

ANALYSIS OF ROUND TRIP DELAY AND PATH, AND RFTM ROUTING PROTOCOL IN WIRELESS SENSOR NETWORK

Thesis submitted in fulfillment of the requirements for the Degree of

MASTERS OF TECHNOLOGY IN ELECTRONICS & COMMUNICATION ENGINEERING

Under the Supervision of

Dr. Rajiv Kumar

By

POONAM KOUNDAL

Enrollment No. 142011



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
WAKNAGHAT, SOLAN - 173234, INDIA

May-2016

ABSTRACT

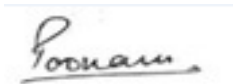
In the recent years, wireless sensor networks (WSN) have various critical applications such as earth quake monitoring, military etc. In case of WSN, a sufficiently large number of sensor nodes are deployed over the wireless sensing area that may suffers a damage/failure due to various reasons like environmental factors, enemy attacks, low battery power, software failure, hardware failure, malfunctioning, energy dissipation and so on. The main goal of the WSN is to collect data from its environment of deployment and then send it to a sink node.

Wireless Sensor Networks provides Quality of Service (QoS) in real time application. The QoS of such Wireless Sensor Networks is mainly affected by the failure of sensor nodes. In order to maintain the better quality of service of this network detection of failure node is essential. In the proposed work, the faulty sensor node is detected by measuring Round Trip Delay (RTD) time of discrete Round Trip Path. Then, RTD is compares with a threshold value to identify the failure node or faulty node. Greater than threshold value or infinity value of RTD is considered as a faulty or failure node.

Several routing schemes have been designed in the recent years for wireless sensor networks (WSN). This protocol improves the reliability of data routing in WSN networks. In future WSN networks are expected to carry different traffic such as voice and video as well as data to serve both real and non-real time applications. Therefore, the reliability and quality of the data transmitted to support diverse applications is very important. In this paper, we proposed a new on demand routing protocol i.e. Reliable Fault-Tolerant Multipath (RFTM) routing protocol. RFTM is a multi-objective routing protocol that meets diverse application requirements. Proposed protocol improves both reliability and link quality to determine the number of desired multiple disjoint paths between the sink and source nodes. RFTM routing protocol provides the fault-tolerance and achieves the desired.

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the M-Tech thesis entitled “**Analysis of round trip delay and path, and RFTM routing protocol in Wireless Sensor Network**” submitted at **Jaypee University of Information Technology, Wagnaghat India**, is an authentic record of my work carried out under the supervision of **Dr. Rajiv Kumar**. I have not submitted this work elsewhere for any other degree or diploma.



Signature of the Scholar

Poonam Koundal

Department of Electronics and Communication Engineering

Jaypee University of Information Technology, Wagnaghat, India.

Date: 25-05-2016

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M-Tech. thesis entitled “**Analysis of round trip delay and path, and RFTM routing protocol in Wireless Sensor Network**”, submitted by **Poonam Koundal** at **Jaypee University of Information Technology, Wagnaghat, India**, is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.



Signature of Supervisor

Name: Dr. Rajiv Kumar

Affiliation: Assistant Professor

Date: 25-05-2016

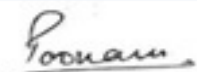
ACKNOWLEDGEMENT

Acknowledgement is not only a ritual, but also an expression of ineptness to all those who have helped in completion process of the project. One of the most pleasant aspects is collecting the necessary and vital information and compiling it afterwards. It is the opportunity to think a contribution towards it.

First of all, I am thankful to our Department where I got the Golden opportunity to undertake this project. I am extremely grateful to my supervisor Dr. Rajiv Kumar, Assistant Professor (Sr. Grade), Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Solan, who helped a lot in completion of this project.

Date: 25-05-2016

(Signature of student)



LIST OF ACRONYMS & ABBREVIATIONS

DR	Desired Reliable
EL	Energy Level
HC	Hop Count
RFTM	Reliable Fault Tolerant Multipath
RREQ	Route Request
RRP	Route Reply
RTD	Round Trip Delay
RTP	Round Trip Path
RTT	Round Trip Time
WSN	Wireless Sensor Network
EZW	Embedded Zero-tree Wavelet
FFT	Fast Fourier Transform
HH	High-High Band of DWT

LIST OF FIGURES

Figure Number	Name of Figure	Page Number
1.1	Wireless Sensor network	1
1.2	Sensor Node Hardware Components	3
3.1	Circular Topology in WSN with Six Sensor node	28
3.2	Illustration of Six Linear RTPs	30
3.3	Illustration of Two Discrete RTPs	31
3.4	Linear and Discrete RTPs Formed for Different Values Of Sensor Nodes in WSN	33
4.1	RREQ Message Format	40
4.2	Route Reply Message	40
4.3	Average Delay Ratio	42
4.4	Number of Paths Discovered	43
4.5	Energy Consumption	44

LIST OF TABLES

Table Number	Name of Table	Page Number
3.1	RTPs Comparison for Maximum, Linear and Discrete for Various Sensor Nodes in WSN	33
3.2	Analysis time of Discrete RTPs with Variable Number of Sensor Nodes for WSN with 100 Sensor Nodes	34

CONTENTS

ABSTRACT.....	i
DECLARATION BY THE SCHOLAR.....	ii
SUPERVISOR’S CERTIFICATE	iii
ACKNOWLEDGEMENT.....	iv
LISO OF ACRONYMS & ABBREVIATIONS.....	v
LIST OF FIGURES.....	vi
LIST OF TABLES	vii
CHAPTER 1	
INTRODUCTION.....	Error! Bookmark not defined.
1.1 INTRODUCTION WIRELESS SENSOR NETWORK.... Error! Bookmark not defined.	
1.2 CLASSIFICATIONS OF WIRELESS SENSOR NETWORK Error! Bookmark not defined.	
defined.	
1.2.1 STATIC AND MOBILE NETWORK.....	4
1.2.2 DETERMINISTIC AND NON-DETERMINISTIC NETWORK.....	4
1.2.3 STATIC-SINK AND MOBILE-SINK NETWORK	4
1.2.4 SINGLE-SINK AND MULTI-SINK NETWORK.....	5
1.2.5 SINGLE-HOP AND MULTI-HOP NETWORK	5
1.2.6 SELF-RECONFIGURABLE AND NON-SELF-RECONFIGURABLE.....	5
1.2.7 HOMOGENEOUS AND HETEROGENEOUS NETWORK.....	6
1.3 FAILURES IN WIRELESS SENSOR NETWORKS.....	6
1.4 ROUTING CHALLANGES.....	7
1.4.1 NODE DEPLOYMENT	7
1.4.2 ENERGY CONSUMPTION	7
1.4.3 DATA REPORTING MODEL.....	7

1.4.4 NODE/ LINK HETROGENITY.....	7
1.4.5 SCALABILITY	8
1.4.6 NETWORK DYNAMIC	8
1.4.7 FAULT TOLERANCE.....	8
1.4.8 DATA AGGREGATION	8
1.4.9 QUALITY OF SERVICE.....	8
1.5 APPLICATIONS OF WSN.....	9
1.5.1 MILITARY APPLICATIONS.....	9
1.5.2 ENVIRONMENTAL APPLICATIONS	9
1.5.3 HEALTH APPLICATIONS	9
1.5.4 HOME APPLICATIONS	9
1.5.5 COMMERCIAL APPLICATIONS	9
1.6 ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORK.....	10
1.6.1 SINGLE PATH ROUTING PROTOCOLS.....	11
1.6.2 MULTIPATH ROUTING	11
1.6.3 BENEFITS OF MULTIPATH ROUTING.....	12
1.7 BASIC PRINCIPLES IN DESIGNING MULTIPATH ROUTING PROTOCOL	12
1.8 PROBLEM FORMULATION.....	13
1.9 ORGANIZATION OF THESIS.....	14
 CHAPTER 2	
LITERATURE SURVEY	13
2.1 LITERATURE SURVEY ON DETECTION ANALYSIS USING RTD and RTP IN WSNs	15
2.2 LITERATURE SURVEY ON RFTM ROUTING PROTOCOL IN WSNs.....	17
2.2.1 DIRECTED DIFFUSION.....	17
2.2.2 BRAIDED MULTIPATH ROUTING PROTOCOL.....	19

2.2.3 INFRASTRUCTURE BASED MULTIPATH ROUTING PROTOCOLS.....	19
2.2.4 NON-INFRASTRUCTURE BASED MULTIPATH ROUTING PROTOCOLS.....	20
2.2.5 CODING BASED MULTIPATH ROUTING PROTOCOL.....	20

CHAPTER 3

DETECTION ANALYSIS USING ROUND TRIP DELAY AND PATH IN WIRELESS SENSOR NETWORK..... 23

3.1 OVERVIEW	23
3.2 ROUND TRIP DELAY AND ROUND TRIP PATH.....	24
3.3 OBJECTIVE OF THE WORK.....	26
3.4 RELATED WORK	26
3.5 PROBLEM FORMULATION.....	27
3.6 PROPOSED WORK.....	28
3.6.1 RTD TIME ESTIMATION	28
3.6.2 EVALUATION OF ROUND TRIP PATHS	29
3.7 ROUND TRIP DELAY AND PATH ANALYSIS.....	29
3.7.1 COMPUTATION OF ROUND TRIP PATHS.....	29
3.8 RESULT ANALYSIS.....	32
3.8.1 COMPUTATION OF MAXIMUM,LINER& DISCRETE METHODS IN WSNs..	32
3.8.2 GENERALIZED RTD MODEL.....	34
3.8.3 ALGORITHM FOR FAULTY SENSOR NODE DETECTION	35

CHAPTER 4

RELIABLE FAULT TOLERANT MULTIPATH ROUTING SCHEME FOR WSN..... 38

4.1 INTRODUCTION.....	38
------------------------------	-----------

4.2 PROPOSED RFTM ROUTING PROTOCOL IN OVERVIEW AND RELATED WORK.....	39
4.2.1 CONTROL PACKETS FORMAT	40
4.2.2 PHASES IN RFTM ROUTIN PROTOCOL	41
4.3 SIMULATION AND EVALUATION.....	42
4.3.1 DATA DELIVERY RATIO	42
4.3.2 NUMBER OF PATHS DISCOVERED	43
4.3.3 ENERGY CONSUMPTION	43
CHAPTER 5	
CONCLUSION.....	45

CHAPTER 1

INTRODUCTION

1.1 Introduction to WSN:

Wireless Sensor Network (WSN) is a wireless network, which consists of thousands of sensor nodes. These sensor nodes are massive, small and of low cost deployed in a sensing area to monitor the status of military applications, environment etc. The target is to sense, collect and process the information about objects in the coverage region, and then send it to the observer for processing and analyzing the information. The sensor node in WSNs can become faulty due to various reasons such as environmental factors, enemy attacks, low battery power, Software failure, and Hardware failure. Better quality of service (QoS) in WSNs is achieved by discarding the data from such faulty sensor nodes. There must be efficient and accurate detection of faulty sensor nodes in WSNs. The main purpose of a wireless sensor network is to monitor the physical environment, and provide the information about that environment in an appropriate fashion to observer for different applications.

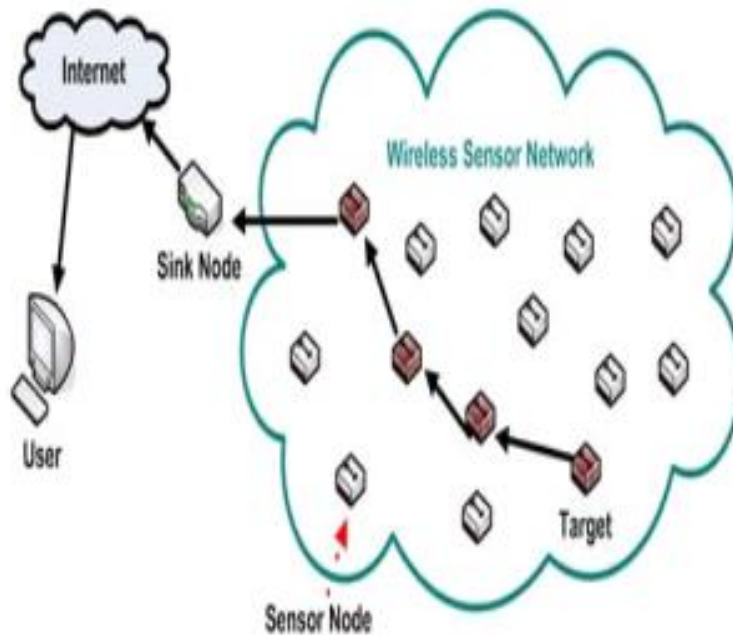


Figure 1.1: Wireless Sensor Network [9]

Typically a WSN consists of various sensor nodes, base station and gateway. All the sensor devices can send the data to base station through gateway device. Sensor devices sense the objects from the environment and pass the signal to the base station. Wireless sensor node is designed in a region where it is meant to collect data from environment through its sensor nodes. Sensor node is also known as a 'mote', is a node in a wireless sensor network that is capable of performing some processing such as sensing information and communicating with neighbor nodes in the network system. Sensor node transmits the data from one node to another node and finally sends to a base station where the data is stored. After this data is processed and displayed in the monitoring area. Wireless sensor networks (WSNs) have the potential applications like environmental monitoring, scientific data collection, medical, military operations and home security.

It is necessary and important to study the method of fault node detection in WSNs for the following various reasons:

- Sensor nodes are often deployed in uncontrollable and hostile environments. Therefore. Faults in sensor nodes can occur more easily as compare to other systems.
- It is so difficult and not practical to examine the functionality of sensor nodes.
- WSNs are deployed in some occasion like monitoring of nuclear reactor where high security is most required. Fault node detection in such specified application of great importance.
- Correct information cannot receive by the controller center because faulty nodes would produce incorrect data.
- Sensor nodes are usually battery powered and limited energy, so it is common for faults to occur due to the battery depletion.

Sensor nodes used in WSN can be divided in two types: normal and faulty sensor node. Faulty nodes can be divided further in two types: “permanent” or “static”. Permanent fault means node will remain faulty until they are replaced. Static means new faults will not generated during fault detection. These faults may be hard or soft. Hard fault is when a sensor node cannot communicate with other nodes because of the failure of a certain module. And Soft fault means the failed nodes can continue to work and communicate with other nodes, but the data sensed or

transmitted is not correct. Sensor nodes used in WSN can be divided in two types: normal and faulty sensor node. Faulty nodes can be divided further in two types: “permanent” or “static”. Permanent fault means node will remain faulty until they are replaced. Static means new faults will not generated during fault detection. These faults may be hard or soft. Hard fault is when a sensor node cannot communicate with other nodes because of the failure of a certain module. And Soft fault means the failed nodes can continue to work and communicate with other nodes, but the data sensed or transmitted is not correct.

The basic components of a node are explained below:

- **Sensor and actuator** - an interface to the physical world designed to sense the environmental parameters. Devices that can observe or control physical parameters of the environment.
- **Controller** – used is to control different modes of operation for processing of data.
- **Memory** - stores programming data and intermediate data.
- **Communication device** - a device for sending and receiving data over a wireless channel.
- **Power Supply**- supply of energy. Usually no tethered power supply is available, some forms of batteries are necessary to provide energy. In some cases, some form of recharging by obtaining energy from the environment is available as well (e.g. solar cells).

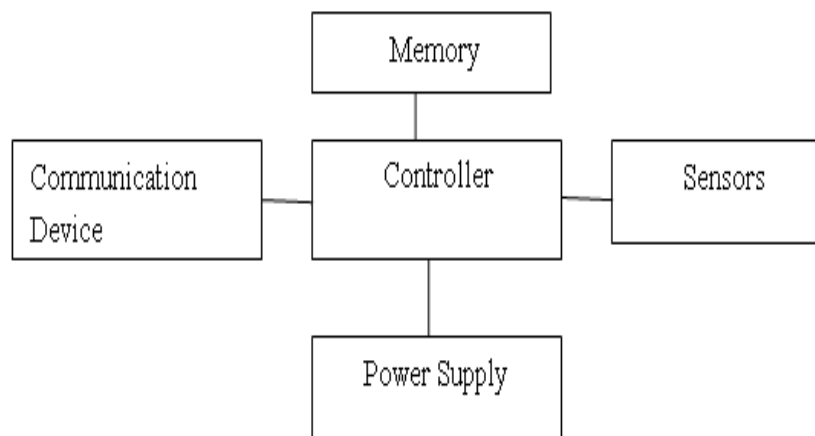


Figure 1.2: Sensor node hardware components

1.2 Classifications of Wireless Sensor Networks

Wireless Sensor Networks are application specific. A WSN network is usually deployed for a specific application and has some different characteristics. There are different categories of WSN according to different criteria. These are given below:

1.2.1 Static and Mobile Network

A sensor network can be static or mobile due to their mobility. In a static sensor network, all sensor nodes are static without movement. It is the case for many applications. However, some sensor applications require mobile nodes to fulfill sensing task. Static sensor network's design is simpler to control and easier to implement. In other hand, the design of mobile sensor networks must consider the mobility effect, which increases the complexity of implementation. Thus static sensor network is less complex as compare to mobile sensor network.

1.2.2 Deterministic and Non-deterministic Network

A sensor network can be deterministic or non-deterministic according to the deployment of sensor are predefined and are fixed once deployed. This type of network can only be used in some limited applications, where the preplanned or predefined deployment is possible. However, it is difficult to deploy sensor nodes in a preplanned manner because of the harsh or hostile environments. Instead of this sensor nodes are randomly deployed without preplanning and engineering. Hence, nondeterministic networks are more scalable and flexible, but require higher control complexity.

1.2.3 Static-Sink and Mobile-Sink Network

A data sink node in a sensor network can be static or mobile. In a static-sink network, the sink node is static with a fixed position located close to or inside a sensing area. All sensor nodes send their sensed data to the sink node. A static sink node makes the network simpler to control, but it would cause the hotspot effect [26]. The size of data traffic (that sensor nodes are required to forward) increases when distance to the data sink becomes smaller. Hence, sensor nodes closest to the data sink tend to fail early, thus resulting in network partition and even disrupting normal network operation. In a mobile - sink network, the sink nodes moves around in the sensing region to collect data from sensor nodes, which can balance the traffic load of sensor nodes and alleviate the hotspot effect in the network. Hence, Mobile-sink is better than Static-sink network because of load balancing.

1.2.4 Single - Sink and Multi-sink Network

There can be single sink or multiple sinks in a sensor network. In a single - sink network, there is only one sink node located close to or inside the sensing area. In this network, all sensor nodes send their sensed data to this sink node. In a multi-sink network, there may be several sink nodes located in different positions close to or inside the sensing region. In this network, sensor nodes can send their data to the closest sink, which can effectively balance the traffic load of sensor nodes and alleviate the hotspot effect in the network.

1.2.5 Single-Hop and Multi-hop Network

There can be single hop or multiple hops in the sensor network. The network with single hop from source node to sink is called Single-hop network. And, the network with multiple numbers of hops between source and sink is called multi-hop network. In a single-hop network, all sensor nodes transmit their sensed data directly to the sink node, which makes network simpler to implement. But, this requires long-range wireless communication, which makes network costly in terms of both energy consumption and hardware implementation. The furthest nodes from the data sink will die much more quickly than those close to the sink nodes. Also, with the increase of network size, the overall traffic load in the network may also increase, which would cause more collisions, and thus increase energy consumption and delivery latency. In other hand, in a multi-hop network, sensor nodes transmit their sensed data to the sink node using short - range wireless communication via one or more intermediate nodes in the path. Each intermediate node must perform routing process and forward the data packet along a multi-hop path. Moreover, data aggregation can be performed at an intermediate node to eliminate data redundancy, thus it can reduce the traffic load in the network and thus improve the energy efficiency of the network. In general, network architecture of single-hop network is simple and thus is easier to control. Thus, single-hop network is suitable for applications in small sensing areas with sparsely deployed sensor nodes. Whereas, a multi-hop networks have a wider range of applications at the cost of higher control complexity.

1.2.6 Self-Reconfigurable and Non - Self-Configurable Network.

On the basis of the configurability of sensor nodes, a sensor network can be self-configurable or non - self-configurable network. Non - self-configurable network is defined as the network in which the sensor nodes have no ability to organize themselves into a network. Instead, sensor nodes have to rely on a central controller to control each sensor node and collect all data from

them. Hence, non-self-configurable networks are only suitable for small - scale networks. In most cases of sensor networks, however, sensor nodes are able to autonomously organize and maintain their connectivity by themselves and collaboratively accomplish a sensing task. A network with such self - configurability is called self-configurable network and this type of network is suitable for large - scale networks to perform complicated sensing tasks.

1.2.7 Homogeneous and Heterogeneous Network

According to whether sensor nodes have the same/ different capabilities, a sensor network can be defined as a homogeneous or heterogeneous network [27]. In a homogeneous network, all sensor nodes have the same capabilities in terms of storage, energy and computation. Whereas, heterogeneous network has some sophisticated sensor nodes that are equipped with more processing and communicating capabilities than other normal sensor nodes. In this case, the sensor network can assign more processing and communication tasks to those sophisticated nodes in order to improve its energy efficiency and thus increase the lifetime.

1.3 Failures in Wireless sensor networks

A fault is defined as the failure of a component of a system. The occurrence of one or many faults may lead to system failure. If failure occurs, the system cannot perform their functions. For example, a link or node failure is called as fault. Multiple link and node failures may lead to failure of network services, which in turn may translate to failure of the whole network. A fault is defined as any kind of defect that leads to an error. An error corresponds to an incorrect system state. Such a state may cause of failure. A failure is the observable of an error, which occurs when the System deviates from its specification and cannot perform its functionality.

The error is defined as the state of the service after trying to read the sensor data and the failure occurs when the application does not send the data within the specified time interval. To provide resilience in faulty situations two main tasks must be performed that are: fault detection and fault recovery.

Fault detection: In this step, check the ability to recognize the functional ability of a device. In other words, to check that is there any faulty node in the system or not. The existence of faulty node in WSN will cause a degradation of the network quality of service. It is desirable to identify, locate and elimination of faulty nodes from network. Otherwise it provides incorrect diagnosis.

Fault Recovery: After the system has detected a fault, the next step is to prevent or recover from it.

1.4 Routing Challenges

Some routing challenges and design issues that affect the routing process in WSNs. These are:

1.4.1 Node Deployment

The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

1.4.2 Energy consumption

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. Life of node depends on battery. Node loses its energy during transmission as well as during reception time.

1.4.3 Data reporting model

Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting can be categorized as either time-driven (continuous), event-driven, query-driven, and hybrid. The time-driven delivery model is suitable for applications that require the monitoring after constant periodic time intervals. In event-driven and query-driven models, sensor nodes react immediately to sudden and drastic changes. Hybrid model is the combination of the previous models.

1.4.4 Node/Link Heterogeneity

In many studies, all sensor nodes were assumed to be homogeneous, i.e. having equal capacity in terms of computation, communication, and power. The existence of heterogeneous set of sensors raises many technical issues related to data routing. For example, some applications might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures, and capturing the image or video tracking of moving objects. These special sensors can be either deployed independently or the different functionalities can be included in the same sensor nodes. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of

service constraints, and can follow multiple data reporting models. For example, hierarchical protocols designate a cluster-head node different from the normal sensors. These cluster heads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory. Hence, the burden of transmission to the BS is handled by the set of cluster-heads.

1.4.5 Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment.

1.4.6 Network Dynamics:

Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc.

1.4.7 Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. Another link is provided to complete the communication path.

1.4.8 Data Aggregation:

Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing can be used for data aggregation.

1.4.9 Quality of Service:

In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained application. Qos depends on the network life time.

In sensor networks, minimizing energy consumption is considered as a major performance criterion to provide maximum network lifetime. While considering energy conservation, routing protocols should also be designed to achieve fault tolerance in communications]. First, it is more probable to face failures in communication nodes in WSNs

than classical networks, as nodes are embedded in unattended places and they use limited power supply. So, the network should not be affected from node's failures and be in an adaptive structure to maintain routing operation.

1.5 Applications of WSNs

1.5.1 Military Application:

- a.) Monitoring inimical forces
- b.) Monitoring friendly forces and equipment
- c.) Military-theater or battlefield surveillance
- d.) Targeting
- e.) Battle damage assessment
- f.) Nuclear, biological, and chemical attack detection

1.5.2 Environmental applications

- a.) Forest fire detection
- b.) Flood detection
- c.) Precision agriculture

1.5.3 Health applications

- a.) Remote monitoring of physiological data
- b.) Tracking and monitoring doctors and patients inside a hospital
- c.) Drug administration
- d.) Elderly assistance

1.5.4 Home applications

- a.) Home automation
- b.) Instrumented environment
- c.) Automated meter reading.

1.5.5 Commercial applications

- a.) Environmental control in industrial and office buildings
- b.) Inventory control
- c.) Vehicle tracking and detection
- d.) Traffic flow surveillance.

1.6 Routing Protocols in Wireless Sensor Networks

Routing protocols for other wireless networks like mobile ad hoc networks cannot be directly applied to WSNs due to the various characteristics of WSNs, such as severe resource constraints and harsh environmental conditions in addition to the existing design challenges in WSNs like energy consumption, node deployment, node mobility and QoS requirements. In WSNs, careful management of resource is required, since each sensor node depends on energy for its activities; thus the failure node or link due to its limited battery lifetime, communication error hardware breakdown, or malicious attack can affect the whole network.

In general, routing protocols proposed for WSNs can be classified into three categories depending on the methods used for finding the path, such as; proactive routing protocol in which all paths are computed and maintained in advance and stored in the routing table (nodes continuously search for routing information within the network, so that when a route is needed it is already available), reactive routing protocol where all paths are created on demand when needed, and hybrid routing protocol which is a mix of the both proactive and reactive routing protocols.

However, in QoS-based routing protocols, the network has to balance its traffic while improving the network performance. Moreover, in many applications, to extend the lifetime of network is considered more important than the quality of data, and this is related to the reduction of the energy dissipation of the sensor nodes. Thus, an energy-aware routing protocol is most important for these networks. For real time applications, data should be delivered in time otherwise data is considered useless. So in case of real-time applications, the network requires a timeliness-aware routing protocol. However, in many other applications, a reliable routing protocol is used since the reliability of data transmission in the network is considered as an important issue. Thus, as a result, the design of routing protocols in WSNs is influenced by many challenging factors. All these factors must be overcome before the efficient communication can be achieved in WSNs. Therefore, many new routing algorithms have been proposed for the problem of routing data in wireless sensor networks. These routing protocols have considered the various characteristics of sensor nodes along with the different application requirements. Routing protocol plays an important role in wireless sensor networks. Routing protocols may be classified as: single path routing protocol and multi-path routing protocol.

1.6.1 Single path Routing Protocol

Single path routing protocol is simple and scalable. Here, the source node selects a single path which can satisfy the application requirements to transmit data towards the destination. Most of the existing routing protocols in WSNs are designed based on the single path routing strategy to deliver data to the destination since it is simple and consumes less energy than multipath routing protocols. This routing protocol is simple because the path between source and destination node can be established in a specific period of time. Also this protocol is scalable because, even if the network changes from ten nodes to thousand nodes, the complexity and the approach to discover the path remains same. The main disadvantage of single path routing is: in this routing, it is easy for the sensor node to select the intermediate data routing nodes from the same part of the network over and over again. Due to this there is depletion of power of those sensor nodes and network partition, which shortens the lifetime of the WSNs [28]. Another disadvantage is that, single path routing protocols are incapable of load balancing traffic in the network. Therefore, this routing protocol cannot be considered effective techniques in WSNs due to the resource constraints and the unreliability of wireless links.

1.6.2 Multipath Routing Protocol

Multipath routing is the most popular technique to improve data transmission reliability, support congestion control and QoS as well as provide fault tolerance in the network. It is an alternative routing technique, in which multiple paths are used to deliver data from source to destination. Because of the nature of multipath routing technique that uses redundant paths, multipath routing can largely address the reliability, load balancing and security issues of single path routing protocols. Thus, multipath routing plays an important role in WSNs. Multipath routing can be effectively used for maximum utilization of network resources. In this technique, node has a choice of next hop for the same destination [28].

There are two important strategies for allocating traffic over available path. First is to distribute data among multiple paths instead of routing all the data along a single path. Second is to forward data using only the path with the best metric and keep other discovered paths as backups that can be used in case of traffic congestion or blocking. Thus, multipath routing is an alternative to single shortest path routing to distribute load and make less congestion in the network. On the basis of the protocol feature and its specification existing multipath routing techniques can be classified into three categories [28]:

A) Infrastructure Based:- construct and maintain specific infrastructure by considering location and resource capabilities.

B) Non-Infrastructure based:- Protocols which do not build any specific infrastructure and decide the next hop on the basis of its local knowledge are called non-infrastructure based routing protocol.

C) Coding Based:- Use variant kinds of coding schemes to fragment the data packet at the source node and then send the chunks through discovered multiple paths.

1.6.3 Benefits of Multipath Routing

Multipath routing has various advantages:

1) Fault Tolerance

Due to presence of multiple paths traffic can move to an alternate path on the occurrence of congestion. Due to this there is less delay and packet loss.

2) Increased Bandwidth

By using multiple path technique, an application can access more bandwidth by using multiple paths simultaneously.

3) Data Reliability

Data reliability is the ratio of the amount of data received by the destination node to the amount of data sent by the sensor node. If there is multiple paths exist, traffic can switch quickly to an alternate path when a link or router fails. In other words, using multipath routing technique increases data reliability by sending the data along multiple paths.

4) Load Balancing

Load balancing can be improved by using multiple paths simultaneously. Due to multiple paths, network resources can be more used by distribution of traffic among several paths. This is reverse to single path routing where one path is completely busy and others are under loaded. So by using multipath routing, load balancing can be achieved.

1.7 Basic Principles in Designing Multipath Routing Protocols

There are various components in multipath routing protocol to construct multiple paths and distribute the traffic over the discovered paths. The performance of the multipath routing protocols is highly dependent on the ability of the proposed protocol to construct high quality,

reliable paths. These components are path discovery, path selection & traffic distribution and path maintenance.

- **Path Discovery:**

The sensor nodes in the WSN act as data sender as well as data router. Once the data packet has arrived at an intermediate routing node, it must select the next node having the capability of passing the data packet in the direction of the sink. The selection of the next node is based on the information including signal strength and residual energy. Along with the information, the source node has to verify that the selected node is not a malicious node, which causes extra message overhead and transmission delay

- **Path Selection and Traffic Distribution:**

After the path construction there are many factors which can be used to select a path from multiple paths to transmit data from source to destination. Some routing protocols use the best path to transmit data and keep the others for backup, where as some may use the paths concurrently to transfer the data through multiple paths for reliability or even traffic distribution. Path length, delay, packet loss rate and residual battery level are some of the basic components of routing cost function. Once the set of paths is selected the routing protocol should determine how to distribute the network traffic so that the resource utilization is maximized, improve performance demands such as throughput, data delivery ratio, delay, life time, reliability etc.

- **Path Maintenance:**

If the sensor node moves outside to the reach of its neighbor then path from source to destination is break. If the path is broken, then the source node has to choose another optimal path. In some cases only few optimal paths are used from several discovered multiple paths. In such a scenario some unnecessary messages are transmitted to unused paths in order to keep them alive. This may consume more energy.

1.8 Problem Formulation:

Firstly, objective of this work is to detect the faulty or failure sensor nodes using round trip delay time and round trip paths in the wireless sensor network. The main target of sensor network is to cooperatively sense, collect, and process the information about the objects in the coverage region, and then sends it to the observer for processing and analyzing. Round trip delay (RTD) time technique is a simple way to obtain the information about the sensor nodes used in wireless

sensor network. The proposed method will detect the failure or fault sensor node for symmetrical network conditions. In this way it helps to detect failed or malfunctioning sensor, which can be used to get correct data in WSN or the exact sensor node can be repaired or working status of the WSN can be checked. The round trip delay can be range from few milliseconds to several seconds between sensor nodes separated by a distance. The time required for detection is in the range of seconds; hence data loss can be avoided.

Second, our objective is to propose a Reliable Fault tolerant Multipath (RFTM) Routing scheme to provide reliable and efficient data delivery from the source to the sink in the wireless sensor network. RFTM is a multi-objective routing protocol that meets diverse application requirements. Proposed protocol improves both reliability and link quality to determine the number of desired multiple disjoint paths between the sink and source nodes. RFTM routing protocol provides the fault- tolerance and achieves the desired.

1.9 Organization of Thesis

Chapter 2 provides the Literature survey of “Detection Analysis Using Round Trip Delay and Path” and “Reliable Fault Tolerant Multipath Routing Scheme in Wireless Sensor Networks”. Chapter 3 provides the details and simulation results of the proposed Fault Detection Using Round Trip Delay and Path in Wireless Sensor network. Chapter 4 provides the detail and simulation results of our proposed Reliable Fault Tolerant Multipath Routing Scheme in Wireless Sensor Networks. Chapter 5 provides the conclusion.

CHAPTER 2

LITERATURE SURVRY

2.1 Literature Survey on Detection Analysis using Round Trip Time and Path in WSNs

Sensor nodes in the WSN are prone to failure; these failure nodes will degrade the QoS of the whole network. To improve the QoS of the network, need to have complete knowledge about detecting the node fault methods due to the following reasons [7], [8]. More importance should be given to some high security applications like identifying fault node, monitoring of nuclear reactor. The sensor node fails because of deployment of low-cost sensors in uncontrollable environment due to this reason failure of nodes occurs more frequently. Energy depletion is another major problem faced in sensor nodes since they are battery powered with limited energy that causes failure of node. Due to dynamic changes in the networks failure of links will cause sensor node to fail permanently or temporarily. Due to occurrence of Congestion in sensor network due to overload and traffic that results in packet loss and node failure. Hardware failure occurs during fabrication process, due to this sensor node becomes faulty. Sensor nodes find application in surveillance, medical, environment monitoring, vehicle tracking, and acoustic data gathering. For all applications accuracy of data is important to the whole system's performance, detecting nodes with faulty readings is an important issue in the network management. Failure of nodes cannot be examined manually to determine the proper functioning of nodes.

The fault node detection approaches are classified into two primary types: centralized and distributed approach. In centralized fault management approach, usually a geographical or logical centralized sensor node identifies faulty or misbehaving nodes in the whole network. This centralized node can be a base station, a central controller. This central node usually has unlimited resources and this node performs wide range of fault management tasks .A very common centralized fault management approach Sympathy is a debugging system and is used to identify and localize the cause of the failures or faults in wireless sensor network application. But, Sympathy algorithm does not provide automatic bug detection. It depends on historical data and metrics analysis in order to isolate the cause of the failure or faults in the network. Sympathy

algorithm may require nodes to exchange neighborhoods list, which is expensive in terms of energy. Also, Sympathy flooding algorithm means imprecise knowledge of global network states and may cause incorrect analysis. Centralized approach is suitable only for certain application. However, it has various limitations. This approach is not scalable and cannot be used for large networks. Also, due to centralized approach all the traffic is directed to and from the central point. Due to this communication overhead and quick energy depletion develops. The central point is a single point of data traffic concentration and potential failure. Moreover, if a network is partitioned, then nodes that are unable to reach the central server are left without any management functionality. Distributed approach is an efficient approach of deploying fault management. Each node controls a sub network and may communicate directly with other node to perform management functions. Distributed approach provides better reliability and energy efficiency and has lower communication cost than centralized management approach.

1. **L. B. Ruiz et al [10]** proposed failure detection scheme called MANNA using management architecture for WSNs. Faulty sensor nodes are able to detect from the above architecture. This approach is too expensive for WSNs. It requires an external manager to perform the centralized diagnosis and the communication between nodes.
2. **M. Lee and Y. Choi [11]** proposed the method to detect the failure in sensor nodes in WSNs. In this method faulty sensor nodes identified on the idea by comparisons between the surrounding nodes that is neighboring nodes and at the each node level dissemination of the decision made. The algorithm is simple while maintaining low false alarm rate it detects faulty sensor nodes with high accuracy for fault probabilities of wide range. In this method the algorithm fails to detect the malicious nodes.
3. **A. Akbari et Al [12]** proposed the method named cluster based recovery algorithm. Sensor node failures changes due to which energy-efficient and responsive to network topology. It is used to detect battery failure node and recovery the battery failure node. The disadvantage of the cluster based recovery algorithm that is while transferring the cluster head that results in heavy data loss.
4. **S. S. Ahuja et Al [13]** presented monitoring cycles (MCs) and monitoring path (MPs) for the detection of link failure in sensor node in WSNs. The limitation of the method three-

edge connectivity in the network, for each monitoring cycles and monitoring locations maintained a separate wavelength.

5. **Ravindra Navanath Duche et. al [1]** proposed the method to detect the faulty sensor node using discrete round trip delay and round trip path. In this method sensor nodes are arranged in circular topology that is in static and using this topology the packet is forwarded from source to destination by routing and Maximum round trip delay is calculated and considered as threshold value. To find the faulty sensor node the round trip delay of the round trip path should be greater than threshold value.

The proposed method of fault detection is based on RTD time measurement of RTPs in wireless sensor network. RTD times of discrete RTPs are compared with the threshold time to determine failed or malfunctioning sensor node in WSN. Generalized model to determine the fault detection analysis time for WSNs by using discrete RTPs is suggested. The process of detection of faulty nodes using RTD & RTP in wireless sensor network can be taken as two parts. In the first part we involves assumption that all the sensor nodes are working correctly and there is no faulty node present in the network and the threshold value is set by measuring RTD time of all the RTPs. However, in second part actual detection of faulty node is done by selecting discrete RTPs and comparing their RTD times with predefined threshold which is set in first part. Round-trip delay, also known as round-trip time, is the time required for a signal pulse or packet to travel from a specific source node through path consisting other nodes and back again. Prove this relationship the various other parameters affecting round trip delay time like speed, data transfer rate, number of sensor nodes in RTD path and other request handled by intermediate nodes are either made constant or disabled. The round trip delay time can range from few milliseconds under ideal conditions to several seconds under adverse conditions between sensor nodes separated by a large distance.

In the propose method, Symmetrical network conditions is used for deploy the sensor node. To detect failed or faulty sensor node, which can be used to get correct data in WSN or the exact sensor node can be repaired or working status of the WSN can be checked. The time required for this detection is in the range of seconds. Here, Data loss can be avoided and also analysis time to be reduced. Sensor node failure in WSNs causes the data loss and also affects the Quality of Service of the network. Fault sensor node detection technique is used to improve the performance

of Wireless sensor networks. The proposed method, the main problem in WSN is the limited battery power which has direct impact on the lifetime of the networks. Faulty nodes affect the QoS parameters such as delay, throughput in Wireless Sensor Networks. Probability of sensor node failure increases with increase in number of sensor nodes in the network. In the proposed method, faulty sensor node is detected by measuring the round trip delay (RTD) time in discrete round trip paths and comparing them with a threshold value. The discrete RTP reduces the number of RTP while compare to the Linear RTP. And, this will reduce the detection time.

2.2 Literature Survey on Reliable Fault Tolerant Multipath Routing scheme in WSNs

2.2.1 Directed Diffusion

Directed Diffusion (DD) is a query based multi-path routing protocol, in which the sink initializes the routing process. Directed diffusion is a classic data-centric routing protocol in Wireless Sensor Networks. In this directed diffusion routing protocol based WSNs, data generated by sensor nodes is named by attribute-value pairs. A destination node floods requests data by sending interests. The data that match the interests are then "drawn" down towards the destination. During the interest data flooding all the intermediate nodes store the interest data received from the neighbors for later use. As the interest data is received by the nodes, the receiver node creates a gradient towards the node from which the data has been received [13]. During this stage multiple paths can be discovered between source and destination. After this, when the source node finds an event matched with the existing data information in the interest table it forwards the data through all the constructed gradients. Based on the performance of the packet reception over each path the destination node selects a best path with minimum delay, the destination node reinforces the selected path by sending a low-rate reinforcement data towards the source node. Then the data is transmitted by source node through the selected path. If there is any failure or fault in the active path then the data can be forwarded through the other available paths providing fault tolerant routing.

In WSN network energy resources are limited, therefore energy saving becomes the most important concern in designing routing protocols. In directed diffusion routing there is neighbor

to neighbor communication in the network. In the directed diffusion, the paths are chosen empirically for minimum delay and maximum data received during a certain period of time. However, in this protocol the communication cost and energy consumption over the whole WSNs have not been paid enough attention. To overcome these kinds of issues, we propose a novel path reinforcement scheme.

2.2.2 Braided Multipath Routing Protocol

Braided Multipath Routing Protocol (BMRP) [14] was proposed to provide fault tolerant routing in wireless sensor networks through constructing several partially disjoint paths. This is similar to Directed Diffusion [13]. In this protocol partially disjoint paths are constructed by using two path reinforcement messages, i.e. primary path reinforcement message and alternative path reinforcement message. The path construction is initialized by the destination by sending a primary path reinforcement message towards its best next-hop neighbor towards the source node, and this process continues till the primary reinforcement message reaches the source node. The reinforcement message is also sent to the alternate path to the next best neighbors towards the source node which are not in the primary path constructing an alternative path along with the primary path. During this process an intermediate node which is not a member of the primary path will choose the best next-hop neighbor towards the sink, and this process continues till the message reaches a node along the primary path. Due to this process backup paths are constructed from all the intermediate nodes which are in the primary path. Whenever a primary path fails, the data can be forwarded through the alternate path.

2.2.3 Infrastructure Based Multipath Routing Protocols

The main concern with infrastructure based routing multipath routing protocols is to construct and maintain specific multipath infrastructure by considering location and resource capabilities. This routing protocol try to discover and maintain multiple paths between source to destination before data transmission, and all the data are transmitted through those discovered multiple paths. The most important feature of this routing protocol is the construction and maintenance of multiple paths from source to destination. The infrastructure provides the reliable and fast data transmission because each intermediate node has its next hop set up in advance. This infrastructure also provides the protocol reducing failure recovery time by using the alternative

paths, which are also discovered in advance. But, building an infrastructure is not enough to create an optimal multipath routing protocol. For achieving reliability, load balancing and security we use different protocols [28].

2.2.4 Non-Infrastructure Based Multipath Routing protocols

Non-Infrastructure multipath routing protocols do not construct any infrastructure in order to transmit the data from source to destination. The main difference between infrastructure based routing protocol and non-infrastructure based routing protocol is: the path is discovered prior to the data transmission in infrastructure based multipath routing protocol. On the other hand, in non-infrastructure based routing protocol, the path is discovered as the data packet moves forward. So, in non-infrastructure multipath routing, every intermediate node makes a decision on the basis of its local knowledge instead of pre-set next hop information, in order to forward the data packet. Because each node makes its own decision to forward the data packet, due to this reason it is possible that instead of sending the data packet towards the destination node, the packet could be sent away from the destination node. Thus, one of the major concerns of non-infrastructure multipath routing protocols is forwarding the data packet in the direction of the destination node [28]. The main advantages of non-infrastructure based routing multipath routing protocol are: firstly, there is no path maintenance required because as the data packet moves forwards the path is created by the intermediate nodes based on their local knowledge. Secondly, the randomized routing mechanism is used by the protocols to route the data, is energy-efficient and helps to obtain load balancing.

But, security, reliability and unnecessary redundancy in transmission are the major issues in both infrastructure and non-infrastructure based multipath routing protocols.

2.2.5 Coding Based Multipath Routing Protocols

Coding based multipath routing protocols use variant kinds of coding schemes in data packet transmission at the source node and then send to the destination through discovered multiple paths. In infrastructure based multipath routing protocols, path construction and maintenance are two major overheads. Data transmission, however, will be straight forward by following the established paths, although in order to achieve reliability the same data packet is also transmitted

through all discovered multiple paths. But, this is energy inefficient and not secure. Whereas, the non-infrastructure based multipath routing protocols have no path construction and maintenance overheads, but have the problem with secure data transmission and less likelihood of successful delivery ratio on the sufficient number of paths. Therefore both the above categories of multipath protocols have mainly two common problems that are: unnecessary redundancy in transmission and security. Coding techniques can be used to overcome these two problems in multipath routing. In coding based multipath routing protocols, if some intermediate data routing nodes get into malicious activity, they will not be able to eavesdrop the network because the data packets are travel in encoded form and can only be decoded at the destination node. Also, it saves a lot of energy by not sending the same copy of data using multiple paths [28].

Coding based multipath routing protocols uses an on-demand routing scheme in which path between source and destination is constructed only when it is required [29]. Thus, this approach helps to conserve energy by not constructing unnecessary paths. Here we proposed a Reliable Fault Tolerant multipath (RFTM) routing scheme which is a on demand routing protocol. RFTM routing Scheme is described briefly below:

- **Reliable Fault Tolerant Multipath Routing Scheme**

Reliable Fault Tolerant Multipath (RFTM) routing protocol is proposed which involves fault recovery process. In this protocol sensed data is transmitted through a shortest path. If there is faulty data occurs in the network, these are recovered very fast. The data is transmitted to base station with minimum delay and energy loss. This technique also controls the data traffic during transmission of data to the base station. In this paper our main purpose is to design a multi objective routing protocol MRFTM. In this protocol, sensor nodes just need to have information of its neighboring nodes not the whole path information. A multi-objective routing protocol MRFTM considers the link quality during data transmission to avoid poor link connectivity when choosing next nodes to route data. This protocol uses multipath routing to deliver data to sink node for desired reliability. The number of paths varies based on the level of reliability required. With the increasing level of reliability the number of paths also increases. When the required reliability is small then only one or few paths are required. The data packets are coded by source node using erasure code [5] and transmit each coded packet through one of the selected paths in

order to provide degree of fault tolerance to different levels of information based on the level of reliability required. The selection criteria of these multiple path depend on different application requirements.

This protocol is used to improve the reliability of data routing in wireless sensor networks. In future WSN networks are expected to carry different traffic such as voice and video as well as data to serve both real and non-real time applications. Therefore, the reliability and quality of the data transmitted to support diverse applications is very important. RFTM is a multi-objective routing protocol that meets diverse application requirements. The protocol improves both reliability and link quality to determine the number of desired multiple disjoint paths between the sink and source nodes. With the erasure coding the packets are encoded at source nodes and the sink node obtains the data packets by decoding. RFTM routing protocol provides the fault-tolerance and achieves the desired reliability that meets the network state and the different.

CHAPTER 3

DETECTION ANALYSIS USING ROUND TRIP DELAY AND PATH IN WIRELESS SENSOR NETWORK

3.1 Overview

Wireless sensor networks (WSNs) with thousand numbers of sensor nodes has potential applications in number of fields , like medical, surveillance, home security, military operations, environmental and industrial monitoring. Sensor nodes in WSNs are often deployed in uncontrollable and hostile environments. Therefore, faults in sensor nodes can occur more easily as compare to other systems. Because of the rapid growth in electronic fabrication technology, manufacturing of the sensor node at low cost with better accuracy and sensitivity is possible. Therefore, large numbers of sensor nodes can be deployed in the field to increase the quality of service (QoS) of the wireless sensor networks. As the numbers of sensor nodes increases, the probability of sensor node failures in such WSNs also increases. Due to such faulty sensor node data analysis will become incorrect or deviate from the mean value. Thus the quality of service (QoS) of WSNs will also decrease. The sensor node in the wireless sensor networks can become faulty due to various reasons such as battery failure, environmental effects, and hardware or software malfunctions. By discarding the data from such faulty sensor nodes in the analysis the quality of service (QoS) can be improve. This required the efficient and accurate detection of faulty sensor nodes in WSNs. Generalized method for the detection of fault node in WSNs by using discrete RTPs is proposed. Detection of fault node is based on inspecting the discrete RTPs for their round trip delay (RTD) time. This method will improve the lifetime as well as quality of service (QoS) of WSNs. Number of experiments are performed in hardware and software based on RTD time measurements. Results of hardware and software indicate that RTD time measurement results in both cases are validating the real time applicability of this method.

In the proposed method, the functionality of sensor nodes is detected by calculating the round trip delay (RTD) time of different round trip paths and then comparing the (RTD) time with the threshold value. Round trip delay (RTD) time measurement method is an easy way to obtain the

information regarding above issues in WSN. The method of fault detection is based on RTD time measurement of RTPs is used. In this method RTD times of discrete RTPs are compared with threshold time to determine failure sensor node. Here method is tested on 6, 30 sensor nodes. Round-trip delay (RTD), also called as round-trip time (RTT), is the time required for a signal or packet to travel from a specific source node through path consisting other nodes and back again to the source node. The round trip delay (RTD) time can range from a few milliseconds under ideal conditions between nearby spaced sensor nodes to several seconds under adverse conditions between sensor nodes separated by a large distance. Round trip delay (RTD) time of the RTP will be change due to the faulty sensor node.

In a network RTD time is mainly affected by the latency, which is the time between a request for data and the complete return of the data. The round trip delay (RTD) time depends on various factors [13]:

- Sensor node Data transfer rate
- Nature of transmission medium.
- The Physical distance between the sensor nodes.
- The Number of nodes in the RTD path.
- Other requests being handled by intermediate nodes.
- Intermediate nodes and source node functions speed
- Interference in the circuit.

3.2 Round Trip Delay (RTD) Time and Round Trip Path (RTP)

Round trip delay (RTD) is the time required for a signal to travel from a specific source node through a path consisting series of other nodes and back again.

Round trip path (RTP) in wireless sensor networks will be formed with at least three sensor nodes including the source node. The number of sensor nodes in the path can be increased to maximum as N-1. The range of sensor nodes in round trip path can be expressed as:

$$3 \leq m \leq (N-1)$$

Where, ‘N’ is the total number of sensor nodes present in WSN and ‘m’ is the number of sensor nodes present in the round trip path. The maximum number of RTPs (P_M) in WSN having N nodes can be calculated by using the given equation;

$$P_M = N(N - m)$$

The Round Trip delay time of the RTP will change due to faulty sensor node. The value of RTD time will be either infinite or higher than the threshold value. Faulty sensor node is detected by comparing the RTD time of the RTPs with the threshold value. The sensor node RTPs with infinite value of RTD time is detected as failure node. If this time is higher than the threshold value then this sensor node is detected as faulty/malfunctioning. The Detection time of faulty/failure sensor node depends upon the numbers of RTPs and RTD time. Therefore, RTD time measurement and evaluation of RTPs is must to minimize the detection time. Round-trip delay (RTD) also called as round-trip time (RTT). It is the time required for a signal to travel from a specific source node through a path consisting other nodes and back again. The round trip delay time for the path consisting three sensors i, j and k $\tau_{RTD} = \tau_1 + \tau_2 + \tau_3$ where, $\tau(i,j)$ is time delay between the sensor pair (i, j). RTD time is a function of various parameters of the wireless network and it can be expressed as RTD time= f(speed, distance, medium, noise, nodes in RTD path & request handled) = $T_s + T_d + T_m + T_n + m + T_{req}$. Thus round trip delay time is the summation of various time delays associated with the respective parameters of the WSN. This time can range from a few milliseconds to several seconds. Minimum three sensor nodes in RTP of WSN are required, because if it is less than three, it cannot form a loop in transmission medium. As the RTD measurement depends upon various parameters of Sensor Node and WSN. The WSN for various paths round trip delay (RTD) measurements has to be categorized as Symmetrical or Asymmetrical network.

A WSN network is briefly defined as Symmetrical network if

- All the sensor nodes are located at equal distance from each other.
- All sensor nodes should have same sensitivity.
- Operating speed of all sensor nodes processing unit has to be equal.
- Same wireless communication module is for all sensor nodes

Otherwise the WSN will be defined as Asymmetrical network [13].

There are various advantages of using sensor nodes in many applications of WSNs, but we also find some disadvantages since, the sensor nodes are of small size and contain non-rechargeable batteries. These disadvantages lead to battery constraint and reduce the lifetime of the network. Round trip delay (RTD) time measurement method is an easy way to overcome the above issues

in WSNs. The method of fault detection is based on RTD time of RTPs. RTD times of discrete RTPs are compared with threshold time to find the faulty sensor node in the network. Round-trip delay (RTD) is also known as round-trip time (RTT). Round-trip time (RTT) is defined as the time required for a signal pulse or packet to travel from a specific source node through a path consisting other nodes and back again. The RTD time can range from a few milliseconds to several seconds under adverse conditions between sensor nodes separated by a large distance. Round trip delay time of the RTP will be change due to the faulty sensor nodes in the network.

3.3 Objective of The Work

The main objective of this work is to detect the faulty or failure sensor nodes using round trip delay time and round trip paths in the wireless sensor network. The main target of sensor network is to cooperatively sense, collect, and process the information about the objects in the coverage region, and then sends it to the observer for processing and analyzing. Round trip delay (RTD) time technique is an simple way to obtain the information about the sensor nodes used in wireless sensor network. The proposed method will detect the failure or fault sensor node for symmetrical network conditions. In this way it helps to detect failed or malfunctioning sensor nodes, which can be used to get correct data in WSN or the exact sensor node can be repaired or working status of the WSN can be checked. The round trip delay can be range from few milliseconds to several seconds between sensor nodes separated by a distance. The time required for detection is in the range of seconds; hence data loss can be avoided.

3.4 Related Work

Failure detection scheme called MANNA is proposed in [10] using management architecture for WSNs. Faulty sensor nodes are able to detect from the above architecture. This approach is too expensive for WSNs. It requires an external manager to perform the centralized diagnosis and the communication between nodes. Method proposed in [11] to detect the failure in sensor nodes in WSNs. In this method faulty sensor nodes identified on the idea by comparisons between the surrounding nodes that is neighboring nodes and at the each node level dissemination of the decision made. The algorithm is simple while maintaining low false alarm rate it detects faulty sensor nodes with high accuracy for fault probabilities of wide range. In this method the

algorithm fails to detect the malicious nodes. Cluster based recovery algorithm is proposed in [12]. Sensor node failures changes due to which energy-efficient and responsive to network topology. It is used to detect battery failure node and recovery the battery failure node. The disadvantage of the cluster based recovery algorithm that is while transferring the cluster head that results in heavy data loss. Method presented in [13] is monitoring cycles (MCs) and monitoring path (MPs) for the detection of link failure in sensor node in WSNs. The limitation of the method three-edge connectivity in the network, for each monitoring cycles and monitoring locations maintained a separate wavelength.

Method to detect the faulty sensor node using discrete round trip delay and round trip path is proposed in [1]. In this method sensor nodes are arranged in circular topology that is in static and using this topology the packet is forwarded from source to destination by routing and Maximum round trip delay is calculated and considered as threshold value. To find the faulty sensor node the round trip delay of the round trip path should be greater than threshold value. The proposed method of fault detection is based on RTD time measurement of RTPs in wireless sensor network. RTD times of discrete RTPs are compared with the threshold time to determine failed or malfunctioning sensor node in WSN. Generalized model to determine the fault detection analysis time for WSNs by using discrete RTPs is suggested.

3.5 Problem Formulation

The sensor node in the wireless sensor networks can become faulty due to various reasons such as: battery failure, environmental effects, and hardware or software malfunctions. By discarding the data from such faulty sensor nodes in the analysis the quality of service (QoS) can be improve. In the proposed method fault node is detected by using round trip delay and round trip path in WSNs. The RTD time of RTPs is compared with the threshold value. If the RTD time of RTP is infinite then sensor node failure is detected, while if the RTD time of RTP is greater than the threshold value then the sensor node malfunctioning or fault is detected. The proposed method is the “Fault node detection using Round Trip Delay and Paths in WSN”. Selecting the minimum number of nodes in formation of RTPs will reduce RTD time and Select discrete RTPs and compare them for quick fault detection. Advantage is to maintain the better QoS under failure conditions, identifying and detecting such faults are more essential.

3.6 Proposed Work

3.6.1 RTD Time Estimation

RTD time mainly depends upon the numbers of sensor nodes present in the round trip path and the distance between them. The accuracy can be increased by reducing the RTD time of RTP. RTD can be decreased only by reducing the sensor nodes in RTP because the distance between sensor nodes in WSNs is determined by the particular applications and can't be decided. RTD time will be reduced by selecting minimum numbers of sensor nodes in the RTP in WSNs. The group of minimum three sensor nodes is essential to form the round trip path (RTP) in WSNs. Hence the minimum round trip delay time (τ_{RTD}) of RTP in WSNs with three sensors node is given by

$$\tau_{RTD} = \tau_1 + \tau_2 + \tau_3$$

Where, τ_1 , τ_2 and τ_3 are the delays for sensor node pairs (1,2), (2,3) and (3,1) respectively. Circular topology with six sensor nodes is shown in Fig. 1. Three consecutive sensor nodes in each RTP are almost at equidistance because of the circular topology. Therefore sensor node pair delays τ_1 , τ_2 and τ_3 will be equal.

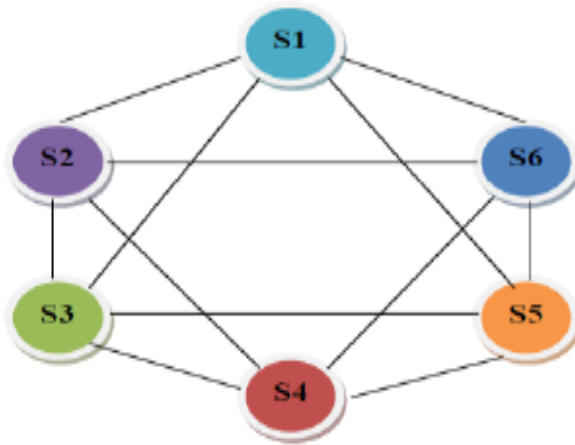


Figure 3.1 Circular topology in WSN with six sensor nodes [2]

Let us assume that ' τ ' be the uniform time delay for all sensor node pairs in RTPs i.e. $\tau = \tau_1 = \tau_2 = \tau_3$.

Round trip delay time for RTP with uniform sensor node pair delay is obtained as:

$$\tau_{RTD} = 3\tau$$

This is the minimum RTD time of an RTP in the Wireless Sensor Network. The sensor node pair delay (τ) is decided by a particular application of WSNs, as it depends upon the distance between the sensor nodes. Hence, the efficiency of proposed method can be improved only by reducing the RTPs in WSNs.

3.6.2 Evaluation of Round Trip Paths

Faulty sensor node is detected by comparing the specific RTPs to which it belongs. More numbers of sensor nodes in the round path will reduce the RTPs created. But due to this individual sensor node will be present in more RTPs. While detecting faults, comparisons of all such RTPs become necessary. This will delay the fault detection process. The maximum numbers of RTPs formed with 'm' sensor nodes is given by

$$P_M = N(N - m)$$

Where, P is the numbers of RTPs.

RTD time of RTP will increase for additional numbers of sensor nodes. The fault detection analysis time will increase exponentially with increase in numbers of sensor nodes N in WSNs. Also the maximum numbers of RTPs produced are not required for comparison to detect the fault. Such selection of RTPs is not an adequate solution to speed up fault detection. Hence optimization of RTPs in WSNs is essential to speed up the fault detection.

3.7 Round Trip Delay and Paths analysis

3.7.1 Computation of Round Trip Paths

Fault detection by analyzing RTD time of maximum number of RTPs will require substantial time and it can affect the performance. Round Trip Paths can be calculated with the help of linear selection of RTPs and Discrete selection of RTPs.

Both techniques are explained below:

A. Linear Selection of RTPs:

In order to reduce the RTPs in the fault detection analysis, instead of taking maximum numbers of RTPs, only few paths corresponding to the number of sensor nodes in WSNs are sufficient. We can consider the RTPs equal to number of sensor nodes in WSNs to reduce analysis time. Because of the linear relationship between N and P this is called as linear RTPs. Hence the

comparison of such three linear RTPs is sufficient to detect the faulty sensor node [1]. The linear RTPs in WSNs with N sensor nodes is given as

$$P_L = N$$

Where, P_L is the number of linear RTPs. It is essential to measure the RTD times of such paths.

Analysis time $\tau_{ANL}(L)$ for linear RTPs is given by:

$$\tau_{ANL}(L) = N * 3\tau$$

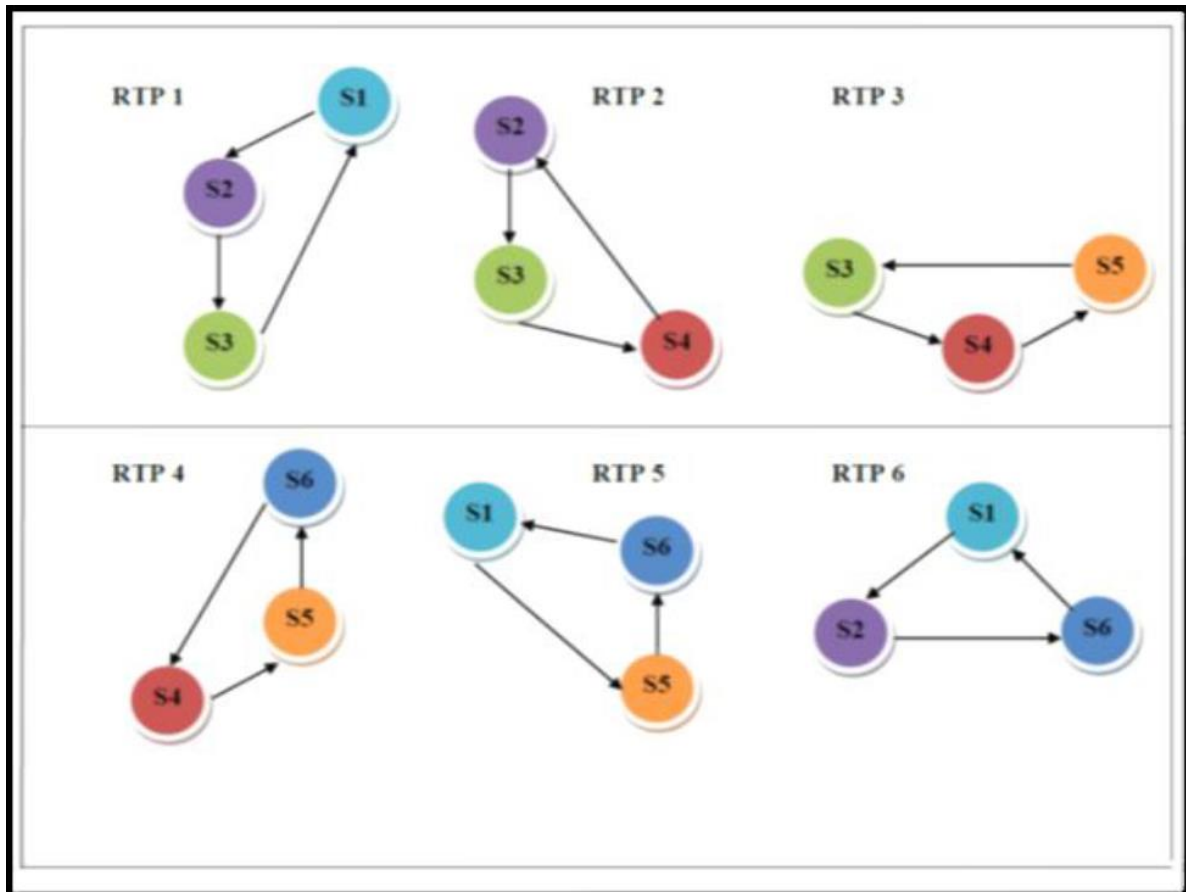


Figure 3.2 Illustration of six linear RTPs [2]

In linear approach for six sensor nodes in circular topology, Six Round Trip Paths are computed as:

RTP 1=S1-S2-S3-S1

RTP 2=S2-S3-S4-S2

RTP 3=S3-S4-S5-S3

RTP 4=S4-S5-S6-S4

RTP 5=S5-S6-S1-S5

RTP 6=S6-S1-S2-S6

Linear RTPs selected will be more for large number of sensor nodes. This will not calculate the fault detection time for large size WSN network. Therefore, further reduction in the numbers of RTPs is must to increase the efficiency of this proposed method. Disadvantages of this approach are redundancy is increased, and reduces number of exact responses in network. Redundant paths in WSNs will slow down the fault detection process.[2]

B. Discrete Selection of RTPs:

Fault detection time for WSNs with large numbers of sensor nodes is significantly high. So there is need to minimize the RTPs in WSNs. Numbers of RTPs are reduced by selecting only discrete paths in the Wireless sensor network. Discrete selection of RTPs are selected from sequential linear RTPs only. They are selected by ignoring the two consecutive paths, after each selected the linear path [1].

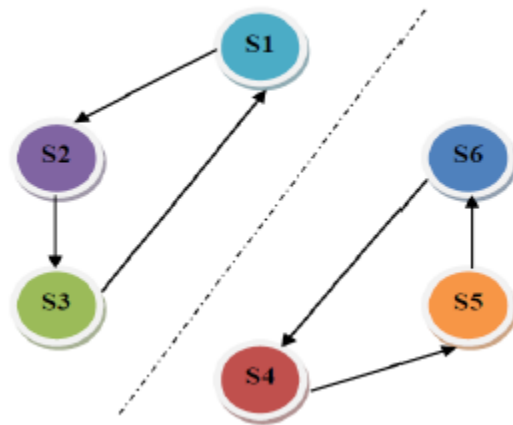


Figure 3.3 Illustration of two discrete RTPs [2]

The Discrete RTPs in WSNs sensor nodes can be Computed by using following equation:

$$P_D = Q + C$$

Q and C are expressed as:

$$Q=[N/m]$$

$$\text{And, } C=\begin{cases} 0 & \text{if } R = 0 \\ 1 & \text{if } R \neq 0 \end{cases}$$

Where, P_D is discrete paths in WSNs, Q is Quotient, m is number of sensor nodes in Round Trip Path i.e $m=3$, N is the number of sensor nodes in wireless sensor networks, C is Correction factor to be added, It will be 0 if remainder is 0 otherwise it is 1.

The analysis time $\tau_{ANL}(D)$ required for detection of faults in discrete RTPs is computed with the help of equation given as:

$$\tau_{ANL}(D) = (Q+C) * 3\tau$$

For $m=3$;

$$\tau_{ANL}(D) = ([N/3] + C) * 3\tau$$

Where, τ is Round Trip Delay (RTD).

Analysis of particular selected discrete path will be sufficient to monitor the fault. Discrete selection of RTPs will save the analysis time to a large extent. Advantages of discrete selection of RTPs are: decreased analysis time, faulty sensor nodes are detected and it maintains the Quality of Service (QoS) under failure conditions.

3.8 Result Analysis

3.8.1 Comparisons for Maximum, Linear and Discrete methods for various WSNs

The number of RTPs is calculated for different number of sensor nodes (N) in maximum, linear, and discrete methods to detect the faulty nodes in WSNs. Here we choose $m=3$. RTPs calculated in maximum case are too high. In linear selection of RTPs method, it has been significantly reduced. Still the numbers of linear RTPs for large value of N is much high. The discrete RTPs calculated are very much optimized as compared to linear selection and maximum cases. RTD time of very few RTPs is measured in case of discrete selection of RTPs will save the utilization

of sensor node in fault detection [1]. The RTD analysis time required for maximum, linear, and discrete RTPs with different numbers of sensor nodes. N is mentioned in Table 3.1.

Table 3.1: RTPs Comparison for Maximum, Linear and Discrete for various WSNs

Round Trip Paths	Numbers of sensor nodes (N) in WSNs			
	6	10	20	100
$P_M = N(N - 3)$	18	70	340	9700
$P_L = N$	6	10	20	100
$P_D = N/m + C$	2	4	7	34

Analysis time saved by using discrete RTPs as compared to linear RTPs is up to 66%. Thus, the efficiency of fault detection method is improved by considering the discrete RTPs.

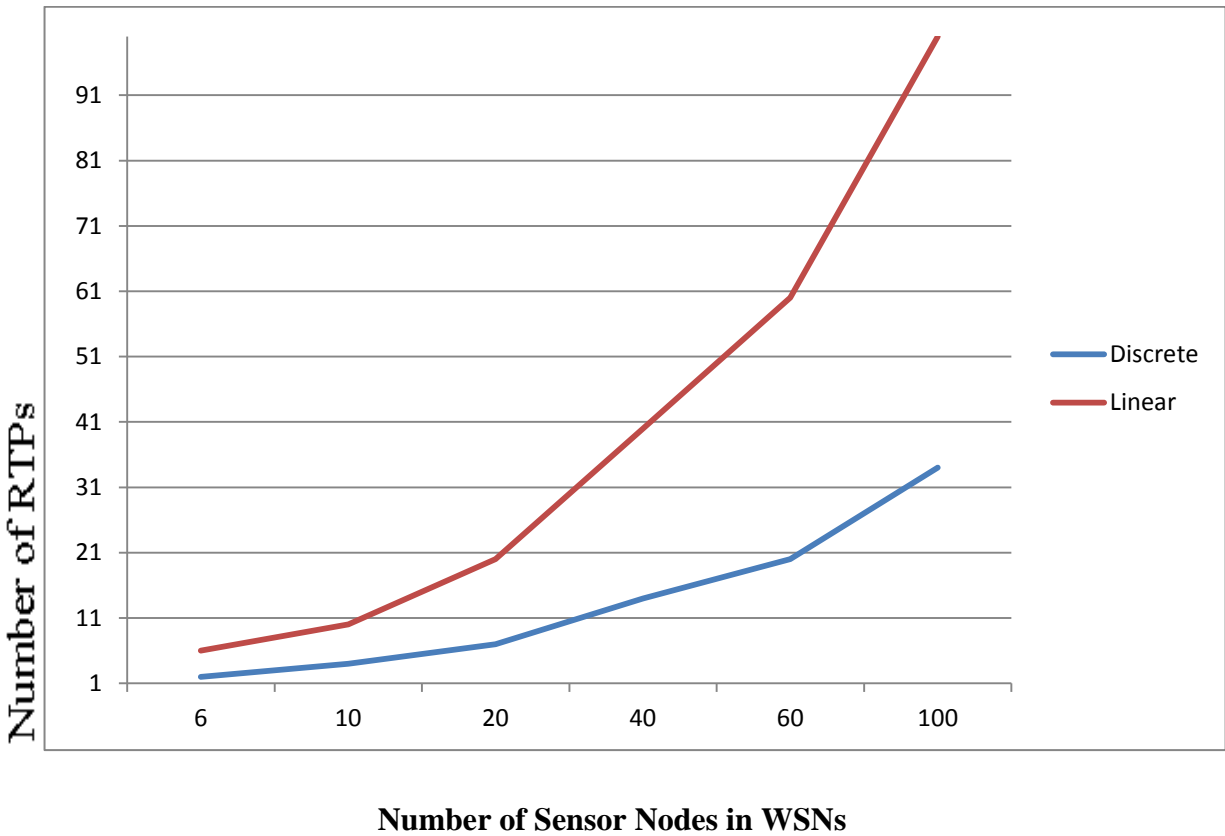


Figure 3.4: Linear and Discrete RTPs formed for different values of sensor node N in WSNs

3.8.2 Generalized RTD time Model

After the calculation of number of RTD paths, the quick detection of fault is done by using the Discrete RTPs. Fault present at the source node in RTP is equal to discrete plus one RTPs analysis [1].

The total numbers of RTPs used to detect fault are given by:

$$P_T = P_D + L$$

Where, P_T is the total number of optimized RTPs and L is the number of sensor nodes excluding source node form in RTP, i.e.

$$L = (m-1).$$

Therefore,

$$P_T = [N/m] + C + (m-1)$$

Table 3.2: Analysis Time of Discrete RTPs with Variable number of sensor nodes in RTP for WSN with 100 sensor nodes

N	m	Q=[N/m]	C	L=m-1	$P_T=Q+C+L$	$\tau_{ANL}=P_T*3\tau$
100	3	33	1	2	36	108 τ
100	5	20	0	4	24	120 τ
100	7	14	1	6	21	147 τ
100	9	11	1	8	20	180 τ
100	10	10	0	9	19	190 τ

Analysis time of this method is depends on the RTD time of RTPs used to examine. Generalized model of analysis time by taking RTPs in WSNs with N sensor nodes and RTP created by grouping of 'm' sensor nodes is given as:

$$\tau_{ANL}(G) = \{[N/m + C + (m-1)] * 3\tau$$

Total number of RTPs and analysis time related to it is calculated by using above equation.

For m=3, the analysis time is lowest. Therefore, selection of sensor node per RTP equal to three is better to enhance the efficiency of this proposed method.

3.8.3 Algorithm for Faulty Sensor Node Detection

Step1: Initially all the sensor nodes are in zero position.

Step2: The Sensor nodes will move to their particular position to form a circular Topology.

Step3: Find RTP, i.e.

$$P_D = Q + C$$

Where,

$$Q = [N/M]$$

$$\text{And, } C = \begin{cases} 0 & \text{if } R = 0 \\ 1 & \text{if } R \neq 0 \end{cases}$$

Step4: Transmission starts between three sensor nodes.

Step5: Step4 continues until all the sensor nodes should be involved in the transmission. Then go to next step.

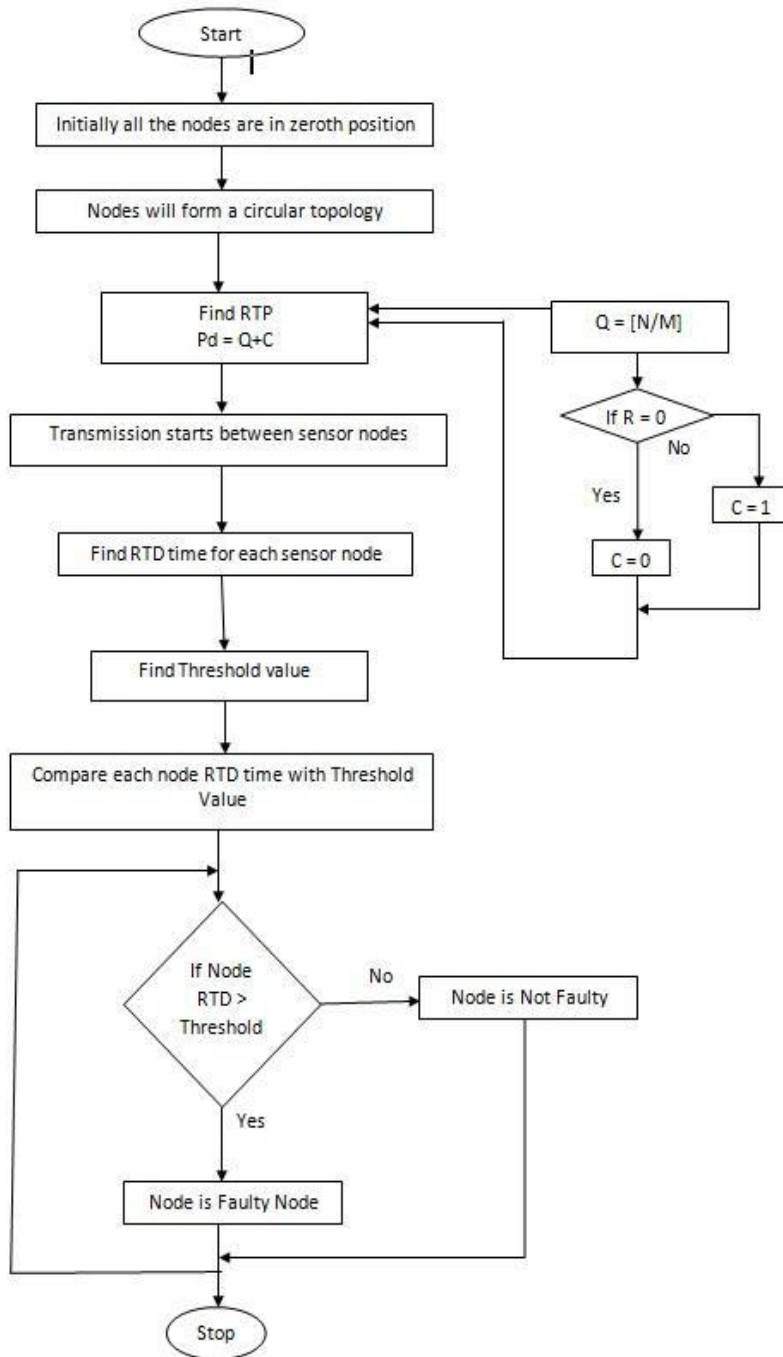
Step6: Find RTD of all the sensor nodes.

Step7: Find Threshold Value.

Step8: Compare each sensor node RTD with Threshold value, and then the nodes having RTD greater than Threshold Value means that node is consider as Faulty sensor node.

Step9: Performance graphs are found to show the Faulty sensor nodes.

FLOW CHART:[2]



On the basis of algorithm mentioned above the value of round trip time (RTT) can be calculated. The programming in TCL works well in finding the total RTT between source and destination node. RTT value is calculated for sending the data packets from the source to destination node. If the time for sending packets exceeds more than the value calculated, the fault node can be identified with the help of calculated Round Trip Delay using Round Trip Path.

CHAPTER 4

Reliable Fault-Tolerant Multipath Routing Scheme for Wireless Sensor Networks

4.1 Introduction

Wireless Sensor Network (WSN) consists of various sensor nodes, base station and gateway and the main objective is to sense, collect and process the information about objects in the coverage region, and then send it to the observer for processing and analyzing the information. In WSN, fault occurrence probability is very high compare to other traditional Wireless networking [15]. The main function of WSNs is to gather information about the environment and transmit the information to destination. Therefore, WSNs is mainly used for diverse applications such as environment monitoring, military surveillance, fire detection and health monitoring. In different applications, different kinds of sensor nodes are used. These sensor nodes may have different level of Quality of service (QoS) requirement that may differ according to various applications.

Multipath routing technique consists of multiple paths instead of a single path for routing. It is successfully used for maximum utilization of network resources. Multipath routing can effectively utilize network bandwidth and balances network traffic as compare to single-path routing. In this routing a node have a choice of next hop for the same destination. Multipath routing provides reduced end to end delay, load balancing, large throughput, bandwidth aggregation and can ensure high reliable data transmission, which is one of the main transmission requirements of wireless sensor networks [17].

Mostly routing protocols might differ depending on the specific applications and network architecture. WSNs routing protocol design is influenced by the network restrictions as well as some other specific metrics, such as; energy consumption. In this paper, Reliable Fault Tolerant Multipath (RFTM) routing protocol is proposed which involves fault recovery process. In this proposed protocol sensed data is transmitted through a shortest path. In case, any faulty data occurs in the network, recovery is very fast. In this paper our main purpose is to design a multi objective routing protocol (MRFTM)[16]. In this protocol, sensor nodes just need to have information of its neighboring nodes not the whole path information. The data is transmitted to

base station with minimum delay and energy loss. This technique also controls the data traffic during transmission of data to the base station. A multi-objective routing protocol MRFTM considers the link quality during data transmission to avoid poor link connectivity when choosing next nodes to route data. This protocol uses multipath routing to deliver data to sink node for desired reliability. The number of paths varies based on the level of reliability required. With the increasing level of reliability the number of paths also increases. When the required reliability is small then only one or few paths are required. The data packets are coded by source node using erasure code [19] and transmit each coded packet through one of the selected paths in order to provide degree of fault tolerance to different levels of information based on the level of reliability required. The selection criteria of these multiple path depend on different application requirements.

4.2 Proposed RFTM Routing Protocol Overview and Related Work

We propose a Reliable Fault-Tolerant Multipath (RFTM) routing protocol. Reliable Fault-Tolerant Multipath (RFTM) is an on-demand routing protocol. In on-demand routing protocol path is created only when it is needed. On-demand routing enhances the security and reliability of the routing protocol and builds multiple disjoint paths using route request/reply (RREQ) phases to provide the fault tolerance mechanism due to availability of alternate path and the use of erasure coding at the source node. Erasure coding is used to increase the protocol security and reliability [18]. Reliability is an important factor for QoS in Wireless Sensor Networks (WSNs), reliable data transport is to provide reliable transmission of data and to have the ability to detect and data repair packet losses in the network.

Route Request (RREQ) phase is started when source node wants to send a message to sink node. When this message is received by each intermediate node then each node generates and maintains its neighbors routing table and updates the RREQ message and also rebroadcasts the message till it reaches the sink node. At the end of this process multiple disjoint paths are obtained from the source to the sink as well as all paths information and the minimum available energy of a node on that path. After receiving RREQ messages the sink node collects all the information in the messages and measures the best paths depending on the required reliability. After this, the sink node starts the route reply phase. In this phase the sink node broadcasts the route reply (RREP) message through selected paths towards the source node [16].

4.2.1 Control Packets format

Source node generates its route table for a route to sink. If there is no route, Source node generates a RREQ message with the following components

- Source and sink ID
- Request ID
- Sender ID
- Desired reliability DR
- Minimum Energy Level(EL), minimum energy available at a node
- Hop count, source node hop count(HC) =0, then increases at each node.
- Successful probability on a link [17]

Suppose a node P receives the RREQ from sink node. P node first checks whether it has received this RREQ before or not. The pairs of all the recent received RREQ are stored by each node. If P node has seen this RREQ from sink node already, P node discards the RREQ. Otherwise it processes the RREQ [20].

As shown in Figure 4.1, the shaded fields will be kept unchanged for the RREQ message while the other fields will be modified at each intermediate node [17].

Request ID	Source ID	Min. Energy Level EL	Sender ID	Hop Count HC	Successful Probability q_i	Desired Reliability DR	Sink ID
------------	-----------	-------------------------	-----------	-----------------	---------------------------------	---------------------------	---------

Figure 4.1: RREQ message format [17]

In this protocol second control message is Route Reply message (RREP). When sink node receives the RREQ message then the sink node broadcasts the RREP message and finding the best path to the source. RREP message consists of the following fields: Request ID, Source ID, Sender ID, Sink ID and Coding ratio, which is a measure of the desired reliability (DR) (Figure 4.2) [17].

Request ID	Source ID	Sender ID	Sink ID	Coding ratio
------------	-----------	-----------	---------	--------------

Figure 4.2: Route Reply Message [17]

4.2.2 Phases in RFTM Routing Protocol

Following three phases exist in this protocol:

- i) Route discovery
- ii) Route Reply
- iii) Multipath construction

i) ROUTE DISCOVERY:

The RFTM routing protocol uses route discovery phase to discover the nodes routing for multiple routes to a given destination. This phase started when the source node has data packet to transmit to the destination [24]. At the end of this process multiple paths are obtained from the source to the destination as well as all paths information. After receiving RREQ messages the destination node collects all the information and measures the best paths depending on the required reliability. After this, the destination node starts the route reply phase.

ii) ROUTE REPLY:

In this phase the sink node broadcasts the route reply (RREP) message through selected paths towards the source node [25]. Data transmission takes places when the source node receives the destination decision carried by the RREP message on the number of paths to transmit data.

RREQ message reaches the destination with a valid route, that destination node responds with a Route Reply (RREP) message. This RREP message travels to the source along the reverse path [21]. All nodes that route the RREP message to the source also make corresponding forward information in their routing table such that the next hop to the destination is the node from which the RREP message was just received by the source. After receiving the RREP message, the source node starts sending the data to the destination. Each RREP message contains the destination sequence number, which is used to prevent routing loops.

iii) MULTIPATH CONSTRUCTION:

After the Route Discovery phase, each node possesses their neighbor information and then the Multipath Construction phase starts [22]. Because the source node location is known to the destination and based on the location of the source the destination starts the route request process. There are two types of nodes primary and alternate. The primary nodes find two paths towards the source; the primary path and the alternate path [23]. The primary path is built with the best

possible neighbor and the alternate path is constructed with the next best neighbor. The alternate nodes find one single path towards the source node.

4.3 Simulation and Evaluation

In this section, we simulate the performance of our routing protocol using MATLAB. In our simulation we use various metrics to evaluate the performance of proposed routing protocol.

4.3.1 Data Delivery Ratio (DDR):

DDR metric indicates the end to end successful transmission. The greater value of packet delivery ratio means the better performance of the protocol. Data Delivery Ratio can be represented as:

$$\text{DDR} = \frac{\text{Packet received at the sink}}{\text{Packet generated by the source}}$$

The result for this metric for different network size is 50 to 200 with different initial energy. Figure 4.3 shows the effects of initial energy on the reliability of the network. This figure shows that how the data delivery ratio increases with the increase of initial energy (IE) and number of nodes in the network.

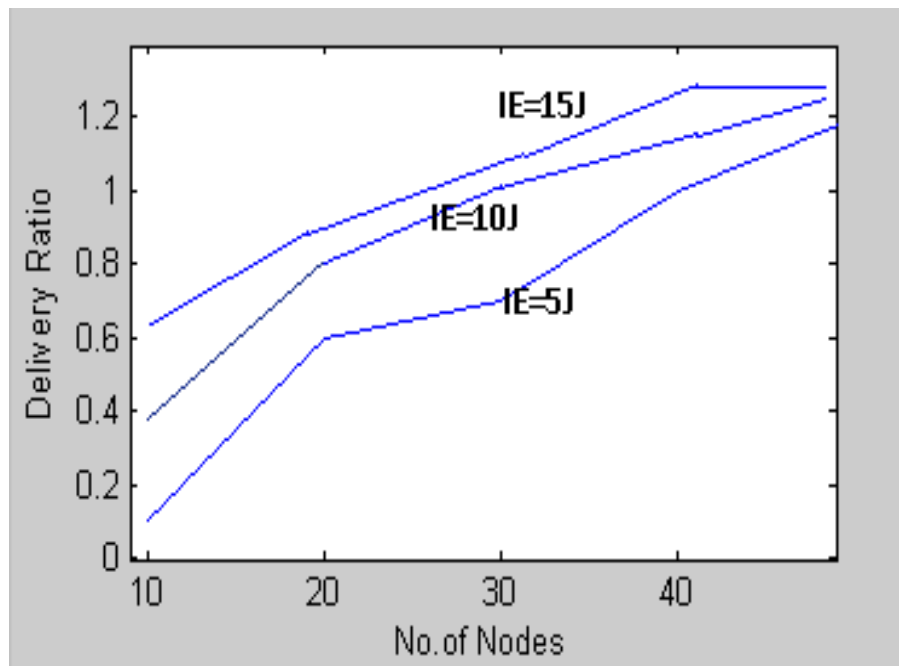


Figure 4.3: Average Delivery Ratio

4.3.2 Number of Paths Discovered

When Mobility of nodes is increases then the average number of path also increases. When node reaches the maximum value then the path between the sources to destination is found for all nodes. After the source has received a path to the destination, it sends the data packet on it. Figure 4.4 represents the average number of paths discovered between the source and destination. Number of paths discovered is related to the number of nodes and desired reliability. For different number of nodes the path number does not affect the reliability since the erasure coding is used.

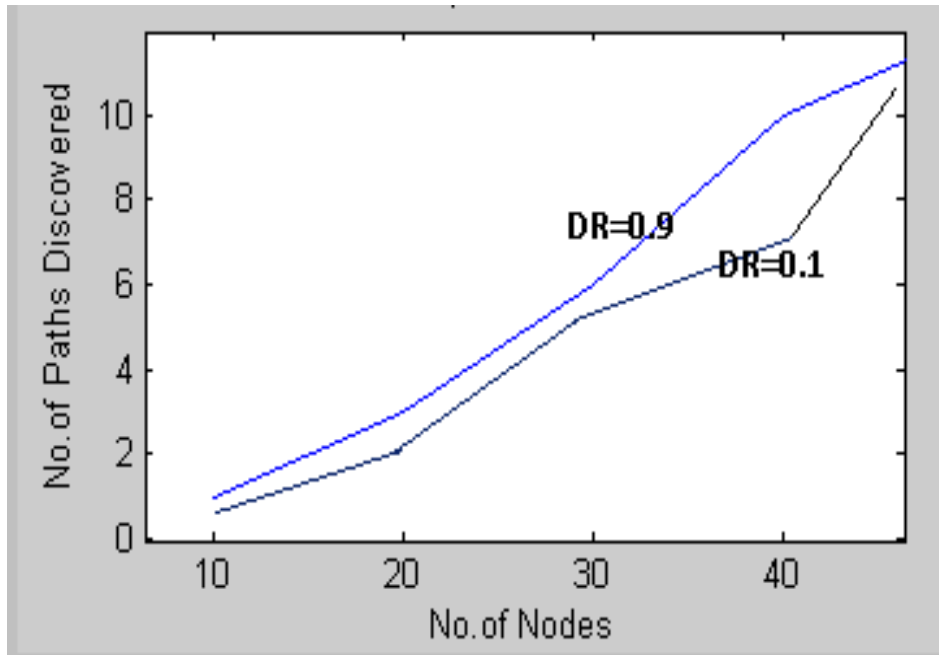


Figure 4.4: Number of Paths Discovered

4.3.3 Energy Consumption:

This metric measures the average energy dissipated by the node in order to data packet transmission from source to destination. It measures the network lifetime. Energy consumption is defined as the difference between the initial level of energy (E_{int}) and the final level of energy (E_{fin}) that is left in the node.

$$(E_{consp}) = E_{int} - E_{fin}$$

Thus the average energy consumption (E_{avg}) is given by:

$$(E_{avg}) = \sum_{i=1}^N (E_{consp}) / N ; \quad N = \text{number of nodes}$$

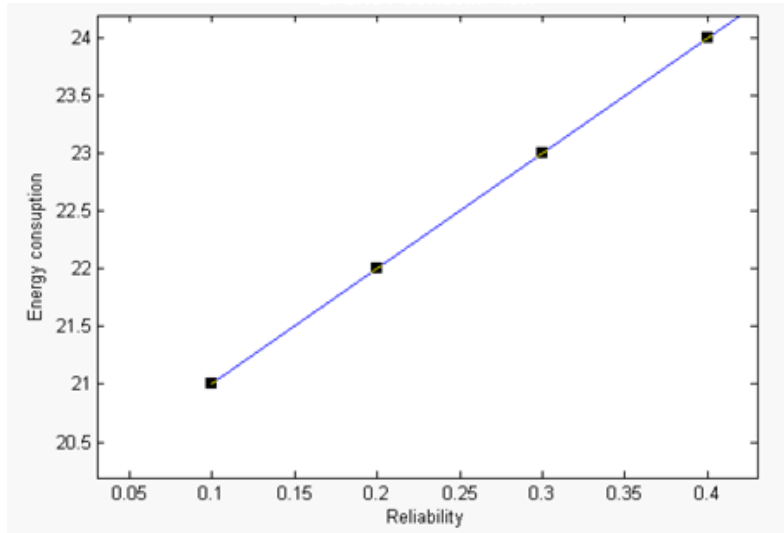


Figure 4.5: Energy Consumption

Figure 4.5 show that more reliability demanded consumes more energy in the network. Thus, in proposed routing protocol data transmission reliability obviously increases while node energy consumption increases.

CHAPTER 5

CONCLUSION

Firstly, in the proposed faulty node detection method in wireless sensor networks, discrete round trip paths are selected and compared with threshold value to identify sensor node behavior. The simple algorithm is used to detect effectively and it enhances fault detection efficiency by selecting the discrete RTPs. Each sensor node in WSNs is rarely utilized in fault detection due to discrete selection of paths, this improves lifetime due to less energy consumption. Therefore, this method improves lifetime and quality of service of WSNs. This method is scalable to wireless sensor networks with large numbers of sensor nodes. The proposed method is successfully implemented on circular topology WSNs with variable sensor nodes (N). Our future work includes simulation work for proposed method and also verifying the performance of this method on other topologies in WSNs.

Secondly, in the proposed faulty node detection method in wireless sensor networks, discrete round trip paths are selected and compared with threshold value to identify sensor node behavior. The simple algorithm is used to detect effectively and it enhances fault detection efficiency by selecting the discrete RTPs. Each sensor node in WSNs is rarely utilized in fault detection due to discrete selection of paths, this improves lifetime due to less energy consumption. Therefore, this method improves lifetime and quality of service of WSNs. This method is scalable to wireless sensor networks with large numbers of sensor nodes. The proposed method is successfully implemented on circular topology WSNs with variable sensor nodes (N). Our future work includes simulation work for proposed method and also verifying the performance of this method on other topologies in WSNs.

REFERENCES

- [1] Ravindra Navanath Duche and Nisha P. Sarwade, “*Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs*”, IEEE SENSORS JOURNAL, VOL. 14, NO. 2, FEBRUARY 2014.
- [2] Vishwanath V Koli et al, “*Sleuthing and Resolving Sensor Node Failure in WSNs*” International Journal of Computer Science and Mobile Computing, Vol.4 Issue.7, July- 2015.
- [3] Girish K and Mrs. Shruthi G, “*Design and Implementation of detecting the failure of sensor node based on RTT time and RTPs in WSNs*”, IJISSET - International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 4, April 2015.
- [4] S. Shamili and D. Manivannan, “*Sensor Node Failure Detection using Multiway Tree based Round Trip Path in Wireless Sensor Networks*” Indian Journal of Science and Technology, Vol. 8(12), June 2015.
- [5] S.Yuvaraj1,K.R.Prasanna Kumar, “*Fault Node Detection in Wireless Sensor Networks Based on Round Trip Delay and Paths*”, INTERNATIONAL JOURNAL OF ADVANCED RESEARCH TRENDS IN ENGINEERING AND TECHNOLOGY (IJARTET), VOL. II, SPECIAL ISSUE VIII, FEBRUARY 2015.
- [6]Nevidhitha Bonnita. P, Dr.Nalini.N, Mohan.B.A, “*Failure detection of sensor nodes based on Round Trip Delay and Paths in Wireless Sensor Networks*”, International Research Journal of Engineering and Technology (IRJET) Volume, 02 Issue: 03 | June-2015.
- [7]Pankaj Chauhan, Tarun Kumar, “*Power Optimization in Wireless Sensor Network*”, International Journal of Engineering and Technical Research (IJETR), Volume-3, Issue-5, May 2015
- [8] L. B. Ruiz, I. G.Siqueira, L. B. Oliveira, H. C. Wong, J. M. S. Nogueira, and A. A. F. Loureiro, “*Fault management in event-driven wireless sensor networks*”, Simulation and experimental analysis of a ZigBee sensor network with fault detection and reconfiguration mechanism,” in Proc. 8th ASCC, May 2011.
- [9] M. Lee and Y. Choi, “*Fault detection of wireless sensor networks*”, Comput. Commun., vol. 31, pp. 3469–3475, Jun.2008.
- [10] A. Akbari, A. Dana, A. Khademzadeh, and N. Beikmahdavi, “*Fault detection and recovery in wireless sensor network using clustering*”, IJWMN vol. 3, no. 1, pp. 130–138, Feb. 2011.

- [11] S. S. Ahuja, R. Srinivasan, and M. Krunz, “*Single-link failure detection in all-optical networks using monitoring cycles and paths*,” *IEEE/ACM Trans. Netw.*, vol. 17, no. 4, pp. 1080–1093, Aug. 2009.
- [12] Ravindra Navanath Duche and Nisha P. Sarwade, “*Round Trip Delay Time as a Linear Function of Distance between the Sensor Nodes in Wireless Sensor Network*”, *International Journal of Engineering Sciences & Emerging Technologies*, Feb 2012.
- [13]Kamalrulnizam Abu Bakar Marjan Radi, Behnam Dezfouli and Malrey Lee. “*Multipath routing in wireless sensor networks: Survey and research challenges MDPI Sensors*”, 12(1):650–685, January 2012.
- [14] Ganesan Deepak, Govindan Ramesh, Shenker Scott, and Deborah Estrin. “*Highly-resilient energy-efficient multipath routing in wireless sensor networks*”,2nd ACM international symposium on Mobile ad hoc networking & computing, MobiHoc '01, pages 251–254, New York, NY, USA, 2001.
- [15] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “*A Survey on sensor networks*,” *IEEE communications Magazine*, vol. 40. no. 8, pp. 102-114, August 2002.
- [16] H. Alwan and A. Agarwal, "*Multi-objective Reliable multipath routing for wireless sensor networks*", *IEEE GLOBECOM Workshops (GC Wkshps), 2010 IEEE*, Miami, FL, 2010,pp.1227-1231.
- [17]H. Alwan and A. Agarwal, “*Reliable Fault-Tolerant Multipath Routing Protocol for Wireless Sensor Networks*”, 25th Biennial Symposium on Communications, Queen University, Canada, 2010.
- [18] M. A. Moustafa, M. A. Youssef and M. N. El-Derini, "*MSR: A multipath secure reliable routing protocol for WSNs*," *Computer Systems and Applications (AICCSA), 2011 9th IEEE/ACS International Conference on*, Sharm El-Sheikh, 2011, pp. 54-59.
- [19] A. Fujimura, S. Y. Oh, and M. Gerla, “*Network coding vs. erasure coding : Reliable multicast in ad hoc networks*”, *IEEE Military Communications Conference 2008 (Milcom 08)*, Nov. 2008.
- [20] Koffka Khan , Wayne Goodridge “*Fault Tolerant Multi-Criteria Multi-Path Routing in Wireless Sensor Networks* “ *I.J. Intelligent Systems and Applications*, 2015, 06, 55-63 Published Online May 2015 in MECS.

- [21] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, A.Hadjidj, “*Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks*”, Journal of Network and Computer Applications, vol. 34, no. 4,pp. 1380–1397,July 2011.
- [22] Kim M, Jeong E, Bang Y.-C, Hwang S, Kim B, “*Multipath energy-aware routing protocol in wireless sensor networks*”, 5th international conference on networked sensing systems, 2008, Pages 127-130.
- [23] K. Akkaya and M.Younis, “*An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks*,” International Conference on Distributed Computing Systems Workshops, pp. 710-715, May 2003.
- [24] H. Alwan and A. Agarwal, “*A Survey on Fault Tolerant Routing Techniques in Wireless Sensor Networks*”, Third International Conference on Sensor Technologies and Applications, Athens/Glyfada, Greece, 2009, pp. 366-371.
- [25] E. Felemban, C.-G. Lee, and E. Ekici, “*MMSPEED: Multipath multispeed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks*”, IEEE Trans. Mob. Comput., vol. 5, no. 6, 2006, pp. 738–754.
- [26] J. Reed , “*Introduction to Ultra Wideband Communication Systems*”, Prentice Hall , Englewood Cliffs, NJ , June 2005.
- [27] T. Melodia , D. Pompili , V. C. Gungor , and I. F. Akyildiz , “*Communication and coordination in wireless sensor and actor networks* ” , IEEE Transactions on Mobile Computing, vol. 6 , no. 10 , Oct. 2007 , pp. 1116 – 1129.
- [28]] Kewei Sha, Jegnesh gehlot, Robert Greve, “*Multipath routing techniques in wireless sensor networks*” Wireless personel communications, vol-70, pp.807-829, 2013
- [29] Mona Gupta, Neeraj Kumar, “*Node disjoint on-demand multipath routing with route utilization in ad-hoc networks*”, International Journal of Computer Applications, vol.70, pp.29-33, 2013.

[30] Bagula, A.; Mazandu, K. “*Energy Constrained Multipath Routing in Wireless Sensor Networks*”, 5th International Conference on Ubiquitous Intelligence and Computing, Oslo, Norway, 23–25 June 2008; pp. 453–467.

[31] Li, W.; Cassandras, C.G. “*A Minimum-Power Wireless Sensor Network Self-Deployment Scheme*”, IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 13–17 March 2005; pp. 1897–1902.

[32] Ben-Othman, J.; Yahya, B. “*Energy Efficient and QoS Based Routing Protocol for Wireless Sensor Networks*”, J. Parall. Distrib. Comput. 2010, 70, 849–857.