4/12/2012

ENSC 427 SPRING 2012

Communication Networks

Long Fei Zhao lfz2@sfu.ca
Jordan Angelov jga21@sfu.ca
StoyanPetrov svp1@sfu.ca

http://www.sfu.ca/~lfz2/index3.html

Evaluation of ZigBee Remote Sensor Networks

ENSC 427 SPRING 2012

Communication Networks

Contents

List of Figures

Figure of Tables

Glossary

APS - Application Support Sublayer

APSDE - Application Support Sublayer Data Entity

APSME- Application Support Sublayer Management Entity

DoS - Denial of Service Attack

ETED- End to End Delay

FIFO First in First out

IPM- Industrial plant monitoring

MAC- Medium Access Control

PAN Personal Area Network

PL- Packet Loss

PDU - Protocol Data Units

RF- Radio Frequency

WSN- Wireless Sensor Network

ZDO- ZigBee Device Object

Abstract

ZigBee is a wireless technology designed to address the unique needs of low-cost, low-power wireless sensor and control networks in any market. Zigbee's "reliable wireless performance and battery operation"[1] makes it ideal for remote sensor networks operating on limited battery power. This project will simulate and explore ZigBee sensor networking using OPNET to study the performance fluctuation of a moderate size network with gradual increase in the number of nodes.

1.0 Introduction

Remote sensor networks offer great flexibility, diversity and potential in many areas of science and engineering. With implementation of ZigBee protocol, and the ability to transmit variable data from an area of interest at a low power, and low cost is an attractive solution in many fields of study and research.

To show that ZigBee technology has seen a gradual incline of popularity, a market research firm, West Technology Research Solutions estimates that the ZigBee market faces an "annual shipments for ZigBee chipsets into the home automation segment alone will exceed 339 million units,"[2] and will show up in "light switches, fire and smoke detectors, thermostats, appliances in the kitchen, video and audio remote controls, landscaping, and security systems."[3]

ZigBee is a category in the IEEE 802 family, along with other popular protocols such as Wi-Fi, Bluetooth, which uses the 2.4 GHz industrial, and scientific and medical (ISM) radio band. However, unlike Wi-Fi and Bluetooth, ZigBee was developed for low power which features long battery life by having lower transfer rates. In applications where a requirement for fast transfer speed is not necessarily essential, ZigBee protocol is an ideal choice due to the low cost implementation that allows the technology to be widely deployed.

2.0 ZigBee Overview

The table below shows the compare and contrast between the three very similar technology of ZigBee, Wi-Fi, and Bluetooth.

	ZigBee	Wi-Fi (802.11n)	Bluetooth
Data Rate	**20,40 and 250 Kbps**	up to 150Mbps	1Mbps
Range	**10-3000m**	70-250m	10-100m
Frequency	**868MHz, (EU)** **900-928MHz, (NA)** **2.4GHz (WL)**	2.4 & 5 GHz	2.4GHz
Complexity	**Low**	High	High
Battery Life (days) [3]	**100 to > 1000**	1 to 5	1 to 7

Table 2.1 Summarizes the features of ZigBee, Wi-Fi and Bluetooth protocols

ZigBee is applicable for low data rate monitoring and control applications in virtually every industry worldwide. ZigBee's primary advantage is the ability to fit into cheap and widely available 8-bit microcontrollers. This allows developers to spend less time developing and debugging with complicated hardware. ZigBee achieves this minimal design by using lower data rates compared to other protocols. Figure 2.1 compares ZigBee with other popular wireless network protocols for Data Rate v.s Range [4]. It is observed that the ZigBee is ideal for low rate applications requiring moderate range.

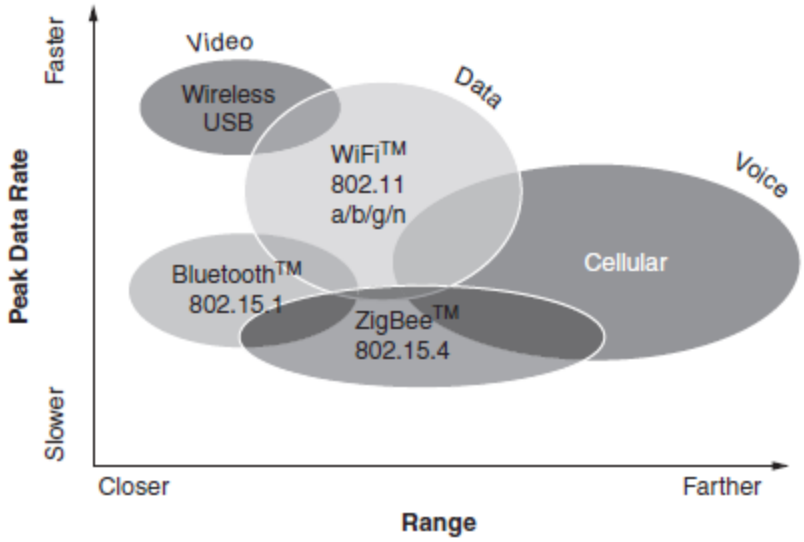

Figure 2.1 Different Network Toplogies [4]

As an example, Industrial Plant Monitoring (IPM) is a perfect application for the ZigBee technology.

ZigBee Wireless sensing and control networks provide accurate and efficient IPM, and are also ideal to deploy in hazardous environments in which you want to minimize human exposure. Advantages of choosing ZigBee in this WSN would include features such as:

- Extend existing manufacturing and process control systems reliably, improve asset management by continuously monitoring critical equipment.[5]
- Automate data acquisition from remote sensors to reduce user intervention.[5]
- Deploy monitoring networks to enhance employee and public safety.[5]
- Obtain accurate readings from pressure sensors, smoke detectors, meters, gauges, and other safety devices, and identify potential problems earlier.[5]
- Remotely monitor hazardous areas that may previously have been as too dangerous for manual monitoring.[5]

2.1 ZigBee Architecture

The ZigBee protocol consists of four critical layers. The top two layers, Application and Network layer (see figure below) are outlined by the ZigBee Alliance to provide the necessary manufacturing standards. The bottom two are Medium Access Control and Physical layer (see figure below) ,their specifications are provided by the IEEE 802.15.4-

2006 standard to ensure coexistence without interference with other wireless protocols such as Wi-Fi and Bluetooth.

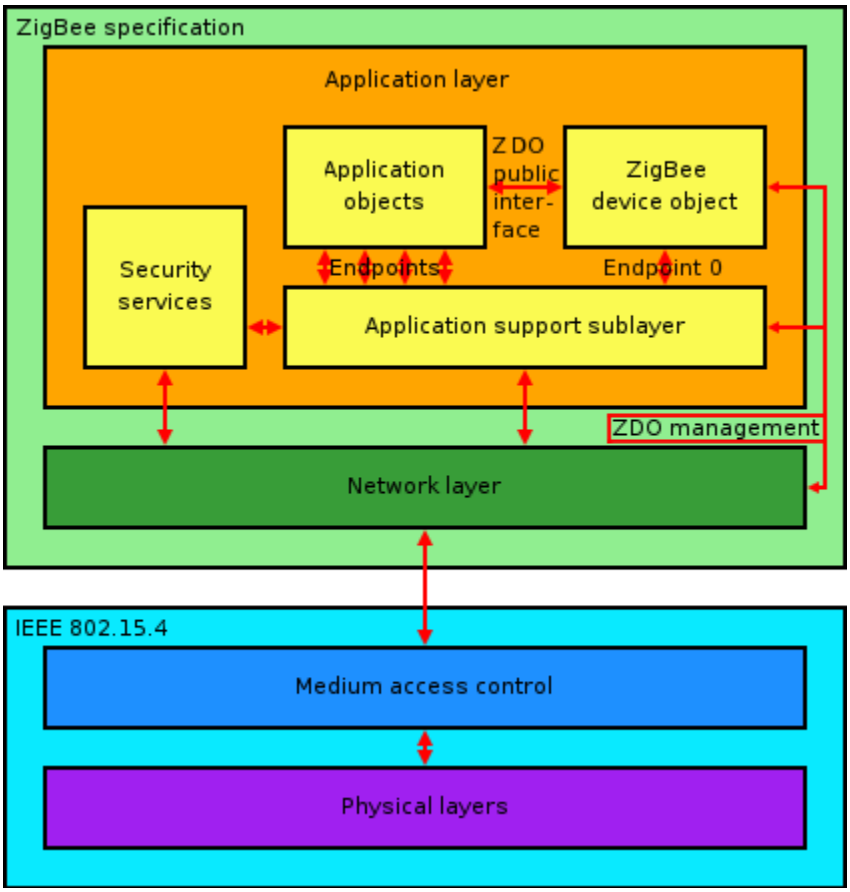

Figure 2.2 ZigBee Protocol Stack [6]

2.1.1 Application Layer

ZigBee's AP Layer consists of the Application Support Sub-layer (APS), ZigBee Device Object (ZDO), and the top-level Application Object. APS sub-layer is in charge of matching two devices based on services and their needs as well as forwarding messages. The ZDO sub-layer is in charge of creating unidirectional local links between source endpoints and destination endpoints, forwarding messages between the devices, and defining or discovering the role of the device within the network, i.e ZigBee Coordinator, Router or End Device, to determine which service they provide [7].

2.1.2 Network Layer

The Network Layer is in charge of starting and defining the network topologies, joining or leaving existing networks, applying security frames to the packets,

routing frames to destination, and discovering and maintaining routes between end devices (sensors). If the network employs a ZigBee Coordinator, the Coordinator will be in charge of initializing and maintaining any devices connected to the network. [7].

2.1.3 Medium Access Control Layer

The MAC layer used in the ZigBee protocol is specified by the IEEE802.15.4 specification. MAC layer within the Zigbee is also referred as long address, and it is a 64 bit number that uniquely describes the ZigBee device. This MAC address is a constant value separate from the ZigBee protocol; it is set during manufacturing of IEEE802.15.4 specification RF chips. It is completely controlled by the hardware.

2.1.4 Physical Layer

ZigBees also use the PHY layer specified by the IEEE802.15.4 specification. ZigBees can operate at three different frequency bands. Worldwide, the 2.4GHz band is used, supporting 16 channels. In North America, the frequency band is 915MHz with 10 channels and in Europe is 868MHz with 1 channel.

2.1.5 Layer Interfacing

The application layer interfaces with the Network layer through the APS layer by using APS data entity (APSDE) through the service access points (APSDE-SAP), Endpoints in Figure 2.1. Interface between Application layer and ZDO is done directly using the ZDO public interface. The APS management entity (APSME) provides interface between the APS layer and the ZDO layer through the service access point (APSME-SAP), Endpoint 0 in Figure 2.1.

APSDE provides:

- Fragmentation and reassembly
- Reliable data transport
- Data transmission service for Protocol Data Units (PDU's) between devices connected on the same network.

APSME provides:

- security services
- establishing the unidirectional links between devices
- Addressing features, adding and removing address to addressing table.

2.1.6 ZigBee Addressing

A typical ZigBee address is shown below,

Channel	PAN ID	Network Address	Endpoint	Cluster	Command	Attribute

The first field is the channel within the transmission RF band associated with this network. The 2.4GHz ZigBee devices support up to 16 different channels, ten channels for 915MHz devices, and 1 channel for 868 MHz devices. Multiple networks can be started on the same channel, and to differentiate the networks, the PAN ID field is used to specify the address of the desired network within the channel.

The Network Address is a unique 16-bit number associated with a node on the ZigBee network. ZigBee coordinators are always with network address 0x00, however, coordinators on the same channel cannot have the same PAN ID. Any ZigBee device, other than a coordinator, that connects is then assigned a random network address.

A single ZigBee device can be associated with multiple, up to 240, virtual tasks, or applications, containing multiple objects, and in order to differentiate the virtual tasks, an endpoint address is used. The endpoint address specifies the desired virtual task, and then cluster is used to address the desired object to deliver a command. The attribute field holds the data to be delivered to the object. This is particularly useful in home automation applications, where a signal ZigBee RF device can be associated with multiple light switches.

2.2 Traffic type and mode of operation

There are two different types of data transmission that we are interested in wireless sensor networks:

Periodic: The application dictates the rate, and the sensor activates to checks for data and then deactivates.

Data is *intermittent:* The application, and events determines the rate, the device needs to connect to the network only when communication is necessary. This type of transmission enables optimum saving on energy, which is more ideal in an actual application of wireless sensor network.

ZigBee employs either one of two mode of operation: the beacon mode and non-beacon mode.

Beacon mode is employed when the ZigBee coordinator runs on battery and where maximum power optimization is desired. In this mode, the end device waits for the coordinator's beacon that gets broadcasted periodically. If data transmission is completed, the coordinator then controls when the next beacon goes off so that the end device and coordinator itself enters sleep mode. Figure 2.3 describes beacon mode of operation

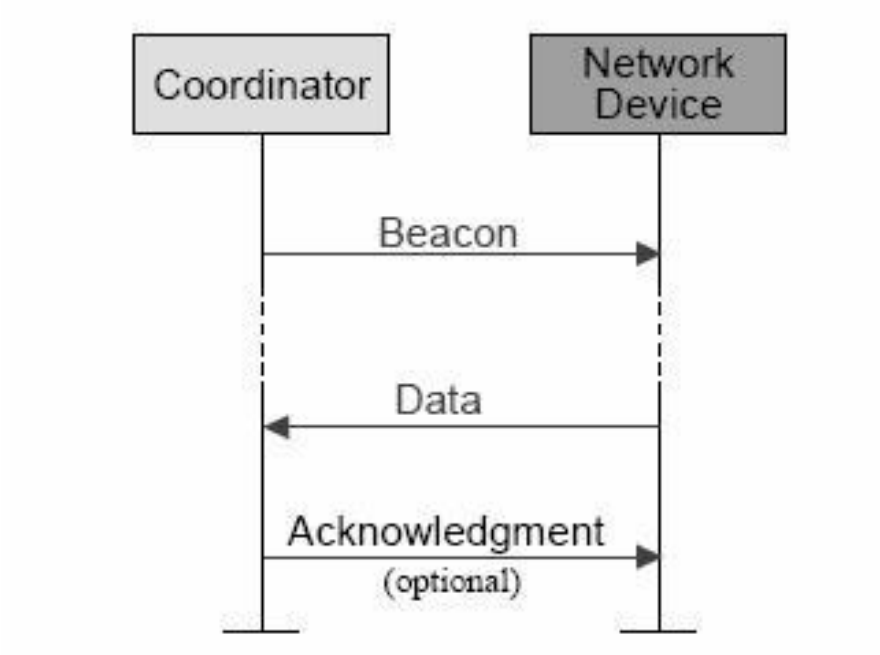

Figure 2.3 Beaconing Mode [8]

The non-beacon mode is desired when the coordinator is powered by a power supply unit, and the end devices are always asleep, the devices wake up on detection of activity or event. For example in a wireless senor network within a greenhouse, the sensor would wake up from sleep when a temperature derivative meets a desired value. The sensors wakes up, as it were, and transmit to the constantly waiting coordinator's receiver where it is powered by a constant power supply. The disadvantage of this is the chances that a sensor finds the channel busy, in which case the receiver could miss data. Please see figure x, that describes the non-beacon mode of operation. Please see figure 2.4, that describes the non-beacon mode of operation.

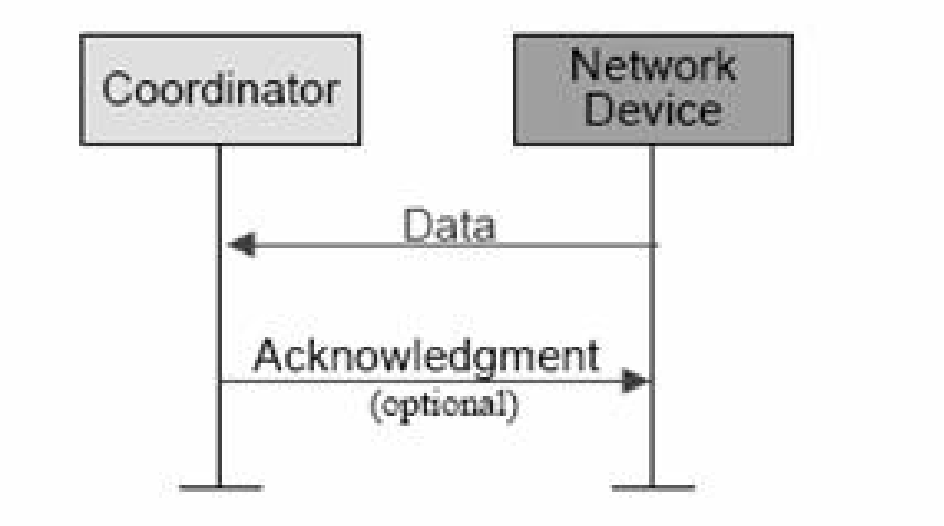

Figure 2.4 Non-Beaconing Mode[8]

In general, the ZigBee protocols minimize the time the device is on, so as to reduce power use. In beaconing mode networks, nodes only need to be active while a beacon is being transmitted. In non-beacon-enabled networks, power consumption is decidedly asymmetrical: some devices are always active, while others spend most of their time in idle. For our interest, Beacon mode is very important to wireless sensor networks, where a typical application would require a battery and maximizing power saving is greatly desired.

2.3 ZigBee Devices

There are three different ZigBee device types that operate on the ZigBee layers, consist of:

The Coordinator: There is one, and only one, ZigBee coordinator in each network to act as the router to other networks. It is designed to initialize the network, store information about the network, select the appropriate channel, and grating access for other devices to connect to its network.

Router: ZigBee routers are used to transmit data from other devices and it is also able to have other nodes attached to it, such as a router or an end device. These other nodes are referred to as child nodes. Routers need lesser memory than a ZigBee coordinator, and require lesser manufacturing costs. It can operate in all topologies and in some cases it can act as a limited coordinator.

End Device: End devices are capable of talking in the network but it cannot relay data from other devices. It requires even less memory, ie no flash, very little ROM and RAM. This device talks only to a network coordinators and routers. An end device does not have the ability to have other nodes connect to its network through the end device, as it

must be connected to the network through either a router, or directly to the coordinator. In more advanced mesh network topologies each device can communicate with other devices irrelevant of their types.

2.4 ZigBee Topologies

The ZigBee protocol can be configured as for multiple networks topologies such as tree, star, cluster and mesh networks supporting up to 65,000 nodes across large areas for different industrial use[8]."Topology" refers to the configuration of the hardware components and how the data is transmitted through that configuration. In mesh networks, connections between nodes are dynamically updated and optimized through sophisticated built in mesh routing table. Dynamically updating the connection allows for self-healing if one of the routers stops functioning due to exhaustion of its battery or if an obstacle blocks the message route, the network can select an alternative route. This is the self-healing characteristic of ZigBee mesh network. An example illustrated in the figure below.

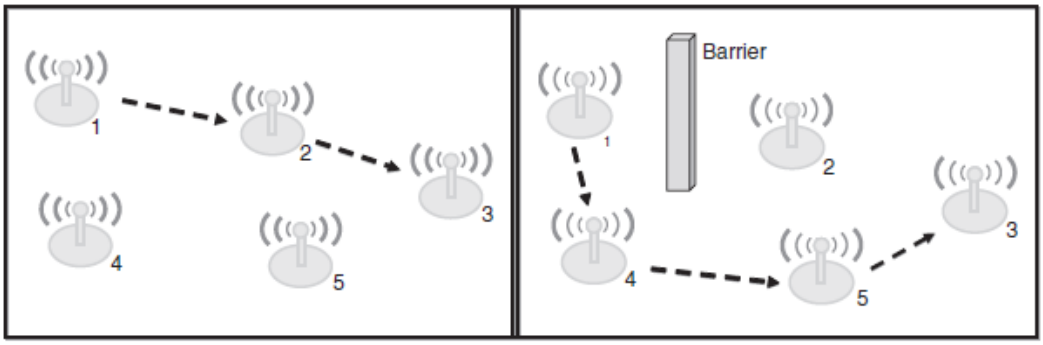

Figure 2.5: Mesh Self Routing of Blocked Paths [8]

In tree topology, the network consists of a central node, which is a coordinator, several routers, and end devices, as shown in figure 2.6. The end nodes that are connected to the coordinator or the routers are called children. Children are only associated with routers and coordinators. Each end device is only able to communicate with its parent (router or coordinator), except in Mesh Topology. A special case of tree topology is called a cluster tree topology. A cluster tree topology is a special case of tree topology in which a parent with its children is called a cluster see figure 2.7.

The star topology consists of a coordinator and several end devices (see figure 2.8). In this topology, the end device communicates only with the coordinator. Any packet exchange between end devices must go through the coordinator. The disadvantage 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 advantage of star topology is that it is simple and packets go through at most two hops to reach their destination.

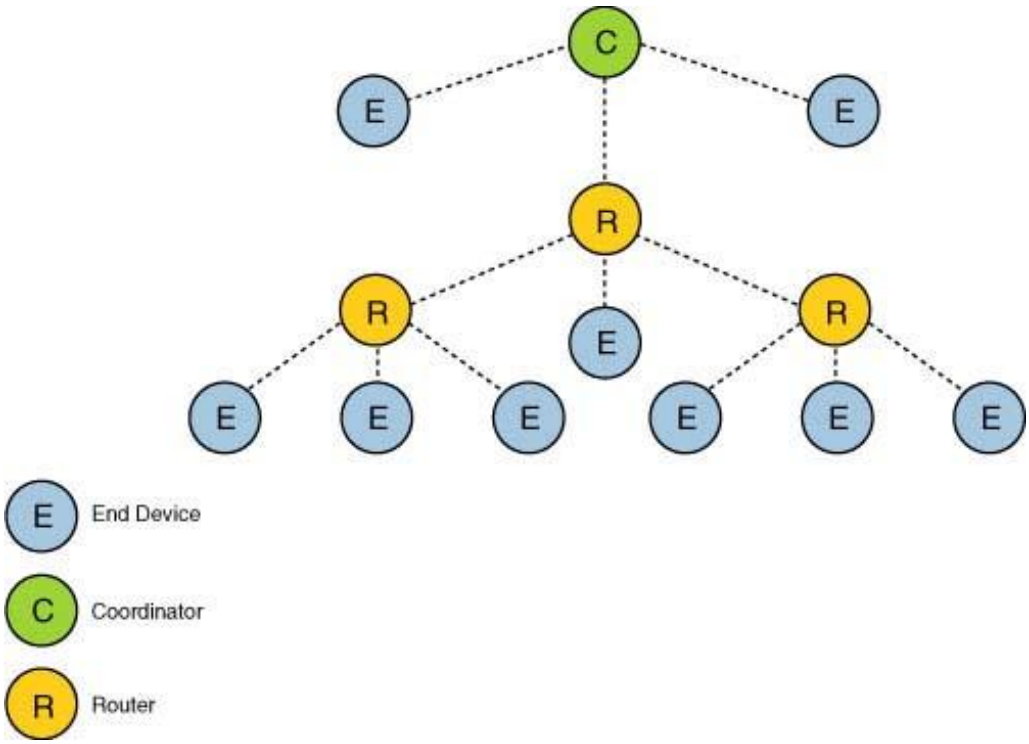

Figure 2.6 Tree Topology[9]

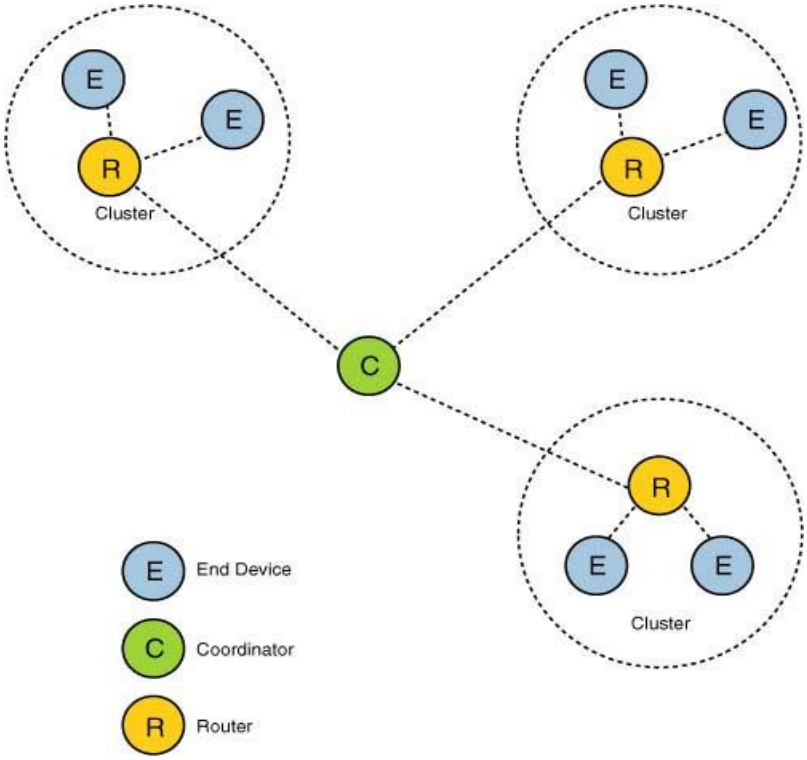

Figure 2.7 Cluster-Tree Topology[9]

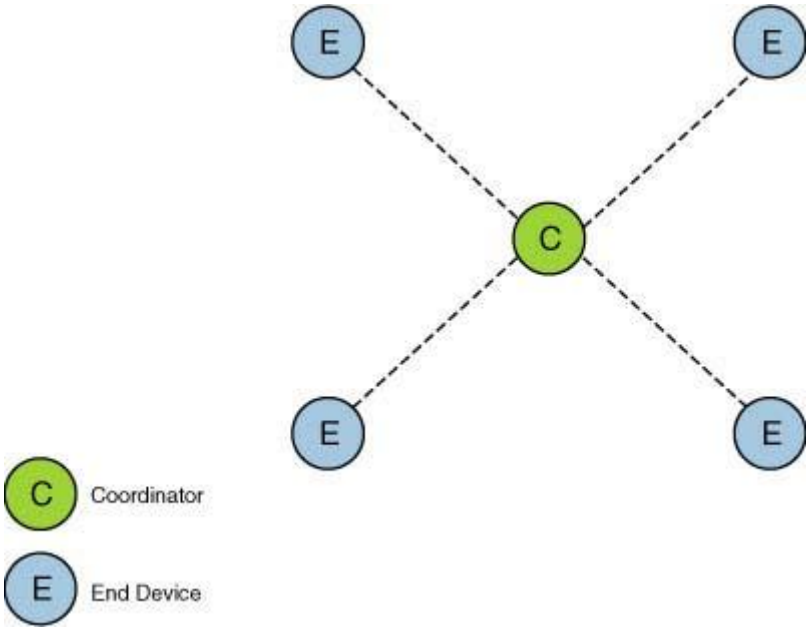

Figure 2.8 Star Topology [9]

Benefits of star topology include simplicity which means that this topology does not require a complex network layer or routing protocols (see figure 2.8 above); performance is generally high, with packets taking a maximum of 1 hop to reach their destination. Limitation of this topology includes: there are no alternative paths between the device and coordinator, so if a path becomes obstructed (i.e.an aluminum wall), communication is lost between the device and coordinator; the radius of the network is limited to maximum range whereas the other 2 topologies can be expanded with the aid of routers; networks must be carefully planned to ensure good connections with no obstacles or interference between the coordinator and the end devices.

Mesh topology is highly reliable and robust. The advantage being that if any individual router becomes inaccessible, alternative routes can rediscovered and used. The use of intermediary devices in relaying data means that the range of the network can be significantly increased, making this topology highly scalable. Weak signals and dead zones can be eliminated by simply adding more routers to the network. The limitation of this topology has a higher communications overhead than the star topology, which can result in increased latency and lower end-to-end performance. Meshed routing requires more complex network protocols. This means the routers require more embedded resources, which can result in increased power consumption and costs.

Tree topology is a combination of star and mesh networks, that takes the benefit of both topologies such as high reliability and long battery life.

3.0 ZigBee Simulation Overview

For the scope of this project, we decide to explore the performance difference in the ZigBee's Star topology and Cluster topology for wireless sensor network applications. We attempt to simulate performance parameters such as end to end delay (ETED), throughput, and packet loss (PL) to give us a better understand between the two topologies. This section will be dedicated to discuss the various scenarios explored under OPNET. The three scenarios that give us the most contrast between the two unique topologies are show in the tables below.

Scenario	Coordinator	Router	End Devices
Exploring sensor network coverage	1	1	1
Increase Transmission rate	1	1	3
Addition Sensors	1	2	9

Table 3.2 Cluster Setup

Scenario	Coordinator	Router	End Devices
Exploring sensor network coverage	1	0	1
Increase Transmission rate	1	0	3
Addition Sensors	1	0	9

Table 3.3 Star Setup

Exploring Sensor network coverage: The goal of this scenario was to observe what effect the range had on the ZigBee network, our belief is that the range would depend on the power of the transmitter.

Increase transmission rate: The goal here was to attempt to breakdown the network by overflowing it with packets, the expectation is that the two network topologies will behave differently.

Additional sensors: The addition of extra sensors was to compare and contrast the effect of increasing the network load; we expect that as the load increases the ETED would increase as well as packet loss would be greater.

3.1 Design Methodology

We implemented our ZigBee wireless sensor networks using the models that are integrated with OPNET 16.0, we provide node and process model in this section for reference. The Figure 3.1 below shows the overall node model. It is consisting of three layers: application, network and MAC layer, and there is one wireless transmitter, and one receiver for wireless communication.

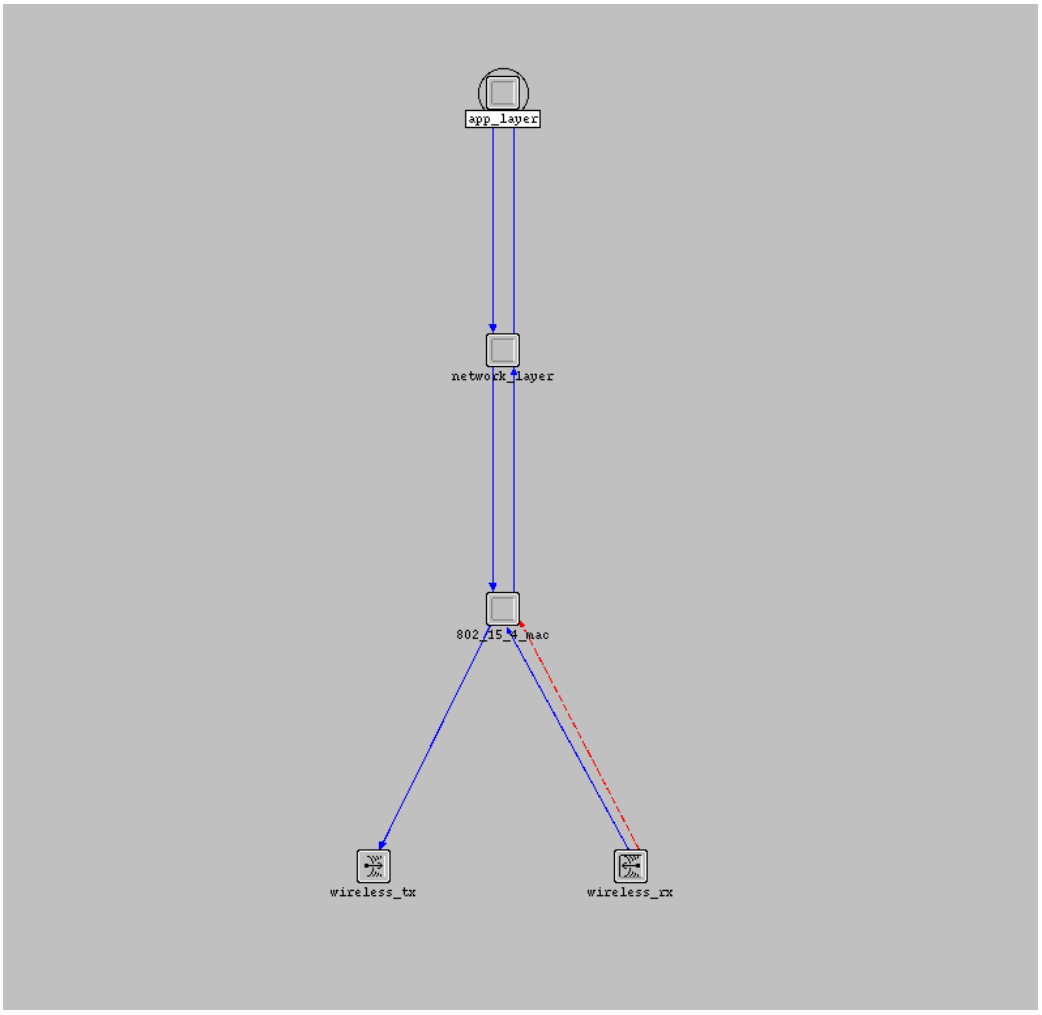

Figure 3.1 OPNET ZigBee Node Model

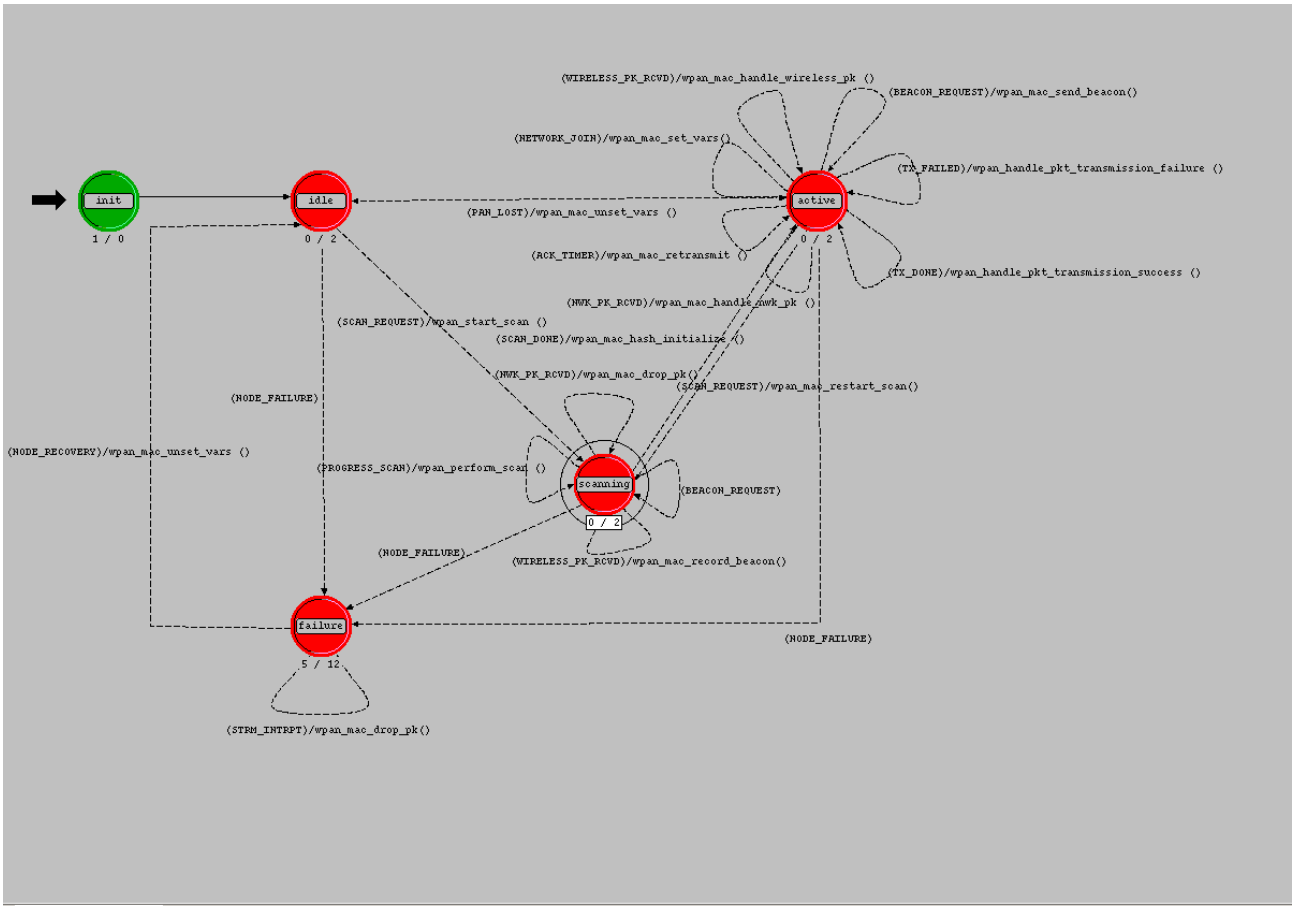

Figure 3.2 MAC Process Model

The figure above (Figure 3.0.2) shows the process model for the ZigBee's MAC. As it can be seen there the MAC can be in 4 predominant states. The idle state is entered when MAC is waiting for packets, the scanning state occurs when the MAC scans for incoming packets and the active state when the MAC processes the incoming/outgoing packets. There is also a fail state which specifies what the MAC must do in case of a failure.

3.1.1 Basic Setup

The basic setup of each topology implemented under OPNET 16.0. Figure 3.3 below demonstrated the symbols used by OPNET for router, coordinator and end device. Also please refer to figure 3.4 for basic cluster topology and figure 3.5 for basic star topology.

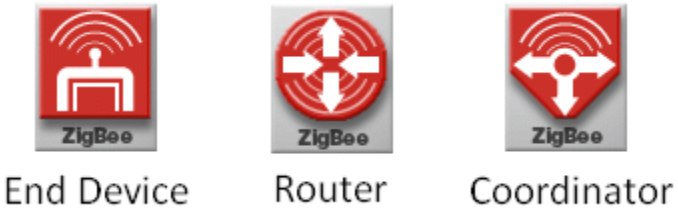

Figure 3.3 OPNET Representations of ZigBee Devices

Figure 3.4 below shows the cluster network topology implemented in the project, consisting of three sensor nodes transmitting packets to a coordinator via a router which also transmits its own data to the coordinator.

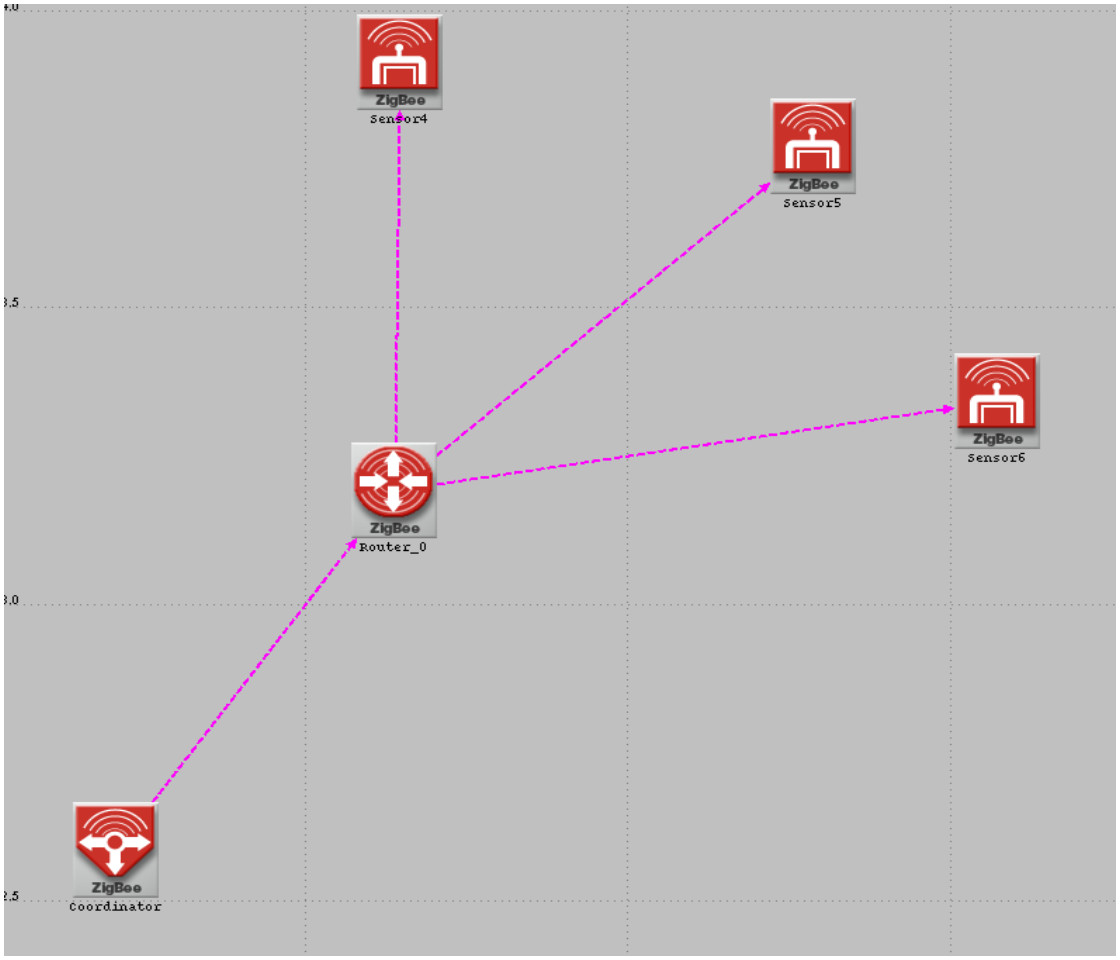

Figure 3.4 Cluster setup

Meanwhile figure 3.5 shows the star topology implemented in the project. It consists of 4 fixed sensor nodes transmitting packets to a coordinator. In both topologies equal amount of data is being sent to the coordinator we have fixed the packet size to 1024 bits and the transmission interval time to 1s (see Figure 3.9 for the full network setup parameters).

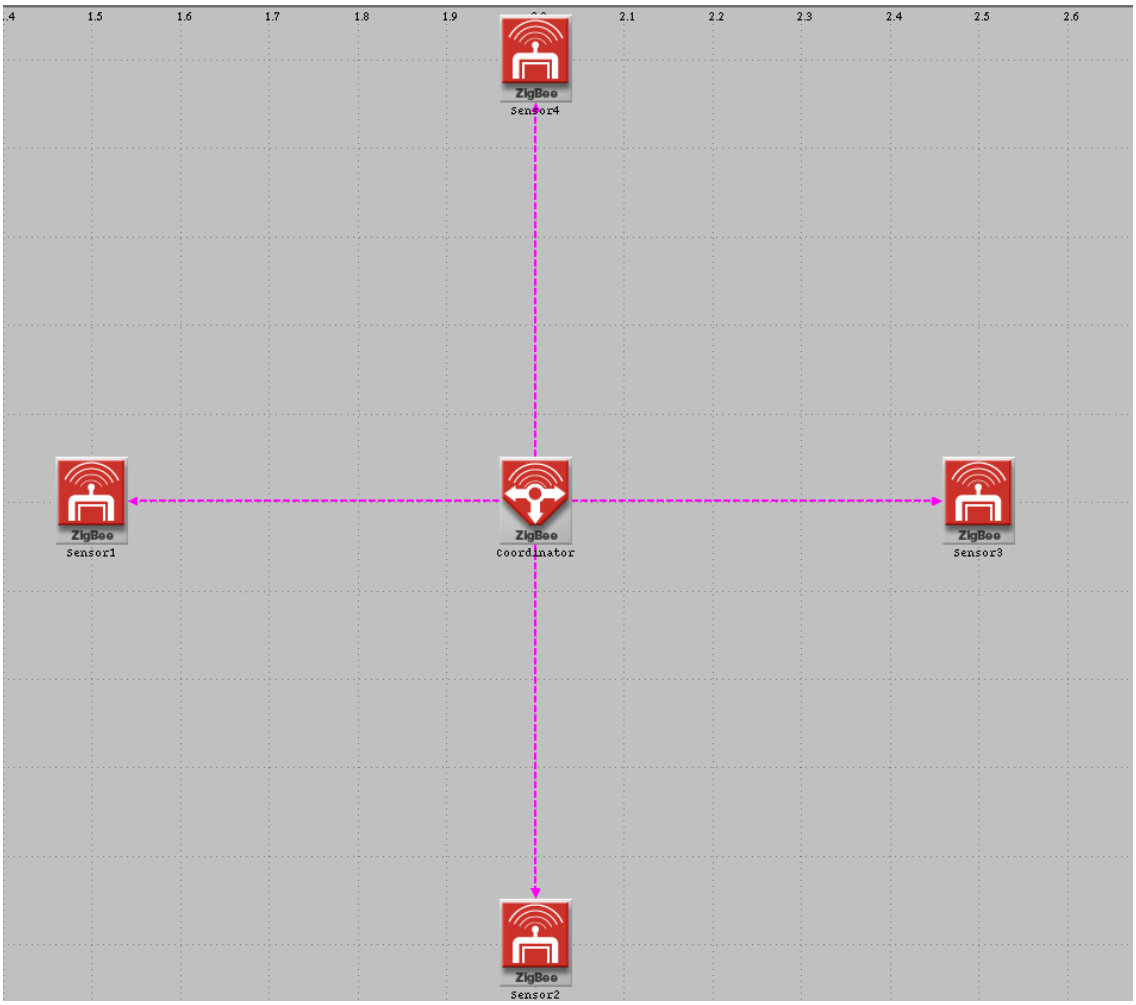

Figure 3.5 Star Setup

After running the simulation for 30 minutes we recorded the results in the following graphs. In figure 3.6 we can see the average end to end delay for both topologies, it is no surprise that we see the delay is larger for the cluster topology than the star due to the packets in the cluster topology having to travel farther to get to the coordinator. In figure 3.7 we observe the average throughput for the two topologies, the dip at the beginning is the initial delay that occurs when the network first sets itself up, and during that time no data is transmitted. As can be seen the star network has a lower throughput than the

cluster, but this is throughput at the MAC layer which resides in all the nodes of the network and because in the cluster network the data travels farther it can be expected that where would be a higher throughput. For packet loss as can be seen in figure 3.7 we observed that on average the star topology exhibited a much larger packet loss than the cluster topology. This we believe is mostly due to the fact that the star topology sends the data all at once to the coordinator and this cause an overflow in the coordinator resulting in packet loss.

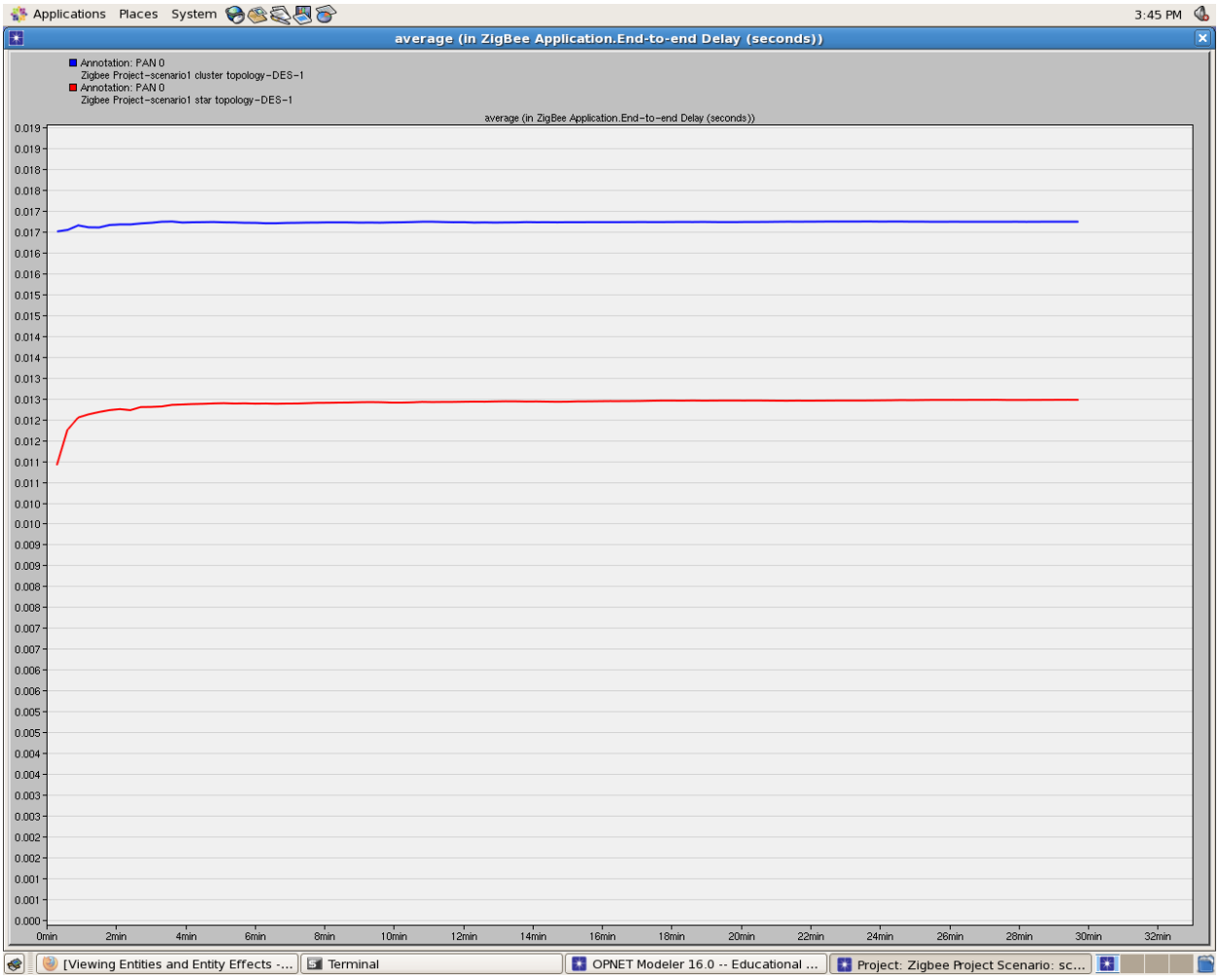

Figure 3.6 ETED

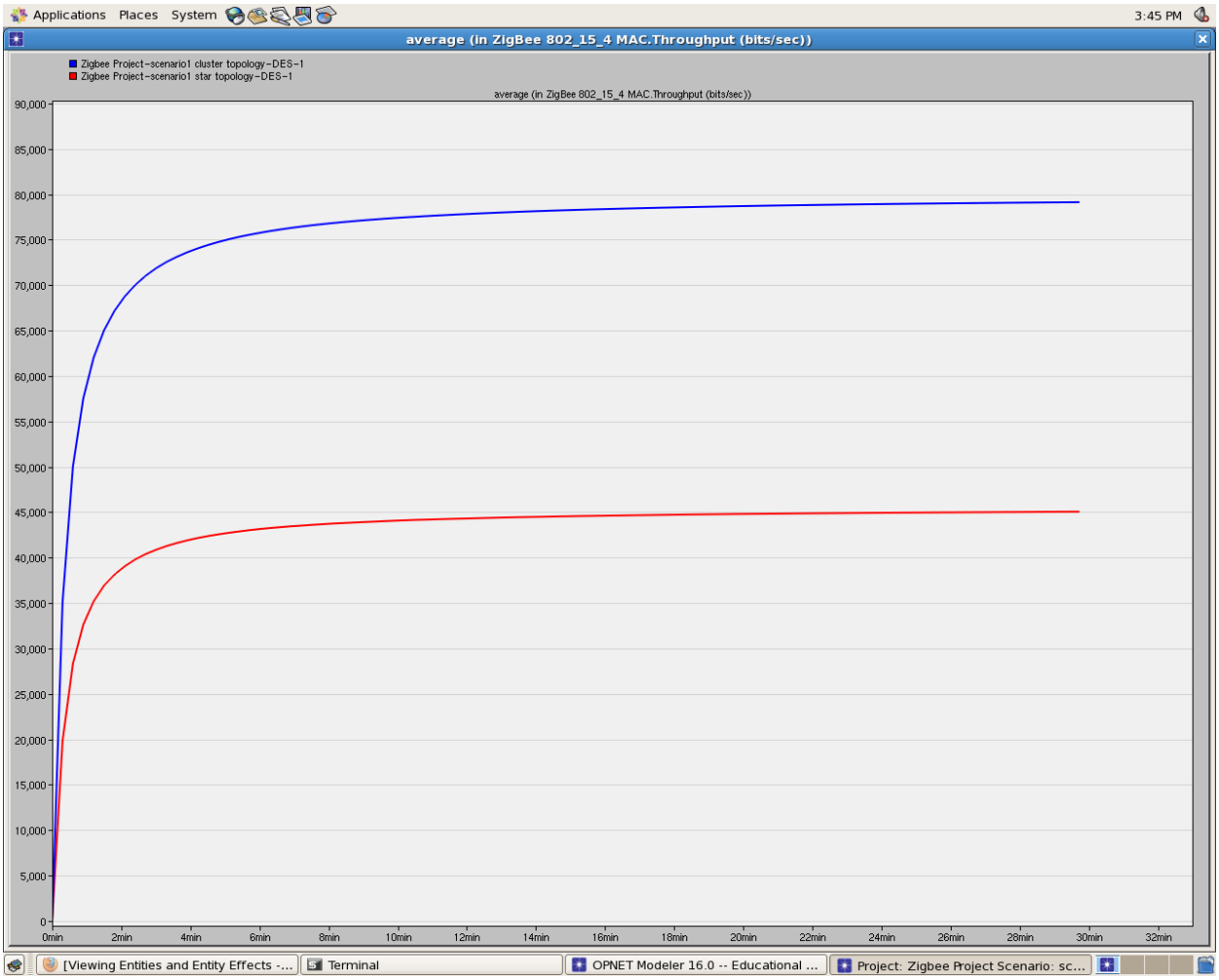

Figure 3.7 Average Throughput

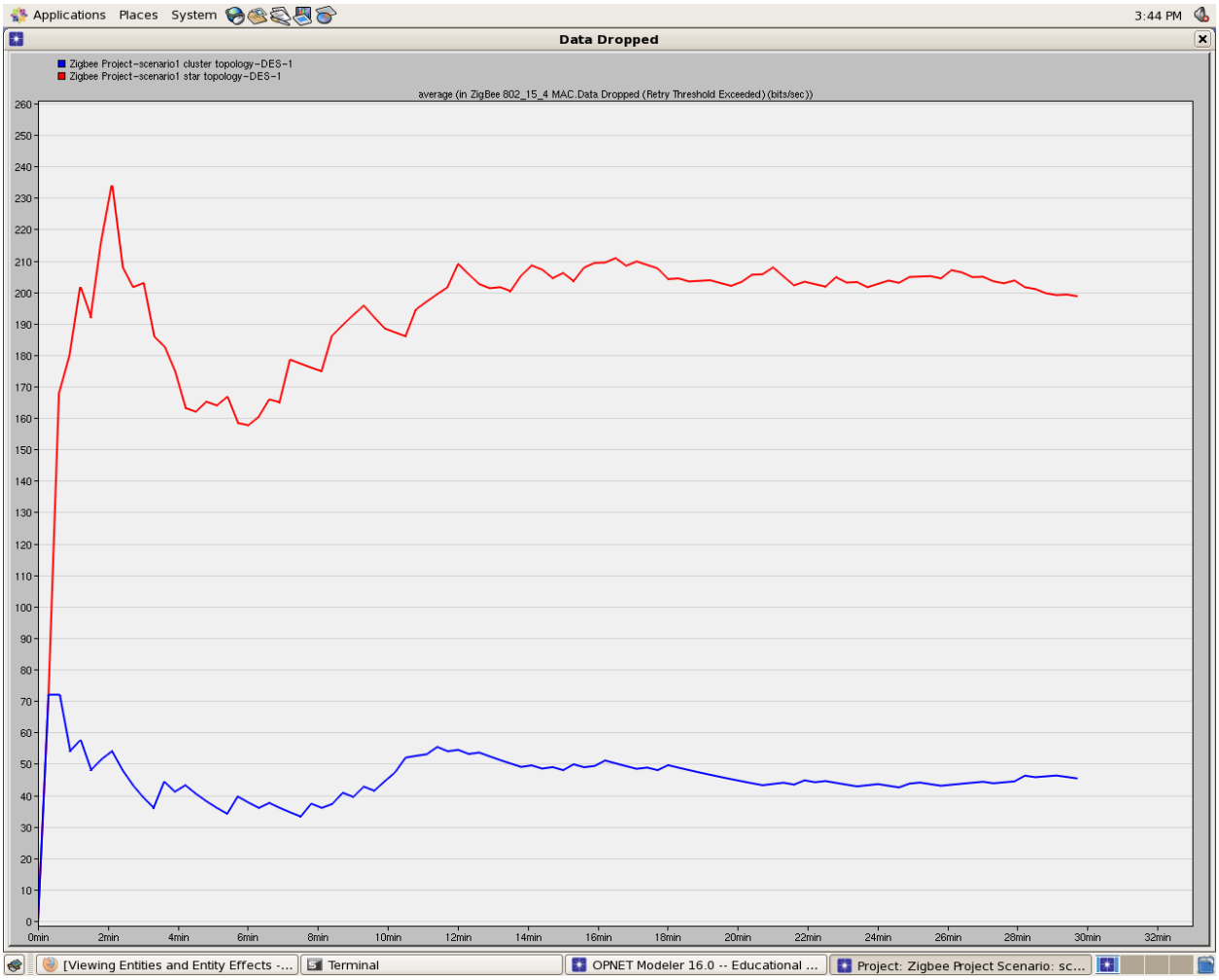

Figure 3.8 Packet Loss

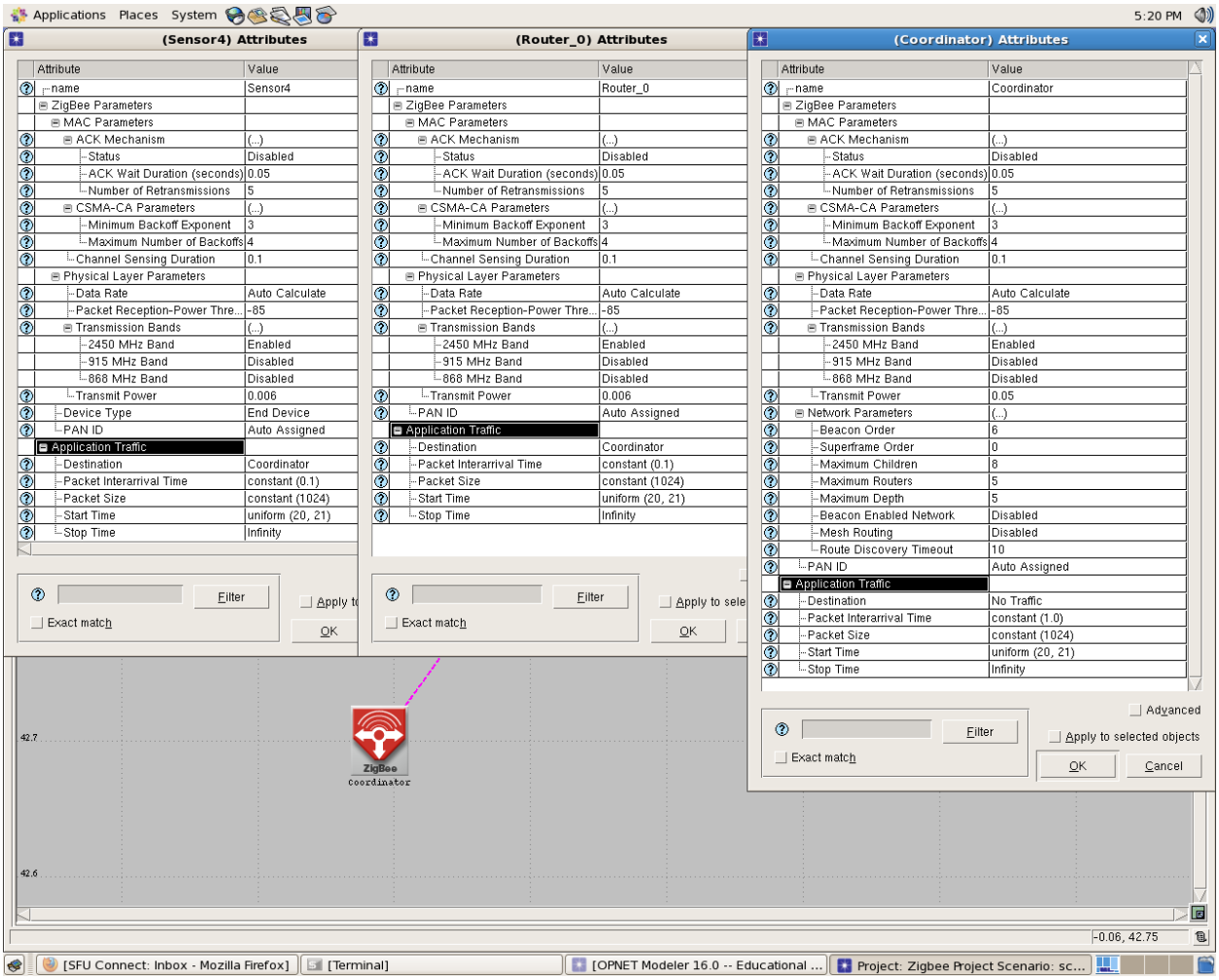

Figure 3.9 Network Setup Parameters

3.1.2 Increasing transmission rate

Our scenarios contain only a handful of nodes transmitting at a relatively small amount of data which is realistic of ZigBee networks; we wanted to see how the two network topologies behaved when we increased the data transmission rate. To do this we took the two network setups in figures 3.4 and 3.5 and we increased the packet transmission interval time variable from every second to every 20mS while leaving the packet size a constant 1024 bits. In terms of end to end delay; as can be seen in figure 3.10 we saw a linearly increasing ETED for both star and cluster topologies. An increasing delay means the network is overflown with data. While both topologies display an increasing delay the star topology's delay is increasing at a much larger rate which would suggest much greater packet loss. As figure 3.11 shows the throughput of the two is relatively the same, the cluster is of course still larger, the smaller difference between the two can be attributed to larger packet loss.

In terms of packet loss, as can be seen in figure 3.12 the number of packets sent by both topologies is the same, however the number of packets received by the coordinator is different for each topology. The cluster topology appears to receive 10% more packets than the star topology even though both topologies lost roughly half the packets initially transmitted.

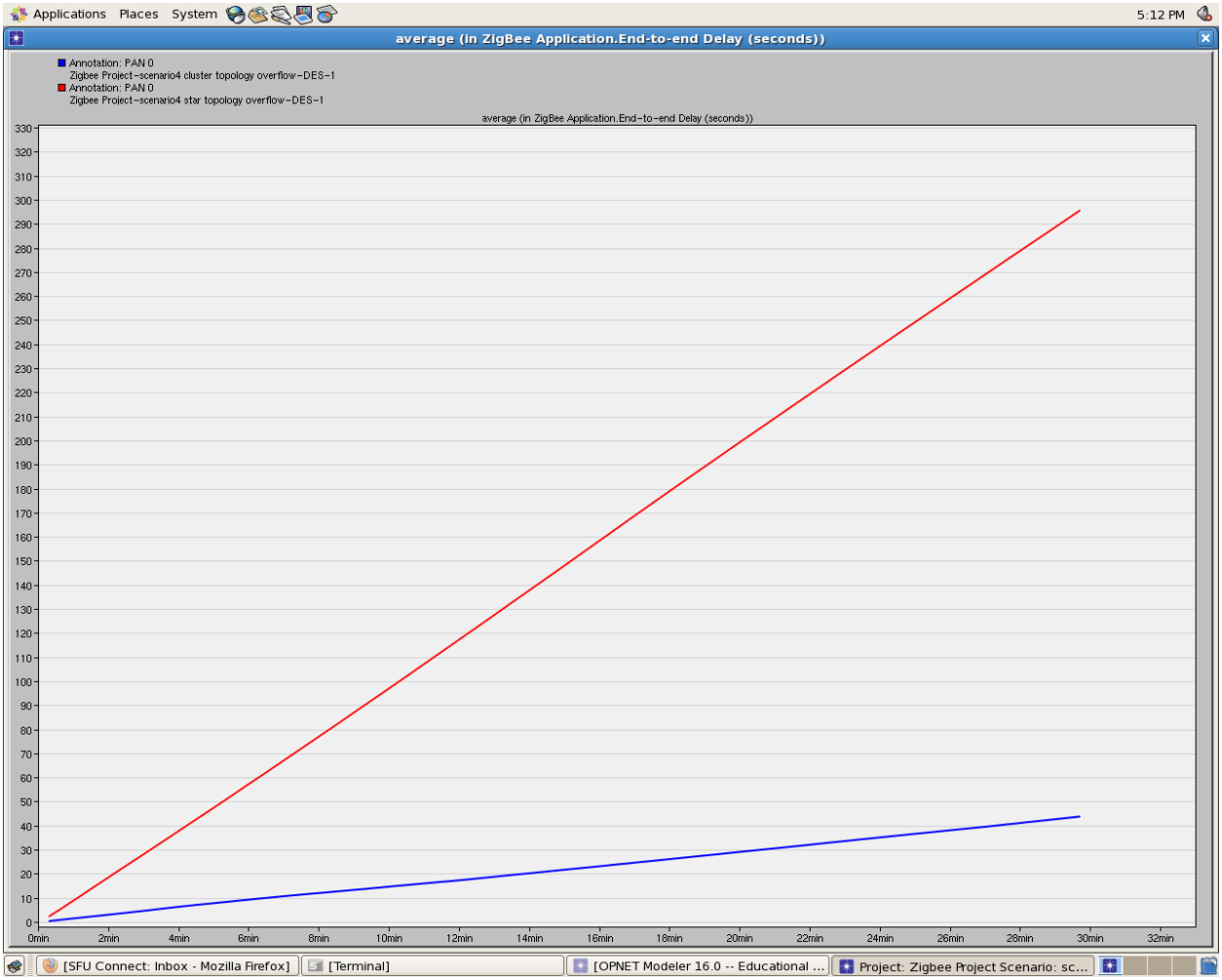

Figure 3.10 Network Overflow ETED

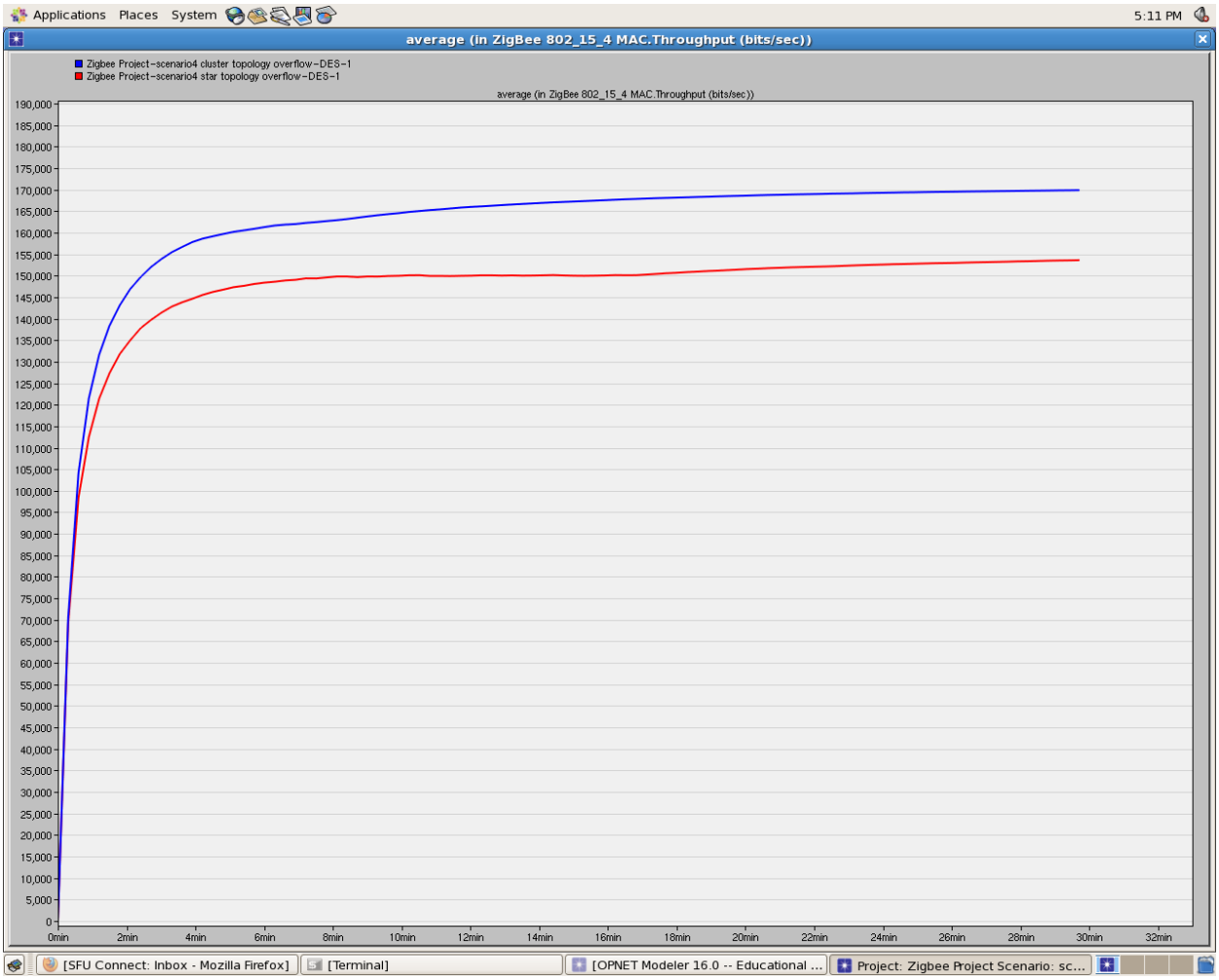

Figure 3.11 Throughput when Increased transmission rate

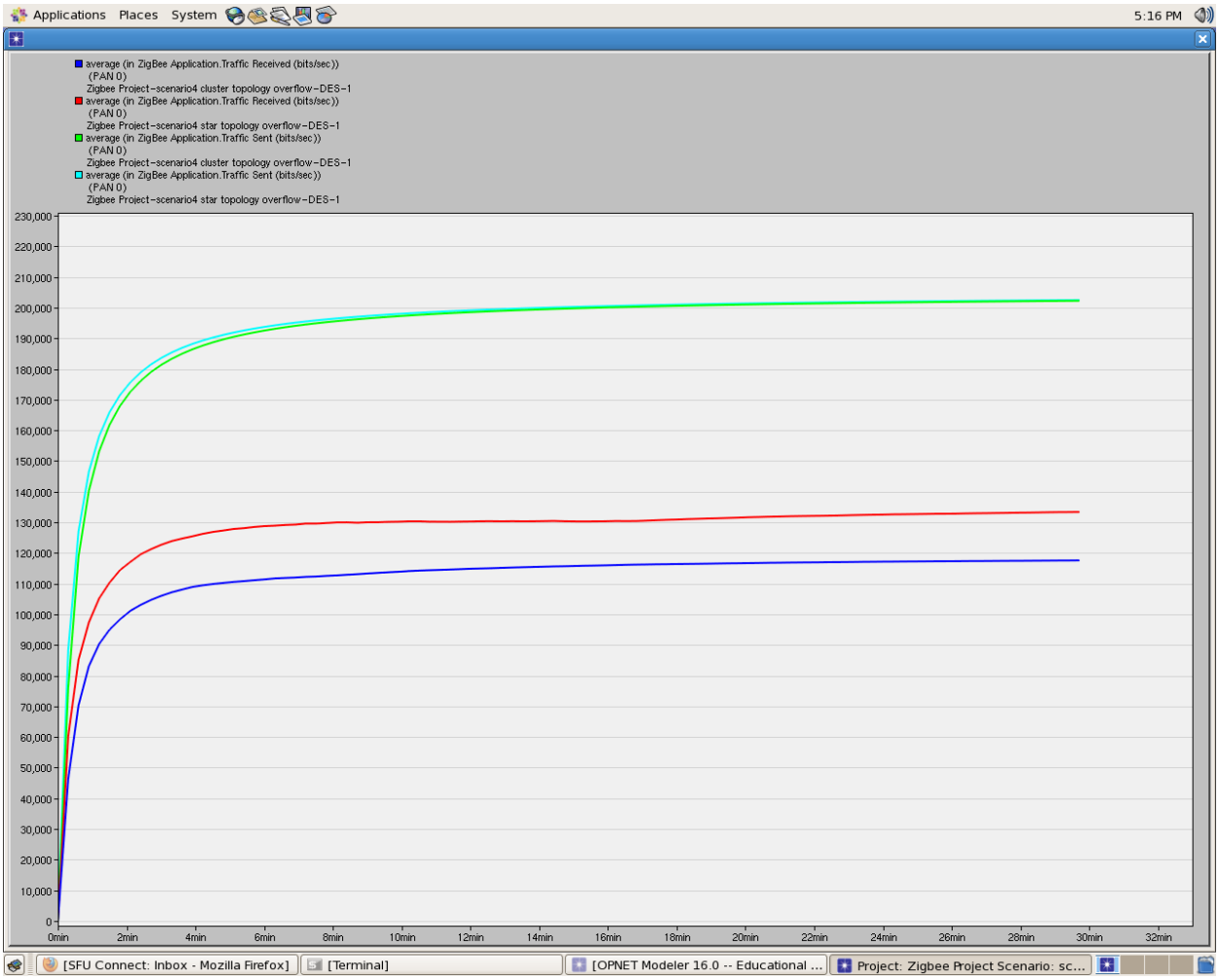

Figure 3.12 Packet Loss with increased transmission rate

3.1.3 Exploring Network Coverage

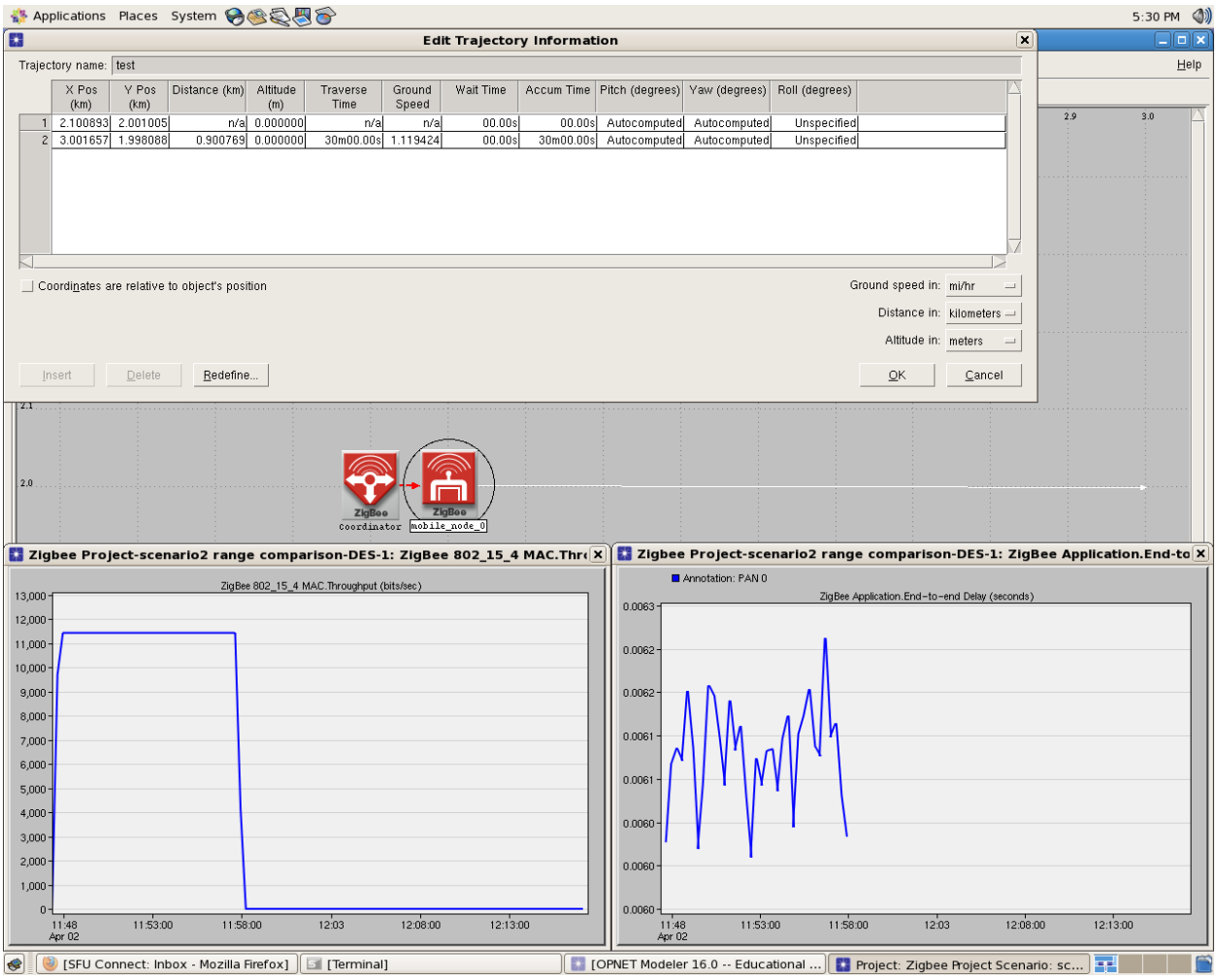

Figure 3.13 End Device Moving Away from Coordinator

In this scenario we ignored the topologies and wanted to know what effect the range had on the network throughput. To do this we created a simple scenario of one mobile node following a trajectory that diverges from a fixed coordinator all the while transmitting data to the coordinator. ETED and Throughput were measured and as can be seen in figure 3.13 the throughput is constant but after a certain time when the mobile node is at a certain distance away from the coordinator the throughput drops to zero. This is because the coordinator has a reception power threshold which means that if the received signal has a low power (below the set threshold) it will be ignored. We observed that this range is almost exclusively dependent on the transmitter power which we fixed at 6mW. This is well within the capabilities of off-the-shelf ZigBee modules which can go as high as 60mW.

3.1.3 Addition of Extra Sensors

In this scenario we wanted to see how the two topologies would behave when the load and traffic were doubled. So we added twice as many nodes to the star topology (Figure 3.14) and doubled the routers and nodes of the cluster setup (Figure 3.15). From figure 3.16 we observed a fairly constant end to end delay for the star topology while the cluster topology exhibited a larger end to end delay which over time increased; this was most likely due to packet loss. But as expected the end to end delay for the star was shorter because the sensor nodes feed directly into the coordinator rather than requiring routing.

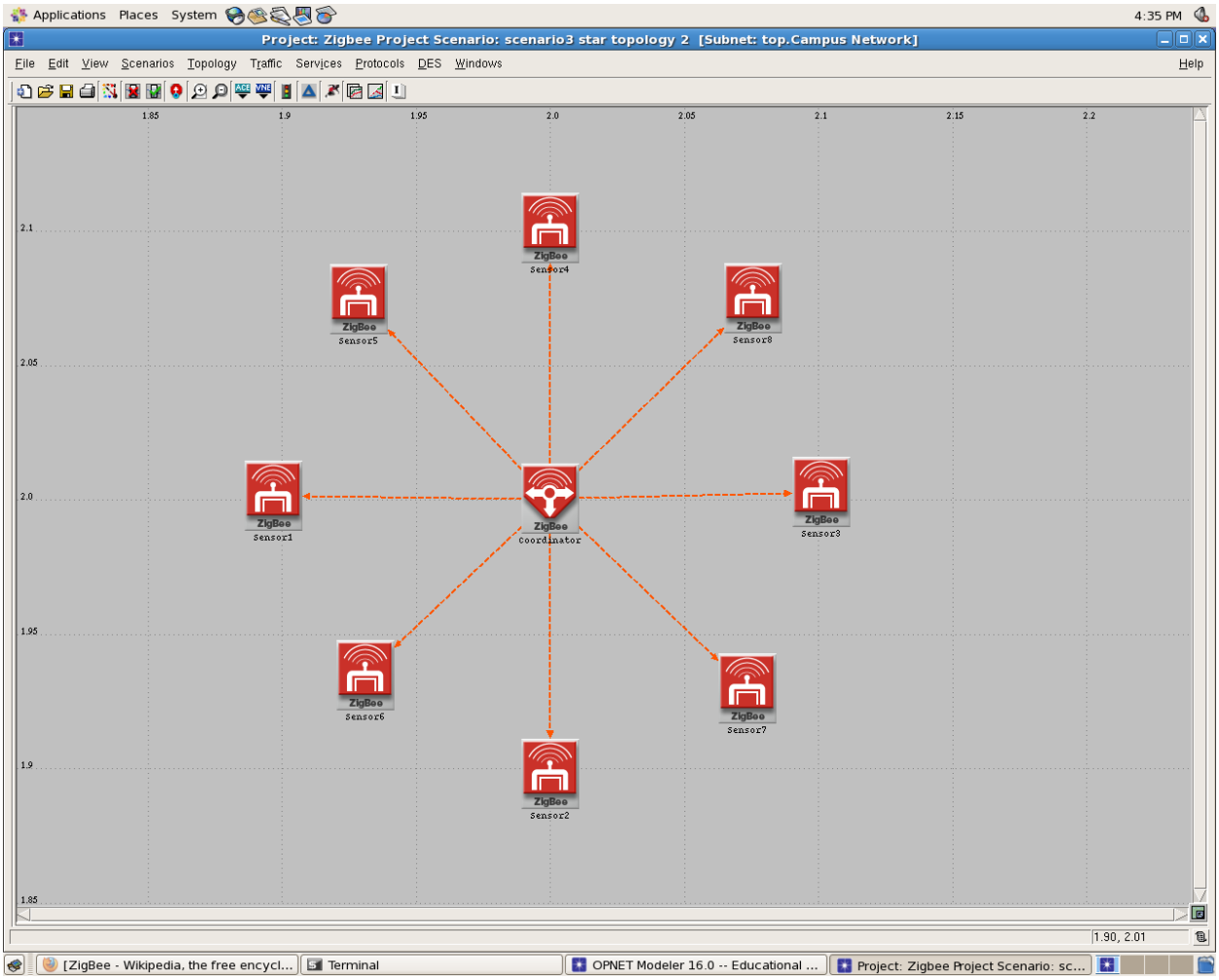

Figure 3.14 Star Setup with Additional Sensors

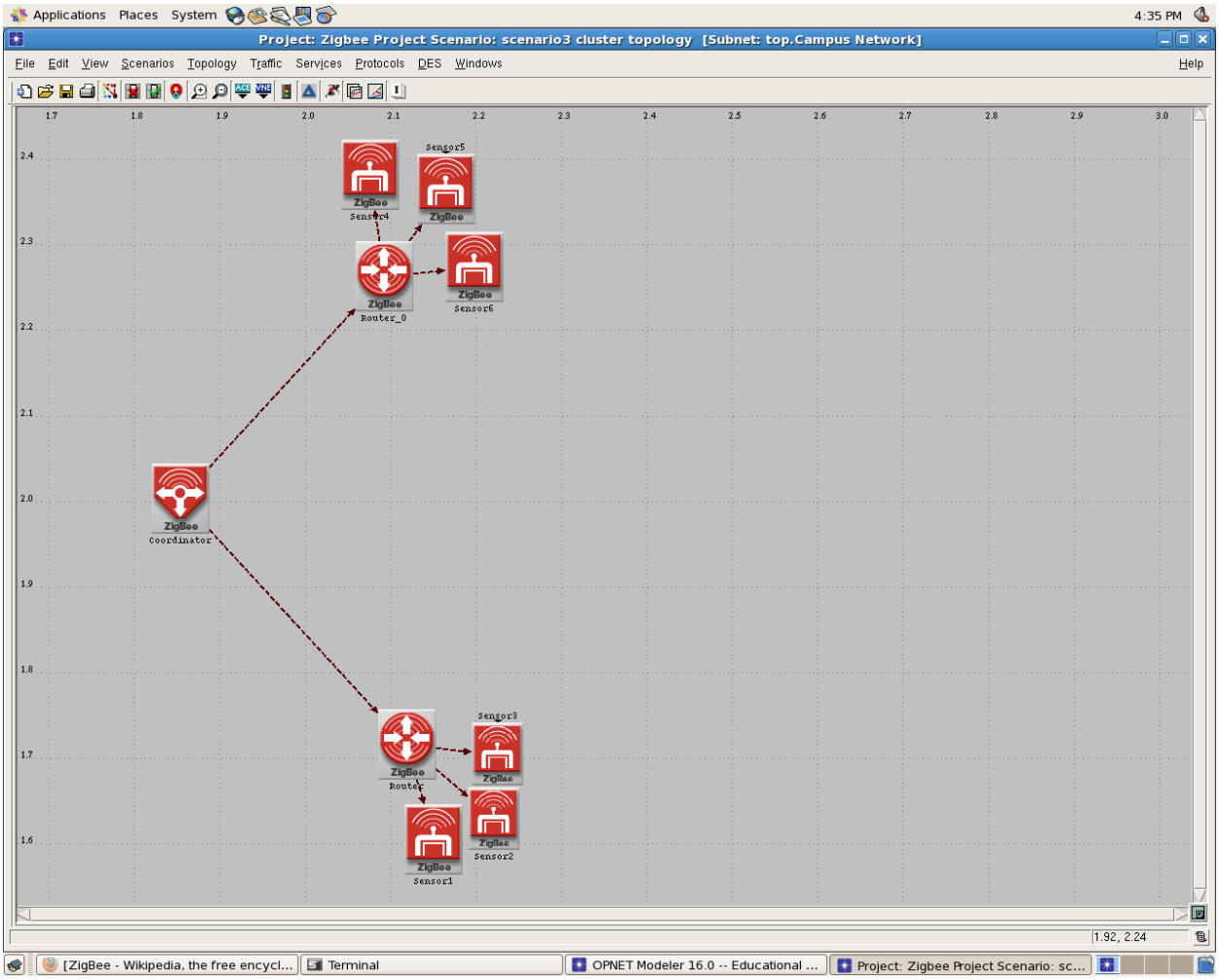

Figure 3.15 Cluster Setup with Additional End Devices

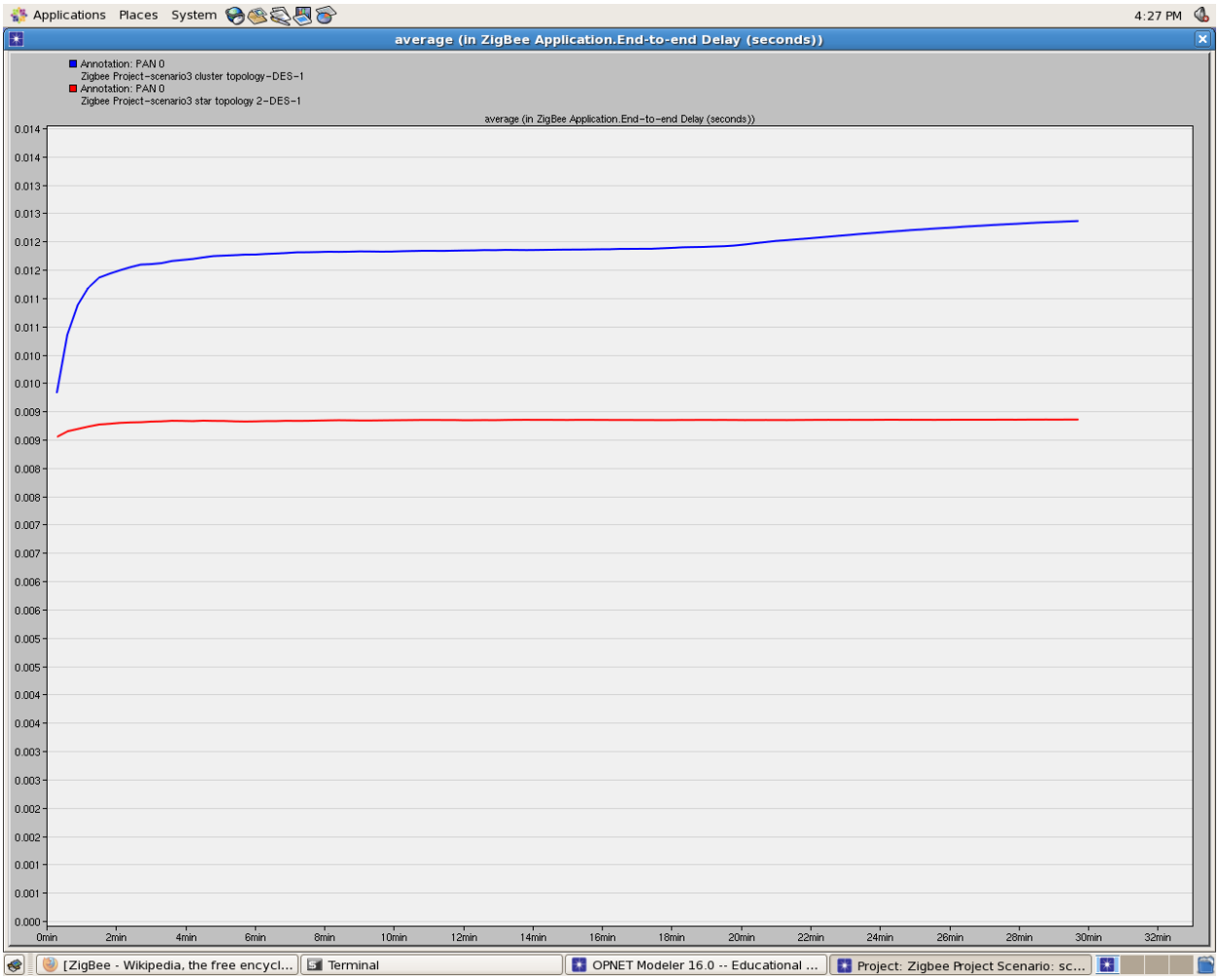

Figure 3.16 ETED for Additional Sensors

From figure 3.17 we observed that the throughput is higher in the cluster topology than the star topology, these results are similar to the throughput of the original network setups (Figure 3.7). As in the original scenario the reason that the MAC throughput is larger in the cluster is that more data is flowing in the MAC layer, for the star topology all data goes from source to destination. For the cluster topology, data flows from source to router and then to destination, this means more traffic on the network MAC layer and hence a higher throughput.

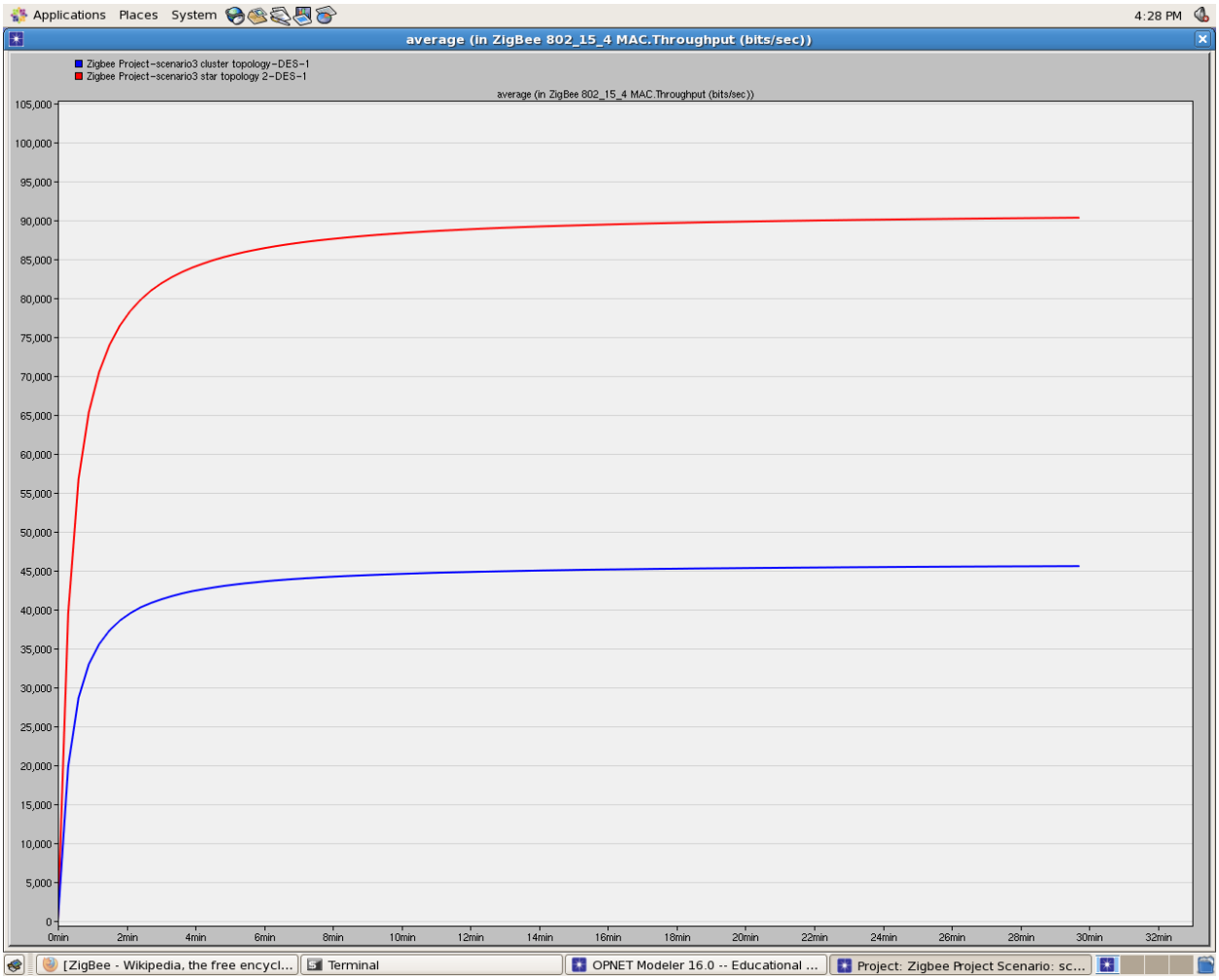

Figure 4.17 Throughput With Additional Sensors

From figure 3.18 we observed that the overall packets dropped by the MAC layer in the cluster topology is far lower than in the star topology. This is the same as was observed before in the original network setup, this time however we observed very little packet loss in the cluster topology while the packet loss was relatively the same for the star topology once averaged. The reason we think that the star topology drops a lot more of the packets is that all the packets are being sent instantaneously and if all the sensors transmit all at once that would overflow the coordinators receive buffer which would cause packet drop.

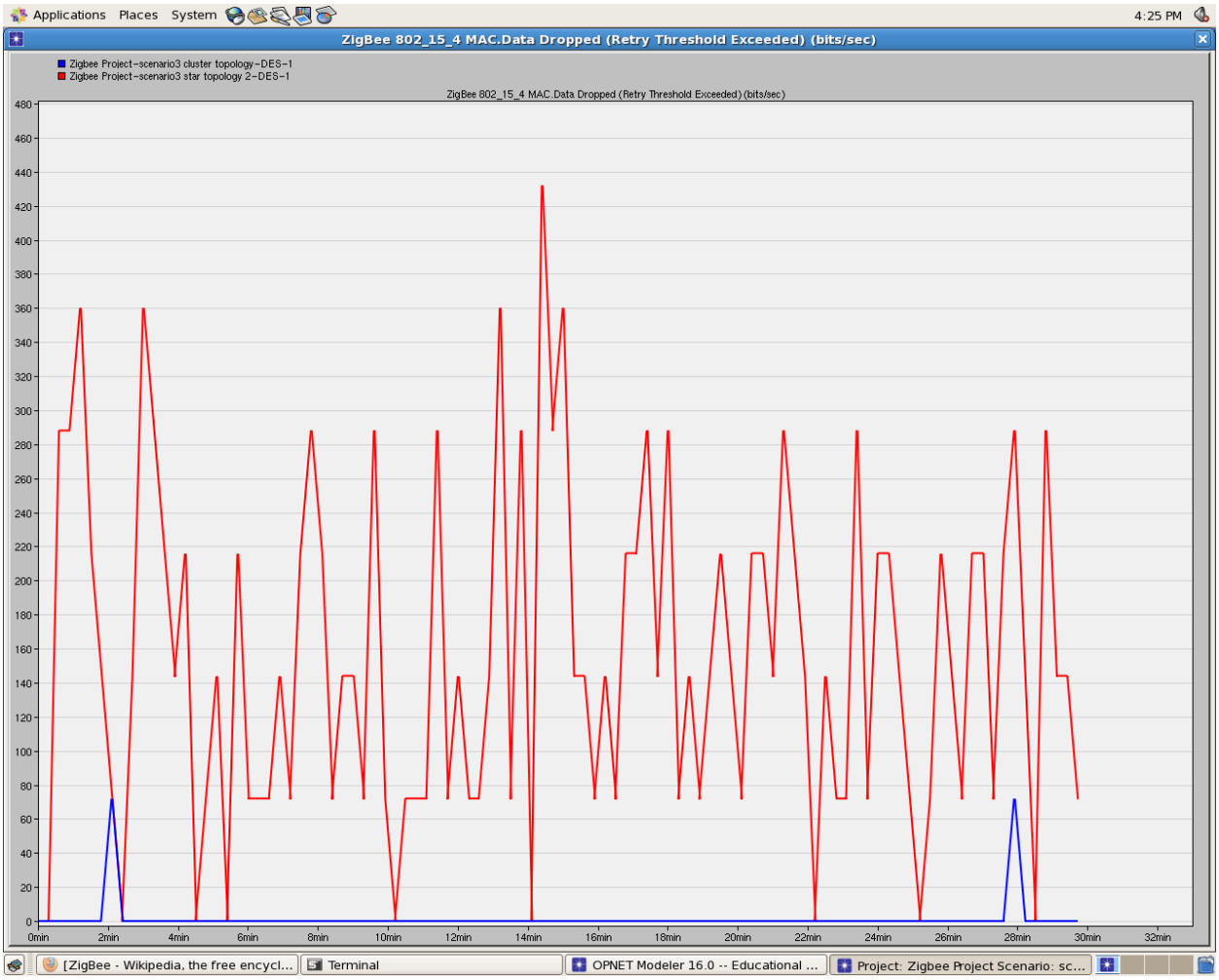

Figure 3.18 MAC Packet Loss

4.0 Discussion and Conclusion

4.1 Results

What we discovered after our three main scenarios is that ETED is smooth and proportional to increase packet size and transmission rate as well as network size and load (as expected). It is observed that the star topology is more prone to Packet Loss for all scenarios. This is because all the end devices are transmitting to only one coordinator, at the "center" of the star. Meaning if there are a lot of transmission collisions, some end devices will fail to get their data delivered as the transmission will be stopped once it exceeds the maximum number of retransmission attempts.

In general, increasing the transmission rate increases the packets lost, due to overwhelming the RF channel. This also occurs when receivers cannot respond fast enough in reading their FIFO buffers. Data in the FIFO buffers is not serviced in time and

gets overwritten with new packets. The cluster topology suffers from the same draw backs, when the network is overwhelmed with information (i.e each router bombards its associated coordinator, it will experience a lot of packet loss). The maximum data rate of ZigBee is 250 Kbits/s however when a lot of devices are transmitting at high rates to one receiving devices, coordinator or receiver, the receiving device will start to ignore packets as they overflow its FIFO buffer.

Throughput in the MAC layer is much higher in cluster topology for all scenarios simply because there are more packets flowing from node to node. Distance between nodes does not affect packet loss if the transmission rate is low, and it signals are within a suitable power range. The transmitter power almost exclusively determines the network range and coverage.

4.2 Future Work

Exploring the Mesh topology and self-healing mechanism and compare and contrast against the Star and Cluster topologies to ultimately determine which is superior. Also since we are exploring WSN, beaconing is also very important, due to Beacon enabled network permits much longer battery life by allowing the device to enter sleep mode periodically and only wake when an event triggers.

Beacon enabled devices are generally vulnerable to Denial of service attack (DOS) attacks, thus future study on potential DOS attacks in Zigbee WSN is intriguing to us. As WSN continue to grow due to the fact that they are low cost and effective such as providing solutions to a number of real world challenges, the need for effective security protocol will also grow. Most of the WSN's routing protocols are easy and straightforward because of this they are vulnerable to security attacks. Various DoS attacks and the impact of DoS on the performance of the system should be a priority going forward for ZigBee.

4.3 What we learned

Limitations in using OPNET's incomplete ZigBee model library and hidden implementation of all layers except the MAC layer. Current models are lacking security and beacon mode functionalities which affect some other features we would like to explore, such as battery life and ways to strength up security and prevent DoS attacks.

The ZigBee protocol is an advanced solution to low power wireless networks. It is reliable, secure and generally easy to implement in hardware. It is future only relies only on the imagination of developers.

Reference

[1]"Making Wireless M2M Easy." Internet: http://www.digi.com/technology/rf-articles/wireless-zigbee, Jan.10, 2012 [Mar. 07, 2012].

[2]" Report predicts ZigBee will dominate two-way low data rate wireless applications in the home." Internet: https://docs.zigbee.org/zigbee-docs/dcn/03-1398.pdf, July.10, 2003 [March.23, 2012].

[4] D.Gislason. *ZigBee Wireless Networking*. Vancouver, BC: Newnes, 2008, pp.

[5]"ZigBee Applications" Internet: http://backup.daintree.net/solutions/applications.php, Feb.10, 2008 [March. 20, 2012]

[6] "ZigBee" Internet: http://en.wikipedia.org/wiki/ZigBee, Mar. 12, 2012 [March. 12, 2012]

[7] Zigbee Standards Organization, "ZigBee Specification" Internet: http://www.medialab.ch/labor/cc2430/Z-Stack/054024r01ZB_AFG-ZigBee-Specification-2006-Download.pdf, Dec.1, 2006 [March.26,2012]

[8] "ZigBee Applications" Internet: http://www.tutorial-reports.com/wireless/zigbee/zigbee-applications.php, Jan.01.2007 [March.10, 2012]

[9] A. Elahi. "Introduction to the ZigBee Wireless Sensor and Control Network." Internet: http://www.informit.com/articles/article.aspx?p=1409785&seqNum=4, Dec. 2, 2009 [Apr.20, 2012]

[10] Zigbee Technology. Internet: http://www.zigbee.org/About/AboutTechnology/ZigBeeTechnology.aspx, Jan.2, 2012 [Feb. 09, 2012].

[11] SinemColeriErgen. " ZigBee/IEEE 802.15.4 Summary" Internet: http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf, Sept.10, 2004 [Feb. 25, 2012]

[12] DusanStevanovic. "Zigbee / IEEE 802.15.4 Standard" Internet:http://www.cse.yorku.ca/~dusan/Zigbee-Standard-Talk.pdf, Jun.20, 2007 [Feb.25, 2012]

[13]Raul Morais. "A ZigBee multi-powered wireless acquisition device for remote sensing applications in precision viticulture" Internet: http://ageweb.age.uiuc.edu/classes/abe425/Lectures/Networks/A%20ZigBee%20multi powered%20wireless%20acquisition%20device%20for%20remote%20sensing%20applications.pdf, Dec 3, 2007 [Feb. 25, 2012]

[14]Tuan Le Dinh. "Design and Deployment of a Remote Robust Sensor Network: Experiences from an Outdoor Water Quality Monitoring Network" Internet: http://eprints.qut.edu.au/33774/1/33774.pdf, Oct.11, 2009 [Feb 25, 2012]