PERFORMANCE ANALYSIS BETWEEN DIFFERENT ROUTING PROTOCOLS OF IEEE 802.15.4

SUBMITTED BY

AZMOL HOSSAIN AZAD

092-19-1130

SUMON HERMON COSTA

092-19-1084

MD. NAZMOL ALAM

093-19-1178

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering

SUPERVISED BY

MD. ZAHIRUL ISLAM

Lecturer

Department of ETE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

January 2014

APPROVAL

This Project titled **"Performance analysis between different routing protocols of IEEE 802.15.4"** has been submitted to the Daffodil International University in partial fulfillment of the requirement for the Degree of Bachelor of science in Electronics and Telecommunication Engineering. This thesis has been accepted as satisfactory by the honorable members of the Board of examiners after its presentation. The presentation has been held on January, 2014.

BOARD OF EXAMINERS

Dr. A.K.M. Fazlul Haque
Associate Professor and Head
Department of ETE
Faculty of Engineering
Daffodil International University

Chairman

Mr. Md. Taslim Arefin
Assistant Professor
Department of ETE
Faculty of Engineering
Daffodil International University

Internal Examiner

Mrs. Shahina Haque
Assistant Professor
Department of ETE
Faculty of Engineering
Daffodil International University

Internal Examiner

Dr. Subrata Kumar Aditya
Professor
Department of Applied Physics
Electronics and Communication Engineering
University of Dhaka

External Examiner

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for His divine blessing makes us possible to complete this project successfully.
The special thank goes to our helpful supervisor **Md. Zahirul Islam**, Lecturer, Department of ETE, Daffodil International University, Dhaka. Deep Knowledge & Keen interest of our supervisor in the field of wireless network influenced us to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this thesis.
We would like to express our heartiest gratitude to **Dr. A. K. M. Fazlul Haque, Associate Professor,** Head**,** Department of ETE ,Md. Taslim Arefin, Assistant Professor, Mrs. Shahina Haque, Assistant Professor and Dr. Subrata Kumar Aditya, Professor, Department of Applied Physics, Electronics and Communication Engineering, University of Dhaka, for their kind help to finish our thesis and also to other faculty members and the staffs of ETE department of Daffodil International University. We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.
Finally, we must acknowledge with due respect the constant supports and patients of our parents.

ABSTRACT

IEEE 802.15.4 is the standard for data communications with business and consumer devices which is designed around low-power consumption allowing batteries to essentially last forever. The ZigBee standard provides network, security and application support services operation on top of the IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer (PHY) wireless standard. It employs a suite of technologies to enable scalable, self-organizing, self-healing networks standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries and the mesh networking provides high reliability and larger range. ZigBee has been developed to meet the growing demand for capable wireless networking between numerous low-power devices. This paper provides a brief description of the newly introduced ZigBee standards. It focus on developing Network Simulator (NS2) models for the ZigBee protocol and the performance evaluation of these models. Several simulations were run and the results were analyzed for the different scenario.

DECLARATION

We hereby declare that, this project **"Performance analysis between different routing protocols of IEEE 802.15.4"** has been done by us under the supervision of **Md. Zahirul Islam, Lecturer, Department of ETE,** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of B.Sc in Electronics & Telecommunication Engineering degree.

Supervised By:

Md. Zahirul Islam
Lecturer
Department of ETE
Daffodil International University

Submitted By:

Azmol

AZMOL HOSSAIN AZAD
ID: 092-19-1130
DIU, ETE

Sumon.

SUMON HERMON COSTA
ID: 092-19-1084
DIU, ETE

Nazmol

MD. NAZMOL ALAM
ID: 093-19-1178
DIU, ETE

TABLE OF CONTENTS

CONTENTS **PAGES**

CHAPTERS **PAGES**

CHAPTER 6: RESULT ANALYSIS **29-32**

CHAPTER 7: CONCLUSION **33-34**

LIST OF FIGURE: **PAGES**

TABLE **PAGES**

Chapter 1
INTRODUCTION

1.1 General Introduction

Use of Wireless Personal Area Networks (WPAN) has steadily grown in recent years. Its popularity comes from the convenience of using wireless signals in open areas such as office space or home rather than having to lay out wires. Removing the constraints of length and troublesome physical installation of wires, wireless solutions provide much more diversity and potentially reduced cost.

ZigBee (IEEE 802.15.4-2006 standard) is a category in the IEEE 802 family, along with some of the well-known protocols such as Wi-Fi, Bluetooth which uses the 2.4 GHz industrial, and scientific and medical (ISM) radio band. ZigBee also utilizes 868 MHz and 915 MHz in different parts of the world according to local standards. Unlike Wi-Fi and Bluetooth, ZigBee was developed for low-rate WPAN (LR-WPAN) which feature long battery life by having low date rates.

The ZigBee protocol was designed to provide static, dynamic, or mesh network topologies supporting up to 65,000 nodes across large areas for industrial use. In order to handle faults caused by various environmental effects, the ZigBee protocol provides a self-healing ability for the network to detect and recover from network or communication link faults without human intervention. This is done through certain features of the ZigBee protocol such as clear channel assessment, retries and acknowledgments, and collision avoidance.

1.2 Goal of the research work

This thesis focuses on the performance analysis of different routing protocol emphasis on the definitions of different routing protocols define by IEEE 802.15.4.To analysis the performance, Network Simulator (NS-2) simulations is used for better result. The real life usage scenario, packet sending, receiving and packet lost is analyzed. The goal is to compare different type of routing protocol.

1.3 Organization of the thesis

The first chapter contains brief General Introduction about wireless personal area network and Goal of the research work.

Second chapter includes another brief detail of IEEE 802.15.4.Including with Introduction, WPAN, and Bluetooth.

Chapter three contains ZigBee technology. It has overview of ZigBee, Specifications, ZigBee layers, Topologies, Power System of ZigBee, Applications and Characteristics of ZigBee.

Chapter four has details description about ZigBee Protocols including Mobile Networks, Routing Algorithm, Protocols (DSR, DSDV, and AODV).

Chapter five includes ZigBee Simulations, also has NS2 general Figure and graphs .

Chapter six contains an important Results and Analysis.

Last of all Chapter seven contains Conclusion.

Chapter 2
IEEE 802.15

2.1 Introduction

IEEE 802.15 is a working group of the Institute of Electrical and Electronics Engineers (IEEE) IEEE 802 standards committee which specifies wireless personal area network (WPAN) standards. It includes seven task groups.

- 1 Task Group 1: WPAN / Bluetooth
- 2 Task Group 2: Coexistence
- 3 Task Group 3: High Rate WPAN
- 4 Task Group 4: Low Rate WPAN
  - 4.1 WPAN Low Rate Alternative PHY (4a)
  - 4.2 Revision and Enhancement (4b)
  - 4.3 PHY Amendment for China (4c)
  - 4.4 PHY and MAC Amendment for Japan (4d)
  - 4.5 MAC Amendment for Industrial Applications (4e)
  - 4.6 PHY and MAC Amendment for Active RFID (4f)
  - 4.7 PHY Amendment for Smart Utility Network (4g)
- 5 Task Group 5: mesh networking
- 6 Task Group 6: Body Area Networks
- 7 Task Group 7: visible light communication

Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)

2.2 Wireless Personal Area Network

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is maintained by the IEEE 802.15 working group. It is the basis for the ZigBee. IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end-user oriented approaches, such as Wi-Fi). The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more. Even lower rates can be considered with the resulting effect on power consumption. As already mentioned, the main identifying feature of IEEE 802.15.4 among WPANs is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality.

Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection.

IEEE 802.15.4-conformant devices may use one of three possible frequency bands for operation.

A personal area network (PAN) is a computer network used for communication among computerized devices, including telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). A wireless personal area network (WPAN) is a PAN carried over wireless network technologies such as

IrDA- Infrared Data Association- The Infrared Data Association (IrDA) is an industry driven interest group that was founded in 1993 by around 50 companies. IrDA provides specifications for a complete set of protocols for wireless infrared communications and the name "IrDA" also refers to that set of protocols. The main reason for using IrDA had been wireless data transfer over the “last one meter” using point and shoot principles.

Wireless USB- Wireless USB is a short-range, high-bandwidth wireless radio communication protocol created by the Wireless USB Promoter Group.

Bluetooth- Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength microwave transmissions in the ISM band from 2400–2480 MHz) from fixed and mobile devices, creating personal area networks (PANs).

Z-Wave- Z-Wave is a wireless communications protocol designed for home automation, specifically to remotely control applications in residential and light commercial environments.

ZigBee- ZigBee is a specification for a suite of high level communication protocols used to create personal area networks built from small, low-power digital radios. ZigBee is based on an IEEE 802.15 standard.

Body Area Network- A body area network (BAN), also referred to as a wireless body area network (WBAN) or a body sensor network (BSN), is a wireless network of wearable computing devices

The reach of a WPAN varies from a few centimeters to a few meters. A PAN may also be carried over wired computer buses such as USB and FireWire.

2.3 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength microwave transmissions in the ISM band from 2400–2480 MHz) from fixed and mobile devices, creating personal area networks (PANs). Created by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Bluetooth was standardized as IEEE 802.15.1.

2.4 Communication and connection:

A master Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone will necessarily begin as master, as initiator of the connection; but may subsequently prefer to be slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatter net, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode. The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion.

Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is difficult. The specification is vague as to required behavior in scatter nets.

Many USB Bluetooth adapters or "dongles" are available, some of which also include an IrDA adapter.

Chapter 3
ZIGBEE TECHNOLOGY

3.1 Overview of ZigBee

Zigbee is IEEE 802.15.4 Low-Rate Wireless Personal Area Network (LR-WPAN) in a large-scale Wireless Sensor Network (WSN) application.

- Low Data, Low Power Wireless Protocol
- Made to conduct wireless sensing and control applications
- No line of sight concerns
- 100-300 ft range
- Cheaper than Bluetooth & Wi-Fi.
- Supports Multiple Topologies

3.2 ZigBee Specifications

Name	**ZigBee 802.15.4**
Transmission Range (meters)	**1-100**
Battery Life(Days)	**100-1,000**
Network Sizes(# of nodes)	**>64,000**
Throughput(kb/s)	**20-250**

Table1: General ZigBee Specifications

3.3 ZigBee Layers

ZigBee consists of four layers. The top two (Application and Network) layers specifications are provided by the ZigBee Alliance to provide manufacturing standards. The bottom two (Medium Access Control and Physical) layers specifications are provided by the IEEE 802.15.4-2006 standard to ensure coexistence without interference with other wireless protocols such as Wi-Fi.

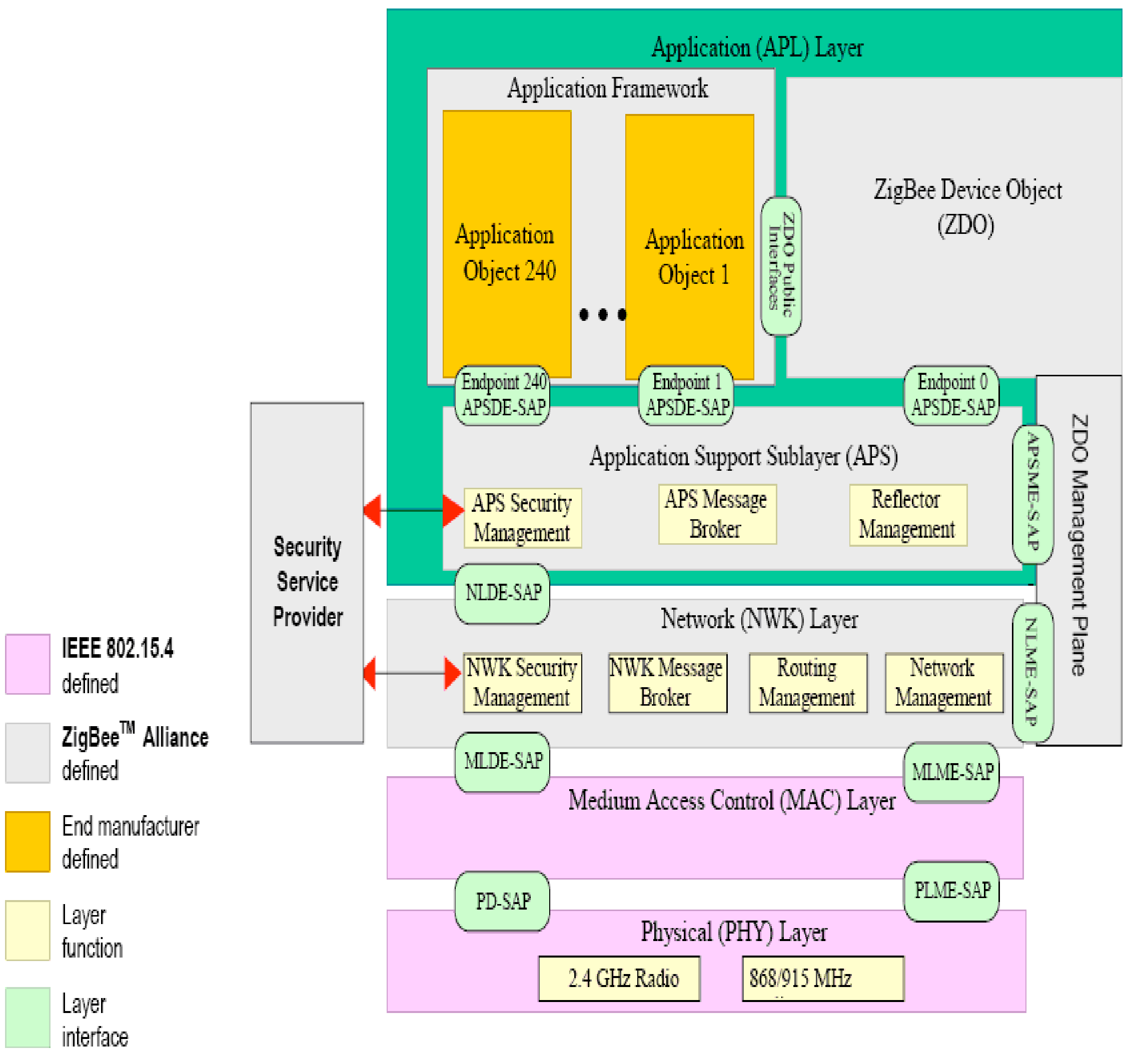

Figure1: Overview of ZigBee Layers.

3.3.1 Application Layer

Applications running on the ZigBee network are contained here. For example,
Applications to monitor temperature, humidity, or any other desirable atmospheric parameters can be placed on this layer for agricultural use. This is the layer that makes the device useful to the user. A single node can run more than one application. Applications are referenced with a number ranging from 1-240. Meaning there is a maximum of 240 applications on a ZigBee device. Application number 0 is reserved for a unique application that exists on all ZigBee devices. Another application number, 255, is also reserved. This number is used to broadcast a message to all applications on a node.

3.3.2 ZigBee Device Object (ZDO)

A special application is on every ZigBee device, and this is the ZigBee Device Object, or ZDO. This application provides key functions such as defining the type of ZigBee device (end device, router, and coordinator) a particular node is, initializing the network, and to also participate in forming a network.

3.3.3 Network Layer

A feature of ZigBee such as the self-healing mechanism is acquired through this layer. As Figure 1 shows, this layer provides network management, routing management, network message broker, and network security management.
This layer is defined by the ZigBee Alliance, which is an association of companies united to work for a better ZigBee standard.

3.3.4 Security Plane

The security plane spans across both the network layer and the application layer. It is here, that security measures such as AES-based encryption is implemented. Another security feature is message timeouts, which adds a frame counter on to each frame. Using this frame counter, the device can determine the age of the message it receives, and detect the possibility that an old message was recorded and is played back to the device (replay attack).

3.3.5 Medium Access Control Sub-Layer

This layer extracted from the IEEE 802.15.4 standard provides services to the network layer above, which is part of the ZigBee stack level. The MAC layer is responsible for the addressing of data to determine either where the frame is going, or coming from. It is also this layer that provides multiple access control such as CSMA/CA allowing for reliable transfer of data. Beaconing is another feature implemented through this layer. Finally, the MAC sub-layer can be exploited by higher layers to achieve secure communication (by measures such as an ACL).

3.3.6 Physical Layer

The physical layer is provided by the IEEE 802.15.4 standard. This standard manages the physical transmission of radio waves in different unlicensed frequency bands around the world to provide communication between devices within a WPAN. The bands are specified in the table below, pairing it with the area that the band is used in.

Frequency Range (MHz)	**Numbers of Channels Available**	**Region used**
868-868.6	1	Europe
902-928	10	North America
2400-2483.5	16	Worldwide

Table 2: Frequency Bands used in 802.15.4

This layer allows for channel selection to avoid radio interference, as well as data exchange with the layer above (MAC sub-layer) providing it with service.

3.4 Network Topologies

ZigBee networks can contain a mixture of three potential components. These Components are a ZigBee coordinator, a ZigBee router, and a ZigBee end device. Different types of nodes will have different roles within the network layer, but all Various types can have the same applications.

ZigBee coordinator – For every ZigBee network, there can be only one coordinator. This node is responsible for initializing the network, selecting the appropriate channel, and permitting other devices to connect to its network. It can also be responsible for routing traffic in a ZigBee network. In a star topology, the coordinator is at the center of the star, and all traffic from any end device must travel to this node. It is still possible for end devices to talk to another end device, but the message must be routed through the coordinator. In a tree topology, the coordinator is at the top of the tree, and in a mesh network, it is the root node of the mesh. A ZigBee coordinator can also take part in providing security services.

ZigBee Router – A router is able to pass on messages in a network, and is also able to have child nodes connect to it, whether it be another router, or an end device. Router functions are only used in a tree or mesh topology, because in a star topology, all traffic is routed through the center node, which is the coordinator. Routers can take place of end devices, but the routing functions would be useless in such cases. If the network supports beaconing, then a router can sleep when inactive, periodically waking up to notify the network of its presence.

ZigBee End Device – The power saving features of a ZigBee network can be mainly credited to the end devices. Because these nodes are not used for routing traffic, they can be sleeping for the majority of the time, expanding battery life of such devices. These nodes carry just enough function to talk to parent nodes, which can be either a router or a coordinator. 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 the following sections, we go into detail about the three different types of topology possible for a ZigBee network. The legend to all topology figures are shown below and each type of device is given a color code for easy viewing.

Figure2: Legend for ZigBee Devices

3.5 Zigbee Topology

Zigbee uses three type of topologies:

- Star Topology
- Tree Topology
- Mesh Topology

In details they are given bellow

3.5.1 Star Topology

In this simple topology, a coordinator is surrounded by a group of either end devices or routers. Even though routers are connected to the coordinator, their message relaying functions are not used. This type of topology is attractive because of its simplicity, but at the same time presents some key disadvantages. In the event that the coordinator stops functioning, the entire network is functionless because all traffic must travel through the center of the star. For the same reason, the coordinator could easily be a bottleneck to traffic within the network, especially since a ZigBee network can have more than 60000 nodes.

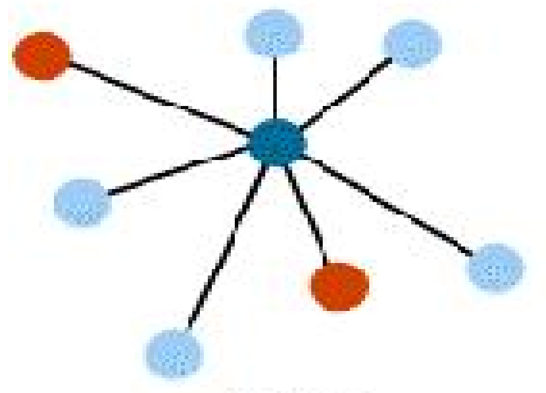

Figure3: Star Topology

3.5.2 Tree Topology

In a tree network, a coordinator initializes the network, and is the top (root) of the tree. The coordinator can now have either routers or end devices connected to it. For every router connected, more child nodes can connect to the router. Child nodes cannot connect to an end device because it does not have the ability to relay messages. This topology allows for different levels of nodes, with the coordinator being at the highest level. For messages to be passed to other nodes in the same network, the source node must pass the message to its parent, which is the node higher up by one level of the source node, and the message is continually relayed higher up in the tree until it can be passed back down to the destination node. Because the number of potential paths a message can take is only one, this type of topology is not the most reliable topology. If a router fails, then all of that router's children are cut off from communicating with the rest of the network.

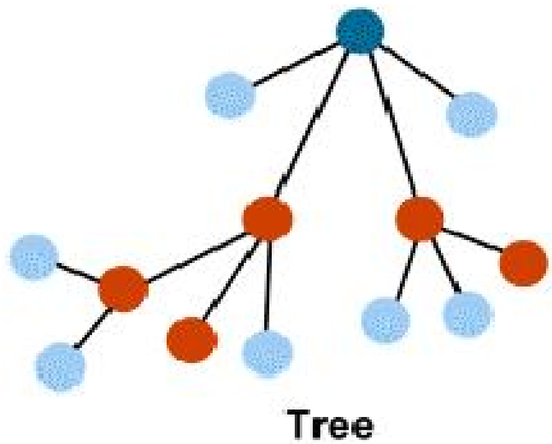

Figure4: Tree Topology

3.5.3 Mesh Topology

A mesh topology is the most flexible topology of the three. Flexibility is present because a message can take multiple paths from source to destination. If a particular router fails, then ZigBee's self healing mechanism (aka route discovery) will allow the network to search for an alternate path for the message to take. In our project, one of the scenarios is to investigate this feature by removing a router from the network during operation, and seeing the end devices find an alternate path to communicate with the coordinator.

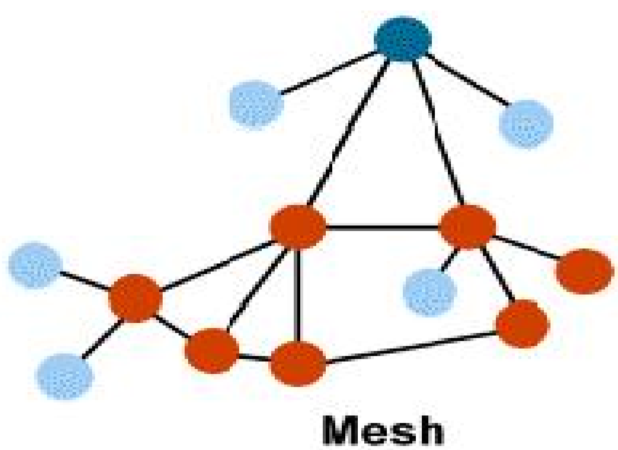

Figure5: Mesh Topology

3.6 Power system for Zigbee

ZigBee technology is completely suitable for the application in power monitoring system and it can provide reliable protection for the operation of electric power systems. Following are the points justifying this statement.

- ✓ Large capacity. Each ZigBee network can support up to 65,000 nodes. It is suitable for the complex structure of power system.
- ✓ The maximum transfer rate can be up to 250 kbps which is in full compliance with data rate needed by the power monitoring system.
- ✓ Strong anti-interference. For the interferences from environments such as cars, mobile phones, generators, power distribution room, transformers and so on, ZigBee technology can prevent well there is no need to hire the public network, so there is no need to pay huge amounts of operating costs .
- ✓ Low power-cost. In low power standby mode, two 5th ordinary dry-cell batteries can be used for 6 months to 2 years. This is the unique advantage of ZigBee to ensure that the monitoring system continue working in the event of the power failure.
- ✓ Short time delay. The delay usually lasts for 15 ~ 20 ms, so it is very suitable for industrial real-time data transmission system.
- ✓ Strong safety. The encryption algorithm uses AES-128 which provides the functions of integrity data checking and authentication.

3.7 Characteristics of ZigBee

ZigBee is poised to become the global control/sensor network standard. It has been designed to provide the following features:

- Low cost (device, installation, maintenance). Low cost to the users means low device cost, low installation cost and low maintenance. ZigBee devices allow batteries to last up to years using primary cells (low cost) without any chargers (low cost and easy installation). ZigBee's simplicity allows for inherent configuration and redundancy of network devices provides low maintenance.

- Low power consumption, with battery life ranging from months to years.
- High density of nodes per network: ZigBee's use of the IEEE 802.15.4 PHY and MAC allows networks to handle any number of devices. This attribute is critical for massive sensor arrays and control networks.
- Maximum data rates allowed for each of the frequency bands are fixed as 250 kbps @2.4 GHz, 40 kbps @ 915 MHz, and 20 kbps @868 MHz
- Different topologies like: star, peer-to-peer, mesh
- High throughput and low latency for low duty-cycle applications (<0.1%).
- Channel access using Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA).
- Addressing space of up to 64 bit IEEE address devices, 65,535 networks.
- 70-100m range.
- Fully reliable "hand-shacked" data transfer protocol.

3.8 Applications of ZigBee

ZigBee networks consist of multiple traffic types with their own unique characteristics, including periodic data, intermittent data, and repetitive low latency data. The characteristics of each are as follows:

• **Periodic data –** usually defined by the application such as a wireless sensor or meter. Data typically is handled using a beaconing system whereby the sensor wakes up at a set time and checks for the beacon, exchanges data, and goes to sleep.

• **Intermittent data –** either application or external stimulus defined such as a wireless light switch. Data can be handled in a beaconless system or disconnected. In disconnected operation, the device will only attach to the network when communications is required, saving significant energy.

• **Repetitive low latency data –** uses time slot allocations such as a security system. These applications may use the guaranteed time slot (GTS) capability. GTS is a method of QoS that allows each device a specific duration of time as defined by the PAN coordinator in the Super frame to do whatever it requires without contention or latency. Reduced Function Device (RFD) meter wakes up and listens for the beacon from the PAN coordinator, if received, the RFD requests to join the network. The PAN coordinator accepts the request. Once connected, the device passes the meter information and goes to sleep. This capability provides for very low duty cycles and enables multi-year battery life. Intermittent traffic types, such as wireless light switches, connect to the network when needed to communicate (i.e. turn on a light). For repetitive low latency applications a guaranteed time slot option provides for Quality of Service with a contention free, dedicated time slot in each super frame that reduces contention and latency. Applications requiring timeliness and critical data passage may include medical alerts and security systems. In all applications, the smaller packet sizes of ZigBee devices results in higher effective throughput values compared to other standards. ZigBee networks are primarily intended for low duty cycle sensor networks (<1%). A new network node may be recognized and associated in about 30 ms.

Waking up a sleeping node takes about 15 ms, as does accessing a channel and transmitting data. ZigBee applications benefit from the ability to quickly attach information, detach, and go to deep sleep, which results in low power consumption and extended battery life.

The key characteristics of ZigBee, Wi-Fi and Bluetooth

	ZigBee	**Wi-Fi**	**Bluetooth**
Range	10-100 meters	50-100 meters	10 – 100 meters
Networking Topology	Ad-hoc, peer to peer, star, or mesh	Point to hub	Ad-hoc, very small networks
Operating Frequency	868 MHz (Europe) 900-928 MHz (NA), 2.4 GHz (worldwide)	2.4 and 5 GHz	2.4 GHz

Complexity (Device and application impact)	Low	High	High
Power Consumption (Battery option and life)	Very low (low power is a design goal)	High	Medium
Security	128 AES plus application layer security	High and password protected	64 and 128 bit encryption
Typical Applications	Industrial control and monitoring, sensor networks, building automation, home control and automation, toys, games	Wireless LAN connectivity, broadband Internet access	Wireless connectivity between devices such as phones, PDA, laptops, headsets

Table3: key characteristics of ZigBee, WI-FI and Bluetooth

Chapter 4
ZIGBEE PROTOCOLS

4.1 Mobile networks

There are two approaches for wireless communication between two hosts .The first is the centralized cellular network in which each mobile is connected to one or another fixed base stations (each base station is responsible for another cell),so that a communication between two mobile stations require them to involve one or more base stations. A second decentralized approach consists based of an ad-hoc network between users that wish to communicate between each other. Due to the more limited range of a mobile terminal (with respect to a fixed base station), this approach requires mobile nodes not only to be sources or destination odd packets but also to forward packets between other mobiles. Cellular station has a much larger range than ad-hoc networks. However ad-hoc networks have that advantage of being quickly deployable as they do not require an existing infrastructure.

In cellular networks the wireless part is restricted only to the access or a network, and within that network classical routing protocols can be used. Ad-hoc network in contrast rely in special routing protocols that have to be adapted to frequent topology changes.

To model well cellular networks, often sophisticated simulation tools of the physical radio channel are needed as well as the simulation of power control mechanism. Ns do not have an advanced physical layer module (although it contains some modeling features of radio channels) .In ad-hoc networks in contrasts the routing protocols are central .ns allow to simulate the main existing routing as well as transport and applications that use them. Moreover it allows taking into account the MAC and link layer, the mobility and some basic feature of the physical layer.

The current routing protocols implemented by ns are

- DSDV-Destination sequenced Vector
- DSR-Dynamic Source Routing
- AODV-Ad-hoc On demand Distance Vector.

4.2 The routing Algorithms

There are several approaches in conventional routing algorithms in traditional wireless networks, and some ideas from these are also used in ad-hoc networks. Among the traditional approaches we shall mention the following:

1. **Link state-** Each node maintains a view if the complete topology with a cost over link. Each node periodically broadcast the link costs of its outgoing link to all other nodes using flooding. Each node updates its vies of the networks and applies a shortest path algorithm for choosing the next -hop for each destination.

2. **Distance Vector**-Each node only monitors the cost or its outgoing links. Instead of broadcasting the information to all nodes, it's periodically broadcast to each neighbor an estimate of the shortest distance or every other node in the network. The receiving nodes use this information to recalculate routing tables using a shortest path algorithm. This method id more compilation efficient, easier to implement and requires less storage space than link state routing.

3. **Source routing** -Routing decisions are takes at the source and packets carry along the complete path they should take.

4. **Flooding -**The sources sends the information to all neighbors who continue to sending it to their neighbor etc. By using sequence numbers for the packets a node is able to relay a packet only once.

Next we describe the Ad-hoc routing protocols complemented in NS2.

4.2.1 Destination Sequenced Distance Vector-DSDV

DSDV is a distance vector routing protocol .Each node has a routing table that indicates for each destination, which the next hop and number of hops to the destination. Each node periodically broadcast routing updates. A sequence number is used to tag each route .It shows the freshness of the route: a route with higher sequence number is more favorable. In addition among two routes with the same sequence number, the one with less hops is more favorable. If a node detects that a route to a destination has broken, then its hop number is set infinity and its sequence number upload (increased) but assigned an odd number: even numbers corresponds to sequence numbers of connected paths.

4.2.2 Ad-hoc On Demand Distance Vector-AODV

AODV is a distance vector type routing .It does not require nodes to maintain routes to destinations that are not actively used. As long as the endpoints of a communication connected have valid routes to each other. AODV does not play a role.

The protocol uses different messages to discover and maintain links. Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs).These message types are received via UDP, and normal IP header processing applies.

AODV uses a destination sequence number for each route entry. The destination sequence number is created any the destination for any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and allows knowing which of several routes is more "fresh". Given the choice between two routes to a destination a requesting node always selects the one with the greatest sequence number.

When a node wants to find a route to another owner, it broadcast a RREQ to all the network till either the destination is reached or another node is found with a "fresh enough" route to the destination (A "fresh enough" route is a valid route entry for the destination whose associated sequence number id at least as great as that contained in RREQ).Then a RREP is sent back to the source and the discovered route is made available.

Nodes that are part of an active route may offer connectivity information by broadcasting periodically local Hello messages (Special RREP messages) to its immediate neighbors .If Hello messages stoop arriving from a neighbor beyond some given time threshold, the connection is assumed to be lost.

When a node detects that a route to a neighbor node is not valid it removes the routing entry and sends a RERR message to neighbor that are active and use the route: this is possible by maintaining active neighbor lists. This procedure is repeated at node receive RERR messages. A source that receives an RERR can reinitiate a RREQ messages.

AODV does not allow handling unidirectional links.

4.2.3 Dynamic Source Routing-DSR

Designed for mobile ad-hoc networks with up to around two hundred nodes with possibly high mobility rate. The protocol works "on demand", i.e. without any periodic updates. Packets carry along the complete path they should take. This reduces overheads for large routing updates at network. The nodes store in their cache all knows routes. The protocol is composed of route discovery and route maintenance. At route discovery a source requesting to send a packet to a destination broadcast a Route Request (RREQ) packet. Nodes receiving RREQ search in their Route Cache for a route to the destination .If a route is not found then the RREQ is further transmitted and the node with a route to the destination are reached .The route back can be retrieved by the reverse hop record. As routes need not be symmetric, DSR checks the Route Cache of the replying node and if a route is found it is used instead. Alternatively one can **piggyback** the reply on a RREQ targeted at the originator .Hence unidirectional links can be handled.

4.3 Route maintenance: When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that data can flow over the link from that node to the next hop. An acknowledgement can provide confirmation that a link is capable of carrying data. acknowledgement are often already part of the MAC protocol in use (such as the link-layer acknowledgement frame defined by IEEE 802.11)or are "passive acknowledgement" i.e. a node knows that its packet is received by an intermediate node since it can hear that the intermediate node further forwards it. If such acknowledgement are not available then a node can request an acknowledgement (which can be sent directly to the source using another route).Acknowledgement may be requested several times (till some given bound),and in the persistent absence of acknowledgement ,the route is removed from the Route Cache and return a "Route Error" to each node that has sent a packet routed over that link since an acknowledgement was last received. Nodes overhearing or forwarding packets should make its all carries routing information to update its own Route Packet.

Chapter 5

ZIGBEE SIMULATION USING NS-2

5.1 A 3 node example for ad-hoc simulation with DSDV

DSDV Protocol Command:

```
set val(chan)       Channel/WirelessChannel        ;# channel type
set val(prop)       Propagation/TwoRayGround       ;# radio-propagation model
set val(netif)      Phy/WirelessPhy                ;# network interface type
set val(mac)        Mac/802_15                     ;# MAC type
set val(ifq)        Queue/DropTail/PriQueue        ;# interface queue type
set val(ll)         LL                             ;# link layer type
set val(ant)        Antenna/OmniAntenna            ;# antenna model
set val(ifqlen)     50                             ;# max packet in ifq
set val(nn)         3                              ;# number of mobilenodes
set val(rp)         DSDV                           ;# routing protocol
set val(x)          500                            ;# X dimension of topography
set val(y)          400                            ;# Y dimension of topography
set val(stop)       150                            ;# time of simulation end
```

5.2 A 3 node example for ad-hoc simulation with DSR

DSR Protocol command:

```
set val(chan)       Channel/WirelessChannel        ;# channel type
set val(prop)       Propagation/TwoRayGround       ;# radio-propagation model
set val(netif)      Phy/WirelessPhy                ;# network interface type
set val(mac)        Mac/802_15                     ;# MAC type
set val(ifq)        Queue/DropTail/PriQueue        ;# interface queue type
set val(ll)         LL                             ;# link layer type
set val(ant)        Antenna/OmniAntenna            ;# antenna model
```

```
set val(ifqlen)      50                          ;# max packet in ifq
set val(nn)          3                           ;# number of mobilenodes
set val(rp)          DSR                         ;# routing protocol
set val(x)           500                         ;# X dimension of topography
set val(y)           400                         ;# Y dimension of topography
set val(stop)        150                         ;# time of simulation end
```

5.3 A 3 node example for ad-hoc simulation with AODV

AODV Protocol Command:

```
set val(chan)        Channel/WirelessChannel     ;# channel type
set val(prop)        Propagation/TwoRayGround    ;# radio-propagation model
set val(netif)       Phy/WirelessPhy             ;# network interface type
set val(mac)         Mac/802_15                  ;# MAC type
set val(ifq)         Queue/DropTail/PriQueue     ;# interface queue type
set val(ll)          LL                          ;# link layer type

set val(ant)         Antenna/OmniAntenna         ;# antenna model
set val(ifqlen)      50                          ;# max packet in ifq

set val(nn)          3                           ;# number of mobilenodes
set val(rp)          AODV                        ;# routing protocol
set val(x)           500                         ;# X dimension of topography
set val(y)           400                         ;# Y dimension of topography
set val(stop)        150                         ;# time of simulation end
```

5.4 General Figure

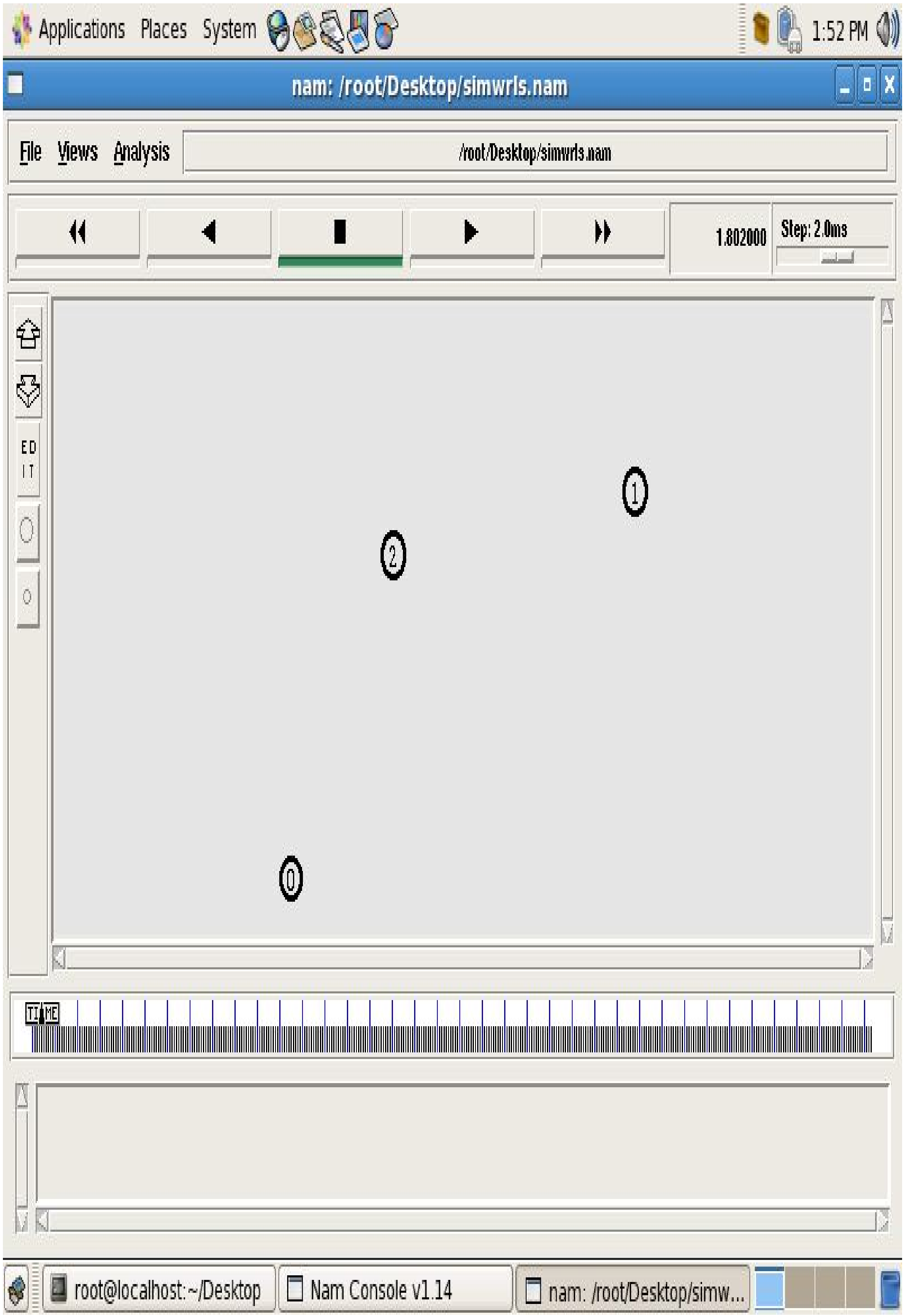

Figure6

5.5 DSDV Graph

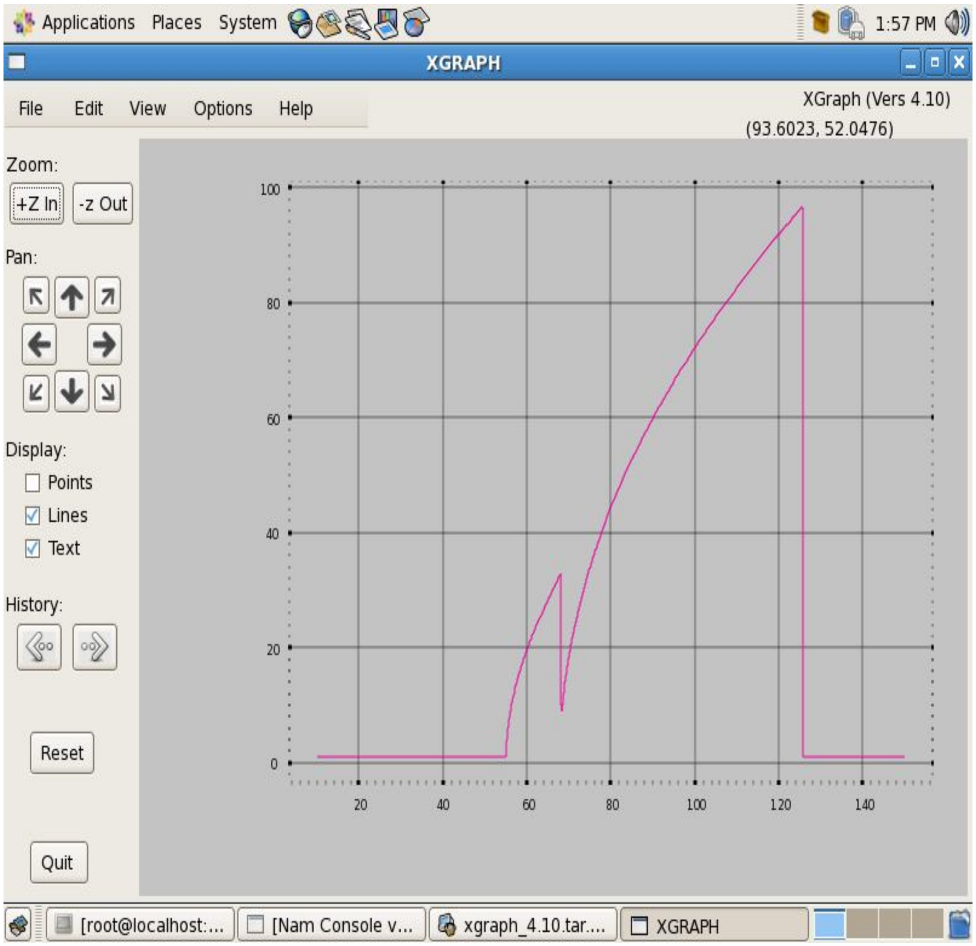

Figure7: (DSDV): Average throughput of receiving packet at node verses packet size (bytes) (tr)

At the beginning the nodes are too far away and a connection cannot be set. The first TCP signaling packet is transmitted at time 10 but the connection cannot be opened. Meanwhile nodes 0 and 1 start moving towards node 2. After 6 second (time) a second reattempt occurs but still the connection cannot be established and the timeout value is doubled to 12 sec. At time 28 another transmission attempt occurs. The timeout value is doubled again to 24 sec and again to 48 sec. Thus at only at time 80 sec the connection has been established. The mobile get further apart till the direct link bakes. The routing protocol is too slow to react and to create an alternative route.

5.6 AODV Graph

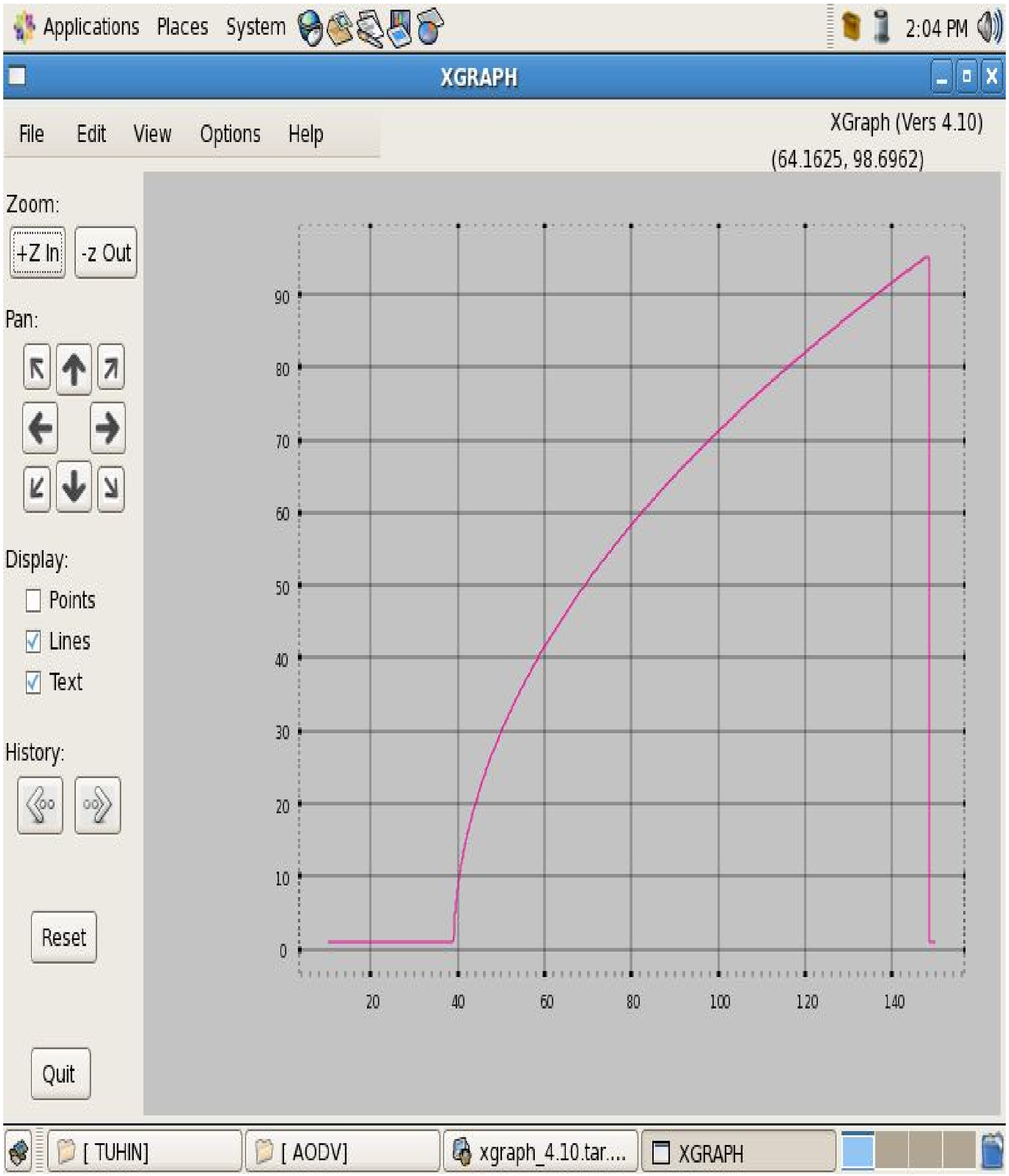

Figure8: (AODV): Average throughput of receiving packet at node verses packet size (bytes) (tr)

5.7 DSR Graph

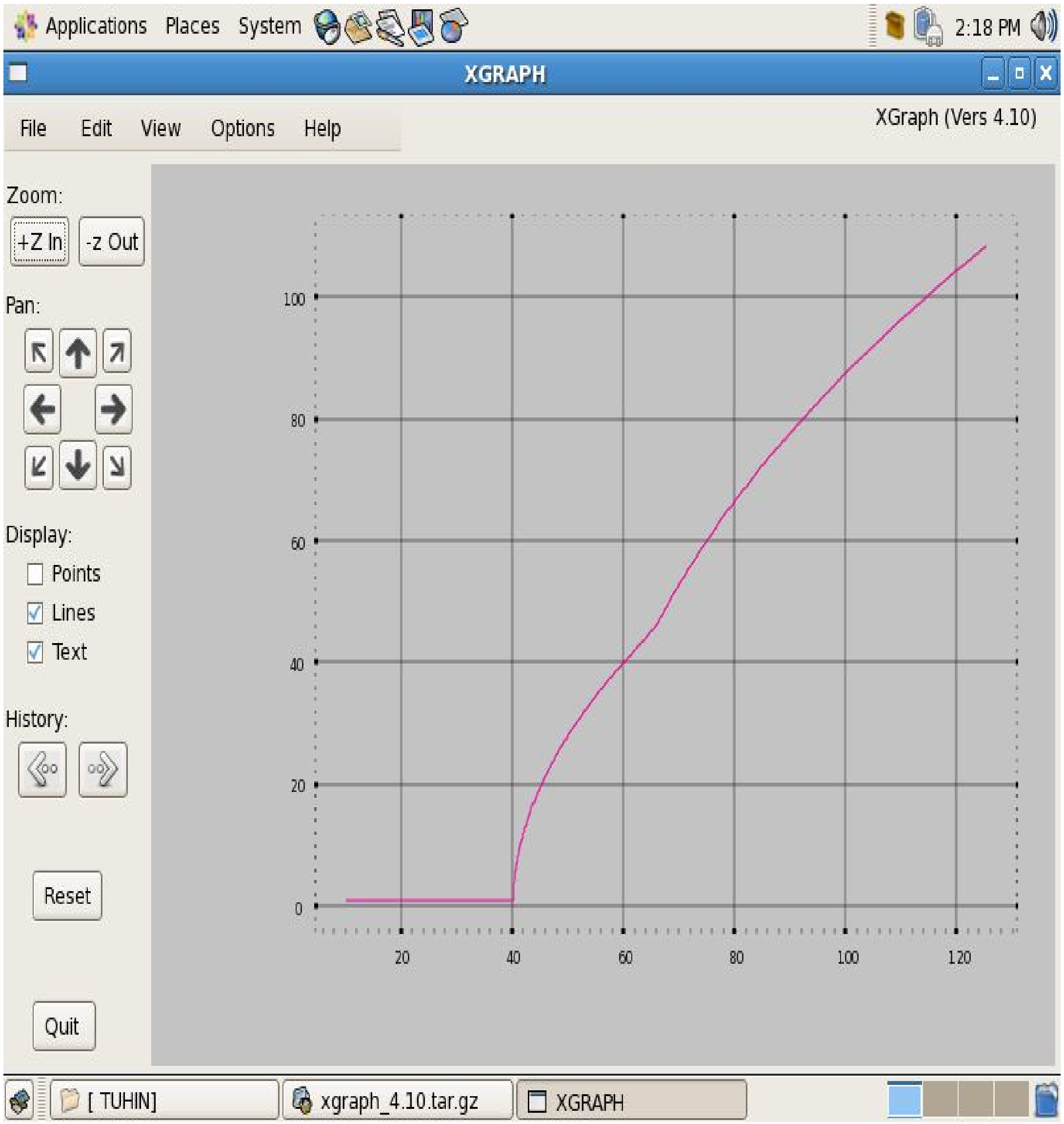

Figure9: (DSR): Average throughput of receiving packet at node verses packet size (bytes) (tr)

Chapter 6

RESULT ANALYSIS

6.1 DSDV Total Packet Figure

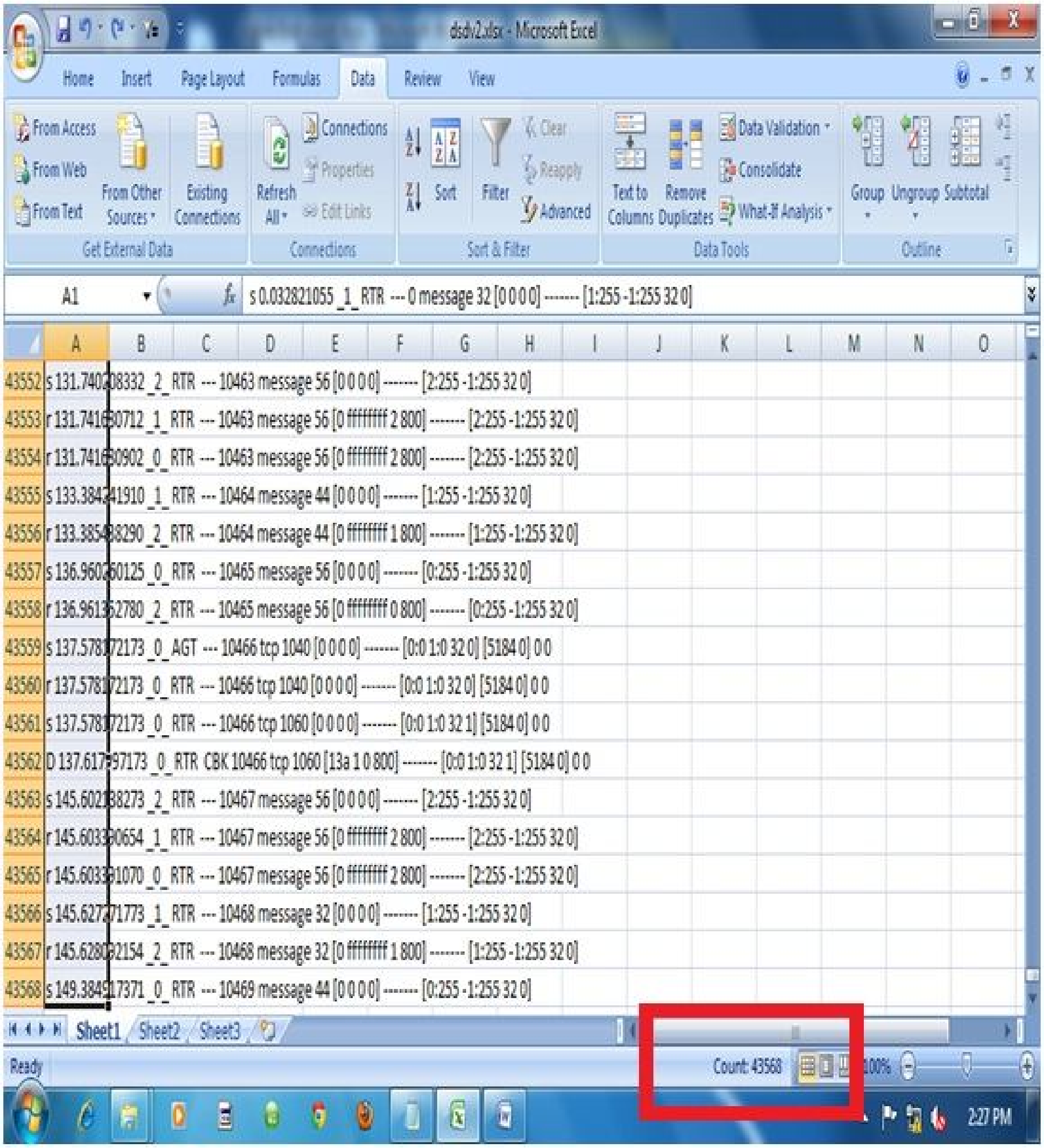

Figure10: 6.1.1 (DSDV)

6.1.2 DSDV Total Sender Packet Figure

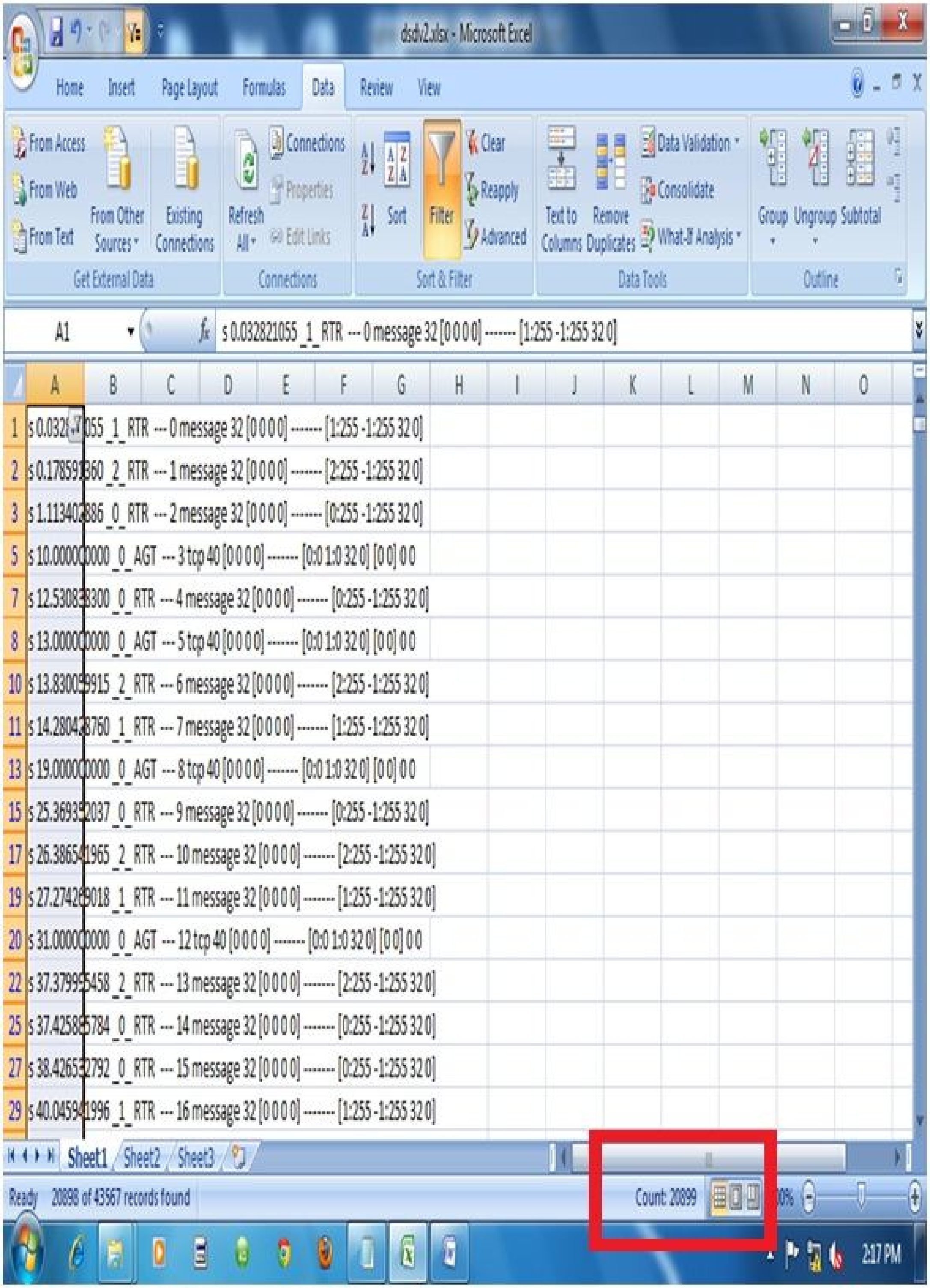

Figure11: 6.1.2 (DSDV-Packet Send)

6.1.3 DSDV Total Received Packet Figure

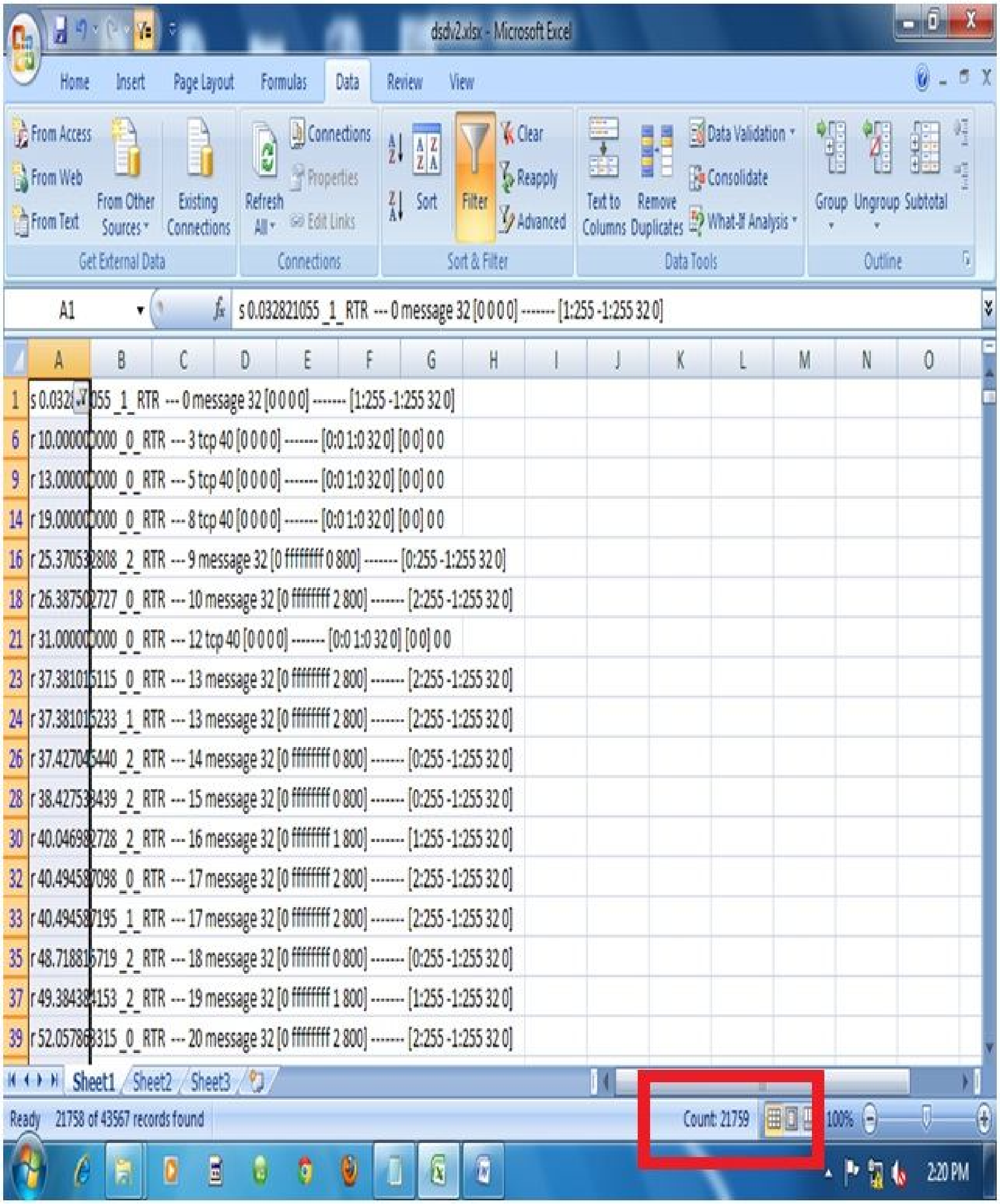

Figure12: 6.1.3(DSDV-Packet Received)

6.2 Comparison on DSDV, AODV and DSR

	Total Packet	**Packet Send**	**Packet Receive**	**Packet loss**
DSDV	**43568**	**20899**	**21759**	**910**
AODV	**54519**	**18184**	**27242**	**9093**
DSR	**76598**	**37369**	**37337**	**1892**

Table4: Comparison on DSDV, AODV and DSR

6.3 Analysis

From our above result, we can analysis that DSDV has best performance with fewer packets lost. DSR is suitable for network with most less packet loss but AODV has highest packet lost in the network and it is not moderate for use. For average use DSDV is the best.

Chapter 7

CONCLUSION

7.1 CONCLUTION

It is likely that ZigBee will increasingly play an important role in the future of computer and communication technology. In terms of protocol stack, ZigBee`s 32 KB is about one-third of the stack size necessary in other wireless technologies (for limited capability end devices, the stack size is as low as 4KB).The IEEE 802.15.4-based ZigBee is designed for remote controls and sensors, which are very many in number, but need only small data packets and mainly, extremely low power consumption for long life. Therefore they are naturally different in their approach to their respective applications arenas. ZigBee technology is designed to best suit these applications, for the reason that it enables reduced cost of development and very fast market adoption.

This comparison study is an attempt towards a comprehensive performance evaluation of three commonly used mobile ad hoc routing protocols (DSR, DSDV and AODV) .Simulation was done with simulation time of 150 seconds and with some varying parameters, using the latest simulation environment ns-2. For short-range wireless communication in AODV, DSR and DSDV are used and the results are compared on the issues like throughput of sent packets, dropped packets, end-to-end delay and are very important for detailed performance evaluation of any networking protocol. We can summarize our final conclusion from our experimental results as follows:

- Increase in the density of nodes yields to an increase in the mean End-to-End delay.
- Increase in the pause time leads to a decrease in the mean End-to-End delay.
- Increase in the number of nodes will cause increase in the mean time for loop detection.

In short, DSDV has the best all round performance. DSR is suitable for networks with moderate mobility rate. It has low overhead that makes it suitable for low bandwidth and low power network. AODV is normal for network with moderate mobility rate.

For the future work, this area will investigate not only the comparison between AODV, DSR and DSDV routing protocols but more on the vast areas, extensive complex simulations could be carried out using other existing performance metrics, in order to gain a more in-depth performance analysis of the ad hoc routing protocols. Other new protocols performance could be studied too.

REFERENCES:

1. www.zigbee.org
2. en.wikipedia.org/wiki/ZigBee
3. www.webcrawler.com
4. www.info.com/Zigbee+Wireless
5. https://www.digi.com/technology/rf-articles/wireless-zigbee
6. en.wikipedia.org/wiki/Mobile_ad_hoc_network
7. https://datatracker.ietf.org/wg/manet/charter.