Master Thesis
Computer Science
Thesis no: MCS-2009-14
Ma y 2009

Evaluation of Routing Protocols in Wireless Sensor Networks

Muhammad Ullah, Waqar Ahmad

Department of
School of Computing
Blekinge Institute of Technology
Soft Center
SE-37225 RONNEBY
SWEDEN

This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):

Muhammad Ullah,
Address: NR922,Villa Voila, 37236 Ronneby, Sweden
E-mail: madullay7281@gmail.com

Waqar Ahmad
Address: Folkparksvagen: 22:18 37240 Ronneby, Sweden
Email: waqarciit@gmail.com

University advisor:
Olle Lindeberg
Department of Interaction and System Design

Department of
School of computing
Blekinge Institute of Technology
SE – 372 25 Ronneby Sweden

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : + 46 457 102 45

ABSTRACT

The evolution of wireless communication and circuit technology has enabled the development of an infrastructure consists of sensing, computation and communication units that makes administrator capable to observe and react to a phenomena in a particular environment. The building block of such an infrastructure is comprised of hundreds or thousands of small, low cost, multifunctional devices which have the ability to sense compute and communicate using short range transceivers known as sensor nodes. The interconnection of these nodes forming a network called wireless sensor network (WSN).

The low cost, ease of deployment, ad hoc and multifunctional nature has exposed WSNs an attractive choice for numerous applications. The application domain of WSNs varies from environmental monitoring, to health care applications, to military operation, to transportation, to security applications, to weather forecasting, to real time tracking, to fire detection and so on. By considering its application areas WSN can be argue as a traditional wired or wireless network. But in reality, these networks are comprised of battery operated tiny nodes with limitations in their computation capabilities, memory, bandwidth, and hardware resulting in resource constrained WSN.

The resource constrained nature of WSN impels various challenges in its design and operations degrading its performance. On the other hand, varying numbers of applications having different constraints in their nature makes it further challenging for such resources constrained networks to attain application expectations. These challenges can be seen at different layer of WSNs starting from physical layer up to application layer. At routing layer, routing protocols are mainly concerned with WSN operation. The presence of these challenges affects the performance of routing protocols resulting in overall WSN performance degradation.

The aim of this study is to identify the performance challenges of WSN and analyze their impact on the performance of routing protocols. For this purpose a thorough literature study is performed to identify the issues affecting the routing protocols performance. Then to validate the impact of identified challenges from literature, an empirical study has been conducted by simulating different routing protocols, taking into consideration these challenges and results are shown. On the basis of achieved results from empirical study and literature review recommendations are made for better selection of protocol regarding to application nature in the presence of considered challenges.

ACKNOWLEDGMENT

In the name of Allah who is the most gracious, merciful and creator of this universe. We are thankful to Him who blessed us with abilities to do this thesis work.

We would like to acknowledge our supervisor Olle Lindeberg, for his frankness and candidness to our research points of view, person with great experiences, who was the real source of encouragement during the entire work of thesis. We are grateful for his invaluable suggestion, fruitful discussions, feedback and patience.

We would also like to acknowledge all the faculty, staff and friend at BTH for their all time support and kindness.

We are thankful to Mr. Ibrar Ali Shah, a great friend, who encouraged and guide us throughout the thesis process.

Huge thanks go to Mr. Arshad Ahmad, a great friend, a great person for his endless support, encouragement, guidance and constant source of motivation not only during the thesis process but throughout the master studies. We also want to acknowledge that this thesis could not be achieved within this time frame if it was not for his review.

Last but not the least; we are thankful to our families for their kind support, encouragement and dedication of their whole life to make it possible to peruse higher studies in Sweden. Certainly, without their moral, emotional and financial support it would not be possible for us to accomplish this work.

List of Acronyms

ACQUIRE	Active Query forwarding In sensor network
APS	Ad-hoc positioning system
ATD	Analogue to digital
APS	Ad-hoc positioning system
ASYM	Asymmetric
CPU	Central Processing Unit
DD	Directed Diffusion
DSR	Dynamic Source Routing
EAR	Energy Aware Routing
FTP	File Transfer Protocol
GAP	Geographic adaptive fidelity
GOAFR	Greedy other adaptive face routing
GEAR	Geographic and energy aware routing
GEAR	Geographic distance routing
HPAR	Hierarchical Power-Active Routing
MMSPEED	Multi path and Multi SPEED
MECN	Minimum energy communication network
MCFA	Minimum Cost Forwarding Algorithm (MCFA)
MANETs	Mobile Ad hoc Networks
MAC	Medium Access Control
MPR	Multipoint Relays
OLSR	Optimized Link State Routing Protocol
OPNET	Optimized Network Engineering Tool
QoS	Quality of service
RREQ	Route Request
RREP	Route Replay
SAR	Sequential Assignment Routing (SAR)
SPIN	Sensor Protocols for Information via Negotiation (SPIN)
SYM	Symmetric
TEEN	Threshold sensitive energy efficient sensor network protocol
UART	Universal Asynchronous Receive and Transmit
WSN	Wireless Sensor Network
WLAN	Wireless Local Area Network

Table of Contents

LIST OF FIGURES

INTRODUCTION

Wireless communication endowed with numerous advantages over traditional wired network and enables to develop small, low-cost, low power and multi-functional sensing devices. These small sensing devices have the capabilities of sensing, computation, self organizing and communication known as sensors. Sensor is a tiny device used to sense the ambient condition of its surroundings, gather data, and process it to draw some meaningful information which can be used to recognize the phenomena around its environment. These sensors can be grouped together using mesh networking protocols to form a network communicating wirelessly using radio frequency channel. The collection of these homogenous or heterogeneous sensor nodes called wireless sensor network (WSN) [1].

The ability of low cost, small size and easy deployment of the sensor nodes make it possible to deploy them in a large number in an area to be investigated [2]. Interestingly, unlike other networks that performs poor with growth in their networks size, WSN get stronger and performs better as much as number of nodes exceeds. In addition, without any complexity in configuration network size can be extended simply by adding additional number of nodes. Therefore, it is said that connectivity using mesh networking will occupy any possible communication path in search of destination using node to node hoping.

Owing all these considerable advantages, application domain of WSNs varies from environmental monitoring, to health care applications, military operation, to transportation, to security applications, to weather forecasting, to real time tracking [3, 4].

WSN is the collection of hundreds or thousands of tiny sensor nodes having the abilities of sensing, computations and communication among each other or with the base station. The functional architecture of sensor nodes consists of four units which are sensor, CPU, radio and power. Among these four units, three units are responsible for accomplishing a task while power unit supplies energy to the overall operation. The function of sensing unit is to measure physical conditions of the environment like temperature, humidity and pressure [5, 6], the processing unit is mainly responsible for processing the data (signals) while communication unit transmit data from the sensor unit to the user through the base station (BS) [7]. These tiny sensor nodes are scattered throughout the investigation area to acquire information from the environment, process it and then transfers it to the base station [4].

By considering WSNs application domain one can presume it like a traditional wired or wireless network. But the reality is very different because traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, enough communication range and computational capabilities [18, 39]. But on the other side, WSNs have a resource constrained nature with respect to energy, computational capabilities and memory resources [9, 3]. Unfortunately despite these constrained resources we have the same expectation from the WSNs as that from the traditional computer networks.

The resource constrained nature of WSNs impels numerous challenges in its design and operations degrading its performance. These challenges include significantly communication management, unattended operational nature, network lifetime and fault-tolerance [10]. Therefore, on one side, to improve WSNs performance these challenges are subjected to be investigated. While on other side, the performance of WSN can be achieved significantly by efficient resource utilization. Resource utilization can be enhanced by focusing on factors involved in WSN operations. Communication in WSN has certainly influences on its resources. The communication pattern of WSNs involves node to node, note to BS and BS to node communication. This communication involves optimal route selection, route maintenance and other computations to compete with user expectation and ensure network performance [7].

According to [11] route selection of each message in communication pattern result in either network delay by choosing long routes consisting many sensor nodes or degrade network lifetime in terms of short routes resulting in depleted batteries. Besides, unnecessary load on a network and delay in operation not only degrades application quality but also wastes network resources. Furthermore, as WSNs deployment can be seen in critical applications so the demands for application vary according to its nature. Different applications have different demands from network which cannot be avoided. Therefore, there is a need of efficient routing protocol which should not only be appropriate for the application demands but also assist network with respect to its limited resources and performs well. To identify and select best routing protocol for an application, it is required to understand the strict demands of that application first and then to select the appropriate protocol to be implemented and simulated. There are several routing protocols developed for WSNs. All these routing protocols have different competing features and qualities. Therefore, the selection of correct routing protocol is vital.

In this thesis we studied two main WSNs application classes i.e. data gathering and object tracking. We identified the strict requirement for each of these classes. Then protocols were studied in details and design and communication challenges for routing protocols were identified. Afterwards, to verify the affect of identified challenges on protocols two different protocols were implemented (simulated) using different scenarios. Selected performance metrics were used as evaluation criterion for protocols considering application demands as well.

Thesis Outlines

The chapter wise organization of this thesis is as follows. Chapter 2 explains the background of the research by introducing the fundamental concepts of WSNs, its application classes and its routing protocols families followed by an overview of related work. Chapter 3 describe problem in detail by emphasizing on protocol’s suitability. Routing challenges identified from literature are also presented in this chapter. Proposed study is explained in Chapter 4, describing selected application classes of WSN, protocols to be evaluated and performance metrics to be used as an evaluation criterion. Chapter 5 explains empirical study, simulation environment and network design. Routing challenges identified from literature are verified by simulating routing protocols in the presence of identified challenges and results with discussion are presented in chapter 6. Chapter 7 concludes the thesis by presenting conclusion and directions for future research.

Chapter 1: BACKGROUND

WIRELESS SENSOR NETWORKS

Wireless sensor network (WSN) is the collection of homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel. The basic task of sensor networks is to sense the events, collect data and send it to their requested destination. Many of the features of these networks make them different from the traditional wired and wireless distributed systems. Traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, enough communication range and computational capabilities. These features make the traditional networks able to meet the communication demands [8, 12].

On the other hand, WSNs are resource constrained distributed systems with low energy, low bandwidth and short communication range. The basic features which make WSNs different from the traditional networks are; self-organizing capabilities, short range communication, multi-hop routing, dense deployment, limitation in energy and memory, and also frequently changing topology due to fading and failures. [13, 12] The constrained resource nature and unpredictable network structure (sensor nodes are scattered densely in an environment) poses numerous design and communication challenges for WSNs. According to [8] "The challenges in the hierarchy of: detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous." Generally, the wireless sensor network operation involve data acquisition and data reporting therefore it has a data acquisition network and data distribution network and a management center responsible for its monitoring and control as shown in Figure 1 below.

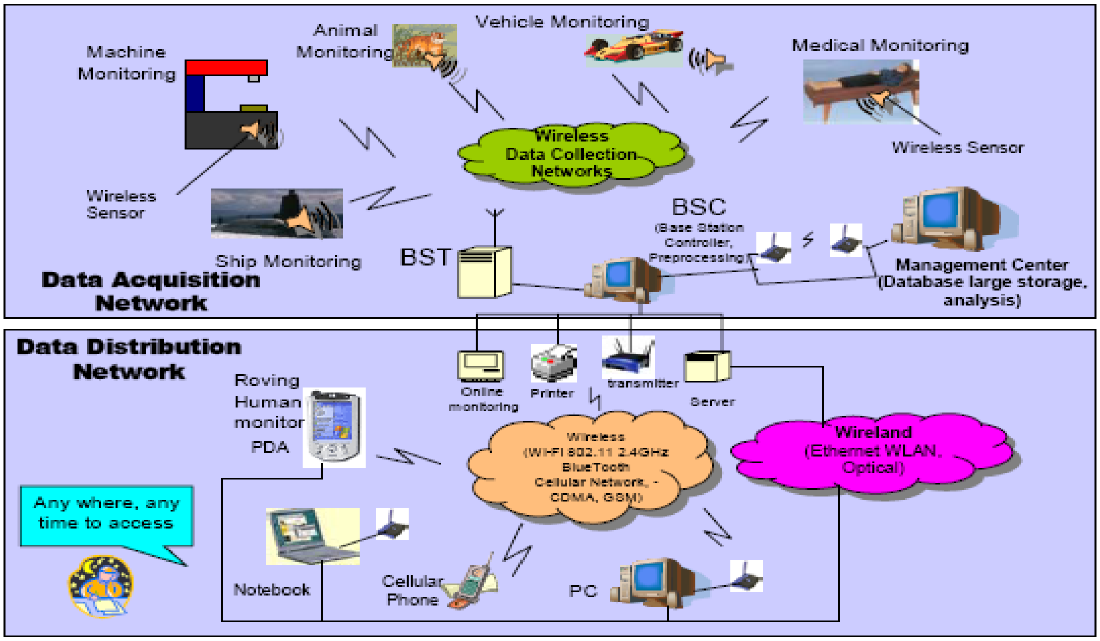
Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor
PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Figure: 1 Wireless sensor network [8]

The fundamental for any WSNs application is based on the integration of modern technologies like sensor, CPU and Radio performing sensing, Processing and communication. Therefore it requires better understanding of modern network technologies as well as of WSNs hardware units in order to have an effective WSN. Despites all these challenges, the importance of WSN cannot be neglected due to its diverse application domain [8].

1.1. Network Components of WSN

The main components of a general WSN are the sensor nodes, the sink (base station) and the events being monitored.

1.1.1. Sensor Node and its Functional Units

In WSN, every sensor node has capabilities of sensing, processing and communicating data to the required destination. The basic entities in sensor nodes are sensing unit, power unit, processing unit and communication unit and memory unit to perform these operations shown in Figure 2 below.

i) Sensing Unit

Sensors play an important role in sensor networks by creating a connection between physical world and computation world. Sensor is a hardware device used to measure the change in physical condition of an area of interest and produce response to that change. Sensors sense the environment, collect data and convert it to fundamental data (current or voltage etc) before sending it for further processing. It converts the analogue data (sensed data from an environment) to digital data and then sends it to the microcontroller for further processing.

There are different categories of sensors which are available and can be used depending on the nature of the intended operation. A typical wireless sensor node is a micro-electronic node with less than 0.5 Ah and 1.2 V power source. Sensors size and their energy consumptions are the key factors to be considered in selection of sensors [13, 14, 6].

ii) Memory Unit

This unit of sensor node is used to store both the data and program code. In order to store data packets from neighboring (other) nodes Random Only Memory (ROM) is normally used. And to store the program code, flash memory or Electrically Erasable Programmable Read Only Memory (EEPRM) is used [13, 14, 6]

iii) Power Unit

For computation and data transmission, the corresponding units in sensor node need power (energy). A node consist a power unit responsible to deliver power to all its units. The basic power consumption at node is due to computation and transmission where transmission is the most expensive activity at sensor node in terms of power consumption. Mostly, sensor nodes are battery operated but it can also scavenge energy from the environment through solar cells [13, 14, 6].

iv) Processing Unit

Sensor node has a microcontroller which consist a processing unit, memory, converters (analogue to digital, ATD) timer and Universal Asynchronous Receive and Transmit (UART) interfaces to do the processing tasks. This unit is responsible for data acquisition, processing incoming and outgoing information, implementing and adjusting routing information considering the performance conditions of the transmission [13, 14, 6].

v) Communication Unit

Senor nodes use radio frequencies or optical communication in order to achieve networking. This task is managed by radio units in sensor nodes that use electromagnetic spectrum to convey the information to their destinations. Usually each sensor node transfers the data to other node or sinks directly or via multi hop routing [13, 14, 6].

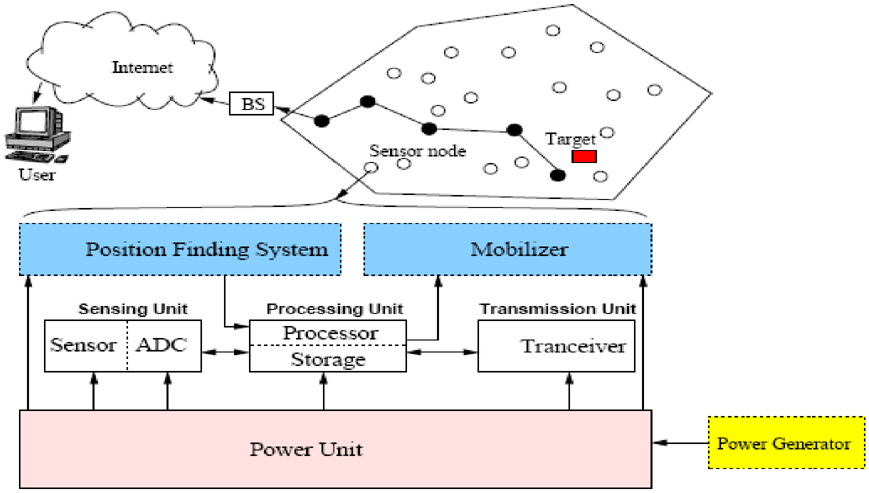

Figure 2: Components of sensor node [6]

1.1.2. Base Station (Sink)

The sink (some time cluster head) is an interface between the external (management center) world and computational world (sensor network). It is normally a resourceful node having unconstrained computational capabilities and energy supply. There can be single or multiple base stations in a network. Practically, the use of multiple base stations decreases network delay and performs better using robust data gathering. Base station in a network can also be stationary or dynamic. The dynamic base stations can influence the routing protocols greatly because of its changing position which will be not clear to all the nodes in a network. Beside mobility of base stations there are other characteristics of base stations like coverage, presence and number of nodes pose routing challenges for routing protocols which are explained in section (2.1) [11, 14].

1.2.WSN Operation

Generally, operation of WSN involves communication between sensor node and base station. The sensor node senses environment, perform some computation (if required) and report gathered information to the base station. If base station is connected with some actuator which triggers the alarm for human intervention in case of an event of interest [11].

1.2.1. Communication Model

Although sensor nodes are identical devices but their characteristics varies with the network structures. Sensor deployment, coverage, transmission power, computation, reporting, addressing and communication pattern greatly affects the routing protocol operation both at nodes and at base stations discussed in chapter (2). Routing protocol used for WSN communication support unicast (one-to-one), multicast (one-to-many) and reverse-multicast (many-to-one) in the following ways [11].

i) Node-to-Node

In a multihop communication data needs to be passed by intermediate nodes in order to reach to destination. Node to node communications is used to pass data from one node to other till the destination. Generally, this type of communication is not required in WSN communication.

ii) Node-to-Base Station

When sensors node want to send responses back to base station, this communication pattern is used. This is a reverse-multi path communication which means that more than one node can communicate to base station directly or indirectly. This communication pattern can also be unicast if there are multiple base stations or there is a special node (group leader), who is responsible to gather sensed information and transmit it to base station [11].

iii) Base Station-to-Node

This type of communication is required when base station wants to request data from nodes. Typically, the mode for communication is anycast (one-to-many) which means any sensor node having the requested date can respond to the base station. This pattern of communication can also be multicast or unicast if the identification of nodes is unique by their IDs or locations etc [11].

1.3. Classification of Sensor

Sensor can be classified on the basis of different aspects, including technological aspects, detection means, their output signals and sensor materials and field of application. Although different classification is needed when looking on its application side but can be categorized in to following categories [20].

1.3.1. Active Sensors

Active sensors stimulate the environment in order to do the measurements. For example seismic sensors, laser scanners, infrared sensors, sonar's and so on [15].

1.3.2. Passive, Directional Sensors

These sensors can monitor the environment without disturbing the environment. Examples of these sensors are: thermometers, humidity sensors, light sensors and pressure sensors etc [15].

1.3.3. Narrow Beam Sensors (Passive)

This is the type of passive sensors requires a clear direction in order to measure the environment (medium) e.g. camera and ultrasonic sensors [15].

1.4 Classification of Sensor Network Applications

According to [15] Wireless sensor networks can be deployed for various type of applications based on its data delivery requirement, application type and application objectives. The demands of applications vary according to application nature. Some applications are more interested in only data collection but not in robust delivery while somewhere delay cannot be tolerated. There are different application classes with different transmission demands. These application classes with different delivery requirements make both software and hardware design of WSN more challenging. Therefore it is required to classify WSNs application in classes in order to understand their nature and requirements. Generally, WSN applications can be classified into following four classes.

1.4.1 Event Detection and Reporting

This class of WSN application consists of sensor nodes which are used rarely. These sensor nodes are inactive most of the time and come to life (active) when a certain event occurs. When the event is detected, individual node sends event report to the sink which may contain some information about the nature of the event and location. The application nature is sensitive in terms of reliability and delay. As soon as an event is detected, WSN reports to sink within no time. A major challenge in this kind of network at application level is to minimize false reporting of the event. Also routing of event to the sink is a design issue from networking point of view. Examples of such applications are [16, 17, 12 and 18].

- Intruder detection in military surveillance
- Quality check at product line/ anomalous behavior
- Detection of forest fire/ Floods
- Seismic activity detection
- Detection of ocean environment

1.4.2 Data Gathering and Periodic Reporting

The functional behavior of sensor nodes in these applications is of continuous nature. In these applications continuous monitoring of some activity is recorded and sent to the sink individually like point-to- point communication. But in case of large network, sink is more interested in distributed computation on gathered data rather than individual node reading in order to avoid traffic volume at sink. Sometimes these sensors can be attached with actuators. The sink might need to store the geographical information of the sensor nodes in the area of interest. Monitoring of humidity in a glass house is an example of such applications. Crucial requirement of these applications is efficient utilization of energy. Examples are; [16, 17, 12 and 5]

- Monitoring humidity, temperature and light etc
- Environmental conditions monitoring
- Home/office smart environments
- Health applications

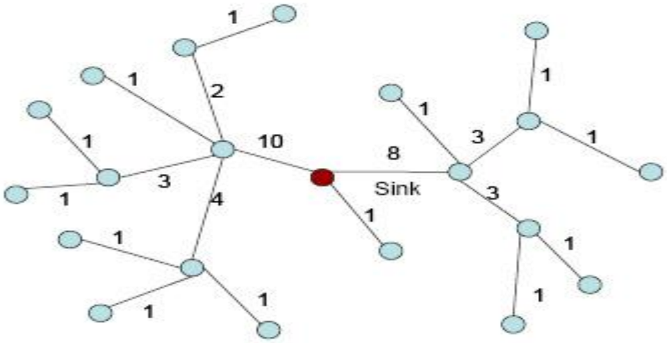

Figure 3: WSN node topology example [5]

1.4.3 Sink-Initiated Querying

The applications in this class also have the additional feature of sink querying besides monitoring. In this case sink has the ability to send a query to a group of sensor nodes for their reading rather than the periodic reporting of the individual node. This allows the sink to gather information of different locations and also helps in validity of the measurements in order to take a decision (trigger an actuator or raise an alarm). Examples of these applications are; [16, 12, 19].

- Environmental control in buildings
- Soil condition monitoring
- Biological attack detection
- Weather monitoring

- Fire alarming

1.4.4 Tracking Based Application

This class of WSN applications consist some of the characteristics of the previous three classes. Tracking applications involve both the detection as well as location information. When a target is detected at any location by a sensor node, it has to notify the sink promptly where accuracy is the main concern. Now, the sink may require initiating queries to the specific set of sensor nodes in order to get the location information of the target. It also helps to verify the measurements of that individual node about the target detection. The decision of triggering actuator or raising an alarm for human intervention is based on the readings received by this set of sensor nodes. Examples of these applications are; [13, 14, 4].

- Targeting in intelligent ammunition
- Tracking of doctors and patients in hospital
- Tracking of inhabitant in a building
- Tracking of animal in forest
- Tracking and controlling the people in park and building

1.5 Classification of Routing Protocols in WSN

Different routing protocols are designed to fulfill the shortcomings of the recourse constraint nature of the WSNs. The deployed WSN can be differentiated according to the network structure or intended operations. Therefore, routing protocols for WSN needs to be categorized according to the nature of WSN operation and its network architecture.WSN routing protocols can be subdivided into two broad categories, network architecture based routing protocols and operation based routing protocols [6, 11].

1.5.1 Route Selection Base Classification of Routing Protocols

The WSN routing protocols can be further classified on the method used to acquire and maintain the information, and also on the basis of path computation on the acquired information. This classification of protocol is based on how the source node finds a route to a destination node [8, 16. 6].

i) Proactive Protocols

Proactive routing protocols are also known as table driven protocols which maintains consistent and accurate routing tables of all network nodes using periodic dissemination of routing information. In this category of routing all routes are computed before their needs [paper]. Most of these routing protocols can be used both in flat and hierarchal structured networks. The advantage of flat proactive routing is its ability to compute optimal path which requires overhead for this computation which is not acceptable in many environments. While to meet the routing demands for larger ad hoc networks, hierarchal proactive routing is the better solution [16, 6, 21, 22].

ii) Reactive Protocols

Reactive routing strategies do not maintains the global information of all the nodes in a network rather the route establishment between source and destination is based on its dynamic search according to demand. In order to discover route from source to destination a route discovery query and the reverse path is used for the query replies. Hence, in reactive routing strategies, route selection is on demand using route querying before route establishment. These strategies are different by two ways: by re-establishing and re-computing the path in case of failure occurrence and by reducing communication overhead caused by flooding on networks [16, 6, 21, 22].

iii) Hybrid Protocols

This strategy is applied to large networks. Hybrid routing strategies contain both proactive and reactive routing strategies. It uses clustering technique which makes the network stable and scalable. The network cloud is divided into many clusters and these clusters are maintained dynamically if a node is added or leave a particular cluster. This strategy uses proactive technique when routing is needed within clusters and reactive technique when routing is needed across the clusters. Hybrid routing exhibit network overhead required maintaining clusters [6, 21, 22].

1.5.2 Architecture Based Routing Protocols

Protocols are divided according to the structure of network which is very crucial for the required operation. The protocols included into this category are further divided into three subcategories according to their functionalities. These protocols are [6, 11]

- Flat-based routing
- Hierarchical-based routing
- Location-based routing

i) Flat-Based Routing

When huge amount of sensor nodes are required, flat-based routing is needed where every node plays same role. Since the number of sensor nodes is very large therefore it is not possible to assign a particular Id to each and every node. This leads to data-centric routing approach in which Base station sends query to a group of particular nodes in a region and waits for response. Examples of Flat-based routing protocols are; [6, 21, 11].

- Energy Aware Routing (EAR)
- Directed Diffusion (DD)
- Sequential Assignment Routing (SAR)
- Minimum Cost Forwarding Algorithm (MCFA)
- Sensor Protocols for Information via Negotiation (SPIN)
- Active Query forwarding In sensor network (ACQUIRE)

ii) Hierarchical-Based Routing

When network scalability and efficient communication is needed, hierarchical-based routing is the best match. It is also called cluster based routing. Hierarchical-based routing is energy efficient method in which high energy nodes are randomly selected for processing and sending data while low energy nodes are used for sensing and send information to the cluster heads. This property of hierarchical-based routing contributes greatly to the network scalability, lifetime and minimum energy. Examples of hierarchical-based routing protocols are; [6, 21, 11]

- Hierarchical Power-Active Routing (HPAR)
- Threshold sensitive energy efficient sensor network protocol (TEEN)
- Power efficient gathering in sensor information systems
- Minimum energy communication network (MECN)

iii) Location-Based Routing

In this kind of network architecture, sensor nodes are scattered randomly in an area of interest and mostly known by the geographic position where they are deployed. They are located mostly by means of GPS. The distance between nodes is estimated by the signal strength received from those nodes and coordinates are calculated by exchanging information between neighboring nodes. Location-based routing networks are; [6, 11]

- Sequential assignment routing (SAR)
- Ad-hoc positioning system (APS)
- Geographic adaptive fidelity (GAP)
- Greedy other adaptive face routing (GOAFR)
- Geographic and energy aware routing (GEAR)
- Geographic distance routing (GEDIR)

1.5.3 Operation Based Routing Protocol Classification

WSNs applications are categorized according to their functionalities. Hence routing protocols are classified according to their operations to meet these functionalities. The rationale behind their classification is to achieve optimal performance and to save the scarce resources of the network. Protocols classified to their operations are:

- Multipath routing protocols
- Query based routing
- Negotiation based routing
- QoS based routing
- Coherent routing

i) Multipath Routing Protocols

As its name implies, protocols included in this class provides multiple path selection for a message to reach destination thus decreasing delay and increasing network performance. Network reliability is achieved due to increased overhead. Since network paths are kept alive by sending periodic messages and hence consume greater energy. Multipath routing protocols are: [6]

- Multi path and Multi SPEED (MMSPEED)
- Sensor Protocols for Information via Negotiation (SPIN)

ii) Query Based Routing Protocols

This class of protocols works on sending and receiving queries for data. The destination node sends query of interest from a node through network and node with this interest matches the query and send back to the node which initiated the query. The query normally uses high level languages. Query based routing protocols are: [6]

- Sensor Protocols for Information via Negotiation (SPIN)
- Directed Diffusion (DD)
- COUGAR

iii) Negotiation Based Routing Protocols

This class of protocols uses high level data descriptors to eliminate redundant data transmission through negotiation. These protocols make intelligent decisions either for communication or other actions based on facts such that how much resources are available. Negotiation based routing protocols are: [6, 23]

- Sensor Protocols for Information via Negotiation (SPAN)
- Sequential assignment routing (SAR)
- Directed Diffusion (DD)

iv) QoS Based Routing Protocols

In this type of routing, network needs to have a balance approach for the QoS of applications. In this case the application can delay sensitive so to achieve this QoS metric network have to look also for its energy consumption which is another metric when communicating to the base station. So to achieve QoS, the cost function for the desired QoS also needs to be considered. Example of such routing are: [23, 6]

- Sequential assignment routing (SAR)
- SPEED
- Multi path and Multi SPEED (MMSPEED)

v) Coherent Data Processing Routing Protocol

Coherent data processing routing is used when energy-efficient routing is required. In this routing scheme, nodes perform minimum processing (typically, time-stamping, suppression etc) on the raw data locally before sending for further processing to other nodes. Then it is sent to other nodes called aggregator for further processing known as aggregation [6, 24].

Data processing in non-coherent processing involves three phases. In first phase target detection, its data collection and preprocessing of its data takes place. Then for the cooperative function the node needs to enter in phase 2 where it shows its intention to neighboring nodes. Here all neighboring nodes must be aware of the local network topology. Finally, in step 3 a center node is selected for further refined information processing. Therefore central node must have enough energy resources and computation abilities [6].

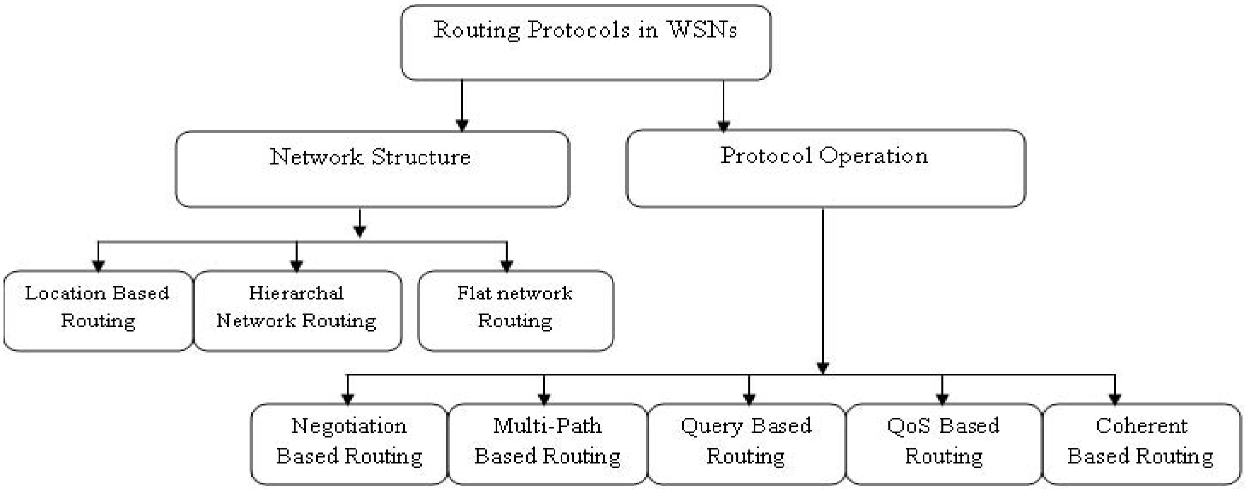

Figure 4: Routing protocols in WSN: A Taxonomy [6]

1.6. Related Work

Various routing protocols [24][25][25][27][28][29][30] have been proposed to be used for WSNs considering different application demands of WSNs. However, not all of these protocols are efficient enough to fulfill all desired features of WSNs applications. Also many protocols are evaluated but there are fewer comparisons between different WSNs routing protocols specially the protocols we selected for our study.

In [31] the performance of two routing protocols i.e. DSDV and AODV in a WSN are compared with respect to packet delivery ratio, End-to-End delay and routing overhead as a performance metrics. The author concluded that AODV performs better than DSDV in terms of delay while DSDV performs better than AODV in the term of latency.

In [32] three different protocols, AODV, DSR and DSDV protocol are evaluated and author reported that the performance of DSR, AODV is better than DSDV in the term of packet delivery ratio and latency of packet transmission in but DSDV is better than DSR, AODV in term number of increasing nodes (scalability).

In [30], three different MANET routing protocols AODV, DSR and OLSR are compared for delay, throughput and routing traffic sent in WSAN for fixed and mobile nodes using OpNet Modler. The author evaluated these protocols also in link failure in mobile nodes and reported OLSR the best fit protocol in all scenarios of WSAN.

Another related study [37] analyzed OLSR, AODV and DSR with a new proposed Efficient Data Gathering (EDGE) protocol against delivery ratio and delay and path length using NS-2 simulator. They showed that EDGE performs better in terms of higher delivery ratio, shorter delay and comparable path length.

Also in [34], a tree based data collection i.e. Scalable Data Collection (SDC) protocol has been evaluated in contrast with OLSR, AODV, OLSR and Direct Diffusion for delivery ratio and delay using NS-2 simulator. The author demonstrated that SDC achieves considerably large delivery ratio and lower delay along with scalability in various scenarios. In this project, we examine the same situation where all nodes in network send traffic to a common base station (destination). We are not intended to argue with the results shown by the authors. Also we are using different environment/scenario with different parameters for our simulations; therefore we draw our own conclusion.

Chapter 2: PROBLEM DEFINITION

Routing is a challenging task in WSNs because of their unique characteristics which makes it different from other wired and wireless networks like cellular or mobile ad hoc network (MANETs). [6, 8] Due to its deployment nature (large scale deployment), the Internet Protocol (IP) based protocols may not be the better choice to be applied on.

- Mostly, the flow of sensed data is towards base station from all sources in all applications.
- Resource management is critical due to their resource constrained nature.
- Application-specific nature.
- Location based data collection needs nodes position awareness.
- Data redundancy is another issue.

Therefore, it is required that routing protocols should have the capabilities to handle these characteristic for reliable and efficient communication. Different routing mechanisms have been proposed to address routing problems in WSNs taking into account WSNs network architecture and application demands.

2.1 Routing Challenges and Design Issues in WSN

There are numerous design and communication challenges in WSNs because of its application domain and their network structures. Besides, it also constraints resources nature makes it more difficult to cope with these challenges. The deployment of WSNs can vary both by its network structure and application type therefore it is required to consider both the design and communication challenges for efficient communication. Furthermore, these challenges have a greater influence on routing protocols design and degrade its performance. Both sensor nodes and base station have the influence on the performance of routing protocols of WSNs in following ways [34, 36, 6].

2.1.1 Routing Protocols and Design Issues at Sensor Node and Base Station

Sensor nodes affect the routing operations due to the following reasons.

1. Node Deployment

In a sensor network a node can be deployed deterministically or randomly. In deterministic way the nodes are placed on pre-determined paths and routing takes place along that path while in random approach the nodes are scattered in a WSN [6, 13].

2. Transmission Media

Sensor nodes communicating with each others in a multi-hop network are linked together by wireless medium hence the operation of this network is affected by some traditional problems that are usually attached with a wireless channel [6, 13].

3. Connectivity

In a sensor network due to high density of a node the sensor nodes are highly connected. This does not prevent shrink in the size of network or its topology in the case of failure in a sensor node. Connectivity of nodes is also dependent on the distribution of nodes randomly [6, 13].

4. Coverage

Sensor node in a WSN captures a view of the environment it is placed in and this view can be short in range or accuracy thus we can say that for the sensor node’s design the coverage parameter is important [6, 13].

5. Fault tolerance

Due to the uncertain deployment nature of WSN, the failure of sensor nodes can be seen due to harsh environmental conditions, physical damage or due to running out of power. But to achieve better performance, the networks should be fault tolerant. If a node failure occurs, the network should have the capabilities to maintain its functionalities and its performance should not be affected or the effect should be minimal [6].

6. Scalability

The deployment of sensor nodes is dependent on nature of application. Sensor node deployment varies with respect to the demand of application, therefore the number of sensor nodes can be hundreds, thousand or even more. To handle network scalability, routing algorithm should have the capability to cope with scalable network [6, 37, 34].

7. Data Aggregation

The data generated by sensor nodes in a WSN is excessive hence Data aggregation is used to combine similar data packets from different nodes to get energy efficiency and optimization the performance of data transmission in routing protocols [6, 13].

8. Quality of Service

Quality of service is determined by different applications differently. In some application the data transmission in time efficient manner is considered to be quality of service while in others low energy consumption or energy conservation is regarded as quality of service. In the later case the emphasis is on energy-aware routing protocols [6, 13].

Besides, the above design issues there also exists communication challenges in WSNs which also degrade the performance of routing protocols. Routing protocols plays an important role in data transmission between source and destination. Therefore it is necessary to choose routing protocols for applications on the basis of routing objectives and application demand. Routing objective can be categorized on the basis of delivery needs.

2.2 Routing Objective

In sensor applications, the demand for message delivery varies from application to application. Some applications only need the successful delivery of the message from source to destination .While some applications are more interested in real time delivery of the message [11].

2.2.1 Non-Real Time Delivery

In this case the applications demand from routing protocols is only the delivery of message from source to destination.

2.2.2 Real-Time Delivery

In this case the demand from routing protocols is the message delivery within a specified time, which means delay cannot be tolerated. Here, in case of delayed delivery the message will be useless.

2.2.3 Network Life Time

In WSN some applications demands from sensor nodes to run application as long as possible. In such networks the objective of routing protocols become crucial, they need to maintain balance energy consumption among all the network nodes. The metric to determine network life time can be use in two different ways based on protocols. In protocols, where each node has the same importance, one metric for network life time can be time until the death of first and second metric can be the average energy consumption of nodes in a networks. It could be the time until last node or high priority node dies for protocols where each node is of not equal importance [11].

2.3 Problem Description

WSNs are deployed densely in a variety of physical environment for accurate monitoring. In critical condition monitoring like, environmental tracking application, accuracy is critical performance metric. Therefore, order of receiving sensed events is important for correct interpretation and knows what actually happening in the area being monitored. Similarly, in intrusion detection applications (alarm application), response time is the critical performance metric. On detection of intrusion, alarm must be signaled within no time. There should be a mechanism at node for robust communication of high priority messages. This can be achieved by keeping nodes all the time powered up which makes nodes out of energy and degrades network life time [38].

Also, there can be a link or node failure that leads to reconfiguration of the network and re-computation of the routing paths, route selection in each communication pattern results in either network delay by choosing long routes or degrade network lifetime by choosing short routes resulting in depleted batteries.[11] Therefore the solutions for such environments should have a mechanism to provide low latency, reliable and fault tolerant communication, quick reconfiguration and minimum consumption of energy. Routing protocols have a critical role in most of these activities. Beside all these problems, the infrastructure less, limited resource (in terms of power, memory and computational capabilities) nature of WSNs makes routing more complicated. Many routing protocols have been designed to address all of the above problems but all of which are more suitable in some situations having better performance while not suitable in other situations having significant limitations. Therefore, it is critical to asses routing protocols for critical monitoring applications.

According to [35], How to measure the goodness of a policy? To do a meaningful assessment of a protocol's performance, performance metrics can be used. This can promote to identify merits and demerits of protocols that helps in finding which network context is best suited and which one is less suited and which one is unsuited. Such a description of protocols attributes results in qualitative metrics. Qualitative metrics then allow the broad categorization of protocols and provide a base for detailed quantitative metrics, which are the basis for detailed evaluation of protocol performance quantitatively. [35].

Hence, to achieve efficient communication, it is required to identify the delivery demand for the communication and to choose a suitable routing protocol. To measure the suitability and performance of any given protocols, some metrics are required. On the basis of these metrics any protocol can be assessed against its performance [35].

The qualitative metrics for any protocols are given below;

- Routing Overhead (bytes)
- Packet Delivery Fraction (PDF)
- Routing Overhead (packets)
- Average Path Length
- Average Route Acquisition Latency/ Median latency (ML)
- Average End-to-End Delay of Data Packets

2.4 Thesis Objectives/ Goals

2.4.1 General Objective

The overall objective of this research is to identify the performance challenges for routing protocols in wireless sensors and to evaluate the existing routing protocols for a selected (Chapter 4) application environment against the set of qualitative performance metrics for any protocol. Furthermore, to identify the delivery demand of the communication for the selected application, to compare different routing protocols for these applications and to identify the protocol suitability in the selected application environment on the basis of performance results in order to attain efficient communication and save network resources.

2.4.2 Specific Objectives

The specific goals of this research include:

- To identify the factors affecting routing protocols performance
- To simulate different routing protocols in a network scenario against performance metrics
- To analyze the results for the chosen metrics against application demands
- To identify the suitability of the protocols for the selected application on the basis of findings (results).
- To draw the conclusion of the research by presenting the outcomes

Chapter 3: RESEARCH METHODOLOGY

In this chapter the methodology we chose for this research is presented in this chapter. Also the reasons behind the selection of these methodologies are discussed.
We have used mixed method approach for this thesis. According to [39], a mixed method methodology is a research methodology that includes both qualitative and quantitative approaches.

3.1. Qualitative Research Methodology

Qualitative approach is used when one is interested to explore any activity [39]. For this research, we used qualitative research methodology in the following way;

3.1.1. Literature Review

In literature review step, a detailed survey of the existing literature about the area of research was carried out for relevant data gathering.

i) WSNs Background Study

In this step, from the basics of WSNs (including Mobile ad hoc networks) were thoroughly studied to understand the different integrated technologies in WSNs, its communication challenges from routing point of view. Also WSN application classes were studied in order to understand the operational mechanism of each of WSN class. Besides, strict requirements of each application class were identified in order to figure out possible tradeoffs among performance metrics for these application classes.
By conducting literature survey, we studied different research articles, papers including books to identify factors which highly influence the routing protocols and affect their performance. In our study we used qualitative research methodology to answer the following research question.
Q. What are the challenges for routing protocol's performance in WSN?

ii) Study/ Selection of WSNs Application Classes and Performance Metrics

After identification of different challenges for routing protocols from literature we explored WSN application classes in order to understand requirement of each application class. Here, we were able to choose different performance metrics with respect to application class. As different application classes have different demands so we chooses these demands as a performance metrics for routing protocols. Besides, different routing protocols used in WSNs were studied to understand their working mechanism, to figure out their capabilities and limitations in different applications.

iii) Selection of Routing Protocols

Finally, routing protocols were selected for simulation in order to evaluate their performance with respect to different application classes and for their demands. Now, we were able to find out the effect of routing challenges on the performance of routing protocols and answer the rest of research questions of our research. To explore the effect of different routing challenges on protocols we then used quantitative approach.

3.2 Quantitative Research Methodology

Quantitative research methodology is used when exploration of cause-effect is of interest [7].
In quantitative part of our methodology, we have performed an empirical study to validate our finding from literature survey. That is the evaluation of routing protocols in the presence of identified challenges.

This is the main task of our research to validate our finding from literature in order to answer our next research question.
Q. How to evaluate the performance of routing protocols in WSNs?

3.2.1. Tool Selection

At this stage of our research, as we had identified different routing challenges in routing protocols from theory, to validate these challenges, a tool needed to be used. We choose OpNet Modler[40] simulator for implementation (simulation) and evaluation of selected routing protocols against the selected performance metrics.

3.2.2. Designing Network for Simulation

Here, we designed our network for simulation study having different network entities and their configuration according to the application classes we have chosen. Then selected routing protocols were simulateded for evaluation against selected metrics.

3.2.3 Simulation Result and Analysis

Finally, different numbers of simulations were executed for each scenario and results were collected and analyzed. The approach used as a research methodology is depicted in figure: below

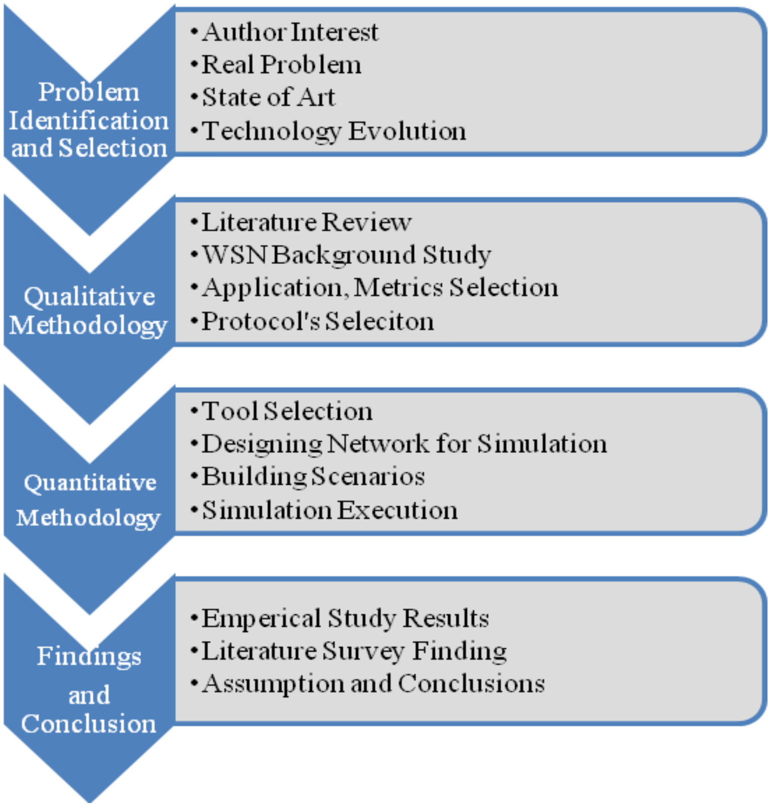

Figure [5]: Research Methodology

CHAPTER 4: PROPOSED STUDY

4.1. Selected WSN Applications

The low-cost, easy deployment, self-configuring nature of WSN makes its desirable for various application classes as compare to other networks. The main application classes of WSN are data gathering, event detection, object tracking and sink-initiated querying. Each application class has its own transmission demands. There are further different applications scenarios in each application class. The application scenarios we have selected belong to the above first three application classes because most of the WSN applications are covered by these classes.

4.1.1 Environmental Data Collection

Environmental data collection scenario belongs to data gathering application class. Sensor nodes deployed in such applications are expected to operate (sense/collect/transmit) at regular basis and for longer period of time. In such applications, data is collected from large number of deployed nodes for several months or year to find out the trend and their dependencies. The network structure of such application consist of a large number of nodes, sensing and transmitting data to the sink continuously. Nodes are deployed evenly in a large area and needs to estimate the optimal routing policy after discovering network topology. In such applications as the nodes are deployed at exact locations so the physical topology of the network remains constant. This means that, the optimal routing policy for transmission can be calculated outside the network instead of at nodes. In data collection applications the sensor nodes remains sleep most of the time and report measurements frequently to the base station.

The routing mechanism in such applications uses tree-based routing where each routing tree has special nodes to sink data having high capabilities. Using tree-based routing mechanism involves child nodes, parent nodes and sinks. In data collection process, child node is responsible to transmit data to its upper (parent) node and then this node is responsible to transmit data to its upper node, following the same way until it reaches to the sink. Each node transmits periodically sensed data following the routing tree (to all Childs) and back to the sink. The better idea is to have short and wide tree. Here, nodes having large number of successors will have to send more data and quickly become energy bottleneck as compared to the leaf node. This can cause node failure leads to reconfiguration of network degrading network life time. Also precise scheduling of communication event is necessary for network lifetime.

Mostly, data collection in such applications is non-real time i.e. for future analysis. Therefore latency is not the strict requirement for application performance which means reasonable delay can be tolerated. Also tasks during typical scenarios (light, temperature, humidity) do not require high reporting. Reporting rate varies with the changes in environmental conditions if it changes frequently. Normal reporting period for such transmission is from 1 to 15 minutes. So the demands of environmental data collection applications are network lifetime, precise scheduling, low data rate and non-real time (delay is acceptable) transmission of data from node to base station.

4.1.2. Tracking of Doctors and Patients in Hospital

Second application's scenario of our study is tracking of doctors and patients in hospital that belong to mobile object detection i.e. is one of WSN application. In this tracking application mobile nodes are used to detect the moving object. In this example, sensor nodes continuously monitor movement of each object and sense the location information of moving object and then send to sink node in a way to track specific object. The process of tracking phenomena is different from event detection, in a way where tracking certain objects involves both phenomena the detection of objects as well as to store information of current location of specific object. Each object can be identified through assigned tracking ID. If object pass out from range of one sensor node and enters to other node's range then information stored in next node, and then that nodes store and transfer information to sink node whenever object remain in the range of that specific node. Sink node require to initial query regarding each object to identify that object.

The scenario as discussed above we have real life example of hospital, where doctors can be considered and nurse as moving objects. Whenever specific patients need a doctor or nurse in emergency situation it will easy to track doctor location using WSN. In this case patients are considered as stationary objects. As compare to moving objects stationary object is easy to track but moving object are difficult to track because in this case each node continuously transfer information of specific object to the next node which will cause to keep each node active.

4.2. Selected Protocols for Evaluation

The mechanism use to find paths from one end node to other through which data can be transfer is known as routing. More simply it can be defined as the process of path selection from one node to another in order to send data. Path selection is desired to be best (optimal) in terms of cost. To keep the cost minimal required applying some metric to find best optimal path in multiple available paths. These metrics (cost functions) can be delay, overhead, throughput and error rate etc. Routing components includes algorithm, database and protocols. Routing protocol is the way for sharing information about current network state among routers. Routing protocols can be evaluated for its performance against the above metrics. Routing protocols are mainly differentiated on the basis of algorithm they use. There are different classifications of routing protocols like static versus dynamic, source routing verses hop-by-hop routing, distance vector verses link state and centralized verses distributed. Protocols can also be classified on the basis of their operations like proactive, reactive hybrid. In our study, we selected two protocols on the basis of their operation nature and routing mechanism. Our selected protocols belong to proactive and reactive families. Besides, one uses source routing and other hop-by-hop routing. This selection was made for the purpose to investigate the difference between sour routing and hop-by-hop routing. Furthermore, to inspect the affect of their reactive and proactive approaches while doing routing by considering their performance.

4.2.1. Optimized Link State Routing Protocol (OLSR)

This protocol works in collaboration with other nodes in a WSN through the exchange of topology information. This exchange of information is done periodically. To avoid the broadcast of unnecessary packet re-transmissions, this protocol uses multipoint relays. In a network, a node broadcasts a message periodically to its neighboring nodes. This is done to compute the multipoint relay set as well as the exchange of information about the neighborhoods. From the information about the neighborhood this node calculates the minimum set of one hop relay point that is needed to reach the two hop neighbors and this set is called the Multipoint relay set.

OLSR differs from link state protocols in two factors based on the dissemination of routing information. First is by construction i.e. only the multipoint relay nodes of a node A need to forward updates about link state that are issued by A. Secondly the size of the link state update of a node A is reduced because it only consists of those neighbors that selected node A as their multipoint relay node. Thus we can conclude that OLSR reduces the Link state protocol. It is used in a network where nodes are densely deployed; the OLSR calculates the shortest path in such networks to an arbitrary destination [24].

i) Neighbor Sensing

In Wireless ad hoc Networks, each node has to certify its nature of link with neighbor nodes because of Radio Transmission. In OLSR specifications there are two types of links SYM (Symmetric) Links and ASYM (Asymmetric) Links. Each node sends hello interval to its 1-hop neighbor's hello message to achieve neighbor sensing which have not to be forwarded. When nodes send the message it contains node neighbor list and their link status, which allow them to deduce the whole 2-hop neighbor and their status. Afterward MPR Selection is made and list is added in to *hello* messages. In final step, using this MPR list a MPR selector list is constructed, which contains a neighbors list which have selected it as MPR. Now the messages received from their MPR selectors will be forwarded by the nodes [25].

ii) MPR Flooding

Best as possible controlled traffic flooding is the aim of Multipoint Relays (MPR). In MPR flooding, MPRs are selected in such a way that when a flooding message is transmitted by the MPR set it must reaches all 2-hop neighbors. MPR(n), the MPR set of a node n, which is also represented as the smaller subset of symmetric 1-hop neighbors of n, having symmetric links with all 2-hop neighbors of n. MPR flooding mechanism makes way to the elimination of transmission duplication as well as reception duplication is minimized by it [25].

iii) Topology Diffusion

The objective of topology diffusion is to create routing tables using periodic topology control messages (TC messages). TC messages are circulated by each node with a non-empty MPR selector set to all network nodes, broadcasting at least links between itself and the nodes in its MPR selector set, to achieve Topology Diffusion. These TC messages contain sufficient information which enables nodes, first to construct their topology table and then to derive their routing table. The routes are using shortest path algorithms, such as "Dijkstra's shortest path algorithm" after their calculation and providing the best possible hops number.

However, there is always a need to recalculate the routing tables to update the route information, as these tables are based on information concerning links to neighbors and topology which can be changed at any instant [25].

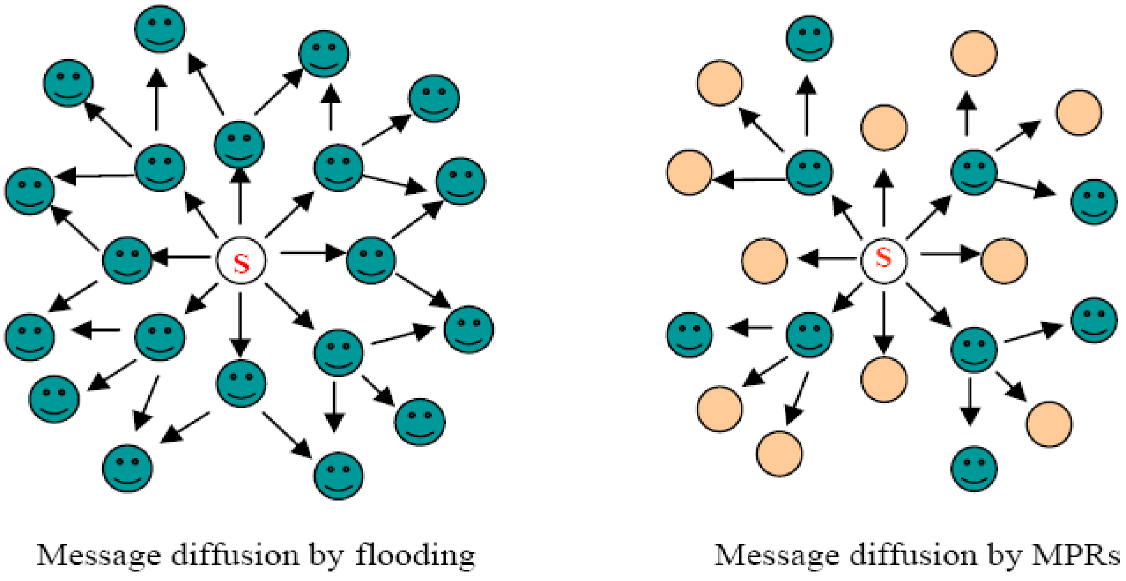

Figure 6: The MPR flooding mechanism [25]

4.2.2. Dynamic Source Routing (DSR)

One of the reactive protocols is dynamic source routing protocol. This protocol makes it possible for all the nodes to find a route to a destination in a multiple network hops dynamically. DSR minimizes the overall network bandwidth overhead because of the fact that it does not use periodic routing messages. By doing so DSR also tries to conserve battery power as well as avoidance of routing updates that are large enough. However there is a support from the MAC layer that informs the routing protocol of any failure in nodes in DSR [27, 41].

Some properties of Dynamic source routing are:

- In DSR the intermediate nodes do not save the up-to date routing information, thus DSR takes the advantage of source routing.
- The network bandwidth is reduced because there are not periodic message advertisements.
- By not sending or receiving advertisements the battery power is also reserved by DSR.
- DSR scans for information in packets that are received and learns about the routes.
- With the use of piggybacking a new request to the source route DSR is able to support unidirectional links.
- There is a serious security threat when the interface is run in promiscuous mood. In this case the interface's address filtering is turned off hence all packets are scanned. In this stage an intruder can listen to all the packets for valuable information such as credit card information, passwords etc.

i) Route Discovery

All the known routes are stored in the cache by DSR. When a node wants to send data to another node, it first broadcasts an RREQ. This RREQ is received by other nodes and as they receive it they start searching their cache for any available route to the destination node. In case on any unavailable routes this RREQ is forwarded while the address of the current node is being recorded in the hop sequence. The RREQ propagates in the network until the availability of a route to the destination or the availability of the destination itself. When this happens an RREP is generated and unicasted to the source node. The contents of this RREP packet are the sequence of hops in the network for reaching the destination node [27, 41].

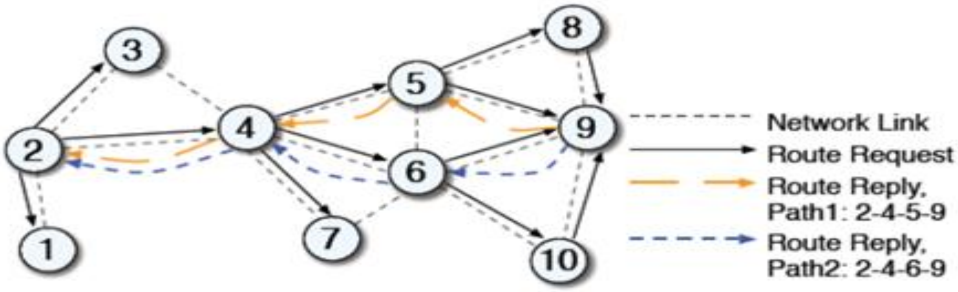

Figure [7]: DSR route discovery for target node [47]

ii) Route Maintenance

In the discovery of an invalid route an error packet is sent to the source node and once this error packet is received, the hop that has error is removed from the cache of the host and all routes containing this erroneous hop are deleted [27].

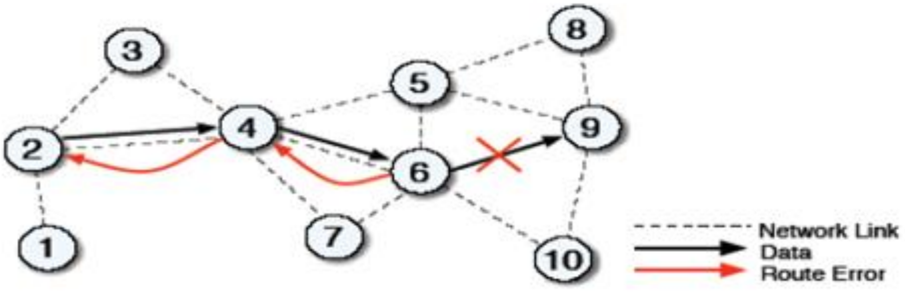

Figure [8]: DSR maintenance for error route [47]

4.3 Selected Performance Metrics for Evaluation

In order to check the protocols performance in terms of its effectiveness there are different metrics to be used. In our study, we use routing overhead, throughput and End-to-End delay for protocols evaluation. The reasons behind the selection of these metrics are the demands of application classes we have selected and also their importance in any data communication network. Furthermore, any protocol needs to be evaluated against these metric in order to check it performance. In order to check the protocol effectiveness in finding routes towards destination, it is interesting to check how much control packets it sends. This metric used to measure the internal algorithm's efficiency of routing protocol. The larger is routing overhead of a protocols (in packets/ bytes), larger will be the wastage of the resources (bandwidth). Similarly, throughput shows protocol's successful deliveries for a time. This means the higher is throughput the better is protocol performance. Also lower is the delay, finer is the protocol performance. On the other hand, these are the metrics which have a greater influence in most of the network communication and use to decide protocols performance. The metrics that we selected for performances evaluation are as follow:

Average End-to-End Delay of Data Packets

It is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receive including the delays due to route acquisition, buffering and processing at intermediate nodes, and retransmission delays at the MAC layer, etc. if the value of End-to-end delay is high then it means the protocol performance is not good due to the network congestion. [42, 43, 17]

$$AED = \frac{\sum_{i=0}^{n} \mathit{Time\ Packet\ Received}_i - \mathit{Time\ packet\ sent}_i}{\mathit{Total\ Numbe\ of\ Packets\ Received}}$$

Routing Overhead (packets)

It is the total number of transmitted packets in a simulation. In a multi hop route, bytes transmitted at each hop count as a single transmission [35, 17]

Throughput

The ratio of total data received by a receiver from a sender for a time the last packet received by receiver measures in bit/sec and byte/sec. It can be expressed mathematically as;

$$\text{Throughput (bit/sec)} = \frac{\text{Number of delivered packet * Packet size * 8}}{\text{Total duration of simulation}}$$

CHAPTER 5: Simulation and Empirical Study

5.1. Simulation and Simulation Model

Simulation is three phase process which includes the designing of a model for theoretical or actual system followed by the process of executing this model on a digital computer and finally the analysis of the output from the execution. Simulation is learning by doing which means that to understand/ learn about any system, first we have to design a model for it and execute it. To understand a simulation model first we need to know about system and model. System is an entity which exists and operates in time while model is the representation of that system at particular point in time and space. This simplified representation of system used for it better understating. The development of simulation is an iterative process resulting in adequate knowledge of understanding. Simulation process can be summarized into three sub fields which are model design, model execution and model analysis shown in Figure below [9].

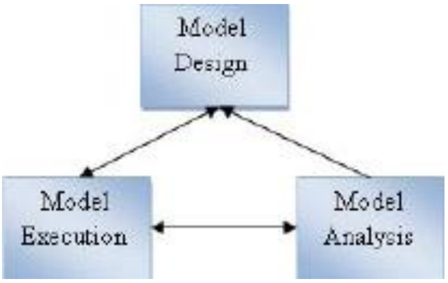

Figure [9]: Three sub-fields of computer simulation [46]

5.1.1. Simulation Tool (OPNET)

Optimized Network Engineering Tool (OPNET version 14.5) modeler is a network simulator provides solutions for managing networks and applications including network engineering, R&D, Operation, Planning and performance management. It is used for modeling communication devices, protocols, technologies and to simulate the performances of these technologies in dynamic virtual network environment. The academic research in Opnet technology provides support for wireless protocols, Mobile Ad hoc network protocols and core network technologies [40].

5.1.2. Network Entities and Functions

Network designed for this simulation is the wireless local area network (WLAN) consisting of basic network entities as sensor nodes (both fixed and mobile) and base station. For application configuration and mobility of the nodes, application configuration, profile configuration and mobility configuration objects are added and configured.

- **Application Configuration**

Application configuration object is used to define the type of application used during simulation. There are eight different type of applications with two different versions light and heavy are supported by Opnet. In this step we select the type of application which will run on network nodes and base station. In this study we used two different types of application i.e. FTP and Voice over IP call. We used FTP application for evaluation of protocols.

Profile Configuration

Profile configuration is used to add the define application to a profile which can have number of application to be used in network. This profile can then easily be implemented on different nodes of interest. We set a profile which supports FTP applications and then assign this profile to all/ selected number of nodes. Our defined profile has two types of application stated earlier.

Base Station

This node of WLAN communicates with nodes in network and interacts to the outer world. Nodes send request and response queries to this station and base station sends to nodes. This station has the support for different applications running at different nodes and control traffic according to the REQ/RES queries by different nodes. The WSN routing protocol is implemented at this node. The node model of this node has all the seven layers of OSI model from MAC layer up to application layer.

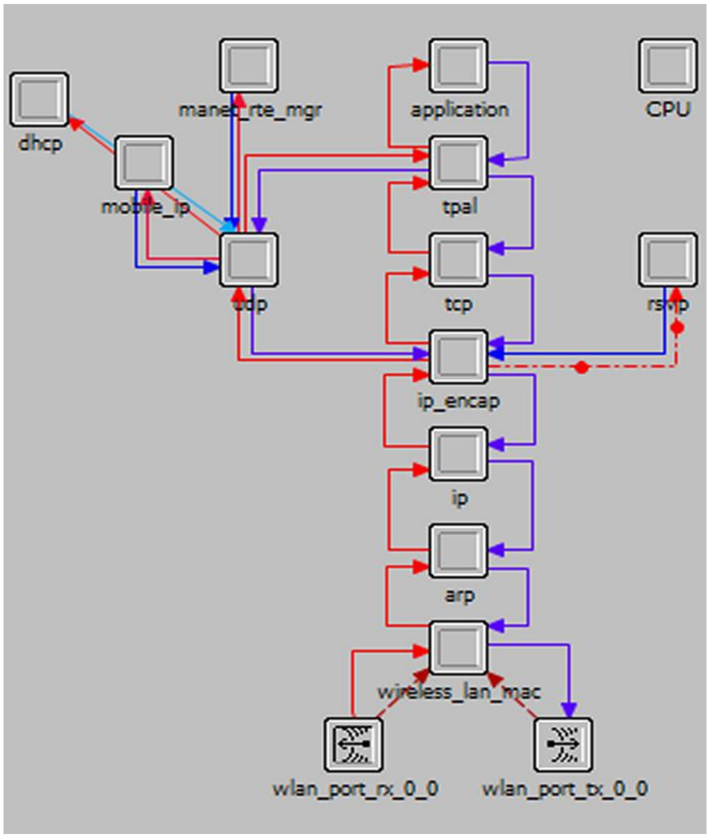

Figure [10]: Node Model of Base Station

The internal structure of a network node is defined in node model. Typically, a node includes different types of fixed and mobile nodes which can be packet switches, workstations, remote sensors and satellite terminals.

Sensor Nodes

These are network entities participating in communication either on demand or regular interval basis depending on the application type and scenarios. All these nodes are connected to the base station directly or via intermediate nodes having their own IDs. There task is to sense the environment and gather data, do some processing on it and forward it to the base station directly or to an upper node in a hierarchy. These nodes are known as submission nodes which can be of different number depending on intended task.

Simulation Setup

We designed two WLANs according to application we selected for this study. First WLAN is made of fixed nodes representing data gathering applications shown in figure 10. While the second WLAN is made of mobile nodes representing object tracking application shown in figure 10. Each of these WLAN was simulated in the presence of different factors having effect on routing protocols performance. We categorized our simulation on the basis of nodes type, scalability, node failure and different number of submission host (source nodes). 30 different scenarios were simulated and results were collected on the basis of following categorization of scenarios.

Fixed nodes Scenarios:

- Low load with 25 nodes
- High load with 50 nodes
- Low load with nodes failure
- High load with of nodes failure

Mobile nodes Scenarios:

- Low load with 25 nodes
- High load with 50 nodes
- Low load with node failure
- High load with node failure

12 scenarios were simulated for fixed nodes and 18 scenarios were simulated for mobile nodes.
Simulation time for each scenario was set to 3,600 seconds and repetitive simulation for each scenario was performed to verify the reliability of our results. The goal of the study was to simulate the behavior of OLSR and DSR for delay, throughput, routing overhead, and network load and energy consumption in the presence of node failure, different number of source nodes and under varying network load (scalability). Therefore, we collected discrete event statistics (DES) both on OLSR and DSR and examine WLAN for delay, load and throughput.

Two different networks were modeled on an area having dimension of 1000 x 1000 meters. First network consisting of fixed nodes and base station spread with in a geographical area. All nodes in this network are considered as a source nodes communicating with constant bit rate. Source nodes are WLAN fixed nodes operating on default power of 0.005 watts while base station is also fixed node operating on 0.001 watts. The application type simulated was FTP at sensor nodes while at base station beside FTP other applications were supported.

The second network was comprised of mobile nodes in the same geographic area having the same data rate, power and application type running at nodes and base station. Besides these parameter, these nodes moves at a constant speed of 10 m/s. The pause time of 10 second was used by mobile node to select a new destination after reaching to its destination.

5.2. OpNet Limitations Acknowledgment

While using OpNet simulator for simulation of routing protocols we were interested to design wireless personal area network (WPAN) by implementing low power, low cost with short t range digital radio base on IEEE 802.15.4-2003 (ZigBee) which is a wireless mesh networking standard, used for high-level communication. But this standard supports the lower protocols layers i.e. physical layer and MAC (Medium Access Control) of data link layer. There is no support for network layer protocols yet. And we were interested to configure and simulate WSN routing protocols on network layer. Also the nature of our network was the same of ad hoc networks. Therefore we needed to use a technology having support for network layer protocols and all those features of network entities need to be designed. Therefore, we used IEEE 802.11. Also our task was to simulate different routing protocols used in WSNs and identifies their effectiveness; therefore, we simulateded protocols which belonged to different families of WSN using OpNet Modler.

CHAPTER 6: RESULTS & ANALYSIS

In this chapter we discussed and analyzed the results of our simulations. We have discussed our results according to the scenarios we choosed in two networks having fixed and mobile nodes. Fixed node network represents data gathering applications in WSN while mobile nodes depicts object tracking applications. For both of these networks we have studied two different scenarios. In first scenario we implemented scalability while in second we applied node failure. We started our discussion by analyzing fixed node network with scalability and then with presence of node failure. Besides, we checked protocols behavior in each of these scenarios for set of performance metrics. Then we analyzed mobile network for the same scenario and protocols are evaluated against the same selected metrics. Finally, a comparison is made and conclusion is presented.

6.1. Fixed Nodes Scenarios with Network Size (Scalability) and Node Failure

In a fixed node network we developed two main scenarios. In first scenario we increased the number of fixed nodes to check protocols behavior with changing network size by looking at WLAN metrics and routing overhead. In second scenario, we check both small and large (25 & 50 nodes) network in the presence of random failure for the same metrics. Both of these scenarios were aimed to depict the data gathering application. Therefore all participating nodes in both scenarios were considered as fixed and submitting nodes, communicating to sink node within a regular interval. The application used for all scenarios was FTP with packet size 512 bytes with packet rate of 4 packet/sec.

Each scenario was simulated for 3600 seconds. 25 fixed nodes were used initially and results were collected with and without node failure. Then nodes were increased up to 50 and after simulation results were collected for end to end delay, throughput, load and routing overhead. In each scenario two different protocols DSR and OLSR were implemented (simulated) in order to evaluate their performance for designed network in the presence of scalability and node failure. The input parameters used for both scenarios were used the same show in table 1 except number of nodes. The results for each metric are show in graph below with respect to scenarios.

Parameter	Value
Environment size	1000 x1000 m
Number of nodes	25 & 50
Traffic type	Constant bit rate
Nodes type	Fixed
Packet rate	4 Packets/sec
Packet size	512 byte
Number of Flows	25 &50
Simulation time	3,600 sec
Number of submission host	25 & 50
Number of receiver	One

Table 1

6.1.1. End-to-End Delay

During the transmission, submitting nodes (sender) in WLAN sends data (packet) to the recipient nodes which receive this data at its MAC layer and then forwarded to higher layers. By end-to-end delay, we mean the end-to-end delay of the entire packet received at WLAN MAC of all nodes in the network and forwarded to higher layer. This includes medium access delay at source MAC, individual reception of all fragments and frames transmission of frames through access point delay if enabled.

In figure 1 (a), we can see the behavior of DSR and OLSR for both 25 and 50 fixed nodes scenario with and without random node failure. If we look at the scenario without node failure, it is clear from the figure that, OLSR gives the lowest and consistent delay as compare to DSR in both small and large network. As the application starts it shows a minor spike but then it stay constant for the rest of the simulation time. OLSR is the proactive protocol which means that whenever application layer is interested to transmit traffic, routes in a network are always available. Periodic nature of routing updates provides fresh route to use. The use of predefined and pre-computed routes towards every node results in consistent nature of delay. OLSR use two types of control messages i.e. Hello and topology control messages. To find information about link status and host's neighbor it use hello message which only sent to one hop away. And to share own advertized neighbors, it broadcast topology control messages periodically.

Now, If we look at graph of 25 and 50 nodes without node failure in Figure 1 (a), it can be seen that it show a minor spick when the application starts running and then directly comes to a constant state throughout the entire simulation duration. This spike is show in time window between 0.0003 and 0005 seconds and then it's consistent behavior in term of delay is show by its value on staying at 0.0004 sec. The reason behind its initial spick (which in negligible) is its initial hello messaging use to share the link status and host's neighbor information. After sharing this information, due to its proactive nature path toward every node is always ready so it gives lowest and consistent delay. This means that, the absence of route discovery mechanism (Pre-computed) in OLSR ensures minimum latency.

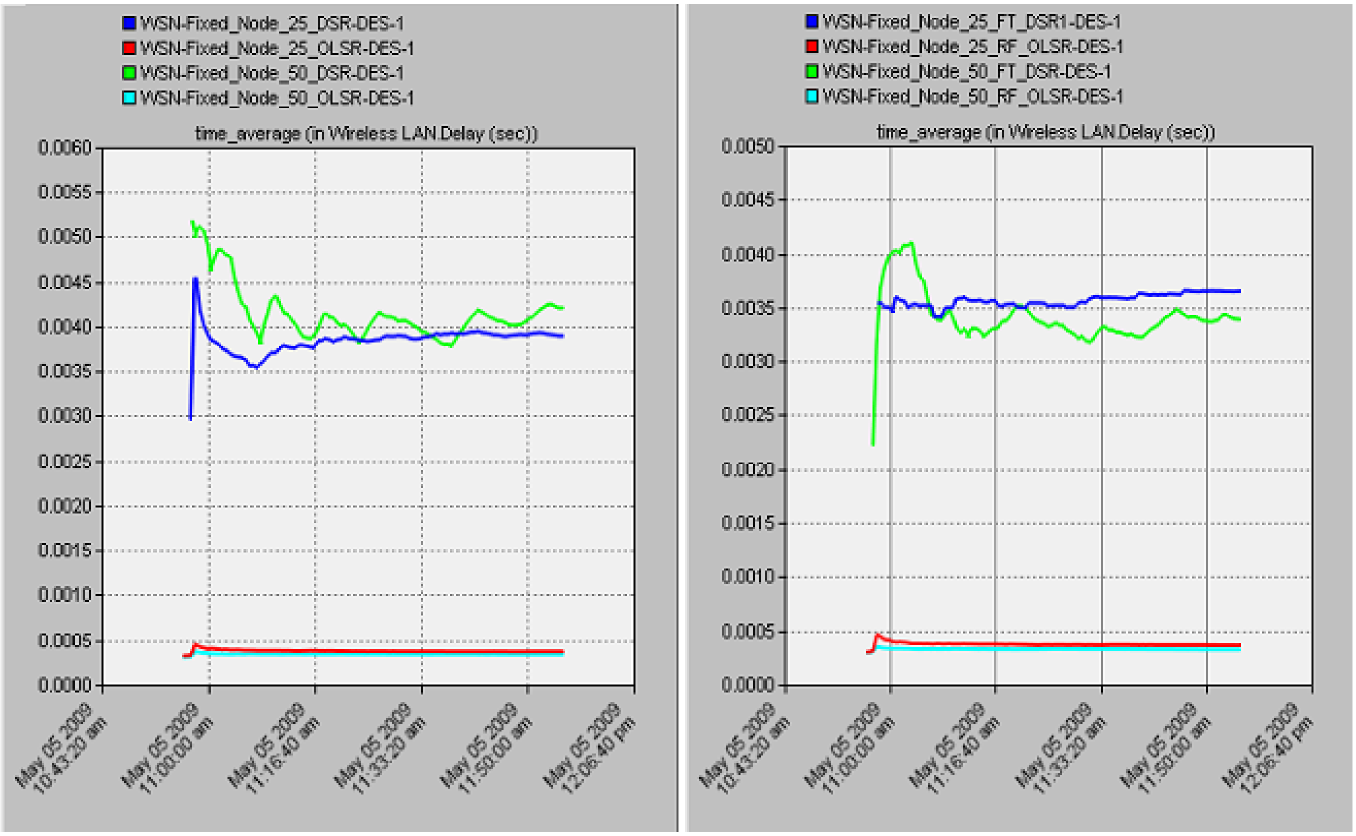

Figure 1: (a) Fixed nodes without Failure (b) Fixed nodes with Failure

This can also be seen in the 50 nodes scenario which gives the same results for delay as for 25 nodes. This means that it performs well in large networks and the reason is again its predefined routing table entries for all nodes. The time required for shortest path computation is not required but only number of control messages will be increased in large networks.

By looking at node failure scenario shown in Figure 1 (b), it is clear that if a node fails, it don't have an effect on delay. The reason behind this is the periodic hello messaging which is used to gather information about the link type and neighbor host as stated earlier. The link type provides information about the lost link so it can be sense in advance if there is a failed link. Therefore and alternate path will be used to reach a destination. While looking at DSR response, it gives considerably higher delay both in small and large networks. The delay for large network is higher as compare to the small network and its varying with the passage of time. This shows the source routing of DSR, which means that the path from any source node to destination node computed on demand basis therefore its gives the varying nature of delay. In node failure case, it gives a slightly low delay because of the fact reduced number of nodes are actively communicating. This can also be seen in 25 nodes case, where it gives a relatively consistent delay as compare to the case of 25 nodes without node failure. This explains that the numbers of nodes were decreased in this case so the delay decreases and behave like a constant delay.

6.1.2.Throughput

The ratio of total data received by a receiver from a sender for a time the last packet received by receiver measures in bit/sec and byte/sec. It can be expressed mathematically as;

$$\text{Throughput (bit/sec)} = \frac{\text{Number of delivered packet * Packet size * 8}}{\text{Total duration of simulation}}$$

This means that if high throughput is to be achieved, network delay should be low. The behavior of both routing protocols both in presence and absence of node failure for a WLAN consisting 25 & 50 is shown in figure 2 below. By looking at figure below we can see the overall throughput at WLAN reduced approximately up to 5o% in presence of node failure with respect to without node failure scenario. This indicates that if nodes will fail in a network, the overall number of transmitting data (bits/bytes/packets) will decreased accordingly because of the less number of active flow at particular time (simulation time). As we are interested in protocols behavior so we will look at each protocol in both scenarios to compare their performances.

In without node failure scenario we can see that, in 25 nodes network DSR throughput rate starts with approx 55000 bit/sec and within no time it decreases up to 49000 bit/sec. the fact is, since DSR operates using source routing which means it construct source route in packet's header by giving the addresses of all nodes the packet has to be forwarded in order to reach the destination. This implies that it does not have any routing table information except source cache, therefore for each node it has to discover a route which involves route discovery, route reply packet and also need route maintenance at each hop. This causes a significant delay before data transmission also increase routing overhead. So it is clear from the graph that it performs worst as compared to OLSR and cannot maintain its rate at which it started. The reason here is the increasing number of nodes for which it has to establish routes. The more will be the number of nodes the more will be degradation in its performance due to the reason of delay at each hop which can be seen in DSR 50 nodes case in the same graph. It is also clear that in small network case (25 nodes), although its throughput rate is effected approx by 50% but then quickly for the rest of simulation time it maintain its transmission rata slightly consistent. While in 50 nodes case, its rate not only decreased to half of its rate at starting time but also it took longer time to maintain its rate slightly stable. This indicates that, if the number of nodes will increased the more time it will take for routing to reach all nodes and route maintenance as well.

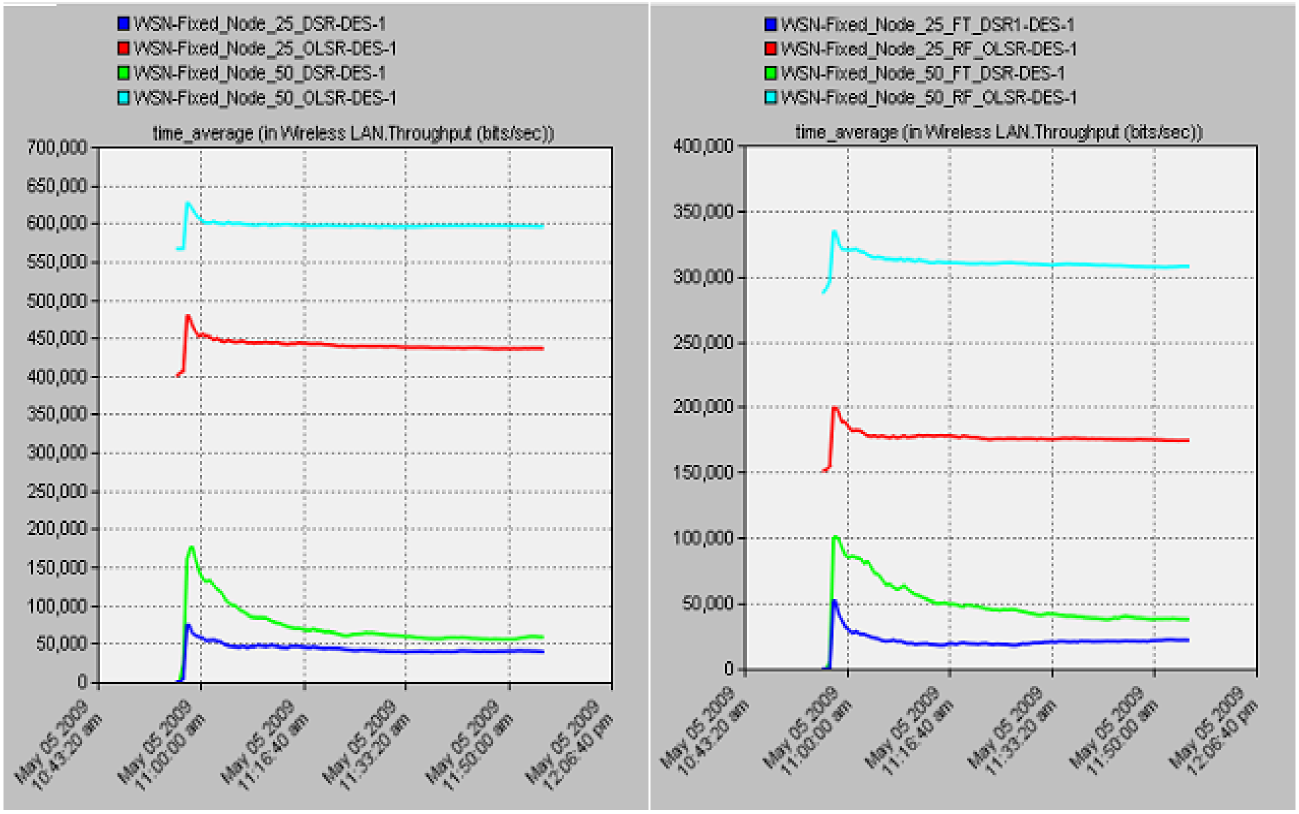

Figure 2: (a) Fixed nodes without Failure (b) Fixed nodes with Failure

While looking at node failure scenario for both 25 & 50 nodes, it depicts that the performance of DSR drops from 50,000 bit/sec to 20,000bit/sec and in 50 nodes scenario it drops slightly with greater ratio i.e. from 100,000 bits/sec to 40,000. This again implies that the presence of random node failure will affect dense populated network badly as compare to small network. The reason is, in a large network it becomes difficult to discover a route from source to destination with the presence of failed node both by resources consumption (memory, energy) and overhead complexities.

Looking at OLSR performance in 25 & 50 nodes scenarios without node failure, it not only out performs but maintains its rate stable after a short spike in both cases. This spike is because of control messages it needs to send to share network information. It is clear that low delay means high throughput, as OLSR experience minimum delay in transmission therefore it performs better by mainly transmitting packets receives from sender not taking into account any activity like route discovery or maintenance etc. Also in node failure case it performance can be viewed as degraded due to the number of failure nodes. Here, it again maintains comparatively better throughput rate than DSR for both small and large network cases. As it drops from 200, 000 to 175,000 bit sec in 25 nodes case and 340,000 to 310,000 bit/sec in 50 nodes case while DSR drops from 50,000 to 25,000 bit/sec and 100,000 to 49,000 bit/sec respectively. This can be concluded that the random failure of nodes affects the throughput rate of DSR roughly about ½ of its starting data rate while 1/8 of OLSR.

6.1.3. Routing Overhead

To find routes, routing protocols used to send control information (packets). These control information along includes basically route request sent, route reply send and route error sent packets. Routing overhead can be define as a ratio of total number of control packets sent to the total number of data packets delivered successful i.e.

$$\text{Routing overhead} = \frac{\text{Total number of control packets sent}}{\text{Total number of successfully delivered data packets}}$$

In order to check the protocol effectiveness in finding routes towards destination, it is interesting to check how much control packets it sends. This metric used to measure the internal algorithm's efficiency of routing protocol. The larger is routing overhead of a protocols (in packets/ bytes), larger will be the wastage of the resources (bandwidth). Therefore, it is necessary to examine the routing overhead of a protocol in order to determine its efficiency. Considering the results in figure 3 (a), we observed the behavior of DSR in 50 nodes case without node failure scenario that DSR generates considerable routing overhead as simulation starts but then after a specific time interval it decreases overhead which indicates the routes establishment after which the overhead decrease regularly. Besides, DSR seems to generate more overhead if network grows as it use source routing therefore if a routes is not available from a node to destination somewhere in the middle it will propagate SOURCE REQUEST in the network. This can also lead to the generation of REQUEST ERRORS messages causing also routing overhead. While in small network of 25 nodes it performs better with negligible routing overhead which is discussed later.

Furthermore, we found a notable change in DSR behavior in 50 nodes network case with nodes failure scenario shown in Figure 3 (b) It gives the routing overhead of 1packet/sec in 25 nodes case when it application runs but then quickly drops its overhead ration to 125bits/sec and stay with this ratio for rest of the simulation time. This implies that for small network DSR outperforms and makes it better choice for routing due to its reactive nature. This means that it sends control messages to nodes only when it is required and do not creates any overhead by sending periodic updates or by maintain routes information. On other hand, in 50 nodes scenario it jumps and gives 7100 bits/sec of routing overhead. A minor drop after I minute can be seen and then again it rises to 7400 bits/sec and stay for about 2 minutes with this rate. Similarly, again a minor rise is clear for the next minute but then a sudden drop up to 4800 bits/sec. the routing overhead rate then further decreasing the same way and shows a slight small rise again at the end of simulation.

So this behavior of DSR in 50 nodes case in node failure scenario shows its operation nature very clearly. As it is clear from the graph that it's routing overhead a smaller than that of without node failure scenario but it treats both the failed and working nodes in the same way. This is because of source routing nature of DSR. As there is neither routing table information nor link status information (hello messages) present to DSR, therefore it starts by sending a large amount of control messages (ROUTE REQUESTS) to different nodes to reach a destination when application just starts running which is shown in the start of simulation. But here we can see the difference in behavior with respect of scenario without node failure. As its overhead does not drop directly in start which means ROUTE REPLIES did not received and ROUTE ERROR generated to source which increase the overhead further. While the direct drop shows the successful route finding via same or different path and reduces overhead.

On the other hand, if we look at behavior of OLSR it gives a consistent nature of routing overhead due to its proactive routing nature. This means that path to all nodes are already defined and calculated. The only overhead created at network is the periodic updates of routing information which is slightly low. Although network size will affect the routing overhead but it remains stable and consistent.

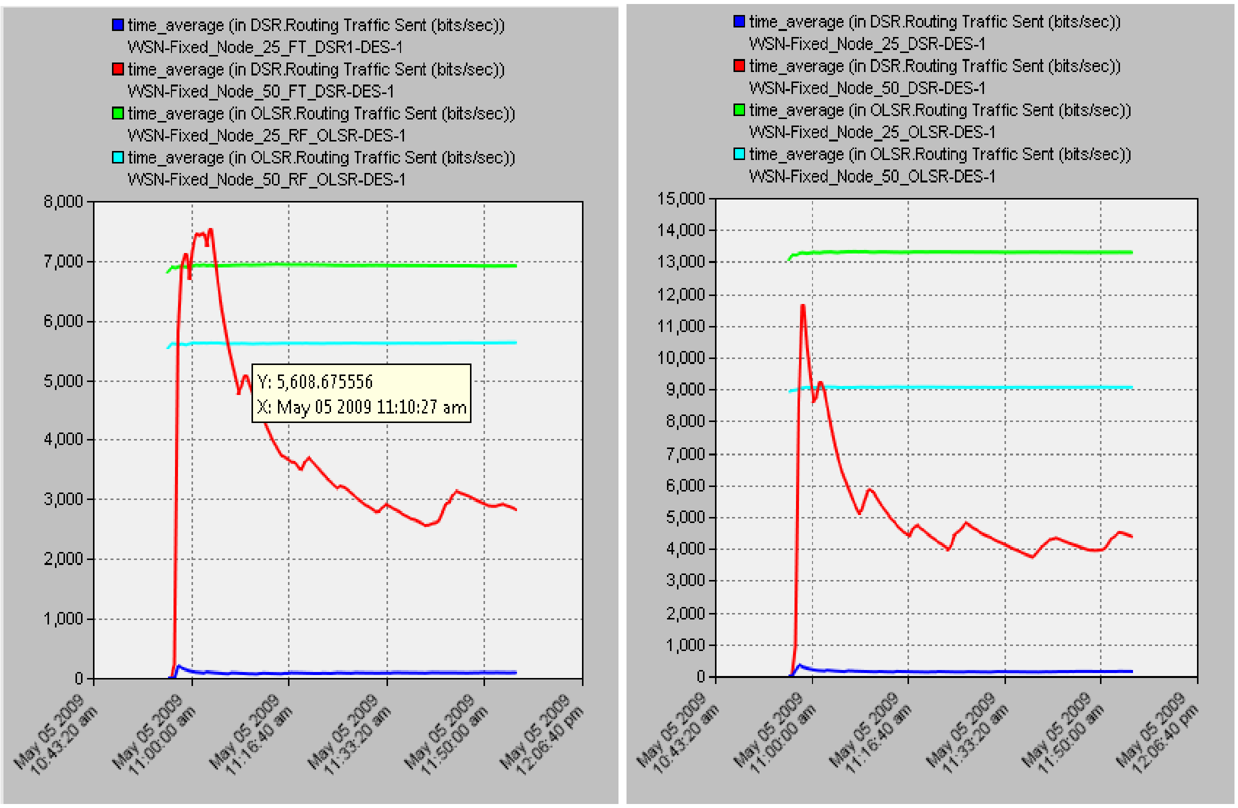

Figure 3: (a)Fixed nodes without Failure (b)Fixed nodes with Failure

6.2. Mobile Nodes Scenarios with Network Size and Node Failure

In mobile nodes network we developed two main scenarios. In first scenario we increased the number of mobile nodes in networks to check protocols behavior with changing network size by looking at WLAN metrics and routing overhead. While in second scenario, we check both small and large (25 & 50 nodes) networks in the presence of random failure for the same metrics to check protocols behavior toward node failure. Both of these two scenarios were aimed to depict the Object tracking applications like medical asset tracking by keeping nodes mobile. In first case all nodes were considered executing nodes to understand the effect of scalability of network on selected protocols performance. Then a random number of nodes were made failed to check the protocols response in presence of failure i.e. re-routing, alternate route selection, updating routing table entries. The effect was analyzed by looking their delay, throughput and routing overhead. The application used for all scenarios was FTP with packet size 512 bytes with packet rate of 4 packet/sec.

Each scenario was simulated for 3600 seconds. 25 fixed nodes were used initially and results were collected with and without node failure. Then nodes were increased up to 50 and after simulation results were collected for end-to-end delay, throughput, load and routing overhead. In each scenario two different protocols DSR and OLSR were implemented (simulated) in order to evaluate their performance for designed networks in the presence of scalability and node failure. The input parameters used for both scenarios were used the same shown in table 2 except the changing number of nodes. The results for each metric are show in Figure 4, 5 and 6 below with respect to scenarios.

Parameter	**Value**
Environment size	1000 x1000 m
Number of nodes	25 & 50
Traffic type	Constant bit rate
Nodes type	Mobile
Packet rate	4 Packets/sec
Packet size	512 byte
Number of Flows	25 &50
Simulation time	3,600 sec
Number of submission host	25 & 50
Number of receiver	One

Table: 2

6.2.1. End-to-End Delay

To analyze the results for end-to-end delay of selected protocols in both scenarios with different number of nodes we will look at each scenario comparing both protocols with respect to number of nodes and type of scenario. Considering the scenario without nodes failure shown in Figure 4 (a), we observe that DSR behaves nearly the same both in 25 and 50 nodes cases. Although delay time of DSR in 25 nodes case is smaller (starting at 0.0030 sec) than that of 50 nodes case (starts at 0.0040) but the delay pattern remains the same. Comparatively looking at OLSR, the case is not the same with respect to DSR and even with respect to number of nodes. It gives notably smaller delay in both cases than DSR and gives smaller and steady delay in 50 nodes as compare to 25 nodes case. This can be argue the way that, DSR uses cache routes which leads to delay. But in case of larger network as the number of cache routes increase resulting in high delay.

The case of OLSR is different. OLSR uses always ready routes and routing updates provides multiple fresh routes for data transmission therefore it experienced lower delay in both 25 and 50 nodes cases. This can also be seen by looking at OLSR delay for 25 and 50 nodes cases. In 25 nodes it starts by giving delay of 0.0005 seconds and then it increases a bit up to 0.0007 seconds and stay stable for the rest of simulation time.

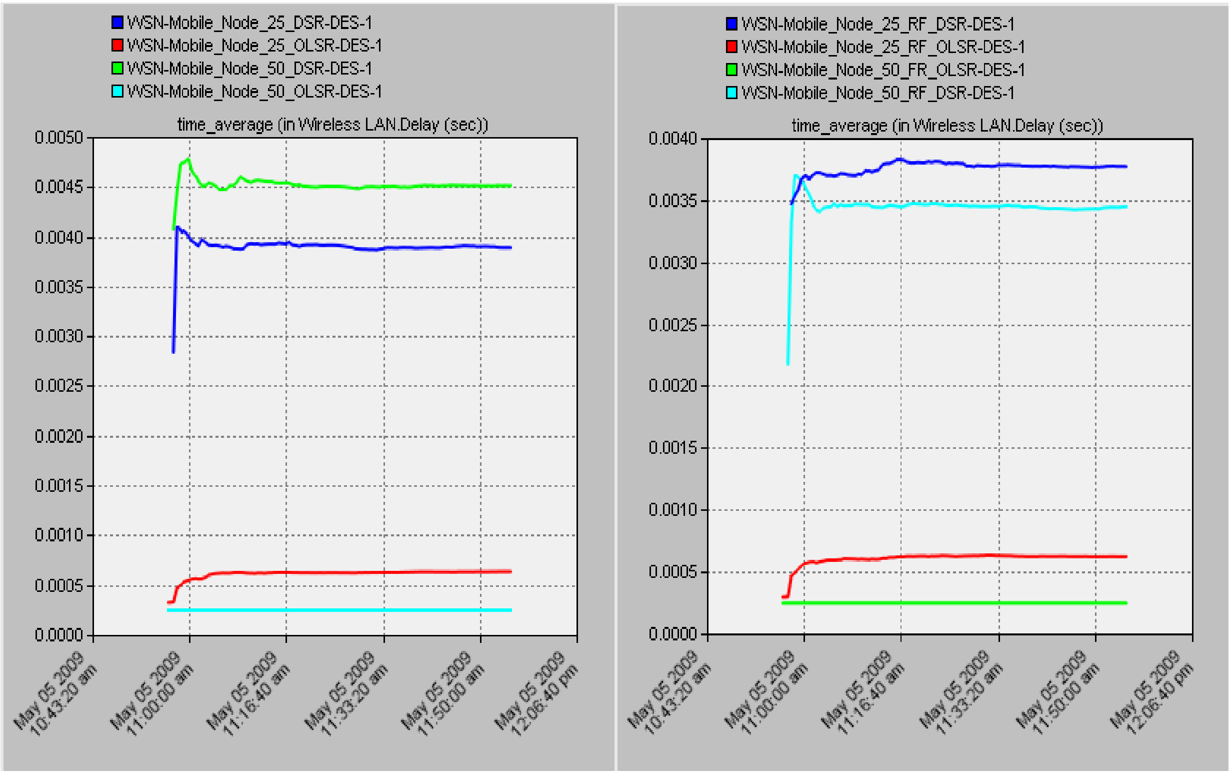

Figure 4: (a) Mobile nodes without Failure (b) Mobile nodes with Failure

Here we can see a smaller rise in its delay due to the smaller number of alternate routes availability but the mobility of nodes do not have any effect on its delay pattern. The reason for this is the multiple routes existence. Because, by looking at 50 nodes scenario it is clear that it gives a lower delay with constant rate. This implies that it performs better with in a large network. The fact behind its consistent and lower delay is its operation nature. As routes are already computed to all nodes so nodes are moving within a defined trajectory therefore it's not a challenging task for OLSR to used different node (hops) to reach a destination. But number of alternate routes to destination can affects the performance of protocols in terms of delay which is clear in 25 nodes case.

On the other hand if we look at node failure scenario presented in Figure 4 (b), we can see an interesting response of DSR. As in25 nodes case, it starts by giving delay of 0.0035 seconds grows up to 0.0037 second in one minute time but then it rises up to 0.0038 seconds in 10 minutes. After that it stays consistent but not really stable till the last 10 minutes of simulation time. While in 50 nodes case, it starts with 0.0022 seconds delay and grow up to 0.0037 and then a fall to 0.0034 and stay consistent for rest of the simulation time 0.0035 seconds.

6.2.2. Throughput

To analyze the results for throughput of selected protocols in both scenarios with different number of nodes we will look at each scenario comparing both protocols with respect to number of nodes and type of scenario. If we look at scenario without nodes failure shown in Figure 5 (a), we can see the response of DSR in 25 and 50 nodes case behaving differently. In 25 nodes case, it show a sudden rise in throughput rate but then goes quietly to steady state with a smaller fraction of change in throughput rate up to 250,000 bits/sec. But in case of 50 nodes, although it gives high throughput but its behavior do not look like stable. Because it is a reactive protocols so it can find routes in small network with less number of

ROUTE REQUEST (route request do not need to propagate throughout the network), small number of ROUT ERROR messages. But, when network grows, the ratio of ROUTE ERROR messages increase affecting throughput rate shown by somehow unstable curve along time window.

Comparatively looking at OLSR, it outperforms as compared to DSR in 25 nodes case but as network grows it drops its rate very poorly. The reason behind this is its nature of working. It computes all paths in advance but as nodes are mobile so its routing table entries do not works in larger network. While in smaller network it is possible to compute paths at runtime but not in larger networks.

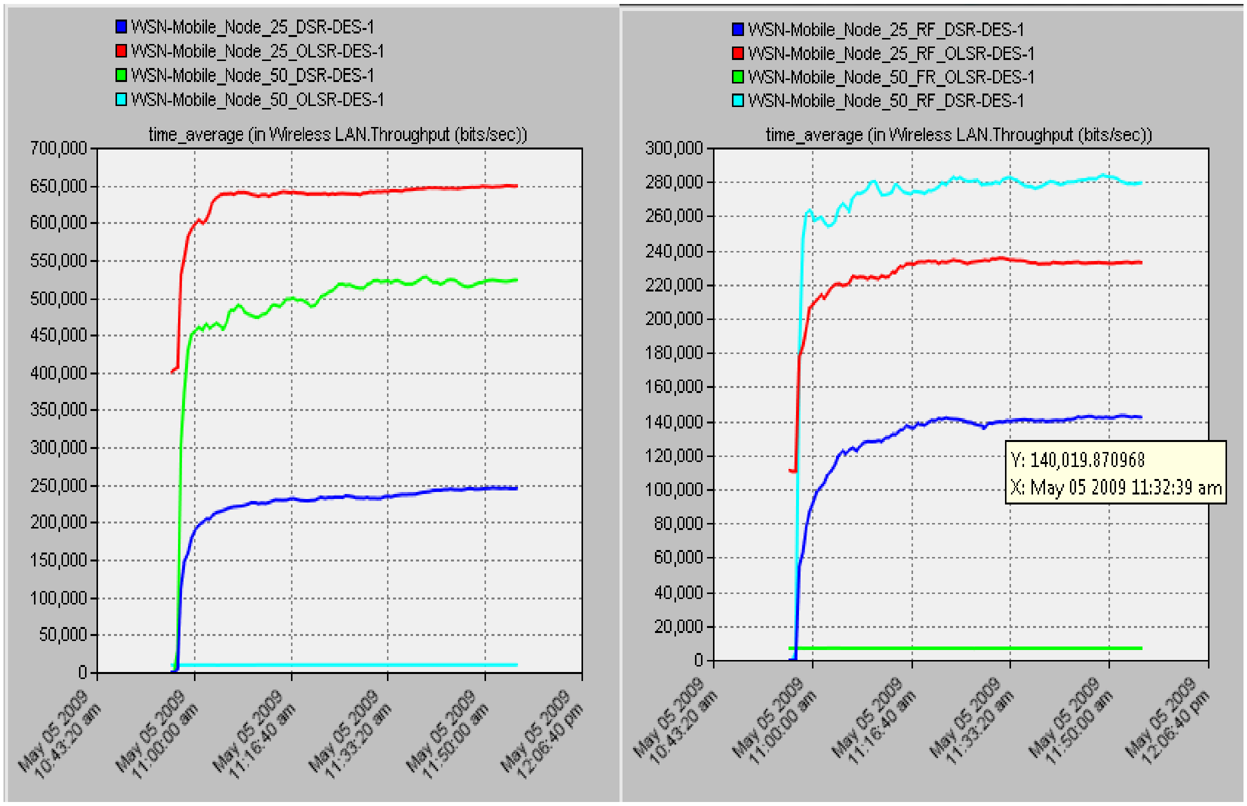

Figure 5: (a) Mobile nodes without Failure (b) Mobile nodes with Failure

While looking at node failure scenario presented in Figure 5 (b), we can see the behavior of DSR in 25 nodes case for throughput. It start with a constant rise and giving throughput about to 59,000 bit/sec at start of simulation and then it moving towards x-axis along with time window up to end of simulation time and keeping its throughput rate slightly consistent with smaller fraction of spikes up to 140,000 bits/sec. while looking at OLSR in the same scenario for 25 nodes case, it can be seen that it reacts the same way as DSR but gives relatively higher throughput. It also keeps its rate more stable than DSR without spikes. The reasons for the less smoothness in 25 nodes case of DSR behavior is its reactive approach. As the simulation starts it gives better data rate due the factor of number of routes it established using demand basis transmission. After a while, as number of failed nodes occurs in transmissions which enforce it to find alternative route or ROUTE ERROR decreasing its throughput rate shown in minor spikes.

While looking at OLSR, it gives relatively higher throughput as compare to DSR but with the same behavior of data rate. Which shows its behavior in smaller networks in presence of failed nodes i.e. it can handle node mobility despite of precompiled routes. The smoothness of OLSR curve along time window shows its response towards failed nodes. As there are smaller number of nodes and node mobility does not affect it badly.

An interesting behavior can be seen if we look at 50 nodes scenario for DSR and OLSR, DSR presents a constantly changing curve represents its re-route discoveries and ROUTE ERROR messages shown by regular spikes along time window. On the other hand, OLSR it gives somehow double throughput as compared to 50 nodes case without node failure. The reason of this behavior is that OLSR cannot tolerate mobility if network grows. So in the case of failure, as some nodes are failed which means the number of executing nodes becomes smaller so it showed it performance slightly better than without node failure.

6.2.3. Routing Overhead

To analyze the results for routing overhead of DSR and OLSR in both scenarios with different number of nodes we will look at each scenario comparing both protocols with respect to number of nodes and type of scenario. Considering the scenario without nodes failure displayed in Figure 6 (a), we observe that DSR behaves totally different in 25nodes case as compare to 50 nodes case. As it uses source routing so the routing overhead (control messages) for smaller network will be small also due to its proactive nature of operation. Because when route is needed then ROUTE REQUEST message will be send and the ratio of ROUTE ERROR will be small.

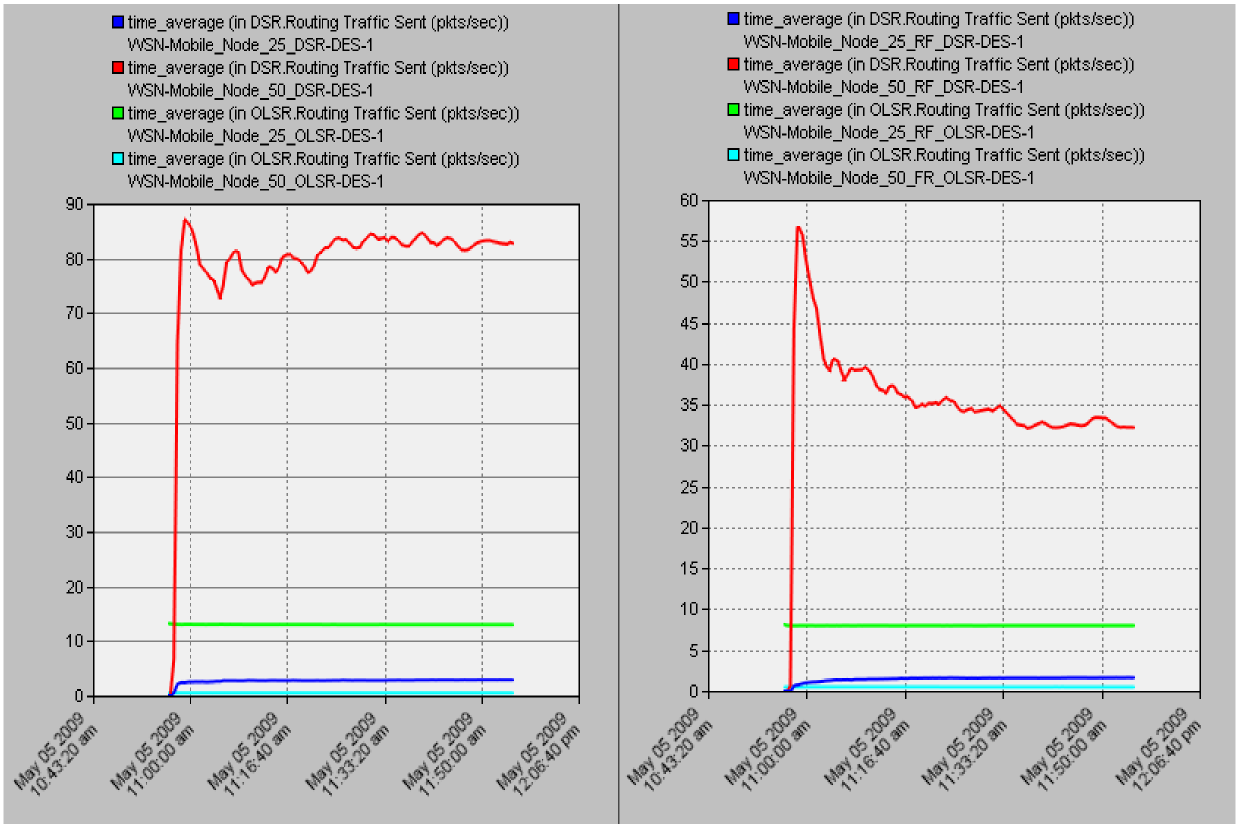

Figure 6: (a) Mobile nodes without Failure (b) Mobile nodes with Failure

But as network grows the routing overhead will definitely increases for that protocol which do real time routing (on time). Therefore it shows a relatively larger overhead in 50 node case. While looking at OLSR performance, it is clear that it outperforms in both small and large network. This is due to its predefined routes it using for each destination (node). So the only overhead it shows is because of routing updates, topology control messages and hello messages used to aware about network, link and node condition.

Similarly, by analyzing both these protocols in node failure scenario shown in Figure 6 (b), for both cases we can see that the overhead is comparatively low but its pattern is same for OLSR and DSR small network case. In OLSR the fact of this consistent behavior is the control messages it uses for monitoring network conditions. Therefore, it can update its routing table and path according to the node failure which can be sensed using topology control and hello messages. But DSR do not use such a mechanism to sense the route or node status in advance. Therefore, node failure affects its performance in large network. Interesting results can be seen in both with and without node failure case for DSR in case of 50 nodes from the above graph.

It dictates that, without node failure the routing overhead increased up to 88 packets/sec and then it varies between 70 to 90 packets/sec but remains irregular and high. While in the case of node failure of 50 nodes, routing overhead grows up to 57 packets/sec but then it decreases to 40 abruptly. Furthermore, it continuously decreases in an inconsistent way and falls up to 35 packets/sec at the end of simulation. The reason here is the network size (active nodes). In first case it checks for different nodes to reach destination which results in higher overhead. After route establishment as the number of nodes remains the same so according to demands just the direction of the routes has to change so show a continuous overhead in irregular form. While in later case, as number of active nodes decreases after failure, so it show a higher overhead to find routes to different nodes. After some time, overhead continuously decreasing due to less number of ROUTE REQUEST and ROUTE ERROR executions. This is done by keeping route cache helps in neglecting the dead nodes and leaves retransmission to higher layer.

6.3. Summary/Observation

In this chapter, we have discussed and analyzed the simulated results. We have simulated and discussed different metrics of wireless sensor networks in different topologies and complexities. End to end delay, throughput and routing overheads are the main metrics we have considered in this chapter. We have taken fixed node and mobile node network scenarios with scalability and node failure and have simulated them for certain period of time. We have set certain parameters for the simulation purposes and have shown the simulated results. In each scenario two different protocols DSR and OLSR were implemented (simulated) in order to evaluate their performance for designed network in the presence of scalability and node failure.

In the case of fixed nodes, we have shown that the metric graphs (shown in Figure 1 to Figure 3 including a, b) for the two protocols depict same and different shapes depending on scenarios. The scenario wise observations are given below based on graph results and tabulated values of each protocol.

Fixed Nodes Network Results

Protocol	Metric	Small Network	Large Network	Small Network with Failure	Large Network with Failure
DSR	Delay (sec)	0.0045	0.0052	0.0035	0.0041
	Throughput (bits/sec)	75,000	190,000	50,000	100,000

	Routing overhead (bits/sec)	200	7600	140	11,800
OLSR	Delay (sec)	0.0005	.0004	0.0005	0.0004
	Throughput (bits/sec)	480,000	640,000	200,000	340,000
	Routing overhead (bits/sec)	7000	13200	5700	9000

- Both in small and large networks OLSR outperform than DSR with prominent difference in delay. Also the presence of node failure has a small affect on DSR but no affect OLSR delay. This illustrates that network size and node failure has no such impact on OLSR delay but it has an impact on DSR performance in terms of delay.
- Both in small and large network OLSR give a higher through than DSR but the effect of node failure in small network on OLSR throughput is higher than that of DSR. While in larger network the effect of node failure on DSR is higher than that of OLSR.
- The routing overhead of OLSR is much higher than that of DSR in both small and large network. In node failure case routing overhead have a smaller effect on both OLSR and DSR overhead in small network but in large network the DSR routing overhead increases while OLSR decrease which means OLSR performs better.

Mobile Nodes Network Results

Protocol	**Metric**	**Small Network**	**Large Network**	**Small Network with failure**	**Large Network with failure**
DSR	Delay (sec)	0.0042	0.0048	0.0038	0.0006
	Throughput (bit/sec)	250,000	480,000	141,000	280,000
	Routing overhead (bits/sec)	2,720	47,872	1,632	31,008
OLSR	Delay (sec)	0.0006	0.0003	0.0006	0.0003
	Throughput (bits/sec)	650,000	239,000	239,000	2000
	Routing overhead (bits/sec)	7,616	544	4,352	544

- By looking at the tabulated results mobile nodes case of each protocol for different metrics in both scenarios, our observations are;

- We observed that both in small and large networks OLSR gives considerably small delay as compare to DSR. The presence of node failure does not affect OLSR delay but have an effect on DSR delay in large network.
- In small networks OLSR give higher throughput than DSR but in large network DSR gives better throughput than OLSR. The affect of node failure on both DSR and OLSR is relatively same but in large network this affect is totally different and DSR give largely high throughput.
- Routing overhead of OLSR in small network is higher than DSR but interestingly in large network it is totally different and DSR generate extremely high routing overhead than OLSR. While node failure on both OLSR and DSR in small network has same affect and in large network, it affects DSR overhead but does not affect OLSR.

Conclusion

In this study, we have evaluated two routing protocols for their responses to node failure and network scalability with respect to their throughput, packet end-to-end delay and routing overhead as a performance metrics. The selected performance metrics were subjected to identify protocols effectiveness and suitability in terms of reliability and efficient use of network resources for two different type of networks i.e. fixed nodes and mobile nodes networks. To measure the reliability of the protocols, throughput and end-to-end delay were used as a metrics and routing overhead was checked to identify protocols behaviour in resource utilization. Because the demand for protocol reliability and effectiveness is vital in any network.

OLSR and DSR were simulateded in two different scenarios having both small and large number of executing nodes with and without random failure of nodes for both fixed and mobile nodes networks. All the nodes in every scenario were used as source nodes sending data to a common base station (destination). This study analyzed and proved that OLSR is more reliable protocol in term of delay and throughput and somewhere an effective protocol in term of routing overhead depending on the network type and size. Although; DSR has its own effectiveness regarding network overhead but overall performance of OLSR is better than DSR. The network type and routing challenges base conclusion is as follow;

OLSR is more superior to DSR in terms of delay for both mobile and fixed nodes networks. Also node failure and network size have no considerable affects on OLSR performance with respect to delay but does have on DSR.

OLSR outperforms in both small and large network with respect to throughput in fixed nodes networks and node failure has considerably smaller affect on OLSR as compare to DSR. But in mobile nodes networks, OLSR performs better for small network while DSR perform good for large network and the effect of node failure affect is different with respect to network size i.e. the effect on DSR is smaller in large network while on OLSR is lesser in small network.

Routing overhead of DSR is smaller both in large and small network than OLSR in fixed node network, but in mobile node networks DSR gives higher overhead than OLSR. Certainly, node failure in mobile and networks with small and large number of nodes, affects DSR badly as compare to OLSR. In one way this can be concluded that for high throughput and minimal delay OLSR is better choice in case of fixed network despite of node failure expectations. Also in mobile nodes networks, OLSR is good choice for both small and large networks with and without node failure for minimal delay but for higher throughput, DSR is better for large network and OLSR is better for small network also with respect of node failure. Relatively, it can also be summarized that both in fixed and mobile nodes networks OLSR is the better choice and for smaller network while DSR.

From the conducted study on selected protocols, we conclude that no one protocol is superior with respect to overall performance. The performance of one protocol may be far better in terms of delay other may be superior in terms of routing overhead. Secondly, network type and size also matters for protocols performance. Therefore, choice for selecting particular routing protocol will depend on application type (expectation from network) and intended use of network.

Future Work

WSNs is quite a hot concept in wireless communication meaning that much research is going on and many issues are subjected to be investigated in this domain. Due to the time limitations, our focus was only on the routing protocols during this study. Though, there are many possible directions needed to be explored. The future directions for WSN vary from network structure to, application types to application demands. Different applications have different sensitivity factors. Different network designs have different constraints with respect to varying challenges.

- There are different issues at design level of WSN, like node deployment, heterogeneity, localization and synchronization which needs to be explored further.
- There are various protocols already developed for WSNs need to be compared with respect to WSNs application classes.
- Different challenges need to be implemented on different protocols in real scenarios to identify protocols efficiencies.
- Routing protocols need to be evaluated with specific performance metrics with respect to application demands in order to identify protocols suitability for different applications.
- Simulations environment could be improved to support more number of routing protocols and provides additional metrics for protocols evaluation.
- Protocols security should be investigated with respect to various natures of attacks to which wireless communication is considered as an attractive target.
- QoS for applications in WSNs needs to explored and appropriate algorithms need to be devolved.

References

[1] S. Gobriel. "Energy-efficient design of ad-hoc and sensor networks", M.Sc, University of Pittsburgh, 2008

[2] Y. Chen and Nasser. “Enabling QoS multipath routing protocol for wireless sensor networks,” in *IEEE International Conference,* 2008, pp. 2421 – 2425.

[3] T. Zia and A. Zomaya. “Security issues in wireless sensor networks,” in *Proceedings of the international Conference on Systems and Networks Communication,* 2006.

[4] Y. Wang, G. Attebury and B. Ramamurthy. “A survey of security issues in wireless sensor networks,” *IEEE communication surveys*, Vol.8, No.2, 2006.

[5] A.al-yasiri and A.sunley. “Data aggregation in wireless sensor networks using the SOAP protocol,” Journal of Physics Conference Series 76**,** 2007.

[6] A.Khetrapal, “Routing techniques for Mobile Ad Hoc Networks Classification and Qualitative/ Quantitative Analysis,” Department of Computer Engineering, Delhi College of Engineering University.

[7] M. N. Elshakankiri, M. N. Moustafa and Y. H. Dakroury. “Energy Efficient Routing Protocol for Wireless Sensor Networks,” in *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Dec. 2008, pp. 393 – 398.

[8] F.L. Lewis, “wireless sensor network,” *Technologies Protocols and Applications,* New York, 2004.

[9] A. Habib. “Sensor network security issues at network layer,” in *2nd International Conference on Advances in Space Technologies Islamabad, Pakistan,* Nov. 2008, pp. 58-63.

[10] A. A. Ahmed, H. Shi and Y. Shang. “A survey on network protocols for wireless sensor networks,” in *Proceedings of Information Technology: Research and Education,* Aug. 2003, pp. 301- 305.

[11] G. Acs and L. Buttyabv. “A taxonomy of routing protocols for wireless sensor networks,” *BUTE Telecommunication department,* Jan. 2007.

[12] M. Lyas and I. Magoub. *Compact wireless and wired sensor system.* CRC Press, 2004.

[13] l Stojmenovic. *The state of the art of sensor network*. John wali and sensor.2005

[14] L.Cui, F. wang and H. Luo. “Network and Parallel Computing,” Springer Berlin / Heidelberg. Ltd.14 Oct 2004.

[15] J. Fraden. *A hand book of modern sensor: Physic, design, and application*. Birkauser, 2004.

[16]I.Akyildiz, W. Su, Y. Sankarasubramaniam,"A survey on sensor networks," IEEE Communications Vol: 40 Issue: 8, pp.102-114, August 2002.

[17] G. Gelet, "Performance Evaluation of Wireless Sensor Network Routing Protocols for Critical Condition Monitoring Application" M.A. thesis. Addis Ababa University, Oct 2007.

[18] Wenning, B.L. Pesch, D.Timm-Giel, A. Görg. "Environmental monitoring aware routing in wireless sensor networks*," in Proceedings of the IFIP joint conference on Mobile and Wireless Communications Networks (MWCN 2008)* and Personal Wireless Communications, 2008, pp. 5-16.

[19] K. Mitta, A. Veda, B.K. Meena, "Data Aggregation, Query Processing and Routing in Sensor Networks," MTech IT, Powai, Mumbai.

[20] T. He, et.al, "Achieving Real-Time Target Tracking Using Wireless Sensor Networks,"in *Proceedings of the 12th IEEE* Vol.4, Issue 7, pp.37-48, April. 2006.

[21] Jamal N.Al-Karaki, A.E. Kamal, "Routing techniques in wireless sensor networks a survey," *Wireless Communications*, IEEE Publication Vol.11, Issue. 6, pp.6- 28, Dec. 2004.

[22] M. Frikha, J.B. Slimane, "Conception and Simulation of Energy-Efficient AODV protocol Ad Hoc Networks," Tunisian Communication's, Tunis.

[23] S. Sharma, D. Kumar and R. Kumar, "QOS-Based Routing Protocol in WSN," Advances in Wireless and Mobile Communications.ISSN 0973-6972 Vol. 1, No. 1-3, pp.51-57, 2008.

[24] X. Hong, K. Xu and M. Gerla."Scalable Routing Protocols for Mobile Ad Hoc Networks," IEEE Network, University of California at Los Angeles, Aug. 2002.

[25] A. Fourati, K.A. Agha, "A shared secret-based algorithm for securing the OLSR routing protocol," LRI, IRIT, CRISTAL University Paris-SUD XI Paris, France.

[26] J. Broch, et.al, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols" in *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98),*Dallas, Texas, USA, Oct. 1998.

[27] D.B. Johnson, D.A. Maltz, J. Broch, "The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," Computer Science Department Carnegie Mellon University.

[28] D. Xiao,M. Wei,Y. Zhou,"Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks,"Industrial Electronics and Applications Vol:2, Issue.May 2006,pp.1-4.

[29] Manjeshwar,A. Agrawal,"TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks,"in Parallel and Distributed Processing Symposium,IEEE Proceedings 15th International,Aug 2008.

[30] Giannoulis S., Antonopoulos C., Topalis E., Koubias S. "ZRP versus DSR and TORA:A comprehensive survey on ZRP performance", Emerging Technologies and FactoryAutomation, ETFA. 10th IEEE conference, 2005.

[31] S.A. Notani, “Performance Simulation of Multihop Routing Algorithms for Ad-Hoc Wireless Sensor Networks Using TOSSIM”, In proceeding in 10th International Conference on Advanced Communication Technology, Vol. 1, pp. 508-513, Feb. 2008.

[32] Tao Yang, et al. “Performance Behavior of AODV, DSR and DSDV Protocols for Different Radio Models in Ad-Hoc Sensor Networks”, In Proceeding International Conference on Parallel Processing Workshops, Sept. 2007.

[33] M. Garcia,H. Coll,D. bri,"Using MANET Protocol in Wireless Sensor and Actor Networks,"in the second International Conference on Sensor Technologies and Applications,IEEE Computer Society,Aug.2008,pp.154-159.

[34] N. Thepvilojanapong,Y. Tobe,K. Sezaki,"On the Construction of Efficient Data Gathering Tree in Wireless Sensor Networks,"IEEE International Symposium IEEE International Symposium Vol:1,Issue:May 2005,pp.648-651.

[35] S. Corson and J. Macker, “Routing Protocol Performance Issues and Evaluation Considerations,” Naval Research Laboratory, Jan.1999.

[36] S. Vijayanand, R.M. suresh, “AN OVERLOOK ON ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS,” *IET-UK International Conference on Information and Communication Technology in Electrical Sciences*, Dr. M.G.R. University, Chennai, Tamil Nadu, India, 2007, pp.557-998.

[37] N. Thepvilojanapong,Y. Tobe,K. Sezaki,"A Scalable Approach to Collect Data in Wireless Sensor Networks,"IEICE Transactions on Communications,oct.2004,pp.890-902.

[38] J. L. Hill, “System Architecture for Wireless Sensor Networks,” PhD dissertation, UNIVERISY OF CALIFORNIA, BERKELEY, spring 2003.

[39] C. B. Seaman, “Qualitative Methods in Empirical Studies of Software Engineering”,IEEE Transactions on Software Engineering, IEEE, vol.25, no.4, 1999, pp.557-572.

[40] T.Larsson, N. Hedman.”Routing protocol in wireless AD-Hoc networks a simulation study,” M.A. thesis. Lulea University, 2007.

[41] K. sanzgiri, et.al “A Secure Routing Protocol for Ad Hoc Networks,” *In Proceedings of the 10 th IEEE International Conference on Network Protocols* .2002.

[42] Opnet Technologies, Inc. “Opnet Simulator,” Internet: www.opnet.com, April 1, 2009 [May. 5, 2009].

[43] Z. Ren and Y. zhou, “An Adaptive Multi-Channel OLSR Routing Protocol Based on Topology Maintenance,” in *Proceedings of the IEEE International Conference on Mechatronics & Automation Niagara Falls,* Canada, July 2005.

[44] C.E. Perkins, E.M. Royer. "Adhoc OnDemand Distance Vector Routing," Sun Microsystems Laboratories Advanced Development Group Menlo Park.

[45] M.S.Corson. et.al, An Internet MANET Encapsulation Protocol (IMEP) Specification. Internet-Draft, draft-ietf-manetimep-spec-00.txt, November 1997. Work in progress.

[46] G. Bellinger. "Modeling & Simulation," Internet: http://www.systems-thinking.org/modsim/modsim.htm, May 5, 2009 [May.12, 2009]

[47] R. Thorulp, "Mobile Ad Hoc Networks and Routing Protocols," *Implementing and Evaluating the DYMO Routing Protocol, Master's Thesis at the University of AARHUS*, pp. 7- 20, 2007.

[48] K. Romer and F. Mattern. "The design of space wireless sensor network," in IEEE Wireless Communications, Dec. 2004.