6RoutingProtocol consists of three different models for routing, namely:

- **Static Routing Protocol:** The static routing protocol is used in cases where the routes are predetermined and the routing protocol does not determine the paths for routing a packet. This class is designed to be inserted in a list and must be used from the Ipv6ListRoutingProtocol in order to establish communication in the network.

- **Global Routing Protocol:** NS-3 global routing performs pre-simulation static route computation on a layer-3 IPv6 topology. The user API from the script level is fairly minimal; once a topology has been constructed and addresses assigned, the user may call ns3::GlobalRouteManager::PopulateRoutingTables() and the simulator will initialize the routing database and set up static unicast forwarding tables for each node. The model assumes that all nodes on an ns-3 channel are reachable to one another, regardless of whether the nodes can use the channel successfully (in the case of wireless). Therefore, this model should typically be used only on wired topologies. Layer-2 bridge devices are supported. API does not yet exist to control the subset of a topology to which this global static routing is applied. If the topology changes during the simulation, by default, routing will not adjust.

- **List Routing Protocol:** The Ipv6ListRoutingProtocol is used when a device must choose from a list of Ipv6RoutingProtocols based on priority of every routing protocol. For example, the list might consist of routing protocols such as the AODV, RIPng etc and the device decides the routing protocol to be used based on certain predetermined priorities for each of the routing protocols in the list.

Furthermore, the Ipv6ListRoutingProtocol consists of an implementation class where the functions are defined in order to act as an interface between the upper and lower layers of the protocol stack. The implementation also takes care of enabling the ICMPv6 messages as and when necessary in order to support the Neighbor Discovery Protocol in the IPv6. The AODV routing protocol which uses IPv6 address is designed and during the time of installation of a routing protocol on the node, it is appended in the Ipv6ListRoutingProtocol with a priority set to the highest priority (0: the value for highest priority in NS-3). Therefore when the IPv6 stack is installed on the node (process explained in detail in subsequent paragraphs), then the Ipv6ListRoutingProtocol refers to the AODV routing protocol installed in the list to determine routes in the network. As seen in the figure 5.4 the AODV routing protocol is placed under the Ipv6ListRoutingProtocol. When

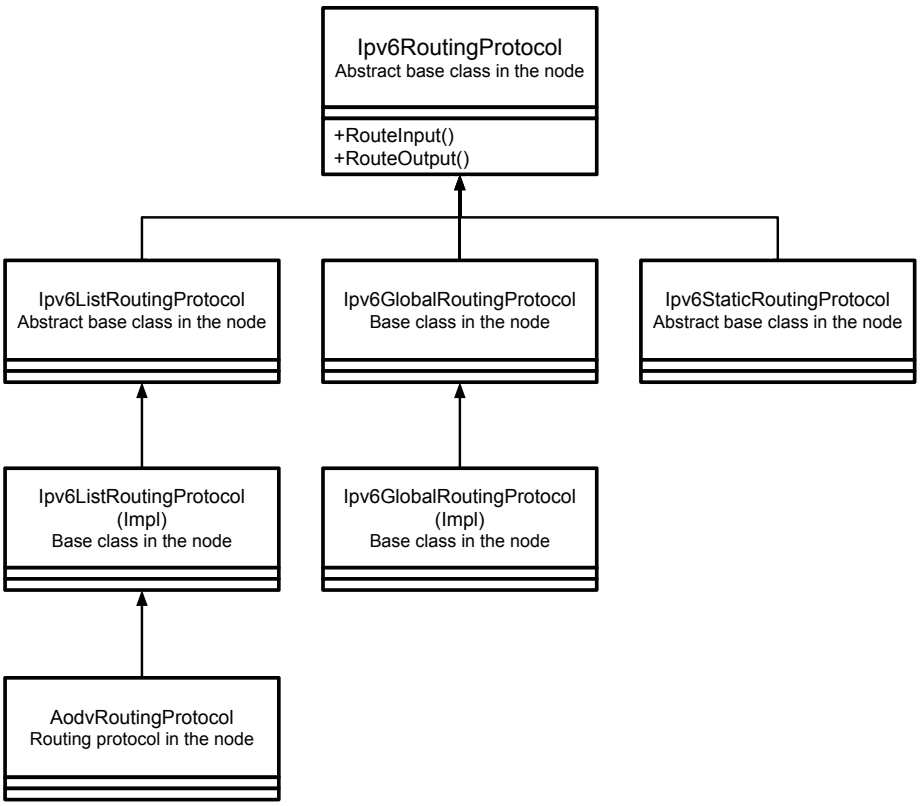

Figure 5.4: The Ipv6RoutingProtocol hierarchy in NS-3 API system

designing the application, the AODV routing protocol is attached in a list of Ipv6RoutingProtocols. The API in NS-3 also facilitates to choose between the IPv4 and IPv6 internet stacks. The figure 5.5 shows the API to switch between the two versions of AODV; the IPv4 and IPv6. The helper functions, InternetStackHelper, provides an option to enable or disable the IPv4 stack using the SetIpv4StackInstall function. If the IPv4 stack is enabled, then the application can be designed to use the IPv4 version of AODV. If the IPv4 stack is disabled, then NS-3 facilitates the use of IPv6 version of the AODV as seen from the figure 5.5. The AODV routing protocol is designed using the existing template of the IPv4 version of the AODV in NS-3. Some of the key implementations to accommodate IPv6 addresses and 802.15.4 standards in the routing protocol are:

- Modify the routing protocol to use IPv6 addresses instead of IPv4
- Replace broadcast addressing mechanism of IPv4 with multicast group addressing in IPv6, such as hello messages, route requests etc.

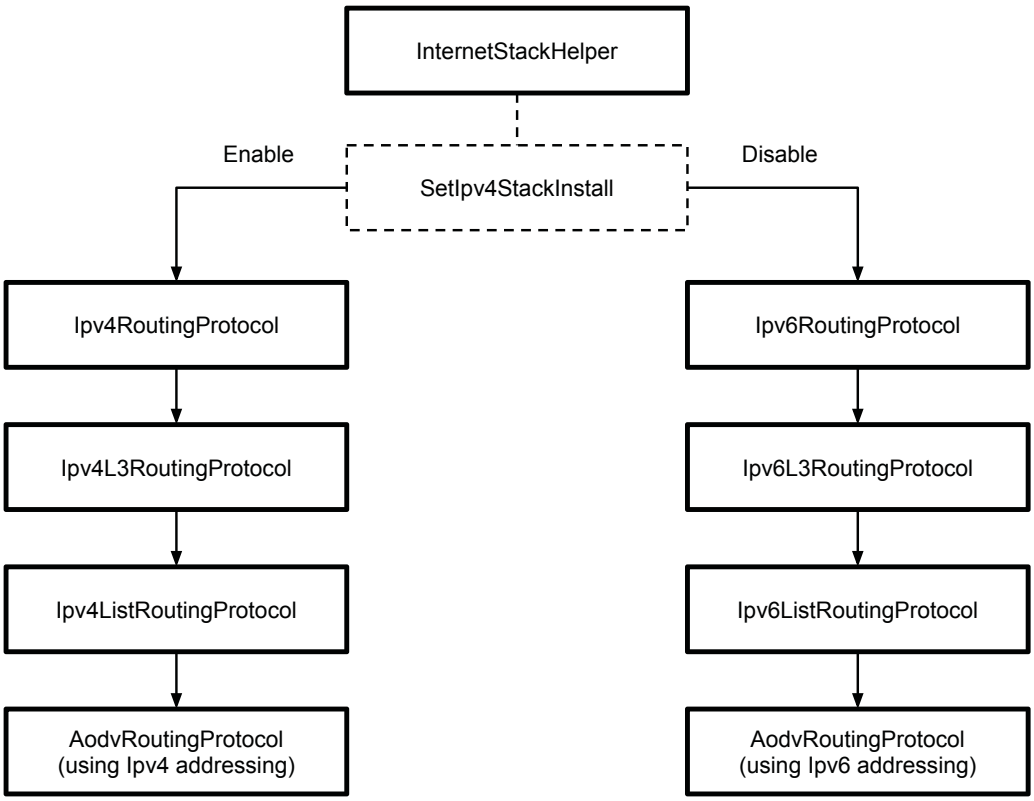

Figure 5.5: The API to switch between the Ipv4 and Ipv6 versions of AODV routing protocol in NS-3

- Obtain link layer feedback messages from the Lr-WPAN (802.15.4) MAC layer to detect link failures
- Modify the routing protocol to detect ICMPv6 messages
- Modify the routing table information to use IPv6 addresses
- Modify the routing protocol to allow the nodes to recognize more than one address assigned to them i.e link local, global scope addresses. In case of IPv4, the nodes had only one address.
- Modify the routing protocol to be able to recognize messages based on prefixes. For example FF02::2 is an all routers multicast message with a prefix of FF02, thereby indicating that it is a multicast message. Such a feature does not exist in IPv4 version of the AODV routing protocol.
- Modify the existing test cases to perform; regression, unit and system level testing.
- Design examples to understand, verify and demonstrate the functionality of AODV routing protocol using IPv6 addressing.
- Design examples to understand, verify and demonstrate the functionality of AODV routing protocol when implemented above the 802.15.4 MAC and PHY.

The implementation of AODV using the IPv6 addressing and related protocols, the testing and demonstrated examples ensure the correctness of the implementation to a large extent. This

provides a platform to simulate large ZigBee networks using the NS-3 simulator. The detailed understanding of the working of the NS-3 simulator and the knowledge of routing protocol helps in designing application scenarios to demonstrate, observe and evaluate ZigBee networks. The routing protocol is designed to also be able to adapt to WiFi networks.

5.4 Models of NS-3

In a simulation environment, it is important to recreate the real life scenarios, run the simulations in possibly different environmental conditions, so as to extract information at greater depths and infer reliable information from the behavior. To recreate the environmental conditions of real life, the NS-3 simulator provides a large number of mathematical models [50] which reproduce some expected behavior, for instance, if the user has to place a node in a building of concrete walls, then the NS-3 provides a mathematical model called as the 'buildings' model in which the user can decide the type of wall and use this in the environment of simulation. The following are some of the mathematical models of NS-3 which will be used in the experimental section and are described below:

- **Mobility Model:** The mobility model helps in assigning positions to the nodes in an experiment. They also provide the flexibility change the position of the node (make the node mobile) at different instances of time. The mobility model used in the experiments is the *"ConstantPositionMobilityModel"* of the NS-3. This model indicates that the positions of the nodes are fixed and the nodes are immobile physically. The *"ConstantPositionMobilityModel"* is used to create a grid structure. The *"ConstantPositionMobilityModel"* is a simple model which will provide the basic understanding of the large ZigBee network behavior which is essential before moving to a set of mobile nodes. Therefore for the sake of clear and basic understanding of the network behavior the *"ConstantPositionMobilityModel"* has been opted.

- **Propagation Delay Model:** The propagation delay models run in coherence with the mobility model. The propagation delay model help in including the delay in communication when there is mobility in the network and relative motions have to be considered for the delays. Since the experiments which shall be conducted are on fixed position nodes, thereby the *"ConstantSpeedPropagationDelayModel"* is used.

- **Propagation Loss Model:** The propagation loss models account for the effects of sources of certain interference in the environment, such as scattering, reflection, diffraction etc. This is important from the aspect of every variable environmental condition in the network including the behavior of the antennas, transmission range etc. In the experiments we use the *"FriisPropagationLossModel"* in collaboration with the *"NakagamiPropagationLossModel"*. These two models help in accounting for sufficient effects of environments to obtain reliable data to infer strong opinions on the behavior of the network. The network can be accounted for more number of sources of interference, but the analysis is in the initial stages to understand a trend of behavior of the network, thereby a choice of sufficiently reliable models are chosen, rather than including complex models.

- **Seeds and Runs:** The behavior of real networks are not easily predictable, they are random in fashion due to ever changing conditions in the network, both within the devices and external to the devices. Thus, when creating mathematical/stochastic models, the functions are designed to use a set of random numbers to add the unpredictability factor. If the experiments are run over a set of large number of such random numbers and result is averaged, then this provides concrete information about the behavior of the network. In NS-3 the randomization factor is provided by the concepts of seeds and runs. A seed is a set of random numbers whose value is equally distributed in the entire set, a run is a subdivision of seed in which every run consists of distinct and non overlapping values. The seeds can be used by time based or event based random number utilization functions. To obtain reliable results,

one can use different sets of seed; but this consists of a possibility of overlapping values, or use a single seed with different sets of runs, thereby ensuring that no overlapping set of values are used by the random numbers. In the experiments conducted (described in subsequent chapters) the seed is fixed, but different runs are used to ensure that no two experiments conducted use the same set of random numbers which might produce same result and that is undesirable.

These models which shall be used in the experiments are with the intention of obtaining reliable information to understand the behavior of large ZigBee networks. The models take care of position of the nodes, mobility, the propagation and delay losses due to the mobility and environment as well as the factor of randomization, thereby covering different aspects of an accurate simulation.

5.5 Summary

A network simulator helps in understanding behavior of computer networks by using mathematical models to reproduce the behavior of real networks. This helps in reducing the expenses largely and is vital for academic and research purposes. Simulations can be helpful in predicting the behavior of a specific set of devices in a specific environmental condition, thereby assisting in analyzing the reliability of a product before it can be actually manufactured. To ensure the reliability prediction is accurate, one must usee an efficiently designed network simualator. This project is an academic plus research project, thereby an open source network simulator; NS-3, is chosen over the proprietary network simulators available in the market. The NS-3 simulator is a complex yet reliable network simulator which requires detailed understanding of its framework (as described in section 5.2) before being able to use it at ease. On understanding the architecture, the ZigBee network layer simulation platform is created (see section 5.3). The models which ensure that the experiments are conducted to obtain concrete data to understand behavior of network is described in section 5.4. This ensures that sufficient information is available before conducting experiments, as described in the next chapter.

Chapter 6

Experiments

Revisiting the chapters described so far, chapter 1 gives a basic introduction of the thesis and states the research goals of the master thesis. The chapter 2 has provided information about the ZigBee standard being the domain of research project which is extended in chapter 3 to the internet protocol and detail description of the IPv6 protocol. The chapter 4 discusses the routing protocol AODV in detail. To achieve one of the research goals; to create platform to simulate large ZigBee networks, implementing the AODV routing protocol which uses IPv6 addressing is essential. The details of this implementation are described in the chapter 4 and the chapter 5 gives an overview of the environment of simulations; NS-3 simulator. All the information described in these chapters provide the base for focusing on the second research goal; to understand the impact of transmission power on performance of network in terms of latency. This chapter describes the experiments performed to achieve the research goal. The section 6.1 describes the different network parameters that have to be analyzed before setting up an application scenario which is done in section 6.1.1. In section 6.2, a hypothesis is stated based on the theoretical understanding and the observations made in experiments. Section 6.3.1 describes the experimental setup to evaluate the hypothesis and results of these experiments are evaluated in section 6.3.3.

6.1 The network parameters

6.1.1 Analyzing the impact of network parameters

The implementation of AODV using the IPv6 addresses has been described in the previous chapters. The chapter on the NS-3 simulator provides an overview of the simulator architecture and the environment for simulation of ZigBee network layer. A simulation model consisting of a routing protocol such as AODV operating using IPv6 protocol provides a platform to the research community to be able to simulate the behavior of a large ZigBee network in various application scenarios associated with the Internet of Things; methodology and reasons are described in subsequent paragraphs. The applications are highly distinct in nature, such as home automation system, lighting systems, smart energy management and many more. Each of the applications function under different constraints and scenarios, for example a lighting system of an office is subjected to regular interference by many devices, the building itself and the human interference, whereas a system of health care monitoring can be in an indoor or outdoor environment. Thus, the applications operate under different constraints designed by some application parameters. The interaction between the devices in the application is handled by the routing protocols by establishing communication routes in the network through message exchanges. One such routing protocol described in previous chapter is the AODV. The AODV routing protocol, provides flexibility to adapt to various application scenarios. The application and routing protocol parameters have to be tuned to one another to obtain optimal behavior of a large network. In the subsequent sections, an application scenario is presented that is used to understand the behavior of these parameters, the latency of message delivery is used as a metric to analyze the performance.

The latency is measured at the application level i.e difference between the time the application message was created at the source node and the time at which the application layer at receiver node senses the message. The figure 6.1 shows an illustration of the setup; the reasons for the choice of a specific setup is explained in detail in further paragraphs.

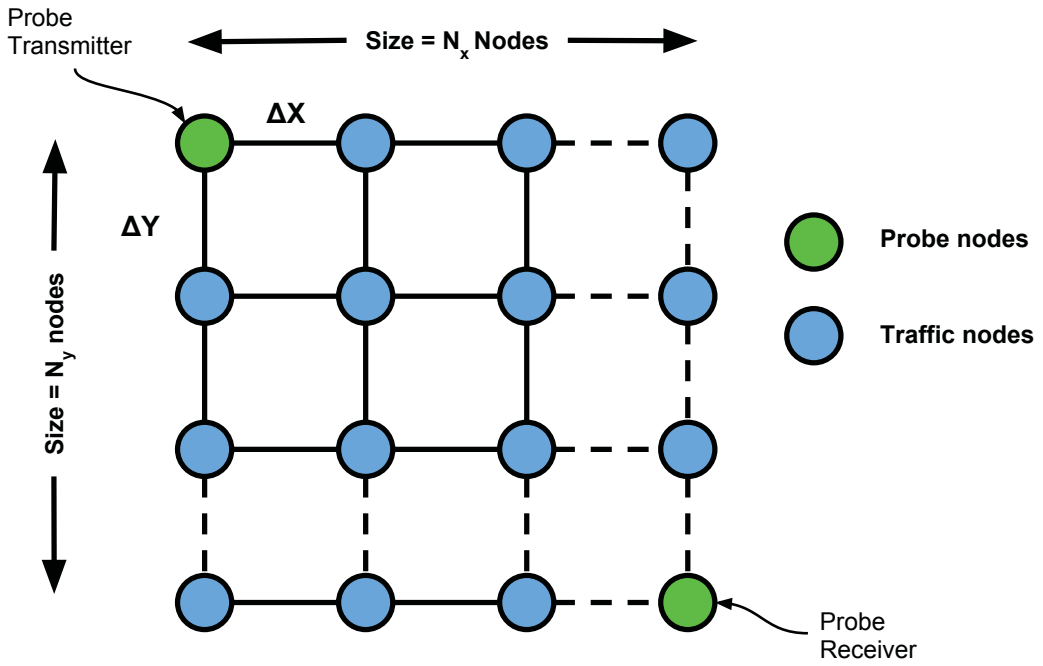

Figure 6.1: An illustration of the flexible setup designed to analyze impact of network parameters

The need to understand impact of network parameters on behavior of network:

The AODV routing protocol offers a fair degree of flexibility to customize the routing protocol, based on the application requirement. The experimental analysis conducted in subsequent paragraphs, indicates that a large number of factors play a crucial role in the behavior of the network. Each of these parameters when modified have a significant impact on the outcome of the experiments. Every experiment conducted takes an average of 19 minutes of real simulation time (the experiments are conducted for a duration of 100 seconds, to balance real simulation time and obtain reliable data), which can vary based on the size of network. Though the experiments are not explicitly extensive to infer concrete data, but are sufficient to understand the behavior of the network based on both theoretical knowledge and experimental results. These experiments are essential before deciding on an application scenario to understand the impact of any one of those parameters on the performance of the network in terms of latency. It is smart engineering to start understanding a large network by dividing it into small sections, and individually evaluating them. In the end, this gives quite a good picture about the network on the whole. Considering the available time for the master thesis, it is necessary to plan the approach after the implementation of the IPv6 version of AODV. Therefore the observations made on the impact of network parameters plays a crucial role in the analysis of the behavior of the network.

The setup is a large grid, to simplify the network and be able to explicitly understand the network in a simple framework, with nodes equally distributed across rows and columns as shown in the figure 6.1. The distance between the nodes, X and Y, can be varied to set the density of the network. To analyze the impact of different parameters, a probe pair (a node which transmits application

level message and a node which is intended receiver of this message) is setup which acts as an indicator of the performance of the network in presence of large number of nodes. The rest of the nodes are considered as traffic nodes, which do not send any messages, except periodic messages to keep the links alive. In a large number of experiments the network parameters are varied in turns (described in subsequent paragraph), keeping rest of the parameters constant and observations are made in the behavior of network. Some of the parameters which are constant at specific values are fixed to values specified in standards: total size of application packet is 33 bytes based on inference from ZigBee standards, generally maximum size of the packet is 33 bytes. For intended application scenario, an home automation system: The transmission power is varied between -32 dBm and 0 dBm, as this is the minimum and maximum transmission power of many ZigBee devices. Hello interval is 10 seconds, since the devices in the intended application scenario, are less active in most cases and it is not necessary to keep links alive regularly, also the data packets help in keeping the necessary links active, which is one of the focus of the experiments. Active route timeout (life time of routes, see chapter on AODV for details) is set at 3 seconds, since the environment in the real application is expected to be dynamic with plenty of sources of interference, therefore stale routes (routes unused for large durations of time) are possible, thereby requiring shorter lifetime of routes. The Delete Period is set to a value of 40 seconds based on the formula defined by standards (2*HelloInterval*Number of allowed hello messages loss(2)) and the MyRouteTimeout period is set to 5.6 seconds based on formula defined in standards (2*PathDiscoveryTime(2.8)).

* **Network size variation** : To understand the impact of change in size of the network, the size of the network in terms of number of nodes is varied, as 4X4 5X5 8X8 10X10 and 15X15 grid structure. The probe transmitter is fixed as the first node and probe receiver is its diagonally furthest node as shown in figure 6.1. The reason for fixing these positions of the probe pair transmitter and receiver is to have maximum physical distance between these nodes. The nodes can be placed anywhere in the network, where the number of source of interference may be higher, but the focus of experiment is to maximize the number of hops required for the message from source node to reach the destination node.

  The parameters kept constant are:

  - Distances X and Y: 5 meters
  - Transmission power: -32 dBm
  - Packet interval: 0.5 seconds
  - Total simulation time: 100 seconds
  - Application start time: 3.1 seconds
  - Traffic pairs: None
  - Packet size: 33 bytes
  - Total packets sent: 193

  Observations and conclusions: With the application scenario as described, following are some of the key observations made and conclusions drawn.

  - It is seen that the size of network and latency are directly proportional.
  - Also the latency significantly increases at larger networks i.e. beyond 36 nodes. This can be explained by the fact that as network size increases, the message from transmitter has to undergo more number of hops to reach the destination node.

* **Inter-node distance variation** : To understand the impact of change in distances between nodes, the inter-node distance is varied to 2, 3, 5 and 10 meters at a transmission power of -25 dBm which is the transmission power at which the nodes at 10 meter distance are comfortably within the range of immediate adjacent neighbors.

The parameters kept constant are:

- Transmission power: −25 dBm

Observations and conclusions:

- At the specified constant transmission power, as the distance between nodes increases, latency increases due to the fact that more number of hops are required to reach the destination.
- At distances 2 and 3 meters, the latency is significantly low as the probe pair is in one-hop vicinity. On increasing the distance between 5 and 10 meters, the latency increases significantly, due to more number of hops to reach the destination and each hop adds a certain amount of delay based on its transmission process, it might have to do more number of retransmissions if the connectivity to its next hop neighbor is of poor quality.

∗ **Packet interval variation** : To understand the impact of changing the application packet transmission interval on the network performance, the packet interval of the probe application packets are increased from a very high data rate of 0.1 and slowly decreased to lower data rates of 0.5, 2.5 and 5 seconds.

The parameters kept constant are:

- Transmission power: −32 dBm

Observations and conclusions:

- At very high data rates, the latency is initially high, but after certain duration of time reduces. This is for the reason that the initial packets have no stable route available yet because the network hasn't discovered shortest path, but eventually the latency variations are comparatively less.
- At data rates beyond 2.5 seconds, the latency is very high as the route lifetime is set to 3 seconds therefore extra latency is due to the new route discovery process.

∗ **Application start time variation** : To understand the impact of the start time of application packets transmission the application start time is varied. The application start time determines the time provided for the network to settle down to discover atleast two one-hop neighbors. The Hello messages are sent at random non overlapping intervals of time from the start of simulation and the hello traffic burst lasts for 0.328 seconds (based on experiments conducted for same scenario where the nodes just send 1 HelloMessage it is observed that the final HelloMessage was sent at 0.328 seconds) in the whole network of below stated configuration. The application start time is increased in steps: 0.1, 0.25, 0.5, 1, 3, 5 seconds.

Observations and conclusions:

- If the application packets are sent before the burst of HelloMessages run out i.e before 0.328 seconds, then the latency increases significantly because the nodes have not discovered any neighbors, thus the packets are queued, thereby increasing the latency.
- If messages are sent after 0.328 seconds, the latency reduces gradually with increase in application start time. Beyond the application start time of 0.5 second, it has little impact on the latency of the network.

Note: The Hello interval has a strong correlation with the application start time. If the Hello interval or its multiples coincide with the application start time, then there is an increase in the latency for the initial set of packets due to large number of CSMA back offs.

* **Packet size variation** : The application packet size has a very important role to play in the performance of the ZigBee network therefore the packet sizes are varied to understand their impact on the performance of the network. The ZigBee uses 802.15.4 standards for the MAC layer, in this case the 802.15.4 defines the maximum payload of the packet as 127 bytes. The packets which are beyond 127 bytes must be fragmented in order to fit into the payload of 802.15.4 MAC frames. The size of application packet is varied as 10, 33, 104, 256 and a maximum of 1024 bytes.

  Observations and conclusions:

  - Any packet size below the 104 bytes are not subjected to fragmentation, therefore having little impact on the overall latency.
  - packets of size 104 bytes and beyond have to be fragmented at the MAC layer as the maximum capacity of 802.15.4 MAC is defined as 127 bytes which includes the headers, footers and payload from upper layers. Beyond 127 bytes, the packets are fragmented and transmitted, thereby significantly decreasing the performance of network due to possibility of loss of fragments leading to retransmissions of fragments. Therefore latency significantly increases with increase in packet size beyond 104 bytes. The more the number of fragments of the packets that the MAC layer has to prepare, the larger the latency.

* **Hello Interval variation** : The Hello interval is an AODV parameter which is used to keep links alive in a network and sent at regular intervals of time. If a large number of hello messages are sent, then the possibility of finding more number of one hop neighbors increases, this is due to fact that some of the hello messages may be dropped when the limit of number of retransmissions is exceeded. In this case a node might be in the vicinity of one-hop neighborhood but fails to receive any message from its neighbors. Therefore, if more number of hello messages are sent, then the probability of getting the hello message delivered to all the nodes in the one-hop neighborhood increases. The Hello interval is decided generally based on the activity of the network, in a highly active network (in terms of data packets exchanged) it is preferred to have larger periods of Hello interval so that the rest of the network does not interfere with the active routes. The required routes are kept active by high data traffic. In the case of networks with low activity, based on the requirement of reliability of communication, Hello interval can be decided. If the network has low activity but requires high reliability of communication, then shorter intervals of Hello messages are recommended. The Hello intervals here are set to values 1, 2, 5, 10 and 20 seconds.

  The parameters kept constant are:

  - Size of network: 10X10
  - Transmission power: -32 dBm
  - Distances X and Y: 5 meters
  - Total simulation time: 100 seconds
  - Packet interval: 0.5 seconds
  - Traffic pairs: Nil
  - Application start time: 3.1 seconds
  - Total packets sent: 193
  - Packet size: 33 bytes
  - Active route timeout: 3 seconds
  - Delete period: 40 seconds
  - My route timeout: 5.6 seconds

  Observations and conclusions:

- At very low Hello interval, with the data packet interval also being low, the latency increases due to large network traffic or stale routes (unused routes).
- As the Hello interval increases, the traffic in network reduces and thereby latency reduces.

* **Active route timeout variation** : The Active route timeout is the lifetime of a route. The lifetime of a route is affected by the dynamicity of the application environment. In a highly dynamic environment with large number of sources for interference the routes must be revalidated at regular intervals of time, than in less dynamic environment. The active route time out period is varied in steps as 3, 5, 10, 20 and 100 seconds.

  Observations and conclusions:

  - If the lifetime is short, then new routes are discovered more often if there was no data communication. Therefore as the number of Hello messages increase, more number of neighbors are discovered and the latency might reduce due to shorter hops, but may also increase if the new route's next hop has poor connectivity.
  - If the lifetime is large, then even if new routes with same number of hops but probably better connectivity are available, the nodes don't opt for this path because the lifetime of existing route has not expired. Thus the node uses same route and this could be a good or poor link quality route, therefore the latency variations are fairly unpredictable.

* **Traffic pairs variation** : Additional traffic pairs are created which send application packets very similar to probe pair in all parameters like packet size, interval, start time. These increase the amount of CSMA back offs. The figure 6.2 shows the setup for understanding the position of these traffic pairs. The traffic pairs consist of 1 long link and 4 short links and all possibly in the path of communication of the probe pair. The parameters kept constant are:
  - Size of network: 10X10
  - Transmission power: -32 dBm
  - Distances X and Y: 5 meters
  - Total simulation time: 100 seconds
  - Packet interval: 0.5 seconds
  - Traffic pairs: 5
  - Application start time: 3.1 seconds
  - Total packets sent: 193
  - Packet size: 33 bytes
  - Hello Interval: 10 seconds
  - Delete period: 40 seconds
  - My route timeout: 5.6 seconds

  Observations and conclusions:

  - Based on the position of the traffic pairs, as shown in the figure 6.2, it can be observed that the traffic nodes are geographically co-located in the vicinity of the probe pair transmitter and receiver. Therefore any transmission by the traffic pair, has a direct impact on the performance of network in terms of latency of message deliver between probe pair. A transmission of one of the traffic pairs adds to the CSMA back-off time of rest of the nodes in the network. Thereby increasing the latency of the network.
  - Any change in the parameters of the traffic pair, similar to that of the probe pairs as previously stated also has a similar impact on the latency of network as that without traffic pairs.

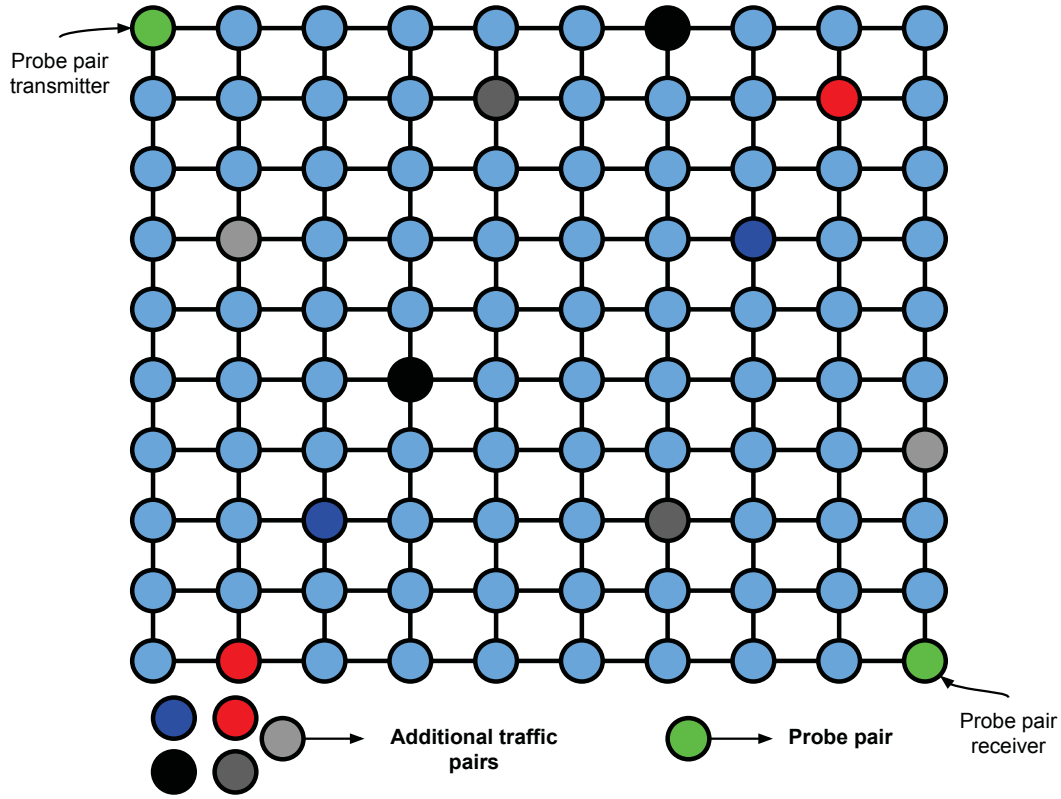

Figure 6.2: An illustration of the setup designed to analyze impact of additional traffic pairs

* **Position change of probe pair** : In order to understand the effect of change in position of probe pairs, similar experiments were conducted in another scenario where the one of the node in the pair was moved to the center of grid. The behavior in all the conditions as described above, were found to be the same. The only difference was the decrease in value of average latency as the number of hops to reach destination would reduce, but the trend remains unchanged.

6.2 The Hypothesis

The research goal is to analyze the impact of transmission power on the latency of a dense network of ZigBee nodes, where the nodes use the Ad-hoc On demand Distance Vector routing protocol to discover the neighbors and establish multi-hop routes in the network. An hypothesis is drafted based on the understanding of a state of the art literature survey, as explained in the chapters so far, about ZigBee devices, AODV routing protocol and impact of transmission power of nodes in a network.

Hypothesis: *In a network of ZigBee nodes that use Ad-hoc On demand Distance Vector routing protocol to establish routes within the network, the increase in transmission power of nodes indeed increases the number of nodes within the one-hop neighborhood. Thereby reduces the required number of hops to reach a destination node, but does not consider the quality of links when establishing these routes. The routing protocol, which is responsible for establishing the routes, does not take into account the case where a link to a node, chosen as the next hop to reach a destination, may*

be of poor quality in terms of connectivity. Therefore, there is a need to consider the quality of link when establishing routes, based on the transmission power of the sender node, to ascertain an efficient performance in terms of latency of the network.

The subsequent sections and chapters explain the approach to experimentally prove the hypothesis and draw conclusions, respectively, from the outcome of the experiments. The approach consists of following steps:

- Setup a suitable environment to perform the experiments

- Run the experiments in the designed environment and obtain reliable data .

- Draw conclusions on the outcome of experiments

6.3 Evaluation of the Hypothesis

6.3.1 Experimental setup

The goal is to analyze the impact of transmission power of the nodes on the latency of the network. The other network parameters are set to constant values based on the experiments performed as described in section 6.1.1. Certain assumptions are made in few parameters which is explained in the experimental setup below:

* Size of Network : The topology of the network is set as a grid topology of 100 nodes distributed equally across 10 rows and 10 columns. This provides a fairly large network considering the fact that an average ZigBee home automation system may contain about 120 ZigBee devices (JN5168).

* Distances X and Y : The inter-node distance in the grid is fixed to 5 meters, a regular grid is chosen to ease the interpretation of simulation results. Generally, the minimum transmission power of ZigBee devices is -32 dBm, and in the application scenario where path loss models are used in the simulations, enable the network to discover neighbors at a fairly small power of -40 dBm with the sensitivity of devices being -110 dBm, at an inter-node distance of 5 meters. This is based on experimental observation. It is for the same reason that the distance between nodes is assigned as 5 meters.

* Total simulation time : A total simulation time of 100 seconds is chosen to balance large enough data sample and the real time needed for simulations given the time constraint of the project.

* Packet interval : A worst case application scenario in an home automation system where the devices send data packets twice every second is assumed. This helps us understand the behavior where there is a fairly large traffic burst introduced due to a single pair of nodes, for example a case where the remote control is being continuously used. Therefore the packet interval is fixed to 0.5 seconds.

* Traffic pairs : For the moment, no external traffic pairs are used, the only possible traffic generated is due to the network maintenance messages generated by the nodes.

* Application start time : Based on the evaluation made in section 6.1.1, the Hello burst lasts for 0.328 seconds and we allow the network to settle down and assume that the application of probe pair starts sending messages after 3 seconds. Since the Hello messages are sent every 10 seconds, and at 30, 60 and 90 seconds of simulation we have unnecessary CSMA back offs due to the packets being attempted to send at same time, therefore we decide to avoid this condition to minimize the impact of CSMA back offs in the data obtained. Thus the application packets are sent at 3.1 seconds.

* Total packets sent : In a total simulation time of 100 seconds, the application starts sending packets at 3.1 seconds. Therefore the application has 96.9 seconds during which it sends 193 packets.

* Packet size : On referring to the ZigBee specifications[16], it is observed that most of the application packets, the maximum total size is 33 bytes and for this reason the application level packet size is set as 33 bytes.

* Hello Interval : The ZigBee devices in the intended application scenario are fairly active, the routes between the probe pairs are kept alive through high data rate application packet transfers. Based on the experiments described in section 6.1.1, 10 seconds is found to be optimal when other application level parameters are fixed.

* Active route timeout : The active route timeout or the lifetime of the route is set as 3 seconds. These are also based on the experimental observations made from the previous section 6.1.1. By setting it to a low value, we are regenerating new routes in case the route expires due to lack of communication between two nodes of a link. In AODV the lifetime is updated every time the route is used for either control or data packet communication. Therefore the reason for loss of a link would be due to lack of any communication in the link for a duration of 3 seconds, in which case the node finds a new route if required. If a new and better route is obtained, then it is accepted and updated in the routing table. Therefore this lifetime does not hamper the routing protocol from finding shorter routes.

* Delete period : If there exists a route between node A and C through B and the link BC breaks, then B informs A that the link is broken. On being informed, A invalidates the route, but the routing table entry still exists. There is a possibility that the link breakage between B and C was temporary and was restored in the next data communication, therefore node A does not delete the route immediately, it waits for a certain duration, defined by Delete period, after which it deletes the routing table entry. The reason that this routing table entry is not deleted for a certain duration of time is that it helps in route discovery process when needed. The Delete period can be defined by a certain equations based on the way the link breakage is ascertained, as defined in [41]. If Hello messages are used to determine the link breakage status, then the minimum value of Delete period should be equal to a value greater than the number of acceptable Hello message loss and Hello interval. This is to imply that if there is no message communication for a duration in which permitted number of Hello messages, that can be lost, and the duration of Hello interval, then there is little possibility of the link being ever reestablished. In the application scenario this equation is used because the Hello messages are used to keep the links alive in case of absence of data messages. The number of allowed Hello message loss is 2 and the Hello interval is 10 seconds. Since the Hello messages can be sent by either of the nodes, therefore a multiplying factor of 2 is used with the product of hello interval and allowed hello message loss, making the product equal to 40 which is chosen as the delete period.

* My route timeout : This is the value set on the lifetime field of a RREP message. This is the maximum time the RREP message can take to reach the intended destination which has been set to a value equal to the path discovery time. The path discovery time is two times the Net traversal time where Net traversal time is the maximum time taken for a packet to travel across the network. The Net traversal time is defined as the product of Node traversal time and Net diameter. The Node traversal time is time for a packet to move from one node to another which is defined as 40 milli seconds which is inclusive of processing time. The Net diameter is the maximum number of hops allowed for a control packet in the network. The Net diameter is in a way defining the boundaries for control packets in a network. In the application scenario, of 10X10 nodes, the worst case hop count is around 25 and considering some buffer values, this has been retained with a default value as set in standards to 35. Therefore the Net traversal time is 2.8 seconds and the path discovery time is 5.6 seconds, which is the My route timeout value.

* Nakagami propagation loss model : The Nakagami propagation loss model is used in the NS-3 simulations to introduce the impact of randomness in the network conditions. The Nakagami propagation loss model is described in the previous chapter Network Simulator: NS-3.

* Friis model : The free space model is used over which Nakagami is implemented in the NS-3, the other sources of interferences such as WiFi, bluetooth etc are not considered in the experiments. The description is available in the chapter Network Simulator: NS-3.

* Constant speed delay model : The topology is fixed to 10X10 grid and there is zero physical mobility of nodes, therefore the constant speed delay model is implemented as described in the previous chapter Network Simulator: NS-3.

* Seeding : The concept of seeding and runs in the NS-3 is as explained in the previous chapter of Network Simulator: NS-3. In the experimental setup, we use a single set of seed, but 5 different runs, thereby using non-overlapping set of random numbers. This ensures reliable outcome of the experiments as it takes into consideration a large number of different sets of random numbers.

Summary: The experiments have been run with the above set of configuration parameters fixed to constant values. For the above stated setup, based on a number of experiments it is determined that the minimum transmission power at which the nodes discover atleast two of their adjacent neighbors to join and be a part of network is -40 dBm. The maximum power at which the probe transmitter, the node 1 in topology (see figure 6.1) can reach the probe receiver, node 100, in a single hop is determined to be -7 dBm. Therefore the power is varied in this range at different steps, the average latency at application level is calculated for every experimental run and an average of 5 runs provides the average latency for a specific transmission power value. The final evaluation is the impact of transmission power on a performance metric, the average latency of the network.

6.3.2 Conduct experiments

The transmission range of a node increases with the increase in the transmission power, thereby allowing the node to find a large number of single hop neighbors. For the configuration parameters stated in the section 6.3.1, experiments are conducted to determine the reachability of the probe pair transmitter node at different power levels. We use the values of ranges for different transmit power and the figure 6.3 is used to explain different scenarios (as described in subsequent paragraphs). The range of transmission powers are experimentally determined. In these experiments, the transmission power is varied in small intervals and the routing table is referred to infer the number of neighbors at the specific transmission over. This helps in understanding the neighborhood of a node at different values of transmission power. In the description below, the probe pair transmitter (node 1) is considered as a reference for discovering the neighborhood at different transmission power levels. It can be inferred from the experimental outcome and with the help of figure 6.3 that, as transmission power increases, the number of nodes within one-hop neighborhood increases. It is possible that the quality of link between the probe pair transmitter node and each of the nodes in its one hop neighborhood be different i.e. one of the nodes might be well connected at a specific transmission power, whereas another node might have poor connectivity at the same transmission power by being just at the border of communication range. From the figure 6.3, for a transmission power of -36 dBm, the probe pair transmitter node (node 1) can reach the diagonal node (node 12) which could be the case of poor connectivity. The diagonal node being in the vicinity of one-hop neighborhood, will have shorter routes to reach the destination node rather than the adjacent nodes (node 2 and 11). Since the AODV routing protocol would prefer the route with lesser number of hops to reach the destination, the route to reach destination will be through this diagonal node. As the transmission power is increased to -27 dBm, the number of nodes in the vicinity of one hop neighborhood further increases, thereby increasing the probability of choosing a low connectivity neighbor as next hop to reach the destination. At -7 dBm, the probe

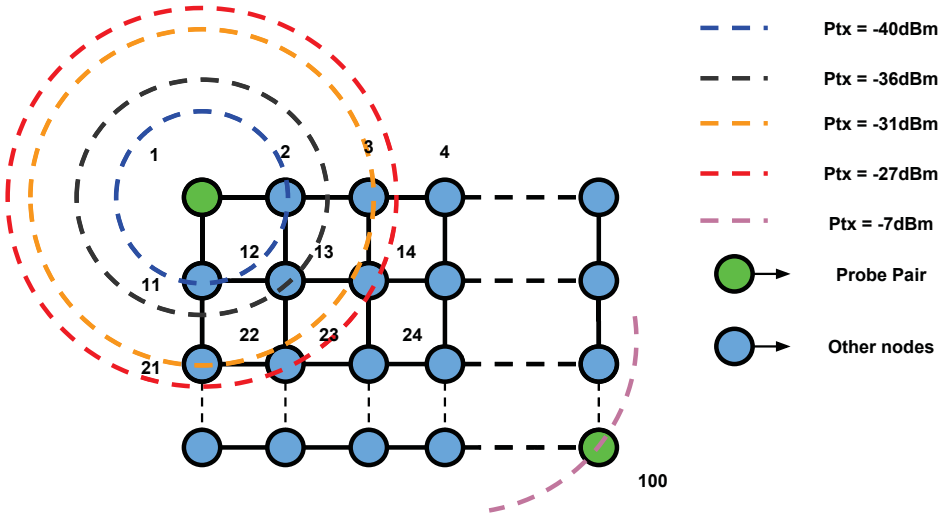

Figure 6.3: An illustration: The range of communication of the probe transmitter node at different power levels

pair transmitter and receiver are in one-hop reach of each other, but just below −7 dBm, the rest of 98 nodes are in one-hop neighborhood but there could be links which are poorly connected but have lesser number of hops to reach the destination. In such a scenario, where there is a possibility of using the links with poor connectivity and yet shorter routes, to evaluate the impact of transmission power on latency of network, experiments are conducted in different ranges of power. In each range of power data is obtained in different levels of granularity so as to evaluate impact of minor and major changes in transmission power. The table below shows the range of transmission power, granularity of the data obtained, number of hops to reach the destination and number of nodes within the one-hop neighborhood.

Table 6.1: Experimentally determined transmission power ranges for the evaluation

Range of transmission power(in dBm)	Number of data samples	Step variation of power (in dBm)	Maximum Number of one hop neighbors
−40 to −36.16	25	0.16	2
−36 to −31.6	25	0.2	3
−31.4 to −27	50	0.08	7
−27 to −7	25	0.8	99

Transmission power between −40 **and** −36.16 **dBm:** In this transmission power range, the probe pair transmitter node is expected to reach only the adjacent nodes (nodes 11 and 2) as shown in the figure 6.4. The total number of one-hop neighbors are 2. The transmission power is increased from −40 dBm to −36.16 dBm in steps of 0.16 dBm, 25 data samples about the packets are obtained.

Transmission power between −36 **and** −31.6 **dBm:** In this transmission power range, the probe pair transmitter node is expected to reach the closest diagonal node (node 12) as shown in the figure 6.5. The total number of one-hop neighbors are 3. As the transmission power is

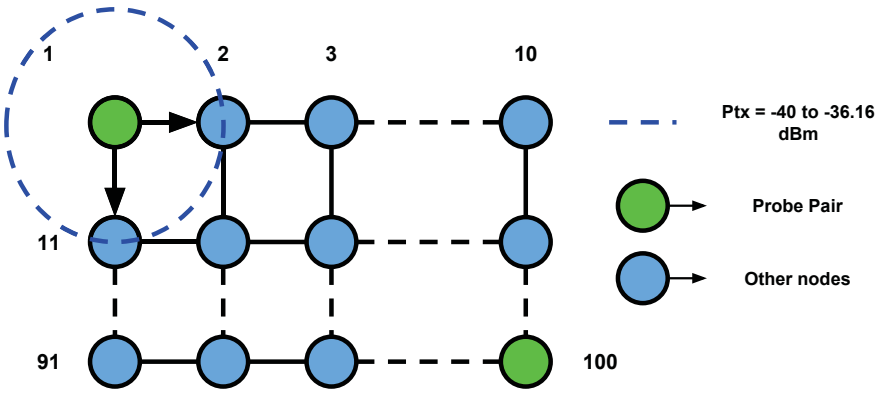

Figure 6.4: An illustration: The reachability of probe pair transmitter node in a range of transmission power between −40 and −36.16 dBm

increased from −36 dBm to −31.6 dBm in steps of 0.2 dBm, 25 data samples about the packets are obtained.

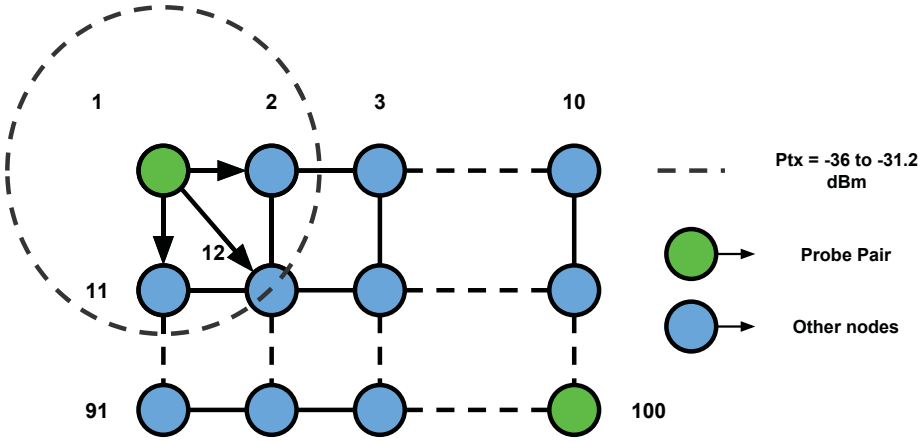

Figure 6.5: An illustration: The reachability of probe pair transmitter node in a range of transmission power between −36 and −31.6 dBm

Transmission power between −31.4 and −27 dBm: In the transmission power range of −31.4 and −27.08 dBm, the probe pair transmitter node is expected to reach the second set of adjacent nodes (nodes 21 and 3) and at −27 dBm, it is just able to reach the next set of diagonal nodes (nodes 13 and 22) as shown in the figure 6.6. The total number of one-hop neighbors within transmission power of −27 dBm is 5, whereas at −27 dBm is 7. As the transmission power is increased from −31.4 dBm to −27 dBm in steps of 0.08 dBm, this accounts for the 50 data samples obtained of latency. The reason behind collecting 50 data samples in this transmission power range is to closely observe the behavior of network for small changes in transmission power, due to the fact that there are many one-hop neighbors in this power range. Only through increasing the granularity of data we can see the increase in number of one-hop neighbors between −27.08 dBm and −27 dBm.

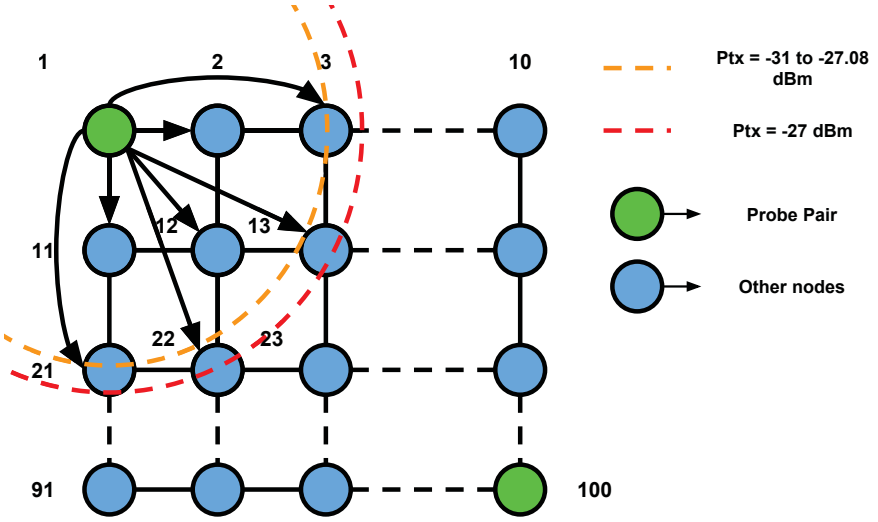

Figure 6.6: An illustration: The reachability of probe pair transmitter node in a range of transmission power between −31.4 and −27 dBm

Transmission power between −27 and −7 dBm: In this transmission power range, the probe pair transmitter node is expected to reach the destination node (node 100) in a single hop as shown in the figure 6.7.The total number of one-hop neighbors are rest of the network of 99 nodes. The transmission power is increased from −27 dBm to −7 dBm in steps of 0.8 dBm, 25 data samples about the packets are obtained.

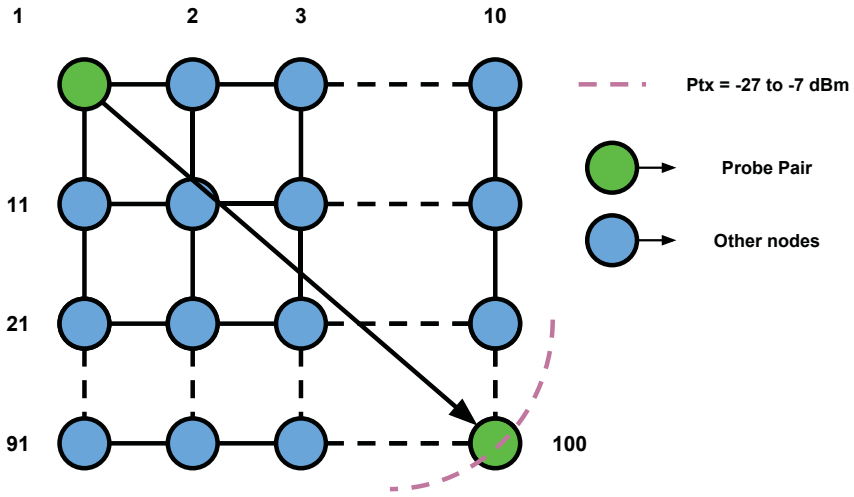

Figure 6.7: An illustration: The reachability of probe pair transmitter node in a range of transmission power between −27 and −7 dBm

The experiment is designed with the configuration parameters and different scenarios, reasoning has been stated in the respective explanations starting from the sections 6.3.2. Packets are sent at application level, have a time stamp tag attached, which is obtained from the simulator timer,

the difference between the time at which the packet was constructed at the application layer and time at which it was processed at the receiver node at the same application layer is defined as latency. Reiterating the approach and goals of the experiments:

- Measure latency of every packet received at the destination node for a specific transmission power.
- Calculate average latency for all the packets received.
- Re-run the experiment with a different 'Run' number, thereby choosing different set of random numbers for the same experimental setup to improve the accuracy of obtained result. Repeat the experiment for a total of 5 'Runs' i.e. 5 different sets of random numbers uniformly distributed in the set (refer section Network Simulator 3).
- There are 5 average latency values over 5 different runs. Calculate average of these 5 results, which gives an accurate measurement of average latency for one specific transmission power value.
- Repeat the process, for different values of transmission power as described in the section 6.3.2.
- Plot graphs of average latency against the transmission power for each range of transmission power. Observe and analyze the behavior.
- Combine the data of all transmission power values and plot a graph of average latency vs the entire transmission power range from -40 dBm to -7 dBm and observe and analyze the behavior.

6.3.3 Evaluation of results

As described in the section 6.3.2, experiments are conducted and from the obtained data, graphs of average latency vs transmission power are plotted in different ranges of power. This section describes the analysis of the obtained graphs and reason for the behavior of the network. The power ranges are an indication of the number of nodes in the one-hop neighborhood i.e. at lower range of transmit power, there are less number of nodes in the one-hop neighborhood (see figures 6.8 and 6.9) and at higher transmit power, there are larger number of nodes in the one-hop neighborhood (see figures 6.10 and 6.11), of the probe pair transmitter node. In the rest of analysis, it is to be assumed that the discussion of latency and one-hop neighborhood is always with respect to the probe pair transmitter.

Transmission power between -40 dBm and -36.16 dBm: The graph in the figure 6.8 indicates how the latency is affected by small changes in transmission power when there are only two nodes in the one-hop neighborhood.

It is to be noted that the minimum transmission power at which the network is established is at -40 dBm, any transmission power lower than this value cannot establish the network because nodes cannot discover each other. At -40 dBm the adjacent nodes, node 11 and 2 (see figure 6.4), are just within the range of communication, thereby the connectivity is poor. At this point, it can be observed from the graph in figure 6.8 that the latency is the highest, this could be due a large number of reasons such as the CSMA back-off or the re-transmission. In 802.15.4 MAC layer, the transmission is considered successful, only if it receives a MAC level acknowledgement, if the acknowledgement is not received in a certain duration of time, then the frames are re-transmitted upto a maximum number of allowed retries beyond which the packet is dropped.

Due to the channel being busy, the nodes of the network will be subjected to random back off periods which adds to the latency of network. When the node performs a CCA, if it finds that the channel is still busy, then the back off period is exponentially increased by a preset factor called as the back-off exponent, which adds to the overall latency of the network.

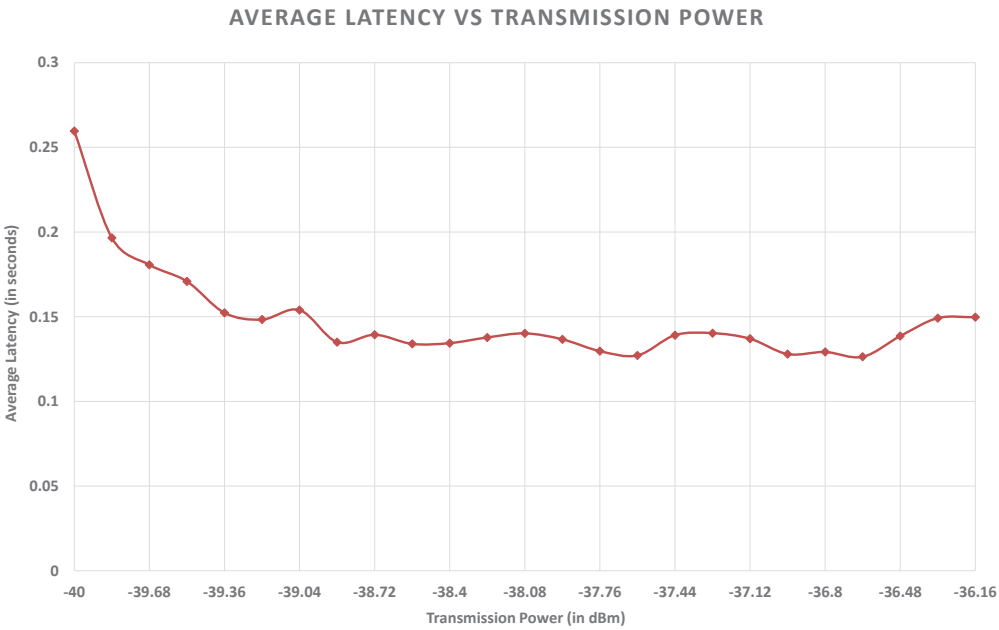

Figure 6.8: A graph of Average Latency vs Transmission power in a range of −40 to −36.16 dBm (2 one-hop neighbors)

As the transmission power increases, the connectivity improves gradually and the average latency reduces as seen from the graph in the figure 6.8. There are two nodes from which the probe pair transmitter could receive a route, if the route is of good connectivity, then the latency variations are less, else the latency is more. Therefore, for the same reason of different route quality, meaning the link quality, we can see in the graph that there are few instabilities which accounts for the path chosen by the routing protocol.

At this point, it is necessary to note The probe transmitter node is situated at the edge of the grid, therefore has neighbors only on one side, while nodes in the middle or edge of the grid have more number of neighbors and this accounts for latency in the network. Though an intermediate node may choose a route among only 2 adjacent nodes which are closer to destination node, but the back offs and re-transmissions could be due to all the adjacent neighbors.

The experiments conducted are for 5 different sets of random numbers, called as runs, and it is expected that if the observation is made over a larger set of runs, then the variations in the latency would be lesser as the average value of latency will be obtained from a large set of possible outcomes.

The changes in latency are observed to be a minimum upto the transmission power where it just has 2 one-hop neighbors i.e. till a transmission power of −36.16 dBm.

Transmission power between −36 dBm and −31.6 dBm: The figure 6.5 gives an illustration of the connectivity of the probe pair transmitter node in the range of transmission power between −36 dBm and −31.6 dBm.

• At −36 dBm the probe pair transmitter node is just able to reach the diagonal node (node 12). The phrase 'just within the range' implies that the link is in the border of the communication range where the connectivity is variable due to the usage of Nakagami propagation loss model in the simulation (as described in chapter 5), which is responsible for simulating the behavior of an an-isotropic antenna in real nodes. If the probe transmitter

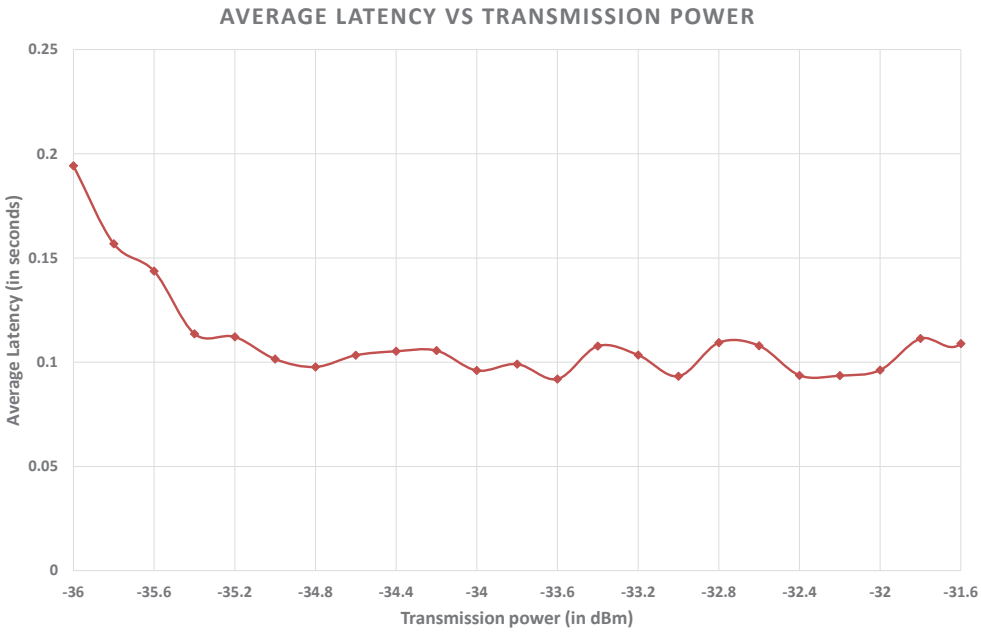

Figure 6.9: A graph of Average Latency vs Transmission power in a range of −36 to −31.6 dBm (3 one-hop neighbors)

node receives even a single hello message from the node with a poor connectivity then it records it as a one-hop neighbor. If it receives a route from the same node with least number of hops to destination, then it continues to use the route assuming the link is active, until the lifetime of the route expires.

• The route could be established by many poor connectivity links thereby reducing the quality of performance of the network in terms of latency. All these facts are evident from the graph indicated in the figure 6.9. As seen from the graph, at −36 dBm of transmission power, there is a sudden increase in the average latency. At this transmission power, node 12 is in the vicinity of one-hop to the probe transmitter node but in the border range of communication. Since this node could provide the shortest path to destination, there is a high probability that the node could be chosen as the next hop in the route.

• The same logic is applicable to the rest of the network which provides the route between source and destination. Therefore a route could be established with poorly connected links. Also, the hidden terminal problem[31] could persist in the network. In which case, the packet might not be delivered, thereby requiring more number of re-transmissions hence adding to the increase in latency.

• It should be noted that the latency, in comparison to the values in the previous range of transmission power, is lesser because the route has lesser number of hops between source and destination nodes. Though the trend is a decreasing one, but there is a degree of discrepancy about the latency of network at every transmission power level.

• As seen from the figure 6.5, now there are 3 nodes within the one-hop neighborhood of the probe pair transmitter node. Therefore choosing the right link to establish an efficient route to the destination node becomes more essential, considering the fact that even though the diagonal node (node 12) may have a shortest route, but there is a possibility that the connection might not be good.

• As seen from the graph in the figure 6.9, there is an increase in the variation of average latency at different transmission power levels, which are seen in with more number

instabilities, in comparison to the previous power range. The key point to note is that, even an increase of just one node in the number of nodes in one-hop vicinity has brought about notable change in the behavior of network in terms of latency of packet delivery.

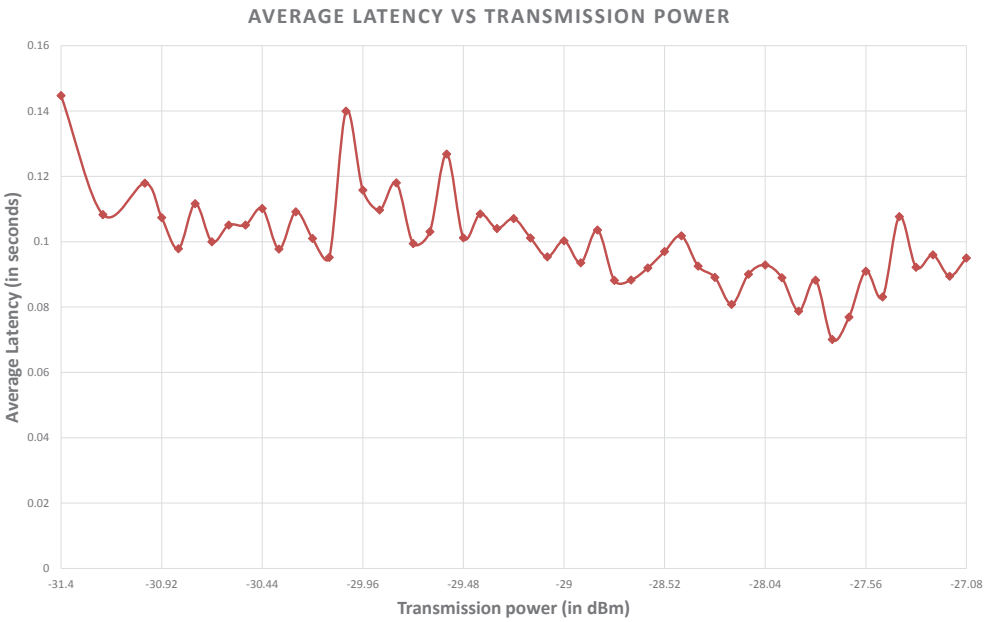

Figure 6.10: A graph of Average Latency vs Transmission power in a range of −31.4 to −27.08 dBm (5 one-hop neighbors)

Transmission power between −31.4 dBm and −27.08 dBm: Referring to the figure 6.6, we can observe that in this transmission power range, a difference of 0.8 dBm in power can vary the number of neighbors in the one-hop neighborhood. As seen from previous two results where an increment in the number of one-hop neighbors affected the behavior of the network notably, an increase of 2 to 4 nodes in one-hop neighbor hood is expected to have a significant effect on the latency of packet delivery in the network.

- As seen from the graph in figure 6.10, at a transmission power value of −31.4 dBm, there is a sudden rise in the latency of network, accounting to the discovery of new nodes in the one-hop neighborhood. At this transmission power, nodes 21 and 3 fall in the one hop vicinity of the probe pair transmitter node. Similar trend could also be seen in the rest of the nodes of the network as they transmit at same power level.

- Therefore at −31.4 dBm, we have 5 nodes in the one hop vicinity, of which two nodes, node 21 and node 3 are much closer to the destination, but in the border of communication range with poor connectivity. It is also more likely that the route through these nodes is chosen by the probe transmitter node as it could consist of lesser number of hops. It is also possible that the routes shift among many poorly connected links, thereby not improving the performance of the network. This accounts for the observation from the graph that there is a peak at −31.4 dBm.

- Since there are more number of nodes to choose from, node 21, node 12 and node 3, all are likely to have same number of hops to destination, but at different link connectivity, there is more instability in the behavior of the network even at small changes of power levels. It is for the same reason that the granularity of obtained data is increased to observe the behavior of network at small power level variations, therefore 50 samples of data are obtained

in the power range. Every data is obtained by increasing the power level by a value of 0.08 dBm.

• Overall, the latency tends to show a decreasing trend as the connectivity increases with raise in power levels. But the fact that still remains is the regular spikes of latency which is due to the choice of bad links with poor connectivity in the vicinity of one hop neighborhood. This behavior could be the case of any node, which is part of the route, in the network at the specific transmission power levels.

• Observing the behavior in three different power ranges; −40 to −36, −36 to −31 and −31 to −27 dBm, it is quite evident that the number of nodes in one hop neighborhood, the transmission power at which these nodes are being reached, the resulting connectivity, all these factors play a vital role in the performance of the network in terms of latency. This can be further substantiated with the results from the last range of transmission power −27 to −7 dBm, where the extracted data is coarse in granularity as explained in the next paragraph.

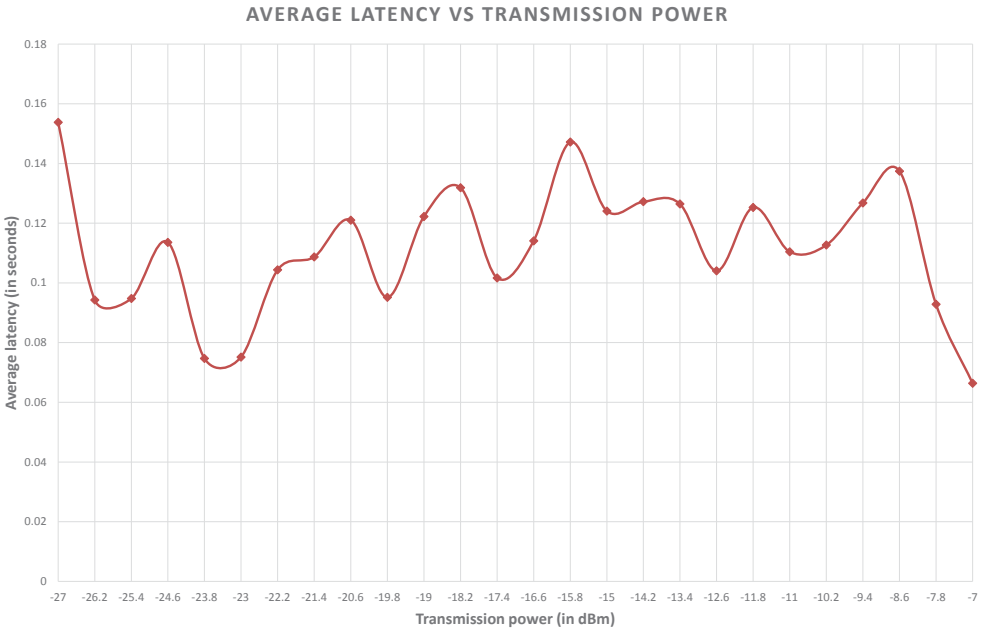

Figure 6.11: A graph of Average Latency vs Transmission power in a range of −27. to −7 dBm (7 to 99 one-hop neighbors)

Transmission power between −27 dBm and −7 dBm: The transmission range where the number of one-hop neighbors increase from 7 all the way till 99 which would include the final destination node itself at −7 dBm.

• From the previous results, it was observed that at −27.08 dBm, the adjacent nodes, node 21 and node 3, are well within good range of communication of probe pair transmitter node. If the transmission power is then increased by just 0.08 dBm, then the nodes 22 and 13 fall in the one-hop neighborhood. This sudden change in neighborhood is reflected by the spike of latency at −27 dBm in the graph shown in figure 6.11.

• Beyond −27 dBm of transmission power and within the value of −7 dBm, there is a drastic increase in the reachability of a node, adding more number of nodes to its list of one-hop neighbors. Thereby increasing the probability of choosing the poorly connected

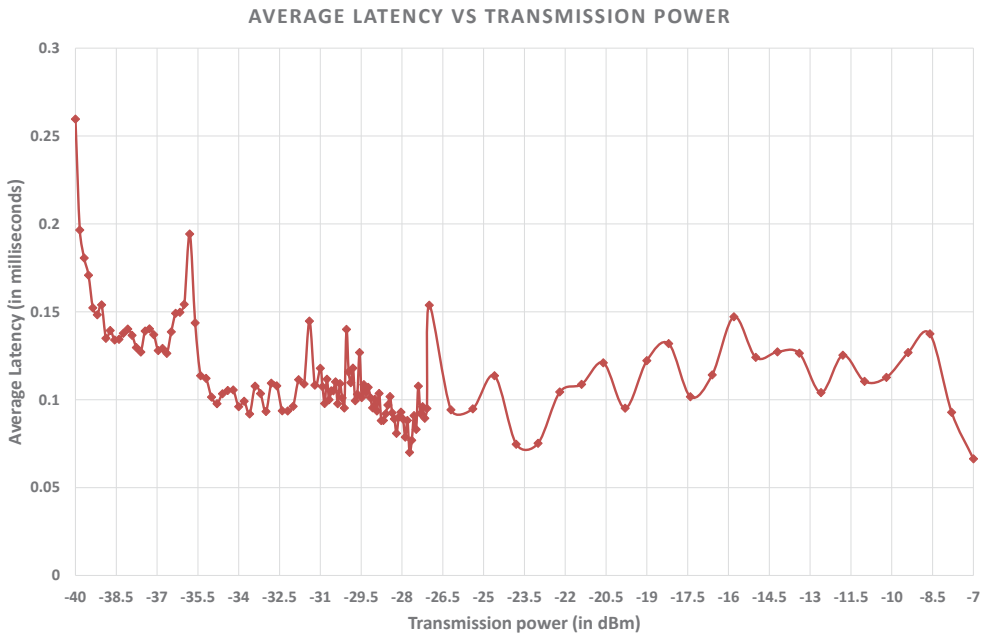

Figure 6.12: Impact of transmission power on latency over the range of power between −40 dBm and −7 dBm

links at every transmission power as the routing protocol measures the link cost in terms of number of hops to the destination.

• Due to large range of power levels between −27 dBm to −7 dBm, and having already established the conclusive behavior of network for change in transmission power over higher data granularity in lower power ranges, the number of data samples obtained in this power range are 25. As seen from the graph in figure 6.11, it is easily noticeable that there is a considerable amount of variation of latency over the changes in transmission power. The network is incapable of choosing the links that lead to efficient routing, in terms of latency, because the metric to choose the route in a network is restricted to just the number of hops, where the route with least number of hops is preferred.

• Upto −7.8 dBm the probe pair transmitter is able to discover all the nodes except the probe pair receiver. At −7 dBm, both the probe pairs are in one-hop neighborhood of each other, therefore a drastic dip in the average latency can be seen in the graph.

• To observe the behavior of the network over the entire range of power, the data from all the above range of powers can be merged into a single plot as shown in figure 6.12.

Summary: The configuration setup for the experiments and the reasoning is as described in the section 6.3.1. An hypothesis is established in the section 6.2, the following sections are aimed at getting evidence for the hypothesis through experiments. The experiments are conducted on specific transmission power ranges, the ranges have been carefully designed based on certain experimental outcomes as described in early parts of section 6.3.2 and a chosen application scenario. The outcome of the experiments are cautiously analyzed and the behavior is reasoned through a structural approach in the section 6.3.3. The final result is gathered and represented in the figure 6.12 which shows the plot of average latency against transmission power values. In the graph from figure 6.12, the spikes (at −36 dBm, −31.4 dBm, −27 dBm and many between −27 and −7 dBm) are noticeable and can be reasoned as the soft spots where the network undergoes a shift (increase, as transmission power increases and vice versa) in the number of

devices under the node's one-hop neighborhood. The large number of peaks in the range -27 dBm and -7 dBm are accounted to the fact that, the power values in the range can offer a large number of nodes in the one-hop neighborhood. These spots are an indication of the poor connectivity of the network, as the chosen routes, consist of links that are in border range of communication of the nodes. The routing protocol is unable to setup reliable routes, as the routes are established based on the hop count, irrespective of the quality in the connectivity of the link. These inferences give an overall picture about the performance of network in terms of a metric namely latency, with respect to change in transmission power of the nodes.

Chapter 7

Conclusions

The goal was set out to establish a platform to be able to simulate the behavior of large ZigBee networks and use the platform to observe the impact of transmission power of nodes on the latency of the network and reason this behavior.

In this chapter, section 7.1 describes the need for the set research goals and summarizes the goals of the thesis. Section 7.2 discusses the outcome of experiments conducted with the intention of achieving the targets, evaluate these results with appropriate reasoning. The section 7.3 describes some of the challenges of the research conducted. In the final section 7.4, recommendations to improve the performance of the network in terms of latency are proposed based on the extensive literature analysis done during the course of thesis.

7.1 Reiterating the goal

The ZigBee devices operate in large number of application profiles, each of which have distinct environmental conditions. For example, the environment of a remote control system in industry is different from a health care system in terms of traffic and mobility. The environment being very dynamic in many cases with a large number of sources of interference, such as WiFi, Microwave ovens etc which use the same frequency of signals. In such cases it would be wiser to minimize the interference caused by the nodes within the network. The intra network interference is mainly due to high transmission power of the nodes, wherein the nodes occupy the communication channel used by large number of nodes. Therefore, one way to minimize the intra network interference would be to choosing the optimal transmission power, but the transmission power has an impact on the way the network is setup and communication path between the nodes.

The transmission power of a device in a network affects its process of network discovery and data communication within the network. In the process of network discovery, the transmission power decides the range of communication of the node and the number of devices with which it is able to establish a direct link communication. When transmitting the data over the network, a high transmission power indicates that the source node reduces distance (in terms of number of hops to reach destination) between itself and the intended destination node, but it also implies that it is interfering with the communication of its neighboring nodes. As the transmission power increases, so does the node's neighborhood, thereby increasing the number of nodes with which it interferes in communication.

The research goal is to analyze the impact of transmission power on the behavior of a network of ZigBee devices in terms of latency. The network needs to strike a balance between the effects of increasing interference with other nodes of the network and reaching the destination with low and acceptable amount of latency. In order to achieve this balance, it is of utmost importance to

understand how the network behaves to the variation of the transmission power and reason the behavior of the network. To understand the behavior of the network it is important to analyze the impact of various parameters, ones which define the application scenario and the ones which provide the flexibility in discovering the network (through a routing protocol). These parameters add a certain degree of predictability to the network, for successfully establishing and maintaining the network, it is essential to be able to predict the outcome under any change in network configurations.

The ZigBee application profiles are closely associated with the IoT and there is a shift of the internet protocol version usage from the IPv4 to IPv6, mainly due to shortage of addressing space in IPv4. In order to achieve the research goals stated previously, as a prerequisite, it is necessary to create a platform to be able to simulate the behavior or a large ZigBee network instead of setting up a large test bed of ZigBee devices which could be expensive at the early stages of research. The research aims at creating this platform, use the platform to analyze the impact of transmission power on the latency of a large and dense network of ZigBee devices.

7.2 The results

The prerequisite for the research goal is established by designing the AODV routing protocol which uses the IPv6 in the NS-3 simulator. Using this as a platform, the ZigBee network layer can be simulated and the behavior of a large ZigBee network can be observed by using the 802.15.4 MAC and PHY layer, with an adaptation layer of 6LowPAN in between the MAC and network layer. The experimental setup is explained in the previous chapter, where the network is simulated to understand the impact of transmission power on the chosen performance metric- latency, of the network. The results as shown in graphs of previous section indicate that the transmission power is directly responsible for the number of nodes in one-hop neighborhood of a device. As the transmission power increases, the number of nodes in the one-hop neighborhood also increase. The routes between source and destination is decided by the AODV routing protocol, which is a reactive routing protocol that determines routes as and when necessary. The link cost metric for determining and differentiating routes in AODV is the number of hops between the source and destination i.e. the route with least number of hops is preferred. The graphs in the chapter 6 show that at certain transmission powers, there are peaks of latency, and it is also experimentally determined that at these power levels, new nodes are discovered which offer shorter routes to destination, but the connectivity in the link is poor. The poor connectivity is accounted for the fact that the new node is in the border range of communication. Therefore, in order to transmit packets in such a link, the nodes have to re-transmit the data a large number of times as the packets might be lost and therefore no acknowledgments will be received by the sender node. Also, if there are other nodes trying to communicate at the same time, then the transmission at the sender node will be delayed due to back-offs at the MAC level due to CCA fails. These situations add to the latency of packet delivery, considering the fact that the latency is measured at the application level.

The probability of choosing the improperly connected links increases with increase in transmission power. The reason behind this is that, as the transmission power increases, then there are more number of nodes in the one-hop neighborhood of the sender node. Also, as the transmission power increases, the chances of accepting routes from a poorly connected link is higher. In the AODV routing protocol, if a node receives just one control message from the neighboring node, then it establishes that node as a one-hop neighbor and as seen in the chapter of 'Experiments' these nodes generally have the shortest route to destination. Thus, the node assumes that the link is active all the time and transmits packets using this poorly connected link, wherein the packets might be dropped eventually, or the latency of packet deliver significantly increases. The significant increase in the latency can be observed in the graph at certain transmission powers such as -36 dBm, -31.4 dBm, -27 dBm and many more between -27 and -7 dBm. At $-7dBm$, the sender and destination node are in one-hop neighborhood, therefore a spike in the average latency

of the network can be seen from the graph. Thereby ascertaining that the poor connectivity is responsible for the increase in latency at these specific transmission power values. The latency at higher transmission powers, between -27 and -7 dBm, is more unstable and there is a degree of unpredictability as seen from the corresponding graphs.

7.3 Challenges of research

Simulating a large ZigBee network to understand the impact of one of the network parameters is a challenge by itself. It is required to determine different network and application parameters that can have even slightest of effects on the network behavior. Some of the key challenges of the research are stated below:

* **Planning:** The thesis requires careful planning as it consists of many phases such as:
    - State of the art literature survey
    - Drafting the architecture of implementation
    - Implementing the modules
    - Testing the implementation
    - Designing experimental setup
    - Conducting experiments
    - Evaluating the results of the experiments
    - Draw inferences from the evaluation

  All these phases have to be completed in a stipulated amount of time (6 months). Therefore this requires smart approach to achieve the targets efficiently.

* **Network parameters analysis:** The simulation of ZigBee network layer consists of AODV routing protocol, which offers a fair degree of flexibility when designing the protocol for specific application scenarios. Thus, it is important to understand how these network paramters of the routing protocol are responsible for the behavior of network.

* **Application parameters analysis:** Setting up the right application scenario by ensuring the experiments are conducted to simulate the behavior of a real network requires careful design of the parameters of application, such as data rate, data size etc.

* **Open source software:** The network simulator, NS-3 is an open source software, with limited support from the forum. The open source software is prone to challenges of understanding and bugs. In this case, certain bugs consumed considerable amount of research time, thereby requiring to adapt to contingency plans.

* **Real simulation time:** The resources available to run simulations are constrained by small memory and lower speed. Therefore, the real simulation time of one application scenario to obtain data of fair degree of granularity takes close to 54 hours in real time, which is a major constraint. Thus, simulations of smaller duration were run in iterations to ascertain the expected behavior in a specific network scenario, following which the larger duration of simulations were executed.

Despite the challenges in research, smart engineering and holistic approach to the research have ensured reliable outcomes and contribution to the research community. Overall, the contribution to the research community consists of a concrete platform in the NS-3 simulator to simulate ZigBee network layer, with wide range of possible applications. A compelling result about the behavior of a large ZigBee network and probable bottle necks of using the AODV routing protocol which can generate interest to explore in greater depth.

7.4 Discussion

The degree of unpredictability and instability can be reduced, to obtain better performance of network in terms of latency, by choosing the right transmission power for every route and striking a balance between the acceptable amount of latency and reduction in transmission power so as to not interfere in communication of other nodes in the network. It can also be taken care by making the routing protocol adaptable to link conditions at specific instances of time. This can be done by changing the link cost metric used in the AODV routing protocol (currently using number of hops to destination) to a more robust metric, a metric which can take into consideration the quality of link to its next hop in the route before transmitting the actual data packets. Using either of these two methods the network performance can be improved considerably.

By adapting the method to choose the right transmission power for every link in the route, it is ensured that the transmission takes place at an optimal power level, which does not increase the number of re-transmissions or the back-offs at the MAC level of other nodes of the network thereby reducing the latency of the network. By this method, it is also ensured that at optimal transmission powers, the connectivity with the next hop in the link is of high quality before transmitting data packets, which in turn reduces number of re-transmissions, thereby reducing the latency of network.

In the other method of adapting the routing protocol to take care of link quality before transmitting data packets by considering a more robust link cost metric, it is ascertained that the data is transmitted only when there is assurance that the packet will be transmitted with very less number of re-transmissions. This in turn reduces the latency of the network. From the experiments it is evident that lesser number of hops to destination cannot ensure a high quality link and performance of the network.

Either of the methods can help in improving the quality of performance of the network, thereby reducing the latency of network. It is evident from the results that transmission power has a direct impact on the latency of network, wherein increase in transmission power might reduce the number of hops to destination and in turn the latency of network, but it has a considerable degree of unpredictability in it. The behavior of the networks should be fairly predictable in order to deliver efficient performance which is of utmost priority in a large number of application profiles. To ensure high quality performance, the network has to be designed with optimal values to the sensitive parameters, ensure that the routing is robust, flexible and deliver high quality routes in the network.

Chapter 8

Future Work

The provision of a platform to simulate the behavior of large ZigBee networks using the NS-3 simulator has unfolded paths for a broad research area. Utilizing this platform, a large number of application profiles of ZigBee can be analyzed in a broader perspective.

The need: The ZigBee has a wide scope of application and this requires extensive research before marketable products can be manufactured. The shift towards IoT and IPv6 calls for major contributions to the research community. Focusing on the needs in the direction of the thesis goals, it is essential to understand the behavior of a large network on more than one currently used performance metric (latency).

Future trends: The NS-3 simulator provides sufficient modules to simulate a number of ZigBee application profiles. Using the modules of NS-3 an environment of a building, a house, or a scenario with different sources of interference, can be simulated using the implemented Network Layer simulation module of ZigBee in this thesis.

Extension of current work: The results from the study, impact of transmission power on latency of the network, kindles the interest to gain deeper insights about the behavior of large ZigBee networks. Following the work, further analysis can be made on other performance metrics such as packet reception ratio, throughput etc thereby providing detail information about the functioning of network. The AODV routing protocol by itself is a point of interest due to the proven need for robustness in the protocol which shall enable it to adapt to different environmental conditions. By implementing a different link-cost metric used in the process of decision making for a route establishment, the routing protocol can be made more efficient.

Research project proposal: The results so far are intriguing and form an interesting research project, where one can focus on different layers of the architecture. Starting from the MAC, the layer can be altered to function like a specific ZigBee device, the routing protocol adaptation, and designing specific applications to recreate and simulate a large ZigBee network application scenario. This allows for exploration of all the layers and understand the behavior of the network, which can then be applied on real hardware networks.

The outcome of thesis are capable of arousing interest, to dwell into depths of exploration on behavior of large ZigBee networks, in the research groups around the world that are interested in ZigBee networks and use the AODV routing protocol.

Bibliography

[1] 802.15.4 physical layer operating frequency bands. http://www.embedded.com/print/4204872. 92

[2] 802.15.4 physical layer super frame format. http://usn-pioneer.tistory.com/12. 93

[3] 802.15.4 topology styles. http://ecee.colorado.edu/~liue/teaching/comm_standards/2010F_802.15/home.html. 91

[4] Cisco business insight: Are you ready for the future. http://www.slideshare.net/CiscoBusinessInsights/convergence-are-you-ready-for-the-future-of-it. 15

[5] EUI-64 format. http://www.openwall.com/presentations/IPv6/img16.html. 18

[6] IEEE 802.15.4 and ZigBee working model. http://m.eet.com/media/1055711/chipcon-fig1.jpg. 9

[7] Ipv6 global and link local addresses. http://mrncciew.com/2013/04/05/ipv6-basics/. 18

[8] Ipv6 Header. https://commons.wikimedia.org/wiki/File:IPv6_header_rv1.png. 22

[9] Ipv6 scoped address architecture. https://www.reddit.com/r/networking/comments/32tkqk/ipv6_scope_question/. 18

[10] ISM operating bands. http://jeromeabel.net/files/ressources/xbee-arduino/images/large/wireless-techniques.png. 7

[11] MANET (Mobile ad hoc network)- Characteristics and Features. http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/. 31

[12] ZigBee Architecture. http://chipdesignmag.com/sld/files/2009/06/zigbee_wirelesshealth1.jpg. 8

[13] Zigbee topology. http://zeitgeistlab.ca/doc/doc_images/zigbee2.jpg. 12

[14] Aarti and S.S.Tyagi. Study of MANET: Characteristics, Challenges, Application and Security Attacks . *International Journal of Advanced Research in Computer Science and Software Engineering*, May 2013. 31

[15] Manal Abdullah and Aisha Ehsan. Routing protocols for wireless sensor networks: Classifications and challenges. *Journal of Electronics and Communication Engineering Research*, 2(2):5–15, 2014. 29, 31

[16] ZigBee Alliance. ZIGBEE SPECIFICATION. Jan. 2008. 9, 63

[17] Noucha Baccour, Anis Koubaa, Luca Mottola, Marco Antonio Zuniga, Habib Youssef, Carlo Alberto Boano, and Mario Alves. Radio Link Quality Estimation in Wireless Sensor Networks: a Survey. *ACM Transactions on Sensor Networks (TOSN)*, Dec. 2012. 2

[18] Shalini Shivhare Basu Dev Shivahare, Charu Wahi. Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property. *International Journal of Emerging Technology and Advanced Engineering*, 2, March 2012. 31, 32

[19] T. Ryan Burchfield, S. Venkatesan, and Douglas Weiner. Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations. *In Proc. Int. Workshop Localized Algor. Protocols WSNs*, pages 15–29, June 2007. 2

[20] Elizabeth M Royer Charles E Perkins. Ad hoc On Demand Distance Vector Routing. *Mobile Computing Systems and Applications 1999 Proceedings WMCSA 99*, pages 90–100, February 1999. 33, 35

[21] Pravin Bhagwat Charles E Perkins. Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for Mobile Computers. *Proceeding SIGCOMM '94 Proceedings of the conference on Communications architectures, protocols and applications*, 24(4):234–244, Oct. 1994. 32, 33

[22] Aminul Haque Chowdhury, Muhammad Ikram, Hyon-Soo Cha, Hassen Redwan, S. M. Saif Shams, Ki-Hyung Kim, and Seung-Wha Yoo. Route-over vs mesh-under routing in 6LoWPAN. *IWCMC '09 Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, pages 1208–1212, 2009. 34

[23] David A. Maltz David B. Johnson. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing*, 353:153–181. 32

[24] Josh Broch David B. Johnson, David A. Maltz. DSR The Dynamic Source Routing Protocol for Multi Hop Wireless Ad Hoc Networks. *Ad hoc networking*, pages 139–172, Jan. 2001. 32

[25] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Dec 1998. 16, 25

[26] Gregory Hackmann, Octav Chipara, and Chenyang Lu. Robust Topology Control for Indoor Wireless Sensor Networks. *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008. 2, 3

[27] Suyash Jain. AN123 – Breaking the 400-Node ZigBee® Network Barrier With TI's ZigBee SoC and Z-Stack Software. April 2014. 2

[28] Ahmed E. Kamal Jamal N. Al-Karaki. Routing Techniques in Wireless Sensor Networks: A Survey. *Wireless communications, IEEE*, pages 6–28, 2004. 29, 31

[29] E. Kim, D. Kaspar, C. Gomez, and C. Bormann. Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network 6LoWPAN Routing. May 2012. 34

[30] Murat Miran Koksal. A Survey of Network Simulators Supporting Wireless Networks. Oct. 2008. 2, 4, 45

[31] D.I. Laurenson. Revisiting the Hidden Terminal Problem in a CSMA/CA Wireless Network. *Mobile Computing, IEEE Transactions*, 7(7):817 – 831, July 2008. 70

[32] Tsung-Han Lee, Hung-Shiou Chiang, Lin-Huang Chang, Ming chun Hsieh, Chih-Hao Wen, and Kian Meng Yap. Modeling and Performance Analysis of route-over and mesh-under routing schemes in 6LoWPAN. *Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference*, pages 3802 – 3806, Oct. 2013. 34, 35

[33] Shan Lin, Jingbin Zhang, Gang Zhou, Lin Gu, Tian He, and John A. Stankovic. ATPC: Adaptive Transmission Power Control for Wireless Sensor Networks. *Proceedings of the 4th international conference on Embedded networked sensor systems*, 2006. 2, 3

[34] Janne Lindqvist. Counting to Infinity. Apr. 2004. 33, 41

[35] Shima Mohseni, Rosilah Hassan, Ahmed Patel, and Rozilawati Razali. Comparative review study of reactive and proactive routing protocols in manets. In *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*, pages 304–309. IEEE, 2010. 31, 32

[36] Md Monzur Morshed, Franz I S Ko, Dongwook Lim, and Md Habibur Rahman. Performance Evaluation of DSDV and AODV Routing Protocols in Mobile Ad-hoc Networks. *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference*, pages 399 – 403, May 2010. 33

[37] Juniper Networking. Learn About Differences in Addressing Between IPv4 and IPv6. Jan 2014. 16

[38] Anneleen Van Nieuwenhuyse, Mario Alves, and Anis Koubaa. Technical report On the use of the ZigBee protocol for Wireless Sensor Networks. June 2006. 2

[39] Amer Nizar and Abu Ali. Comparison study between IPV4 and IPV6. *IJCSI International Journal of Computer Science Issues*, May 2012. 16

[40] Jianli Pan and Raj Jain. A survey of network simulation tools: Current status and future developments. *Email: jp10@ cse. wustl. edu*, 2008. 2, 4, 45

[41] C. Perkins and E. Belding-Royer. Ad hoc On-Demand Distance Vector (AODV) Routing. July. 2003. 35, 63

[42] NS3 Project. ns-3 Model Library. Jan 2012. 46

[43] NS3 Project. ns-3 Manual. May 2011. 46

[44] NS3 Project. ns-3 Tutorial. Nov 2013. 48

[45] Surendra H Raut and Hemant P Ambulgekar. Proactive and reactive routing protocols in multihop mobile ad hoc network. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4):152–157, 2013. 31, 32

[46] Tim Rooney. IPv4-to-IPv6 Transition and Co-Existence Strategies. 2011. 16

[47] Jang Ping Sheu, Kun Ying Hsieh, and Yao Kun Cheng. Distributed Transmission Power Control Algorithm for Wireless Sensor Networks. *Journal of Information Science and Engineering*, 2009. 2, 3

[48] Vivek Shrivastava, Dheeraj Agrawal, Arunesh Mishra, and Suman Banerjee. Understanding the Limitations of Transmit Power Control for Indoor WLANs . *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, 2007. 2, 3

[49] Shio Kumar Singh, MP Singh, DK Singh, et al. Routing protocols in wireless sensor networks–a survey. *International Journal of Computer Science & Engineering Survey (IJCSES) Vol*, 1:63–83, 2010. 29, 31

[50] Mirko Stoffers and George Riley. Comparing the ns–3 Propagation Models. *Modeling Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), 2012 IEEE 20th International Symposium*, 2012. 52

[51] tutorialspoint. Learn Ipv6. 17, 20, 22

[52] Dr. Ovidiu Vermesan and Dr. Peter Friess. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. 2013. 1

Appendix A

6LowPAN

A.1 Motivation for 6LowPAN

The Internet of Things is a phenomenon that has revolutionized technologies that affect everyday life and has been the triggering point to bring about changes in all the devices that are connected to the internet. The usage of IPv6 in the Internet of Things demands that all the devices be able to adapt to the IPv6 addressing. The Wireless Sensor Network devices represent a major part of the future IoT applications, with billions of information devices being used for sensing, monitoring and controlling a large system. In this case of such large contribution of WSN devices, it is essential that they run a standard networking protocol. The WSN devices which use the 802.15.4 standards (MAC addresses in compatible with IPv6 address), specifically, need to be able to route information, using the network protocol, to any IP enabled device. Some of the important facts about IPv6 and 802.15.4 MAC:

- The IPv6 header is of size 40 Octets
- The UDP header is of size 8 Octets
- The 802.15.4 MAC header can be upto 25 Octets (with no security). If security is included, for example with AES−CCM−128 security of 21 Octets, then maximum header size of 802.15.4 MAC is about 46 Octets.
- The 802.15.4 frame size is of 127 Octets, therefore size left for application data is:

  Without security: 127−25−40−8 = 54 Octets

  With security: 127−46−40−8 = 33 Octets (AES−CCM−128)
- The IPv6 requires that the links established in the network support an MTU of 1280 Octets
- The devices must allow the link-layer mesh routing under the IP-topology as devices may use link-layer multihop (mesh under routing)
- The devices must allow the IP-routing over the 802.15.4 MAC layer (route-over routing)

Based on these facts, it is conclusive that, to use IPv6 and 802.15.4 together, a fragmentation and reassembly layer between the IPv6 and 802.15.4 MAC layers is required.

The advancements in the domains of internet and wireless brings about improved state-of-the-art technology into the market on a regular basis. Thus, using internet over the wireless devices demands that the devices be:

- Inter-operable with all the other potential internet networks, as the information from the wireless devices are not necessarily transferred to other wireless devices, rather would be transferred across a large number of distinct devices over the internet.

- Able to route to device of the IP-domain with different types of security installed over the recipient device.
- Robust and adaptable to external factors such as interference, errant and heterogeneous devices.

The devices should posses the above characteristics and still be able to meet the basic yet critical requirements of a wireless device such as:

- Reliability and adaptability
- Long life and limited amount of energy consumption
- Manage a large number of devices within the same network
- Resource constrained operation

The above requirements strengthen the need for a layer to perform certain duties to make IPv6 over 802.15.4 compatible. This adaptation layer is defined as the 6LowPAN layer between IPv6 and 802.15.4 as shown in the figure A.1. In the simulation of a ZigBee network layer, this layer is equally important to be able to make the use of IPv6 compatible over the 802.15.4 MAC. The section A.2.1 describes the dispatch codes used in 6LowPAN to identify the fragments, section A.2.2 describes the 6LowPAN frame formats and section **??** explains in brief fragmentation and reassembly of frames.

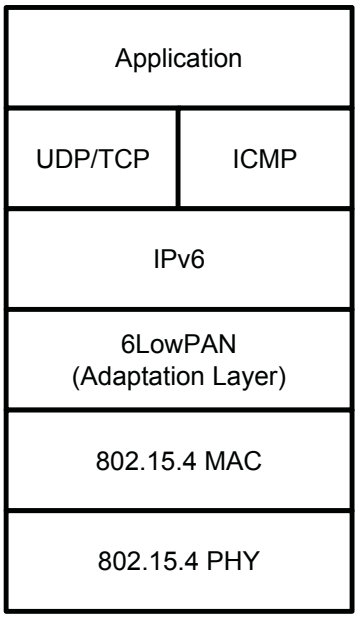

Figure A.1: 6LowPAN adaptation layer between IPv6 and 802.15.4 MAC layers

A.2 6LowPAN frame formats

The 6LowPAN group of the IETF has defined the process for encapsulation and header compression mechanisms for the IPv6 packets to be processed by the 802.15.4 based devices. In the following subsections, the working and functionality of 6LowPAN is explained in brief.

A.2.1 Dispatch codes

The 6LowPAN frames indicate the type of data included in the frame by using dispatch codes. The dispatch codes have predefined meaning as shown in the table A.1.

Table A.1: Dispatch codes of 6LowPAN frames

Bit pattern	Short code	Description
00 xxxxxx	NALP	Not a LowPAN packet
01 000001	IPv6	Uncompressed IPv6 header
01 000010	LowPAN HC1	HC1 compressed IPv6 header
01 010000	LowPAN BC0	BC0 broadcast header
01 111111	ESC	Additional dispatch octets to follow
10 xxxxxx	MESH	Mesh routing header
11 000xxx	FRAG1	Fragmentation header (first)
11 100xxx	FRAGN	Fragmentation header (nth)

The headers in the stack begin with a header type followed by zero or more number of header fields. Every header has the information about the entire frame and the bit pattern stores this information which is decoded on reception and reassembly. The HC1 compression indicates that the header has been compressed, the fragmentation pattern indicate the fragment number of the packet which helps in reassembly. The frame formats for compressed and uncompressed headers are described in the section A.2.2.

A.2.2 Header compression formats

The headers of IPv6 are compressed using the HC1 compression format and here in brief the frame formats for the compression is described for two extreme cases; an uncompressed IPv6 header (worst case scenario) and a fully compressed IPv6 header (best case scenario). The figure A.2 shows the 6LowPAN frame format for a worst case scenario of compression where the IPv6 header remains uncompressed. The dispatch code (as described in section A.2.1) for an uncompressed IPv6 header is $(01000001)_2$. With no security included, 54 octets are available for application payload, whereas with a security; for example AES-CCM-128, 33 octets are available for the application payload. As seen from the figure A.2 the ratio of application payload to header information is really bad. The figure A.3 shows the header compression done by the 6LowPAN header compression

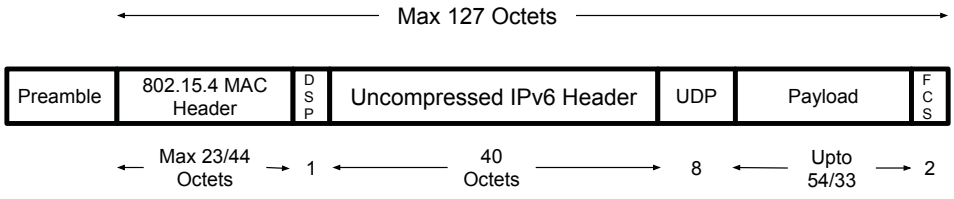

Figure A.2: Uncompressed IPv6 address in a 6LowPAN frame (worst case scenario)

techniques. The dispatch code for HC1 compression is $(01000010)_2$. Without inclusion of security features application payload between 92 and 71 octets are allowed with just HC1 compression, if the frame has HC2 compression too, then between 97 and 76 bytes of payload data can be included. The HC1 compression byte may indicate that the HC2 compression will be followed in

subsequent frames. The figure A.3 shows the maximum compression for link-local acrshortipv6 addresses. Any non-compressible header fields are carried after the HC1 or partial compression tags (HC1/HC2 tags). The basic idea behind the compression is to omit any header fields that can be calculated from the context and send the remaining fields. The compression also supports arbitrary combinations of compression and uncompressed header fields. The acrshortipv6 packets

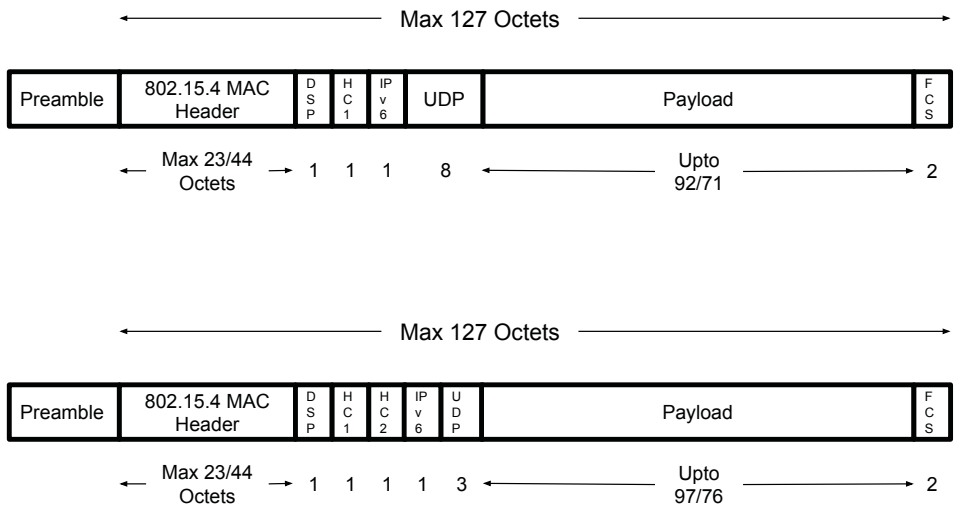

Figure A.3: Compressed IPv6 address in a 6LowPAN frame (best case scenario)

are too large in size to fit into a single 802.15.4 frame, therefore fragmentation is necessary. The first fragment always carries the datagram size and a datagram tag to indicate to which datagram the fragment belongs. The subsequent fragments carry datagram tag, datagram size and the offset of the fragment. This helps in reassembling the packet and request for a re-transmission for the specific lost fragment. The time limit for reassembly is generally 60 seconds.

A.3 Summary

The 6LowPAN turns the 802.15.4 devices into the future IP-enabled links. The 6LowPAN is an open standard which includes TCP, UDP, HTTP, COAP and websockets. It requires no gateway, the router connects the 6LowPAN network to IP. It also supports mesh networking where one-to-one and many-to-one connections, which is robust and scalable. it provides interoperability between low power devices and existing IP devices using standard routing techniques. It also provides a platform for future standardization of communication functions among low power 802.15.4 devices. The 6LowPAN enables the ability to work within resource constraints of low power, low memory, low-bandwidth devices like the WSN.

Appendix B

802.15.4

B.1 Introduction

In today's world we have the premier industries which are globally diversified manufacturers of high quality engineering products and systems. The goal of all the organizations is to add value to the current products and improve the quality of future offerings by introducing wireless technology to enable:

- Increase in productivity
- Improvement in safety
- Better convenience for the end user
- Betterment in reliability of product/service
- An overall low cost system

The vision of the companies is to use a large number of sensors and actuators in a small space which operate wireless. Wireless generally implies that the system operates under low power, with low communication range and with constraints of energy consumption. Furthermore, the system must be self organizing with low cost reliable technology involved in it. Some of the key advantages of wireless include:

- No connectors required
- Flexible connectivity
- Improves resource sharing among devices
- The devices can be installed easily
- The devices can be mobile and still the system functions efficiently

The wireless devices generally operate over low power, mostly battery operated. Therefore these batteries should last long, atleast 3-5 years in the applications of Automotive industry, 5 to 10 years in Industrial applications. Low operation power implies, low range of communication, thereby the network of devices rely on multiple hops to establish end to end communication in the network. The multi-hop networks requires certain protocols to enable the devices to be self-organizing over a network. On any change in the environmental condition or due to physical mobility of devices, the network should be able to adapt to these changes.

The basic challenges at the entry-level of wireless technology are:

- **Frequency of Operation:** The existence of standard and non-standard technologies operating over the ISM band makes the choice of operating frequency difficult. For example, Microwave devices operate at 2.4 GHz, which acts as an hindrance of co-existence and jamming in wireless applications. The spread spectrum technologies is one of the ways to mitigate the issue of co-existence.

- **Interoperability:** The standard and non-standard technologies operate over different layers/structure of implementation, the wireless devices must be able to interoperate with these devices. Despite the presence of large number of standards, the devices must be able to function among all these distinct device technologies.

- **Cost and availability:** The overall cost of the device includes transceiver, chipset, module and external components such as the antenna. The batteries are additional cost if required. The mass manufacture of these devices demand that optimal cost structure be designed for the wireless devices.

On considering all the above challenges, the 802.15.4 standards were defined for the wireless devices which operate on low power and low data rate in the wireless personal area networks. The standard specifies the Media Access Control and Physical layers for the devices. The higher layers can be designed based on the application requirements. Some of the main characteristics of the 802.15.4 are:

- Operational data rates of 250 kbps, 40 kbps, 20 kbps.
- Permits different topologies of operation such as start, mesh, tree, cluster tree.
- Supports low latency devices
- The channel access is controlled by the CSMA/CA mechanism
- The protocol defines full handshake between devices for a reliable communication
- The design focuses on low power consumption
- Offers many frequency bands of operation (channels are smaller divisions of frequency bands)

  16 channels in 2.4 GHz ISM band

  10 channels in 915 MHz ISM band

  1 channel in European 868 MHz band

All these characteristics make the 802.15.4 standard apt for low power wireless devices applications. In section B.2 the protocol architecture is described in brief, where section B.2.2 describes the physical layer standards and section B.2.1 defines the MAC level of the 802.15.4 standard.

B.2 802.15.4 protocol architecture

The devices that use the 802.15.4 standard are designed to conceptually interact with each other over a wireless network. The protocol architecture is as shown in the figure B.1. The 802.15.4 standard defines the lower two layers (MAC and PHY) of the OSI model. The upper layers are dependent on the user specific application requirements. The Logical Link Control (LLC) layer acts as a sublayer to provide multiplexing mechanism that make it possible for several protocol (such as IP) to operate over the MAC layer. The LLC layer can be a combination 802.15.4 defined or any other LLC based on the application requirement. The section B.2.2 describes the PHY layer and section B.2.1 describes the MAC layer of the architecture.

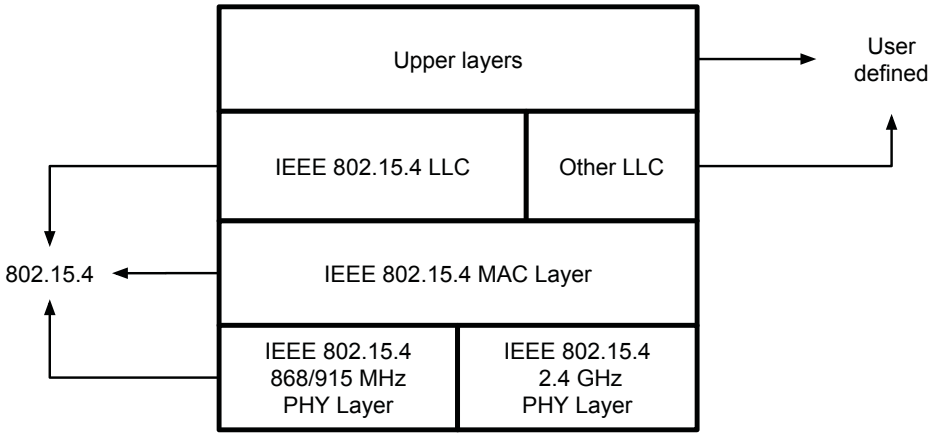

Figure B.1: 802.15.4 standard protocol architecture

B.2.1 Media access control layer

The MAC layer is responsible for transmitting the MAC frames using the PHY layer. It also manages the access to the PHY layer. It controls the frames validation, guaranteed time slots for communication, node associations etc. The MAC layer also has the provision for security measures. The 802.15.4 MAC design drives have the following characteristics:

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range of operation
- Very low power consumption

Overall, the 802.15.4 MAC is a simple yet flexible protocol. The MAC layer of the 802.15.4 permits the following distinct topologies of the network, based on the 2006 standards (as shown in the figure B.2, image taken from [3]):

- **Star topology:** In star topology communication is only between devices and a single central controller termed as the PAN coordinator. If any devices wishes to communicate to any other device over the network, then the communication has to go through the central PAN coordinator. The PAN coordinator can also be a single point of failure, upon which the communication in the network is jeopardized. The PAN coordinator is a Full Function Device (FFD), described later, and the other devices can be either FFD or a RFD. Applications that may use the star topology include the home automation, personal computer, toys, personal health care etc.
- **Peer to Peer topology:** In the peer to peer topology, ever device can communicate with every other device over the network, if possible with a direct connection or over multi hop routes. This could support topologies such as the mesh topology where a more complex routing protocol decides the communication establishment and maintenance. This topology also has a PAN coordinator, but it is different from the start topology as communication can be established between other devices as well. The PAN coordinator helps in establishing the network by allowing nodes to join and leave the network. The applications that can benefit from the peer to peer topology could be industrial controlling systems, wireless sensor networks, intelligent agriculture etc.

There are 2 different types of devices associated with each topology:

- **Full function device:** A FFD is a device that is capable of relaying the messages across the network. It can transmit and receive the messages to any other device in the network. An FFD can operate in three modes, as a PAN coordinator, a coordinator and an end device. If an FFD is the sole device controlling the whole PAN, then it is called as a PAN coordinator. A regular coordinator is used to extend the coverage of network.
- **Reduced function devicea:** A RFD can only speak to an FFD and has the bare minimum functionality to be a part of the network. It does not posses the ability to relay messages across a network. The RFD devices are intended for very simple applications such as a light switch, an infra red sensor etc where there is not much amount of computation.

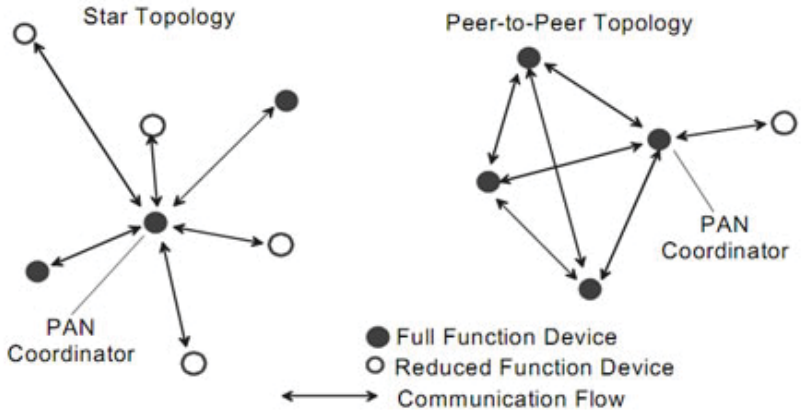

Figure B.2: 802.15.4 MAC permitted topology styles

B.2.2 Physical layer

The PHY layer provides the services for data transmission and reception as well as manage the PHY layer entities. It manages the PHY layer transceiver, performs channel selection, energy management and signal management functions. The PHY layer operates in one of the following three bands as shown in the figure B.3, image taken from [1]. The operational frequency bands are:

- **868 MHz:** The 868 MHz operates on a single channel in the Europe. Based on the standards revision of 2006, the band supports data rates between 100 and 250 kbps. It has four different variations based on the modulation scheme used, three of which use the DSSS and the band of 868 MHz uses either the BSK or the O-QPSK.
- **902-928 MHz:** This band of frequencies operates in different channels each of which have a channel separation of 2 MHz as shown in the figure B.3. This band of frequencies is generally used in devices operating in the continents of America.
- **2.4-2.4835 GHz:** The 2.4 GHz band is used by devices spread across the world, it operates over 16 channels as shown in the figure B.3. Each channel is separated by a channel spacing of 5 MHz between channels 11 and 26.

The general parameters of the 802.15.4 PHY layer are:

- **Transmit power:** The devices are capable of transmitting atleast at 1mW power.

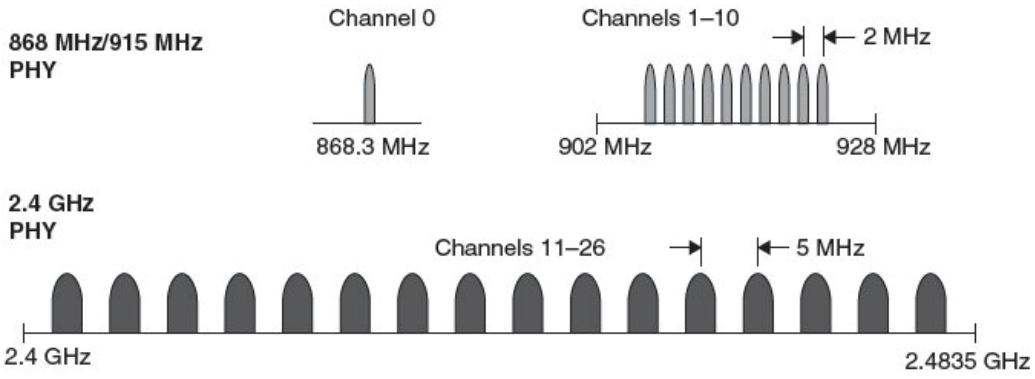

Figure B.3: 802.15.4 PHY layer operating bands of frequency of the RF transceiver

- **Receiver sensitivity:** Based on the operational band of frequency, the receiver sensitivity is −85 dBm and 2.4 GHz of operation and is −92 dBm at 868/915 MHz of frequency band.
- **RSSI measurements:** The RSSI measurements are done to indicate the strength of the received signal, as well as for the process of Clear Channel Assessment (explained in section B.2.1).

As seen from the above information, the 802.15.4 PHY standards are specifically designed for operation at low power and low data rates and are highly suitable for the ZigBee networks as adapted by the ZigBee standard.

B.3 Data transport architecture

The MAC controls the access to the physical layer through certain mechanisms in a structured fashion. The data is transmitted using frames and super frames, the channel access for the frames is granted by a mechanism called as the CSMA/CA. The frames are basic units of communication which are fundamentally of four different types, namely:

- Data frames
- Acknowledgment frames
- Beacon frames
- Command frames

Additionally a superframe structure is defined by the coordinator, two beacons in the superframe act as the limit of the frame helping in synchronization of the devices. The super frame structure is as shown in the figure B.4, image taken from [2]. The superframe consists of 16 slots of equal length, which contains active and inactive parts, used by the coordinator for power saving. The contention for the media access is controlled by the mechanism of CSMA/CA, where two or more frames contest for the access of channel to transmit their information. Every transmission must be ended before the second beacon frame of the super frame structure. In some of the applications, the contention is eliminated to allocated guaranteed time slots, thereby making the access to media during those time slots as contention-less. Superframes are generally used for the low-latency devices that have to be associated with the network even during the inactive periods. if acknowledgments for reception of frames are requested, then acknowledgement messages are sent by the devices.

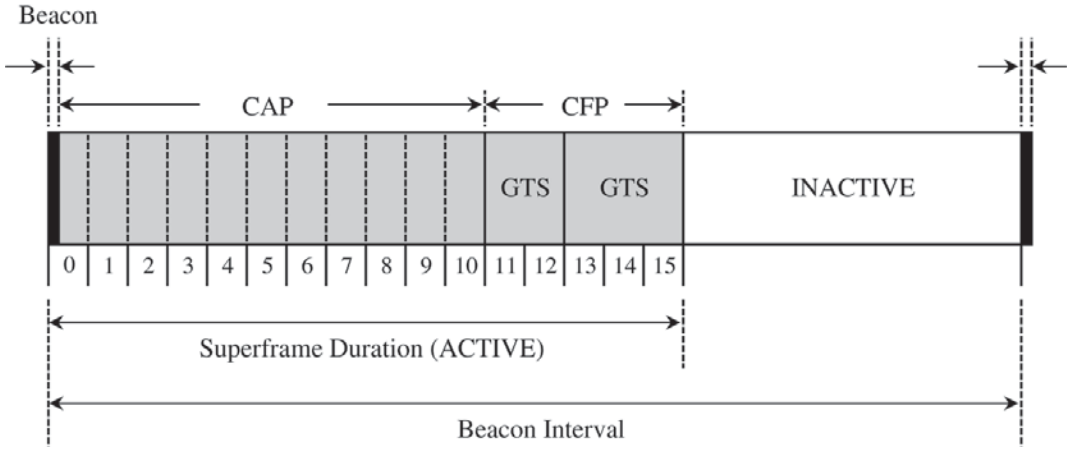

Figure B.4: 802.15.4 Super frame format

The data transport mechanism is designed with simplicity and efficiency by using the super frames and the CSMA/CA mechanism. The flexibility provided by the simple MAC protocol of 802.15.4 has attracted wide range of applications, especially in the ZigBee application profiles, where the ZigBee standard uses the 802.15.4 MAC and PHY layers.

B.4 Security

The 802.15.4 standard from a security perspective is prone to passive eavesdropping problem just like other wireless technologies which could lead to potential active tampering of information. The ad-hoc applications are constrained by many resources and this makes it difficult to include a large barrier of security to prevent any malicious attacks. The devices used have limited capability in terms of storage, transmission power, energy consumption, computation power etc. These constraints limit the security options for the devices. But most of these security aspects are generally taken care by the higher layers and are considered out of scope here.

The cryptographic mechanism in this standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. The cryptographic mechanism provides particular combinations of the following security services:

- **Data confidentiality:** Assurance that transmitted information is only disclosed to parties for which it is intended.
- **Data authenticity:** Assurance of the source of transmitted information (and, hereby, that information was not modified in transit).
- **Replay protection:** Assurance that duplicate information is detected.

These security measures are very minimal and provide protection against outside attacks, but not the malicious devices present within the network.

B.5 Summary

The main features of this standard are network flexibility, low cost, very low power consumption, and low data rate in an adhoc self organizing network among inexpensive fixed, portable and moving devices. It is developed for applications with relaxed throughput requirements which cannot handle the power consumption of heavy protocol stacks. The device comprises a PHY,

which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer. The PHY provides two services: the PHY data service and PHY management service. The PHY data service enables the transmission and reception of PHY protocol data units across the physical radio channel. The MAC sublayer provides two services: the MAC data service and the MAC management service. The features of MAC sublayer are beacon management, channel access, Guaranteed Time Slots management, frame validation, acknowledged frame delivery, association and disassociation. Despite the security is minimum, but it will be taken care by the higher layers designed by the user based on their requirements.

Acronyms

6LowPAN IPv6 Low power Personal Area Network. 3–5, 34, 36, 49, 78, 88–90

AODV Ad-hoc On demand Distance Vector. 4, 5, 28, 32–36, 38–40, 42–45, 49–53, 57–59, 61, 63, 65, 66, 78–81

APDU Application Protocol Data Unit. 10

API Application Program Interface. 48, 50–52

APS Application Support Sub-layer. 8, 9

ARP Address Resolution Protocol. 25

BGP Border Gateway Protocol. 28

BSK Binary Shift Keying. 94

CCA Clear Channel Assessment. 71, 78, 95

CLI Command Line Interface. 47

CSMA Carrier Sense Multiple Access. 60, 62–64, 70

CSMA/CA Carrier Sense Multiple Access/Collision Avoidance. 92, 95

DAD Duplicate Address Detection. 26

DHCP Dynamic Host Configuration Protocol. 25, 28

DHCPv6 Dynamic Host Configuration Protocol version 6. 18, 25, 28

DNS Domain Name System. 28

DSDV Destination Sequence Distance Vector. 31–33

DSR Dynamic Source Routing. 32, 33

DSSS Direct Sequence Spread Spectrum. 94

EUI Extended Unique Identifier. 18

FFD Full Function Device. 11, 12, 93, 94

GUI Graphical User Interface. 47

ICMP Internet Control Message Protocol. 28, 44

ICMPv6 Internet Control Message Protocol version 6. 16, 23–25, 28, 44, 51, 52

IETF Internet Engineering Task Force. 3, 16, 17, 88

iMANET Internet based Mobile Ad hoc Network. 31

IoT Internet of Things. 1, 2, 7, 15, 16, 29, 57, 78, 81, 87

IPv4 Internet Protocol version 4. 1, 4, 5, 15–18, 21, 22, 25, 27, 28, 37, 44, 48, 52, 53, 78

IPv6 Internet Protocol version 6. 1, 3–5, 15–22, 24–28, 34–37, 42–45, 48–53, 57, 58, 78, 81, 87–89

LLC Logical Link Control. 92

Lr-WPAN Low-Rate Wireless Personal Area Network. 7, 52

M-MANET Military Mobile Ad hoc Network. 31

MAC Media Access Control. 3–5, 9, 12, 18, 25–27, 34, 48–50, 52, 53, 60, 61, 70, 78, 80, 81, 87, 88, 92–97

MANET Mobile Ad hoc Network. 31–33

MCPS MAC Common Part Sub-layer. 9

MLME MAC sub-Layer Management Entity. 9

MTU Maximum Transmission Unit. 87

NAT Network Address Translation. 16

NDP Neighbor Discovery Protocol. 5, 16, 18, 25, 26, 28, 51

NLDE Network Layer Data Entity. 9, 10

NLME Network Layer Management Entity. 9, 10

O-QPSK Offset Quadrature Phase Shift Keying. 94

OLSR Optimized link state Routing. 31

OSPF open Shortest Path First. 28

PHY Physical. 3–5, 9, 12, 34, 48–50, 53, 78, 92–96

QoS Quality of Service. 16

RERR Route Error. 41, 42, 44, 45

RFD Reduced Function Device. 12, 93, 94

RIPng Routing Information Protocol next generaion. 28, 51

RREP Route Reply. 36–43, 65

RREPACK Route Reply Acknowledgment. 40, 42, 44

RREQ Route Request. 36–43

RSSI Received Signal Strength Indicator. 95

RSVP Resource reSerVation Protocol. 23, 24

SAP Service Access Point. 9, 10

SLAAC Stateless Address Auto Configuration. 16

SPAN Smart Phone Ad hoc Network. 31

TCP Transmission Control Protocol. 23, 24, 50

UDP User Datagram Protocol. 23, 24, 49, 50, 87

VANET Vehicular Ad hoc Network. 31

VoIP Voice over Internet Protocol. 16

WSN Wireless Sensor Network. 4, 7, 29, 30, 47, 87, 90

ZDO ZigBee Device Object. 8