

ON SECURITY AND OPPORTUNISTIC ROUTING IN WIRELESS SENSOR NETWORKS

Thesis submitted in fulfillment for the requirement of the Degree of

Doctor of Philosophy

By

NAGESH KUMAR



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

April, 2018

Copyright @ JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

April, 2018

ALL RIGHTS RESERVED

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled “**On Security and Opportunistic Routing in Wireless Sensor Networks**” submitted at **Jaypee University of Information Technology, Wagnaghat, Solan (HP), India** is an authentic record of my work carried out under the supervision of **Dr. Yashwant Singh and Dr. Pradeep Kumar Singh**. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my PhD Theses.



Nagesh Kumar

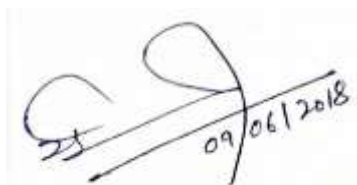
Department of Computer Science Engineering

Jaypee University of Information Technology, Wagnaghat, Solan (HP), India

Date: 09-06-2018

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “**On Security and Opportunistic Routing in Wireless Sensor Networks**”, submitted by **Nagesh Kumar** at **Jaypee University of Information Technology, Wahnaghat, Solan (HP), India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

Handwritten signature of Dr. Yashwant Singh, dated 09/06/2018.

Dr. Yashwant Singh
Associate Professor
Central University of Jammu
Date: 09-06-2018

Handwritten signature of Dr. Pradeep Kumar Singh, dated 09/06/2018.

Dr. Pradeep Kumar Singh
Assistant Professor
JUIT, Solan
Date: 09-06-2018

Acknowledgement

Indeed the words at my command are not adequate, either in form of spirit, to express the depth of my humility and humbleness before Almighty one without whose endless benevolence and blessings this tedious task could not have been accomplished.

I express my sincere gratitude to Vice-Chancellor Prof. (Dr.) Vinod Kumar, and Director and Academic Head Prof. (Dr.) Samir Dev Gupta, for their kind support extended to me for successful completion of this research work.

I place on record unbounded gratitude to my teachers and supervisors, Dr. Yashwant Singh, Associate Professor, Department of Computer Science and Information Technology, Central University of Jammu, J & K, India and Dr. Pradeep Kumar Singh, Assistant Professor (Senior Grade), Department of Computer Science Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat, Solan (HP), India for showing me the real path of sincerity and dedication. In them I found that the best are not only efficient, effective and result driven, but at “core they are persons with the best qualities as human beings”. Humanity, scientific potentials, kindness, coolness, simplicity, novelty of ideas are the arms of their great personality. I am grateful and indebted to Dr. Yashwant Singh and Dr. Pradeep Kumar Singh for allowing me to work under their supervision, and for their invaluable painstaking efforts taken towards my study.

I owe my thanks to Prof. (Dr.) S. P. Ghrera, Brig. (Retd.) Head Department of Computer Science & Engineering and Information Technology, Dr. Vivek Sehgal, Dr. Shailendra Shukla, Dr. Rakesh Kumar Bajaj, Mrs. Triambica Gautam and other faculty members for providing me assistance, moral support, valuable suggestions and necessary facilities during the course of my research work.

I also like to thank Mr. Amit Kumar Shrivastva, Mr. Ravi Raina, and Lab. Technicians of all computer labs in JUIT, for their help and cooperation.

Thanks are due for my dear friends Vandana Mohindru, Dinesh Kumar and Nidhi Sharma for their support and encouragement during my research work. I also acknowledge Hardeh Kumar, Amit Sharma, Munish Patial, Randhir Bhandari, Ashish Ohri and Nitin Sharma for their valuable support.

It will never be possible for me to pay for the price of sacrifices which my parents have made for my success, the hardships to which they came across during my study, the afflictions with which they suffered, the tears which they shed for me and an agonizing long spell which they crossed for my ultimate settlement. These are the devote prayers of my mother Smt. Kashmiran Sharma, dreams of my father Sh. Gian Chand Sharma and fervent feelings of my elder brother Dr. Rajesh Sharma and his wife Mrs. Chandan Sharma, my elder sister Mrs. Neeta Sharma and her husband Mr. Chaman Lal Sharma, younger sister Mrs. Reeta Sharma and her husband Mr. Ajay Sharma, youngest sister Miss Suneeta Sharma and love and affection of my nephews Shaurya and Aakash

brought me to this zenith. I also express my heartfelt reverence to my father and mother in laws Mr. Kashmir Chand Sharma and Mrs. Suneeta Devi, Aadarsh and Monika as their love, affection and blessings are unreturnable.

Diction is not enough to express my gratitude to my beloved wife Sonia Sharma, whose selfless love, constant encouragement, obstinate sacrifices, sincere prayers and blessings have always been the most vital source of inspiration and motivation in my life. She has always been my source of constant strength and love and has stood by me in every step of my life, through thick and thin.

Place: JUIT, Wajnaghat

Date: 09-06-2018



(Nagesh Kumar)

Table of Contents

Table of Contents

Content	Page Number
Declaration by the Scholar	i
Supervisor's Certificate	ii
Acknowledgement	iii
Table of Contents	v
Abstract	ix
List of Abbreviations	xi
List of Figures	xiii
List of Tables	xvi
CHAPTER 1 INTRODUCTION AND MOTIVATION	1
1.1 Introduction	1
1.2 Genesis of Problem	2
1.3 Problem Statement	4
1.4 Objectives	4
1.5 Approach Followed	5
1.6 Contributions	7
1.7 Chapter's Layout	10
CHAPTER 2 REVIEW OF LITERATURE	13
2.1 Introduction	13
2.2 Basic Building Blocks of Routing in WSN	14
2.2.1 Topologies	15
2.2.2 Design Issues for Routing Protocols in WSN	17
2.3 Routing Categorization and Analysis	19
2.3.1 Classification of Protocols	20
2.3.2 Analysis and Discussions	34
2.4 Related Work	37

2.4.1 Trust Aware Routing in WSN	38
2.4.2 Packet Load Balancing based OR Protocols	39
2.5 Simulation Environment and Tools	39
2.6 Parameters of Evaluation	40
CHAPTER 3 ENERGY EFFICIENT OPPORTUNISTIC ROUTING METRIC	42
3.1 Introduction	42
3.2 Motivation and Related Work	42
3.3 Proposed OR Metric: Energy Depletion Factor (EDF)	44
3.3.1 Energy Cost Model	44
3.3.2 Energy Depletion Factor	45
3.4. Experimental Results and Performance Analysis	47
3.4.1 Simulation Scenario	48
3.4.2 Results and Analysis	48
3.5 Conclusion and Future Scope of Work	51
CHAPTER 4 ENERGY EFFICIENT OPPORTUNISTIC ROUTING PROTOCOL	52
4.1 Introduction	52
4.2 Motivation and Related Work	53
4.3 Proposed OR Protocol	54
4.3.1 Models and Assumptions	55
4.3.2 Proposed OR Protocol	56
4.4. Experimental Results and Performance Analysis	60
4.4.1 Simulation Scenario	60
4.4.2 Results and Analysis	61
4.5 Conclusion and Future Scope of Work	64
CHAPTER 5 TRUST AWARE OPPORTUNISTIC ROUTING METRIC	65
5.1 Introduction	65
5.2 Motivation and Related Work	66
5.3 Proposed Trust Aware OR Metric	68

5.3.1 Phase 1: Identification of Elements	69
5.3.2 Phase 2: Trust Evaluation	70
5.4. Experimental Results and Performance Analysis	72
5.4.1 Simulation Setup	72
5.4.2 Experimental Results	73
5.5 Conclusion and Future Scope of Work	76
CHAPTER 6 TRUST AWARE AND ENERGY EFFICIENT OPPORTUNISTIC ROUTING	77
6.1 Introduction	77
6.2 Motivation and Related Work	78
6.3 Modified_MDOR	79
6.3.1 Forwarder Selection Metric	80
6.3.2 Algorithm	81
6.3.3 Experimental Results and Performance Analysis	83
6.4 TAEROR: OR Protocol for WSN	86
6.4.1 Assumptions	87
6.4.2 Working	87
6.4.3 Experimental Results and Performance Analysis	93
6.5 Conclusion and Future Scope of Work	97
CHAPTER 7 TRUST AND LOAD BALANCING BASED OPPORTUNISTIC ROUTING PROTOCOL	99
7.1 Introduction	99
7.2 Proposed OR Protocol (TPBOR)	100
7.2.1 Opportunistic Routing Design	100
7.2.2 Relay Selection Criteria	101
7.2.3 Trust and Packet load Balancing Based OR (TPBOR)	102
7.4. Experimental Results and Performance Analysis	104
7.4.1 Results and Discussions	105
7.5 Conclusion and Future Scope of Work	109
CHAPTER 8 CONCLUSION AND FUTURE SCOPE OF WORK	110
8.1 Introduction	110

8.2 Comparative Analysis	111
8.3 Future Perspectives	112
Bibliography	114
Appendix A: Authors' Publications List	126
Appendix B: Research Papers	127
B.1 Routing Protocols in Wireless Sensor Networks	127
B.2 An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks	170
B.3 An energy efficient and trust management based opportunistic routing metric for wireless sensor networks	177
B.4 Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Network	183
B.5 An Energy Efficient Trust Aware Opportunistic Routing Protocol for Wireless Sensor Network	188
B.6 Trust and packet load balancing based Secure Opportunistic Routing Protocol for WSN	203

ABSTRACT

The sensor networks are the result of advancements in micro-technologies and are increasing in demand. This is because of the abilities of sensors to operate in unattended and hostile environments. Due to advancements in nanotechnology and micro-system developments, researchers can now develop small sensor nodes which may be deployed to collect field data. Sensor nodes are able to gather data from the area of interest and communicate the same to high processing capacity nodes. Sensor nodes are able to communicate any type of chemical or physical data collected from their surroundings. The data collection and communication is not easy as it will be difficult to reach certain areas of interests like dense forests or deep in the sea or inside the core of the earth. These types of environments may be monitored by using wireless sensor networks, which consists of small-sized sensor nodes with limited resources. In wireless sensor networks (WSN), the data must reach to an infrastructure processing node. The sensor nodes follow a common communication pattern by using routing mechanisms. Routing is the most important phase of network operations because the sensor nodes have limited resources to perform all the network operations. Traditional routing protocols cannot cope up with the failures and malicious activities in unstable application environments. Therefore alternative methods must be designed and researched to achieve performance goals.

The opportunistic routing (OR) in wireless sensor networks (WSN) is gaining popularity due to high throughput, low delays, and good packet delivery ratios. Providing data integrity, availability and reliability with less energy exhaustion are very important in WSN. To achieve all of these properties, the routing protocols must ensure the security of route selection process to avoid the participation of malicious nodes. Also, there is a need for energy conservation while providing security to increase the network lifetime and throughput. This thesis work is carried out to optimize energy efficiency, security of route selection process and equal distribution of packet load among all nodes in the network. Firstly, to provide energy efficiency OR metric named as energy depletion factor (EDF) is proposed which distributes the energy consumption load among all nodes equally in the network. The metric calculates the impact of each transmission and reception on the residual energy of each node. Secondly, an energy efficient OR protocol is proposed by using EDF, which improves energy efficiency, delays, and throughput of the network.

To provide the security for route selection process, trust management OR metric is proposed. Based on this metric a new trust-aware and energy efficient opportunistic routing protocol (TAEROR) is proposed which avoids malicious nodes to be a part of the routing process. This protocol increases throughput and lifetime of the network. To reduce the congestion in the network the thesis presents a new trust and packet load balancing OR protocol (TPBOR). This protocol involves queue size of each sensor node in relay selection process. This will reduce the congestion inside a single relay node and distribute the packet load among all relay nodes. This thesis balances between energy, security and traffic load inside the network. The proposed work may be utilized in different applications of WSN where; energy, network lifetime and throughput are important factors.

List of Abbreviations

Abbreviations

ACQUIRE	Active Query Forwarding in Sensor Networks
AODV	Ad-hoc On Demand Distance Vector
BAOR	Buffer Aware Opportunistic Routing
CADR	Constrained Anisotropic Data Routing protocol
DD	Directed Diffusion
DSDV	Destination Sequenced Distance Vector
EAOR	Energy Aware Opportunistic Routing
EAR	Energy Aware Routing
EAX	Expected Anypath Transmission
EDF	Energy Depletion Factor
EEOR	Energy Efficient Opportunistic Routing
EOMR	Energy Efficient Opportunistic Multicast Routing
EQGOR	Efficient QoS-aware Geographic Opportunistic Routing
ETX	Expected Transmission Count
ExOR	Exclusive Opportunistic Routing
FORLC	Fair Opportunistic Routing with Linear Coding
FSPL	Free Space Path Loss
GAF	Geographic Adaptive Fidelity
GEAR	Geographic and energy-aware routing
IDDR	Data Integrity and Delay Differentiated Routing
LCOR	Least-Cost Opportunistic Routing
LEACH	Low Energy Adaptive Clustering Hierarchy
MATLAB	Matrix Laboratory
MDOR	Middle position Dynamic energy Opportunistic Routing
MECN	Minimum Energy Communication Network
MOOR	Multi-hop Optimal Position based Opportunistic Routing
NS2	Network Simulator 2
ODEUR	Opportunistic Distance Enabled Unicast Routing

OR	Opportunistic Routing
ORTR	Opportunistic Real Time Routing
ORW	Opportunistic Routing for WSN
PDR	Packet Delivery Ratio
PEGASIS	Power Efficient Gathering in Sensor Information Systems
PFR	Packet Forwarding Ratio
POR	Packet based Opportunistic Routing
PRR	Packet Reception Ratio
QEOR	QoS Aware Opportunistic Routing
R3E	Reliable Reactive Routing Enhancement
RR	Rumor Routing
SAR	Sequential assignment routing
SOFA	Stop-On-First Acknowledgement
SOP	Self-Organizing Protocol
SPIN	Sensor Protocol for Information via Negotiation
TAEROR	Trust Aware Energy efficient Reliable Opportunistic Routing
TAOR	Trust Aware Opportunistic Routing
TEEN	Threshold Sensitive Energy Efficient Sensor Network protocol
TESRP	Trust and Energy aware Secure Routing Protocol
TLAR	Trust and Location Aware Routing
TPBOR	Trust and Packet load Balancing based Opportunistic Routing
WSN	Wireless Sensor networks

List of Figures

List of Figures

Figure Number	Figure Name	Page Number
Figure 1.1	Work Flow Diagram	6
Figure 1.2	Chapter's Layout	11
Figure 2.1	WSN Communication Architecture Including Sensor Node Components	13
Figure 2.2 (a)	Single-hop Communication	15
Figure 2.2 (b)	Multi-hop Communication	15
Figure 2.3 (a)	Mesh Topology	16
Figure 2.3 (b)	Grid Topology	16
Figure 2.4	Two -Tier Hierarchical Cluster Topology	17
Figure 2.5	Categorization of Routing Protocols	19
Figure 2.6 (a)	Problem of Implosion	21
Figure 2.6 (b)	Overlapping Problem	21
Figure 2.7	The working of SPIN Protocol	22
Figure 2.8	Phases of Directed Diffusion Interest Broadcast, Gradient setup and Data Delivery	23
Figure 2.9	PEGASIS Chaining	26
Figure 2.10	Data gathering in Hierarchical PEGASIS	27
Figure 2.11	Clustering in TEEN and APTEEN Protocols	28
Figure 2.12	MECN Relay region of transmit-relay node pair (i, r)	29
Figure 2.13	Virtual Grid in GAF	29
Figure 2.14	Node State transition Diagram	29
Figure 2.15	Layered Architecture – Implementation of EXOR	32
Figure 3.1	Example Scenario	45
Figure 3.2 (a)	Number of nodes alive after each round	49
Figure 3.2 (b)	Average network lifetime in seconds	49

Figure 3.3 (a)	Number of packets delivered at base station after each round	50
Figure 3.3 (b)	Throughput	50
Figure 3.4 (a)	Path loss calculated after each round	50
Figure 3.4 (b)	Average Path Loss	50
Figure 3.5 (a)	Delay calculated after each round	51
Figure 3.5 (b)	Average end-to-end delay	51
Figure 4.1	Neighbor Table Elements	56
Figure 4.2	Forwarder Set Elements	57
Figure 4.3	Flowchart of Proposed OR Protocol	59
Figure 4.4	Comparison on the basis of Packet Delivery Ratio	61
Figure 4.5	Comparison on the basis of End-to-End Delay	62
Figure 4.6	Comparison on the basis of Energy Consumption	62
Figure 4.7	Comparison on the basis of Duplicate Packets	63
Figure 4.8	Average Network Lifetime based Comparison	64
Figure 5.1	Average Risk Level	73
Figure 5.2	Average Energy Consumption	74
Figure 5.3	Average Network Lifetime	74
Figure 5.4	Average End-to-End Delay	75
Figure 5.5	Average Path Loss	75
Figure 6.1	Reputation Based Energy Efficient OR Protocol	82
Figure 6.2	Performance in Terms of Packet Delivery Ratio	84
Figure 6.3	Performance in Terms of End-to-End Delay	85
Figure 6.4	Performance in Terms of Energy Consumption	86
Figure 6.5	Example scenario of Relay selection in TEAROR	92
Figure 6.6	Flowchart for Proposed Relay Selection Algorithm	92
Figure 6.7	Performance on the basis of Average risk level	94
Figure 6.8	Performance on the basis of Packet Delivery Ratio	95
Figure 6.9	Performance on the basis of End-to-end Delay	96
Figure 6.10	Performance on the basis of Total Energy Consumption	96

Figure 6.11	Network Lifetime	97
Figure 7.1	Flowchart for TPBOR	104
Figure 7.2	Performance on the basis of Average risk level	105
Figure 7.3	Performance on the basis of Packet Delivery Ratio	106
Figure 7.4	Performance on the basis of End-to-end Delay	107
Figure 7.5	Performance on the basis of Total Energy Consumption	107
Figure 7.6	Average Number of Packets Transmitted by each Node	108

List of Tables

List of Tables

Table Number	Table Name	Page Number
Table 2.1	Routing Categorization and Comparison	36
Table 3.1	Simulation Settings	48
Table 4.1	Energy Consumption Parameters description	58
Table 4.2	Simulation Settings	60
Table 5.1	Simulation Parameters	72
Table 6.1	Parameters for Simulation	83
Table 6.2	Simulation Settings	93
Table 7.1	Simulation Settings	104
Table 8.1	Comparative analysis of Modified_MDOR, TAEROR and TPBOR	112

CHAPTER 1

INTRODUCTION AND MOTIVATION

1.1 Introduction

Wireless sensor networks (WSN) are increasing in demand due to the abilities of sensor nodes to be deployed in unattended environments. Also, recent advancements in nanotechnology and micro electro mechanical systems and the data communication mechanisms give a rise to develop small sized sensor nodes [1] [2]. These sensor nodes may be deployed in any area of application's interest. The sensor nodes are able to collect data via sensors and are able to communicate the same through small radio, toward the end-users. Sensor nodes are able to communicate any type of chemical or physical data collected from their surroundings. Most of the time it will be difficult to reach certain environments of applications like dense forests or deep in the sea or inside the core of the earth. These types of environments may be monitored by using wireless sensor networks, which consists of small-sized sensor nodes with limited resources. In WSN data must reach an infrastructure processing node called as a base station. Hence, the nodes have to follow a common communication pattern by using certain routing approaches. Routing is the most important phase of network operations because the sensor nodes have limited resources to perform all the network operations [3].

Opportunistic routing (OR) for WSN is an energy efficient communication technique which involves almost every sensor node of the network to participate in the communication process. This technique utilizes the broadcasting nature of wireless networks [4]. As the name implies OR techniques search for the best opportunity to forward a packet towards the base station, even in absence of a connected end-to-end path. OR algorithms can work on setting up OR algorithms works on a hop-by-hop basis and the best hop is decided on specific criteria depending on the algorithm. Hence, there is no need for a stable end-to-end connection from source to the base station.

Opportunistic routing can easily adapt the changes in an unstable network. The packets in an opportunistic communication, in the network, can be delivered through different routes according to network or environment (surrounding) conditions. In this thesis, new energy efficient and trust aware opportunistic protocol has been proposed, simulated and evaluated on the basis of the simulation results.

1.2 Genesis of Problem

Networking the sensor nodes which are left unattended in outside environment will affect the application like forest fire detection, target tracking, and other disaster management applications. When the nodes are left unattended in a hostile environment than communicating data packets will become a challenging task. This is because the sensor nodes are having limited capabilities like network operations rely on battery power only, limited storage capacity and short radio communication ranges. The very important parameter to be considered over here is the battery power. The whole network relies on battery power as there will be no source of power available in hostile and unattended environments. Out of all the network operations, transmission and reception of data packets and acknowledgments consume most of the battery power. Also if malicious or selfish nodes are present inside the network than the routing will be the most expensive process in terms of power consumption.

Fixed path routing techniques will suffer a lot in the presence of malicious nodes [5]. Because every time the data is transmitted through the same path will result in transmission failures due to packet dropping by malicious nodes. Opportunistic routing (OR) may overcome the problems in fixed path routing by utilizing the broadcasting nature of wireless radios. Using OR each potential relay node near to the source node will have the opportunity to transmit data packets further.

OR protocols always search for the best possible opportunity to forward a packet towards the base station, even in absence of a connected end-to-end path. OR algorithms works on a hop-by-hop basis and the best hop is decided on specific criteria depending on the algorithm. Hence, there is no need for a stable end-to-end connection from source to the base station. Opportunistic routing can easily adapt the changes in an unstable network. The packets in an opportunistic communication, in the network, can be delivered through different routes according to network or environment (surrounding) conditions.

Due to broadcasting nature OR protocols may be exposed to internal or external attacks. To avoid attacks, the nodes must cooperate with each other so that any intruder can be detected. Detecting attackers and malicious nodes will improve the reliability of data packets. In OR the secure route selection is important, which lead to the improved lifetime and trustworthiness among all nodes. The energy saving requirements can be fulfilled by utilizing OR because there is no need of reconstructing the source-destination path again and again. OR gives no guarantee

of data or route selection security. The major research gaps in existing opportunistic routing protocols are as follows.

Lack of energy efficiency

Almost all of the OR protocols select next-hop based on certain routing metric. Like for first opportunistic routing protocol proposed i.e. ExOR [4], expected transmission count (ETX) [6] will be used as the next-hop selection metric. This metric is an end-to-end routing metric which will first count the number of expected transmissions from the source to destination node. ETX do not consider the energy consumption as a primary parameter and will not be suitable for battery-powered sensor nodes.

Security of routing process

This is also a typical problem when nodes are deployed in hostile environments. The attacker may compromise the existing nodes and make them inject attacks like grey-hole and black-hole attacks. As the sensor nodes are having limited capabilities the cryptosystems may not be directly applied to WSN [5]. Therefore the nodes must cooperate with each other to identify the malicious nodes. These malicious nodes must be prevented from taking part in the routing process. Instead of cryptosystems, trust and reputation aware systems may be used which are efficient and use lesser resources.

Packet load balancing

Besides security and energy efficiency there is another important factor for consideration in WSN, is packet load balancing. If there is a problem of congestion in the buffer of the relay nodes than data packets will suffer from high end-to-end delays [8]. This may reduce the throughput and reliability of the network. To overcome this problem there must be buffer-aware routing protocols. Buffer ware routing protocols can divide the load of relaying packets towards the base station among all the relay candidate nodes.

This thesis will try to solve these major problems in the upcoming chapters. The more details about the contributions of the thesis are discussed in the upcoming section. After overcoming these research gaps the proposed OR protocols can work efficiently in the presence of malicious nodes. Also, the proposed approaches will optimize the use of resources provided to sensor nodes. Proposed works in this thesis are compared to themselves also to check which protocols optimize the results. The protocols can be applied to any application of WSN to improve the performance of network.

1.3 Problem Statement

In the development of opportunistic routing protocols for WSN, there is a need for answering certain questions. The first question is, can routing processes able to distribute the load of energy consumption equally among all the nodes? If yes, then how can this be made possible as OR is broadcasting in nature? If the energy efficiency is achieved through equal distribution, how to tackle the problem of high end-to-end delays? Reducing delays will surely improve the throughput of the network. Another question is, how the nodes can coordinate can each other to form a topology? Moreover, despite self-organizing nature, the routing protocol must adapt to the topology changes. Broadcasting nature of wireless radios will generate the problem of duplicate packets at the base station, when a number of relay nodes have the opportunity to transmit the same packet. Can routing approach reduce the duplicate packets by using a coordination mechanism for relay nodes? The routing protocol must be able to avoid the malicious nodes during routing process to improve the performance. The question is, how opportunistic routing will detect and avoid malicious nodes with optimum utilization of resources? In a network each node must participate in routing process so that the packet load will be distributed among all nodes equally.

1.4 Objectives

The following objective has been formulated, on the basis of the above problem statement and achieved in this research work.

- a) To develop a new energy efficient opportunistic routing metric, which will distribute the energy consumption load equally among all nodes in the network.
- b) To develop a new energy efficient opportunistic routing protocol for WSN, which will improve the throughput of the network and also reduce the end-to-end delay. Also, the proposed protocol must be able to reduce duplicate packets received at the base station.
- c) To develop a trust and reputation based OR metric, which will avoid the malicious and selfish nodes during the routing process. The metric should also ensure the optimal utilization of resources.
- d) To develop a secure and energy efficient OR protocol, which will improve the network lifetime and avoid the malicious nodes during the routing process. The protocol must manage the trust levels between nodes by utilizing most important trust evaluation parameters.

- e) To optimize between security, energy, and packet load in WSN. This OR protocol must ensure that each node must transmit an equal number of packets in the network. This protocol must ensure the optimization of energy consumption, packet load and security of route selection process.

1.5 Approach Followed

To identify the problems that may be encountered during the design of routing protocols a detailed survey of routing techniques was carried out. The research gaps were identified on the basis of literature. After research gaps, certain parameters are identified which can be used to improve the performance of the network. On the basis of research gaps above objectives are defined.

To improve the energy efficiency of the network, there must be the distribution of energy load among all the nodes. To achieve this task the most important factor are combined to form a composite routing metric. This routing metric composed of the energy consumptions take place to complete radio operations which are transmission and reception of data packets and acknowledgments. There will be very small energy consumption in other network operations like sensing, generating data packets and acknowledgments. To calculate the impact of various energy consumptions on the nodes' residual energies this opportunistic routing metric is proposed. For the testing of proposed metric MATLAB [9] was used with AODV [10] as base protocol.

For improving the network performance further in terms of end-to-end delays and throughput, a new opportunistic routing metric was proposed. The approach used to propose a new OR protocol was to identify the factors which can cause the various performance issues. The proposed energy efficient OR metric was used in this protocol to identify the best relay nodes. To ensure efficient and reliable data transmissions forwarder set selection algorithm is devised which identify the weak nodes and remove them from forwarder set. For reducing the number of duplicate packets transmitted to the base station, a coordination algorithm is used among all the candidate nodes. The simulation scenarios were created in NS2 [11] and compared with existing energy-efficient protocols.

Next, to fulfill the gap of security breach inside the network, the main security holes were identified. Out of these holes, the important ones were identified and a composite metric was proposed. The composite metric was a trust-aware routing metric which calculates the trust value for neighbor nodes with respect to the source node. The metric was developed to be

dynamic in nature and may identify the malicious nodes at the time of routing process. For the testing purpose, MATLAB is used with DSDV [12] as base protocol.

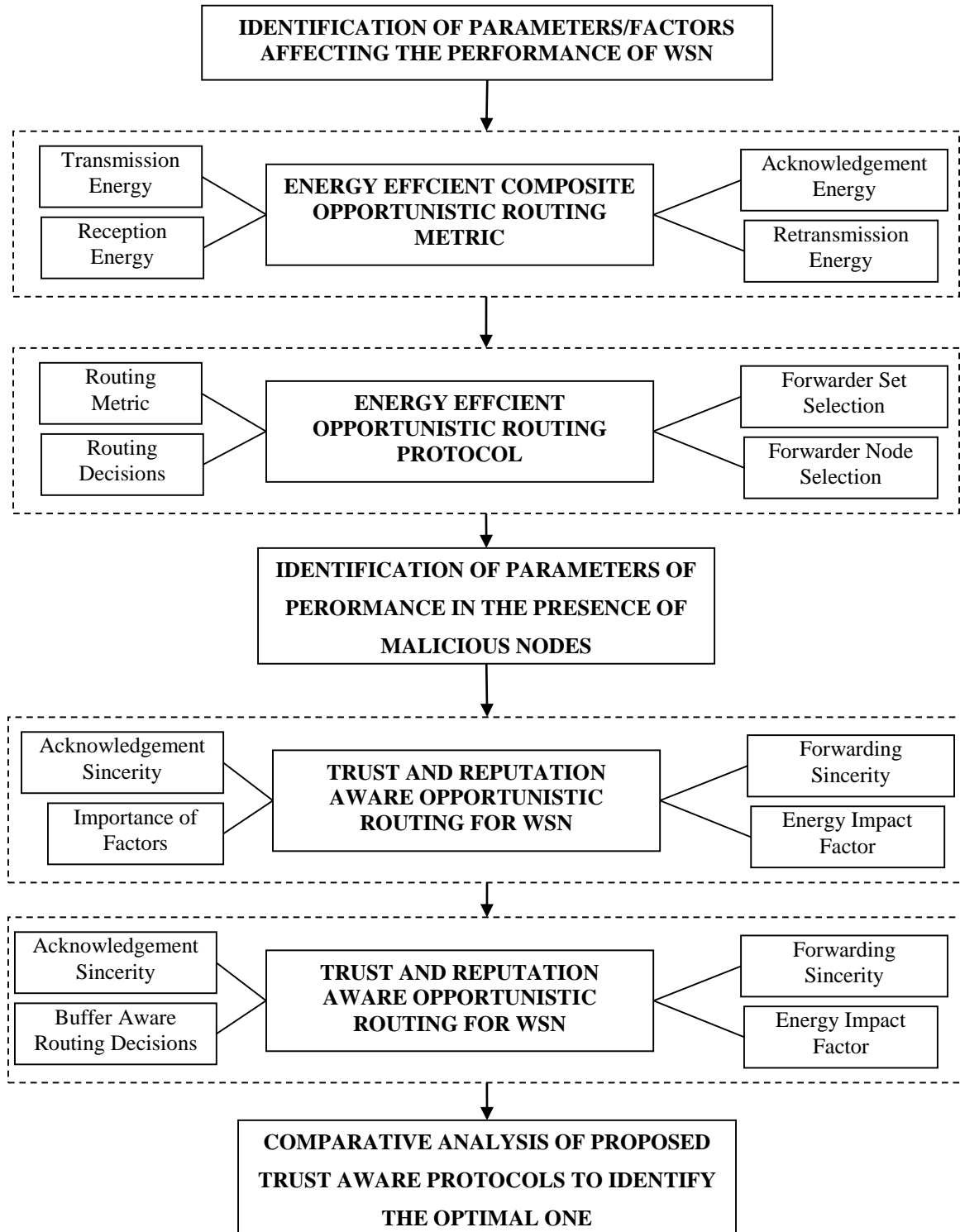


Figure 1.1: Work Flow Diagram

To handle the problems with the proposed trust-aware routing metric, a trust-aware OR protocol is devised. Firstly the trust-aware routing protocol was defined by taking existing MDOR [13] protocol as base protocol. After testing this protocol on NS2 it is being observed that the trust-aware protocols may improve the performance of the network. Based on this assumption a new protocol was proposed which improve the performance of the network. To accomplish the design of the protocol the trust-aware routing metric is modified to improve the performance. This new routing metric was used to embed in between the relay selection algorithm for proposed protocol. This protocol is implemented on NS2 and results were compared to existing trust-aware protocols.

To overcome the problem of overloaded nodes a new approach was proposed. This proposed mechanism was the extension of previously proposed trust-aware OR protocol. To tackle with packet load a new load balancing factor was proposed, which involve the buffer size of each relay node. The current buffer size was tested for each node selected as a next-hop forwarder. The protocol was tested on NS2 and results were compared to existing trust-aware and load balancing based protocols. Finally, all of the three trust-aware protocols were compared to check which one is capable of optimizing the resource utilization. The thesis was concluded on the basis of this comparative analysis.

1.6 Contributions

The thesis will explore the various routing mechanisms proposed for WSN to improve the energy efficiency, security, and reliability. Wireless sensor networks are suitable for many applications including disaster management, health care, and surveillance systems. The most important task which consumes most of the resources is a source of the base station communication process. In this thesis, all the communication processes have been explored and analyzed. The contribution of this research is published in form of a book chapter as follows:

N. Kumar and Y. Singh, "Routing Protocols in Wireless Sensor Networks," *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, Hershey, PA, USA: IGI Global, pp. 86-128, 2016. DOI: 10.4018/978-1-5225-0486-3.ch004.

After the analysis of all communication protocols and their categories, it is being observed that opportunistic routing protocols may present better results than other fixed path routing protocols. Therefore, from the analysis of OR protocols, the research gaps are extracted as explained in the previous section. An opportunistic routing metric name as energy depletion

factor (EDF) proposed in Chapter 3 to provide the energy efficiency for the network which was the first research gap. The metric is used with AODV [10] for the testing purpose and simulated on MATLAB. EDF distributes energy consumption load equally among all the network nodes and prevents the selection of the same node as relay node again and again. The contribution of this research was published as:

N. Kumar and Y. Singh, "An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks," *Indian Journal of Science and Technology*, vol. 9, no. 32, August, p. 7, 2016, DOI:10.17485/ijst/2016/v9i32 /100197.

As AODV routing protocol consumes a lot of energy but using EDF there was an improvement in energy efficiency and throughput and reduced end-to-end delays and path loss. Another contribution for improving these parameters further is the new opportunistic routing protocol which is energy efficient. The protocol proposed is meant to reduce the energy consumption and improve the network lifetime. One more purpose of designing this protocol is the reduction of duplicate packets at the base station. As OR uses broadcasting abilities of wireless links it may be possible that multiple nodes will transmit the same packet to the base station. To accomplish this task proposed protocol runs a coordination algorithm on the basis of EDF to select only one node as a next-hop forwarder. The proposed protocol is simulated in NS2 and compared to existing energy efficient OR protocols EFFORT [14], EEOR [15], EOMR [16] and QEOR [17]. The contribution towards this research is in communication as follows:

N. Kumar and Y. Singh, "Reducing Energy Consumption and Duplication of packets in WSN: Opportunistic Routing Perspective," *Informatica, An International Journal of Computing and Informatics*.

Proposed energy efficient OR protocol works well with the assumption that there are no malicious activities and no selfish nodes. The protocol assumes 100% coordination among all the nodes in the network. If the nodes are deployed in the hostile and unattended environment there is a great possibility of attacks. Most of the applications of WSN will face black-hole and grey-hole attacks, in which the malicious nodes drop the packets instead of forwarding them. Chapter 5 introduce a trust and reputation aware routing metric which is able to tackle this problem. The metric is a composite metric which calculates the trust value of each relay node. The metric composed of sincerity in packet forwarding, impact of energy depletion and acknowledgment sincerity as trust evaluation parameters. These parameters are the most important to improve the performance of the network. The proposed trust-aware metric was

tested by using DSDV [12] as the base protocol in MATLAB simulation environment. The contribution of this research was published as follows:

N. Kumar and Y. Singh, "An energy efficient and trust management based opportunistic routing metric for wireless sensor networks," In Proc. Fourth IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2016), Wagnaghat, India, 2016, pp. 611-616, DOI:10.1109/PDGC.2016.7913196.

The proposed trust-aware metric able to spot and avoid the mischievous sensors during the routing process. But it introduces a high end-to-end delay due to the overhead of metric calculation. To handle this problem Chapter 6 provides two opportunistic routing protocols: modified_OR and TAEROR. Modified_MDOR is the modification proposed to existing MDOR [13] protocol. There are only two trust evaluation parameters i.e. packet forwarding ratio and energy impact, are used for calculating the consolidated trust value. The malicious nodes were identified on the basis of the consolidated trust value. This protocol is for the testing of the trust and reputation based mechanism in WSN. It is simulated in NS2 and compared to the base protocol MDOR [13] and trust based protocol TLAR [18]. The research contribution is published as:

N. Kumar, Y. Singh, P. Kr. Singh, "Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Network," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-6, pp. 29-33, 2017.

To make the reliable data delivery network acknowledgments must be taken into account. This will improve the network throughput also. To address this problem a novel trust-aware protocol is proposed named as TAEROR. It is proposed to include acknowledgment sincerity as third trust evaluation factor. Also, the evaluation parameters used in Modified_MDOR were altered to give better results. The performance of TAEROR was compared to existing trust aware protocols TLAR [18], TESRP [19] and TAOR [20]. The performance is better as compared to using simulations in NS2. The contribution to this research is:

N. Kumar, Y. Singh, P. Kr. Singh, "An Energy Efficient Trust-Aware Opportunistic Routing Protocol for Wireless Sensor Network," *International Journal of Information System Modeling and Design (IJISMD)*, vol. 8, no. 2, pp. 30-44, 2017 DOI:10.4018/IJISMD.2017040102.

In Chapter 7 the work of Chapter 6 is enhanced to involve the buffer inspection of each relay node. The objective was to develop a new protocol named as TPBOR which can optimize the packet load, energy efficiency, and route selection security. To optimize and distribute the

packet load among all the network nodes equally, buffer size of each sensor node was taken into consideration. A new load balancing buffer-aware routing metric was introduced to balance the load equally among all the sensor nodes so that the packets do not suffer any extra delays in waiting queues. This protocol optimizes the resource utilization and also provide security for the route selection process. The research contribution is published as follows:

N. Kumar and Y. Singh, “Trust and packet load balancing based Secure Opportunistic Routing Protocol for WSN,” In Proc. 4th IEEE International Conference on Signal Processing, Computing and Control (ISPCC- 2017), Wagnaghat, India, 2017, pp. 463-467, DOI:10.1109/ISPCC.2017.8269723.

1.7 Chapter’s Layout

The layout of the chapter and thesis organization illustrated in figure 1.2 is described as follows.

Chapter 1 provides the basic introduction of wireless sensor networks, communication mechanisms and opportunistic routing, the genesis of the problem, problem statement and the objectives, the approach followed, major research contributions made by this work and lastly describes the chapters’ layout.

Chapter 2 discusses a detailed literature survey on WSN and communication protocols for the same. This chapter also discusses various design issues for routing protocols. The comparative analysis of routing protocols is presented and also the tools and techniques for testing the proposed work will be discussed. Lastly, this chapter provides various parameters of consideration.

Chapter 3 will discuss the newly proposed energy efficient opportunistic routing metric named as energy depletion factor (EDF). The simulation and analysis of EDF are discussed by comparing to traditional routing protocols i.e. AODV [10] and DSDV [12].

Chapter 4 provides a detailed discussion of proposed energy efficient and reliable OR protocol. The phases of the proposed protocol will be discussed and analyzed. The simulation and analysis of proposed protocol are discussed by comparing to existing energy efficient opportunistic routing protocols.

Chapter 5 will present a solution to tackle the problem of malicious nodes and selfish nodes. This chapter will discuss a new trust-aware OR metric to handle malicious nodes during the routing process. The simulation and analysis of proposed metric are discussed by comparing to traditional routing protocols i.e. AODV [10] and DSDV [12].

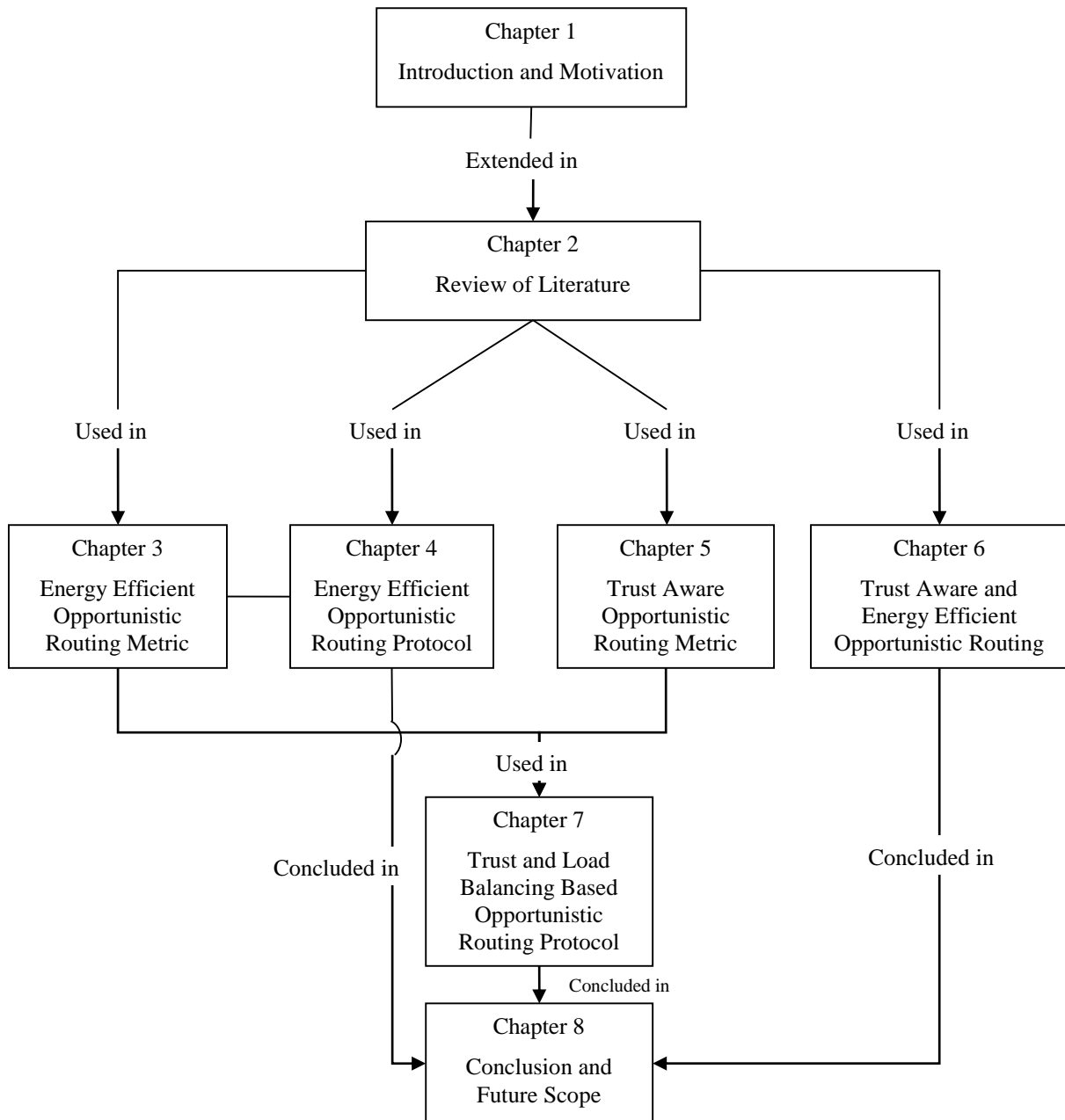


Figure 1.2: Work Flow Diagram

Chapter 6 provides a detailed discussion of two newly proposed trust-aware and reliable OR protocols. The phases of both the protocols will be discussed. The simulation and analysis of both protocols will be discussed by comparing these to previously proposed trust and reputation based opportunistic routing protocols for WSN.

Chapter 7 discuss the solution to load balancing problem during routing process in WSN. It provides a detailed study of a new OR protocol which will distribute the packet load and energy consumption and provide security to the routing process by avoiding malicious nodes. Overall this protocol will optimize the use of resources and security of the route selection process.

Chapter 8 gives the conclusions after comparing the three proposed trust-aware protocols and an evaluation of the contributions in the thesis is presented. This chapter also describes direction for the future work.

CHAPTER 2

REVIEW OF LITERATURE

2.1 Introduction

Wireless sensor network are of growing interest due to advancements in micro electro mechanical systems, nanotechnology and advanced wireless communication techniques. These advancements give rise to build small sized sensor nodes which are of low cost and can perform multiple functions at a time [3] [2]. The multiple tasks involve collecting data from deployment area, processing this data and transmitting the same toward the base station which is an infrastructure processing node. WSN contains such type of sensor nodes with wireless radios. The pictorial representation can be seen in figure 2.1, which represent both wireless sensor networks and the major components of a sensor node.

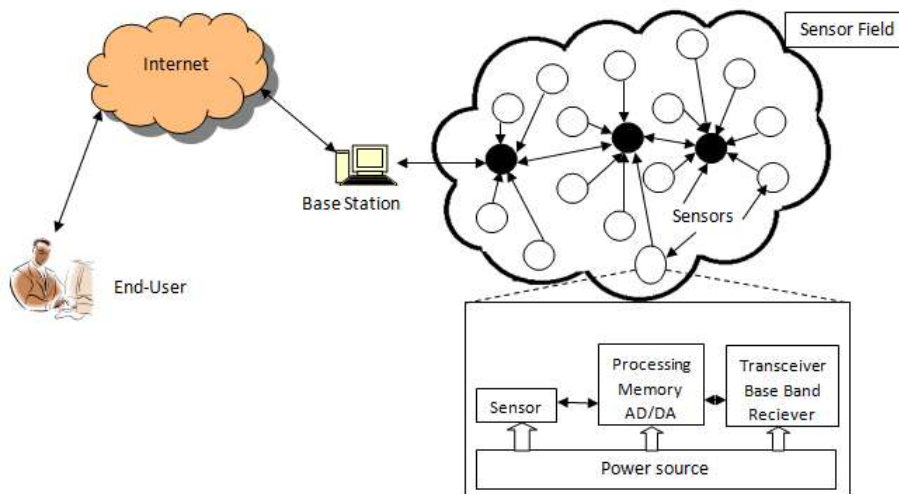


Figure 2.1: WSN Communication Architecture Including Sensor Node Components

WSN may collect any type of physical or chemical data with the help of sensor nodes. The remote stations may be monitored by using sensor nodes accurately and quickly. Most of the WSN application the locations or positions of sensor nodes need not to be engineered or predetermined. This property of wireless sensor network will also make these useful for applications in which the nodes are left unattended. This property also make the deployment to be random instead of fixed. But, designing protocols for such networks will be a tough task because the topologies cannot be formed. The sensor nodes will organize themselves in any random topology. The protocols designed for WSN must address this issue and capable of

handling random topologies. The communication protocols especially must take care that only useful data will be transmitted to the base station.

The nodes in WSN are densely scattered and networking these nodes is a tough task as it affects the performance of network. The applications like disaster management, surveillance and target tracking require high performance and reliability of data [21]. Therefore, for these type of applications routing becomes a challenging research area. Also the routing becomes more challenging as WSN are having different characteristics than conventional wired and wireless networks. As the sensor nodes are randomly deployed it will be difficult or almost impossible to use global addressing. Therefore, classical IP addressing based protocols cannot be applied directly to sensor networks. There are limited resources available with sensor nodes like energy, storage, computational capacity and transmission range.

The protocols are required to use these resources efficiently so that the network can be used for longer times. Another issue for routing protocols to look out, is the flow of data as all the sensor nodes will follow similar pattern of communication. The flow of data is always from sensor nodes toward the base station as shown in figure 2.1. Another problem is of data redundancy because of dense deployment of nodes. The nearby nodes may generate similar data and this will increase duplicated data at the base station. This data redundancy should be removed. To solve these problems numerous of routing protocols has been proposed by taking care of resource utilization. The sensor nodes organize themselves to form different topologies for communication which are discussed in the following section along with communication framework.

2.2 Basic Building Blocks of Routing in WSN

In WSN the sensor nodes are left unattended and this makes these useful to many applications like calamity management, investigation of battle grounds and target tracking. As the sensor nodes are battery powered, all the operations will be dependent on this only. The most important factor here to consider is the battery power of a node. The network lifetime of WSN depends directly on the battery power of nodes. The whole network relies on battery power as there will be no source of power available in hostile and unattended environments [3]. Out of all the network operations transmission and reception of data packets and acknowledgements consumes most of the battery power. Also if malicious or selfish nodes are present inside the network than the routing will be the most expensive process in terms of power consumption.

The major task of network layer is to build efficient route from source node to base station. Base stations are used as infrastructure processing nodes or gateway nodes. The routing protocols will be based on two types of network communication patterns. One is single-hop communication pattern and the other one is multi-hop communication pattern. In single-hop communication pattern the nodes communicate data packets directly to the destination node. On the other hand, multiple-hop communication uses multiple forwarder or relay nodes to communicate data packets. There is one another technique called as hybrid communication in which nodes can communicate data packet using single and multiple-hop communication techniques. Most of the routing protocols are dependable upon multiple-hop communication pattern because this type of communication is reliable and also the network remain connected to destination node [3]. Hybrid communication is most feasible technique and followed by almost all of the routing algorithms for WSN. WSN are classified into opportunistic type of networks, in which a dynamic routing protocols will be very useful.



Figure 2.2: (a) Single-hop Communication and (b) Multi-hop Communication

2.2.1 Topologies

The sensor nodes in a WSN can be arranged in any type traditional wireless network topologies. But as requirement of some applications to deploy sensor nodes in an environment where manual deployment is not possible, the nodes may be deployed randomly. This random deployment make the sensor nodes to arrange themselves in any topology. The routing protocols must cope up with this self-organization. Dynamic routing protocols must be aware of random deployment and should increase the reliability of network in hostile environments. The following types of topologies are common in WSN.

Single-hop star

This topology will make each sensor node to transmit data packets directly to base station. It is simple and easy to implement. The guarantee of data delivery in this topology is very low.

Because when a wireless node broadcast data packets, there is no guarantee that the base station can receive that packet or not. This is totally dependable on the transmission power and range of radio of the sensor node. Figure 2.2 (a) shows this type of topology which is a single-hop communication pattern.

Multi-hop Mesh and Grid

To increase the coverage of area under consideration using WSN mesh and grid topologies are used. These type of topologies are shown in figure 2.3 (a) and (b) these topologies follow multi-hop data communication pattern. Routing protocols that may work with these type of topologies are dynamic in nature and also use the device memory to store the routing information.

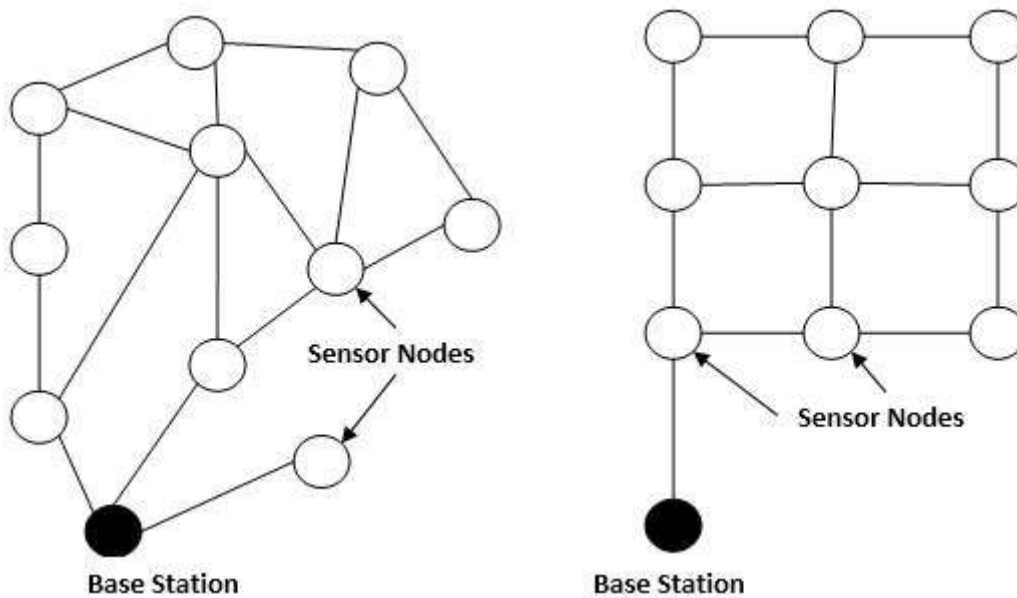


Figure 2.3: (a) Mesh Topology and Figure 3 (b) Grid Topology

Two-tier Hierarchical Cluster

Clusters are the subparts of a network in which some of the sensor nodes are arranged in certain pattern to communicate data to cluster heads. Cluster heads may be chosen from the sensor nodes itself or may be deployed separately. WSN will be divided into multiple such clusters. The sensors in a cluster will communicate only with their head node. Cluster heads can communicate with each other to transmit data packets toward destination. Figure 2.4 demonstrate this type of topology.

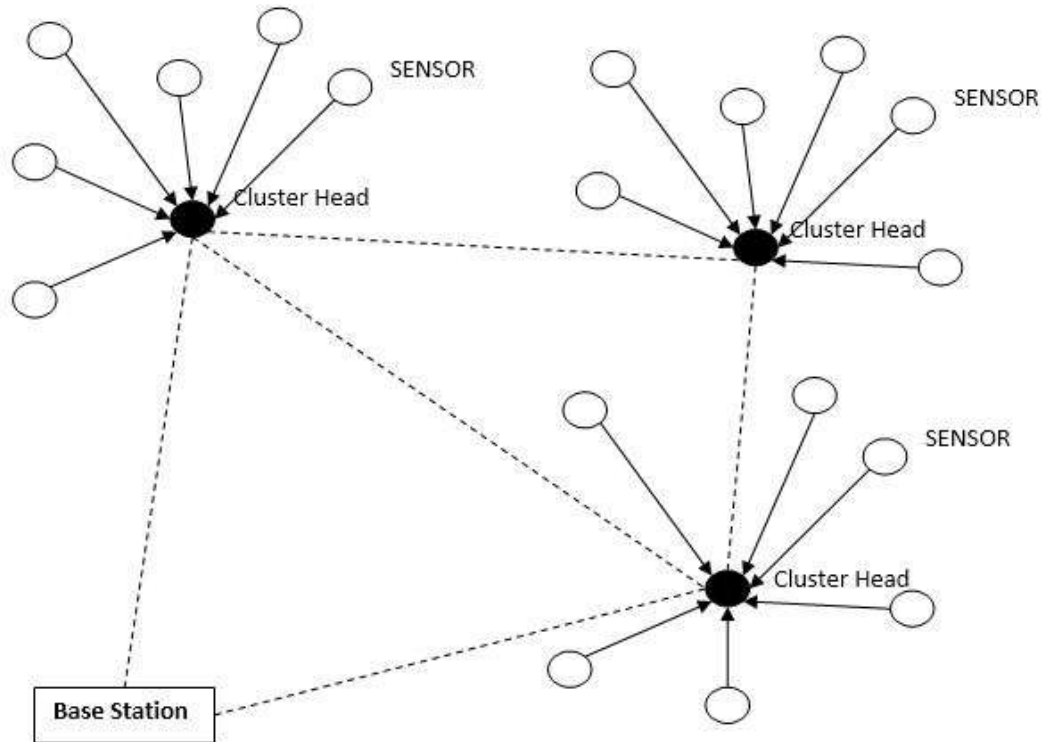


Figure 2.4: Two -Tier Hierarchical Cluster Topology

These topology are most commonly used in WSN to make data communication successful and reliable. While using routing protocols for these topologies certain design issues must be considered so that the routing will give best results.

2.2.2 Design Issues for Routing Protocols in WSN

Dynamic routing protocols are very useful in WSN because of the opportunistic nature of these networks. While designing dynamic routing protocols for these networks certain issues and problems must be considered. These issues must be addressed to extract best possible results. The architecture of WSN will also affect the performance of dynamic routing protocols. Such type of issues will be described briefly in this section.

Architecture of network

Most of the applications of WSN assumes sensor nodes to be static in the deployment area. The nodes will not move and the locations of the nodes will be constant in this case. But there are certain examples in which the nodes can move [22], means the deployment area contains mobile nodes. Communicating data packets in mobile sensors based WSN is very tough task. There may be no path stability and the routes need to be built again and again. In these cases the optimal utilization of resources is not possible [23]. The event which will occur in the deployment area may be static or dynamic in nature. During static events reactive routing

protocols will be helpful. The topology of the network will also be dynamic in nature during a dynamic event and hence requires to alter path information time to time.

Placement of Nodes

This is another important issue while designing routing mechanisms. The placement of sensors in the deployment area is completely depends on applications of WSN. The node placement may be manual or self-organizing in nature. The manual placement involves man power to place the nodes at important subareas of the deployment field. The communication routes may also be defined and stored inside the sensor nodes. On the other hand, in self-organizing placement of nodes the nodes develop the routes dynamically on the basis of routing protocols [24] [25]. Some applications also require the nodes to form clusters for data communication. This is also a challenging task and it increase the overhead of route selection process.

Energy efficiency

Energy consumption inside sensor nodes to perform various network operations needs to be handled carefully. Because if a node will not be able to communicate data packets due to lack of energy it will be considered as dead node. A dead node means the network is in loss of certain capabilities, hence, this will reduce the network lifetime. Most of the energy of battery powered sensor nodes will be consumed during data transmission and reception. In short radio of a sensor node is expensive in terms of energy consumption. The energy consumption may be reduced by the intelligent routing protocols like which can perform dynamic route selection at the time of transmission to reduce the retransmissions [24].

Model for reporting data

This is the issue related with how and when the data will be reported to the base station. Paper [25] categorized the data reporting models depending on the types of applications. According to authors, the data reporting models may be based on event occurrence, query imposed by base station, continuous data delivery and hybrid. In event occurrence based data delivery model the nodes will communicate data to base station only if there is any activity occur in the area of deployment. Continuous data delivery require the nodes to transmit data continuously whether the event is occurring or not. Also there may be time intervals defined for transmitting the collected data. Another type of data reporting is query based in which the nodes will wait for a query from the base station to transmit data. Hybrid type of data reporting may be the combination of any or all of the data reporting techniques discussed here. The working of

communication techniques will be greatly influenced by these models. Also it depends on the application [26] which type of reporting model is to be used.

Fault Tolerance

The sensor nodes in WSN can be deployed in an unattended and hostile environment. This leads to frequent failures of sensors and degrade the performance of the network. Frequent node failures can occur due to low energy, damage caused by natural hazard or any other environmental factor. The protocols designed for WSN must cope up with these failures and the network performance must not be reduced. There should be alternative paths for transmitting data packets toward base station [22].

Node Connectivity

The sensor nodes in WSN are mostly having a short communication range. This will lead to disconnection among nodes if the sensors are not in communication range with each other. Also the nodes may fail in between and hence it will affect the performance of routing protocols. Connectivity between sensors will lead to good network performance. Connectivity directly depends on how the nodes are distributed in the network.

The routing protocols must consider the issues discussed above so that the quality-of-service may be achieved. For addressing these issues the properties of WSN must be taken care of whenever designing a routing protocol.

2.3 Routing Categorization and Analysis

The routing protocols proposed by different authors over the years have been classified by many authors [1] [3]. Mostly the routing protocol for WSN can be differentiated on the basis of their working and data collection abilities. Figure 2.5 below depicts the categories of routing mechanisms available for WSN.

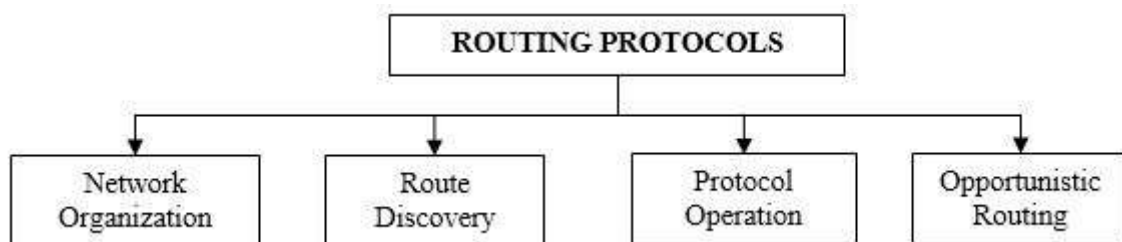


Figure 2.5: Categorization of Routing Protocols

The protocols which are based on network organization depends on the structure of sensor networks. The structure of sensor networks mostly defined by the application type. The

network may have a flat structure which means that the nodes will be having same type of roles. It may be hierarchical in which the clusters and the data will be communicated with the help of cluster heads. Another type of network structure based algorithms are depends on location of the sensor nodes.

The second category i.e. route discovery, depends on the path selection techniques. The main task of routing algorithm in this is when to discover the route. The route may be discovered on the basis of sensor node's demands which is called as reactive routing. Another is when the routes are discovered before the actual communication happens which are called as proactive routing protocols.

Also the routing protocols may be categorized based on their actions and working. Some protocols try to provide quality-of-service by setting some parameters for quality measurement. While some other protocols try to reduce the duplicated data by performing data aggregation. Some protocols are based on the transmission types means whether the protocols are unicasting, multicasting or broadcasting. Protocol operation always affect the performance and lifetime of the network.

Another dynamic routing category is opportunistic routing (OR) which decide the route of the packet only when the communication is started. The OR utilizes the broadcasting nature of wireless links and transmit data through multiple relay nodes. The relay nodes will have to coordinate with each other to reduce the duplicate data transmissions. OR always have to select the best possible next-hop relay to accomplish the data transmission task successfully. Opportunistic routing protocols are reliable and utilize the transmission range of a node efficiently [1-5]. OR protocols available in the literature presented good results in terms of reliability and availability of data packets.

2.3.1 Classification of Protocols

The routing protocols for WSN may perform different operations like transmission and data aggregation. Many authors and researchers around the world have developed routing protocols which are capable of increasing the increasing the performance of network. There are certain simplest approaches which do not fall in any of the categories i.e. flooding and gossiping. Another type of classification follow certain rules and patterns.

(a) Flooding and Gossiping

Flooding and gossiping proposed by [27] are the two simplest approaches to solve the problem of routing packets. Flooding is kind of routing in which the data is broadcasted and each sensor

node will forward the data further until it reaches destination node. Flooding is intended to transmit data packets to each node in the network. This process may result in heavy traffic patterns and also increase the number of duplicate packets at base station. The number of times a data packets must be forwarded can be restricted in flooding. The packets always include the address of destination node and also the packet sequence number. Based on this packet sequence number the destination node has to remove the identical data packets [27].

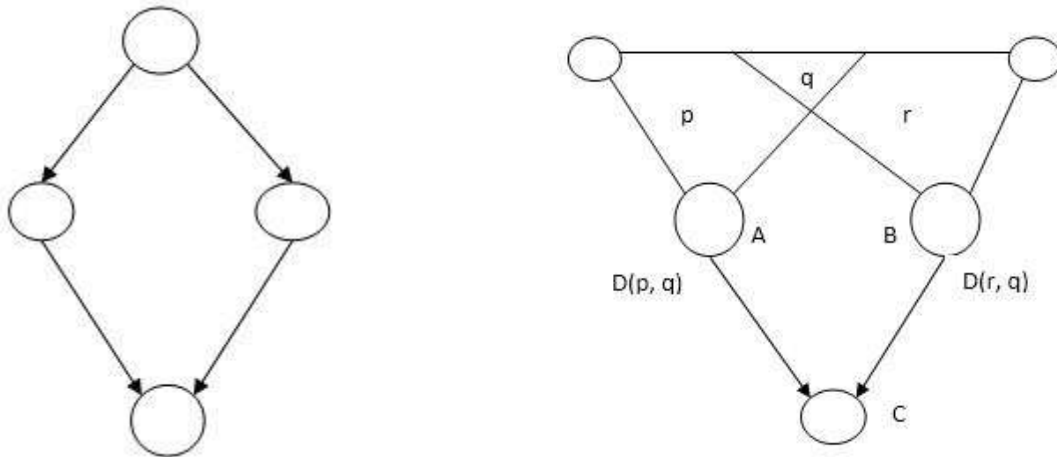


Figure 2.6: (a) Problem of Implosion and (b) Overlapping Problem [27]

Flooding mechanism give a rise to three another problems implosion, overlapping and resource blindness. Implosion occurs by when there is number of duplicate packets are received at a particular relay or destination node. Another problem is the overlapping problem in which two or more sensor nodes are collecting data from the same subarea of the deployment field. Third problem occur due to the problem of decaying energy inside the nodes. When a node decays all of its energy without employing any energy saving scheme the network will lose some of its functionalities. There is another type of flooding called as gossiping as proposed in [27] solve the implosion problem. Unicasting is used in gossiping rather than using broadcasting. But this may lead to congestion problem and also introduces high delays.

(b) Data-Centric Routing

In most of the applications of WSN the data packets generated by a node about certain event is more important that the node itself. The data packets must arrive at destination node as soon as possible. Data packets are redundant and require refinement during the communication. Data centric routing protocols are such protocols which can reduce the data redundancy and make the data communication reliable and efficient. The protocols based on the data centric approach are discussed below.

Sensor Protocols for Information via Negotiation (SPIN)

SPIN is a data centric routing protocol which focused on the data distribution among all nodes [26]. The meta-data is used to represent the actual data with the help of descriptors. Prior to start the actual data transmission SPIN protocol advertise the data of the source node. For advertisements meta-data is used and when the data is received by other nodes they check for the novelty of this data. The novel data will be further forwarded toward new neighbors otherwise the nodes will reject this data. The rejection acknowledgement will be sent immediately to the source nodes so that source nodes can also discard the same. Three types of messages are used in SPIN i.e. REQ, which communicate the request to advertise the meta-data to other sensor nodes, ADV, which is used to transmit the meta-data, and DATA which is used to transmit actual data.

The problem of implosion, overlap and blindness will be removed by this protocol. SPIN also achieve required energy efficiency and improve the network lifetime. The change in topology will be handled locally by each sensor node. The major problem with this protocol is the guarantee of data delivery and also overhead of collecting meta-data from each node. This process will lead to delays in packet transmissions. Also there can be a problem of congestion when multiple nodes try to transmit data packets and meta-data together. Figure 2.7 below shows the working of SPIN protocol.

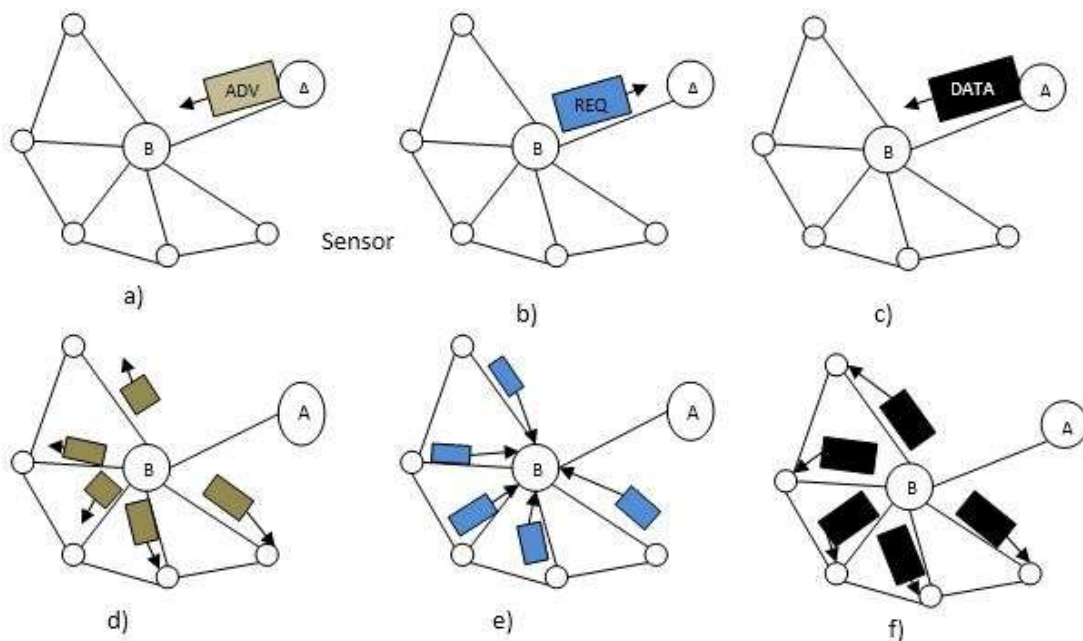


Figure 2.7: The working of SPIN Protocol [26]

Here, in figure 2.7 above node A advertises data to neighbor B. Now node B request the data from A. After receiving request node A sends the data to B and node B also advertise this new data towards its neighbors. Now as the data is new neighbors of B also request this data from B. Receiving the request node B transmits the data.

Directed Diffusion

This is another data centric routing protocol which was proposed to overcome the problem of unnecessary wastage of energy during network operations. Directed diffusion [28] used the naming mechanisms for data to diffuse it across the network. The data is collected on the basis of its attributes. This protocol is uses the query driven architecture of WSN. The query will be generated by infrastructure processing node which can be a sink or base station or a gateway node. At the time of query generation some attribute values are inserted in this so that the nodes transmit data about these attributes only. The attribute can be an object, an interval or duration or any particular location inside the deployment field. Sensor nodes when receive this query will compare their collected data with the attributes. If a match is found the communication will be started. Data aggregation is also employed in directed diffusion by using Srteiner Tree Algorithm [29]. The routes are built on the basis of gradients and the attribute values. There is possibility to rebuilt routes when a gradient is failed to deliver data packet successfully due to any obstacles. Directed diffusion reduces redundant network operations and also have the capability to repair routes. No addressing scheme is required in this protocol and aggregation and energy saving to some extent are another advantages of this protocol. There is an overhead of storage due to multiple path stored inside a node. Directed diffusion can only be applied to query based applications of WSN.

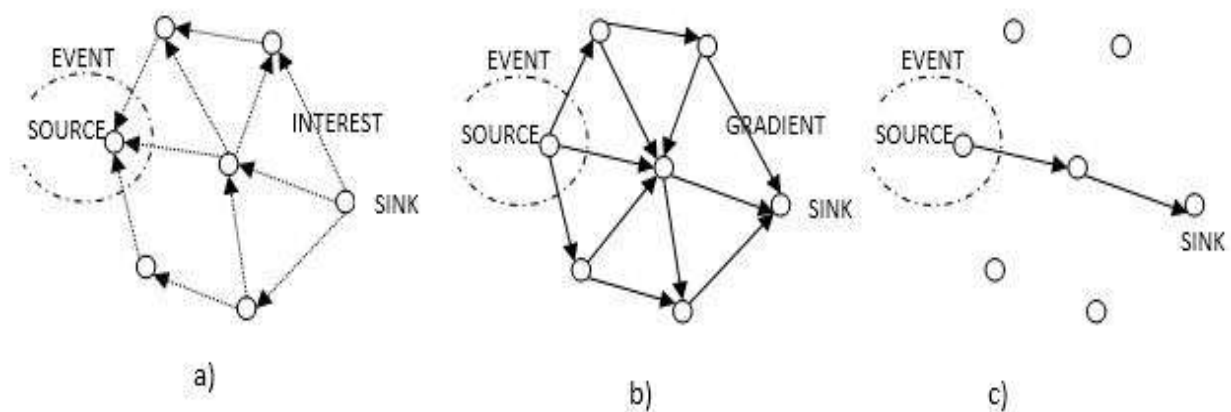


Figure 2.8: Phases of Directed Diffusion a) Interest Broadcast b) Gradient setup c) Data Delivery [29]

Energy-aware Routing

This algorithm was proposed in [30] and it is data centric as well as energy efficient. This routing protocol utilizes a group of sub paths which require less energy consumption. Providing the energy efficiency the protocol helped to improve the network lifetime. The protocol checks for each route for total energy consumption and selects the best one with optimal value. It was observed by the authors that choosing a path which consume lesser energy always will lead to failure of the nodes on that path. Hence, using multipath routing mechanism with link probability is useful. The protocol completes its working in three major parts discussed as follows. In the setup phase flooding mechanism is used in this step to form the routing table. While collecting information about neighbors, energy consumption for each neighbour is calculated and stored inside the table. If a sensor N_i transmit the request to a sensor N_j . N_j will run the following equation to calculate expected energy consumption.

$$C_{N_i N_j} = \text{cost}(N_i) + \text{Metric}(N_j, N_i) \dots\dots\dots (1) [30]$$

This cost calculation metric is the composite metric consist of transmission and reception energy cost and the residual energy of a node. If the metric value is very high for a path it will be rejected and deleted fro the routing table. A probability will be assigned to each node during the formation of routing table calculated as below.

$$P_{N_i N_j} = \frac{1 / C_{N_j N_i}}{\sum_{k \in FT_j} 1 / C_{N_j N_i}} \dots\dots\dots (2) [30]$$

Now the full path cost to reach the destination, will be calculated by node N_j .

$$C_{N_i N_j} = \sum_{i \in FT_j} P_{N_j N_i} C_{N_j N_i} \dots\dots\dots (3) [30]$$

The second step is the data communication step in which the data packets are generated by including the routing table will be constructed. Third step is the route recovery in which a checking of routes is done. Flooding mechanism is used in this phase to check whether the routes are still connected or some nodes are dead on the route. The improvement of lifetime was the main motive of this protocol and it had achieved up to 44% of this goal. The route construction is complicated as compared to other data centric algorithms.

Rumor Routing

It is proposed in [31] and had been applied to such applications of WSN in which location based routing mechanisms cannot be used. Rumor routing is inspired by directed diffusion in

which the flooding mechanism is used where the location data is not available about the nodes. Directed diffusion fails where a very small amount of data is required by the base station and flooding data in this case will increase in congestion and overhead of huge energy consumption. Rumor routing refines this process and sends the data request only to those nodes at which the event has occurred. Hence, only those data were flooded which is required by the base station. Rumor routing mark this data important and agents are used to flood this data. Agents were provided with high energy efficiency and can travel long distances in the network. The agents were created by the source nodes where the event has occurred. The agents are marked important and relay nodes will forward these agents on high priority. There is requirement of one reliable path and multiple paths are not stored inside the sensor nodes. The nodes failures are handled efficiently with better energy efficiency than directed diffusion. If the number of events are very large than this algorithm may lead to congestion problem.

(c) Hierarchical Routing Protocols

This is the second classification of routing protocols for WSN and use hybrid communication pattern to transmit data packets toward base station. This type of communication improve energy efficiency with route selection processes. Some of the routing mechanisms of this category also form clusters. But, clusters require cluster heads and cluster heads must coordinate with other nodes related to its area. The protocols falls in this category are efficient and popularly used in many applications.

Low-energy adaptive clustering hierarchy (LEACH)

Proposed by [24], this protocol is very popular and common to be used in multiple applications. The clusters are formed in this protocol on the basis of the range the radios. Cluster heads are elected on the basis of energy information provided by all of the sensor nodes. Cluster heads then will collect data from all other nodes in the cluster and communicate the same to base station. The cluster heads are formed rotationally after some period of time as required by the applications. For electing cluster heads the decision will be taken by all the sensors by opting a random number between 1 and 0. The node will be elected as cluster head if and only if the opted number is greater than or equal to the threshold calculated by using equation below.

$$T(n) = \left\{ \begin{array}{l} \frac{p}{1 - p^{*(r \bmod (1/p))}}, n \in G \\ 0, otherwise \end{array} \right\} \dots\dots\dots (4) [24]$$

Here, p represent the percentage of cluster heads chosen, current round is r and set of nodes which are not chosen as cluster heads yet represented by G . there are so many variants available till date for LEACH protocol. Some popular variants are Multi-hop LEACH [32], Centralized LEACH (LEACH-C) [33], Fixed number of clusters LEACH (LEACH-F) [34], Q-LEACH [35] etc. In LEACH it is easy to form clusters but changing the cluster heads again and again is a complicated task.

Power Efficient Gathering in sensor Information Systems (PEGASIS) and Hierarchical-PEGASIS

PEGASIS was proposed by [36] and is inspired by the design of LEACH. In PEGASIS the sensors construct a chain for data transmission and forward data in that chain only. At one level of chain only one node will be selected as data forwarder. For the next transmission another node will be selected out of chain to transmit data. Greedy algorithm approach is used to construct the chains. The sensor nodes are assumed to have the capability to aggregate and then transmit data toward the base station. The problem with this protocol was there are no mechanisms to take routing decisions dynamically.

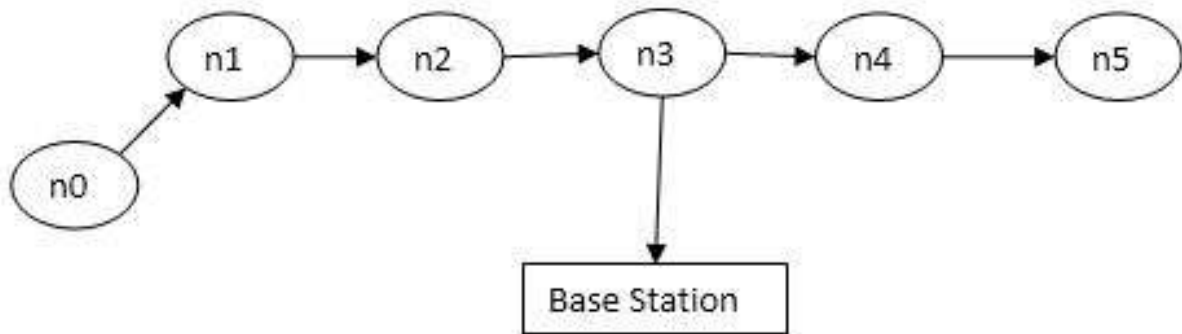


Figure 2.9: PEGASIS Chaining [36]

Here, in PEGASIS the clusters are not formed but the chain of nodes may be assumed as clusters and the chain heads replacing the cluster heads, will be chosen on the basis of greedy approach. PEGASIS has shown good performance as compared to LEACH. The number of data communication are reduced by doing aggregations at the chain heads.

There is variant of PEGASIS proposed by [37] before the actual publication of PEGASIS. The problem with data aggregation in PEGASIS has been overcome in hierarchical PEGASIS. The delay of data aggregation has been reduced and the throughput of the network is improved. Collisions are major problem in this new protocol.

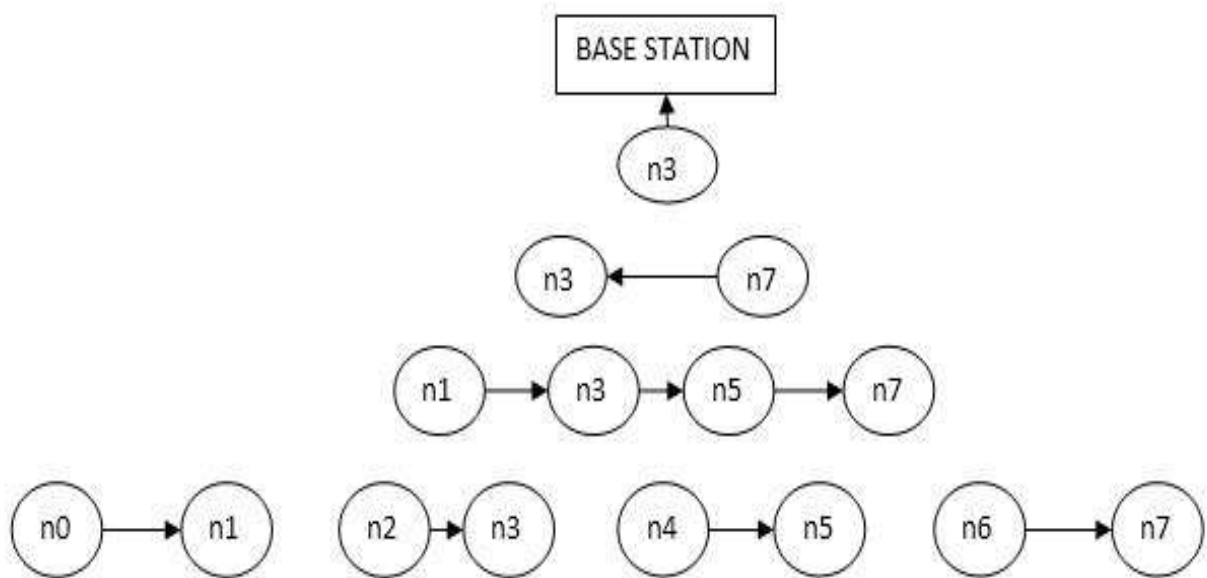


Figure 2.10: Data gathering in Hierarchical PEGASIS [37]

Threshold sensitive Energy Efficient sensor Network protocol (TEEN) and Adaptive TEEN

These protocols were proposed by [38] to overcome the problems of proactive routing protocols discussed previously. TEEN is a type of reactive routing and the routes are constructed only when there is a need of data transmission. The data delivery time is the major parameter used in TEEN and APTEEN [38] both. The value of a sensed event must reach the base station within a given time. The continuous data communication model has been used in these protocols. Hence, both of these protocols were data centric as well as hierarchical.

Clusters are formed for those nodes which are in a particular subarea of the deployment field. The nodes near to base station are directly connected to it. The base station communicates two ideal values for an event, to communicate: hard threshold and soft threshold. If the event value matched with hard one it means this value needs to be transmitted immediately to base station. The soft threshold allowed the nodes to transmit values only when there is not much difference between the previous and new sensed values.

Data delivery is reliable and also these protocols are good enough for event based applications. The problem with these algorithms is that if the threshold value is not matched then the network is becomes useless.

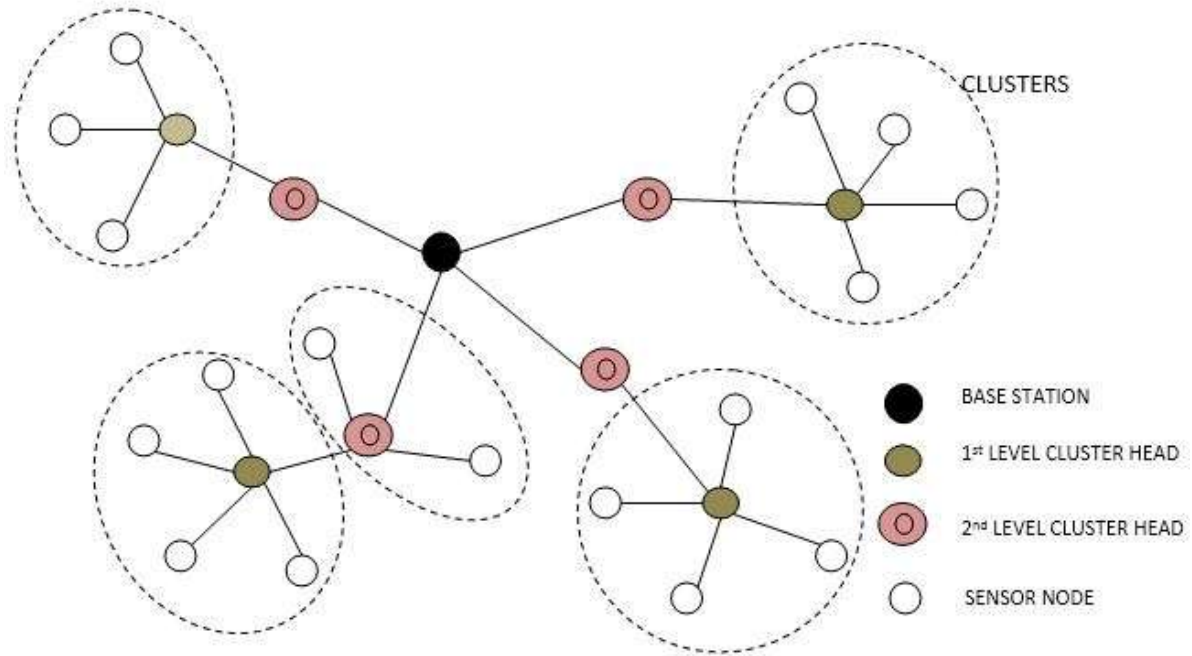


Figure 2.11: Clustering in TEEN and APTEEN Protocols [38]

(d) Location Based Routing Protocols

Some applications of WSN require to share the location coordinates value with each other and also with the base station. These location coordinates can be collected from the field with the help of a GPS system. The protocols which are based on these location information provided by the nodes are fall under the category of location based routing protocols. Most of these protocols calculates the distance between source and destination, source and relay and also relay and destination to optimize the energy consumption. In some cases the base station requires information from given region of deployment area. There are so many protocols available which are using location information of a node. Few important and popular protocols will be discussed in this section.

Minimum energy communication network (MECN) and Small MECN (SMECN)

MECN [39] has used the low energy GPS system and try to save the network energy by self-organizing nodes. A minimum spanning tree was generated by the destination node on the basis of energy as cost parameter. The topology formed by the base station node will be of minimum cost and nodes are fixed for a particular region inside the deployment field. The enclosure graph will be constructed by the source node by including lesser number of nodes than minimum spanning tree. In this enclosure graph the source node extract the shortest path by using energy consumption as cost parameter.

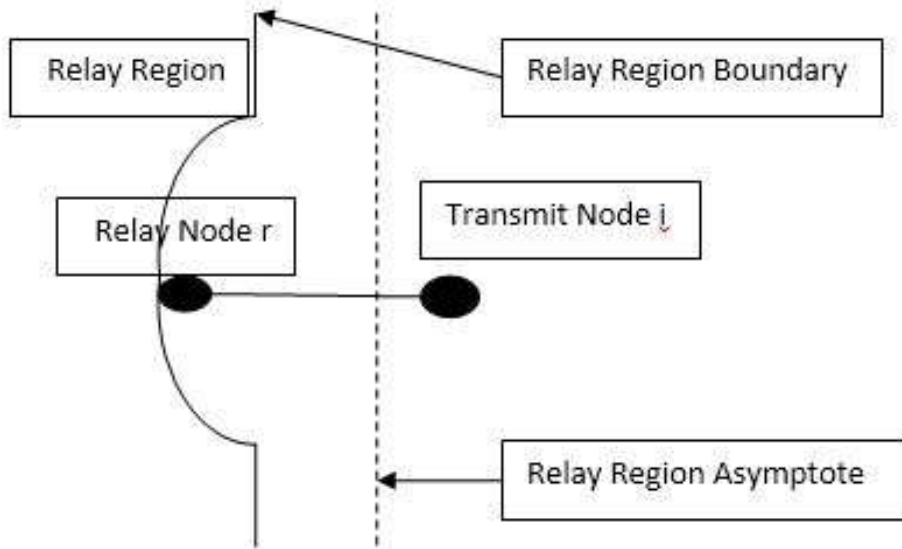


Figure 2.12: MECN Relay region of transmit-relay node pair (i, r) [39]

SMECN [39] is the proposed extension to MECN. The difference between the two is that SMECN considered the obstacles in the way of data transmission and can divert paths alongside these obstacles. The advantages of these both protocols are energy efficiency and improved network lifetime. But, these algorithms are not suitable for small size networks.

Geographic adaptive fidelity (GAF)

GAF proposed in [40] used the location coordinates to find out the best routes in the network. Deployment area will be divided into virtual grids and sensor nodes use GPS to calculate their locations w.r.t. these grids. Certain nodes which are not working properly or are not needed for some time will be turned down to sleep modes. But this do not affect the current routes and the transmission goes on smoothly. GAF keeps track of the best routes on the basis of virtual grids.

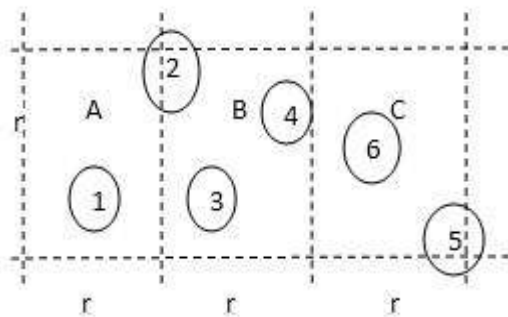


Figure 2.13: Virtual Grid in GAF [40]

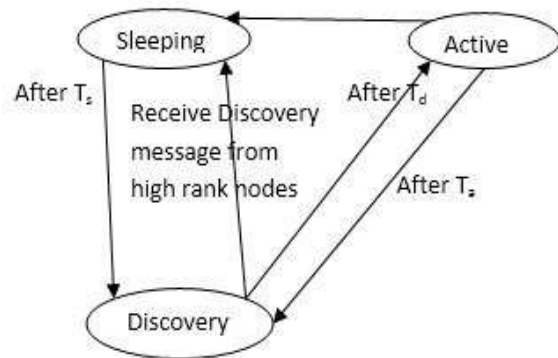


Figure 2.14: Node State transition Diagram [40]

Turning down some nodes to sleep mode will save the network energy and also increase the network lifetime. An example can be seen in the figure 2.13 below in which a virtual grid is formed. Node 1 in virtual grid A can reach nodes 2, 3 and 4 easily in B. Now as recommended by GAF out of 2, 3 and 4 two nodes can sleep because all these nodes can also reach the nodes in grid C. Hence it will save the energy of two nodes and these can be used later when the active node died. The nodes can be in any of three states: discovery, active and sleep as shown in figure 2.14 below.

(e) Network Flow and QoS-aware Routing protocols

These type of routing protocols employs QoS functions or parameters while taking the routing decisions during routing process. The network flow based protocols selects the route on the basis of network flow approaches like optimal path calculation. QoS aware protocols try to optimize many parameters together like reliability, availability and delays etc. Some of most important protocols is this classification are discussed as below.

Maximum Lifetime Routing in Wireless Sensor Networks

This protocol is based on the network flow approach and is proposed in [41]. The protocol tried to improve the network lifetime on the basis of cost of a link identified as energy consumed by that link to transmit one packet from source to destination. This cost will be calculated for each link from source node and a link which is having optimal value will be selected as actual route for data transmission. The optimization problem will be taken as the lifetime maximization problem. Cost of a link can be formulated as the factor of residual energy of a node. Equation below gives the calculation of cost on a link i to j. Here, E_i is the residual energy of node i.

$$C_{ij} = \frac{1}{E_i - e_{ij}} \quad \text{and} \quad C_{ij} = \frac{e_{ij}}{E_i} \dots\dots\dots (5) [41]$$

The shortest route will be calculated by using the above cost as link cost and the Bellmen-Ford algorithm is used. The output of the algorithm will be the path having highest residual energy. There is a problem in this algorithm that it cannot work with larger number of nodes and not suitable for most of the applications of WSN.

Energy-aware QoS routing protocol

This is QoS based protocol proposed in [42] and it utilized the rela time packet traffic load created by the image sensors. The end-to-end delay was the major parameter of consideration in this protocol. The cost of route is calculated by taking end-to-end delays through multiple

paths into consideration. The parameters used for routing were residual energy of a node, energy dissipation in transmission and packet error rate. A queuing mechanism is used to utilize the resources equally in real and non-real time traffic patterns. Dijkstra's algorithm [43] was used as basic method to find out the shortest paths by taking the end-to-end delay as routing parameter. The main advantage of this protocol is that it provides optimal values of QoS parameters. But, the link and resource utilization of this protocol is very poor.

(f) Opportunistic Routing Protocols

Opportunistic routing (OR) for WSN is an energy efficient communication technique which involve almost every sensor node of the network to participate in communication process. This technique utilizes the broadcasting nature of wireless networks [4] [45]. As the name implies OR techniques search for the best opportunity to forward a packet towards base station, even in absence of a connected end-to-end path. OR algorithms works on hop-by-hop basis and the best hop is decided on a specific criteria depending on the algorithm. Hence, there is no need of a stable end-to-end connection from source to base station. Opportunistic routing can easily adapt the changes in an unstable network. The packets in an opportunistic communication, in the network, can be delivered through different routes according to network or environment (surrounding) conditions. The energy efficient and good performer OR protocols will be discussed in this section.

Exclusive Opportunistic Routing (Ex-OR)

Ex-OR is first protocol proposed by [4] in the category of opportunistic routing. Here, MAC and routing mechanisms were collaborated to make the final decision of route selection (Figure 2.15). The source node when broadcast the data the route selection process begins. Next-hop the selection next-hop relay will be made by running a coordination mechanism and calculating a routing metric called as expected transmission count (ETX) [6]. Ex-OR explores the diversity of a node and transmits data with multiple options available.

Next-hop relay will only be selected out of a forwarder group. This forwarder group contains the best possible nodes to transmit data packets. The nodes in the forwarder group will be assigned with some priorities and always the highest priority node will transmit the data packet further. The priority here in Ex-OR is on the basis of ETX which is the total number of hop-count from source to destination using different possible paths. The route which is having minimum ETX which directly meant to be the closest node to destination will be selected a next-hop forwarder.

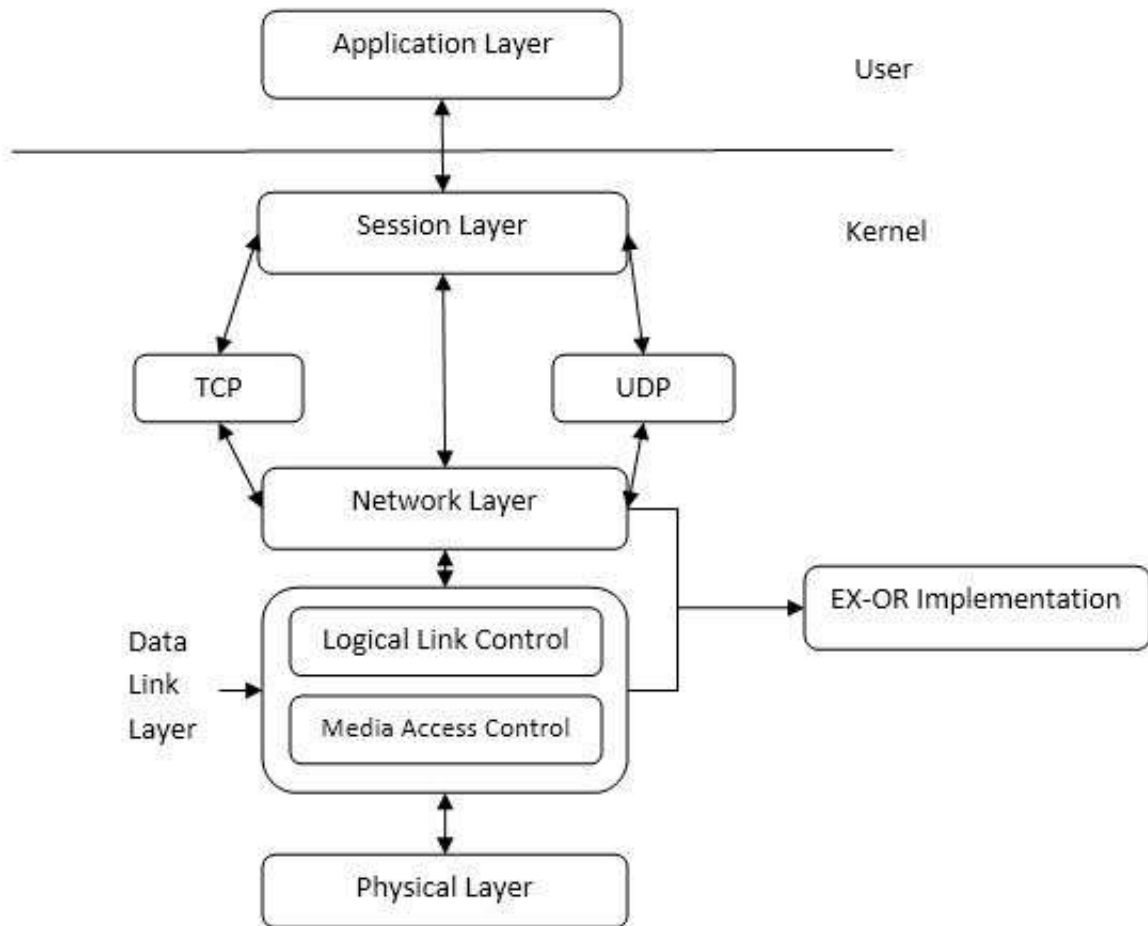


Figure 2.15: Layered Architecture – Implementation of EXOR

This will reduce the number of duplicate transmissions. The process continues on each relay node also until destination is reached. Ex-OR gives best throughput than other category protocols discussed above but poor in energy efficiency and may not be directly applied to WSN.

Energy Efficient Opportunistic Routing (EEOR)

EEOR is another protocol proposed in [15] was an energy efficient OR protocol. There were two cases discussed in this protocol for constant transmission power and dynamic transmission power. This protocol was simulated and tested for performance on TOSSIM simulator. EEOR calculates the required energy cost by each node in the neighbor list of source node and then create the forwarder set on the basis of this cost. The end-to-end cost is calculated using the link energy cost from source to destination via multiple nodes. This routing information will be stored inside the sensor node just like distance vector routing. The expected cost then updated after certain period of time defined by the application. Whenever any source node wanted to transmit data it just use the information stored in it and broadcast data packet by

including forwarder list. The node having high priority will become the next-hop relay node and rest of the nodes will discard the packet. EEOR gives the guarantee to deliver data and also duplicate data packets at destination are reduced significantly. As energy cost is calculated from source to destination always it will increase the overhead of transmitting control packets periodically.

EFFORT

EFFORT is also an energy efficient OR protocol proposed by [14] maximize the lifetime of wireless sensor network. Authors have proposed a routing metric which is opportunistic in nature. The metric is based on the residual energy of the node and calculated globally from source to destination always. EFFORT utilized the opportunistic behavior of wireless sensor networks mainly, the route diversity and reliability of transmissions. The priorities are assigned to the nodes in the forwarder group on the basis of routing metric called as opportunistic end-to-end cost (OEC). EFFORT try to improve the network lifetime by distributing the energy consumption load among all the links. NS2 has been used as simulation tool for testing the results of EFFORT. This protocol improve the lifetime and transmission reliability of the network. The implementation of this protocol is complex and the performance is good only if the network is dense.

Energy Efficient Opportunistic Multicast Routing Protocol (EOMR)

EOMR proposed in [16] is purely meant to reduce the energy cost for wireless sensor network. Rather than using broadcasting this protocol use multicast mechanism to transmit data packets toward the base station. Multicast can target the query driven applications easily and also efficient in allocating number of tasks to different nodes. The authors stated that sensor nodes will consume high energy w.r.t. communication of data packets when unicasting is used and there may be a wastage of resources like energy, bandwidth and storage when broadcasting is applied. But multicasting will optimize these parameters and is better to use with sensor networks. This protocol is also a grid based approach and will locate the sensor nodes on the basis of grids only. The sensor nodes did not forced to store the topology information of whole network but they should know the topology and number of nodes of their own grid. The optimal route selection is created by the destination node only. To decide the optimal route transmission energy and hop-count is used. When the route setup is finalized by destination it sends an acknowledgement to source node for transmitting data. EOMR is a good performer in WSN and works only with static sensors.

Middle Position Dynamic Energy OR (MDOR)

MDOR is proposed in [13] considers that choosing a node which is far away from source node but nearer to destination and vice versa cannot be a solution to solve the energy consumption problem. The energy consumption will be different for different data packets and this must be taken care of during the routing process. Hence, to solve this issue dynamic energy consumption scenario is used. Another point in this protocol is that the distance should be optimal from source to destination so that the link diversity can be utilized efficiently. The concept of two different protocols is combined in this protocol i.e. EEOR [13] and MOOR [45]. EEOR as discussed previously is energy cost based routing protocol and it selects the relay node which consume minimum energy in transmitting data packets. MOOR decides the next hop relay node on the basis of distance. It selects the relay node which is having lowest distance from the destination node. MDOR always choose the moderate distance nodes from source to destination. MDOR optimizes the results of these two protocols and is efficient for dense networks.

QoS Aware and Energy Efficient OR (QEOR) Protocol

QEOR was proposed in [17] is a protocol proposed recently to provide QoS with lesser energy consumption for WSN. The authors have proposed that QoS and energy efficiency are critical to be achieved together. This protocol proposed a QoS routing metric which will select the next-hop forwarders on the basis of packet error rate. QEOR impose a dynamic energy consumption scheme like MDOR to achieve energy efficiency during the routing process. The priorities are assigned to relay nodes on the basis of reliability of buffers and links. Implicit acknowledgement scheme is used to handle the transmission failures and reporting the packet success rate. QEOR is simulated with the help of NS2 and results are better as compared to other OR protocols proposed previously. This protocol reduces the end-to-end delays and packet error rate. This increased the reliability and throughput of the network.

2.3.2 Analysis and Discussions

The most critical and energy consuming network operation for WSN is routing. The routing for WSN is totally different to that of in traditional networks. A brief overview of the basic and popular routing protocols has been given in this chapter. The categorization and comparison on the basis of basic parameters is presented in table 2.1.

The network organization based category based protocols utilizes the network structure most of the time. The network organization based protocols are further be classified as data centric,

hierarchical and location based routing protocols. The protocols that falls under the category of data centric protocols impose less calculation overheads during the routing process. Most of the protocols of this category are based on continuous data transmissions or queries asked by the base station. The radio consumes a lot of energy during these types of communication patterns. Hence, the protocols are not energy efficient and hence reduce the lifetime of the network.

Another subcategory is the hierarchical routing protocols which are mostly based on the cluster formation by the sensor nodes. The cluster heads are chosen based on the capabilities of sensor nodes. The data packets will be transmitted through these cluster heads only. Another capabilities of cluster heads involve the aggregation of data which will remove the redundant data and coordinating with other cluster heads in the network. The research interest in these type of protocols involve the cluster formations and election of cluster heads.

Third classification in the network organization based protocols is the location aware routing protocols. These protocols work on the basis of geographic information of sensor nodes. Most of the protocols which fall under this category are distance based and make routing decisions by calculating distance between source nodes to destination. These protocols works efficiently for small sized networks. The research gaps in these protocols are energy efficiency and guarantee of data delivery.

Network flow and QoS based communication protocols try to improve the data forwarding quality during routing, inside the network. The protocols falls under this category will always construct routes on the basis of a QoS based routing metric. The QoS function must be designed in such a way that it will optimize the resource utilization and gives best performance results. QoS based routing protocols are mostly applied to those WSN applications in which imaging sensors are used.

Opportunistic routing is the other category discussed over here in which the broadcasting abilities of wireless links are utilized. As sensor networks are opportunistic in nature these protocols provide high throughput and reliability than other types. This is new research topic for WSN. There are a few routing protocols proposed in this category and the performance results are pretty good. The protocols are able to improve throughput, energy efficiency, and scalability. QoS is still a research gap in these protocols. Other research gaps involved the number for duplicate packets, energy consumption due to broadcasting, security of data packets as well as the routing process and also the high end-to-end delays.

Comparative analysis of this research provide a conclusion that OR protocols are having good performance. The OR protocols can work with any number of nodes and these are scalable also. It is clear from the literature that most of the protocols are proposed for static sensors only there is a great need of good protocols for mobile sensors also. Table 2.1 give a brief overview of the features compared for various routing protocols.

Table 2.1: Routing Categorization and Comparison

Routing Protocol	Classification	Power Usage	Data Aggregation	Query based	Over head	Data delivery model
Flooding and Gossiping [27]	Data Centric	High	Nil	No	Low	Continuous
SPIN [26]	Data-centric	Ltd.	Yes	Yes	Low	Event driven
DD [28]	Data-centric	Ltd	Yes	Yes	Low	Demand driven
EAR [30]	Data-centric	Low	Nil	No	High	Event Driven
RR [31]	Data-centric	Low	Yes	Yes	Low	Demand driven
CADR [47]	Data-centric	Ltd	Yes	Yes	Low	Continuously
COUGAR [48]	Data-centric	Ltd	Yes	Yes	High	Query driven
ACQUIRE [49]	Data-centric	Low	Yes	Yes	Low	Complex query
R3E [50]	Data Centric	Low	Yes	No	Low	Continuous
LEACH [24]	Hierarchical	High	Yes	No	High	Cluster-head
PEGASIS [36]	Hierarchical	Ltd	No	No	Low	Chains based
TEEN & APTEEN [38]	Hierarchical	High	Yes	No	High	Active threshold
Younis <i>et.al.</i> [46]	Hierarchical	Ltd	No	Yes	Low	Cluster Based
SOP [23]	Hierarchical	Low	No	No	High	Continuous
MECN and SMECN [39]	Location Based	Low	No	Yes	High	Query Driven
GAF [40]	Location	Ltd	No	No	Mod	Virtual grid
GEAR [51]	Location	Ltd	No	No	Mod	Demand driven
Chang and Tassiulas [52]	Network Flow and QoS Aware	Low	No	No	Mod	Continuous
Dasgupta <i>et.al.</i> [53]	Network Flow and QoS Aware	Low	Yes	Yes	Mod	Continuous
SAR [25]	Network Flow and QoS Aware	High	Yes	Yes	High	Continuous
Akkaya and Younis [42]	Network Flow and QoS Aware	Low	No	No	Mod	Real Time Traffic
SPEED [54]	Network Flow and QoS Aware	Low	No	Yes	Less	Geographic

IDDR [55]	Network Flow and QoS Aware	Low	No	No	Low	Continuous
EEOR [15]	Network Flow and QoS Aware	Low	No	No	High	Continuous
Ex-OR [4]	Opportunistic	High	No	No	High	Continuous
ORTR [56]	Opportunistic	Low	No	No	Low	Real Time Traffic
ORW [57]	Opportunistic	Low	No	No	Mod	Continuous
EFFORT [14]	Opportunistic	Ltd	No	No	Mod	Active
ODEUR [58]	Opportunistic	Low	No	No	High	Continuous
Zeng <i>et.al.</i> [59]	Opportunistic	High	No	No	High	Continuous
FORLC [60]	Opportunistic	Ltd	No	No	Mod	Continuous
EAOR [61]	Opportunistic	Low	No	No	Mod	Continuous
EQGOR [62]	Opportunistic	Low	No	No	Low	Continuous
SOFA [63]	Opportunistic	Low	No	No	Low	Continuous
MOOR [44]	Opportunistic	High	No	Yes	Low	Query Driven
EOMR [16]	Opportunistic	Low	Yes	Yes	Low	Query Driven
MDOR [13]	Opportunistic	Ltd	No	No	Low	Continuous
QEOR [17]	Opportunistic	Ltd	No	No	Mod	Continuous

2.4 Related Work

In [1] authors had presented the basic concepts of WSN, applications of these networks, design issues, hardware constraints involved in these. Also the paper had presented the protocol stack for sensor networks. The protocol stack discussed in this survey was a five layer network model. Authors raised a point that ad-hoc routing mechanisms may not work well for sensor networks and more attention should be given for developing sensor oriented protocols. Energy constraint is the reason given by the authors for not using the traditional routing protocols for WSN. Authors have presented a discussion about the requirements of WSN like networking, security etc.

In [3] authors presented a detailed literature on routing protocols for wireless sensor networks and discussed various issues involved in these protocols. Authors have categorized the discussed routing protocols into three classifications i.e. location based, data centric and hierarchical routing protocols. The authors have discussed and presented each routing protocol in detail under each classification. Also the methodology of each category was discussed and concluded with the open research questions.

There are so many other literature [2] [7] [21] based papers published in different journals, conferences and books for wireless sensor networks. But as thesis is more focused to

opportunistic routing discussed above and the security of route selection processes, the trust based secure routing mechanisms will be discussed in upcoming subsection.

2.4.1 Trust Aware Routing in WSN

Whenever it comes to security of the network cryptographic systems will come to the mind of every researcher. But cryptographic techniques [64-68] has been proved to consume high energy in computation and occupy more storage space. As already being said that energy efficiency is an important performance parameter and delay is also a critical performance factor, cryptosystems cannot be used. Instead of using cryptosystems for the security purpose if sensor nodes could avoid selecting malicious or non-cooperative nodes as relay nodes than the energy consumption and delay will be less. For doing this trust management systems can be used. Some of the trust aware protocols used in thesis for comparison are discussed below.

In [18] authors have proposed a trust and location aware routing (TLAR) protocol for WSN. The objective of TLAR was to provide a lightweight and dependable routing algorithm for WSN. TLAR consist of two main modules one is trust assessment and second is routing. Trust value was calculated on the basis of forwarding sincerity, packet integrity, network acknowledgements, energy, and secondary trust values. A consolidated trust value is calculated and the nodes which were having lower trust values, not included in routing process.

In [19] proposed a new trust aware routing protocol named as trust and energy aware secure routing protocol (TESRP) for sensor and actuator networks. This protocol exploited the trust distribution method for finding out the malicious and selfish nodes. This protocol considered the trust value of a node and energy dissipation by the same in performing network operations. Hop-counts are also taken into consideration to identify the shortest path to base station. TESP is intended to be energy efficient and impose small communication overhead during the network operations.

Another efficient routing protocol for WSN is trust aware opportunistic Routing (TAOR) [20]. This protocol was energy efficient and also reduces the end-to-end delays. The next-hop relay nodes are decided on the basis of link delivery probabilities but also trust values of neighbor nodes were involved in route selection. TAOR was proved to have good results in the presence of malicious nodes.

Trust management systems can build up coordination among nodes and avoid malicious nodes in routing process. The sensor nodes which having lower trust factors will not be selected for transmission or reception of data packets. There are very few trust based opportunistic routing

protocols are available in literature. OR must involve trust values inside the routing metric to avoid malicious nodes so that there will be improvement in the network performance.

2.4.2 Packet Load Balancing based OR Protocols

Load balancing of packet transmission is required when there is a continuous data flow in the network. The buffers of relay nodes gets full and the incoming packets are either dropped or face high delays [8]. This will reduce the throughput of the network. To overcome this problem there must be buffer aware routing protocols. Buffer aware routing protocols can divide the load of relaying packets towards the base station among all relay candidate nodes. Working in this direction some opportunistic routing protocols are proposed for wireless networks. Load balancing is an important aspect to consider and must be employed in WSN to improve the performance of the network.

In [68] authors have proposed a buffer aware opportunistic routing (BAOR) mechanism which combine the location and buffer length of relay nodes to assign priorities. This will prevent the situation where a larger number of packets queue in the buffer of relays on the shortest path. Network simulation results showed that BAOR outperformed traditional OR schemes in terms of both network throughput and end-to-end packet latency.

In [69] authors have proposed a packet based opportunistic routing protocol (POR) which has used packet-piggyback-overhearing technique to schedule the packet delivery by different source nodes. POR works well with large scale networks and suitable for wireless sensor networks. To achieve the best scheduling “Push-Pull” mechanism was used. POR is a lightweight protocol in terms of energy consumption. POR can balance the network traffic among each node in the network. POR shows good simulation results as compared to traditional routing schemes.

2.5 Simulation Environment and Tools

In this section simulation tools used in this thesis are presented. To accomplish the simulation task and present the results in form of graphs two popular tools are utilized i.e. MATLAB and Network Simulator (NS). MATLAB [9] is used for simulating the routing metric based on existing protocols. MATLAB is because it is fast and efficient to provide results. NS is a simulation tool in which the protocols may be simulated easily and it gives good simulation based results. Bothe tools are discussed as in following subsections.

The simulation models for energy depletion factor proposed in Chapter 3 and trust aware routing metric proposed in Chapter 5 are built upon MATLAB. MATLAB is a popular tool for simulations of networks and it is high performance tool for computations and graphic visualizations. The combination of analysis capabilities, flexibility, reliability, and powerful graphics makes MATLAB the premier software package for scientific researchers. An interactive environment is provided by the MATLAB with numerous of inbuilt mathematical functions and simulation tools. For simulating the proposed protocols in Chapter 4, Chapter 6 and Chapter 7 network simulator (NS) is used [11]. NS is based on two programming languages C++ and object based tool command language (OTcL) [11]. The algorithms will be coded in C++ and the simulation scenarios are coded in OTcL. Users can code their proposed work in NS by specifying specific network topologies, proposed protocols and all other network requirements. Network Animator (NAM) [11] is used to see the visualization of the network setup. NS-2.35 version is used in this thesis to code the proposed work.

2.6 Parameters of Evaluation

This section will discuss the basic parameters used for evaluation of proposed work. The proposed protocols are compared with existing protocols by using these parameters. These parameters are commonly used for comparative analysis of routing protocols.

Energy Consumption

This is the most important factor for measuring the performance of protocols in WSN. It is measure as the total energy consumed to perform all the network operations in sending one packet from source to base station [70]. Another definition considers the total energy consumption until the network is operational.

Network Lifetime

Network lifetime is directly dependent on the energy consumption inside the network. It is measured as the time elapsed between the starting of the network and the time at which first node of the network is assumed to be dead. The nodes is assumed to be dead when it is not capable of performing network operations especially data transmissions. Losing a node will also lose some capabilities of network [70].

End-to-End Delay

End-to-end delay is the average time elapsed in sending one packet toward the base station and receiving the same successfully at base station. Let T_i be the time separating the transmission

of a packet i from the source node and its reception at destination. Let P_T be the total number of packets that are correctly received. The average end-to-end delay is given as in equation below [24].

$$ED = \frac{\sum_i^{N_c} T_i}{P_T} \dots\dots\dots (6)$$

Path Loss

In the networking field, free-space path loss (FSPL) [71] is measured as the loss in the strength of signal of a packet in form of electromagnetic wave that would result when it is transmitted through any free space (commonly air), without any hurdles nearby to cause any diffractions or reflections. The equation for path loss to be measured in decibels (dB) is as given below.

$$Path_Loss = 32.4 + 20\log_{10}(f_c) + 20\log_{10}(d) \dots\dots\dots (7)$$

Where, f_c is the signal frequency (Hertz) and d is the distance between sender and receiver.

Packet Delivery Ratio (PDR)

It is measured as the ratio of number of packets successfully received at base station to the number of packets sent by the source node [24].

$$PDR = \frac{\sum \text{Number of successfully delivered packets}}{\sum \text{Number of packets sent}} \dots\dots\dots (8)$$

Throughput

Throughput can be measured as the bits sent per second by each source node toward the base station. In this thesis throughput is measured as the number of packets transmitted in a given time toward the base station [24].

Risk Level

Risk level is used as performance parameter for trust aware protocols. It is measured as the number of mischievous sensors encountered during the routing process [20]. The number of malicious nodes are counted on the basis of trust values and for the protocols in which security is not applied risk level is measured on the basis of packet dropping ratio.

CHAPTER 3

ENERGY EFFICIENT OPPORTUNISTIC ROUTING METRIC

3.1 Introduction

Energy consumption is a major constraint in WSN because sensor nodes have been supplied with a limited amount of energy. Most of the nodes' total energy will be consumed in transmission and reception of data packets during network operation. Optimize energy consumption in transmission and reception of data packets relies on an optimal route selection process. Routing protocols should select the best possible route so that the energy consumption can be minimized. Most of the energy efficient routing protocols for WSN depends on the routing metric used to select the best possible route. Traditional routing protocols fail to provide energy efficiency in WSN because the route once selected will be furnished up for entire data transmission. This will cause node failures due to energy depletion of same nodes again and again. Opportunistic routing (OR) will provide real-time data delivery and decrease the delay in the network to provide energy efficiency. While using OR retransmissions will be less and hence less energy will be consumed. OR protocols also depends on a routing metric for next-hop selection.

This chapter presents a new energy-aware OR metric for WSN called as an energy depletion factor (EDF). EDF is designed on the basis of residual energy of a node. It considers energy consumed during transmission, retransmission, and reception of data packets and acknowledgments during the network operation. EDF can be used directly with existing OR protocols for WSN.

3.2 Motivation and Related Work

Ad-hoc on demand distance vector (AODV) [10] and destination sequenced distance vector (DSDV) [12] routing protocols are most popular and usually employed in networking. These protocols make the route selection on the basis of smallest hop-count from source to destination. AODV is a source initiated protocol and built the route only when it is needed from the source. The routing table has been maintained in both AODV and DSDV. The table will be usable as long as the source needed it. Both of these protocols are not basically built to reduce energy consumption and not purely meant for WSN.

Routing protocols for WSN must reduce the energy consumption to extend the life of the sensor network. Routing protocols for WSN introduce such routing metrics which are capable to cut the energy use inside the nodes to prolong the node's lifetime [72] [73] [74]. [72] Presented an energy efficient routing metric which tried to optimize the energy use to extend the network lifetime. Authors of [73] proposed two routing metrics for single and multiple links which put in energy efficiency during data packet transmission. The nominated study was able to lessen the energy use and optimize data delivery rate and energy expenditure. This employment was extended in [72] which has put in residual energy inside the forwarder selection metric. In these all protocols, the end-to-end delay for data packets is high and there will be a wastage of broadcasting abilities of sensor nodes. The information theory suggested that traditional routing may not be the best-routing solutions [74].

The broadcasting abilities of wireless radios installed on sensor nodes can be used efficiently by using opportunistic routing. Opportunistic routing takes the advantages of cooperative diversity by using broadcasting nature of wireless links [4]. The data packets will be conveyed through multiple relay nodes. Due to multiple relays, the data can be delivered to the destination through any path and it will reduce the retransmissions. If any of the nodes fails in between any path, there will be an optional path to finish the data transmission. The next hop selection must be energy efficient and also there should be a coordination method in between the relays. The process of OR can accomplish these tasks using OR metrics, which will aid in data forwarding efficiently.

Expected transmission count (ETX) [6] was proposed as an OR metric for wireless networks. This metric selected the optimal path on the basis of the lesser number of hop counts. Based on ETX the researchers around the world has proposed Expected Any-path transmission (EAX) [75], modified ETX (mETX) [76], Effective Number of Transmissions (ENT) [76], Expected Transmission Time (ETT) [77], Expected Data Rate (EDR) [78], Expected One hope Throughput (EOT) [79], Opportunistic End-to-end Cost (OEC) [14], and Opportunistic Expected One hope Throughput (OEOT) [80]. The writers of these metrics have also proposed OR protocols using these. OEC and OEOT focus on the energy efficiency and tried to reduce the end-to-end delay in the network.

These all OR metrics can be split into two classes dependent on the routing facts collection methods and calculation of the metric: local OR metrics and global OR metrics. The local class OR metrics will be worked out and maintained in a distributed fashion at each sensor node in the network [79] [81] [82]. While the global OR metrics will be worked out at the root node

only by compiling info from other nodes on multiple paths [4] [75] [83-86]. Local OR metrics cause low overhead in terms of computation and in terms of energy cost. On the other hand, source node will consume lots of its energy in communicating and working out the routing metric and deciding the whole route. In [24] the authors have proposed an OR approach for WSN by using a routing metric totally dependent upon the transmission power of data packets. The transmission power was assumed to vary during different transmissions. Total energy consumption was dependent on the number of transmissions made to the relay nodes. The proposed metric was local in nature. While OEC which was a global OR metric which decide the complete route first and then transmit the data packets toward the destination. As the distribution of energy cost among all the nodes of the network is important, in next section a new distributive OR metric will be advised. It is also local in nature and consumes lesser amount of power for computation.

3.3 Proposed OR Metric: Energy Depletion Factor (EDF)

Energy depletion factor is an energy efficient OR metric for WSN which improve the network lifetime by distributing energy load equally among all the nodes during network operations. EDF takes into account the residual energy of a node and calculates the impact of each transmission and reception of data packets. The basic energy consumption and EDF model will be discussed in following subsections.

3.3.1 Energy Cost Model

The sensor nodes in a sensor network have been supplied a limited amount of energy. In most of the applications, the sensor nodes are left unattended and deployed in such areas in which it will not be possible to install backup power sources. Hence, sensor nodes have to rely on small size battery for performing network operations. Most of the energy consumption inside a node will take place in transmitting and receiving data packets. Retransmissions and path loss will also cause lots of energy consumption. In [13] the equations for first-order transmission and reception energy calculation are given which has been rewritten over here. A sensor will consume E_{Trans} energy when it transmits an n -bit data packet over distance l , it will be given by the equation (1) below:

$$E_{Trans}(n,l) = \begin{cases} n.E_{R_elect} + n.E_{R_fs}.l^2, & \text{if } l < l_0 \\ n.E_{R_elect} + n.E_{R_amp}.l^4, & \text{if } l \geq l_0 \end{cases} \dots\dots\dots (1)$$

E_{R_elect} is the electronic energy consumed by a radio of a node to receive or transmit a data packet. When a sensor node receives n bit packet, it will ingest $E_{Receieve}$ amount energy given by equation (2) below:

$$E_{Receieve}(n) = n.E_{R_elect} \dots\dots\dots (2)$$

Whenever a forwarder candidate node has to send an n -bit data packet to the base station, its radio circuit consumes, $E_{Forward}$ energy calculated by equation (3).

$$E_{Forward}(n,l) = E_{Trans}(n,l) + E_{Receieve}(n)$$

$$= \begin{cases} 2n.E_{R_elect} + n.E_{R_fs}.l^2, & \text{if } l < l_0 \dots\dots\dots (3) \\ 2n.E_{R_elect} + n.E_{R_amp}.l^4, & \text{if } l \geq l_0 \end{cases}$$

E_{R_amp} is the electronic energy consumed to amplify a data packet, where the distance is l .

3.3.2 Energy Depletion Factor

The proposed metric is named as EDF because it tells the routing protocol to resolve the next hop on the basis of residual energy. The metric calculates the impact of each transmission and reception on the residual energy of each node. The nodes which are having a lesser impact will be selected as the next hop relay sensor. This metric will distribute the energy consumption load among all the nodes and improve network lifetime. Authors of [14] have discussed that the transmission and reception radio energy is same for all nodes, but the impact of these on the residual energy of each node will always be different.

Let's await at one example, consider two relay nodes C1 and C2 in the network having residual energies as 5 and 2 units respectively. Here, the assumption is that the distance between source and C1 is greater than that of distance between source and C2.

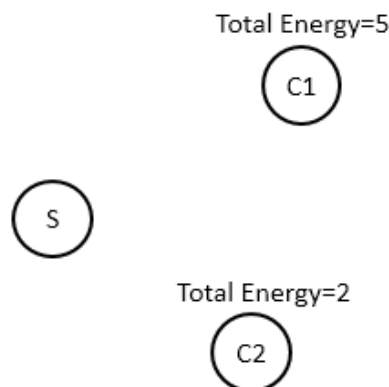


Figure 3.1: Example Scenario

Suppose, for transmitting one data packet the node's radio will consume 1 unit of energy. According to the distance factor, if C2 transmits the data packets further toward the destination, it will cost 50% of its residual energy. On the other hand, if C1 will be chosen as a relay node, it will cost its 20% of energy. Hence here we can consider that the impact of just one transmission is different for both C1 and C2. Also, C2 will use up all of its energy only in just two transmissions. EDF will make a node to calculate these impacts and helps the source node to find out the energy efficient nodes for the route selection. Each node will calculate EDF independently for other relay nodes and this will always select energy efficient nodes for routing.

The impact (SEC_{Ni}) on the residual energy (RE_{Ni}) of a node (Ni) by using energy consumption inside the node (EC) as follows from an equation (4).

$$SEC_{Ni} = \frac{EC}{RE_{Ni}} \dots\dots\dots (4)$$

This impact calculation SEC_{Ni} avoids the exhaustion of energy of each node in the network. With respect to above, example source node transmits packets towards C1 and C2. On reception of a packet, the impact SEC_{Ni} will be calculated by both C1 and C2. The impact comes out to be 0.3008 for C1 and 0.88 for C2. As the impact on C1 is less than the impact on C2, C1 will be chosen as a next-hop relay node and will do the same procedure until the destination has been reached. There will be different types of energy consumptions inside a node and hence those can be used to provide a composite routing metric. The components of EDF are as follows.

- a. **Transmission Impact** ($E_{tx:Ni \rightarrow fwd}$): It is the energy impact on a node Ni used in transmitting the n bit data packet toward its neighbor nodes using radio power E_{Trans} (eq. (1)), calculated as follows:

$$E_{tx:Ni \rightarrow fwd} = \frac{E_{Trans}}{RE_{Ni}} \dots\dots\dots (5)$$

- b. **Receiving Impact** ($E_{rx:Ni}$): It is the energy impact on a node Ni consumed in receiving an n -bit packet from neighbor nodes using radio power $E_{Receive}$ (eq. (2)), calculated as follows:

$$E_{rx:Ni} = \frac{E_{Receive}}{RE_{Ni}} \dots\dots\dots (6)$$

c. **Retransmission Impact** ($E_{re_tx:Ni \rightarrow fwd}$): It is the impact calculation on the residual energy of a node spent on retransmitting n bit data packet towards neighbor nodes consuming radio power in transmitting data packets and receiving acknowledgments. This energy cost of retransmitting data packets can be calculated by using Eq. (3). The impact can be estimated as follows:

$$E_{re_tx:Ni \rightarrow fwd} = \frac{E_{Forward}}{RE_{Ni}} \dots\dots\dots (7)$$

d. **Acknowledgement Impact** ($E_{ACK:Ni \rightarrow source}$): It is the energy impact on a node N_i used in transmitting the n bit acknowledgments toward its neighbor nodes using radio power E_{Trans} (eq. (1)), calculated as follows:

$$E_{ACK:Ni \rightarrow source} = \frac{E_{Trans}}{RE_{Ni}} \dots\dots\dots (8)$$

All of these values will be aggregated to compute the overall impact, in form of EDF, of transmission and reception on the node's residual energy. EDF will be calculated at each relay node and this process will end only after the destination is reached. The relay node having a minimum value of EDF will be selected as next hop relay node and it will forward the first data packet. Other relay nodes will wait for the acknowledgments. In this manner, the relay nodes will be selected opportunistically in the path choice procedure. The EDF can be computed as follows.

$$EDF_{Ni} = \frac{E_{tx:Ni \rightarrow fwd} + E_{rx:Ni} + E_{re_tx:Ni \rightarrow fwd} + E_{ACK:Ni \rightarrow source}}{RE_{Ni}} \dots\dots\dots (9)$$

The EDF will distribute energy consumption load equally among all nodes in the network and give a chance to every relay node to participate in the routing process. For the purpose of testing EDF, it is being applied as a routing metric in AODV and compared to other commonly used metric minimum distance and minimum energy again applied in AODV for next hop selection. The simulation scenario and results are discussed in the following sections.

3.4. Experimental Results and Performance Analysis

Before start discussing the simulation settings and results following assumptions will be brought into account.

- a. There will be one sink node (base station) and sensor nodes will be randomly deployed in a square area.
- b. All nodes will generate data and this data will be transmitted towards the base station.

3.4.1 Simulation Scenario

The proposed metric is applied in AODV [10] protocol to select the energy efficient routes. AODV is also modified to use minimum energy and minimum distance as routing metric. After modification to AODV, all three modified AODV protocols are simulated using MATLAB by using the simulation settings shown in Table 3.1 below. The nodes are randomly deployed in 500 x 500 m² area. Immediately, after complete deployment, nodes broadcast hello packets to collect the information about the neighbors. The results are plotted in the form of graphs and also the average results are shown for better analysis.

Table 3.1: Simulation Settings

Parameter	Description
Examined Protocols	AODV_Min_Energy, AODV_Min_Distance, Proposed (AODV_EDF)
Simulator	MATLAB
Area	500 m x 500 m
Range of Radio	75 m
Number of Nodes	50, 100, 200
Size of Packet	46 bytes
Data Rate	250 kbps
Initial Energy	10.0 J
Electronic Energy (E_{elec})	$50 * 10^{-9}$ J
Amplification Energy (E_{amp})	$10 * 10^{-9}$ J
Number of Rounds	300

3.4.2 Results and Analysis

The nodes are static and considered to be deployed randomly in a specified area with a single base station. Data transmission will only be considered and counted in successful transmissions only when it reaches the base station. The source node will be selected arbitrarily and it will generate data packets continuously. The sensor node will be considered dead only when the residual energy will be below 0.2 Joules.

After putting up the simulation scenario, the simulation will be completed in many rounds. In each round, a new source will be selected and the results are recorded. The performance of all three modified AODV recorded and discussed as follows.

Network Lifetime: It is delineated as the total time elapsed from the starting time of the network and time at which the first networked sensor runs out of energy to transmit a data packet. Because to lose a node could mean that the network could lose some functionalities. The average network lifetime is indicated in figure 3.2 below. The nodes will communicate data packets towards the base station and this operation will cost some of the energy of a node. The node will be considered to be dead only when it decays all of its energy. In case of minimum energy and minimum distance, same nodes will get selected as relay nodes again and again. Hence, this will result in exhaustion of energy of each node on the same route. This will decrease the network lifetime and increase the delay due to the reconstruction of the path. On the other hand, using EDF will aid in allocating energy consumption load equally among all the nodes. This will be done by selecting a different relay node from available choices. The significant difference can be seen from the results that the protocol using EDF performs better than that of minimum energy and minimum distance.

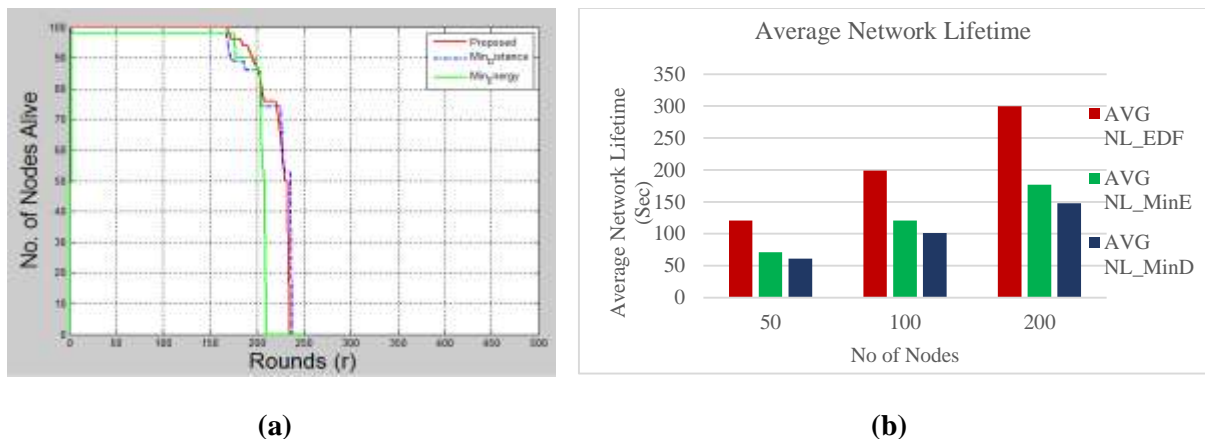


Figure 3.2: a) Number of nodes alive after each round b) Average network lifetime in seconds

Throughput: Generally throughput is defined as the average number of packets transmitted from source to destination. Here in MATLAB, the simulation was performed in rounds and hence, the throughput is defined as an average number of packets transmitted towards the base station. The throughput calculation is same for all three protocols. From figure 3.3 the results can be seen for each round of simulation and it shows the good performance of proposed metric EDF. This is because of the packets transmitted towards base station using only reliable relay nodes which are having a lower impact on their residual energy. The energy consumption will

be distributed among all nodes equally and hence there will be an increase in a number of successfully delivered packets. There will be a decrease in throughput when a number of retransmissions increases. The problem of retransmission will occur in both minimum energy and minimum distance because of node failures. This is why the results are better for proposed routing metric.

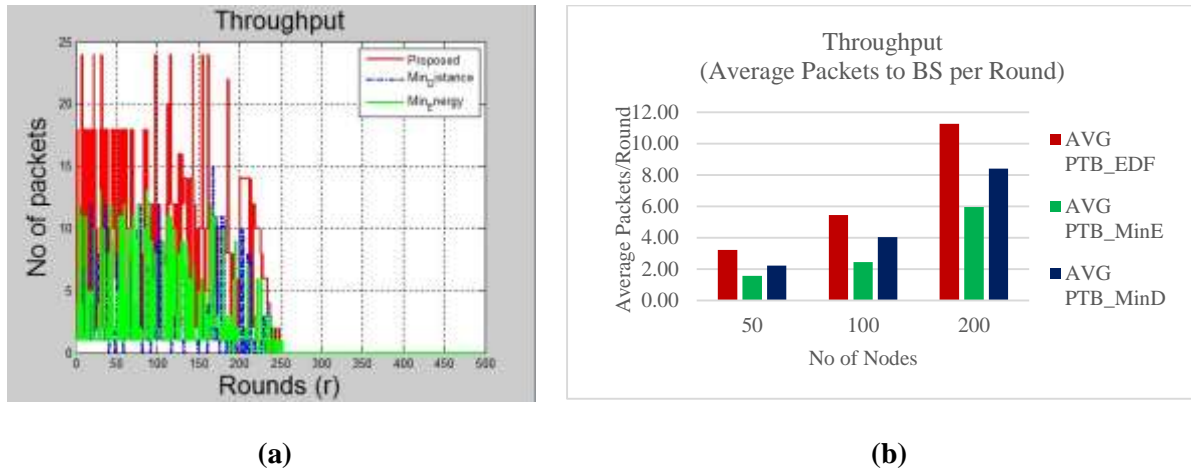


Figure 3.3: a) Number of packets delivered at base station after each round b) Throughput

Path Loss: Free space path loss model has been considered for simulation purpose. Path loss is defined as the strength reduction of the packet during the propagation on the wireless channel. The path loss will cause energy consumption of a node during the amplification process. If path loss is high then retransmission will also occur frequently. High path loss will cause high energy consumption due to amplification and retransmissions. The number transmission failures are less in case of EDF and hence it will impose less path loss and becomes energy efficient.

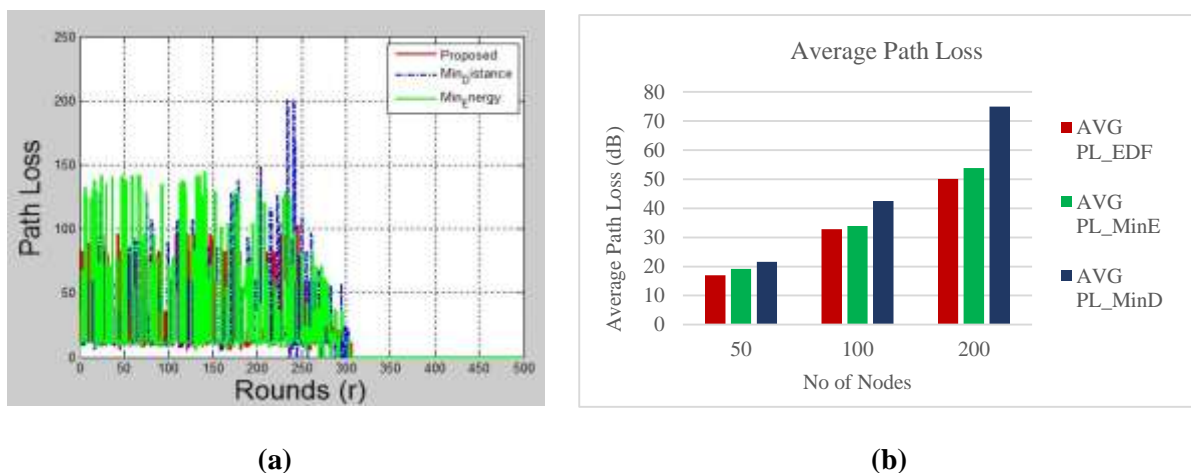


Figure 3.4: a) Path loss calculated after each round b) Average Path Loss

End-to-end delay: This can be measured as the total time elapsed in transmitting a data packet from the source node and receiving the same at the base station. The average delay per packet can be seen in figure 3.5 below. From the figure it may be depicted that the proposed EDF metric impose less delay because of its opportunistic nature. As the number of choices will be available for the transmission of data packets there will be a lesser chance of a packet to be in a waiting queue. This will reduce the packet inter-arrival time. In other two modified AODV protocols the packets will be transmitted through the same path again and again and hence this will queue up the packets inside a single relay node. It will increase the waiting time of the packet and hence the end-to-end delay also.

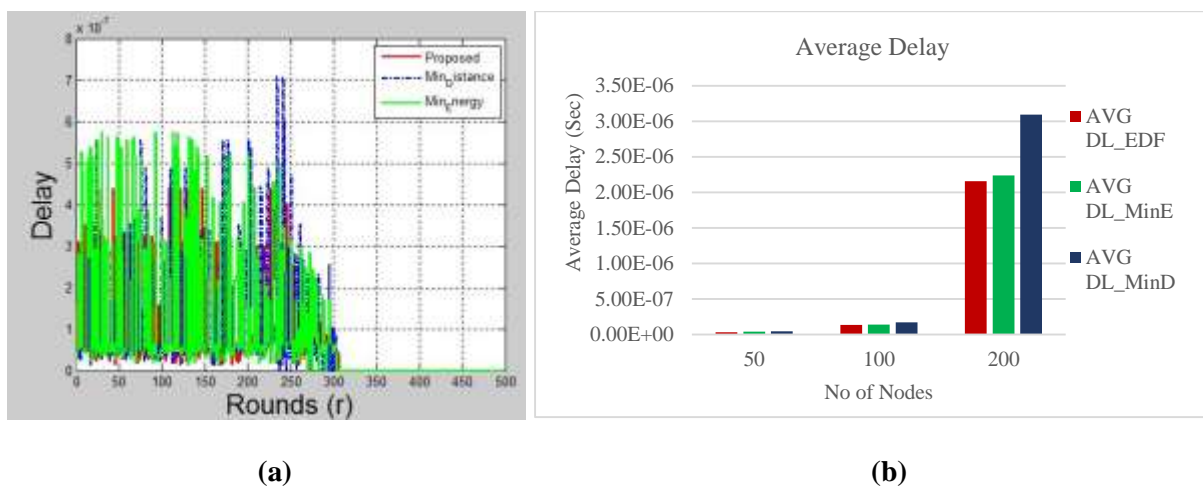


Figure 3.5: a) Delay calculated after each round b) Average end-to-end delay

3.5 Conclusion and Future Scope of Work

Energy depletion factor is an opportunistic routing metric which distributes the energy load of transmission and reception of data packets among all the nodes of the network equally. The broadcasting nature of wireless links has been utilized in this metric and all the neighbor nodes can be used as relay nodes. This will reduce the number of retransmissions of data packets. Hence, due to this, the energy consumption will be reduced and this will improve the lifetime of the network. EDF equally anticipates the energy consumption and remaining energy of each node in the network. The routing mechanism used over here is AODV. AODV has been modified to use minimum energy, minimum distance, and EDF as next hop selection metric. All three modified protocols were simulated by using MATLAB and after simulation, the results are plotted. The results depicted the better performance of EDF. EDF can be used with any opportunistic routing protocol to provide the energy efficiency in the network.

CHAPTER 4

ENERGY EFFICIENT OPPORTUNISTIC ROUTING PROTOCOL

4.1 Introduction

There are a variety of applications in which WSN is in common use, like health monitoring, environment monitoring, intruder detection and tracking objects. All of these applications use such sensors which are low in cost. These sensor nodes have certain limitations like low energy, low storage capacity, the short range of radios etc. But, small size and low cost of sensor nodes make users use these for data collection. Moreover, wireless sensors can organize themselves to form a wireless network and start working without any intervention of human beings. Hence, the sensor nodes can be deployed in such fields also where it is impossible for the humans to reach. In this unattended environment the network lifetime is very important because as long as the network will survive, it will send required the information. The network lifetime is directly dependent on the energy consumptions inside the nodes. Most of the times, WSN are designed by the researchers to operate in unattended environments for a long period of time. This is because the battery replacement or recharging is not feasible or most of the times are impossible. Hence, there is a great need of preserving the battery life to increase the life of sensors and the whole network.

Most of the energy of sensor nodes will be consumed in communication i.e. in transmitting and receiving data packets. Hence, there is a great need for energy efficient communication techniques. The task of communication techniques, however, is not limited to provide energy efficiency, but also distribute the residual energy of the network efficiently and reduce the packet losses. Hence, whenever designing a routing protocol, the impact of this protocol on a lifetime of the network must be one of the major goals. In WSN, energy efficiency should be a major concern while designing the new routing technique. In most of the real-life applications of WSN such as industrial process control monitoring and intruder detection, the throughput of the network is critical and of major concern.

Opportunistic routing (OR) for WSN is an energy efficient communication technique which involves almost every sensor node of the network to participate in the communication process. This technique utilizes the broadcasting nature of wireless networks [4]. As the name implies

OR techniques search for the best opportunity to forward a packet towards the base station, even in absence of a connected end-to-end path. OR algorithms works on a hop-by-hop basis and the best hop is decided on specific criteria depending on the algorithm. Hence, there is no need for a stable end-to-end connection from source to the base station. Opportunistic routing can easily adapt the changes in an unstable network. The packets in an opportunistic communication, in the network, can be delivered through different routes according to network or environment (surrounding) conditions. In this chapter, a new energy efficient opportunistic protocol has been proposed, simulated and evaluated on the basis of the simulation results.

4.2 Motivation and Related Work

Reducing energy consumption is a critical issue in WSN and the researchers in are focusing on it. In recent years, researchers have proposed OR algorithms for WSN, which are mainly focusing on the routing operation and data forwarding. In most of the recent researches, the OR algorithms' designs try to select forwarders on the basis of previously proposed metrics as well as candidate coordination also. [45] and [69] have presented various surveys on OR for ad-hoc networks and WSN.

The very first and famous OR algorithm proposed is ExOR [4]. ExOR selects candidate set on the basis of ETX metric. The ETX was proposed in [6], which simply compute the number of hops from source to destination, and also it computes the number of transmissions and retransmissions required on a link up to the destination. In ExOR every node run shortest path algorithm by considering ETX metric as link weight. The nodes, which are on the minimum weight path, are selected as the candidate forwarders.

Working in the same direction [83] proposed LCOR algorithm, which works to get the optimized route using optimal candidate selection algorithm. LCOR used EAX as forwarder selection metric, which was originally proposed by [75]. EAX is especially proposed metric to fir for the requirements of OR protocols. But there is a great loss of energy in calculating EAX for each node in the network. Another OR algorithm was proposed by [84] named as SOAR which also uses ETX as candidate forwarder selection metric. The algorithm, after calculating the ETX, works on the shortest path algorithm. The sensor nodes which are on the shortest path or close to the shortest path are selected as new candidate forwarders.

A real-time opportunistic routing protocol, (ORTR) was proposed by [56]. The new concept of power regulation to follow the delay controls. ORTR was based on the duty cycles, however, if a low duty cycle has been applied than there may be no nodes in the forwarder area because

neighboring nodes cannot hear the broadcasting. Saving energy is a very crucial task in WSN and most of the energy has been consumed in communication between nodes.

In [14] author have proposed an OR algorithm, EFFORT, which is based on the network lifetime maximization. The authors have found that unreliable links are the main consumer of energy of the network. Hence, this paper utilizes the properties of OR to build a new distributed OR algorithm. Continuing research in this area, [61] proposed a novel communication protocol known as energy-aware opportunistic routing (EAOR). As claimed by the authors, EAOR maintains a balance between QoS and energy efficiency in the network. The primary objective of designing EAOR was to increase network lifetime and reducing the packet delay.

[15] proposed an energy efficient opportunistic routing protocol (EEOR) which addressed the forwarder selection and prioritization issues. The author's worked on reducing the energy consumption during the selection of forwarder nodes. Two power models have been considered in this chapter which were the adjustable and non-adjustable power models. Authors have implemented these two models and proposed opportunistic routing algorithms for optimal forwarder set selection. Proposed work was tested and simulated on TOSSIM and TinyOS.

[16] presented an OR protocol named as energy-efficiency opportunistic multicast routing protocol (EOMR) which is based on grid formation inside the network. Nodes will decide their location on the basis of these grids. The authors have also proposed routing metrics through which the nodes will decide the forwarder list. The nodes needed to know only the topology of their own grid rather than the whole network.

In paper [17] authors have worked on the QoS factors and proposed a QoS calculation function which is incorporated with opportunistic routing for WSN. The aim of the authors was to propose an opportunistic routing protocol which incorporates QoS factors in the routing process. The method was to define a multi-metric QoS aware forwarder set selection approach. The performance of the protocol was good as compared to ExOR and EEOR by the authors.

4.3 Proposed OR Protocol

OR protocols discussed in related work considers energy efficiency as the main parameter in routing process and also all of these are based on opportunistic routing. This chapter also tries to introduce a new energy efficient opportunistic routing protocol for WSN. Before discussing the proposed protocol models and assumptions are presented as in the following subsection.

4.3.1 Models and Assumptions

This section gives an overview of the models and assumptions considered during simulation of the proposed approach.

Network Model

A wireless sensor network of N nodes deployed randomly over an area of size $M \times M$ is considered. The network can be seen as a communication graph $G = (V, L)$, with following possessions:

- $V = \{V_1, V_2, \dots, V_n\}$, $|V|=N$, set of all sensor nodes in the network.
- L is the set of all direct links between nodes. $(i, j) \in L$ if and only if V_i can directly transfer data to V_j (V_j is in the Communication range of V_i).
- $NBT(V_i)$ is a neighboring list of a node V_i . V_j will be in the neighboring list of V_i if and only if there is a direct communication link between V_i and V_j .
- All the traffic of data packets has been assumed to travel toward base station only.
- ACK is considered to be back on the same path on which the data has been sent already.

Energy Cost Model

The energy model of a sensor node depends on its radio, i.e. the maximum energy consumption is considered to be in transmitting and receiving data packets. The energy consumption equations are as given in [88].

Transmission Energy (transmitting k -bit packet)

$$E_{tx}(k,d) = k \cdot E_{radio} + k \cdot E_{amp} \cdot d^2 \dots \dots \dots (1)$$

Receiving Energy (receiving k -bit packet)

$$E_{rx}(k) = k \cdot E_{radio} \dots \dots \dots (2)$$

Acknowledgment sending and receiving energy

$$E_{ACK}(n,l) = E_{T_elec}(n,l) + E_{R_elec}(n) \\ = \begin{cases} 2n \cdot E_{elect} + n \cdot E_{amp} \cdot l^2, & \text{if } l < l_0 \\ 2n \cdot E_{elect} + n \cdot E_{amp} \cdot l^4, & \text{if } l \geq l_0 \end{cases} \dots \dots \dots (3)$$

4.3.2 Proposed OR Protocol

This section will briefly discuss the proposed OR protocol. The protocol has been completed in many phases. Proposed protocol phases will be discussed below. The proposed protocol will complete its functioning after all the phases have been completed.

Start Phase

This phase is the initializing phase of proposed OR protocol. This phase begins immediately after the deployment of sensor nodes in the field. Also, this phase will be repeated periodically. The nodes contact each other via sending hello messages. Hello, messages contain the information about the node which has generated these. These messages are used to form a neighbor list as well as for calculating the packet reception ratio (*PRR*) of each link. The sensor nodes which response to hello packets has been added to the neighbor list of corresponding hello packet node. The structure of the neighbor list has been given in figure 4.1. The receiver of hello packet add its own identification and location to the reply and broadcast it. If source node gets reply packet, it will add the replying node to its neighbor list with increasing *REP_Count* (Number of replies, initially 0) value. This process has been repeated five times in our protocol. In this way, the neighbor list of each node in the network has been formed. Collisions will be managed by the MAC layer of the network.

Node_ID	Location	REP_Count	Energy
---------	----------	-----------	--------

Figure 4.1: Neighbor Table Elements

Forwarding Set Selection

After completion of start phase a neighbor table has been formed. From the neighbor table, the eligible forwarder candidate nodes have to be selected. To construct a forwarder set *PRR* has been calculated using following equation:

$$PRR_i = \frac{REP_Count_i}{PG_{source}} \dots\dots\dots (4)$$

where *REP_Count_i* is the reply count for a neighbor *i* and *PG_{source}* is the total number of hello packets generated at the source node. Each node which is having *PRR* greater than the threshold (0.2) has been added to forwarder list of the node *i*. This process is repeated for each new data transmission process. The forwarder list elements can be seen in Figure 4.2. The forwarder list has been sorted and a priority has been assigned to each forwarder.

Node_ID	Location	PDR	Priority
---------	----------	-----	----------

Figure 4.2: Forwarder Set Elements

```

Algorithm 1
Forwarder_Set_Selection (S=Source, D=Destination)
//When any node S want to send a packet towards D, it will follow this algorithm
Begin
Let NTB (S) be the neighbor list of node S
Let REP_Count (node) :=0
For count:= 1 to 5 repeat
    Broadcast "Hello_Packet" as {SID, Coordinates (x, y), REs} from S;
    IF (reply == True and node !∈ NTB(S))
        Add the replying node to the neighbor list NBT(S) with following values updated
            {Node_ID, Location, Energy};
    Else IF (reply == True and node ∈ NTB(S))
        REP_Count (node):= REP_Count (node) + 1;
    Else
        count := count + 1;
    endIF
    count := count + 1;
endFor

For each node in NTB (S) repeat
    Calculate PRR (node);
    IF PRR (node) >= 0.2
        Add node to forwarder set (FL(S));
    endIF
endFor
Forwarder Set FL(S) is formed;
end

```

Forwarding Node Selection

After getting the forwarder set the network setup has been completed. Now the forwarder node has been selected on the go. When a node has data to send than it first prepares the packet and broadcast it with the forwarder set. The node which has received the packet first will check whether it is on forwarder list or not. If it is not on forwarder list it simply discards the packet. But in case it is on the forwarder list it first calculates the value of Energy Depletion Factor (EDF). EDF has been proposed in [88]. EDF is used to find out the node which is having the best performance in terms of energy. EDF calculates the impact on the energy of a node during each reception and transmission. EDF of a node can be calculated as follows.

$$EDF_{Ni} = \frac{E_{tx:Ni \rightarrow fwd} + E_{rx:Ni} + E_{re_tx:Ni \rightarrow fwd} + E_{ACK:Ni \rightarrow source}}{RE_{Ni}} \dots\dots\dots (6)$$

The description of each term is given in table 4.1 and the calculation are as given in equation 7 below.

$$E_{tx:Ni \rightarrow fwd} = \frac{E_{Trans}}{RE_{Ni}}; E_{rx:Ni} = \frac{E_{Receive}}{RE_{Ni}}; E_{re_tx:Ni \rightarrow fwd} = \frac{E_{Forward}}{RE_{Ni}}; E_{ACK:Ni \rightarrow source} = \frac{E_{Trans} + E_{Reieve}}{RE_{Ni}} \dots (7)$$

Table 4.1: Energy Consumption Parameters description

Parameter	Description
EDF_{Ni}	Energy Depletion Factor for node Ni
$E_{tx:Ni \rightarrow fwd}$	Transmission energy consumption for node Ni
$E_{rx:Ni}$	Receiving energy consumption for node Ni
$E_{re_tx:Ni \rightarrow fwd}$	Retransmission energy consumption for node Ni
$E_{ACK:Ni \rightarrow source}$	Energy consumed by node Ni in transmitting and receiving
RE_{Ni}	Residual energy of node Ni
E_{Trans}	Transmission energy cost of radio board of a sensor
$E_{Receive}$	Reception energy cost of radio board of a sensor
$E_{Forward}$	Combined energy cost of radio board of a sensor for transmission

After calculation of EDF, if it is less than the threshold value (EDF_{th}) a timer has been set in the node with respect to the value of EDF. The node will wait until it receives an acknowledgment for corresponding packet or the timer expires. Here, the timer for lowest EDF will be lowest and automatically the lowest EDF node become the first to send the data packet.

Algorithm 2

Forwarder_Node_Selection (S=Source, D=Destination)

//When any node S want to send a packet towards D and it has already constructed a forwarder list, it will follow this algorithm

Begin

For each node, $i \in FL(S)$ repeat

 Calculate $EDF(i)$

 IF $EDF(i) \geq EDF_{th}(node)$

 Set Timer (i):= value of EDF

 Else

 Remove node i from $FL(S)$

 endIF

endFor

IF Timer (i): = NULL

 Broadcast data packet as $\{i, D, Coordinates(i), Data\}$ from i

Else

 Wait for the timer to be Null

endIF

end

Acknowledgment and Recovery

Proposed protocol use the selective acknowledgments. When a node has received a packet, it sets a timer for receiving the packet and a value of counter sets to 1. The counter value is incremented each time the packet has been received. If counter equals to 5 or the timer expire before receiving another packet the acknowledgment has been prepared and sent. The acknowledgment contains the first packet sequence number (start_sqn), fifth packet sequence

number (end_sqn) and missing packet sequence numbers (miss_sqn). The receiver of acknowledgment extracts the start_sqn, end_sqn and miss_sqn from it. Then it checks if start_sqn belongs to the queue of packets inside it. If so, it will simply erase the packet from memory and check for miss_sqn. If miss_sqn found in the queue then the packet matching miss_sqn will be retransmitted. If there is no miss_sqn found inside receiver then the acknowledgment will be forwarded towards source node.

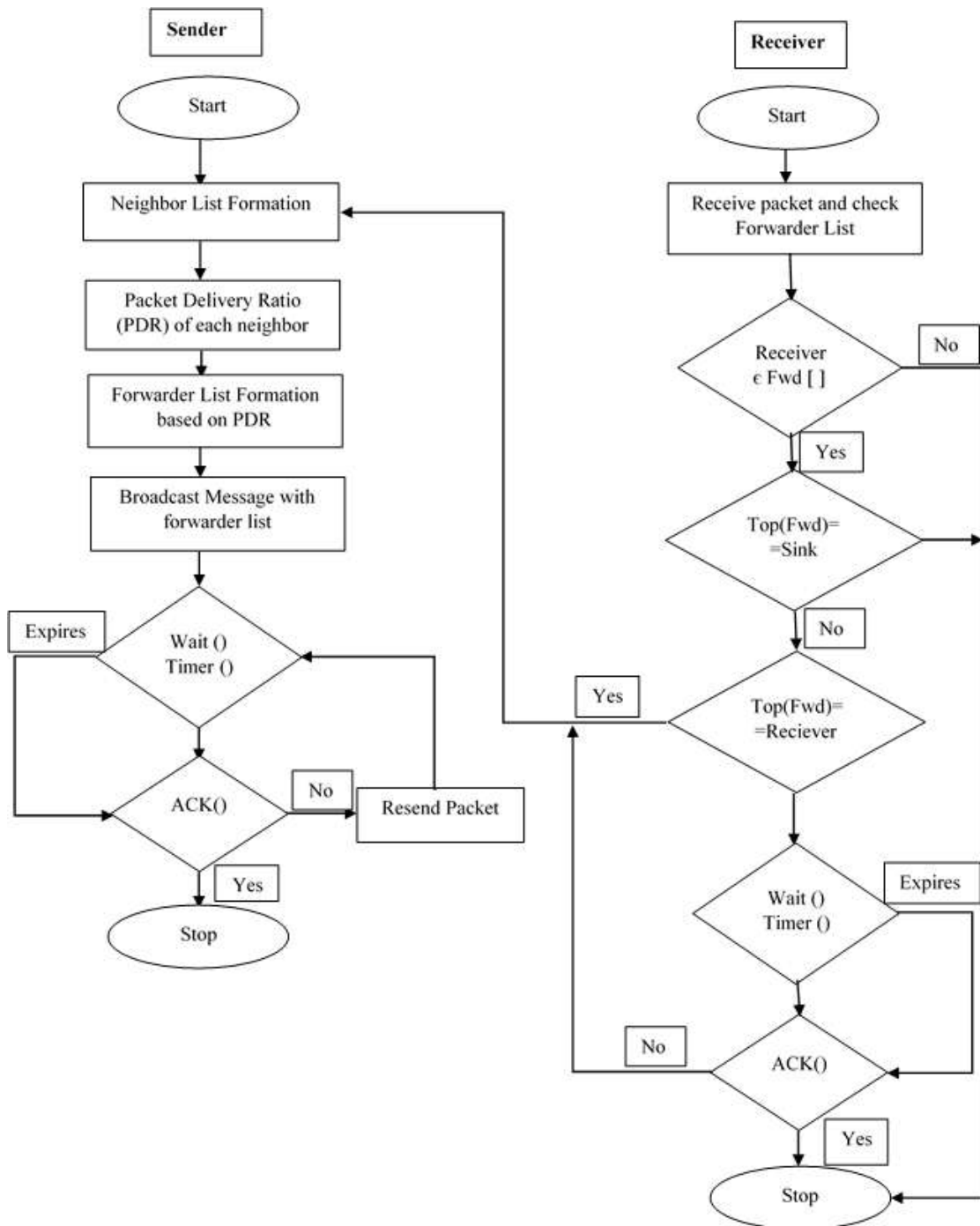


Figure 4.3: Flowchart of Proposed OR Protocol

Flow Graph of Proposed Protocol

Figure 4.3 shows the flowchart of the proposed protocol. The flowchart depicts all the phases of the proposed protocol. This is the combined flowchart for the proposed protocol and it shows both sending and receiving processes discussed in above subsections.

4.4. Experimental Results and Performance Analysis

For the purpose of testing of proposed protocol simulation technique has been used. The simulator used for testing is network simulator (NS2). The simulation scenario has been created by using wireless sensor network and sensor node properties. Table 4.2 below shows the simulation parameters used as settings in the NS2 environment. The working and results of the proposed algorithm are compared to existing energy aware opportunistic routing protocols EOMR [16], EEOR [15], EFFORT [14], and QEOR [17]. These all protocols are claimed to be energy efficient by the respective authors.

4.4.1 Simulation Scenario

All Compared protocols are simulated again using the network settings similar to the proposed protocol using NS2. After simulation, the results have been collected and plotted for better understanding.

Table 4.2: Simulation Settings

Parameter	Description
Examined Protocols	EFFORT [14], EEOR [15], EOMR [16], QEOR [17], Proposed Protocol
Simulator	NS-2.35
Area of Field	500 m x 500 m
Range of Radio	75 m
Number of Nodes	25, 50, 100
Size of Packet	46 bytes
Data Size	10 Kbytes for each transmission
Data Rate	250 kbps
Initial Energy	10.0 J
Electronic Energy (Eelec)	$50 * 10^{-9}$ J
Amplification Energy (Eamp)	$10 * 10^{-9}$ J

The sensor nodes are randomly deployed in $500 \times 500 \text{ m}^2$ area. After deployment, network initialization phase will be started and nodes start communicating with other nodes to construct the neighbor lists. The simulation records the average results for desired parameters discussed in results and discussion section.

4.4.2 Results and Analysis

Results are recorded and verified by performing extensive simulations for all analyzed protocols, including proposed protocol. The results collected are purely simulation based on all compared protocols implemented on the same platform i.e. NS2 and tested for same parameters. The results are presented in form of graphs.

The performance effect on WSN with varying number of nodes has been completed using simulations for all compared protocols. The variation in a number of nodes is from 10 to 200. Average results are plotted in form of graphs after completing numerous simulations.

Figure 4.4 presents the average packet delivery ratio for all compared protocols. As the proposed protocol focuses on energy efficiency mainly, the packet delivery ratio will remain almost same as QEOR, but outperforms EOMR, EEOR, and EFFORT. This is because the improved energy efficiency leads to long network lifetime and hence more packets will be transmitted towards the destination. The energy consumption is equally distributed over the network and hence this will increase the network lifetime. The node failure probability will be less if each node will participate equally in data transmission. This will increase the network lifetime and also the number of packets transmitted toward the destination. The selective acknowledgment scheme of the proposed protocol will make it easier for the nodes to identify which packet is lost and needs retransmission with less energy consumption.

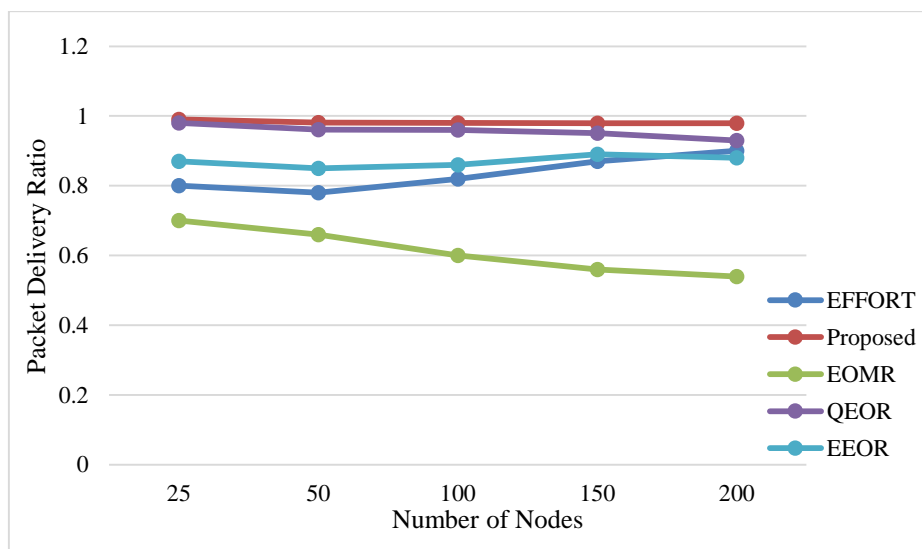


Figure 4.4: Comparison on the basis of Packet Delivery Ratio

The transmission delays are presented in form of average end-to-end delays introduced during the transmission and reception of data packets. The average end-to-end delays for proposed protocol, QEOR, EOMR, EEOR and EFFORT with respect to a number of nodes are presented

in figure 4.5. Balancing the energy consumption will reduce the node failure probability and hence reduces path failure probability also. The transmission delays will be reduced when there are fewer path failures during the routing process. The data retransmissions also reduced due to fewer node failures. The proposed protocol hence performs better than other protocols.

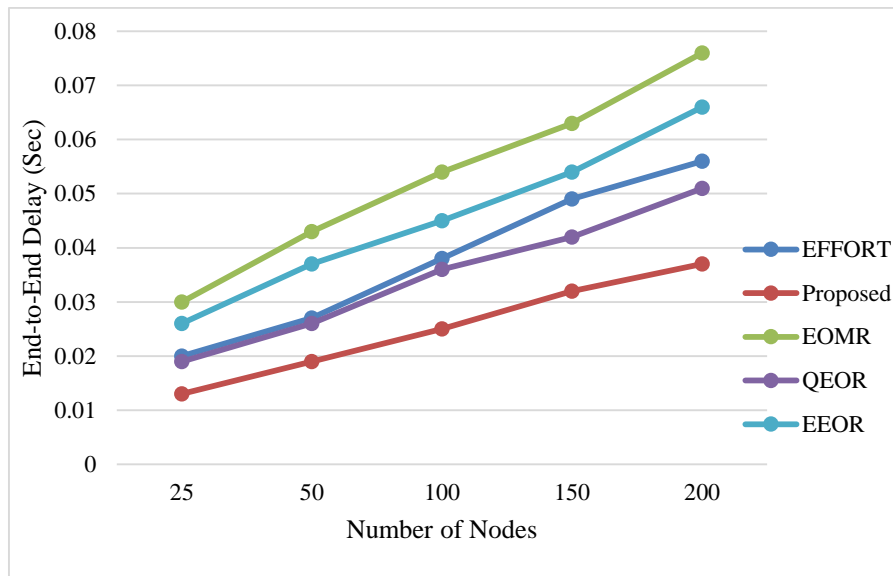


Figure 4.5: Comparison on the basis of End-to-End Delay

Energy consumption is the main criteria for measuring the performance of energy efficient protocols for WSN. Figure 4.6 shows the average energy consumed during each simulation in the whole network. As discussed previously the energy consumption is distributed among each node by using the EDF routing metric in proposed protocol.

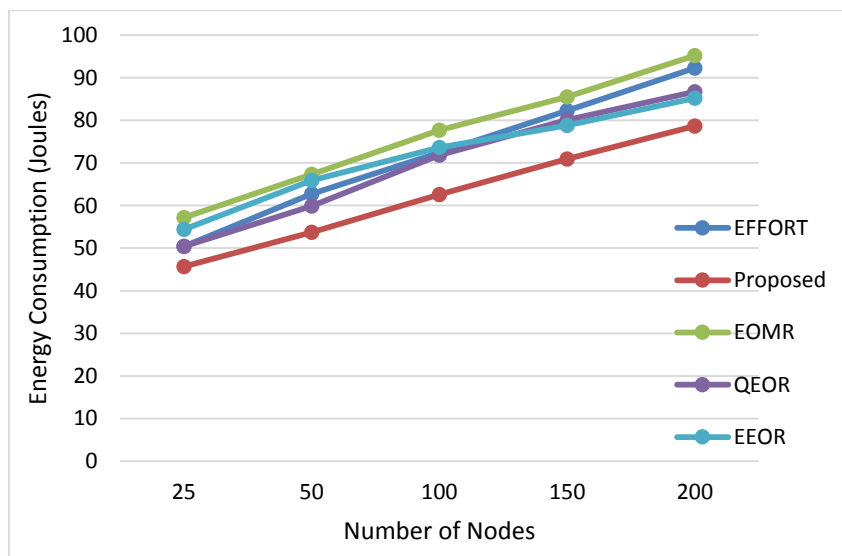


Figure 4.6: Comparison on the basis of Energy Consumption

Selection of relay node is the main task in the proposed protocol and EDF will make sure the highest energy node will be selected as a relay node. EDF will calculate the impact of all types of energy consumptions on the sensor node's residual energy. Other protocols like QEOR, EEOR, EOMR, and EFFORT do not consider this type of impacts on the residual energy. Therefore, the proposed protocol performs better than other protocols in terms of energy consumption as one can see from the figure 4.6.

Next analysis is the number of duplicate packets received at the base station. It can be seen from the figure 4.7 that the number of duplicate packets at the base station for the proposed protocol is lesser than other protocols. This because proposed protocol runs a coordination algorithm between all of the relay nodes to choose only one of them to transmit data packet further. In proposed protocol, forwarder node selection algorithm (Algorithm 2) will make sure that only one node will forward the packet towards the destination. Rest of the nodes in the forwarder set will wait for acknowledgment that the packet is received by destination or not. As selective acknowledgments have been used, control packets are not required in the network.

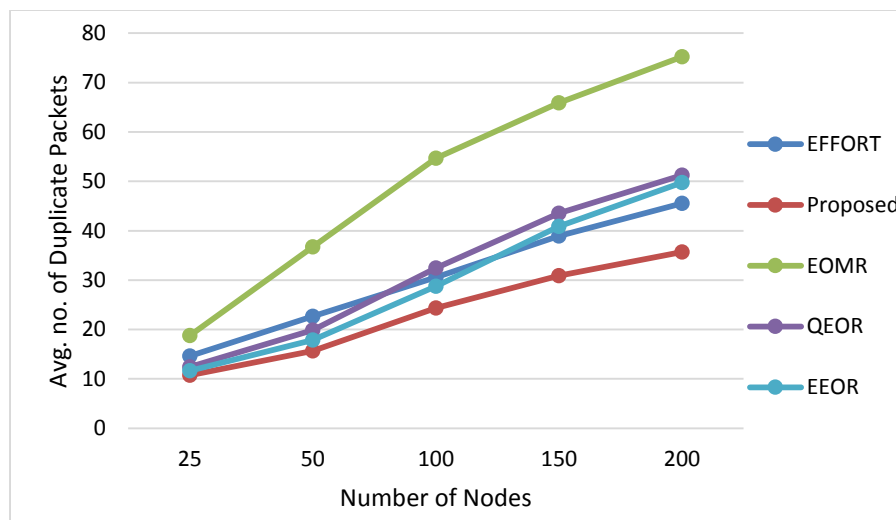


Figure 4.7: Comparison on the basis of Duplicate Packets

The network lifetime for proposed protocol increases considerably because of the improved energy efficiency. As discussed all above factors will influence the network lifetime. But, most important is the energy consumption across all nodes in the network. As energy efficiency for the proposed protocol is improved, this will increase the lifetime of the network. Even after the first node failure in the network, the packet will reach the destination node without any interruption. Nodes which are having enough energy to transmit the data packet will be selected as new forwarders using proposed routing metric (EDF). Also, the packet overhead is reduced

and hence there will be less energy consumption during packet and acknowledgment transmissions and receptions.

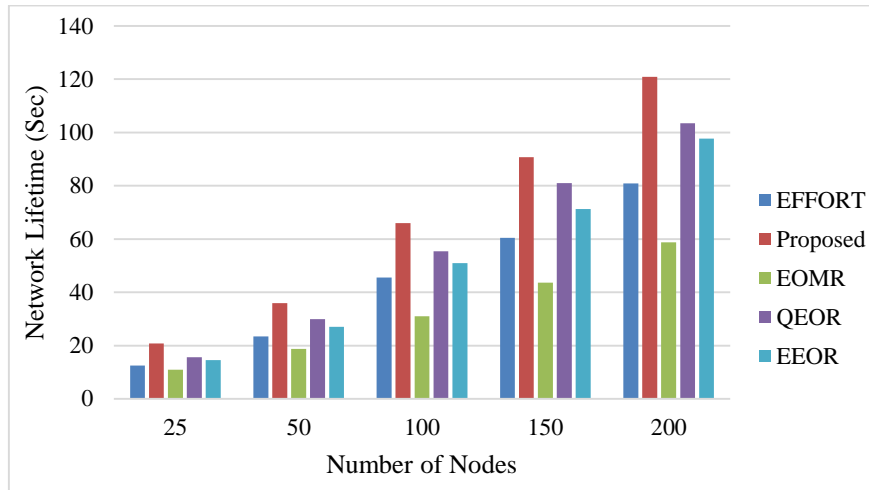


Figure 4.8: Average Network Lifetime based Comparison

Overall, by analyzing these all performance parameters, the proposed protocol shows improvement over the existing protocols. Proposed protocol balances the energy consumption in the network among all nodes and tries to keep each node alive for a long time. This will improve the network lifetime and throughput of the network.

4.5 Conclusion and Future Scope of Work

This chapter presented a new energy efficient opportunistic routing protocol. This protocol tries to balance the energy consumptions in transmission and reception of data packets among all nodes of the network. A new routing metric called as energy depletion factor (EDF) has been used to calculate the impact of each communication on sensor nodes. There are three main processes in proposed protocol calculation of routing metric EDF, forwarder set selection algorithm and forwarder node selection algorithm. Forwarder set selection algorithm distributes the energy consumption among all nodes in the network. While forwarder node selection algorithm selects one high priority node out of forwarder set. Forwarder node selection algorithm can be seen as coordination method, among all nodes, for proposed protocol. As the energy efficiency in the network improves, the other performance factors are influenced and improved. Proposed protocol reduces the end-to-end delay, average energy consumption and packet overhead. This will ultimately lead to improvement in network lifetime and throughput of the network. Simulation results depicted all of these performance metrics compared to existing protocols i.e. EEOR, EOMR, QEOR, and EFFORT.

CHAPTER 5

TRUST AWARE OPPORTUNISTIC ROUTING METRIC

5.1 Introduction

Most of the applications of WSN necessitate sensor nodes to be installed in the unattended hostile environment. Some applications are critical like defense, and healthcare etc. These applications require reliable and timely data delivery. Whenever the nodes are deployed it is assumed that the nodes are cooperative in nature. But as the environment is hostile in nature the nodes may be compromised or malicious nodes may be deployed by some attackers to disrupt the functioning of WSN. There will be a lot of possibility of internal and external attacks [1] [2]. Hence, there will be a requirement of securing data and routing process from these attacks.

Always when it is concerned about security, cryptosystems come into the picture. But as far WSN is concerned these systems are not very efficient and reliable [87]. Because, as the sensor nodes are having limited capabilities and inadequate resources it is almost impossible to employ cryptosystems for securing WSN. For providing the security in WSN the sensor nodes must be cooperative in nature with each other. But 100% coordination among all nodes is not possible. This is because the sensor nodes may be captured and misconfigured by some intruders. The intruders may put wrong information inside the network like false routing information, energy information or modified data packets etc. Attackers may destroy the network by compromising the sensor nodes inside the network.

Although, the researchers around the world tried to find out some security solutions and developed cryptographic methods [64-68] which will detect and avoid attacks inside the network. These algorithms commonly work for attacks imposed from outside the network. Suppose to conduct an inside attack the attackers have captured any of the nodes from the network. It will be impossible then to recognize these types of attacks using cryptosystems. Also, the cryptosystems will consume a lot of energy and it will take too much time for calculations. As already been said that energy efficiency is an important performance parameter and delay is also a critical performance factor, cryptosystems may not be used. Instead of using cryptosystems for the security purpose if sensor nodes could avoid selecting malicious or non-cooperative nodes as relay nodes than the energy consumption and delay will be less. For doing

this trust management systems may be used. Trust management systems may build up coordination among nodes and avoid malicious nodes in the routing process. The sensor nodes which are devising lower trust factors will not be selected for transmission or reception of data packets.

In the earlier chapters, it has been discussed that the WSN are opportunistic networks which must utilize the broadcasting abilities. The broadcasting nature of wireless links will result in great threats to data packets and the routing process. The main purpose over here is to secure the route selection process with low energy consumption. There are very less or no OR protocols which provide security to route selection process. In OR protocols security may be enhanced by utilizing trust-based relay selection in the network. For improving the possibility of a data packet to arrive at the base station with less energy consumption trust and reputation-based path fidelity info may be utilized.

OR works in two major stages, one is forwarder list formation and second is the relay node selection out of forwarder list. Whenever the source node has data to be sent to the base station it will first construct the forwarder list out of the neighbor list. Forwarder list will contain only the potential forwarder nodes that may be selected as relay nodes. Out of forwarder list relay nodes will be selected and a priority will be assigned on the basis of certain routing metric. Routing metric will be a criterion which a node should fulfill to get selected as a relay node. The routing choice in OR is chastely reliant on routing metric elected for picking relays in the network.

This chapter will present a new energy consumption and trust-aware OR metric which can work with any routing algorithm for WSN. The metric may be used with existing OR protocols for WSN to prolong network lifetime and increase the security of the routing process. The major contributions of this chapter are the newly proposed trust-aware metric and comparative analysis of the proposed metric by employing it to commonly used AODV [10] routing protocol.

5.2 Motivation and Related Work

Opportunistic routing improves the reliability and availability of data in real time. The researchers mostly concentrate on the forwarder set and relay node selection out of forwarder set. ExOR (Exclusive OR) [4] was the first and famous protocol proposed for wireless networks. The authors have proved that this new concept of routing can provide efficiency and improved throughput over other routing techniques. For a selection of relay nodes, the authors

have adopted expected transmission count (ETX) [6]. The OR protocols present in the literature [83] [84] mainly focus on efficient and real-time data delivery. But, the reliability and energy efficiency may be achieved only when security will be considered as an important aspect. In literature, a few of OR protocols are present which are employing security during the routing process.

In wireless networks providing security during routing process is a critical task, because wireless channels are open, and the data packets are broadcasted most of the time [89]. Cryptosystems may be used to provide security to the wireless networks, but these systems can avoid outsider attacks very well rather than the internal attacks. In WSN there is a great possibility of insider nodes to be compromised and impose threats to routing process and data packets. Hence, to improve the security against the insider attacks the routing process must ensure that the nodes which are compromised could not get selected as relay nodes. Also, there is a need of such security methods for WSN that are energy efficient and reliable. Hence, the instead of cryptosystems, the trust management systems may be used in which the nodes will run a coordination algorithm and selects relays on the basis of the value of a trust metric. This trust metric avoids the malicious or selfish nodes during the route selection process. The trust values are easy to compute and will ensure security and trust awareness among nodes within the network.

Trust-based routing protocols have been focused and developed by the researchers around the world for ad-hoc networks, internet of things and other mobile and static networks. CONFIDANT [5], CORE [91] and SORI [90] etc. are the commonly referred routing protocols for wireless networks. In [92] authors have presented a trust and reputation aware protocol for routing data packets in wireless networks. The authors have developed relay selection metrics and named them as RTOR, TORDP, and GEOTOR that may be used with OR protocols directly. These metrics do not employ for WSN because of the lack of energy efficiency. For WSN there is a limited number of trust-aware protocols proposed till date.

In previous three years, trust and reputation centered methods have been engrossed by researchers. Due to limited capabilities of sensor nodes, the researchers around the world try to maintain balance among resource utilization and security. Trust management is effective in WSN because of less energy consumption and coordination among nodes. Trust-aware routing framework (TARF) was proposed in [93], which is a dynamic trust-aware routing configuration. The common cryptosystem has been used as the corresponding function and secures WSN from various threats. TARF was not energy efficient and hence the lifetime of

the network was reduced. EMPIRE [94] is another probabilistic and distributed observing approach. EMPIRE improve the security of the network and reduce energy consumption. Continuing the research in this area ETARP [95] construct routes by utilizing maximum resources will lower transmission cost. The metric calculation overhead was high and hence ETARP consumes more energy in dense networks. In [96] authors tried to reduce the energy consumption and extra calculation overhead during routing process for WSN. They have proposed trust-aware routing protocol called as TESRP. TLAR [18] is the latest trust-aware protocol proposed for WSN. The consolidated trust values (CTV) have been calculated for each node in the network and the relay selection will be dependent upon these CTVs. The importance factors for various trust parameters were dynamically adjusted in CTVs. End-to-end delays are high due to calculation overhead in this protocol.

This chapter gives a trust-aware and energy efficient OR metric. This metric is a composite value of important parameters affecting the performance of networks like energy, data transmission and reception etc. The proposed metric has been applied to AODV for relay node selection and compared with AODV [10] and DSDV [12].

5.3 Proposed Trust-Aware OR Metric

Most of the protocols proposed for WSN have not considered the security as a primary concern as discussed in related work. In this chapter energy efficiency and trust management are combined to form a composite routing metric. Energy consumption calculations for receiving and transmitting packets will be similar to [88]. The broadcasting nature of wireless radios consumes a lot of energy in transmitting data packets. Opportunistic routing reduces this energy consumption by selecting only the best nodes as relays.

The working of an OR protocol always depends on relay selection metric. If the relay selection metric can avoid the mischievous or selfish nodes to get selected as a next-hop relay than the trust management may be achieved. This chapter gives an energy efficient and trust based opportunistic routing metric which is of distributive type. The data required by the metric are the ID of a node, residual energy and packet reception ratio (PRR). Each node will collect these values from neighbor nodes and calculates the packet forwarding ratio, acknowledgment sending and receiving ratio and residual energy based on energy consumption of a node. All of these parameters are then combined to form a composite routing metric. The in-between distance (D) of two sensor nodes is used to justify the progress of data packets (PFP) (eq 1 and eq 2). PFP specifies that the packet is making a positive progress towards the destination.

$$Dist_{i,j} = \sqrt{(x_{co_i} - x_{co_j})^2 + (y_{co_i} - y_{co_j})^2} \quad \text{where } 0 \leq i, j \leq k, \text{ and } i \neq j \quad (1)$$

$$PFP_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d} \quad \text{where } s=\text{source}, d=\text{destination}, 0 \leq n_i \leq k \quad (2)$$

The route selection in OR protocols for WSN is dynamic and the relay nodes are selected at transmission time only. The routing metric prioritizes the relay nodes and highest priority node will transmit the data first toward the destination. Here the trust value is calculated for all neighbor nodes that may be selected as relay nodes. The metric calculation will be completed in two phases discussed below.

5.3.1 Phase 1: Identification of Elements

This is a data collection phase and packet reception ratio (PRR) is calculated for selecting only potential nodes for data transmission (eq 3).

$$PRR_i = \frac{P_{recieved}}{P_{sent}} \quad \text{where } 0 \leq PRR_i \leq 1 \quad (3)$$

On the basis of PRR of a node i the potential forwarders are extracted from the neighbor list. The trust value for each node in the forwarder list has been calculated using following elements.

Sensor Node Identification (ID): This is the identity of a node which provides the values of location and remaining energy inside a node. The node which wants to transmit data packets towards the destination will collect this information from all neighbor nodes.

- $ID_i = \langle NodeID_i, Location_coordinates_i, Energy_i \rangle \quad \text{where } 0 \leq i \leq k$

Forwarding Sincerity (F): This parameter depends on the value of successful and unsuccessful packet forwarding by a node in the forwarder list. The success and failure counters are associated with each node in the network. This factor will help in identifying and avoiding the nodes, during routing process, which is dropping numerous of packets.

- F_i : Packet forwarding sincerity of node i
- FS_i : Packet forwarding success count of node i
- FF_i : Packet forwarding failure count of node i .

Energy Consumption (E_{total}): The energy consumed by a node to perform various network operations will be calculated by this element. The element's value will totally be dependent on the residual energy of respective node. The node's lifetime is dependent on the residual energy

and also the network lifetime depends on the number of nodes alive at a particular time. Hence, this factor will help in computing the lifetime of a node as well as the whole network.

- E_{total_i} : Total residual energy of node i

$$E_{total} = E_{total} - (E_{tx} + E_{rx} + E_{ack}) \quad (4)$$

Where, E_{tx} : energy spent in transmitting a data packet, E_{rx} : energy spent in receiving a data packet, E_{ack} : energy spent in transmitting and receiving acknowledgments in the network.

Acknowledgement Sincerity (ACK): This element monitors the acknowledgments in the network. The success and failure counters are associated with each node and will be inserted inside an acknowledgment at each relay node. Acknowledgment sincerity is useful in finding the retransmission probability of packets. This element will avoid those nodes which are suppressing the acknowledgments and impose retransmissions inside the network.

- ACK_i : Acknowledgement sincerity of node i
- $SACK_i$: Successful acknowledgment count of node i
- $FACK_i$: Unsuccessful acknowledgment count of node i .

Trust Value (T): This element will be computed, by combining the above discussed all elements, in phase 2 i.e. trust evaluation. The trust value will be calculated dynamically and updated time to time automatically by each node in the network.

This feature provides the overall trust value of a sensor and it will be estimated on the basis of all trust assessment aspects. This value is vigorous in nature since it requests to be updated over the time for each new communication of data packets.

- T_i : Trustworthiness of node i .

5.3.2 Phase 2: Trust Evaluation

In this phase, all the trust factors are evaluated. The values of trust factors are calculated and logged into the trust matrix. The values of trust factors for different nodes are discrete and cannot be converted directly to single logical value. Hence, in this phase the quantization of these trust factors is important. After quantization, the values are reduced to 0 to 1. Here, 0 means completely untrusted node and 1 means fully trusted node. The quantification of each element involved in trust calculation will be done by following equations.

Forwarding Sincerity (F_i)

$$F_i = \frac{FS_i - FF_i}{FS_i + FF_i}, \text{ subject to } 0 \leq F_i \leq 1 \quad (5)$$

Energy Depletion Value (E_{total_i})

$$E_{total_i} = \frac{E_{tx} + E_{rx} + E_{ack}}{E_{total}}, \text{ subject to } 0 \leq E_{total_i} \leq 1 \quad (6)$$

Acknowledgement Sincerity (ACK_i)

$$ACK_i = \frac{SACK_i - FACK_i}{SACK_i + FACK_i}, \text{ subject to } 0 \leq ACK_i \leq 1 \quad (7)$$

This will quantize the values of trust parameters. For each trust parameter, the weights are assigned according to their importance. The weight value for least important factors will be lower than that of important factors. The weights can also be application dependent as if the application requires reliable data delivery that the forwarding sincerity will be the most important factor and energy will be the least important factor. Keeping track of each trust factor individually for each node will be difficult. Hence, all factor are combined to form a composite routing metric (T_i).

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma}, \text{ where } 0 \leq \alpha, \beta, \gamma \leq 1 \quad (8)$$

Here, $\frac{\alpha}{\alpha + \beta + \gamma}$ is the coefficient of forwarding sincerity factor (F_i), $\frac{\beta}{\alpha + \beta + \gamma}$ is the coefficient for energy consumption (E_{total_i}) and $\frac{\gamma}{\alpha + \beta + \gamma}$ is for acknowledgment sincerity factor (ACK_i). The trust value will be from 0 to 1 which means that the nodes having value 0 are malicious and untrusted. While trust value 1 will indicate the fully trusted nodes without any malicious activity. The energy consumption has also been taken as an important factor and hence the node which is having low energy will not be selected as relay nodes. The nodes which are performing malicious activities like dropping data packets, queuing up data packets or reporting false energy information will be detected and excluded from the routing process.

5.4. Experimental Results and Performance Analysis

Security and energy efficiency will be the primary concern over here. Hence, proposed trust-aware opportunistic routing metric have to be tested for security and energy efficiency. To accomplish this task the metric should be applied to an existing protocol. Here, DSDV has been chosen to apply the proposed metric. The modified DSDV will select next hop relay nodes on the basis of the proposed trust-aware OR metric. The modified DSDV will be compared to original DSDV [29] and AODV [30]. All of the protocols are simulated in MATLAB and applied for routing the packets in wireless sensor networks.

5.4.1 Simulation Setup

Simulation in MATLAB assumes 500 m X 500 m area for deployment of sensor nodes. Successful communication of data packets is considered only when the base station receives data packet accurately. A number of simulations were conducted in with one base station only. Continuous data communication has been considered for random deployment of N sensor nodes in the network.

Table 5.1: Simulation Parameters

Parameter	Description
Examined Protocols	AODV [10], DSDV [12], Proposed
Simulator	MATLAB
Area	500 m x 500 m
Range of Radio	75 m
Number of Nodes	25, 50, 100 (5%,10%,15%,20% malicious/selfish nodes)
Size of Packet	46 bytes
Data Rate	250 kbps
Initial Energy	10.0 J
Electronic Energy	$50 * 10^{-9}$ J
α, β and γ	0.4, 0.3 and 0.2 respectively

One random source node will be selected to transmit data towards the base station using multi-hops. The sensor node will be considered dead is the energy is less than the electronic energy needed to transmit data towards the neighbor nodes. IEEE 802.15.4 [52] will be used as a standard for data link and physical layers. Table 5.1 above shows the different simulation settings for testing of proposed metric.

5.4.2 Experimental Results

The simulation area contains 25-100 nodes deployed randomly for collecting data. The proposed metric will be applied to the routing protocol for communicating data packets. The performance of the proposed metric has been recorded and plotted.

Safety Performance: AODV, DSDV and Modified DSDV (based on proposed metric) are simulated in MATLAB with similar parameters and simulation settings. The random deployment of nodes includes the malicious nodes also, which are 5 to 20% of total nodes deployed in the network. It is believed that as the number of malicious nodes is increasing in the network, the complexity of providing security and managing trust levels between nodes will be rising. The route setup process will be dependent upon the routing metric used for next-hop relay selection in the network. If one route is failing, then the source node has to re-setup the route and then retransmit the data packets. In the proposed metric the route selection involves the trust factors i.e. forwarding sincerity, acknowledgment sincerity and residual energy of relay nodes. Hence, the proposed metric helps in avoiding malicious nodes in the route selection process. This will reduce the risk level i.e. a number of mischievous nodes met through the transmitting process. The AODV and DSDV work normally without any security or trust metric and will have the high probability of selecting malicious nodes as next-hop forwarders. When a malicious node drops down the packet, it needs to be retransmitted and also the route setup process will also need a revision. Through the trust-aware routing metric, the malicious nodes may be detected and avoided during the routing process. Figure 5.1 below conclude that the proposed protocol employ security during routing process and can avoid malicious nodes easily as compared to normal AODV and DSDV.

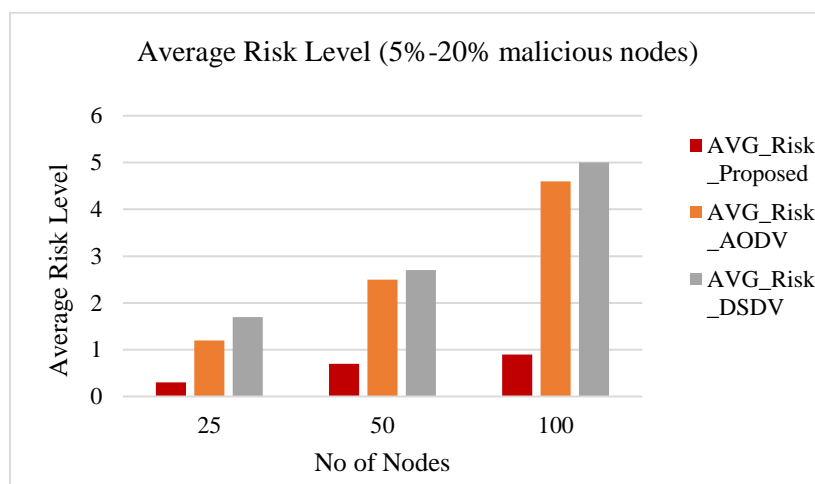


Figure 5.1: Average Risk Level

Energy Efficiency Performance: First order energy model [88] has been considered for measuring the performance of all of the compared protocols. The remaining energy for each node will be computed and included in the trust value calculation. Again, the performance has been tested in the presence of malicious nodes from 5 to 20% nodes of the total nodes. Figure 5.2 shows the performance in terms of energy. The figure will also depict the effect of a number of malicious nodes on the average energy consumed during routing a data packet toward the base station. The proposed metric considered the residual energy of each neighbor node and hence, it shows low energy consumption in successful transmission of one data packet towards the base station. The lifetime of wireless sensor networks depends on the lifetime of sensor nodes and hence it is necessary to select only those nodes which will impose less energy consumption during network operations. Figure 5.2 depicts that an increase in a number of malicious nodes will also increase the energy consumption inside the network. This will reduce the network lifetime, but if the number of nodes is large in the network than the network lifetime will be increasing (figure 5.3).

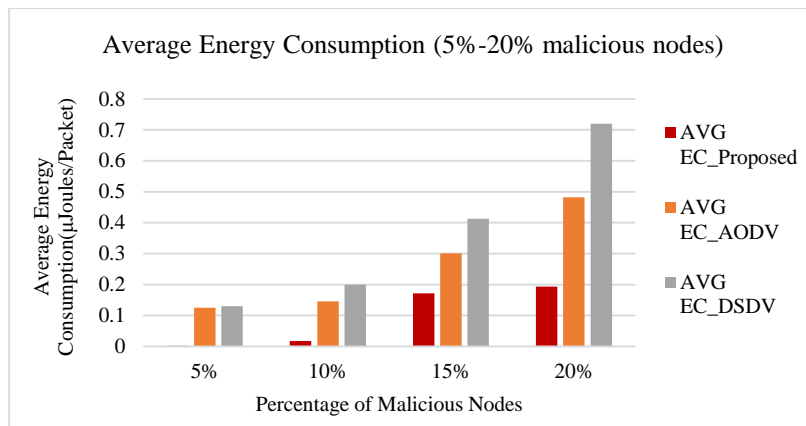


Figure 5.2: Average Energy Consumption

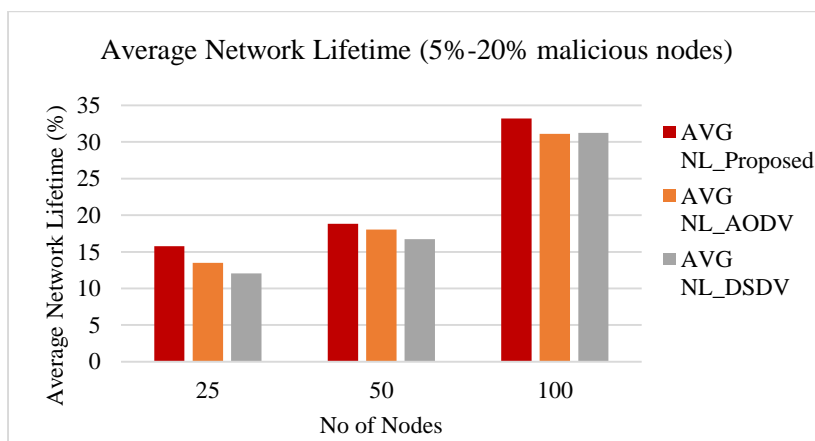


Figure 5.3: Average Network Lifetime

End-to-end delay (figure 5.4) will be increasing for the proposed protocol because of the calculation of routing metric and finding the best possible relay node according to trust value. While, in AODV and DSDV the routing process is simple, and these protocols simply opt for reconstruction of route upon route failure. This is why the delay is a little bit less for these protocols as compared to proposed protocol. In figure 5.5 the performance in terms of path loss in the presence of malicious nodes may be predicted. The proposed protocol imposes less path loss because of broadcasting nature and selecting the most trusted node as the next-hop relay.

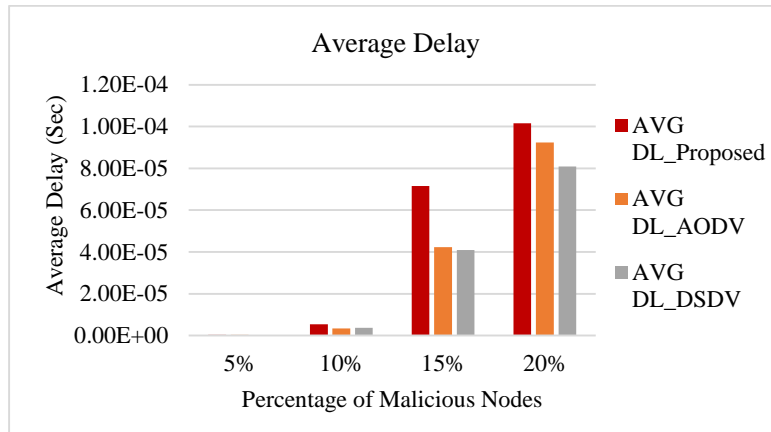


Figure 5.4: Average End-to-End Delay

From the different performance results for all three protocols, the conclusion is that there will be a requirement of trust-aware metric if the network is operating under the presence of malicious nodes. The performance of the proposed metric is good when it is used with DSDV as next-hop selection metric. The only problem is a high end-to-end delay and this will be improved with a new protocol is designed with the help of this metric for reducing end-to-end delay.

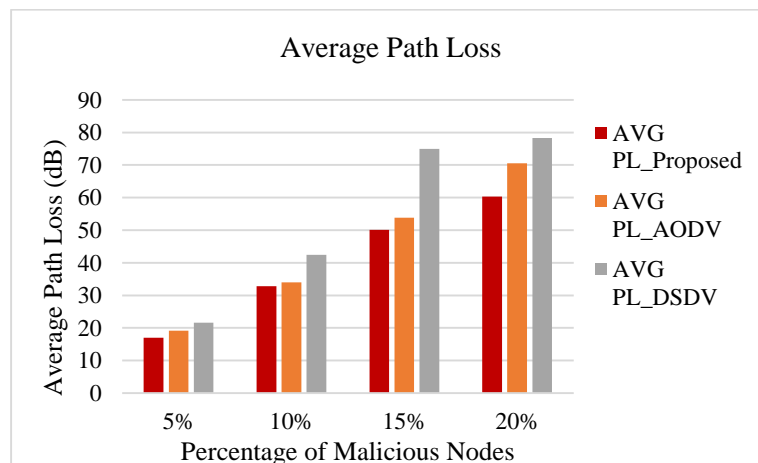


Figure 5.5: Average Path Loss

5.5 Conclusion and Future Scope of Work

A new protocol was proposed in this chapter which included three node trust factors. The metric is the composite metric which involves forwarding sincerity, acknowledgment sincerity and residual energy of each relay node to compete for packet transmission. The proposed metric has been applied to infamous DSDV routing protocol. The performance was compared to AODV and original DSDV when applied for relay node selection in wireless sensor networks. It may be concluded from the performance results that the proposed metric improves the security of route selection process by avoiding malicious nodes. As the impact of each transmission and retransmission is considered inside the trust value, nodes which are having good energy will always be selected as a next-hop relay node. Simulation results depicted the good performance in terms of energy efficiency and safety.

To improve the performance in terms of end-to-end delay there will be a need for new routing protocol which can cope up with delays in the network. The proposed metric only deals with a number of dropped packets and will not work efficiently in the presence of Sybil, wormhole, and node clone attacks. Hence, new parameters may be used in trust value calculation, which can improve the performance of the network in the presence of these attacks also.

CHAPTER 6

TRUST AWARE AND ENERGY EFFICIENT OPPORTUNISTIC ROUTING

6.1 Introduction

As WSN are increasing in demand due to advancements in micro-electromechanical systems. Due to the small size of sensor nodes, these can easily be deployed and also these small sensors can collect field data to transmit to the base station. But the sensor nodes are constrained in terms of resources like energy, storage and communication range etc. The routing protocols for WSN must optimize the use of these limited resources. Also, the sensor nodes may be left unattended in the desired area of application. Performance of WSN in terms of energy efficiency, delays, a lifetime of network and throughput mostly depends on communication and security methods.

Opportunistic routing (OR) is the recently proposed routing mechanism [97], which provide high throughput and introduce low end-to-end delays. OR mechanisms are having two major phases as discussed in previous chapters. In first phase, the source node selects best nodes to forward data among all of its neighbors and construct a forwarder node set. Out of the forwarder node set in the second phase, the forwarder nodes are prioritized and sorted. The node on the topmost of the forwarder set according to priority, will transmit the data packet first. To assign priorities to the nodes routing metric is used which may be a single metric or a composite metric.

Designing the opportunistic routing protocol requires an opportunistic communication metric. An OR metric selects the relay nodes dynamically and also give the opportunity to each neighbor node to become a relay node. But, to reduce the duplication of data packets the metric must ensure the coordination among all nodes in the forwarder set. As the routing metric is important, researchers have focused on these metrics [80] [88] [98] and develop new OR metrics for wireless and ad-hoc networks. These metrics may be classified into two major categories end-to-end selection metrics and local selection metrics. The link delivery probability will be considered from source to destination in end-to-end selection metrics. While in local selection metrics only the neighbor information has been collected and the next-hop will be decided on the basis of this information only. The local selection metrics impose fewer

delays in data transmission but increase the coordination overhead among nodes. In a real scenario, the nodes may be affected by some malicious attacks which will decrease the performance of the network. The malicious attacks need special security methods other than cryptosystems [64-68] due to the limited resources of sensor nodes.

Reputation and trust-aware systems are the special category security protocols that may be used in WSN to manage the coordination among all sensor nodes. These protocols are energy efficient and impose less overhead in routing decisions. Trust and reputation based routing techniques are the subcategories of security protocols. These systems use trust metrics and if a node is having unsatisfied value, it will be discarded from the forwarder list of the source node. This chapter proposes a new reputation-based OR metric and protocol. This metric considers energy efficiency and reputation of a node on the basis of packet forwarding ratio (PFR), to select next-hop candidate forwarders. The chapter proposes an extension to the previous work i.e. middle position dynamic energy OR algorithm. It is being extended to improve energy efficiency and provide reputation-based security to network and data.

6.2 Motivation and Related Work

Opportunistic routing with trust and reputation based security mechanisms was engrossed by numerous researchers during last five to six years. Trust and reputation aware routing protocols consume lesser resources as discussed in chapter 5. These systems consume lesser energy and are easy to compute as compared to cryptosystems. CONFIDANT [5], SORE [90], and CORE [91] are some of the trust and reputation based routing protocols proposed during last five years. In literature, there are limited trust and reputation aware opportunistic routing protocols are available. For example in [92], the authors have proposed a trust and reputation aware OR framework for wireless ad-hoc networks. The authors have proposed three opportunistic routing metrics based on the requirements of the network. In WSN also certain authors have applied trust and reputation aware routing protocols and acquired good results in terms of energy efficiency, throughput, and end-to-end delay.

For WSN the researchers strained to preserve the balance among the sensor properties and safety of the network. Trust-aware routing framework (TARF) was developed by [93] and it was based on cryptosystems. TARF secure the network using the cryptographic method and hence consume a lot of resources. To provide energy efficiency efficient monitoring procedure in reputation system (EMPIRE) was proposed in [94]. The reputation and routing models in EMPIRE were probabilistic and distributive in nature. To improve the energy efficiency this

protocol reduces the number of monitoring responsibilities for each node in the network. Another protocol proposed was energy efficient and trust-aware routing (ETARP) [95]. ETARP utilize the resources of each node carefully and reduce the routing cost in terms of energy and link bandwidth. Similar routing protocol was proposed in [19], named as trust and energy aware routing protocol (TESRP) which is intended to be energy efficient and reduced the communication overhead during the network operation.

Recently proposed protocol, trust and location-aware routing (TLAR) [18] utilize different parameters to proposed a consolidated routing metric. The main parameters considered in TLAR were sincerity in packet forwarding, acknowledgment sincerity, the integrity of packets, energy information by neighbors and indirect trust values i.e. feedbacks of other neighbor nodes. Using too many parameters will result in high end-to-end delays and also reduce the overall throughput of the network. Another efficient routing protocol for WSN is trust-aware opportunistic Routing (TAOR) [20]. This protocol was energy efficient and also reduces the end-to-end delays. Overall there are limited trust and reputation aware methods available for wireless sensor networks in the literature. This chapter will give two different trust and reputation aware routing protocols for WSN in the upcoming sections. First one is an extension of middle position dynamic energy OR (MDOR) protocol [13], which is efficient in terms of energy. But this protocol does not employ any security mechanism and will be inefficient in the presence of malicious nodes. Another protocol proposed in this chapter is energy efficient and trust-aware reliable opportunistic routing (TAEROR) protocol, which is based on direct trust values collected by the source nodes to avoid malicious nodes during the routing process.

6.3 Modified_MDOR

Middle position dynamic energy opportunistic routing (MDOR) [13] consider that each node has same capabilities but the transmission and reception energies of a radio may be different. Dynamic energy consumption considers different energy consumption for each packet. The protocol was based on two different energy efficient protocols EEOR [15] and MOOR [44]. EEOR considers the most energy efficient transmission through relay nodes towards the base station. Hence, this will always choose only those nodes which are nearest to the source node. On the other hand, MOOR selects the relay nodes on the basis of the distance between the relay and the destination node. Hence, MOOR will always choose those nodes which are nearest to the destination node and receives packets successfully. MDOR choose those nodes as relay nodes which are neither near to source node nor to the destination node. MDOR always choose the middle distance node between the source and the destination. But if malicious nodes are

taken into consideration than the middle node may be the malicious one. Hence, there will be a need for some security mechanism which can avoid these malicious nodes during the routing process.

The proposed protocol modified_MDOR considers trust value of each node to select the next-hop forwarder sensor node. This proposed protocol calculates the reputation of each neighbor node which are middle nodes considered in forwarder list. The trust value constitutes of energy efficiency and packet forwarding ratio (PFR) of each node. The nodes with lower trust values will be discarded from the forwarder lists and cannot participate in the routing process. The protocol works in two phases: forwarder selection metric calculation and the routing algorithm discussed in below subsections.

6.3.1 Forwarder Selection Metric

For the selection of relay nodes and making forwarder list, a relay selection metric is required for opportunistic routing. Modified_MDOR also use an opportunistic routing metric which will compute the trust cost for each sensor node. This metric has two fragments: packet forwarding ratio and energy impact. The first fragment i.e. packet forwarding ratio (*PFR*) calculated the forwarding ratio of each node by using a number of packets forwarded by each forwarder node and a number of packets sent to the same. *PFR* of a node *i* will be calculated by the following equation.

$$PFR_i = \frac{P_fwd_{i \rightarrow next_hop}}{P_sent_{source \rightarrow i}} \dots\dots\dots (1)$$

Where, $P_fwd_{i \rightarrow next_hop}$ is the number of packets relayed by the node *i* towards its next-hop node and $P_sent_{source \rightarrow i}$ is the number of packets sent by the source node towards node *i*.

Energy impact is the second part of the trust value which is based on the node's residual energy. This factor calculates the impact of energy consumption on the node's residual energy. It consists of energy consumed during various network operations like data transmission, reception, and energy consumed by sensor board.

$$E_effect = \frac{E_{recieving} + E_{transmitting} + E_{ack_sending}}{E_{total}} \dots\dots\dots (2)$$

The receiving ($E_{receiving}$), transmitting ($E_{transmitting}$) and acknowledgment ($E_{ack_sending}$) energy consumptions are calculated by using the first order energy model given in MDOR [24]. Total energy (E_{total}) is the residual energy of a sensor node. These two parts i.e. PFR and E_{total} are combined to form a composite metric i.e. trust metric (T_Value) calculated by the following equation.

$$T_Value = \frac{\alpha.PFR + \beta.E_effect}{\alpha + \beta} \dots\dots\dots (3)$$

Here, α and β are the important factors for both trust value parts i.e. PFR and E_effect respectively. After the trust value is computed for every fellow node, the source node will run the modified_MDOR algorithm to find out the next-hop relay nodes.

6.3.2 Algorithm

Opportunistic routing takes the advantages of multiple routes and hence impose higher throughputs than other traditional routing techniques. Sending data through multiple routes may increase the number of duplicate packets at the destination node. To reduce the numbers of duplicate packets, the routing algorithm must set a priority among all possible routes and the packet must be transmitted through higher priority route first. To define the priorities OR uses routing metrics which may be a single metric or a composite metric. MDOR prioritize among the possible next-hop forwarders on the basis of distance. It selects those nodes which are neither near to source nor far away from the destination. MDOR do not employ any security method to avoid malicious nodes during the routing process. This will delay the packets and also if the malicious nodes are dropping the packets then there will be a need of retransmissions. In modified_MDOR the trust values are included and only those nodes will be selected as next-hop forwarders which are having trust values above a certain threshold.

Modified_MDOR starts functioning when any source node is having data to be sent to the base station. The source node first sends “hello packets” to form the neighbor list. The nodes which are responding to the “hello packets” will be included to the neighbor list. Distance from source and base station to each neighbor node is calculated and then the neighbor list is sorted in ascending order.

The node at the middle position of the neighbor list will be given higher priority to send data first. But, first trust value will be calculated for this higher priority node. If the trust value (T_value) is below a certain threshold then the node will be discarded from the neighbor list and marked as a malicious node.

Algorithm: Modified_MDOR (S, D)

Input: Source node S, Target node D, Distance(S, D).

Output: Successful transmission of a data packet from node S to node D

1. Define S as Source Node
2. Create neighbor list NGH for S
3. Sort neighbor list according to distance
4. if D is neighbor of S
5. Send data packets to D
6. else
7. FNL is the subset of NGH (FNL is the forwarder node list)
8. Select the middle node (FWD) from FNL i.e. (neither near to S nor near to T).
9. Calculate trust value (T_Value) for each middle node using equation 3.
10. if $T_Value \geq 0.2$
11. Start communication with FWD
12. else
13. {
13. Discard FWD from FNL.
14. Select a second middle node from FNL and name it as FWD.
15. Repeat from step 9 to 14
16. }
17. if FWD is equal to D then stop the algorithm
18. else repeat step 2 to step 18 until D is reached

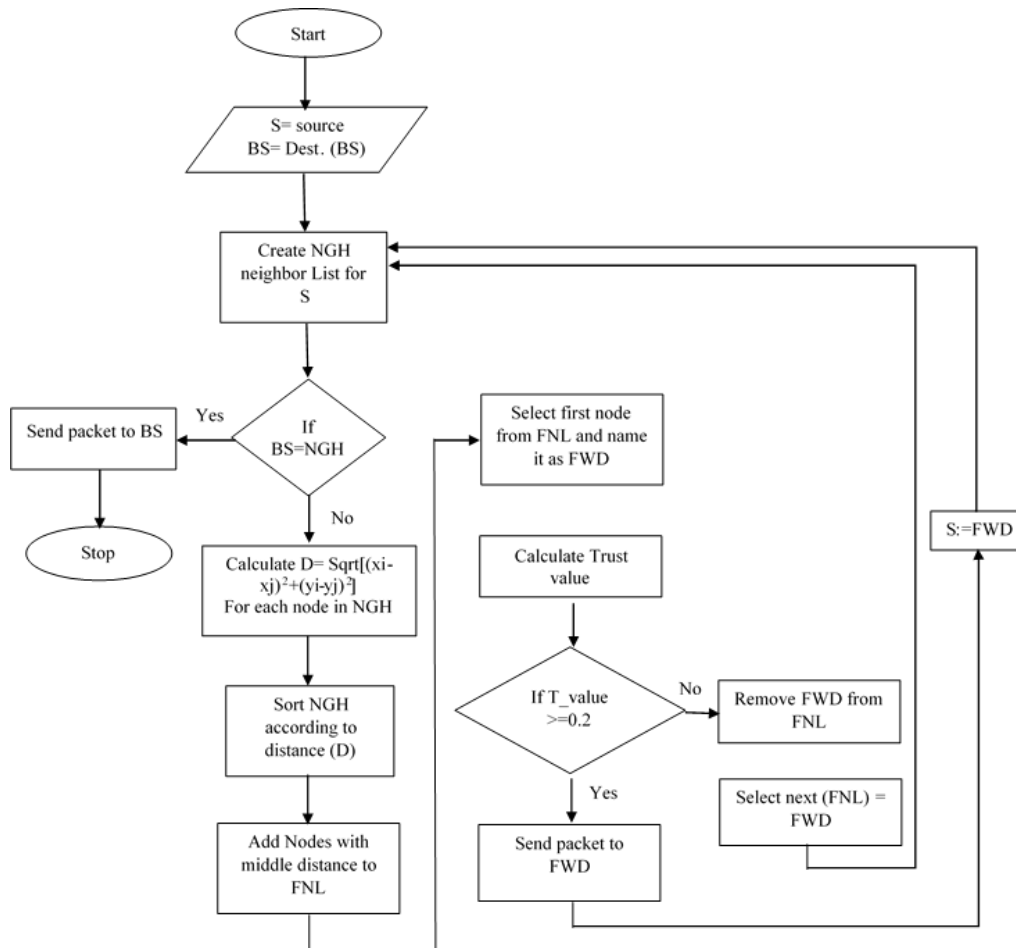


Figure 6.1: Reputation-Based Energy Efficient OR Protocol

The threshold value for modified_MDOR has been fixed to 0.2 after extensive simulations performed with different threshold values like 0.1, 0.2, 0.3,.....,1. The algorithm for modified_MDOR is as presented below. The working of modified_MDOR is almost same as MDOR except for the trust value calculation and deciding the next-hop relay nodes on the basis of trust values. The trust value involves the packet forwarding ratio i.e. the node's sincerity in forwarding data packets towards the base station. This will reduce the possibility of black-hole, worm-hole and grey-hole attacks. For providing the energy efficiency and reduce the false energy reports from the nodes the trust value involves energy impact on different nodes. The energy impact will avoid those nodes in the routing process which are having a lesser amount of energy. This will improve the network lifetime and hence increase throughput. The flowchart for the algorithm has been shown in figure 6.1.

6.3.3 Experimental Results and Performance Analysis

To test the performance of proposed protocol simulations have been performed. Results are compared to base protocol MDOR [13] and trust-aware recently proposed routing protocol i.e. TLAR [18]. TLAR, as discussed in the literature, is trust and location based communication mechanism which involve consolidated trust values to avoid mischievous sensors through the communication process. The simulation was performed by using NS2 which is a reliable tool for network simulations.

Simulation Parameters

The proposed modified_MDOR protocol, original MDOR, and TLAR are simulated in NS2.

Table 6.1: Parameters for Simulation

Parameter	Value
Simulator	NS-2.35
Examined Protocols	Proposed OR, TLAR [21], MDOR [20]
Deployment Area	500 m x 500 m
Communication Range	75 m
No. of Nodes (N)	100
No. of Mischievous nodes	10, 20, 30, 40 and 50
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	50J
Initial Trust Value	1
Energy consumed to run the radio ($E_{\text{electronic}}$)	50 nJ/bit
Buffer Length	20 packets

The similar settings were used to perform the simulations for all the protocols. The simulation situations are revealed in table 6.1. To present a good analysis of results number of malicious nodes are deployed in between the network. The node deployment is random for all nodes including malicious nodes. The malicious nodes may be identified by their different behavior. The malicious activities include dropping all or selected packets to impose black and grey hole attacks. The malicious nodes also do not forward or generate network acknowledgments.

Results and Discussions

The performance of modified_MDOR, MDOR and TLAR are recorded and plotted in form of graphs. The first performance parameter is the packet delivery ratio which is measured as the ratio of a number of packets delivered to the base station to a number of packets generated at the source node. Modified_MDOR has been recorded good performance (Figure 6.2) in the presence of malicious nodes.

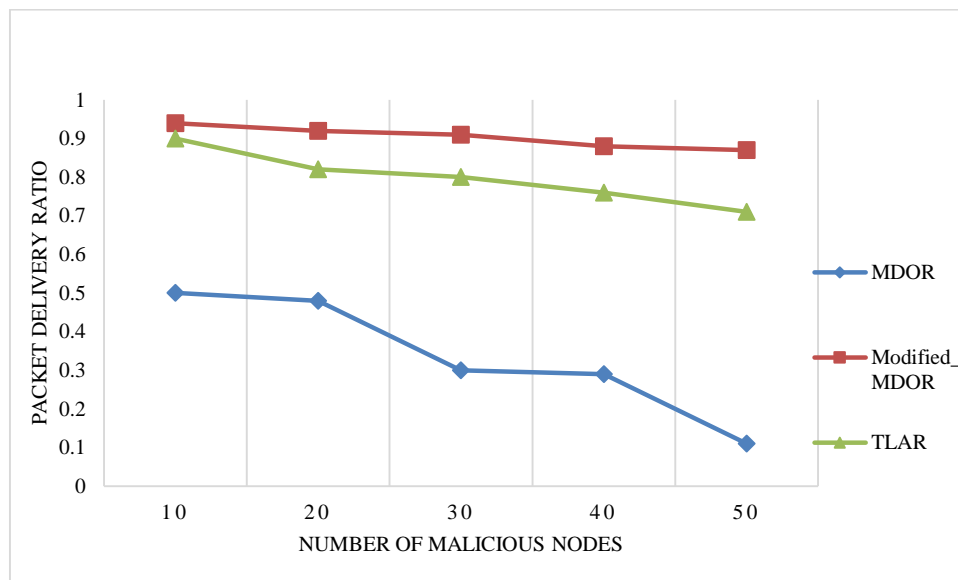


Figure 6.2: Performance in Terms of Packet Delivery Ratio

Modified_MDOR avoids those nodes which are having lower trust values and also the nodes which are having less residual energy. The packet delivery ratio will decrease when a number of malicious nodes increases. TLAR also shows good performance but rapidly decreases when the number of malicious nodes is increasing. MDOR do not employ any malicious node detection and avoidance method and hence the packet delivery ratio is the lowest for it.

Next performance parameter is end-to-end delay, which is measured as the time elapsed in successfully transmitting one packet from source node toward the destination node. The figure 6.3 can depict that MDOR presents low delay when the number of malicious nodes are less but

goes on increasing when malicious nodes are increasing. MDOR presents low delays because it always selects the middle position node on the basis of distance as next-hop relay node. But in modified_MDOR and TLAR the source node first compute the trust values for each node in the neighbor list and then assign priorities. This will increase the time elapsed in selecting the next-hop relay node. Also TLAR uses more parameters in trust value calculation and that's why it recorded high end-to-end delays. The overhead of trust value calculation in case of TLAR is high as compared to modified_MDOR.

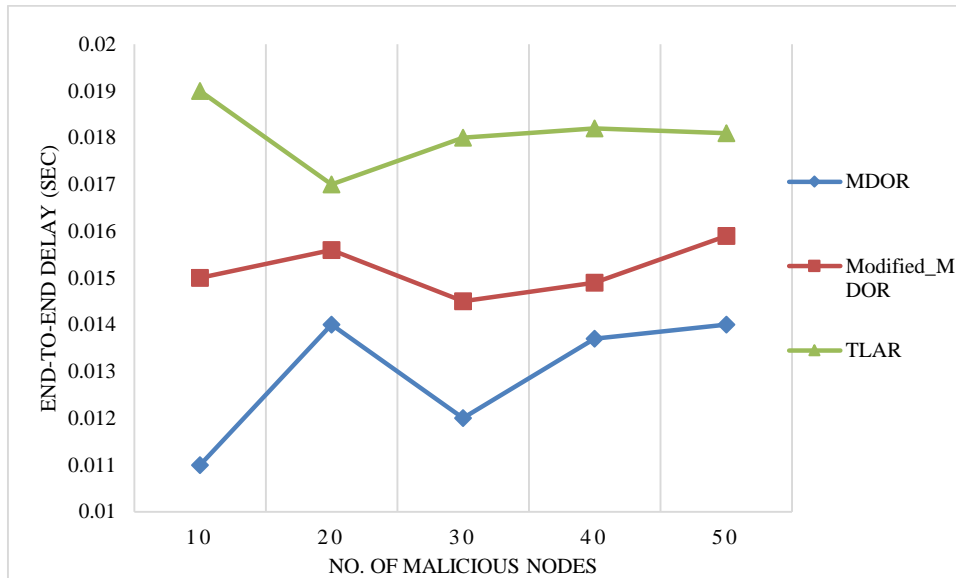


Figure 6.3: Performance in Terms of End-to-End Delay

Energy efficiency is another important performance parameter which is measured as the total energy consumption in the network until the first the node runs out of energy. The total energy consumed by each node may be calculated as the sum of energy consumed various network operations like transmission, reception and generation of data packets, acknowledging data packets, forming neighbor lists and calculating trust values. Modified_MDOR consumes lesser amount of energy as compared to TLAR and MDOR. MDOR do not employ any security method to avoid malicious node and hence has reconstruct the routes and retransmit the data packets when there is a failure in data delivery. Although MDOR introduces dynamic energy consumption for various operations in the network, but due to malicious nodes the energy consumption is high. TLAR also shows high energy consumption as the malicious nodes are increasing because of the extra overhead in collecting all the parameters used in consolidated trust value. The lifetime of the network will be increased if the energy efficiency of the routing protocol is good.

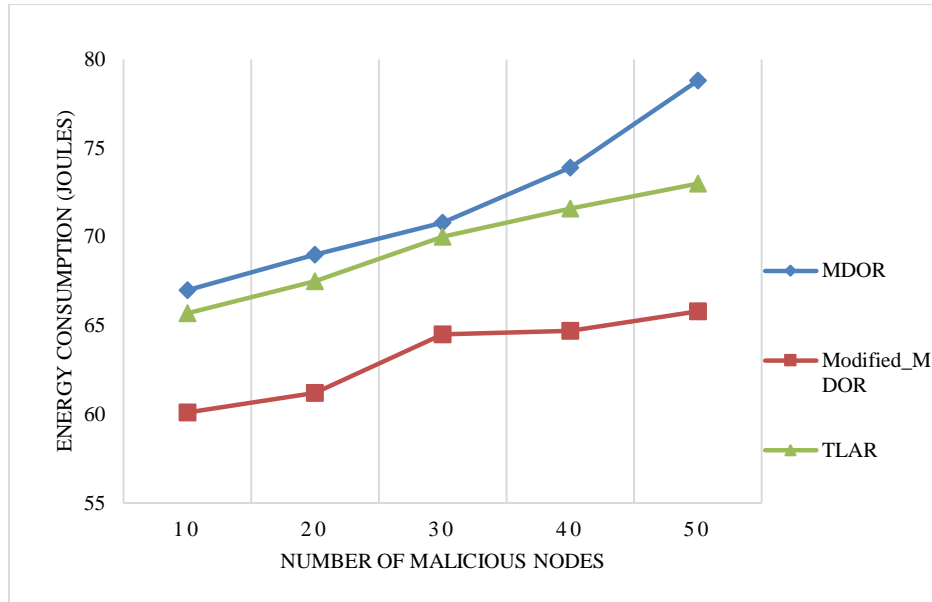


Figure 6.4: Performance in Terms of Energy Consumption

From all the performance results it is depicted that the modified_MDOR works well in the presence of malicious nodes. This means that modified_MDOR is able to detect and avoid the malicious nodes during the routing process. Also trust and reputation based routing protocols are able to secure the network internally. These methods consumes lesser energy and are able to increase the lifetime of WSN. The proposed protocol impose lesser overhead on the node's resources. It optimize the use of resources and distribute the resource consumption among all the nodes equally. From here it will be concluded that the trust and reputation based systems are used to avoid the malicious nodes and these can also save the network from internal attacks. Modified_MDOR is just a testing of trust based opportunistic routing protocols which reveals good performance. Hence a few more important parameters other than packet forwarding ratio and energy must be considered for trust evaluation so that more number of attacks may be detected and avoided. In the next section of this chapter a novel trust and reputation aware protocol is discussed which will be able to detect black-hole, grey-hole and worm-hole attacks.

6.4 TAEROR: OR Protocol for WSN

TAEROR is a trust and reputation aware protocol that is specially designed by taking care of the resource constraints present in WSN. This protocol try to solve the problems in existing trust-aware protocols like high energy consumption, end-to-end delays, low network lifetime and low throughput. TAEROR is based only on the direct trust values as collected by the source node about its neighbors. Every node which becomes a source node will first form a 1-hop neighbor list and then collect information like residual energy, a number of packets successfully

forwarded and number of network acknowledgments transmitted successfully. TAEROR utilizes the broadcasting nature of the wireless radios equipped on the sensor nodes. The packets will be transmitted through the best next-hop available in the forwarder set. This protocol also presents a new trust-aware opportunistic routing metric which will help in finding out the best possible next-hop as a relay node. After designing the protocol, it is simulated and compared to the existing trust-aware protocols. In this section, TAEROR will be deliberated in detail. The situations assumed for the proposed protocol are depicted in the next subsection.

6.4.1 Assumptions

- i. Random deployment of the nodes in the selected application area is considered for the simulation.
- ii. Total energy, energy consumed in transmission and reception of data packets are equal for each node.
- iii. A self-centered or loaded sensor will drop out the data packets received by it and communicate false information about residual energy and remaining buffer memory.
- iv. To impose black-hole attack the malicious nodes drop all the packets received in their buffer and to impose grey-hole attack these nodes drop selected packets after some time intervals.

6.4.2 Working

Opportunistic routing is dynamic routing technique which always selects the next-hop relay node at the time of transmission. TAEROR is also opportunistic in nature with trust and reputation based relay selection. This protocol optimizes the resource consumption by all sensor nodes in the network. As discussed in earlier chapters that forwarder list formation and assigning priorities to each node in the forwarder list is an important task in OR, TAEROR tries to select the next-hop relay nodes on the basis of trust values of nodes. To find out which node is the best to relay a trust-aware routing metric is defined. Based on this trust metric TAEROR will select next-hop forwarders. The nodes which are having low trust values will be discarded from the forwarder list.

To complete the successful packet transmission TAEROR executes in two major phases: trust evaluation and relay selection. Initially after random deployment of nodes in the specific area of interest a random source will be chosen. This source node will start communicating data packets to a fixed destination called as a base station. To do so source node will first form a

neighbor list (*NGH*). This neighbor list is formed on the bases of “hello packets” as in case of modified_MDOR in the previous section. As soon as the neighbor list is completed the source node start collecting the information about neighbors. The information will be about residual energy, successful transmissions, and successful acknowledgments. For calculating the energy cost, first order radio model is used [88]. This trust evaluation phase will prioritize the forwarder nodes and the highest priority node will forward the data packet first. Trust evaluation phase is discussed as in the following subsection.

Trust Evaluation

This is a trust value calculation phase of TAEROR. The relay nodes from a source to destination will be elected based on the trust value of the sensor. The consolidated trust value will act as a composite routing metric including the impact on residual energy (*E*), forwarding sincerity (*F*) and acknowledgment sincerity (*ACK*) as its components. Whenever any node generates a data packet to be sent to the base station of the network, it will act as the source node. The source node forms the neighbor list (*NGH*) on the basis of replies of “hello packets” received from different nodes. For every node in the neighbor list, the consolidated trust value will be calculated and stored. This trust metric is based on the probability of each sensor node to act as malicious (*P_m*). The probability can be calculated as a consolidation of dropping ratio (*R_U*) and delaying ratio (*R_{delay}*). The dropping ratio can be calculated as the ratio of a number of packets dropped by a node to the number of packets generated at the source node and sent to the same node. Similarly, delaying ratio can be calculated as the number of packets delayed inside the buffer of a node and a total number of packets generated at the source node.

$$P_m = (1 - R_U) - R_{delay} \dots\dots\dots(1)$$

$$R_U = N_{dr} / N_s \dots\dots\dots(2)$$

$$R_{delay} = N_{delay} / N_s \dots\dots\dots(3)$$

The probability of being mischievous is computed over here may always not represent the actual behavior of a sensor node. The actual behavior may oscillate around the value of *P_m*. After the calculation of *P_m* the consolidated trust value calculation will be started. Firstly, the source node collects the information about the number of packets successfully forwarder by a neighbor node (*SF(i,j)*) and also a number of packets which are not acknowledged or not forwarded successfully (*UF(i,j)*). Here, *i* is the source node and *j* is the node which is inside

the neighbor list of i . After collecting these values the forwarding behavior i.e. packet transmission sincerity factor ($F(i, j)$) will be calculated by the equation below.

$$F(i, j) = \frac{SF_{(i,j)}}{SF_{(i,j)} + UF_{(i,j)}} (1 - P_m) \dots\dots\dots (4)$$

Similarly, the acknowledgment sincerity i.e. generating and forwarding acknowledgments will be calculated by using the successful ($SACK(i,j)$) and unsuccessful ($UACK(i,j)$) acknowledgment counts.

$$ACK(i, j) = \frac{SACK(i, j)}{SACK(i, j) + UACK(i, j)} (1 - P_m) \dots\dots\dots (5)$$

The next factor is calculating the impact of network operations on the residual energy (E_{impact}) of each neighbor node. Here, it is being considered that the most of the sensor's energy will be consumed in performing radio operations. The radio operations mainly involve three kinds of energy consumptions. First is transmission ($E_{Fwd}(j)$) energy, calculated as the energy which is required by a node j to transmit a data packet. Second is the receiving energy consumption ($E_{Rcv}(j)$), which is the energy consumed during the reception of data packets at node j . The third one is the need of energy by a node j to receive and forward the network acknowledgments from and towards a node i . These three energy factors are summed up and divided by the residual energy ($E_{total}(j)$) of the neighbor node j . The impact will be calculated as in the following equation.

$$E_{impact}(i, j) = \frac{E_{Fwd}(j) + E_{Rcv}(j) + E_{ack}(i, j)}{E_{total}(j)} (1 - P_m) \dots\dots\dots (6)$$

This impact calculation factor is very useful in distributing the energy consumption load among all the nodes equally. If the E_{impact} value is high for certain node this means that the node cannot transmit data but it can still sense data. Hence, if this node is used as relay node it will soon be dead and the network will also consider as dead. Therefore, instead of choosing this node as relay opportunistic routing will choose another neighbor node which is having lesser E_{impact} value.

Consolidated trust value will now be computed by using three factors calculated above. Each factor will be associated with one important parameter. The importance parameter can be tuned according to the needs of the applications. Here, α is the important parameter for $F(i, j)$, β is

for $E(i, j)$ and γ is for $ACK(i, j)$. Including these important parameters, the direct trust value will be calculated as in the following equation.

$$RT(i, j) = \frac{\alpha * F(i, j) + \beta * E(i, j) + \gamma * ACK(i, j)}{\alpha + \beta + \gamma} \dots\dots\dots (7)$$

The direct trust values will be computed for every sensor on the neighbor list. But this will not be the final trust value as the trust value may be out of date for every single sensor on the neighbor list. This means that the nodes may change their behavior over time and that's why trust value must incorporate aging parameter [20]. The older value must be incorporated into the new one to compute the final trust value ($FT(i, j)$). $FT(i, j)$ is the final trust value for node j w.r.t. sensor i will compute the behavior of each node and help relay selection algorithm to find out the malicious nodes.

$$FT(i, j) = \sigma * NewRT(i, j) + \lambda * (1 - \sigma) * OldRT(i, j) \dots\dots\dots (8)$$

Here, the aging factor is $0 < \sigma < 1$ and $0 < \lambda < 1$ is the importance of $NewRT(i, j)$. Both aging and importance factor depends on the application of WSN and may be tuned according to the requirements. This final trust value now will be ready to be used in relay selection algorithm presented below.

Relay Selection Algorithm

Selecting best next-hop relay nodes is the primary task in OR protocols. Whenever a source has to transmit the data packets to the base station a list of potential forwarder nodes out of all neighbors will be created. Out of these potential forwarders, only one node will be selected to forward the data packet first to lessen the total of identical data packets received at the base station. This task of prioritizing among all the potential forwarders and selecting one out then which is of higher priority is performed by the relay selection algorithm. Before starting with the relay selection algorithm it must be measured that whether the data packet of making positive progress (FP) towards the base station or not. It can be measured by using the distances between source and base station ($D_{s,d}$) and relay node and a base station ($D_{ni,d}$) with k will be the total sensors in the network.

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \text{ where } 0 \leq i, j \leq k, \text{ and } i \neq j \dots\dots\dots (9)$$

$$FP_{n_i}^{s,d} = D_{s,d} - D_{n_i,d}, \text{ where s=source, d=destination, } 0 \leq n_i \leq k \dots\dots\dots (10)$$

The input to relay selection algorithm is a source node (S) which will be selected randomly out of all the nodes in the network. Source node always tries to transmit data packets towards the fixed base station (D). The neighbor list (NGH) will be formed on the basis of replies of “hello packets” broadcasted by the source node. After the formation of NGH , the trust value will be calculated using equation (8) for each node. This final trust value (FT) for each node in the neighbor list will decide that which node will be a potential forwarder. The nodes which are having FT value greater than threshold value will be added to the forwarder list (FL). After the formation of FL , this list will be sorted in descending order according to FT and the node with highest trust value will be selected as a next-hop relay node. This relay node will transmit the data packets first received from the source node. The packets generated at source node include the minimum allowed trust value and the forwarder list. Now, the new receiver will become the source node and follow the same procedure as followed by the previous one. The execution of algorithm will be continued on each relay node selected on the path and this procedure will end only when the base station is reached.

Algorithm: Relay Selection (S=Source, D=Destination)
<pre> When node S want to send a packet Let t_{min} be the minimum acceptable trust factor of a node x be the number of 1-hop neighbors of S Let $FT[Z]$ be the node trust factor of node Z Let Max_NH be the maximum number of neighbors which are allowed in forwarder list (FL) FL= empty Sort all 1-hop neighbors of S in descending order according to $FT[Z]$ For ($Z=1$; $FL < Max_NH$ and $Z \leq x$; $Z=Z+1$) Do If ($FT[Z] \geq t_{min}$) then Add Z's ID in FL EndIf EndFor If ($FL \neq empty$) Broadcast MSG (S, D, FL, t_{min}) EndIf </pre>

Figure 6.5 presents an example of the algorithm execution. The source node is represented as S and base station is represented as D . S will create its neighbor list as $\{1, 2, 3, 4\}$ and compute the trust value FT for each of these nodes. Assume that the values of FT for nodes 1, 2, 3 and 4 are 0.3, 0.5, 0.7 and 0.5 respectively. The neighbor list will then be arranged according to values of FT in diminishing order. The new neighbor list after sorting will be $\{3, 2, 4, 1\}$. Now consider the maximum number of relay nodes allowed in forwarder set is 3. Then forwarder set FL will be $\{3, 2, 4\}$. After the relay node list is formed the data packet is communicated by

comprising the forwarder list, least allowable trust value, and base station identification. The sensor on the top of forwarder list, number 3 in this case, will communicate the data packet first executing the similar process. This process will be continuous till the base station D is not found.

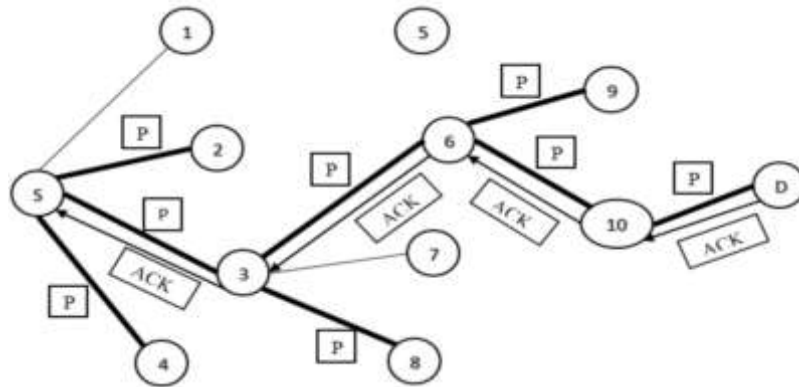


Figure 6.5: Example of Relay selection in TAEROR

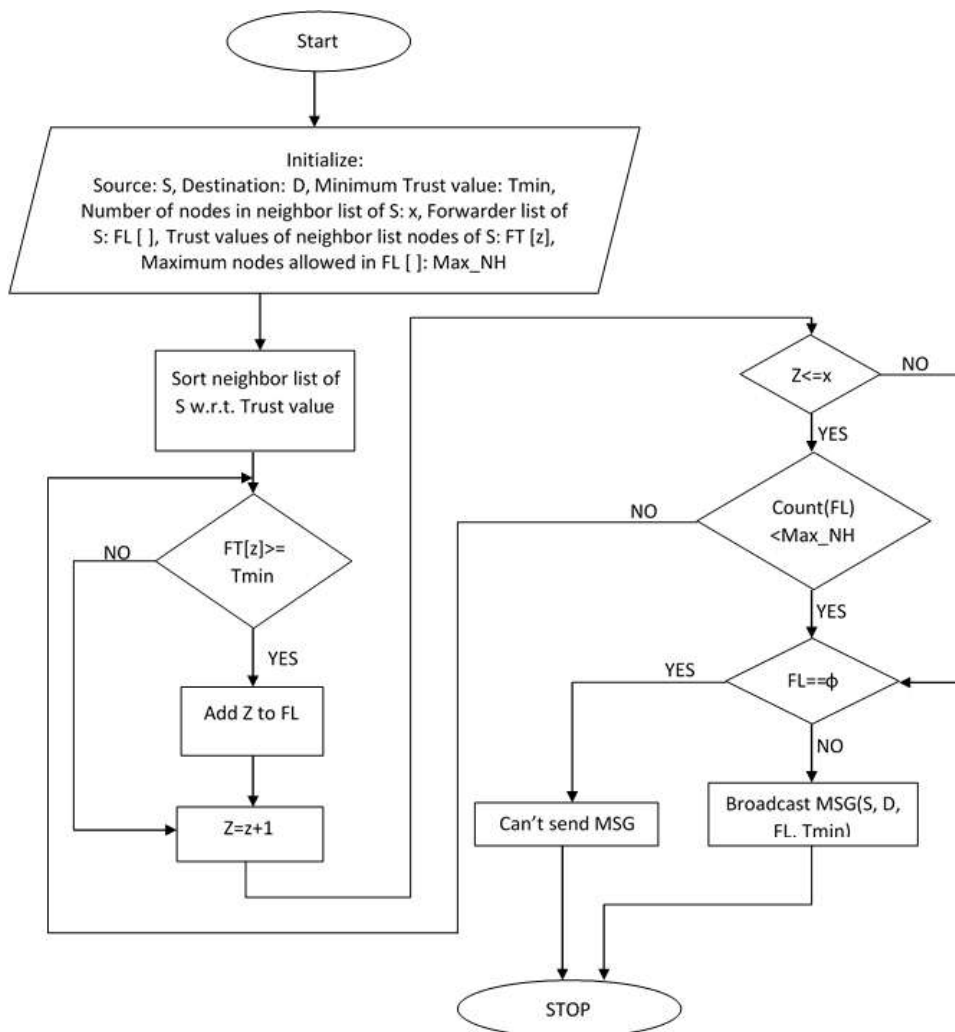


Figure 6.6: Flowchart for Proposed Relay Selection Algorithm

Forwarder list contains the nodes which are capable of forwarding data toward the base station. Every node in the forwarder will have the chance to forward data packets. But if the highest priority node successfully forwards the data packet than no other node will forward he data again. The sensors which are selfish or mischievous, will not be selected during the forwarder list selection. These nodes will be avoided during the routing process. TAEROR hence, able to detect the mischievous nodes on the basis of trust values and those nodes will be discarded from the neighbor lists of all nodes. The data delivery will be reliable because the packet will be forwarded to the base station only be the trusted nodes. TAEROR will also reduce the number of duplicate packets at the base station with the help of relay selection algorithm. The flowchart for TAEROR protocol's relay selection algorithm is as given in figure 6.6.

6.4.3 Experimental Results and Performance Analysis

For the experimental analysis of proposed protocol TAEROR is simulated on NS2. The simulation scenarios are created and results are recorded.

Table 6.2: Simulation Settings

Parameter	Value
Simulator	NS-2.35
Deployment Area	500 x 500 m ²
Transmission Range	60 m
No. of Nodes (N)	25, 50, 100
No. of Mischievous nodes	10, 20, 30, 40 and 50
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	50J
Initial Trust Value	1
Default σ and λ	0.90 and 0.4
Energy consumption to run the radio ($E_{electronic}$)	50 nJ/bit

The performance of the protocol was compared to existing trust-aware routing protocols i.e. TLAR [18], TESRP [19] and TAOR [20]. These all protocols are simulated again in using NS2 so that the platform and simulation settings will be same for all protocols. The simulation parameter settings are shown in table 6.2. The application area considered for the simulation is assumed to have malicious nodes which are turned malicious after some of the simulation time is elapsed.

The malicious nodes may conduct black-hole and grey-hole attacks. When a malicious node drops all the incoming packets than it will be called as a black-hole attack. In this case, the number of packets must be retransmitted and this will reduce the performance of the network. Similarly, the grey-hole attack will be imposed when a malicious node selectively drops packets after some interval of time. This attack is difficult to identify because the forwarding ratio and the trust value will not be zero in this case. TAEROR protocol tackles both types of attacks intelligently by collecting the acknowledgments sincerity besides forwarding sincerity. It is also assumed during simulation that malicious and selfish nodes do not generate any data packets. The simulations are performed again and again to get a better view of results for all compared protocols. The results are plotted in form of graphs and these are virtuously simulation based. The parameters for testing of the protocols are always same for all simulation and for all protocols.

Firstly the security performance has been tested by using a number of mischievous nodes faced through the routing mechanism. Figure 6.7 presents the performance of all the protocols in terms of an average number of mischievous nodes met through the transmitting process. The safety performance is measured in terms of a number of malicious nodes because every-time a malicious node is encountered the path needs reconstruction from the source node. AS all the compared protocols are trust and reputation based if a node is having low trust value it will be considered as a malicious node.

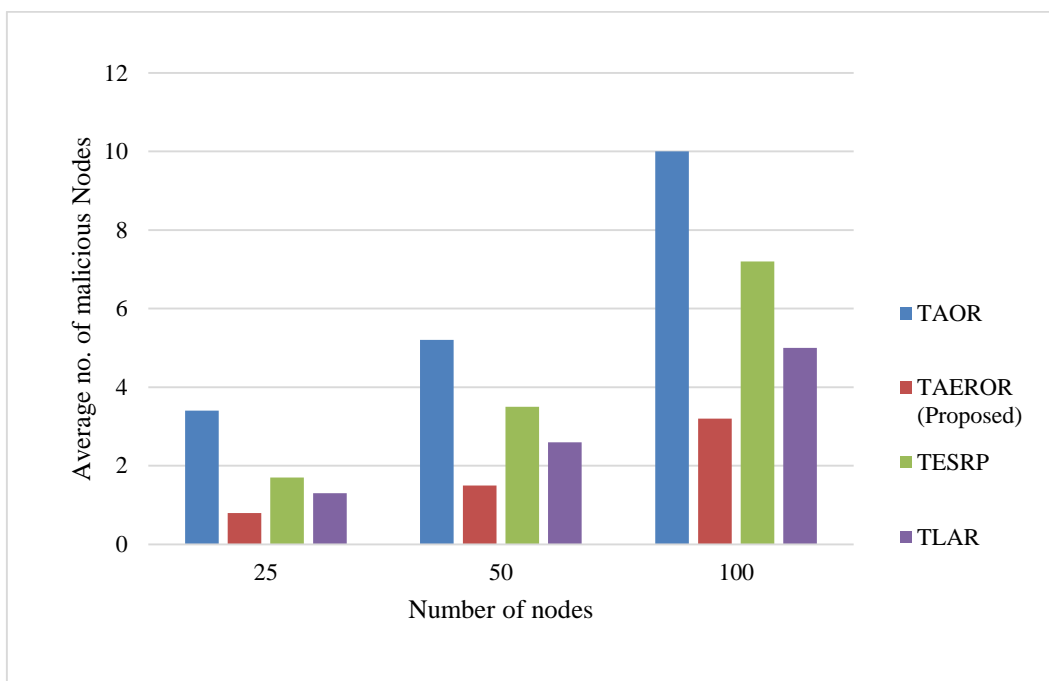


Figure 6.7: Performance on the basis of Average risk level

TAEROR calculates the trust value for each node in the neighbor list of the source node and helps the source node to identify the malicious nodes. The nodes which are not taking part in routing process sincerely like the nodes which are not forwarding data packets and acknowledgments will be discarded by the relay selection algorithm. The malicious nodes will not be able to communicate any other data packets in near future and are ignored by other nodes. TLAR presents the similar results because it employs the similar procedure on the basis of trust values. TESRP and TLAR both do not employ any mechanism to handle the selfish nodes and will end-up in low-security performances.

The packet delivery ratio is measured as the ratio of a number of packets successfully delivered at the base station to the number of a packet generated during simulation by different source nodes. Figure 6.8 presents packet delivery ratio for all the simulated protocols in the presence of a different number of malicious nodes. The delivery ratio for TAEROR and TLAR is almost similar because both the protocols have the ability to avoid black-hole and grey-hole attacks. These protocols avoid both selfish and malicious nodes and discard these nodes from the neighbor list of source nodes. TAOR presents good results but fails in providing energy efficiency and similar is the case with TESRP.

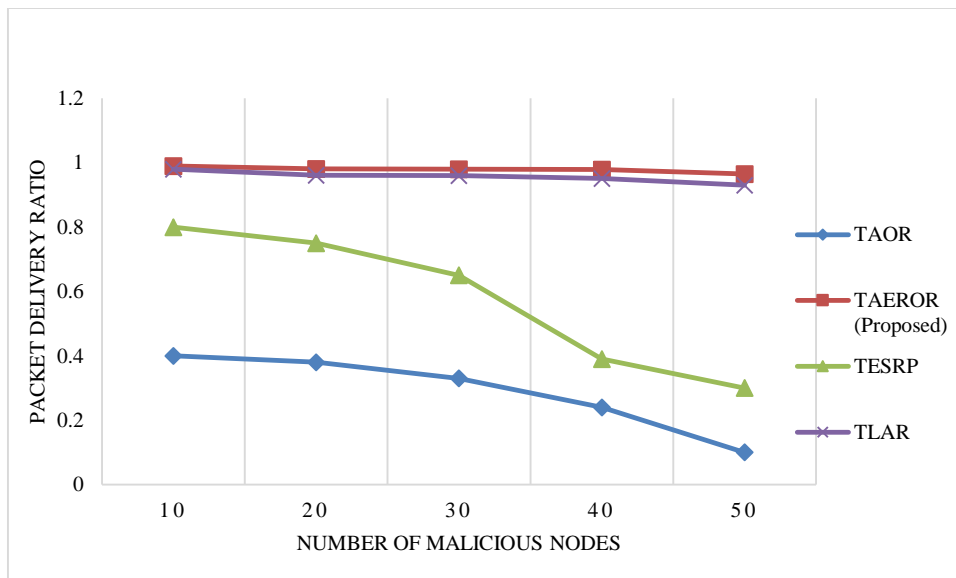


Figure 6.8: Performance on the basis of Packet Delivery Ratio

Another performance parameter is an end-to-end delay (Figure 6.9) which is also a major performance parameter for routing protocols. This performance parameter is directly related to the reliability and quality-of-service of the network. The end-to-end delay will only be calculated at the time of the successfully delivery of the data packet. In the presence of

malicious nodes if there is no security mechanism than end-to-end delay will be high. Also for high overhead of trust value calculation as in case of TLAR, the trust value will be high. TAEROR and TAOR present a good performance by introducing lesser delays because of the direct trust value calculations only. But, in case of TLAR and TESRP overheads of trust value calculations are high because of more parameters and indirect trust values also. That is why the end-to-end delays in these are high.

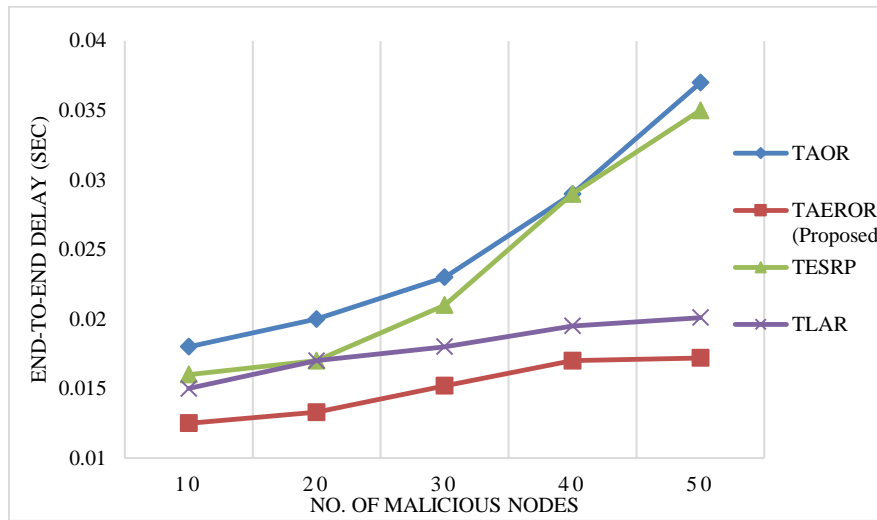


Figure 6.9: Performance on the basis of End-to-end Delay

The most important parameter related to unattended wireless sensor networks is the energy efficiency. Most of the energy consumption will take place during the routing process. Because the most important network operations that are packet transmissions, receptions and acknowledgment sending receiving will be performed during the routing process.

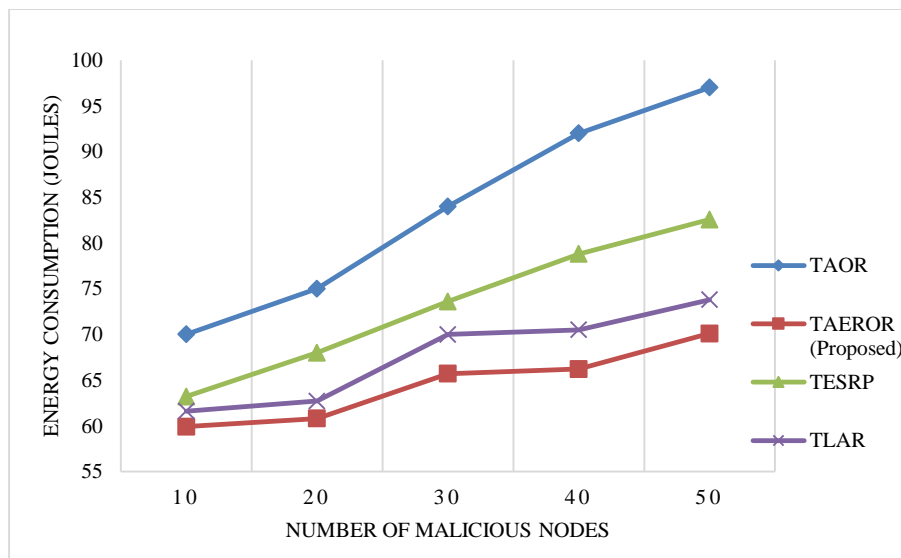


Figure 6.10: Performance on the basis of Total Energy Consumption

As Proposed protocol TAEROR consider the impact of each energy consumption on the node's residual energy it presents high energy efficiency (Figure 6.10). This is because each time the transmission started to form the same source the relay node will not always be same. Hence, the transmission task of nodes will be distributed among all the neighbors of the source node. Also, the trust evaluation overhead is very low in TAEROR which improve the energy efficiency of each node which is selected as the source node. Due to good energy efficiency, the network lifetime will also increase.

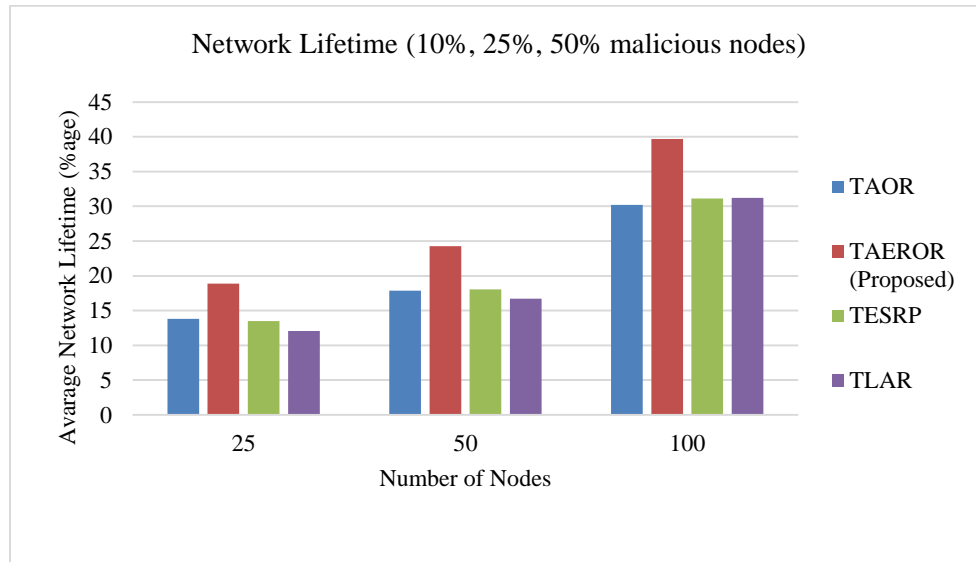


Figure 6.11: Network Lifetime

The network lifetime here can be measured as the total time elapsed from the starting time of network and time at which the first network node runs out of energy to send a packet. This is because to lose a node could mean that the network could lose some functionalities. The network lifetime calculated for all compared protocols is similar. The network lifetime was tested for all protocols in the presence of malicious and nodes. The proposed protocol TAEROR have better network lifetime than other compared protocols because of lesser energy consumption.

6.5 Conclusion and Future Scope of Work

In WSN most of the traditional cryptosystems will not work well because of the resource constraints. In recent years trust and reputation aware methods prove to be far better for WSN because of low energy consumption and fewer resource requirements. TAEROR is a similar contribution to the secure opportunistic routing protocols, especially for WSN. Another important contribution of this chapter is the modified_MDOR protocol which is also a good

alternative over cryptosystems. Both the proposed protocols were able to detect selfish and malicious nodes. These nodes than were discarded from the neighbor list and never used again for transmitting data towards the base station. Both the protocols present good simulation performance as compared to the existing trust-aware routing protocols. In future directions, more parameters may be considered during trust value calculation. But as seen from the simulation results for TLAR more parameters introduce high end-to-end delays and low energy efficiency. Hence, the trust evaluation must consider only the most important parameters like energy, forwarding sincerity, data reliability etc.

CHAPTER 7

TRUST AND LOAD BALANCING BASED OPPORTUNISTIC ROUTING PROTOCOL

7.1 Introduction

Opportunistic routing overcomes the disadvantages of fixed path routing protocols. But, there may be an increase in a number of attacks because of the broadcasting or multicasting of data packets. To avoid attacks, the nodes must cooperate with each other so that an intruder may be detected. Detecting attackers and malicious nodes will improve the reliability of data packets. In OR the secure route selection is important, which lead to the improved lifetime and trustworthiness among all nodes. The energy saving requirements may be fulfilled by utilizing OR because there is no need of reconstructing the source-destination path again and again. OR gives no guarantee of data or route selection security.

Whenever network security is required, most of the researchers talk about cryptosystems and authentication systems. But, if these systems are implemented in WSN than there will be a problem of high energy consumption due to large calculations [92]. The network lifetime will be less in this case. The security method must assure that the sensor node selected as a relay node is trustworthy or not. For solving this purpose researchers have focused on developing new trust and reputation aware protocols in last three to four years.

Some of the trust-based routing protocols still using cryptosystems to cope up with inside as well as outside attacks. Trust-aware routing framework (TARF) [93] is one of these protocols. TARF is routing framework which is inspired by the theory of trust for social networks. Although this protocol is good but it fails to provide energy efficiency when applied to wireless sensor networks. This is because of the cryptography applied during the routing process. EMPIRE [94], as the name given by the authors, is another trust-based routing protocol for wireless networks. By including the trust among the relay node selection EMPIRE tried to decrease the number of tasks assigned to each relay node in the network. Authors believe that reducing the number of tasks will save energy of relay node and this will improve the network lifetime. Continuing research in this area authors of [95] has proposed energy efficient trust-aware routing protocol (ETARP) for WSN. This protocol selects relay nodes on the basis of packet communication cost. It focuses on optimal utilization of resources. In [96] authors have

proposed trust-aware energy efficient secure routing protocol (TESRP) to improve energy efficiency. This protocol improves the lifetime of the network and tried to maintain trust among all the sensor nodes. Trust and location-aware routing protocol (TLAR) [18] was proposed recently to maintain trust among nodes by using direct and indirect values of different parameters. TLAR collects these values and includes a consolidated trust value. The weights were assigned to each parameter according to their importance. These weights may be attuned vigorously during the operation of the network.

Instead of security and energy efficiency, there is another important factor for consideration in WSN, is load balancing. The protocols discussed earlier provide only trust management among nodes and focused energy efficiency only. Now, if there is a problem of congestion in the buffer of the relay nodes than the packets suffer from high end-to-end delays. Also, this will reduce the throughput of the network. To overcome this problem there must be buffer-aware routing protocols. Buffer ware routing protocols can divide the load of relaying packets towards the base station among all relay candidate nodes. Working in this direction Buffer aware opportunistic routing (BAOR) [68], ORPL-LB [8] and POR [69] protocols were proposed for wireless networks. Security and energy efficiency are not major motives of these protocols and hence these protocols cannot be directly employed with wireless sensor networks.

In this chapter, a new trust and energy efficiency aware routing protocol is proposed and named as trust ad packet load balancing OR protocol (TPBOR). TPBOR can directly be employed to WSN and it provides energy efficiency and trust management among all nodes. This protocol also balances the packet load and equalize the number of packets transmitted by each sensor node toward the base station. The protocol will be discussed in the upcoming section.

7.2 Proposed OR Protocol (TPBOR)

The proposed routing protocol specially designed for WSN and hence three major parameters are considered in designing this protocol i.e. trust management, energy efficiency and packet load balancing. TPBOR is an opportunistic protocol and may be used directly with any of WSN applications.

7.2.1 Opportunistic Routing Design

Opportunistic routing works in two major phases: forwarder candidate set selection and prioritizing the forwarder set to select the next-hop forwarder. The second phase is crucial and needs a priority metric to decide which node will be the first to forward data packets to the base station. Also if the candidate forwarder set is large in size than it will increase the computation

cost but there will be a significant increase in packet delivery ratio. The routing metric should prioritize all the nodes on the basis of some parameters like energy, distance, link reliability and packet delivery ratio of node etc. The prioritization among nodes should be optimal. If only one metric is chosen for the priority then there will be a problem of selecting one node as forwarder node again and again. In this case OR protocol will behave like fixed path routing. Hence, the routing metric should be a composite metric which can make the optimal route selection. TPBOR introduce a new routing metric which will optimize the route selection on the basis of trust value and buffer capacity of a node at a particular time.

7.2.2 Relay Selection Criteria

As OR protocol depends on the routing metric which will prioritize the nodes in the forwarder set. While designing an OR protocol one must define a next-hop forwarder selection criteria. In TPBOR the relay selection criteria consist of three phases. The 1st phase the progress of data packet in the network will be measured on the basis of positive distance covered by it toward the base station.

$$Dist_{i,j} = \sqrt{(co_x_i - co_x_j)^2 + (co_y_i - co_y_j)^2} \dots\dots\dots (1)$$

Where $0 \leq i, j \leq k$, and $i \neq j$

$$Progress_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d} \dots\dots\dots(2)$$

Where s=source, d=destination, $0 \leq n_i \leq k$

The 2nd phase is to the buffer of each node in the forwarder set will be tested. The buffer size of each node is limited. Hence, when a number of packets are transmitted through the same node again and again, the delay of packets inside the buffer will be increased. Also, if there is no space available on the buffer of selected relay node than there will be an upsurge in a number of dropped packets. The queue test introduced in TPBOR will test the buffer of each node and make sure that the overloaded nodes will not get selected as next-hop forwarder nodes again and again. The following equation will complete the queue test of a node and avoid the nodes for which the test value is high.

$$Queue_Test_i = w. \frac{Q_{num}}{Q_{size}} \dots\dots\dots(3)$$

Where Q_{num} is the number of packets stored currently in the queue, Q_{size} is the total size of the queue of a node and w is the weighting factor.

In the 3rd phase, the trust value for each node will be calculated as proposed in chapter 5. Trust value will shortlist the forwarder set according to the behavior of the nodes in the forwarder set.

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma} \dots\dots\dots(4)$$

Where $0 \leq \alpha, \beta, \gamma \leq 1$ and F_i , E_{total_i} , and ACK_i are forwarding sincerity, energy depletion value, and acknowledgment sincerity respectively.

7.2.3 Trust and Packet load Balancing Based OR (TPBOR)

In literature, the most effective opportunistic routing algorithms are those which are distributive in nature. Distributive here means that the metric calculation and next-hop relay node selection will be dynamic. TPBOR is designed to behave as distributive OR protocol. TPBOR decides the next-hop on the basis of the buffer availability and the behavior of neighbor nodes.

Whenever the network starts its operation the nodes start communicating data towards the base station. The node first broadcast the RTS (Request to send) signal. The nodes which are receiving this request will reply to the sender node with their energy, queue size, and location coordinates. The replying nodes will be added to the neighbor list (NB) of sender node. After neighbor list formation, the queue size factor ($Queue_Test_i$) is checked for each node. If this factor is greater than the threshold value (0.25 here) than the node will not be added to the forwarder list (FL). This will prevent the overloaded nodes to be selected as the next hop forwarder. This will reduce the end-to-end delay for packet forwarding in the network.

After the formation of forwarder list (FL), the forwarder node will be selected. The forwarder node will be the trusted one. The trust value for each node in FL has been calculated by using equation 4. The node in FL which is having the highest trust value will be selected as next hop forwarder node. Also, the nodes which are having trust value lower than 0.2, will be discarded from the forwarder list (FL). The threshold value of trust i.e. 0.2 has been fixed after extensive simulations have been carried out with values 0.0 to 1.0.

As the trust value is calculated dynamically and it involved energy consumption of a node, the energy consumption will be distributed across all nodes in the network. This will prolong the lifetime of the network. The trust value helps the protocol to avoid malicious nodes. Malicious

node is defined as the node which does not forward data packets to impose black-hole attack and grey-hole attack. The trust value will be updated dynamically for each session of data transmission.

TPBOR, hence provide security from black-hole attack and grey-hole attack by transmitting data through trusted nodes only. Also, there will be low overhead for the trust value calculation because the existing values are used like energy, forwarding ratio, and acknowledgment sincerity. Also, only the nodes which are rich in energy will be selected as next hop forwarders, will increase the network lifetime. The algorithm below depicts the relay selection process of TPBOR.

<p>Algorithm: Relay_Selection (S, D, Distance(S, D))</p> <p>Input: Source node S, Destination D, Distance (S, D)</p> <p>Output: Successful transmission of a data packet from S to D</p>
<ol style="list-style-type: none"> 1. Create neighbor <i>NGH</i> for S 2. Broadcast RTS from S 3. Add the replying node to <i>NGH</i> 4. If D belongs to <i>NGH</i> 5. Stop algorithm 5. Create <i>FL</i> as forwarder list for S 6. For each node in <i>NGH</i> 7. Calculate <i>Queue_Test</i> using equation 3 8. If <i>Queue_Test</i> (node_i)\geq0.25 then 9. Add node_i to <i>FL</i> 10. For each node in <i>FL</i> 11. Calculate Trust value (<i>T</i>) using equation 4 12. If <i>T</i> (node_i) < 0.2 13. Discard node_i from <i>FL</i> 14. else 15. Select the node having the largest trust value as next hop forwarder (<i>FD</i>) 16. Relay_Selection (FD, D, Distance(FD, D))

The whole protocol will work on the principle of opportunistic routing in WSN. The trust value calculation helps the protocol to avoid attacks on data packets and routes. As the routes are secured the network performance will automatically increase in terms of throughput. The simulation results will be discussed in the next section.

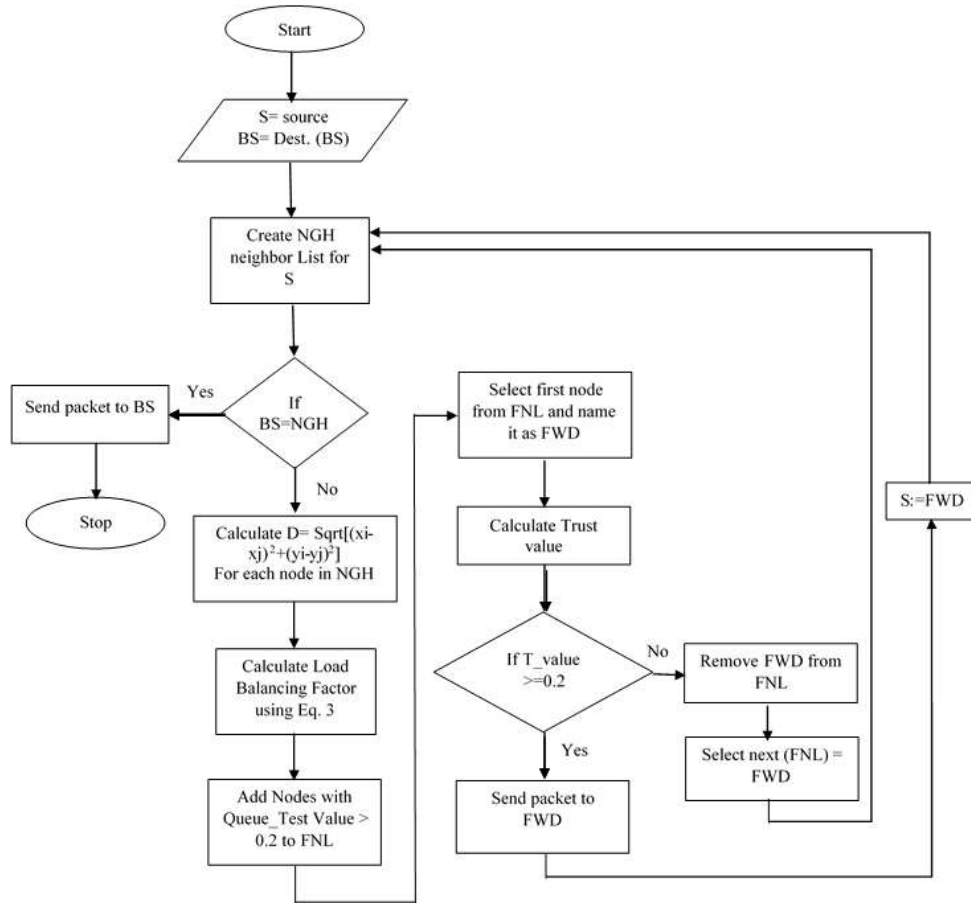


Figure 7.1: Flowchart for TPBOR

7.4. Experimental Results and Performance Analysis

TPBOR has been tested on NS2 by creating simulation scenario. Table 7.1 below depicts the simulation settings in the NS2 environment.

Table 7.1: Simulation Settings

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 m x 500 m
Transmission Range	75 m
No. of Nodes (N)	25, 50, 100
No. of Malicious nodes (%)	10, 20, 30, 40 and 50
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	50J
Initial Trust Value	1
Default α , β and γ	0.3, 0.4 and 0.3
Energy dissipation to run the radio	50 nJ/bit
Buffer Length	20 packets

The performance has been compared to BAOR (Buffer aware opportunistic routing) [68] which have not applied any security to the algorithm but applied packet load balancing. The other algorithm to which TPBOR has been compared is TLAR (Trust and location-aware routing) [18] which has applied security in form of direct and indirect trust value calculations.

The simulation settings shown above has been applied to all compared protocols. The existing protocols i.e. BAOR and TLAR are re-implemented in NS2. The simulation results will depict the better performer in the presence of black-hole and grey-hole attacks. A different number of malicious nodes have been generated during the simulation to get a good view of simulation results. The deployment of nodes in the interested area is random. Generation of malicious nodes also takes place at random locations. The malicious nodes do not act like normal nodes in the network. These malicious nodes do not generate any data packets. To generate a black-hole attack, malicious nodes drop all the packets coming to them. Similarly, to impose grey-hole attack selective number of packets have been dropped by malicious nodes.

7.4.1 Results and Discussions

After completing extensive simulations for all three protocols the performance has been recorded and presented in form of graphs. The results are purely simulation-based and all three protocols were tested on the same platform with same parameters. Figure 7.2 below shows the safety performance of all compared protocols i.e. BAOR [68], TLAR [18] and TPBOR. The safety has been measured as the average number of malicious nodes encountered during the routing process. TPBOR has encountered very less number of malicious nodes as compared to other two algorithms.

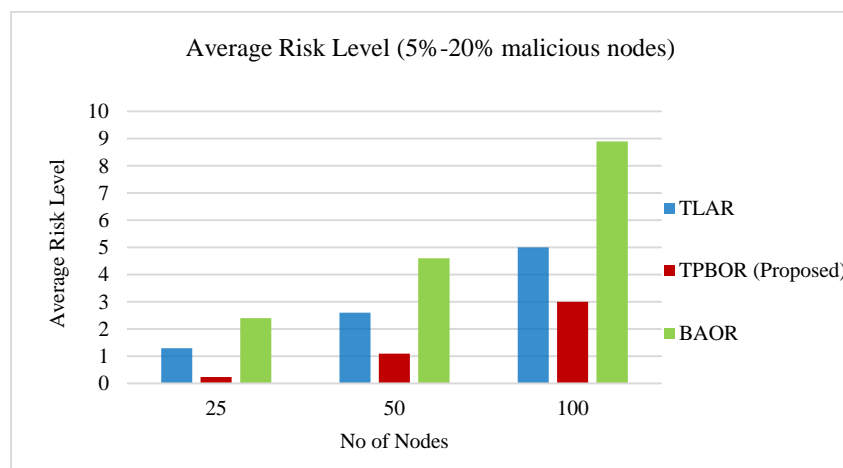


Figure 7.2: Performance on the basis of Average risk level

This is because the forwarder sincerity value F_i for a node i depicts the black-hole and grey-hole attacks. Because it monitors the number of packets forwarded towards the base station. The trust value (T) also includes the acknowledgment sincerity which will make sure that the packets are flowing towards the base station. Similar factors have been considered in TLAR. But the overhead of collecting feedback (indirect trust values) is high in this case. BAOR does not consider any type of security and hence encounter the highest number of malicious nodes during the routing process.

The performance of all three protocols on the basis of packet delivery ratio has been depicted in figure 7.3 below. This is measured as an average number of packets delivered divided by the number of packets sent towards the base station in presence of a different number of malicious nodes. TPBOR has little bit high packet delivery ratio than TLAR in when the number of malicious nodes is less. But as we increase the number of malicious nodes in the network the overhead in TLAR goes on increasing and hence there is rapid fall in Packet delivery ratio of the network. But in case of TPBOR the routing process completely depends upon direct trust values and there is less overhead. This will increase the number of packets delivered at the base station and hence TPBOR performs well. In case of BAOR as the number of malicious nodes encountered is more the packet delivery ratio will be high.

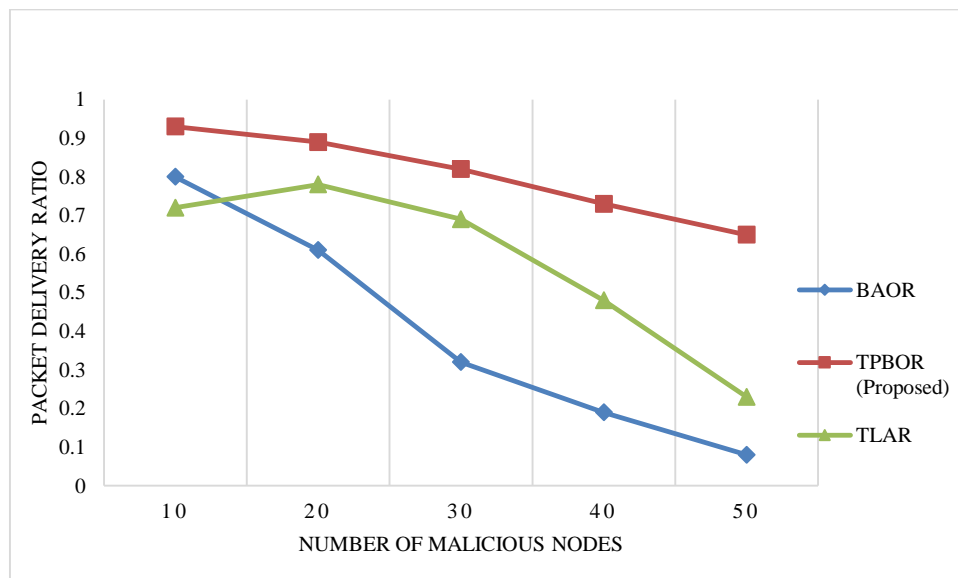


Figure 7.3: Performance on the basis of Packet Delivery Ratio

Next performance factor taken here is an end-to-end delay in figure 7.4 below. The end-to-end delay has been measured as the total time taken to deliver a data packet at the base station from the source node. The end-to-end delay will be calculated only for successfully delivered

packets. It may be depicted from the figure that the end-to-end delay of BAOR is lower initially because it only calculates the back-off value and forwards the data packets. But the end-to-end delay in presence of malicious nodes will become higher. In case of TLAR and TPBOR the extra overhead is the calculation of trust values. TPBOR shows here some improvement because it only relies on direct trust value and need not wait for the feedbacks of other nodes. TPBOR performs best in the presence of malicious nodes.

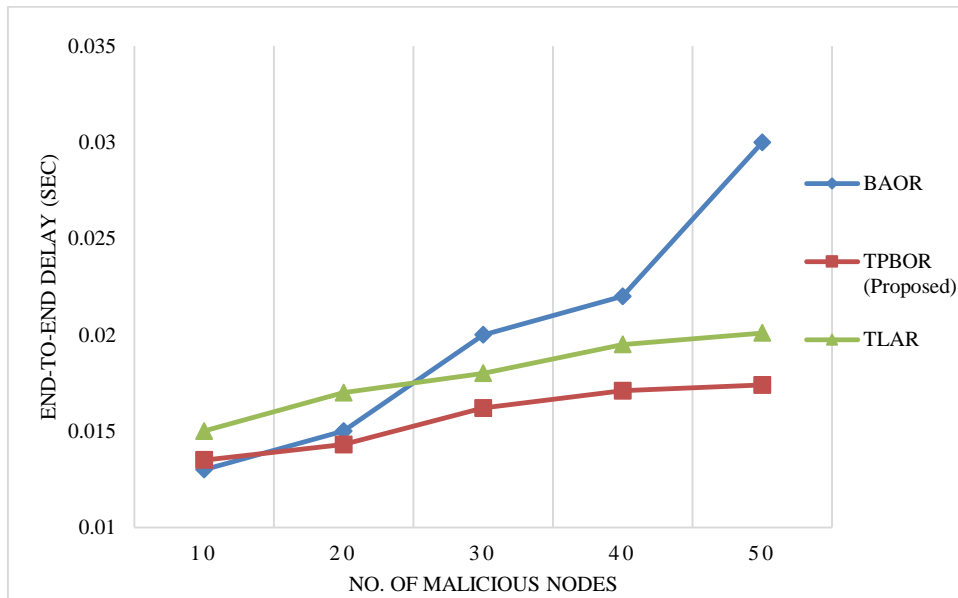


Figure 7.4: Performance on the basis of End-to-end Delay

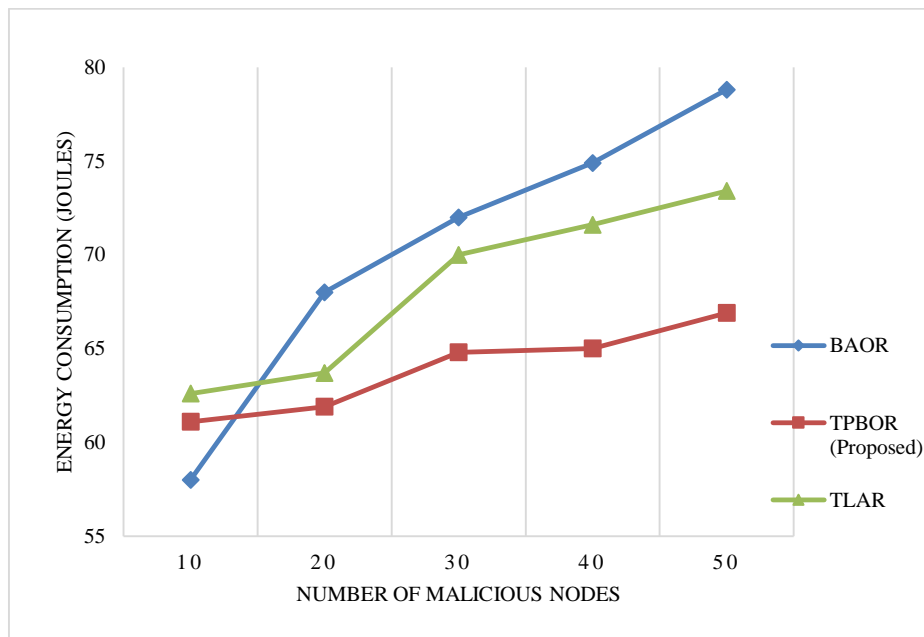


Figure 7.5: Performance on the basis of Total Energy Consumption

In WSN energy consumption is the most important factor to monitor. This will decide on the network lifetime and hence here the performance of all three algorithms has been tested on the basis of average energy consumption. The energy consumption in the network depends on the energy consumed at node's radio for transmitting and receiving packets. The energy consumption of BAOR will be lowest initially because of less overhead and less number of malicious nodes (figure 7.5). But with the increase in a number of malicious nodes, the energy consumption also increases in the network. TPBOR consumes very less energy as compared to BAOR and TLAR in presence of malicious nodes. Because the computation overhead is low and also the trust value distributes the energy consumption among all nodes. Hence, TPBOR turns out to be an energy saver algorithm.

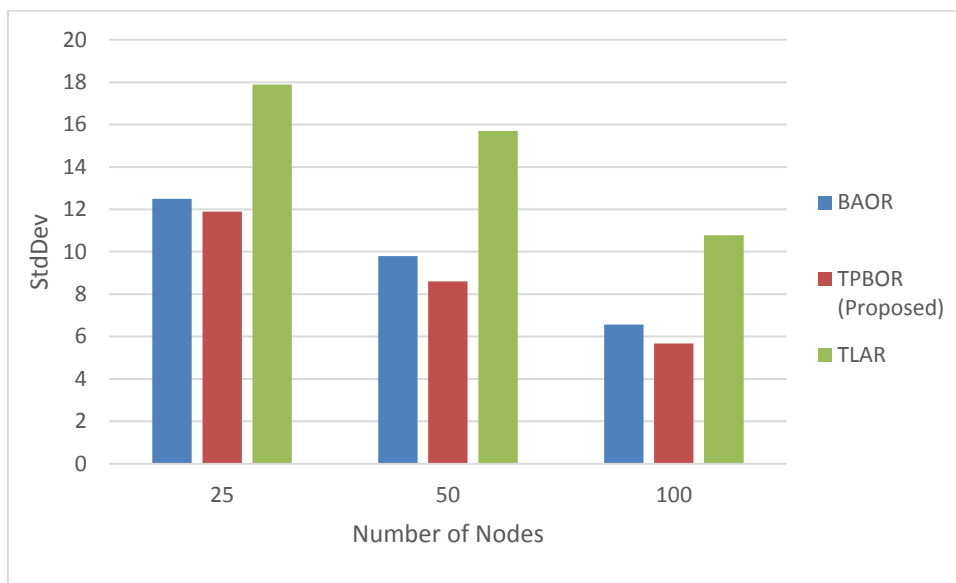


Figure 7.6: Average Number of Packets Transmitted by each Node

Figure 7.6 presents the analysis on the basis of the standard deviation of a number of packets transmitted by each node during the network operation. The formula for standard deviation as presented in [23] is as follows in equation 5.

$$stdDev = \sqrt{\frac{1}{N} \sum_{i=1}^N (n_i - \mu)^2} \dots\dots\dots (5)$$

Where N is total nodes, n_i is the number of packets relayed by node i and μ is the mean number of packets relayed by each node. Proposed protocol TPBOR shows the improvement over BAOR in load balancing. This is because the trust value involved in the routing algorithm avoids the malicious nodes and reduce the number of retransmissions. Also due to the opportunistic behavior of TPBOR number of nodes can participate in routing process and. The

buffer check condition will reduce the delay as well as distribute the packet load equally among all relay nodes. TLAR do not employ any load balancing strategy and it will present a poor standard deviation. Overall, TPBOR presents a good performance as compared to BAOR and TLAR.

7.5 Conclusion and Future Scope of Work

This chapter presented an opportunistic routing protocol for WSN with an added security feature. Trust and reputation based routing protocols help to avoid the malicious nodes on the path. Also, trust management may be used to avoid duplication and unnecessary packet forwarding towards the base station. The proposed protocol TPBOR introduced impact on energy into the trust value so that only energy efficient nodes can take part in the routing process. TPBOR also introduces the relay selection criteria to select the best next-hop to forward data packets. In relay selection criteria queue size of each node has been considered. If a node is loaded with a number of packets than this node will not be included in routing process until it forward some of its packets toward the destination. Hence, each node can transmit its data to the base station without congestion. Also, the trust management reduces the overhead of security and hence it will prolong the network lifetime. The simulation results have shown that TPBOR performs better in presence of malicious nodes in the network. In future directions we can consider more parameters in trust value calculation, but the more the parameters more will be computational overhead. Hence, only those parameters should be considered which are seem to be important in the network like energy, packet delivery etc.

CHAPTER 8

CONCLUSION AND FUTURE SCOPE OF WORK

8.1 Introduction

In this thesis, the routing protocols for WSN were studied and categorized. The primary objectives of the thesis were classified into three categories i) reducing energy consumption during network operations to improve the network lifetime, ii) providing security to route selection process by means of trust and reputation and iii) optimizing the packet load, energy efficiency and security of route selection. Other contributions of thesis involved reducing end-to-end delays and path loss and improving the throughput of the network.

For the first primary objective, one opportunistic routing metric and one opportunistic routing protocol were proposed in Chapter 3 and Chapter 4. The opportunistic routing metric proposed in Chapter 3 was named as Energy Depletion Factor (EDF) which distributes the energy consumption during various network operations, among all the network nodes. This metric was tested by including it in AODV's route selection process. As EDF seems to be working fine with existing routing protocols, in Chapter 4 by using it a novel opportunistic routing protocol was proposed. The proposed protocol tried to optimize the use of resources during various network operations like packet generation, transmission, reception and handling acknowledgments. From these two proposals, it may be concluded that the impact of energy consumption in various network operations is not always the same for all sensor nodes in the network. Therefore, the routing protocol should not always select the same node again and again as a relay node. Also, the distribution of energy consumption among all the nodes is important.

Towards the second objective, one trust-aware opportunistic routing metric and two trust based opportunistic routing protocols were proposed in Chapter 5 and Chapter 6. The trust-aware opportunistic routing metric proposed in Chapter 5 introduced forwarding sincerity, energy depletion and acknowledgment sincerity as trust evaluation parameters. The reason for choosing these parameters is the importance of energy and throughput during the network operations. The proposed trust-aware metric was tested by using DSDV as base protocol. The proposed metric works well and present good simulation results for random deployment of sensor nodes in the specified area. End-to-end delays will be high in this case due to the

overhead of metric calculation. To overcome this problem in Chapter 6 two trust based opportunistic routing protocols were proposed. The first one is the modification of existing MDOR [13] protocol named as modified_MDOR. This protocol introduces only two trust evaluation parameters i.e. packet forwarding ratio and the total energy consumption during network operations. Modified_MDOR reduces the chances of a malicious node to become a next-hop relay node. The malicious nodes were identified on the basis of the consolidated trust value calculated by the source node for each neighbor node. Modified_MDOR is based on the direct trust values with two parameters only. But, to make the reliable delivery of data packets acknowledgments must also be taken into consideration. TAEROR is proposed to include acknowledgment sincerity as trust evaluation factor. Also, the evaluation parameters used in Modified_MDOR were altered to give better results. The performance of TAEROR was compared to existing protocols TLAR [18], TESRP [19] and TLAR [20]. The performance is better as compared using simulations in NS2.

The third objective was to balance the packet transmission load among all the nodes equally. In context to this objective, the overall target is to optimize the packet load among all node, distribute energy consumption load and avoid malicious and selfish nodes during the routing process. For completing this objective one opportunistic routing protocol was proposed in Chapter 7 and named as TPBOR. This protocol utilizes the trust-aware routing metric proposed in Chapter 5 to provide security during route selection process and energy efficiency. To handle the incoming packet load buffer size of each sensor nodes was taken into consideration. Load balancing metric was defined by using the original buffer size and the currently available space inside the buffer. This metric was introduced to balance the load equally among all the sensor nodes so that the packets do not suffer any extra delays in waiting queues. This protocol optimizes the resource utilization and also provide security for the route selection process.

8.2 Comparative Analysis

Overall this thesis presented contributions toward the opportunistic routing as well as routing for wireless sensor networks. There were three trust-aware and resource optimization based protocols proposed in Chapter 6 and Chapter 7. These protocols have certain differences among them. TPBOR protocol presented in Chapter 7 presented the optimized results in terms of packet load, energy efficiency and trust management among all the nodes of the network. The comparative analysis of these three protocols can be seen in table 8.1 below.

From the table 8.1, it can be depicted that the best performer is TPBOR as it optimizes the resource utilization. The risk level of TPBOR is the lowest which means it was able to identify and avoid a number of malicious nodes during the routing process. The energy consumption and end-to-end delay are high in this case. But, as it is reducing the risk level this protocol is more suitable for WSN applications. Modified_MDOR and TAEROR are also good in performance and can be used for various applications where the load balancing is not a primary concern.

Table 8.1: Comparative analysis of Modified_MDOR, TAEROR, and TPBOR

Proposed Protocol	Risk Level	Energy Consumption (Joules)	Packet Delivery Ratio	End-to-End Delay	Load Balancing (StdDev)
Modified_MDOR	4.20	68.71	0.76	0.015	17.91
TAEROR	3.61	67.84	0.82	0.016	10.98
TPBOR	3.56	70.52	0.87	0.021	6.10

8.3 Future Perspectives

Wireless sensor networks are the current hot research area among researchers nowadays. There is a lot of research going on this research area and hence there are much more issues researchers are facing. The research work in this thesis focused only on the routing concepts. Although, there are many more research issues in which authors can work. In future directions, more options can be explored about routing concepts in WSN like deployment, coverage, more trust evaluation parameters etc.

The future directions for WSN may vary from network structure to, application types to application demands. Different applications have different sensitivity factors. Different network designs have different constraints with respect to varying challenges.

- There are different issues at design level of WSN, like node deployment, heterogeneity, localization and synchronization which needs to be explored further.
- There are various protocols already developed for WSNs need to be compared with respect to WSNs application classes.

- Different challenges need to be implemented on different protocols in real scenarios to identify protocols efficiencies.
- Routing protocols need to be evaluated with specific performance metrics with respect to application demands in order to identify protocols suitability for different applications.
- Simulations environment could be improved to support a number of routing protocols and provides additional metrics for protocols evaluation.
- QoS for applications in WSNs needs to be explored and appropriate algorithms need to be developed.

The trust-aware protocols proposed in Chapter 6 and Chapter 7 can further be extended to include the more important parameters and the security of route selection process will be enhanced. These protocols may be enhanced to use the feedbacks of other neighbor nodes which are also called as indirect trust evaluation parameters. Also, different applications of WSN have different sensitivity factors, different network designs have different constraints with respect to varying challenges. There are different issues at design level of WSN, like node deployment, heterogeneity, localization and synchronization which needs to be explored further. There are various protocols already developed for WSNs need to be compared with respect to WSNs application classes.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, 393-422, 2002.
- [2] I. F. Akyildiz, I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad hoc networks*, vol. 2, no. 4, pp. 351-367, 2004.
- [3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad hoc networks*, vol. 3, no. 3, pp. 325-349, 2005.
- [4] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," In Proc. ACM SIGCOMM'05, New York, USA, pp. 133-144, 2005.
- [5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 15, 2008.
- [6] D. S. J. De Couto, D. Aguayo, J. Bicket and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Networks*, vol. 11, no. 4, pp. 419-434, 2005.
- [7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey" *Computer Networks*, vol. 52, no. 12, pp. 2292-2330, 2008.
- [8] M. Michel, S. Duquenooy, B. Quoitin and T. Voigt, "Load-Balanced Data Collection through Opportunistic Routing," In Proc. International Conference on Distributed Computing in Sensor Systems, Fortaleza, pp. 62-70, 2015.
- [9] Mathworks. Global Optimization Toolbox: User's Guide (r2011b). Retrieved November 10, 2015 from www.mathworks.com/help/pdf_doc/gads/gads_tb.pdf.
- [10] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc on-demand distance vector (AODV) routing," No. RFC 3561, 2003.
- [11] VINT Project. The ns Manual - 2011. Retrieved July 12, 2015 from https://www.isi.edu/nsnam/ns/doc/ns_doc.pdf.
- [12] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," In Proc. ACM SIGCOMM computer communication review, New York, USA, pp. 234-244, 1994

- [13] M. Sharma and Y. Singh, "Middle Position Dynamic Energy Opportunistic Routing for Wireless Sensor Networks," In Proc. IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 948-953, 2015.
- [14] C. C. Hung, K. C. J. Lin, C. C. Hsu, C. F. Chou and C. J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," In Proc. 19th International Conference on Computer Communications and Networks (ICCCN), Zurich, pp. 1-6, 2010.
- [15] X. Mao, S. Tang, X. Xu, X. Y. Li, and H. Ma, "Energy-efficient opportunistic routing in wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 22, no. 11, pp. 1934-1942, 2011.
- [16] Z. Zhang, S. Wen, W. Yang and F. Zhao, "Energy-efficient Opportunistic Routing Protocol in Wireless Sensor Networks," *Applied Mechanics & Materials*, vol. 610, pp. 797-807, 2014.
- [17] A. Tiab, L. Bouallouche-Medjkoune and S. Boulfekhar, "A new QoS aware and energy efficient opportunistic routing protocol for wireless sensor networks," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 33, no. 1, 52-68, 2017.
- [18] P. R. Vamsi and K. Kant, "Trust and Location-Aware Routing Protocol for Wireless Sensor Networks," *IETE Journal of Research*, vol. 63, pp. 1-11, 2016.
- [19] A. Ahmed, K. A. Bakar, M. I. Channa and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Networks and Applications*, vol. 21, no. 2, pp. 272-285, 2016.
- [20] M. Salehi and A. Boukerche, "Trust-aware opportunistic routing protocol for wireless networks," In Proc. 10th ACM symposium on QoS and security for wireless and mobile networks, pp. 79-86, 2014.
- [21] W. W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*. Wiley, A John Wiley and Sons Ltd. Publication, 2010.
- [22] S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," In Proc. 6th ACM SIGMOBILE Mobile Computing and Communications Review, pp. 28-36, 2002.

- [23] L. Subramanian and R. H. Katz, "An architecture for building self-configurable systems," In Proc. First ACM/IEEE Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC), Boston, MA, 2000.
- [24] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," In Proc. 33rd Annual Hawaii International Conference on System Sciences, Hawaii, 2000.
- [25] K. Sohrabi, J. Gao, V. Ailawadhi and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Transaction on Personal Communications*, vol. 7, no. 5, pp. 16-27, 2000.
- [26] W. R. Heinzelman, J. Kulik and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," In Proc. 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom'99), Seattle, WA, 1999.
- [27] S. M. Hedetniemi, S. T. Hedetniemi and A. L. Liestman, "A survey of gossiping and broadcasting in communication networks," *Networks*, vol. 18, no. 4, pp. 319-349, 1988.
- [28] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," In Proc. 6th annual international conference on Mobile computing and networking, Boston, 2000.
- [29] B. Krishnamachari, D. Estrin and S. Wicker, "The impact of data aggregation in wireless sensor networks," In Proc. 22nd International Conference on Distributed Computing Systems Workshops, 2002.
- [30] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," In Proc. IEEE Wireless Communications and Networking Conference, Orlando, FL, 2002.
- [31] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," In Proc. 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, 2002.
- [32] R. V. Biradar, S. R. Sawant, R. R. Mudholkar and V. C. Patil, "Multihop routing in self-organizing wireless sensor networks," *IJCSI International Journal of Computer Science*, vol. 8, no. 1, 155-164, 2011.

- [33] W. Xinhua and W. Sheng, "Performance comparison of LEACH and LEACH-C protocols by NS2," In Proc. Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), Hong-Kong, China, 2010.
- [34] V. Kumar, S. Jain and S. Tiwari, "Energy efficient clustering algorithms in wireless sensor networks: A survey," *IJCSI International Journal of Computer Science*, vol. 8, no. 5, 2011.
- [35] B. Manzoor, N. Javaid, O. Rehman, M. Akbar, Q. Nadeem and A. Iqbal, "Q-LEACH: A new routing protocol for WSNs," *Procedia Computer Science*, vol. 19, pp. 926-931, 2013.
- [36] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," In Proc. IEEE Aerospace conference proceedings, Big Sky, Motana, 2002.
- [37] L. Stehpanie, C. S. Raghavendra and M. S. Krishna, "Data Gathering in Sensor Networks using the Energy Delay Metric," In Proc. 15th International Symposium on Parallel & Distributed Processing, 2001.
- [38] A. Manjeshwar and D. P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In Proc. 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Fransisco, CA, 2001.
- [39] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333-1344, 1999.
- [40] Y. Xu, J. Heidemann and D. Estrin, "Geography-informed energy conservation for ad hoc routing," In Proc. 7th Annual ACM International Conference on Mobile computing and networking (MobiCom'01), Rome, Italy, 2001.
- [41] C. Jae-Hwan and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 4, pp. 609-619, 2004.
- [42] K. Akkaya and M. Younis, "An energy-aware QoS routing protocol for wireless sensor networks," In Proc. 23rd International Conference on Distributed Computing Systems Workshops, Rhode Island, 2003.
- [43] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, "Section 24.3: Dijkstra's algorithm," *Introduction to Algorithms* (Second ed.), MIT Press and McGraw-Hill. pp. 595-601, 2001. ISBN: 0-262-03293-7.

- [44] C. R. Yamuna Devi, B. Shivaraj, S. S. Iyengar, S. H. Manjula, K. R. Venugopal and L. M. Patnaik, "Multi-hop optimal position based opportunistic routing for wireless sensor networks," In Proc. IEEE Region 10 Symposium, 2014.
- [45] A. Boukerche and A. Darehshoorzadeh, "Opportunistic routing in wireless networks: Models, algorithms, and classifications," *ACM Computing Surveys*, vol. 47, no. 2, pp. 22, 2015.
- [46] M. Younis, M. Youssef and K. Arisha, "Energy-aware routing in cluster-based sensor networks," In Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS), Fort Worth, TX, 2002.
- [47] M. Chu, H. Haussecker and F. Zhao, "Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks," *International Journal of High Performance Computing Applications*, vol. 16, no. 3, pp. 293-313, 2002.
- [48] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," *ACM SIGMOD Record*, vol. 31, no. 3, pp. 9-18, 2002.
- [49] N. Sadagopan, B. Krishnamachari and A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks," In Proc. First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.
- [50] N. Jianwei, C. Long, G. Yu, S. Lei, and S. K. Das, "R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 784-794, 2013. DOI:10.1109/tii.2013.2261082
- [51] Y. Yu, R. Govindan and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," Retrieved from UCLA Computer Science Department (ucla/csd-tr-01-0023), 2001.
- [52] J.-H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," In Proc. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE, 2000), Tel Aviv, Israel, pp. 22-31, 2000.
- [53] K. Dasgupta, K. Kalpakis and P. Namjoshi, "An efficient clustering-based heuristic for data gathering and aggregation in sensor networks," *Wireless Communications and Networking*, vol. 3, pp. 1948-1953, 2003.

- [54] T. He, J. Stankovic, C. Lu and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks," In Proc. 23rd International Conference on Distributed Computing Systems, 2003.
- [55] J. Zhang, F. Ren, S. Gao, H. Yang, and C. Lin, "Dynamic routing for data integrity and delay differentiated services in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 2, pp. 328-343, 2015.
- [56] J. Kim and B. Ravindran, "Opportunistic real-time routing in multi-hop wireless sensor networks," In Proc. ACM symposium on Applied Computing, 2009.
- [57] O. Landsiedel, E. Ghadimi, S. Duquennoy and M. Johansson, "Low power, low delay: opportunistic routing meets duty cycling," In Proc. ACM/IEEE 11th International Conference on Information Processing in Sensor Networks (IPSN), 2012.
- [58] B. I. Wenning, A. Lukosius, A. Timm-Giel, C. Gorg and S. Tomic, "Opportunistic distance-aware routing in multi-sink mobile wireless sensor networks," In Proc. ICT mobile summit, 2008.
- [59] K. Zeng, W. Lou and H. Zhai, "On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks," In Proc. 27th Conference on Computer Communications, IEEE (INFOCOM '08), Phoenix, Ariz, USA, 2008.
- [60] Y. Li, Y. A. Liu, and P. Luo, "Link probability based opportunistic routing metric in wireless network," In Proc. WRI International Conference on Communications and Mobile Computing (CMC'09), 2009.
- [61] P. Spachos, P. Chatzimisios and D. Hatzinakos, "Energy aware opportunistic routing in wireless sensor networks," In Proc. IEEE GLOBECOM Workshops (GC Workshops), 2012.
- [62] L. Cheng, J. Niu, J. Cao, S. K. Das and Y. Gu, "Qos aware geographic opportunistic routing in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1864-1875, 2014.
- [63] M. Cattani, M. Zuniga, M. Woehrle and K. Langendoen, "SOFA: Communication in Extreme Wireless Sensor Networks," *Wireless Sensor Networks*, vol. 83, no. 54, pp. 100-115, 2014.

- [64] C. Lyu, D. Gu, X. Zhang, S. Sun, Y. Zhang and A. Pande, "SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs," *Computer Communications*, vol. 59, pp. 37-51, 2015.
- [65] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure Routing based on Social Similarity in Opportunistic Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 594-605, 2016.
- [66] Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," In Proc. International Conference on Mobile Ad Hoc and Sensor Systems (IEEE), Vancouver, BC, pp. 437-446, 2006.
- [67] Y. Zhou, X. Tan, X. He, G. Qin, and H. Xi, "Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature," *Information Assurance and Security Letters*, pp. 18-23, 2010.
- [68] W. Cui, Y. Yao and L. Song, "Buffer-aware opportunistic routing for wireless sensor networks," In Proc. 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, pp. 268-271, 2017.
- [69] Z. Liu, C. Wei, C. Qin, H. Li, X. Niu and L. Wang, "POR: A Packet-Based Opportunistic Routing Protocol for Wireless Sensor Networks," In Proc. International Conference on Computer Sciences and Applications, Wuhan, pp. 158-162, 2013.
- [70] B. A. Bakr, and L. Lilien, "Extending Wireless Sensor Network Lifetime in the LEACH-SM Protocol by Spare Selection," In Proc. Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011.
- [71] Ian. Poole, "Free Space Path Loss: Details, Formula, Calculator," <https://www.radioelectronics.com>, Adrio Communications Ltd. Retrieved 18 July 2016.
- [72] M. Busse, T. Haenselmann and W. Effelsberg, "A lifetime-efficient forwarding strategy for wireless sensor networks," *Wireless Sensor Network*, [Poster Abstract], 2006.
- [73] M. Busse, T. Haenselmann and W. Effelsberg, "An Energy-Efficient Forwarding Scheme for Wireless Sensor Networks," In Proc. WOWMOM'06, IEEE Computer Society, Washington, DC, USA, pp. 125-133, 2005.
- [74] Q. Cao, T. He, L. Fang, T. F. Abdelzaher, J. A. Stankovic and S. H. Son, "Efficiency Centric Communication Model for Wireless Sensor Networks," In Proc. 25th IEEE INFOCOM, Barcelona, Spain, pp. 1-12, 2006.

- [75] Z. Zhong, J. Wang, S. Nelakuditi, G. H. Lu, "On selection of candidates for opportunistic anypath forwarding," In Proc. 10th ACM SIGMOBILE, University of South Carolina, Columbia, SC, pp. 1-2, 2006.
- [76] C.E. Koksal and H. Balakrishnan, "Quality-aware routing metrics for time-varying wireless mesh networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 11, pp. 1984-1994, 2006.
- [77] R. Draves, J. Padhye, B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," In Proc. 10th annual international conference on Mobile computing and networking, Microsoft Research Redmond, WA, pp. 114-128, 2004.
- [78] J. C. Park and S. K. Kasera, "Expected data rate: an accurate high-throughput path metric for multi-hop wireless routing," In Proc. 2nd IEEE SECON'05, Santa Clara, CA, pp. 218-228, 2005.
- [79] K. Zeng, W. Lou, J. Yang, I. D. R. Brown, "On throughput efficiency of geographic opportunistic routing in multihop wireless networks," *Mobile Networks and Applications*, vol. 12, no. 5-6, pp. 347-357, 2007.
- [80] C. J. Hsu, H. I. Liu and W. K. G. Seah, "Opportunistic routing: A review and the challenges ahead," *Computer Networks*, vol. 55, no. 15, pp. 3592-3603, 2011.
- [81] D. Chiarotto, O. Simeone, M. Zorzi, "Spectrum leasing via cooperative opportunistic routing techniques," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 2960-2970, 2011.
- [82] X. Mao, S. Tang, X. Xu, X-Y. Li, H. Ma, "Energy-efficient opportunistic routing in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 11, pp. 1934-1942, 2011.
- [83] H. Dubois-Ferriere, M. Grossglauser, M. Vetterli, "Valuable detours: Least-cost anypath routing," *IEEE/ACM Transactions on Networking*, vol. 19, no. 2, pp. 333-46, 2011.
- [84] E. Rozner, J. Seshadri, Y. A. Mehta, L. Qiu, "SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 12, pp. 1622-1635, 2009.
- [85] C. Wei, C. Zhi, P. Fan and K. Ben Letaief, "AsOR: an energy efficient multi-hop opportunistic routing protocol for wireless sensor networks over Rayleigh fading

- channels,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2452-2463, 2009.
- [86] J. Wu, M. Lu and F. Li, “Utility-based opportunistic routing in multi-hop wireless networks,” In Proc. 28th International Conference on Distributed Computing Systems ICDCS'08, Beijing, pp. 470-477, 2008.
- [87] V. Mohindru and Y. Singh, “Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack,” *Indian Journal of Science and Technology*, vol. 9, no. 32, pp. 8-15, 2016.
- [88] N. Kumar and Y. Singh, “An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks,” *Indian Journal of Science and Technology*, vol. 9, no. 32, pp. 1-7, 2016.
- [89] D. Hui-hui, G. Ya-jun, Y. Zhong-qiang, and C. Hao, “A wireless sensor networks based on multi-angle trust of node,” In Proc. International Forum on Information Technology and Applications (IEEE, 2009), Chengdu, China, pp. 28-31, 2009.
- [90] Q. He, D. Wu and P. Khosla, “SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks,” In Proc. IEEE Wireless communications and networking conference (WCNC'04), 2004.
- [91] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation,” In Proc. Springer Mobile Ad-hoc Networks Advanced communications and multimedia security, pp. 107-121, 2002.
- [92] M. Salehi, A. Boukerche, A. Darehshoorzadeh and A. Mammeri, “Towards a novel trust-based opportunistic routing protocol for wireless networks,” *Wireless Networks*, vol. 22, no. 3, pp. 927-943, 2016.
- [93] H. Deng, Y. Yang, G. Jin, R. Xu and W. Shi, “Building a trust-aware dynamic routing solution for wireless sensor networks,” In Proc. IEEE GLOBECOM Workshops, Miami, Florida, USA, pp. 153-157, 2010.
- [94] I. Maarouf, U. Baroudi, and A. R. Naseer, “Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks,” *IET communications*, vol. 3, no. 5, pp. 846-858, 2009.

- [95] P. Gong, T. M. Chen and Q. Xu, "ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, p. 10, 2015. DOI:10.1155/2015/469793.
- [96] A. Adnan, B. Kamalrulnizam Abu, C. Muhammad Ibrahim and K. Abdul Waheed, "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network," *Mob. Netw. Appl.*, vol. 21, no. 2, pp. 272-285, 2016.
- [97] N. Kumar and Y. Singh, "Routing protocols in wireless sensor networks," *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, pp. 86-128, 2017.
- [98] K. Liu, N. Abu-Ghazaleh and K. D. Kang, "Location verification and trust management for resilient geographic routing," *Journal of Parallel and Distributed Computing*, vol. 67, no. 2, pp. 215-228, 2007.
- [99] E. Abdellah, S. Benalla, A. B. Hssane and M. L. Hasnaoui, "Advanced low energy adaptive clustering hierarchy," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 2, no. 7, pp. 2491-2497, 2010.
- [100] S. K. Baji Baba, K. R. R. Mohan Rao, "Improving the Network Life Time of a Wireless Sensor Network using the Integration of Progressive Sleep Scheduling Algorithm with Opportunistic Routing Protocol," *Indian Journal of Science and technology*, vol. 9, no. 17, pp. 1-6, 2016.
- [101] P. Bonnet, J. Gehrke and P. Seshadri, "Querying the physical world," *Personal Communications*, vol. 7, no. 5, pp. 10-15, 2000.
- [102] M. I. Channa and K. M. Ahmed, "A Reliable Routing Scheme for Post-Disaster Ad Hoc Communication Networks," *Journal of Communication*, vol. 6, no. 7, 549-557, 2011.
- [103] O. Chipara, Z. He, G. Xing, Q. Chen, X. Wang and C. Lu, "Real-time power-aware routing in sensor networks," In Proc. 14th IEEE International Workshop on Quality of Service, New Haven, CT, pp. 83-92, 2006.
- [104] S. Choudhury, S. D. Roy and S. A. Singh, "Trust management in ad hoc network for secure DSR routing," *Novel algorithms and techniques in telecommunications, automation and industrial electronics*, pp. 495-500, 2008.

- [105]J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electron Notes Theory Computer Science*, vol. 197, no. 2, pp. 131–140, 2008.
- [106]A. Darehshoorzadeh and L. Cerda-Alabern, "Distance progress based opportunistic routing for wireless mesh networks" In Proc. 8th International Wireless Communications and Mobile Computing Conference (IWCMC), 2012.
- [107]S. C. Ergen, P. Varaiya, "PEDAMACS: Power efficient and delay aware medium access protocol for sensor networks" *IEEE Transactions Mobile Computing*, vol. 5, no. 7, pp. 920-930, 2006.
- [108]K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279-298, 2012.
- [109]M. Haque, A. S. K. Pathan, C. S. Hong and E. N. Huh, "An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks," *KSII Transactions on Internet & Information Systems*, vol. 2, no. 5, 2008.
- [110]Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21-38, 2005.
- [111]N. Kumar, and Y. Singh, "An energy efficient and trust management based opportunistic routing metric for wireless sensor networks," Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Wagnaghat, pp. 611-616, 2016.
- [112]N. Mantas, M. Louta, E. Karapistoli, G. T. Karetsos, S. Kraounakis and M. S. Obaidat, "Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey," *IET Networks*, 2017.
- [113]A. Mohaisen, J. W. Choi, and D. Hong, "On the insecurity of asymmetric key-based architecture in wireless sensor networks. *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 3, no. 4, pp. 376-384, 2009.
- [114]M. Naghshvar, T. Javidi, "Opportunistic routing with congestion diversity in wireless multi-hop networks," In Proc. IEEE INFOCOM'10, San Diego, CA, pp. 1-5, 2010.
- [115]J. M. Rabaey, M. J. Ammer, J. L. da Silva, D. Patel and S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking," *Computer*, vol. 33, no. 7, pp. 42-48, 2000.

- [116]K. Romer, "Tracking real-world phenomena with smart dust," In Proc. 1st European Workshop on Wireless Sensor Networks, Berlin, Germany, 2004.
- [117]R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee and Y. J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 20, no. 11, pp. 1698-1712, 2009.
- [118]J. Wang, J. U. Kim, L. Shu, Y. Niu and S. Lee, "A distance-based energy aware routing algorithm for wireless sensor networks," *Sensors*, vol. 10, no. 10, pp. 9493-9511, 2010.
- [119]S. Wen, Z. Zhang, W. Yang and S. Hou, "An Energy-efficient Opportunistic Multicast Routing Protocol in Mobile Wireless Sensor Networks," *Journal of Networks*, vol. 9, no. 7, pp. 1819-1827, 2014. DOI:10.4304/jnw.9.7.1819-1827
- [120]T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless personal communications*, vol. 69, no. 2, pp. 805-826, 2013.

Appendix-A

Authors' Publications

1. **N. Kumar** and Y. Singh, "Routing Protocols in Wireless Sensor Networks," *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, Hershey, PA, USA: IGI Global, pp. 86-128, 2016. DOI: 10.4018/978-1-5225-0486-3.ch004.
2. **N. Kumar** and Y. Singh, "An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks," *Indian Journal of Science and Technology*, vol. 9, no. 32, August, p. 7, 2016, DOI:10.17485/ijst/2016/v9i32 /100197.
3. **N. Kumar** and Y. Singh, "An energy efficient and trust management based opportunistic routing metric for wireless sensor networks," In Proc. Fourth IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2016), Wagnaghat, India, 2016, pp. 611-616, DOI:10.1109/PDGC.2016.7913196.
4. **N. Kumar**, Y. Singh and P. Kr. Singh, "Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Network," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-6, pp. 29-33, 2017.
5. **N. Kumar**, Y. Singh and P. Kr. Singh, "An Energy Efficient Trust-Aware Opportunistic Routing Protocol for Wireless Sensor Network," *International Journal of Information System Modeling and Design (IJISMD)*, vol. 8, no. 2, pp. 30-44, 2017 DOI:10.4018/IJISMD.2017040102.
6. **N. Kumar** and Y. Singh, "Trust and packet load balancing based Secure Opportunistic Routing Protocol for WSN," In Proc. 4th IEEE International Conference on Signal Processing, Computing and Control (ISPCC- 2017), Wagnaghat, India, 2017, pp. 463-467, DOI:10.1109/ISPCC.2017. 8269723.

Communicated Paper(s)

7. **N. Kumar** and Y. Singh, "Reducing Energy Consumption and Duplication of packets in WSN: Opportunistic Routing Perspective," *Informatica, An International Journal of Computing and Informatics*.
8. **N. Kumar** and Y. Singh, "Energy Efficient and Packet Load Balancing based OR protocol for WSN," *IETE Journal of Research*.

Appendix B
Research Papers

Chapter 4

Routing Protocols in Wireless Sensor Networks

Nagesh Kumar

Jaypee University of Information Technology, India

Yashwant Singh

Jaypee University of Information Technology, India

ABSTRACT

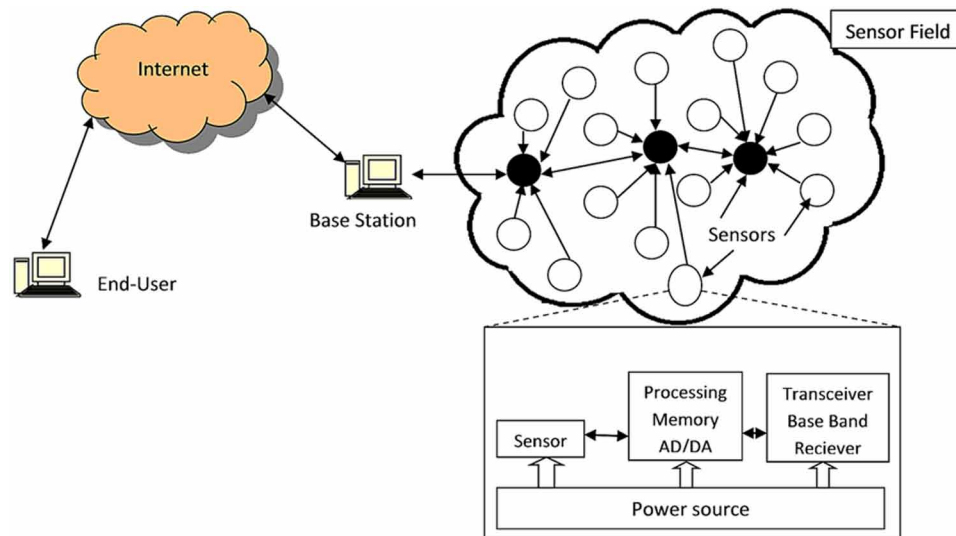
In Wireless Sensor Network (WSN), the routing protocols have been given attention because most of the routing protocols are application and architecture dependent. This chapter presents routing protocols for wireless sensor networks and also classifies routing in WSN. Chapter gives five main classifications of routing protocols in WSN which are data-centric, hierarchical, location-based, network flow and QoS aware and opportunistic routing protocols. The focus has been given on advancement of routing in WSN in form of opportunistic routing, in which the sensor nodes utilize broadcasting nature of wireless links and the data packets can be transmitted through different paths. The routing protocols for WSN are described and discussed under the appropriate classification. A table of comparison of routing protocols on the basis of power usage, data aggregation, scalability, query basis, overhead, data delivery model and QoS parameters has been presented.

INTRODUCTION

The recent advancements in the micro-electro-mechanical systems (MEMS) technology, communication techniques in wireless networks and nanotechnology give arise to develop small sensor nodes that are low-cost multifunctional energy constrained devices (Akkaya & Younis, 2005; Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). These nodes can communicate over radio frequencies in small distances. The sensors constitute sensing, data processing and communicating hardware and software components. *Wireless Sensor networks* (WSN) are the dense collection of such sensors. The WSNs gather and communicate the physical or chemical data to monitor and control physical or chemical environments from remote stations with accuracy.

DOI: 10.4018/978-1-5225-0486-3.ch004

Figure 1. Wireless sensor network example



In most of the applications the position of the sensors need not to be engineered or pre-determined and this allows the distribution of the sensor nodes randomly. The WSN left unattended in most of the applications for long time. Hence, the protocols designed for WSN must contain the self-organizing capabilities. Rather than sending only raw data the sensor nodes should also be capable of carrying out some simple computations on raw data and transmit only the useful data towards the sink/base station.

Networking the unattended densely scattered sensor nodes has significant impact on many applications like disaster management, security, battle field surveillance (Dargie & Poellabauer, 2010). Routing WSN is very challenging task because WSNs are having different characteristics than conventional networks. First of all, as the sensor nodes are randomly deployed, global addressing is not possible. Hence, the user cannot apply classical IP-based protocols to WSNs. Second, the sensor nodes are constrained with respect to energy, transmission power, processing capacity, and storage capacity and therefore require resource management. Third, in contrast to classical communication in networks, the communications in WSN always require the flow of data from multiple sensor nodes (sources) towards the sink/base stations (Figure 1). Fourth, the data gathered from different regions in WSN have significant redundancy because multiple sensor nodes can generate the same data within particular area of deployment. Due to these types of differences, to solve the problem of data routing in WSN many algorithms has been proposed till date. These algorithms consider almost every characteristic of WSN. The sensor nodes organize themselves to form different topologies for communication which are discussed in the following section along with communication framework.

The organization of chapter is as follows. Rest of this section will briefly summarize the communication in WSN and classification of routing protocols in WSN. In the Section 2, various design issues for routing protocols in WSNs are covered. Section 3 summarizes all types of routing protocols available under different classifications like Data centric, hierarchical, location based, Network flow and QoS, and opportunistic routing. Section 4 concludes the chapter with comparison tables of the studied routing algorithms and points out the good approach for routing in WSN.

Communication in WSN

The network layer's main responsibility is to setup routes from sources (sensor nodes) towards sink/base-stations (gateway nodes/processing nodes). Almost all types of routing algorithms based on two kinds of network topologies which are shown in Figure 2. Figure 2, shows the Single-hop communication topology, in which every sensor node is capable of transmitting data to the sink node directly. This is the simplest approach where the data transferred reached directly the destination. But in practice this approach is not reliable and sometimes impossible therefore, another topology is used which is known as the multi-hop communication as shown in Figure 3. In this type of communication, the task of the network layer on each sensor node is to decide the route towards destination through multiple relays. The sender node act as source, sink as destination and the in between sensor nodes act as relays. This type of communication topology is little bit challenging to setup within the resource constrained WSNs. As WSNs are dynamic in nature, hence, the routing protocols must adapt the changes in the network.

1. **Topologies:** The developments in technology of WSNs give arise to the deployment of sensor nodes in any traditional topologies. The sensor nodes in a wireless sensor network are deployed randomly and this random deployment of sensor nodes have taken traditional network topologies in new directions. Sensor applications in today's world require the networking protocols which can reduce the complexity of the networking and also reduce the cost of routing, but it should increase the reliability of the network. This subsection describes basic types of WSN topologies.
 - a. **Single-Hop Star:** In this type of topology each node communicates directly with the gateway node/sink node/base station. This is the simplest technique among communication topologies. But there is no guarantee of packet delivery. Scalability and robustness of this topology is very poor. Figure 2 depict this type of communication topology.
 - b. **Multi-Hop Mesh and Grid:** This type of topology is designed for covering the large areas of sensor networks. These are also known as the multi-hop communication topologies. In this type of topology the sensor nodes transmit the data packets from sensor to sensor until these data packets reach the destination (gateway/sink/base station). These topologies need

Figure 2. Single-hop communication model

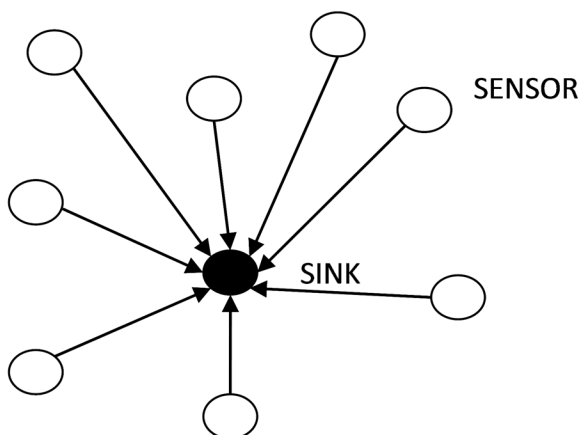
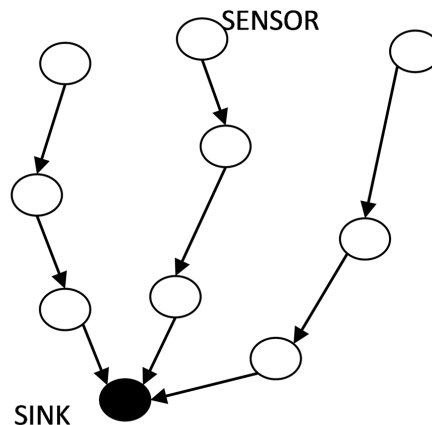


Figure 3. Multi-hop communication model



some routing algorithms to decide the next-hop in the communication. Figure 4 and Figure 5 shows the examples of these topologies.

- c. **Two-Tier Hierarchical Cluster:** In this type of topology the entire network is divided into regions, which will constitute of specific nodes. The sensor nodes in a particular region will report their data to a cluster head. After receiving the data the cluster head perform some data aggregation and fusion operations on the data. Now each cluster head forms a network with other cluster heads which are covering some other regions. The network of clusters can be interlaced more and more means the tier two clusters can send their data to a new cluster head which is covering all tier two cluster heads. In this way the data is finally sent to the gateway/sink/base station. Figure 6 depicts this type of topology.

Classification of Routing Protocols

Routing Protocols has been classified by many authors in many different ways. Figure 7 shows the classification which is based on the network structure or organization, the process of route discovery, the operation of routing protocol, and the advanced routing protocols based on opportunistic route selection.

- 1. **Network Organization:** Network Organization classifies the routing protocols for WSN into three classes:
 - a. Flat-based routing protocols assume that all sensor nodes are having equal functionality or role,
 - b. Hierarchical-based routing protocols assume that different sensor nodes may perform different tasks in the routing process, that is, some nodes may act as only forwarder of data received

Figure 4. Mesh topology

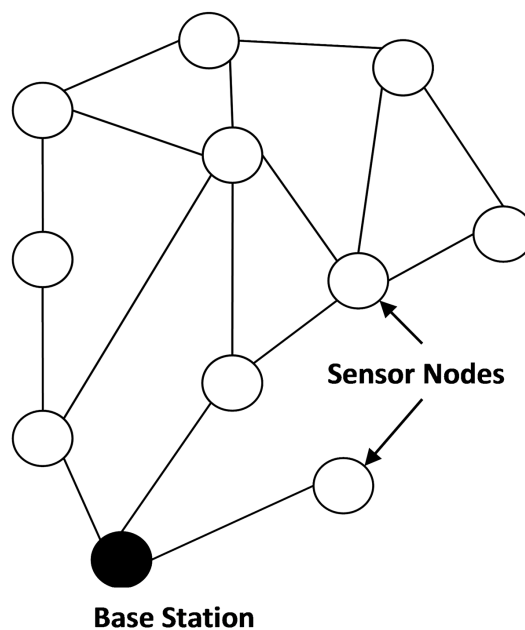


Figure 5. Grid topology

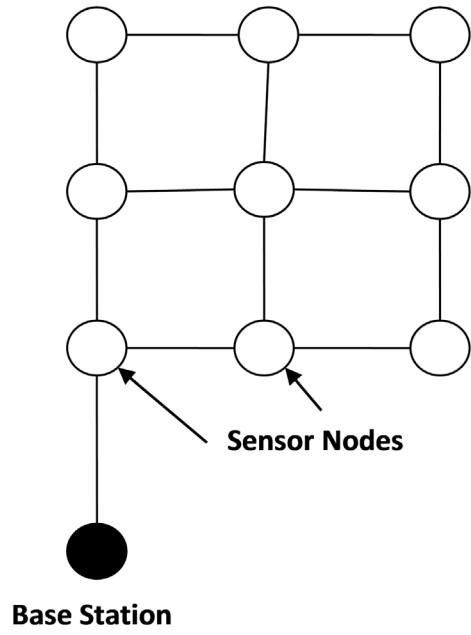


Figure 6. Two-tier hierarchical cluster topology

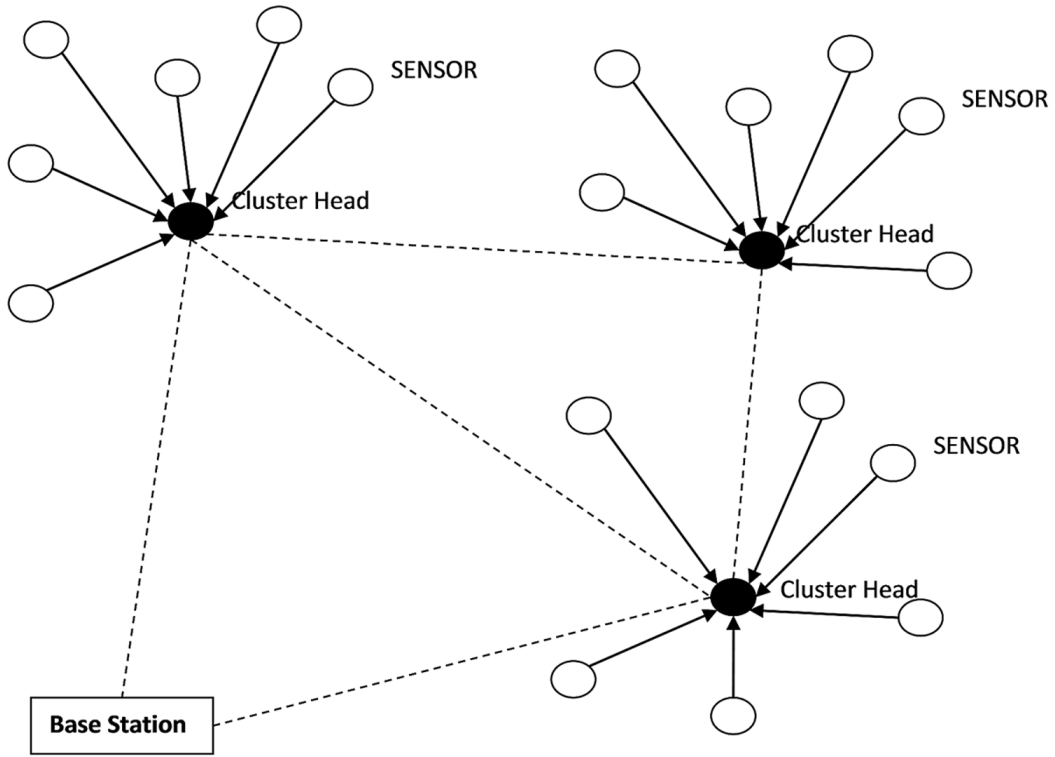
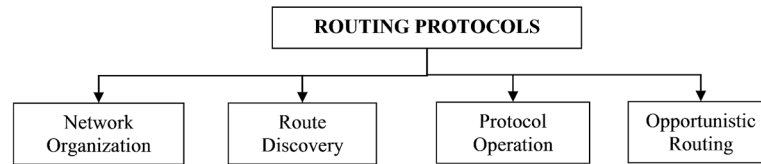


Figure 7. Classification of routing protocols for WSN



from other nodes, while other sensor nodes generate and propagate the sensed data on their own, and

- c. In Location-based routing protocols the routing decisions rely on the location information from sensor nodes.
2. **Route Discovery Process:** The responsibility of the routing protocols is to identify or discover the routes from a source or sender to specified receiver. The route discovery process may be different for different routing protocols, and hence used to differentiate between routing protocols. First are the reactive protocols which establish the routes only when a source node tries to send data towards a receiver. In other words, it is called as *on-demand* route discovery. Hence, the working of these protocols causes delays in transmission. On the other hand, the second type of protocols that is, proactive routing protocols finds and store the routes before they needed. These types of routing protocols are *table-driven*, because the routing information is stored in the routing table, which is local to each sensor. The routing table on each sensor node contains a list of destinations addresses in combination with one or more next-hop neighbor sensor nodes that further lead towards the destinations. The proactive routing protocols solve the problem of route discovery delays but they may introduce overhead by storing such routes which may never be used in the routing process ever.
3. **Protocol Operation:** The operations of routing protocols are also different. Hence one can classify the routing protocols based on their operation, like, some routing protocols reduce redundant data transmissions by exchanging messages between neighboring sensor nodes before actual data transfers occur. Some other protocols use multiple paths simultaneously for better fault tolerance and better performance. There are some other routing protocols which are receiver-initiated, that is, the destination node (base station) when in the need of some data it throws a query towards the sensor nodes and the sensor nodes in response provide the data.

There are QoS-based routing protocols also in which certain parameters need to be satisfied which are QoS metrics, like low latency, low energy consumption, or low packet loss etc. Finally, some protocols are also differing in the way they support in-network data processing. Like the Coherent-based protocols supports only a minimum amount of data processing before sending the data. On the other hand, the non-coherent-based protocols allow the sensor nodes to perform significant local processing of the raw data before it to other nodes for further processing.

4. **Opportunistic Based Routing:** Opportunistic Routing differ from traditional routing protocols in the sense that it selects the route at transmission time only. These types of algorithms utilize the broadcast nature of the wireless networks that is, instead of selecting a predetermined path for transmission, Opportunistic routing broadcasts a data packet to a set of neighboring nodes. Then,

neighbor nodes, which are receiving the data packet successfully, run a coordination algorithm to select the best relay node to forward the data packet. In other words, the opportunistic routing protocols work in following three steps:

- a. Broadcast a data packet to neighbor nodes.
- b. Select the best neighbor as relay node by using a coordination algorithm.
- c. Forward the data packet from that relay node towards destination.

The advantages of opportunistic routing:

- **Reliability:** Opportunistic Routing algorithms can transmit data packet through any possible route rather than a fixed path. It reduces the failure in transmission as well as the transmission delays. A simulation in (Biswas & Morris, 2005) has also proven that Opportunistic Routing protocols outperform the conventional routing protocols when loss rates of routes are high. Hence it increases the reliability of the network.
- **Transmission Range:** Opportunistic Routing increases the transmission range by considering all possible routes, which include good quality routes (short-range) and poor quality routes (long-range), within a single transmission; hence, a data packet may directly jump to the farthest relay node which receives the data packet successfully. As a result, the performance improved. The theoretical analysis was presented in (Akkaya & Younis, 2005). The experimental analysis was presented in (Min et al., 2001; Rabaey, Ammer, da Silva, Patel, & Roundy, 2000). These analyses have shown that opportunistic routing has the ability to increase the performance of the network by using the long-range transmissions also.

DESIGN ISSUES FOR ROUTING PROTOCOLS IN WSN

The operations of routing protocols depend on application areas of WSN. There are different goals and issues which have to be considered to achieve best performance from the network. Also the routing protocol performance is directly related to the architectural model of the Wireless Sensor Network. This section describes such issues and impact of the routing protocols on architecture of WSN.

Network Parameters

Almost all types of Wireless sensor network architectures assume that all the sensor nodes are stationary objects. There are few setups that also use the mobile sensors (Tilak, Abu-Ghazaleh, & Heinzelman, 2002). On the other hand, it is sometimes necessary that support the mobility of sink nodes or cluster-heads (Lakshminarayanan Subramanian & Randy H. Katz, 2000). So in these mobile nodes the routing becomes challenging task. The route stability becomes the biggest optimization factor in addition to energy, bandwidth etc. Also as presented in (Tilak et al., 2002) the sensed event can also be dynamic or static depending on the application. For example, in forest fire detection application the event is static. While in a moving target detection/tracking application, the event is dynamic. When the events are static the reactive routing protocols can be used efficiently by generating traffic when needed. In Dynamic events the topology may be changed in most of the applications which requires changing the route periodically.

Node Deployment

Node deployment is another factor to be considered which affect the performance of the routing protocols. This is totally application dependent factor. Node deployment can be either deterministic or self-organizing. In deterministic, one can place sensor nodes manually and the routes in the network are predetermined. While in self-organizing, the nodes are scattered/distributed randomly in the application area and the nodes organize them to form some topology and finds the routes. (W. R. Heinzelman, Chandrakasan, & Balakrishnan, 2000; Sohrabi, Gao, Ailawadhi, & Pottie, 2000). The clustering becomes an important issue when the distribution of the sensor nodes is not uniform.

Energy Consumption without Losing Accuracy

Each data transmission consumes a significant amount of energy and energy is the scarcest resource in the wireless sensor networks. The transmission power of any radio transmitter is proportional to the distance squared or it can be higher if there is presence of some obstacles in the path. Also, multi-hop routing uses less energy than single-hop routing. But multi-hop routing introduces overhead of topology maintenance. The single-hop routing is very efficient if the sensor nodes and the cluster heads/sinks are very close to each other (W. R. Heinzelman et al., 2000).

Data Reporting Model

The data reporting models have been presented in (Sohrabi et al., 2000) which are totally application dependent. The authors divided the data delivery models in following categories: continuous, event-driven, query driven and hybrid. In the continuous data delivery model, the sensor nodes can be active every time and sends data continuously or there can be some time interval has been defined by the base station for the sensor nodes to be active and transmit sensed data. In event-driven and query driven models, the transmission of data is initiated when an event occurs or a query is generated by the base station. The hybrid model is the combination of all types of approaches discussed for data delivery. These models affect the performance of routing protocols the routing protocol is highly influenced by the data delivery model, especially with regard to the minimization of energy consumption and route stability. For instance, it has been concluded in (Wendi Rabiner Heinzelman, Kulik, & Balakrishnan, 1999) that for a habitat monitoring application where data is continuously transmitted to the sink, a hierarchical routing protocol is the most efficient alternative. This is due to the fact that such an application generates significant redundant data that can be aggregated on route to the sink, thus reducing traffic and saving energy.

Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base station which requires actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption or rerouting packets through regions of the network where more energy is available (Tilak et al., 2002). Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

Connectivity

The connectivity in between sensor nodes mostly depends upon the node density. High node density in wireless sensor networks predefines that the sensor nodes are completely isolated from each other. Therefore, connectivity should be high. However, the high connectivity does not assure that the topology will remain constant and it does not prevent the size of the network from shrinking due to node failures. Hence in addition, connectivity between nodes also depends on the random distribution of nodes.

Quality of Service

Some application of WSN needs the data to be transmitted in certain period of time from the time the data being sensed; otherwise the sensed data will be useless. Therefore, there is a bound in data delivery time introduces quality of service factor. As the energy gets decreased, the WSN tries to reduce the quality of data transfer to save energy in sensor nodes which then leads to increased lifetime of the network. Therefore, there is a need of routing protocols which can save energy in the network.

PROTOCOLS CLASSIFICATION

In WSN the routing protocols are always intended for transmitting and aggregating data between sensor nodes and the base stations. There are different routing protocols have been proposed by many researchers for wireless sensor network. The classification of routing protocols for WSN can be done on the basis of different parameters explained in section 2.1. This section will discuss the different types of routing protocols. Flooding and gossiping are the protocols which are not having any specific parameters. Hence, it is not in, any of the classification of routing protocols.

Flooding and Gossiping

There were two classical and simple strategies presented in (Hedetniemi, Hedetniemi, & Liestman, 1988) to transmit data from sensor node to the base station in wireless sensor network. In flooding the source sensor node broadcast the data packet to its immediate neighbors. After receiving the data packet each sensor node rebroadcast the data packet to their neighbors. This process will continue until all the nodes in the network receive the packet.

The data packet has to travel maximum number of hops and if there exists a route to the destination, and the communication is lossless, flooding guarantees the data packet to reach the destination. The simplicity of the flooding is its main advantage but there are many disadvantages of using flooding. The main disadvantage is the problem of heavy traffic and measures should be taken so that the packet does not travel through the network indefinitely. For example, to limit the number of times a packet is forwarded one can use the maximum-hop count a packet can travel. It should be small enough so that the data packet does not travel too long and large enough so that it can reach its intended destination. Further, the address of the source in the destination can be combined with a sequence number to uniquely identify the data packets so that the destination can discard the duplicate data packets (Hedetniemi et al., 1988).

There are some additional problems in flooding mechanism explained in (Hedetniemi et al., 1988): the first problem is *Implosion* which is caused by receiving duplicate data packets on the same node

Routing Protocols in Wireless Sensor Networks

(Figure 8). The other problem *Overlap* (Figure 9) problem arises when two sensor nodes sensing in the same region send identical data packet to the same neighbor. The third one is *Resource blindness* problem (Wendi Rabiner Heinzelman et al., 1999) which is caused when the sensor nodes consume large amount of energy without consideration of any energy saving schemes.

Figure 8. The implosion problem
Wendi Rabiner Heinzelman et al., 1999.

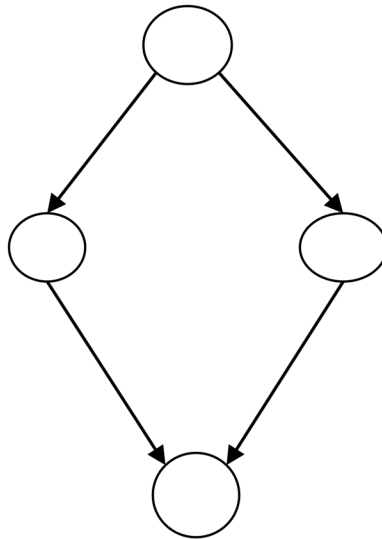
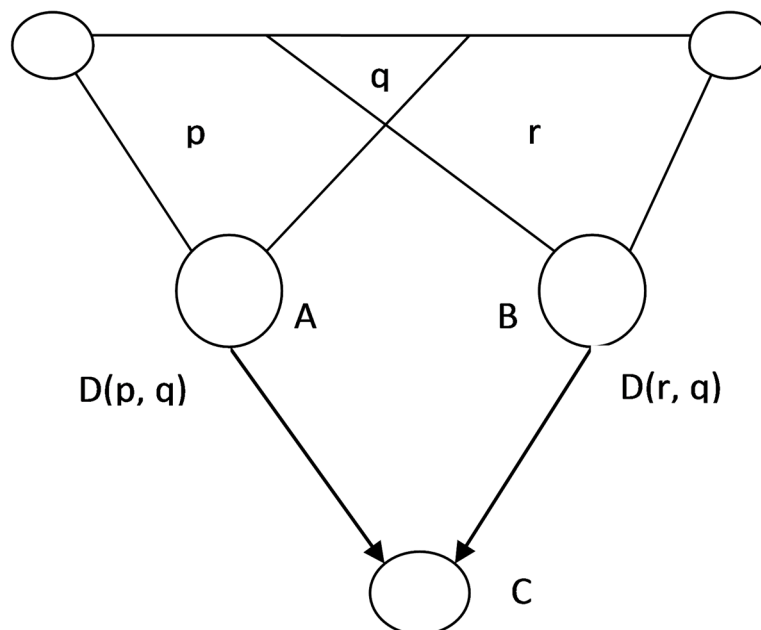


Figure 9. The overlap problem
Wendi Rabiner Heinzelman et al., 1999.



The other variation of Flooding is gossiping as presented in (Hedetniemi et al., 1988) remove the problem of implosion. In this the sensor node does not necessarily broadcast the data packet but transmit the packet to a single neighbor which is selected randomly. But also this introduces the problem of delays in transmission of data.

Data-Centric Routing

Based on the applications of sensor networks most of the time it is not possible to assign global addresses to sensor nodes. Also in many applications of WSN the data generated by the sensor nodes is more important rather than the node which has generated the data. Since there is significant redundancy in data that is generated in a particular region, there is wastage of energy. Hence there is a need of data aggregation/ data fusion. Hence, the data centric routing algorithms focus on data retrieval, data aggregation and the data fusion of a particular type of data type described by some attributes, as opposed to collecting the data from particular type of sensors. This section provides review of data-centric routing protocols.

1. **Sensor Protocols for Information via Negotiation:** SPIN protocol was designed under the category of data-centric routing because its main focus was on data dissemination (Wendi Rabiner Heinzelman et al., 1999). SPIN uses meta-data to define/name the original data by using high level descriptor. In SPIN a data advertisement mechanism is followed before the actual data transmission, in which each sensor node sends its meta-data to all of its neighbors. Each node on receiving, check this meta-data for novelty. If the data is new then it is again transmitted to the next level neighbors. The sensor nodes which do not have the new data can request the data from the data generator node and can have the data. The SPIN protocol uses three types of messages:

- a. **ADV:** Advertise the meta-data.
- b. **REQ:** Request data from a sensor node.
- c. **DATA:** carry actual data when requested.

Advantages:

- SPIN removes the problem of redundant data, overlapping of data and resource blindness. Hence it can achieve a lots of energy efficiency.
- Topological changes are localized.

Disadvantages:

- It cannot guarantee the delivery of data.
- Meta-data calculation introduces extra overhead.

2. **Directed Diffusion:** This algorithm was proposed to avoid unnecessary operation done by network layer on data which consume a lot of energy. The idea is to diffuse the data by using naming data schemes in sensor network. The idea proposed in this algorithm (Intanagonwiwat, Govindan, & Estrin, 2000) is to use some attribute value pairs for the data. The query sent to the sensor node should be on demand basis which should contain the attribute pairs. The attribute list can contain attributes like objects, interval, duration, geographic area etc.

When sink generates a query it defines an interest which consists of attribute value pair. It broadcast this interest towards the deployment area. The sensor nodes, on receiving this interest value, compare this to the data sensed by them. Sensor nodes can also do the data aggregation by using Srteiner Tree Algorithm (Krishnamachari, Estrin, & Wicker, 2002). The nodes reply the data back

Routing Protocols in Wireless Sensor Networks

Figure 10. The working of SPIN protocol: a) Node A advertises its data to its neighbor B; b) B request the data from A; c) Node A sends the data to B; d) now Node B advertises this new data towards its neighbors; e) nodes request data from B; f) Node B sends the data

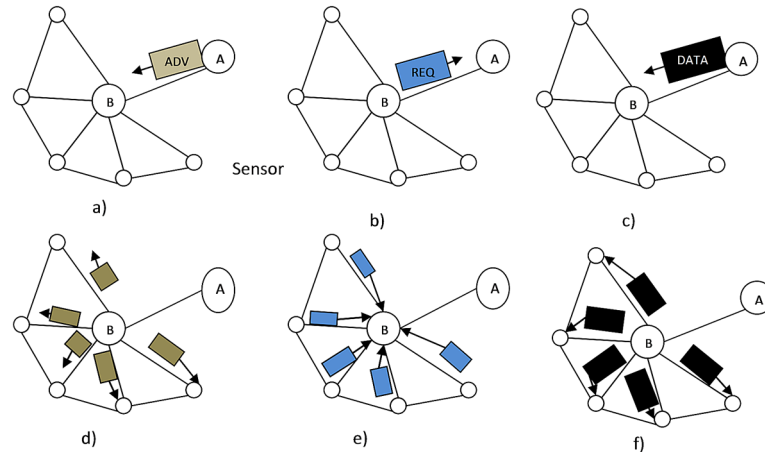
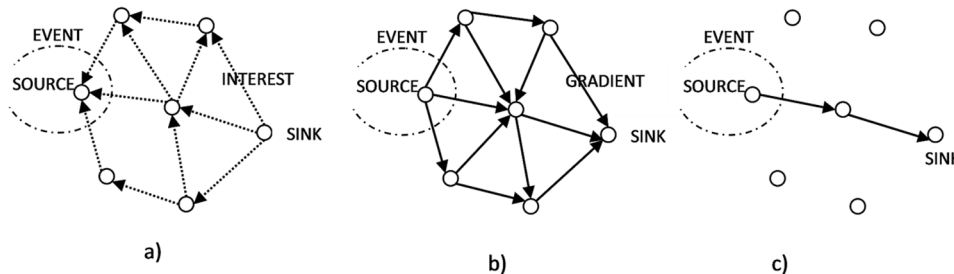


Figure 11. Phases of directed diffusion: a) interest broadcast; b) gradient setup; c) data delivery



to the sink node if any match found with respect to the interest by using gradient. Gradient is a reply link towards the neighbors of the replying sensor nodes. The routes are established with the help of interest and gradients.

Alternative paths can also be followed when the original; path fails due to some node failures or obstacles.

Advantages:

- Avoid unnecessary network layer operations.
- Path can be repaired.
- Save energy, when repairing any path.
- No need of node addressing mechanism.
- Nodes can perform aggregation and caching of data in addition to sensing task.

Disadvantages:

- Extra overhead of saving multiple path information.
- Cannot be applied to every application of sensor networks because it is only query driven.
- Naming schemes are application dependent and require being set manually again and again.
- Matching process also consumes energy and space.

3. **Energy-Aware Routing:** Shah and Rabaey (Shah & Rabaey, 2002) have proposed an algorithm that uses a set of sub-optimal paths to save energy and increase the lifetime of network. The sub-optimal paths are calculated by using probability functionality, which is dependent on energy consumption in every route. The authors have observed that using minimum energy consumption path every time results in failure of some nodes on that path. Hence it is convenient to use multiple paths with probability of fewer failures so that the network lifetime can be increased. It was assumed in the algorithm that the sensor nodes are having class based addressing which contains type and location of sensor node. The algorithm has three phases:

a. **Setup Phase:** In this phase the routing table is constructed by flooding messages to neighbor nodes. Also the energy consumption has been calculated at each sensor node. If node N_i send the request to node N_j , N_j will calculate the cost by using following equation (Shah & Rabaey, 2002):

$$C_{N_i N_j} = cost(N_i) + Metric(N_j, N_i)$$

The metric is the combination of transmission cost and receiving cost with residual energy in the sensor node. After calculating the path cost the very high cost paths are discarded. Each sensor node assigns a probability to its neighbors in routing table (forwarding table (FT)) given by following equation (Shah & Rabaey, 2002):

$$P_{N_j N_i} = \frac{\frac{1}{C_{N_j N_i}}}{\sum_{k \in FT_j} \frac{1}{C_{N_j N_k}}}$$

Now N_j will compute the actual full path cost to reach the destination (Shah & Rabaey, 2002):

$$C_{N_i N_j} = \sum_{i \in FT_j} P_{N_j N_i} C_{N_i N_j}$$

b. **Data Communication Phase:** In this phase each node sends data packet by choosing neighbor from its forwarding table (FT).

c. **Route Maintenance Phase:** To keep all the paths/routes alive localized flooding is performed to check whether there are any dead nodes/ dead paths.

Advantages:

- Increase lifetime of the sensor network up to 44%.

Disadvantages:

- Complicated route set up as compared to other algorithms.

4. **Rumor Routing:** Rumor routing (Braginsky & Estrin, 2002) has been used in the areas in which geographic routing protocols cannot be applied. This algorithm is a little variation of directed diffusion algorithm which floods the data to entire network when there is no geographical information

available. But, sometimes the sink node has required a little amount of data, hence flooding the whole data results in extra energy consumption. In rumor routing the request is sent only to those nodes which have observed some event. To flood the sensed events in the network, *agents* are used. *Agents* are the packets with long lifetime. When an event is detected by some node, it adds value of this event to its local table and creates an agent and creates a query for distant nodes in order to propagate the agent in the network. This type of routing maintains only one path in network from source node to destination (sink).

Advantages:

- It can efficiently handle Node failures.
- It saves more energy than directed diffusion protocol.

Disadvantages:

- It does not perform well when very large numbers of events are generated together.
- Overhead of adjusting parameters again and again like time-to-live for queries and agents.

5. **Gradient-Based Routing:** The other version of directed diffusion had been proposed by (Schurgers & Srivastava, 2001), which is known as Gradient Based Routing (GBR). The idea behind GBR is to maintain the record of number of minimum hops required to reach the sink node. The number of hops are recorded when the sink node sends the interest towards the sensor nodes. These minimum numbers of hops are in combination called as the *height*. The nodes can calculate the gradient from this height value. The gradient of a link is the difference between the node's height and that of its neighbor through that link. The sensor node, after sensing the data, will send it by using the link with greatest value of gradient. The author tries to balance the traffic in the network and also performing some function in the network itself like data aggregation. The data spreading techniques are:

- a. Stochastic scheme,
- b. Energy-based scheme, and
- c. Stream-based scheme (Schurgers & Srivastava, 2001).

Advantages:

- Through simulation GBR has been shown to outperform Directed Diffusion in terms of total communication energy.
- Balances the load across the entire network.

Disadvantages:

- Node failure recovery is absent.
- Do not guarantee data delivery at destination node.

6. **Constrained Anisotropic Data Routing Protocol (CADR):** Constrained Anisotropic Data Routing protocol is also based on directed diffusion protocol and it was proposed by (Chu, Haussecker, & Zhao, 2002). This is totally a query driven approach in which the sink sends a query to only those regions from which it needs data. The data packets are requested only from those sensors which are close to the particular event area asked by sink node. The routes are built according to the path through which the query has been received. The data is routed from source node on the basis of local information or cost gradient and the base station's (sink) requirements.

Advantages:

- Simulation results shows that that it is more energy-efficient than other directed diffusion type algorithms.

Disadvantages:

- Causes delays in transmission of data.
 - Do not assure reliable delivery of data.
7. **COUGAR:** Yao and Gherke (Yao & Gehrke, 2002) had proposed a new data centric protocol in 2002, which assumes the network as a bid database system. They provide a support of new layer of query in between the network layer and application layer and utilize in-network data processing. The authors assumed that the sensor network has separate gateway node which are having the ability to set a query plan for the incoming query and after planning sends the query toward the sensor nodes. The sensor nodes are capable of processing information and transmitting it towards gateways. When the query is planned, the data aggregation and data fusion information has been provided within query and also the leader is specified in a particular area which can handle multiple functions and is having enough energy.
- Advantages:
- This protocol provides reliable data delivery.
 - The node failures are being reduced and it increases the lifetime of the sensor network.
- Disadvantages:
- Increases the overhead of network by additional query layer.
 - Synchronization required for in-network data processing.
 - Leader selection should be dynamic rather than static.
8. **ACQUIRE:** ACtive QUery forwarding In sensoR nEtworks (ACQUIRE) (Sadagopan, Krishnamachari, & Helmy, 2003) had been proposed for query based applications of WSN. ACQUIRE is totally query based data-centric routing protocol. The protocol views the entire network as a distributed database which is well suited for the complex queries. The process of querying the sensor nodes works as follows: Sink node forwards the query towards sensor nodes. Each sensor node on receiving the query, respond partially towards sink node on the basis of pre-cached information. If this pre-cached information is not up-to date than the node will gather the information, which is up-to date from its surrounding nodes. When the node finds all the information needed to resolve the query than it forwards this information towards sink by using the reversed path or the shortest path.
- Advantages:
- ACQUIRE mechanism provides efficient query mechanism.
- Disadvantages:
- The results for this protocol have not been validated.
 - During calculations the reception costs have not been taken into consideration.
9. **Reliable Reactive Routing Enhancement for WSNs:** Niu *et.al.* found that an efficient and reliable data communication on unreliable wireless channels is the major challenge in WSNs and IWSNs (Industrial WSNs) when applied on dynamic environments (Jianwei, Long, Yu, Lei, & Das, 2013). To cope with these challenges authors have proposed a reactive type of routing protocol known as Reliable Reactive Routing Enhancement (R3E). R3E increases the reliability and energy efficiency in unreliable WSNs.

Authors have proposed a biased back-off technique to find the guide route during route discovery process. The data packets are transmitted to the destination on this guide route using greedy approach. In this protocol location information is not required. R3E showed improvement in packet delivery ratio with high energy efficiency and low delivery latency.

Hierarchical Routing Protocols

Hierarchical routing protocols have been designed for managing energy efficiently by using multi-hop communication. The multi-hop communication can save a lot of energy by involving all the sensor nodes in the network. Some protocols in this category also form clusters providing cluster head which can perform data processing task also. Formation of cluster totally based on energy information related to nodes. This section describes various routing protocols which work on this principle like LEACH, PEGASIS etc.

1. **LEACH:** Low-energy adaptive clustering hierarchy (W. R. Heinzelman et al., 2000) algorithm is most popular in many applications of sensor networks. LEACH divides the entire wireless sensor network into clusters according to the signal strength of receiving data and forms cluster heads which will act as routers toward destination (W. R. Heinzelman et al., 2000). This will be helpful in saving energy, since the communication, processing, fusion is all done only by the cluster head and other nodes.

LEACH protocol changes cluster heads randomly time-to-time to maintain a balance in energy consumption in the entire sensor network (W. R. Heinzelman et al., 2000). The decision of choosing cluster head has been made by the sensor nodes by choosing a random number between 0 and 1. One node will become a cluster head if the chosen number is less than the given threshold value which can be calculated by following equation (W. R. Heinzelman et al., 2000):

$$T(n) = \left\{ \begin{array}{l} \frac{p}{1 - p \times \left(r \bmod \left(\frac{1}{p} \right) \right)}, n \in G; 0, \text{Otherwise} \end{array} \right\}$$

where p is the percentage of cluster heads, r is current round and G is the set of nodes, which are not the cluster heads in last 1/p rounds.

Many researchers have developed routing protocols for WSNs by enhancing LEACH strategy. Various descendants of LEACH are Multi-hop LEACH (Biradar, Sawant, Mudholkar, & Patil, 2011), LEACH-C (Centralized LEACH) (Xinhua & Sheng, 2010), LEACH-F (Fixed number of clusters LEACH) (Kumar, Jain, & Tiwari, 2011), LEACH-E (Energy Efficient LEACH) (Kumar et al., 2011), LEACH-B (Balanced LEACH) (Kumar et al., 2011), LEACH-A (Advanced LEACH) (Abdellah, Benalla, Hssane, & Hasnaoui, 2010), Q-LEACH (Quadrature LEACH) (Manzoor et al., 2013), LEACH-SM (LEACH with Spare Management) (Bakr & Lilien, 2011).

Advantages:

- The clusters are easy to form and are very useful in data aggregation which removes the chances of data duplication at sink node.

Disadvantages:

- Energy consumption is high which reduces the lifetime of the network.

2. **PEGASIS and Hierarchical-PEGASIS:** Power Efficient GATHERing in sensor Information Systems (Lindsey & Raghavendra, 2002) is the next version of LEACH proposed by Lindsey and Raghavendra.

In this protocol the nodes form a chain for communication and transmit data from node to node and select one node among them to transmit data to the base station. Greedy approach is applied to form the chain (Lindsey & Raghavendra, 2002). Nodes aggregate and eventually forward the data to the base station/sink node.

Instead of using single-hop as in case of LEACH, the PEGASIS protocol uses multi-hop routing technique. PEGASIS works better than LEACH about 100-300% for different network topologies and sizes. It decreases the number of transmissions by using data aggregation and removes the overhead caused by dynamic clustering. But it introduces delays when the chain formed by sensor nodes is very long because it will take long time to decide that which node will forward the data to sink node.

To solve the problems in PEGASIS the extension of PEGASIS given by (Stehpanie, Raghavendra, & Krishna, 2001). The authors had proposed a solution which is related to data gathering by taking energy x delay metric into consideration. To decrease delay simultaneous transmissions are allowed in this protocol. But this can cause collisions and interferences in the signals. To avoid these problems Hierarchical PEGASIS uses two approaches, one is signal coding like CDMA and the second is approach is to allow transmission by only those nodes which are separated by regions/spatially.

Advantages:

- Energy efficient protocol.
- Works faster in small deployment areas.

Disadvantages:

- There is no procedure for dynamic topology adjustments.
- Sometimes there is a problem of selecting one node as a leader for consecutive transmissions results in depletion of that sensor node.

Figure 12. PEGASIS chaining

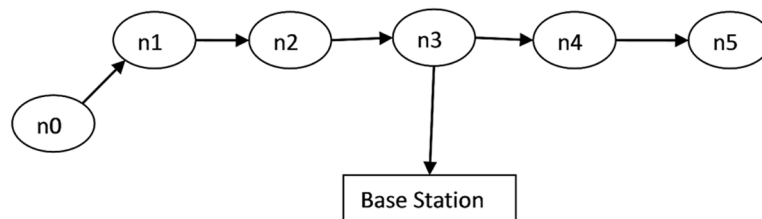
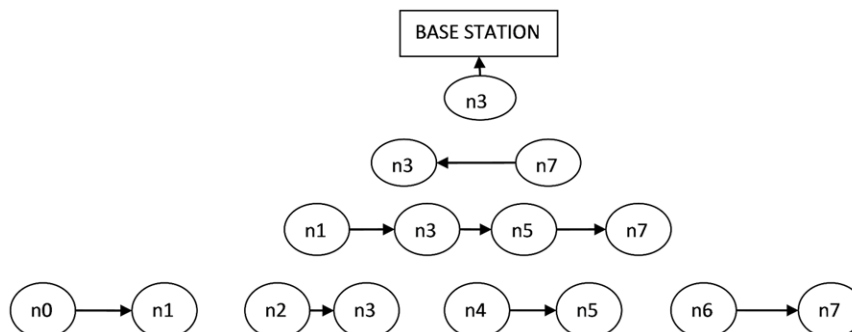


Figure 13. The chain based binary scheme of data gathering in hierarchical PEGASIS



3. **TEEN and APTEEN:** Threshold sensitive Energy Efficient sensor Network protocol (TEEN) (Arati Manjeshwar & Agrawal, 2001) is the reactive, event-driven type of protocol designed for the applications in which the time is the biggest factor. This means that if an event is generated in a particular region of deployment and is detected by a sensor node, the value of that event should reach the destination before a particular given time, otherwise it would be useless.

The sensor nodes in the network sense data continuously, but they transmit the data only when the changes in the value of sensed events are meeting a threshold value. This protocol is the combination of both hierarchical and data centric approaches. TEEN protocol start forming the clusters of those nodes which are closer to each other, and the process of forming clusters continues until the base station/sink node has not been reached. After forming the clusters the protocol allow the cluster head to broadcasts two value of an attribute i.e. hard threshold and soft threshold values. If the value of a sensed event is meeting the hard threshold value exactly only then the sensor node is allowed to transmit the value of that sensed event otherwise not. But in case of soft threshold the nodes are allowed to transmit value of sensed event when the difference between upper and lower values of sensed event is equal to soft threshold value.

Advantages:

- Reliable data delivery.
- Suitable for application where the data requirement by the end user is totally event driven.

Disadvantages:

- If the threshold values are not reached then the sensor nodes can never transmit the data.
- Not suitable for applications where data needed on regular interval basis.
- Collisions can occur in particular cluster.

To overcome the problems of periodic data transfers, an extension to TEEN has been proposed by (A. Manjeshwar & Agrawal, 2002) which they called as Adaptive TEEN (APTEEN). The working of this protocol is same as TEEN except the query generation system. The APTEEN allows querying in three different ways:

- a. **Historical Query:** Past data values analysis.
- b. **One-Time Query:** Generated to gather only one type of event.
- c. **Persistence Query:** Query generated to gather the data of events in a particular period of time.

Advantages:

- The results are better than LEACH protocols.

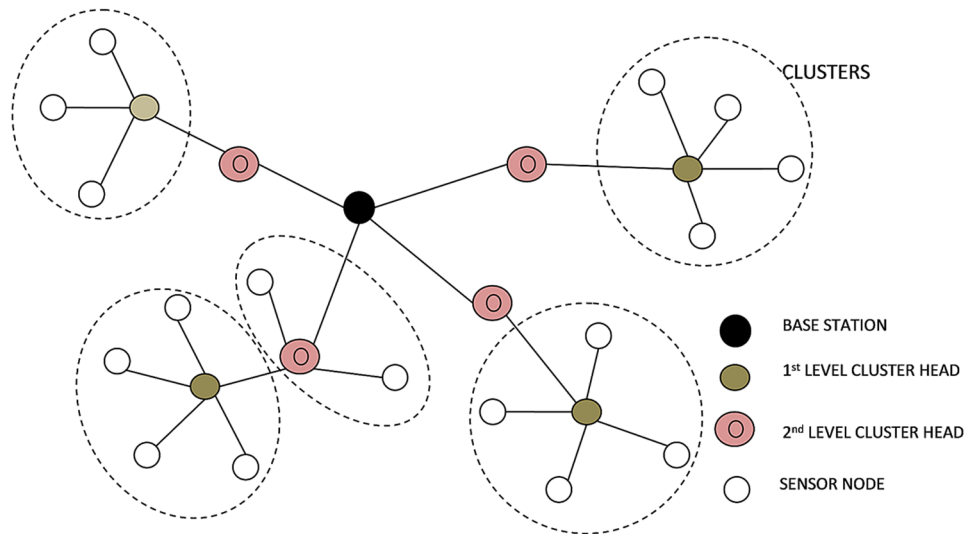
Disadvantages:

- The complexity of cluster formation mechanism introduces an overhead to this protocol.

4. **Energy-Aware Routing for Cluster-Based Sensor Networks:** Younis *et.al.* (Younis, Youssef, & Arisha, 2002) proposed a different type of hierarchical protocol which follows the principle of three tier architecture. This algorithm introduces the new cluster heads which are having high energy capacity and data aggregation capabilities. These new devices/nodes are called as gateways. The gateways are responsible for gathering data from all the sensor nodes in its cluster area by setting up efficient routes and also after performing some processing on data sends this data to the base station/sink nodes. The protocol uses TDMA technique for the communication between sensor nodes and gateways. After forming the clusters, the sensor nodes in the network can be in one of the following four states:

- a. **Sensing State:** The node senses the environment and generates data at a constant rate.
- b. **Relaying State:** The node involves only in communication, to relay the data from other active nodes.

Figure 14. Clustering in TEEN and APTEEN protocols



- c. **Sensing-Relaying State:** When a node is both sensing and relaying messages from other nodes.
- d. **Inactive State:** Node turnoff it's sensing and communication circuitry in this state and goes to sleep.

To save the energy when communication is going on, a cost function in terms of energy consumption has been defined, which finds a least-cost path between sensor nodes and gateway nodes.

Advantages:

- Save a lot of energy in communication.
- Node failures and hence path failures are very less.

Disadvantages:

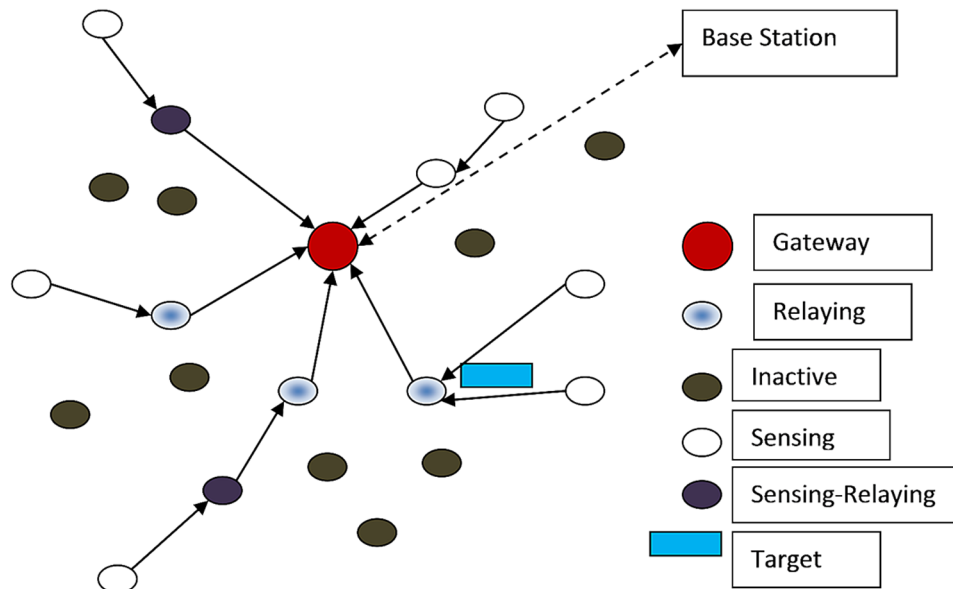
- Gateways are to be set up manually, and hence random deployment is not possible.
- Not suitable for all kind of applications of wireless sensor networks.

5. **Self-Organizing Protocol:** Subramaniam and Katz (L. Subramaniam & R. H. Katz, 2000) develop taxonomy of the sensor network applications and on the bases of that taxonomy they have designed a new routing protocol known as self-organizing protocol. They have designed an architecture which can support different types of sensor nodes (like stationary and mobile). The sensors monitor and record the environmental data and forward this data to a router. The routers are the stationary nodes and are the main components for communicating data. To identify the region and type of the sensor node, addresses are provided to them. The protocol consists of four phases:

- a. **Discovery Phase:** Sensor nodes discover the neighbor nodes.
- b. **Organization Phase:** The hierarchy of nodes is formed on the basis of location of the node and creates the routing tables. Also Broadcast trees are constructed for message to be transferred through.
- c. **Maintenance Phase:** In this phase the routing tables are updated and energy levels of nodes are recorded. The nodes tell the neighbors about its routing table and energy level. Local Markove loops are used to construct and maintain the broadcast trees.

Routing Protocols in Wireless Sensor Networks

Figure 15. A typical cluster in a Wireless Sensor Networks



- d. **Self-Organization Phase:** In this phase reorganization of the network has been done if there are any node failures, partitions etc. occurs.

Advantages:

- The protocol works on heterogeneous WSNs and can be suitable for many applications.
- Energy level is maintained throughout the network.

Disadvantages:

- Reorganization of the network introduces the overhead for the sensor nodes.

Location Based Routing Protocols

There is a wide variety of applications where WSNs are applied. In some of the applications the location information is needed by the routing protocol. This location is the geographic position of the sensor node. The geographic positions can be detected with the help of a global positioning system (GPS). This information is needed to calculate the distance between two nodes for the purpose of signal strength calculations.

The principle of such protocols is to send a query towards a particular region only, from where the base station needs data. Many location based protocols have been designed for mobile ad-hoc networks. But some of the protocols which are based on energy saving can also be applied to the wireless sensor networks. This section presents few of such protocols.

1. **MECN and SMECN:** Minimum energy communication network (MECN) (Rodoplu & Meng, 1999) is a self-reconfiguring protocol that maintains the energy consumption as minimum as possible by using low power GPS. It generates minimum spanning tree at base station minimum power topology. The tree contains only the routes from source node base station which consume the lesser energy. When forming the topology MECN spot relay regions for each node in the network.

Relay region can be defined as the area of surrounding of the sensor node, in which the node can transmit data by using as less energy as it can. After defining the relay region and spanning tree the enclosure graph is constructed by using lesser number of nodes among which communication requires very less energy. MECN works in two phases mainly:

- a. **Enclosure Graph Construction:** It is a sparse graph, consists of all enclosure of each sensor node in the network. The graph contains all possible minimum energy links which are globally optimal.
- b. **Find Shortest Path:** In this phase the protocol finds the shortest path by using the Bellmann-Ford shortest path algorithm with power consumption as a cost factor.

The small minimum energy communication network (SMECN) (Rodoplu & Meng, 1999) is an extension of MECN. Unlike MECN, SMECN considers the hurdles in the way of communication between two nodes also. Although the network is still considered as connected, the minimum energy relaying is smaller (in terms of cast edges in graph) than in case of MECN. Hence numbers of transmissions are decreased hop-by-hop. SMECN uses less energy than MECN and also cost of the routes is very less.

Advantages:

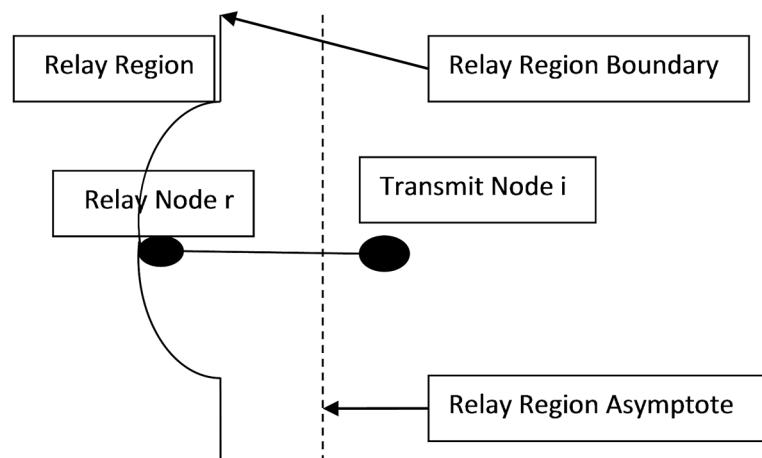
- Save a lot of energy used in transmission of data.

Disadvantages:

- Sub-network with smaller numbers of nodes introduces more overhead in finding the routes.

2. **Geographic Adaptive Fidelity (GAF):** Geographic adaptive fidelity (Xu, Heidemann, & Estrin, 2001) is an energy aware protocol which finds the routes on the basis of sensor node's location information. The algorithm divides the entire deployment area in virtual grids. Each sensor node in a virtual grid uses its GPS location to identify that to which virtual grid it belongs. The algorithm employs the strategy to turn off unnecessary nodes in the network without affecting the routing devotion. On the basis of the GPS location the nodes belongs to the same point on a virtual grid are considered as equivalent in terms of cost of packet transmission. Hence GAF keep some of these nodes in sleeping state in order to save energy. Hence, when the numbers of nodes are getting higher, GAF increases the lifetime of the network. A situation of forming virtual grids is shown

Figure 16. MECN relay region of transmit-relay node pair (i, r)



below in Figure 17. In this situation we can see that node 1 can reach the nodes 2, 3, and 4 in virtual grid B and also nodes 2, 3, and 4 can reach node 5 that is virtual grid C. Hence according to GAF protocol two of the nodes among 2, 3, and 4 in region B can sleep and one of them will transmit the data. According to GAF the nodes can change their states. The states are shown in Figure 18:

- a. **Discovery:** Finding out the neighbor nodes in the virtual grid.
- b. **Active:** The nodes in this state are participating in the routing Process.
- c. **Sleep:** In this state the transmission radio of the nodes has been turned off.

GAF protocol had been implemented for both non-mobility and mobility of nodes in the sensor network. In order to handle mobility of nodes the protocol allows the nodes to sends their information to neighbor nodes in the virtual grid about their leaving information.

Figure 17. Virtual grid example in GAF

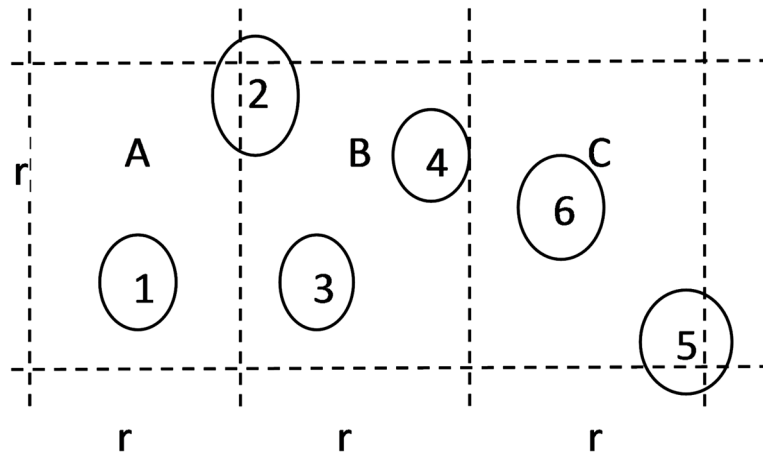
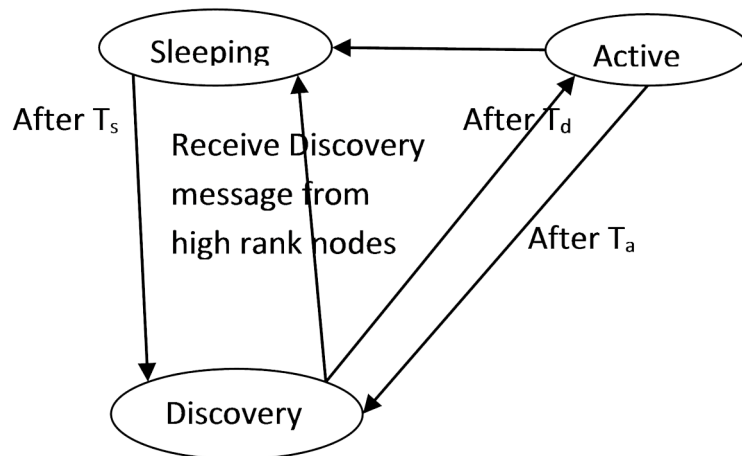


Figure 18. State transition diagram of a node



Advantages:

- Simulation results showed that the performance of GAF is as well as in case of normal ad-hoc routing protocols.
- Increases network lifetime by decreasing packet losses.

Disadvantages:

- One of the nodes in grid act as a leader, but it does not perform any data aggregation and data fusion task.

3. **Geographic and Energy-Aware Routing (GEAR):** Geographic and energy aware routing has been proposed by (Yu, Govindan, & Estrin, 2001), which can build routes on the basis of geographic information of the neighbors. The main idea behind this protocol was to restrict the number of interests in directed diffusion by only sending interests to a specified region, rather than forwarding the interest to each sensor node in the network. Each node in the network retains the estimated cost of transmitting a packet towards the destination. Also the node will retain a learning cost to reach the destination through its neighbors. If there is no neighbor node to the any of sensor node through which it can transmit data towards the destination region, it is considered as a hole. If there are no holes in the network, than the learning cost and the estimated cost are considered to be equal. The algorithm works in two phases:

- a. **Target Region Forwarding:** On receiving any packet each sensor node will check, if there is/ are any neighbor(s) exists, which can be selected as next hop for transmission of data. If there is only one than the sensor node has to select this only neighbor as a next hop for forwarding the data. But, if there are multiple neighbors then forwarder will select a node as next hop, which is nearest to the target region. If there is no node closer to the forwarder node than it means there is a hole. In this case the node will pick neighbor based on the learning cost to forward the data packet.
- b. **Within the Region Forwarding:** The packet is diffused in the region by using recursive geographic forwarding or by means of restricted flooding.

Advantages:

- GEAR reduces energy consumption.
- Packet delivery is very good as compared to other protocols.

Disadvantages:

- There is extra overhead of selecting the next neighbor for forwarding the data packets.

Network Flow and QoS-Aware Routing Protocols

Some of approaches have been proposed by many authors do not fit in the above classification and is considered under network flow and QoS-aware protocols for some regions. The network flow based protocols, setup the paths by considering them as network flow problems, to find out the optimal transmission path. The QoS-aware protocols consider the end-to-end delays while establishing the routes in the network. Some of these protocols have been discussed in this section.

1. **Maximum Lifetime Routing in Wireless Sensor Networks:** Based on the network flow approach, Chang and Tassiulas gave a solution to the routing problem in Sensor Networks (Jae-Hwan & Tassiulas, 2004). The main idea behind the protocol design is to maximize the lifetime of the network. To fulfill this purpose they had given the cost of a link as a function of remaining energy in the node and the minimum required energy for packet transmission on that link. Now finding the optimal traffic distribution is the possible solution to the routing problem. The optimal traffic distribution is used to maximize the lifetime of the network. The authors have proposed two algorithms in order to solve this maximization problem. The difference between two algorithms is the link cost calculation and the involvement of the residual energy of the sensor nodes. The link costs on a link i - j are given by the following equations (Jae-Hwan & Tassiulas, 2004):

$$C_{ij} = \frac{1}{E_i - e_{ij}}$$

and

$$C_{ij} = \frac{e_{ij}}{E_i}$$

where E_i is the residual energy of node i . Now to find out the shortest path towards the destination node Bellman-Ford shortest path algorithm is used. The algorithm gives the path with largest residual energy from source to destination.

Advantages:

- The simulation results show that the link costs are better than Minimum Transmitted energy algorithm.

Disadvantages:

- Not applicable to all type of applications of wireless sensor networks.

2. **Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks:** Kalpakis *et.al.* proposed that optimal routes can be setup in the network, when maximum lifetime data gathering problem is solved (Dasgupta, Kalpakis, & Namjoshi, 2003). Hence, they have proposed new algorithm for routing and data gathering which is a polynomial time algorithm. The authors also gave the definition for lifetime of the network. The lifetime of the sensor network is the number of rounds or periodic data readings from sensor nodes until the first sensor node dies. The schedule of data gathering had been specified for each round which specifies that how sensor nodes will gather the data and how it will transmit this data towards the sink node. The schedule have a tree for each round in which the root is the sink nodes and the intermediate and leaves elements are the other sensor nodes. The data gathering lifetime is dependent on the schedule. To maximize the lifetime data gathering the authors have proposed an algorithm called as MLDA (Maximum Lifetime Data Gathering). While setting up the routes the algorithm considers the data aggregation. The algorithm develops a flow network on the basis of the schedule and number of rounds and the optimal network flow has been extracted from this network flow. Now a schedule has been constructed by using this optimal network flow.

To design a schedule a variant of above algorithm has been considered, which is called as maximum lifetime data routing (MLDR). This algorithm models the problem as a network flow problem by considering energy constraints of sensor nodes. Then this problem is solved by using linear integer programming problem.

The author also proposed another algorithm called as CMLDA in order to reduce the delays and improve the working in large sensor networks. His algorithm introduces clustering with MLDA.

Advantages:

- Both MLDA and MLDR proves to be better than Hierarchical-PEGASIS in terms of system lifetime.

Disadvantages:

- MLDA introduces some delays for the transmission of data packets.
- MLDA and MLDR do not perform well when the sensor network is very large.
- The algorithms are expensive in terms of computations.

3. **Sequential Assignment Routing (SAR):** Sequential assignment routing (Sohrabi et al., 2000) is the first protocol that is designed by introducing Quality-of-Service factors in routing decisions. This protocol is a table driven protocol designed under multipath routing scheme and can achieve high energy efficiency and fault tolerance. The protocol starts working by creating trees rooted at the one-hop neighbors of the sink node. While creating the tree the protocol maintain the QoS metric level as good as possible by taking into consideration the energy available on each path and the priority level of each packet. By using these trees multiple paths from sink to each sensor node has been created. Among these multiple paths one of the paths is selected on the basis of energy resources and QoS metric on that path. The recovery from failures can be done by maintaining consistency in the routing tables of upstream and downstream nodes in the path.

Advantages:

- Simulation results show that SAR offers less power consumption than the minimum-energy metric algorithm.
- SAR maintains multiple paths and hence it is easy to recover from failures and it ensures fault tolerance.

Disadvantages:

- Suffers from overhead when the numbers of nodes in the network are huge.

4. **Energy-Aware QoS Routing Protocol:** Energy-aware QoS routing protocol has been proposed by Akkaya and Younis (Akkaya & Younis, 2003) in which the real time traffic is generated by imaging sensors. The proposed protocol finds the least cost path by considering end-end delays during establishing a connection. The communication parameters used to calculate the path cost from source to destination are remaining energy in nodes, transmission energy, error rate etc. The authors have incorporated a queuing model which is class based and support both best efforts and real time traffic. The queuing model allows the sensor nodes to share the services for both real time and non-real time traffic in the wireless sensor network. The protocol establishes the least cost paths by using an extended version of the Dijkstra's algorithm and picks a path which satisfies the end-to-end delay requirement.

Advantages:

- It performs well with respect to QoS and Energy metrics.

Disadvantages:

- The available links utilization is very poor.

Routing Protocols in Wireless Sensor Networks

5. **SPEED:** SPEED is a QoS aware routing protocol designed for sensor networks that provides soft real time and end-to-end data delivery guarantees (He, Stankovic, Lu, & Abdelzaher, 2003). Each node will maintain the information about its surrounding nodes and uses geographic forwarding technique to find the routes. The Protocol ensures a transmission speed of the data packet so that the end-to-end delays can be estimated. The protocol also provides the congestion management when the network is congested. The module which provides the routing functionality in SPEED is called as Stateless geographic Non-deterministic Forwarding (SNGF). SNGF works with four other modules which belongs to the network layer. The modules are shown in the Figure 19. The other modules are:

- a. **Beacon Exchange:** Gather information about the sensor nodes and their location.
- b. **Delay Estimation:** Delays are calculated by taking into consideration the elapsed time to receive an acknowledgement from the neighbor of each node which is sent by neighbor as a response of received data packet. The SNGF decides which node meets the requirements of speed of data packet on the basis of these delay estimations.
- c. **Neighborhood Feedback Loop:** It is responsible for providing the relay ratios which are calculated by means of miss ratios of the neighbors of each node. The SNGF generates a random number between 0 and 1 and compare the relay ratio with it, if the relay ration is less than this number than the packet is dropped.
- d. **Backpressure Rerouting:** This module is used to prevent voids, when a sensor node has been failed to find the next hop for transmission. It also controls the congestion in the network by sensing the messages about new routes for the source.

Advantages:

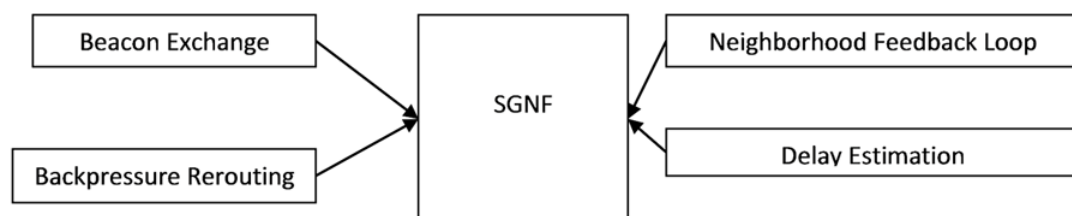
- SPEED performs better in terms of end-to-end delays and miss ratio.
- Transmission energy cost is less due to the simplicity of the algorithm and also control packet overhead is less.

Disadvantages:

- SPEED does not consider any further good energy metrics in its routing protocol. Therefore, for more realistic understanding of SPEED there is need of more energy conservation metrics.

6. **Dynamic Routing for Data Integrity and Delay Differentiated Services in WSNs:** Zhang *et.al.* have designed Data Integrity and Delay Differentiated Routing (IDDR) (Zhang, Ren, Gao, Yang, & Lin, 2015) protocol by considering QoS for applications of WSNs. According to authors different WSN applications have different QoS requirements. The basic QoS requirements are low delay and high data integrity. These two requirements cannot be always satisfied simultaneously for every application of WSN. IDDR utilizes the concept of potentials from physics to give mul-

Figure 19. SPEED's components of routing



tipath dynamic routing procedure. IDDR form a hybrid virtual potential field, which separates the data packets for different applications of single WSN. IDDR assigns weights to each data packet according to different QoS requirements (Zhang et al., 2015). Then the packets are routed towards the base station. The routes are decided in such a way that it can improve the performance, data integrity and the end-to-end delay according to requirements of applications. To prove the stability of IDDR authors have used Lyapunov Drift technique. IDDR improves data integrity and delay differentiated services.

Opportunistic Routing Protocols

The popularity of WSNs has increased very quickly in recent years. This popularity leads to the generation of new applications of WSNs. There are still many major challenges in WSN because of energy constraints, unattended environments etc. The communication between sensor nodes needs some efficient and reliable routing protocols which can improve the lifetime of the sensor network. Also a routing protocol must consider the communication range of the sensor node which is not very high. While applying any routing protocol in WSN these all factors must be considered. Wireless communications may also lead to packet losses due to interferences and channel errors. In WSN the sensor nodes are deployed randomly in many applications at very large scale. This also causes major hurdles in communication between nodes. Hence the advancement of the available routing protocols becomes the necessity. The researchers from different regions of world tried to improve the existing routing protocols and this leads to new generation routing called as opportunistic routing.

Opportunistic routing uses broadcast nature of wireless links and tries to solve all of communication problems in WSN. Any sensor node can overhear the packet, but, only one will forward the packet towards next-hop. The next-hop selection process is based on opportunistic decisions/rules. This section will provide introduction of some of the available opportunistic routing protocols.

1. **Energy Efficient Opportunistic Routing in WSN:** Mao *et.al.* have proposed an algorithm on the basis of selecting and prioritizing list of forwarders nodes (Mao, Tang, Xu, Li, & Ma, 2011). The paper has presented two cases, where the transmission power of each node is fixed or dynamically adjustable. The authors have named the proposed algorithm as EEOR (Mao et al., 2011). The algorithm was tested with the help of TOSSIM simulator.

The paper presents two cases in terms of transmission power. One is that some sensor nodes cannot adjust their transmission power, means that the transmission power is same for each transmission. The other case is of the sensor nodes that can adjust the transmission power.

The main idea behind EEOR is to first find out the expected cost needed by a sensor node to send a packet to a destination when the sensor node decided its forwarder list. The expected cost for the target has been assumed to be zero initially and infinite for all other nodes. To decide the routes from source to destination the mechanism used is similar to that of Distance-Vector Routing (Mao et al., 2011). The expected costs are calculated periodically by each node and the tables are updated. When a node wants to transmit a data packet, it simply broadcast the packet and let one node from its forwarder list to forward the packet.

Advantages:

- The data delivery is guaranteed.

Routing Protocols in Wireless Sensor Networks

- Problem of duplication of data packets has been resolved by allowing only one node from forwarder list to forward the data.

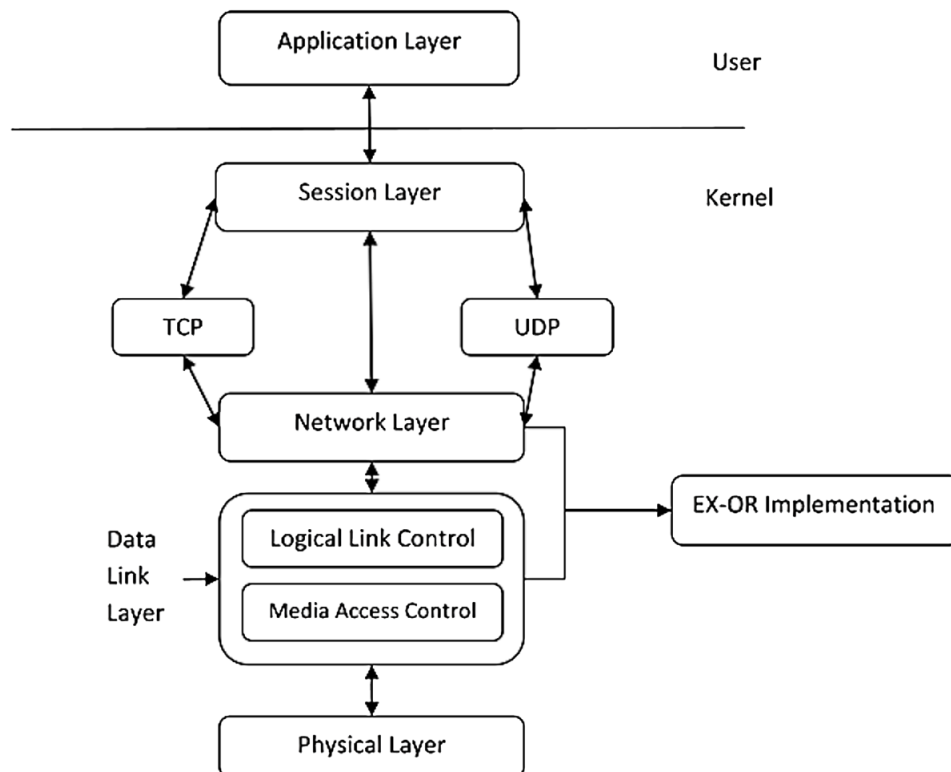
Disadvantages:

- Energy cost of communication agreement has been omitted from the cost calculation which is an extra overhead.
- The expected cost calculations can introduce delays in network communication and the data cannot be delivered in expected time.

2. **Ex-OR: Opportunistic Multi-Hop Routing for Wireless Networks:** Ex-OR was proposed by Biswas and Morris in 2005 (Biswas & Morris, 2005). This protocol is an integration of routing and MAC protocols. In Ex-OR the routes are established after the transmission of data packet. After transmission of a data packet next hop is selected on the basis of multiple opportunities available for data transmission routes.

The data packets are broadcasted by the source node and the next forwarder will be selected only after finding the best set of nodes which are able to forward the data packets further to next hop or destination nodes. The protocol ensures that only the sensor node in the best condition will forward the data packets further. To select the best forwarder node the Ex-OR forms the batches of data packets and the source node includes a list of forwarder candidates in each packet prioritized on the basis of the closeness to the destination (Biswas & Morris, 2005). Receiver node will further do the same process until the whole batch of packets reach the destination node/ sink node and provide acknowledgement to the source node via same path.

Figure 20. Layered architecture – implementation of EXOR



Advantages:

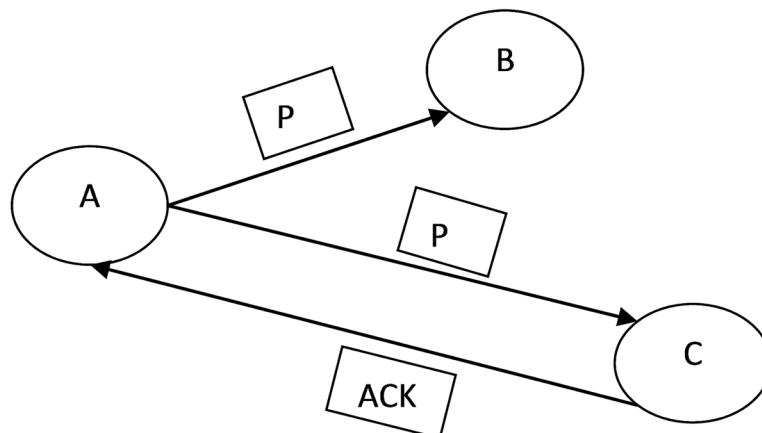
- Provides higher throughput.
- Acknowledgements prevent unnecessary transmissions.

Disadvantages:

- Response time might be affected by the larger amounts of buffering in high efficiency networks.

3. **Opportunistic Real Time Routing in Multi-Hop Wireless Sensor Networks:** Kim and Ravindran have observed that the routing protocols for WSNs which are of low data rate suffers a lot from instability of route links and maintaining the routing metrics (Kim & Ravindran, 2009). Opportunistic Routing protocols for WSNs also suffer from problems like real-time data support and high power consumption. To solve these types of problems, authors have proposed a new opportunistic routing protocol called as Opportunistic Real Time Routing (ORTR) (Kim & Ravindran, 2009). ORTR guarantees the delivery of data packets in a given time constraint. It also provides efficient energy consumption and increases the lifetime of WSN. To fulfill the requirement of time constraint, ORTR defines an area in which the data has to be delivered. The next hops are selected by considering the balancing factor of energy consumption for the purpose of increasing lifetime of network. ORTR is a guaranteed real-time data delivery service routing protocol with efficient energy consumption across the wireless sensor network.
4. **Low Power, Low Delay - Opportunistic Routing Meets Duty Cycling:** Landsiedal *et.al.* have proposed a different opportunistic routing protocol ORW (Opportunistic Routing for WSN) (Landsiedel, Ghadimi, Duquennoy, & Johansson, 2012). The basic idea of ORW is to make use of duty cycled protocols. The ORW uses low power listening MAC like X-MAC (Buettner, Yee, Anderson, & Han, 2006). In this low power listening scheme the source node sends data packets until the receiver gets active and acknowledges these packets. The authors make use of opportunistic routing instead of unicast forwarding scheme. As the source node sending data packets continuously so the first node that wakes up, receive the packets and able to communicate/forward these packets, will participate in the routing process as shown in Figure 21 (Landsiedel et al., 2012). The node A sends packet P to both B and C. Node C wakes up first and acknowledge the packet. So C will take the routing process further.

Figure 21. ORW routing process



ORW makes use of unreliable links also, as shown in Figure 21. Instead of transmitting A-> B-> C ORW transmits A-> C directly and saves energy. ORW is an energy efficient protocol which provides a good forwarder selection mechanism. The number of hops for a packet is also minimized.

Advantages:

- Energy efficiency is provided by the protocol.
- ORW works well into duty-cycled wireless sensor networks.
- Increases resilience to wireless link dynamics.

Disadvantages:

- Data packets can be forwarded to such sensor nodes which are having fewer capabilities.
- ORW cannot provide good throughput in low density networks.
- ORW does not support Mesh Routing.

5. **EFFORT (On Enhancing Network Lifetime Using Opportunistic Routing in WSN):** EFFORT (Hung, Lin, Hsu, Chou, & Tu, 2010), the name given by its' authors, has been designed especially for lifetime maximization of wireless sensor networks by utilizing opportunistic routing. The authors have developed a distributed opportunistic routing scheme by taking the advantages of opportunistic routing into consideration, like path diversity and transmission reliability. For the design of this protocol a new metric have been proposed by the authors for the forwarder selection and prioritization of next hop nodes. The authors have observed that most of the opportunistic routing algorithms depend on the design of the mechanisms for forwarder selection and prioritization. Opportunistic routing becomes most challenging in WSN when the reliability of link and the residual energy has been considered while designing any opportunistic routing strategy. The authors propose a metric and called it as OEC (Opportunistic End-to-end Cost) metric (Hung et al., 2010). OEC is used to decide the forwarding set at each sensor node and also relay sequence. Based on this metric EFFORT routing algorithm has been developed which compute optimal OEC value.

- a. **OEC:** OEC has been designed as a criterion of forwarder list selection and prioritization of relay nodes. The authors have defined scarcity energy cost (SE_Cost) of energy consumption (EC) (Hung et al., 2010) for a sensor j with residual energy RE_j as (Hung et al., 2010):

$$SE_Cost = \frac{EC}{RE_j}$$

This SE_Cost can be treated as loss to the network lifetime. The OEC metric tries to minimize the SE-cost value for each transmission. The sensor node can calculate its OEC value by using all forwarders' OEC value (Hung et al., 2010).

$$OEC_s(F_s, pri()) = C_{Tx:s \rightarrow fwd} + C_{Rx:fwd \leftarrow s} + C_{fwd \rightarrow d} + C_{reTx}$$

where, OEC_s are end-to-end transmission costs from node s to any sink node. F_s is the forwarding set of sensor node s . The $pri()$ is the priority of any node. $C_{Tx:s \rightarrow fwd}$ is SE_Cost of a sender used to broadcast a unit of data. $C_{Rx:fwd \leftarrow s}$ is the SE-Cost of the receiving a unit of

data. $C_{fwd \rightarrow d}$ is expected end-to-end SE_Cost. C_{reTx} is the retransmission cost of a unit of data.

- b. **EFFORT Working:** It uses OEC metric for each data forwarding steps of EFFORT are as follows:
 - i. Compute OEC values.
 - ii. Based on OEC select forwarding candidates list and assign priority to them.
 - iii. Transmit data on the optimal OEC value sensor node, re-compute and update OEC values.

The authors have simulated EFFORT in NS2 simulator using MICAZ in the simulation setting as hardware and parameters are set according to (Vuran & Akyildiz, 2006).

Advantages:

- EFFORT considers energy cost of end-to-end data forwarding and also residual energy of the sensor nodes.
- EFFORT ensures transmission reliability.
- EFFORT achieves network lifetime enhancement.

Disadvantages:

- Algorithm design and implementation is very complex.
- Performance degrades when the sensors in the network are scattered far away from each other.

6. **Opportunistic Distance Aware Routing in Multi-Sink Mobile WSNs:** Wenning *et.al.* have proposed a new opportunistic routing protocol and named it as Opportunistic Distance Enabled Unicast Routing (ODEUR) (Wenning, Lukosius, Timm-Giel, Gorg, & Tomic, 2008). ODEUR is based on two measures: RSSI (Received Signal Strength Indication) and MG (Mobility Gradient). RSSI indicates the energy level of data packet received at sink node, which tells about the relative distance of source to sink. ODEUR defines minimum RSSI requirements for the communication purpose. Based on RSSI measure the nodes are able to devise MG as a measure of relative movements of nodes with respect to sink nodes. MG can have three different values 0, 1 and -1. If MG is 0, it indicates that the distance between the sensor node and the sink node remains constant, MG equals to 1 indicates that the sensor node is moving towards the sink node and MG equals -1 indicates that sensor node is going away from the sink node. Based on these two metrics a table of neighbor nodes have been developed by the sink node and the node which is in the best condition can be selected as best neighbor to forward data.

ODEUR is a good approach for multi-sink WSNs. It has short end-to-end delays and it guarantees the data delivery.

7. **On End-to-End Throughput of Opportunistic Routing in Multi Rate and Multi Hop Wireless Networks:** n idea of opportunistic routing was proposed by (Zeng, Lou, & Zhai, 2008). The algorithm they have presented makes use of broadcasting and spatial diversity of unreliable wireless links.

The design of algorithm was based on Concurrent Transmitter Sets (CTS). CTSs provide the information about the data packet conflicts during data transmission. The currently available routing protocols for wireless networks follow the concept of wired networks routing protocols. This idea does not provide good throughput. The innovative thought was “Can we make use of the successful receptions of these neighboring nodes instead of re transmitting the packets on the specified

link to save precious band width and energy?” Inspired by this idea a new routing paradigm called Opportunistic routing has been proposed in (Zeng et al., 2008).

To improve the end-to-end throughput Conservative CTS (CCTS) and Greedy CTS (GCTS) are used for developing an opportunistic routing algorithm. CCTS is the set of forwarders. All the nodes in CCTS are able to transmit the packets simultaneously and all the links coupled with them are available for data transmission. CCTS requires every opportunistic recipient to be obstruction free for one communication. This results in lower bound of end to end capacity. Hence GCTS has been used to increase the throughput from end-to-end. GCTS are the forwarders, which can transmit data simultaneously and only one link, is available with each node to transmit the data packets. The authors also take the rate of transmission into consideration. According to (Zeng et al., 2008) low rate communication covers a long range of transmission while high rate communication covers short range. This trade-off between transmission rate and the distance affects the throughput of data transmission.

The authors have proposed a selection scheme for data transmission rate. The algorithm compares multi-rate Opportunistic Routing with single-rate Opportunistic Routing throughput capacity. The simulation results showed that Opportunistic Routing has big prospective to get better end-to-end throughput and the scheme working at multi-rates attain high throughput than that working at any single rate.

Advantages:

- Improves throughput of the network.

Disadvantages:

- Suitable for Mobile Ad-hoc Networks.
- The node energy is not considered as a major factor and this can reduce the lifetime of the WSN.

8. **Link Probability Based Opportunistic Routing Metric in Wireless Networks:** Most of the opportunistic routing protocols are dependent on the metric/scheme used in the selection of the forwarders list. (Li, Liu, & Luo, 2009) analyses these opportunistic routing metrics which are used in designing an opportunistic routing protocol. The authors have also give STR (Successful Transmission Rate) opportunistic routing metric. Based on this metric the authors have proposed FORLC (Fair Opportunistic Routing with Linear Coding) routing protocol which improves performance of network, by increasing throughput and decreasing the data packet transmission cost. The algorithm was a multi-hop routing algorithm which is an improvement to single hop routing protocol by deciding multiple routes for data packets delivery. This increases the packet delivery ratio and also avoids the duplication of data packets.

The source node transmits only those data packets which are not yet been delivered to any high priority sensor node. These high priority nodes will forward the data first and rest of the node will wait until the data is transmitted.

Fair opportunistic routing protocol makes a set of forwarder candidates which are fair for transmission without any priority. This set of forwarders contains the nodes which are closer to destination node. MORE (MAC independent Opportunistic Routing and Encoding) is a typical fair opportunistic routing scheme which supports spatial reuse and multi – cast with ETX as the metric to choose the candidate set. The challenge is to achieve lower number of duplicate transmissions between source and destination with higher throughput.

Advantages:

- Avoid duplication of data packets.
- Reduce the overhead of expected cost calculations.

Disadvantages:

- If the higher priority node fails or under attack during transmission of data, then there will be no guarantee of data delivery.
- Data and energy losses occur during transmission of data on unreliable wireless links.

9. **EAOR - Energy Aware Opportunistic Routing in Wireless Sensor Network:** Energy consumption by sensor nodes in wireless sensor network is the biggest challenge that can decrease the lifetime of WSN and threaten the successful deployment of sensor nodes. (Spachos, Chatzimisios, & Hatzinakos, 2012) presented a new opportunistic routing algorithm, EAOR for wireless sensor networks. The algorithm was designed to balance the energy consumption in the network and also maintain the Quality-of-Service.

EAOR allows sensor nodes to exchange information regarding energy and location. The working of this protocol is same as that of traditional opportunistic routing protocols. The main difference is the criteria of selection of next relay node. The source node sends a RTS (Request-to-send) packet towards its neighbors. The node which is in good condition to take part in routing process will send back a CTS (Clear-to-send) (Spachos et al., 2012) packet towards source node. After receiving the CTS packet the source node will reply with a DATA signal which contains the actual data packet. EAOR tries to send data packets towards the nodes that are closer to destination nodes. The simulation of the algorithm has been done with the help of OMNeT++. The simulation shows that it performs better than other traditional routing protocols in WSN.

Advantages:

- EAOR performs 35% better in energy consumption than traditional routing protocols.
- Increases network lifetime by 25%.

Disadvantages:

- The throughput of the network is similar to that of previously proposed opportunistic routing algorithms, and that is less.
- The energy distribution is not good when the network is of small size.

10. **QoS Aware Geographic Opportunistic Routing in WSNs:** Cheng *et.al.* have believed that QoS routing is very challenging and very important among all the research issues in WSNs (Cheng, Niu, Cao, Das, & Gu, 2014). QoS is very important and first and foremost requirement in the mission critical applications like monitoring and surveillance systems. These types of applications require time constrained and reliable delivery of data.

The authors tried to solve this kind of problems and proposed a new opportunistic routing protocol known as Efficient QoS-aware Geographic Opportunistic Routing (EQGOR) (Cheng et al., 2014). The protocol selects the forwarding candidate nodes in an efficient manner and then prioritized them, which improves the energy efficiency, latency and time complexity. The simulation of the protocol has been done with the help of network simulator NS2. It improves the ability and network lifetime of WSNs.

11. **SOFA - Communication in Extreme Wireless Sensor Networks:** Stop-On-First Acknowledgement (SOFA) (Cattani, Zuniga, Woehrle, & Langendoen, 2014) has been proposed by Cattani *et.al.* by utilizing the concepts of duty cycles. The authors have observed that WSNs can deliver up-to 99.9% of sensed data with duty cycles. But the performance is mainly dependent on various pre-assumed factors like low traffic rates, static sensor nodes etc. Authors have investigated these factors and

Routing Protocols in Wireless Sensor Networks

found that the assumptions are not always true in real life scenario. To overcome this problematic situation the authors have proposed SOFA routing protocol (Cattani et al., 2014). This protocol is based on the opportunistic any cast forwarding which can reduce the communication time of sensor nodes. This is a stateless algorithm which makes it to work with mobile sensors easily.

The protocol was implemented in Contiki OS and tested in simulation as well as on test-bed of 100 nodes also (Cattani et al., 2014).

Advantages:

- Communication between sensor nodes is reliable.
- SOFA can work with both static and mobile sensors.

Disadvantages:

- The algorithm was implemented in Contiki OS, and may not be compatible other operating systems available for WSNs.
 - The algorithm was tested on 100 nodes test-bed. But many applications require a WSN to have thousands of sensor nodes.
12. **Multi-Hop Optimal Position Based Opportunistic Routing for WSN:** Multi-hop Optimal Position based Opportunistic Routing (MOOR) (Yamuna Devi et al., 2014) have been proposed by Devi *et.al.* in 2014. The authors have utilizes the opportunistic routing and apply a broadcasting scheme to design this new protocol called as MOOR. The protocol considers the communication between source and destination pairs as most important.

MOOR decides the routes which are containing minimum number of hops between source and destination. The data packets will be transmitted on the route which is of smaller distance. MOOR has a good end-to-end delays and it also increases the lifetime of the network.

The average end-to-end delays by using MOOR are lesser than that of EEOR, to which the authors have compared it.

13. **Energy Efficient Opportunistic Multicast Routing Protocol in WSN:** Wen *et.al.* have proposed Energy Efficient Opportunistic Multicast Routing (EOMR) (Wen, Zhang, Yang, & Hou, 2014) for minimizing the energy consumption in multicast routing. Multicast is an important scenario in WSNs with respect to allocation of tasks and targeting the queries. Unicast in WSN results in high cost of communication and low efficiency and also in broadcasting there is wastage of radio link frequencies and bandwidth.

EOMR minimizes these kinds of problems in WSNs. The whole network has been divided into grids and each node has to locate its coordinate in a certain period of time. The sensor nodes in the network need not to know the topology of the entire network. But they form the topology within their own grid. Nodes then use the opportunistic routing to communicate data packets. The destination nodes have to decide the optimal route in the network with respect to number of hops and the communication cost. After deciding the route, the destination sends an acknowledgement to source along that optimal route.

As compared with the existing multicast routing protocols EOMR performance is good in terms of energy consumption, link reliability and delay reduction. The other version of this algorithm was also proposed by the authors known as E-OMRP (Energy efficient Opportunistic Multicast Routing Protocol) (Wen et al., 2014) which can work with mobile WSNs.

COMPARATIVE ANALYSIS AND CONCLUSION

Routing in WSN is very crucial task and has attracted attention of researchers in the recent years. In WSN routing challenges are different to that of traditional networks. This chapter presented classifications of routing protocols for WSN. Table 1 shows the categorization and characteristics of routing protocols in WSN.

The protocols which are mostly dependent on the network structure of WSN have been categorized as under network organization protocols. This category is further divided into three sub-categories. Firstly, the protocols which are based on the name of data and query are classified as data centric routing protocols. The protocols under this sub-category have very less computational overhead, but as the protocols are query and continuous data flow driven the communication cost (cost of transmission of data) is very high. The protocols do not optimize the route setup. Among all the protocols rumor routing and CADR are very good in reducing the overhead of communication. ACCQUIRE and R3E also perform well in low density WSN.

Second subcategory under network organization is the cluster based routing protocols, also called as hierarchical routing protocols. The protocols under this category are based on the grouping of sensor nodes in the network. The sensor nodes in the network relay the data towards the base station through cluster heads. The overhead in these types of protocols is the cluster formation and the cluster head selection. Cluster heads are the nodes which are less energy constrained. Cluster heads performs data aggregation of received sensed data and sends it towards the base station. The most interesting research issue in such protocols is the process of formation of clusters and the selection of cluster heads among different sensor nodes. The cluster formation should be in such a way so that it will increase the energy efficiency and reliability of the routing protocol. The process of data aggregation and fusion is also a very interesting issue in this category. The cluster based protocols proposed by researcher till date do not optimize the cluster head selection and do not provide the Quality-of-service.

The third subcategory protocols under network organization make use of location of sensor nodes and are categorized under location based routing protocols. The protocols in this category make use of sensor node location to find out the optimal routes. But these protocols are not energy efficient, mainly in mobile sensor networks. The energy aware approaches based on location of sensor nodes are used only for small networks, like the WSN which contain 50 to 100 sensors only. The open research issue in this area is how efficiently and cleverly the protocols utilize the location information about sensor nodes.

The protocols under network flow and QoS based routing tried to provide a quality of service in data delivery in WSN. Although all the previous category protocols try to reduce the communication cost of the network, but does not guarantee the reliable delivery of data. Quality-of-service is highly needed in case of video and imaging sensor networks in real time applications. In current literature a few protocols are proposed which try to provide the QoS in energy constrained WSN. Also the protocols in this category can be applied only in the applications of small WSN.

Routing Protocols in Wireless Sensor Networks

Table 1. Classification and comparison of routing protocols in WSN

Routing Protocol	Classification	Power Usage	Data Aggregation	Scalability	Query Based	Over head	Data Delivery Model	QoS
Flooding and Gossiping	Data Centric	High	Nil	Ltd.	No	Low	Continuous	No
SPIN	Data-centric	Ltd.	Yes	Ltd	Yes	Low	Event driven	No
DD	Data-centric	Ltd	Yes	Ltd	Yes	Low	Demand driven	No
EAR	Data-centric	Low	Nil	Ltd	No	High	Event Driven	No
RR	Data-centric	Low	Yes	Good	Yes	Low	Demand driven	No
CADR	Data-centric	Ltd	Yes	Ltd	Yes	Low	Continuously	No
COUGAR	Data-centric	Ltd	Yes	Ltd	Yes	High	Query driven	No
ACQUIRE	Data-centric	Low	Yes	Ltd	Yes	Low	Complex query	No
R3E	Data Centric	Low	Yes	No	No	Low	Continuous	No
LEACH	Hierarchical	High	Yes	Good	No	High	Cluster-head	No
PEGASIS	Hierarchical	Ltd	No	Good	No	Low	Chains based	No
TEEN & APTEEN	Hierarchical	High	Yes	Good	No	High	Active threshold	No
Younis <i>et.al.</i>	Hierarchical	Ltd	No	Ltd	Yes	Low	Cluster Based	No
SOP	Hierarchical	Low	No	Good	No	High	Continuous	No
MECN and SMECN	Location Based	Low	No	Good	Yes	High	Query Driven	No
GAF	Location	Ltd	No	Good	No	Mod	Virtual grid	No
GEAR	Location	Ltd	No	Ltd	No	Mod	Demand driven	No
Chang and Tassiulas	Network Flow and QoS Aware	Low	No	Ltd	No	Mod	Continuous	No
Kalpakis <i>et.al.</i>	Network Flow and QoS Aware	Low	Yes	Ltd	Yes	Mod	Continuous	No
SAR	Network Flow and QoS Aware	High	Yes	Ltd	Yes	High	Continuous	Yes
Akkaya and Younis	Network Flow and QoS Aware	Low	No	Ltd	No	Mod	Real Time Traffic	Yes
SPEED	Network Flow and QoS Aware	Low	No	Ltd	Yes	Less	Geographic	Yes
IDDR	Network Flow and QoS Aware	Low	No	No	No	Low	Continuous	Yes
EEOR	Network Flow and QoS Aware	Low	No	Good	No	High	Continuous	No
Ex-OR	Opportunistic	High	No	Good	No	High	Continuous	No
ORTR	Opportunistic	Low	No	Yes	No	Low	Real Time Traffic	No
ORW	Opportunistic	Low	No	Ltd	No	Mod	Continuous	No
EFFORT	Opportunistic	Ltd	No	Ltd	No	Mod	Active	Yes
ODEUR	Opportunistic	Low	No	Good	No	High	Continuous	No
Zeng <i>et.al.</i>	Opportunistic	High	No	Good	No	High	Continuous	Yes

continued on following page

Table 1. Continued

Routing Protocol	Classification	Power Usage	Data Aggregation	Scalability	Query Based	Over head	Data Delivery Model	QoS
FORLC	Opportunistic	Ltd	No	Ltd	No	Mod	Continuous	No
EAOR	Opportunistic	Low	No	Good	No	Mod	Continuous	Yes
EQGOR	Opportunistic	Low	No	Good	No	Low	Continuous	Yes
SOFA	Opportunistic	Low	No	Good	No	Low	Continuous	No
MOOR	Opportunistic	High	No	No	Yes	Low	Query Driven	No
EOMR	Opportunistic	Low	Yes	Good	Yes	Low	Query Driven	No

The other category discussed in this chapter is opportunistic routing. The WSN are opportunistic type of networks. Hence, the use of opportunistic routing in WSN is a very good idea. In this chapter the fourth classification of routing protocols as opportunistic routing protocols had been presented. Opportunistic routing is the recent research area in WSN and has attracted many researchers. There are some protocols presented in the table below which are recently proposed for WSN. Most of the opportunistic routing protocols provide energy efficiency, scalability and reliability. But quality of service is still a big research issue in this category. Also the opportunistic routing has not been yet applied to real life applications of WSN.

From the comparative analysis table it can be seen that the opportunistic routing protocols have very good performance. Also, if we have to work with thousands of sensor nodes in WSN, than we have to develop such routing protocols that can cope with the challenges in such large networks. From the literature we can see that most of the routing protocols work only with static WSN, but there is a requirement of mobile sensor networks in today’s scenario of applications. Hence, there is a need of routing

Table 2. Routing protocols in various applications

Application Type	Project	Node Deployment	Topology	Size	Routing Protocol
Habitat monitoring	Great Duck (Mainwaring, Culler, Polastre, Szewczyk, & Anderson, 2002)	Manual one time	Cluster Head	10-100	SPAN, GAF
Environment monitoring	PODS Hawaii (“PODS: A remote ecological micro-sensor network,”)	Manual one time	Multi-hop Multi-path	30-50	DD
	Food Detection (Bonnet, Gehrke, & Seshadri, 2000)	Manual	Multi-hop	200	COUGAR, ACQUIRE
Health	Artificial Retina (Schwiebert, Gupta, & Weinmann, 2001)	Manual one time	Cluster Head	100	LEACH
	Vital Sign (Baldus, Klabunde, & Muesch, 2004)	Manual	Star	10-20	GBR, SAR, SPEED
Military	Object Tracking (Romer, 2004)	Random	Multi-hop	200	GAF
Home/Office	Aware Home (Kidd et al., 1999)	Manual Iterative	Three Tiered	20-100	APTEEN, GEAR
Production/ Commercial	Cold Chain (W. R. Heinzelman et al., 2000)	Manual, Iterative	Three Tiered	55	SAR

protocols which can be operational in both static and mobile WSN. From the working of opportunistic based routing protocols it can be concluded that opportunistic routing is capable to cope with both static and mobile WSN.

Another future research issues in routing protocols is the integration of wireless and wired networks. Since the routing requirements of applications of WSN are different, so the research is necessary for handling each application with best route selection.

Table 1 summarizes the properties and classification of the routing protocols discussed in the previous sections. The table also incorporates the theoretical comparison based on the study of various routing protocols.

REFERENCES

- Abdellah, E., Benalla, S., Hssane, A. B., & Hasnaoui, M. L. (2010). Advanced low energy adaptive clustering hierarchy. *International Journal on Computer Science and Engineering*, 2(7), 2491–2497.
- Akkaya, K., & Younis, M. (2003, May). *An energy-aware QoS routing protocol for wireless sensor networks*. Paper presented at the 23rd International Conference on Distributed Computing Systems Workshops. doi:10.1109/ICDCSW.2003.1203636
- Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3), 325–349. doi:10.1016/j.adhoc.2003.09.010
- Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422. doi:10.1016/S1389-1286(01)00302-4
- Bakr, B. A., & Lilien, L. (2011, June 30-July 2). *Extending Wireless Sensor Network Lifetime in the LEACH-SM Protocol by Spare Selection*. Paper presented at the Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). doi:10.1109/IMIS.2011.142
- Baldus, H., Klabunde, K., & Muesch, G. (2004). *Reliable Set-Up of Medical Body-Sensor Networks*. In *Wireless Sensor Networks* (Vol. 2920, pp. 353–363). Springer Berlin Heidelberg.
- Biradar, R. V., Sawant, S. R., Mudholkar, R. R., & Patil, V. C. (2011). Multihop routing in self-organizing wireless sensor networks. *International Journal of Computer Science Issues*, 8(1), 155–164.
- Biswas, S., & Morris, R. (2005). *ExOR: opportunistic multi-hop routing for wireless networks*. Paper presented at the ACM SIGCOMM Computer Communication Review, Philadelphia, PA. doi:10.1145/1080091.1080108
- Bonnet, P., Gehrke, J., & Seshadri, P. (2000). Querying the physical world. *Personal Communications, IEEE*, 7(5), 10–15. doi:10.1109/98.878531
- Braginsky, D., & Estrin, D. (2002). *Rumor routing algorithm for sensor networks*. Paper presented at the 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, GA.
- Buettner, M., Yee, G. V., Anderson, E., & Han, R. (2006). *X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks*. Paper presented at the 4th international conference on Embedded networked sensor systems. doi:10.1145/1182807.1182838

- Cattani, M., Zuniga, M., Woehrle, M., & Langendoen, K. (2014). *SOFA: Communication in Extreme Wireless Sensor Networks*. In *Wireless Sensor Networks* (Vol. 8354, pp. 100–115). Springer International Publishing.
- Cheng, L., Niu, J., Cao, J., Das, S. K., & Gu, Y. (2014). Qos aware geographic opportunistic routing in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(7), 1864–1875. doi:10.1109/TPDS.2013.240
- Chu, M., Haussecker, H., & Zhao, F. (2002). Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. *International Journal of High Performance Computing Applications*, 16(3), 293–313. doi:10.1177/10943420020160030901
- Dargie, W. W., & Poellabauer, C. (2010). *Fundamentals of Wireless Sensor Networks: Theory and Practice*. Wiley.
- Dasgupta, K., Kalpakis, K., & Namjoshi, P. (2003). An efficient clustering-based heuristic for data gathering and aggregation in sensor networks. *Wireless Communications and Networking*, 3, 1948–1953.
- He, T., Stankovic, J., Lu, C., & Abdelzaher, T. (2003). *SPEED: A stateless protocol for real-time communication in sensor networks*. Paper presented at the 23rd International Conference on Distributed Computing Systems.
- Hedetniemi, S. M., Hedetniemi, S. T., & Liestman, A. L. (1988). A survey of gossiping and broadcasting in communication networks. *Networks*, 18(4), 319–349. doi:10.1002/net.3230180406
- Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, 4-7 Jan). *Energy-efficient communication protocol for wireless microsensor networks*. Paper presented at the 33rd Annual Hawaii International Conference on System Sciences Hawaii. doi:10.1109/HICSS.2000.926982
- Heinzelman, W. R., Kulik, J., & Balakrishnan, H. (1999, August). *Adaptive protocols for information dissemination in wireless sensor networks*. Paper presented at the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom'99), Seattle, WA. doi:10.1145/313451.313529
- Hung, C.-C., Lin, K. C.-J., Hsu, C.-C., Chou, C.-F., & Tu, C.-J. (2010). *On enhancing network-lifetime using opportunistic routing in wireless sensor networks*. Paper presented at the 19th International Conference on Computer Communications and Networks (ICCCN). doi:10.1109/ICCCN.2010.5560128
- Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000, August). *Directed diffusion: a scalable and robust communication paradigm for sensor networks*. Paper presented at the 6th annual international conference on Mobile computing and networking, Boston, MA. doi:10.1145/345910.345920
- Jae-Hwan, C., & Tassiulas, L. (2004). Maximum lifetime routing in wireless sensor networks. *IEEE/ACM Transactions on Networking*, 12(4), 609–619. doi:10.1109/TNET.2004.833122
- Jianwei, N., Long, C., Yu, G., Lei, S., & Das, S. K. (2013). R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks. *Industrial Informatics. IEEE Transactions on*, 10(1), 784–794. doi:10.1109/tii.2013.2261082

Routing Protocols in Wireless Sensor Networks

Kidd, C. D., Orr, R., Abowd, G. D., Atkeson, C. G., Essa, I. A., & MacIntyre, B. (1999, October). *The aware home: A living laboratory for ubiquitous computing research*. Paper presented at the International workshop on cooperative building. doi:10.1007/10705432_17

Kim, J., & Ravindran, B. (2009, March). *Opportunistic real-time routing in multi-hop wireless sensor networks*. Paper presented at the ACM symposium on Applied Computing. doi:10.1145/1529282.1529766

Krishnamachari, B., Estrin, D., & Wicker, S. (2002). *The impact of data aggregation in wireless sensor networks*. Paper presented at the 22nd International Conference on Distributed Computing Systems Workshops. doi:10.1109/ICDCSW.2002.1030829

Kumar, V., Jain, S., & Tiwari, S. (2011). Energy efficient clustering algorithms in wireless sensor networks: A survey. *International Journal of Computer Science Issues*, 8(5).

Landsiedel, O., Ghadimi, E., Duquennoy, S., & Johansson, M. (2012). *Low power, low delay: opportunistic routing meets duty cycling*. Paper presented at the ACM/IEEE 11th International Conference on Information Processing in Sensor Networks (IPSN). doi:10.1145/2185677.2185731

Li, Y., Liu, Y.-a., & Luo, P. (2009). *Link probability based opportunistic routing metric in wireless network*. Paper presented at the WRI International Conference on Communications and Mobile Computing (CMC'09). doi:10.1109/CMC.2009.170

Lindsey, S., & Raghavendra, C. S. (2002, March). *PEGASIS: Power-efficient gathering in sensor information systems*. Paper presented at the IEEE Aerospace conference proceedings, Big Sky, MT. doi:10.1109/AERO.2002.1035242

Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., & Anderson, J. (2002). *Wireless sensor networks for habitat monitoring*. Paper presented at the 1st ACM international workshop on Wireless sensor networks and applications.

Manjeshwar, A., & Agrawal, D. P. (2001, April). *TEEN: a routing protocol for enhanced efficiency in wireless sensor networks*. Paper presented at the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA. doi:10.1109/IPDPS.2001.925197

Manjeshwar, A., & Agrawal, D. P. (2002). *APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless*. Paper presented at the Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, Ft. Lauderdale, FL.

Manzoor, B., Javaid, N., Rehman, O., Akbar, M., Nadeem, Q., Iqbal, A., & Ishfaq, M. (2013). Q-LEACH: A new routing protocol for WSNs. *Procedia Computer Science*, 19, 926–931. doi:10.1016/j.procs.2013.06.127

Mao, X., Tang, S., Xu, X., Li, X.-Y., & Ma, H. (2011). Energy-efficient opportunistic routing in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(11), 1934–1942. doi:10.1109/TPDS.2011.70

- Min, R., Bhardwaj, M., Cho, S.-H., Shih, E., Sinha, A., & Wang, A. (2001). *Low-power wireless sensor networks*. Paper presented at the Fourteenth International Conference on VLSI Design. PODS: A remote ecological micro-sensor network. Retrieved from www2.hawaii.edu/~esb/pods/overview.html
- Rabaey, J. M., Ammer, M. J., da Silva, J. L., Patel, D., & Roundy, S. (2000). PicoRadio supports ad hoc ultra-low power wireless networking. *Computer*, 33(7), 42–48. doi:10.1109/2.869369
- Rodoplu, V., & Meng, T. H. (1999). Minimum energy mobile wireless networks. *IEEE Journal on Selected Areas in Communications*, 17(8), 1333–1344. doi:10.1109/49.779917
- Romer, K. (2004). *Tracking real-world phenomena with smart dust*. Paper presented at the 1st European Workshop on Wireless Sensor Networks, Berlin, Germany.
- Sadagopan, N., Krishnamachari, B., & Helmy, A. (2003). *The ACQUIRE mechanism for efficient querying in sensor networks*. Paper presented at the First IEEE International Workshop on Sensor Network Protocols and Applications. doi:10.1109/SNPA.2003.1203365
- Schurgers, C., & Srivastava, M. B. (2001). *Energy efficient routing in wireless sensor networks*. Paper presented at the Military Communications Conference (MILCOM) Communications for Network-Centric Operations: Creating the Information Force, McLeen. doi:10.1109/MILCOM.2001.985819
- Schwiebert, L., Gupta, S. K. S., & Weinmann, J. (2001, July). *Research challenges in wireless networks of biomedical sensors*. Paper presented at the 7th annual international conference on Mobile computing and networking (MobiCom '07). doi:10.1145/381677.381692
- Shah, R. C., & Rabaey, J. M. (2002, March). *Energy aware routing for low energy ad hoc sensor networks*. Paper presented at the IEEE Wireless Communications and Networking Conference, Orlando, FL. doi:10.1109/WCNC.2002.993520
- Sohrabi, K., Gao, J., Ailawadhi, V., & Pottie, G. J. (2000). Protocols for self-organization of a wireless sensor network. *IEEE Transaction on Personal Communications*, 7(5), 16–27. doi:10.1109/98.878532
- Spachos, P., Chatzimisios, P., & Hatzinakos, D. (2012). *Energy aware opportunistic routing in wireless sensor networks*. Paper presented at the IEEE GLOBECOM Workshops (GC Wkshps). doi:10.1109/GLOCOMW.2012.6477606
- Stehpanie, L., Raghavendra, C. S., & Krishna, M. S. (2001). *Data Gathering in Sensor Networks using the Energy Delay Metric*. Paper presented at the 15th International Parallel and Distributed Processing Symposium.
- Subramanian, L., & Katz, R. H. (2000, August). *An architecture for building self-configurable systems*. Paper presented at the First ACM/IEEE Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC), Boston, MA. doi:10.1109/MOBHOC.2000.869214
- Subramanian, L., & Katz, R. H. (2000, August). *An architecture for building self-configurable systems*. Paper presented at the First Annual Workshop on Mobile and Ad Hoc Networking and Computing, Boston, MA. doi:10.1109/MOBHOC.2000.869214
- Tilak, S., Abu-Ghazaleh, N. B., & Heinzelman, W. (2002). A taxonomy of wireless micro-sensor network models. *Mobile Computing and Communications Review*, 6(2), 28–36. doi:10.1145/565702.565708

Routing Protocols in Wireless Sensor Networks

Vuran, M. C., & Akyildiz, I. F. (2006). *Cross-layer analysis of error control in wireless sensor networks*. Paper presented at the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON'06) doi:10.1109/SAHCN.2006.288515

Wen, S., Zhang, Z., Yang, W., & Hou, S. (2014). An Energy-efficient Opportunistic Multicast Routing Protocol in Mobile Wireless Sensor Networks. *Journal of Networks*, 9(7), 1819–1827. doi:10.4304/jnw.9.7.1819-1827

Wenning, B.-l., Lukosius, A., Timm-Giel, A., Gorg, C., & Tomic, S. (2008). *Opportunistic distance-aware routing in multi-sink mobile wireless sensor networks*. Paper presented at the ICT mobilesummit

Xinhua, W., & Sheng, W. (2010). *Performance comparison of LEACH and LEACH-C protocols by NS2*. Paper presented at the Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), Hong Kong, China. doi:10.1109/DCABES.2010.58

Xu, Y., Heidemann, J., & Estrin, D. (2001, July). *Geography-informed energy conservation for ad hoc routing*. Paper presented at the 7th Annual ACM International Conference on Mobile computing and networking (MobiCom'01), Rome, Italy. doi:10.1145/381677.381685

Yamuna Devi, C. R., Shivaraj, B., Iyengar, S. S., Manjula, S. H., Venugopal, K. R., & Patnaik, L. M. (2014). *Multi-hop optimal position based opportunistic routing for wireless sensor networks*. Paper presented at the Region 10 IEEE Symposium.

Yao, Y., & Gehrke, J. (2002). The cougar approach to in-network query processing in sensor networks. *SIGMOD Record*, 31(3), 9–18. doi:10.1145/601858.601861

Younis, M., Youssef, M., & Arisha, K. (2002, October). *Energy-aware routing in cluster-based sensor networks*. Paper presented at the 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS), Fort Worth, TX.

Yu, Y., Govindan, R., & Estrin, D. (2001). *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks (ucla/csd-tr-01-0023)*. UCLA Computer Science Department.

Zeng, K., Lou, W., & Zhai, H. (2008, April). *On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks*. Paper presented at the The 27th Conference on Computer Communications, Phoenix, AZ.

Zhang, J., Ren, F., Gao, S., Yang, H., & Lin, C. (2015). Dynamic routing for data integrity and delay differentiated services in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 14(2), 328–343. doi:10.1109/TMC.2014.2313576

KEY TERMS AND DEFINITIONS

Broadcast: The nature of communication of the wireless medium networks like WSN which allows the nodes to transmit the data to every other node in the routing table. Opportunistic routing protocols utilizes the broadcasting nature of WSN to transmit data with good quality-of-service.

Communication Overhead: The total number of packets are to be transferred or transmitted from one node to another is known as the communication overhead. It includes the overhead of routing process, routing table and packet preparation in a sensor node.

Data Aggregation: Data aggregation is defined as the process of removing the duplicate data packets by combining the received and sensed data by a node. The data aggregation has been done by the nodes which are intermediate to source and sink/base station.

Deployment: The setting up of the network components in a network is known as deployment. In other words, the setting up of a functional sensor network in real world application/environment is known as deployment of.

Network Lifetime: Generally defined as the time during which the network is operational. In other words the lifetime of network is defined as the operational time of the network during which it is able to perform the dedicated task(s).

Opportunistic Routing: Opportunistic routing uses broadcast nature of wireless links and tries to solve all of communication problems in WSN. Any sensor node can overhear the packet, but, only one will forward the packet towards next-hop. The next-hop selection process is based on opportunistic decisions/rules.

Quality-of-Service (QoS): Quality-of-service is subjected to low-level, networking device observable attributes mainly bandwidth, delay, jitter, and packet loss rate. The QoS attributes in WSN are mainly dependent on the application like event detection level, tracking accuracy, event classification error and missing reports.

Routing: Routing is the process transmitting the data packet from source to destination via best routes within the network. It is basically the technique for the propagation of packets between multiple nodes.

Scalability: The ability of a sensor network to always perform equally irrespective of the increasing or decreasing size of the network. It is an important factor in WSN because there are thousand number of nodes present in the network.

Sink/Base Station (BS): A sink/base station is the type of sensor node which possesses high power, large memory and it is the entity, where information is required. Sink/base Station can be a part of the wireless sensor network field like sensor/actuator or it could be the node outside the field of sensors. It can also act as a gateway to other sensor nodes in the WSN field.

Topology: Topology is the way of arranging the entities of a network in such a way that it can operate efficiently and provide good quality-of-service. In other words, the organization of the all network components is known as topology.

An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks

Nagesh Kumar* and Yashwant Singh

Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan - 173234, Himachal Pradesh, India; engg.nagesh2@gmail.com, yashu_want@yahoo.com

Abstract

Objectives: Opportunistic Routing (OR) algorithms depends on metric design applied to the forwarder selection and prioritization. The objective is to define new OR metric, which reduces energy consumption in WSN. **Methods/Statistical Analysis:** In Wireless Sensor Network (WSN), sensor nodes have been supplied with a small amount of energy, using small size battery. Opportunistic Routing (OR) can minimize energy consumption by reducing delay and providing real time data delivery. OR reduces number of retransmissions in network by increasing the number of tentative forwarders. But most of the OR algorithms depends on metric design applied to the forwarder candidate selection and prioritization. **Findings:** In this paper, a new energy aware opportunistic routing metric called as Energy Depletion Factor (EDF) is proposed for WSN. This metric takes into consideration energy as well as delay. This metric can directly be used with existing opportunistic routing protocols. This metric extends the lifetime of the network by distributing energy consumption load equally in the network. It tells the routing algorithm that which forwarder node is having what impact on its battery life. EDF is local opportunistic routing metric, which reduces end-to-end delay in the network and also increases the network lifetime. To calculate EDF, the concept of residual energy of each node has been used. **Application/Improvements:** This metric can directly be used with existing opportunistic routing protocols. Simulation results presented the improvement of network lifetime and throughput by using EDF as a routing metric in WSN.

Keywords: Energy Depletion Factor, End-To-End Delay, Energy Efficiency, Network Lifetime, Opportunistic Routing Metric, Routing Algorithm

1. Introduction

Wireless sensor network is an emerging technology with a rapid increase in number of applications. Due to recent technical advancements in WSN, it is now feasible for sensor nodes not only to gather non-real time data but also to collect data in more problematical real-life applications. WSN has been prolonged to take account of actuator nodes with sensor nodes and some researchers call it as sensor and actuator networks¹.

As all the actuators and sensor nodes are energy constrained, the WSN researchers from different parts of world are trying to diminish the energy consumption and increasing the network lifetime of network. In real life applications of WSN, lifetime should be increased without risking the real time communication from node

to node or to base station (sink). Taking the example of surveillance system the data should be reported to base station within a few seconds of exposure. Unluckily, there are only few researches in the world which are working on real time communication in WSN.

There is a lot of research work that focuses upon the communication techniques because radio communication unit consumes most of the energy of sensor node. The receiver and transmit electronics consume almost about one thousand CPU units².

To reduce or optimize the energy consumption, lot of energy aware metrics was proposed in the literature. However, most of these ignore the real time aspect of the real-time requirements. In³ Proposed a real time power aware routing algorithm (RPAR, which decreases the communication delays in view of transmission power,

*Author for correspondence

in the workload of the network. The algorithm do not optimize the network lifetime. In² Proposed a routing algorithm which works in a real time scenario and try to reduce the network lifetime. But, in this algorithm the link reliability has not been considered and hence the algorithm's reliability also decreases. In WSN, a routing algorithm that does not consider the reliability of the link may suffer from high delays in delivering the packets and there will be increased number of retransmissions. This will increase the energy consumption.

To tackle with these problems⁴ designed a new protocol using Expected Transmission Count (ETX)⁵ as a metric and named it as ExOR (Exclusive Opportunistic Routing). This method is not mainly for WSN, because it do not consider the energy efficiency as its' primary objective. The idea was to reduce number of retransmissions of data packets. ETX was directly affects the throughput because it is based on the delivery ratios of wireless links.

In this paper the conception is to present a new opportunistic routing metric which can optimize between power consumption and delay in WSN. This paper tries to find out a new metric which can consider the requirements of real time communications, i.e. delay, energy and link reliability.

The rest of this research paper is organized as follows. In section 2, outline of related work will be given. Section 3 provides proposed routing metric and its mathematical analysis. Experimental analysis has been given in section 4. Simulations will compare the performance of proposed metric approach with the existing ones in this section. Finally, section 5 gives the conclusions.

2. Related Work

The most popular table-driven routing algorithms Ad-hoc on-demand Distance Vector (AODV) and Destination-Sequenced Distance Vector routing (DSDV), use smallest hop counting as a metric to decide the next forwarder node. AODV is also source initiated protocol⁶. Source initiated, here means that route will be decided only when there is a requirement by the source node. The routes have been maintained by the routing table as long as the source requires these routes. AODV neglects the energy issue and is not suitable for WSN.

For WSN several routing protocols has been proposed for example⁷⁻⁹. In⁹ Presents an energy metric which is optimally bounded and tries to increase the network lifetime⁸ have presented two energy efficient data forwarding

schemes for single link and multiple links. Authors are able to reduce the energy consumption through this metric and able to find a trade-off between energy and delivery rate. These schemes has been enhanced later in⁷, which considers the nodes' remaining energy into the forwarding metric. However, in all of these researches the consideration of delay in real-time applications is missing and there will be wastage of properties of broadcasting in wireless sensor networks.

Opportunistic routing metrics introduce the concept of reducing the number of retransmissions to save energy and taking the advantages of broadcasting nature of wireless networks. Broadcasting helps to discover as many paths in the network as possible. The transmission will takes place on any of these paths. If a path fails, the transmission can be completed by using some another path using other forwarder having the same packet.

As discussed earlier ETX was the first metric proposed for opportunistic routing in wireless networks. Working in the same direction many researchers have proposed new routing metrics such as EAX (Expected Any-path transmission)¹⁰, mETX (modified ETX)¹¹, ENT (Effective Number of Transmissions)¹¹, ETT (Expected Transmission Time)¹², EDR (Expected Data Rate)¹³, the EOT (Expected One hope Throughput)¹⁴, OEC (Opportunistic End-to-end Cost)¹⁵, and Opportunistic Expected One hope Throughput (OEOT)¹⁶ and designed algorithms based on these. The last two metrics illustrate the trade-off between the advancement of packets and the packet forwarding time by incorporating routing aspects related to advancements of packets, forwarding delay, and link reliability.

The computation of opportunistic routing metrics mentioned above can be divided into two classes (global or local) reliant on the routing facts collection model (whether local or global). A global cost metric has been, typically, preserved by source node in the network^{4, 10, 17-21} whether the local computation has been maintained in distributive manner^{14, 22, 23}. A very low overhead has been introduced in calculating local metrics, while global metrics may lead to high computation overhead because of acquiring whole network knowledge.²⁴ Presented a different opportunistic routing approach and routing metric which is based on the transmission power control while transmitting a packet. The energy cost will be dependent on the number of transmissions made to a particular forwarder. But, the overhead of changing transmission power every time and maintaining the record of each

node will be high. The proposed routing metric is also local in nature and perform distributive computations.

3. Proposed Routing Metric

Most of the researches discussed in related work above focuses transmission on unreliable links. In this paper new opportunistic energy efficient routing metric has been proposed, which extends the lifetime of the network by distributing energy consumption equally in the network. Lifetime here can be referred to as the percentile of nodes alive in the network after each round of routing. Basic energy cost model and the proposed metric has been given in the following subsections.

3.1 Energy Cost Model

In a wireless sensor network the sensor nodes have been supplied with a small amount of energy, depending on the application, using small size battery. Sensor nodes in WSN necessitate energy for sensing, processing, receiving and transmitting packets. The equations below given in²⁵, are the first order equalities for energy indulgence. A sensor node will take E_{Trans} energy when it wants to transmit n bit packet over distance l , it will be given by equation (1) below:

$$E_{Trans}(n, l) = \begin{cases} n.E_{R_elect} + n.E_{R_fs}.l^2, & \text{if } l < l_0 \\ n.E_{R_elect} + n.E_{R_amp}.l^4, & \text{if } l \geq l_0 \end{cases} \quad (1)$$

When a sensor node receives n bit packet, it will ingest $E_{Receive}$ amount energy given by equation (2) below:

$$E_{Receive}(n) = n.E_{R_elect} \dots \dots \dots \quad .. (2)$$

Whenever a forwarder candidate node have to send n -bit data packet toward the base station, it's transmit electronic circuit consumes, $E_{Forward}$ energy.

$$E_{Forward}(n, l) = E_{Trans}(n, l) + E_{Receive}(n) \\ = \begin{cases} 2n.E_{R_elect} + n.E_{R_fs}.l^2, & \text{if } l < l_0 \\ 2n.E_{R_elect} + n.E_{R_amp}.l^4, & \text{if } l \geq l_0 \end{cases} \quad (3)$$

The description of parameters for sensor nodes is given in table 1.

3.2 Energy Metric

The metric proposed in this paper is named as Energy Depletion Factor (EDF), because this metric tells the rout-

ing algorithm that which forwarder node is having what impact on its battery life. As said earlier by¹⁵ the transmission and reception energy for a packet may always be same for all nodes in the network but the impact of this energy consumption on life or residual energy of each node and also life of network will not always be same. For example, suppose that the residual energy of two nodes N_1 and N_2 is 6 units and 3 units, respectively. Also the distance of the next hope from N_1 is greater than that of N_2 . Now a single unit of energy consumption cost 50% of residual energy of N_1 and for N_2 it is 20%. In this scenario the node N_1 will die only after two transmissions. So in order to identify these types of impacts on the lifetime of the network EDF is aimed. Similar work has been done by¹⁵, but the metric proposed by them was fall in the category of global opportunistic metrics and the end-to-end delay in this case is high. EDF is local opportunistic routing metric, which reduces end-to-end delay in the network and also increases the network lifetime.

Table 1. Wireless parameters description

Parameter	Definition	Value/Unit
E_{R_elect}	Energy dissipation to run the radio	50 nJ/bit
E_{R_fs}	Free space model of transmitter amplifier	10 pJ/bit/m ²
E_{R_amp}	Multi-path model of transmitter amplifier	0.0013 pJ/bit/m ⁴
n	Data length	2,000 bits
l_0	Distance threshold	$\sqrt{\frac{E_{R_fs}}{E_{R_amp}}n}$

To calculate EDF, the concept of residual energy of each node has been used. Firstly, the scariness (SEC_{Ni}) on residual energy (RE_{Ni}) of a sensor node N_i has been calculated over energy consumption (EC), as follows:

$$SEC_{Ni} = \frac{EC}{RE_{Ni}} \dots \dots \dots \quad \dots \dots \dots (5)$$

SEC_{Ni} prevent the depletion of the whole energy of a node. Taking the example given earlier suppose some source node broadcast the packet to N_1 and N_2 (Neighbors of S). After receiving the packet the SEC_{Ni} for transmission is computed. According to the above example SEC_{Ni} cost of transmission for both N_1 and N_2 comes out to be 0.3008 and 0.88 respectively. Now as the distance of node N_1 is greater, but SEC_{Ni} is less than that of N_2 , it will

become the forwarder, and forward the packet first. If we choose N_2 as a forwarder because of less distance it will drains out of its energy soon, decreasing the network lifetime immediately as a result. This is the case of only transmission energy consumption. To compute SEC_{Ni} for all energy consumption in a node and the network EDF has been formulated. EDF metric contains the following components: 1) SEC_{Ni} cost from node to its forwarders, 2) SEC_{Ni} cost of receiving data, 3) the estimated SEC_{Ni} cost of retransmission, and 4) SEC_{Ni} cost of acknowledgement. The EDF for node N_i is computed hop-by-hop opportunistically by the following equation:

$$EDF_{Ni} = \frac{E_{tx:Ni \rightarrow fwd} + E_{rx:Ni} + E_{re_tx:Ni \rightarrow fwd} + E_{ACK:Ni \rightarrow source}}{RE_{Ni}} \dots (6)$$

Each term in this equation can be given in detail as below.

- a) $E_{tx:Ni \rightarrow fwd}$ is the SEC cost of the node N_i used in broadcasting the k -bit data packet from N_i to its' forwarders using transmission power E_{Trans} (equation (1)) and is given by the following formula:

$$E_{tx:Ni \rightarrow fwd} = \frac{E_{Trans}}{RE_{Ni}} \dots \dots \dots (7)$$

- b) $E_{rx:Ni}$ is the SEC cost of the node N_i used in receiving a k -bit data packet from source or other nodes receiving power $E_{Receive}$ (equation (2)) and is given by the following formula:

$$E_{rx:Ni} = \frac{E_{Receive}}{RE_{Ni}} \dots \dots \dots (8)$$

- c) $E_{re_tx:Ni \rightarrow fwd}$ is the SEC cost of retransmitting a packet to its' forwarders using transmission power E_{Trans} and receiving power $E_{Receive}$. This transmission and receiving cost has been combined into a single energy cost denoted as $E_{Forward}$ (equation (3)). This cost is given by the following formula:

$$E_{re_tx:Ni \rightarrow fwd} = \frac{E_{Forward}}{RE_{Ni}} \dots \dots \dots (9)$$

- d) $E_{ACK:Ni \rightarrow source}$ is the SEC cost of the node N_i in broadcasting the k -bit acknowledgement packet from N_i using transmission power E_{Trans} (equation (1)) and is given by the following formula:

$$E_{ACK:Ni \rightarrow source} = \frac{E_{Trans}}{RE_{Ni}} \dots \dots \dots (10)$$

After the calculation of all these values, EDF for node N_i is computed using equation (6). Similar process will be followed by other forwarder nodes in the forwarder list of source node. The forwarder with the minimum value of EDF will be the candidate who forwards the data packet first and rest of all nodes in forwarder list will wait for acknowledgement from this node. EDF will do energy consumption distribution, as there is not always a single node transmitting data again and again. The forwarder is selected on the go opportunistically.

4. Experimental Results and Performance Analysis

The following norms are considered in this research paper.

- a) Research considers that WSN contains a base station/sink and erratically dispersed static sensor nodes.
- b) Nodes produce data arbitrarily to transmit to base station.
- c) End-to-end delay has been considered as the time elapsed between initialization of communication from source node and reception of first packet at the base station.

4.1 Performance Analysis

The performance of proposed metric has been tested by performing simulations in MATLAB. Here, single base station application has been considered with static sensor nodes in a specified field. The transmission has been considered successful only when base station receives the packet. We have done many experiments considering the single base station only. The data source has been chosen randomly from N sensor nodes. The source chosen start transmitting the data towards base station by using multiple hops. The simulation will terminate the sensors having energy lower than 0.2 joules.

AODV routing is used as routing protocol in this paper. AODV has been modified to use proposed metric, minimum energy and minimum distance as next hop selection parameters. After this, we have compared the performances of all three types in terms of following performance parameters: 1) Network Lifetime, which is

defined as a percentage of energy available in the network and it depends on the number of dead nodes after each simulation rounds, 2) Throughput, which is defined as the average number of packets received at base station per round, 3) Path Loss, which is the loss of packets or bits during the transmission of packets, due to the transmission channel, 4) End-to-End Delay, which is the average time of transmitting data form source to sink per round.

Figure 1 show that the network lifetime in first few rounds is 100 percent because no node is dead by that time. But after some time nodes start decaying, and the network lifetime goes on decreasing until whole of the network stops functioning. The figure shows that the proposed metric presents better lifetime preservation than the other two metrics. From this we can depict the good performance of opportunistic routing metric. EDF selects best forwarder among all of the neighbors of source node. In figure 2, the throughput of the network can be seen. Throughput of the network is the biggest factor of network performance. Proposed opportunistic routing metric (EDF) has shown a far better throughput than the other schemes. The throughput depends on many factors, but in this case we have considered the number of packets received at base station per round. The number of packets transmitted and received depends on the lifetime of the network and also delay introduces in transferring the packets from source to base station.

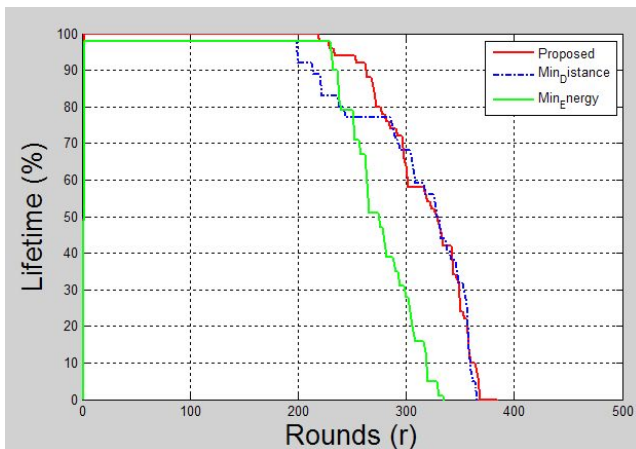


Figure 1. Network Lifetime.

Figure 3 shows the path loss incurred during the transmission of packets in each round of routing. Path loss is also a major factor, because number of successful packets received at base station depends on the path loss. If path loss is high, as in case of minimum energy

and minimum distance metrics, than number of packets dropped increases and throughput decreases. Also the number of retransmissions increases due to increase in path loss. Figure 4 gives the end-to-end delay, which shows the performance of the network in terms of reliable and efficient delivery of the packets. Again EDF shows good performance and reduces end-to-end delay during transmissions.

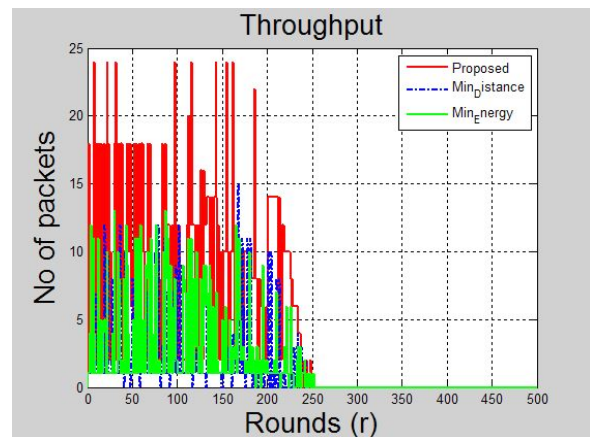


Figure 2. Throughput.

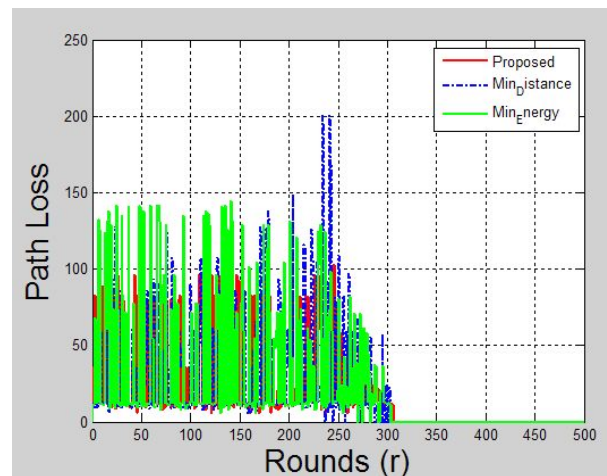


Figure 3. Path Loss.

5. Conclusion

In this paper, we have proposed an opportunistic routing metric called as EDF (Energy Depletion Factor). This metric is a distributed routing metric. The metric exploit the advantages of broadcasting in opportunistic routing and decide the next hop centered on the energy depletion of sensor nodes. The metric mutually contemplates the energy cost of transmission and residual energy of

each sensor and the transmission reliability through a particular neighbor. The routing metric can be efficiently computed at any node with a less overhead. The routing has been conducted by using AODV mechanism and selecting forwarders on the basis of proposed metric. Simulation results show that EDF increases the network lifetime, throughput by reducing the path loss and end-to-end delays.

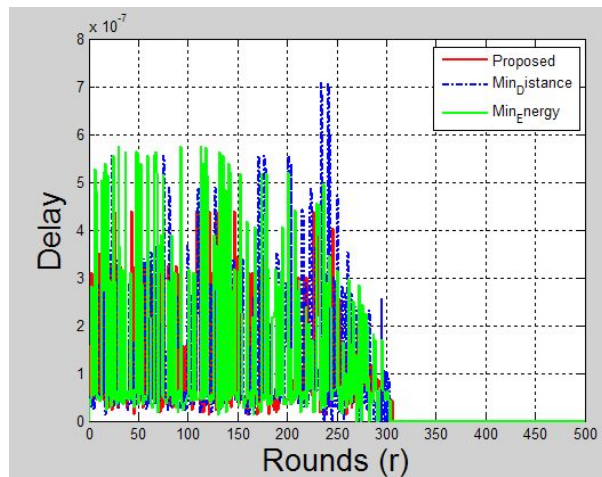


Figure 4. End-to-End Delay.

6. References

- Akyildiz IF, Kasimoglu IH. Wireless sensor and actor networks: research challenges. *Ad hoc networks*. 2004; 2(4):351–67.
- Ergen SC, Varaiya P. PEDAMACS: Power efficient and delay aware medium access protocol for sensor networks. *IEEE Transactions Mobile Computing*. 2006; 5(7):920–30.
- Chipara O, He Z, Xing G, Chen Q, Wang X, Lu C. Real-time power-aware routing in sensor networks. *Proceedings of 14th IEEE International Workshop on Quality of Service*, New Haven, CT. 2006; 83–92.
- Biswas S, Morris R. ExOR: Opportunistic multi-hop routing for wireless networks. *Proceedings of ACM SIGCOMM'05*, New York, USA. 2005; 133–44.
- De Couto DSJ, Aguayo D, Bicket J, Morris R. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*. 2005; 11(4):419–34.
- Royer EM, Perkins CE. An implementation study of the AODV routing protocol. *Proceedings of 3rd IEEE Wireless Communications and Networking Conference*, Chicago, IL. 2000. p. 1003–8.
- Busse M, Haenselmann T, Effelsberg W. A lifetime-efficient forwarding strategy for wireless sensor networks. *Wireless Sensor Network*. [Poster Abstract], 2006; 20.
- Busse M, Haenselmann T, Effelsberg W. An Energy-Efficient Forwarding Scheme for Wireless Sensor Networks. *Proceedings of WOWMOM'06*, IEEE Computer Society, Washington, DC, USA. 2005; 125–33.
- Cao Q, He T, Fang L, Abdelzaher TF, Stankovic JA, Son SH. Efficiency Centric Communication Model for Wireless Sensor Networks. *Proceedings of 25th IEEE INFOCOM*, Barcelona, Spain. 2006; 1–12.
- Zhong Z, Wang J, Nelakuditi S, Lu G-H. On selection of candidates for opportunistic anypath forwarding. *Proceedings of 10th ACM SIGMOBILE*, University of South Carolina, Columbia, SC. 2006; 1–2.
- Koksal CE, Balakrishnan H. Quality-aware routing metrics for time-varying wireless mesh networks. *IEEE Journal on Selected Areas in Communications*. 2006; 24(11):1984–94.
- Draves R, Padhye J, Zill B. Routing in multi-radio, multi-hop wireless mesh networks. *Proceedings of 10th Annual International Conference on Mobile Computing and Networking*, Microsoft Research Redmond, WA. 2004. p. 114–28.
- Park JC, Kasera SK. Expected data rate: an accurate high-throughput path metric for multi-hop wireless routing. *Proceedings of 2nd IEEE SECON'05*, Santa Clara, CA. 2005; 218–28.
- Zeng K, Lou W, Yang J, Brown Iii DR. On throughput efficiency of geographic opportunistic routing in multihop wireless networks. *Mobile Networks and Applications*. 2007; 12(5-6):347–57.
- Hung C-C, Lin KC-J, Hsu C-C, Chou C-F, Tu C-J. On enhancing network-lifetime using opportunistic routing in wireless sensor networks. *Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN)*, Zurich. 2010. p. 1–6.
- Hsu C-J, Liu H-I, Seah WKG. Opportunistic routing: A review and the challenges ahead. *Computer Networks*. 2011; 55(15):3592–603.
- Rozner E, Seshadri J, Mehta YA, Qiu L. SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks. *IEEE Transactions on Mobile Computing*. 2009; 8(12):1622–35.
- Dubois-Ferriere H, Grossglauser M, Vetterli M. Valuable detours: Least-cost anypath routing. *IEEE/ACM Transactions on Networking*. 2011; 19(2):333–46.
- Wei C, Zhi C, Fan P, Ben Letaief K. AsOR: an energy efficient multi-hop opportunistic routing protocol for wireless sensor networks over Rayleigh fading channels. *IEEE Transactions on Wireless Communications*. 2009; 8(5):2452–63.
- Wu J, Lu M, Li F. Utility-based opportunistic routing in multi-hop wireless networks. *Proceeding of 28th International Conference on Distributed Computing Systems ICDCS'08*, Beijing. 2008. p. 470–7.

21. Naghshvar M, Javidi T. Opportunistic routing with congestion diversity in wireless multi-hop networks. Proceedings of INFOCOM'10 IEEE, San Diego, CA. 2010; 1–5.
22. Chiarotto D, Simeone O, Zorzi M. Spectrum leasing via cooperative opportunistic routing techniques. IEEE Transactions on Wireless Communications. 2011; 10(9):2960–70.
23. Mao X, Tang S, Xu X, Li X-Y, Ma H. Energy-efficient opportunistic routing in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(11):1934–42.
24. Coutinho RWL, Boukerche A, Vieira LFM, Loureiro AAF. Transmission power control-based opportunistic routing for wireless sensor networks. Proceedings of 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Canada. 2014. p. 219–26.
25. Wang J, Kim J-U, Shu L, Niu Y, Lee S. A distance-based energy aware routing algorithm for wireless sensor networks. Sensors. 2010; 10(10):9493–511.
26. Mikkili RT, Thyagarajan J. A real-time routing protocol with controlled dissemination of data queries by mobile sink in wireless sensor networks. Indian Journal of Science and Technology. 2015 Aug; 8(19):1–10.
27. Baji BSK, Mohan Rao KRR. Improving the network life time of a wireless sensor network using the integration of progressive sleep scheduling algorithm with opportunistic routing protocol. Indian Journal of Science and Technology. 2016 May; 9(17):1–6.
28. Vinothini M, Umamakeswari A. Reliable data transmission using efficient neighbor coverage routing protocol in wireless sensor network. Indian Journal of Science and technology. 2014 Dec; 7(12):2118–23.

An Energy Efficient and Trust Management based Opportunistic Routing Metric for Wireless Sensor Networks

Nagesh Kumar

Department of CSE and IT
Jaypee University of Information Technology
Waknaghat, Solan, INDIA-173234
engg.nagesh2@gmail.com

Yashwant Singh

Department of CSE and IT
Jaypee University of Information Technology
Waknaghat, Solan, INDIA-173234
yashu_want@yahoo.com

Abstract— Applications of Wireless Sensor Networks (WSN) require reliable delivery of unaltered data. Data security in transit is an important issue for reliable delivery of data in WSN. Existing cryptographic methods are not meet the requirements for WSN because of their limited resources and opportunistic behavior of wireless nodes. In last four years, reputation and trust aware methods are used to solve the issue of security in WSN. In this paper, we have defined a novel opportunistic routing (OR) metric for sensor networks. The metric is derived by using energy consumption and trustworthiness of sensor nodes. The simulation result shows that the metric is able to detect a malicious activity in the network segment. This metric effectively and efficiently prevent from malicious activities and maintain data integrity.

Keywords- WSN, Trust, Secure Routing, Opportunistic Routing, Routing Metric.

I. INTRODUCTION

WSN are considered to be an emerging area of research due to large and excellent applications. Distributed sensing and control areas are being enabled in last four years due to a extensive range of real time applications of ubiquitous computing [1]. Development of small sized sensor nodes gave the freedom for researchers to obtain information from unobtainable situations (like under ocean), and in other hostile environments (like battlefield). Most attractive applications of WSN include defense, environmental monitoring, health care and infrastructural [2]. To obtain high quality of data from WSN, sensor nodes must cooperate within the network for distribution and gathering of data and for sharing topology information. Because of hostile nature of deployment field, sensor nodes are in a lot of risk of external and internal attacks [2]. Hence, there is a need of security during communication between sensors in the network.

Cryptographic algorithms are not efficient in case of energy and storage in WSN, because of inadequate resources available in between sensor nodes [3]. Hence, there is a need of cooperation among sensor nodes in the network for security purpose. But, taking the assumption of hundred percent coordination is not valid. Sensor nodes in the deployment fields can easily be misconfigured, captured or hijacked by the attackers. The attackers may try to inject false information in

the network or try to destroy the network. However in recent years, researchers [4-8] have proposed cryptography based routing algorithms/protocols, but these algorithms are mostly provide solution for outside attacks. These algorithms are ineffective when there are insider attacks from malicious sensor nodes. If we apply cryptographic algorithms for fighting with inside attacks, than a lot of energy will be wasted and network dies soon. Hence there should be cooperation and trust management between sensor nodes. To make successful deliveries of data packets at base station the trust management must be applied to routing process. The sensor nodes which are having low trust values must not be included in routing process.

As WSN are opportunistic networks in nature [9], rather than using fixed path routing, opportunistic routing is very useful. But, when we talk about secure opportunistic routing protocols/algorithms, either there are no proposed secure OR protocols/algorithms in literature or there are very few which are not much efficient in terms of energy and storage. The OR protocols must provide security and efficiency together. The security in opportunistic routing protocols can be improved by applying routing decisions on the basis of trust values of sensor nodes in the network. To increase the probability of a packet to reach destination, sensor nodes can utilize the trust based route dependability information.

In opportunistic routing major phases are: forwarder set selection and forwarder node selection. The source, when has data to be sent over wireless link, firstly choose the forwarder set from the neighbor set. For this purpose there is a requirement of certain criteria to be set. The forwarder set selection process exclude those nodes which are not able to fulfill the criteria. After this process the candidate forwarder is selected and given high priority on the basis of opportunistic routing metric (like ETX [10], mETX [11], EAX [12] etc.). The routing decision in OR is purely dependent upon the metric chosen for selecting candidate forwarder node [13].

In this paper, a novel trust aware and energy efficient opportunistic routing metric has been proposed which is specially designed for OR protocols in WSN. This metric will be compatible with previously proposed OR protocols for WSN. The metric not only expand the lifespan of the network

but also reliability and integrity of data. Major contributions of this research work are given below.

- A novel OR metric is developed, which contemplates the node trust value and energy efficiency as major design factors. The parameters for designing the trust aware and energy efficient OR metric are energy of the nodes, trust assessment of nodes and packet delivery ratio among nodes.
- Simulation has been planned and implemented to check performance of proposed OR metric and framework applied to existing OR protocols. Simulation results validate that incorporating the proposed trust metric into Destination Sequenced Distance Vector Routing (DSDV) protocol. It can considerably increase the efficiency and reliability of DSDV communications among nodes in unfriendly surroundings.

The rest of the research paper is prepared as follows. Section 2 contains literature review of research in simple OR protocols and trust based OR protocols in sensor networks. A broad description of the proposed trust and energy aware opportunistic routing metric is presented in Section 3. Section 4 covers the simulation and evaluation of the proposed work in view of various network constraints. Lastly, Section 5 concludes the paper and discuss certain forthcoming works.

II. RELATED WORK

This section presents a view on previously completed research work in OR protocols and trust management in WSN. This section gives an overview of few important and efficient protocols and provide a short explanation of trust and reputation management systems for WSN.

The reason behind choosing OR for WSN is to increase the reliability of communication among nodes and availability of data on time. Most of the research in OR protocols focuses on the candidate selection and coordination among nodes. Liu et al. [14], Hsu et al. [13], and Boukerche and Darehshoorzadeh [15] published detailed reviews on OR notions, representations, and classifications.

The first and popular OR protocol has been proposed by Biswas and Morris [2], and called as EXOR [10]. The authors shown that this new idea of routing can work more efficiently and effectively in wireless networks. They have developed a metric, known as Expected Transmission Count (ETX) [10], for forwarder candidate set selection. This metric computes the number of transmissions required for data packet to reach terminus. Forwarder candidate nodes was chosen from the set of neighbor nodes. Later Expected anypath transmission (EAX) [12] metric has been proposed by Dubois-Ferrie`re et al. [16]. On the basis of this metric they have proposed an OR protocol and named it as LCOR. But, EAX is computationally complex and expensive for large scale wireless networks. Similar to EXOR, [17] presented SOAR which utilizes ETX as metric for forwarder selection, but it mainly tries to reduce number of replicated data packets to be received at destination node. In existing OR protocols the focus has been given on timely data delivery and no or very little emphasis has been given to security of data and routes in communication.

Security is always crucial in wireless networks, as the data packets are sent on unsecured and open wireless links [18]. Cryptography methods provide external security to the network, so that any attacker from outside cannot harm the network [3]. But to cope with internal attacks there is a need of coordination among nodes and security within the network. To provide internal security in WSN there is a need of lightweight methods. Because, sensor nodes have less capabilities like less energy, low storage and small computation power etc. Trust and management systems are very lightweight and easily computable and improve security of communication within the network.

Researchers in recent year have developed trust and reputation management protocols and algorithms for ad-hoc networks, internet of things and other mobile wireless networks. Some common names of protocols include CONFIDANT [19], CORE [20] and SORI [21] etc. Salehi et al. [22] has proposed three metrics and a trust based routing context for wireless networks recently. There have proposed three routing metrics i.e. RTOR [22], TORDP [22] and GEOTOR [22], for opportunistic routing protocols for calculating the trust value. They have proposed a trust aware opportunistic routing protocol previously, which is also developed for wireless networks. But these all are not purely meant for WSN and does not work well in sensor networks. Also for opportunistic routing, to the top of our knowledge, a few trust based systems have been proposed in the past.

Trust management in WSN has also been focused during last three years. As sensor nodes have limited resources, researchers try to balance between security and utilization of resources. Deng et.al. have proposed a dynamic routing structure for WSN, which incorporates social network theories of trust and named it as TARF [23]. TARF uses conventional cryptographic approaches as complementary methods and provide security solutions for WSN. Energy efficiency is an issue in this protocol. Working in WSN security EMPIRE [24] protocol has been proposed. This is probabilistic and distributed monitoring approach. It tries to decrease monitoring tasks per node and save energy, by maintaining the appropriate security level. Another trust based routing protocol for WSN has been proposed and named as ETARP [25]. This protocol define routing paths on the basis of maximum utilization of resources with lesser communication cost. But this is also not, much energy efficient approach having greater overhead. Recently, TESRP [26] has been proposed by Ahmed et.al which is also designed to save energy and lower the cost and overhead in routing process for WSN. TLAR [27] has been proposed especially for WSN. TLAR calculates the consolidated trust values using direct and indirect observations of its neighbors. This routing scheme adjust the route weight values dynamically again and again. This increase the overhead and communication delay introduces.

In this research work we have presented a trust based energy efficient opportunistic routing metric for WSN. It is being evaluated by extensive simulations to check the effect of new metric on various performance parameters. The routing metric proposed here has been checked with existing broadcasting algorithm DSDV.

III. TRUST AWARE ENERGY EFFICIENT OR METRIC

As discussed in literature very few researchers have focused on security and energy efficiency in opportunistic routing for WSN. In this research a new trust aware energy efficient opportunistic routing metric has been proposed, provide security of data in transit and improve lifetime of the network. Energy cost model will be the same as in our research paper published recently [28].

In opportunistic routing the most important phase is considered is the forwarder candidate set selection. In wireless sensor network, after sensing data, each sensor node form a list of its neighbors. From neighbor list, the forwarder candidates has been chosen and is given a priority value. The highest priority node will first transmit the data first. Opportunistic routing make it possible to utilize broadcasting nature of wireless links. To find the best wireless link routing metrics have been applied to OR.

In this section a new opportunistic metric has been introduced especially for OR protocols in WSN. This metric is distributive in nature. This metric needs information about forwarder nodes' ID, energy and packet reception ratio. After collection of these values, the node calculates forwarding ratio, acknowledgement impact and energy consumption. By including these all values trust value has been calculated. Distance (D) between nodes is not required as major criteria, especially for opportunistic routing in WSN. Hence, distance will be used only for checking the packet forwarding progress (PF) towards destination (Eq. 1 and Eq. 2).

$$Dist_{i,j} = \sqrt{(x_{co_i} - x_{co_j})^2 + (y_{co_i} - y_{co_j})^2}$$

$$\text{where } 0 \leq i, j \leq k, \text{ and } i \neq j \quad (1)$$

$$PF_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d}$$

$$\text{where } s=\text{source, } d=\text{destination, } 0 \leq n_i \leq k \quad (2)$$

A. Proposed Metric

In opportunistic routing the forwarder node and the path of data packets have been decided at the time of transmission. Each sensor node maintain a matrix of trust evaluation factors about other nodes and calculate the trust value for each forwarder candidate in neighbor list. Metric calculation involves two step process as described in below.

Step 1: Trust Evaluation

In this step, sensor node, when has data to send, form its neighbor list and extract the forwarder candidates on the basis of packet reception ratio (PRR) as calculated below in Eq. 3.

$$PRR_i = \frac{P_{received}}{P_{sent}}$$

$$\text{where } 0 \leq PRR_i \leq 1 \quad (3)$$

As soon as the forwarder list has been made, the nodes now start calculating the trust value for each node in forwarder list. The trust calculation phase contains following trust elements.

- 1) Node Identification (ID): This factor contains the location information and the identity of the forwarder candidate node. Source node collect this information from each node in the forwarder list.

$$ID_i = \langle NodeID_i, Location_coordinates_i, Energy_i \rangle$$

where $0 \leq i \leq k$

- 2) Forwarding Sincerity (F): This factor represents, whether the forwarder candidate node is forwarding the data packets successfully or not. This record is maintained by using the calculation of success and failure counts. Initially this value will be 1 for each forwarder node.

- F_i : Forwarding sincerity of node i
- FS_i : Forwarding success count of node i
- FF_i : Forwarding failure count of node i .

- 3) Energy Depletion (E): This factor calculates the energy consumption for each transmission made by a node. This factor is based on the information of node's total energy. Also. This factor is used to calculate the lifetime of the node and the network. This factor is used to check whether the energy depletion is greater than threshold or not. If it is greater than threshold than the node cannot transfer data packets and excluded from the forwarder set. Otherwise a priority has been set according to the value of this factor.

- E_{total_i} : Total energy impact of node i

$$E_{total} = E_{total} - (E_{tx} + E_{rx} + E_{ack}) \quad (4)$$

where, E_{tx} : Transmission energy, E_{rx} : Receiving energy, E_{ack} : Acknowledgement sending and receiving energy.

- 4) Acknowledgement Sincerity (ACK): This factor calculates the acknowledgement sending and receiving sincerity among nodes. This record is maintained by using the calculation of success and failure counts of acknowledgements transmissions. Also, this value is useful to calculate the probability of retransmission of packets. Initially this value will be 1 for each forwarder node.

- ACK_i : Acknowledgement sincerity of node i
- $SACK_i$: Acknowledgement success count of node i
- $FACK_i$: Acknowledgement failure count of node i .

- 5) Trust Value (T): This factor gives the total trust value of a node and it will be estimated on the basis of all

trust evaluation factors. This value is dynamic in nature, because it needs to update again and again for every new transmission of data packets.

- T_i : Trustworthiness of node i .

Step 2: Trust Value Calculation

All trust evaluation factors, discussed above, values has been recorded in a matrix. As these values are discrete, we cannot directly judge the value in a logical decision of trusting a node or not. Hence, the next step is to quantize the values of trust factors, so that the values will be transformed into incessant values from -1 to +1. Here -1 means no trust and +1 means full trust. Trust quantification for every trust element can be calculated as below:

- 1) Forwarding Sincerity

$$F_i = \frac{FS_i - FF_i}{FS_i + FF_i}, \text{ subject to } -1 \leq F_i \leq 1 \quad (5)$$

- 2) Energy Depletion Value

$$E_{total_i} = \frac{E_{rx} + E_{rx} + E_{ack}}{E_{total}}, \text{ subject to } -1 \leq E_{total_i} \leq 1 \quad (6)$$

- 3) Acknowledgement Sincerity

$$ACK_i = \frac{SACK_i - FACK_i}{SACK_i + FACK_i}, \text{ subject to } -1 \leq ACK_i \leq 1 \quad (7)$$

Finally using these values total trust has been computed, which involves the weighting process. Each trust evaluation factor has been assigned a weight. The weights represents the importance of each trust factor. The value will be 0 for unimportant factor and 1 for most important factor. These weights are dependent on the type of the applications of WSN. After the completion of this process the trust value will be calculated by the following equation.

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma}, \text{ where } -1 \leq \alpha, \beta, \gamma \leq 1 \quad (8)$$

Here, α is the weight adjustment for forwarding sincerity, β is the weight adjustment for Energy depletion and γ is the weight adjustment for acknowledgement sincerity. If the energy value is lower than specified verge, than node will be excluded from the forwarder list, because this node is not able to forward data packets. And the value of trust, T_i in this case will be -1.

As each sensor is involved in calculating the trust value in the network, some malicious nodes which are creating problems like inconsistent data, malicious data, and blocking data packets at one point can be detected and reported in this step.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section depicts the security and energy performance of proposed trust aware opportunistic routing metric. The metric

has been applied in DSDV protocol and simple DSDV [29], Ad-hoc On Demand (AODV) [30] and modified DSDV (proposed) has been tested in WSN scenario. The security performance comprises the average number of malicious nodes have encountered during a transmission. A specific malicious ratio has been given in every simulation. On the other hand, energy performance is calculated by checking the energy efficiency of each node after each successful or unsuccessful transmission in the presence of malicious nodes.

A. Simulation Setup

The simulations has been carried out by using MATLAB. The scenario considered over here contains single base station with static sensor nodes in a field of 500 x 500 m. Transmission has been considered successful only when base station receives the packet. Many experiments has been conducted considering single base station and continuous communication model with N sensor nodes. The source has been chosen randomly, which will initiate the communication.

TABLE I. SIMULATION PARAMETERS

Parameter	Description
Area	500 x 500 m
Range of Radio	200 m
Number of Nodes	50-100
Type of Traffic	Constant Bit Rate (CBR)
Size of Packet	127 bytes
Data Rate	20 kbps
SNR Threshold	10
Initial Energy	10.0 J
Electronic Energy	$50 * 10^{-9}$ J

At a time only one source node has been selected and it will forward the data towards sink/base station using multiple hops. The simulation will terminate the sensors having energy lower than 0.001 joules. For physical and data link layers, IEEE 802.15.4 framework has been chosen, which perfectly fits for low data rate applications and it provides long lifetime of batteries of nodes [31]. As mentioned in [31], constant bit rate traffic with a data rate, 20 kbps with a packet size, 127 bytes has been simulated here. Table 1 shows the simulation settings in MATLAB.

B. Experimental Results

The number of nodes considered here varies from 50 to 100 deployed in the simulation area. One can deploy nodes in any field of application as the position of nodes is random. This metric can be applied to any application of WSN.

a) *Safety Performance*: The safety performance has been measured for three protocols i.e. DSDV, AODV and modified DSDV. The different malicious nodes percentages (5%-20%) has been considered during simulation. It has been assumed that as the mischievous sensor nodes ratio increases in the network, the difficulty in managing security in route setup has

been rises. It can be seen from figure 1 that the average risk level of modified DSDV has been lower as matched to DSDV and AODV protocols. This is because, in AODV and DSDV while choosing the next-hop for data transmission do not consider the values of number of successful transmission and node energy. When a mischievous node is chosen as next-hop it will not forward the packet or drop the packet. This malicious node will be detected in modified DSDV using proposed trust aware metric and will be avoided for the next transmission. This conclude that trust aware metric can attain a high level of security.

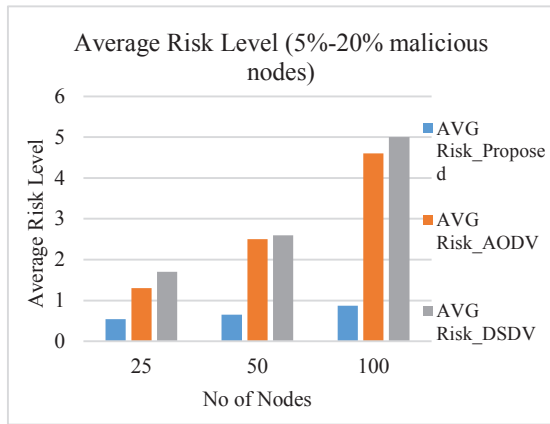


Figure 1: Average Risk Level

From figure 1 the average risk level increases as there is increase in the number of mischievous nodes in network. The risk level for all three protocols increase as mischievous nodes increase in the network, because of the problem in choosing nodes as next-hop. Every time a malicious node drop the packet, there is a need of setting up route again and retransmitting missing packets. As the average risk level in AODV and DSDV is high, we can conclude that, there is no security has been considered in the routing metric of these protocols.

b) Energy Efficiency Performance: To test the energy performance of three protocols, general energy model has been considered from our previously published research paper [28]. Figure 2 shows average energy cost for different simulations under different malicious nodes ratios (5%-20%). It can be observed from figure 2 that modified DSDV with proposed metric shows high energy efficiency as compared to AODV and DSDV. AODV and DSDV shows poor performance in terms of energy efficiency. Figure 3 shows the average network lifetime which varies with number of nodes and the number of malicious nodes. Proposed metric shows good performance in maintain good lifetime, but reduces in performance when the mischievous nodes increases in the network. Energy efficiency reduces because, if there are larger number of mischievous sensor nodes in the network, there will be problems in route setup. End-to-end delay will be increases and also the path loss increases (figure 4 and figure 5) in this case.

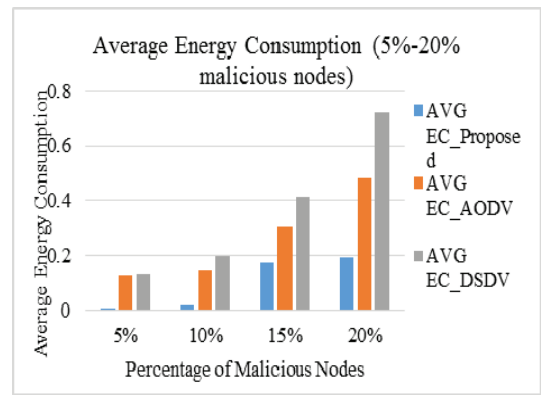


Figure 2: Average Energy Consumption

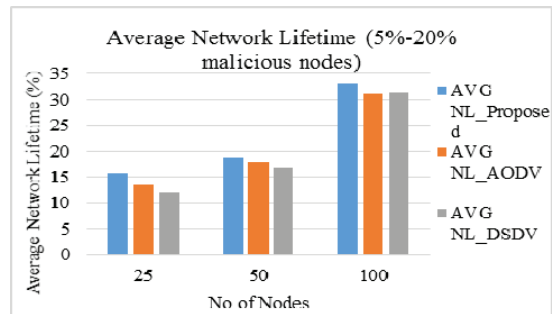


Figure 3: Average Network Lifetime

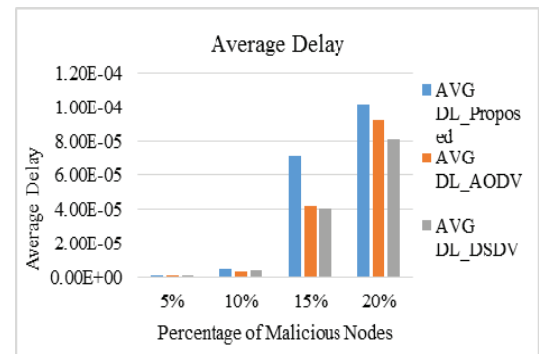


Figure 4: Average End-to-End Delay

From overall results obtained above it can be concluded that the proposed metric works well with DSDV in maintaining the safety and energy efficiency in the network. Proposed metric has advantages of equal energy load distribution and maintaining security, over existing route setup metrics used in AODV and DSDV. The only disadvantage is that the end-to-end delay will be high due to little computation overhead.

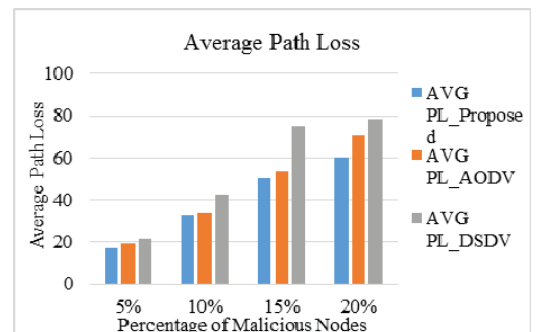


Figure 5: Average Path Loss

V. CONCLUSION AND FUTURE SCOPE

In this research work, we have developed a new trust and energy aware routing metric and applied it to DSDV protocol. The routing metric focuses on the trustworthiness and efficiency of sensor nodes in the network. The trustworthiness can be computed as a factor of forwarding sincerity, energy cost and acknowledgement sincerity of a node. These factors are most important for the existence and successful operation of WSN in unfriendly situation and malicious attacks. The routing metric can be viewed as a composite metric. It assigns weights for energy, forwarding sincerity and acknowledgement sincerity of a node. If a node is not satisfying in these three sincerity conditions, it will not be considered as next-hop for data transmission. The route selection has been improved and false link failure notifications has been avoided. The simulation results have shown the betterment of the proposed metric in terms of safety and energy efficiency.

In future, we will propose a new secure trust based opportunistic routing protocol to reduce end-to-end delays and increased security of data in transit. We will aim to simulate the trust based routing metric in presence of other potential security attacks like wormhole, selfish, and Sybil attack.

REFERENCES

- [1] Akyildiz, I.F., and Kasimoglu, I.H.: 'Wireless sensor and actor networks: research challenges', *Ad hoc networks*, 2004, 2, (4), pp. 351-367
- [2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E.: 'Wireless sensor networks: a survey', *Computer networks*, 2002, 38, (4), pp. 393-422
- [3] Mohindru, V., and Singh, Y.: 'Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack', *Indian Journal of Science and Technology*, 2016, 9, (32), pp. 1-7
- [4] Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y., and Pande, A.: 'SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs', *Computer Communications*, 2015, 59, pp. 37-51
- [5] Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., and Song, Y.-J.: 'Group-based trust management scheme for clustered wireless sensor networks', *IEEE transactions on parallel and distributed systems*, 2009, 20, (11), pp. 1698-1712
- [6] Yao, L., Man, Y., Huang, Z., Deng, J., and Wang, X.: 'Secure Routing based on Social Similarity in Opportunistic Networks', *IEEE Transactions on Wireless Communications*, 2016, 15, (1), pp. 594-605
- [7] Yao, Z., Kim, D., and Doh, Y.: 'PLUS: Parameterized and localized trust management scheme for sensor networks security', in *proceedings of International Conference on Mobile Ad Hoc and Sensor Systems (IEEE, 2006)*, Vancouver, BC, pp. 437-446
- [8] Zhou, Y., Tan, X., He, X., Qin, G., and Xi, H.: 'Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature', *Information Assurance and Security Letters 1 (2010)*, 2010, pp. 18-23
- [9] Kumar, N., and Singh, Y.: 'Routing Protocols in Wireless Sensor Networks', in *Niranjan, K.R., and Ashok Kumar, T. (Eds.): 'Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures'* (IGI Global, 2016), pp. 86-128
- [10] Biswas, S., and Morris, R.: 'ExOR: opportunistic multi-hop routing for wireless networks', in *Proceedings of 35th SIGCOMM Computer Communication Review (ACM, 2005)*, Philadelphia, Pennsylvania, USA, pp. 133-144
- [11] Koksal, C.E., and Balakrishnan, H.: 'Quality-aware routing metrics for time-varying wireless mesh networks', *IEEE Journal on Selected Areas in Communications*, 2006, 24, (11), pp. 1984-1994
- [12] Zhong, Z., Wang, J., Nelakuditi, S., and Lu, G.-H.: 'On selection of candidates for opportunistic anypath forwarding', *ACM SIGMOBILE Mobile Computing and Communications Review*, 2006, 10, (4), pp. 1-2
- [13] Hsu, C.-J., Liu, H.-I., and Seah, W.K.G.: 'Opportunistic routing : A review and the challenges ahead', *Computer Networks*, 2011, 55, (15), pp. 3592-3603
- [14] Liu, K., Abu-Ghazaleh, N., and Kang, K.-D.: 'Location verification and trust management for resilient geographic routing', *Journal of Parallel and Distributed Computing*, 2007, 67, (2), pp. 215-228
- [15] Boukerche, A., and Darehshoorzadeh, A.: 'Opportunistic routing in wireless networks: Models, algorithms, and classifications', *ACM Computing Surveys (CSUR)*, 2015, 47, (2), pp. 22
- [16] Dubois-Ferriere, H., Grossglauser, M., and Vetterli, M.: 'Valuable detours: Least-cost anypath routing', *IEEE/ACM Transactions on Networking*, 2011, 19, (2), pp. 333-346
- [17] Rozner, E., Seshadri, J., Mehta, Y.A., and Qiu, L.: 'SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks', *IEEE Transactions on Mobile Computing*, 2009, 8, (12), pp. 1622-1635
- [18] Hui-hui, D., Ya-jun, G., Zhong-qiang, Y., and Hao, C.: 'A wireless sensor networks based on multi-angle trust of node', in *Proceedings of International Forum on Information Technology and Applications (IEEE, 2009)*, Chengdu, China, pp. 28-31
- [19] Ganeriwal, S., Balzano, L.K., and Srivastava, M.B.: 'Reputation-based framework for high integrity sensor networks', *ACM Transactions on Sensor Networks (TOSN)*, 2008, 4, (3), pp. 15
- [20] Michiardi, P., and Molva, R.: 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks': 'Advanced communications and multimedia security' (Springer, 2002), pp. 107-121
- [21] He, Q., Wu, D., and Khosla, P.: 'SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks', in *Proceedings of Wireless communications and networking conference (IEEE, 2004)*, Atlanta, GA, USA, pp. 825-830
- [22] Salehi, M., Boukerche, A., Darehshoorzadeh, A., and Mammeri, A.: 'Towards a novel trust-based opportunistic routing protocol for wireless networks', *Wireless Networks*, 2016, 22, (3), pp. 927-943
- [23] Deng, H., Yang, Y., Jin, G., Xu, R., and Shi, W.: 'Building a trust-aware dynamic routing solution for wireless sensor networks', in *Proceedings of Globecom Workshops (IEEE, 2010)*, Miami, Florida, USA, pp. 153-157
- [24] Maarouf, I., Baroudi, U., and Naseer, A.R.: 'Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks', *IET communications*, 2009, 3, (5), pp. 846-858
- [25] Gong, P., Chen, T.M., and Xu, Q.: 'ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks', *Journal of Sensors*, 2015, 2015
- [26] Adnan, A., Kamalrulnizam Abu, B., Muhammad Ibrahim, C., and Abdul Waheed, K.: 'A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network', *Mob. Netw. Appl.*, 2016, 21, (2), pp. 272-285
- [27] Vamsi, P.R., and Kant, K.: 'Trust and Location-Aware Routing Protocol for Wireless Sensor Networks', *IETE Journal of Research*, 2016, 63, pp. 1-11
- [28] Kumar, N., and Singh, Y.: 'An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks', *Indian Journal of Science and Technology*, 2016, 9, (32), pp. 1-7
- [29] Perkins, C.E., and Bhagwat, P.: 'Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers', in *Proceedings of SIGCOMM computer communication review (ACM, 1994)*, New York, USA, pp. 234-244
- [30] Perkins, C., Belding-Royer, E., and Das, S.: 'Ad hoc on-demand distance vector (AODV) routing', No. RFC 3561, 2003
- [31] Chang, J.-H., and Tassioulas, L.: 'Energy conserving routing in wireless ad-hoc networks', in *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE, 2000)*, Tel Aviv, Israel, pp. 22-31

Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Networks

Nagesh Kumar¹, Yashwant Singh², Pradeep Kumar Singh¹

¹*Department of Computer Science and Engineering,
Jaypee University of Information Technology,
Waknaghat, Solan, INDIA-173234*

²*Department of Computer Science and Information Technology
Central University of Jammu, INDIA
engg.nagesh2@gmail.com*

Abstract—Selection of the best next-hop in Opportunistic Routing (OR) is a crucial task in wireless sensor networks (WSN). To increase the throughput, network lifetime and reliability of WSN, there is a need of an optimal OR protocol. To improve the reliability of network, reputation management is important. Reputation management gives a chance to nodes to transmit data on secure and reliable routes. This paper gives a new reputation based OR metric and protocol, in which the next hop selection is based on its reputation. The proposed OR metric considers the reputation level as a primary selection parameter for next-hop. New OR metric relies on energy efficiency and packet delivery ratio of next-hop. Proposed OR protocol selects all middle position neighbors as next-hop and potential forwarder will be decided on the basis of new OR metric. Energy consumption is considered to be dynamic. The protocol has been compared with Middle Position Dynamic Energy Opportunistic Routing (MDOR), and Trust and Location Aware Routing Protocol (TLAR). Simulation results depict that the proposed OR protocol optimized the throughput and network lifetime.

Index Terms—End-to-end Delay; Energy Efficiency; Next-Hop Selection; Reputation; Trust; Opportunistic Routing; Throughput.

I. INTRODUCTION

WSN are most demanded networks in present scenario because of their abundance of applications in real life like defense, environment, and health. In most of the applications the sensor nodes are left unattended, and expected to operate on their own [1, 7]. Although, sensor nodes in WSN are resource constraints having less capabilities, less energy and less storage capacity. Hence, the researchers have to focus on the development of protocols which are able to work with these constraints. Also, the unattended nodes are prone to several attacks, which in turns reduces the capabilities of the network. Most important capability parameters for WSN are throughput, end-to-end delay, and network lifetime (energy efficiency). The performance of these parameters is dependent on routing protocols, and security methods used while transmitting data.

In recent years, OR has been introduced as a new routing paradigm to be used in ad-hoc and sensor networks. OR methods select a set of potential forwarder nodes, which will cooperate to forward data toward base-station (sink/destination) [7]. The idea of designing OR is to utilize the broadcasting property of wireless nodes. The selection of

potential forwarders is based upon a routing metric, which is used to shortlist these forwarders from neighbor list. The set of shortlisted candidates is called as candidate set. Next-hop forwarder will be a node in between this candidate set, which is being chosen on the basis of next-hop selection metric.

Researchers [10, 11] have focused on developing new OR metrics [23] for candidate set selection and also forwarder candidate selection. These metrics can be implemented as end-to-end selection metrics or local selection metrics. The end-to-end selection method selects the candidate set on the basis of delivery probability of links from source to destination. While, in the case of local selection methods, candidate set has been decided on the basis of neighborhood information only. Local selection metrics introduces an improvement in reducing delays in the network [23]. In both candidate selection methods it is being assumed that sensor nodes will coordinate with each other. But in a real scenario, if a node has been affected by a malicious attack, then it may or may not coordinate with other nodes. For example, in a black-hole attack the affected node stop forwarding the packets towards other nodes. These types of problem need special treatment mechanisms in routing algorithms.

Working in this direction, there is a huge research has been carried out to tackle with security attacks on routing process. But most of the methods are based on cryptosystems [2-6] which are not efficient in resource constrained WSN. Hence, trust and reputation based methods have been introduced in recent years. These trust and reputation models are the subsets of security methods. These methods use trust based metrics, and if a node having inappropriate trust metric value it will be isolated from the neighbor list of each node.

This paper introduces a novel reputation based OR metric. This metric considers energy efficiency and reputation of a node on the basis of the packet forwarding ratio (PFR), to select next-hop candidate forwarders. The paper proposes an extension to the previous work, i.e. middle position dynamic energy OR algorithm. It is being extended to improve energy efficiency and provide reputation based security for network and data.

The structure of the rest of the paper is as follows. The next section of the paper presents the research related to OR and reputation based routing protocols by other authors. A broad description of the proposed reputation and energy aware OR protocol has been presented in section 3. Section 4 covers the performance analysis and simulation of the

proposed work in view of various network constraints. Lastly, section 5 concludes the paper and discuss certain forthcoming works.

II. RELATED WORK

This section provides a brief view of related research work carried out for OR and reputation management, in recent years. This section describes energy efficient OR protocols, and reputation based routing protocols.

ExOR [8] the first OR protocol was introduced to increase the overall throughput of wireless ad-hoc networks. The idea was to utilize the broadcasting capabilities of wireless antenna. The protocol was based on a metric called as expected transmission count (ETX) [8]. This metric calculates the minimum number of transmissions required to send a packet from source to destination. Working in the same direction expected any path transmission (EAX) [9] was proposed, which was more efficient for WSN than ETX. Based on this metric an OR protocol was proposed named as LCOR [12]. This protocol was expensive in terms of energy for large scale WSN. SOAR [13] has been developed recently by using ETX as next-hop selection metric. It reduces the number of duplicate packets in the network. Middle position dynamic energy OR (MDOR) [24] was proposed to reduce the end-to-end delay and improve network throughput. MDOR is good in terms of optimizing the network lifetime and end-to-end delays. It selects middle sensor node from the neighbor list on the basis of the location of the node. In these simple OR protocols the focus has been given on timely data delivery and a little focus has been given on energy efficiency and security of communication process and data.

Trust and reputation management methods are of greater interest in WSN. Because, these methods are lightweight in terms of calculation and energy consumption. There are some trust and reputation aware protocols proposed in the last five years like CONFIDANT [14], CORE [15], and SORI [16] etc. As far as OR is concerned there are very few trust aware OR methods are available in the literature. Salehi et.al [17] have proposed OR framework on the basis of their proposed metrics (RTOR, TORDP and GEOTOR). But this framework is mainly concerned for wireless ad-hoc networks and performance will be degraded in wireless sensor networks. For WSN few researchers have developed trust aware routing methods like TARF [18], EMPIRE [19], ETARP [20], TLAR [22] and TESRP [21].

This paper presents a reputation based OR protocol, which is the extension to MDOR [24] and provide data reliability and good throughput in the presence of malicious nodes. The protocol will be briefly discussed in the upcoming section. New OR protocol is reputation and energy efficiency based and hence is more reliable than MDOR.

III. PROPOSED WORK

The proposed OR protocol considers reputation and energy efficiency as major components of candidate selection metric. The reputation of a node is used to isolate the malicious sensor nodes from neighbor list. The energy efficiency component calculates the effect of each transmission on the energy of transmitting and receiving nodes. Every time the algorithm run in the network the new candidate set for each node may not be the same always.

Following sub-sections discuss the proposed work in detail.

A. Forwarder Selection Metric

The proposed forwarder selection metric has two components: packet forwarding ratio and energy effect. Packet forwarding ratio is used to identify the nodes which are not sincerely forwarding the received packets and not acknowledging the packets forwarded toward them. *PFR* for a node *i* can be calculated by the following equation.

$$PFR_i = \frac{P_fwd_{i \rightarrow next_hop}}{P_sent_{source \rightarrow i}} \quad (1)$$

where, $P_fwd_{i \rightarrow next_hop}$ is the number of packet forwarded by the node *i* towards its next-hop node and $P_sent_{source \rightarrow i}$ is the number of packets sent by the source node towards node *i*.

The second component is the energy effect calculation on a node's total energy. This effect is dependent upon the energy consumed during transmission, reception and sensing acknowledgements. This effect on energy consumption for each node can be calculated as follows.

$$E_effect = \frac{E_{receiving} + E_{transmitting} + E_{ack_sending}}{E_{total}} \quad (2)$$

Receiving ($E_{receiving}$), transmitting ($E_{transmitting}$) and acknowledgement ($E_{ack_sending}$) sending energies have been calculated as given in MDOR [24]. Total energy (E_{total}) is the amount of energy remaining in the corresponding sensor node. After calculation of these two components the reputation value (T_Value) of a sensor node is calculated by the following equation.

$$T_Value = \frac{\alpha.PFR + \beta.E_effect}{\alpha + \beta} \quad (3)$$

Here, α and β are the adjustment values for both trust value components *PFR* and E_effect respectively. These are the weights according assigned to the components on the basis of the importance of each factor.

B. Reputation based Energy Efficient OR Protocol

In WSN the sensor node collects data from the field and send it toward base station. OR utilizes multiple routes advantage of wireless links, and selects one of the best suitable routes for data communication. As discussed in MDOR [24] it selects the forwarder nodes from the neighbor list, which are neither near nor too far away from the destination. This protocol optimizes the distance of the forwarder from source and destination. This process continues till the data packets reach the destination. But as we can see there is no mechanism of avoiding a malicious node in MDOR [24]. We have introduced a reputation management for the middle position nodes.

For the middle position sensor nodes, the trust aware forwarder selection metric has been calculated. If the T_Value is below a certain threshold, then it will not be selected as next-hop. This node will be removed from forwarder list. The trust value (T_Value) threshold has been fixed to 0.2 in our algorithm. This value has been fixed after

extensive simulations has been carried out with different trust values like 0.1, 0.2, 0.3... 1. If the trust value is too higher than most of the nodes will not be able to transmit data after some energy consumption. This is because the trust value is dependent on energy consumption of the node. Also, if the trust value is very low than a single node will be selected again and again to transmit data. This is because we are selecting only middle nodes as next forwarder. This process of trust value calculation will be repeated for all nodes until the destination is reached. For every new data transmission the trust value has been updated by recalculation. The algorithm below shows the new Reputation based Energy Efficient OR Protocol. Also a flowchart has been given in Figure 1.

Input: source node S, target node D, dist(S, D). Output: Successful transmission of data packet from node S to node D 1. Define S as Source Node 2. Create neighbor list NGH for S 3. Sort neighbor list according to distance 4. if D is neighbor of S 5. Send data packets to D 6. else 7. FNL is the subset of NGH (FNL is the forwarder node list) 8. Select the middle node (FWD) from FNL i.e. (neither near to S nor near to T). 9. Calculate trust value (T_Value) for each middle node using equation 3. 10. if $T_Value \geq 0.2$ 11. Start communication with FWD 12. else 13. { 13. Discard FWD from FNL. 14. Select second middle node from FNL and name it as FWD. 15. Repeat from step 9 to 14 16. } 17. if FWD is equal to D then stop algorithm 18. else repeat step 2 to step 18 until D is reached

Whole algorithm works same as MDOR except that it calculates the trust value for each node on forwarder list and select forwarder on the basis of this trust value. As the trust value considers forwarding sincerity as a parameter, the attacks like a black hole, worm hole can be detected and prevented easily in this case. Also trust value considers the energy consumption effect also there will be improvement in lifetime of sensor node and obvious improvement in network lifetime of WSN.

IV. SIMULATION RESULTS AND ANALYSIS

The performance of proposed protocol has been recorded in the presence of malicious nodes and compared to two other algorithms i.e. MDOR [24] and TLAR [22], which are proposed recently for WSN. TLAR is a trust and location aware routing protocol, which calculates trust value for the nodes in between the source and destination nodes. It has considered five trust metrics for trust value calculation.

A. Simulation Parameters

The performance of proposed algorithm has been tested by creating simulation using NS2. Table 1 shows the settings of parameters in NS2 simulation environments.

All the three protocols have been built over NS-2.35 and being tested for performance parameters. For the purpose of getting a better view of analysis the protocols have been tested by generating a different number of malicious nodes in the network. All the malicious node has been chosen randomly. The malicious node behaves differently in the network. Such as they do not forward the received packets,

send no acknowledgements and do not coordinate properly with other normal nodes in the network.

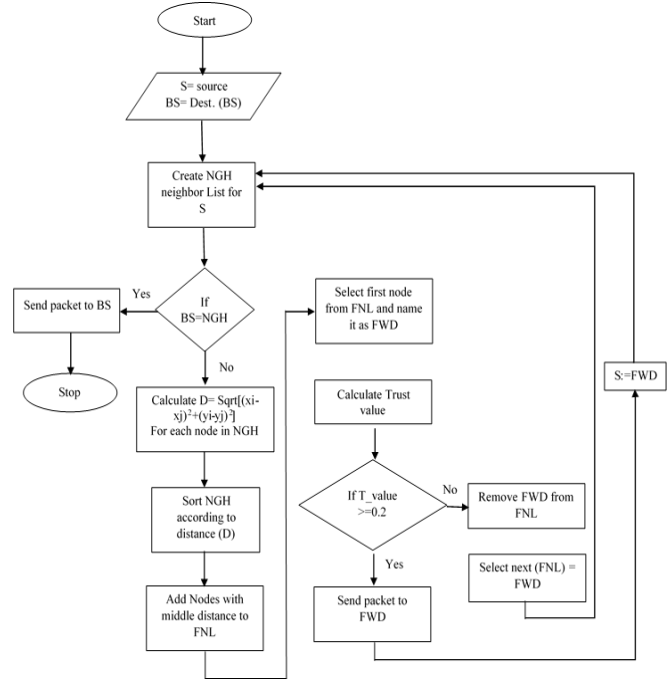


Figure 1: Reputation Based Energy Efficient OR Protocol

Table 1
Parameters for Simulation

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 x 500 m ²
Transmission Range	60 m
No. of Nodes (N)	100
No. of Malicious nodes	10, 20, 30, 40 and 50
Traffic Type	CBR (Constant Bit Rate)
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	100J
Initial Trust Value	1
Default α and β	0.4 and 0.3
Energy dissipation to run the radio ($E_{electronic}$)	50 nJ/bit
Buffer Length	30 packets

B. Results and Discussions

The network performance has been measured for all three protocols, and presented in the form of graphs. Figure 2 shows the performance of protocols on the basis of the packet delivery ratio (PDR) in the presence of malicious nodes. It can be seen that the proposed method has moderately high PDR as compared to MDOR [24] and TLAR [22]. This is due to the fast calculation of reputation value in the case of the proposed protocol. MDOR does not have any method to tackle with malicious nodes.

Hence, with the increase in malicious nodes packet delivery ratio for MDOR decreases rapidly. In TLAR, as discussed earlier, there is a need to calculate five trust metrics and hence this will increase overhead. Therefore, TLAR shows low performance as compared to the proposed approach.

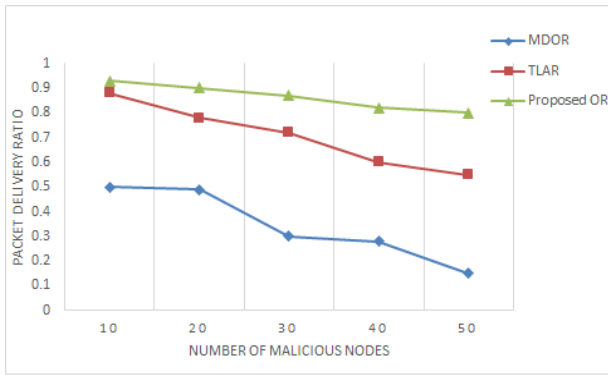


Figure 2: Comparison of MDOR, TLAR and Proposed OR in terms of Packet Delivery Ratio

Figure 3 presents the End-to-End delay. It can be depicted from the figure that end-to-end delay in case of MDOR is low because of the absence of reputation and trust methods. But in case of TLAR and Proposed protocol the end-to-end delay goes on fluctuating around similar values. If we talk about average End-to-End delay, proposed protocol shows little bit improvement over TLAR. This is because of the less overhead for the calculation of reputation values in the case of the proposed protocol.

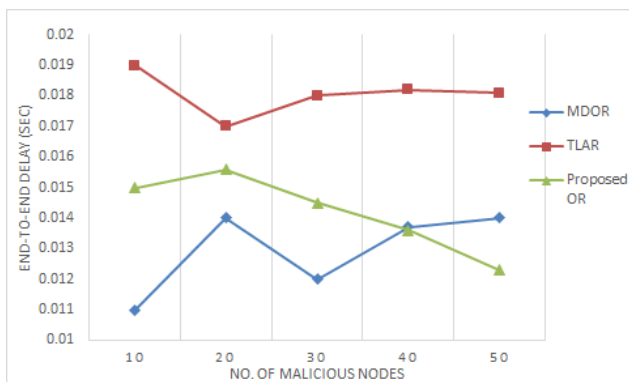


Figure 3: Comparison of MDOR, TLAR and Proposed OR in terms of End-to-End Delay

Figure 4 plots the energy consumption in the network. It is defined as the average energy consumption per node in the network, while performing the various tasks in the network. Most of the energy consumed in transmitting and receiving packets during network operation. Hence the energy consumption directly proportional to the radio energy consumption while transmitting and receiving packets. Proposed OR protocol has the lowest energy consumption as compared to TLAR and MDOR. MDOR mainly meant for dynamic energy consumption and do not work well when the energy consumption for transmission and reception of packets has been fixed. Similarly TLAR is mainly designed to provide secure routing and energy efficiency has not been paid much attention. Hence, proposed protocol works better. As far as the energy efficiency of the network has been improved, the network lifetime will automatically be increased.

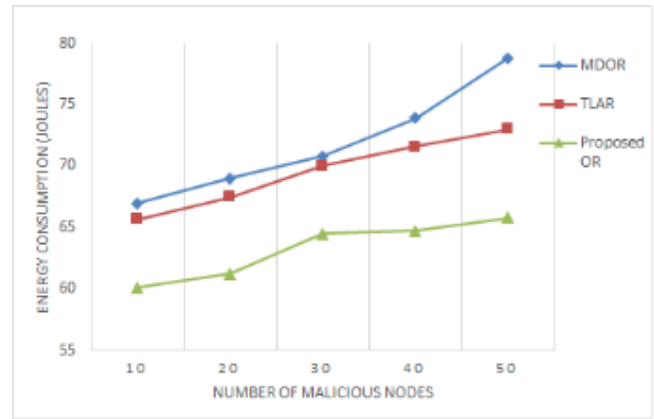


Figure 4: Comparison of MDOR, TLAR and Proposed OR in terms of Energy Consumption

V. CONCLUSION

In this paper, a novel OR protocol has been presented, which introduces reputation awareness in the next-hop selection. Reputation management is an important feature. It can be used to avoid a number of unnecessary and duplicate transmissions in the presence of malicious nodes. Also the proposed protocol is energy efficient, because it considers the effect of each transmission and reception of packets on node's total energy. The proposed protocol's candidate forwarder selection metric is composed of these two components. The simulation and performance analysis has been done by comparing the proposed protocol, MDOR and TLAR. The results showed that proposed OR protocol has good performance in the presence of malicious nodes. The proposed method optimizes the energy efficiency, end-to-end delay and packet delivery ratio in WSN. In the future direction we can consider more parameters and metrics' components to improve network performance by considering the properties of WSN.

REFERENCES

- [1] Akyildiz, I.F., and Kasimoglu, I.H.: 'Wireless sensor and actor networks: research challenges', *Ad hoc networks*, 2004, 2 (4), pp. 351-367.
- [2] Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y., and Pande, A.: 'SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs', *Computer Communications*, 2015, 59, pp. 37-51.
- [3] Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., and Song, Y.-J.: 'Group-based trust management scheme for clustered wireless sensor networks', *IEEE transactions on parallel and distributed systems*, 2009, 20 (11), pp. 1698-1712.
- [4] Yao, L., Man, Y., Huang, Z., Deng, J., and Wang, X.: 'Secure Routing based on Social Similarity in Opportunistic Networks', *IEEE Transactions on Wireless Communications*, 2016, 15 (1), pp. 594-605.
- [5] Yao, Z., Kim, D., and Doh, Y.: 'PLUS: Parameterized and localized trust management scheme for sensor networks security', in *proceedings of International Conference on Mobile Ad Hoc and Sensor Systems (IEEE)*, Vancouver, BC, 2006, pp. 437-446.
- [6] Zhou, Y., Tan, X., He, X., Qin, G., and Xi, H.: 'Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature', *Information Assurance and Security Letters* 1, 2010, pp. 18-23.
- [7] Kumar, N., and Singh, Y.: 'Routing Protocols in Wireless Sensor Networks', in *Niranjan, K.R., and Ashok Kumar, T. (Eds.): 'Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures'* (IGI Global, 2016), pp. 86-128.
- [8] Biswas, S., and Morris, R.: 'ExOR: opportunistic multi-hop routing for wireless networks', in *Proceedings of 35th SIGCOMM Computer*

- Communication Review (ACM, 2005), Philadelphia, Pennsylvania, USA, pp. 133-144.
- [9] Zhong, Z., Wang, J., Nelakuditi, S., and Lu, G.-H.: 'On selection of candidates for opportunistic anypath forwarding', ACM SIGMOBILE Mobile Computing and Communications Review, 2006, 10 (4), pp. 1-2.
- [10] Hsu, C.-J., Liu, H.-I., and Seah, W.K.G.: 'Opportunistic routing: A review and the challenges ahead', Computer Networks, 2011, 55 (15), pp. 3592-3603.
- [11] Liu, K., Abu-Ghazaleh, N., and Kang, K.-D.: 'Location verification and trust management for resilient geographic routing', Journal of Parallel and Distributed Computing, 2007, 67 (2), pp. 215-228.
- [12] Dubois-Ferriere, H., Grossglauser, M., and Vetterli, M.: 'Valuable detours: Least-cost anypath routing', IEEE/ACM Transactions on Networking, 2011, 19 (2), pp. 333-346.
- [13] Rozner, E., Seshadri, J., Mehta, Y.A., and Qiu, L.: 'SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks', IEEE Transactions on Mobile Computing, 2009, 8, (12), pp. 1622-1635
- [14] Ganeriwal, S., Balzano, L.K., and Srivastava, M.B.: 'Reputation-based framework for high integrity sensor networks', ACM Transactions on Sensor Networks (TOSN), 2008, 4 (3), pp. 15.
- [15] Michiardi, P., and Molva, R.: 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks': 'Advanced communications and multimedia security' (Springer, 2002), pp. 107-121.
- [16] He, Q., Wu, D., and Khosla, P.: 'SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks', in Proceedings of Wireless communications and networking conference (IEEE, 2004), Atlanta, GA, USA, pp. 825-830.
- [17] Salehi, M., Boukerche, A., Darehshoorzadeh, A., and Mammeri, A.: 'Towards a novel trust-based opportunistic routing protocol for wireless networks', Wireless Networks, 2016, 22 (3), pp. 927-943
- [18] Deng, H., Yang, Y., Jin, G., Xu, R., and Shi, W.: 'Building a trust-aware dynamic routing solution for wireless sensor networks', in Proceedings of Globecom Workshops (IEEE), Miami, Florida, USA, 2010, pp. 153-157.
- [19] Maarouf, I., Baroudi, U., and Naseer, A.R.: 'Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks', IET communications, 2009, 3 (5), pp. 846-858.
- [20] Gong, P., Chen, T.M., and Xu, Q.: 'ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks', Journal of Sensors, 2015.
- [21] Adnan, A., Kamalrulnizam Abu, B., Muhammad Ibrahim, C., and Abdul Waheed, K.: 'A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network', Mob. Netw. Appl., 2016, 21 (2), pp. 272-285.
- [22] Vamsi, P.R., and Kant, K.: 'Trust and Location-Aware Routing Protocol for Wireless Sensor Networks', IETE Journal of Research, 2016, 63, pp. 1-11.
- [23] Kumar, N., and Singh, Y.: 'An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks', Indian Journal of Science and Technology, 2016, 9 (32), pp. 1-7.
- [24] Sharma, M., & Singh, Y. Middle Position Dynamic Energy Opportunistic Routing for Wireless Sensor Networks. In IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 948-953.

An Energy Efficient Trust Aware Opportunistic Routing Protocol for Wireless Sensor Network

Nagesh Kumar, Jaypee University of Information Technology, Wanknaghat, India

Yashwant Singh, Central University of Jammu, Jammu, India

Pradeep Kumar Singh, Department of CSE and IT, Jaypee University of Information Technology, Wanknaghat, India

ABSTRACT

As the wireless sensor networks (WSN) are gaining popularity the need of reliable delivery of data packets becomes more important. The reliable delivery is only possible when the routing protocols are efficient and secure. Because of lack of resources it is not possible to use existing cryptosystems to provide security in WSN. But, trust aware routing can provide the security with lesser resources, which become popular in last three to four years. In this paper, a new energy efficient and trust aware reliable opportunistic routing (TAEROR) protocol is proposed. The protocol consists of a trust metric and also a relay selection algorithm. The trust aware metric detects the malicious nodes on the basis of forwarding sincerity, energy consumption and acknowledgement sincerity. Relay selection algorithms avoid these malicious nodes to get selected in the routing process. The protocol is simulated and compared to existing trust aware routing protocols. Proposed protocol TEAROR presents better results than the other compared protocols.

KEYWORDS

Energy Efficiency, Opportunistic Routing, Sensor, Trust, WSN

1. INTRODUCTION

In most of the applications of Wireless Sensor Networks (WSN), the sensor nodes are operating independently without any external interference. This unsupervised operation of WSN leads to expose nodes to variety of malicious attacks. There are many protocols (Haque et al., 2008) (Hu et al., 2003) (Zhang et al., 2008) (Mohaisen et al., 2009) (Ahmed et al., 2016) developed, most of which are based on cryptographic and authentication systems. These algorithms/protocols are not successful for wireless sensor networks for the following reasons:

1. These protocols are mostly based on the assumption that all nodes in the network are helpful and truthful during the routing process. This assumption makes the protocols unrealistic especially for insider attacks (Slehi et al., 2016);

DOI: 10.4018/IJISMD.2017040102

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2. The sensor nodes are having limited resources like battery power, storage capacity and processing capacity. These constraints restrict the use of the most of cryptographic algorithms. Because cryptosystems need to be executed with high processing, storage and power consumption (Ahmed et al., 2016);
3. In cryptographic and authentication systems there is requirement of centralized key management agent which is not possible to install in WSN.

For the purpose of security of data packets and routing processes in WSN trust and reputation based systems were proved to be more efficient against node mischievousness occurrences. Trust and reputation aware methods are new to solve the problem of security without using cryptosystems (Cordasco and Wetzl, 2008). The trust of a node in wireless communication networks can be defined as the "...degree of reliability of neighbor nodes performing routing process (sending and receiving packets) ..." (Govindan and Mohapatra, 2012). These methods help the sensor nodes in making decisions about other nodes to select them as next-hop forwarders, in other words trust and reputation based routing methods predict the future behavior of neighbor nodes. As the WSN are opportunistic networks in nature, hence, trust and reputation based security systems are more suitable. In opportunistic networks every node on the routing path have the opportunity of send data toward the destination and no fixed path is followed. Hence, trust and reputation based methods helps the opportunistic routing processes to decide the best next-hop forwarder. Trust based methods in WSN are similar to the human behavior system, where two nodes will communicate to each other only when the trust level of receiving node is up to the mark at a certain period of time. The trust values of sensor nodes in WSN should be updated after a certain period of time for the purpose of maintaining low risk level. As the trust based routing protocols do not involve the malicious and misbehaving nodes into the routing process, the throughput and energy efficiency of the network will be improved automatically.

Working on trust and reputation based methods in recent years many protocols have been proposed (Srinivasan et al., 2006) (Ganeriwal et al., 2008) (Michiardi and Molva 2002) (Zaharia et al., 2013) (Tanachaiwiwat et al., 2004) (Gheorghie et al., 2013) (Choudhary et al., 2008) (Channa and Ahmed, 2011). However, most of the protocols have fixed path routing processes. In WSN the fixed path routing processes introduce delays and also if any node on the fixed path is dead, then routing processes are needed to rebuild it. Also, existing trust and reputation based approaches have many vulnerabilities. For example, most of the trusted nodes, in a trust based routing protocol, are the neighbor nodes which are having low energy. This will lead to a short network lifetime. There are several number of packets flow in the network at the same time, which increase the overhead of routing processes. Also, most of the trusted protocols are designed for MANETS and executed on strong hardware platforms having good resources. There is a need of dynamic trust based routing processes to detect the malicious behaviors in the network.

Opportunistic routing provides the ability to sensor nodes to utilize the broadcasting capabilities in a better way. Although there is a risk to data and routing process because of broadcasting, because when the node broadcast a packet it can also be received by malicious nodes. The malicious nodes can misuse these packets to destroy network or to spread false information. The motivation is to provide security to these packets as well as enhance the network lifetime by reducing the energy consumption. The trust aware protocols provide this facility with less energy consumption. The trusted nodes will be included in the routing process and the malicious or untrusted nodes will be avoided.

This paper announces a new trust based and reliable opportunistic routing protocol for WSN. The protocol has been designed to overcome the limitations of existing trust based routing schemes

discussed above. The proposed protocol introduces the direct trust evaluation for each 1-hop neighbor node. The trust evaluation is based on the forwarding sincerity, energy consumption and acknowledgement forwarding sincerity of 1-hop neighbor nodes. The protocols is opportunistic in nature and selects best next-hop always, when a node has the data to be transferred toward base station (destination). The proposed protocol is independent of node's location and it proves to be best in the presence of substantial network load. The proposed protocol always selects the best next hop, which is energy efficient and trustworthy. The simulation results depict the good performance of proposed protocol in the presence of hostile environment. It improves the network throughput, energy efficiency and end-to-end delays in the network.

In the rest of this paper the related work will be discussed in section 2. Section 3 provides the details about proposed protocol following with simulation results in section 4. Section 5 will discuss the conclusion and future perspective of the paper.

2. RELATED WORK

As far as opportunistic routing has been concerned there is a lot of work has been carried out by many authors (Kumar and Singh, 2017). But there is either no or very few trust or reputation aware secure opportunistic routing protocols proposed in past years (Slehi et al., 2016). Nowadays many researchers are focusing in this direction, because trust aware routing processes are lightweight and easy to implement in real applications. Opportunistic routing is mainly constituted of two phases, i.e. candidate set selection and forwarder selection out of that candidate set. (Liu et al., 2007), (Hsu et al., 2011) and (Darehshoorzadeh and Cedra-Alabern, 2012) published detailed reviews on OR notions, representations, and classifications.

The first and foremost opportunistic routing algorithm proposed was Ex-OR (Exclusive opportunistic routing) (Biswas and Morris, 2005). The algorithm worked well in the presence of wireless links. The algorithm was based on a routing metric known as expected transmission count (ETX), which is concerned with number of transmissions required for a packet to reach the destination. Working in same direction LCOR (Dubois-Ferriere et al., 2011) was proposed using the modified metric expected anypath transmission (EAX) (Zhong et al., 2006). SOAR (Rozner et al., 2009) also used the ETX and a mechanism to reduce number of duplicate packets sent towards the base station. Opportunistic routing was focused by many researchers, especially for WSN, by designing new routing protocols like POR (Liu et al., 2013), DPOR (Darehshoorzadeh and Cedra-Alabern, 2012) and CBF (Fubler et al., 2003), etc. All of these protocols do not consider security as a major parameter and apply no security method.

The packets in the sensor network transmitted through wireless channels and are exposed to attackers. Cryptosystems provide security from external attacks, but fails to cope up with internal malicious nodes in the network. For the purpose of securing network from internal attackers the cooperation among all sensor nodes is most important. To accomplish this task lightweight trust and reputation aware protocols are very important and these can provide security from internal as well as external attackers. Working in this direction many protocols have been proposed for wireless networks. Some common examples are CORE (Michiardi and Molva, 2002), SORI (He et al., 2004), CONFIDANT (Ganeriwai et al., 2008), PFM (mantas et al., 2017) and (Salehi et al., 2016) etc. All of these protocols are not primarily made for WSN, and hence do not work efficiently when used with WSN.

In WSN trust and reputation based systems has been focused by many researchers around the world in recent two or three years. The researchers tried to maintain the balance between the sensor resources and security of the network. A dynamic trust aware routing framework (TARF) has been proposed by (Deng et al., 2010). This framework utilizes the social network trust principles with traditional cryptographic models to secure the network. Another protocol efficient monitoring procedure in reputation system (EMPIRE) (Maarouf et al., 2009) was proposed for the purpose of probabilistic and

distributive monitoring methods. The authors tried to reduce the number of monitoring jobs for each node and hence reduce energy consumption in the network. Energy efficient and trust aware routing (ETARP) (Gong et al., 2015) is another protocol for WSN which ensures the maximum utilization of resources with minimum routing cost. Similarly, trust and energy aware secure routing protocol (TESRP) (Ahmed et al., 2016) reduces energy consumption and also lower the routing overhead in the network. Trust and location aware routing (TLAR) (Vamsi and Kant, 2016) is proposed recently and consider different parameters like forwarding sincerity, network acknowledgements, packet integrity, energy information, and feedbacks of other nodes. But the overhead and end-to-end delay increases when there is involvement of too many parameters.

From literature it is clear that trust management for WSN is being recognized only in last three to four years. Hence, there is not enough research work in the literature in terms of opportunistic routing techniques. Energy efficiency and link reliability has not been considered in most of the protocols. In this research work, a new trust aware routing protocol has been proposed and compared by using simulation with other existing protocols. The performance will be tested on the basis of simulations performed for various parameters.

3. PROPOSED PROTOCOL

In this section, proposed protocol will be discussed in detail. Before going into the details assumptions for the protocol are as follows:

1. The nodes are deployed randomly in the application area to be monitored;
2. The resources like energy, buffer size and computation power are fixed and same for every node;
3. A selfish or overloaded node will drop all the packets coming to it and also presents false energy and storage information;
4. Malicious nodes randomly drop some of the packets and lead to grey-hole attack. Some malicious nodes drop all of the packets and will lead to black hole attack.

3.1. Trust Aware Energy Efficient and Reliable Opportunistic Routing Protocol (TAEROR)

TAEROR is a dynamic routing protocol for wireless sensor networks. It is designed especially for WSN by considering the limited resources of each sensor node in the network. This protocol is based on opportunistic routing technique. In opportunistic routing forwarder candidate selection is the most important step. Hence, while designing an opportunistic routing algorithm a metric has to design, which helps the protocol to select good forwarder candidates.

The protocol TAEROR will be completed in multiple phases. In the starting stage of the network the neighbor nodes are identified and a neighbor list (NGH) is formed in each node. This will be completed by using hello packets, the nodes which are replying to the hello packets will be added to NGH. After forming neighbor lists, the trust-based opportunistic routing metric has been calculated and forwarder candidates will be selected. Energy cost model will be the same as in (Kumar and Singh, 2016). All of the phases will be discussed in the following subsections.

3.1.1. Trust Evaluation

This phase evaluates the trust value of a node and the next-hop relay will be selected on the basis of this trust value. The trust metric is based on the beta distribution and probability of a node being malicious. Only the direct trust values are taken into account in the proposed metric. Every time a when a node has data packets for transmission toward base station it initiates the opportunistic routing process. After forming the neighbor list, the trust value has been calculated for each node in the neighbor list. The trust value incorporates the probability of a node being malicious (P_m), forwarding sincerity (F),

acknowledgement sincerity (*ACK*) and energy depletion (*E*). The probability of a node being malicious is calculated on the basis of packets dropped during the routing process. It is calculated by using the unsuccessful packet forwarding ratio and the delay ratio for packet forwarding:

$$P_m = (1 - R_U) - R_{delay} \quad (1)$$

where, R_U is the ratio of unsuccessful packet forwarding divided by the number of packets sent toward a node:

$$R_U = N_{dr} / N_s \quad (2)$$

where, N_{dr} is the number of dropped packets by a node and N_s is the number of packets sent towards the same node:

$$R_{delay} = N_{delay} / N_s \quad (3)$$

where N_{delay} is the number of packet which are delayed by a node and N_s is the number of packets sent towards the same node. By substituting the value of Equation (2) and Equation (3), the probability of a node being malicious is calculated. The calculated probability may be slightly different from the original behavior of the node, but the behavior of a node will fluctuate around this probability value.

After the probability has been calculated the trust evaluation process starts. The trust evaluation requires the values of forwarding sincerity, energy depletion and acknowledgement sincerity. Suppose there are two nodes i and j for which we want to calculate the values of these parameters. The forwarding sincerity ($F(i, j)$) is calculated as follows:

$$F(i, j) = \frac{SF_{(i,j)}}{SF_{(i,j)} + UF_{(i,j)}} (1 - P_m) \quad (4)$$

where, $SF(i,j)$ is the number of successful packet forwarding from i to j and $UF(i,j)$ is the number of unsuccessful packet forwarding from i to j . The acknowledgement sincerity has been calculated as follows. Here, $SACK(i,j)$ and $UACK(i,j)$ are the number of successful and unsuccessful acknowledgement forwarding respectively:

$$ACK(i, j) = \frac{SACK(i, j)}{SACK(i, j) + UACK(i, j)} (1 - P_m) \quad (5)$$

Energy is the important factor in WSN and should be conserved to improve the lifetime of the network. Hence, in the trust value calculation for TEAROR, the energy depletion (E_{impact}) has been introduced which is being calculated as follows:

$$E_{impact}(i, j) = \frac{E_{Fwd}(j) + E_{Rcv}(j) + E_{ack}(i, j)}{E_{total}(j)} (1 - P_m) \quad (6)$$

where, $E_{Fwd}(j)$ is the energy required by node j to forward a packet further to its neighbors. Similarly, $E_{Rcv}(j)$ is the energy required by node j to receive the packets from node i and $E_{ack}(i,j)$ is the energy consumed in sending acknowledgement from j to i . $E_{total}(j)$ is the total energy of the node j . this factor will tell about the impact of one transmission from node i to node j , on node j . If the impact is high, the trust value will be low. This will help in distributing the energy consumption among all the nodes.

After, all of sincerity factors are calculated, trust value will be computed. The trust value involves the aging factor. Each node has the formerly computed trust value for each neighbor. Hence, it must be included with recently calculated trust value (Salehi et.al., 2014). This is to be done because the sensor nodes, during their lifetime, may change their behavior. The newly computed trust value will help in monitoring the behavior of the nodes in the network. Following Equation (7) will calculate the new trust value ($RT(i,j)$) for node j with respect to node i :

$$RT(i,j) = \frac{\alpha * F(i,j) + \beta * E(i,j) + \gamma * ACK(i,j)}{\alpha + \beta + \gamma} \quad (7)$$

where α , β and γ are the importance factors. Means whichever sincerity factor out of three is most importance will be multiplied with highest value. By including previous behavior of the node j Equation (8) gives the final trust value ($FT(i,j)$) for node j with respect to node i :

$$FT(i,j) = \sigma * NewRT(i,j) + \lambda * (1 - \sigma) * OldRT(i,j) \quad (8)$$

where, $0 < \sigma < 1$ represents the aging factor and $0 < \lambda < 1$ represents the weight of the $NewRT(i,j)$. These factors may be set to a value according to the simulation scenario and application of the network. In this way the final trust value has been calculated and used in relay selection algorithm which is being discussed in next subsection.

3.1.2. Relay Selection Algorithm

In opportunistic routing the relay selection out of some potential forwarders is very important task. Although, each potential forwarder have the opportunity to send data packet towards base station, but relay selection algorithm will decide the node which will forward the packet first. If this algorithm is not used than each node in the forwarder list will forward the data packets and base station will receive multiple duplicate packets. To monitor the packet transmission process, data packet forwarding progress (FP) is calculated using distance between source and destination ($D_{s,d}$) and distance between the destination and relay nodes ($D_{n_i,d}$) (Equation (9) and Equation (10)). Here, k is the total number of nodes in the network:

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \text{ where } 0 \leq i, j \leq k, \text{ and } i \neq j \quad (9)$$

$$FP_{n_i}^{s,d} = D_{s,d} - D_{n_i,d}, \text{ where } s=\text{source}, d=\text{destination}, 0 \leq n_i \leq k \quad (10)$$

The proposed relay selection algorithm below, starts at a random source node (S), which have data to be sent toward the base station (D). The list of 1-hop neighbor nodes for S has been formed. After forming this list, node trust factor (FT) has been calculated for each node in neighbor list. The value of FT will decide whether the node can be part of forwarder list (FL) or not. Sorting of the nodes in neighbor list is done by using the trust factor (FT). The nodes which are having FT value greater or equal to the minimum acceptable trust value (t_{min}) will be added to FL . But the capacity of FL will

be according to WSN application requirements. *FL* will be the list of potential forwarders, which can be trusted by the source node *S*. The data packets will be constructed including forwarder list and minimum trust value. Similar procedure will be followed by the receiver nodes. The node which is on the top of the forwarder list will forward the data packet first. The relay selection algorithm is the essential part of opportunistic routing process. This will decide the complexity of opportunistic routing process.

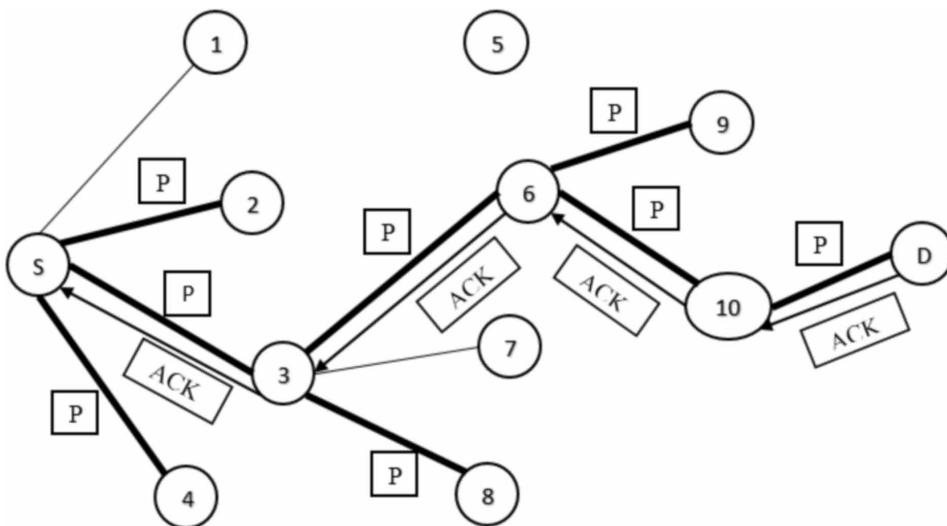
Consider the example network in Figure 1, which considers node *S* as source node and *D* as the destination node (base station). *S* will form its neighbor list as {1, 2, 3, 4} and calculate the trust value for each node in this list. Suppose the trust values for each node 1, 2, 3 and 4 are 0.2, 0.4, 0.6 and 0.4 respectively. The neighbor list will then be sorted according to trust values in descending order. After sorting the neighbor list will be {3, 2, 4, 1}. Now consider the number of forwarder nodes allowed in forwarder list are 3. Then forwarder list *FL* will contain {3, 2, 4}. After the forwarder list is formed the data packet is transmitted by including this forwarder list, minimum allowed trust value and destination address. The node which is on the top of forwarder list, 3 in this case, will forward the data packet first by following the same procedure. This process will be continued until the destination *D* is not found.

In relay selection algorithm (Algorithm 1), every node in the forwarder list will get the opportunity to send packet toward destination. Some of the nodes which are malicious or selfish nodes will not be included in forwarder list, because of low trust value. Hence, the TAEROR protocol will avoid such nodes to be included in the routing process. The packet *P* will travel only through the trusted nodes. Like in Figure 1, node 1 in the neighbor list of *S* will not be included in the forwarder list because of having low trust value. Similar is for node 7. Also, as only the top node on forwarder list is allowed to send packet further first, there will be no or very less duplicate packets received at destination (see Figure 2).

4. EXPERIMENTAL RESULTS AND ANALYSIS

TAEROR has been tested through extensive simulations on NS2 by creating simulation scenario. The simulation parameters' settings are shown in Table 1. The performance of TAEROR has been compared to existing trust aware routing protocols for WSN i.e. Trust and location aware routing

Figure 1. Example scenario of relay selection in TEAROR

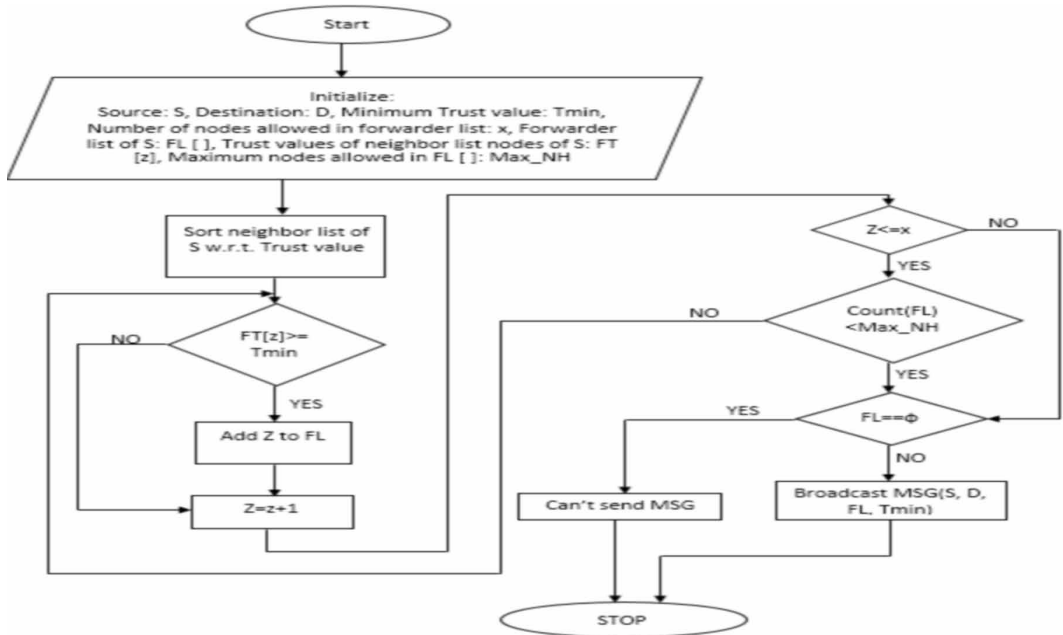


Algorithm 1. Relay selection (S = Source, D = Destination)

```

When node S want to send a packet
Let  $t_{min}$  be the minimum acceptable trust factor of a node
x be the number of 1-hop neighbors of S
Let FT[Z] be the node trust factor of node Z
Let Max_NH be the maximum number of neighbors which are allowed
in forwarder list (FL)
FL= empty
Sort all 1-hop neighbors of S in descending order according to
FT[Z]
For (Z=1; FL < Max_NH and Z <= x; Z=Z+1)
Do
    If (FT[Z] >=  $t_{min}$ ) then
        Add Z's ID in FL
    EndIf
EndFor
If (FL!=empty)
    Broadcast MSG (S, D, FL,  $t_{min}$ )
EndIf
    
```

Figure 2. Flowchart for proposed relay selection algorithm



(TLAR) (Vamsi and Kant, 2016), Trust and energy aware secure routing protocol (TESRP) (Ahmed et al., 2016) and Trust aware opportunistic routing Framework (TAOR) (Salehi and Boukerche, 2014). All of these protocols are recently proposed protocols for wireless and sensor networks. The simulation settings shown in Table 1 has been applied to all compared protocols. The existing

Table 1. Simulation settings

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 x 500 m ²
Transmission Range	60 m
No. of Nodes (N)	25, 50, 100
No. of Malicious nodes	10, 20, 30, 40 and 50
Traffic Type	CBR (Constant Bit Rate)
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	100J
Initial Trust Value	1
Default σ and λ	0.90 and 0.4
Energy dissipation to run the radio ($E_{electronic}$)	50 nJ/bit

protocols i.e. TLAR (Vamsi and Kant, 2016), TESRP (Ahmed et al., 2016) and TAOR (Salehi and Boukerche, 2014) are re-implemented in NS2.

The simulation performance of all protocols has been tested in presence of black-hole and grey-hole attacks. Malicious nodes and selfish nodes has been created in the simulation environment based on the assumptions of proposed TAEROR protocol. The sensor nodes are assumed to be randomly deployed in area to be monitored. The malicious or selfish nodes do no generate any data packets, and also produce false network information. Black hole attack is created when the malicious node drops all of the packets coming to them. And grey hole attack is generated when selective packets has been dropped.

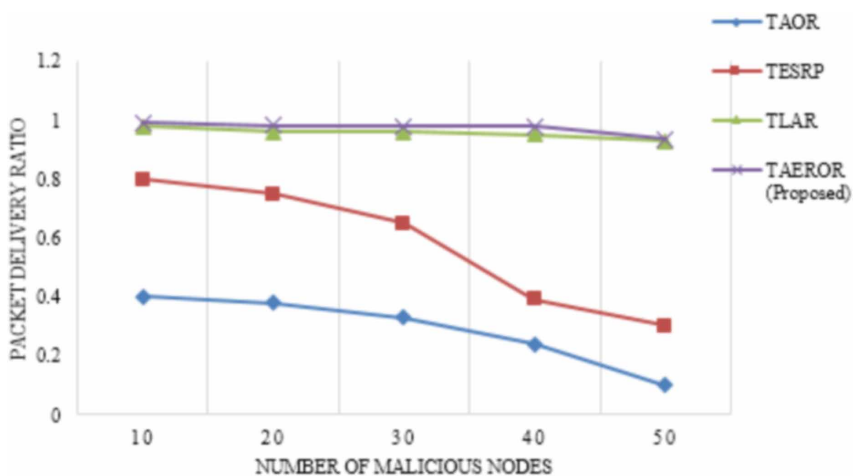
After completing extensive simulations for all protocols, the performance has been recorded and presented in form of graphs. The results are purely simulation based and all three protocols were tested on the same platform with same parameters. The security performance has been tested by using number of malicious nodes encountering during the routing process (Figure 3). As the routing is based on trust value, the nodes which are having very low trust values must be excluded during routing process. Proposed protocol TAEROR do the same thing. On the basis of forwarding sincerity values the nodes which are not forwarding the data packets i.e. implementing black-hole attack or grey-hole attack, will be excluded from routing path. Hence, there will be lesser number of malicious nodes encountered during routing process. Similar procedure has been followed by TLAR (Vamsi and Kant, 2016), hence it will present similar results. TESRP (Ahmed et al., 2016) and TAOR also calculated the forwarding sincerity values of nodes to avoid including malicious nodes into routing process. But the selfish nodes cannot be detected in these protocols.

The packet delivery ratio (Figure 4) also increase when any protocol is able to avoid black-hole and grey-hole attacks. This is because the number of retransmissions will be lesser. The proposed protocol TAEROR avoid the malicious nodes to be selected as the next-hop forwarder and hence secure the network from black-hole and grey-hole attacks. Similarly, TLAR (Vamsi and Kant, 2016) also do the same thing, but, it also used the feedbacks from other nodes and obviously, the nodes which are malicious will give positive feedbacks for other malicious nodes and negative feedbacks for good/healthy nodes. TAOR (Salehi and Boukerche, 2014) gives better results, but fails in providing energy efficiency. Similar is the case with TESRP (Ahmed et al., 2016).

Figure 3. Performance on the basis of average risk level



Figure 4. Performance on the basis of packet delivery ratio



The end-to-end delay (Figure 5) is also a major performance factor and all the protocols has been tested for the same. It is calculated as the total time consumed to deliver a data packet at destination node, when same packet is initiated from source node. End-to-end delay will be calculated only for successful packet deliveries. End-to-end delay will be high if greater number of malicious nodes encountered during routing process and also if overhead of selection of next-hop forwarder is high. TAEROR and TAOR (Salehi and Boukerche, 2014) calculate only direct trust values and avoid malicious nodes to be selected as next-hop forwarder, that's why the end-to-end delay is low. But, in case of TLAR (Vamsi and Kant, 2016) and TESRP (Ahmed et al., 2016) there will be overheads of calculating trust values and hence introduces more delays.

Energy consumption (Figure 6) is an important performance measurement factor in WSN. Energy consumption will decide the lifetime of the network. The major energy consuming processes in routing are transmitting and receiving packets and acknowledgements in the network. TAEROR, the proposed protocol considers all of these energy consumptions in the trust factor calculation

Figure 5. Performance on the basis of end-to-end delay

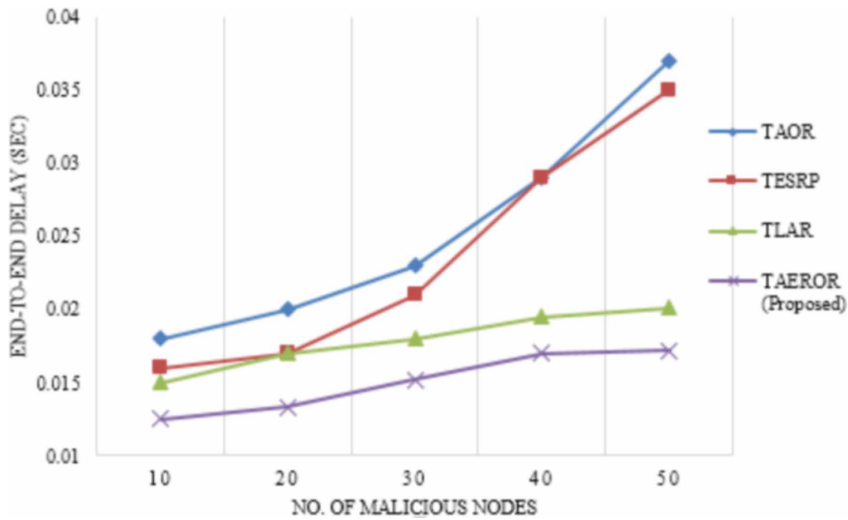
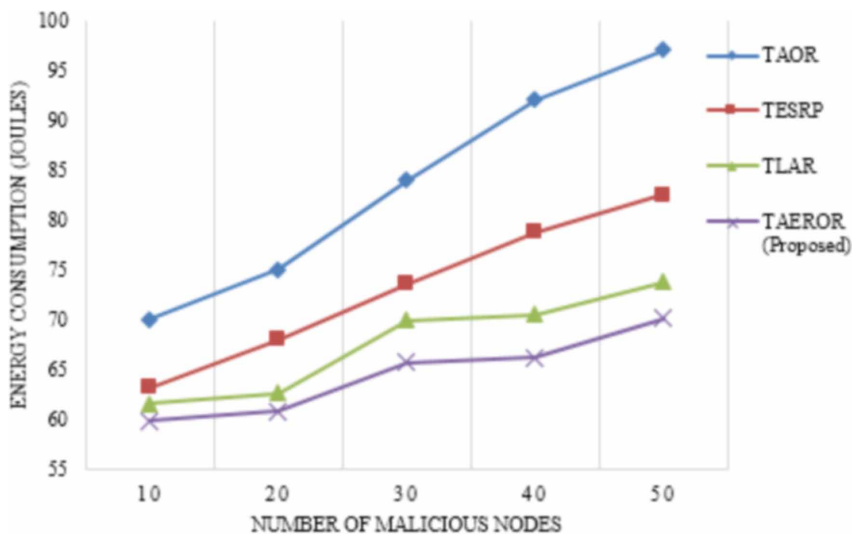


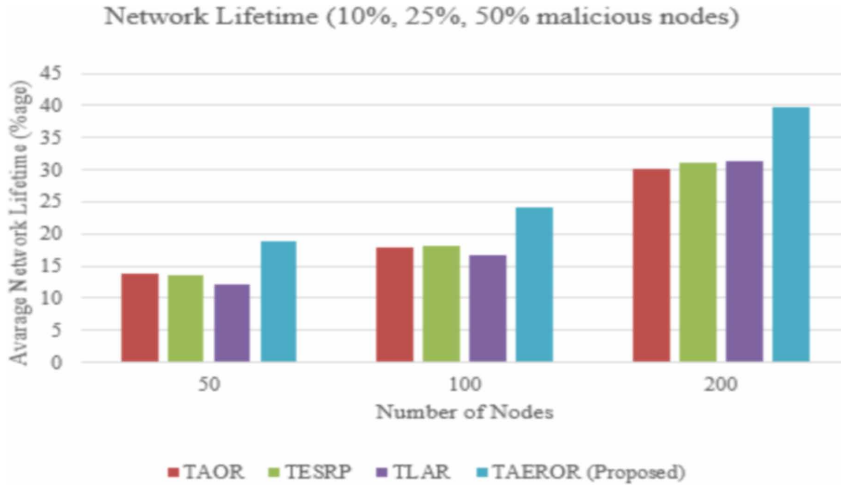
Figure 6. Performance on the basis of total energy consumption



and hence consume very less energy as compared to other algorithms. The overhead of trust factor calculation is also less because of simple calculations. The network lifetime also increases because of less energy consumption in the network.

There are different measures through which the network lifetime can be calculated. One way is to wait for the whole sensor nodes to decay their energy. Another way is when one node is dead the network is considered to be dead. In this paper for all compared protocols the average network lifetime has been calculated by using the percentage of number of nodes still alive even after the network is considered to be dead. The network is considered to be dead when the nodes stops communicating data packets towards the base station. The network lifetime has been checked for different number of nodes and in the presence of different number of

Figure 7. Network lifetime



malicious nodes. The proposed protocol presents better network lifetime than others because of less energy consumption. Also, the energy consumption is distributed among all nodes through trust value (see Figure 7).

5. CONCLUSION AND FUTURE SCOPE

Opportunistic routing is gaining popularity in wireless network types, especially for wireless sensor networks. Most of the opportunistic routing protocol proposed for WSN has not considered security as major issue. Also in WSN, the traditional security methods like cryptosystems, cannot be used because of lack of resources. Hence, in this paper a trust aware opportunistic routing protocol TAEROR is proposed, which is avoid malicious nodes to be involved in routing process. A trust calculation factor is proposed which considers forwarding sincerity, energy consumption and acknowledgement sincerity as major factors. A relay selection algorithm is also the part of protocol, which used the trust values to decide which node is qualified to take part in routing process. The trust value introduction in relay selection algorithm, secure the network from black-hole and grey-hole attacks. Simulation results shows the good performance of proposed protocol as compared to other recently proposed protocols i.e. TLAR, TAOR and TESRP. In future directions, we can consider more parameters in trust value calculation, but the more the parameters more will be computational overhead. Hence, only those parameters should be considered which seem to be important in the network like energy, packet delivery, etc.

REFERENCES

- Ahmed, A., Bakar, K. A., Channa, M. I., & Khan, A. W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. *Mobile Networks and Applications*, 21(2), 272–285. doi:10.1007/s11036-016-0683-y
- Biswas, S., & Morris, R. (2005). ExOR: Opportunistic multi-hop routing for wireless networks. *Computer Communication Review*, 35(4), 133–144. doi:10.1145/1090191.1080108
- Channa, M. I., & Ahmed, K. M. (2011). A Reliable Routing Scheme for Post-Disaster Ad Hoc Communication Networks. *Journal of Communication*, 6(7), 549–557.
- Choudhury, S., Roy, S. D., & Singh, S. A. (2008). Trust management in ad hoc network for secure DSR routing. In *Novel algorithms and techniques in telecommunications, automation and industrial electronics* (pp. 495-500).
- Cordasco, J., & Wetzel, S. (2008). Cryptographic versus trust-based methods for MANET routing security. *Electronic Notes in Theoretical Computer Science*, 197(2), 131–140. doi:10.1016/j.entcs.2007.12.022
- Darehshoorzadeh, A., & Cerda-Alabern, L. (2012). Distance progress based opportunistic routing for wireless mesh networks. *Paper presented at the 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*. doi:10.1109/IWCMC.2012.6314199
- Deng, H., Yang, Y., Jin, G., Xu, R., & Shi, W. (2010). Building a trust-aware dynamic routing solution for wireless sensor networks. *Paper presented at the 2010 GLOBECOM Workshops (GC Wkshps)*. IEEE. doi:10.1109/GLOCOMW.2010.5700197
- Dubois-Ferrière, H., Grossglauser, M., & Vetterli, M. (2011). Valuable detours: Least-cost anypath routing. *IEEE/ACM Transactions on Networking*, 19(2), 333–346. doi:10.1109/TNET.2010.2070844
- Füßler, H., Widmer, J., Käsemann, M., Mauve, M., & Hartenstein, H. (2003). Contention-based forwarding for mobile ad hoc networks. *Ad Hoc Networks*, 1(4), 351–369. doi:10.1016/S1570-8705(03)00038-6
- Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, 4(3), 15. doi:10.1145/1362542.1362546
- Gheorghe, L., Rughinis, R., & Tataroiu, R. (2013). Adaptive trust management protocol based on intrusion detection for wireless sensor networks. *Paper presented at the Networking in Education and Research, 2013 RoEduNet International Conference* (12th ed.). doi:10.1109/RoEduNet.2013.6714201
- Gong, P., Chen, T. M., & Xu, Q. (2015). ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. *Journal of Sensors*.
- Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys and Tutorials*, 14(2), 279–298. doi:10.1109/SURV.2011.042711.00083
- Haque, M., Pathan, A.-S. K., Hong, C. S., & Huh, E.-N. (2008). An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks. *Transactions on Internet and Information Systems (Seoul)*, 2(5), 265–279. doi:10.3837/tiis.2008.05.004
- He, Q., Wu, D., & Khosla, P. (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. *Paper presented at the Wireless communications and networking conference WCNC '04*. IEEE.
- Hsu, C.-J., Liu, H.-I., & Seah, W. K. (2011). Opportunistic routing—A review and the challenges ahead. *Computer Networks*, 55(15), 3592–3603. doi:10.1016/j.comnet.2011.06.021
- Hu, Y.-C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1), 175–192. doi:10.1016/S1570-8705(03)00019-2
- Hu, Y.-C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2), 21–38. doi:10.1007/s11276-004-4744-y
- Kumar, N., & Singh, Y. (2016). An energy efficient and trust management based opportunistic routing metric for wireless sensor networks. *Paper presented at the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. doi:10.1109/PDGC.2016.7913196

- Kumar, N., & Singh, Y. (2016). An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks. *Indian Journal of Science and Technology*, 9(32). doi:10.17485/ijst/2016/v9i32/100197
- Kumar, N., & Singh, Y. (2017). Routing protocols in wireless sensor networks. In *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures* (pp. 86-128).
- Liu, K., Abu-Ghazaleh, N., & Kang, K.-D. (2007). Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, 67(2), 215–228. doi:10.1016/j.jpdc.2006.08.001
- Liu, Z., Wei, C., Qin, C., Li, H., Niu, X., & Wang, L. (2013). POR: A Packet-Based Opportunistic Routing Protocol for Wireless Sensor Networks. *Paper presented at the 2013 International Conference on Computer Sciences and Applications (CSA)*. doi:10.1109/CSA.2013.43
- Maarouf, I., Baroudi, U., & Naseer, A. R. (2009). Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. *IET Communications*, 3(5), 846–858. doi:10.1049/iet-com.2008.0324
- Mantas, N., Louta, M., Karapistoli, E., Karetos, G. T., Kraounakis, S., & Obaidat, M. S. (2017). *Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey*. IET Networks.
- Michiardi, P., & Molva, R. (2002). *Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks* *Advanced communications and multimedia security* (pp. 107–121). Springer.
- Mohaisen, A., Choi, J. W., & Hong, D. (2009). On the insecurity of asymmetric key-based architecture in wireless sensor networks. *Transactions on Internet and Information Systems (Seoul)*, 3(4), 376–384. doi:10.3837/tiis.2009.04.003
- Rozner, E., Seshadri, J., Mehta, Y., & Qiu, L. (2009). SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks. *IEEE Transactions on Mobile Computing*, 8(12), 1622–1635. doi:10.1109/TMC.2009.82
- Salehi, M., & Boukerche, A. (2014). Trust-aware opportunistic routing protocol for wireless networks. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks* (pp. 79-86). doi:10.1145/2642687.2642692
- Salehi, M., Boukerche, A., Darehshoorzadeh, A., & Mammeri, A. (2016). Towards a novel trust-based opportunistic routing protocol for wireless networks. *Wireless Networks*, 22(3), 927–943. doi:10.1007/s11276-015-1010-4
- Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 20(11), 1698–1712. doi:10.1109/TPDS.2008.258
- Srinivasan, A., Teitelbaum, J., & Wu, J. (2006). DRBTS: distributed reputation-based beacon trust system. *Paper presented at the 2nd IEEE international symposium on Dependable, autonomic and secure computing*. doi:10.1109/DASC.2006.28
- Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2004). Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. *Paper presented at the 2004 IEEE International Conference on Performance, Computing, and Communications*. doi:10.1109/PCCC.2004.1395061
- Vamsi, P. R., & Kant, K. (2016). Trust and location-aware routing protocol for wireless sensor networks. *Journal of the Institution of Electronics and Telecommunication Engineers*, 62(5), 634–644. doi:10.1080/03772063.2016.1147389
- Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, 52(12), 2292–2330. doi:10.1016/j.comnet.2008.04.002
- Zahariadis, T., Trakadas, P., Leligou, H. C., Maniatis, S., & Karkazis, P. (2013). A novel trust-aware geographical routing scheme for wireless sensor networks. *Wireless Personal Communications*, 69(2), 805–826. doi:10.1007/s11277-012-0613-7

Zhang, K., Wang, C., & Wang, C. (2008). A secure routing protocol for cluster-based wireless sensor networks using group key management. *Paper presented at the 4th International Conference on Wireless Communications, Networking and Mobile Computing WiCOM'08*. doi:10.1109/WiCom.2008.889

Zhong, Z., Wang, J., Nelakuditi, S., & Lu, G.-H. (2006). On selection of candidates for opportunistic anypath forwarding. *Mobile Computing and Communications Review*, 10(4), 1–2. doi:10.1145/1215976.1215978

Zhou, Y., Tan, X., He, X., Qin, G., & Xi, H. (2010). Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature. *Information Assurance and Security Letters*, 1, 18–23.

Nagesh Kumar is currently pursuing a PhD from Jaypee University of Information Technology, Wanknaghat, Solan, Himachal Pradesh, India. The author received an MTech in Computer Science from Himachal Pradesh University, Shimla (HP), India. Nagesh's area of interests are Wireless Sensor Network, Internet and QoS routing.

Yashwant Singh is currently working as Associate Professor in Department of Computer Science & IT at Central University of Jammu, Jammu and Kashmir. He has 12 years of experience in academics at reputed Colleges and Universities in India. He has completed his PhD in Computer Science from Himachal Pradesh University, Shimla, H.P., India. He received his Master of Engineering from Punjab Engineering College, Chandigarh, India. He has obtained his Bachelor of Engineering from SLIET, Longowal, Punjab, India. Dr. Singh is a Member of IEEE, Member CSI, Member ACM and Life Member of ISTE. He was general chair IEEE PDGC-2014 and associated as TPC member, session chair & reviewer of various Conferences & Journals in India and abroad.

Pradeep Kumar Singh is currently working as an Assistant Professor (Senior Grade) in Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT), Wanknaghat, H.P. He has 10 years of vast experience in academics at reputed colleges and universities of India. He has completed his PhD in Computer Science & Engineering from Gautam Buddha University (State Government University), Greater Noida, UP, India. He received his MTech (CSE) with Distinction from Guru Gobind Singh Indraprastha University, New Delhi, India. He has obtained his BTech (CSE) from Uttar Pradesh Technical University (UPTU), Lucknow, India. Dr. Singh has life membership of Computer Society of India (CSI) and promoted to Senior Member Grade from CSI. He is member of ACM, IACSIT-Singapore and IAENG-Hong Kong. He has worked as publicity chair of five IEEE International Conferences and associated as TPC member & reviewer of various Conferences & Journals too.

Trust and Packet Load Balancing Based Secure Opportunistic Routing Protocol for WSN

Nagesh Kumar, Yashwant Singh
 Department of Computer Science & Engineering & IT
 Jaypee University of Information Technology
 Waknaghat, Solan (HP), India
 engg.nagesh2@gmail.com, yashu_want@yahoo.com

Abstract— Opportunistic routing in wireless networks has grown the popularity because it utilizes the broadcasting abilities of wireless links. Wireless sensor networks (WSN) also adopted opportunistic routing in recent years. In WSN, most important objectives of the researchers are to maintain the data integrity, availability and reliability with minimum energy consumption. If any WSN user have to achieve all of these objectives than, he has to ensure the security of the network first. Existing cryptographic schemes are not efficient for WSN, because of high energy consumption. This paper presents a new trust and packet load balancing based opportunistic routing (TPBOR) protocol. The proposed protocol is energy efficient and secure by utilizing the trusted nodes in the routing process. Also the proposed protocol balance the overall network traffic and distribute the traffic load equally in the network. The simulation results show that proposed OR protocol has significantly improves the network performance and reduces the end-to-end delays as compared to existing packet load balancing trust based routing protocols for WSN.

Keywords— *wireless sensor networks; routing protocol; trust; load balancing; opportunistic routing scheme.*

I. INTRODUCTION

Wireless sensor networks (WSN) become popular in last decade and attract research interests in real life applications. The small sized sensor nodes available nowadays has the capability to sense, process and communicate the information and hence these can be used in numerous of applications. In most of applications WSN are data centric and hence require high throughput with long network life [1]. Also the real time data delivery requires less delays in data transmissions. For such wireless communication networks secure routing protocols play a major role in improving the performance.

Routing protocols available prior to opportunistic routing transmit the packets along a predetermined path [6]. This makes attackers easy to interfere in the routing process. Also if any of the node dies in between the path than the source has to reconstruct the path and retransmit the packets. Opportunistic routing (OR) [7] transmit packets through multiple relays by utilizing the broadcasting nature and spatial diversity of wireless radios. The sensor nodes need the coordination with each other to perform opportunistic routing. A number of OR

protocols has been proposed which makes it a new research area in WSN to improve lifetime and performance in real life applications. Also to improve the reliability and availability of data, security of packets and routes is important.

Instead of using fixed path routing researchers nowadays are focusing on the multipath routing and opportunistic routing. But there is no guarantee of security of data packets in transit [2]. For security one has to use the cryptography or authentication schemes, which require a lot of processing power and energy [16]. This will make WSN stop functioning in short time period. Hence, the researchers are suggesting to use the trust and reputation aware methods for security of data and routing processes. As sensor nodes have limited resources, researchers try to balance between security and utilization of resources. Many Trust and reputation based routing protocols has been proposed in last three years.

Using conventional cryptosystem in [17] authors have proposed a dynamic routing protocol for WSN named as TARF. This algorithm uses theories trust for social networks. This algorithm fails to provide energy efficiency in the network. Working in same direction a trust based routing protocol has been proposed in [18] and named as EMPIRE. It is a probabilistic approach and it try to reduce tasks per node to improve energy efficiency. Trust based protocols significantly improve the energy efficiency with security mechanism. In [19] ETARP protocol for WSN chooses next-hop nodes which lower the communication cost by optimal utilization of resources. Overhead of communication and next-hop calculation are still issues in this protocol. To reduce energy consumption and improve lifetime of the network [20] proposed a protocol called as TESRP. Similar protocol TLAR [21] has been proposed for WSN which incorporates the consolidated trust calculation using direct and indirect values of trust. This protocol give weights to the parameters used in the trust value calculation. The weights has been adjusted dynamically during network operation. All of these protocols do not provide load balancing in the network. The relay candidates have to receive the packets and transmit the same toward base station. But if the buffer of the relay node is full than the source has to wait for the buffer to be cleared. Some of the protocols proposed in this direction like Buffer aware opportunistic routing (BAOR) [23], ORPL-LB [24] and POR

[25]. But, these protocols do not provide security for data packets and routing process.

This paper presents a new Trust and Packet load Balancing OR protocol (TPBOR). This protocol has specially been designed for WSN. This protocol calculated the trust value of each node before starting a communication. TPBOR selects the next hop relay on the basis of trust value and buffer awareness. Based on these two values relay selection criteria has been developed and next hop nodes will be selected on the basis of this criteria. The performance has been tested on the basis of simulations. The results of simulation show that TPBOR outperforms the existing Trust aware protocols and also the packet load balancing based protocols.

Rest of this paper is as organized. Section II discusses the TPBOR protocol in detail. Implementation and analysis of the protocol has been given in section III. Section IV gives the conclusion of the paper and also some of future work.

II. PROPOSED PROTOCOL (TPBOR)

This section discusses the proposed protocol i.e. TPBOR and the issues in the opportunistic routing protocol design process.

A. Opportunistic Routing Design

In WSN opportunistic routing is new mechanism which utilizes spatial diversity and broadcasting nature of wireless links. There are two major processes in OR: forwarder set selection and forwarder node selection from forwarder set. If the forwarder set selected contains large number of nodes than it will be costly, in terms of computation, to find a single forwarder node. But also larger candidate sets can increase the packet delivery ratio. Most of OR protocols form the candidate sets on the basis of replies of neighboring nodes. The second design issue i.e. forwarder node selection is also a critical process [7]. The node selected as forwarder must have the capability to forward the data packets and also packets should make significant progress toward destination in the network. The selection criterion depends upon the routing metric chosen. The routing metric can be one or combination of two or more metrics. On the basis of these metrics the forwarder node is selected and it will act as the next hop forwarder in the network. OR gives opportunity to each node in forwarder set by prioritizing them on the basis of routing metric.

B. Relay Selection Criteria

Relay selection criteria in this paper has been proposed to select the next hop forwarder. Relay selection metric will consist of three phases. In first phase the packet forwarding progress has been checked by using the distance calculation of each neighbor.

$$Dist_{i,j} = \sqrt{(co_x_i - co_x_j)^2 + (co_y_i - co_y_j)^2}$$

$$\text{where } 0 \leq i, j \leq k, \text{ and } i \neq j \quad (1)$$

$$Progress_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d}$$

$$\text{where } s=\text{source}, d=\text{destination}, 0 \leq n_i \leq k \quad (2)$$

In the second phase load of each node has been tested. Initially, there will be no packets in the queue of every node in the network. But as the network starts functioning the nodes start collecting data from the field. This data must be transmitted, through multiple relays, toward the base station. Hence, the node which will be having less number of packets or no packets in its queue, should be selected as next hope. Hence here the routing algorithm first have to check the queue size of the forwarder nodes. This can be done by following equation.

$$Queue_Test_i = w \cdot \frac{Q_{num}}{Q_{size}} \quad (3)$$

where Q_{num} is the number of packets stored currently in the queue, Q_{size} is the total size of the queue of a node and w is the weighting factor (0.5 in this case).

The third phase of relay selection metric is to calculate the trust value to find out the most reliable node among all neighbors. The trust metric [26] will be calculated with the help of following.

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma} \quad (4)$$

where $-1 \leq \alpha, \beta, \gamma \leq 1$ and F_i, E_{total_i} and ACK_i are similar as calculated in [26].

C. Trust and Packet load Balancing Based OR (TPBOR)

TPBOR is a distributive opportunistic routing algorithm. To accomplish the operation of TPBOR. WSN is a network in which all the sensor nodes communicate the data collected, to the base station. The energy consumption and packet load should be balanced, so that the network will function reliably and for longer time. Opportunistic routing utilizes the advantages of broadcasting nature of WSN and hence involve each and every node in routing process.

In the initial phase when the network starts functioning, the nodes start sensing the data. After sensing is done the nodes will forward the data towards the base station. The node first broadcast the RTS (Request to send) signal. The nodes which are receiving this request will reply to the sender node with their energy, queue size and location coordinates. The replying nodes will be added to the neighbor list (NB) of sender node. After neighbor list formation, the queue size factor ($Queue_Test_i$) is checked for each node. If this factor is greater than the threshold value (0.25 here) than the node will not be added to the forwarder list (FL). This will prevent the overloaded nodes to be selected as the next hop forwarder. This will reduce the end-to-end delay for packet forwarding in the network.

After the formation of forwarder list (FL), the forwarder node will be selected. The forwarder node will be the trusted one. The trust value for each node in FL has been calculated by

using equation 4. The node in FL which is having the highest trust value will be selected as next hop forwarder node. Also the nodes which are having trust value lower than 0.2, will be discarded from the forwarder list (FL). The threshold value of trust i.e. 0.2 has been fixed after extensive simulations has been carried out with values 0.0 to 1.0.

As the trust value is calculated dynamically and it involved energy consumption of a node, the energy consumption will be distributed across all nodes in the network. This will prolong the lifetime of the network. The trust value helps the protocol to avoid malicious nodes. Malicious node is defined as the node which do not forward data packets to impose black-hole attack and grey-hole attack. The trust value will be updated dynamically for each session of data transmission.

TPBOR, hence provide security from black-hole attack and grey-hole attack by transmitting data through trusted nodes only. Also there will be low overhead for the trust value calculation because the existing values are used like energy, forwarding ratio and acknowledgement sincerity. Also only the nodes which are rich in energy will be selected as next hop forwarders, will increase the network lifetime. Algorithm below depicts the relay selection process of TPBOR.

Algorithm: Relay_Selection (S, D, Distance(S, D))
 Input: Source node S, Destination D, Distance (S, D)
 Output: Successful transmission of data packet from S to D

1. Create neighbor NGH for S
2. Broadcast RTS from S
3. Add the replying node to NGH
4. If D belongs to NGH
5. Stop algorithm
5. Create FL as forwarder list for S
6. For each node in NGH
7. Calculate $Queue_Test$ using equation 3
8. If $Queue_Test (node_i) \geq 0.25$ then
9. Add $node_i$ to FL
10. For each node in FL
11. Calculate Trust value (T) using equation 4
12. If $T (node_i) < 0.2$
13. Discard $node_i$ from FL
14. else
15. Select the node having largest trust value as select next hop forwarder (FD)
16. Relay_Selection ($FD, D, Distance(FD, D)$)

Whole protocol will work on the principle of opportunistic routing in WSN. The trust value calculation helps the protocol to avoid attacks on data packets and routes. As the routes are secured the network performance will automatically be increases in terms of throughput. The simulation results will be discussed in the next section.

III. SIMULATION RESULTS AND ANALYSIS

TPBOR has been tested on NS2 by creating simulation scenario. Table 1 below depicts the simulation settings in NS2 environment.

The performance has been compared to BAOR (Buffer aware opportunistic routing) [23] which have not applied any

security to the algorithm, but applied packet load balancing. The other algorithm to which TPBOR has been compared is TLAR (Trust and location aware routing) [21] which has applied security in form of direct and indirect trust value calculations.

Table 1: Simulation Settings

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 x 500 m ²
Transmission Range	60 m
No. of Nodes (N)	100
No. of Malicious nodes	10, 20, 30, 40 and 50
Traffic Type	CBR (Constant Bit Rate)
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	100J
Initial Trust Value	1
Default α , β and γ	0.3, 0.4 and 0.3
Energy dissipation to run the radio ($E_{electronic}$)	50 nJ/bit
Buffer Length	30 packets

The simulation settings shown above has been applied to all compared protocols. The existing protocols i.e. BAOR and TLAR are re-implemented in NS2.

The simulation results will depict the better performer in the presence of black-hole and grey-hole attacks. Different number of malicious nodes have been generated during the simulation to get good view of simulation results. The deployment of nodes in the interested area is random. Generation of malicious nodes is also takes place at random locations. The malicious nodes do not act like normal nodes in the network. These malicious nodes do not generate any data packets. To generate black-hole attack, malicious nodes drop all the packets coming to them. Similarly, to impose grey-hole attack selective number of packets have been dropped by malicious nodes.

A. Results and Discussions

After completing extensive simulations for all three protocols the performance has been recorded and presented in form of graphs. The results are purely simulation based and all three protocols was tested on the same platform with same parameters.

Figure 1 below shows the safety performance of all compared protocols i.e. BAOR [23], TLAR [21] and TPBOR. The safety has been measured as the average number of malicious nodes encountered during the routing process. TPBOR has encountered very less number of malicious nodes as compared to other two algorithms. This is because the

forwarder sincerity value F_i for a node i depicts the black-hole and grey-hole attacks. Because it monitors the number of packets forwarded towards the base station. The trust value (T) also includes the acknowledgement sincerity which will make sure that the packets are flowing towards the base station. Similar factors has been considered in TLAR [21]. But the overhead of collecting feedback (indirect trust values) is high in this case. BAOR [23] does not considered any type of security and hence encounter highest number of malicious nodes during routing process.

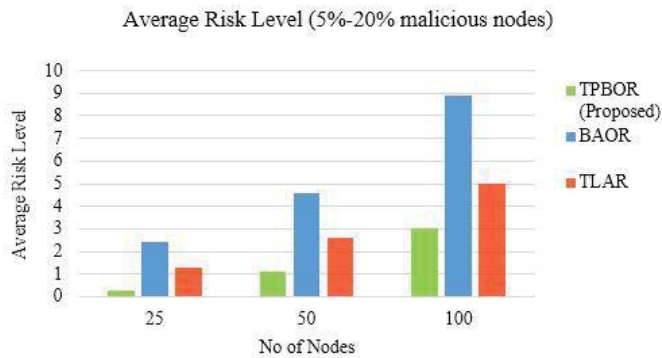


Fig. 1. Performance on the basis of Average risk level

The performance of all three protocols on the basis of packet delivery ratio has been depicted in figure 2 below. This is measured as average number of packets delivered divided by number of packets sent towards the base station in presence of different number of malicious nodes. TPBOR has little bit high packet delivery ratio than TLAR [21] in when the number of malicious nodes are less. But as we increase the number of malicious nodes in the network the overhead in TLAR [21] goes on increasing and hence there is rapid fall in Packet delivery ratio of the network. But in case of TPBOR the routing process completely depends upon direct trust values and there is less overhead. This will increase the number of packets delivered at the base station and hence TPBOR performs good. In case of BAOR [23] as the number of malicious nodes encountered are more the packet delivery ratio will be high.

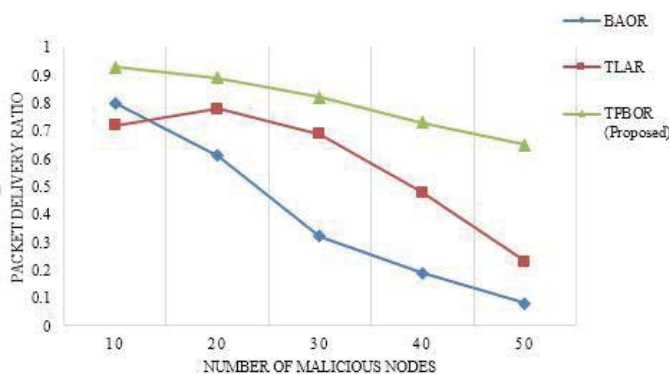


Fig. 2. Performance on the basis of Packet Delivery Ratio

Next performance factor taken here is end-to-end delay in figure 3 below. The end-to-end delay has been measured as the total time taken to deliver a data packet at the base station

from source node. End-to-end delay will be calculated only for successfully delivered packets. It can be depicted from the figure that the end-to-end delay of BAOR [23] is lower initially because it only calculates the back-off value and forward the data packets. But the end-to-end delay in presence of malicious nodes will become higher. In case of TLAR [21] and TPBOR the extra overhead is the calculation of trust values. TPBOR shows here some improvement because it only relies on direct trust value and need not wait for the feedbacks of other nodes. TPBOR performs best in the presence of malicious nodes.

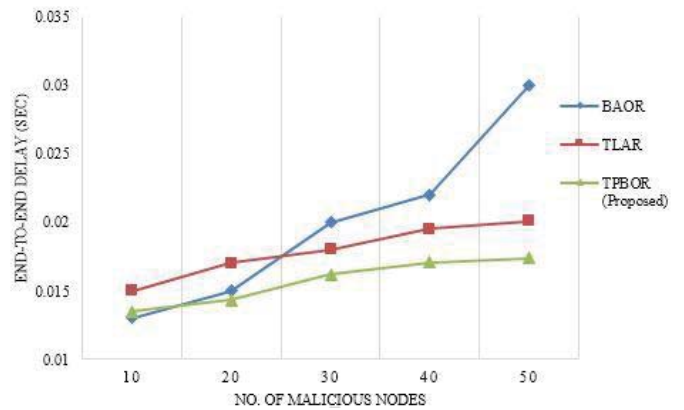


Fig. 3. Performance on the basis of End-to-end Delay

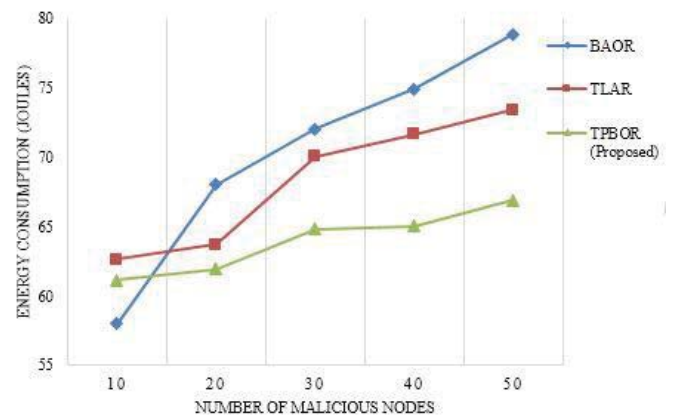


Fig. 4. Performance on the basis of Total Energy Consumption

In WSN energy consumption is the most important factor to monitor. This will decide on the network lifetime and hence here the performance of all three algorithms has been tested on the basis of average energy consumption. The energy consumption in the network depend the energy consumed at node's radio for transmitting and receiving packets. The energy consumption of BAOR [23] will be lowest initially because of less overhead and less number of malicious nodes (figure 4). But with the increase in number of malicious nodes the energy consumption also increases in the network. TPBOR consumes very less energy as compared to BAOR [23] and TLAR [21] in presence of malicious nodes. Because the computation overhead is low and also the trust value distributes the energy consumption among all nodes. Hence, TPBOR turns out to be an energy saver algorithm.

IV. CONCLUSION

This paper presented an opportunistic routing protocol for WSN with added security feature. Trust and reputation based routing protocols helps to avoid the malicious nodes on the path. Also trust management can be used to avoid duplication and unnecessary packet forwarding towards base station. The proposed protocol TPBOR introduced impact on energy into the trust value so that only energy efficient nodes can take part in the routing process. TPBOR also introduces the relay selection criteria to select the best next-hop to forward data packets. In relay selection criteria queue size of each node has been considered. If a node is loaded with number of packets than this node will not be included in routing process until it forward some of its packets toward destination. Hence, each node can transmit its data toward the base station without congestion. Also the trust management reduce overhead of security and hence it will prolong the network lifetime. The simulation results has shown that TPBOR performs better in presence of malicious nodes in the network. In future directions we can consider more parameters in trust value calculation, but the more the parameters more will be computational overhead. Hence, only those parameters should be considered which are seem to be important in the network like energy, packet delivery etc.

References

- [1] Akyildiz, I.F., and Kasimoglu, I.H.: 'Wireless sensor and actor networks: research challenges', *Ad hoc networks*, 2004, 2 (4), pp. 351-367.
- [2] Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., and Song, Y.-J.: 'Group-based trust management scheme for clustered wireless sensor networks', *IEEE transactions on parallel and distributed systems*, 2009, 20 (11), pp. 1698-1712.
- [3] Yao, L., Man, Y., Huang, Z., Deng, J., and Wang, X.: 'Secure Routing based on Social Similarity in Opportunistic Networks', *IEEE Transactions on Wireless Communications*, 2016, 15 (1), pp. 594-605.
- [4] Yao, Z., Kim, D., and Doh, Y.: 'PLUS: Parameterized and localized trust management scheme for sensor networks security', in *proceedings of International Conference on Mobile Ad Hoc and Sensor Systems (IEEE)*, Vancouver, BC, 2006, pp. 437-446.
- [5] Zhou, Y., Tan, X., He, X., Qin, G., and Xi, H.: 'Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature', *Information Assurance and Security Letters* 1, 2010, pp. 18-23.
- [6] Kumar, N., and Singh, Y.: 'Routing Protocols in Wireless Sensor Networks', *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, IGI Global, 2016, pp. 86-128.
- [7] Biswas, S., and Morris, R.: 'ExOR: opportunistic multi-hop routing for wireless networks', in *Proceedings of 35th SIGCOMM Computer Communication Review (ACM, 2005)*, Philadelphia, Pennsylvania, USA, pp. 133-144.
- [8] Zhong, Z., Wang, J., Nelakuditi, S., and Lu, G.-H.: 'On selection of candidates for opportunistic anypath forwarding', *ACM SIGMOBILE Mobile Computing and Communications Review*, 2006, 10 (4), pp. 1-2.
- [9] Hsu, C.-J., Liu, H.-I., and Seah, W.K.G.: 'Opportunistic routing: A review and the challenges ahead', *Computer Networks*, 2011, 55 (15), pp. 3592-3603.
- [10] Liu, K., Abu-Ghazaleh, N., and Kang, K.-D.: 'Location verification and trust management for resilient geographic routing', *Journal of Parallel and Distributed Computing*, 2007, 67 (2), pp. 215-228.
- [11] Dubois-Ferriere, H., Grossglauser, M., and Vetterli, M.: 'Valuable detours: Least-cost anypath routing', *IEEE/ACM Transactions on Networking*, 2011, 19 (2), pp. 333-346.
- [12] Rozner, E., Seshadri, J., Mehta, Y.A., and Qiu, L.: 'SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks', *IEEE Transactions on Mobile Computing*, 2009, 8, (12), pp. 1622-1635.
- [13] Ganeriwal, S., Balzano, L.K., and Srivastava, M.B.: 'Reputation-based framework for high integrity sensor networks', *ACM Transactions on Sensor Networks (TOSN)*, 2008, 4 (3), pp. 15.
- [14] Michiardi, P., and Molva, R.: 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks': 'Advanced communications and multimedia security' (Springer, 2002), pp. 107-121.
- [15] He, Q., Wu, D., and Khosla, P.: 'SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks', in *Proceedings of Wireless communications and networking conference (IEEE, 2004)*, Atlanta, GA, USA, pp. 825-830.
- [16] Salehi, M., Boukerche, A., Darehshoorzadeh, A., and Mammeri, A.: 'Towards a novel trust-based opportunistic routing protocol for wireless networks', *Wireless Networks*, 2016, 22 (3), pp. 927-943.
- [17] Deng, H., Yang, Y., Jin, G., Xu, R., and Shi, W.: 'Building a trust-aware dynamic routing solution for wireless sensor networks', in *Proceedings of Globecom Workshops (IEEE)*, Miami, Florida, USA, 2010, pp. 153-157.
- [18] Maarouf, I., Baroudi, U., and Naseer, A.R.: 'Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks', *IET communications*, 2009, 3 (5), pp. 846-858.
- [19] Gong, P., Chen, T.M., and Xu, Q.: 'ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks', *Journal of Sensors*, 2015.
- [20] Adnan, A., Kamalrulnizam Abu, B., Muhammad Ibrahim, C., and Abdul Waheed, K.: 'A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network', *Mob. Netw. Appl.*, 2016, 21 (2), pp. 272-285.
- [21] Vamsi, P.R., and Kant, K.: 'Trust and Location-Aware Routing Protocol for Wireless Sensor Networks', *IETE Journal of Research*, 2016, 63, pp. 1-11.
- [22] Kumar, N., and Singh, Y.: 'An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks', *Indian Journal of Science and Technology*, 2016, 9 (32), pp. 1-7.
- [23] Cui, W., Yao, Y. and Song, L.: 'Buffer-aware opportunistic routing for wireless sensor networks', *14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2017, pp. 268-271.
- [24] Michel, M., Duquenois, S., Quoitin, B. and Voigt, T.: 'Load-Balanced Data Collection through Opportunistic Routing', *International Conference on Distributed Computing in Sensor Systems*, Fortaleza, 2015, pp. 62-70.
- [25] Liu, Z., Wei, C., Qin, C., Li, H., Niu, X. and Wang, L.: 'POR: A Packet-Based Opportunistic Routing Protocol for Wireless Sensor Networks', *International Conference on Computer Sciences and Applications*, Wuhan, 2013, pp. 158-162.
- [26] Kumar, N. and Singh, Y.: 'An energy efficient and trust management based opportunistic routing metric for wireless sensor networks', *Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Wagnaghat, 2016, pp. 611-616.