A Thesis

entitled

Simulation Studies on ZigBee Communications for Home Automation and Networking

by

Prathamesh Ajgaonkar

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Master of Science Degree in Electrical Engineering

Dr. Lingfeng Wang, Committee Chair

Dr. Mansoor Alam, Committee Member

Dr. Vijay Devabhaktuni, Committee Member

Dr. Patricia Komuniecki, Dean
College of Graduate Studies

The University of Toledo

December 2010

An Abstract of
Simulation Studies on ZigBee Communications for Home Automation and Networking

by

Prathamesh Ajgaonkar

Submitted to the Graduate Faculty in partial fulfillment of the requirements for
the Master of Science Degree in Electrical Engineering

The University of Toledo
December 2010

ZigBee is a new wireless technology based on the 802.15.4 standard which is extensively used in wireless communication. It focuses on standardizing and enabling interoperability of various products. It can provide a cost-effective and energy-efficient means for short-range networking. Compared with other wireless communication technologies, it is seen that ZigBee is not only more reliable, but also cheaper and importantly more energy-conservative. ZigBee communication in the field of Home Automation and Networking will be seen. ZigBee is used as a communication medium in home automation and networking. In this study, simulations on Ad hoc On-Demand Distance Vector (AODV) ZigBee routing protocol with different traffic scenarios like CBR, FTP, and Poisson and having different network topologies have been performed. The trace files generated after the simulations are evaluated to calculate parameters like end-to-end packet delay and jitter, which are key parameters in determining QoS. Various types of queue types such as Drop Tail, Stochastic Fair Queue (SFQ), and Random Early Detection (RED) are used to calculate delay and jitter, by taking various traffic scenarios into consideration. The results are then evaluated.

Acknowledgements

I would like to express profound gratitude to my advisor, Dr. Lingfeng Wang, for his generous support, encouragement, supervision and valuable suggestions throughout this research work. I would also like to thank my co advisor Dr. Mansoor Alam for his timely inputs throughout my research. Dr. Mansoor Alam is very approachable and always makes time for me.

My family, friends and well-wishers are with me in spirit everyday and are my strength. I owe everything in my life to my family.

Contents

Abstract	iii
Acknowledgements	iv
Contents	vii
List of Tables	viii
List of Figures	xi
List of Abbreviations	xii
1 Introduction	4
2 ZigBee Standard	5
2.1 Introduction to ZigBee Specification.....	6
2.2 ZigBee Network Characteristics.....	7
2.3 ZigBee Device Types.....	8
2.4 ZigBee Topologies.....	12
2.5 ZigBee Protocol Architecture.....	14
3 ZigBee in Home Automation and Networking	15
3.1 Home Area Network.....	18
3.2 Home Automation.....	18
4 ZigBee Routing Simulations using Network Simulator-2 (ns-2)	19

4.1 Introduction of Network Simulator-2 (ns-2).....	20
4.2 Ad hoc On-Demand Distance Vector (AODV) ZigBee protocol simulations.....	22
4.2.1 AODV simulations for star topology having FTP traffic.....	27
4.2.2 AODV simulations for star topology having CBR traffic.....	31
4.2.3 AODV simulations for star topology having Poisson traffic.....	35
4.2.4 AODV simulations for peer-to-peer topology having FTP traffic.....	40
4.2.5 AODV simulations for peer-to-peer topology having CBR traffic.....	44
4.2.6 AODV simulations for peer-to-peer topology having Poisson traffic.....	47
5 Trace Analysis	49
5.1 End-to-end Packet Delay for CBR Traffic (Drop Tail Queue).....	50
5.2 Jitter in CBR Traffic (Drop Tail Queue).....	51
5.3 End-to-end Packet Delay for FTP Traffic (Drop Tail Queue).....	52
5.4 Jitter in FTP Traffic (Drop Tail Queue).....	53
5.5 End-to-end Packet Delay i.e. delay for Poisson Traffic (Drop Tail Queue).....	54
5.6 Jitter in Poisson Traffic (Drop Tail Queue).....	55
5.7 End-to-end Packet Delay i.e. delay for CBR Traffic (SFQ).....	57
5.8 Jitter in CBR Traffic (SFQ).....	58
5.9 End-to-end packet delay i.e. delay for FTP Traffic (SFQ).....	59
5.10 Jitter in FTP Traffic (SFQ).....	60
5.11 End-to-end packet delay i.e. delay for Poisson Traffic (SFQ).....	61
5.12 Jitter in Poisson Traffic (SFQ).....	62
5.13 End-to-end Packet delay i.e. delay for CBR Traffic (RED).....	63
5.14 Jitter in CBR Traffic (RED).....	64

5.15 End-to-end packet delay i.e. delay for FTP Traffic (RED).....	65
5.16 Jitter in FTP Traffic (RED).....	66
5.17 End-to-end packet delay i.e. delay for Poisson Traffic (RED).....	67
5.18 Jitter in Poisson Traffic (RED).....	68
6 Conclusion and Future Work	72
References	83

List of Tables

2.1 ZigBee, Bluetooth, and Z-wave Characteristics.....	7
5.1 End-to-end Packet Delay and Jitter (Drop Tail Queue).....	69
5.2 End-to-end Packet Delay and Jitter (SFQ).....	69
5.3 End-to-end Packet Delay and Jitter (RED).....	69

List of Figures

2-1 Uses of ZigBee.....	6
2-2 Star topology.....	9
2-3 Mesh topology.....	10
2-4 Tree topology.....	11
2-5 Cluster tree topology.....	12
2-6 ZigBee stack architecture.....	13
3-1 ZigBee enabled Home Area Network (HAN) Architecture.....	17
4-1 NS model where a C++ object has a corresponding OTcl object.....	20
4-2 NS-2 model as seen from a user's outlook.....	20
4-3 The Home Area Network (HAN) setup having FTP Traffic (star topology).....	23
4-4 Partial synchronization of the nodes with coordinator having FTP Traffic (star topology)	24
4-5 Communication between nodes having FTP Traffic (star topology).....	25
4-6 Synchronization of the nodes with coordinator having FTP Traffic (star topology).....	26
4-7 Partial synchronization of the nodes with the PAN coordinator having CBR Traffic (star topology).....	28
4-8 Communication between nodes having CBR Traffic (star topology).....	29
4-9 Synchronization of the nodes with the PAN coordinator having CBR Traffic (star topology).....	

topology).....	30
4-10 Partial synchronization of the nodes with the PAN coordinator having Poisson Traffic (star topology).....	32
4-11 Communication between nodes having Poisson traffic (star topology).....	33
4-12 Synchronization of the nodes with the PAN coordinator having Poisson Traffic (star topology).....	34
4-13 The HAN setup for simulation having FTP Traffic (peer-to-peer topology).....	36
4-14 FTP traffic between node 1 and node 2 (peer-to-peer topology).....	37
4-15 FTP traffic between nodes 3, 4; 5, 6 (peer-to-peer topology).....	38
4-16 FTP traffic between node 7 and node 8 (peer-to-peer topology).....	39
4-17 CBR traffic between node 1 and node 2 (peer-to-peer topology).....	40
4-18 CBR traffic between node 3 and node 4 (peer-to-peer topology).....	41
4-19 CBR traffic between nodes 5 and 6 (peer-to-peer topology).....	42
4-20 CBR traffic between node 7 and node 8 (peer-to-peer topology).....	43
4-21 Poisson traffic between node 1 and node 2 (peer-to-peer topology).....	44
4-22 Poisson traffic between node 3 and node 4 (peer-to-peer topology).....	45
4-23 Poisson traffic between nodes 5, 6; 7, 8 (peer-to-peer topology).....	46
5-1 Delay for CBR Traffic (Drop Tail Queue).....	49
5-2 Jitter in CBR Traffic (Drop Tail Queue).....	50
5-3 Delay for FTP Traffic (Drop Tail Queue).....	51
5-4 Jitter in FTP Traffic (Drop Tail Queue).....	52
5-5 Delay for Poisson Traffic (Drop Tail Queue).....	53
5-6 Jitter in Poisson Traffic (Drop Tail Queue).....	54

5-7 Delay for CBR Traffic (SFQ).....	56
5-8 Jitter in CBR Traffic (SFQ).....	57
5-9 Delay for FTP Traffic (SFQ).....	58
5-10 Jitter in FTP Traffic (SFQ).....	59
5-11 Delay for Poisson Traffic (SFQ).....	60
5-12 Jitter in Poisson Traffic (SFQ).....	61
5-13 Delay for CBR Traffic (RED).....	63
5-14 Jitter in CBR Traffic (RED).....	64
5-15 Delay for FTP Traffic (RED).....	65
5-16 Jitter in FTP Traffic (RED).....	66
5-17 Delay for Poisson Traffic (RED).....	67
5-18 Jitter in Poisson Traffic (RED).....	68

List of Abbreviations

HVAC..... Heating, Ventilating, and Air Conditioning

AMI.....Advanced Metering Infrastructure

HAN..... Home-Area Network

HART.....Highway Addressable Remote Transducer

IETF..... Internet Engineering Task Force

LR-WPAN...low-rate wireless personal-area network

MAC.....Media Access Control

WPANs.....Wireless Personal Area Networks

FFD.....Full Function Device

RFD.....Reduced Function Device

ZTC.....ZigBee Trust Center

MAC..... Media Access Control Layer

APS.....Application Support Sub layer

ZDO.....ZigBee Device Object

CBC.....Cipher Block Chaining

FTP.....File Transfer Protocol

CBR.....Constant Bit Rate

AODV.....Ad-hoc On Demand Distance Vector

WLAN.....Wireless Local Area Network

Chapter 1

Introduction

Wireless technology is fast replacing wired technology in almost all the fields, primarily because it is less costly and also because it is more efficient as compared to wired networks [1]. In a wireless network, there are no cables as in wired network. This is the main difference between them [2, 3]. The main parts of a wireless network are the router and its clients. The router is joined to the internet with the help of a modem. The wireless clients are configured by attaching a wireless card, and thus they can communicate with the router and other devices [4]. Two types of wireless networks exist: Local Area Network (LAN) and Metropolitan Area Network (MAN). A Local Area Network is small in size as compared to a Metropolitan Area Network [5]. In a LAN there are a limited number of computers in the network. A LAN is mostly used in private organizations. In a MAN there are many computers in the network. It is used in places like a large college campus. In general a MAN consists of many LANs [6]. A wireless network has more advantages as compared to its disadvantages. The most prominent advantage is its ability to reach anywhere in the world with minimum cost and time involved [8]. Home Area Network (HAN) deals with the communication between the devices in the home. It can help in energy management by putting the devices to sleep which are no longer required. It tries to minimize the use of devices when there is a peak demand for energy, and tries

to maximize the operation of the devices when energy demand is low [9]. Let us study about ZigBee specification. ZigBee is a new wireless standard which is extensively used in wireless communication. It was developed by the ZigBee Alliance, which is a global network of over 200 foremost original equipment manufacturers i.e. OEMS which help in creating wireless solutions for residence, commercial and industrial applications [11]. It focuses on standardizing and enabling interoperability of various products. The ZigBee specification includes protocols like Ad-hoc On-demand Distance Vector (AODV) and neuRFon which are used in wireless communication between the nodes [12, 13]. Here AODV will be used for conducting simulations. ZigBee protocols are concerned about low power applications which ultimately result in energy conservation. ZigBee is used in low data rate applications which help in cost reduction [14]. It uses three device types: Network Coordinator, Full Function Device, and Reduced Function Device. A network coordinator has more memory and computing power as compared to Full Function device and Reduced Function device [15, 16]. ZigBee supports star, peer-to-peer and cluster tree topologies. The ZigBee protocol architecture consists of many layers like the Physical Layer, Media Access Control (MAC) Layer, Network Layer, Application Support Sublayer (APS), and Application Layer [19, 20]. Now ZigBee security will be taken into consideration. ZigBee is much secured as compared to other technologies, as its security is based on a 128-bit Advanced Encryption Standard (AES) Algorithm which is very difficult to penetrate [21, 22]. ZigBee follows two security modes: Standard Security mode and High Security mode [24]. In most situations High security mode is preferred, as it offers more security as compared to Standard security mode [25, 26]. Network Simulator is based on two languages: C++ and Object Oriented Tool Command language

(OTcl) [27, 28]. ZigBee routing simulations using Network Simulator-2 (ns 2) will be seen [30]. It was observed that many protocols like Bluetooth, Wi-Fi and Z-wave support only one topology i.e. all of these protocols can work smoothly only on a particular concerned topology [31, 32]. This was a major drawback; as if the network followed other topology these communication protocols would be useless. There was a need for a wireless communication protocol which would be suitable for multiple topologies [33]. It was seen that ZigBee specification would be suitable for more than topology [35]. Simulations were then carried out to prove this fact using ns-2 with different scenarios. It was seen through simulations that ZigBee could indeed work on multiple topologies [39, 40]. ZigBee is mainly used in low power applications because, the PHY and MAC layers adopt the standard of IEEE802.15.4, which makes the solutions independent of RF IC vendors due to the 2.4GHz standardized radio by IEEE 802.15.4 [44, 45]. Therefore, ZigBee is more cost-effective for designing short-range wireless communication applications [48]. Based on the PHY and MAC layers, the specifications of ZigBee introduce reliable and secure network topologies, including mesh, star and cluster-tree topology [49, 50]. ZigBee networks have the following requirements and features: low power assumption, low cost, low packet throughput, lots of network nodes, low request on quality of service, security control, and high reliability [51, 52]. The second chapter deals with ZigBee specification. In the third chapter relation between ZigBee Communications and Home Networking along with Home Automation is seen. ZigBee is used to provide an efficient wireless communication standard for Home Area Networking (HAN) devices [55]. They can communicate with each other through ZigBee standard. In home automation, ZigBee can help in supervising resources like electricity, gas, and

water which helps in preservation of energy and also helps in reducing the expenses [59, 60]. People can control Heating, Ventilating, and Air Conditioning (HVAC) applications from anywhere in the house [63, 64]. In the fourth chapter, ZigBee routing simulations using Network Simulator-2 (ns-2) are carried out for different topologies having different traffic setups [69, 70]. In the last chapter trace analysis is carried out with the help of traces file (.tr) which are generated by Tcl files [72, 73]. Parameters like end-to-end packet delay i.e. delay and jitter are determined through trace files for different traffic setups like CBR traffic, FTP traffic, and Poisson traffic having queue mechanisms such as; Drop Tail Queue, Stochastic Fair Queue (SFQ), and Random Early Detection (RED) [75]. The results are then evaluated and corresponding comparisons are made.

Chapter 2

ZigBee Standard

ZigBee is an innovative standard developed by the ZigBee Alliance, primarily for Wireless Personal Area Networks (WPANs). The word ZigBee originates from honeybee “zigzag waggle” dance.

2.1 Introduction to ZigBee Specification

ZigBee mainly aims for low data rate applications and helps in energy conservation. The ZigBee protocol stack is built on top of the IEEE 802.15.4, which defines the Media Access Control (MAC) and physical layers for low-rate wireless personal-area network (LR-WPAN). The ZigBee standard offers a stack profile that defines the network, security, and application layers. The ZigBee specification is an open standard that allows manufacturers to build up their own applications that require low power and low cost.

Figure 2-1 throws some light on the overall uses of ZigBee:

Figure 2-1: Uses of ZigBee

2.2 ZigBee Network Characteristics

Several standards exist for wireless networks like, Wi-Fi, Bluetooth, and WiMax. ZigBee faces competition from such standards. The following are some chief attributes of the ZigBee standard:

- Low battery consumption
- Low data rate
- Low cost
- It supports up to 65,000 nodes in a single network
- It uses small packets as compared to Wi-Fi and Bluetooth
- ZigBee can automatically establish its network

Table 2.1 shows a comparison between ZigBee specification with Z-wave and Bluetooth.

Table 2.1: ZigBee, Bluetooth, and Z-wave Characteristics

Technology/ Properties	Z-wave	Bluetooth	ZigBee IEEE 802.15.4
Application	Residential and commercial applications	Wire replacement	Control and monitoring, sensory applications
Frequency bands	900MHz, 908MHz	2.4GHz	2.4 GHz, 868 MHz, 915MHz
Battery life (days)	Multi-year life	1–7	100–2,000
Security	No security system	Strong security	Security with AES
Bandwidth	9.6 Kbps	700 Kbps	192 Kbps
Range (feet)	300	20	900
Topology	Mesh	Star	Star, tree, cluster tree, and mesh

From the above table it is observed that ZigBee has large battery life as compared to Wi-Fi and Bluetooth. The other main advantage is that it can support multiple topologies, whereas Wi-Fi and Bluetooth support only Tree topology. In addition, a ZigBee end device can be in a sleep mode while keeping its association with the network.

2.3 ZigBee Device Types

ZigBee network primarily uses three device types:

- Network Coordinator
- Full Function Device
- Reduced Function Device

These devices will be discussed as follows:

- **Network Coordinator:** It is the most advanced of the three types and requires maximum memory along with computing power. It has the ability to maintain the overall network knowledge. Each network has exactly one coordinator.
- **Full Function Device:** It can function as a network coordinator if it is supplied with additional memory and computing power. It supports 802.15.4 functions and features which are supported by the standard.
- **Reduced Function Device:** It has limited functionality as compared to network coordinator and full function device. This is primarily done to reduce the cost and complexity. An end device is basically a Reduced Function Device (RFD).

Apart from these device types, a ZigBee network also includes ZigBee trust center (ZTC) which provides security management, security key distribution, and device authentication.

2.4 ZigBee Topologies

ZigBee supports star, peer-to-peer i.e. mesh, tree and cluster tree topologies. They will be discussed in detail as follows:

- **Star Topology:** In the star topology, there are several nodes and a central coordinator. The nodes are in the form of end devices. Here the packet exchange i.e. the communication between the nodes takes place through the coordinator. Whenever a packet is exchanged between two nodes, it has to be routed through the coordinator. The coordinator is the main part of the topology. The main drawback of this topology is the operation of the network depends on the coordinator of the network, and because all packets between devices must go through coordinator, the coordinator may become bottlenecked. The benefit of star topology is that it is uncomplicated and packets go through at most two hops to reach their destination. Figure 2-2 shows Star topology.

Figure 2-2: Star topology

- **Mesh Topology:** It is also called as peer-to-peer topology. Here several nodes communicate independently with each other without the intervention of the coordinator. It is self-healing, i.e. if the path is broken during communication between

two nodes, the nodes can find another path for communication and continue the process. Figure 2-3 shows the Mesh i.e. the peer-to-peer topology.

- **Tree Topology:** The network consists of a central node (root tree), which is a coordinator, several routers, and end devices. The end nodes that are connected to the coordinator or the routers are called children. A special case of tree topology is called a cluster tree topology. Tree topology is shown in figure 2-4.

E- End Device

R-Router

C- Coordinator

Figure 2-3: Mesh topology

E- End Device

R-Router

C- Coordinator

Figure 2-4: Tree topology

Cluster tree topology: It is a special case of tree topology in which a parent along with its children is called a cluster. Each cluster is identified by a different cluster ID. Figure 2-5 shows Cluster tree topology.

E- End Device

R-Router

C- Coordinator

Figure 2-5: Cluster tree topology

2.5 ZigBee Protocol Architecture

The ZigBee protocol architecture is divided into three sections as follows:

- IEEE 802.15.4, which consists of the MAC and physical layers

- ZigBee layers, which consist of the network layer, the ZigBee device object (ZDO), the application sublayer, and security management
- Manufacturer application: Manufacturers of ZigBee devices can use the ZigBee application profile or develop their own application profile

Figure 2-6 shows ZigBee stack architecture.

AO – Application Object

Figure 2-6: ZigBee stack architecture

- Physical Layer performs modulation on outgoing signals and demodulation on incoming signals.
- Medium Access Control (MAC) layer accesses the network by using carrier-sense multiple access with collision avoidance (CSMA/CA), transmits beacon frames for synchronization, and provides reliable transmission.
- The Network Layer starts a new network, manages devices which are leaving or joining the network, and helps in neighbor discovery.
- The application support sublayer (APS) provides the services needed for application objects (endpoints) and the ZigBee Device Object (ZDO) to interface with the network layer for data and management services. It also provides the communication for applications.
 - Application object: An application object is same as the endpoint. It holds an application program and defines the input and output to the APS.
 - ZigBee Device Object (ZDO): A ZigBee Device Object is an application endpoint that performs control and management of application objects.
- Application Layer consists of application objects (endpoints), which hold user applications and ZigBee device objects (ZDOs).

Chapter 3

ZigBee in Home Automation and Networking

ZigBee is a very promising protocol in the upcoming field of Home Automation and Networking. Home Automation and Networking is a component of Smart Grid. Smart Grid means an intelligent power system which deals with the transmission, generation, and distribution of electricity to the consumers. Basically Home Automation and Networking deals with the following terms:

- Home Area Network (HAN)
- Home Automation

ZigBee is involved in these technologies mainly for the low power communication purpose along with other related purposes which will be seen and discussed in depth.

3.1 Home Area Network

ZigBee's primary role is to power the Home Area Network (HAN) and other related networks for residential and commercial purposes. Its main purpose is energy management and energy optimization. It provides an open wireless standard for the HAN enabling device networks like HVAC in order to maintain load control. In the residential

segment there are devices like thermostats, water meters, gas meters, electricity meters, electric vehicle chargers, smoke detectors, security products and other related devices which are connected to each other and communicate with the outside world with the help of ZigBee. It provides a reliable two-way communication between the Advanced Metering Infrastructure (AMI) network and the HAN. ZigBee helps in providing a platform for future customer owned products which control the utility information along with the meter data. With the use of HAN, consumers can have control over their energy usage and can plan the consumption of electricity accordingly, when there is no peak period and cost of energy is low. It supports three types of communications like, consumer specific signaling, control signaling and public price signaling. It helps in setting up communications to other HAN devices. Figures 3-1 shows the ZigBee enabled Home Area Network (HAN) Architecture.

Figures 3-1: ZigBee enabled Home Area Network (HAN) Architecture

As shown in the figure, the ZigBee enabled HAN consisting of the home automation devices communicate with the utility systems with the help of the respective meters. Home Area Network which will be widely used in the future.

3.2 Home Automation

ZigBee is widely used in Home Automation (HA). The HA systems not only provide interoperability between the various devices which are electrical in nature but also help in providing an interactive interface for the people to control and adjust their operations. ZigBee will monitor the accurate usage of electricity, gas and water and thereby help in energy conservation and optimization of these resources. It will reduce the energy expenses through optimized HVAC management. It means that people can easily control and manage applications like lighting, heating and cooling from anywhere in the home.

ZigBee simulations will be taken into consideration. Here Ad-hoc On-Demand Distance Vector (AODV) ZigBee routing protocol will be used for simulations using different topologies like star topology and peer to peer topology having different traffic scenarios like FTP traffic, CBR traffic and Poisson traffic. The simulations will be discussed in the following chapter.

Chapter 4

ZigBee Routing Simulations using Network Simulator-2 (ns-2)

In this chapter, ZigBee routing simulations with the help of Network Simulator-2.34 i.e. ns-2.34 will be discussed. Now prior to that, Network Simulator will be discussed in brief.

4.1 Introduction of Network Simulator-2 (ns-2)

The ns simulator in general covers a large number of applications, of protocols, of network types, of network elements and of traffic models. NS simulator is based primarily on two languages: an object oriented simulator, written in C++, and an OTcl (an object oriented extension of Tool Command language) interpreter, used to execute user's command scripts. Here there are two class hierarchies: the compiled C++ hierarchy and the interpreted OTcl one, with one to one correspondence between them. The following figure 4-1 shows the correspondence between a C++ object and a corresponding OTcl object. The C++ hierarchy allows achieving efficiency in the simulation and faster execution times. With the help of the OTcl script a particular network topology can be defined and implemented. The OTcl makes use of the objects compiled in C++ through an OTcl linkage that creates a matching of OTcl object for each of the C++ object. Basically, ns-2 is a discrete event network simulator. It is mostly used in ad-hoc routing protocol research.

Figure 4-1: NS model where a C++ object has a corresponding OTcl object

From the user's outlook, NS-2 is an OTcl interpreter that takes an OTcl script as input and produces a trace file as output.

Figure 4-2: NS-2 model as seen from a user's outlook

4.2 Ad hoc On-Demand Distance Vector (AODV) ZigBee protocol simulations

In this part, simulations on Ad hoc On-Demand Distance Vector (AODV) routing protocol, which is a ZigBee specification protocol will be performed. It will be performed for two different types of network topologies like star topology and peer-to-peer topology having different traffic scenarios like File Transfer Protocol (FTP) traffic, Constant Bit Rate (CBR) traffic and Poisson traffic. The basis of simulations using different topologies is to prove that ZigBee protocol can work using different topologies. But this is not the case with other communication protocols like Bluetooth and Z-wave which rely only on a single topology and do not support more than one topology. Bluetooth only supports Star topology and Z-wave supports Mesh topology. So consider a situation where nodes are arranged in mesh topology and Bluetooth is to be used. Here Bluetooth cannot be used as it supports only star topology. So in this case, we have to use either ZigBee or Z-wave technology. Consider another situation where nodes are arranged in Star topology and Z-wave communication protocol is to be used for communication between the nodes. Again this will create problem, as Z-wave protocol supports only Mesh topology. So in this case we have to use either Bluetooth or ZigBee. It is seen that ZigBee protocol has a significant advantage over other communication protocols as it is compatible with multiple topologies. Hence it was decided to prove the fact that ZigBee specification is well-suited for different topologies, by performing simulations on AODV routing protocol for star and peer-to-peer topologies. Peer-to-peer topology is based on mesh topology. It is seen that ZigBee works comfortably on both topologies using different traffic scenarios. Simulation screenshots are attached as a proof. The process for the simulations using ns-2 is as follows:

- First of all a scenario file (.scn) is created
- Then a Tcl (Tool Command Language) file (.Tcl) is written
- Then these files are fed to the ns-2 simulator which generates the trace files (.tr) along with the network animator files (.nam) which help in animation of the routing. Screenshots of the deployment result of the .nam file in various scenarios have been attached.

Simulations with star topology will be seen first and afterwards simulations with peer-to-peer topology will be considered.

4.2.1 AODV simulations for star topology having FTP traffic

Simulation of AODV ZigBee protocol for star topology having FTP traffic will be discussed. Here several screenshots of the simulation process have been attached and explained in detail. The following are the screenshots of AODV ZigBee protocol for star topology and having FTP traffic. HAN environment is taken into consideration. In the simulations various components of the HAN like Security and Alarm, Remote Control, Door Control, Environmental Monitoring i.e. Environmental Monit, Meter, Temperature, Motion Detector, Lighting are taken into consideration. All these nodes are managed and controlled by the PAN Coordinator. The following screenshots throw more light on the simulations. Figure 4-3 shows HAN setup having FTP Traffic (star topology).

Figure 4-3: HAN setup having FTP Traffic (star topology)

Figure 4-4 depicts the synchronization of the nodes (shown by green color) with the PAN coordinator, while some nodes are still to be synchronized.

Figure 4-4: Partial synchronization of the nodes with coordinator having FTP Traffic (star topology)

Figure 4-5 depicts communication between node 0 and node 2.

Figure 4-5: Communication between nodes having FTP Traffic (star topology)

Figure 4-6 shows that all nodes are synchronized with the coordinator and communication takes place between node 0 and node 3.

Figure 4-6: Synchronization of the nodes with coordinator having FTP Traffic (star topology)

As seen from the above figures, it is seen that node 0 is the Personal Area Network (PAN) coordinator which coordinates with other nodes. There are in total nine nodes. The AODV ZigBee routing protocol is used. The simulation period is 180 seconds. The X and Y coordinates of topography under consideration is 60 m. The type of traffic is FTP. Consider here all the nodes to be a part of a Home Area Network (HAN). The node 0 acts as a main node as it is a coordinator. Here in order for any node to communicate with each other, it needs first to communicate with the coordinator i.e. node 0, as node 0 then passes this message to the concerned destination node. For example, if node 2 wants to communicate with node 3, then first node 2 has to communicate with node 0 and then node 0 passes the message to node 3. The above HAN configuration is in the form of Star topology. Consider that we have Z-Wave technology available with us for communication between the nodes in the HAN. This technology will not work because Z-Wave only supports mesh topology. Here ZigBee comes into picture as it supports multiple topologies and the simulation proves that ZigBee works successfully on a HAN setup having star topology.

4.2.2 AODV simulations for star topology having CBR traffic

ZigBee routing simulations for star topology having CBR traffic will be considered. The following screenshot explains it in detail. The setup of the HAN environment remains the same as shown in Figure 4-3. Figure 4-7 shows the synchronization of the nodes (shown by green color) with the PAN coordinator, while some nodes are still to be synchronized for a HAN having star topology and CBR traffic.

Figure 4-7: Partial synchronization of the nodes with the PAN coordinator having CBR Traffic (star topology)

Figure 4-8 shows communication between node 0 and node 4.

Figure 4-8: Communication between nodes having CBR Traffic (star topology)

Figure 4-9 shows that all nodes are synchronized with the coordinator and communication takes place between node 0 and node 4.

Figure 4-9: Synchronization of the nodes with the PAN coordinator having CBR Traffic (star topology)

In the above figures node 0 is the PAN coordinator. Here in this scenario also, there are nine nodes. Node 0 controls the communication between various nodes as it is the coordinator. Consider a scenario where HAN is having star topology. Consider that we have Wi-Fi technology for communication between the nodes in the above HAN setup. The nodes will not be able to communicate using Wi-Fi because, it supports only tree topology. The communication will come to a halt. Here ZigBee comes into picture, as it supports star topology. ZigBee can be used for communication in HAN having star topology and having CBR traffic.

4.2.3 AODV simulations for star topology having Poisson traffic

AODV simulations for star topology having Poisson traffic will be seen with the help of screenshots. The setup of the HAN for star topology having Poisson traffic remains the same as shown in Figure 4-3. The following are some of the screenshots.

Figure 4-10 depicts the synchronization of the nodes (shown by green color) with the PAN coordinator, while some nodes are still to be synchronized.

Figure 4-10: Partial synchronization of the nodes with the PAN coordinator having Poisson Traffic (star topology)

Figure 4-11 shows communication between node 0 and node 2.

Figure 4-11: Communication between nodes having Poisson traffic (star topology)

Figure 4-12 shows that all nodes are synchronized with the coordinator and communication takes place between node 0 and node 4.

Figure 4-12: Synchronization of the nodes with the PAN coordinator having Poisson Traffic (star topology)

The above screenshots portray the ZigBee protocol simulation on star topology having Poisson traffic. Here also Node 0 acts as a coordinator. There are total nine nodes here including the coordinator. Poisson traffic is considered which is based on the Poisson model. Let us assume the nodes are arranged in star topology. Here if we assume that 6LoWPAN i.e. IPv6 over Low Power Wireless Personal Area Networks wireless technology is available for communication in the star topology, then it will not work for this topology as 6LoWPAN supports only mesh topology. We have to use ZigBee protocol as it supports many topologies. ZigBee will be able to support the communication in the above HAN setup.

4.2.4 AODV simulations for peer-to-peer topology having FTP traffic

Here ZigBee AODV simulations will be done for peer-to-peer topology. In peer-to-peer topology there is no coordinator, so the nodes can communicate directly. The first screenshot shows the setup of the HAN environment. Here there are various components of HAN like Security and Alarm, Lighting, Motion Detector, Temperature, Meter, Environmental Monitoring i.e. Environmental Monit, Door control, Remote Control and HVAC.

Figure 4-13 shows HAN setup for simulation having FTP Traffic (peer-to-peer topology).

Figure 4-13: The HAN setup for simulation having FTP Traffic (peer-to-peer topology)

Figure 4-14 shows FTP traffic between two nodes (peer-to-peer topology).

Figure 4-14: FTP traffic between node 1 and node 2 (peer-to-peer topology)

Figure 4-15 shows FTP traffic between two pairs of nodes (peer-to-peer topology)

Figure 4-15: FTP traffic between nodes 3, 4; 5, 6 (peer-to-peer topology)

Figure 4-16 shows FTP traffic between nodes (peer-to-peer topology)

Figure 4-16: FTP traffic between node 7 and node 8 (peer-to-peer topology)

Here as seen from the simulation diagrams there is no coordinator to manage the communication between the nodes. Nodes communicate independently with other nodes.

Let us consider that the nodes are a part of a smart grid and they have Bluetooth technology for communication. Now communication will not occur as Bluetooth supports only star topology. So here we have to use the ZigBee technology as it supports peer-to-peer topology.

4.2.5 AODV simulations for peer-to-peer topology having CBR traffic

In this case the HAN setup for simulation remains the same as in the above case. The following are some of the screenshots. Figure 4-17 shows CBR traffic between nodes (peer-to-peer topology).

Figure 4-17: CBR traffic between node 1 and node 2 (peer-to-peer topology)

Figure 4-18 shows CBR traffic between two nodes (peer-to-peer topology).

Figure 4-18: CBR traffic between node 3 and node 4 (peer-to-peer topology)

Figure 4-19 shows CBR traffic between node 5 and node 6 (peer-to-peer topology)

Figure 4-19: CBR traffic between nodes 5 and 6 (peer-to-peer topology)

Figure 4-20 shows CBR traffic between two nodes (peer-to-peer topology).

Figure 4-20: CBR traffic between node 7 and node 8 (peer-to-peer topology)

Consider the nine nodes as a part of a HAN. Let us assume that they use Wi-Fi technology to communicate with each other. But here in this case, the nodes will not be

able to communicate with each other as Wi-Fi supports only tree topology, and does not support peer-to-peer topology. So the solution to this problem is to use ZigBee technology as it supports peer-to-peer topology along with other topologies.

4.2.6 AODV simulations for peer-to-peer topology having Poisson traffic

In this case also the setup remains the same as in the previous cases. Figure 4-21 shows Poisson traffic between nodes (peer-to-peer topology).

Figure 4-21: Poisson traffic between node 1 and node 2 (peer-to-peer topology)

Figure 4-22 shows Poisson traffic between node 3 and node 4 (peer-to-peer topology).

Figure 4-22: Poisson traffic between node 3 and node 4 (peer-to-peer topology)

Figure 4-23 shows Poisson traffic between two pairs of nodes (peer-to-peer topology).

Figure 4-23: Poisson traffic between nodes 5, 6; 7, 8 (peer-to-peer topology)

The above figures depict ZigBee protocol AODV simulation on peer-to-peer topology having Poisson traffic. Here if we consider a scenario where the above HAN has Wibree

technology for communication purpose. This will not work properly because Wibree does not support peer-to-peer topology.

From all the above simulations it is seen that that ZigBee protocol works smoothly on multiple topologies. Out of the two topologies which were taken for consideration, it is seen that peer to peer topology is slightly better than star topology, as in star topology if the coordinator is affected; communication between the nodes comes to a halt. For example if the coordinator stops working due to some internal problems, it will not be able to communicate between the nodes and as a result entire network comes to a standstill. This is not the case in peer to peer topology. In a peer to peer topology, a central coordinator does not exist which controls the entire network. Nodes independently communicate with each other. Here even if the communication between two nodes is affected it will not affect the communication between the other nodes in the network and overall the network runs smoothly.

In the next chapter, analysis of the trace files is taken into consideration for determining parameters like end-to-end packet delay i.e. delay and jitter. In this chapter ZigBee simulations were seen. The simulations were carried out taking different queue types into account like; Drop Tail, Stochastic Fair Queue (SFQ), and Random Early Detection (RED). These queue types will be discussed in the next chapter. The performance of various traffic scenarios like CBR, FTP, and Poisson for getting delay and jitter by taking particular queue type into consideration is evaluated.

Chapter 5

Trace Analysis

The Tcl file helps in the generating the trace file which helps in determining factors like end-to-end packet delay i.e. delay and jitter which are key components in determining the quality of service (QoS). Quality of service is a term which is used to describe the desired service quality. For meeting the standards of the expected quality of service, delay and jitter should be as low as possible. Jitter is defined as deviation in amplitude or width of the pulses in a signal. Jitter can be thought of as shaky pulses. Here delay and jitter are calculated in various scenarios and the observations are discussed.

Case 1:

In the first case, simulations are carried out taking Drop Tail queue type under consideration. Then delay and jitter are calculated for CBR Traffic, FTP Traffic and Poisson Traffic, which are the types of traffic under consideration. The graphical results are obtained and the corresponding results are discussed in detail. Now delay and jitter for CBR traffic will be discussed first. Before that Drop Tail queue type will be seen in brief.

- **Drop Tail Queue**

Drop Tail or Tail Drop is a simple type of queue which is used by routers to decide when exactly to drop packets. Here each packet is treated identically. With Drop tail, when the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough space to accept the incoming traffic. The name “Drop Tail” arises from the effect of the principle on the incoming datagrams. Once a queue has been filled all the additional datagrams are discarded, thus dropping the tail of the sequence of datagrams.

5.1 End-to-end Packet Delay for CBR Traffic (Drop Tail Queue)

Figure 5-1: Delay for CBR Traffic (Drop Tail Queue)

Figure 5-1 shows end-to-end Packet delay i.e. delay for CBR traffic where Drop Tail queue type is considered. The simulation time was 180 sec. It is seen from the figure that delay in seconds for around 1 - 2000 packets is 0.15 seconds. Delay varies from 0.15 sec. to 0.21 sec. for the packets having packet ID from around 2000 to 4500. After that for the remaining packets the delay is again approximately 0.15 sec. On the whole, delay for CBR traffic is around 0.15 seconds.

5.2 Jitter in CBR Traffic (Drop Tail Queue)

Figure 5-2: Jitter in CBR Traffic (Drop Tail Queue)

From figure 5-2 it is seen that Jitter is 0 for time from 0-50 seconds. Between around 50 seconds-120 seconds, jitter varies from around -0.02 to 0.021. Between around 120 seconds-180 seconds, jitter is 0. On the whole, jitter in CBR Traffic is 0.

5.3 End-to-end Packet Delay for FTP Traffic (Drop Tail Queue)

Figure 5-3: Delay for FTP Traffic (Drop Tail Queue)

As seen from the figure 5-3, end-to-end packet delay i.e. delay for packets having packet ID from around 1-8000 varies approximately between 0.12 seconds-0.21 seconds. Delay for packets having packet ID from around 8000-18000 varies approximately between 0.12 seconds and 0.2 seconds. Delay for packets having packet ID from around 18000-25000 varies around between 0.12 seconds and 0.15 seconds. On the whole delay for FTP Traffic is around 0.14 seconds.

5.4 Jitter in FTP Traffic (Drop Tail Queue)

Figure 5-4: Jitter in FTP Traffic (Drop Tail Queue)

As seen from the figure 5-4, Jitter varies between around 0 and 0.018 in the time interval 0 seconds-60 seconds. Between time interval 60 seconds and 120 seconds the jitter is approximately between -0.01 and 0. Between 120 seconds-180 seconds the value of jitter is around 0. On the whole the value of jitter is around 0 and it is seen from the diagram that the value of jitter exponentially increases as the time increases.

5.5 End-to-end Packet Delay i.e. Delay for Poisson Traffic (Drop Tail Queue)

Figure 5-5: Delay for Poisson Traffic (Drop Tail Queue)

As seen from the figure 5-5, delay is around 0.154 seconds for packets having Packet ID from around 1 to 60. Then delay varies from around 0.154 seconds to 0.164 seconds for

packets having ID from around 60 to 80. Delay varies from 0.164 seconds to 0.16 seconds for packets having ID from around 80 to 120. Delay is nearly 0 for packets having ID from around 120 to 200. On the whole delay for Poisson traffic is around 0.154 seconds. As seen from the diagram, delay decreases exponentially as the time increases i.e. delay decreases as number of packets go on increasing.

5.6 Jitter in Poisson Traffic (Drop Tail Queue)

Figure 5-6: Jitter in Poisson Traffic (Drop Tail Queue)

As seen from the figure 5-6, jitter is 0 from time around 0 sec. to 50 sec. After that it varies a lot from around 50 sec. to 110 sec. In that period jitter varies from around -0.01 to 0.008. In the remaining time period jitter is usually 0. On the whole jitter in Poisson Traffic is 0.

Case 2:

In the first case, Drop Tail queue was used in carrying out the simulations. In the second case, the queue type is changed to Stochastic Fair Queue i.e. SFQ. In a similar way delay and jitter are calculated for CBR Traffic, FTP Traffic and Poisson Traffic by taking SFQ under consideration. The graphical results are obtained and the corresponding results are discussed in detail. Delay and jitter for CBR traffic will be discussed first. Before that SFQ queue type will be seen in brief.

- **Stochastic Fair Queue (SFQ)**

Stochastic Fair Queuing (SFQ) is a variation to the Fair Queuing scheme that tries to overrule its limitations. With SFQ, a hash table is used to map packets to corresponding queues. All flows that occur to hash to the same queue are handled in the same way, as if they belong to the same flow. This reduces the number of queues. The main drawback of this method is that flows that collide with other flows are treated unfairly. Hence the fairness guarantees are probabilistic in nature. Hence it is named as Stochastic Fair Queuing. If the size of the hash index is larger than the number of active flows, the probability of unfairness is small.

5.7 End-to-end Packet Delay i.e. Delay for CBR Traffic (SFQ)

Figure 5-7: Delay for CBR Traffic (SFQ)

As seen from the figure 5-7, delay is around 0.16 sec. for packets having ID around 1-1000. Delay varies from 0.18 to 0.16 seconds for packets having ID around 1000-3500. Delay is around 0.16 sec. for remaining of the packets. On the

whole, delay is around 0.16 seconds. As seen from the figure, delay seems to be decreasing as time increases and more packets start flowing.

5.8 Jitter in CBR Traffic (SFQ)

Figure 5-8: Jitter in CBR Traffic (SFQ)

As seen from the figure 5-8, it is seen that Jitter is around 0 for around 0 sec.-30 sec. After that there is a wide variation in Jitter. Jitter varies around -0.015 to 0.015 for around 30 sec.-40 sec. Jitter varies around -0.005 to 0.005 for around 40 seconds to 100 seconds. After that for the remaining time, Jitter is around 0. On the whole, Jitter is around 0.

5.9 End-to-end Packet Delay i.e. Delay for FTP Traffic (SFQ)

Figure 5-9: Delay for FTP Traffic (SFQ)

As seen from the figure 5-9, delay varies from around 0.11 sec. to 0.21 sec. for the packets having ID from around 1-4000. It then varies from around 0.11 sec. to 0.2 sec. for packets having ID from around 4000 to 9000. After that for the remaining packets delay varies from 0.11 sec. to 0.15 sec. On the whole, delay is around 0.14 seconds.

5.10 Jitter in FTP Traffic (SFQ)

Figure 5-10: Jitter in FTP Traffic (SFQ)

As seen from the figure 5-10, in the beginning jitter varies from around 0 to 0.04. For around 5 sec.-30 sec., jitter varies from around 0 to 0.02. Jitter is around -0.005 to 0.008 for time around 30 sec. to 60 sec. After that, Jitter varies around mainly 0 to 0.005 for the remaining time. On the whole Jitter is around 0.002.

5.11 End-to-end Packet Delay i.e. Delay for Poisson Traffic (SFQ)

Figure 5-11: Delay for Poisson Traffic (SFQ)

As seen from the figure 5-11, there is a large variation in delay. For packets having ID from around 1-40, delay is around 0.154 sec. There is a very large deviation in delay for the packets having ID from around 40 to 100. Delay varies from around 0.156 sec. to 0.166 sec. for packets having ID from around 40 to 100. For the remaining packets, delay is around 0.154 sec. On the whole, delay is around 0.155 sec. As seen from the figure, delay decreases exponentially as time increases and more packets start flowing in.

5.12 Jitter in Poisson Traffic (SFQ)

Figure 5-12: Jitter in Poisson Traffic (SFQ)

As seen from the figure 5-12, Jitter is nearly 0 from time around 0 sec. to 30 sec. Then after that, there is a lot of deviation in jitter and it fluctuates a lot. It varies from -0.01 to 0.02 for some time. Then for a brief period from around 45 sec. to 100 sec. the jitter varies around -0.01 to 0.01. Then for the remaining time jitter is nearly 0. On the whole, jitter is 0.

Case 3:

In the third case, the queue type is changed to Random Early Detection i.e. RED. Delay and jitter are calculated for CBR Traffic, FTP Traffic and Poisson Traffic by taking RED under consideration. The graphical results are obtained and the corresponding results are discussed in detail. Delay and jitter for CBR traffic will be discussed first. Before that RED queue type will be seen in brief.

- **Random Early Detection (RED)**

It is also known as random early discard or random early drop. It is an active queue management algorithm. It is similar to a congestion avoidance algorithm. It monitors the queue size and drops packets based on statistical probabilities. It accepts the incoming packets, if the buffer is empty. If a queue starts growing, then it starts to drop incoming packets.

5.13 End-to-end Packet Delay i.e. Delay for CBR Traffic (RED)

Figure 5-13: Delay for CBR Traffic (RED)

As seen from the figure 5-13, delay is around 0.15 seconds in the beginning. For the packets with ID from around 2000-4000, delay varies from 0.2 sec. to 0.16 sec. For the remaining time, delay is around 0.15 seconds. Overall, the delay is around 0.15 seconds.

5.14 Jitter in CBR Traffic (RED)

Figure 5-14: Jitter in CBR Traffic (RED)

From the figure 5-14, it is seen that jitter is 0 for 0 sec. to 50 sec. After that there is deviation in the jitter. It varies from around - 0.02 to 0.02 for around 50 sec. to 55 sec. After this till 100 sec. jitter varies from -0.005 to 0.005. For the remaining time jitter is 0. On the whole jitter is 0.

5.15 End-to-end Packet Delay i.e. Delay for FTP Traffic (RED)

Figure 5-15: Delay for FTP Traffic (RED)

From the figure 5-15, it is seen that delay varies from around 0.11 sec. to 0.15 sec. for majority of the time apart from some time in beginning where delay is around 0.2 sec. On the whole delay is around 0.145 sec.

5.16 Jitter in FTP Traffic (RED)

Figure 5-16: Jitter in FTP Traffic (RED)

It is seen from the figure 5-16 that Jitter is high in the beginning. It is in the range of 0.04. After that till around 40 sec. jitter varies from around 0 to 0.02. From around 50 sec. to 100 sec. jitter varies from around -0.01 to 0.01. For the remaining time it is around 0. On the whole jitter is around 0.

5.17 End-to-end Packet Delay i.e. Delay for Poisson Traffic (RED)

Figure 5-17: Delay for Poisson Traffic (RED)

From the figure 5-17, it is seen that delay is around 0.154 sec. for the first 60 packets. After that there is a wide deviation in the delay. It varies from around 0.155 sec. to 0.16 sec. for the packets having ID from around 60 to 100. After that the delay is again 0.154 sec. for the remaining time. On the whole delay is around 0.154 sec. It is also seen that delay decreases exponentially as the time increases and more packets start coming in.

5.18 Jitter in Poisson Traffic (RED)

Figure 5-18: Jitter in Poisson Traffic (RED)

From the above figure 5-18 it is seen that jitter is 0 from 0 sec. to 60 sec. After that there is deviation in jitter on a large scale. It varies from -0.006 to 0.006 between 60 sec. and 100 sec. After that, for the remaining time the jitter is 0. Overall the jitter is 0.

The following tables summarize the results:

- **For Drop Tail Queue**

Table 5.1: End-to-end Packet Delay and Jitter (Drop Tail Queue)

	End-to-end Packet Delay i.e. Delay (sec)	Jitter
CBR Traffic	0.15	0
FTP Traffic	0.14	0
Poisson Traffic	0.154	0

- **For Stochastic Fair Queue (SFQ)**

Table 5.2: End-to-end Packet Delay and Jitter (SFQ)

	End-to-end Packet Delay i.e. Delay (sec)	Jitter
CBR Traffic	0.16	0
FTP Traffic	0.14	0.002
Poisson Traffic	0.155	0

- **For Random Early Detection (RED)**

Table 5.3: End-to-end Packet Delay and Jitter (RED)

	End-to-end Packet Delay i.e. Delay (sec)	Jitter
CBR Traffic	0.15	0
FTP Traffic	0.145	0
Poisson Traffic	0.154	0

From the above tables for various queue types it is seen that there is some jitter in FTP Traffic when SFQ is considered. Apart from this, jitter is 0 when remaining queues are considered. Maximum delay of 0.16 sec. is observed for CBR traffic when SFQ is considered.

Chapter 6

Conclusion and Future Work

➤ Conclusion

- From the simulations it is seen that ZigBee protocol works efficiently on more than one topology, which is not the case with most other protocols like Bluetooth, Wi-Fi and Z-wave. This is its main advantage over other protocols, as it can support many topologies without any difficulty. So ZigBee can be used in Home Automation and Networking irrespective of the network topology.
- Following are some of the prospects of ZigBee communication in smart grid enabled homes:

➤ *Energy conservation*

- Energy cost can be controlled by automated systems to conserve energy.

➤ *Control*

- Automated control of the household appliances
- Devices can be controlled from anywhere in the house

➤ *Safety*

- Different types of devices can be linked into a single system which enhances the security

- Wi-Fi is a key wireless networking technology for the home environment along with ZigBee. Collaboration of ZigBee and Wi-Fi for Home Area Networking and Automation applications can help in increasing the efficiency of the operations by implementing energy saving schemes, as primarily both these protocols aim in energy conservation. Combination of these technologies will ultimately benefit the customers, as it will help in energy management which will result in cost reduction.
- When various queue types are taken into consideration while calculating jitter for various types of traffic scenarios like CBR, FTP, and Poisson, it is seen that there exists jitter of 0.002 in FTP traffic when SFQ queue type is considered.
- Delay of 0.16 sec. is observed for CBR traffic when SFQ is considered. This is the maximum delay recorded in the observations.
- Drop Tail queue and Random early Detection (RED) should be given preference over SFQ queue type, as SFQ in general exhibits jitter as well as large delay which decreases the QoS.
- Delay and jitter for Drop Tail and RED are nearly the same.
- FTP traffic exhibits the jitter, while CBR and Poisson traffic do not have jitter.

➤ **Future Work**

- In ZigBee emphasis is given on reliability and security. In achieving these features speed is compromised. Methods should be derived to increase the speed, so that overall efficiency of ZigBee related applications is improved.
- In ZigBee mesh networks, router nodes must be powered on at all times which can limit the lifetime of battery-powered ZigBee networks. Power saving mechanisms need to be implemented to increase the lifetime of the nodes.
- Out of the three queue types, it is seen that when Stochastic Fair Queue (SFQ) is used there is jitter and large delay as compared to Drop Tail queue and Random Early Detection (RED) queue. Reasons should be found out for this issue which can help in reducing jitter and delay for SFQ.

References

- [1] **Baronti P, Pillai P, Chook V, Chessa S, Gotta A, Hu Y**, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. Communications 2007; 30: 1655–1695.
- [2] **Ahamed R**, THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA COMMUNICATION SYSTEM. Journal of Theoretical and Applied Information Technology 2009; 129-135.
- [3] **Gorday P, Hester L, Callaway E**, Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks. IEEE Communications Magazine 2002; 70-78.
- [4] ZigBee: The Choice for Energy Management and Efficiency - ZigBee White Paper - June 2007.
- [5] **Bhambri P, Jindal C, Bathla S**, Future Wireless Technology-ZIGBEE. Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT) 2007; 154-156.
- [6] Getting Started with ZigBee and IEEE 802.15.4, Daintree Networks 2008.
- [7] zigbee/ZigBee.htm: Wikipedia
- [8] www.zigbee.org
- [9] **P. Kinney**, ZigBee Technology: Wireless Control that Simply Works, White Paper dated 2 October 2003

- [10] **Sheng-Fu Su**, The Design and Implementation of the ZigBee Protocol Driver in Linux, White Paper dated 26 July 2005.
- [11] IEEE 802 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, IEEE Computer Society, 2003.
- [12] ZigBee Specification v1.0, ZigBee Alliance, December 14th, 2004.
- [13] **Kohvakka, M., Kuorilehto, M., Hännikäinen, M., & Hännikäinen, T. D** (2006). Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications. Paper presented at the Proceedings of the 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Terromolinos, Spain. 48-57.
- [14] **Gorbis, M., & Pescovitz D**, (2006). IEEE fellow's survey: Bursting tech bubbles before they balloon. *IEEE Spectrum*, 43(9), 50-55.
- [15] **Tseng, Y., & Pan M**, (2006). Quick convergecast in ZigBee/IEEE 802.15.4 tree based wireless sensor networks. *MobiWac '06: Proceedings of the international workshop on Mobility management and wireless access*, 2006, 60-66.
- [16] **Ran, P., Sun, M., Zou Y**, (2006). ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing. *APSCC '06*, December 2006, 400-404.
- [17] **Chen, B., Wu, M., Yao, S., & Binbin N**, (2006). ZigBee technology and its application on wireless meter reading system. *Industrial Informatics, 2006 IEEE International Conference on*, August 2006, 1257-1260.
- [18] **Ibrahim E**, (2009). Southern California Smart Grid research Symposium, April 2009.

- [19] **Varchola, M., Drutarovsky M**, (2007). ZigBee based Home Automation Wireless Sensor Network, 2007, 4.
- [20] **Osipov M**, (2008). Home Automation with ZigBee, Springer-Verlag Berlin Heidelberg, 2008, 263-270.
- [21] **Pelletier J**, (2009). ZigBee-Powered Smart Grids: Coming to a Home near you, 2009.
- [22] **Carcelle, X., Heile, B., Chatellier, C., Pailler P**, (2007). Next WSN applications using ZigBee, 2007, 239-254.
- [23] Going green with AMI and ZigBee Smart Energy. Daintree Networks 2008.
- [24] **Ocenasek P**, (2009). Towards Security Issues In ZigBee Architecture, 2009, 587-593.
- [25] **Bapat, J., Koomullil, G., Lakshmi A**, Data Communication over the Smart Grid, IEEE 2009, 273-279.
- [26] **Bennett, C., Highfill D**, Networking AMI Smart Meters, IEEE Energy 2030, November 2008, 1-8.
- [27] **Bauer, M., Dostert, K., Wang C**, Packet-Oriented Communication Protocols for Smart Grid Services over Low-Speed PLC, IEEE 2009, 89-94.
- [28] **Cleveland, F.M.**, Cyber Security Issues for Advanced Metering Infrastructure, IEEE 2008.
- [29] **O.B. Akan, I.F. Akyildiz**, Event-to-sink reliable transport in wireless sensor networks, IEEE/ACM Transactions on Networking 13 (5) (2005) 1003–1016.
- [30] **I.F. Akyildiz, W.J. Su, Y. Sankarasubramaniam, E. Cayirci**, A survey on sensor networks, IEEE Communications Magazine (2002) 102–114.

- [31] **I.F. Akyildiz, W.J. Su, Y. Sankarasubramaniam, E. Cayirci**, Wireless sensor networks: a survey, *Computer Networks* 38 (2002) 393–422.
- [32] **M. Aly, K. Pruhs, P.K. Chrysanthis**, **KDDCS**: a load-balanced innetwork data-centric storage scheme for sensor networks, in: *Proceedings of the 15th ACM International Conference on Information and Knowledge Management (CIKM 2006)*, November 2006, pp. 317–326.
- [33] **G. Amato, S. Chessa, F. Conforti, A. Macerata, C. Marchesi**, Health care monitoring of mobile patients, *Ercim news* (n. 60) (2005). G. Amato, P. Baronti, S. Chessa, **MaD WiSe**: programming and accessing data in a wireless sensor network, in: *International Conference on Computer as a Tool (EUROCON 2005)*, November 2005, pp. 1846–1849.
- [34] **G. Amato, P. Baronti, S. Chessa, V. Masi**, The Stream System: a data collection and communication abstraction for sensor networks, in: *2006 IEEE International Conference on Systems, Man, and Cybernetics*, October 2006.
- [35] **G. Amato, P. Baronti, S. Chessa**, **MaD-WiSe**: a distributed query processor for wireless sensor networks, Technical Report ISTI-2006- TR-39.
- [36] **A. Bachir, D. Barthel, M. Heusse, A. Duda**, Hidden node avoidance in wireless sensor networks, in: *International Conference on Wireless Networks, Communications and Mobile Computing*, Volume 1, 2005, pp. 612–617.
- [37] **M. Bahramgiri, M.T. Hajiaghayi, V.S. Mirrokni**, Fault-tolerant and 3-dimensional distributed topology control algorithms in wireless multi-hop networks, in: *Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN02)*, Miami, FL, 14–16 October 2002, pp. 392–397.

- [38] **L. Bao, J.J. Garcia-Luna-Aceves**, A new approach to channel access scheduling for ad hoc networks, in: The Proceedings of the 7th International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy, July 2001, pp. 210–221.
- [39] **C. Bettstetter**, On the minimum node degree and connectivity of a wireless multihop network, in: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, Switzerland, July 2001, 2002.
- [40] **V. Bharghavan, A. Demers, S. Shenker, L. Zhang**, MACAW: a media access protocol for wireless LAN's, in: Proceedings of the ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, London ,UK, August September 1994, pp. 212–225.
- [41] **D. Blough, M. Leoncini, G. Resta, P. Santi**, The K-neigh protocol for symmetric topology control in ad hoc networks, in: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Annapolis, MD, 2003.
- [42] **P. Bonnet, J. Gehrke, P. Seshadri**, Querying the physical world, IEEE Personal Communications 7 (5) (2000) 10–15. P. Bonnet, J. Gehrke, P. Seshadri, Towards sensor database systems, in: Proceedings of the 2nd International Conference on Mobile Data Management (MDM 2001), Hong Kong, China, January 2001, pp. 3–14.
- [43] **P. Bose, P. Morin, I. Stojmenovic, J. Urrutia**, Routing with guaranteed delivery in ad hoc wireless networks, Wireless Networks 7 (6) (2001) 609–616.
- [44] **B. Bougard, F. Catthoor, D.C. Daly, A. Chandrakasan, W. Dehaene**, Energy efficiency of the IEEE 802.15.4 standard in dense wireless microsensor networks: modeling and improvement perspectives, in: Proceedings of Design, Automation, and Test in Europe (DATE), March 2005.

- [45] **J. Brack, J. Gao, A. (Andrew) Jiang**, MAP: medial axis based geometric routing in sensor networks, in: Proceedings of the 11th International Conference on Mobile Computing and Networking (MobiCom 2005), Cologne, Germany, August–September 2005, pp. 88–102.
- [46] **BTnodes** - A Distributed Environment for Prototyping Ad Hoc Networks.
- [47] **N. Bulusu, J. Heidemann, D. Estrin**, GPS-less low cost outdoor localization for very small devices, IEEE Personal Communications Magazine 7 (5) (2000) 28–34.
- [48] **S.A. Camtepe, B. Yener**, Key distribution mechanisms for wireless sensor networks: a survey, Technical Report TR-05-07, Rensselaer Polytechnic Institute, March 23, 2005.
- [49] **Q. Cao, T. Abdelzaher**, Scalable logical coordinates framework for routing in wireless sensor networks, in: Proceedings of the 25th IEEE International Real-Time Systems Symposium (RTSS 2004), Lisbon, Portugal, December 2004, pp. 349–358.
- [50] **S. Capkun, M. Hamdi, J.-P. Hubaux**, GPS-free positioning in mobile ad-hoc networks, in: Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS 2001), Maui, HI, USA, January 2001, pp. 3481–3490.
- [51] **A. Caruso, S. Chessa, S. De, A. Urpi**, GPS free coordinate assignment and routing in wireless sensor networks, in: Proceedings of the 24th Joint Conference of the IEEE Computer and Communications Societies (Infocom 2005), Miami, FL, USA, March 2005, pp. 150–160.
- [52] **A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, J. Zhao**, Habitat monitoring: application driver for wireless communications technology, in: Proceedings

of the 1st ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, San Jose, Costa Rica, April 2001, pp. 20–41.

[53] **B. Chen, K. Jamieson, H. Balakrishnan, R. Morris**, Span: an energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks, *ACM Wireless Networks Journal* 8 (5) (2002) 481–494.

[54] **T. Van Dam, K. Langendoen**, An adaptive energy-efficient mac protocol for wireless sensor networks, in: *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys 2003)*, Los Angeles, CA, USA, November 2003, pp. 171–180.

[55] **J.R. Douceur**, The Sybil attack, in: *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS02)*, 2002.

[56] **C.C. Enz, A. El-Hoiydi, J.-D. Decotignie, V. Peiri**, WiseNET: an ultralow-power wireless sensor network solution, *Computer* 37 (8) (2004) 62–70.

[57] **L. Eschenauer, V.D. Gligor**, A key management scheme for distributed sensor networks, in: *Proceedings of the 9th ACM conference on Computer and Communications Security (CCS02)*, Washington, November 2002, pp. 41–47.

[58] **Q. Fang, J. Gao, L.J. Guibas**, Locating and bypassing routing holes in sensor networks, in: *Proceedings of the 23th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom 2004)*, Hong Kong, March 2004, pp. 2458–2468.

[59] **Q. Fang, J. Gao, L.J. Guibas, V. de Silva, L. Zhang**, GLIDER: gradient landmark-based distributed routing for sensor networks, in: *Proceedings of the 24th Annual Joint*

Conference of the IEEE Computer and Communications Societies (Infocom 2005), Miami, FL, USA, March 2005, pp. 339–350.

[60] **R. Fonseca, S. Ratnasamy, J. Zhao, C. Tien Ee, D. Culler, S. Shenker, I. Stoica**, Beacon vector routing: scalable point-to-point routing in wireless sensornets, in: Proceedings of the 2nd Symposium on Networked Systems Design & Implementation (NSDI 2005), Boston, MA, USA, May 2005.

[61] **D. Ganesan, R. Govindan, S. Shenker, D. Estrin**, Highly-resilient, energy-efficient multipath routing in wireless sensor networks, ACM SIGMOBILE Mobile Computing and Communications Review 5 (4) (2001) 11–25.

[62] **T. Gao, D. Greenspan, M. Welsh**, Improving patient monitoring and tracking in emergency response, in: Proceedings of the International Conference on Information Communication Technologies in Health, July 2005.

[63] **G. Gaubatz, J. Kaps, B. Sunar**, Public Key Cryptography in sensor networks – revisited, in: Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[64] **D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, D. Culler**, The nesC language: a holistic approach to networked embedded systems, in: Proceedings of the ACM SIGPLAN conference on programming language design and implementation (PLDI 2003), San Diego, CA, USA, June 2003, pp. 1–11.

[65] **L. Girod, D. Estrin**, Robust range estimation using acoustic and multimodal sensing, in: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2001), Maui, HI, USA, October–November 2001, pp. 1312–1320.

- [66] **P. Gupta, P.R. Kumar**, Critical power for asymptotic connectivity in wireless networks, in: W.M. McEneaney, G. Yin, Q. Zhang (Eds.), *Stochastic Analysis, Control, Optimisation and Applications*, Birkhauser, Boston, M.A, 1998, pp. 547–566.
- [67] **A. Hac**, *Wireless Sensor Network Designs*, John Wiley, New York, 2003.
- [68] **T. He, C. Huang, B.M. Blum, J.A. Stankovic, T. Abdelzaher**, Range-free localization schemes for large scale sensor networks, in: *Proceedings of the 9th International Conference on Mobile Computing and Networking (MobiCom 2003)*, San Diego, CA, USA, September 2003, pp. 81–95.
- [69] **J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, K.S.J. Pister**, System architecture directions for networked sensors, in: *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-IX)*, Cambridge, MA, USA, November 2000, pp. 93–104.
- [70] **B. Hohlt, L. Doherty, E. Brewer**, Flexible power scheduling for sensor networks, in: *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN 2004)*, Berkeley, CA, USA, April 2004, pp. 205–214.
- [71] **H. Karl, A. Willig**, *Protocols and Architectures for Wireless Sensor Networks*, John-Wiley, New York, 2005.
- [72] **Y.-C. Hu, A. Perrig, D.B. Johnson**, Packet leashes: a defense against wormhole attacks in wireless networks, in: *Proceedings of the 22nd Joint Conference of the IEEE Computer and Communications Societies (Infocom)*, 2003.
- [73] **Z. Huang, C. Shen, C. Srisathapornphat, C. Jaikaeo**, Topology control for ad hoc networks with directional antennas, in: *Proceedings of the IEEE International Conference in Computer Communication and Networks (ICCCN02)*, Miami, FL, 14–16 October

2002, pp. 392–397.

[74] **L.-J. Hwang, S.-T. Sheu, Y.-Y. Shih, Y.-C. Cheng**, Grouping strategy for solving hidden node problem in IEEE 802.15.4 LRWPAN, in: Proceedings of 1st International Conference on Wireless Internet, July 2005, pp. 26–32.

[75] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4-2003 “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), New York, IEEE Press. October 1, 2003.

[76] **C. Intanagonwiwat, R. Govindan, D. Estrin**, Directed diffusion: a scalable and robust communication paradigm for sensor networks, in: Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, USA, August 2000, pp. 56–67.

[77] **D.B. Johnson, D.A. Maltz**, Dynamic source routing in ad hoc wireless networks, Mobile Computing, vol. 353, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.

[78] **X. Ji, H. Zha**, Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling, in: Proceedings of the 23th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom 2004), Hong Kong, March 2004, pp. 2652–2661.

[79] **J.M. Kahn, R.H. Katz, K.S.J. Pister**, Next century challenges: mobile networking for “Smart Dust”, in: Proceedings of the 5th International Conference on Mobile Computing and Networking (MobiCom 1999), Seattle, WA, USA, August 1999, pp. 271–278.

- [80] **R. El Kaissi, A. Kayssi, A. Chehab, Z. Dawy, DAWWSEN:** a defence mechanism against wormhole attacks in wireless sensor networks, in: Proceedings of the 2nd International Conference on Innovations in Information Technology (IIT'05), Dubai, UAE, September 2005.
- [81] **B. Karp, H.T. Kung,** GPSR: greedy perimeter stateless routing for wireless networks, in: Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, USA, August 2000, pp. 243–254.
- [82] Wikipedia: Network Simulator-2 (NS-2).