A NOVEL ENERGY EFFICIENT ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

SHIVA MURTHY G

DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA

SURATHKAL, MANGALORE -575 025

MAY, 2012

Abstract

Wireless sensor network (WSN) is a distributed, multi hop, self-organized network consisting of large number of autonomous, tiny sensor nodes deployed in a phenomena to observe or sense and communicate the sensed data to the sink node.

Routing the sensed data from the source to sink node in a resource constrained environment in wireless sensor networks is still a challenge. There are many attempts made to route the data in the resource constrained scenarios. Optimal path between the source and destination is selected by the routing protocols to satisfy the resource constraints such as energy, bandwidth and computation power. The routing protocols take into account the metrics like minimum hop, minimum transmission cost, high residual energy, etc. to route the data. Many routing protocols attempt to reduce the energy usage in the nodes to increase the network lifetime. Selecting an optimal path between the source and destination and sending the data through that path may not increase the lifetime of the network.

The multi-path routing protocols select the available paths between the source and destination. The data is distributed among the multiple paths and the usage of energy for the data transmission is spread among the number of nodes over multiple paths. In the recent past, many researchers presented node disjoint multipath routing protocols. Several node disjoint multipath routing protocols available today are on demand. Many wireless sensor network applications have immobile sensor node and static topology. In static topology networks reactive protocols suffer excessive routing overhead compared to proactive routing protocols.

In this research work, a novel sink initiated, proactive, Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) for wireless sensor networks based on the rate of energy consumption and traffic through the node is proposed. It also provides digital signature based security in the data routing. It uses MD5 hash function to generate digital signatures. RSA and ECDSA are employed in the proposed EENDMRP. The performance of

the EENDMRP is compared with Ad hoc on demand multipath routing protocol. The performance of EENDMRP is analysed through the routing metrics such as packet delivery fraction, normalized routing load, average end-to-end delay, average node energy spent and network lifetime. The proposed EENDMRP minimises the number of control messages used in the route construction, reduces the normalised routing load, increases the packet delivery fraction, reduces the end-to-end delay and increases the network lifetime. The EENDMRP also reduces the residual energy variance after the data transfer and defends the data tampering or altered routing, selective forwarding and byzantine attacks.

Acknowledgments

It would not have been possible to write this doctoral thesis without the blessings of almighty. I praise God, the almighty for providing me this opportunity and granting me the capability to proceed successfully.

First, I would like to express my sincere gratitude to my supervisor Prof. R.J.D'Souza for his guidance, support and encouragement throughout my research work. I feel proud to have worked under him.

I thank the members of my Research Proposal/Progress Assessment Committee (RPAC), Prof. Ram Mohana Reddy, IT Dept and Dr. Santhosh George, MACS Dept, for their suggestions and valuable inputs that made the dissertation work effective.

I am thankful to the Director and all the office staff of NITK for extending the support and facilities to pursue the research work in the institute successfully. I thank the HOD of MACS dept for extending support, facilities and co-operation to carry out my research work during my stay in NITK. I also thank all the faculty members of MACS dept for their encouragement to complete the thesis in time.

I am grateful to Prof. Varaprasad G, B.M.S College of Engineering, Bangalore, for extending his support and guidance throughout this work. I take this opportunity to acknowledge the constant and often exhaustive support and encouragement extended to me by my wife, son and family members.

Finally, I would like to express my gratitude to my friends, Fr.Johny Jose, Syed Naimathulla Hussain, Venkataramana, Mohit, Sreenivasappa, Ganala Santhoshi, Ajay Kumar, Muruli, Ramesh, Balaji, Kiran, Mahipal Reddy and others at NITK for their encouragement, and the continued support which helped me to complete this work.

SHIVA MURTHY G

Contents

Abstract **i**

Acknowledgments

List of Tables **vi**

List of Figures **vii**

List of Abbreviations **ix**

Nomenclature **xi**

1 Introduction **1**

1.1 Preliminaries 1

1.1.1 Technical Details of Sensor Node 2

1.1.2 Wireless Sensor Networks: Technical Challenges and Requirements . 5

1.1.3 Wireless Sensor Network Applications 7

1.2 Routing in Wireless Sensor Networks 9

1.2.1 Routing Protocol Design Issues 9

1.2.2 Energy Efficient Routing Protocol Classification 11

1.3 Motivation 15

1.4 Scope of the Research Work 17

1.5 Outline of the Thesis 17

2 Literature Review **19**

2.1 Multipath Routing Protocol 19

2.2 Advantages of Multipath Routing Protocol 20
2.3 Classification of Multipath Routing Protocol 20
2.3.1 Multipath Construction Initiated 21
2.3.2 Data Transmission Techniques 22
2.3.3 Traffic Sharing Techniques 22
2.3.4 Multipath Generation Techniques 23
2.4 Related Works in Node Disjoint Multipath RoutingProtocol 25
2.5 Outcome of the Literature Review 39
2.6 Problem Statement 40
2.7 Objectives of the Research Work 40
2.8 Summary 40

3 Analytical Model for Node Disjoint Multipath Routing Protocol for WSN 42
3.1 Assumptions 42
3.2 Analytical Model for Node Disjointedness in Multipath Routing Protocol . . 43
3.3 Network Lifetime Model for Node Disjoint Multipath Routing Protocol . . . 45
3.3.1 Path Failure Model 46
3.3.2 Network Lifetime Model 46
3.4 Route Redundancy Model for Node Disjoint Multipath Routing in WSNs . . 48
3.4.1 Single Node Redundancy over Single Path 48
3.4.2 Single Node Level Redundancy through Multiple Nodes over Single Path 48
3.4.3 Single Node Level Redundancy through Multiple Levels 49
3.5 Results and Discussion 49
3.6 Summary 57

4 Energy Efficient Node Disjoint Multipath Routing Protocol for WSNs 59
4.1 Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) . . 59
4.1.1 Route Construction Phase 60
4.1.2 Primary Path Selection Criteria 62
4.1.3 Route Maintenance Phase 65
4.2 Results and Discussion 66
4.2.1 The Energy Model 66

4.3 EENDMRP Performance Analysis 67
4.3.1 Effects of Transmission Range 68
4.3.2 Packet Delivery Fraction (PDF) 72
4.3.3 End-to-End Delay 74
4.3.4 Normalized Routing Load (NRL) 76
4.3.5 Average Energy Spent 78
4.3.6 Network Lifetime 80
4.4 Summary 81

5 Effective Load Sharing Mechanism in EENDMRP 82
5.1 Related Works 82
5.2 Load Sharing Mechanisms 85
5.2.1 Statistically Based Load Sharing Mechanism 85
5.2.2 Ratio Based Load Sharing Mechanism 87
5.3 Results and Discussion 88
5.4 Summary 91

6 Security in Energy Efficient Node Disjoint Multipath Routing Protocol for WSNs 93
6.1 Security Requirements in Wireless Sensor Networks 94
6.2 Security Threats in Wireless Sensor Networks Routing Protocols 95
6.2.1 Spoofed Routing Information 96
6.2.2 Selective Packet Forwarding 96
6.2.3 Sybil Attack 96
6.2.4 Sinkhole Attack 97
6.2.5 Wormholes Attack 97
6.2.6 Hello Flood Attacks 98
6.2.7 Acknowledgment Spoofing 98
6.3 Public Key Cryptography in Wireless Sensor Networks 98
6.4 Digital Signature based Security in EENDMRP 99
6.4.1 RSA Public Key Crypto System based Security in EENDMRP 100
6.4.2 Security in EENDMRP 101
6.4.3 Correctness of RSA Public Key Crypto System in EENDMRP 102

6.4.4 ECDSA Public Key Crypto System based Security in EENDMRP . . 103
6.4.5 Defending the WSN Threats 106
6.5 Results and Discussion 107
6.6 Summary 109

7 Conclusions and Future Enhancements **111**
7.1 Future Enhancements 112

References **127**

List of Publications Based on the Research Work **128**

List of Tables

2.1 Summary of the Review 36

3.1 Simulation Parameters 53
3.2 Path Reliability for Different Node Reliability and Levels 53
3.3 Reliability of Node Disjoint Multipath Network for Different Node Probability 54

4.1 Simulation Parameters 67
4.2 Notations of EENDMRP Path Selection Criteria 68
4.3 Improvement in Average Energy Spent 71
4.4 The Effect of Transmission Range on Node Residual and Average Energy Spent 72

6.1 NIST Guidelines for Public-Key Sizes with Equivalent Security Levels 104
6.2 Energy Spent (in J) in Public Key Communication overhead in EENDMRP . 109
6.3 Digital Signature Size Ratio between RSA and ECDSA 109

List of Figures

1.1 Block diagram of a Sensor Node 3
1.2 Classification of Energy Efficient Routing Protocols 12
1.3 Traffic Distribution in the Network 16

3.1 Node disjoint Multipath Network 44
3.2 Reliability of a Single Path with Varied Data rate 50
3.3 Reliability of a Single path and Multipath with Equal Data rate in the Network 51
3.4 Reliability of Multipath Routing with Varied Data rate and Number of Nodes 51
3.5 Reliability of Multipath Routing ($\gamma = 0.5$) 52
3.6 Reliability of Multipath Routing ($\gamma = 2$) 52
3.7 Path Reliability When the Node Probability is 0.5 55
3.8 Path Reliability When the Node Probability is 0.5, 0.7 and 0.9 55
3.9 Path Reliability When the Node Probability is 0.5, 0.7 and 0.9 56
3.10 Reliability of Node Disjoint Multipath Network when Node Probability is 0.5 56
3.11 Reliability of Node Disjoint Multipath Network when Node Probability is 0.7 57
3.12 Reliability of Node Disjoint Multipath Network when Node Probability is 0.9 57

4.1 Formation of Stages in the Network 60
4.2 Format of Route CONstruction (RCON) Packet 61
4.3 Format of Node Routing Table 61
4.4 Route Construction Phase 62
4.5 Route Construction Phase in EENDMRP 66
4.6 Effects of Transmission Range on Number of Paths 69
4.7 Effect of Number of Nodes on Total Energy Spent 70

4.8 Effects of Transmission Range on Average Energy Spent 71
4.9 Effects of Number of Nodes on PDF 73
4.10 Variation of Average End-to-End Delay with Number of Nodes 74
4.11 Comparison of End-to-End Delay Variation with Number of Nodes in EENDMRP 75
4.12 Variation of NRL with Number of Nodes 76
4.13 Comparison of NRL Variation with Number of Nodes in EENDMRP 77
4.14 Variation of Average Energy Spent with Number of Nodes 79
4.15 Comparison of Network Lifetime Variation with Number of Nodes 80

5.1 Comparison of Variance in the Residual Energy Levels in AOMDV 88
5.2 EENDMRP with Ratio Based Load Sharing 89
5.3 EENDMRP with Statistically Based Load Sharing 90
5.4 Variation in the Residual Energy Levels with Number of Nodes 90
5.5 Lifetime in AOMDV and EENDMRP with Load Sharing 91

6.1 Node Disjoint Multipath 107
6.2 Variation of Energy Consumption of RSA and ECDSA with the public key size 108

List of Abbreviations

ADC	: Analog-to-Digital Converter
AODV	: Ad Hoc On demand Distance Vector
AOMDV	: Ad Hoc On demand Multipath Distance Vector
ATM	: Asynchronous Transfer Mode
BS	: Base Station
CRE	: Current Residual Energy
CTS	: Clear To Send
CMRP	: Concurrent Multipath Routing Protocol
DARPA	: Defense Advanced Research Projects Agency
DoS	: Denial of Service
ECC	: Elliptic Curve Cryptography
ECDSA	: Elliptic Curve Digital Signature Algorithm
EDM	: Explicitly Disjoint Multipath
EENDMRP	: Energy Efficient Node Disjoint Multipath Routing Protocol
ERMR	: Energy-efficient and Reliability-ensured Multipath Routing
FQL	: Filled Queue Length
FML-MP	: Fuzzy Maximum Lifetime Multi-Path
GPS	: Global Positioning System
LIEMRO	: Low-Interference Energy-Efficient Multipath Routing Protocol
LWIM	: Low Power Wireless Integrated Micro sensors
MAC	: Medium Access Control

List of Abbreviations (cont...)

MANET	: Mobile Ad Hoc Networks
NDMLNR	: Node Disjoint Multipath Routing Considering Link and Node Stability
NRL	: Normalized Routing Load
NC	: Node Cost
PDF	: Packet Delivery Fraction
PNDMSR	: Power-aware Node-Disjoint Multipath Source Routing
PP	: Primary Path
PC	: Path Cost
QoS	: Quality of Service
RCON	: Route CONstruction
RERR	: Route Error
RFTM	: Reliable Fault-Tolerant Multipath
RREP	: Route REPly
RREQ	: Route REQuest
REC	: Rate of Energy Consumption
SMRP	: Sub-branch Multipath Routing Protocol
USM	: Ubiquitous Structural Monitoring
WINS	: Wireless Integrated Network Sensors
WMSN	: Wireless Multimedia Sensor Network
WSN	: Wireless Sensor Network

Nomenclature

N	: Total number of nodes in the network
L	: Total number of links in the Network
K	: Number of paths
k	: Number of node disjoint multipaths
m	: Number of nodes in each node disjoint path
RE_j	: Residual Energy of j^{th} node, $j = 1, 2, ..., m$
RE^{τ}	: Residual Energy threshold
E_{tx}	: Energy required to send one packet of data
E_{rx}	: Energy required to receive one packet of data
P	: Probability
χ	: Probability of k number of node disjoint sets
P_k	: Probability of k number of multiple paths
P_{knd}	: Probability of k number of node disjoint paths
λ	: Data Rate
Tr	: Transmission Range
R	: Reliability
γ	: Criticality Factor
U	: Number of levels in redundancy
V	: Number of nodes in each level
H	: Number of hops in each level
St_i	: i^{th} Stage
E_{diff}	: Energy difference

Nomenclature (Cont...)

Pa_i	: i^{th} Path
pkt_{ts}	: Number of packets to send
P_{key}	: Public key
d_{sign}	: Digital Signature
$H(M)$	: Message Digest
p, q	: Prime Numbers
Q_S	: ECDSA Source Node Public Key
$(r1, r2)$	: ECDSA Digital Signature

Chapter 1

Introduction

The Defense Advanced Research Projects Agency (DARPA) USA, in early 1980s supported the initial research in wireless sensor network. It motivated researchers by continuing to fund a number of prominent research projects like Smart Dust, NEST etc. commonly regarded as the cradles of sensor network research. The type of applications considered by these projects led to a de facto definition of a wireless sensor network as a large-scale (thousands of nodes, covering large geographical areas), wireless, ad hoc, multi-hop, unpartitioned network of homogeneous, tiny (hardly noticeable), mostly immobile (after deployment) sensor nodes that would be randomly deployed in the area of interest (Kay and Mattern 2004).

The wireless sensor network is also defined as, "is a distributed, multi hop, self-organized network consisting of large number of autonomous, tiny sensor nodes deployed in a phenomena to observe or to sense and communicate the sensed data to the destination node".

1.1 Preliminaries

Due to advances in wireless communications and electronics over the last few years, the development of networks of low-cost, low-power, multifunctional sensors has received increasing attention. The research in Wireless Sensor Network (WSN) is multidisciplinary. It contributes to a variety of open issues in application domain, hardware, communication and networks in order to implement an efficient system. Recent advances in the micro electro mechanical devices with low power, short range transceiver, processor with low capacity and a limited power unit contributed in designing sensor node (Akyildiz et al. 2002). WSN is a variant of Mobile

Ad hoc NETworks (MANET) consisting of a finite number of tiny, autonomous devices called wireless sensor nodes. Basic features of sensor networks are:

- Dense deployment
- Self-organizing capabilities,
- Short range broadcast communication
- Co-operative effort of sensor nodes
- Multi hop routing
- Frequently changing topology due to fading and node failures
- Limited energy, transmission power, memory and computing power

1.1.1 Technical Details of Sensor Node

A WSN consists of hundreds or thousands of tiny sensor nodes. These sensor nodes have the capability to communicate among themselves to make the information reach the destination in a single hop or in multiple hops. Sink is a common destination node for all the sensor nodes in the network. A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data (Al-Karaki and Kamal 2004). Sensor nodes are usually scattered in a phenomena, which is an area of interest for observation and study. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment.

Basically, a sensor node comprises of a sensing unit, processor, transceiver, mobilizer, position finding system and power units. Some of the units in sensor node are optional. The optional units are identified in the Figure 1.1 with dotted boxes.

- Sensor

  A sensor is an electromechanical device that measures a physical quantity in the environment such as temperature, pressure, etc. These continual analog signals sensed by the

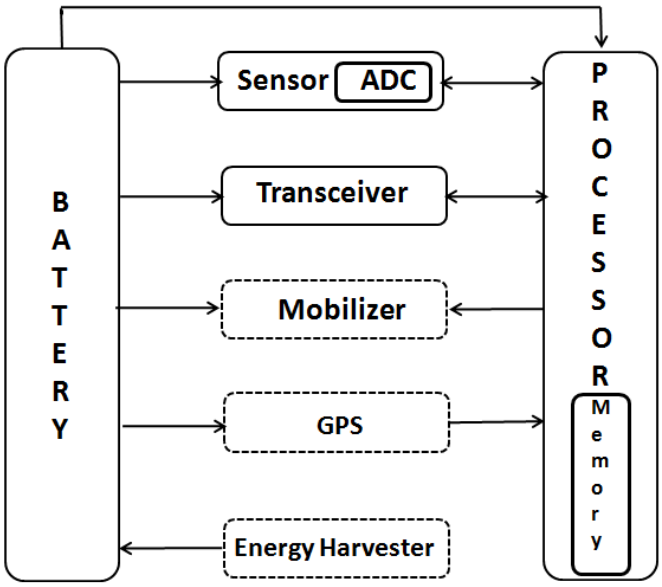


Figure 1.1: Block diagram of a Sensor Node

sensors are digitized by an Analog-to-Digital Converter (ADC) and sent to destination node.

- Processor

  It is a low power processor with an operation speed ranging between 4MHz and 8MHz. This processor has an internal flash memory capable of storing operating system and application code.

- Transceiver

  The functionalities of both transmitter and receiver are combined into a single device known as a transceiver. The operational states are transmit, receive, idle and sleep. WSNs use license free communication frequencies such as 173, 433, 868 and 915 MHz and 2.4 GHz. It includes a digital direct-sequence spread spectrum baseband modem with 30 to 250 Kbps data rate.

- Power Unit

  The sensor node consumes power for sensing, communicating and data processing. More energy is required for data communication than any other process. Usually, a sensor node has two 3.3 V battery source packed in a unit.

- Mobilizer

  It supports sensor nodes to move from one location to another location. It is a type of motor which supports node mobility.

- Position Finding System

  Location of the sensor nodes is identified in the network using the position finding system or Global Positioning System (GPS).

There are a number of sensor node manufacturers in the market today. Two commonly used sensor node products are the MicaZ and the T-Mote Sky. While sharing a number of common features, the two devices are built around different microcontrollers and are arranged in considerably different configurations. In 1996, Low Power Wireless Integrated Microsensors (LWIMs) were produced by UCLA and the Rockwell Science Center. By using commercial, low cost CMOS fabrication, LWIMs demonstrated the ability to integrate multiple sensors, electronic interfaces, control and communication on a single device. LWIM supported over 100 Kbps wireless communication at a range of 10 meters using a 1 mW transmitter.

In 1998, the same team built a second generation sensor node the Wireless Integrated Network Sensor (WINS). Commercial WINS from Rockwell Science Center consists of a processor board with an Intel Strong ARM SA1100 32-bit embedded processor (1 MB SRAM and 4 MB flash memory), a radio board that supports 100 Kbps with adjustable power consumption from 1 to 100 mW, a power supply board and a sensor board. These boards are packaged in a 3.5" x3.5"x3" box .

In 2001, the MICA family of sensor nodes was released. This family included Mica2, Micaz etc. Though the MICA has 8 bit 4 MHz micro controller, it offered enhanced capabilities in terms of memory and radio compared to the preceding products. It consumed 200 mw in the active state and 0.8 mw in sleeping state.

Specically, Mica was designed with 4 KB Ram, 128 KB flash and a simple bit-level radio using RFM TR1000 that supported up to 40 Kbps with almost the same power consumption as the radio module on WeC sensor node. Mote architecture allowed several different sensor boards, or a data acquisition board, or a network interface board to be stacked on top of the main processor/radio board. The basic processor/radio board was approximately one inch by two inches in size.

1.1.2 Wireless Sensor Networks: Technical Challenges and Requirements

WSN design is motivated and influenced by one or more of the following technical challenges (Vehbi et al. 2010):

- Massive and random deployment

  A WSN is an application dependent research domain, where most applications demand large number of sensor nodes (few hundreds to thousands)(Khan et al. 2009). The deployed sensor nodes randomly organize their network connectivity without centralized infrastructure.

- Data redundancy

  In WSN, the large number of sensor nodes leads to high density in the network. Its observations are highly correlated in the space domain. So, the data redundancy among the sensed data is common in WSN.

- Limited resources

  WSN design and implementation are constrained by four types of resources:

  1. Energy
  2. Computation Power
  3. Memory
  4. Bandwidth

  The tiny nature of sensor nodes is bound to have limited battery power supply. At the same time, their memories are limited and can perform only restricted computational functionality. The bandwidth in the WSNs is low because of its limited data rate in the network.

- Ad hoc architecture and unattended operation

  The self-organized topology among the randomly deployed sensors is ad hoc in nature. Sensor nodes deployed in the phenomena are unattainable by the humans in most of the applications.

- Dynamic topologies and environment

  The network topology is ad hoc in a randomly deployed WSN. It is unpredictable, though the nodes are immobile. The network topology changes due to exhaust of sensor node's battery. It can also change due to harsh environmental changes in the weather like, heavy wind, storm, hurricanes etc. It relocates the sensor position from its initial position. These harsh environmental conditions and dynamic network topologies may cause a portion of the sensor network to be disconnected.

- Error Prone Wireless Medium

  In wireless medium, the risk of jamming and potential for interference is high. The speed and the viability of the wireless signals drop as more and more users use the same frequency. The various types of unauthorized access in the wireless network like malicious node's behaviour, man in the middle attack etc. makes the network to misbehave.

- Quality of Service (QoS)

  The wide variety of applications envisaged in WSNs will have different QoS requirements and specifications (Nandi and Yadav 2011). The QoS is the ability of the network to result in predictable performance. The performance may be availability of high bandwidth (throughput), low delay latency (delay) and low error rate. In real time WSN applications, it is important to maintain jitter and low rate of out-of-order packets arrival.

- Diverse Applications

  WSN has landmarked its importance in a variety of applications (Kaseva et al. 2011). Designing the application specific WSN is more appropriate than generalized WSN. The WSN should meet the technical and performance requirements of the specific applications.

- Security Requirements

  Security is a technical issue to be considered in WSN (Meghdadi et al. 2011). In WSN, passive or active attacks may be seen. The passive attack like denial of service leads to misbehaviour of the network. Notification of erroneous information to the neighbouring

nodes is another passive attack. It leads to degrading the network performance through drastic decrease in network lifetime or excessive usage of node energy etc. The active attacks like modifications of data sent in the intermediate node lead to erroneous data reception at the destination.

- Integration with Internet and other Networks

  It is of fundamental importance for the commercial development of sensor networks to provide services that allow querying the network to retrieve useful information from anywhere and at any time (Akyildiz et al. 2002). For this reason, future wireless multimedia sensor networks (WMSN) will be remotely accessible from the Internet and will therefore need to be integrated with the IP architecture (AlNuaimi et al. 2011). In the future interconnected world, multiple sensors will be able to dynamically exchange information all over the world in semantically interoperable ways. Both the traditional WSN approach and the future WSN can coexist at the same time. There may be applications where more static nodes and dynamic entities can collaborate towards a common goal (Roman et al. 2009).

1.1.3 Wireless Sensor Network Applications

The WSN marked its importance in a variety of applications (Al-Karaki and Kamal 2004). The WSN applications can be classified into two categories: (i) Monitoring and (ii) Tracking (Yick et al. 2008). Monitoring applications include indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans and vehicles. Below we describe a few example applications that have been deployed and tested in the real environment.

- Outdoor/Environmental Monitoring

  In a disaster management setup, a large number of sensors can be dropped by a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas and making the rescue crew more aware of the overall situation.

- Health and Wellness Monitoring

  The medical sensor network system integrates heterogeneous devices, some wearable on the patient and some placed inside the living space (Virone et al. 2006). Together they inform the health care provider about the health status of the resident. For example, some of them are devoted to continuous medical monitoring for degenerative diseases like Alzheimers, Parkinsons or similar cognitive disorders.

- Inventory Location Monitoring

  Large number of sensors are deployed aiming to help increase the efficiency of a humanitarian distribution center by providing higher freight and resource visibility and state monitoring ability. Such architecture integrates sensors, passive and active RFID systems into a unified WSN backbone (Yang et al. 2011).

- Factory and Process Automation

  WSN is one of the most important industrial drives to its commercial success for factory automation applications. WSN is used in supervisory control and data acquisition. It is also used for diagnostics, testing, maintenance and machine control in the industries (Zhuang et al. 2007).

- Seismic and Structural Monitoring

  WSN can be used to show performance necessary for general seismic observation and vibration measurement of buildings. It may also be used in detecting the damages and monitoring in aircrafts, bridges, ships etc (Kurata et al. 2008).

- Tracking Objects, Animals, Humans and Vehicles

  Sensors are distributed randomly, in a large scale region to be monitored. The possible scenarios can be border control, battle field surveillance, traffic flow measuring or animal monitoring, etc. However, in many tracking applications, the motion characteristics of the object under tracking may vary with time due to the uncertainty and unpredictability in the target motion model (Blair and Bar-Shalom 1996). Moreover, different types of objects may have different kinds of motion characteristics (Yang and Feng 2006).

1.2 Routing in Wireless Sensor Networks

Routing plays an important role in communicating the data from source to destination in networks. In routing, the routes may be predetermined or found as and when required between the source and destination. Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like MANETs or cellular networks (Akkaya and Younis 2003)(Al-Karaki and Kamal 2004). In the first place, the overhead of ID maintenance is high, due to the relatively large number of sensor nodes. Hence it is difficult to build a global addressing scheme. Thus the traditional IP based protocols may not be suitable in WSN. In WSNs, sometimes getting the data is more important than identifying the nodes that sent the data. This is because, WSN is a data centric network rather than address centric network as in MANETs. Secondly, sensor nodes are tightly constrained in terms of energy, processing and storage capacities. Thus, they require careful resource management. Thirdly, generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization.

1.2.1 Routing Protocol Design Issues

The routing protocols designed for the MANETs are not well suited for the WSN because of the reasons discussed above. It hints the necessity of designing a dedicated routing protocol, which consumes resources like energy and bandwidth very effectively. While designing dedicated energy efficient routing protocol, the following important design issues are to be considered. They are (Al-Karaki and Kamal 2004):

- Network Model

  In many WSN applications, the network model follows many sources and one destination (sink node). However, some typical applications may have many sources and multiple-sink nodes. In multiple-sink node scenarios, selecting a sink node from the available multiple nodes is also an important design factor in the routing protocols.

- Node Deployment

  It is an application dependent operation affecting the routing protocol performance, which can be either deterministic or randomized.

- Node/Link Heterogeneity

  The existence of heterogeneous set of sensors gives rise to different types of data to be routed in the same network. It has created many technical problems such as sending different kinds of sensed data to a common sink node or specific kind of sink nodes, etc. These types of problems need to be overcome (Jin et al. 2009).

- Data Reporting Model

  Data sensing, measurement and reporting in WSN is dependent on the application and the time criticality of the data reporting. Data reporting can be categorized as time-driven (continuous), event-driven and query-driven.

- Energy Consumption without Losing Accuracy

  The energy-conserving mechanisms of data communication and processing in the WSN are of utmost necessity.

- Scalability

  WSN routing protocols should be scalable enough to meet the application requirements without degrading the quality of service.

- Network Dynamics

  Mobility of sensor nodes is necessary in many applications, though most of the network architectures assume stationary sensor nodes. In some applications, both source and destination nodes are mobile.

- Fault Tolerance

  The overall task of the sensor network should not be affected by the failure of sensor nodes.

- Connectivity

  Sensor nodes are expected to be highly connected. Connectivity depends on the density and distribution of nodes.

- Coverage

  In WSNs, a given sensor's view of the environment is limited both in range and in accuracy. It can only cover a limited physical area.

- Quality of Service (QoS)

  Data should be delivered within a certain period of time. However, in a good number of applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than quality of data sent. Hence, the energy-aware routing protocols are required to capture QoS requirement.

- Data Aggregation

  Data aggregation is the technique to collect data from different sources. It eliminates the data redundancy in the received node and forwards it to sink or to neighbouring nodes.

- Transmission Media

  In a multi-hop WSN, the communication nodes are linked by a wireless medium. The traditional problems associated with a wireless channel(e.g. fading, high error rate) may also affect the operation of WSN. One approach of Medium Access Control (MAC) design for WSNs is to use TDMA based protocols that conserve more energy as compared to contention based protocols like CSMA (e.g. IEEE 802.11).

- Security

  The WSN may operate in a hostile environment. The routing in such environments require low-latency, high survivability and secure networks. High intrusion detection also is needed.

1.2.2 Energy Efficient Routing Protocol Classification

These design issues made many researchers to propose new algorithms for routing the data in sensor networks. These routing mechanisms have considered the characteristics of sensor

nodes along with the application and architecture requirements. The energy efficient routing protocols are broadly classified as network based, protocol operation based , based on number of paths and application based as shown in the Figure 1.2.

- Network Based Classification

  The network based routing protocols are further categorized based on mobility, network type and type of communication.

  In a static network, both the sensor nodes and the sink nodes are immobile whereas in a dynamic network, either the sensor node or the sink node or both the sensor node and sink node are mobile. Based on mobility characteristic of the nodes, the routing protocols can be classified as static network based routing protocols and dynamic network based routing protocols.

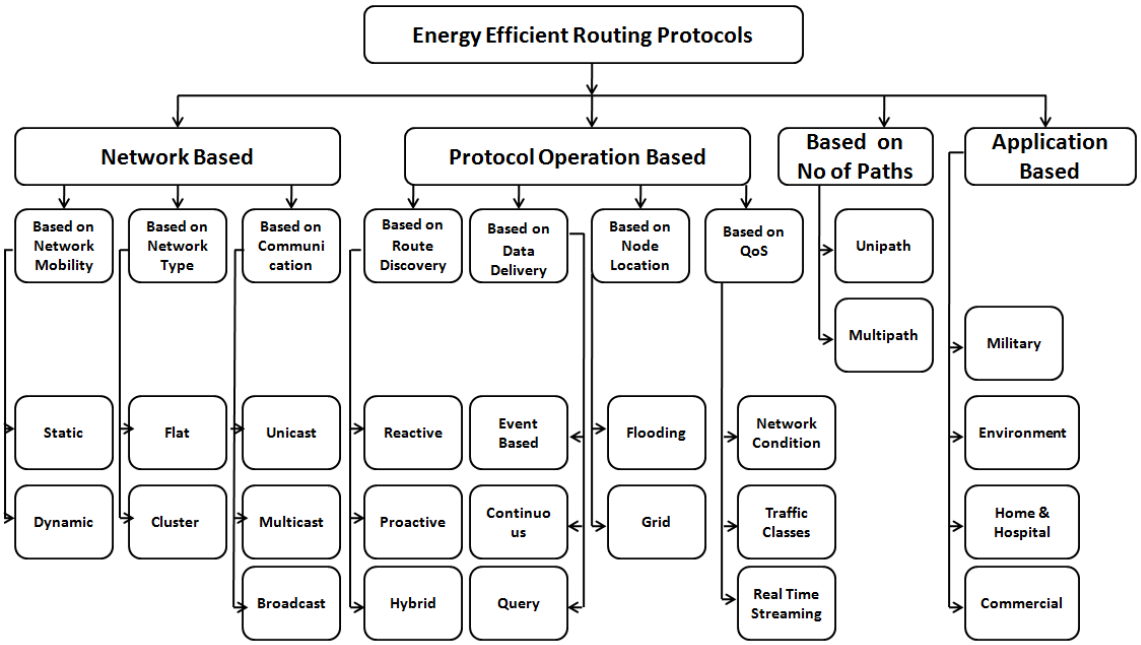


Figure 1.2: Classification of Energy Efficient Routing Protocols

The routing protocols can also be classified on the basis of type of network as flat or cluster (Hierarchical). In flat routing protocols, all the nodes in the network are treated as equal (Intanagonwiwat. et al. 2000; Braginsky and Estrin 2002; Chu et al. 2002). The sensor node sends the data to sink node through multiple hops. A hierarchical routing protocol is an approach for WSNs, where some of the nodes are more powerful than oth-

ers. In hierarchical protocols (Heinzelman et al. 2000; Lindsey and Raghavendra 2002; Manjeshwar and Agrawal 2001; Younis et al. 2002), different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be combined (aggregated). The node with highest available network resources is selected as a cluster head. The cluster head does the aggregation and forwards data to the sink node.

The routing protocols based on the type of the communication are classified as unicast, multicast and broadcast. The applications where direct data transmission from sensor node to sink node follows is unicast (Sadagopan 2003); whereas in multicast, a set of nodes among the neighbouring nodes are selected to route the data from the source node to sink node based on the multicast node selection criteria (Intanagonwiwat. et al. 2000; Chu et al. 2002). In broadcast type of protocols, the node broadcasts the data or message to all its neighboring nodes without any constraint (Braginsky and Estrin 2002; Schurgers and Srivastava 2001). The neighbouring node transmits the received data or message until it reaches the destination.

- Protocol Operation Based Classification

  The routing protocol is classified on the basis of protocol operation as, route discovery based, data delivery model based, node location based and QoS based.

  The route discovery based routing protocol, in turn, is classified as proactive, reactive and hybrid. In the proactive routing protocols, each node maintains a routing table, which attempts to maintain consistent, up-to-date routing information to every other node in the network (Jacquet et al. 2002). This is done in response to change in the network by having each node update its routing table and propagate the updates to its neighbouring nodes. In proactive protocols, when a packet needs to be forwarded, the route is already known and can be immediately used.

  In the reactive routing, the routes are discovered only when a source node needs to send the data to the sink node (Park and Corson 2004; Toh 1997). Here, the route discovery and route maintenance are two main procedures.

  The hybrid routing protocol divides the routing scenario into a number of zones (Haas et al. 2003). The hybrid protocols combine the advantages of proactive and reactive approaches by maintaining an up-to-date topological map of a zone, centered on each

node. Within the zone, routes are immediately available. The hybrid protocols employ a route discovery procedure, which can benefit from the local routing information of the zones when the destination node is outside the zone.

The data delivery based routing protocols are classified as continuous, event based and query based. The continuous data delivery model periodically sends the sensed data to the sink node (Ye et al. 2002; Ko and Vaidya 1998; Heinzelman et al. 2000). The sensor nodes periodically enable the transmitter to send the data to the sink node. The event-driven data model sends the data to the sink node directly or through its neighbouring nodes (Yu et al. 2001). The node senses predetermined attributes due to the occurrence of a certain event.

In the query-driven models, the sink node raises a query for certain data. The source node is intimated of the data request through messages. The source node sends the requested data to the sink node (Akkaya and Younis 2003; Felemban et al. 2006).

The node location based routing protocols are classified as flooding and grid routing. An agent based flooding is a derivative of naive flooding. Each agent carries the location of source. Then, at each step, the packet is forwarded to a neighbour with least deviation on the forward direction using location information of neighbouring nodes (Shokrzadeh and Haghighat 2007). In grid based routing, the phenomenon is divided into a number of grids. The grid information helps to identify location of nodes easily and help in routing.

The QoS addressing routing protocols are classified on the basis of network conditions, traffic classes and real time streaming. The routing protocols based on the network conditions, test the availability of network resources among the neighbouring nodes (Savidge et al. 2005) to route the data.

The routing protocol based on traffic classes route the different types of data like temperature, pressure, humidity, moving image, still image etc. based on its traffic type and priorities (Hu and Kumar 2003). The routing protocols may consider the real time data to route. It provides three types of real-time communication services, namely, real-time unicast, real-time multicast and real-time anycast (Felemban et al. 2006; Setton et al. 2005).

- Application Based Classification

  The WSN has diversified applications in various fields (Ronan et al. 2008). The routing protocol selected for one kind of applications may not be suitable for other types.

  The routing protocols based on the applications are classified as military, monitoring, home, hospital and commercial applications. Each application has its own requirement like data reporting. The data reporting can be periodical or triggered by events. In military applications, the routing protocols like to have continuous sensed data for decision making. The military applications involve military situation awareness sensing intruders on bases, detection of enemy units movements on land/sea, chemical/biological threats and battlefield surveillance (Carlos F et al. 2007).

  The habitat and environment monitoring applications like monitoring rare species in the forest, gathering information in a disaster area, forest fire detection etc. are typical applications of WSN. The home and hospital applications have small wireless sensors attached to the patient body; measure vital sign data and transmit them via the established sensor network to an external observation unit.

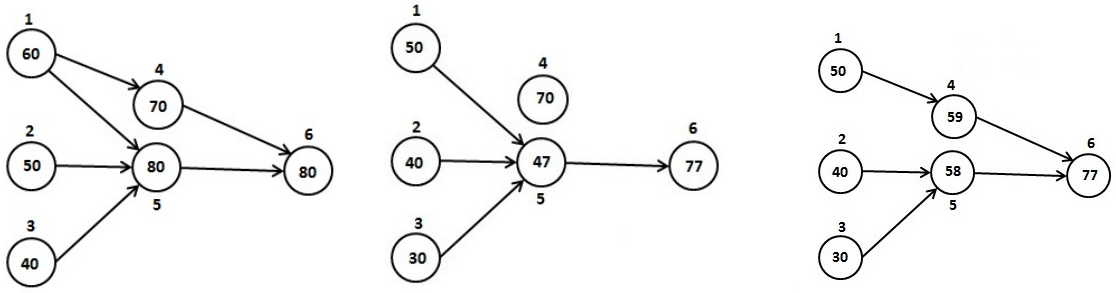
  The commercial applications are automotive tyre pressure monitoring, active mobility, coordinated vehicle tracking, airports smart badges and tags and wireless luggage tags. In monitoring applications, when the event is detected or triggered the data must be sent to the base station.

- Number of Paths Based Routing Protocols

  The routing protocols can be classified based on the number of paths used for data routing. It can be classified as unipath or multipath routing. In unipath routing, the source node identifies a best path between source and destination and routes the data through it. In multipath routing, multiple number of paths are identified between source and destination. The sensed data is sent through these multiple paths to the destination.

1.3 Motivation

WSN is a resource constrained network. Routing in a resource constrained network is a challenge (Zoumboulakis and Roussos 2011). Enhancing the network lifetime by effective re-



(a) (b) (c)

Figure 1.3: Traffic Distribution (a) Initial Network (b)Network Without Traffic Distribution (c) Network With Traffic Distribution

source utilization and maintaining the performance of a routing protocol, makes it still more challenge able. The following example illustrates how the uniform node energy could be used effectively and increase the network lifetime. Consider a network of six nodes. All the nodes can send data to the sink node. The transmission energy cost and reception energy cost in the node is 1J/ Data Packet and 0.1J/Data Packet respectively. The initial energy in all the nodes is as shown in Figure 1.3(a). In Fiugre 1.3(a), the circle represents a sensor node, the number outside the node indicates the node ID and the number inside the node indicates residual energy of that node. 10 packets from nodes 1, 2 and 3 are sent to the sink node through node 5. The maximum traffic passes through node 5. So, the energy depletion in node 5 is more than that in other nodes. The residual energy in all the nodes after the transmission is shown in Figure 1.3(b). When the nodes 2 and 3 send the traffic through node 5 and node 1 sends the traffic through node 4, the residual energy in all the nodes is as shown in Figure 1.3(c). This study illustrates that uniform distribution of energy consumption among the nodes in the network is very much necessary to enhance the network lifetime.

Figure 1.3(b) shows that traffic through the node or the rate of energy consumption is an important factor to be studied while devising energy efficient routing protocols. The uniform distribution of the traffic among all the possible paths between the source and destination makes the uniform and efficient usage of the node residual energy. Thus spending the energy uniformly among sensor nodes in the multiple paths, increases the network lifetime. It is also seen that the network lifetime is long when the variance in the residual energy of the nodes is less. These facts motivate us to design an energy efficient protocol for WSNs.

1.4 Scope of the Research Work

Enhancing the operational lifetime of the network and providing secure data transfer environment is the major issue in the WSNs (Chang and Tassiulas 2004; Yousefi et al. 2011). Recent researchers have attempted to increase the network lifetime through effective and energy efficient routing mechanisms (Batra et al. 2011; Hung et al. 2011). In the recent past, many researchers proposed the multipath routing protocols to increase the network operational lifetime (Ghica et al. 2010; Heikalabad et al. 2011). This work focuses on enhancing the network operational lifetime of the network by proposing the energy efficient node disjoint multipath routing protocol.

In the proposed Energy Efficient Node Disjoint Multipath Routing Protocol(EENDMRP), the node disjoint paths are identified between the source and the sink node. The primary path among the node disjoint paths from the source is selected based on the maximum ratio of residual energy to rate of energy consumption and minimum filled queue length path. The EENDMRP is a flat, event driven, proactive and node disjoint multipath routing protocol. The security is provided in the data transfer using the digital signature. Most of the WSN applications have event driven data reporting model requirement. The multipath routing protocols perform better in terms of uniform energy usage among the sensor nodes in the network. Since the data traffic in the network is distributed among the multiple paths in the network, the network lifetime is increased.

To make it more energy efficient, the protocol also looks at the filled queue of each sensor node. A node with many messages waiting in its queue has already committed to spend its energy. This fact is also considered while evaluating the residual energy. This approach makes the calculation of residual energy more accurate.

1.5 Outline of the Thesis

This thesis is organized into eight chapters. A panoramic view of each chapter is given below:

In literature review chapter (Chapter 2), we discuss the state of art of the techniques and protocols to route the data between the source and sink node through node disjoint multipath routing protocols. The lacunae of related node disjoint multipath routing protocols are also

presented. At the end of chapter 2, the possible solutions to address the lacunae in the state of the art routing protocols are presented.

In analytical model for node disjoint multipath routing protocols in WSNs (Chapter 3), we discuss the route discovery model for node disjoint multipath routing protocols. We designed the lifetime analytical model for data transfer phase and route redundancy model for route maintenance for node disjoint multipath routing protocol in WSNs. The work presents the evaluation of the analytical model.

In energy efficient node disjoint multipath routing protocol for WSNs (Chapter 4), we present the proposed Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) for WSNs. We propose the efficient route discovery, data transfer and route maintenance in the routing protocol. The proposed protocol evaluates important routing metrics like average end-to-end delay, Packet Delivery Fraction (PDF), Normalized Routing Load (NRL), average energy spent and network lifetime. The proposed protocol is compared with ad hoc on demand multipath routing protocol.

In Effective Load Sharing Mechanism in EENDMRP (Chapter 5), the work presents effective load sharing mechanism for node disjoint multipath routing protocol. New metrics like residual energy variance among the nodes is also taken into account to evaluate the effectiveness of the load sharing mechanism in the proposed EENDMRP.

In digital signature based crypto system for node disjoint multipath routing protocol (Chapter 6), the work presents the proposed crypto system for node disjoint multipath routing protocol. It discusses the crypto system susceptibility to common routing threats in EENDMRP. It also discusses the correctness of the proposed digital signature based crypto system in EENDMRP.

In conclusions and future enhancements (Chapter 7), the conclusions of the research work are drawn by highlighting the contributions of the work and research findings. Future enhancements to this work are also presented in this chapter.

Chapter 2

Literature Review

The WSN contains hundreds or thousands of short range, low cost and tiny sensor nodes in the network. The WSN is formed without the aid of any established infrastructure. A large amount of data can be collected from a number of sensor nodes. Distributed sensing in the WSN provides the robustness and improves the fault tolerance. All the sensor nodes in the network send data to the common destination called base station or sink node. A sensor node in the network may send the data to the sink node directly or it may take multiple hops to reach the sink node.

2.1 Multipath Routing Protocol

Routing the sensed data from the source to sink node in a resource constrained environment such as WSNs is still a challenge. An optimal path is selected based on the metrics such as the gradient of information, the minimum hop, minimum transmission cost, high residual energy etc. to route the data (Zheng et al. 2009; Cheng et al. 2010; Erdene-Ochir et al. 2010; Jin et al. 2009) between source and destination. The optimal path between the source and destination is selected by the routing protocols to satisfy the resource constraints such as energy, bandwidth and computation power. Selecting an optimal path between the source and destination and sending the data through that path may not increase the lifetime of the network. The energy usage in such an approach is not as efficient as that in the multi-path routing approaches.

The multi-path routing protocols (Ganesan et al. 2002) select the available multiple paths between the source and destination. The overhead of route discovery in multi-path routing is

much more than that of single-path routing. On the other hand, the frequency of route discovery is much less in a network which uses multi-path routing. Since, the network can still operate even if one or a few of the multiple paths between a source and a destination fail, it is commonly believed that using multipath routing results in a higher throughput. Since, multipath routing distributes the load better, the overall throughput would be higher (Ganjali and Keshavarzian 2004).

2.2 Advantages of Multipath Routing Protocol

- Smoothing out the traffic
- Alleviating the network congestion
- Improving the fault tolerance
- Load balancing
- Supporting quality of service (QoS)
- Reducing the end-to-end delay
- Reducing the frequency of route discoveries
- Improving the network security
- Reduction in energy consumption per unit time
- Extending the network lifetime

2.3 Classification of Multipath Routing Protocol

The multipath routing protocols are classified into four major categories. They are based on:

- Multipath Construction Initiated
- Multipath Generation Technique
- Data Transmission Technique

- Traffic Sharing Technique

2.3.1 Multipath Construction Initiated

In the multipath routing protocol, the multiple paths between any source and destination in the network are needed to send the data. The identification or generation of multiple paths between any source and destination can be initiated by the sensor node which would communicate the data to the sink node; or the route identification or generation can be initiated by the sink node (Challal et al. 2011).

The multipath construction initiated technique classification can be further classified as source initiated and destination initiated route discovery mechanism.

- Source Initiated Route Discovery Mechanism

  Radi et al. (2010) proposed a multipath routing protocol. To start route establishment process, a route request packet (Route Request) is sent from the source to the sink. At each node, the best next hop neighbour is selected according to the cost function.

- Sink Initiated Route Discovery Mechanism

  Lou (2005) proposed an Efficient N-to-1 Multipath Routing Protocol in WSN. It is a sink initiated routing protocol. The N-to-1 multipath discovery protocol is based on the simple flooding initiated at the base station.The route discovery packets are flooded in the network. This flooding in the route discovery process is to find multiple node-disjoint paths from every sensor node to the common destination (i.e. the sink node) simultaneously.

  Vidhyapriya and Vanathi (2007) proposed an adaptive multipath routing for WSN. In this protocol, the sink node starts the multipath path construction phase to create a set of neighbours (i.e. the address of all nodes) that are able to transmit data from the source. During this process, route request messages are exchanged between the nodes. Each sensor node broadcasts the route request packet once and maintains its own routing table.

2.3.2 Data Transmission Techniques

The multipath routing protocols classification based on data transmission techniques can be further classified into consecutive and concurrent data transmission multipath routing protocols.

- Consecutive Data Transmission Multipath Routing Protocols

  In the consecutive data transmission multipath routing protocol, the source node sends part of the data through one of the paths among the multiple paths. The next part of the data is sent through the next path among the multiple paths one after the other (Alwan 2010).

  Radi et al. (2010) proposed Low-Interference Energy-efficient Multipath Routing protocol (LIEMRO) for WSNs. This protocol is mainly designed to improve packet delivery ratio, lifetime and latency, through discovering multiple interference-minimized node-disjoint paths between source node and sink node. In LIEMRO, upon receiving route reply packet at the source node, the first path is formed and is ready to be used. Concurrently with data transmission over the first path, creation of the second route can be started by the source node. This is performed by sending the second route request packet to the sink. To establish a new route, each node's best next hop is the neighbour node which has minimum cost and is not part of any route to the sink.

- Concurrent Data Transmission

  In Concurrent Multipath Routing Protocol (CMRP) (Tsirigos and Haas 2001), the data traffic is split among the number of different paths simultaneously. CMRP is developed for mobile ad hoc networks to improve QoS, reliability, load balance and security.

2.3.3 Traffic Sharing Techniques

The classification of multipath routing protocols based on traffic sharing techniques is further classified as multipath routing protocols with load sharing mechanism and without load sharing mechanism.

- Multipath Routing Protocols with Load Sharing Mechanism

  Alwan (2010) proposed a multipath routing protocol in which source node decodes each data packet of size M bits it receives into M fragments each of size b. It generates another K coding fragments to produce a coding ratio of $M/(M + K)$. This parameter will be determined by the sink depending on the desired reliability required by the source. Selecting high coding ratio increases the reliability of data transmission. The $(M + K)$ fragments are then transmitted as sub-packets $x_1, x_2, ..., x_n$ over n available paths between the source node and the sink, where $\sum_{i=1}^{n} x_i = (M + K)$. The allocation of fragments on each path is determined with a load balancing algorithm. To reconstruct the original packet, at least M fragments should be received by the sink, allowing at most K lost fragments.

  Ghica et al. (2010) proposed a load balancing mechanism using virtual channels to better exploit the nodes in a given stream-pipe, each one using a different sequence of anchor points along the respective bezier curve.

- Multipath Routing Protocols without Load Sharing Mechanism

  Guan and He (2010) proposed an energy efficient multipath routing protocol for WSN. In this the source node sends the data along multiple paths discovered in the route discovery phase to sink node. These multipath routing protocols send the sensed data to the sink node without a dedicated data traffic distribution mechanism (Sarma and Nandi 2010; Marina and Das 2006).

2.3.4 Multipath Generation Techniques

The classification of multipath routing protocols based on multipath generation techniques is further classified as multiple paths, partially-disjoint paths, link-disjoint paths, node-disjoint paths, zone-disjoint paths and primary path routing protocols.

- Partially-Disjoint Multipath Routing Protocols

  Minhas et al. (2009) proposed a Fuzzy Maximum Lifetime Multi-Path (FML-MP) routing algorithm. FML-MP is a partially disjoint multipath routing protocol. A set of π shortest paths p_h^q between source and destination are found using Dijkstra's algorithm,

where $\pi \geq 1$, $h = 1, 2, ..., \infty$ and $q = 1, 2, ..., \pi$. The first shortest path is searched and the nodes lying on that path are assigned a considerably high weight in order to discourage their inclusion in the subsequent path searches. Thus the path search will only resort to a braided path (i.e. inclusion of any of these already used nodes) when there is absolutely no better alternative path available.

- Link-Disjoint Multipath Routing Protocols

  Marina and Das (2006) proposed Ad-hoc On-demand Multi-path Distance Vector (AOMDV) for MANETs. AOMDV is designed to suit either link or node disjoint multipath routing protocol. According to the need, user can choose it either as a link disjoint routing protocol or node disjoint routing protocol. In link-disjoint multipath routing protocols, an intermediate node between the source and destination may be chosen by several routes. But, any link between the source and destination may not be common link among the possible multiple paths. It is a link disjoint multipath routing protocol. AOMDV requires the maintenance of last hop information for every path (in addition to next hop) to generate link disjoint multipaths between source and destination.

- Node-Disjoint Multipath Routing Protocols

  In node disjoint multipaths, except the source and destination node any other intermediate node should not be part of more than one path. Challal et al. (2011) proposed Sub-branch Multipath Routing Protocol(SMRP). It employs a node disjoint multipath selection scheme seeking to enhance the fault tolerance of the network and to conserve the energy of sensors.

  Xiaoming and Tao (2011) proposed an Energy-efficient and Reliability-ensured Multipath Routing (ERMR) algorithm for wireless multimedia sensor networks. In this multiple node-disjoint routing paths are constructed from the source node to the sink node by considering the residual energy of nodes, the local link reliability and the distance between nodes.

- Zone-Disjoint Multipath Routing Protocols

  Oh et al. (2010) proposed Explicitly Disjoint Multipath (EDM) routing protocol for WSN. The EDM is a zone based multipath routing protocol. EDM uses only localized

information exchange based on the geographic routing between neighbouring nodes. EDM builds the distributed K multiple paths requested by an application. EDM removes the flooding overhead used in the multipath discovery process and significantly reduces the signaling overhead compared to the existing multipath routing methods in the densely populated sensor network.

- Primary Path Routing Protocols

  Primary path is the best path among available multiple paths between the source and destination. The multipath routing protocol, initially identifies the primary path and constructs a small number of alternate paths to satisfy link or node disjoint paths. As soon as a failure is detected on the primary path, nodes can quickly reinforce an alternate path without the need for network wide flooding to initiate discovery (Ganesan et al. 2002).

2.4 Related Works in Node Disjoint Multipath Routing Protocol

In the recent past many researchers proposed a number of node-disjoint multipath routing protocols for WSN. These protocols attempted to prolong the network operational lifetime of the WSN. Many multipath routing protocols enhanced the network lifetime through mechanisms like energy efficient techniques, effective fault tolerance mechanisms, high end-to-end reliability, and balance energy consumption among the nodes in the routing.

Vidhyapriya and Vanathi (2007) proposed energy efficient adaptive multipath routing for WSNs. It is a sink initiated multipath routing protocol. The protocol spread the traffic over the nodes lying on different possible paths between the source and the sink, in proportion to their residual energy and received signal strength. The rationale behind traffic spreading is that for a given total energy consumption in the network, at each moment, every node should have spent the same amount of energy. The objective is to assign more loads to under-utilized paths and less loads to over-committed paths so that uniform resource utilization of all available paths can be ensured. The adaptive multipath routing protocol has multipath construction phase, data transmission phase and data aggregation phase.

- Multipath Construction Phase

  In this phase, route request messages are exchanged between the nodes. Initially, sink node broadcasts the route request message to its neighbouring nodes. The route request message contains the following fields: The Source ID, Destination node ID, Packet Sequence Number, Hop Count, Energy Threshold Value and Signal Strength.

- Route Discovery Phase

  Each sensor node broadcasts the route request packet once and maintains its own routing table. When a sensor node disseminates a data packet, it only needs to know its neighbouring node to transfer. It does not need to maintain the whole path information. It is necessary to store the routing information and reduce the overhead of sensor node.

- Data Transfer Phase

  After multiple paths are discovered, the source node begins to transmit data packets with the assigned rates on each path. The initial data rate assignments for the paths may not be optimal for the duration of the connection. The sink node has to redistribute the data rates over paths to optimize the usage of network resources occasionally. In order to detect a path failure, the sink also monitors the inter-arrival delay of data packets on each path. When the delay is above a pre-determined threshold, the sink presumes that the path is broken. If the number of current working paths is equal to or lower than two, the sink will send a RESET message to the source through the optimal path to indicate that the sink starts to re-initiate the path search phase. Otherwise, the sink readjusts the data rate allocation over other functional routes. The source node uses a different path every time to extend the lifetime of the network system based on the information available in the routing table. Data is cached in the sender until an ACKnowledment (ACK) is received from the receiver. If no ACK is received within a timeout period, an error report is generated and the data will be sent back to the original source of this data in order to retransmit.

- Data Aggregation

  All nodes will aggregate data except the node that sensed the event (source node) and generated the data. When a node receives data packets from its different lower level

nodes, it will rearrange the packet(s) by the Sink ID field of packet.

The adaptive multipath routing protocol is a sink initiated on demand kind of routing protocol. The control message used is high, because, the route reply packet sent is communicated by the sink to source node. In dense and large WSNs, it consumes high energy in route discovery phase. The traffic through the node is not taken into consideration to evaluate the node's residual energy.

AOMDV is proposed by Marina and Das (2006). It is a source initiated, reactive (Node/link) disjoint multipath routing protocol. AOMDV extends the AODV protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths so computed are guaranteed to be loop-free and disjointed. Primary design goal behind AOMDV is to provide efficient fault tolerance in the sense of faster and efficient recovery from route failures. AOMDV finds routes on demand using a route discovery procedure. The core of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjointed. AOMDV route update rules, applied locally at each node, play a key role in maintaining loop-freedom and disjointedness properties. It has route discovery, data transfer and route maintenance phases.

- Route Discovery (Computing Multiple Loop-free Paths) Phase

  Source node initiates route discovery mechanism by flooding Route REQuest (RREQ) packets to its neighbouring nodes. The neighbouring nodes rebroadcast to its neighbouring nodes until RREQ packets reach the destination. While rebroadcasting the RREQ, formation of loop paths are avoided using the advertised hop count field in the RREQ packet. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as at the destination. Multiple Route REPlies (RREP) traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes.

- Data Transfer Phase

  The source node picks up a path among the multiple paths constructed between the source node and destination. The data is sent through the selected path. The selected path is used until it fails and then switched to an alternate path. The selection of path for data transfer is based on the order of their creation.

- Route Maintenance Phase

  In AOMDV, route maintenance is done by means of Route ERRor (RERR) packets. When an intermediate node detects a link failure (via a link-layer feedback), it generates a RERR packet. The RERR propagates towards all traffic sources having a route via the failed link and erases all broken routes on the way. A source upon receiving the RERR initiates a new route discovery if it still needs the route. Apart from this route maintenance mechanism, AOMDV also has a timer-based mechanism to purge stale routes. AOMDV uses very small timeout values to avoid stale paths. This may limit the benefit of using multiple paths. AOMDV uses a moderate setting of timeout values and additionally uses HELLO messages to pro-actively remove stale routes.

  In AOMDV, the multiple routes between the source and destination are generated on demand. The source node broadcasts the RREQ packets to its neighbouring nodes. When RREQ packet reaches the destination node, destination node generates RREP packet. It traverses in the RREQ reverse path to the source node. If the source has more number of multiple paths to destination with maximum number of hops, the control overhead is high in resource constrained WSN.

Radi et al. (2010) proposed a Low-Interference Energy-Efficient Multipath Routing Protocol (LIEMRO) for improving QoS in Event-Based Wireless Sensor Networks. This protocol is mainly designed to improve packet delivery ratio, lifetime and latency, through discovering multiple interference-minimized node-disjoint paths between source node and sink node. LIEMRO has initialization phase, route discovery and establishment phase and route maintenance phase.

- Initialization Phase

  At the initialization phase, each node obtains some information regarding its neighbours. At the first step of this phase, each node broadcasts a fixed number of control packets and records the number of successfully received packets from its neighbours.

- Route Discovery and Establishment Phase

  In route establishment phase, a route request packet is sent from the source to the sink. At each node, the best next hop neighbour is selected according to the cost function

$Cost_{i,j}$, is the cost of the link between node i and node j.

$$Cost_{i,j} = (ETX_j + 1/p_{i,j}q_{i,j}) * (1/ResBatt_j) * (1 + Interference\ Level_j) \quad (2.1)$$

where, ETX_j is the link cost of node j to the sink, contained in the neighbour table of node i. $p_{i,j}$ and $q_{i,j}$ are the forward and backward packet reception rates between node i and node j, respectively. $ResBatt_j$ is the remaining battery of node j and $Interference\ Level_j$ is the maximum interference level that node j has experienced. In addition to forwarding RREQ packet, each node also keeps the ID of the node from which this packet has been received. At each node, upon reception of RREQ packet, a variable named route-path is set to 1 to denote that this node is selected to be a part of route 1. When the route-request packet reaches the sink node, sink node replies to this packet by transmitting a route-reply packet to the node from which route-request packet has been received. Along the reverse path from the sink to the source, receiving RREP packet at each node forces it to set its route-path variable to 2. This means that a confirmed path passes through this node.

- Route Maintenance Phase

  If any node on an active path, after a fixed number of efforts, could not receive Clear To Send (CTS) packet or ACK packet from the next hop node, then it sends an error message to the source node (through the reverse path). After the source node receives such error massage, it disables the path from which this message has been received and redistributes network traffic over other active paths.

  In LIEMRO, control packets are used to identify the neighbouring nodes. Similar to AOMDV, route-request packets are broadcast in the network to identify the path between source and destination. The generation of multiple paths in LIEMRO is quite different from on demand multipath routing protocols. Once, after generating the first path between the source and destination, source finds the second path. Usage of neighbouring control signals and separate route request packets for each path in the network demands high control overhead in the network.

Alwan (2010) proposed Reliable Fault-Tolerant Multipath (RFTM) which is an on demand routing protocol for WSNs. To determine the number of desired multiple disjoint paths

between the source and sink nodes, the RFTM takes into account both reliability demand and link quality. The RFTM protocol assures the high reliability and lengthens the network lifetime. The RFTM protocol has route construction phase and data transmission phase.

- Route Construction Phase

  The RFTM protocol is a source initiated mutlipath routing protocol. The source node floods the route request message to its neighbouring nodes. The route request message has the following fields: Source ID, Sink ID, Request ID, Sender ID, Desired reliability, Minimum Energy Level, Hop count and probability of successful link. On receiving the route request message, neighbouring node generates and maintains its routing table using the Request ID. It updates the route request message and rebroadcasts the message till it reaches the destination or an intermediate node that has an up-to-date route to the destination. To avoid duplicate route request flooding in the network, on receiving the duplicate route request message it discards and floods one to its neighbouring nodes. The sink node evaluates the best paths depending on the desired reliability by the source node and the wireless network condition reported in the route request messages. Then the RREP is sent to the source node.

- Data Transmission Phase

  In data transmission phase, fragment of data packets delivered in the node disjoint paths is evaluated using success probability value. The success probability q_i is given by,

$$q_i = \prod_{k=0}^{n_i-1} {q_i}^{(k)} \tag{2.2}$$

  where, k is the number of links on the path n_i, ${q_i}^{(k)}$ is the success probability of path n_i.

  The RFTM protocol floods the route request packets in the network. The sink node sends the reply packets to the source. But, the route reply message is again broadcast in the network. The route request message and route reply message broadcast mechanism incurs a higher control message overhead in RFTM. The current traffic through the node is not taken into consideration to evaluate effective residual energy.

Challal et al. (2011) proposed sub-branch Multipath Routing Protocol (SMRP). It is a secure and efficient disjoint multipath construction for fault tolerant routing in WSNs. It assures

high level of reliability through a secure multipath routing construction.

In SMRP, root nodes (sink's neighbours) represent the comparison factor between routes in node-disjoint protocols. Two routes are said to be of the same quality, if they come from the same root node. Since, the number of root nodes is constant during a round, discoverable alternative paths is limited by the cardinality of this set of nodes.

The SMRP allows 2-hops neighbours of the sink node to become sub-roots and thereby construct their own sub-branches. A sensor will accept paths within the same branch only if they come from different sub-branches. Similarly, in the network all the nodes generate their branches and update their routing table.

- Route Discovery Phase

  SMRP is a sink initiated multipath routing protocol. The sink initiates the route discovery periodically by broadcasting the RREQ in the network. Every node updates its routing table as it generates routes to the sink node. The RREQ message has the sequence number identifying the current round r, the ID of the sending node, 'parent' and the ID of the sub-root, i.e. the second sensor having relayed this RREQ 'sub-Branch'. While finding the alternative routes, the nodes verify their intersection with already discovered paths. If the received sub-branch tag does not exist in the routing table, then the sending node is selected as an alternative parent and the new route is added to the routing table.

- Data Transfer Phase

  In SMRP, the sensed data by the sensor node is forwarded to the sink node through full duplication, random parent selection and (t, n)-loss tolerant duplication techniques. In full duplication technique, a packet is first duplicated and then sent through all the constructed paths to the sink. In random parent selection technique, one parent is selected from among the different parents belonging to the different paths and used to forward the packet to the sink node. In (t, n)-loss tolerant duplication scheme, a packet is processed using a specific (t, n)-loss tolerant algorithm. A (t, n)-loss tolerant algorithm provides as a result n pieces of information such that only t of n pieces are required to reconstruct the original packet. All the n pieces are sent through the different constructed paths. If

the sink receives at least t of n pieces, it would reconstruct the original packet using the (t, n)-loss tolerant algorithm.

The SMRP generates the multiple paths using minimum number of control messages. The multiple paths generated look into only the sub-root disjointedness, but they fail to identify the complete node disjointedness between the source and sink node. The violation of disjointedness property in the paths may lead to the excessive node usage in the network, leading to network partition. The availability of multiple paths between the source and sink node assures the fault tolerance. The paths selected between the source and destination may not be the energy efficient paths.

Bheemalingaiah et al. (2009) proposed Power-aware Node-Disjoint Multipath Source Routing (PNDMSR) for MANETs. PNDMSR is a source initiated node disjoint multipath routing protocol. It supports real-time traffic, which balances the node energy utilization to increase the network lifetime. It takes the network congestion into account to reduce the routing delay across the network and increases the reliability of the data packets reaching the destination. PNDMSR protocol has route discovery, route selection and route maintenance phases.

- Route Discovery Phase

  When a source node wants to send data to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the data. If the node does not have such a route, then it initiates the route discovery process by broadcasting a RREQ packet to its neighbouring nodes. The RREQ packet has the following fields: Type field indicates the type of packet; SA field carries the source address of node; ID field is used to identify the packet;DA field carries the destination address of node; TTL field is used to limit the life time of packet initially, by default it contains zero; Hop field carries the hop count, initially, by default it contains zero value; Cost field carries the cumulative cost. The cost of the node is added to the cost field when the packet passes through it. Initially, by default it contains zero value; Path field (route record) carries the path accumulations, when a packet passes through a node; its address is appended at the end of this field. In the PNDSMR, when an intermediate node receives a RREQ packet, it

checks whether its own address is already listed in the route record of the route request message. If its address exists, then it drops the RREQ packet, or else broadcasts the message to its neighbours. When all the multiple route requests reach the destination, the destination appends its address to each route request. The destination node computes the optimal paths and informs the source node in the reverse path of RREQ.

- Route Selection Phase

  In PNDMSR, each path is selected based on cost function .The main objective of cost function is to give more weight/cost to the node with less energy. The path cost $C(P_j)$ of path P_j is evaluated using the function,

  $$C(P_j) = \sum_{i=1}^{k-1} f_i(c_i^t) \tag{2.3}$$

  where $f_i(c_i^t)$ is the cost function of node n_i and k is the number of intermediate nodes between source and destination.

- Route Maintenance Phase

  When a link fails, the node sends a RERR packet to inform the source node about the broken link. After receiving the REER, the source node removes the route from the routing table. The PNDMSR uses the other routes in the routing table. Otherwise, it initiates discovery process to continue the data transmission.

In PNDMSR, RREQ is generated by the source node. The RREQ packet is broadcast in the network. The destination node, after receiving RREQs, sends the RREP in the reverse path. If the network is dense, identifying the multiple node disjoint paths is cost effective. The number of control messages used is higher. The optimal path is selected based on the path cost. The path cost is evaluated using the node's residual energy. Finding the optimal paths based on the residual energy may not be optimal as compared to node's rate of energy consumption.

Upadhayaya and Gandhi (2010) proposed a Node Disjoint Multipath Routing considering Link and Node Stability (NDMLNR) protocol. NDMLNR aims to improve the QoS in the network. NDMLNR routes the data based on link stability degree of the paths. The link stability degree is evaluated using the link expiration time and energy drain rate.

The NDMLNR has route discovery and route maintenance phases.

- Route Discovery Phase

  When the source node needs to send data packet to destination node, it broadcasts the RREQ packets to its neighbouring nodes. The NDMLNR is designed for MANET. So, the source is not allowed to maintain route cache for a long time, because the network conditions change very frequently in terms of position and energy level of the nodes. Every node maintains its neighbour information table. The neighbouring nodes receive the RREQ and update its neighbour information table. The intermediate nodes are not allowed to send the RREP message to the source.

- Route Maintenance Phase

  When the link stability of a node falls below the link stability threshold, it informs its predecessor node by sending the NODEOFF message. The predecessor sends the ROUTEDISABLE message to the source node. Then the source node sends the data packets in the alternate path. If no alternate path exists, the source node starts the route discovery procedure again.

  NDMLNR protocol is an on demand node disjoint multipath routing protocol. It is well suited for the MANETs. It generates the node disjoint multiple paths based on the link stability and rate of energy consumption parameters. The usage of the RREQ, RREP, NODEOFF and ROUTEDISABLE messages incurs extra control overhead in the network. The energy efficiency in the network is not assured in routing. Even though the generated routes assure the confidence in data routing, minimum end-to-end delay, energy efficiency mechanism and traffic sharing techniques are not shown.

Xiaoming and Tao (2011) proposed Energy-efficient and Reliability ensured Multipath Routing protocol (ERMR). It is a source initiated, reactive, node-disjoint multipath routing algorithm that considers the residual energy of nodes, the local link reliability and the distance between nodes. ERMR attempts to provide high end-to-end reliability and reduce energy consumption to enhance the network lifetime. It has route construction phase and data transfer phase.

- Route Construction Phase

  When the source needs to send data to sink, the route construction is initiated by the

source node. It constructs the route between source and sink using the neighbouring node evaluation function. The node which has maximum evaluation function is selected as the next hop node in the route between source and sink. The node evaluation function is evaluated using its residual energy, its link reliability between current node to the next hop node and the distance between the nodes. The unique nature of its route construction is that once the node is selected for one route then it is marked as used. This node is not allowed to participate in another route between the same source and sink. In this way, it establishes multiple node disjoint paths between source and sink.

- Data Transfer Phase

  The data is transmitted simultaneously among the selected paths for routing between source and sink. The multiple paths are selected for routing based on their path reliability. The paths are sorted according to their path reliability. The path which has maximum reliability is termed as optimal path. The next path is chosen as the next maximum reliability path and so on. To attain higher end-to-end reliability, data is sent concurrently in all the routes. To maintain minimum residual energy usage in the routing, minimum number of routes are used.

  In ERMR, there is no usage of any control messages for route construction between source and sink. But, end-to-end delay is a bit higher than the other node disjoint path routing protocol (Upadhayaya and Gandhi 2010; Bheemalingaiah et al. 2009). The routes are constructed based on the node residual energy. But the traffic through the node is not taken into consideration to evaluate residual energy. It is very important to verify if the present residual energy is sufficient to handle present data traffic and the planned data traffic. When data is sent simultaneously in multiple node disjoint paths, ERMR does not show how the data traffic is split among the multiple node disjoint paths. Also, ERMR does not show how the route maintenance is done in routing protocol.

Table 2.1: Summary of the Review

Sl.No	Author,Year and Protocol	Description	Routing Parameters	Limitation
1	(Vidhyapriya and Vanathi 2007) Energy Efficient Adaptive Multipath Routing for Wireless Sensor Networks	It is a sink initiated, reactive node disjoint mulipath protocol. This protocol is attempted to provide a reliable transmission with low energy consumption, by efficiently utilizing the energy availability and the received signal strength of the nodes.	Residual Energy and Signal Strength	High control message overhead and ineffectiveness in node's residual energy consideration.
2	(Marina and Das 2006) Ad hoc On-demand Multipath Distance Vector Routing	It is a source initiated, reactive, node/link disjoint mulipath protocol. AOMDV's objective is to provide efficient fault tolerance in the sense of faster and efficient recovery from route failures.	end-to-end delay	High control message overhead and not energy efficient.
3	Radi et al. (2010) Low-Interference Energy-Efficient Multipath Routing Protocol	It is source initiated, reactive multipath routing protocol. This protocol aims to improve packet delivery ratio, lifetime and latency, through discovering multiple interference-minimized node- disjoint paths between source node and sink node.	residual energy and interference level	High control overhead and ineffectiveness in node's residual energy consideration

Sl.No	Author,Year and Protocol	Description	Routing Parameters	Limitation
4	(Alwan 2010) Reliable Fault-Tolerant Multipath routing protocol	It is a source initiated, reactive, node disjoint multipath routing protocol. Its objective is to lengthen the network lifetime, provide fault-tolerance and achieve the desired reliability in the network.	Residual Energy, Hop Count and Link Quality	High control overhead and ineffectiveness in node's residual energy consideration
5	(Challal et al. 2011) Sub-branch Multipath Routing Protocol.	It is a sink initiated,proactive, multipath routing protocol. Its objective is to reduce energy consumption,increase fault tolerance and network resilience.	Hop Count	Lack of energy efficiency technique
6	(Bheemalingaiah et al. 2009) Power-aware Node-Disjoint Multipath Source Routing (PNDMSR)	It is a source initiated, reactive, node disjoint multipath routing protocol. Its objective is to balance the energy spent among the nodes and to increase the network reliability and lifetime.	Residual Energy and Battery Cost Function	High control overhead and ineffectiveness in node's residual energy consideration

Sl.No	Author,Year and Protocol	Description	Routing Parameters	Limitation
7	(Upadhayaya and Gandhi 2010) Node Disjoint Multipath Routing Considering Link and Node Stability protocol.	It is a source initiated, reactive, node disjoint multipath routing protocol. Its objective is to improve the QoS in the network.	Link Stability and Rate of energy Consumption	High control overhead and Lack of energy efficient mechanism
8	(Xiaoming and Tao 2011) Energy-efficient and Reliability-ensured Multipath Routing.	It is a source initiated,reactive, node-disjoint multipath routing algorithm. Its objective is to maintain high end-to-end reliability and reduce energy consumption and to enhance the network lifetime.	Hop Count,Link Reliability and Residual Energy	Ineffectiveness in node's residual energy consideration

2.5 Outcome of the Literature Review

In most of the WSN applications, the data traffic flows towards the common sink node i.e. it follows n-to-1 traffic flow model in the network. Routing the sensed data traffic from the source node to the sink through multiple paths is much efficient than the optimal single path (Sangi et al. 2010). In the recent past, many researchers presented node disjoint multipath routing protocols

Several node disjoint multipath routing protocols available today are on demand or reactive routing protocol. In reactive routing, a route is searched only when needed. When a source node has data packets addressed to a sink node and there is no route to it, the node initiates a route discovery process. Some of the node disjoint multipath routing protocols discussed in the previous section have source initiated route discovery mechanism. When the network topology is dynamic, the proactive routing protocols suffer from excessive routing overhead by periodic message exchange in the network. The network resources such as node energy and bandwidth of the network are wasted in the proactive routing overhead in MANETs. Many WSN applications consider immobile sensor node and static topology. The proactive routing strategy can be used when the topology of the network is fixed and nodes in the network are immobile (Saaranen and Pomalaza-Ráez 2004). It is necessary to study the effects of reactive and proactive routing protocols in WSN environment.

Most of the node disjoint multipath routing protocols aim to reduce the end-to-end delay, increase the network reliability, distribute the traffic evenly among the multiple paths, reduce the congestion, increase the fault tolerance and increase the network lifetime. The node disjoint multipath routing protocols make the routing decision or find the node disjoint multiple paths based on the residual energy of the nodes, link stability, signal strength and minimum hop.

Whenever a node wants to route the data based on residual energy, the routing algorithm reads the current residual energy in the node. This value may not be the actual available residual energy of that node. This is because many data packets may be queued up in the node buffer for processing. Once the data is queued in the node buffer, the particular node commits to process the queued data packets. The energy expenditure on the data reception is done, but still the node has not spent its energy to forward these data packets. Hence to make routing decision more effective and energy efficient, effective residual energy (taking buffered data

into account) and rate of energy consumption are to be considered.

2.6 Problem Statement

This research work is aimed at designing and developing a novel secure sink initiated, proactive, energy efficient node disjoint multipath routing protocol for WSNs based on the rate of energy consumption and data traffic through the node.

2.7 Objectives of the Research Work

The goal of this research work is to propose a novel energy efficient routing protocol for WSNs by focusing on the four major aspects listed below:

(i) Designing an analytical model for node disjoint multipath routing protocol for WSNs.

(ii) Proposing a novel node disjoint multipath routing protocol based on rate of energy consumption and data traffic through the node.

(iii) Designing an effective load sharing mechanism for node disjoint multipath routing protocol, which minimizes the variance among the node residual energy.

(iv) Digital signature based security model for node disjoint multipath routing protocol.

2.8 Summary

In this chapter, we discussed the importance of multipath routing. The merits of multipath routing over the single path routing are highlighted. The advantages of multipath routing are enumerated. The classification of multipath routing protocols based on multipath construction initiated, data transmission techniques, traffic sharing techniques and multipath generation techniques are discussed systematically.

The detailed review of the node disjoint multipath routing protocols is done. In the review of the node disjoint multipath routing protocols, its route discovery mechanisms, and multipath

selection criteria are discussed. The feasibility and importance of proactive routing protocols for WSN is focused in the discussion. WSNs have numerous immobile sensor nodes and their topology is static. So, instead of reactive routing techniques, employing proactive or table driven techniques are more suitable.

The significance in evaluation of node residual energy is also discussed. To achieve energy efficiency in routing protocol, rate of energy consumption and traffic through the node is important. To enhance the network operational lifetime, effective load sharing mechanism is needed in the multipath routing.

Chapter 3

Analytical Model for Node Disjoint Multipath Routing Protocol for WSN

In this chapter, we discuss the feasible assumptions made throughout this work. We clearly specify the node disjoint multipath routing protocols analytical model. Here, we discuss the probability of node disjoint path generation in distributed WSNs. It is also focused on the lifetime analysis of node disjoint multipath routing protocol, when it is operated under different data rates and varied number of multiple paths between source and sink. We design the analytical model for route maintenance in node disjoint multipath networks. We analyse the path reliability and network reliability under varied levels of redundancy for a node and varied number of node disjoint multipath paths between source and sink.

3.1 Assumptions

Designing a general routing protocol suitable for all constraints, requirements and network characteristics of WSNs is hard practically and more or less impossible. tIn this work we propose an energy efficient node disjoint multipath routing protocol for WSN. It is necessary to make feasible assumptions, while designing a routing protocol. The following assumptions made throughout this work.

- Consider N identical wireless sensor nodes that are deployed randomly in a phenomenon and a common sink node. All the sensor nodes send the sensed information to the

destination i.e. sink node, in multiple hops.

- The WSN is an undirected graph $G(N, L)$ where, N is the set of nodes and L is the link set where $L \subset NXN$. The link $(i, j) \in L$ if nodes i and j can communicate with each other. n_i is the set of all the nodes that can reach in one hop from node i.
- Each sensor node has a fixed transmission range 'Tr'.
- There are K multiple paths available from any source to the sink node in the network. The source node selects node disjoint paths between the source and destination to route the sensed data to the destination.
- The required transmission and reception power per packet in a sensor node is fixed.
- The sensor, microprocessor and the radio in the sensor node consume power. We assume that the medium access control operates the radio in sleep mode when the node is not transmitting or receiving a packet.
- The link between the i^{th} hop node and j^{th} hop node gets disconnected when the residual energy falls below the threshold value or when its energy is drained out.
- The lifetime of the sensor network is assumed to be until any sensor node drains out of its energy.

3.2 Analytical Model for Node Disjointedness in Multipath Routing Protocol

The theoretical analysis of k node disjoint path availability is discussed by Abbas and Abbasi (2006) and Bheemalingaiah et al. (2009). The probability that there exists k node disjoint paths is estimated as follows: Let the nodes in the network be assigned unique id's. Select k subsets of the nodes randomly. Then i^{th} subset contains m_i nodes such that $\sum_{i=1}^{k} m_i \ll N$.

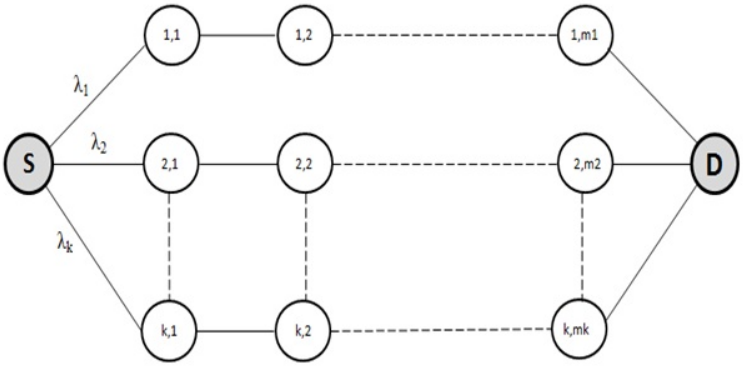


Figure 3.1: Node disjoint Multipath Network

The probability χ that all these k subsets are node disjoint is,

$$\chi = \prod_{i=2}^{k} \frac{\begin{pmatrix} N-2-\sum_{j=1}^{i-1} m_j \\ m_i \end{pmatrix}}{\begin{pmatrix} N-2 \\ m_i \end{pmatrix}} \tag{3.1}$$

The number of nodes used in the calculation is $(N-2)$, because the source and destination are excluded. Let us assume that between a given source node S and sink node D, there exist k node-disjoint paths. The i^{th} path has m_i nodes as shown in Figure 3.1. It denotes j^{th} node of i^{th} path by the subscript i, j, where $1 \leq i \leq k, 1 \leq j \leq m_i$. It may be noted that the end points of all k paths are fixed by the source node and sink node. Consider the i^{th} path: The probability that there exists a link between nodes 1 and 2 is $\varepsilon_{(1,2)}$ and subsequently the probabilities that there exist links between the nodes (2,3), (3,4),..., (m_{i-1}, m_i) are $\varepsilon_{(2,3)}$, $\varepsilon_{(3,4)}$, ...,$\varepsilon_{(m_{i-1},m_i)}$ respectively. Let Ω be the probability that there exist links from the S to D in an order (1,2,3,...,m_i) then, $\Omega = \varepsilon_{(S,1)}.\varepsilon_{(1,2)}.\varepsilon_{(2,3)}.\varepsilon_{(3,4)}....\varepsilon_{(m_{i-1},m_i)}.\varepsilon_{(m_i,D)}$

We further assume that $\varepsilon_(u,v) = \varepsilon, \forall (u.v) \in L$ then $\Omega = \varepsilon^{m_i+1}$. For m_i intermediate nodes along a path, there can be $m_i!$ possible orderings. Suppose $L_o \mid o = 1_i^m!$ denotes the event of occurrence of o^{th} such ordering. For O = $m_i!$. Let $P(L_i)$ be the probability of occurrence of the event L with i^{th} ordering. According to the addition theorem of probability, we have

$$P[\bigcup_{o=1}^{O} L_o] = \sum_i P(L_i) - \sum_{i<j} P(L_iL_j) + \sum_{i<j<k} P(L_iL_jL_k).....(-1)^{O+1} \sum_{i<j<k<...<O} P(L_iL_j....L_O) \tag{3.2}$$

Let P be the probability that there exists a path with m_i intermediate nodes from the source to destination, then

$$\begin{aligned} P &= \begin{pmatrix} O \\ 1 \end{pmatrix} \Omega - \ldots + (-1)^{O+1} \begin{pmatrix} O \\ O \end{pmatrix} \Omega^0 \\ &= [1-(1-\Omega)^O] \\ &= [1-(1-e^{m_i+1})^{m_i!}] \end{aligned}$$

Let P_k be the probability that there exist k multiple paths between the nodes S and D. Then,

$$P_k = \prod_{i=1}^{k} [1-(\varepsilon^{m_i+1})^{m_i!}] \tag{3.3}$$

Combining Equations 3.1 and 3.3, P_{knd} the probability that there exist k node-disjoint paths between a given source node S and D is obtained as,

$$P_{knd} = \chi P_k \tag{3.4}$$

3.3 Network Lifetime Model for Node Disjoint Multipath Routing Protocol

The realistic lifetime model for certain types of systems is modelled using exponential distribution (Hoyland and Rausand 1994; Le et al. 2010). The assumptions of exponentially distributed system lifetime are:

(i) A used unit is stochastically as good as new. There is no reason to replace a functioning unit.

(ii) For the analysis of the reliability function of a unit, it is sufficient to collect data on the number of hours of observed time in operation and the number of failures. These assumptions strengthen the modeling of wireless sensor node lifetime as exponential distribution. Probability density function of lifetime of a sensor node is,

$$p(x) = \lambda e^{-\lambda x}; x > 0, \lambda > 0$$

where x is the lifetime of the sensor node that follows exponential distribution with the parameter λ. Lower the value of λ, higher is the expected sensor node lifetime. Here, λ is considered as the data rate through the sensor node. Because, higher the data rate through the sensor node, lower is the sensor node lifetime expected. The cumulative distribution function that the node will work up to x is,

$$P(X \leq x) = \int_0^x p(x)dx = \int_0^x \lambda e^{-\lambda x} dx = 1 - e^{-\lambda x} \tag{3.5}$$

The reliability of the node, i.e., probability that the node will not fail before x, is

$$\begin{aligned} P(X > x) &= 1 - P(X \leq x) \\ &= 1 - (1 - e^{-\lambda x}) \\ &= e^{-\lambda x} \end{aligned} \tag{3.6}$$

3.3.1 Path Failure Model

Let the path Pa_i has m nodes, where $i = 1, 2, ..., k$. Then, R_{pa}, the probability of failure of path Pa_i is,

$$\begin{aligned} R_{Pa} &= P(min(X_1, X_2, X_3, ...X_m) > x) \\ &= P(min(X_1 > x, X_2 > x, ...X_m > x)) \\ &= \prod_{j=1}^{m} P(X_i > x) \\ &= \prod_{j=1}^{m} e^{-\lambda x} \\ R_{Pa} &= e^{-m\lambda x} \end{aligned} \tag{3.7}$$

3.3.2 Network Lifetime Model

Consider that, the node-disjoint multipath network has k number of paths and m number of nodes in each path. The data rate through each path is assumed to be λ. This implies that the data is equal in each path. If it is assumed that the lifetime of the network is until death of a

node due to its energy depletion, then the reliability of the network is,

$$\begin{aligned} R_{ks} &= \prod_{i=1}^{k}\prod_{j=1}^{m} P(X_i > x) \\ &= e^{-km\lambda x} \end{aligned} \tag{3.8}$$

If the lifetime of the network is considered, as no path exists between the source and destination, the reliability of network is,

$$\begin{aligned} R_{kp} &= P(max(X_1, X_2, X_3, ..., X_k) > x) \\ &= P(max(X_1 > x, X_2 > x, X_3 > x, ..., X_k > x)) \\ &= 1 - P(max(X_1, X_2, X_3, ..., X_k) \leq x) \\ &= 1 - \prod_{i=1}^{k} P(X_i \leq x) \\ &= 1 - \prod_{i=1}^{k} (1 - e^{\lambda m x}) \\ R_{kp} &= 1 - (1 - e^{\lambda m x})^k \end{aligned} \tag{3.9}$$

To increase the lifetime of the network, the source adjusts the data rate to each path according to its residual energy. Let the node-disjoint multipath network consist of k number of paths and m_1, m_2, m_3,...,m_k be the number of nodes with $\lambda_1, \lambda_2, \lambda_3, ..., \lambda_k$ as the data rate in each path respectively, then the reliability of the network is,

$$R_{kn} = 1 - \{(1 - e^{-\lambda_1 m_1 x})(1 - e^{\lambda_2 m_2 x})(1 - e^{-\lambda_3 m_3 x})....(1 - e^{-\lambda_k m_k x})\} \tag{3.10}$$

The lifetime of the sensor network follows exponential distribution. Weibull distribution is also used to model the lifetime of the sensor networks to suit real scenarios. The Weibull distribution introduces another parameter γ. The parameter γ is the sensor node criticality. The sensor node criticality may be the traffic through the node, its rate of energy consumption or node congestion level. Then the distribution function for the lifetime of the sensor network becomes:

$$P(X \leq x) = 1 - e^{-(\lambda x)^{\gamma}} \tag{3.11}$$

Higher network lifetime can be achieved when $\gamma < 1.0$. If $\gamma = 1.0$, then the equation (3.11) behaves as exponential distribution model. The reliability functions for WSN equations (3.8), (3.9) and (3.10) are updated as equation (3.12), (3.13) and (3.14) respectively.

$$R_{w,ks} = e^{-km(\lambda x)^{\gamma}} \tag{3.12}$$

$$R_{w,kp} = 1 - (1 - e^{-m(\lambda x)^{\gamma}})^{k} \tag{3.13}$$

$$R_{w,kn} = 1 - \{(1 - e^{-m_1(\lambda_1 x)^{\gamma}})(1 - e^{-m_2(\lambda_2 x)^{\gamma}})(1 - e^{-m_3(\lambda_3 x)^{\gamma}})...(1 - e^{-m_k(\lambda_k x)^{\gamma}})\} \tag{3.14}$$

3.4 Route Redundancy Model for Node Disjoint Multipath Routing in WSNs

Improving the throughput in the routing protocols for WSNs is very much necessary. Once the residual energy of a node falls to zero or its received signal strength is too weak to communicate, the links in the network fail. In some WSN applications, the communication link fails when the residual energy falls below the threshold energy value or received signal strength is weak in a node. The reliability of the path decreases in such situations.

3.4.1 Single Node Redundancy over Single Path

Suppose that there are m nodes in a path from the source to the sink node. There exist $m-1$ links between source and the sink node. In a path, if any one node is redundant or node for a hop between the node $\delta 1$ and node $\delta 2$, then the reliability R_{sl} is the probability that each node is working properly or data through the node reaches to the next hop node. If p_j is the probability of node j which is working properly, then

$R_{sl} = 1 - (1 - p_j)$

3.4.2 Single Node Level Redundancy through Multiple Nodes over Single Path

Suppose a single node in a path has multi-level single node redundancy between the nodes $\delta 1$ and $\delta 2$, then the reliability R_{sml} is the probability that data through the multi-level node reaches the next hop node without fail and is given by,

$R_{sml} = 1 - \prod_{u=1}^{U} (1 - p_u)$

where,U is the number of levels and p_u is the probability of u^{th} level node working properly.

3.4.3 Single Node Level Redundancy through Multiple Levels

Suppose a single node in a path between source and sink node has redundancy in multiple nodes with multiple levels between the node $\delta 1$ and node $\delta 2$, then the reliability R_{mml} is the probability that data through the node reaches the next hop without fail and is given by,

$R_{mml} = 1 - \prod_{u=1}^{U}(1 - \prod_{v=1}^{V} p_{uv})$

where, V is the number of nodes in each u^{th} level and p_{uv} is the probability of u^{th} level nodes working properly.

To make analysis more realistic and to satisfy all the criteria in the node redundancy, like multi hop nodes having different probability values between the present hop to the next in a path, let us assume that, there are m number of nodes in a path between the source and sink node. Every node may have multiple multi hop node redundancy. If the nodes between the hops in any level have different probabilities, then the reliability R_p of the path is given by

$$R_p = \prod_{u=1}^{U}(1 - \prod_{v=1}^{V}(1 - \prod_{h=1}^{H} p_{uvh})) \prod_{j=1}^{m-UV} p_j$$

where,H is the number of hops in each u^{th} level and p_{uvh} is the probability of u^{th} level nodes working properly.

If the node disjoint multipath network has k number of paths between the source and destination, then R, the reliability of node disjoint multipath network that the data sent from the source node reaches the destination without fail is,

$$R = 1 - \prod_{i=1}^{k}[1 - \prod_{u=1}^{U}(1 - \prod_{v=1}^{V}(1 - \prod_{h=1}^{H} p_{uvh}))] \prod_{j=1}^{m-UV} p_j$$

3.5 Results and Discussion

Simulations are conducted using MATLAB R2008a tool to analyze the network reliability. Higher network reliability indicates higher network lifetime. The simulations are conducted to study the reliability when one path is selected between the source and destination with varied data traffic through that path. Figure 3.2 shows that higher the data rate, lower is the reliability and lesser the data rate, the higher is the reliability. It also shows that the lifetime of the

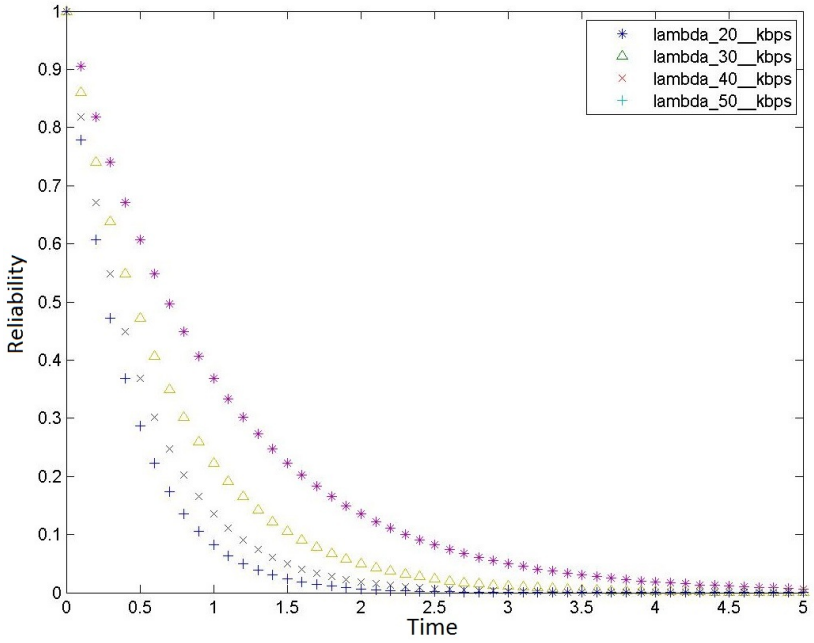


Figure 3.2: Reliability of a Single Path with Varied Data rate

network is long when data rate is less. But in most of the single path or optimal path routing protocols, once the optimal route is selected, all the traffic is sent through the same path. The nodes on the optimal path drain its energy very fast, thus partitioning the network soon. Figure 3.2 shows that when the data rate is low (λ is 20 Kbps), network reliability is higher and when data rate is high (λ is 50 Kbps) network reliability is low, i.e. network lifetime is short.

Figure 3.3 shows the network lifetime for single path and multiple paths. In the single path approach, 30 Kbps of data rate is sent along a path with three nodes between source and destination. The multipath approach has two paths with a data rate of 15 Kbps in each path. It is seen that there is a significant improvement of 60% network lifetime in the multipath approach.

The global objective of the multipath routing is to increase the network lifetime by distributing the traffic among available k number of paths. The network lifetime is maximized, if the energy available on all the nodes is same, after a given data transmission. The data rate and number of nodes in each path are varied to analyze the network reliability. The simulations conducted for the scenarios are described in Table 3.1. The data was selected for the simulation to match the features of MOT300 (MICA) The maximum data rate supported by the mica mote is 50 Kbps to 60 Kbps. So, the data rate of 60 Kbps is taken at the source. Two

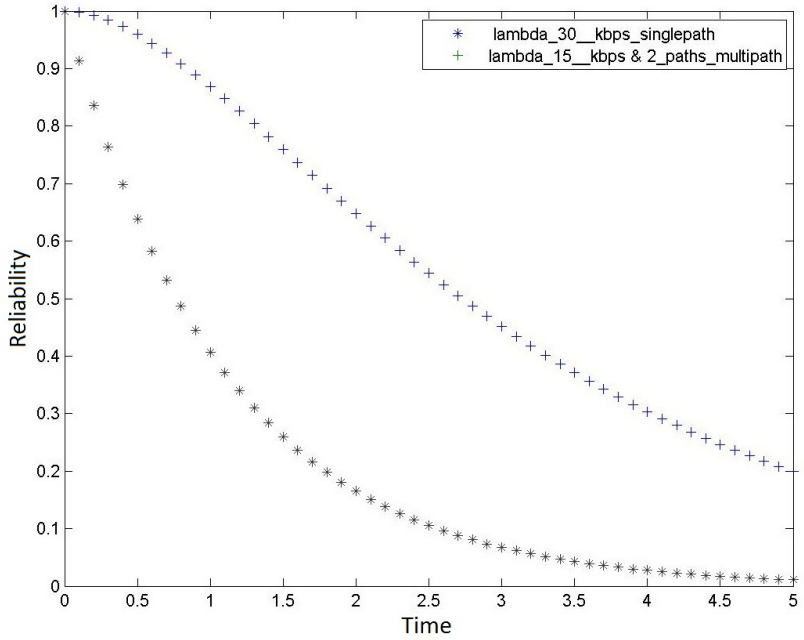


Figure 3.3: Reliability of a Single path and Multipath with Equal Data rate in the Network

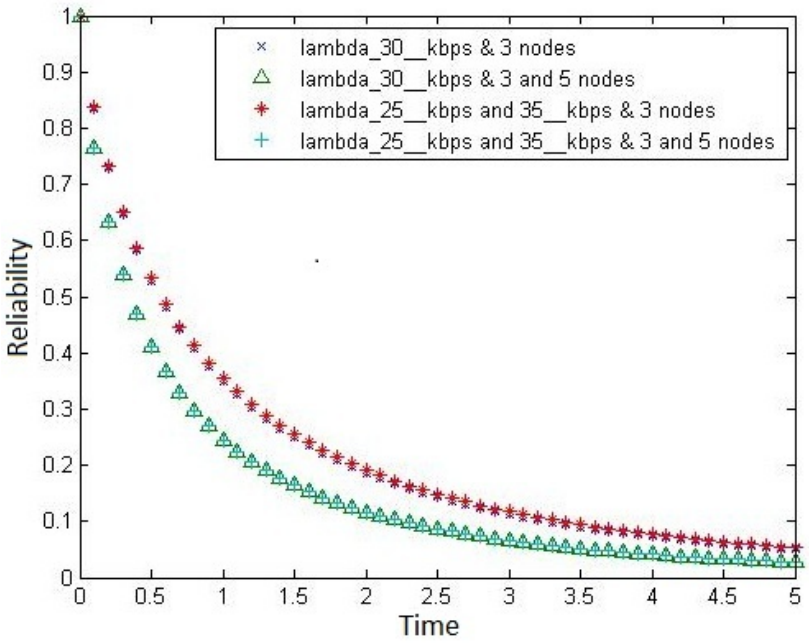


Figure 3.4: Reliability of Multipath Routing with Varied Data rate and Number of Nodes

node-disjoint paths are available between source and destination.

It is observed that when the data rate along the two paths is controlled in such a way that the residual energy on both the paths are equal, the network lifetime is maximized. In the scenario

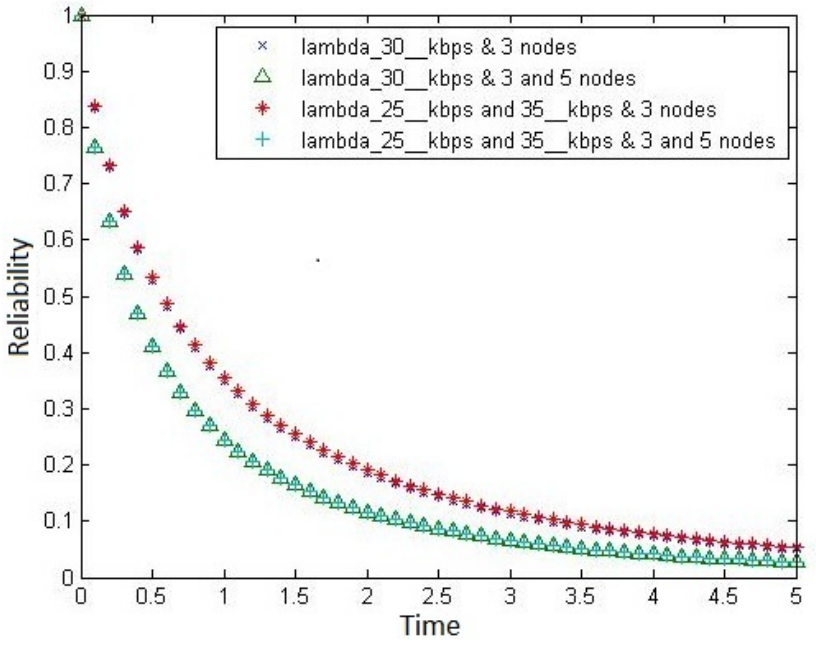


Figure 3.5: Reliability of Multipath Routing with Varied Data rate and Number of Nodes ($\gamma = 0.5$)

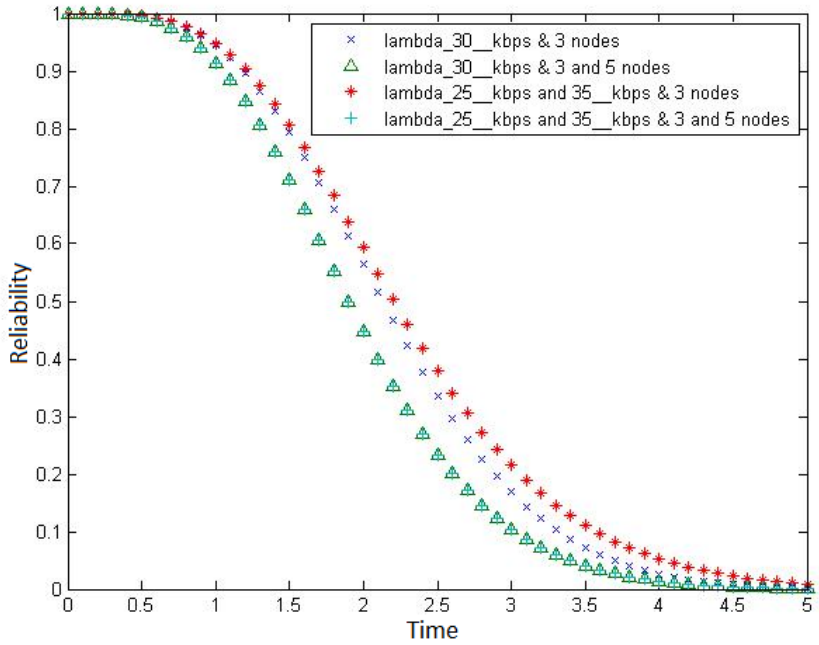


Figure 3.6: Reliability of Multipath Routing with Varied Data rate and Number of Nodes ($\gamma = 2$)

where both the paths have three nodes each, data rate of 20 Kbps and 40 Kbps performed better as shown in the Figure 3.4. There is an improvement of 15% of network lifetime compared to other scenarios.

Table 3.1: Simulation Parameters

Sl.No	Number of Nodes		Data Rate	
	path 1	path 2	path 1	path 2
1	3	3	30 Kbps	30 Kbps
2	3	5	30 Kbps	30 Kbps
3	3	3	20 Kbps	40 Kbps
4	3	5	35 Kbps	25 Kbps

The simulations are conducted to establish the results with additional node criticality parameter γ. The simulation is conducted with the data given in Table 3.1. When ($\gamma < 1$), the network reliability is higher as compared to ($\gamma > 1$) and ($\gamma = 1$), This is because, as the traffic through the node is higher, lifetime of the node decreases. Figures 3.5 and 3.6 show the network reliability for the multipath network with γ = 0.5 and γ = 2.0 respectively. It is seen that when γ = 2.0, the network reliability approaches zero, when the time is 5 units. However, when γ is 0.5, the network lifetime is 40% longer compared to γ = 2.0 even when the time is 5 units.

Table 3.2: Path Reliability for Different Node Reliability and Levels

Node Probability	Number of Nodes	Number of Levels				
		1	2	3	4	5
0.5	2	0.25	0.4375	0.5781	0.6835	0.7626
	4	0.0625	0.1210	0.1760	0.2275	0.2758
	6	0.0156	0.0310	0.0461	0.0610	0.0757
	8	0.0039	0.0077	0.0116	0.0155	0.0193
0.7	2	0.49	0.7399	0.8673	0.9323	0.9654
	4	0.2401	0.4225	0.5611	0.6665	0.7466
	6	0.1176	0.2214	0.3130	0.3938	0.4651
	8	0.0576	0.1119	0.1631	0.2114	0.2568
0.9	2	0.81	0.9639	0.9931	0.9986	0.9997
	4	0.6561	0.8817	0.9593	0.9860	0.9951
	6	0.5314	0.7804	0.8971	0.9517	0.9774
	8	0.4304	0.6756	0.8152	0.8947	0.9400

The reliability of redundant paths in a node disjoint multipath network is analyzed here.

Table 3.3: Reliability of Node Disjoint Multipath Network when, Number of Levels is 2 for Different Node Probability

Node Probability	Number of Nodes	Number of Paths		
		2	3	4
0.5	2	0.6835	0.8220	0.8998
	4	0.2275	0.3210	0.4032
	6	0.0610	0.0901	0.1183
	8	0.0155	0.0232	0.0308
0.7	2	0.9323	0.9824	0.9954
	4	0.6665	0.8074	0.8888
	6	0.3938	0.5281	0.6326
	8	0.2114	0.2997	0.3781
0.9	2	0.9986	0.9999	0.9999
	4	0.9860	0.9983	0.9998
	6	0.9517	0.9894	0.9976
	8	0.8947	0.9658	0.9889

Initially, reliability of a path is studied in different levels of redundancy. For simplicity, the work is restricted to five levels of redundancy in a path. The number of nodes considered in a path is 2 to 8. The node probability values are taken between 0.5 and 0.9. The reliability of a node disjoint multipath network is analyzed through redundant paths. The number of paths between source and sink node is considered as 2,3 and 4.

Table 3.2 shows the reliability of a path Pa_i when the node probabilities are 0.5,0.7 and 0.9. In Table 3.2, the path reliability is high when the number of levels is high and number of nodes is low. When node probability is 0.5 and number of nodes is 2, the path reliability is 0.25 at redundancy level 1. As the level is increased to 5, the path reliability is 0.7626. There is a 205% increase in path probability as the number of redundancy levels increased from 2 to 5. When the number of nodes in a path is increased from 2 to 8, the % increase in path reliability reduces to 97.45. When the number of nodes in the path is 8 and redundancy level is 5, the path reliability is 0.0193. This is much less compared to redundancy level 1 or 2, number of nodes being 4. It indicates that, to get high path reliability, the number of nodes in redundant path should be less and it should have maximum levels of redundancy for the nodes. This is

shown in the Figures 3.7, 3.8 and 3.9. Similarly, Table 3.3 shows that, the path reliability is high when number of nodes is 2 and number of level is 5. When the node probability is 0.7, number of nodes in the path is 2 and redundancy level is 5 then the path reliability is 0.9654. When the node reliability is 0.9, number of nodes in the path is 2 and redundancy level is 5 then the path reliability is 0.9997.

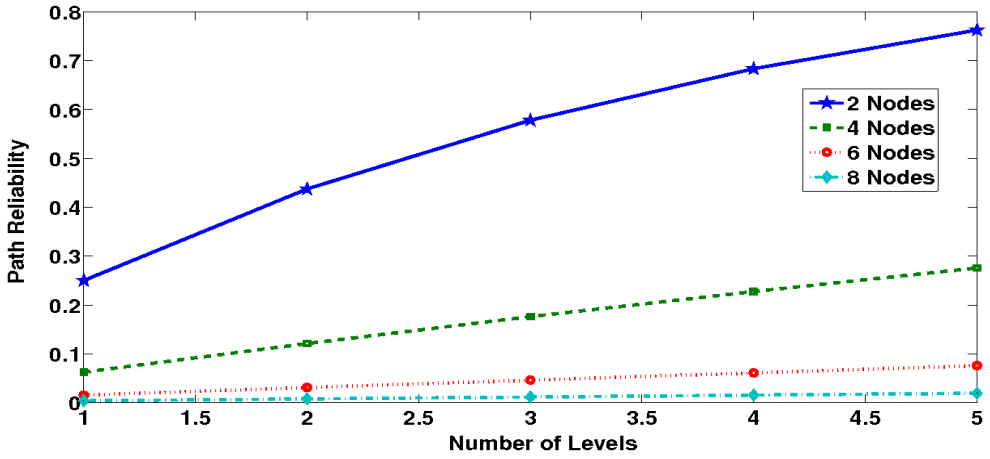


Figure 3.7: Path Reliability When the Node Probability is 0.5

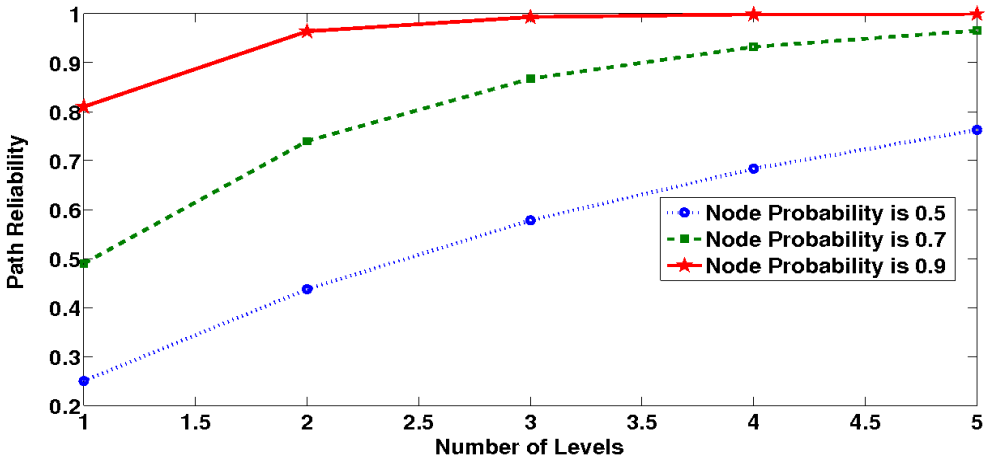


Figure 3.8: Path Reliability when the Node Probability is 0.5, 07 and 0.9 & Number of Nodes is 2

Figures 3.10, 3.11, and 3.12 show the reliability of a node disjoint network when the redundant paths are varied from 2 to 4. In Figure 3.10, the reliability of the network is shown when the node probability is 0.5. It also shows that, when a network has 4 paths, and the number of nodes in each path is 2, then the network reliability is 0.8998. When number of

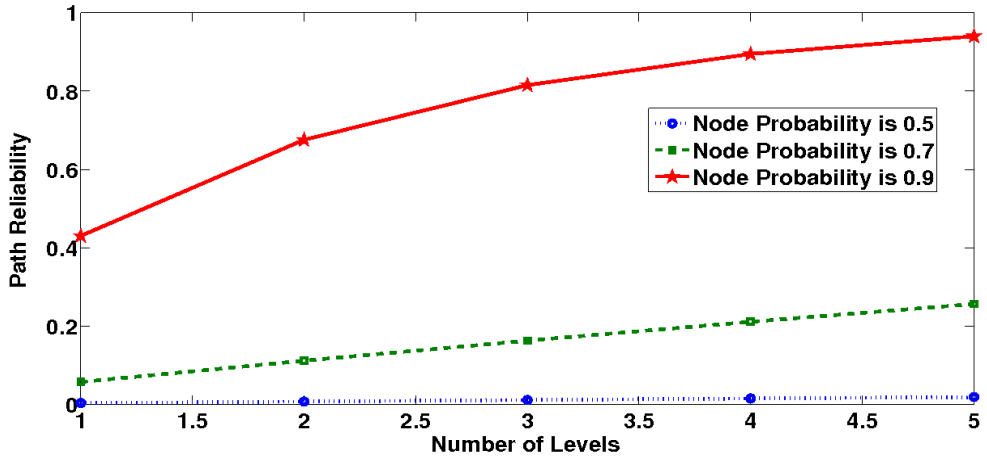


Figure 3.9: Path Reliability when the Node Probability is 0.5, 07 and 0.9 & Number of Nodes is 8

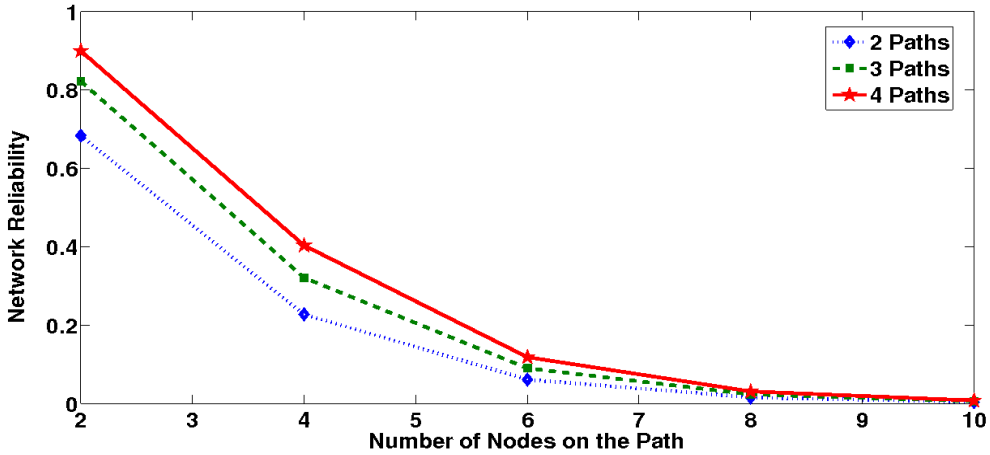


Figure 3.10: Reliability of Node Disjoint Multipath Network when, Number of Levels is 2 and Node Probability is 0.5

paths is 4 and the number of nodes in the path is 8, the network reliability is 0.0308. This is much less compared to the case when the number of paths is 2 or 3 and number of nodes is 2 or 4 in a path. It indicates that, to have high network reliability, number of nodes in a path should be less and it should have maximum number of node disjoint multipaths between source and sink node. Similarly Figures 3.11, and 3.12 show that, the network reliability is high when number of nodes is 2 and number of node disjoint paths is 4. If the node reliability is 0.7, number of nodes in the path is 2 and number of node disjoint paths is 4 then the network reliability is 0.9954 and when the node reliability is 0.9, number of nodes in the path is 2 and number of node disjoint paths is 4, then the network reliability is 0.9999.

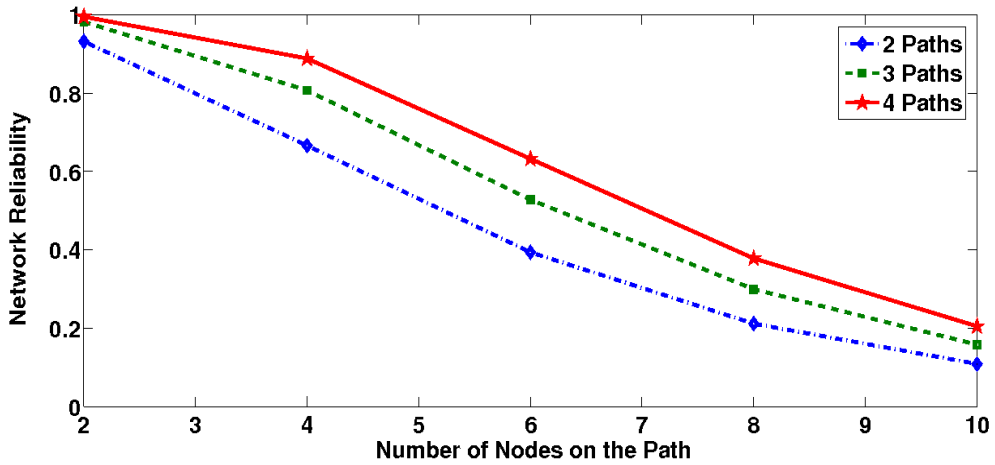


Figure 3.11: Reliability of Node Disjoint Multipath Network when, Number of Levels is 2 and Node Probability is 0.7

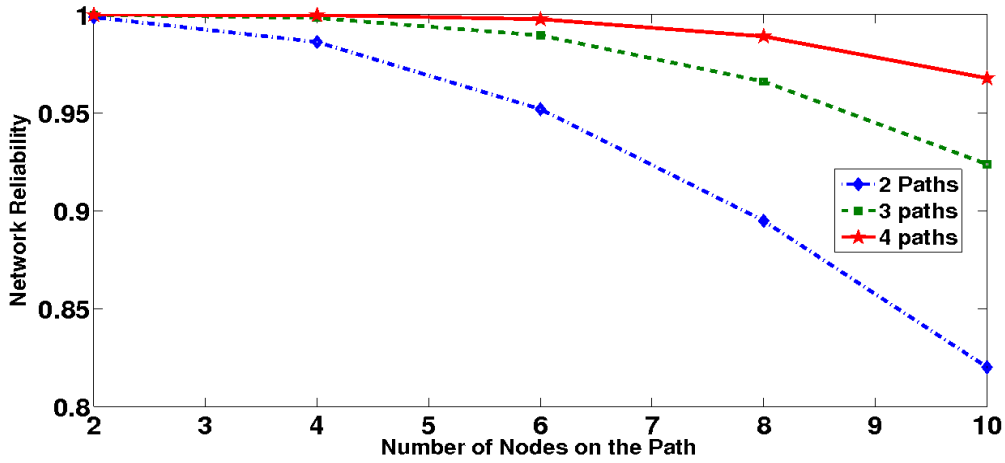


Figure 3.12: Reliability of Node Disjoint Multipath Network when, Number of Levels is 2 and Node Probability is 0.9

3.6 Summary

This chapter proposes an analytical model for the lifetime of node-disjoint multipath in WSNs. The analytical model covers early node death and no path existence between the source and destination. To provide the realistic network analysis, different data rates and different number of nodes were modeled in multipath routing. The node criticality parameter γ in the model enhances the scope of network reliability analysis. The simulation results confirm that the network lifetime is increased when data rate along the multiple paths is varied in accordance with the available node residual energy. The simulation results also establish an increase of

15% in the network lifetime when γ is changed from 0.5 to 1 and an increase of 40% when γ is changed from 0.5 to 2. The network reliability is increased in node disjoint multipath networks, when each node disjoint path has maximum number of redundant paths and minimum number of nodes in each redundant path. To improve the reliability through the redundant paths in the network, it is suggested to have a maximum number of paths between source and destination. It is necessary to have minimum number of nodes in each redundant path.

Chapter 4

Energy Efficient Node Disjoint Multipath Routing Protocol for WSNs

The objective of this research work is to propose an energy efficient node disjoint multipath routing protocol for WSN. In this chapter, the proactive nature of route discovery mechanism is presented. It also presents how this proactive nature of route discovery mechanism reduces the route discovery overhead in EENDMRP for WSN. Different primary path selection criteria among multiple paths are discussed. The results of route discovery and energy efficient data routing and network lifetime in EENDMRP and AOMDV are also discussed.

4.1 Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP)

EENDMRP is a sink initiated, proactive, node disjoint, multipath routing protocol. In EENDMRP, it is attempted to justify that proactive routing is suitable for WSN environments. One objective of this work is to demonstrate the efficient energy usage of this protocol. EENDMRP operates in three phases. They are (i) Route Construction Phase (ii) Data Transmission Phase and (iii) Route Maintenance Phase.

4.1.1 Route Construction Phase

Song et al. (2009) proposed an improved corona model with levels for analyzing sensors with adjustable transmission ranges in a WSN with circular multi-hop deployment. The authors assume that all nodes in the same corona have the same transmission range termed the transmission range of that corona. In EENDMRP, WSN is divided into number of stages based on the number of hops between the source and destination as shown in Figure 4.1. In EENDMRP, WSN is assumed to consist of a number of stages St_i, $i = 1, 2, ..., l$,based on the number of hops between the source and destination. The sink is a stage zero, St_0 node. Every node in St_1 can communicate with the sink node. We assume that a St_i node can communicate with nodes on the same stage St_i and next stage St_{i+1}. But, it cannot communicate with stage St_{i-1} nodes. This prevents the formation of paths with loops.

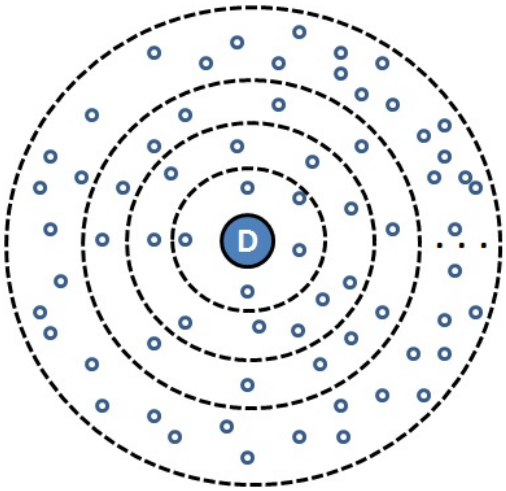


Figure 4.1: Formation of Stages in the Network

The sink node starts the multipath route construction phase to generate its routing tables. During this process Route CONstruction (RCON) packets are exchanged between the nodes. Each sensor node broadcasts the RCON packet once and maintains its own routing table. The format of the RCON packet is as shown in the Figure 4.2. It has Packet Type (to differentiate between control packet and data packets), RCON Hop count (Number of hops away from the sink), RCON Source (original sender of RCON), Node Energy level (residual energy of forwarded node), Sequence Number (to identify whether received packet is fresh or duplicate) and Path (packet traversed from sink to node) fields. If there is no route to the sink via RCON packet received node, then that node processes the RCON packet. If the route to sink from

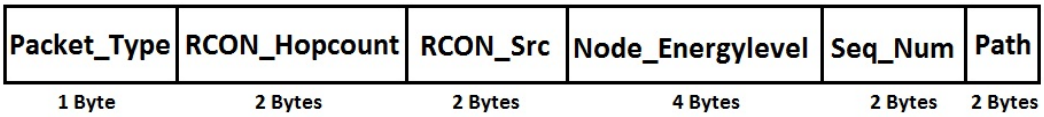


Figure 4.2: Format of Route CONstruction (RCON) Packet

that node is already available in the node's routing table then it checks the packet's hop count value. If packet hop count is smaller than node's hop value and its residual energy is above the threshold energy value, then RCON is processed; otherwise it drops the packet. The node that receives the RCON packet, updates the RCON packet. The updated RCON with hop count increased by one, updates the forward node id and appends its node id to the path. The node, which receives the route construction packet, updates its routing table information such as node's hop count and route to the sink node. Similarly, all the nodes in the network receive the route construction packet and update its routing table. This process is repeated until all the nodes in the network generate its routing table. The format of the routing table contains node id, number of hops away from the sink, node weight, residual energy, possible disjoint paths between that node to the sink node and neighbouring node's public key. The format of the routing table is shown in Figure 4.3.

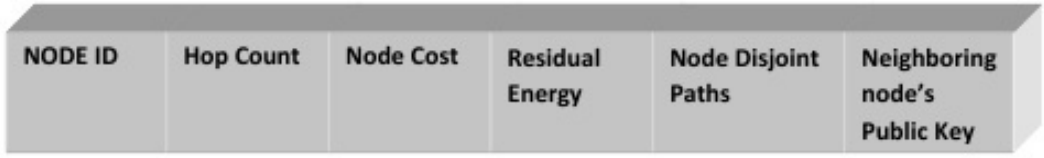


Figure 4.3: Format of Node Routing Table

The route-construction phase is illustrated with the following example. The network in Figure 4.4 is a 10 node network. The node D is the sink node. The sink node initiates the route construction phase by broadcasting RCON packet to its neighbouring nodes i.e. nodes 4, 6 and 9. The node 4 receives the RCON packet from the sink node. It updates its routing table if its residual energy is above the threshold energy value and its hop count is greater than the RCON packet hop count. Node 4 rebroadcasts the RCON packet to its neighbouring nodes 3, 6 and sink node. The node 6 and sink node discard the RCON packet sent from the node 4, since its hop count value is less than that of the RCON packet hop count. The node

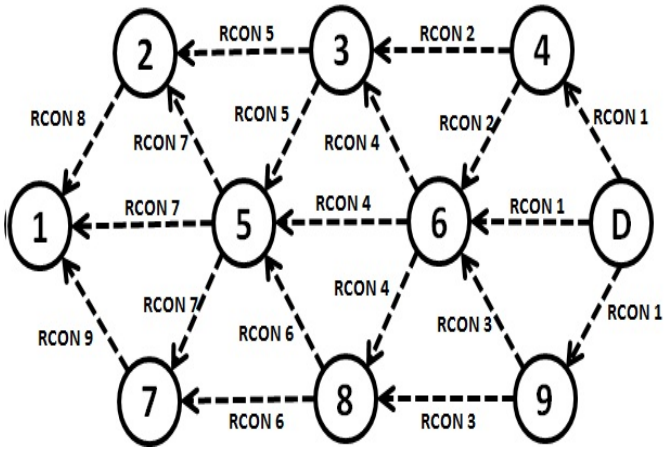


Figure 4.4: Route Construction Phase

3 receives the RCON packet from node 4 since its hop count value is greater than that of the received RCON packet hop count. The node 6 updates the RCON packet received by the sink node and broadcasts to its neighbouring nodes. Here, the nodes 3, 5 and 8 receive the packet. But, the nodes 4, 9 and sink node discard the packet as their hop count is less than that of the received RCON packet hop count. Similarly, node 9 updates the RCON packet received by the sink node and broadcasts to its neighbouring nodes. Here, the nodes 6,8 and sink receive the RCON packet. The node 6 and sink nodes discard the RCON packet sent from node 4, since its hop count value is less than that of the RCON packet. This will be continued until all the nodes in the network generate its routing tables.

4.1.2 Primary Path Selection Criteria

In multipath routing protocols, selecting the best path among the multiple paths is one of its kinds of routing. The primary path selection is an appealing mechanism in multipath routing, as it shows the optimality among the multiple paths between the source node and destination. Later, among these multiple paths, the paths that satisfy node disjointedness are termed as alternate paths or node disjoint paths. These node disjoint paths are generated using the algorithm 1(Node Disjoint Path Generation Algorithm). When the primary path fails, alternate paths are taken into action for data routing. The routing table in each node contains all possible paths between those nodes and the sink node. The primary path is selected from the many node disjoint paths through any of the three primary path selection criteria.

Algorithm 1 Node Disjoint Path Generation Algorithm

Let $K \leftarrow \{Pa_1, Pa_2, Pa_3, ..., Pa_K\}$
Let $Pa_1, Pa_2, Pa_3, ..., Pa_K$ *be the* Pa *number of multiple paths at the source node*
Initialise $\{ND\} \leftarrow PP$
for $i = 0$ *to* $K - 1$ ***do***
    if *((nodes on* $Pa_i \bigcap$ *nodes on path in* $\{ND\}$*) = = Null)* ***then***
        $\{D\} \leftarrow Pa_i$
    end if
end for
if $(\{ND\} == PP)$ ***then***
    Print No node disjoint path is found
else
    Print Node Disjoint path(s) found
end if

- Case (i): Minimum Number of Hops

  The primary path (PP) is chosen among the multiple paths available between source and destination from the node's routing table, based on the number of hops. It is a simple mechanism to find the primary path. It assures that, the node disjoint path, which has minimum hops between source and destination, is selected as the primary path.

$$PP = min(no - hops_i), \ \ where\, i \in k \tag{4.1}$$

  This mechanism may assure minimum end-to-end delay between source and destination. But, it fails to ensure energy efficiency and longer network lifetime. This is because the nodes on the minimum hops route to the destination may not have sufficient residual energy to support the data traffic through it. Without having the global view of the node's residual energy levels, sending data traffic through these paths may lead to faster depletion of residual energy level. It may result in network partition also.

- Case (ii) Maximum Residual Energy

  The primary path is chosen from the node's routing table based on the maximum resid-

ual energy of the path. A path with sufficient residual energy may accept many route requests. This will cause it to exhaust its energy soon, resulting in an early death. This work proposes an effective and efficient mechanism to evaluate the residual energy taking node buffer information and remaining battery power. The energy required to process the committed data packets buffered in the node is taken into consideration to evaluate the effective residual energy of a node. The actual residual energy of a node is evaluated by excluding the energy required to process the committed data packets buffered in the node from the current residual energy of a node. The residual energy, RE_j of a j^{th} node is evaluated using

$$RE_j = CRE_j - (FQL_j * E_{tx}) \tag{4.2}$$

where CRE_j is the current residual energy of node j, FQL_j represents the filled data packets in the j^{th} node queue and E_{tx} is the energy required to transmit per data packet.

$$PP = max(Pa_i(Min(RE_j\, where,\ j \in m)\, and\, i \in k) \tag{4.3}$$

In this mechanism, the primary path is chosen based on the node's residual energy. Initially, a minimum residual energy node is identified in a path. It is tagged as the i^{th} path's residual energy. Similarly, the residual energy levels of all the available k node disjoint paths residual energy are identified. This is because, some nodes in the path may have very high residual energy and some other nodes may have low energy level. If the node which have maximum residual energy is termed as that path's residual energy, and the data traffic is sent according to the path's residual energy, then nodes which have minimum residual energy may drain its energy fast and result in network partition. Hence, it is better to have minimum residual energy node in the path named as path's residual energy and send data traffic accordingly.

- Case (iii): Maximum Path Cost

  In this mechanism, the primary path is chosen from the available node disjoint multi paths between source and destination based on maximum path cost (PC). To choose primary path, based on maximum path cost, the effective node parameters, like rate of energy consumption, filled queue length and effective residual energy, are taken into

consideration. To identify the path cost, rate of energy consumption of j^{th} node is calculated. If the data traffic through the node is high, or if a node acts as an intermediate node for a large number of routes to sink, then the rate of energy consumption is high. To calculate j^{th} Node Cost (NC_j), the data packets queued up in the j^{th} node's buffer are also taken into consideration. Every node in the path finds its cost. The capability of handling the data traffic by a node is less, if its node cost is low.

If the j^{th} node has the minimum node cost compared to all the nodes in the path i, then j^{th} node cost becomes the cost of path i. Similarly, the path cost PC_i of all the paths is evaluated to choose the primary path. The path which has maximum path cost, is chosen as the primary path among all the multiple paths between the source node and destination. The average rate of energy consumption of the j^{th} node, REC_j is evaluated using the well-known Exponential Weighted Moving Average (EWMA) technique.

$$REC_j = \alpha * REC_{old} + (1 - \alpha) * REC_{new} \tag{4.4}$$

where, REC_{old} is the previous rate of energy consumption, REC_{new} is the current rate of energy consumption, The coefficient $\alpha \in (0, 1)$ represents the degree of weighting decrease and is a constant smoothing factor. To better reflect the current condition of energy expenditure of nodes, this work sets α value as 0.3 as in Kim et al. (2003).
Node Cost NC_j of the j^{th} node is calculated as

$$NC_j = (RE_j / REC_j) * FQL_j \tag{4.5}$$

where, RE_j is the residual energy of the j^{th} node, FQL_j is the filled queue length of the j^{th} node.
Path cost PC_i of i^{th} path, is evaluated as,

$$PC_i = min\{NC_j \; where, \; j \in m \; , \; i \in k\} \tag{4.6}$$

where, m is the number of nodes in the i^{th} path.

$$PP = max\{PC_i \; where, \; i \in k\} \tag{4.7}$$

4.1.3 Route Maintenance Phase

Figure 4.5 illustrates the operation of route maintenance phase. The link between the nodes 2 and 3 is broken. During the data transfer phase, any link can fail because of reasons like

physical misplacement of node, the node's energy is below the threshold energy value during the transfer of data, etc. Then the node 2 sends the RERR packet to its data source. It also sends to the source which has route to sink node through that node. Node 2 checks its routing table to find the alternate path from node 2 to sink node and selects the best route among the paths to sink node. Then node 2 generates and sends the RERR message to the source node. The RERR message provides the information about the link failure and an alternate path between the nodes which generated the route error packet and sink node. The source node receives the RERR message and updates its routing table by discarding the failed path. Data packets from the source node are redistributed among the rest of the paths.

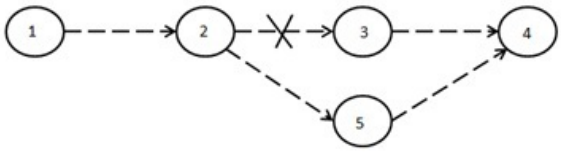


Figure 4.5: Route Construction Phase in EENDMRP

4.2 Results and Discussion

Simulations are carried out using the network simulator-2 (NS-2) version NS-2.34. The NS-2 is an object-oriented discrete event time simulator. More details on NS-2 simulator is presented in Appendix A. The simulation parameters set in the simulations are shown in the Table 4.1.

4.2.1 The Energy Model

A typical sensor node comprises of four basic units. They are (i) Sensing unit, (ii) Processing unit, (iii) Transceivers and (iv) Battery unit. The energy model sets the energy consumption by sensing unit, processing unit, and transceivers unit. The energy model is designed as follows: The work assumes that sensor node processing unit is operating at 4 MHz as in mica the energy consumed for sensing one bit of data is E_{sense}, the energies required for data transmission and reception per packet are E_{tx} and E_{rx} respectively. A battery in the sensor node is working at 2.7 V - 3.3 V. In active mode, the current drawn rate is considered as E_{active}. The $E_{tx-elet}$ and $E_{rx-elet}$ are the energies spent in data transmission and reception per bit respectively. $C_{amplify}$

is the current consumed by a sensor transmitter to transmit a unit distance d and $\nu \geq 2$ is a constant which depends on the attenuation the signal will suffer in the environment. Then, the energies required to transmit and receive per packet E_{tx} and E_{rx} are evaluated as,

$$E_{tx} = [(E_{tx-elet}) + C_{amplify} * d^{\nu}] * pkt_{size} \tag{4.8}$$

$$E_{rx} = (E_{rx-elet}) * pkt_{size} \tag{4.9}$$

Energy consumed per clock cycle in active mode is evaluated as,

$$E_{active} = (E_{active})/4MHz \tag{4.10}$$

Table 4.1: Simulation Parameters

Sl.No	**Parameters**	**Values**
1	Channel	Wireless Channel
2	Propagation	Two Ray Ground
3	MAC Type	802.15.4
4	Queue Type	DropTail
5	Queue Limit	100 packets
6	Antenna Type	Omni Directional
7	Number of Nodes	10 to 100
8	Packet Type	CBR
9	Area	120 * 120 Sq.m
10	Simulation Duration	120 seconds
11	Number of Sink	One
12	Initial Energy	5 Joules
13	Transmission Energy E_{tx}	35.00e-3 W
14	Reception Energy E_{rx}	20.00e-3 W
15	Idle Energy E_{idle}	20.00e-6 W

4.3 EENDMRP Performance Analysis

The performance of EENDMRP is analysed through the effective routing protocol metrics like, Packet Delivery Fraction(PDF), Normalised Routing Load (NRL), average residual energy,

average spent energy, average end-to-end delay, and network lifetime. The performance of EENDMRP is also analysed by comparing the different primary path selection criteria and the effects of different transmission range. The performance of the proposed EENDMRP is compared with AOMDV. Table 4.2 shows EENDMRP with different path selection criteria in notations.

Table 4.2: Notations of EENDMRP Path Selection Criteria

Sl.No	EENDMRP Path Selection Criteria	Notation
1	Case (i) Primary path selected based on minimum number of hops	EENDMRP(1-0-0)
2	Case (ii) Primary path selected based on maximum residual energy	EENDMRP(0-1-0)
3	Case (iii) Primary path selected based on maximum path cost	EENDMRP(0-0-1)

4.3.1 Effects of Transmission Range

The effective transmission range in the network is very important to increase the network lifetime. Increasing the transmission range of a node results in less number of hops between a source and destination and enhances overall network connectivity. However, it results in inefficient bandwidth and node residual energy usage. The effect of transmission range in EENDMRP is studied. Generally, a large transmission radius necessarily implies that more nodes are affected by each transmission, thereby limiting the effective bandwidth of neighbouring nodes. The larger the transmission radius, the more are the number of nodes affected by transmissions.

For short transmission radius, the number of nodes communicating by a single transmission is small, so the number of nodes that receive the broadcast packets in the network is also less. It largely avoids the processing power spent on discarding useless packets. As the transmission range increases, the number of hops between the source and sink node reduces; but the distance between the nodes in a hop increases. Hence, the transmission energy required to send the data also increases, as the energy spent on the data transmission is directly proportional to the distance between the nodes. In this work, transmission range is varied between 20 meters and 40 meters.

Figure 4.6 shows the effect of transmission range on generating number of paths between

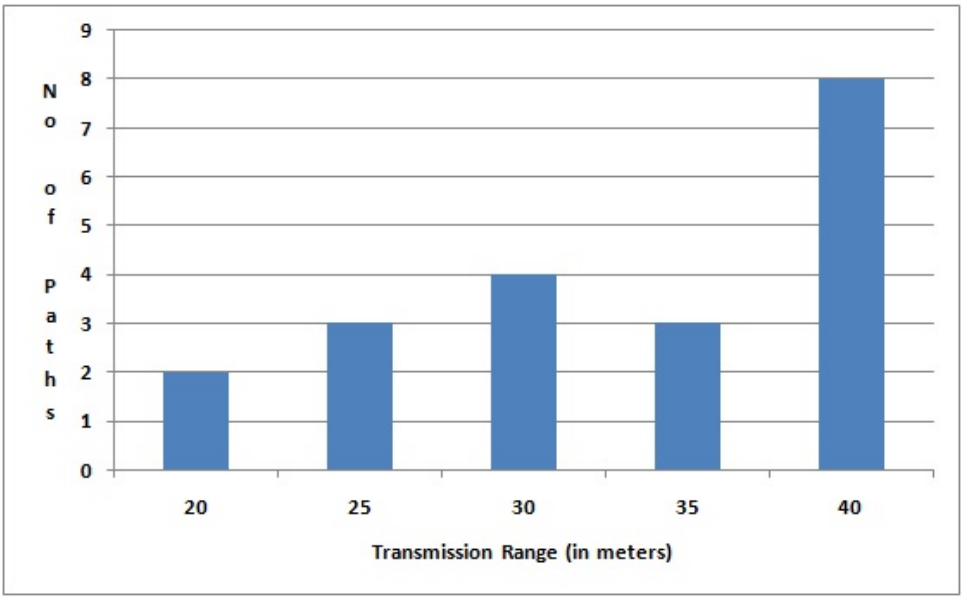


Figure 4.6: Effects of Transmission Range on Number of Paths

the source and destination. When the transmission range increases, the number of possible node disjoint paths between the source and destination also increases. If more number of neighbouring nodes exist in the transmission range, possibility of node disjoint paths is also high. Similarly, when the transmission range is low the number of neighbouring nodes appearing in the source node routing table is less. When the number of neighbouring nodes is less the possibility of occurring node disjoint paths is also less. Figure 4.6 shows that when the transmission range is 20 meters, the number of disjoint paths is 2 and when it is 40 meters the number of node disjoint paths is 8. When the transmission range is 25 and 35 meters the number of node disjoint paths is 3. This is because, equal number of neighbouring nodes exist in the node's transmission ranges.

Figure 4.7 shows the total energy spent when the data is transmitted through different number of node disjoint paths. When the number of node disjoint paths increases, the total energy spent also increases. But, one interesting result seen in the Figure 4.7 is when the number of node disjoint paths is 3. In this case the total energy spent is 22 J, which is less compared to the total energy spent through 2 node disjoint paths. This is because when the transmission range is 25 and 35 meters the number of paths is 3. The number of hops between the source and destination node is less when transmission range is 30 meters as compared to

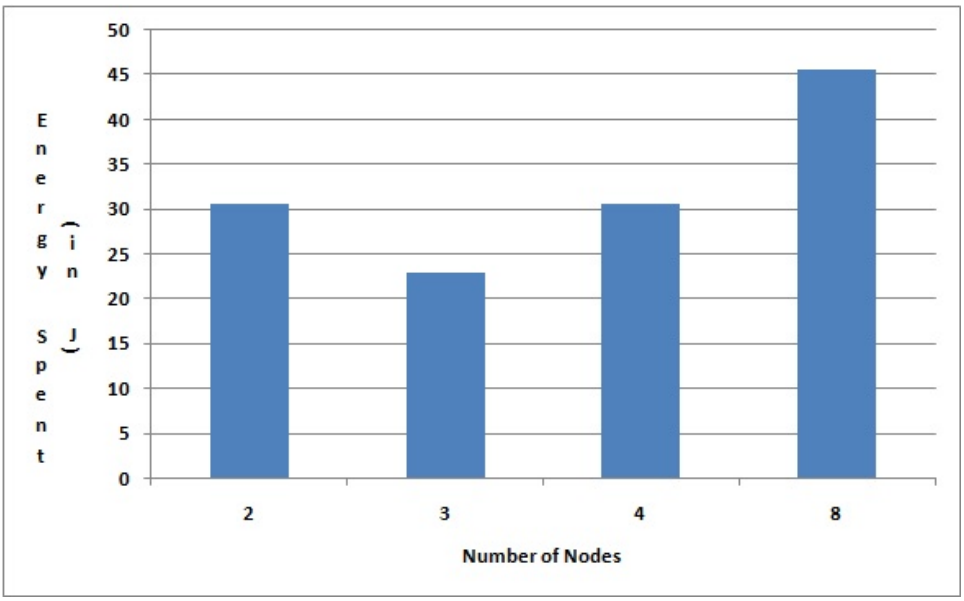


Figure 4.7: Effect of Number of Nodes on Total Energy Spent

20 meters. The presence of minimum number of intermediate nodes between the source and destination consumes minimum total energy. The energy consumption is directly proportional to the distance between the nodes. When the transmission range is 40 meters, the number of disjoint paths is more and distance between the nodes is also high as compared to 20 to 35 meters. So, the total energy spent is also high when the number of paths is 8. The inference from the Figure 4.7 is that the effective utilization of node energy depends on both number of hops and transmission range. There is an energy saving of 24.8% when data is transmitted through 3 node disjoint paths as compared to 4 paths. 49.5% of energy savings observed when data is transmitted through 3 node disjoint paths as compar+786ed to 8 paths.

Figure 4.8 shows the average energy spent on varying the transmission range in the network. The average energy spent is less when the transmission range is 40 meters. The average energy spent in 20 meters transmission range is high as compared to 25 to 40 meters range in the network. When the transmission range is high the number of nodes participated and number of node disjoint paths in the routing are more between source and destination in the network. As the number of node disjoint paths is more, data traffic sent is less in each node disjoint path. So, the energy spent in each node in data forwarding is also less. Figure 4.8 shows that when the transmission range is 20 meters the average energy spent is high. This is because, the data sent in number of node disjoint paths is 2 and number of nodes partici-

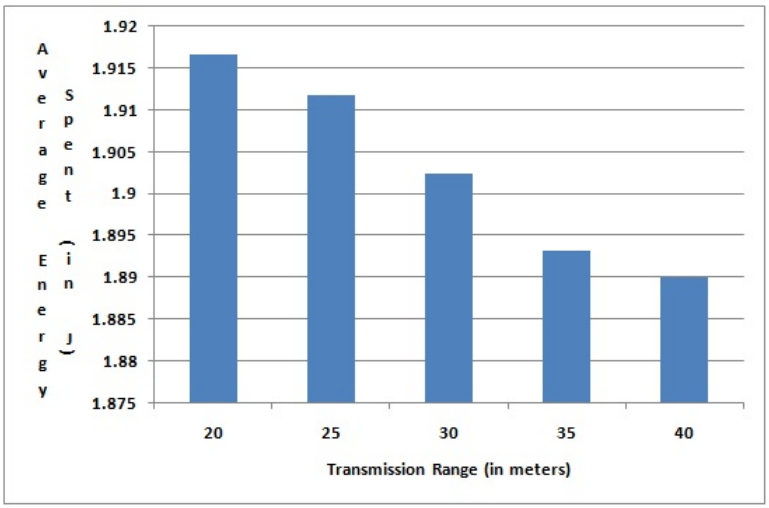


Figure 4.8: Effects of Transmission Range on Average Energy Spent

pated in routing is 16 which are less compared to 8 node disjoint paths and 24 nodes when the transmission range is 40 meters. The improvement in average energy spent when transmission range is 40 meters compared to 20, 25, 30 and 35 meters is shown in the Table 4.3.

Table 4.3: Improvement in Average Energy Spent

Sl.No	**Transmission Range**	**Improvement in Average Energy Spent**
1	20	1.4%
2	25	1.15%
3	30	0.7%
4	35	0.16%

Figure 4.8 shows that when the transmission range is 40 meters the average energy spent is the minimum as compared to 20 to 35 meters range in the network. But, Figure 4.7 shows that the total energy spent is high when the network is set to 40 meters transmission range. Spreading the traffic among maximum number of nodes increases the network lifetime by using maximum number of paths. The number of nodes participated in the routing is high and total energy spent is high, even though average energy spent is less in each node. Table 4.4 shows that, when the transmission range is 35 meters, the number of nodes participated in routing is less and the total energy spent is also less. The average energy spent in each node

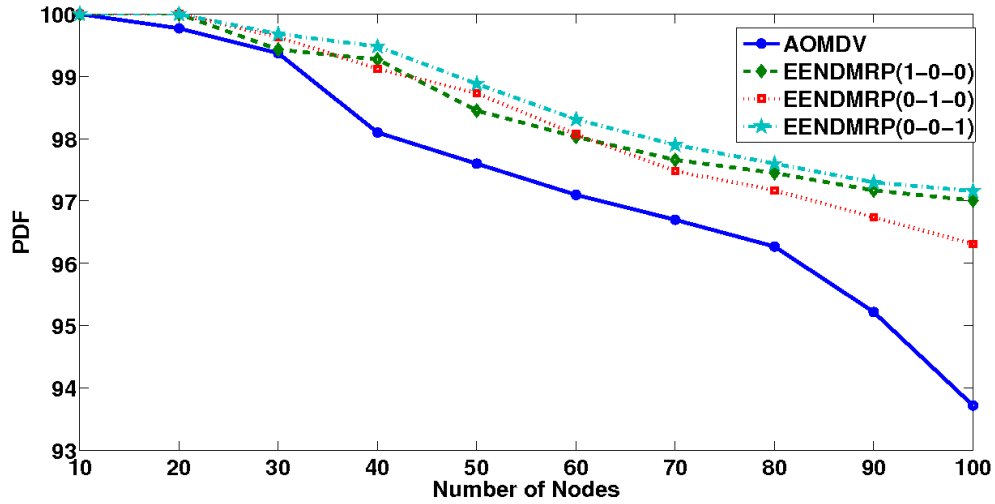
Table 4.4: The Effect of Transmission Range on Node Residual and Average Energy Spent

Transmission Range in mtrs	Number of paths	Number of Nodes	Total Spent Energy	Average Energy Spent
20	2	16	30.66	1.9162
25	3	15	28.677	1.9118
30	4	16	30.57	1.9106
35	3	12	22.9859	1.9154
40	8	24	45.5665	1.8960

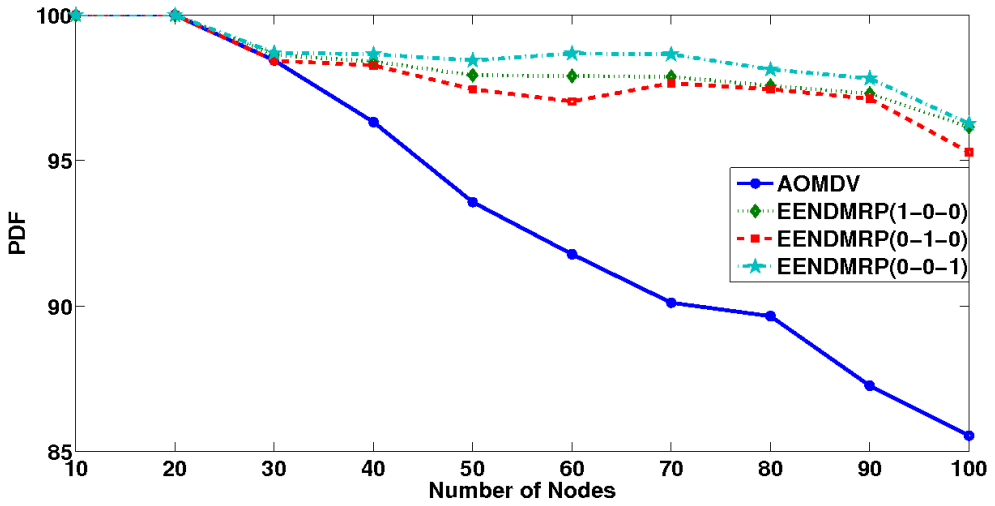
is almost equal to 1.91 J in all the nodes. The average energy variance is 0.01% J which is insignificant compared to the saving in total energy spent. There is a saving of 49.5% of saving in total energy spent when transmission range is 35 meters as compared to 40 meters.

4.3.2 Packet Delivery Fraction (PDF)

Figures 4.9(a) and 4.9(b) show the PDF in AOMDV and EENDMRP for grid topology and random topology respectively. The PDF in random topology is less, as compared to grid topology. This is because of the randomness of node locality and the higher number of hops between the source and sink node. When the number of nodes is increased, the number of hops in the path occurrence also increases. When the number of nodes is 100, the PDF is 85.54% in random topology and 96.26% grid topology. The PDF is high in EENDMRP compared to AOMDV. The number of packet drops is less in EENDMRP as compared to AOMDV. The effective primary path selection mechanism in EENDMRP avoids the packet drops in the network. The primary path is chosen from the node routing table, based on the maximum path cost in EENDMRP. The path cost is chosen using the filled queue length of the node. The minimum value of the node's cost in the path is the cost of that path. If any node's filled queue length is maximum in a path, then chances of selecting that path as primary path is minimum. It indicates that the primary path is selected which is high in residual energy and less in filled queue length. The packet drops are avoided in EENDMRP after the queue is filled. In AOMDV, the multiple paths are selected from the source node to sink node. In AOMDV, path is selected for sending the data packets from source node to sink node in the order of generation of multiple paths. The randomness in path selection makes the path more



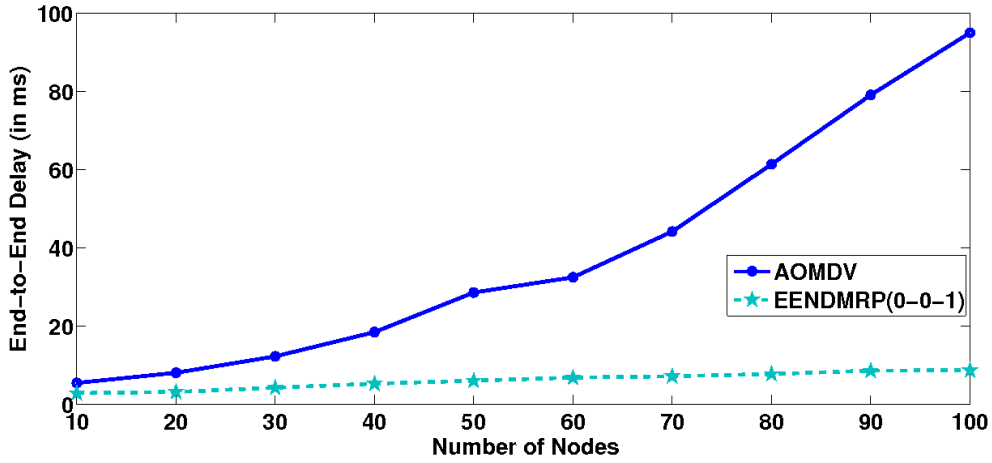
(a)



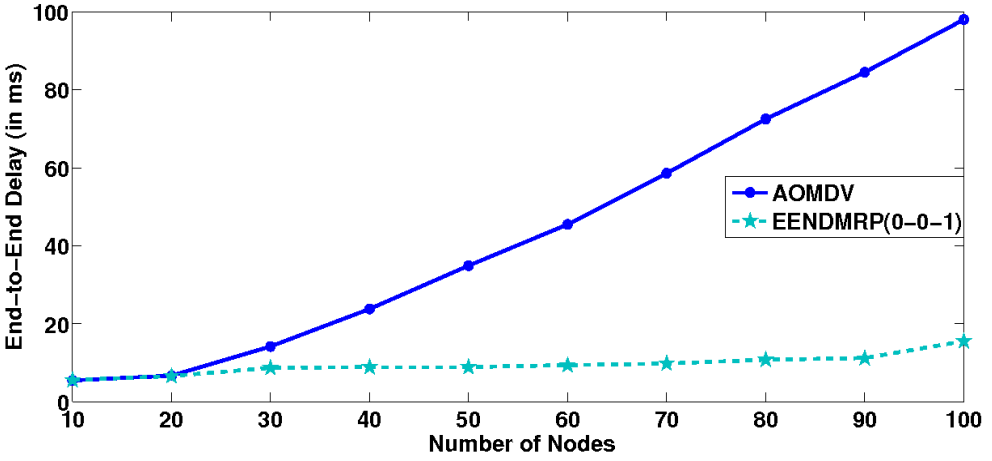
(b)

Figure 4.9: Effects of Number of Nodes on PDF (a) in Grid Topology (b) in Random Topology

vulnerable to packet drops in the network. In Figure 4.9(a), when the number of nodes is 10, the PDF is 100% in both AOMDV and EENDMRP, because the source reaches the destination in one or two hops. When the number of nodes in the network is 100, the PDF in AOMDV is 93.72% and in EENDMRP it is 97.16% . There is an increase of 4% of PDF in EENDMRP as compared to that in AOMDV.



(a)

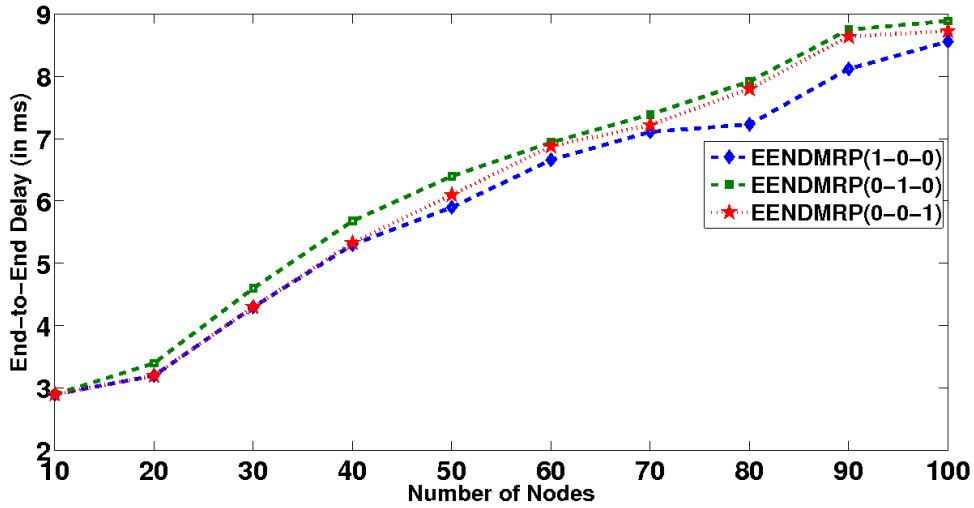


(b)

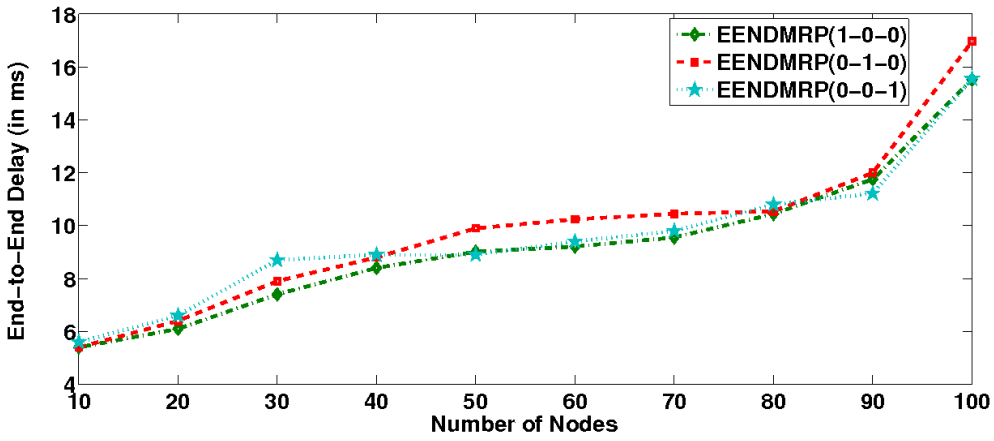
Figure 4.10: Variation of Average End-to-End Delay with Number of Nodes (a) in Grid Topology (b) in Random Topology

4.3.3 End-to-End Delay

Figures 4.10(a) and 4.10(b) show the average end-to-end delay in AOMDV and EENDMRP when network topology is grid and random respectively. Average end-to-end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, retransmission delay at the MAC, and propagation and transfer times of data packets. The average end-to-end delay of AOMDV and of EENDMRP in grid and random topologies are almost the same. This is because, the common simulation area taken is 150*150 sq.mtrs for both grid and random topologies. The change in average end-to-end delay is 0.02 ms and 3.5



(a)



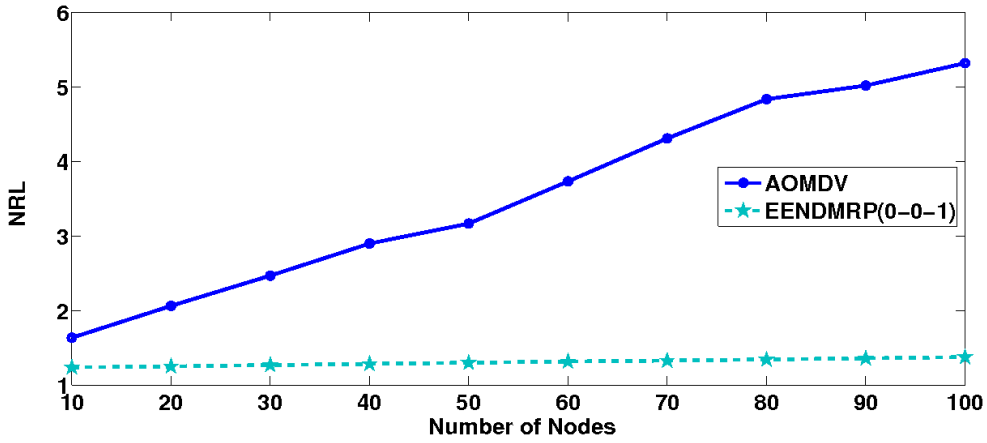
(b)

Figure 4.11: Comparison of End-to-End Delay Variation with Number of Nodes in EENDMRP(1-0-0), (0-1-0) and (0-0-1) (a) in Grid Topology (b) in Random Topology

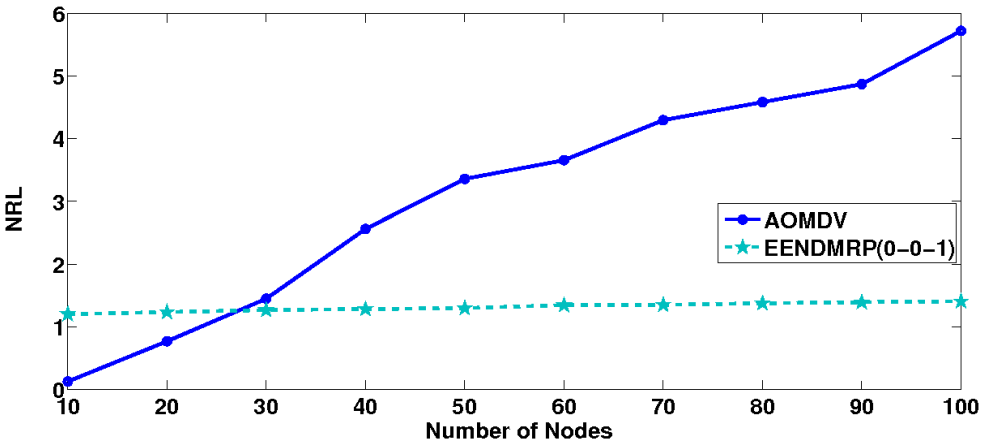
ms in AOMDV and EENDMRP respectively. Figure 4.10(a) shows end-to-end delay incurred in sending the data from the source node to sink node in the AOMDV and EENDMRP. The end-to-end delay is reduced in the EENDMRP as compared to the AOMDV. The EENDMRP is a proactive multi-path routing table and routes are readily available to the sink node. In route construction phase, the node receives the RCON packet only when its hop count is greater than the RCON packet's hop count. The AOMDV is a reactive multi-path routing protocol. When the source node gets data to sink node, the route discovery is done from the source node to sink node. The end- to-end delay is more in the AOMDV because of its reactive nature and the

path selected to route the data may not be of the minimum hop. When the number of nodes is 100, the average end-to-end delay is 8.73 ms in AOMDV and and 95 ms in EENDMRP. The average end-to-end delay is 9.88 times less in EENDMRP as compared to AOMDV. When the number of nodes is 10, the average end-to-end delay is 0.89 times less in EENDMRP as compared to AOMDV.

4.3.4 Normalized Routing Load (NRL)



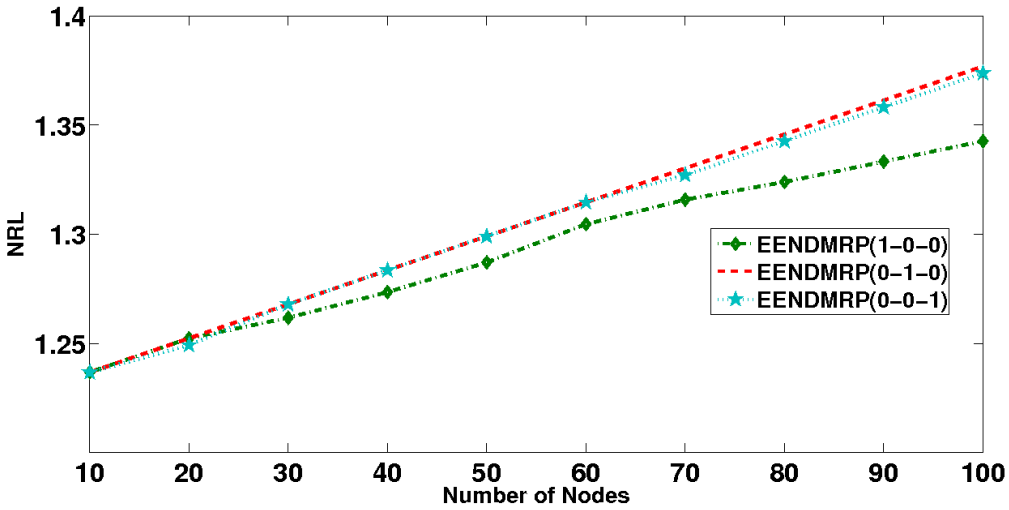
(a)



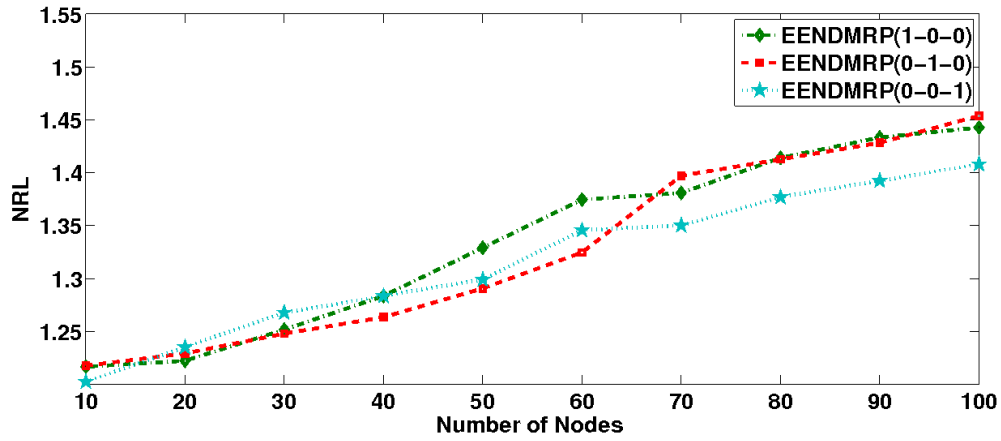
(b)

Figure 4.12: Variation of NRL with Number of Nodes (a) in Grid Topology (b) in Random Topology

NRL is the number of routing packets transmitted per data packet delivered to the desti-



(a)



(b)

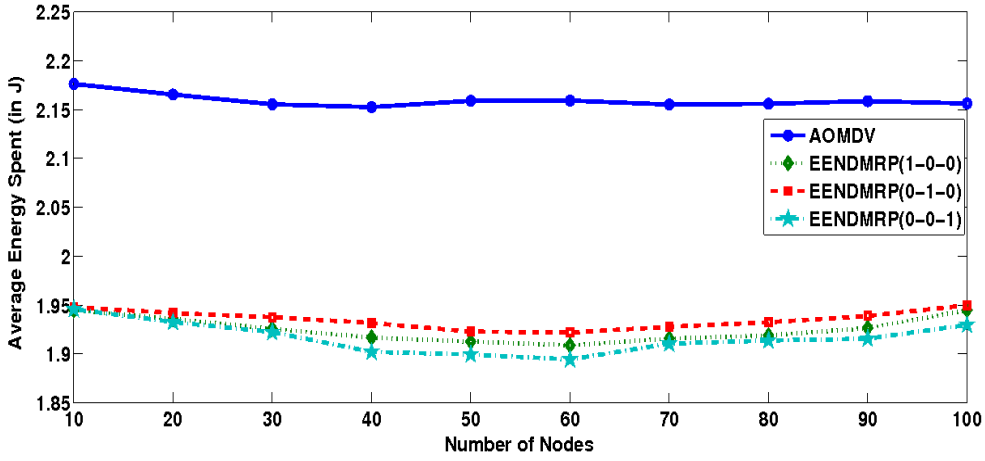
Figure 4.13: Comparison of NRL Variation with Number of Nodes in EENDMRP(1-0-0),(0-1-0) and (0-0-1) (a) in Grid Topology (b) in Random Topology

nation. Each hop-wise transmission of a routing packet is counted as one transmission. Figures 4.12(a) and 4.12(b) show the NRL in AOMDV and EENDMRP. The NRL in AOMDV's grid topology is more compared to random topology, when the number of nodes is less in the network. It is because the source is reaching the destination in one hop and AOMDV is reactive protocol. Hence, it need not broadcast the RREQ packets in the network. The NRL is 0.12 and 0.81 in AOMDV, when the number of nodes is 10 and 20 respectively in random topology network. In grid topology, the source node may not reach the sink in one or two hops, even when the number of nodes is 10 or 20. In AOMDV, the number of control messages used in

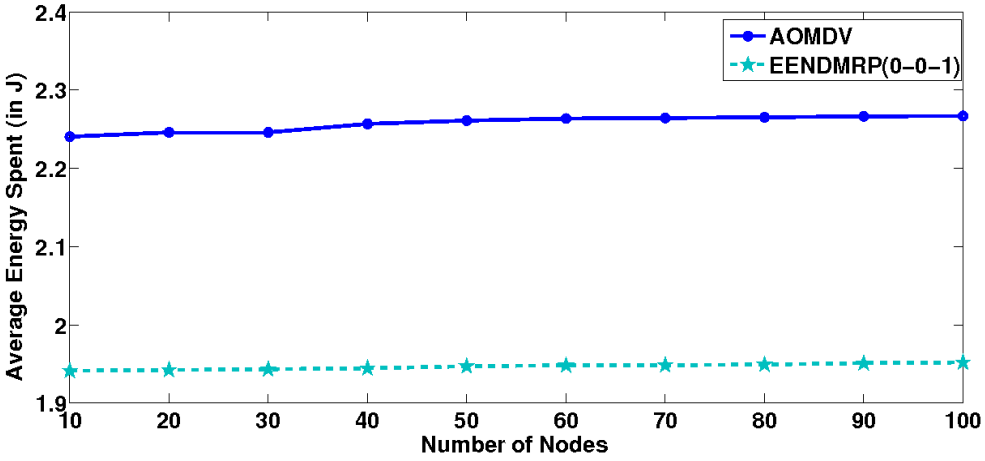
constructing multiple paths is high as compared to the EENDMRP. The source node broadcasts the RREQ packets to its neighbouring nodes. The RREQ packet is re-broadcast until the destination or an intermediate node receives the RREQ packet. The destination generates multiple route replies. These replies travel along multiple loop-free reverse paths to the source which are established during the route request propagation. In every node's route construction phase, a number of RREQ packets and its multiple route replies travelled in multiple routes in multi hops consuming high routing packet overhead per data packet transmission. As the number of nodes increases in the network or when the number of hops between the source and destination is high, then the control messages are also high. In Figure 4.12(a), when the number of nodes is 70, the NRL is increased sharply as compared to a steady increase in 50 nodes. This is because, the source selected in the simulation is a maximum hop distance node in the network to the destination comparing to 50 nodes simulation. The NRL in the EENDMRP is low compared to the AOMDV model, because of its proactive routing nature. The number of control messages used in the EENDMRP is low. In the EENDMRP model, the RREP packets are avoided from the destination node. The multiple routes are constructed in all the nodes in an iteration of route construction phase. There is an increase of 0.3 times and 3.8 times NRL in AOMDV compared to EENDMRP, when the number of nodes is 10 and 100 respectively in the network.

4.3.5 Average Energy Spent

Average energy spent by the sensor nodes in the network is one of the important metrics. Figures 4.14(a) and 4.14(b) shows the average energy spent by the nodes in AOMDV and EENDMRP when network topology is grid and random respectively. Figure 4.14(a) shows the average energy spent by each node in the network. The average energy spent by each node in the EENDMRP is less as compared to the AOMDV. The EENDMRP is a proactive protocol. In the route construction phase, all the nodes in the network generate their routing table and find the path to the sink node. In AOMDV, route to sink node is generated only when it is required. Thus the energy spent on the route discovery is reduced drastically. The average energy spent in AOMDV is more because, the data traffic is not distributed on number of paths. Instead, the alternate node disjoint paths are used in routing based on its order of



(a)

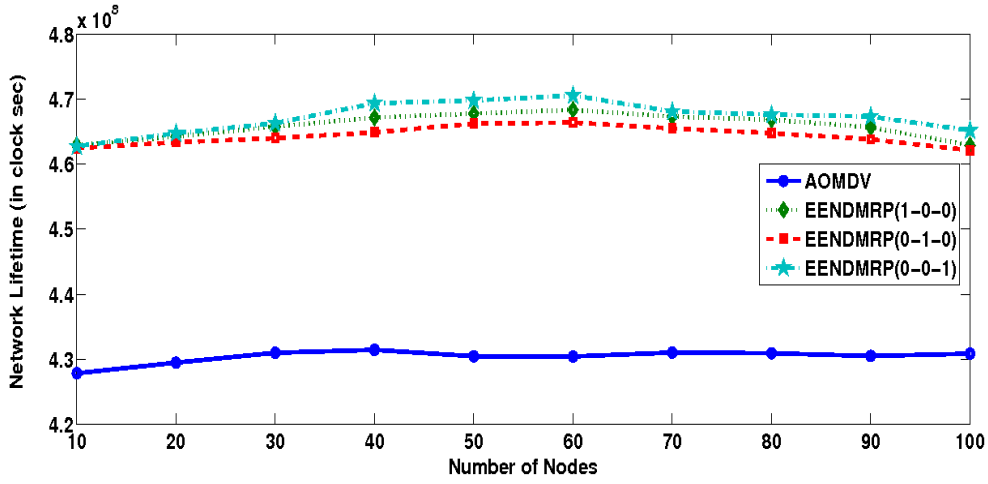


(b)

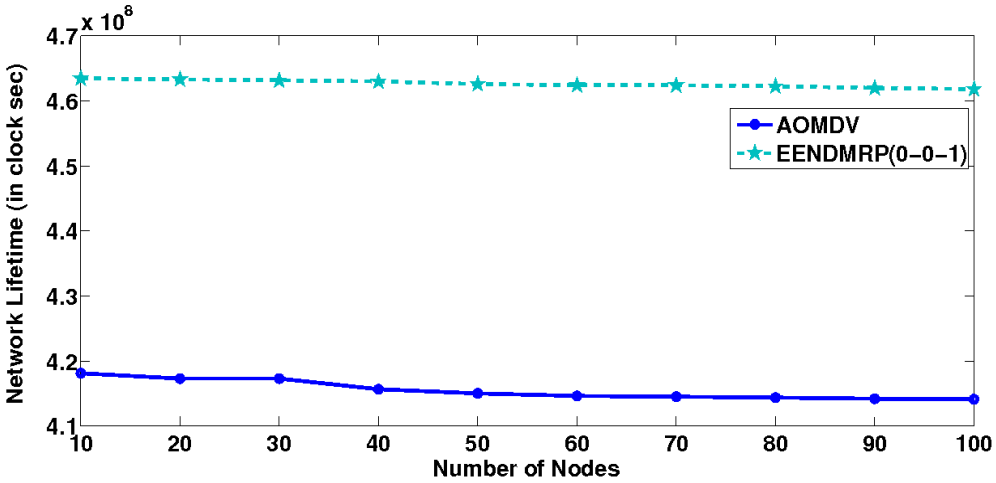
Figure 4.14: Variation of Average Energy Spent with Number of Nodes (a) in Grid Topology (b) in Random Topology

route discovered. The average energy spent is less when the number of nodes is 50, 60 and 70 nodes in EENDMRP. It is because the availability of number of node disjoint paths is high as compared to 100 nodes. When the number of node disjoint paths is high, the data traffic sent in each path is less. Hence, the average energy spent is less with 70 nodes in the network. In Figure 4.14(a) when the number of nodes is 60 there is an energy saving of 13.97% and when the number of nodes is 100, there is an energy saving of 11.73% in EENDMRP compared to AOMDV.

4.3.6 Network Lifetime



(a)



(b)

Figure 4.15: Comparison of Network Lifetime Variation with Number of Nodes (a) in Grid Topology (b) in Random Topology

Improving operational lifetime of the sensor network is a mandatory routing protocol metric in WSN. The effectiveness of the routing protocol is observed based on its contribution in the increase of operational network lifetime. The network is analysed through the complete depletion of the node's residual energy. Figures 4.15(a) and 4.15(b) show the average energy spent by the nodes in AOMDV and EENDMRP when network topology is grid and random respectively. When the number of nodes is 100, there is a reduction of 2.59% of network lifetime in random topology as compared to grid topology. There is 0.03J of increase in energy

spent in EENDMRP when it is in random topology compared to grid topology. But the increase of energy spent in AOMDV is high i.e. 0.11J when it is in random topology as compared to grid topology. It is because of maximum number of hops between the source and destination and high control signals usage in random topology as compared to grid topology. Figure 4.15(a) shows that the operational lifetime of the sensor network is high in EENDMRP compared to AOMDV. When the number of nodes is 60 and 100, the residual energy is 3.1056 and 3.0702, which is 8.5% and 7.3% higher in EENDMRP compared to AOMDV.

4.4 Summary

In this chapter, we proposed the EENDMRP for WSNs. In EENDMRP, the table driven route discovery mechanism is designed. The node disjoint multiple paths are generated based on minimum hops, maximum residual energy and maximum path cost. The primary path based on maximum path cost is selected based on rate of energy consumption and filled queue length in the nodes. EENDMRP is compared with AOMDV routing protocol. The performance of the EENDMRP is evaluated using the routing protocol metrics like PDF, average end-to-end delay, NRL, average energy consumption and network lifetime. It is also evaluated using the grid topology and random topology in the simulation. It is observed that EENDMRP performs better than AOMDV in terms of PDF, NRL, average end-to-end delay and network lifetime.

Chapter 5

Effective Load Sharing Mechanism in EENDMRP

Classical multipath routing has focused on the use of multipaths primarily for load balancing and fault tolerance. The data in multipath routing are sent along different paths, to achieve resilience to failure of a certain number of paths. This data spreading mechanism in multipaths can distribute energy usage among nodes in the network as a means to increase network lifetime (Ganesan et al. 2002; Vidhyapriya and Vanathi 2007).

In this chapter, we discuss two effective load sharing mechanisms: (i) Statistically based and (ii) Ratio based load sharing. The objective of these two load sharing mechanisms is to distribute the data traffic among the multiple paths based on its effective residual energy. It reduces the residual energy variance among the sensor nodes after the data transmission in the network and thus increases the network lifetime.

5.1 Related Works

Maxemchuk (1975) first proposed a traffic dispersion in multipath routing. In dispersive routing, a message is divided into a number of sub messages, which are transmitted in parallel over disjoint paths in the Asynchronous Transfer Mode (ATM) networks. The author focused on reducing the average end-to-end communication delay in dispersed routing as compared to single path transmission. The siring-mode mechanism proposed by Dejean et al. (1991) is a different approach than the traffic dispersion routing. In this mechanism, the long bursts

of data are divided into smaller sub-bursts called strings and these are distributes them on a number of parallel links in the ATM networks.

Many multi-path routing protocols are proposed. Marina and Das (2006) proposed Ad hoc On Demand Multi-path Distance Vector(AOMDV) routing protocol. The AOMDV protocol is a node/link disjoint multi-path routing algorithm and it is a variant of Ad hoc On Demand Distance Vector Routing(AODV) protocol. The AOMDV protocol reduces delay and routing overhead as compared to the AODV protocol. The data distribution mechanism is not used in this work. The multiple paths are made use of to improve the fault tolerance. It also attempted to reduce the frequency of path generation. The multiple paths are used according to their generation in the route discovery phase. The alternate paths are used once the first generated path fails. Hence, the nodes in any alternate paths having minimum residual energy may exhaust their energy fast. This also leads to network partitioning.

Ganesan et al. (2002) proposed a partially disjoint-multi-path routing protocol. This protocol increases resilience to the node failure and it provides energy efficient recovery from failure in WSNs. The protocol is not focused on the energy efficient multiple path construction and load sharing among the multiple paths.

Bheemalingaiah et al. (2009) proposed Power-Aware Node-Disjoint Multi-path Source Routing(PNDMSR) for real-time traffic, which balances the node energy utilisation to increase the network lifetime. It takes the network congestion into account to reduce the routing delay across the network. It also increases the reliability of the data packets reaching the destination. It is a source initiated route discovery mechanism. The protocol maintains k optimal paths among the possible node disjoint paths. Selecting the number of k node-disjoint-paths and traffic distribution among the multiple paths are not indicated.

Mao et al. (2006) presented an analytical framework for the optimal partitioning of real-time multimedia traffic that minimizes the total end-to-end delay. Specifically, it formulates optimal traffic partitioning as a constrained optimization problem using deterministic network calculus and derives its closed-form solution. The framework discusses how to minimize the end-to-end delay in the multi-path routing, but minimizing the energy usage and network lifetime are not taken into consideration.

Vidhyapriya and Vanathi (2007) proposed an energy efficient adaptive multi-path routing technique. It is a sink initiated routing protocol. It utilizes the multiple paths between the

source and sink. The authors claim that the rationale behind traffic spreading is that for a given total energy consumption in the network, at each moment, every node should have spent the same amount of energy. They have not shown the traffic spreading mechanism among the multiple paths. The authors have not discussed how the equal residual energy is spent in nodes.

Gallardo et al. (2007) proposed generalised load sharing mechanism for multipath routing protocol. It smoothens out the data traffic and effectively balances the load on the multiple paths and supports QoS. This mechanism shares the load based on the route weight. Every route in the multiple paths has its route weight. It achieves better load balance among bottleneck nodes and distribution of energy consumption when some nodes have minimum residual energy. But, it fails to guarantee the minimum or low variance in the residual energy of the nodes which participated in routing.

Ming-hao et al. (2011) proposed a load balancing algorithm. It allocates the data traffic among the multiple paths based on its path link cost. The path link cost is the cumulation of all the link's cost in the path. The link cost is evaluated taking residual energy and hop count into account. The data traffic is sent in a path according to its ratio between the total path's cost to its path link cost. The data traffic through the node is not taken into consideration while evaluating path link cost. It may drain its energy fast, since it allows many routes through it. The result fails to confirm the minimum residual variance among the sensor nodes.

Radi et al. (2011) proposed a load balancing algorithm to regulate the data traffic among the multiple paths. The load balancing algorithm estimates the optimal traffic rate of the paths according to their relative quality. Specifically, a lower traffic rate is assigned to paths with higher interference levels. The path quality is measured based on:

(i) Experienced interference level of the path

(ii) Accumulated residual battery level of the nodes

(iii) Probability of backward and forward packet reception over the links

The objective of the load sharing in LIEMRO (Radi et al. 2010) is to balance the load based on its experienced interference levels. Accumulated residual energy levels in a path are taken into consideration to balance the load. But nodes with low residual energy may also be a part of the route. they lose their energy fast and network partition may occur. The result fails to confirm the minimum residual variance among the sensor nodes.

5.2 Load Sharing Mechanisms

We propose two load sharing mechanisms in EENDMRP. These load sharing mechanisms share the data among the number of node disjoint paths between source and destination. They are, (i) Statistically based load sharing mechanism and (ii) Ratio based load sharing mechanism These are shown in algorithms 2 and 3.

5.2.1 Statistically Based Load Sharing Mechanism

Let us assume that k number of multiple node disjoint paths exist between source and sink node. Load at the source node is shared among the multiple node disjoint paths based on its minimum residual energy node in each path. Let RE_i be the minimum residual energy of node in path Pa_i , Pkt_{ts} be the number of packets to send through Pa_i. where, $i = 1, 2, ..., k$. The effective minimum residual energy of the path is evaluated by taking into account, the energy required to transmit the data which is already buffered in node queue for the transmission. It is shown in chapter 4.

$$Pkt_{ts} = \begin{cases} E_{diff}/(E_{tx} + E_{rx}) & energy\ deviation > 0 \\ \lambda/k & energy\ deviation = 0 \end{cases} \tag{5.1}$$

where, λ is the data rate and $E_{diff} = RE_i - \frac{\sum_{i=1}^{k} RE_i}{k}$

In WSN, if routing protocol follows only one path every time to send the sensed data to sink, then nodes in that path will lose energy very fast. This in turn leads to death of nodes and then network will be disconnected. In multipath routing protocols even though the data is sent in multiple paths, ineffective data distribution through a path causes few nodes to drain their energy fast. Therefore, effective node load sharing algorithm is needed in multipath routing protocols. The load sharing mechanism shares the data traffic among the multiple paths and maintains the minimum residual energy variance in the nodes. The source node finds the minimum residual energy RE_i in each path and stores them as $RE_1, RE_2, ..., RE_k$ for k multiple paths. RE_{avg}, the average of all RE_i's is evaluated. The residual energy deviation of a node from the RE_{avg} is evaluated. The positive residual energy deviation confirms that, the Pa_i is able to handle data traffic which consumes energy deviation from the RE_{avg}. Then considering the energy needed to transfer and receive the packet, it can easily calculate the

number of packets to send 'Pkt_{ts}' in a particular path. It minimises the variance among the nodes which participated in routing. This avoids the over utilisation of high residual energy node in the network. The source node reduces node disjoint path by one only when, it receives RERR packet from any node participating in routing or any node's residual energy falls below the residual energy threshold value RE^{τ} in a path. This process continues until residual energy deviation becomes zero i.e., the residual energy in all the paths become equal. Then the load distribution follows round robin method to send the data in the multiple paths. This load sharing algorithm increases the WSNs lifetime by distributing the traffic among the multiple paths based on its available residual energy level.

Algorithm 2 Statistically Based Load Sharing Algorithm

1: $RE_1, RE_2, ..., RE_k$ *the minimum residual energies of* k *multiple paths, respectively.*
2: $\bar{X} \leftarrow (\sum_{i=1}^{k} RE_i)/k$
3: $X \leftarrow (\sum_{i=1}^{k} {RE_i}^2)/k$
4: $Std.Dev \leftarrow \sqrt{X - \bar{X}^2}$
5: ***while*** $Std.Dev \neq 0$ ***do***
6: ***for*** $i = 1$ ***to*** k ***do***
7: ***if*** $(RE_i - \bar{X}) > 0$ ***then***
8: $E_{diff} = RE_i - \bar{X}$
9: $Pkts_{ts} = (E_{diff}/(E_{tx} + E_{rx}))$
10: $RE_i = RE_i - E_{diff}$
11: ***end if***
12: ***end for***
13: ***if*** *RERR is received by the source node by the path ——* $RE_i \leq RE^{\tau}$ ***then***
14: *discard path from the source routing table*
15: $k \leftarrow k - 1$;
16: ***else***
17: $\bar{X} \leftarrow (\sum_{i=1}^{k} RE_i)/k$
18: $X \leftarrow (\sum_{i=1}^{k} {RE_i}^2)/k$
19: $Std.Dev \leftarrow \sqrt{X - \bar{X}^2}$
20: ***end if***
21: ***end while***

Theorem 5.2.1 *The time complexity of statistically based load sharing algorithm is* $O(T * k)$

Proof: Let us analyse the calculation complexity of statistically based load sharing algorithm for the worst case. The residual energy variance may be nil after iterating T times, and the data traffic spreading is done among k number of node disjoint multipaths, so the calculation time for data traffic spreading takes place at most $T * k$ times. $C1$ is the amount of time taken to update the number of paths and $C2$ is the amount of time taken to recalculate residual energy variance. The algorithm may update the number of paths or recalculate residual energy variance. So, it may take $T * max\{C1, C2\}$ amount of time to execute. Since, $C1$ and $C2$ are the constants, the worst case computational complexity of statistically based load sharing algorithm is $O(T * k)$.

5.2.2 Ratio Based Load Sharing Mechanism

In the ratio based load sharing algorithm, once all the node-disjoint path costs are collected at the source node, the source node cumulates all the path costs. The percentage of total data packets through each path is evaluated from the ratio of its path cost to the total path cost. It is shown in the algorithm 3.

Algorithm 3 Ratio Based Load Sharing Algorithm

1: $PC_1, PC_2, ..., PC_k$ *are the path costs of* k *multiple paths respectively.*
2: *costsum=0*
3: ***for*** $i = 1$ ***to*** k ***do***
4: $\quad costsum = costsum + PC_i$
5: ***end for***
6: ***for*** $i = 1$ ***to*** k ***do***
7: $\quad Pkts_{ts} = (PC_i/costsum) * 100$
8: $\quad$ *Send* $Pkts_{ts}$ *packets in* Pa_i *path*
9: ***end for***

Theorem 5.2.2 *The very low residual energy variance among the nodes in the network enhances the network lifetime.*

Proof: Let us assume that, the residual energy variance $var(RE)$ is high in the wireless sensor network (N, L) where, N is the number of nodes and L is the number of links in the network. There exists k number of node disjoint paths between the $source$ and $sink$ nde. Each path has m_i number of nodes where, $i = 1, 2, ..., k$. It is possible that, if $var(RE)$ is high in the sensor network (N, L) then, the $var(RE)$ in m_i number of nodes in k number of node disjoint paths is also high. If residual energy RE_j of j^{th} node is less than residual energy threshold RE^{τ} in path Pa_i and Pkt_{ts} is the number of packets to send in path Pa_i, then the energy consumed in E_{tx} and E_{rx} for first few data packets may exhaust RE_j. Hence its network becomes disconnected. It leads to the conclusion that high $var(RE)$ reduces the network lifetime. So, the converse of it proves that, low $var(RE)$ in network increases the network lifetime.

5.3 Results and Discussion

The performance parameters taken into consideration are energy variance among the sensor nodes, average residual energy in the sensor nodes and network lifetime. The energy variance among the sensor nodes is an important performance parameter to evaluate the load sharing mechanism in WSNs. It can be seen that higher the energy variance among the sensor nodes, lower is the network lifetime.

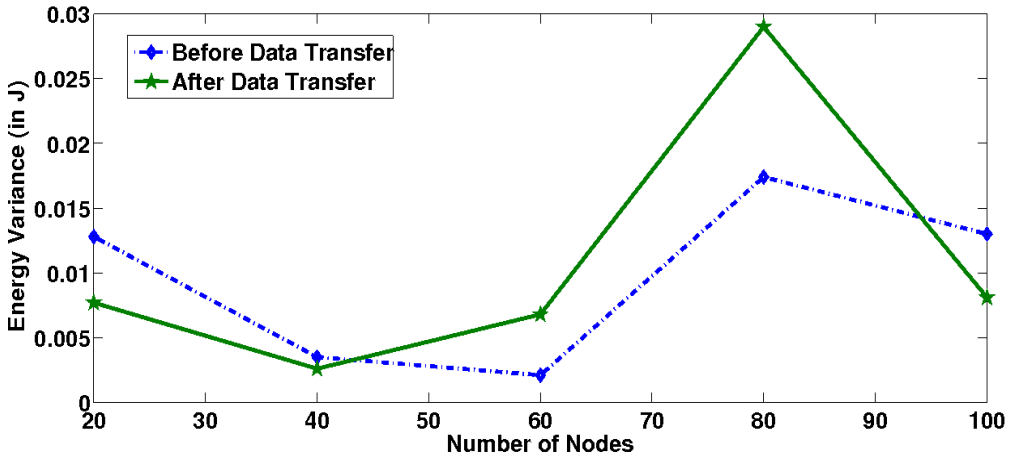


Figure 5.1: Comparison of Variance in the Residual Energy Levels in AOMDV

The proposed load sharing mechanism for energy efficient node disjoint multi-path routing protocol is compared with the AOMDV model. The simulation parameters that are used in

the simulation are as shown in the Table 4.1. Figure 5.1 shows the variance in residual energy levels in the AOMDV model. The variance in the residual energy level before and after the data transmission varies between 0.003 J and 0.03 J. If the variance in the residual energy is high, then the probability of reduction in network lifetime is high. To improve the network lifetime in WSNs, maintaining the uniform residual energy among the nodes, is of utmost importance. It can be observed that the absence of effective load sharing mechanism in the AOMDV model results in high variance in the residual energy levels. The Figures 5.2, 5.3 and 5.4 show the variance in the residual energy levels in the nodes on node disjoint multipaths between the source and sink node. The energy variance is observed before the data transfer and after the data transfer in the EENDMRP and AOMDV multiple paths. The number of nodes considered for the simulation is from 20 to 100.

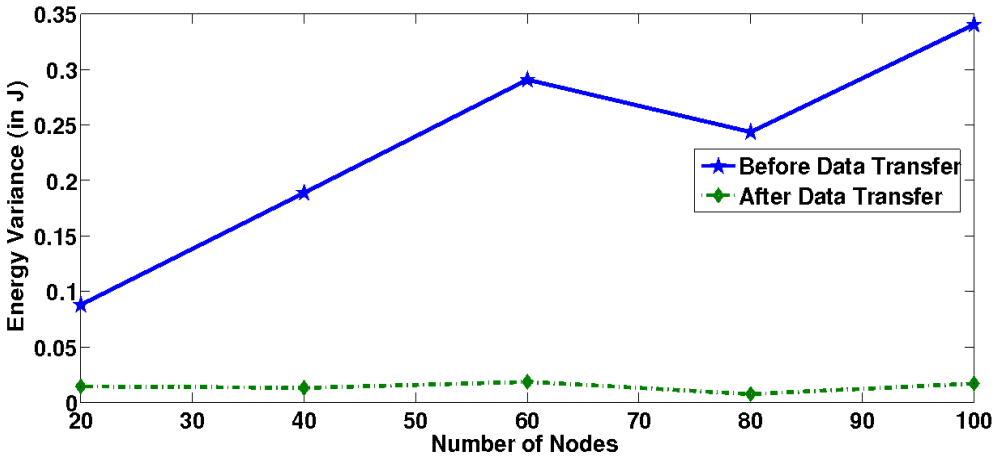


Figure 5.2: Variation of Variance in the Residual Energy Levels with Number of Nodes (EENDMRP with Ratio Based Load Sharing)

Figures 5.2 and 5.3 show the variance of residual energy levels in the EENDMRP with ratio based load sharing and with statistically based load sharing mechanism, respectively. Figure 5.2 shows 0.230 J of average energy variance with ratio based load sharing mechanism before the data transmission and 0.014 J of average energy variance with ratio based load sharing mechanism after the data transmission. There is a reduction of 93.8% energy variance among the residual energy level in the nodes. Figure 5.3 shows 0.230 J of average energy variance with statistically based load sharing mechanism and 0.001 J of average energy variance with statistically based loading mechanism before and after the data transmission respectively. There is a reduction of 98.8% energy variance among the residual energy level in

the nodes. The statistically based load sharing mechanism improves the energy variance by 5% as compared to the ratio based load sharing mechanism.

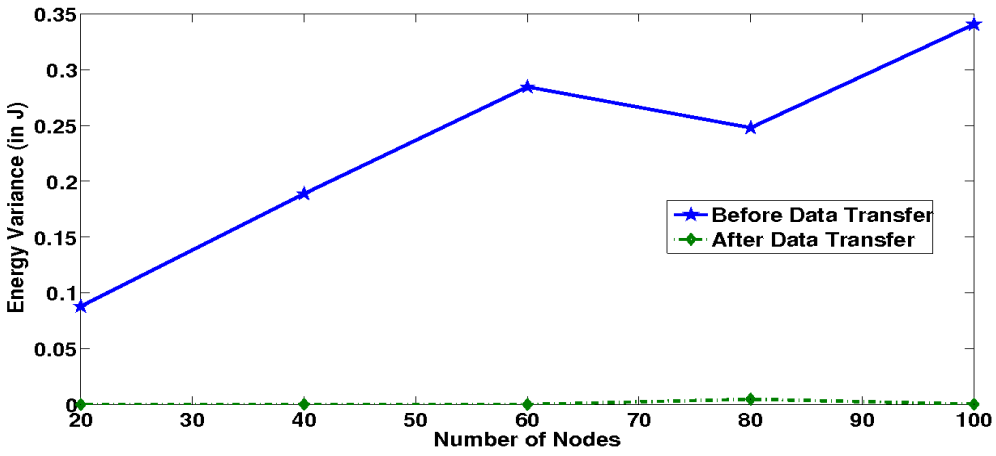


Figure 5.3: Variation of Variance in the Residual Energy Levels with Number of Nodes(EENDMRP with Statistically Based Load Sharing)

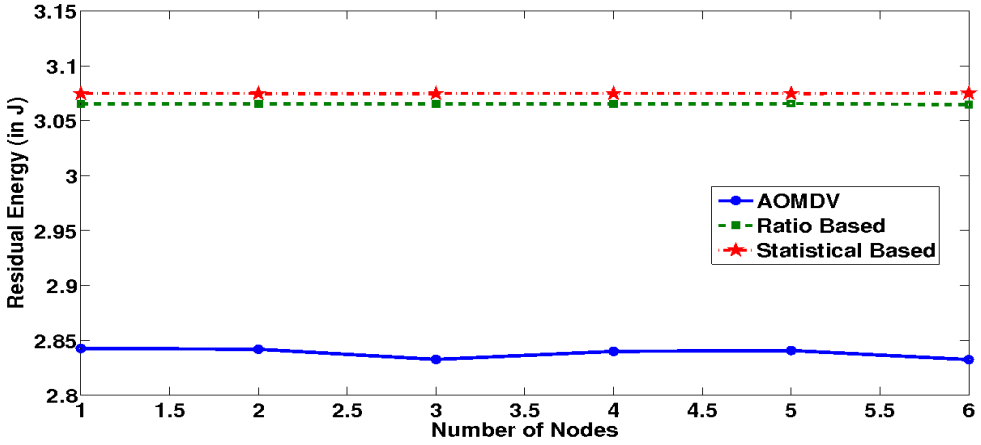


Figure 5.4: Variation in the Residual Energy Levels with Number of Nodes

In the statistically based load sharing algorithm, the number of packets required to send through each node-disjoint path is evaluated by finding the difference in energy level between the mean residual energy and the path residual energy. This mechanism minimises the energy variance by evaluating the standard deviation among the minimum residual energy levels in the node disjoint paths. The residual energy levels among the nodes in the node disjoint path are shown in Figure 5.4. If the number of nodes is 100, then the number of hops between the source nodes and sink node is 6. The average residual energy levels are 2.746 J in AOMDV,

3.065 J in EENDMRP with ratio based sharing and 3.074 J in EENDMRP with statistically based load sharing. There is an energy saving of 11.14% in the EENDMRP with statistically based load sharing as compared to the AOMDV model. Figure 5.5 shows the improvement in

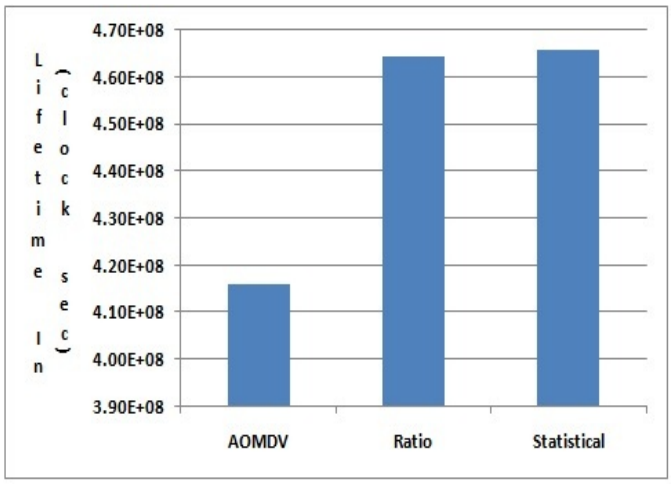


Figure 5.5: Lifetime in AOMDV, EENDMRP with Statistically Based Load Sharing and EENDMRP with Ratio Based Load Sharing

network lifetime of the proposed EENDMRP model due to effective load sharing mechanism. The network lifetime increases when the energy variance among the sensor nodes in the network remains very low. There is an improvement of 10.6% of network lifetime in statistically based load sharing and 10.3% of network lifetime in ratio based load sharing compared to the AOMDV.

5.4 Summary

This work proposes statistically based and ratio based load sharing mechanisms for energy efficient node disjoint multi-path routing protocol. The main objective is to reduce the energy variance among the sensor nodes in the node disjoint paths by spending the residual energy of a node uniformly compared to other nodes on the node disjoint paths. The statistically based load sharing mechanism distributes the traffic among the multiple paths by looking at the residual energy variance between mean residual energy and the minimum residual energy available in the node along the path. The ratio based load sharing mechanism distributes the traffic by evaluating ratio of its path costs to the total path cost. There is a reduction of 93.8% energy variance with ratio based load sharing mechanism and 98.8% energy variance with

statistically based load sharing mechanism in the sensor nodes. There is an energy saving of 11.14% in the EENDMRP with statistically based load sharing compared to the AOMDV model. There is an improvement of 10.6% network lifetime in the statistically based load sharing and 10.3% network lifetime in the ratio based load sharing mechanism as compared to the AOMDV model.

Chapter 6

Security in Energy Efficient Node Disjoint Multipath Routing Protocol for WSNs

In WSNs, a large number of sensor nodes are deployed in phenomena usually in few sq.m to sq.km, where the operational conditions are often harsh or even hostile. These networks operate without a centralised controlling unit or fixed infrastructure like power and wired communication channel. These sensor nodes are largely distributed in the phenomena (sometimes remote place) which is left unattended. The sensor nodes are used in a wide spectrum of applications such as in military, health care and environmental applications, where they manage highly sensitive information. These characteristics of WSN make them vulnerable to threats like node capture,physical tampering, eavesdropping, denial of service, etc. These threats attempt to compromise few legitimate nodes in the network (Sen 2009). Compromise of data is unacceptable in WSN applications since they are expected to provide timely and reliable information. Furthermore, if routing is compromised, then the entire WSN is endangered. In the context of sensitive applications, establishing reliability and availability is considered vital for an application to serve its objectives successfully. Security mechanisms have been designed to offer security in multipath routing. The security mechanisms enhance the availability, resilience and reliability of the network (Stavrou and Pitsillides 2010).

In this chapter, it is proposed to provide security in data routing using public key crypto system. It is attempted to provide security in WSNs routing though the digital signature. MD5 hash function is employed to generate message digest. RSA and ECDSA public key crypto system is used to provide the secure data routing in EENDMRP. It provides the authentication,

integrity and non-repudiation in the WSNs. It defends routing threats such as defending data tampering or altered routing, selective forwarding and byzantine attacks. The correctness of the RSA and ECDSA in EENDMRP is proved. The communication overhead is also analysed.

6.1 Security Requirements in Wireless Sensor Networks

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. Wang et al. (2006) and Sen (2009) bring out the following security requirements for WSNs.

- Availability, which ensures that the desired network services are available even in the presence of internal or external attack such as Denial-of-Service (DoS) attacks.
- Authorization, which ensures that only authorized sensors can be involved in providing information to network services.
- Authentication, which ensures that the communication from one node to another node is genuine. A malicious node cannot masquerade as a trusted network node in the network. It is essential for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node.
- Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients. In order to protect the nodes against traffic analysis attacks, sensor node's public information also need to be encrypted.
- Integrity, which ensures that a message sent from source node to sink is not modified by any malicious intermediate nodes.
- Non-repudiation, which denotes that a node cannot deny the facts about sent and received messages.
- Freshness, which implies that the data is recent and ensures that no adversary can replay old messages. To maintain freshness of the packet, a time specific counter may be used.

- Time synchronization: WSN performs communication in a distributed manner. A collaborative WSN may require synchronization among a group of sensors. It enables better duty-cycling of the radio, accurate and secure localization, beam forming and other collaborative signal processing (Ganeriwal et al. 2005).

- Localization: It is assumed that locators location information sent by each locator are trusted and which cannot be compromised by any attacker. These location information are sent in the beacon information. It is encrypted using a shared global symmetric key that is distributed among the sensor nodes in advance.

6.2 Security Threats in Wireless Sensor Networks Routing Protocols

According to the security requirements in WSNs, the various types of attacks on WSNs can be categorized as follows (Shi and Perrig 2004):

- Attacks on secrecy and authentication
  Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

- Attacks on network availability
  Attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

- Stealthy attacks against service integrity
  In a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential.

The network layer of WSNs is vulnerable to the different types of threats such as spoofed routing information, selective packet forwarding, sinkhole, sybil, wormhole, hello flood, and

acknowledgment spoofing (Sen 2009). Other possible attacks in network layer are, sniffing, data integrity, energy drain, black hole attack, and node replication attack.

6.2.1 Spoofed Routing Information

This is the most common direct attack against a routing protocol. This attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network and increase end-to-end latency (Karlof and Wagner 2003). The standard solution for this attack is authentication, i.e. routers will only accept routing information from valid routers. By adding a message authentication code to the message, the receivers can verify whether the messages have been spoofed or altered. To defend against replayed information, counters or timestamps can be included in the messages (Wang et al. 2006).

6.2.2 Selective Packet Forwarding

A significant assumption made in multi-hop networks is that all nodes in the network will accurately forward received messages (Karlof and Wagner 2003). A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet.The defense against selective forwarding attacks is using multiple paths to send data. It also can avoid malicious node by initiating an alternate route discovery after a fixed time slot.

6.2.3 Sybil Attack

In Sybil attack, one node presents more than one identity in the network (Karlof and Wagner 2003; Sen 2009; Shi and Perrig 2004). Fault-tolerant schemes, distributed storage, and network-topology maintenance protocols are easily compromised by Sybil attacks. For example, a distributed storage scheme may rely on three replicas of the same data to achieve an assured level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while in reality it has not (Wang et al. 2006). Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinated information with their neighbors

to efficiently route the geographically addressed packets. Using the Sybil attack, an adversary node can represent its identity in more than one place at once (Karlof and Wagner 2003).

6.2.4 Sinkhole Attack

In a sinkhole attack, an attacker makes a compromised node look more attractive to neighbouring nodes. The compromised node may forge routing decision parameters such as signal strength, number of hops near to the sink node, residual energy capacity etc. It results in the surrounding nodes choosing the compromised node as the next node to route their data traffic. This type of attack makes selective forwarding very simple and common, as all traffic from a large area in the network will flow through the adversary's node (Karlof and Wagner 2003; Wang et al. 2006). The WSNs are more prone to sinkhole attacks due to their specialized communication pattern. For example,laptop-class adversary with a powerful transmitter can advertise to its neighbouring nodes about its reachability to sink node, its high residual energy, etc. Since, all packets share the same ultimate destination (in networks with only one base station), a compromised node needs only to provide a single high quality route to the base station in order to influence a potentially large number of neighbouring (surrounding) nodes (Karlof and Wagner 2003).

6.2.5 Wormholes Attack

A wormhole is a low-latency link between two portions of the network over which an attacker replays network messages (Wang et al. 2006). An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes, which would normally be multiple hops away from the base station that they are only one or two hops away via the wormhole. This can easily create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station. The neighbouring nodes around the adversary node, send data traffic through it which is actually less attractive (Karlof and Wagner 2003). Wormhole attacks are likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

6.2.6 Hello Flood Attacks

Karlof and Wagner (2003) introduced Hello Flood attacks in WSNs. Many routing protocols in WSNs require nodes to broadcast HELLO packets. It confirms to their neighbors that, it is within the communication range of the sender. This assumption may not be true: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor (Karlof and Wagner 2003). An adversary need not construct legitimate HELLO packet traffic in order to use the HELLO flood attack. It can simply rebroadcast overhead packets.

6.2.7 Acknowledgment Spoofing

Few routing algorithms in sensor networks require acknowledgments to be used (Patel et al. 2009). An attacking node can spoof the acknowledgments of overheard packets destined for neighboring nodes in order to provide false acknowledgment to those neighboring nodes. The adversary node convinces the sender that a weak link is strong or that a dead/disabled node is alive (Karlof and Wagner 2003).

6.3 Public Key Cryptography in Wireless Sensor Networks

Public key encryption is a cryptographic method, which uses asymmetric-key pair: a public and a private key. Asymmetric key pair is used to encrypt and decrypt messages. The public key is made public and is distributed widely and freely. The private key is never distributed and must be kept secret. In public key cryptography, data encrypted with the public-key can only be decrypted with its private key; conversely, data encrypted with the private key can only be decrypted with its public key. This characteristic is used to implement encryption and digital signature. The digital signature in public key encryption provides the authentication security in the system. The highlight of public key cryptography is in providing confidentiality without sharing the secret or private keys. In general, public key cryptography is best suited for an open multi-user environment.

Public key crypto system's counterpart, symmetric key crypto system, is also used in WSN security. The symmetric key crypto system, uses the same key both for encrypting and

decrypting data. Many researchers proposed different symmetric key distribution (sharing) techniques for WSNs (Wadaa et al. 2004; Das and Giri 2011; Jain and Jain 2011; Zhang et al. 2011). These algorithms are relatively easy to implement and need only limited computation power for encryption which (at least some of them) are known to be hard to break even with massive resources. Symmetric key system expects that, all participating nodes have to agree on a common key prior to exchanging data. One simple solution is to replace the common key very frequently at small time intervals for securing WSNs. This periodical sharing of new shared key may induct control overhead in the network if, periodicity is very small and WSNs size is large. This solution is the simplest way for securing WSN. It uses only a single shared key to encrypt traffic over the network, and this key may be periodically updated to ensure more security against eavesdropping (Xu and Ge 2009).

In the recent past various researchers attempted to implement security in WSNs using public key encryption. Public key cryptography provides authentication and confidentiality. The high processing overhead and energy cost makes the implementation of public key cryptography in WSNs infeasible. Few researchers proposed mechanisms to reduce processing and energy cost in elliptic curve cryptography (ECC) (Huang et al. 2011).

6.4 Digital Signature based Security in EENDMRP

In this work we focus on the security to be provided in routing protocol with concern to privacy, authentication and non-repudiation of the data in the network. The security in EENDMRP is analysed using RSA Public key crypto system and ECDSA crypto system. Public key of the crypto systems is communicated to the receiver in two mechanisms. They are, sending the public key in the route construction packet, or sending the source public key along with digital signature.

- Case(i): Sending the source public key in the route construction packet:
  During the route construction phase, the sink broadcasts RCON packet to its neighbouring nodes. The neighbouring node receives the route construction packet. The public key of the sink is appended in its routing table. The neighbouring node updates route construction packet with its public key. It rebroadcasts the route construction to its neighbouring nodes. Similarly, all the nodes in the network update their routing table

with its neighbouring node's public key. If the node receives the route construction packet from the St_{i+1} stage nodes, then it receives the packet. It updates its routing table with the St_{i+1} stage node's public key and discards the packet without forwarding to its neighbouring nodes. The objective is that every node should know the public key of every neighbouring node i.e. the nodes which are reachable in one hop.

- Case(ii): Sending the source node's public key along with digital signature:
  Here, the source node's public key is sent along with the digital signature in public key P_{key} cryptography. During data transfer phase, the source generates the message digest $H(M)$, digital signature d_{sign}. In EENDMRP, the data packet has the path field which specifies the route to sink node with all the intermediate node id's. The source verifies the next neighbouring node in the route, and sends the data packet along with the P_{key}, $H(M)$, and d_{sign}. The neighboring node which receives the data packet with P_{key}, $H(M)$ and d_{sign}, forwards it to its neighbouring node without decrypting it. This process is repeated until the sink node receives the data packet with P_{key}, $H(M)$, and d_{sign}. The sink node, after receiving the data packet along with P_{key}, $H(M)$, and d_{sign} decrypt the $H(M)$ and verifies the authorisation of source node's d_{sign}.

The advantage in sending the source node's public key along with digital signature is that, the energy spent on updating the neighbouring node's P_{key} in every node is avoided. The energy spent on decrypting and encrypting the data packet in every hop between the data source and sink also is avoided. It assures energy efficiency compared to sending the source node's public key in the route construction packet.

6.4.1 RSA Public Key Crypto System based Security in EENDMRP

The security in EENDMRP is designed using the asymmetric (public) key crypto system (digital signature). To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It is used to provide both secrecy and digital signatures. Its security is based on the intractability of the integer factorization problem (Xu and Ge 2009).

The major advantages of RSA are that it does not increase the size of the message. It may be used to provide privacy and authentication over communication links through digital

signatures (Watro et al. 2004). In the past, the constraints of sensor networks have fostered a belief in some researchers that many Internet level security techniques are too heavyweight for sensor networks and that new alternatives must be developed. This opinion has been very valuable in that it has led to interesting new research, But Watro et al. (2004) demonstrate that with careful design, the widely used RSA public key crypto system can be deployed on even the most constrained of the current sensor network devices.

The verification time of RSA is found to be more than 30 times faster than ECDSA. The signature generations is measured to be 8 times slower than ECDSA. Westhoff et al. (2005) suggest that an optimal choice of a digital signature depends on the demand of the application. The RSA is well suited for certificate based systems that require few signature generation and large number (thousands) of verifications. They also state that, when the number of hops is more than 5 between the source and sink node, RSA performs better than ECDSA in CPU execution cost per packet. If the number of hops is less than 5 between source and destination, the ECDSA is better than RSA. Wander et al. (2005) presented the interesting result that the power required to transmit one bit is equivalent to roughly 2090 clock cycles of execution on the microcontroller. This confirms that the energy cost of computation is small compared to that of data transmission. The cost of receiving one byte (28.6 μ J) is roughly half of the cost required to transmit a byte (59.2 μ J).

The results presented in Weiner (1998) and Watro et al. (2004) assert that RSA can also be used in public key cryptography in WSN. But the results in Wander et al. (2005) show that communication energy cost is higher than the computation cost.

6.4.2 Security in EENDMRP

During the data transmission phase, the source node selects the node-disjoint paths to the sink node and sends the data traffic through it. The source node picks M amount of data to send in the node-disjoint primary path to the sink. The MD5 hash function H is used to create message digest $H(M)$ at the source node. The source node generates the digital signature $d_{sign} = (H(M))^d \, mod \, n$ by encrypting the message digest $H(M)$ with its private key d , where $n = p * q$, p and q are random prime numbers with $p \neq q$. The source node forwards d_{sign} with data M, (d_{sign}, M) to its neighbouring node along with the path that it takes to reach

the sink.

The neighbouring node on reception of (d_{sign}, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of $d_{sign}^{e}\ mod\ n$ with message digest $H(M)$. The $d_{sign}^{e}\ mod\ n$ is decrypted using sender's public key (e, n) using the formula,

$$\begin{aligned} d_{sign}^{e}\ mod\ n &= ((H(M))^{d}\ mod\ n)^{e} mod\ n \\ &= (H(M))^{ed}\ mod\ n \end{aligned} \tag{6.1}$$

By applying Little Fermat's theorem and Chinese Remainder Theorem to Equation (6.7), it can be shown that

$$d_{sign}^{e}\ mod\ n = H(M) \tag{6.2}$$

If the generated $H(M)$ by the receiver is equal to the decrypted $H(M)$ of digital signature d_{sign}, then the receiver accepts the data; otherwise rejects the data and informs the sender that the sent data is altered by generating route error packet. This process is repeated in every hop of the node disjoint path between source and destination. The proposed public key crypto system provides authentication, integrity and non-repudiation in the wireless sensor network.

6.4.3 Correctness of RSA Public Key Crypto System in EENDMRP

The confirmation of the data source in the EENDMRP at the sink node is shown in the following steps.

We know that, the digital signature d_{sign} is generated using $d_{sign} = ((H(M))^{d} mod\ n)$ and decrypted using source public key e

$$\begin{aligned} H(M) &= (d_{sign}^{e}(mod\ n)) \\ &= (((H(M)^{d})^{e}(mod\ n)) \\ &= (H(M))^{ed} mod\ n \\ &= (H(M))^{1+k(p-1)(q-1)} mod\ n \\ H(M) &= (H(M)).(H(M))^{k(p-1)(q-1)} mod\ n \end{aligned} \tag{6.3}$$

using, $ed \equiv 1 mod\ (\phi(n))$ and replacing $(\phi(n))$ with $ed = 1 + k(p-1)(q-1)$.

The Little Fermat's theorem states that if $a > 1$ be an integer and p is any prime with $(a, p) = 1$ then $a^{p-1} \equiv 1 mod\ p$

Hence,

$$H(M)^{p-1} mod\ p = 1 \tag{6.4}$$

Similarly, $H(M)^{q-1} mod\ q = 1$

Consider,

$$H(M)[H(M)]^{k(p-1)(q-1)} (mod\ p) \tag{6.5}$$

on rearranging (6.5) is equivalent to

$$H(M)[H(M)^{(p-1)} (mod\ p)]^{k(q-1)}$$

using (6.4) it is equivalent to $H(M)$

Similarly,

$$H(M)[H(M)]^{k(p-1)(q-1)} (mod\ q) = H(M) \tag{6.6}$$

Chinese Remainder Theorem states that, if

$a \equiv b(mod\ p)$, and $a \equiv b(mod\ q)$ then, $a \equiv b(mod\ p.q)$

using (6.5) and (6.6) together with Chinese Remainder Theorem, it can be shown that

$H(M)[H(M)]^{k(p-1)(q-1)} = H(M)(mod\ p.q)$

from Equation (6.3)

$H(M) \equiv H(M)(mod\ n)$ since, $n = p.q$

Hence it confirms that the data received at the sink node is the data sent from last hop of the path.

6.4.4 ECDSA Public Key Crypto System based Security in EENDMRP

Neil Koblitz introduced Elliptic Curve Cryptography (ECC) in 1987. ECC works with points on a curve. The security of this type of public key cryptography depends on the elliptic curve discrete logarithm problem. The main advantage of elliptic curve cryptography is that the keys can be much smaller (Kute et al. 2009). It became an accepted alternative to RSA crypto systems. The advantages of ECC over RSA are significant in smaller parameter usage. The

smaller parameters in ECC reduce enormous processing time and network resources in the communication system. These advantages are specifically important in environments where power consumption, processing power, storage space and bandwidth are limited (Balitanas 2009).

The ECDSA is well suited for resource constrained environments such as smart cards, cellular phones, PDAs, digital postage marks and sensor networks. 128-bit protection is necessary to achieve relatively lasting security in the system. Table 6.1 shows that, for 80 bit security, RSA requires 1024 bit key length whereas for ECC based public key cryptography 163 bits are just enough. There is nearly six fold increase in the ECC public key size as compared to RSA. The requirement of the public key length in ECC and RSA for 80 bit security requirements are 2 times and 12 times respectively.

Table 6.1: NIST Guidelines for Public-Key Sizes with Equivalent Security Levels (Balitanas 2009)

Security Bits	**RSA**	**ECC**
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

- ECDSA Security in EENDMRP

  We assume that every node in the network knows its domain parameters for an elliptic curve. The elliptic curve domain parameters over finite field F_p are $p, a, b, G,$ and n. where, p is the prime number defined over the finite field F_p, a and b are the parameters defining the curve $y^2(mod\, p) = x^3 + ax + b(mod\, p)$. G is the generator point (x_G, y_G), a point on the elliptic curve chosen for cryptographic operations and n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and $n - 1$. Every node i has its own private key, d_i and public key Q_i. Every node generates its public key using $Q_i = d_i * G$.

  In the data transmission phase, the source node selects the node-disjoint paths to the sink node and sends the data traffic through it. The source node picks the M amount of data

to send in the node-disjoint primary path to the sink node. The MD5 hash function is used to create message digest $H(M)$ at the source node. Generate the digital signature $(r1, r2)$.

$r1$ and $r2$ are evaluated as $r1 = x1(mod\, n)$, where $(x1, y1) = c * G, (c < n)$ is a chosen random integer where $r1 \neq 0$.

$r2 = c^{-1}((H(M)) + d_S * r1)(mod\, n)$. If $r2 = 0$, then change the random integer c. The source node forwards the digital signature $((r1, r2), M)$ in the selected node disjoint path.

The neighbouring node which receives $((r1, r2), M)$ initiates the initial verification by checking whether $r1$ and $r2$ are the integers in $[1, n-1]$. If, $r1$ and $r2$ are in $[1, n-1]$ then it honours the digital signature. Otherwise it dishonours the digital signature and discards the message M or data packet received. The actual verification of $((r1, r2), M)$ is done by the neighboring node. The neighbouring node applies the MD5 hash function on received message M and generates its $(H(M))$. The neighbouring node calculates $(l1, l2)$, where, $(l1, l2) = ((H(M)) * r2^{-1} * G + r1 * r2^{-1} * Q_S)(mod\, n)$ and Q_S is source node's public key. If $l1$ is equal to $r1$, then the neighbouring node confirms the source node's digital signature and the receiver accepts the data packets M, otherwise it rejects the data packet M. The receiver node informs the sender that the sent data is altered through by generating route error packet. This process is repeated in every hop of the node disjoint path between the source and sink.

- Correctness of ECDSA in EENDMRP

  We know that,

$$\begin{aligned}(l1, l2) &= ((H(M)) * r2^{-1} * G + r1 * r2^{-1} * Q_S)(mod\, n) \\ &= [((H(M)) * G + r1 * Q_S)]r2^{-1}(mod\, n) \end{aligned} \tag{6.7}$$

  substituting the public key Q_S of source node by $d_S * G$.

$$\begin{aligned}(l1, l2) &= [((H(M)) * G + r1 * d_S * G)]r2^{-1}(mod\, n) \\ &= [(H(M)) + r1 * d_S]r2^{-1} * G(mod\, n) \end{aligned} \tag{6.8}$$

from $r2 = c^{-1}((H(M)) + d_S * r1)(mod\ n)$, the above equation (6.8) becomes

$$\begin{aligned}(l1, l2) &= k * r2 * r2^{-1} * G(mod\ n) \\ &= c * G(mod\ n) \\ &= (x1, y1)(mod\ n) \\ l1 &= x1(mod\ n) \\ l1 &= r1\end{aligned}$$

6.4.5 Defending the WSN Threats

The specific wireless sensor network attacks defended in this work are: data tampered or altered routing, Sybil attack, HELLO attacks, selective forwarding, sink hole and Byzantine attack.

- Defending Data Tampered or Altered Routing

  The most direct attack against routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false-error messages, partition the network, increase end-to-end latency, etc. In digital signature based crypto system, public key of the sender is required to decrypt the message digest at the data receiver node. If the decrypted digital signature and evaluated message digest at the receiver are equal, then it proves the data integrity and non-repudiation in the network.

- Selective Forwarding and Sink Hole

  Multi-hop networks are often based on the assumption that participating nodes will faithfully forward received messages. In selective forwarding attack, the malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet that it receives. In the EENDMRP model, there is no chance of the malicious node to drop the packets or to divert the data traffic in the network, because the source node selects the node-disjoint path to route the data from its routing table. Every intermediate node knows its next neighbouring node.

So there is no chance of the malicious node to getting the data traffic from the legitimate node in the node-disjoint path and divert the data traffic.

- Byzantine Attack

  In this attack, a compromised node or a set of compromised nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets in non- optimal routes and selectively dropping packets. It is very difficult to detect the Byzantine attacks, since the networks do not exhibit any abnormal behaviour. The EENDMRP model is a sink initiated, proactive multi-path routing protocol. The routes are constructed in the route construction phase, which is initiated by the sink node. Every node in the network can communicate with or forward the RCON packets to its next stage nodes and not to the previous stage nodes. This mechanism avoids the formation of loops. The node disjoint multi path from the source to sink node is selected from its routing table. Selecting a non-optimal path by the malicious node to the sink node is not possible. The primary path and node disjoint paths are selected by the source node.

6.5 Results and Discussion

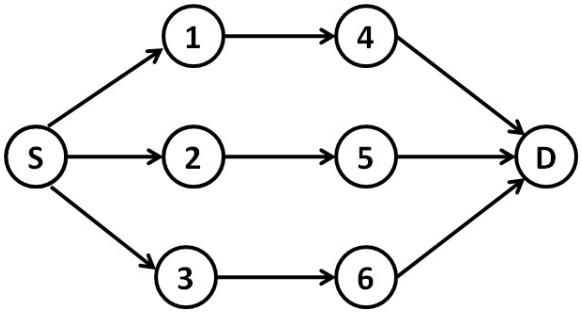


Figure 6.1: Node Disjoint Multipath

In this chapter security in EENDMRP using RSA and ECDSA public key crypto systems is discussed. The work shows the correctness of RSA and ECDSA in EENDMRP. It analyses the communication overhead during transmission of public keys and digital signatures in both RSA and ECDSA. It also analyses the energy spent for public key and digital signature transmission in EENDMRP. The simulation parameters set up are as shown in Table 4.1. The work analyses the energy spent for public keys and digital signatures in RSA and ECDSA in

EENDMRP for the network shown in the Figure 6.1. The energy spent in public key communication is shown in Table 6.2. The public key size is varied from 32 bits to 1024 bits. We

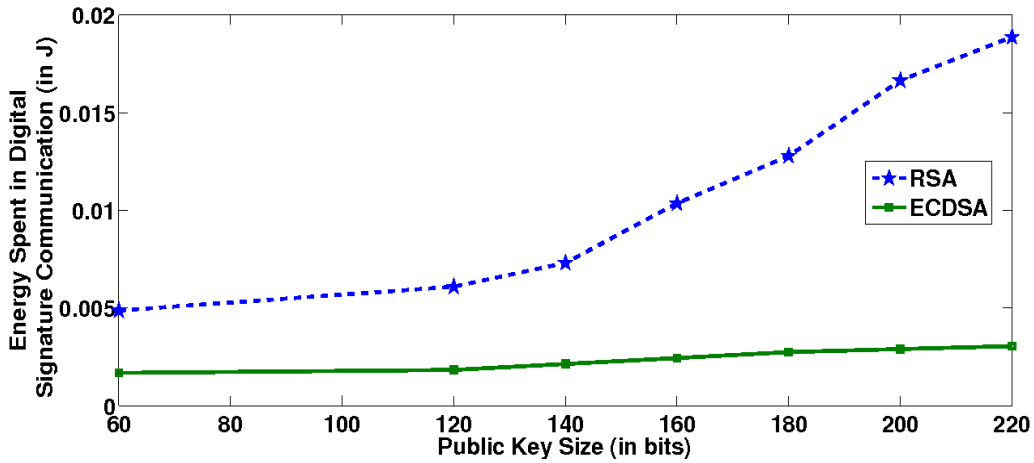


Figure 6.2: Variation of Energy Consumption of RSA and ECDSA with the public key size

discussed in section 6.4 that public key communication can be communicated through 2 types.
Case (i): Sending the source public key in the route construction packet and
Case (ii): Sending the source node's public key along with digital signature
From Table 6.2, it can be seen that, the energy spent in case(i) is 55.5% more as compared to case(ii). This is because, in case(ii), the receiver must know the public key of the data traffic sender to decrypt. So initially, every node knows the public key of its neighboring nodes through the RCON packet exchange. In EENDMRP with case(i), the sink node broadcasts the public key to its neighbouring nodes. The neighbouring node after receiving RCON packet, updates its routing table with the sink node public key. It updates the route construction packet with its public key and rebroadcasts to its neighboring nodes. If the node receives the route construction packet from the St_{i+1} stage nodes, then it receives the packet. It updates its routing table with the St_{i+1} stage node's public key and discards the packet without forwarding to its neighbouring nodes.

Figure 6.2 shows the energy spent in d_{sign} communication in EENDMRP. The d_{sign} is generated using the smaller size of P_{key} between 60 and 220 bits. For smaller P_{key}, the energy spent in communication is less. The energy spent in RSA d_{sign} is very high compared to that in ECDSA. When the key size is 60 bits in RSA the energy spent is 0.0048 J and in ECDSA the energy spent is 0.0016 J. There is an increase of 4.5 times of average energy

Table 6.2: Energy Spent (in J) in Public Key Communication overhead in EENDMRP

P_{key} **(in bits)**	P_{key} **in Route Construction Packet**	P_{key} **with** d_{sign}
32	0.04399776	0.026523072
64	0.08799552	0.053046144
128	0.17599104	0.106092288
256	0.35198208	0.212184576
512	0.70396416	0.424369152
1024	1.40792832	0.848738304

Table 6.3: Digital Signature Size Ratio between RSA and ECDSA

P_{key} **(in bits)**	**Ratio**
60	2.909
120	3.333
140	3.428
160	4.25
180	4.666
200	5.725
220	6.2

saving in EENDMRP with RSA as compared to ECDSA. The ratio between the energy spent in EENDMRP with RSA and ECDSA is increasing with the increase in the key size. It can be seen from Table 6.3 that when the key size is 60 bits its ratio is 2.9 and when the key size is 220 bits it is 6.25.

6.6 Summary

In this chapter, secure data routing in EENDMRP is shown. To have security in data routing, RSA and ECDSA public key encryption are used. MD5 hash function is used in the digital signature generation. EENDMRP provided authentication, integrity and non-repudiation for WSNs. The correctness of the RSA and ECDSA in EENDMRP is proved. The public key broadcasting in the network is analyzed through two techniques, (i) sending the source public

key in the route construction packet and (ii) sending the source node public key along with the digital signature. Sending the source node public key along with the digital signature mechanism reduces the energy spent by 47.4% as compared to sending the public key in the route construction packet mechanism. The size of the digital signature generated in RSA increases as the size of public key is increased. When the key size is 60 and 120 bits it is 2.9 and 6.2 times more than the ECDSA in EENDMRP. The digital signature based security in EENDMRP, defended routing threats specifically, defending data tampering or altered routing, selective forwarding and Byzantine attacks.

Chapter 7

Conclusions and Future Enhancements

The major objective of this thesis is to propose a sink initiated, proactive, node disjoint multipath routing protocol for WSN based on rate of energy consumption and traffic through the node. In this thesis we have discussed the advantages of proactive routing protocol as compared to reactive protocols in static topology WSNs. The novelty of this work is the sink initiated route discovery with proactive node disjoint multipath data routing. In this work we have considered the filled data packets in the node's queue to evaluate the node's residual energy in the routing. In this thesis, the classifications of energy efficient routing protocols are discussed. Also highlighted is the classification of mutipath routing protocols in WSN.

We have designed the lifetime analytical model for data transfer phase and route redundancy model for route maintenance for node disjoint multipath routing protocol in WSN. The simulation results confirm that the network lifetime is increased when data rate along the multiple paths is varied in accordance with the available node residual energy. The network reliability is increased in node disjoint multipath networks, when each node disjoint path has maximum number of redundant paths and minimum number of nodes in each redundant path.

In the proposed EENDMRP, the sink node initiates route construction mechanism. In this phase, all the nodes in the network generate multiple node disjoint paths between source and destination. This is also updated in its routing table. Every node generates node disjoint multiple paths from its routing table. The primary path is constructed based on number of hops, residual energy and path cost. The primary path, constructed based on path cost, performs better in PDF, average energy spent and network lifetime. But the primary path constructed based on number of hops, performs better in average end-to-end delay. EENDMRP performs

better than the AOMDV. The EENDMRP increases PDF by 4% , reduces average end-to-end delay by 9.8 times, reduces NRL by 3.8 times , reduces 11.73% of energy spent and increases network lifetime by 7.3% compared to AOMDV. The performance of EENDMRP is also analysed for grid and random topology networks. In grid topology, the EENDMRP performs better than random topology. In average end-to-end delay, random topology performs better than grid topology when the number of nodes is less.

In the proposed EENDMRP, an effective load sharing mechanism is introduced. Here, we proposed (i) Statistically based load sharing mechanism and (ii) Ratio based load sharing mechanism. The objective of load sharing mechanism is to balance the energy expenditure among the nodes. The performance of the load sharing mechanisms is analysed through a new metric called the residual energy variance. The residual energy variance is identified before the data transfer and after the data transfer. The results show that statistically based load sharing mechanism performs better than ratio based mechanism and AOMDV routing protocol. There is a reduction of 98.8% residual energy variance in the statistically based load sharing when compared with those before and after the data transfer. There is a 4.5% and 88.8% of improvement compared to ratio and AOMDV in residual energy variance maintenance.

In addition to energy efficient data routing in WSNs, security is added in the EENDMRP. To have security in data routing, RSA and ECDSA public key encryption is used. MD5 hash function is used in the digital signature generation. The security provided is authentication, integrity and non-repudiation for routing. The correctness of the RSA and ECDSA in EENDMRP is proved. The digital signature based security in EENDMRP, defended routing threats specifically, defending data tampering or altered routing, selective forwarding and Byzantine attacks.

7.1 Future Enhancements

The proposed EENDMRP may be extended in different directions.

- In the EENDMRP, the data considered are physical data and all the data have equal importance. The multimedia data such as still image data, moving image data are not considered. In multimedia data routing, priority among the data to be routed is needed.

Priority based load sharing in the node disjoint multipath networks offers multi objective problem.

- In a highly dense network, more number of multiple paths may be generated. In this, to decide how many paths to be used and which paths are to be used to optimize the network resources in resource constrained WSN is a challenge.
- Usage of public key cryptography in WSN with the benefits of ECDSA's public key generation and RSA's verification technique in a security system may result in an effective crypto system suitable for WSNs.

Appendix-A

Network Simulator (Version 2), widely known as NS2, is simply an event- driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides the users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator, the foundation of which is based on NS. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter Network Testbed (VINT) project. Currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle is just a string in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object. In the OTcl domain, a handle acts as a front end which interacts with users and other OTcl objects. It may define its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures after simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. To analyze a particular behavior of the network, users can extract a relevant subset of text-based data and transform it to a more conceivable presentation.

References

Abbas, A. M. and Abbasi, T. A. (2006). "An Analytical Framework for Disjoint Multipath Routing in Mobile Ad hoc Networks". In *Proceeding of The IFIP International Conference on Wireless and Optical Communications Networks*, pages 5–8.

Akkaya, K. and Younis, M. (2003). "an energy-aware qos routing protocol for wireless sensor networks". In *Proceeding of International Conference on Distributed Computing Systems Workshops (ICSDSW)*, pages 710–715.

Akyildiz, I. F., Sankarasubramaniam, Y., and Cayirci, E. (2002). "wireless sensor networks: A survey". *Computer Networks*, 38(4):393–422.

Al-Karaki, J. N. and Kamal, A. E. (2004). "Routing Techniques in Wireless Sensor networks:A Survey". *IEEE Wireless Communications*, 11(6):6–28.

Al-Karaki, J. N., Ul-Mustafa, R., and Kamal, A. E. (2004). "Data Aggregation in Wireless Sensor Networks - Exact and Approximate Algorithms". In *Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR) 2004*, pages 241–245.

AlNuaimi, M., Sallabi, F., and Shuaib, K. (2011). "A Survey of Wireless Multimedia Sensor Networks Challenges and Solutions". In *International Conference on Innovations in Information Technology (IIT), 2011*, pages 191–196.

Alwan, H. (2010). Reliable fault-tolerant multipath routing protocol for wireless sensor networks. In *2010 25th Biennial Symposium on Communications (QBSC)*, pages 323–32.

Balitanas, M. O. (2009). "Wi Fi Protected Access-Pre-Shared Key Hybrid Algorithm". *International Journal of Advanced Science and Technology*, 12(1):35–44.

Batra, N., Jain, A., and Dhiman, S. (2011). ”an optimized energy efficient routing algorithm for wireless sensor networks”. *International Journal of Innovative Technology & Creative Engineering*, 1(5):41–45.

Bheemalingaiah, M., Naidu, M. M., Sreenivasa Rao, D., and Varaprasad, G. (2009). ”Power-aware Node-Disjoint Multipath Source Routing with Low Overhead in MANET”. *International Journal of Mobile Network Design and Innovation*, 3(1):33–45.

Blair, W. and Bar-Shalom, T. (1996). ”Tracking Maneuvering Targets with Multiple Sensors: Does more Data always mean better estimates?”. *IEEE Transactions on Aerospace and Electronic Systems*, 32(1):450–456.

Braginsky, D. and Estrin, D. (2002). ”Rumor Routing Algorithm for Sensor Networks”. In *Proceedings of the First Workshop on Sensor Networks and Applications (WSNA)*, pages 22–31.

Cai, K., Xiong, S., Shi, J., and Wei, G. (2008). ”An Energy-efficient Multiple Paths Routing Algorithm for Wireless Sensor Networks”. In *11th IEEE Singapore International Conference on Communication Systems,ICCS 2008*, pages 1690–1694.

Carlos F, G., Pablo, H. G., Joaquin, G., and Perez-diaz, J. A. (2007). ”Wireless Sensor Networks and Applications: a Survey”. *IJCSNS International Journal of Computer Science and Network Security*, 7(3):264–27.

Challal, Y., Ouadjaout, A. A., Lasla, N., Bagaa, M., and Hadjidj, A. (2011). ”Secure and Efficient Disjoint Multipath Construction for Fault Tolerant Routing in Wireless Sensor Networks”. *Journal of Network and Computer Applications*, 34:1380–1397.

Chang, J.-H. and Tassiulas, L. (2004). ”Maximum Lifetime Routing in Wireless Sensor Networks ”. *IEEE/ACM Transactions on Networking*, 12(4):609–619.

Cheng, L., Das, S. K., Cao, J., CanfengChen., and JianM. (2010). ”Distributed Minimum-Transmission Multicast Routing Protocol for Wireless Sensor Networks”. In *39th International Conference on Parallel Processing*, pages 188–197.

Chu, M., Haussecker, H., and Zhao, F. (2002). ”Scalable Information Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks”. *The International Journal of High Performance Computing Applications*, 16(3):293–313.

Das, A. K. and Giri, D. (2011). ”An Identity Based Key Management Scheme in Wireless Sensor Networks”. *CoRR*, 1103(4676):arXiv:1103.4676.

Dejean, J. H., Dittmann, L., and Lorenzen, C. N. (1991). ”Performance Improvement of an ATM Network by Introducing String Mode”. In *Proceeding of IEEE lNFOCOM '1991*, pages 1394–1402.

Djamel, D. and Balasingham, I. (2011). ”Traffic-Differentiation-Based Modular QoS Localized Routing for Wireless Sensor Networks”. *IEEE Transactions on Mobile Computing*, 10(6):797–809.

Erdene-Ochir, O., Minier, M., Kountouris, A., and Valois, F. (2010). ”Toward Resilient Routing in Wireless Sensor Networks: Gradient-Based Routing in Focus”. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference*, pages 478–483.

Felemban, E., Lee, G. C., and Ekici, E. (2006). ”MMSPEED: Multipath multi- SPEED Protocol for QoS Guarantee of Reliability and timeliness in Wireless Sensor Networks”. *IEEE Transaction on Mobile Computing*, 5(6):738–754.

Gallardo, J. R., Gonzalez, A., Villasenor-Gonzalez, L., and Sanchez, J. (2007). ”Multipath routing using generalized load sharing for wireless sensor networks”. In *IASTED International Conferences on Wireless and Optical Communications*, pages 1–6.

Ganeriwal, S., Capkun, C., Han, C. S., and Srivastava, M. . B. (2005). ”Secure Time Synchronization Service for Sensor Networks”. In *Proceedings of the 4th ACM Workshop on Wireless Security*, pages 97–106.

Ganesan, D., Govindan, R., Shenker, S., and Estrin, D. (2002). ”Highly-Resilient, Energy-Efcient Multipath Routing in Wireless Sensor Networks”. *Mobile Computing and Communications Review*, 1(2):1–13.

Ganjali, Y. and Keshavarzian, A. (2004). ”Load Balancing in Ad Hoc Networks: Single-path Routing vs. Multi-path Routing”. In *Proceeding of IEEE INFOCOM 2004*, pages 1120–1125.

Gao, T., Jin, R., Wang, L., and and, J. Q. (2010). ”A Novel Node-Disjoint Multipath Routing Protocol for Wireless Multimedia Sensor Networks”. In *2nd International Conference on Signal Processing Systems (ICSPS) 2010*, pages 790–794.

Ghica, O., Trajcevski, G., Scheuermann, P., Bischof, Z., and Valtchanov, N. (2010). ”Controlled Multi-Path Routing in Sensor Networks Using Bezier Curves”. *Computer Journal*, pages 1–25.

Guan, K. and He, L.-M. (2010). ”A Novel Energy-Efficient Multi-Path Routing Protocol for Wireless Sensor Networks”. In *2010 International Conference on Communications and Mobile Computing*, pages 214–218.

Haas, Z. J., Pearlman, M. R., and Samar, P. (2003). ”The Zone Routing Protocol (ZRP) for Ad Hoc Networks”. Technical report, IETF Draft.

He, T., Stankovic, J. A., Lu, C., and Abdelzaher, F. T. (2005). ”A Spatio Temporal Communication Protocol for Wireless Sensor Networks”. *IEEE Transacton on Parallel Distributed Systems*, 16(10):995–1006.

Heikalabad, S. R., Rasouli, H., Rahmani, N., and Nematy, F. (2011). ”QEMPAR: QoS and Energy Aware Multi-Path Routing Algorithm for Real-Time Applications in Wireless Sensor Networks”. *IJCSI International Journal of Computer Science Issues*, 8(1):466–471.

Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. (2000). ”Energy-efficient communication protocol for wireless microsensor networks”. In *Proceedings of the 33rd AnnualV Hawaii International Conference on System Sciences (HICSS)*, pages 3005 – 3014.

Hou, T., Jianping, Y., and Midkiff, S. F. (2006). ”Pan Maximizing the Lifetime of Wireless Sensor Networks through Optimal Single-Session Flow Routing”. *IEEE Transactions on Mobile Computing*, 5(9):1255–1266.

Hoyland, A. and Rausand, M. (1994). *"System Reliability Theory: Model and Statistical Methods"*. Wiley & Sons, Inc.

Hu and Kumar, S. (2003). "Multimedia Query with QoS Considerations for Wireless Sensor Networks in Telemedicine". In *proceeding of socieity of Photo-Optical Instrumentaion Enginneers Intnernational COnference on Internet Multumedia Mangament Systems*, pages 1–11.

Huang, X., Sharma, D., Aseeri, M., and Almorqi, S. (2011). "Secure Wireless Sensor Networks with Dynamic Window for Elliptic Curve Cryptography". In *Electronics, Communications and Photonics Conference (SIECPC), 2011*, pages 1–5.

Hung, M. C.-C., Lin, K. C.-J., Chou, C.-F., and Hsu, C.-C. (2011). "EFFORT: Energy-Efficient Opportunistic Routing Technology in Wireless Sensor Networks". *Wireless Communications and Mobile Computing*, page doi: 10.1002/wcm.1140.

Hyung-WookYoon., Lee, B.-H., Lee, T.-J., and Chung, M. (2004). "Energy Efcient Routing with Power Management to Increase Network Lifetime in Sensor Networks". *, Springer-Verlag Lecture Notes in Computer Science*, 3046:46–55.

Intanagonwiwat., Govindan, R., and Estrin, D. (2000). "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks". In *Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_00)*, pages 56–67.

Jacquet, P., Muhlethaler, P., and Qayyum, A. (2002). "Optimized Link State Routing Protocol". Technical report, ETF Internet Draft.

Jain, Y. K. and Jain, V. (2011). "An Efficient Key Management Scheme for Wireless Networks". *International Journal of Scientific & Engineering Research*, 2(2):1–7.

Jin, Z., Jian-Ping, Y., Si-Wang, Z., Ya-Ping, L., and Guang, L. (2009). "A Survey on Position-Based Routing Algorithms in Wireless Sensor Networks Algorithms". *Algorithms*, 2:158–182.

Jung., hoon. Lee, J., and hee. Roh, B. (2008). ”An Optimized Node-Disjoint Multi-path Routing Protocol for Multimedia Data Transmission over Wireless Sensor Networks”. In *International Symposium on Parallel and Distributed Processing with Applications*, pages 958–963.

Karlof, C. and Wagner, D. (2003). ”Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”. *Ad Hoc Networks*, 1:293–315.

Kaseva, V., Hämäläinen, T. D., and Hännikäinen, M. (2011). ”A Wireless Sensor Network for Hospital Security: From User Requirements to Pilot Deployment”. *EURASIP Journal on Wireless Communications and Networking*, 2011.

Kay, R. and Mattern, F. (2004). ”The Design Space of Wireless Sensor Networks”. *EEE Wireless Communications*, 11(6):54–61.

Khan, P., Hussain, M., and Kwak, K. S. (2009). ”Medical Applications of Wireless Body Area Networks”. *International Journal of Digital Content Technology and its Applications*, 3(3):1–9.

Kim, D., Garcia-Luna-Aceves, J. J., and Obraczka, K. (2003). ”Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate”. *IEEE Transactions on Mobile Computing*, 2(4):161–173.

Ko, H. Y. and Vaidya, N. (1998). ”Location-Aided Routing (LAR) in Mobile Ad Hoc Networks”. In *ACM/IEEE International Conference on Mobile Computing and Networking*, pages 66–75.

Kurata, N., Suzuki, M., Saruwatari, S., and Morikawa, H. (2008). ”Actual Application of Ubiquitous Structural Monitoring System using Wireless Sensor Networks”. In *World Conference on Earthquake Engineering*.

Kute, V. B., Paradhi, P. R., and Bamnote, G. R. (2009). ”A Software Comparision of RSA and ECC”. *International Journal Of Computer Science And Applications*, 2(1):61–65.

Le, Z., Becker, E., Konstantinides, D. G., Ding, C., and Makedon, F. (2010). ”Modeling Reliability for Wireless Sensor Node Coverage in Assistive Testbeds”. In *PETRA 10*, pages 23–25.

Lindsey, S. and Raghavendra, C. S. (2002). ”PEGASIS: Power Efficient Gathering in Sensor Information Systems”. In *Proceedings of the IEEE Aerospace Conference*, pages 1125–1130.

Lindsey, S., Raghavendra, C. S., and Sivalingam, K. (2001). ”Data Gathering in Sensor Networks Using the Energy Delay Metric”. In *Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing*, pages 2001–2008.

Lou, W. (2005). ”An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks”. In *IEEE 2nd International Conference on Mobile Adhoc and Sensor Systems, MASS 2005*.

Manjeshwar, A. and Agrawal, D. P. (2001). ”TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks”. In *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, pages 2009–2015.

Manjeshwar, A. and Agrawal, D. P. (2002). ”APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks”. In *Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing*, pages 95–202.

Mao, S., Panwar, S. S., and Thomas, H. Y. (2006). ”On Minimizing End-to-End Delay With Optimal Traffic Partitioning”. *IEEE Transactions on Vehicular Technology*, 55(2):681–690.

Marina, M. K. and Das, S. R. (2006). ”Ad Hoc On-Demand Multipath Distance Vector Routing”. *Wireless Communications and Mobile Computing*, 1(6):969–988.

Maxemchuk, N. F. (1975). ”Dispersity Routing”. In *Proceeding of ICC ’75*, pages 28–37.

Meghdadi, M., Ozdemir, S., and Güler, I. (2011). ”A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”. *IETE Tech Rev*, 28(2):89–102.

Ming-hao, T., Ren-lai, Y., Shu-jiang, L., and Xiang-dong, W. (2011). ”Multipath Routing Protocol with Load Balancing in WSN Considering Interference”. In *6th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2011*, pages 1062–1067.

Minhas, M. R., Gopalakrishnan, S., and Leung, V. C. M. (2009). "An Online Multipath Routing Algorithm for Maximizing Lifetime in Wireless Sensor Networks". In *2009 Sixth International Conference on Information Technology: New Generations*, pages 581–586.

Nandi, S. and Yadav, A. (2011). "Cross Layer Adaptation for QoS in WSN". *International Journal of Computer Networks & Communications*, 3(5):287–301.

Oh, H. W., Jang, J. H., Moon, K. D., Park, S., Lee, E., and Kim, S.-H. (2010). "An Explicit Disjoint Multipath Algorithm for Cost Efficiency in Wireless Sensor Networks". In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1899–1904.

Park, S. and Corson, M. (2004). "Temporally-Ordered Routing Algorithm (TORA)". Technical report, IETF Internet Draft.

Patel, K., Chern, L. J., Bleakley, C. J., and Vanderbauwhede, W. (2009). "MAW: A Reliable Lightweight Multi-Hop Wireless Sensor Network Routing Protocol". In *2009 International Conference on Computational Science and Engineering*, pages 487–593.

Rabaey, J. (2001). "Pico Radio Supports Ad Hoc Ultra-Low Power Wireless Networking". *IEEE Computers*, 33(01):42–48.

Radi, M., Dezfouli, B., Bakar, K. A., Razak, S. A., and Nematbakhsh, M. A. (2011). "Interference-Aware Multipath Routing Protocol for QoS Improvement in Event-Driven Wireless Sensor Networks". *Tsinghua Science and technology (Elsevier)*, 16(5):475–490.

Radi, M., Dezfouli, B., Razak, S. A., and Bakar, K. A. (2010). "LIEMRO: A Low-Interference Energy-Efficient Multipath Routing Protocol for Improving QoS in Event-Based Wireless Sensor Networks". In *Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM)*, pages 551–557.

Raghunathan., Schurgers, C., and Srivastava, M. B. (2009). "Preliminary Design on the Development of Wireless Sensor Network for Paddy Rice Cropping Monitoring Application in Malaysia". *IEEE Signal Processing Magazine*, 19(2):40–50.

Roman, R., Lopez, J., and Alcaraz, C. (2009). "Do Wireless Sensor Networks Need to be Completely Integrated into the Internet?". Technical report.

Romer. and Mattern, F. (2004). "The Design Space of Wireless Sensor Networks". *IEEE Wireless Communications*, 11(6):54–61.

Ronan, M. R., Keane, M. T., and Coleman, G. (2008). "Applications A Wireless Sensor Network Application Requirements Taxonomy". In *The Second International Conference on Sensor Technologies and Applications*, pages 209–216.

Saaranen, A. and Pomalaza-Ráez, C. A. (2004). "Comparison of Reactive Routing and Flooding in Wireless Sensor Networks". In *Proceedings of Nordic Radio Symposium*, pages 1–5.

Sadagopan, N. (2003). "The ACQUIRE Mechanism for Efficient Querying in Sensor Networks". In *Proceedings of the First International Workshop on Sensor Network Protocol and Applications*, pages 149–155.

Sangi, A. R., Liu, J., and Liu, Z. (2010). "Performance Comparison of Single and Multi-Path Routing Protocol in MANET with Selfish Behaviors". In *World Academy of Science, Engineering and Technology*, pages 28–32.

Sarma, N. and Nandi, S. (2010). "A Multipath QoS Routing with Route Stability for Mobile Ad Hoc Networks". *IETE TECHNICAL REVIEW*, 27(5):380–397.

Savidge, L., Lee, H., Aghajan, H., and Gold Smith, A. (2005). "QoS-based Geographic Routing for Event-Driven Image Sensor Networks". In *Proceeding of IEEE/CreateNet International Workshop on Broadband Advanced Sensor Networks*, pages 991–1000.

Schurgers, C. and Srivastava, M. . B. (2001). "Energy Efficient Routing in Wireless Sensor Networks". In *The MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information*, pages 357–361.

Sen, J. (2009). "A Survey on Wireless Sensor Network Security". *International Journal of Communication Networks and Information Security (IJCNIS)*, 1(2):59–82.

Setton, E., Yoo, T., Zhu, X., Goldsmith, A., and Girod, B. (2005). ”Crosslayer Design of Ad Hoc Networks for Real-Time Video al-time Video Streaming”. *IEEE Wireless Communication*, 12(4):59–65.

Shah, R. and Rabaey, J. (2002). ”Energy Aware Routing for Low Energy Ad Hoc Sensor Networks”. In *IEEE Wireless Communications and Networking Conference*, pages 350–355.

Shi, E. and Perrig, A. (2004). ”Designing Secure Sensor Networks”. *Wireless Commun. Magzine*, 11(6):38–43.

Shokrzadeh, H. and Haghighat, A. T. (2007). ”Directed Roumer Routing in Wireless Sensor Networks”. In *Proceeding of ICEE*, pages 1–5.

Song, C., Liu, M., Cao, J., Zheng, Y., Gong, H., and Chen, G. (2009). ”Maximizing Network Lifetime Based on Transmission Range Adjustment in Wireless Sensor Networks ”. *Computer Communications*, 32:1316–1325.

Stavrou, E. and Pitsillides, A. (2010). ”A Survey on Secure Multipath Routing Protocols in WSNs”. *Computer Networks*, 54:2215–2238.

Subramanian, L. and Katz., R. (2000). ”An Architecture for Building Self Configurable Systems”. In *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing*, pages 63–73.

Toh, C. (1997). ”Associativity-Based Routing for Ad-hoc Mobile Networks”. *Wireless Personal Communications*, 4(2):1–36.

Tsirigos, A. and Haas, Z. J. (2001). ”Multipath Routing in the Presence of Frequent Topological Changes”. *, IEEE Communication Magazine*, 39(11):132–138.

Upadhayaya, S. and Gandhi, C. (2010). ”Node Disjoint Multipath Routing Considering Link and Node Stability protocol: A characteristic Evaluation”. *IJCSI International Journal of Computer Science Issues*, 7,(2):18–25.

Vehbi, C. G., Lu, B., and Gerhard, P. H. (2010). "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid". *IEEE Transactions on Industrial Electronics*, 57(10):3557–3564.

Venkataraman, M., Chatterjee, M., and Kwiat, K. (2009). "Traffic Based Dynamic Routing for Wireless Sensor Networks". In *Proceedings of WCNC 2009*, pages 1–6.

Vidhyapriya and Vanathi, P. T. (2007). "Energy Efficient Adaptive Multipath Routing for Wireless Sensor Networks". *IAENG International Journal of Computer Science*, 34(1):1–9.

Virone, G., Wood, A., Selavo, Q., Fang, L., Doan, Z., and Stankovic, J. A. (2006). "An Advanced Wireless Sensor Network for Health Monitoring". In *Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2)*, pages 1–4.

Wadaa, A., Olariu, S., and Wilson, L. (2004). "Scalable Cryptographic Key Management in Wireless Sensor Networks". In *Proceeding of 24th International Conference Distributed Computing Systems Workshops*, pages 1–7.

Wander, A. S., Gura, N., Eberle, H., Gupta, V., and Shantz, S. C. (2005). "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks". In *Third IEEE International Conference on Pervasive Computing and Communications, PerCom 2005*, pages 324–328.

Wang, Y., Attebury, G., and Ramamurthy, B. (2006). "A Survey of Security Issues in Wireless Sensor Networks". *IEEE Communications Surveys & Tutorials*, 8(2):1–24.

Watro, R., Kong, D., fen. Cuti, S., Gardiner, C., Lynn1, C., and Kruus, P. (2004). "Sensor Networks with Public Key Technology". In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04*, pages 59–64.

Weiner, M. J. (1998). "Performance Comparison of Public Key Cryptosystems". *Technical news letters of RSA*, 4(1):3–5.

Westhoff, C. D., Lamparter, B., and Weimerskirch, A. (2005). "On Digital Signatures in Ad Hoc Networks". *Wiley Journal European Transactions on Telecom*, 16(5):411–425.

Xiaoming, W. and Tao, Y. (2011). "ERMR: Energy-Efficient and Reliability-ensured Multipath Routing for WMSNs". *Chinese Journal of Electronics*, 20(2):329–332.

Xu, C. and Ge, Y. (2009). ”The Public Key Encryption to Improve the Security on Wireless Sensor Networks”. In *Second International Conference on Information and Computing Science*, pages 11–15.

Yang, H., Yang, L., and Yang, S.-H. (2011). ”Hybrid Zigbee RFID Sensor Network for Humanitarian Logistics Centre Management”. *Journal of Network and Computer Applications*, 34(3):938–948.

Yang, L. and Feng, C. (2006). ”Adaptive Tracking in Distributed Wireless Sensor Networks”. In *Proceedings of 13th Annual IEEE International Symposium and Workshop on Engineering of Computer Based Systems*, pages 103–111.

Yao, Y. and Gehrke, J. (2002). ”The cougar Approach to in-network Query Processing in Sensor Networks”. In *SIGMOD Record*, pages 9–18.

Ye, F., Luo, H., Cheng, H., Lu, S., and Zhang, L. (2002). ”A Two-tier Data Dissemination Model for Large-Scale Wireless Sensor Networks”. In *Proceedings of ACM/IEEE MOBICOM*, pages 148–159.

Yick, Mukherjee, B., and Ghosal, D. (2008). ”Wireless Sensor Network Survey”. *Computer Networks*, 52(12):2292–2330.

Younis, M., Youssef, M., and Arisha, K. (2002). ”Energy-aware Routing in Cluster-based Sensor Networks”. In *Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pages 129–136.

Yousefi, H., Yeganeh, M. H., and Movaghar, A. (2011). ”long lifetime routing in unreliable wireless sensor networks”. In *2011 IEEE International Conference on Networking, Sensing and Control (ICNSC)*, pages 457–462.

Yu, Y., Estrin, D., and Govindan, R. (2001). ”geographical and energy- aware routing: A recursive data dissemination protocol for wireless sensor networks”. Technical report, UCLA Computer Science Department Technical Report.

Zhang, H. and Shen, H. (2010). ”Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks”. *IEEE Transactions on Parallel and Distributed Systems*, 21(6):881–896.

Zhang, X., He, J., and Wei, Q. (2011). ”eddk: Energy-efficient distributed deterministic key management for wireless sensor networks”. *EURASIP Journal on Wireless Communications and Networking*, 2011:1–11.

Zheng, M.-C., Zhang, D.-F., and Luo, J. (2009). ”minimum hop routing wireless sensor networks based on ensuring of data link reliability”. In *Fifth International Conference on Mobile Ad-hoc and Sensor Networks*, pages 212–217.

Zhuang, L. Q., Goh, M. K., and Zhang, J. B. (2007). ”The Wireless Sensor Networks for Factory Automation: Issues and Challenges”. In *12th IEEE Conference on Emerging Technologies in Industrial Automation (ETFA'07)*, pages 141–148.

Zoumboulakis, M. and Roussos, G. (2011). Complex event detection in extremely resource-constrained wireless sensor networks. *MONET*, 16(2):194–213.

List of Publications Based on the Research Work

Refereed Journals

1. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2010). ' Energy Aware Routing Protocols for WSN: A Survey', *International Journal of Wireless and Communications Networking*, 2(1):69-77.

2. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2012). ' Network Lifetime Analytical Model for Node Disjoint Multipath Routing in Wireless Sensor Networks', *International Journal of Communication Networks and Distributed Systems (IJCNDS)*. Accepted for publication. To be appear in forthcoming issue.

3. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2012). 'Effects of Transmission Range on Energy Efficient Node Disjoint Multipath Routing protocol for WSNs', *International Journal of Information Processing*. Accepted for publication. To be appear in forthcoming issue.

4. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G. 'Digital Signature Based Secure Node Disjoint Multipath Routing for Wireless Sensor Networks', *IEEE Sensor Journal* Accepted for publication.

Conference Proceedings

1. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2011). 'Energy Efficient Node Disjoint Multipath Route Discovery Mechanism for Wireless Sensor Networks', *First International Conference, CIIT 2011, Pune, India* , Springer CCIS seires, Vol. 250, pp.802-807.

2. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2011). 'Performance Analysis of NodeDisjoint Paths in Multipath Routing for Wireless Sensor Networks', 2^{nd} *International Conference on Methods and Models in Science and Technology(ICM2ST11)*, American Institute of Physics (AIP) Conference Proceedings Vol. 1414, pp.240-244.

3. Shiva Murthy, G. D'Souza, R. J. and Varaprasad, G(2012). 'Reliability Analysis of Route Redundancy Model for Energy Efficient Node Disjoint Multipath Routing in

Wireless Sensor Networks', *International Conference on Modelling and Optimization and Computing (ICMOC 2012)*, Elsevier Procedia Engineering. April 10-11 2012, NIU, Kumarakoil, India.