DEVELOPMENT OF ROUTE RECOVERY PROCESS OF LINK FAILURE OVER MOBILE SENSOR NETWORK BY USING CHECK POINT ROUTE RECOVERY ALGORITHM

A Thesis Submitted to

SRI KRISHNADEVARAYA UNIVERSITY, ANANTAPURAMU.

In partial fulfillment of the award of the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & TECHNOLOGY

BY

Mr. A. RAVI CHANDRA REDDY, M.Sc. (cs),

Under the supervision of

Dr. V. RAGHUNATHA REDDY

Assistant Professor

Department of Computer Science & Technology

Department of Computer Science & Technology

SRI KRISHNADEVARAYA UNIVERSITY

ANANTAPURAMU-515003

INDIA

March 2016

DEVELOPMENT OF ROUTE RECOVERY PROCESS OF LINK FAILURE OVER MOBILE SENSOR NETWORK BY USING CHECK POINT ROUTE RECOVERY ALGORITHM

Thesis Submitted to

SRI KRISHNADEVARAYA UNIVERSITY, ANANTAPURAMU.

In partial fulfillment of the award of the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & TECHNOLOGY

BY

K. HANUMANTHU NAIK
M.C.A.

Under the supervision of

Dr. V. RAGHUNATHA REDDY
M.C.A., Ph.D.,
Assistant Professor
Department of Computer Science & Technology

DEPARTMENT OF COMPUTER SCIENCE & TECHNOLOGY

SRI KRISHNADEVARAYA UNIVERSITY

ANANTAPURAMU-515 003, ANDHRA PRADESH, INDIA

AUGUST 2016

SRI KRISHNADEVARAYA UNIVERSITY

ANANTAPURAMU

CERTIFICATE

*This is to certify that the thesis entitled "***Development of Route Recovery Process of Link Failure over Mobile Sensor Network by using Check Point Route Recovery Algorithm***" is a bonafide research work done by* ***K. HANUMANTHU NAIK****, under my supervision during the period 2011-2016 in the Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapuramu, for the award of the degree of Doctor of Philosophy. This research work has not previously formed the basis for the degree or diploma by any University or Institution.*

Date: **(Dr. V. RAGHUNATHA REDDY)**

Place: Anantapuramu **Research Supervisor**

DECLARATION

I declare that the thesis entitled "***Development of Route Recovery Process of Link Failure over Mobile Sensor Network by using Check Point Route Recovery Algorithm"*** is original and has been carried out by me in the Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India and has not been submitted to any other university or Institution for the award of any other Degree or Diploma.

Date: **(K. HANUMANTHU NAIK)**

Place: S.K.UNIVERSITY

ACKNOWLEDGEMENTS

I feel immense pleasure in expressing my profound sense of gratitude to my research supervisor ***Dr.V.Raghunatha Reddy*, Assistant Professor, Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu**, for his inspiring guidance, kind concern, infallible help, constant encouragement, and inspiration, without which this work might not have been completed. I had privilege to carry out my research work. I learnt many moral and ethical standards from him in academic and non-academic fields.

I want to express my sincere and respectful thanks to all my teaching members ***Prof. B.Sathyanarayana*,** Chairman, BOS, ***Prof. T.Bhakara Reddy***, Head of the Department, ***Prof. G.A.Ramachandra*, *Prof. N.Geethanjali*, *Prof. M.Nagendra, Dr. J.Keziya Rani, Dr. P.Devaraaju*** and non-teaching staff of the **Department of Computer Science and Technology, Sri Krishnadevaraya University** for their constant encouragement and review of this work with valuable suggestions.

I record my sincere thanks to my research friends ***A. Ravi Chandra Reddy, N.Ramesh Babu, G.Thippana, P. Krishnaiah and P.Sumalatha*** for their valuable suggestions and encouragement during the course of my thesis. I offer my sincere thanks to ***K.Sankar Naik, S.N.Meera Vali*** for their constant encouragement.

I have great pleasure in expressing my heartiest thanks to ***Dr. P.V. Subba Reddy***, Assistant Professor, National Institution of Technology (NIT), Warangal and ***Mr. A.Nagarjuna***, EMC^2 Software Company, Bangalore for providing an opportunity to fulfill my long-cherished dream of pursuing research and providing necessary infrastructure, technical support with all modern amenities.

I am grateful to my parents ***Sri. K.Beeka Naik*** and ***Smt. K.Bhaddemma*** by the way of inspiration, patience and encouragement at all times but most conspicuously during this period. I dedicate this thesis to them.

I want to express my deep gratitude to my uncle ***Sri. K.Lakshma Naik*** without whose constant support, help and cooperation, my endeavor of research work. I

would like to thank my brothers ***K.Tirupal Naik*** and ***K.Dass Naik*** and my sisters and brother-in-law's and all other relatives for their continuous support.

Further I would like to thank all my friends and well-wishers who supported me in every step of my life and encouragement to purse PhD from this reputed university. I also thank all the anonymous reviewers of my journal papers of this thesis for their constructive comments and valuable recommendations which made me to progress ahead into much depth of the subject.

In the end, I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

K.HANUMANTHU NAIK

ABSTRACT

Mobile Sensor Networks (MSNs) is a collection of sensing devices that can wirelessly communicate with each link among all the mobile nodes. In dynamic topology the nodes are free to move and frequently change their positions. Link failure is a major issue of the current wireless mobile sensor network due to node mobility, node energy loss or drain to battery power. This research work has been made to compare the performance of three prominent mechanisms support of AODV routing protocol for Mobile sensor network: Divert Failure Route Recovery (DFRR), Proposed AODV (PRO-AODV) and Check Point Route Recovery (CPRR) mechanisms. PRO-AODV and DFRR mechanisms were designed to avoid a link failure route recovery process, based on node sequence number and in advance node signal strength connection in a highly dynamic ad hoc network. CPRR mechanism overcomes the problems of low energy in a node, node monitoring and blocking of node and rectification of a process for an active communication. The CPRR mechanism maintains sensor activities on actor nodes, link failure route recovery process can be done by using the help of static, dynamic sensors and Network Topology Management (NTM) for optimal connection in MSNs. The performance evaluation of these three methods are analyzed at different time intervals. The entire work is compiled by NS-2 simulator. The evaluation and implementation of efficient routing establishment methods are analyzed by using different parameter metrics.

The entire theme of the thesis is presented in **six chapters**. The **first chapter** is an **introduction** of mobile ad-hoc network (MANET), Characteristics, and routing protocols for MANET. Wireless sensor network (WSN) is studied with

respect to the basic architecture of sensor node, and applications of WSN. Description about Mobile Wireless Sensor Network (MWSNs) and three tier architecture of MWSNs. The process of energy management schemes in mobile sensor networks is discussed. At the end of the chapter motivation for research work and organization of the thesis is presented.

The **second chapter**, provides **Review of Routing Schemes** where routing is a major challenge of WSN. Routing schemes are categorized into two types namely static and dynamic routing. Routing protocols must be paid enough attention for energy restricted nature of WSNs. Routing protocols detect the most feasible route from the source to destination. The major issue for route failure, classification of failure and route recovery process in sensor networks are studied. Energy efficient techniques are also studied and classified into sub categories. The recent and previous papers are reviewed for clarification.

The **third chapter,** deals with the existing work related to divert failure route recovery approach, a link failure problem on Mobile Sensor Network by using Divert Failure Route Recovery (DFRR) mechanism for optimization of round trip path algorithm. The Round trip path detection algorithm, circular topology, and flow chart of DFRR Process is explained. The first proposed method PRO-AODV mechanism focuses route repair of the links based on energy level of sensor nodes by detecting efficient route between the source and destination in a mobile sensor network.

The **fourth chapter,** presents the development of proposed **Check Point Route Recovery Algorithm** for prevention of node failure in Mobile Sensor Networks. The CPRRA is used to detect the energy drain in a node, before the energy of that node is completely drained. The link failure node replaces using static sensor and dynamic sensor node. The sensor nodes are examined by considering the packet delivery rate and energy backup. This method reduces the energy consumption by detecting effective routes between the sources to destination. Dynamic sensor mechanism is used to find the nearest node whose energy level is high and has less links of a node. The Network Topology Management (NTM) helps to maintain the link between the nodes. The CPRR algorithm generates valuable results through NS-2 simulation with several parameter metrics.

The **fifth chapter,** describes the comparison of **performance evaluation** of the four methods. The evaluation of performance of the four methods are based on parameter metrics such as packet delivery ratio, end-to-end delay, average delay, detection time, throughput, energy consumption and draining rate of energy. The CPRR proposes a new routing approach to reduce the energy consumption and to enhance lifetime of the Mobile WSN. The experimental results of the CPRR work are compared with proposed and existing works such as Proposed AODV (PRO-AODV) routing, Ad hoc On-demand Distance Vector (AODV) routing, Divert Failure Route Recovery (DFRR) based Round Trip Path algorithm.

The **sixth chapter** presents conclusion and the perspectives to extend the future scope of this work.

CONTENTS

BIBLIOGRAPHY

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF ABBREVATIONS

ABR	Associated Based Routing
AODV	Ad Hoc On-Demand Distance Vector
AODV-RD	Ad Hoc on Demand Distance Vector-Reliable Delivery
AS	ApplicationState
BS	Base Station
CGSR	Cluster head Gateway Switch Router
CPRR	Check Point Route Recovery
CPRRA	Check Point Route Recovery Algorithm
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access
DC-AODV	Delay Constraint Ad Hoc on Demand Distance Vector
DFRR	Divert Failure Route Recovery
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
IP	Internet Protocol
LEACH	Low-Energy Adaptive Clustering Hierarchy
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MCs	Monitoring Cycles
MPs	Monitoring Paths

LIST OF ABBREVATIONS

MSN	Mobile Sensor Network
MWSNs	Mobile Wireless Sensor Networks
NAM	Network Animator
NS2	Network Simulator2
OLSR	Optimized Link State Routing Protocol
OS	Operating System
PDR	Packet Delivery Ratio
PEGASIS	Power-Efficient Gathering For Sensor Information Systems
PRO-AODV	Proposed Ad hoc On-demand Distance Vector
QoS	Quality of Service
READ	Residual Energy Aware Dynamic Topology
RERR	Route Error Message
RF	Radio Frequency
RR	Rumor Routing
RREP	Route Reply Message
RREP-ACK	Route Reply Acknowledgment
RREQ	Route Request Message
RTD	Round Trip Delay
RTP	Round Trip Path
RTT	Round-Trip Time

LIST OF ABBREVATIONS

S-MACS	Self-Organizing Mac For WSNS
SN	Sensor Node
SPIN	Sensor Protocols For Information Via Negotiation
Tcl	Tool command language
TDMA	Time Division Multiple Access
TORA	Temporary Ordered Routing Algorithm
TRAMA	Traffic Adaptive Medium Access
VANETs	Vehicular Ad Hoc Networks
WMN	Wireless Mesh Network
WRP	Wireless Routing Protocol
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol

CHAPTER 1

INTRODUCTION

CHAPTER 2

REVIEW OF ROUTING SCHEMES

CHAPTER 3

ROUTE RECOVERY PROCESS OF DFRR & PRO-AODV MECHANISMS

CHAPTER 4

ROUTE RECOVERY PROCESS OF CHECK POINT ROUTE RECOVERY ALGORITHM

CHAPTER 5

PERFORMANCE EVALUATION

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

LIST OF PUBLICATIONS

BIBLIOGRAPHY

1.1. Introduction

A wireless network is a type of computer network that uses wireless data connections for connecting network nodes [1]. A wireless ad-hoc network is a computer network in which the communication links are wireless. Each node participates in routing, by forwarding data to other nodes. So the determination of the way in which information is forwarded by nodes is made dynamically on the basis of network connectivity [2]. Wireless ad-hoc networks can be further classified into Mobile Ad hoc Network (MANET), Wireless Mesh Network (WMN), Wireless Sensor Network (WSN), Mobile Wireless Sensor Network (MWSN) and other such applications.

Mobile Ad hoc Network (MANET) [3] is a collection of wireless mobile nodes forming a brief network without the help of any centralized system. The Ad- hoc configuration is dynamic i.e., nodes enter and leave the network continuously. In MANET, each node acts as a node. In addition, as a router with an arbitrary topology movement every node should work as a router and forward data packets to the destination device. The source sends the message or packet communication to destination node through the intermediate nodes. All nodes are equipped with wireless system for functioning and is connected dynamically in arbitrary communication.

This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication by installing a base station (BS) as access point. In this mobile ad hoc networks, communication between two mobile nodes completely rely on the Wi-Fi access and the cellular base station is the backbone of the network shown in figure 1.1. In a MANET, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. The obligations regarding sorting out and overwhelming the system are conveyed through the terminals themselves. The complete network is mobile, and in this way the individual terminals are permitted to move freely with respect to each other. In this type of network, a few pairs of terminals may not be able to communicate directly with one another and in such cases relaying on some messages are needed so that they're delivered to their destinations. The nodes of these networks additionally perform as routers that discover and maintain routes to different nodes in the networks. The hubs might be situated in or on planes, ships, trucks, and such vehicles maybe even on individuals who carry small gadgets.

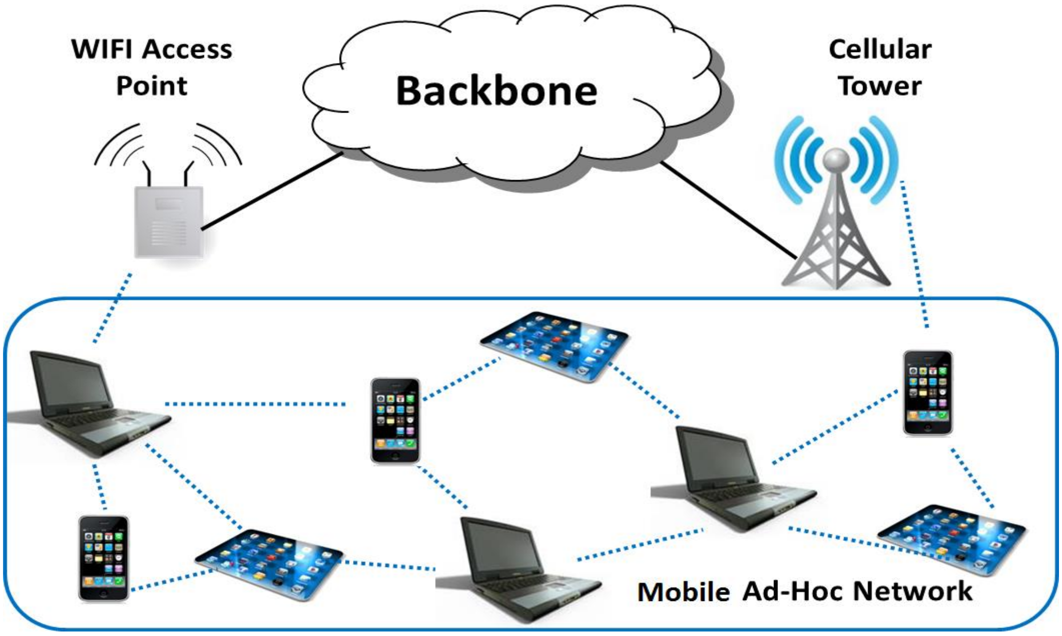


Figure.1.1: Mobile Ad-Hoc Network

The MANET plays a major role in wireless communication and provides effective communication. Some of the applications are as follows:

- Military Battlefield
- Emergency Operations
- Civilian Environment
- Local level view
- Personal area network and Bluetooth
- Commercial Sector

1.2. Characteristics of MANET

The characteristics of MANET such as dynamic topology, multi-hop routing, frequent link breakages, limited power and limited bandwidth capacity posture challenges for the redesigning, for more effectiveness of the above mentioned applications.

- **Dynamic Topologies:** Nodes are allowed to move arbitrarily with various speeds and the network topology may change randomly with any prior information. The nodes in the MANET set up routing among themselves as they travel around. The connections might be unidirectional or bidirectional.
- **Multi hop routing:** When a node tries to send information to different nodes which are out of its correspondence range, the packet should be forwarded via relay of intermediate nodes.
- **Bandwidth constrained, variable capacity links:** Wireless connections bring down the variable capacity links than those of their hardwired partners. Likewise, because of various accesses, blurring, noise, and other conditions the wireless links have low throughput.

- **Energy constrained operation:** Some or all of the nodes in a MANET may depend on batteries. In this situation, the most important system design criteria for optimization may be energy conservation.
- **Limited physical security:** Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The expanded probability of spying, spoofing, and denial-of-service attacks should be carefully considered. Existing connection security systems are frequently connected to remote systems to decrease security threats. As an advantage, the decentralized nature of network control in MANET provides additional strength against the single point of failure of more centralized approaches.

1.3. Routing Protocols in Mobile Ad-hoc Network

Routing protocols in the units of ad hoc networks are mobile, the network topology is subjected to frequent changes, implying that routing protocols must react quickly to changes in topology. Routing in ad hoc networks should be a distributed algorithm that computes multiple, loop-free routes while keeping the communication overhead to a minimum [4]. The existing routing protocols developed for wired networks, do not fit the needs of ad hoc networks as they would consume a large amount of the network's bandwidth and of the unit's processing power. For these reasons, routing in ad hoc networks is a challenging field.

A number of routing protocols have been suggested for wireless mobile ad-hoc networks as shown in figure 1.2.

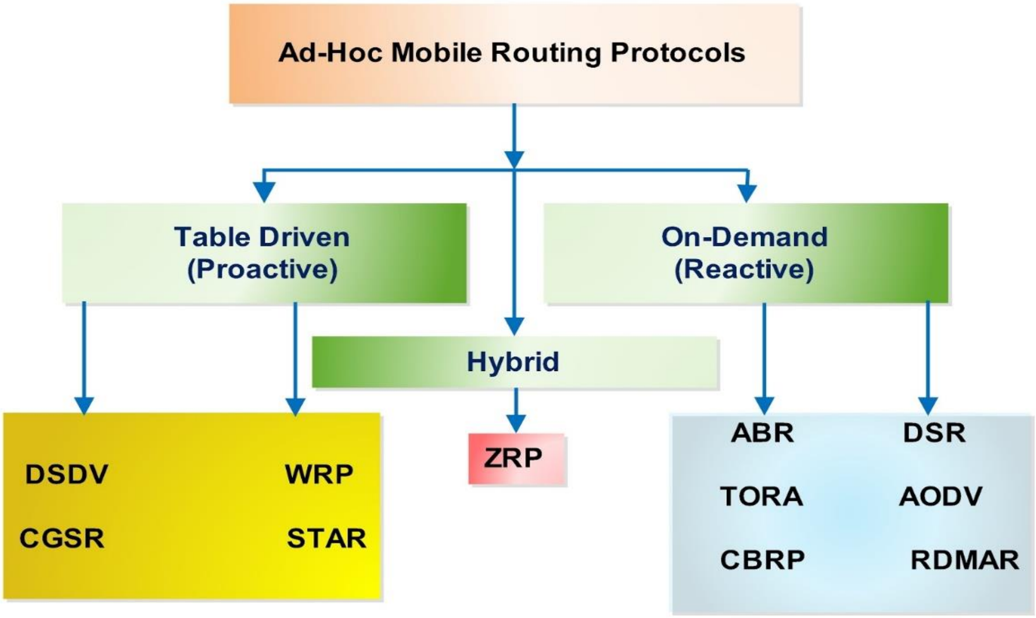


Figure.1.2: Mobile Ad-Hoc Routing Protocols.

Mobile Ad-hoc Routing protocols can be classified into three categories:

i. Table driven or Proactive routing protocols

ii. On-Demand or Reactive routing protocols

iii. Hybrid routing protocols

i. Table driven / Proactive Routing Protocols

Table-driven or proactive routing protocols finds routes to all possible destinations ahead of time. The routes are recorded in the routing tables of the nodes and are updated within the pre-defined intervals. The proactive routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Proactive routing protocols are faster in decision making but cause problems, when the topology of the network continually changes. These protocols require every node to maintain one or more tables to store updated routing information from other nodes.

A. Destination sequenced distance vector [DSDV]

The DSDV [5] is table driven based routing algorithm. DSDV is the improved version of Bellman Ford routing algorithm. Each DSDV node maintains two routing tables. The first table is for forwarding packets, and the second table for advertising incremental updates. The routing table updates are sent periodically to every other node. In this way, all the nodes will have latest information and maintain table consistency. The nodes will maintain a routing table that consists of a sequence number.

A node or a mobile device will make an update in its routing table and send the information to its neighbour upon receiving the updated information and make an update in its own routing table. The update is made by comparing the sequence number received if it is greater than present sequence number and it will make use of the latest number. If there is a link failure in one of the nodes will change the metric value to infinity and broadcast the message.

B. Wireless Routing Protocol [WRP]

WRP [6] is also based on table driven approach and this protocol makes use of 4 tables. They are:

- Distance table, which contains information like destination, next hop, distance.
- Routing table, which contains routing information.
- Link cost table, which contains cost information to each neighbour.
- Message retransmission list table, this table provides sequence number of the message, a retransmission counter, acknowledgements and list of updates sent in update message.

Whenever there is a change in the network, an update will be made which will be broadcasted to other nodes. Other nodes upon receiving the updated information will make an update in own their tables. If there is no update in the network a hello message should be sent.

C. Cluster head Gateway Switch Router [CGSR]

CGSR is also a table driven routing protocol. In this algorithm the mobile devices will be grouped to form a cluster. This grouping is based on the range and each cluster is controlled by cluster head. All the mobile devices will maintain 2 tables and they are cluster member table and routing table. The cluster member table will have the information about the cluster head for each destination and the routing table will have routing information. In this protocol the packet cannot be directly sent to the destination. Instead cluster heads are used for routing. CGSR routing involves cluster routing, where a node finds the best route over cluster heads from the cluster member table.

D. Source Tree Adaptive Routing (STAR)

The Source Tree Adaptive Routing protocol is based on the link state algorithm. Each router maintains a source tree, which is a set of links containing the preferred paths to destinations. This protocol has significantly reduced the amount of routing overhead disseminated into the network by using a least overhead routing approach (LORA) to exchange routing information [8]. This approach eliminated the periodic updating procedure present in the Link State algorithm by making update dissemination conditional. As a result the Link State updates are exchanged only when certain event occurs. Therefore STAR perfectly suits for large network as it has significantly reduced the bandwidth consumption for the routing updates. At the same time reducing latency by using predetermined routes. However, this protocol may have significant memory and processing overheads in large and highly mobile networks, because each node is required to maintain a partial topology graph of the network, which changes frequently as the neighbours keep reporting different source trees.

ii. On-Demand/Reactive Routing Protocols

Reactive or On-Demand routing protocols are on-demand procedures and create routes only when requested to do so by source nodes. A route request initiates a route-discover process in the network and is completed once a route is discovered. If it exists, at the time of request, a route is maintained by a route-maintenance procedure until either the destination node becomes irrelevant to the source or the route is no longer needed. Control overhead of packets is smaller than of proactive protocols.

a. Associated Based Routing [ABR]

ABR [9] is an efficient on-demand or source initiated routing protocol. In ABR, the destination node decides the best route, using node associativity. ABR is suitable for small networks, as it provides fast route discovery and creates shortest paths through associativity. Each node keeps track of associativity information by sending messages periodically.

If the associativity value is more, it means mobility of nodes is less. In ABR the source which wants to send the packet to the destination will create a query packet and broadcast in the network. Query packet generation is required for discovering the route. The broadcast continues as long as destination is reached. Once the destination is reached it creates the reply packet and sends back to the source.

The query packet will have the following information.

1. Source id
2. Destination id
3. All intermediate node id
4. Sequence number
5. CRC and
6. Time to live [TTL]

A node sends an update packet to the neighbours' and waits for the reply. If update is received back, then an associative tick will be incremented higher then what it was. It means the particular mobile device is still a part of the network, otherwise it might not be.

b. Dynamic Source Routing [DSR]

DSR [10] is a source initiated or on demand routing protocol in which source finds unexpired route to the destination to send the packet. It is used in the network where mobile nodes move with moderate speed. As a result of this Control Overhead is significantly reduced.

DSR has two phases.

- Route discovery
- Route maintenance

The function of the route discovery is as follows: the source which wants to send the information to the destination will create a route request message by adding its own identification number and broadcasts them in the network. The intermediate nodes will continue the broadcast by adding their own identification number. When the destination is reached a route reply message is generated which will be sent back to the source. The source can receive multiple route replies indicating the presence of multiple paths.

The function of the route maintenance is as follows: the source will pick up one of the paths and will use it for transmission. If there is a link failure, one of the nodes will detect and will create a route error message which will be sent back to the source. In this case the path has to be re-established for further transmission.

c. Temporary Ordered Routing Algorithm [TORA]

It is also a source initiated routing algorithm, creates multiple routes for any source/destination pair. The advantage of multiple routes is that route discovery is not required for every alteration in the network topology.

TORA consists of three phases,

- Route Creation/discovery
- Route maintenance
- Route erasure

TORA [11] uses three types of packets: Query Packets for route creation, Update Packets for both source and destination and third packet for maintenance. The route will be discovered from the source to destination only when a request is made for the transmission. In this algorithm the source will generate a query packet which will be broadcasted in the network and this continues as long as a node that is directly connected to the destination is identified. When the destination is identified an update packet will be generated and sent back to the source. The update packet will have the path information if there are more than one update packet received by the source, it means that there are multiple paths to the destination, and the source has to choose the best path available.

d. Ad-hoc On-demand Distance Vector [AODV]

AODV (Ad Hoc On-Demand Distance Vector) Routing Protocol changes the Proactive protocol on the way of creating routing. AODV [12] routing protocol allows nodes to create new routes to destinations. The routing information as well as exchange to the routing tables should be maintained by intermediate nodes. Source node to destination node of a communication connection have valid routes in each other, AODV routing permits mobiles nodes to response link break and changes in dynamic network topologies in time manner. This routing protocol works the number of broadcasts by creating routes based on, on-demand route obtained system. The route discovery and route maintain links are used in AODV routing protocol following control messages are:

Route Request Message (RREQ),
Route Reply Message (RREP),
Route Error Message (RERR),
Route Reply Acknowledgment (RREP-ACK) Message,
HELLO Messages.

- **Route Discovery**

The source node [13] initiates to send a message to destination node through its neighbour node destination sequence number and not its broadcasts a RREQ message. The RREQ message process takes two types: one, if there is a known route to the destination and the source node can send RREQ message uniquely identified by source address, broadcast ID. Source node initiates a RREQ message with the current sequence number of Source node and the last known destination sequence number of Destination node and broadcast ID. This broadcast ID is incremented each time source node sends a RREQ message. In route discovery phase the path from source to destination is identified by broadcasting route request packet [RREQ]. When the intermediate node receive RREQ they will create a backward pointer and continue the broadcast when the route request packet reaches the destination a route reply [RREP] would be generated. The destination node can send a Route Reply (RREP) message back to source node, otherwise they will rebroadcast the RREQ to their set of neighbour nodes. The message keeps getting rebroadcast until its lifetime is up. If source node does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan time and a new ID number. This entry contains the IP address and current sequence number of source node, number of hops to source and the address of the neighbour from whom destination got the RREQ messages. The destination node sets up a reverse route entry in its route table for the source node. Every node here maintains its own sequence number and IP address.

The route request packet can have the following information.

1. Source id
2. Destination id
3. Sequence number
4. Backward pointer information
5. CRC and
6. Time to live [TTL]

In the above network the RREQ will be broadcasted by the source node to the destination node and the neighbours will check whether RREQ is already processed. If it is already processed the packet will be discarded. If it is not processed a backward pointer is created and the broadcast continues. When the packet is reached at destination a route reply is created [RREP] in the above network. The first RREP is sent to the source can have the path information. When the source receives this information it will be stored in the routing table. Meanwhile the destination can create one more RREP which can have the information. The destination will send this RREP to the source and will also ask the source to discard old path as the new path is having minimum number of hops.

- **Route Maintenance**

The source node and destination node establish a route in a unicast, route maintained as long as source node needs the route. If source node moves during an active session, it can reinitiate route discovery to establish a new path to destination node. When a route fails to do it function, a destination node or an intermediate node sends a route error (RERR) message to source node. The source node receives a RERR, it first checks whether the node that sent the RERR is its next hop to any of the destinations listed in the RERR. The link break is detected, either by a Medium Access Controller (MAC) layer acknowledgment or by not receiving HELLO messages. HELLO messages may be used to discover route links to neighbour nodes. In such a case, every node broadcasts periodic HELLO messages to all its neighbour nodes. If the sending node is the next hop to any of these destinations, the node invalidates these routes in its route table and then propagates the RERR back towards the source. The RERR continues to be forwarded in this manner, until it is received by the source. Once the source node receives the RERR message, it can reinitiate route discovery with the route request and route reply message process if it faces a link broken state. Intermediate node invalidates its route table entries for both nodes, creates a RERR message listing these nodes, and sends the RERR forward towards the source node. In route discovery period, route repairing node has not received a RREP message for that destination node. However, if the repairing node receives a RREP message, it ensures low overhead and average end to end delay.

e. Cluster Based Routing Protocol (CBRP)

Cluster Based Routing Protocol [14] is an on-demand routing protocol, where the nodes are divided into clusters. It uses clustering's structure for routing protocol. Clustering is a process that divides the network into interconnected substructures, called clusters. Each cluster has a cluster head as coordinator within the substructure. Each cluster head acts as a temporary base station within its zone or cluster and communicates with other cluster heads. CBRP is a routing protocol designed to be used in mobile ad hoc networks. The protocol divides the nodes of the ad hoc network into a number of overlapping or disjoint 2-hop diameter clusters in a distributed manner. Each cluster chooses a head to retain cluster membership information. There are four possible states for the node: NORMAL, ISOLATED, CLUSTERHEAD and GATEWAY. Initially all nodes are in the state of ISOLATED. Each node maintains the NEIGHBOR table wherein the information about the other neighbour nodes is stored cluster heads have another table (cluster heads NEIGHBOR) wherein the information about the other neighbour cluster heads is stored [14].

f. Relative Distance Micro-discovery Ad Hoc Routing (RDMAR)

Relative Distance Micro-discovery Ad Hoc Routing [15] is a source-initiated on-demand routing protocol and allows nodes to maintain routes to destinations that are in active communication. RDMAR uses no periodic beaconing to keep routing table's updated thus significantly reducing network bandwidth overhead, conserving battery power and reducing the probability of packet collision. In addition, in RDMAR nodes do not make use of their routing caches to reply to route queries. Using other nodes' cashes results in a storm of route replies and repetitive updates in hosts' caches. Yet early query quenching cannot stop the propagation of all query messages which are flooded all over the network. Furthermore, RDMAR does not rely on any specific location aided technology in order to compute routing patterns and to limit the query flood to a restriction region. Finally, in the presence of asymmetrical links traditional link-state or distance vector protocols may compute routes that do not work. Several factors such as interference, shadowing, differing radio or antenna capabilities, may turn a link to function asymmetrically. RDMAR, however, has been designed to compute correct routes even in the presence of asymmetric links.

iii. Hybrid routing protocol

The hybrid routing protocol combines the advantages of the proactive and reactive approaches by maintaining an up-to-date topological map of a zone centred on each node. Within the zone, routes are immediately available. This hybrid routing protocol works in scalable routing for large networks in Zone Routing Protocol.

❖ Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) [16] reaches a destination which is outside its zone. This employs a route discovery procedure, which can benefit from the local routing information of the zones. ZRP route discovery process is route table lookup and/or inter zone route query search. When a route is broken due to node mobility and if the source of the mobility is within the zone, it will be treated like a link change event and an event driven route updates used in proactive routing will inform all other nodes in the zone. If the source of mobility is a result of the border node or other zone nodes, then route repair in the form of a route query search is performed in the worst case of the source node is informed of route failure.

1.4. Wireless Sensor Network

A wireless sensor network (WSN) is a wireless sensing and networking technology that has attracted much attention because of its wide applications. A typical WSN consists of a number of tiny nodes called sensors. The Sensor networks are designed to perform some high level information processing tasks. Sensors have some unique characteristics compared to other networking devices. A simple sensor node has four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. It may have some additional units based on the applications, for example, a location finding system, a power generator, and a mobilizer [17]. The sensing unit is further divided into two parts: sensors and analog-to-digital converters (ADC). The processing unit, equipped with a small storage unit, helps the sensor node to collaborate with the other nodes in order to perform the assigned sensing jobs. The transceiver unit connects the sensor to the network. Some routing and sensing tasks need finding the locations of other sensors so some of the sensors might have a location finding system. The sensor node basic components is shown in the figure 1.3 which shows the details of sensor.

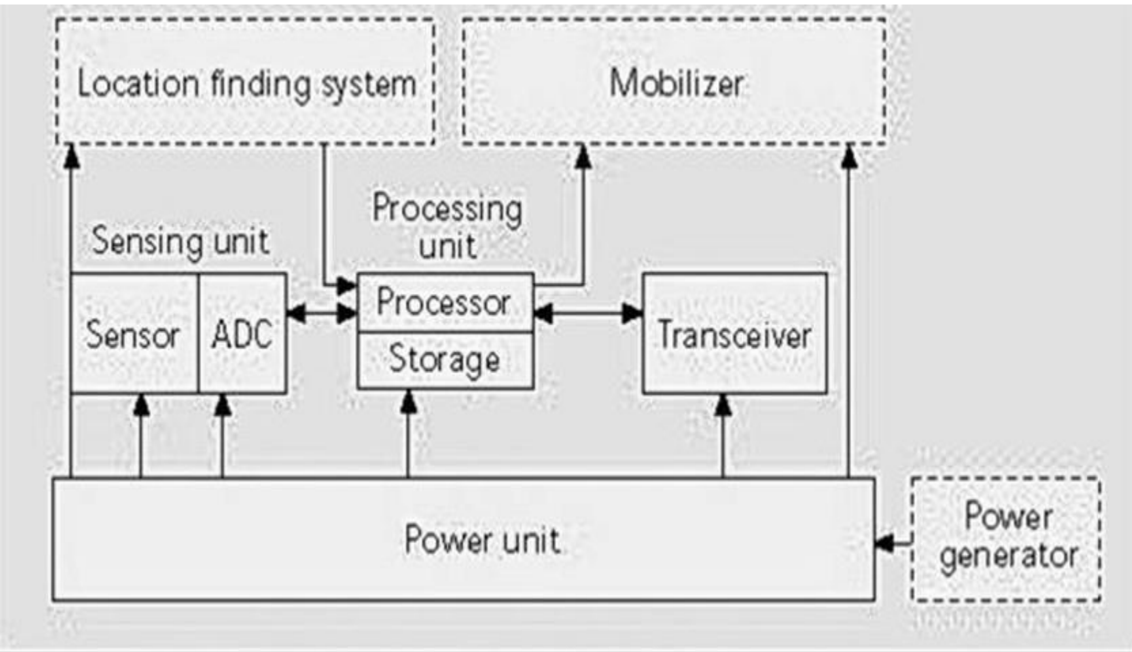


Figure 1.3: The relationship between the components of in a basic sensor node.

1.5. Architecture of Basic Sensor Node

A functional block diagram of a versatile wireless sensing node is provided in Figure 1.4. Modular design approach provides a flexible and versatile platform to address the needs of a wide variety of applications. For example, depending on the sensors to be deployed, the signal conditioning block can be re-programmed or replaced. This allows for a wide variety of different sensors to be used with the wireless sensing node. Similarly, the radio link may be swapped out as required for a given applications' wireless range requirement and the need for bidirectional communications. The use of flash memory allows the remote nodes to acquire data on command from a base station, or by an event sensed by one or more inputs to the node. Furthermore, the embedded firmware can be upgraded through the wireless network in the field. A key feature of any wireless sensing node is to minimize the power consumption by the system.

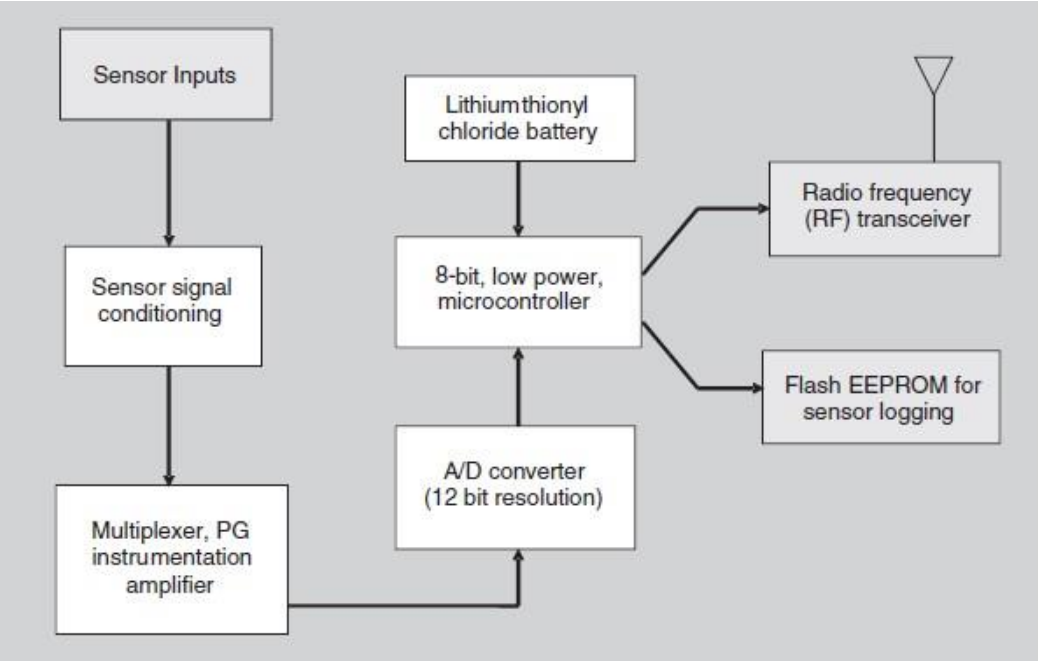


Figure 1.4: Wireless sensor node functional block diagram

Generally, the radio subsystem requires the largest amount of power. Therefore, it is advantageous to send data over the radio network only when required. This sensor event-driven data collection model requires an algorithm to be loaded into the node to determine when to send data based on the sensed event. Additionally, it is important to minimize the power consumed by the sensor itself. Therefore, the hardware should be designed to allow the microprocessor to judiciously control power to the radio, sensor, and sensor signal conditioner.

Based on the applications, the sensors are deployed randomly or deterministically to collect the information from the environment in a WSN. In a military battleground, sensors are sometimes typically deployed randomly to collect the information. But in associate degree environment observation system sensors are deployed deterministically at time intervals and at the essential places to observe the aspects of the environment. Normally lots of sensors are deployed at various intervals to study the environment to sense the information. Unlike different traditional networking devices, sensors have restricted power or energy provided in their batteries. Moreover, they have limited processing power, restricted memory and limited transmission range. A WSN in addition has one or more base stations that send some queries and gather the information from the sensor nodes. A base station is also known as a data collector or a sink node [18]. Normally the base stations and the sensor nodes are fixed in their position, but depending on the applications they'll be mobile too.

The sensors in a WSN send the data to a base station after doing some local processing. This communication can occur directly if the base station is within the transmission range of the sensors. If the base station is within the transmission range of the sensors then the sensors use multi-hop communications (using alternative intermediate sensors). A neighbour of a sensor is named as next hop if the sensor uses that neighbour to route a message. The intermediate devices are used to setup the routing of the messages to their destination. The following Figure 1.5 shows a multi-hop routing in a WSN. The circles denote sensor nodes.

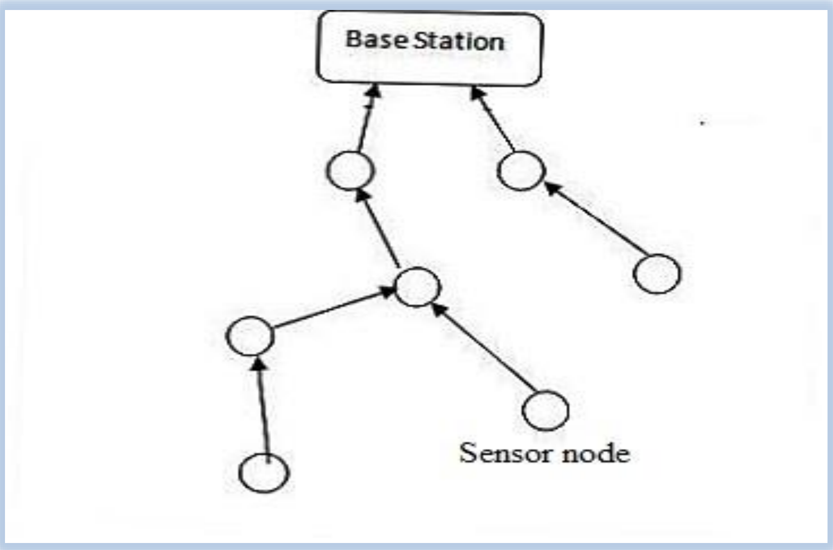


Figure 1.5: Multi-hop Routing in WSN

Since the energy of the sensors is limited and they use multi-hop communications to reach the base station, energy efficient routing protocols and the placement of the base station play a vital role in a WSN. The Base Station communicates with the user via sensor or satellite communication. It is located near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the base station by a multi-hop infrastructure less architecture.

1.6. Applications of WSNs

The WSNs are important in supporting a lot of extremely different real world applications, but a couple of the envisioned application scenarios shall be highlighted [19]. These are shown in the figure 1.6.

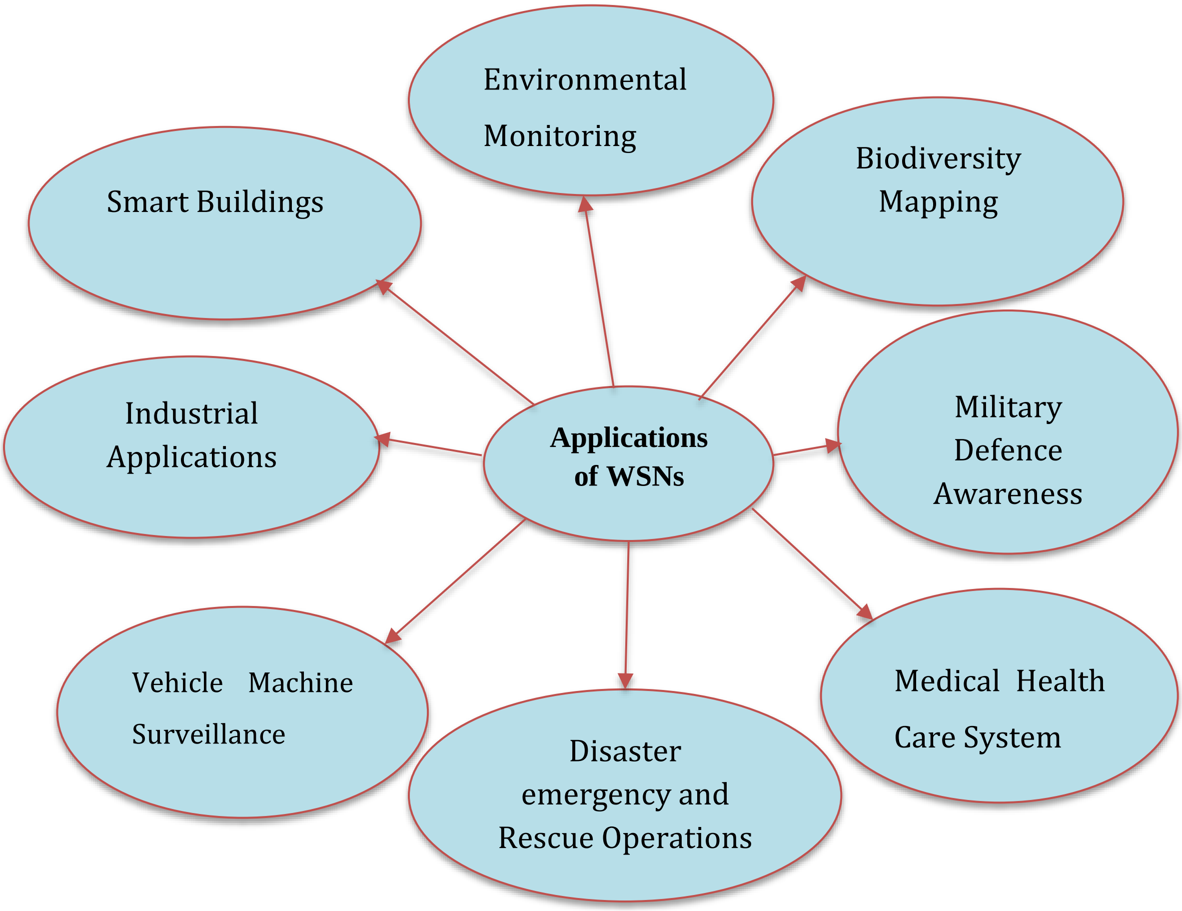


Fig.1.6: Applications of WSNs

i. Environment Monitoring
ii. Biodiversity Mapping
iii. Smart Intelligent Buildings
iv. Industrial Applications
v. Vehicle Machine Surveillance
vi. Disaster emergency and rescue Operations
vii. Military defence awareness
viii. Medical health care system

i. Environment (Monitoring of Environment)

Environmental tracking, such as forest detection, animal tracking, flood detection, forecasting and weather prediction, and other applications like prediction of seismic activities and monitoring. For controlling the environment, with respect to chemical pollutants, WSNs are extremely useful. The major advantages of WSNs are they are unattended, operated wirelessly and sensors are close to the objects that have to be observed.

ii. Biodiversity Mapping

WSN applied to agriculture allows irrigation and fertilizing by placing soil/humidity composition sensors into the fields. Pest control can be done effectively from a high- resolution surveillance of land. Farm animals breeding can have the advantage from attaching a sensor to each cow, which pedals the health status of the cow by checking its body temperature, step counting and raises alarms if the thresholds are exceeded.

iii. Smart Intelligent Buildings

Sensor nodes used to keep an eye on mechanical stress levels of buildings in seismically active zones. WSN extensively increases the comfort level for a better, real-time, high-resolution monitoring of humidity, temperature, airflow, and other physical parameters in a building.

iv. Industrial Applications

An industrial process monitoring, automated building climate control, civil structural health monitoring, habitat and ecosystem monitoring, Rapid development in structural planning and building emergency responses, etc.

v. Vehicle Machine Surveillance

The sensors embedded in the roadsides can gather data about traffic surroundings at a much higher grained resolution. These act as the vehicles to exchange danger warnings regarding road conditions or traffic jams ahead. Here the major advantage of WSNs is that the cable free operation, by using low-cost machinery in the sensors, and maintenance that drawback is easily avoided. The idea is to fix Sensor Nodes to cause difficulties to reach areas of machinery where they can detect vibration patterns, the need for maintenance. Examples could be robotics or the axles of a train.

vi. Disaster emergency and rescue Operations

The most often mentioned application types of WSN are disaster relief operations (example wildfire detection). The sensors are deployed over a wildfire from an airplane. They jointly produce a temperature map of the area with high temperature that can be accessed from the outside.

vii. Military defence awareness

Military applications, such as tracking and surrounding monitoring surveillance applications use these networks. The sensor nodes from sensor networks are dropped to the field of interest and are remotely controlled by a user. Security detections, Enemy tracking's are also performed by using sensor networks. At the time of war, it will be help to collect information from the enemy land and monitor that information at a far secure area, and safely devise a concept for the counter attack. Tracking locations of terrorist organizations and then set up the attack at an acceptable time.

viii. Medical health care system

Efforts are made to detect human being on a daily basis life pattern by measuring behavioural and physiological parameters using sensors. Health applications, such as tracking and monitoring of patients and doctors use these networks. For this purpose specialized sensors being developed to measure human body characterizing parameters such as heart rate, temperature, glucose level monitoring and cancer detectors.

1.7. Mobile Wireless Sensor Networks

Mobile Wireless Sensor Networks (MWSNs) recently launched a growing popular class of WSN community in which mobility plays a key role in the execution [20].

Mobile nodes monitoring in a Mobile Wireless Sensor Network. The design a cellular automaton based algorithm for monitoring mobile nodes in an MWSN restricted to a transmission range. To the best of our knowledge, this is the first cellular automaton based algorithm for communication in mobility problem. The mobile sensors are initially deployed in a square block where all the nodes are monitored by at least one of the mobile sensors. However, when the mobile nodes start moving they might not be monitored. For this reason, the mobile nodes also need to move and design a new movement algorithm. Note that, the speed of the mobile nodes should be higher than the mobile sensors. Otherwise, the problem becomes more complex. To compare our new algorithm, in terms of the percentage of the nodes monitored, with the increase of time and find that after a certain period of time this number becomes almost static and monitor a good portion of the nodes continuously. Mobility also can improve the coverage.

The nodes are generally mobiles in MWSNs, the topology is dynamic. New routing and Medium access control (MAC) protocols are needed in MWSNs. Traditional WSN routing protocols, which describe how to pass messages through the network so they will most likely reach their destination, typically rely on routing tables or recent route histories. In dynamic topologies, table data become outdated quickly, and route discovery must repeatedly be performed at a substantial cost in terms of power, time, and bandwidth [20].

The Mobile sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Mobile Sensor Networks support some specific applications such as sensors that can be attached to unknown vehicles for surveillance, Sensors to study air quality and environmental monitoring, sensors to track the movements of animals and their migration patterns, feeding habits, emergency search and rescue operations. Sensors can also be used in military battlefields among troopers to coordinate defence or attack, and Medical health care etc.

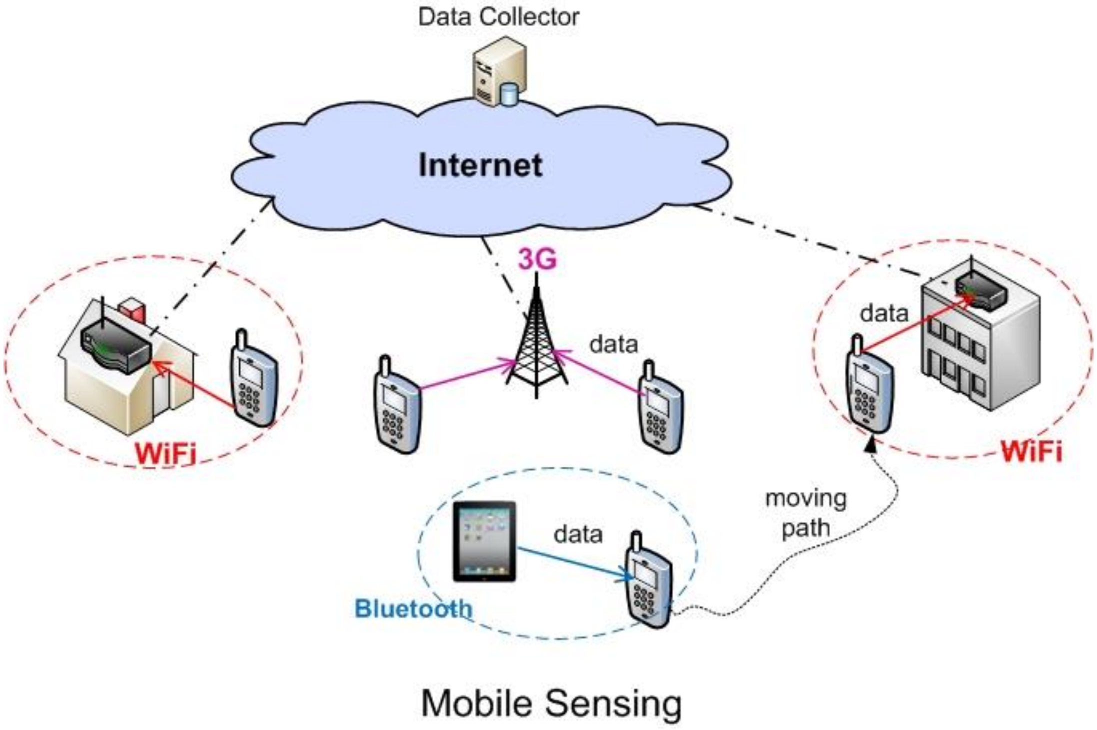


Fig.1.7: Mobile Wireless Sensor Network

Mobile devices communicate in real world through signals which are attached to base stations or connected to Wi-Fi with internet. All this works under Mobile wireless sensor network which is shown in the figure 1.7. In a static sensor network, the network may be disconnected, due to node failure. Mobile sensors can be used to re-establish the connectivity of the network. If the sinks or destinations of the network are stationary, owing to the traffic load, the sensors close to the sinks can die earlier. Introducing mobility to the sinks can solve this problem. Though sensor networks have been used successfully in different applications of our daily life, there are some critical issues that can’t be solved using static sensor networks, for example, deploying the sensors deterministically in environmental monitoring or in a battlefield. To overcome these issues, mobility is included in the sensor networks.

1.8. Three-tier Architecture for Mobile Sensor Networks

Mobile wireless sensor networks have three tier categories [21]. The figure 1.8 shows three tier architecture of a mobile sensor network and it is discussed below.

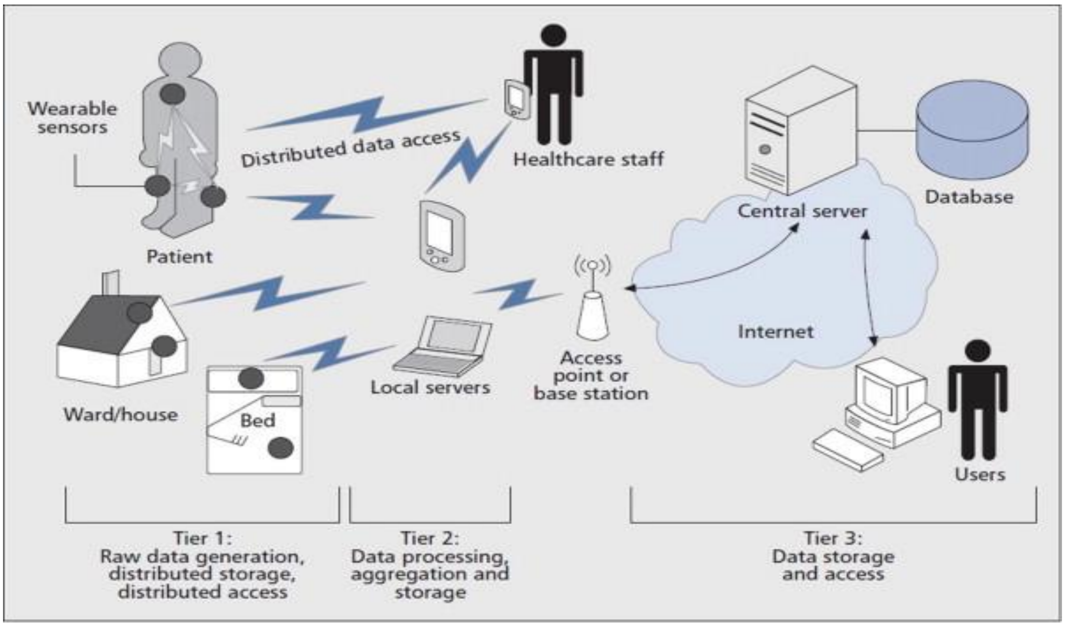


Figure 1.8: Three-Tiered Sensor Network Architecture

- **Planar or Tier 1:** A planar network consists of a set of heterogeneous devices that can communicate over the same network in an ad hoc manner. These devices can be mobile or stationary, but all devices communicate over the same network. Basic navigation systems such as [22] have a flat architecture.
- **Tier 2:** A typical second-tier network consists of static and mobile nodes. Mobile nodes make an overlay network that helps to move data within the network. The nodes of this overlay network can have more processing power, longer communication range and higher bandwidth. These nodes can be used to maintain the connectivity of the network.
- **Tier 3:** This type of network is used in different applications simultaneously. In a third-tier network three types of nodes are available,

static nodes, mobile nodes and access points. The mobile nodes gather data from the static nodes and pass the data to the access points.

1.9. Contrast Between WSNs and MSNs

Introducing mobility with the nodes of the network can change different parts of the networks. The perspectives that can be changed because of inclusion of versatility are [23].

In the static sensor networks, sensors don't move once they send data. It is impossible to get the area data of the sensors. As for as MWSN is concerned, the sensors move inside the network extra time, energy, and obtain the locations of the sensors.

The sensors in an MWSN can move effectively based on network topology. The routing tables execute their function with the help of network topology and it will updated with time. Most of the typical routing algorithms of WSN cannot adopt the dynamic change of the routing tables, therefore different routing techniques of mobile ad hoc networks (MANET) can be adopted in these cases.

Power utilization in an MWSN is much higher than a WSN because portability needs a great deal of energy. Normally, a much bigger energy supply or self-charging ability is utilized as a part of an MWSN. The sinks are static in an average WSN, where as an MWSN sink nodes can be portable and they can visit the sensors to accumulate the information. So information gathering procedures can be very distinctive in an MWSN.

Besides the hardware complexity, there is significant algorithmic complexity involved in deploying mobile sensors. The design of algorithms for the optimal movement plan for the nodes in an MWSN is quite challenging. The configuration of calculations for the ideal development arrangement for the nodes in a MWSN is very testing.

1.10. Challenges in Mobile WSNs

Mobile WSNs are possibly one of the fastest growing areas in the wireless ad hoc networking field. In spite of their innumerable applications, WSN has a few limits. These are limited data transfer capacity, limited energy supply, and limited computing power. Some of these major challenges experienced by wireless mobile sensor networks are listed out below.

I. Dynamic Network Topology
II. Power Consumption
III. Localization
IV. Scheduling
V. Security

I. Dynamic Network Topology

Since nodes for the most part are moving in MWSNs, the topology is dynamic. New routing and new protocols are needed in Mobile WSNs. Traditional WSN routing protocols, achieve their destination by depending on routing tables or recent route histories. In dynamic topologies, table data became outdated quickly, and route discovery must repeatedly be performed at a generous expense as far as power, time, and bandwidth are concerned. Fortunately, there is a dynamic wing of research dedicated to routing in a MSNs.

II. Power Consumption

Power consumption models differ vastly from WSNs to MWSNs. For both types of networks, wireless communication causes a significant energy cost and must be used efficiently. In any case, mobile entities require additional power for mobility, and are often equipped with a much larger energy reserve, or have a self-charging capability that enables them to plug into the power grid to recharge their batteries. The Mobile WSNs are expected to operate in insensitive environment with minimum or no human supervision and maintenance. It is clearly understood that the energy level begins to diminish on increased number of communications. Thus, it's a primary need to utilize the resource effectively.

III. Localization

Sensor node localization [25] is another major challenge of Mobile WSNs. In many situations, it is useful for a node in a WSN to know about its area in the present situation. The information about the location is important, so as to track the node which transmits the data. In statically deployed networks, node position can be determined once during initialization. However, those nodes that are mobile must continuously obtain their position as they traverse the sensing region [26]. This requires additional time and energy, as well as the accessibility to a rapid localization service.

A low-power, conservative, and sensibly precise system is required for area revelation. Basically for location discovery proximity-based approaches, exploiting geometric properties of a given scenario, and trying to analyse distinguishing proprieties of the position of a sensor node in similarity with premeasured properties are used. Whereas in the proximity-based approaches to measure the location of a sensor node using the sensor node's neighbourhoods information.

IV. Scheduling

Scheduling is more important, as it can spare the energy and builds the lifetime of the sensor node. It is important to schedule which node should be in a dynamic and which one in inert state. The essential consideration of energy efficient sleep/wake scheduling is in WSN. Finding an optimal sleep/wake scheduling strategy that would minimize computation and communication overhead, and be resilient to node failures, and provide high-quality data service is extremely challenging.

V. Security

Attributable to the wireless nature of the network is that the nodes are prone to several security breaches such as eavesdropping, impersonation, data tamper, data replication and modification. The absence of focal coordination makes them more vulnerable to attacks. Wireless nodes can easily be compromised by the adversary and thus a strong security policy needs to be enforced. Common security threats that can happen to the sensor nodes are host impersonation, information disclosure, energy depletion, buffer overflow and interference are presented [27].

In the host impersonation type of attack a compromised node can act as another node and react with appropriate control packets to create wrong route entries. Where as in the information disclosure type of attack a compromised node act as spy by intentional disclosure of confidential information to unauthorized nodes. In energy depletion type of attack, basically intended at depleting the battery power by directing needless traffic through them, the nodes become dead. In the buffer overflow attack the routing table removes the unnecessary routing entries. Interference is the common attack in military applications to jam the wireless communication by a creating noise.

1.11. Energy Management Schemes in MWSNs

Energy management schemes are characterized as the procedure of dealing with the sources and consumption of energy in a node or in the network is important for improving the lifetime of the network. The lifetime relies on the current application. The precise definition of lifetime is the time until the first node fails (runs out of energy) or the time when for the first time a point in the observed region is no longer covered by at least a single sensor node. A portion of the energy management function to find routes that result in the minimum total energy consumption in the network, utilizing dispersed planning to enhance battery life and taking care of the processor and interface devices to minimize power consumption. Energy management schemes can be comprehensively characterized into the following categories:

I. Transmission Power Management Schemes
II. Battery Energy Management Schemes
III. Processor Power Management Schemes
IV. Device Power Management Schemes

The figure 1.9 shows the classification of four categories of energy management schemes.

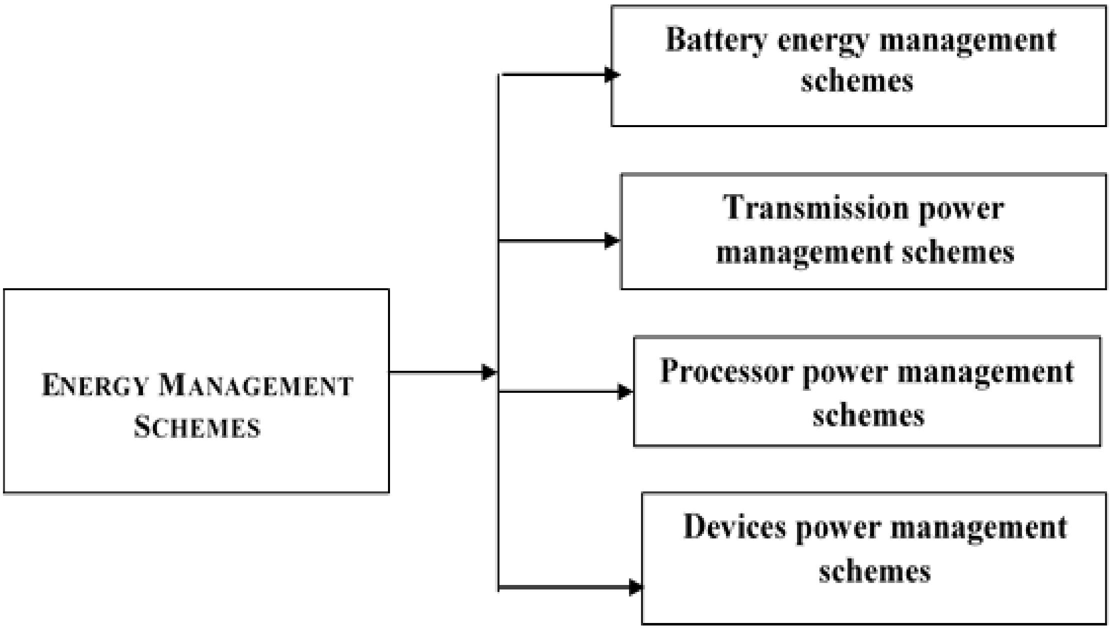


Fig.1.9: Classification of Energy Management Schemes

I. Transmission Power Management Schemes

In the transmission power management [28], the components used in the communication part, consumes a major portion of the energy in WSNs. The variety in transmission control fundamentally impacts the reachability of a node. The power consumed by the radio frequency (RF) module of a node is determined by the state of the operation, the transmission power and the innovation technique utilized for the hardware. Some of the solutions anticipated to calculate the optimum transmissions range are dynamic power adjustment policies, distributed topology control algorithms, constructing distributed power control loop and concentrated topology control calculations.

II. Battery Energy Management Schemes

The battery energy management is aimed at extending the battery life of a node by taking advantage of its synthetic properties and discharge patterns [29]. The past three decades the making of batteries has been undergoing unbelievable changes. They are of nickel-cadmium, lithium polymer, and lithium-ion. The principle factors considered while outlining a battery are the natural effect, cost, supply voltage, and charge/release qualities.

III. Processor Power Management Schemes

The processor power management scheme deals with the technique that try to diminish the power consumed by the processor. The power consumption was diminished by decreasing the number of calculations performed by the processor. The processor power spending minimizes by reducing the clock speed and the number of directions executed per unit time. The processor power consumption should also be reduced by putting the CPU into different power saving modes during low processing load conditions.

IV. Device Power Management Schemes

The device power management scheme can diminish power consumption of a node significantly [30]. This can be accomplished by specifically placing devices into various power-saving modes depending on their utilization. The low-power consumption design of hardware marks a considerable improvement in the energy preservation. To address these issues advanced power management features built into the operating system (OS) and application software's for managing devices efficiently are required.

Energy management is defined as the process of managing the sources and consumption of energy in sensor node or in the network. The energy of sensor network as a whole for enhancing the communication of the network. The form of batteries are to provide energy to a sensor node. The research work has three types of sensor nodes: an actor node to move freely in communication network, a static node and a dynamic sensor node. For the re-establishment of link failure, route recovery process is used, based on energy level of a node in wireless mobile sensor network. In this work applying sensor actions and energy level of nodes is computed by considering energy of a sensor node and packet delivery ratio. Network efficiency is usually measured by life time, packet delivery ratio and energy consumption. Energy consumption is measured in joules. Energy consumption varies with number of packets transmitted.

1.12. Advantages and Disadvantages of MWSNs

MWSNs gained their popularity because of the usage of low-cost and communicable intelligent sensors. These features make it possible and applicable to track objects, detect intrusion and to monitor the environment.

- **Advantages of MWSNs**

The important advantages of MWSNs networks are listed below. They are:

- The deployment cost of MWSNs is very low
- No physical infrastructure is needed
- Easily extended the range
- Avoids a lot of wiring
- Can accommodate new devices at any time

- Flexible to go through physical partitions
- It can be accessed through a centralized monitor

- **Disadvantages of MWSNs**

Some of the major drawbacks of wireless sensor networks are:

- The speed of WSN is slow when compared to wired networks
- It is comparatively insecure and can be easily hacked
- Lack of central coordination.

1.13. Quality of Service in MWSNs

A few distinctive characteristics of MWSNs, are large-scale random deployment, limited resources, and novel data-centric communication protocols. It is not easy to define the exclusive quality of service (QoS) [31] parameters for an assortment sort of MSNs. A number of real-time applications and mission critical systems are needed to assure performance guarantee from the system on which they are implemented. With their emergence in WSNs, the issue of QoS appeared. The intention of a WSN is to watch and report events occurring in a particular area.

Some regular QoS parameters in WSNs are event detection, reporting probability, event detection delay, missing reports, approximation accuracy and tracking accuracy. Based on these parameters, an essential QoS parameters in MWSNs are scope and presentation scope is a gauge of how well the sensor system watches or conceal an event. This relies on upon the extent and affectability of the detecting hubs, area, and thickness of the Sensor Nodes in the predefined zone. The scope issue is useful for including additional Sensor Nodes when the scope is poor.

1.14. Motivation of Research work

Motivated by all the current and previous research works, this research work concentrates on making progress or development that pave the way for rectification of link breakages of wireless sensor networks. Mobile Sensor Network is composed of several sensor nodes that have limited memory and power. The main task of the sensor nodes is to collect data, process the data and communicate with other sensors. The power source of a sensor node is its battery with limited power. Power is very important to the sensor nodes to complete the given task effectively. If the node energy is drained in the middle of the process, then the entire work of the sensor will be in vain. Thus, the power backup is very important for the sensor nodes.

In ad hoc networks, link failure problem is rectified by basing on mobility movement. In wireless mobile sensor network, when connection between a node and another node fails, the re-establishment process will be done basing on a calculating energy level of a sensor node. The sensor networks focuses on fast development recovery and improvement of lifetime of network. When there is link failure problem, the divert failure route recovery process is used by concentrating on round trip path detection algorithm which is there in mobile sensor networks. The proposed work approaches development of network route recovery process of link failure problem, by re-establishing the link based on check point route recovery algorithm. The experimental results are compared with the existing work and proposed research work in mobile sensor network is shown as better than mobile ad hoc network.

1.15. Organization of the Thesis

The objective of the research work is to improve the route recovery process of mobile sensor network and balance the energy consumption of sensor nodes, which leads to improvement of link failure prediction on mobile wireless sensor networks (MWSNs). The actor nodes which moves freely any particular area in MWSNs have also been investigated. The thesis is organized into six chapters in the following way.

- The First chapter deals with the **Introduction** about MANETs, Wireless sensor networks, and Mobile Sensor Networks.
- The Second chapter discusses **Literature Review of Routing Schemes on Mobile Wireless Sensor Network.** This chapter presents the researches and survey that have been carried out by several researchers recently.
- The Third chapter presents the **Route Recovery Process in DFRR and PRO-AODV mechanisms.**
- In the Fourth chapter, design of the architecture and implementation have been proposed in the **Check Point Route Recovery Algorithm (CPRRA)** over link failure problem.
- The Fifth chapter contains **Comparison of Performance Evaluation** on three mechanisms, the implementation results, graphs of each mechanism and the performance comparison of CPRRA with other mechanism results.
- In the last chapter, the topic is **conclusion and future scope** of studies is presented.

1.16. Summary

The complete chapter is about the introduction of mobile ad-hoc network (MANET), Characteristics, and routing protocols of MANET. Wireless sensor network (WSN) is studied with respect to the basic architecture of sensor node, and application of WSNs. A study on Mobile Wireless Sensor Network (MWSNs), three tier architecture of MSN, Contrast between WSN and MWSN, and Challenges in Mobile WSNs is made. The performance of energy management of mobile wireless sensor networks, advantages and disadvantages of mobile sensor networks and Quality of Service in MSNs are explained. At the end of the chapter the motivation for research work and organization of the thesis, conclusion and future scope presented.

2.1. Introduction

Routing is the process of selecting best paths in a network along which to forward traffic through networks. Routing support for mobile nodes is presently being formulated as mobile technology. In wireless sensor network routing can be deployed to support a wide variety of applications in many different situations composed of mobile sensor nodes. WSN does not require a physical infrastructure, deployment cost is very low and its many applications deploy WSN for monitoring or tracking purposes. Achieving this task efficiently requires the development of an energy-efficient routing protocol to set up routes between sensor nodes to the destination node. The route selection must be such that the lifetime of the network is maximized. The characteristics of the environment within which sensor nodes typically operate, coupled with severe resource and energy limitation, make the routing problem very challenging.

The unique characteristic [32] brings to sharp focus new routing design requirements that go beyond those typically encountered in wired and wireless ad hoc networks. Meeting these design requirements presents a distinctive and set of challenges. The challenges can be attributed to multiple factors, including severe energy constraints, limited computing and communication capabilities, the dynamic topology within which sensors are deployed, and data traffic models. Each and every challenge mentioned above is a separate area of research. The major challenge of WSN is its restricted battery backup. Energy conservation of sensors is the most researchable topic because the sensors become inactive, as soon as the energy of the sensor is drained.

The objective of this chapter is to discuss issues central to routing in WSNs and describe different approaches used to develop routing protocols for these networks. The first part discuss routing schemes of sensor node applications. The goal is to highlight the unique and distinctive features of the nature of the traffic typically generated in WSNs. In the second part of the chapter is provide a brief taxonomy of the basic routing strategies used to strike a balance between responsiveness and energy efficiency. Achieving this balance brings about new challenges that span the network in a manner that differs from ad hoc network as well as wireless sensor networks. In the third part of the chapter review a number of protocols that address the problem of routing in today's WSNs. Although the field is in its infancy and routing in WSNs remains largely relegated to research, multiple strategies have emerged as workable solutions to the routing problem. As the application of WSNs to different fields becomes more apparent, advances in network hardware and battery technology will pave the way to practical cost-effective implementations of these routing protocols.

2.2. Routing Schemes

The Routing schemes can be classification of several delivery semantics. The delivery semantics are unicast, delivers a message to a single specific node, any cast delivers a message to anyone out of a group of nodes, typically the one nearest to the source, multicast delivers a message to a group of nodes that have expressed interest in receiving the message, geocast delivers a message to a geographic area, and broadcast delivers a message to all nodes in the network. Routing scheme can be categorized into two types of topology distribution as Static Routing and Dynamic Routing.

2.2.1. Static Routing

Static routing [33] is a form of routing that occurs when a router set up manually configure, do not change and administration requires. Static routing allows routing tables in specific routers to be set up in a static manner so network routes for packets are set. If a router on the route goes down, the destination may become unreachable. Routers forward packets using from route table entries that are manually configured and routing tables that are built and maintained automatically through an ongoing communication between routers.

2.2.2. Dynamic Routing

Dynamic routing [34] performs the same function as static routing except it is more robust. Dynamic routing allows routing tables in routers to change as the possible routes change. Dynamic routing is network technique that provides optimal data routing and calculates routes based on received updated network state information. The routing protocol, which consists of the semantics used to transport topology information across a network or internetwork and the algorithms used to determine the shortest path to any given destination within the network. The devices actually running the protocols and switch packets along the paths the routing protocols have chosen as the best paths to each reachable destination within the network. The topology information carried within the routing protocol, representing the topology of the network and the reachable destinations within the network. To protect routing within a network, it is necessary to protect each piece of the routing system, rather than focusing on the routing protocol and its semantics and algorithms. In the case of wireless sensor networks, dynamic routing is employed because nodes may frequently change their position and die at any moment.

2.3. Routing challenges and design issues in WSNs

Wireless Sensor Networks share many characteristics [32] with wired and ad hoc networks, they additionally show various one of a unique characteristic which set them apart from existing networks. Wireless sensor networks have several restrictions, for example, limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. In the following, summarize some of the routing challenges and design issues that affect routing process in WSNs.

2.3.1. Network Scale and Time-Varying Characteristics

Sensor nodes operate with restricted computing, storage, and communication capabilities under serious energy constraints, to the large number of conceivable sensor-based applications, the densities of the WSNs may vary widely, ranging from very sparse to very dense. Furthermore, in many applications, the sensor nodes, in some cases numbering in the hundreds if not thousands, are deployed in an ad hoc and often unsupervised way over wide coverage areas.

In these networks, the behaviour of sensor nodes is dynamic and highly adaptive, as the need to self-organize and conserve energy power sensor nodes to change their behaviour constantly in response to their current level of activity or the scarcity in the networks. Moreover, sensor nodes may be required to modify their behaviour in response to the inconsistent and unpredictable behaviour of wireless connections caused by high noise levels and radio-frequency interference, to prevent extreme execution performance degradation of the application supported.

2.3.2. Resource Constraints

Sensor nodes are designed with minimal complexity for large-scale arrangement at a diminished expense. Energy is a key concern in WSNs, which must accomplish a long lifetime while working on restricted battery reserves. Multi-hop packet transmission over wireless networks is a major source of power consumption. Decreasing energy consumption can be achieved by dynamically controlling the duty cycle of the wireless sensors. The energy management problem, however, becomes especially challenging in many mission-critical sensor applications. The requirements of these applications are such that a predetermined level of sensing and communication performance constraints must be maintained after at the same time. Therefore, a question arises as to how to design scalable routing algorithms that can operate efficiently for a wide range of performance resource constraints and design requirements. The development of these protocols is fundamental to the future of WSNs.

2.3.3. Sensor Applications Data Models

The data model describes the flow of information between the sensor nodes and the data sink. These models are highly dependent on the nature of the application in terms of how data are requested and used. Several data models have been proposed to address the data-gathering needs and interaction requirements of a variety of sensor applications [35, 36]. A class of sensor applications requires data collection models that are based on periodic sampling or are driven by the occurrence of specific events. In other applications, data can be captured and stored, possibly processed and aggregated by a sensor node, before they are forwarded to the data sink. Yet a third class of sensor applications requires bidirectional data models in which two-way interaction between sensors and data sinks is required [37].

The need to support a variety of data models increases the complexity of the routing design problem. Optimizing the routing protocol for an application's specific data requirements while supporting a variety of data models and delivering the highest performance in scalability, reliability, responsiveness, and power efficiency becomes a design and engineering problem of enormous magnitude.

2.4. Routing strategies in wireless sensor networks

The WSN routing problem presents a very difficult challenge that can be posed as a classic trade-off between responsiveness and efficiency. This trade-off must balance the need to accommodate the limited processing and communication capabilities of sensor nodes against the overhead required to adapt to these. In a WSN, overhead is measured primarily in terms of bandwidth utilization, power consumption, and the processing requirements on the mobile nodes. Finding a strategy to balance these competing needs efficiently forms the basis of the routing challenge. Furthermore, the intrinsic characteristics of wireless networks gives rise to the important question of whether or not existing routing protocols designed for ad hoc networks are sufficient to meet this challenge [38]. Routing algorithms for ad hoc networks can be classified according to the manner in which information is acquired and maintained and the manner in which this information is used to compute paths based on the acquired information. Three different strategies can be identified: proactive, reactive, and hybrid [39].

The proactive strategy, also referred to as table driven, relies on periodic dissemination of routing information to maintain consistent and accurate routing tables across all nodes of the network. The structure of the network can be either flat or hierarchical. Flat proactive routing strategies have the potential to compute optimal paths. The overhead required to compute these paths may be prohibitive in a dynamically changing environment. Hierarchical routing is better suited to meet the routing demands of large ad hoc networks.

Reactive routing strategies establish routes to a limited set of destinations on demand. These strategies do not typically maintain global information across all nodes of the network. They must therefore, rely on a dynamic route search to establish paths between a source and a destination. This typically involves flooding a route discovery query, with the replies traveling back along the reverse path. The reactive routing strategies vary in the way they control the flooding process to reduce communication overhead and the way in which routes are computed and re-established when failure occurs.

Hybrid strategies rely on the existence of network structure to achieve stability and scalability in large networks. In these strategies the network is organized into mutually adjacent clusters, which are maintained dynamically as nodes join and leave their assigned clusters. Clustering provides a structure that can be leveraged to limit the scope of the routing algorithm reaction to changes in the network environment. A hybrid routing strategy can be adopted whereby proactive routing is used within a cluster and reactive routing is used across clusters. The main challenge is to reduce the overhead required to maintain the clusters.

The traditional routing algorithms for ad hoc networks tend to exhibit their least desirable behaviour under highly dynamic conditions. Routing protocol overhead typically increases dramatically with increased network size and dynamics. A large overhead can easily overwhelm network resources. Furthermore, traditional routing protocols operating in large networks require substantial intermodal coordination, and in some cases global flooding, to maintain consistent and accurate information, which is necessary to achieve loop-free routing. The use of these techniques increases routing protocol overhead and convergence times. Consequently, although they are well adapted to operate in environments where the computation and communications capabilities of the network nodes are relatively high compared to sensor nodes, the efficiency of these techniques conflict with routing requirements in WSNs. New routing strategies are therefore required for sensor networks that are capable of effectively managing the trade-off between optimality and efficiency.

2.4.1. Routing Protocols for WSNs

The design of routing protocols for WSNs must consider the power and resource constraints of the network nodes, the time-varying nature of the wireless channel, and the possibility for packet loss and delay. To address these design requirements, several routing strategies for WSNs have been proposed. The routing protocol have one class to adopt a flat network architecture in which all nodes are considered peers. A flat level network architecture has few advantages, including insignificant overhead to maintain the infrastructure and the potential for the discovery of multiple routes between communicating nodes for fault tolerance.

A second class of routing protocols conventions forces a structure on the network to accomplish energy efficiency, stability, and scalability. In this class of protocols, network nodes are organized in clusters in which a node with higher residual energy, for example, assumes the role of a cluster head. The cluster head is responsible for coordinating activities within the cluster and forwarding information between clusters. Clustering has potential to reduce energy consumption and extend the lifetime of the network.

A third class of routing protocols uses a data-centric approach to disseminate interest within the network. The approach uses attribute-based naming, whereby a source node queries an attribute for the phenomenon rather than an individual sensor node. The interest dissemination is achieved by assigning tasks to sensor nodes and expressing queries to relative to specific attributes. Different strategies can be used to communicate interests to the sensor nodes, including broadcasting, attribute-based multicasting, geo-casting, and any casting.

A fourth class of routing protocols uses location to address a sensor node. Location-based routing is useful in applications where the position of the node within the geographical coverage of the network is relevant to the query issued by the source node. Such a query may specify a specific area where a phenomenon of interest may occur or the vicinity to a specific point in the network environment. In the following sections, several routing algorithms that have been proposed for data dissemination in WSNs are described.

2.4.2. Flooding and Its Variants

Flooding is a common technique frequently used for path discovery and information dissemination in wired and wireless ad hoc networks. The routing strategy is simple and does not rely on costly network topology maintenance and complex route discovery algorithms. Flooding uses a reactive approach whereby each node receiving a data or control packet sends the packet to all its neighbors. After transmission, a packet follows all possible paths. Unless the network is disconnected, the packet will eventually reach its destination. Furthermore, as the network topology changes, the packet transmitted follows the new routes. The concept of flooding in data communications network. As shown in the figure, flooding in its simplest form may cause packets to be replicated indefinitely by network nodes. To prevent a packet from circulating indefinitely in the network, a hop count field is usually included in the packet. Initially, the hop count is set to approximately the diameter of the network. A similar effect can be achieved using a time-to-live field, which records the number of time units that a packet is allowed to live within the network. At the expiration of this time, the packet is no longer forwarded. Flooding can be further enhanced by identifying data packets uniquely, forcing each network node to drop all the packets that it has already forwarded. Such a strategy requires maintaining at least a recent history of the traffic, to keep track of which data packets have already been forwarded.

Despite the simplicity of its forwarding rule and the relatively low-cost maintenance that it requires, flooding suffers several deficiencies when used in WSNs. The first drawback of flooding is its susceptibility to traffic implosion, this undesirable effect is caused by duplicate control or data packets being sent repeatedly to the same node. The second drawback of flooding is the overlap problem to which it gives rise, overlapping occurs when two nodes covering the same region send packets containing similar information to the same node. The third and most severe drawback of flooding is resource blindness. The simple forwarding rule that flooding uses to route packets does not take into consideration the energy constraints of the sensor nodes.

2.4.3 Low-Energy Adaptive Clustering Hierarchy

Low-energy adaptive clustering hierarchy (LEACH) is a routing algorithm designed to collect and deliver data to the data sink, typically a base station [41]. The main objectives of LEACH are:

- Extension of the network lifetime
- Reduced energy consumption by each network sensor node
- Use of data aggregation to reduce the number of communication messages

To achieve these objectives, LEACH adopts a hierarchical approach to organize the network into a set of clusters. Each cluster is managed by a selected cluster head. The cluster head assumes the responsibility to carry out multiple tasks. The first task consists of periodic collection of data from the members of the cluster. Upon gathering the data, the cluster head aggregates it in an effort to remove redundancy among correlated values. The second main task of a cluster head is to transmit the aggregated data directly to the base station. The transmission of the aggregated data is achieved over a single hop. The third main task of the cluster head is to create a TDMA-based schedule whereby each node of the cluster is assigned a time slot that it can use for transmission. The cluster head advertises the schedule to its cluster members through broadcasting. To reduce the likelihood of collisions among sensors within and outside the cluster, LEACH nodes use a code-division multiple access–based scheme for communication.

The basic operations of LEACH [41] are organized in two distinct phases. The first phase, the setup phase, consists of two steps, cluster-head selection and cluster formation. The second phase, the steady-state phase, focuses on data collection, aggregation, and delivery to the base station. The duration of the setup is assumed to be relatively shorter than the steady-state phase to minimize the protocol overhead. LEACH exhibits several properties which enable the protocol to reduce energy consumption. Energy requirement in LEACH is distributed across all sensor nodes, as they assume the cluster head role in a round-robin fashion based on their residual energy. LEACH is a completely distributed algorithm, requiring no control information from the base station. The cluster management is achieved locally, which obliterates the need for global network knowledge. Furthermore, data aggregation by the cluster also contributes greatly to energy saving, as nodes are no longer required to send their information directly to the sink. It has been shown using simulation that LEACH outperforms conventional routing protocols, including direct transmission and multi-hop routing, minimum-transmission-energy routing, and static clustering–based routing algorithms.

2.4.4. Power-Efficient Gathering in Sensor Information Systems

Power-efficient gathering in sensor information systems (PEGASIS) and its extension, hierarchical PEGASIS [42], are a family of routing and information-gathering protocols for WSNs. The main objectives of PEGASIS are twofold. First, the protocol aims at extending the lifetime of a network by achieving a high level of energy efficiency and uniform energy consumption across all network nodes. Second, the protocol strives to reduce the delay that data incur on their way to the sink.

The network model considered by PEGASIS [42] assumes a homogeneous set of nodes deployed across a geographical area. Nodes are assumed to have global knowledge about other sensors' positions. Furthermore, they have the ability to control their power to cover arbitrary ranges. The nodes may also be equipped with CDMA-capable radio transceivers. The nodes' responsibility is to gather and deliver data to a sink, typically a wireless base station. The goal is to develop a routing structure and an aggregation scheme to reduce energy consumption and deliver the aggregated data to the base station with minimal delay while balancing energy consumption among the sensor nodes. Contrary to other protocols, which rely on a tree structure or a cluster-based hierarchical organization of the network for data gathering and dissemination, PEGASIS uses a chain structure.

Based on this structure, nodes communicate with their closest neighbors. The construction of the chain starts with the farthest node from the sink. Network nodes are added to the chain progressively, starting from the closest neighbour to the end node. Nodes that are currently outside the chain are added to the chain in a greedy fashion, the closest neighbour to the top node in the current chain first, until all nodes are included. To determine the closest neighbour, a node uses the signal strength to measure the distance to all its neighbour nodes. Using this information, the node adjusts the signal strength so that only the closest node can be heard. A node within the chain is selected to be the chain leader. Its responsibility is to transmit the aggregated data to the base station. The chain leader role shifts in positioning the chain after each round. Rounds can be managed by the data sink, and the transition from one round to the next can be tripped by a high-powered beacon issued by the data sink. Rotation of the leadership role among nodes of the chain ensures on average a balanced consumption of energy among all the network nodes. It is worth noting, however, that nodes assuming the role of chain leadership may be arbitrarily far away from the data sink. Such a node may be required to transmit with high power in order to reach the base station.

2.4.5. Sensor Protocols for Information via Negotiation

Sensor protocols for information via negotiation (SPIN) is a data-centric negotiation- based family of information dissemination protocols for WSNs [43]. The main objective of these protocols is to efficiently disseminate observations gathered by individual sensor nodes to all the sensor nodes in the network. Simple protocols such as flooding and gossiping are commonly proposed to achieve information dissemination in WSNs. Flooding requires that each node sends a copy of the data packet to all its neighbors until the information reaches all nodes in the network. Gossiping, on the other hand, uses randomization to reduce the number of duplicate packets and requires only that a node receiving a data packet forward it to a randomly selected neighbour node. The simplicity of flooding and gossiping is appealing, as both protocols use simple forwarding rules and do not require topology maintenance. The performance of these algorithms in terms of packet delay and resource utilization, however, quickly deteriorates with the size of the network and the traffic load. This performance drawback is typically caused by traffic implosion and geographical overlapping. This protocols such as flooding and gossiping do not alter their behaviour to adapt communication and computation to the current state of their energy resource. This lack of resource awareness and adaptation may reduce the lifetime of the network considerably, as highly active nodes may rapidly deplete their energy resources.

The main objective of SPIN [43] and its related family members is to address the shortcomings of conventional information dissemination protocols and overcome their performance deficiencies. The basic tenets of this family of protocols are data negotiation and resource adaptation. Semantic-based data negotiation requires that nodes running SPIN the content of the data before any data are transmitted between network nodes. SPIN exploits data naming, whereby nodes associate metadata with data they produce and use these descriptive data to perform negotiations before transmitting the actual data. A receiver that expresses interest in the data content can send a request to obtain the data advertised. This form of negotiation assures that data are sent only to interested nodes, thereby eliminating traffic implosion and reducing significantly the transmission of redundant data throughout the network. Furthermore, the use of Meta data descriptors eliminates the possibility of overlap, as nodes can limit their requests to name only the data that they are interested in obtaining.

The SPIN [43] protocol family addresses the major drawbacks of flooding and gossiping. Simulation results show that SPIN is more energy efficient than flooding or gossiping. Furthermore, the results also show that the rate at which SPIN disseminates data is greater than or equal to the rate of either of these protocols. SPIN achieves these gains by localizing topology changes and eliminating dissemination of redundant information through semantic negotiation.

2.4.6. Directed Diffusion

Directed diffusion [44] is a data-centric routing protocol for information gathering and dissemination in WSNs. The main objective of the protocol is to achieve substantial energy savings in order to extend the lifetime of the network. To achieve this objective, directed diffusion keeps interactions between nodes, in terms of message exchanges, localized within a limited network vicinity. Using localized interaction, direct diffusion can still realize robust multipath delivery and adapt to a minimal subset of network paths. This unique feature of the protocol, combined with the ability of the nodes to aggregate response to queries, results into significant energy savings. The main elements of direct diffusion include interests, data messages, gradients, and reinforcements. Directed diffusion uses a publish-and-subscribe information model in which an inquirer expresses an interest using attribute–value pairs. An interest can be viewed as a query or an interrogation that specifies what the inquirer wants.

Directed diffusion has the potential for significant energy savings. Its localized interactions allow it to achieve relatively high performance over unoptimized paths [44]. Furthermore, the resulting diffusion mechanisms are stable under a range of network dynamics. Its data-centric approach obliterates the need for node addressing. The directed diffusion paradigm, however, is tightly coupled into a semantically driven query-on-demand data model. This may limit its use to applications that fit such a data model, where the interest-matching process can be achieved efficiently and unambiguously.

2.5. Failure classifications in Wireless Sensor Network

The exploration of different types of failures to get a better grasp in the world of failure era. Failure classification of wireless sensor network is categorized in figure 2.1 show in the following.

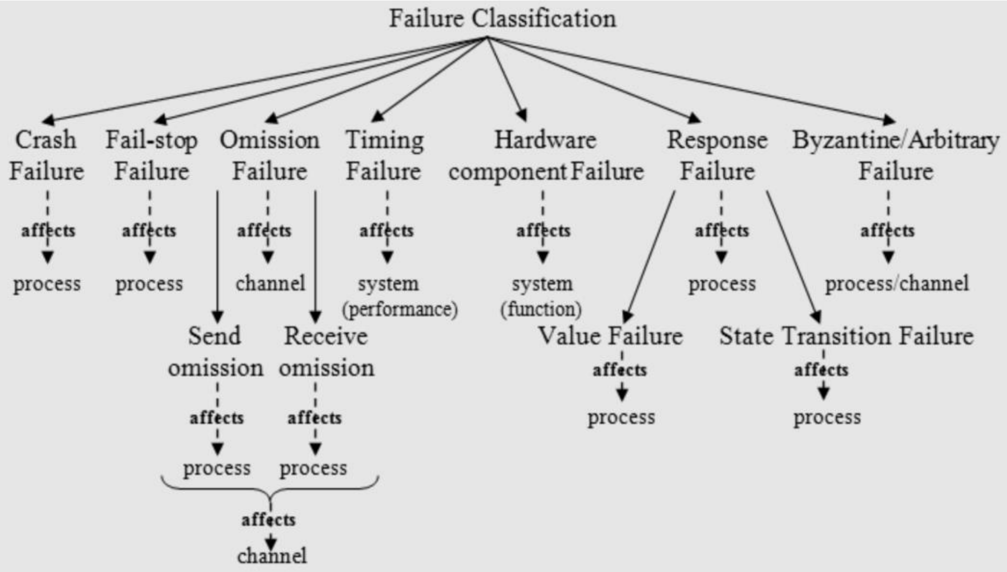


Figure 2.1 Classification of failure in wireless sensor network

The specific uninterrupted activity effects of fault leads to crash-stop failures [45]. Crash-stop failure affects the process or functional unit and makes it to remain at halting state, at which no further defective output are produced. Fail-stop failures are also referred as fail-silent failures. Fail-stop failure is similar to that of crash-failure but can be easily detected by other processes while the former cannot be. The major causes of omission failure are network transmission error or insufficiency of buffer space. Due to omission failure, system fails to respond to the incoming queries. Both receive and send omission confirms the failing stage, to respond to processed incoming messages as well as to processed outgoing massages respectively. The combined effect of receive and send omission are notified as channel omission. Most of the hardware failures are associated with generic hardware components of sensor nodes. Liable reflection of environmental disasters causes hardware failures. Another important class of failure is timing failure, related to periodic operational scheme of WSN system. Timing failure is one which directs the synchronous distributed WSN system or real-time WSN system to respond outside the specified time interval. Since there is no standard assurance are provided for response time in asynchronous WSN system, timing failures said to have null effects on those.

Failure [45] is majorly due to the outcome of incorrect response by the system. There is possibilities of two kinds of response failure may happen, namely value failure and state transition failure. Value failure causes the system to provide faulty reply to the requested queries. For example some group of sensor nodes respond with wrong sensory data to the sink node. State transition failure directs the system to deal with collapsed set of control flow, which ultimately triggers unintended default action at wrong time and produce irrelevant set of information as response. In any system dealing with byzantine failure are simply "messy" because byzantine/arbitrary failure makes the system to produce random values at arbitrary time. During processing, this type of failures tend to omit intended processing assessments but prefers unintended processing measures lead to message corruption and responding with multiple delivery in communication medium.

2.6. Energy Efficient Processes

Wireless sensor network of energy efficient process to retain the energy level of those nodes for a long period, and is made up of tiny energy hungry sensor nodes. Energy efficient processes are classified into five major classes [46] and the following classes is describe in figure 2.2.

- Data Reduction
- Protocol Control Reduction
- Routing Techniques in WSNs
- Duty Cycling
- Topology Control

2.6.1. Data Reduction

The main objective of data reduction is to minimize the production, processing and transmission of data, as much as possible. Data reduction techniques can be classified into two classes and they are following below.

i. Data Production
ii. Data Processing and Transmission

i. Data Production

The dynamic topology of WSNs has sown the seeds to several techniques, namely sampling and prediction based techniques. In the sampling-based techniques, the data sampled by the sensor nodes are minimized. This minimization leads to reduced energy consumption and least communication cost. In the Prediction based techniques, the sink node can predict the readings by examining the reading history of readings. This functionality allows the sensors to be in switched off state. These techniques work on the basis of a data model, in which the model provides a local response to the query rather than for data transmission. These techniques can be classified into two on the basis of centralized and clustering nature.

In the centralized framework, every sensor node transmits the sensed readings to the sink node. A model is generated with these readings and the upcoming readings can be predicted on a comparison. In the cluster-based model, the cluster head and the sink node manages a prediction model and the cluster head compares the sensed reading with the predicted model.

ii. Data Processing and Transmission

After the process of data acquisition, data is needed to be processed for certain reasons. While processing data, the energy consumption has to be managed with an eagle eye. For this sake, two major techniques are exploited and they are

a. Data Compression
b. Data Aggregation

a. Data Compression

Data compression is the process in which the data to be transmitted is compressed or reduced by bits. Data compression is one of the possible technique that can help to reduce the amount of data exchanged between sensor nodes ensuing in power saving. Any data compression scheme proposed for WSNs must be lightweight because sensor nodes are naturally powered by batteries with limited capacity. Data compression reduces the transmission overhead and also improves the speed of transmission. This results in minimum utilization of energy being spared. Several techniques exist to achieve data compression [47] and mostly employed compression techniques with respect to WSNs are

- Coding by Ordering
- Pipeline in Network Compression
- Distributed Compression

Coding by Ordering

In coding by ordering, one sensor node is dedicated exclusively for compression purpose. All the sensed data are collected and transmitted to the compression node. Certain node's sensed data are dropped but it can be manipulated by following the various coding order.

Pipeline in Network Compression

The collected data are kept in the temporary buffer of the compression for a certain period of time. During this interval, the compression node clubs all the data packets into a single packet, by eliminating duplicated packets.

Distributed Compression

Distributed compression possesses a compression node that needs lesser or no communication between sensors. The distributed sensing, where it is desirable to have high sensor density for reliability, accuracy, and low cost deployment.

b. Data Aggregation

Sensor nodes are pint-sized and thus, the memory component must be much smaller. The memory can be handled effectively only by eliminating duplication of data. Data aggregation techniques mainly focus on distributed data processing along with node coordination. Data aggregation is handled by several popular existing techniques [46] and they are

i. Cluster-based Structure
ii. Tree-based Structure
iii. Structure-less Protocol.

i. Cluster-based Structure

In cluster-based structure, the nodes are systematized into clusters and a cluster head is employed. A cluster head can directly communicate with the sink node. The main task of cluster head is to aggregate data. LEACH protocol follows this structure [40, 41]. The improved version of LEACH is PEGASIS, which systematizes all the nodes into a chain. PEGASIS is even enhanced and named as hierarchical-PEGASIS [42].

ii. Tree-based Structure

Tree-based structure is another variation, in which the sensor can estimate the distance of which the event has happened. The root node is chosen by taking the distance between the node and the event triggered area. This structure is based on several traditional algorithms such as Steiner Minimum Tree and Multiple Shared Tree [38, 48].

iii. Structure-less Protocol

In this technique, all the bottlenecks with regard to structured methodology are eliminated. The packets are transmitted to one-hop neighbors, by exploiting suitable casting. As this technique does not depend on structure, it is well-suited for dynamic topology.

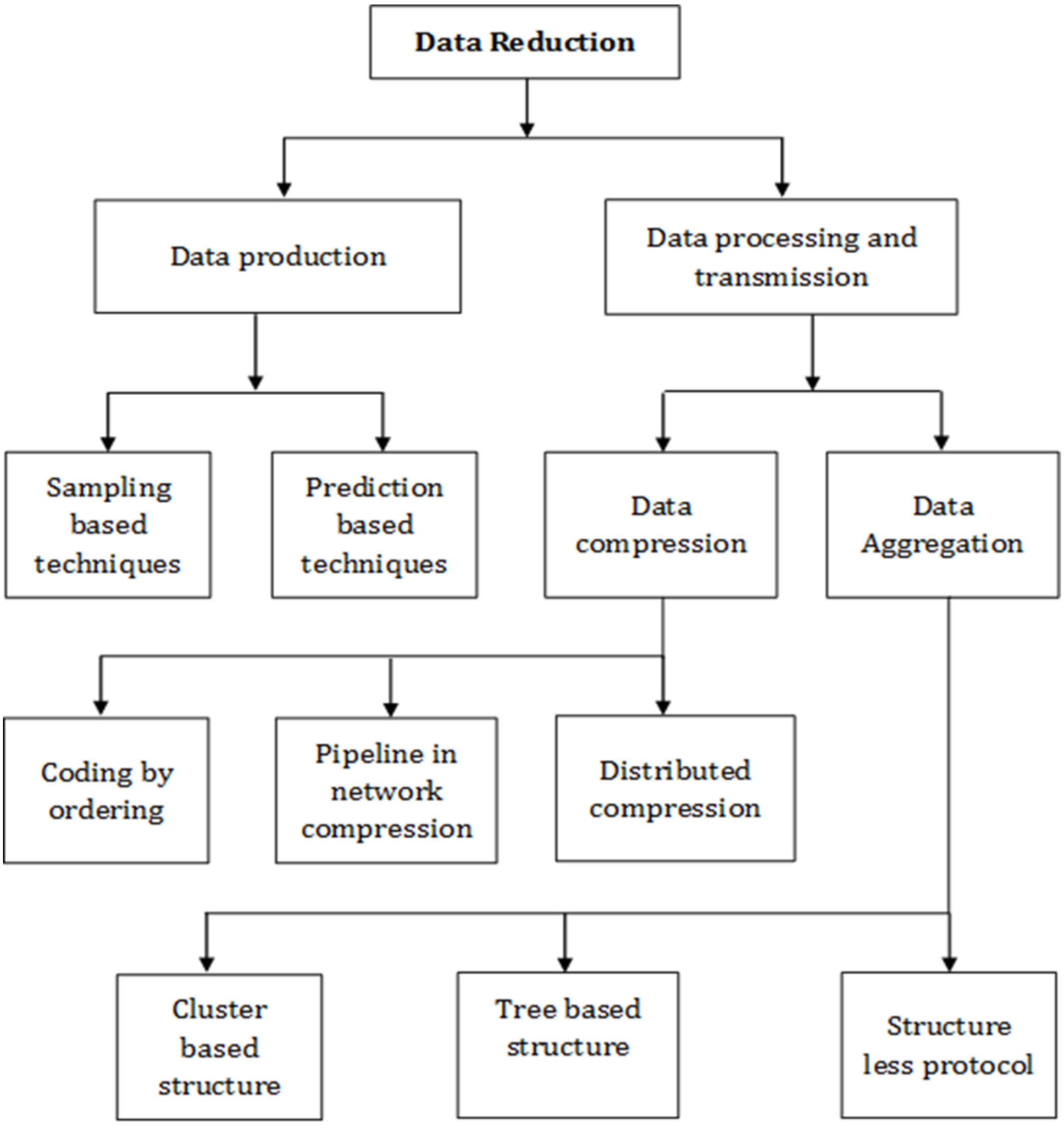


Figure 2.2 Data Reduction in WSN

2.6.2. Protocol Overhead Reduction

Another major reason for energy depletion is the protocol overhead. If this overhead is managed properly, energy can be preserved and in turn the lifetime of the network is improved. The protocol overhead can be classified [46] into the following figure 2.3.

I. Adaptive Transmission with Respect to its Mobility and Distance
II. Cross Layering for Network Resource Optimization
III. Optimal Flooding

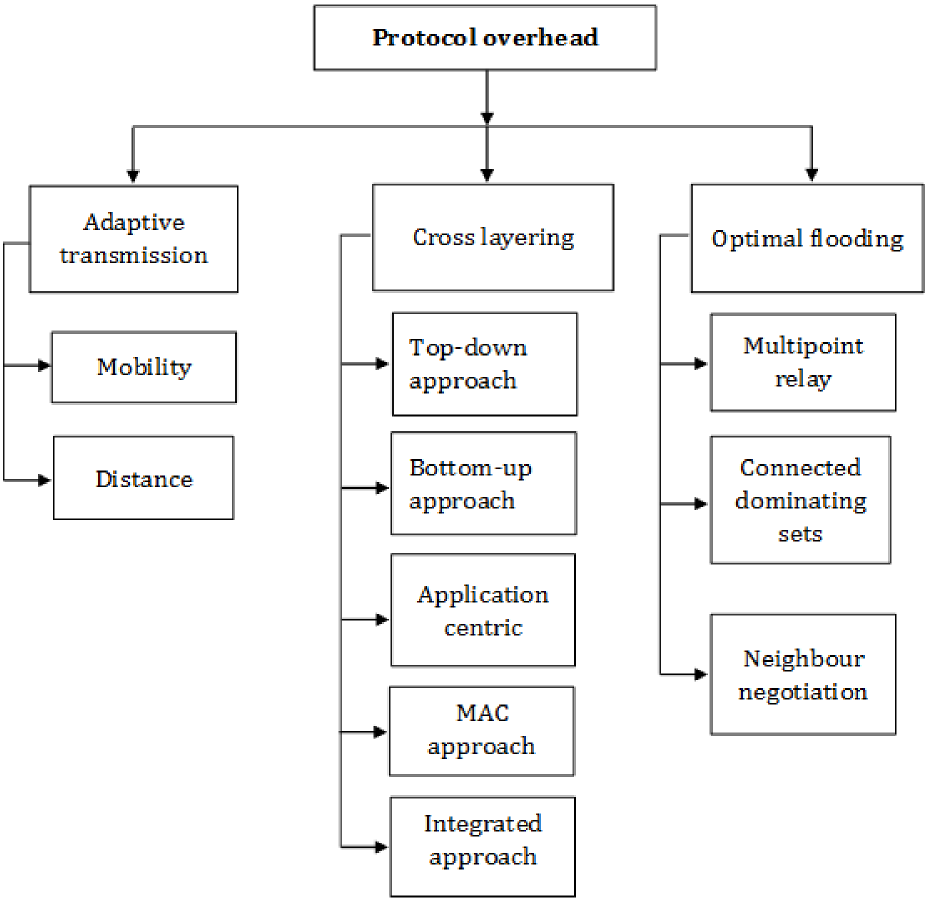


Figure 2.3 Protocol Overhead in WSN

I. Adaptive Transmission with Respect to its Mobility and Distance

Communication protocols interchange control messages for every time interval. The resulting overhead can be reduced by minimizing the frequency of control message interchange. This saves considerable energy. The choice of time interval must suit the dynamic topology of WSNs also. Mobility is used for dipping the energy spending. In a static WSN data packets coming from SNs follow a multi-hop path towards the BS. If some of the SNs are mobile, the traffic flow can be altered if mobile devices are accountable for data collection directly from static SNs. Static SNs wait for the passage of the mobile device and route messages towards it. Hence, the communications take place in directly with a limited multi-hop traversal. As the end result, static SNs can save energy.

Communication protocols transmit control packets more frequently for finding the neighbours and to determine effective routes for packet transmission. Owing to the dynamic topology or mobility of the WSNs, the existing connection may fail, this may results in the need for more control packets. The work proposed in [49] follows this principle by incorporating min and max time interval for finding its neighbours. The max time interval indicates the time interval of transmitting hello messages in a static network. The min time interval detects the dynamic topology by considering the lastly sent message.

This concept indicates the fact that the distance between two entities is directly proportional to the time it takes to forward the packet. This is based on the fish eye concept.

II. Cross Layering for Network Resource Optimization

Every WSN is expected to be energy efficient, scalable and reliable. These performance metrics can be justified by the cross layering approaches. The standard approaches are listed below [50].

i. Top-down Approach
ii. Bottom-up Approach
iii. Application-centric Approach
iv. MAC-centric Approach
v. Integrated Approach

i. *Top-down Approach*

The layers at the top formulate the parameters and action plans to the layers present at the bottom.

ii. *Bottom-up Approach*

The layers present at the bottom abstracts its bandwidth change and losses for the layers present at the top. However, this solution is not appropriate for multimedia applications.

iii. *Application-centric Approach*

This approach relies on the application and this approach can follow either top-down or bottom-up approach. The main goal of this approach is to optimize the parameters of lower layers.

iv. *MAC-centric Approach*

In MAC-centric approach, the MAC layer determines the necessary degree of Quality of Service (QoS). The needs of application layer are considered and the transmission flow is determined.

v. *Integrated Approach*

In integrated approach, several approaches can be clubbed together. The main issue of this approach is the complexity of strategy formulation.

III. Optimal Flooding

Flooding is commonly employed in WSNs for localization and route discovery processes. The main issue of flooding with regard to WSN is the power consumption. Flooding is a high-priced activity for the energy restricted WSN. In [52], certain techniques are listed to reduce the number of transmissions. They are:

a) Multipoint Relay

b) Connected Dominating Sets

c) Neighbour Negotiation

a) *Multipoint Relay*

Multipoint relay approach is used in optimized link state routing protocol (OLSR). Packet retransmission is done by a group of neighbours of the source node. This group of neighbours are called as multipoint relays. The multipoint relays are one hop neighbours of the source node that can connect to two hop neighbours.

b) *Connected Dominating Sets*

This approach is normally employed in Mobile Ad hoc Networks (MANET). Every node verifies whether it is a part of connected dominating set or not. In case, if the node is a part of the connected dominating set, then it retransmits the broadcast message.

c) *Neighbour Negotiation*

In the neighbour negotiation approach, the packets are forwarded to the concerned nodes alone. On the other hand, the above discussed approaches distribute the data to all the nodes of the network. In this approach, the metadata of the data is exchanged between the neighbours. In case, if a node is concerned to receive the data, then it requests for that data.

2.6.3. Routing Schemes in WSNs

Routing protocols must be paid enough attention for energy restricted nature of WSNs. Routing protocols detect the most feasible route from the source to destination. Routing protocol devise for WSNs is heavily influenced by many challenging factors, those are connectivity, scalability, communication range, computational capabilities, transmission media, control overhead and QoS. The major intention of the routing schemes is to minimize the energy utilization in order to extend the WSNs lifetime. The routing schemes divided into two type based protocols is shown in figure 2.4.

For considering these challenges routing protocols for WSNs are classified [50] into data-centric, hierarchical-based, geographical based and opportunistic based routing protocols depending on the network structure and multipath based, query based, negotiation based and location based routing protocols depends on their operation.

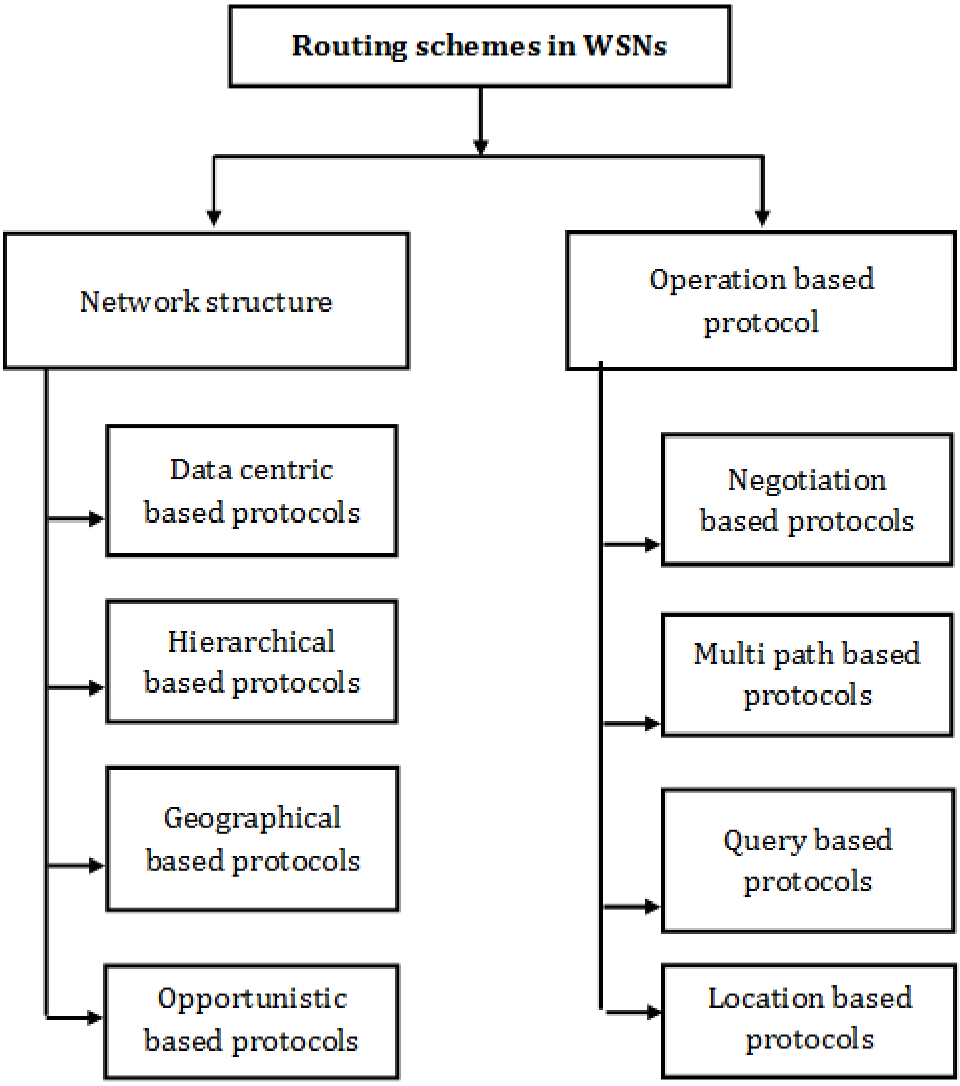


Figure 2.4 Routing Schemes in WSN

2.6.3.1. Based on Network Structure

In this section of routing protocols, the network structure is one of the determinant factors. These routing protocols further classified into

a. Data-centric Based Protocols
b. Hierarchical Based
c. Geographical Based
d. opportunistic

a. *Data-centric Based Protocols*

Data centric protocols preserve energy by interrogating sensors on the attributes of data. The packets are routed by considering the content of the packet. In these routing protocols, the sink sends queries to firm regions and waits for data from the sensors located in the chosen regions, because data is being requested through queries. This can be achieved by two different approaches and they are SPIN and Directed Diffusion. In SPIN (Sensor protocols for information via negotiation) [43], uses negotiation and resource adjustment to address the deficiencies of flooding. The basic idea of SPIN is to reduce redundant data by the negotiation in between the SNs to keep energy. A threshold based resource-aware procedure is used for extending the network lifetime. The SNs advertise the available data through ADV and wait for requests from interested SNs. The main advantage of the SPIN protocol was the topological changes are localized [51]. In view of the fact that, each SN needs to know only its single-hop neighbors.

The directed diffusion routing protocol [44], is helpful in scenarios where the SNs themselves produce request/queries for data sensed by other SNs, instead of all queries arising only from a BS. This improves on data diffusion using interest gradients. In this routing protocol each SN names its data with attributes, and the other SNs express their interest depending on these attributes. The sink node distributes an interest packet to all sensor nodes and the concerned nodes alone will reply the sink, with a gradient message.

b. *Hierarchical Based Protocols*

Hierarchical based protocols can also be called as clustered protocols. These protocols reduce the packet flow towards the sink node. Clustered protocols spare least amount of energy when compared to flat networks. On the other side, it is difficult to establish and maintain clusters in a dynamic environment. Some of the known hierarchical protocols are low-energy adaptive clustering hierarchy (LEACH) and PEGASIS [42].

In LEACH [41], the sensors systematize themselves as a part of a cluster and a SN is chosen as the cluster head. The cluster head is recycled then and there, so as to preserve energy. PEGASIS improves LEACH and it systematizes all the SNs as a chain and the primary SN is selected alternatively.

c. *Geographical Based Protocols*

In support of many WSN applications, it is essential to address physical locations. When the position of source and destination is well-known as are the positions of intermediate nodes, this information can be used to support in the routing process. Geographic routing protocols are classified into two types. Those are geo-casting routing and position-based routing protocols. In WSNs, generally the geo-casting aspect of geographic routing is significantly added essential.

Geographical protocols know the geographical information of the SNs and thus this information is used to detect routes. In [53], an energy efficient protocol namely GEAR is presented with two stages. In the first stage, the packet is forwarded to the geographical area at which the destination node is present. In the second stage, the packet is forwarded to the destination node.

d. *Opportunistic Based Protocols*

Opportunistic based routing protocols consider space diversity and the node mobility of wireless sensor networks. Opportunistic routing protocols [54] can be categorized into protocols based on broadcast and space diversity and protocols based on node mobility. The protocols based on broadcast and space diversity approaches manage several transmission entities. With this information, transmission entity set is framed. Protocols based on mobility spares less energy when compared to other protocols. These protocols may broadly categorise into mobile sink and mobile relay based protocols.

Learning based approach is presented to formulate a reliable and efficient method is presented in [53, 54]. The sensor nodes in the proximity of the sink node grasp the locomotion for a certain period of time and define it as a probability density function. Protocols based on mobile relay are brought in the concept of opportunistic networks [55], in which the source to destination path is not made sure. The packet can be forwarded to the destination only through the intermediary node.

2.6.3.2. Operation Based Routing Protocol

In this categorization of routing protocols, the operation of the protocol determines exact classification. The protocols in this group can be classified as multipath based, query based, negotiation based and location based.

i. Multipath Based Routing Protocols

The lifetime of WSNs can be considerably enhanced if the routing protocol is able to maintain several paths instead of a single path to the destination. Protocols fall these category are called multipath protocols. By employing these protocols, the fault tolerance of the WSN is significantly increased.

Multipath routing [56] was working to improve the reliability of unreliable environments. Here, reliability is enhanced by using several paths in sending the same packet from source to destination. By using this method, traffic increases drastically. An expansion of this algorithm is to decrease the complexity of finding the paths by defining the rectangular area bounded by the responding SN and the BS as the routing area.

ii. Query Based Routing Protocols

In this type of routing protocols, the base station propagates the query for sensing task from each sensor node. All the sensor nodes have tables consisting of the sensing tasks queries they received, and send back data matching these tasks whenever you like they receive it. The rumour routing (RR) [57] is an agent-based path formation algorithm. The RR protocol uses a set of long lived agents to generate paths towards the events they meet. Here, the SN may produce an agent in a probabilistic approach, and agents have a lifetime of a definite number of hops after which they die. In the RR protocol, every SN maintains a list of its neighbours and is modernized whenever fresh events are encountered.

iii. Negotiation Based Routing Protocols

The negotiation based routing protocols use high level data descriptors in order to reduce the redundant data transmissions. The main thought behind these protocols is to restrain duplicate information and is done by conducting a series of earlier negotiations.

iv. Location Based Routing Protocols

In these routing protocols, SNs are identified by means of their locations. The distance between the neighbour sensor nodes is approximate on the basis of incoming signal strength. The active SNs should cover the entire sensing area, and provide basic routing and broadcasting functionalities. To preserve energy the SNs should go to sleep if there is no action.

2.6.4. Duty Cycling

Duty cycling deals with the cycling of SNs activities by active and sleeping modes. The sleep mode of a node consumes energy during its idle listening. Switching off the sensor node alone saves full energy and thus it is needed to switch off the sensor node whenever necessary. Duty Cycling is largely decided on the networking subsystem. Such techniques can be applied at a high or a low level of granulation.

2.6.4.1. High Degree of Granulation

When more sensors are deployed in the sensing area, the expected issue is duplication. Thus, duplicated nodes are needed to be switched off, which saves as much energy is possible. The remaining nodes can satisfy the requirements of the applications. In the work proposed in [38], the sensing area is treated as a virtual grid and the grid contains several cells. Each cell has got a leader or a head node, which alone needs to be active. All the remaining nodes of a cell can sleep. There are several works proposed by following this approach.

2.6.4.2. Low Degree of Granulation

The main objective of this level of granulation is to frame an agenda of functionality for nodes. The nodes are allowed to sleep, if it has no job to do. The MAC protocols are classified into three types [50]. Those are TDMA based, Contention based and Hybrid protocols.

In TDMA based protocols, the time interval is broken down into several time slots. Each and every time slot is utilized to transmit or receive data. The outcome of this technique is the collision free medium access to the sensor nodes. An example for this is the protocol TRAMA, proposed in [58].

The contention based protocols do not have any bandwidth reservation mechanisms. All ready nodes compete for the channel concurrently, and the winning node gains access to the channel. This protocol does not provide QoS guarantees to sessions. Some of the examples are S-MACS, T-MAC, D-MAC and B-MAC.

S-MACS (Self-Organizing MAC for WSNs) [59] is an infrastructure-building protocol working for link layer association and network start-up. SMACS is a distributed protocol which enables a collection of sensor nodes to find out their neighbours and establish transmission/reception schedules for communicating with them without the need for any local or global sensor nodes. It assigns a channel to a link straight away after the link's existence is discovered.

In hybrid protocols, the class toggle between time division multiple access (TDMA) and carrier sense multiple access (CSMA) to provide room for dynamic traffic patterns. An example for this type is Z-MAC [59]. CSMA is executed in low traffic and TDMA is utilized for high traffic conditions.

2.6.5. Topology Control

The main objective of topology control is to regulate the topology, which can preserve energy as much as possible. The idea of topology control is severely associated with that of network redundancy. Dense sensor networks normally have some quantity of redundancy. Topology control protocols are thus aimed at dynamically adapting the network topology, based on the application needs, so as to permit the network operations while minimizing the quantity of active nodes. This will improve the sensor network lifetime. Some criterion should be used to decide which SNs to be activate or which SNs to be deactivate. A well-connected topology needs lesser energy and this statement is proved in [60]. WSN devices are heterogeneous and thus three different topology control algorithms are presented and those are DLMST, DRNG and READ.

DLMST and DRNG formulate a reduced topology by taking local information into account. In case, if the initial network is well-connected, then the reduced topology being framed by these topology control algorithms confines to the properties of the network. READ is the Residual Energy Aware Dynamic topology. This topology control algorithm considers the strongest devices for network connectivity. As this type of protocol takes strongest devices into account, maximum energy is preserved and thus the lifetime of the network is improved. READ takes the weighted cost into account. The weighted cost is that the energy needed to forward and receive packets between a node pair. It considers the available energy of each node [61]. Thus, the energy efficient techniques of WSNs are studied thoroughly and with the knowledge gained by this literature, the lifetime of the WSNs is planned to get improved.

2.7. Review of related work

A lot of research work has been carried out in this domain. Some of the recent works are listed as follows.

Li Ya, Wang Pengjun, Luo Rong, Yang Huazhong, Liu Wei [62] A reliable technique for energy efficient communication between nodes was presented. It also used an Energy-aware routing based on beaconing (EARBB) which provided a reliable and energy efficient routing scheme for both information collection and dissemination. Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre [63], Presented techniques like, DTN (Delay Tolerant) Know Thy Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing Networking are networks of self-organizing wireless nodes where end -to-end connectivity was intermittent.

Qinghua Li and Guohong Cao, [64] "Mitigating Routing Misbehavior in Disruption Tolerant Networks", they discussed about the selfish or malicious nodes that may drop the received packets. Such routing misbehaviour reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Arjan Durresi, Vamsi Paruchuri [65], "Delay-Energy Aware Routing Protocol for Sensor and Actor Networks", An adaptive energy management scheme that controls the wake up cycle of sensors based on the experienced packet delay, extend the area of networking according to the demand it does not has any boundaries. Synchronous wakeup approach is used by ad hoc power save (PS) mode.

Reuven Cohen and Boris Kapchits, [66] "Energy-Delay Optimization in an Asynchronous Sensor Network with Multiple Gateways", The problem in this paper is constructing efficient routing trees and the problem of wake up frequency assignment in a network with multiple routing trees. Sayid Mohamed Abdule, Suhaidi Hassan [67], has proposed by a Divert Failure Route Protocol Schemes as a solution to link failure. DFRP tries to avoid a link failure in advance. K.A.Shah, M.R.Gandhi [68], focus on the performance of AODV routing algorithm with reference to local route repair techniques of link route repair. P.Priya Naidu, Meenu Chawla [69], presents enhanced AODV-Local Repair Trial protocol, extended to achieve broadcasting and minimizing the flooding. LIU Jian, LI Fang-min [70], proposes an improvement of AODV protocol based on reliable delivery in MANETs, a link failure fore-warning mechanism and metric of alternate node in order to better selecting based on route breaks. Qing Li, Cong Liu, Han-hong Jiang [71], Presented a mechanism of link failure forecast into the link restored and improved routing protocol. This mechanism of improved protocol (AODV_LFP) AODV based on Link Failure Prediction. Li Qiong and Yang Jun [72] proposes AODV routing protocol needs improved optimization. The routing table in AODV maintains only one route to the destination node and the source node needs to re-initiate the route discovery process as a route fails. Reinaldo Gomes, Eduardo Souto, Judith Kelner, Djamel Sadok [73] to deal with this work to avoiding routes composed by nodes with little energy in selection process and improve the energy consumption of the nodes.

Michael Pan, Sheng-Yan Chuang and Sheng-De Wang [74] has proposes to evaluate the effects of the route repair, are aimed to efficiently repair the link errors. Jing Feng, Huaibei Zhou[75] deals with self-repair algorithm for the ever changing topology and limited bandwidth, it is very hard to maintain good routes, and link break is frequently occurred in mobile Ad Hoc networks. Hua Qu, Peng

Zhang, Ji-hong Zhao[77] presents the improved local repair scheme concerns about the status of nodes and regards the change of status as the basis of local repair. LIU Jian, LI Fang-min[78] presents an AODV with reliable delivery (AODV-RD), a link failure fore-warning mechanism, metric of alternate node in order to better select, and also repairing action after primary route breaks basis of AODV-BR. Suhazlan Suhaimi, Kamaruddin Mamat, S.R Azzuhri[79] proposes investigate the performance of AODV in situations of link failures due to mobility of nodes and consequent route recovery mechanism. Zilu Liang, Yuzo Taenaka, Takefumi Ogawa, Yasushi Wakahara[80] presents the recovery of every link in a route before its break, while the route recovery process actually starts only when the upstream node of a link confirms the link break.

Jyoti Jain, Roopam Gupta, T.K. Bandhopadhyay [81] ACO in the process of route discovery and in load balancing. P. Priya Naidu and Meenu Chawla [82] Routes can be locally repaired by the node that detects the link break along the end to end path .Enhanced Ad Hoc on Demand Distance Vector Local Repair Trial using Diameter Perimeter Model. Banoj Kumar panda, Bibhudatta Dash, Rupanita Das, Ajit Sarangi [83] proposed to change in mobility link between neighbors nodes can break a number of times as a result of which the performance of a network may be hampered. Shijie Li, Xu Li, Qijing Feng [84]presents An Improved AODV Local Repair Algorithm Based on Delay Constraint with new local repair algorithm delay constraint (DC-AODV) is proposed. Muhammad Khalil Afzal, Hyun-Ho Shin, Byung-Seo Kim, and Sung Won Kim [85] proposed a link quality aware local recovery protocol for AODV based Ad hoc networks. Xingyun PENG, Yi WU, Zhexin XU, and Xiao LIN [86] the vehicles mobility and versatile topology lead to frequent failure of VANET links propose a new scalable routing scheme named AODV-MR (AODV with multi-RREP). Krishna Mahajan Devesh Malik M.A Rizvi D. Singh Karaulia [87] proposed Event Driven Dynamic Path Optimization For AODV does not re-initiate route discovery until link failure or route break occurs which incurs large overhead and increase in delay and is not energy efficient. So dynamic optimal route discovery should be done.

2.8. Summary

The major challenge of WSN routing is explained in this chapter. Further routing is categorized into two types of topology distribution known as static and dynamic routing. Routing challenges and design issues of WSN presents network scale, time-varying characteristics, resource constrain, and Data Models. Routing strategies and Failure classification of wireless sensor network is discussed. The routing protocols must be paid enough attention for energy restricted nature of WSNs. Routing protocols detect the most feasible route from the source to destination. The routing protocols are classified into data-centric protocols, hierarchical protocols, geographical or location based protocols. The major issue for route failure, classification of failure and route recovery process in sensor network are studied. Energy efficient techniques are studied and classified into major categories. Literature review of work on recent and previous works are briefly presented.

3.1. Introduction

The route recovery process of Divert Failure Route Recovery (DFRR) mechanism uses round trip path algorithm to detect a failure node while going through the number of sensor nodes. The energy consumption of all the sensor nodes has to be kept balanced. The energy level of sensor node computation and the lifetime of sensor node improvement is effective if the energy utilization is balanced. This chapter is divided into two parts, the first part presents the DFRR routing mechanism and the second part explains about Proposed Ad hoc On-demand Distance Vector (PRO-AODV) routing mechanism.

Here the sensing actions are applied to every node. This RTP algorithm uses to detect the number of failed sensor nodes. Divert failure route recovery (DFRR) mechanism concentrates on round trip path detection algorithm with the support of Round Trip Delay (RTD) time measurement in mobile sensor networks.

Proposed Ad hoc On-demand Distance Vector (PRO-AODV) mechanism maintain a routing table for every node and also retains route information. Each route is established from the source to the destination. Whenever there is a link failure, the sensor nodes themselves re-initiate the route discovery process. The route maintenance process forwards both the route request message and route reply message. In route recovery section, when a particular node is about to fail, it takes the required information from the nearest node, until the former gets into normal mode. A backup routing table is built when the speed of the node movement is less than a threshold value.

The link failure or node failure problem of route repair process is based on DFRR and PRO-AODV mechanisms. The lifetime of a sensor node, and its energy-efficient route recovery process is based on energy levels of sensor node in a mobile sensor networks.

3.2. Route Recovery Process of DFRR mechanism

In this approach, link failure of route recovery process is implemented by Divert Failure Route Recovery (DFRR) mechanism. The mobility of circular topology is changed by a mobile sensor nodes, when there is link failure due to link mobility. When the number of mobile nodes in any given contest increases, it results node blocking and node monitoring of link errors. This problem can be overcome by depending on intermediate node or neighbouring node.

3.2.1. Circular Topology

The real time experiment with six sensor nodes are implemented in WSN. The sensor nodes are placed at one-foot distance among each node in circular topology network environment of WSN. Circular topology with six sensor nodes is shown in the figure. 3.1.

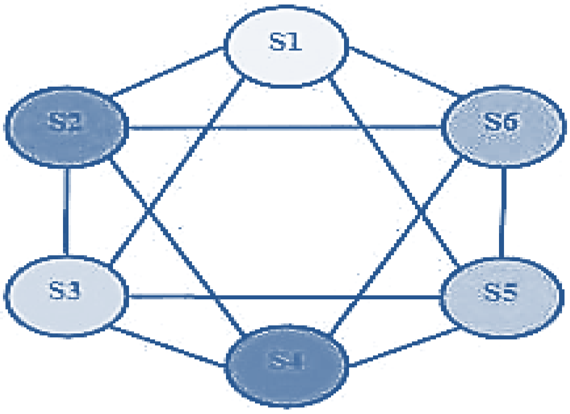


Figure 3.1: Sensor nodes in Circular Topology

The DFRR approach can be implemented to detect a failure node in Centralized network as well as in Distributed networks. The utilization of round trip path algorithm (RTP) is to detect the failure node based on round trip delay (RTD) time measurement. A few RTPs are analyzed during fault detection in order to improve the lifetime of the network as well as the quality of service in WSNs.

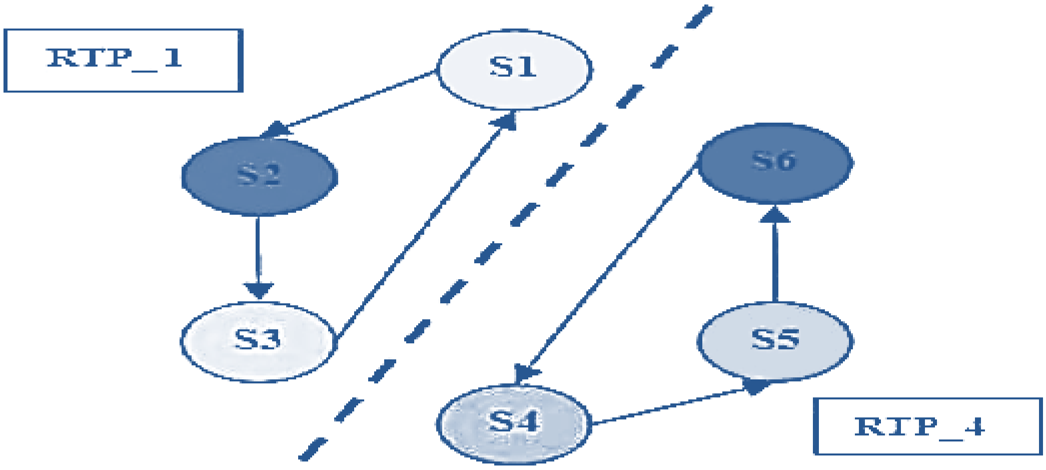


Figure.3.2: Represent of two discrete RTPs.

The round trip paths are formed by combining the adjacent three sensor nodes. The figure.3.2 represents how RTP process works in a circular topology of sensor node connection route transmission between 1, 2 and 3 nodes. Construction of these three nodes is maintained by RTP_1. In the same way, a route transmission between 4, 5 and 6 nodes is maintained by RTP_4.

The monitoring cycles and monitoring paths to maintain route construct, transmission of a route between nodes, and round trip delay time is calculated in each RTPs. The calculation of Round Trip Paths in network area with RTD time values on sensor nodes is measured. RTD time is mainly dependent upon the numbers of sensor nodes present in the round trip path and the distance between each sensor node. Selecting a minimum number of sensor nodes in the RTP will reduce the RTD time. The round trip path (RTP) in WSNs is formed by grouping minimum of three sensor nodes [24]. Hence the minimum round trip delay time (τ_{RTD}) of RTP_1 for three sensor nodes.

$$\tau_{RTD} = \tau_1 + \tau_2 + \tau_3 \qquad 3.1$$

Where τ_1, τ_2, and τ_3 are the delays for sensor node pairs (1,2), (2,3),(3,1) respectively. Three consecutive sensor nodes in each RTP are almost at equidistance because of circular topology. As a result sensor node pair delays τ_1, τ_2 and τ_3 will be equal. Let 'τ ' be the uniform time delay for all sensor node pairs in RTPs i.e. $\tau = \tau_1 = \tau_2 = \tau_3$. Round trip delay time for RTP_1 with uniform sensor node pair delay is obtained by the equation as

$$\tau_{RTD} = 3\tau \qquad 3.2$$

This is the minimum RTD time of an RTP in WSNs. It is determined by the sensor node pair delay (τ), as it depends on the distance between the sensor nodes.

Discrete selection of RTPs implementation of the first level optimization the analysis time is curtailed up to a certain limit. If this limit exceeds and the growth of RTPs becomes high, RTD time may be enhanced. In the presence of a number of sensor nodes, if the RTD time exceeds, the fault identification time is significantly enhanced. So again there is need to minimize RTPs in WSNs. The second level of optimization focuses on the number of RTPs reduced by selecting only discrete paths in WSNs. They are selected by ignoring two consecutive paths, after each selected linear path. In this way, RTP's are selected in discrete steps of three as each RTP consists of three sensor nodes [24]. The equation to select the discrete RTPs in WSNs is given by

$$P_d = Q + C \qquad 3.3$$

Where P is the numbers of discrete RTPs. Q and C in above equation are expressed as

$$Q = [N/M]$$

$$C = 0 \quad \text{if } R = \begin{cases} 0, \text{ otherwise} \\ 1 \end{cases}$$

Where Q is the quotient, M is the numbers of sensor nodes in RTP, R is a remainder, N is total numbers of sensor nodes in WSN and C is correction factor to be added. Correction factor will be 0 if the remainder is 0 otherwise it is 1.

3.2.2. Round Trip Path Algorithm

The Round Trip Path algorithm is describes stepwise in as follows:

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

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

Step3: Find Round Trip Path, i.e.

$$P_d = Q+C$$

Step4: Transmission starts between three sensor nodes.

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

Step6: Find RTD of all the sensor nodes.

Step7: Find Threshold Value.

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

Step9: Performance animation file is found to show failure sensor nodes.

Round Trip Path (RTP) algorithm identifies faulty nodes while detecting the number of sensor nodes. Round trip detection delay time is compared with threshold time to determine the faulty node or node that is failed. This reduces the energy level of the battery, which reduces the lifetime of the network.

The Round Trip Delay (RTD) time measurement technique is a simple approach to obtain the information with respect to above issue in WSN. The technique for a failed node detection is based on RTD time measurement of Round Trip Paths. Round Trip Delay times on discrete Round Trip Paths are compared with a threshold time to determine the failure sensor node.

3.2.3. System Design for DFRR mechanism

The system design of flow diagram how to detect faulty nodes are represent in the figure 3.3.

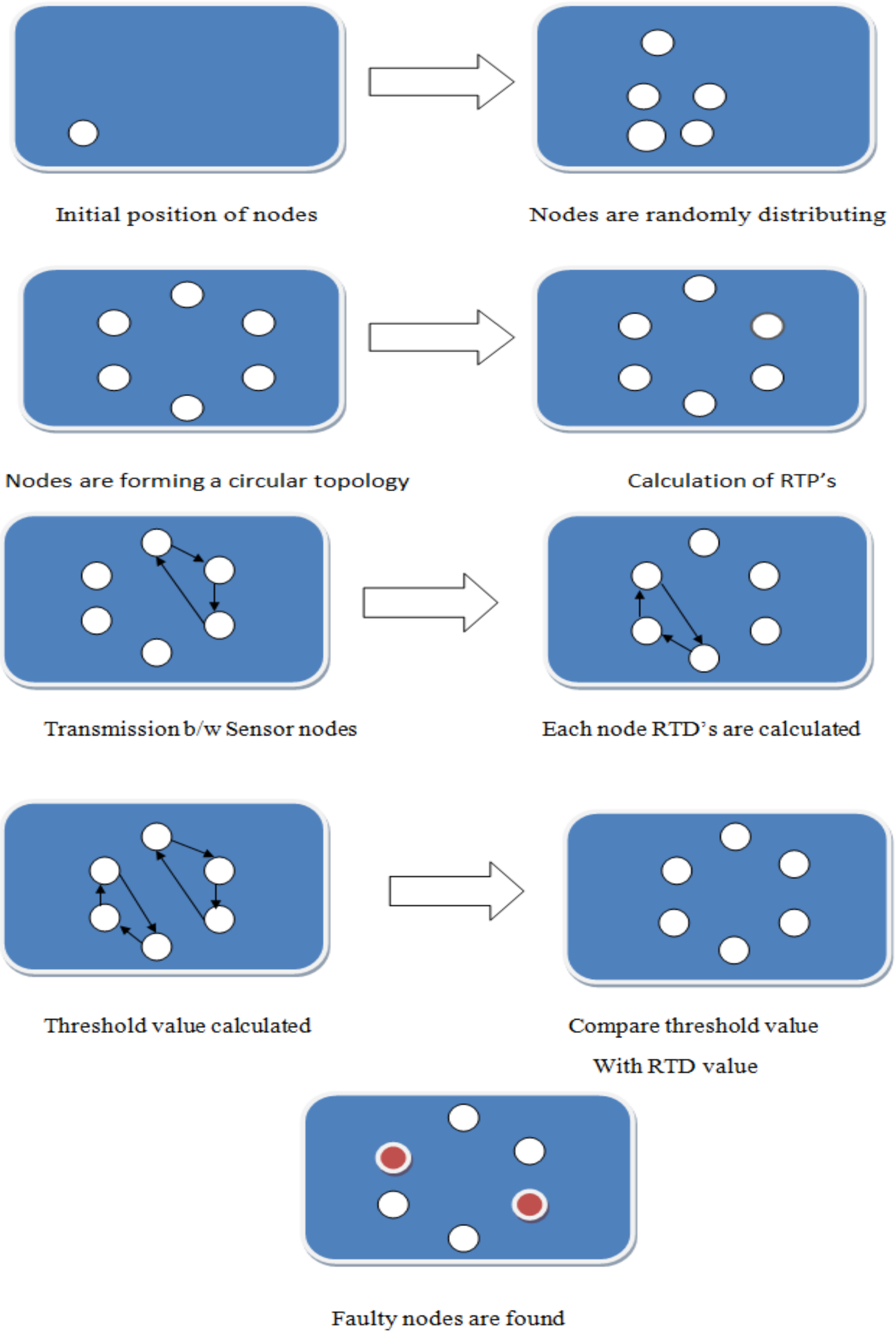


Figure 3.3: Flow of system design in DFRR mechanism

The system design of flow diagram represents the faulty node detection which is based on monitoring cycles (MCs) and monitoring paths (MPs). Threeedge connectivity in the network, the separate wavelength for each monitoring cycle and monitoring locations are the limitations of Divert Failure Route Recovery mechanism.

The flow chart of DFRR mechanism using RTP algorithm implemented on a node is in failure condition is represented in the following figure3.4.

3.2.4. Flow chart of DFRR mechanism

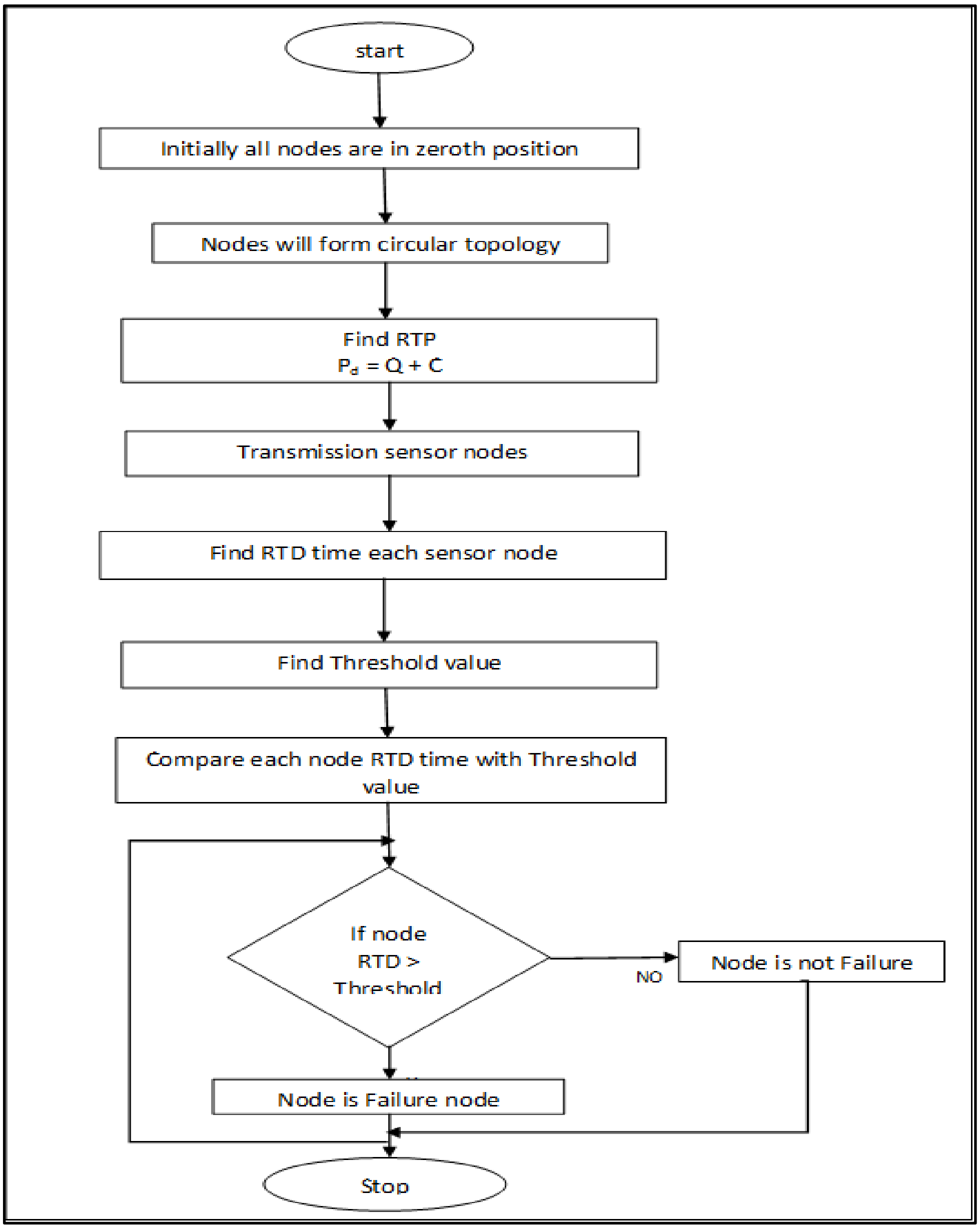


Figure.3.4: Flow Chart of DFRR mechanism

The proposed mechanism plan to implement the schemes have focused on re-establishing severed links without considering the effect on the length of distance between sensor nodes get before pre-failure information.

3.3. Performance Analysis for DFRR mechanism

In this section, the performance of DFRR mechanism results is evaluated in Network Simulator. The simulation evaluations in Network Simulator (NS-2.35) [76] and Linux Mint (17 version) operating system will be conducted to perform experiments and results analysis on the performance ability of RTP algorithm with the discussed in DFRR mechanism.

The DFRR mechanism is experimented on WSNs with sensor nodes designed by using microcontroller and ZigBee procedures. RTD detection of algorithm is compared with threshold time to determine the failed nodes. Appropriate threshold RTD time is determined by simulating various WSNs.

The design and implementation of our testbed using Network Simulator (NS- 2.35) [76] with the support of DFRP protocol, simulation results and various performance parameter metrics in simulation network scenario are generated. This experimental simulation area is in 500m*500m within the space of 200 random configuration sensor nodes. The total simulation time taken in 150 seconds.

The simulation model of energy parameter values such as initial energy, radio transmission power (Tx), receive power (Rx) and idle power of sensors. The simulation parameter values and energy model values of sensor node details for DFRR mechanism is shown in Table 3.1.

Parameters	Values
Network Range	500*500 m
Data Packet Size	512 Bits
Routing Protocol	DFRP
Initial Energy	100 joules
Transmission power	35mW
Receive power	40mW
Idle power	7mW
Simulation Time	150
Number of nodes	200

Table.3.1: Simulation Parameter Values for DFRR mechanism

In the following table 3.2, it is observed that the performance metrics of DFRR (Divert Failure Route Recovery) mechanism are noted with respect to simulation time from 10 to 150 seconds. The node mobility of network is based on DFRR mechanism to observe the lifetime of the network.

Simulation Time (sec)	Packet Delivery Ratio (PDR)	End to End Delay (sec)	Average Delay x 10^{-3} (sec)	Throughput (Kbit/sec)
10	7.69	0.30	205.85	1.44
20	54.92	0.35	206.36	2.55
30	66.17	0.63	362.71	4.64
40	74.05	1.25	516.86	3.92
50	72.64	0.79	500.85	4.93
60	78.51	0.17	546.34	7.69
70	76.17	0.67	609.50	7.80
80	77.06	0.98	713.98	8.50
90	78.09	1.08	767.22	9.34
100	79.05	1.73	767.22	9.93
110	81.64	0.61	802.52	11.16
120	81.25	1.25	982.19	12.89
130	85.76	1.16	999.12	12.78
140	87.33	1.02	972.91	11.42
150	88.96	0.89	950.04	13.21

Table 3.2: Analysis of Metrics results in DFRR mechanism

The performance of experimental results in DFRR mechanism is based different parameter metrics such as packet delivery ratio calculates in percentage, average delay and end to end delay are measured in seconds. The throughput is calculated in Kbit per second and the energy consumption is measured in joules. The route detection time is measured in seconds with respect to number of sensor nodes deployed in network transmission range.

3.4. Route Recovery Process of PRO-AODV mechanism

The second part of this chapter is an implementation of AODV routing protocol design and improvement of the same is named "Proposed AODV (PRO-AODV) route recovery mechanism". In this PRO-AODV routing mechanism, the distance between the points where the link fails source node to destination node is quit fast. Whenever, PRO-AODV route discovery from the source to destination re-established, a significant overhead, network congestion as well as high bandwidth utilization are caused. In view of oversized transmission delay in AODV routing protocol, PRO-AODV routing protocol is put forward and this mechanism of route repair is introduced into the process of data transmission.

In this section, the PRO-AODV mechanism is primarily maintained by three steps and they are: route discovery, route maintenance, and route recovery. The AODV standard protocol handles the link failure problem after the link is broken and an intermediate node sends an error message to the sender. Then the sender will rebroadcast a new route request message throughout a network. In the PRO-AODV mechanism, when a link failure occurs, the node that detects the link failure sends an error message packet back to the source and the source will initiate a new route discovery process. This route discovery process is explained in the following section.

3.4.1. Route Discovery

Route discovery process maintains a source node in the network which needs to communicate with other nodes. The first need is to determine whether routing table is valid for a route to exist to the destination node. If the route is set up, the destination node can communicate with the origin node directly. If there is no effective route to reach a destination node, need to broadcast within a certain range of Route Request (RREQ). When an intermediate node receives the RREQ, the source node determines that it received the RREQ. If the node receives message repeatedly, then it is discarded. Otherwise, a reverse route to source node needs to be created. When an intermediate node has an effective route to the destination node, it can communicate with the destination node directly.

3.4.2. Route Maintenance

Route maintenance of active routes in AODV [12] is done by continuous monitoring of link status of next hops. HELLO messages are sent periodically to the neighbour node to check whether the link exists. The Route Error (RERR) message is sent upstream to source node, when a link failure is noticed. Source node finds an alternate route to the unreachable nodes by reinitiating the route discovery. Every node in active path consumes a certain amount of energy for the active participation in communication.

In PRO-AODV mechanism the energy level goes down and reaches a minimum and the associated links connection between sources and destination gets disconnected. The reason for disconnection or link failure may be limitation on transmission range and mobility. Alternate route discovery process can re-initiate the route process in the network area. When Route Reply (RREP) message receives a broadcast from a neighbour, it updates its local connectivity information. However, RREP message remains there a certain period of time without sending or broadcasting, except a 'hello 'message is sent to its neighbours a hello. The hello messages are not rebroadcast as they are used only to maintain the local connectivity. If the sensor node fails in receiving broadcasts and hello messages from a neighbour node for a certain period of time, it considers that destination is not a neighbour node anymore. The source node receives a message which it is supposed to forward to the destination node and the source node generates a link failure notification. The PRO-AODV mechanism can use Hello messages to maintain local route connectivity among neighbours, and this is required by the AODV routing protocol.

Normally each source node maintains a route to a specific target. Once there is a route failure, it will return to initiate the route discovery process that will also increase the network load. With high-speed node mobility, the network topology changes very frequently, and this shortcoming is particularly prominent.

The link can reduce sending RREQ news and lessen the network load, which, in certain conditions, is more effective routing setup to backup routing table. The backup routing table deposits another effective routing, which is from the source to the destination node. This process can be discussed in route recovery section.

3.4.3. Route Recovery

In the route recovery process, the intermediate nodes, according to their movement and speed, establish a backup routing table. Backup routing table deposits another effective routing, which is from the source to the destination node. The routing table starts a backup route first, when the route has a broken chain, and needs to re-route discovery only when the first backup route fails. This can reduce the RREQ flooding, thereby reducing the load on the network.

The fast moving nodes will result in sudden changes in the network topology; in this case, it is not suitable to create a backup routing table. In normal cases, it is suitable to create a backup routing table. Set a node in the middle of moving speed of V_i, node numbers n, speed frequency impact factor as a, speed thresholds that determine whether the backup route to V, then

$$V = a\frac{\sum_{i=0}^{n} Vi}{n} \qquad \text{-------------------------- } 3.4$$

Adjust the speed frequency influence factor a, and the protocol obtains a different improved performance. The experimental results show that the improved AODV routing protocol can effectively inhibit the packet delivery rate, reducing end to end delay and throughput, as well as reduce the routing load.

In the PRO-AODV routing process, initially set up route discovery of all the nodes communication between each other. Selecting route from the source node to the destination node. The messages to exchange the information of all control messages form source to destination.

The flow diagram of PRO-AODV mechanism is shown in Figure 3.5.

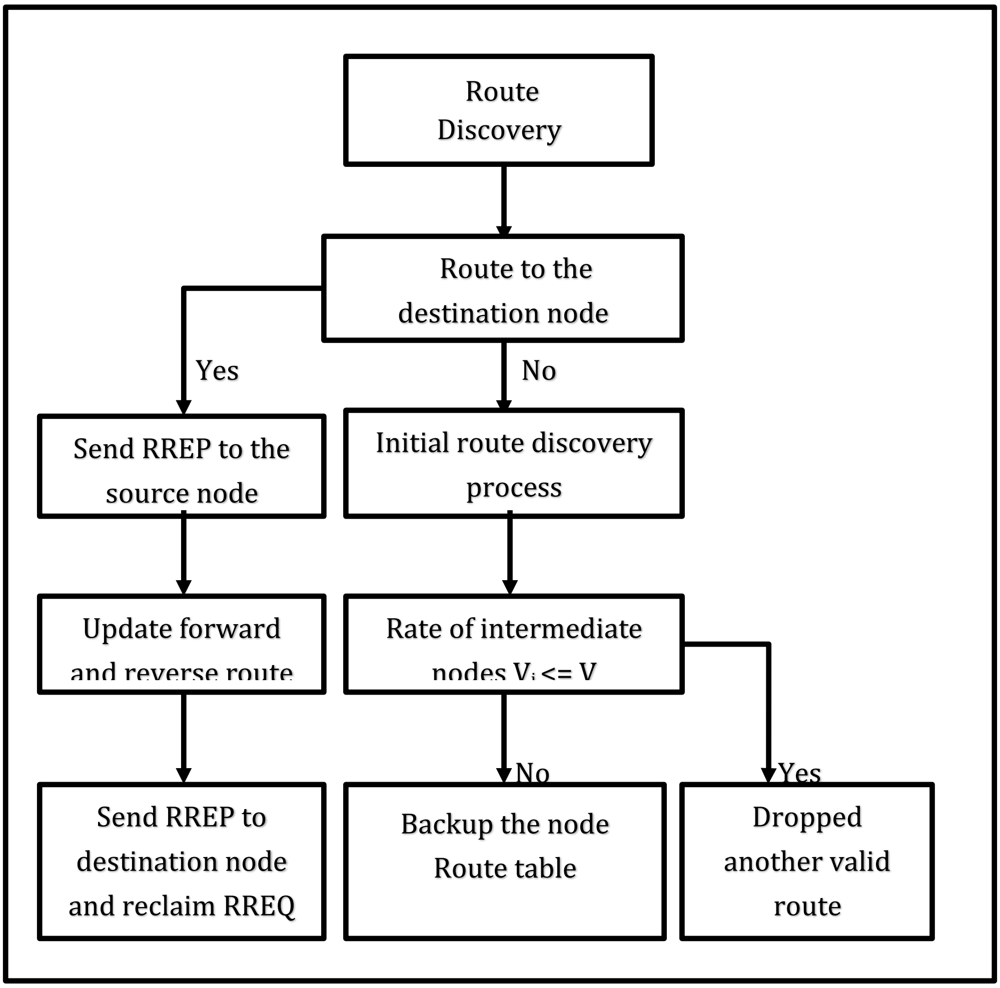


Figure 3.5: Flow diagram of PRO-AODV mechanism

The PRO-AODV routing process is an important mechanism of on-demand routing protocol, with an agreement to increase the routing load, and reducing the cost of energy consumption to improve network performance. So, based on the AODV Routing Protocol in the text, in-depth analysis of AODV Routing Protocol in the process has been conducted and came up with a good application in WSNs improvement of PRO-AODV Route Recovery mechanism.

3.5. Performance Analysis for PRO-AODV mechanism

This experimental simulation network area is in 500m*500m with the space of 200 sensor nodes are randomly distributed. The total time taken for each simulation is 150 seconds. The experimental analysis results are displayed by the PRO-AODV mechanism. There are four performance evaluation parameter metrics: packet delivery ratio, end-to-end delay, average delay, and throughput. The simulations have been performed using Network Simulator 2 (version 2.35) is open source software that provides scalable simulations. The simulation performance of network transmission details and the parameter values for PRO-AODV mechanism is shown in Table 3.3.

Parameter	Values
Network range	500*500m
Routing Protocol	AODV
Transmission range	250 m
Bandwidth	2 Mbps
Simulation time	150 s
Number of Nodes	200
Packet rate (packet/s)	4.0

Table 3.3: Simulation Parameter Values in PRO-AODV mechanism

3.5.1. Performance metrics

The performance metrics employed in this work are packet delivery ratio, Average delay, End to end delay, throughput, and energy consumption by varying the simulation time. The route detection time analysis is made with respect to number of sensor nodes. The following six parameter metrics are:

- **Packet Delivery Ratio:** The ratio between the number of data packets sent and number of data packets received at a destination.

$$\text{Packet delivery ratio} = \frac{\text{Number of Packets received}}{\text{Number of Packets Sent}} \times 100$$

- **End-to-End Delay:** The time taken by the data packet to reach from source to destination node.

$$\text{End} - \text{to} - \text{End Delay} = \frac{\text{Arrival time} - \text{sent time}}{\text{Total number of connections}}$$

- **Average Delay:** The time difference between the packets received time, sent time and total time taken for the packets received by all nodes.

$$\text{Average Delay} = \frac{\text{Total End to End Delay}}{\text{Total number of Packets received}}$$

- **Throughput:** The total number of data packets delivered per unit of time.

$$\text{Throughput} = \frac{\text{Total number of transferred packets}}{\text{Time taken (secs)}}$$

- **Route Detection Time:** Route detection time is the time it takes to find an optimal route with respect to number of nodes. The formula is given by the time at which the route is found is subtracted from the start time of route discovery.

$$\text{Route Detection Time} = \text{Route Discovery Time} - \text{Initial Time}$$

- **Energy Consumption:** Energy consumption calculates the present energy of all nodes are subtracted from initial energy of all nodes. This calculates the total energy consumed by the node with respect to time.

$$\text{Energy consumption} = \text{Initial Energy} - \text{Present Energy}$$

3.5.2. PRO-AODV mechanism Experimental Results

The experimental results of PRO-AODV mechanism is based on several parameter metrics such as packet delivery ratio, average delay, end to end delay, throughput, energy consumption by varying the simulation time and the route detection time analysis with respect to number of nodes in mobile sensor network. The simulation time is measured in seconds with respect to number of sensor nodes deployed in network transmission range. The performance of parameter metrics of PRO-AODV mechanism experimental results is shown in Table 3.4.

Simulation Time (sec)	Packet Delivery Ratio (PDR)	End to End Delay (sec)	Average Delay x 10^{-3} (sec)	Throughput (Kbit/sec)
10	10.15	0.21	152.63	1.21
20	23.22	0.23	154.36	2.61
30	55.96	0.45	205.24	5.26
40	66.12	1.12	368.15	5.92
50	74.25	0.65	456.25	6.85
60	81.17	0.23	589.75	8.54
70	82.36	0.36	612.85	8.75
80	81.69	0.65	635.12	10.65
90	84.43	0.98	653.58	9.63
100	84.56	1.92	685.47	11.58
110	83.26	0.35	712.56	12.15
120	86.15	1.25	796.58	13.14
130	87.85	0.76	815.46	14.09
140	89.58	0.68	826.96	12.25
150	94.56	0.52	846.24	14.22

Table 3.4: Analysis of Metrics Results in PRO-AODV mechanism

The PRO-AODV improvement is in the use of the node's mobility rate to change the routing process dynamically and to reduce the energy of sensor node lifetime in the route discovery process. Energy consumption is measured in joules. Energy consumption rises with number of packets transmitted. It measures the amount of energy consumed for the transmission of all the packets which includes both control and information exchange packets.

The energy consumption analysis of DFRR and PRO-AODV results with respect to simulation time is shown in the following Table3.5.

Simulation Time (sec)	Energy Consumption(J)	
	DFRR	PRO-AODV
10	11.5	12.6
20	16.6	21.2
30	22.0	26.0
40	27.5	29.0
50	29.7	33.5
60	32.2	38.5
70	38.6	42.2
80	41.7	45.0
90	43.5	49.0
100	52.3	56.0
110	60.2	62.0
120	69.5	69.0
130	75.8	78.0
140	82.6	86.0
150	85.5	95.0

Table 3.5: Analysis of Energy Consumption Results

The route detection time analysis of DFRR and PRO-AODV results with respect to number of nodes as shown in the following Table3.6.

Number of Nodes	Route Detection Time (sec)	
	DFRR	PRO-AODV
20	16.3	13.1
40	17.4	14.3
60	18.6	15.2
80	17.5	16.4
100	19.7	18.1
120	20.5	19.3
140	21.6	20.5
160	23.1	22.5
180	24.8	23.4
200	28.8	25.6

Table 3.6: Analysis of Route Detection Time Results

The performance of DFRR mechanism results are evaluated using NS-2 [76] and compared with DFRR and PRO-AODV. First, the results of six parameter values are generated and then the performance of two mechanisms are compared and concluded that PRO-AODV is better performer.

The performance comparison of the two mechanisms relating to the route discovery approaches is discussed in the present chapter. Simulation results of DFRR and PRO-AODV mechanisms are represented.

3.6. Summary

The main focus of this chapter is on two routing algorithms explained into two sections. The first section presents the Divert Failure Route Recovery (DFRR) mechanism with the use of round trip path algorithm and the second section explains about Proposed Ad hoc On-demand Distance Vector (PRO-AODV) to solve problem of link failure on route recovery process. The performance evaluation is based on experimental results of PRO-AODV mechanism with six parameter metrics with respect to simulation time and number of nodes present in the MSN.

4.1. INTRODUCTION

A Mobile Sensor Network (MSN) is a network consists very large number of mobile sensor nodes to gain information from the environment and to communicate with each other sensor nodes. In this chapter, the fast route recovery of link failure problem in MSN is done by using energy level computation and Check Point Route Recovery (CPRR) approach.

Check Point Route Recovery (CPRR) algorithm is used to detect the energy drain of a node, to replace that node before it is completely drained. This approach is to detect failure node and replaces by the nearest actor node. Reactive type of routing protocol refers to simultaneously selecting the best path between the source and the destination on demand basis. Route recovery process is based on actor node among all sensors nodes communicate in a mobile sensor network. While communication between all the sensor nodes, it consumes more energy than all other operations. The CPRR algorithm that focuses on the fast recovery of failure node is based on the minimum energy requirement during communication among all sensors. The functioning of mobile sensor node is of two types: Static sensor node, maintains the connection links to actor nodes and Dynamic sensor node replaces the node with the failed node after taking backup information.

The Check Point Route Recovery (CPRR) algorithm proposes the steps which involve route discovery, failure node detection, and selection of node replacement process to effect the successful communication in mobile sensor network. Network Topology Management (NTM) technique helps to maintain the link between the nodes to detect when energy loss of a particular node. During node replacement time, there are possibilities for the direct link break between the nodes where NTM technique helps to maintain the links. This work focuses on design concepts of Check Point Route Recovery algorithm with the help of architecture diagram and design of proposed work.

The CPRR algorithm analyse and explain the sensor nodes how they work. The CPRR algorithm divided into two phases, data flow diagram and also show in design diagram. The experimental results for proposed CPRR work is explained in the form of graphical presentation and compared with PRO-AODV results.

4.2. Sensor nodes for route recovery process

Check Point Route Recovery (CPRR) Algorithm function is to find out the energy drain in an actor node, even before the energy of that particular node is completely drained. This check point route recovery algorithm supports two types of sensor nodes. They are as follows:

- Actuator/Actor node
- Mobile sensor node

4.2.1 Actor Node

An actuator node is a sensor node, which is capable of performing sensor processing and gathering sensor information. The actor node is also called an actuator node. Every actor node has a special Internet Protocol (IP) addressing. The nodes communicate wirelessly after being deployed in a sensor network. It will periodically send messages to their neighbours in one hop counts. Missing messages can be used to detect the failure of actor nodes. Once a failure node is detected in the neighbourhood, then one-hop neighbour of failure node would be determined. The impact of the failed node is critical to network connectivity. The CPRR Algorithm serves the shortest route of all nodes with the support of static and dynamic sensor nodes.

4.2.2 Mobile Sensor node

The mobile sensor node finds the following issues in a mobile sensor network. First it finds out delayed messages or missing messages and also detects the energy drain in a particular node. The functioning of mobile sensor node acquiring with two types of network IP addresses. They are as follows:

a. Static mobile sensor node
b. Dynamic mobile sensor node

a. Static mobile sensor node

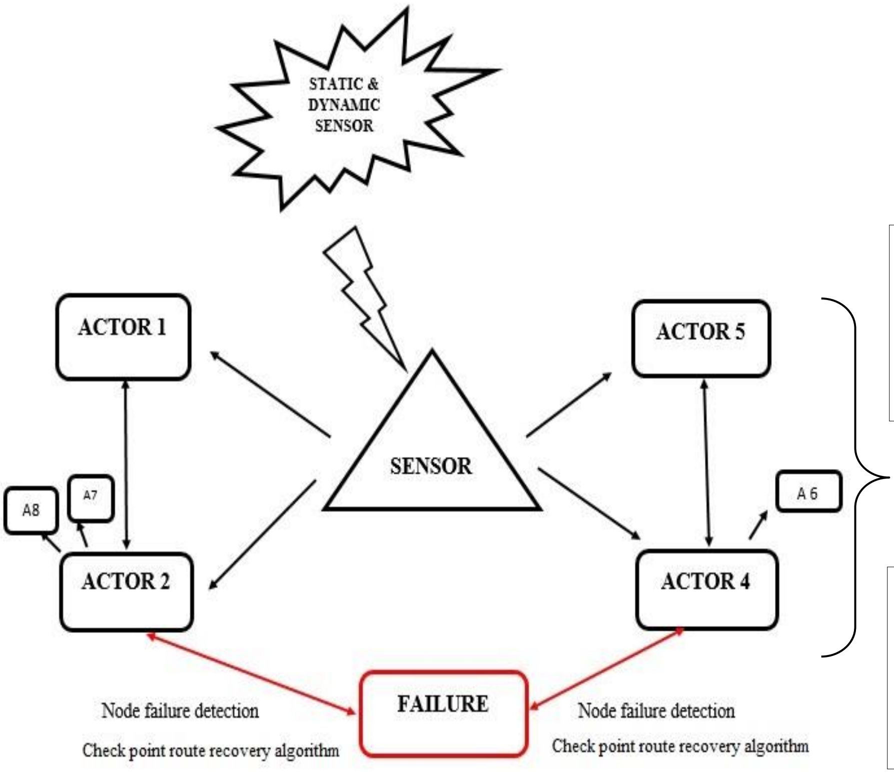
The network IP address in a static configuration setup manually. The static sensor node IP address could not change automatically. The static sensor node monitors each and every actor node and if there is energy loss in any node then it intimate to the dynamic sensor node.

b. Dynamic mobile sensor node

The network IP address in a dynamic sensor node can change randomly distribution. The dynamic mobile sensor node finds the nearest node whose energy level is high and has the lowest number of links. The dynamic sensor node after receiving the information searches for a node which is nearest to the failure node and whose energy is high. The dynamic sensor node selects a node for replacement based on priority. A failure node will come back it position after gaining all its energy.

4.3. Architecture of CPRR algorithm

The architecture defines the structure of the proposed CPRR algorithm which comprises different components, their externally visible properties and the relationship among them. The architecture shows the four steps along with the algorithm used in them in order to implement the CPRR architecture. The architecture of Check Point Route Recovery algorithm is shown in the Figure 4.1.



Actor 5 informed to move towards Actor 4 by Network Topology Management technique to prevent link breaks.

Actor 4 selected to replace and recover the failure node by check point route recovery algorithm.

Figure.4.1: The architecture of CPRR algorithm

The check point route recovery algorithm gives a list of steps involved in this proposed method and they are as follows:

- Routing discovery
- Failure node detection
- Selection of node for replacement
- Network Topology Management technique

4.3.1. Routing discovery

Route discovery process is works based on Ad-hoc On-demand Distance Vector (AODV) routing procedures. AODV [12] is a reactive type of routing protocol refers to simultaneously selecting the best path between the source and the destination on demand. The pro-active type of routing protocol refers to finding the shortest path between each and every sources to destination and saving it to a routing table. Further, the saved path for each and every source to destination is taken from this routing table. The reactive type of routing protocol concurrently calculates the best path on demand. Routes are established on demand as they are needed. Reactive routing protocol finds a path between the source and the destination only when the path is needed i.e., if there is data to be exchanged between the source and destination.

In AODV [12] every hop has the constant cost of one. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. The routes age quickly owing to accommodating the movement of the mobile nodes, Link breakages can happen at any time. These breakages can be locally repaired very efficiently. Source, destination, and next hop are addressed by using IP addressing. AODV uses IP in a special way. Only one route in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. The route where the energy consumption is less, is known as the best routing. By selecting the best route, the energy consumption of each and every node can be minimized. It helps to retain the energy of each node. Thus by minimizing the energy consumption, the life span of the nodes can be maximized.

4.3.2. Failure node detection

Check Point Route Recovery (CPRR) Algorithm calculates the energy levels of each node by sending messages. Actor nodes will periodically send messages to their neighbours to ensure that they are functional, and also report changes to the one-hop neighbours. Missing messages can be used to detect the failure of actor nodes. Once a failure is detected in the neighbourhood, the one-hop neighbour nodes of the failure actor node would determine the impact, i.e., whether the failed node is critical to network connectivity link failure node detection as shown in the figure 4.2.

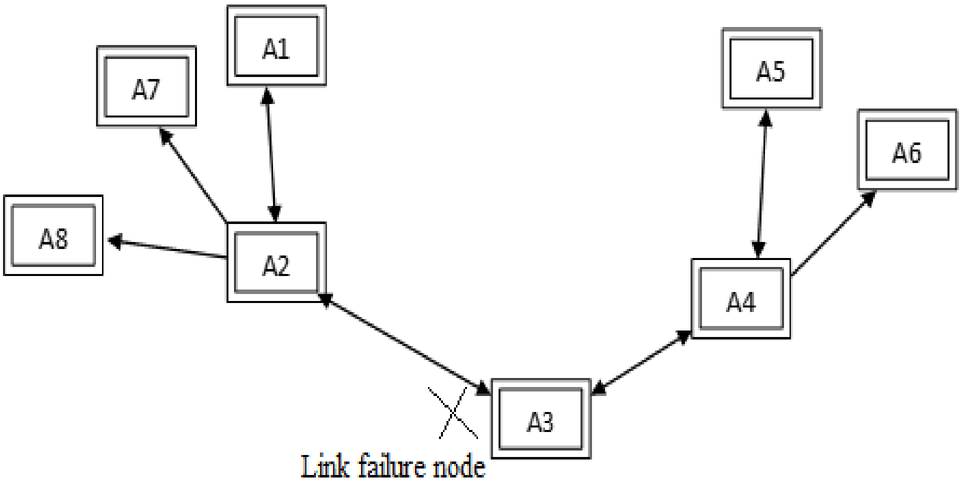


Figure 4.2: Link failure node detection

The figure 4.2 represented actor node A3 have missing messages, then link failure problem rises with the compare between A2 and A3 nodes of energy level.

Actor node A4 is the nearest node whose energy level is high and has (A5, A6) the lowest number of links.

The Mobile Sensor Network (MSN) sensing action on actor nodes and disconnection of link in a node must be considered. Static and Dynamic sensor nodes to develop a link failure problem in actor nodes with the help of the energy level of a sensor node. Let A= {A_1, A_2, …………, A_n} be the set of actor nodes participating for the routing in a mobile sensor network. Let M_1 and M_2 be a pair of mobile nodes using sensors in A as a neighbour nodes. Data packets are to be routed from M_1 to M_2 through an optimally chosen set $A' \subset A$ of neighbour actor nodes by forming communication links.

Let E^i_{max} and E^j_{min} denote the maximum and minimum actor node energies at Actor A_i and A_j. Then the shortest route from m_1 to m_2 will be optimal if

$$E^{\,i}_{max} - E^{j}_{min} < \xi(\delta M_k) \qquad \text{--------------} \qquad 4.1$$

Where ξ zero or inversely proportional to energy nodes will favour the formation of routes through high-energy nodes. (δM) is the difference between the shortest routes from A_i to M_k.

Let the maximum energy of neighbour actor node route denote the one obtained by following the maximum energy nodes from m_1 to m_2 such that a route is formed. The maximum energy of neighbour actor node route will be optimal if

$$(\delta E) > \xi(l_d - l_s) \qquad \text{--------------------} \qquad 4.2$$

Where (δE) is the difference in energies between the maximum and minimum of neighbour actor nodes of A_i.

The l_d and l_s are the lengths of the maximum energy and shortest routes from A_i, respectively.

Energy efficiency of a sensor node is there in maintaining a backup node and in creating a link between two or more sensor nodes.

4.3.3. Selection of node for replacement

The node which is selected for replacement should have high energy and should be nearest to the failure node. The selected node for replacement should have less links to remaining nodes. If the static node detects energy loss in a particular node then it informs the dynamic node that the particular node's energy is about to drain. The static node intimates the dynamic node through signals. The dynamic node, after receiving the information, searches for a node which is nearest to the failure node and whose energy is high. The dynamic node selects a node for replacement based on priority.

The dynamic node which is in mobility searches for a node which is nearest to the failure node. The dynamic node finds a node whose energy level is high and who has lesser links when compared to other nodes. When the dynamic node replaces the failure node with another node, that particular node takes all the backup from the failure node. The node which took backup will do all the functionalities of the failure node until the failure node has retained its energy. When the failure node has regained all its energy, it will come back to its position. The static node and the dynamic node are the main functionalities done with the help of Check Point Route Recovery (CPRR) algorithm.

4.3.4. Network Topology Management Technique

The node replacement is done by Network Topology Management (NTM) technique. The Network Topology Management technique is helps to maintain the link between the nodes when energy loss is detected in a particular node. During the node replacement time, there are possibilities for the failure of direct links between nodes. In such cases the NTM technique to maintain the links between the nodes without affecting the packet transmission.

The network topology management technique is also be considered as failure management process. Network topology management must function as self-healing and serve as a failure handling service.

A sensor has m_1 mobile neighbour nodes it can communicate with m2 mobile neighbour nodes. During node replacement time, the NTM operates some sensor nodes do not stop working and loss their link functionality. The network topology management will calculate the distance between m_1 and m_2 nodes communication coverage range (R). It will recalculate the distance threshold (d_{th}) and sensing radius(r) of m_1, m_2 mobile nodes, and then follow the replaced procedure to adjust their links using the following:

$$R_2 = R_1.\frac{m_1+1}{m_2+1} \qquad \text{----------------4.3}$$

$$d_{th2} = \sqrt{\frac{2}{\sqrt{3}}}R_2 = \sqrt{\frac{m_1+1}{m_2+1}}\ .d_{th1} \qquad \text{--------------- 4.4}$$

$$r_2 = \frac{d_{th2}}{\sqrt{3}} = \sqrt{\frac{m_1+1}{m_2+1}}\ .r_1 \qquad \text{---------------- 4.5}$$

where all subscripts “1” refer to the value before self- healing process starts, and the subscripts “2” refer to the new calculated value.

The network topology management technique is structured by repositioning nodes from the various segments in order to re-establish connectivity. This process takes place continuously, due to the rush environment, limited energy and hardware resources in Mobile Sensor Network.

4.4. Check Point Route Recovery algorithm

The CPRR algorithm well suits for route reestablishment based on energy level of sensor nodes in the MSNs. The route discovery process of mobile sensor nodes configures in every route. The process of CPRR algorithm is divided into two phases, which are initial energy set-up phase and check point recovery phase. The working analyzer of CPRR algorithm is provided below.

4.4.1. CPRR Algorithm Analyzer

The energy value between every two sensor nodes is computed and the value obtained is the energy threshold. The packet delivery rate is computed by the one hop neighbour and the values are normalized between [0, 1].

The CPRR algorithm analyzer divided into two phases and it describes step by step, the detail information is explain in the following section.

<u>Initial Energy Set up Phase</u>

```
maxEnergy(i)= 1      //high energy as access point from sensor
minEnergy(i)=0       //low energy as access point from sensor
for each actor $A_j$ do
$A_j \longrightarrow M_i$ :Broadcast(hello)
end for
```

```
each sensor $M_i$ receives $A_j$ ::Broadcast(hello)
for each sensor $M_i$ do
    for each actor $A_j$ do
        If Energy($M_i$, $A_j$) < minEnergy(i) then
            minEnergy(i)= Energy($M_i$, $A_j$)
            minEnergyActor(i)= $A_j$
        end if
    end for
end for
for each sensor $M_i$ do
    $M_i \longrightarrow$ minEnergyActor(i)::(ACK)
end for
```

Check Point Recovery Phase

```
for each route do
    for each subnet do
        Weight(i,j)=$E_{sent}$ (i,j)*max{$E_{consume}$(i), $E_{consume}$(j)}
        route = check point( Weight(i,j) )   //link failure of route
        if $E_{remain}$ (k)≤0 then
            Break
            $M_i \xrightarrow{\text{Check point}}$ $A_j$::(Packet data )   // route rectifies in CPRR
        end if
    end for
end for
```

4.4.2. Flow diagram for CPRR Algorithm

A flow diagram describes the flow of the CPRR Algorithm working process to be executed in order to complete a task. This flow diagram consists of five main steps. The flow diagram is shown in Figure 4.3.

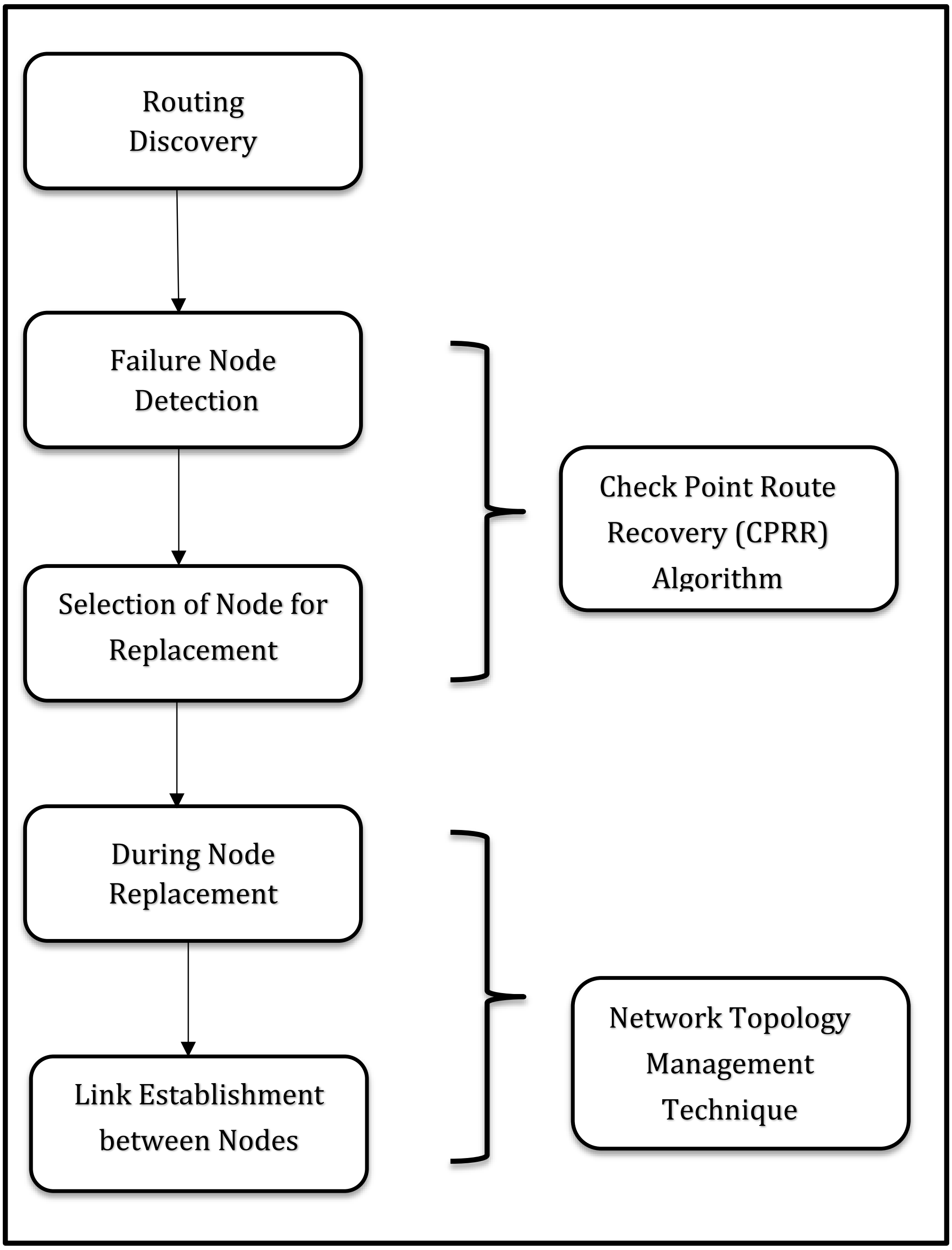


Figure 4.3: CPRR Algorithm Flow Diagram

The design of the proposed work is done with initial set up of the route discovery method of sensor nodes, and calculates the energy level of static sensor nodes. Each actor node connects to all others nodes. The communication is possible between actor node and dynamic sensor nodes. The functioning between actor, static and dynamic sensor nodes are denoted by flow lines. The functioning behaviour and specific flow of event with CPRR mechanism is represented in the following figure 4.4.

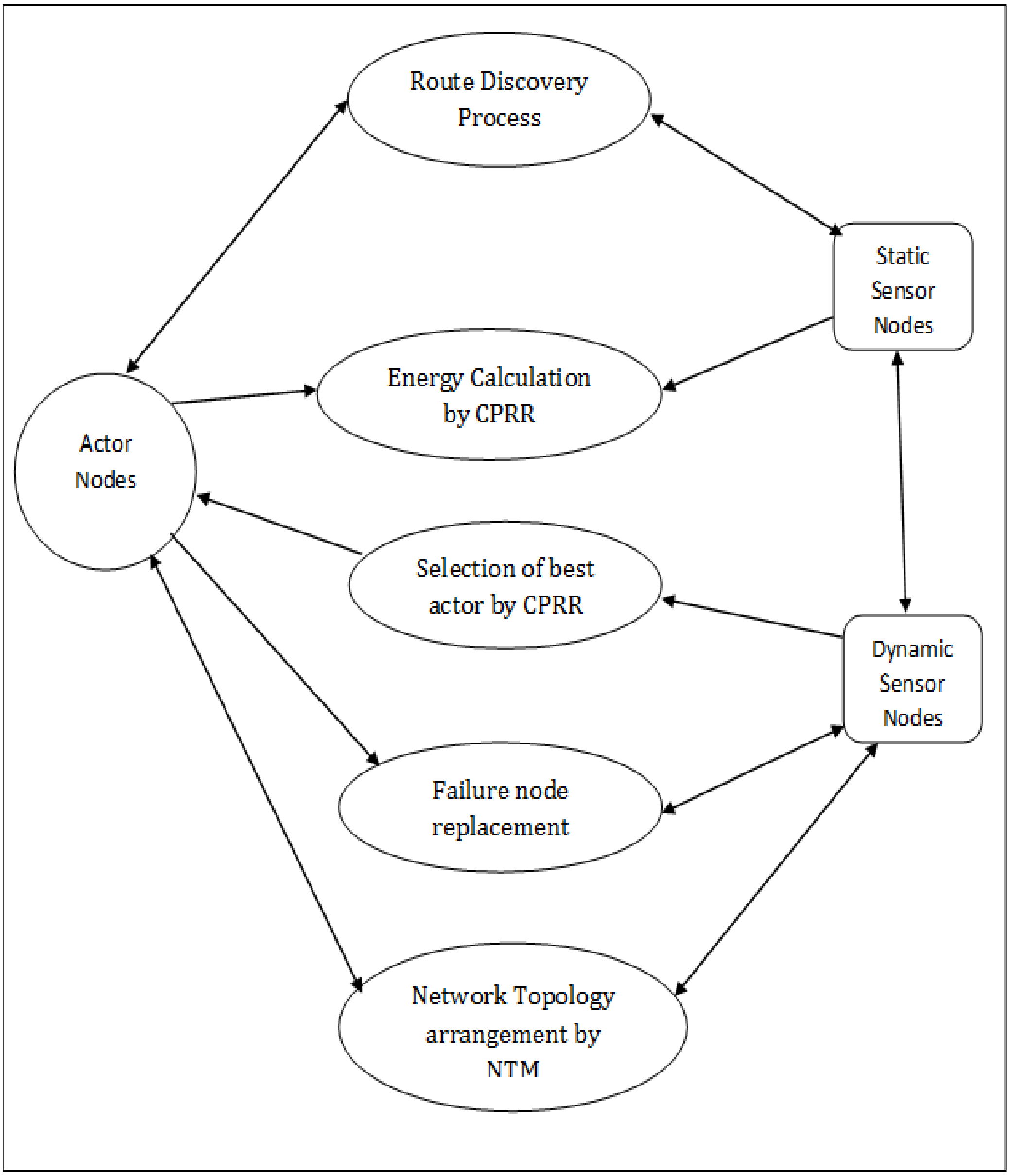


Figure 4.4: The functioning and design of the proposed CPRR mechanism

4.5. Performance Analysis

In wireless sensor communication, a measurement of framework, and an analysis of data packets are developed to level the traces. This work paves a way for improving the route establishment process of mobile sensor networks through two different approaches based on energy level of sensor nodes. In this section, the most prominent experimental results of the CPRR is compared with the first method such Proposed Ad hoc On Demand Vector (PRO-AODV) mechanism. The Check Point Route Recovery (CPRR) methodology is expected to produce better results, when compared with PRO-AODV mechanism.

4.5.1. Simulation Environment

The performance of the proposed CPRR result is evaluated. NS2 [76] is used for carrying out the simulation. The network simulator generates two types of files. First file is network animator (NAM) and second one is trace (result) file. 200 sensor nodes are distributed randomly over 500 x 500 m network region. The time taken for each simulation is 150 seconds.

The simulation parameter values of each data packet size (512bits), support of AODV routing protocol and The simulation model of energy parameter values such as initial energy (100J), radio transmission power (35mW), receive power (40mW) and idle power (7mW) of sensors. The energy consumption for switching between awake and sleeping modes is negligible and thus not considered.

4.5.2. Performance metrics

The performance metrics employed in this work are packet delivery ratio, Average delay, End to end delay, route detection time, throughput, and energy consumption by varying the number of nodes and the network lifetime analysis is made with time in a mobile sensor network. The results of the performance of CPRR mechanism is evaluated using NS-2 [76] and they are compared with those of PRO-AODV mechanism. The performance of quantitative parameter metrics results are described and after that the performances of metrics results are compared with the both two mechanisms such as CPRR, PRO-AODV for the simulation evaluation.

4.5.3. Simulation Evaluation

The performance of the proposed work is evaluated in NS2 simulation. The proposed work is simulated by using NS2 with 200 sensor nodes, which are distributed randomly configure over 500 x 500m network region. The performance of parameter metrics employed in this work such as packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption and route detection time. In simulation graphs, the analysis of first the proposed (PRO-AODV) and second proposed (CPRR) work are compared. The Proposed Ad hoc On Demand Vector (PRO-AODV) mechanism experimental results are taken for comparison purpose from chapter 3. That results are displayed in the tables 4.1, 4.3 and 4.4.

A. ***Packet Delivery Ratio:*** The ratio between the number of data packets sent and the number of data packets received at destination.

$$\text{Packet delivery ratio} = \frac{\text{Number of Packets received}}{\text{Number of Packets Sent}} \times 100 \quad \text{---------4.6}$$

Simulation Time	Packet Delivery Ratio (PDR)	End to End Delay (sec)	Average Delay x 10^{-3} (sec)	Throughput (Kbit/sec)
10	10.15	0.21	152.63	1.21
20	23.22	0.23	154.36	2.61
30	55.96	0.45	205.24	5.26
40	66.12	1.12	368.15	5.92
50	74.25	0.65	456.25	6.85
60	81.17	0.23	589.75	8.54
70	82.36	0.36	612.85	8.75
80	81.69	0.65	635.12	10.65
90	84.43	0.98	653.58	9.63
100	84.56	1.92	685.47	11.58
110	83.26	0.35	712.56	12.15
120	86.15	1.25	796.58	13.14
130	87.85	0.76	815.46	14.09
140	89.58	0.68	826.96	12.25
150	94.56	0.52	846.24	14.22

Table 4.1: Performance Metrics of PRO-AODV Results

Simulation Time	Packet Delivery Ratio (PDR)	End to End Delay (sec)	Average Delay x 10^{-3} (sec)	Throughput (Kbit/sec)
10	8.33	0.12	99.898	2.5
20	60.14	0.14	168.67	2.95
30	66.16	0.16	296.71	5.50
40	75.43	0.90	477.12	6.92
50	83.27	0.33	578.93	8.92
60	87.53	0.12	604.16	9.87
70	83.33	0.15	611.72	10.26
80	88.87	0.71	605.86	10.73
90	90.37	0.96	629.63	11.42
100	91.53	1.08	629.63	12.14
110	94.34	0.15	622.49	12.76
120	93.72	1.03	611.47	14.57
130	92.09	0.24	631.36	13.62
140	92.54	0.32	632.26	14.87
150	96.54	0.41	619.33	15.28

Table 4.2: Performance Metrics of CPRR Results

In the above table 4.1, it is observed that the PRO-AODV experimental results with different parameter metrics are recorded with respect to time. In the table 4.2 the CPRR experimental results with different performance metrics are recorded with respect to time from 10 to 150 seconds.

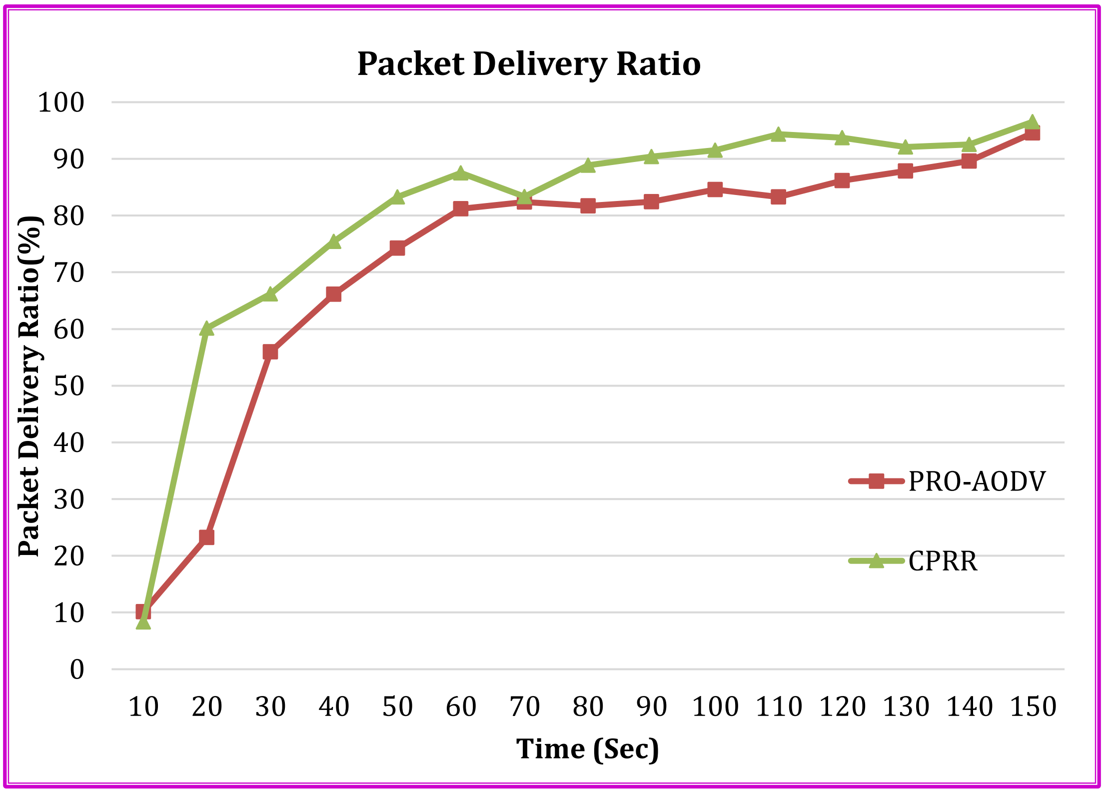


Figure 4.5: Packet Delivery Ratio with respect to Time

In the above figure simulation time is represented on x-axis varies from 10 to 150 sec. The packet delivery ratio is measured in percentage is represented on the y-axis. The CPRR method as packet delivery ratio reach 96.54% at the end of simulation. The comparison of packet delivery ratio analysis in CPRR, PRO-AODV produces 96.54%, 94 % respectively. It is evident that the CPRR provides greater packet delivery ratio than the PRO-AODV method.

B. End-to-End Delay

The time taken by the data packet to reach from source to destination node.

$$\text{End} - \text{to} - \text{End Delay} = \frac{\text{Arrival time} - \text{sent time}}{\text{Total number of connections}} \quad \text{-----------} \ 4.7$$

The following figure 4.6, shows the simulation time represented on x-axis with time from 10 to 150 sec. The End-to-End Delay is represented on y-axis.

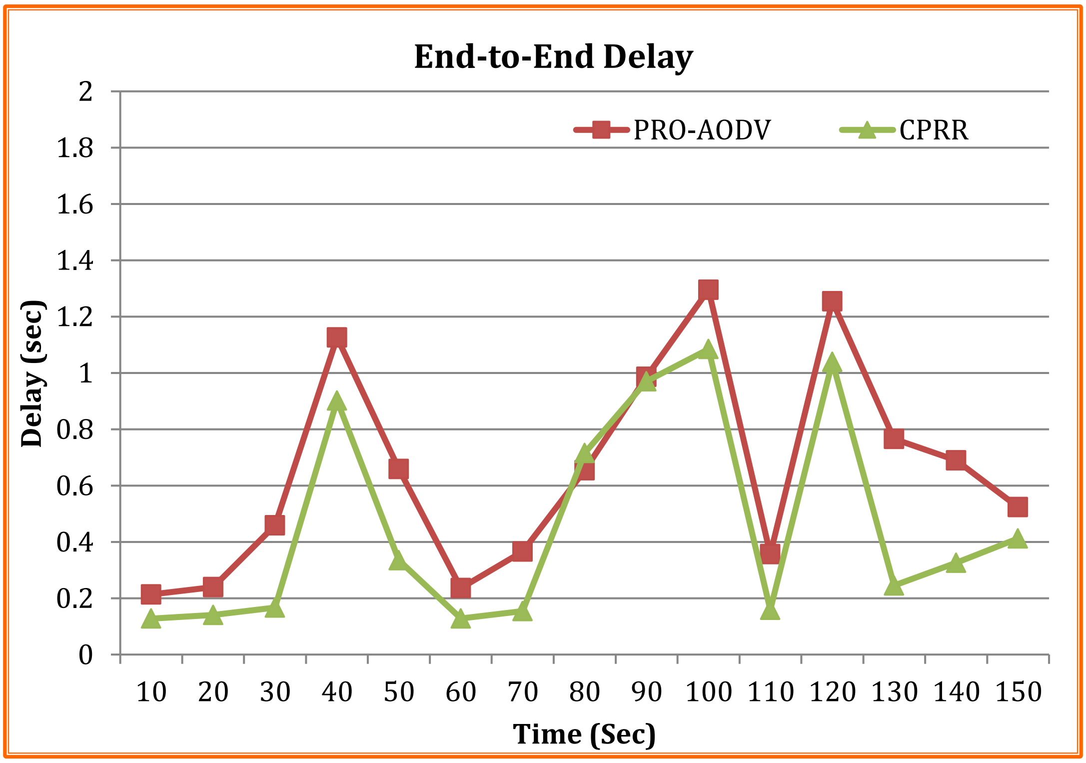


Figure 4.6: End-to-End Delay with respect to Time

In the above figure, it is clearly represented that CPRR proves a minimum End-to-End Delay rather than the PRO-AODV method. On an average, CPRR takes the least time to deliver a packet from one end to the other with 0.03 to 1.71 seconds. PRO-AODV takes 0.21 to 1.92 seconds to deliver packets from one end to the other end.

Specific point of simulation time, all the methods including CPRR consumes maximum time for End-to-End Delay transmission due to loss of energy in the nodes. The CPRR took minimum time than PRO-AODV for End-to-End Delay.

C. **Throughput:** The total number of data packets delivered per unit of time.

$$\text{Throughput} = \frac{\text{Total number of transferred packets}}{\text{Time taken (secs)}} \qquad \text{-----------} \ 4.8$$

In the following figure 4.7, the simulation time represented on x-axis varies from 10 to 150 seconds of time. The throughput is measured in Kbits per second represented on y-axis.

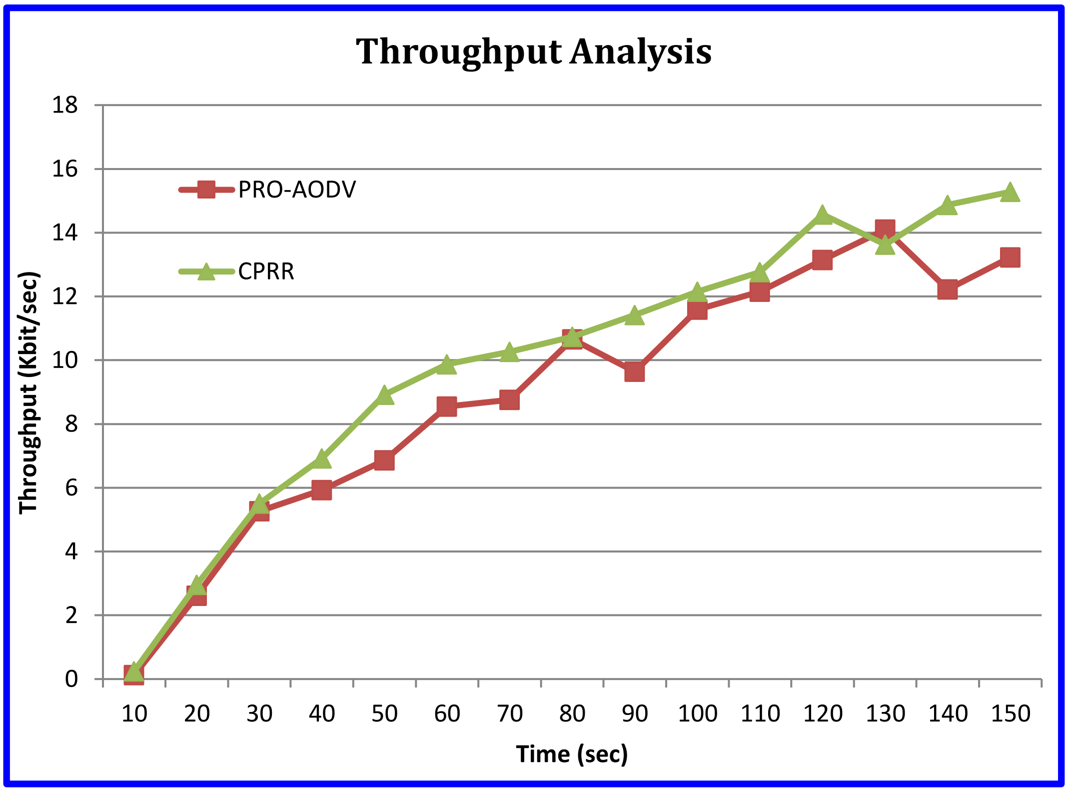


Figure 4.7: Throughput with respect to Time

In the above figure, it is inferred that the CPRR shows the highest throughput. It is clear that, the throughput is found that the proposed CPRR forwards the values of 0.25 to 15.28 Kbits per second and PRO-AODV forwards the values of 0.12 to 14.22 Kbits per second.

D. Average Delay: The time difference between the packets received time, sent time and total time taken for the packets received by all nodes.

$$\text{Average Delay} = \frac{\text{Total End to End Delay}}{\text{Total number of Packets received}} \quad \text{------------ } 4.9$$

In the following figure 4.8, the simulation time is represented on x-axis. The average delay represented on y-axis.

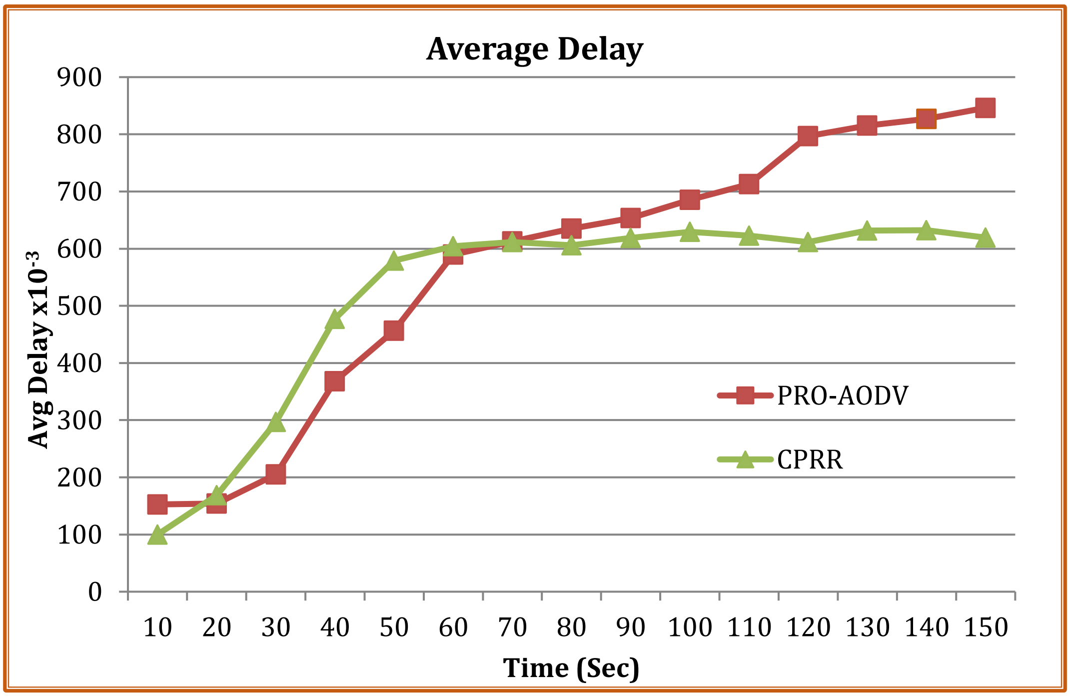


Figure 4.8: Average Delay with respect to Time

In the above figure, it is noticed that CPRR takes the minimum average delay when compared with PRO-AODV method. It is clear that CPRR takes the least time to deliver a packet from one end to the other with 0.09 to 0.61 seconds. PRO-AODV takes 0.15 to 0.84 seconds to deliver packets from one end to the other end.

E. Energy Consumption with Respect to time

Energy consumption calculates the present energy of all nodes are subtracted from initial energy of all nodes. This calculates the total energy consumed by the node with respect to time.

$$\text{Energy consumption} = \text{Initial Energy} - \text{Present Energy} \qquad 4.10$$

In the following table 4.3, it is observed that the energy consumption of PRO-AODV, CPRR results are displayed with respect to the simulation time varies from 10 to 150 seconds.

Simulation Time	Energy Consumption(J)	
	PRO-AODV	CPRR
10	12.6	10.2
20	21.2	16.0
30	26.0	21.0
40	29.0	23.0
50	33.5	28.0
60	38.5	31.0
70	42.2	36.5
80	45.0	39.2
90	49.0	42.0
100	56.0	49.0
110	62.0	54.0
120	69.0	65.0
130	78.0	74.0
140	86.0	79.0
150	95.0	83.0

Table 4.3: Energy Consumption Analysis

In the following figure 4.9, the simulation time is represented on x-axis where the energy consumption measured in joules is represented on y-axis.

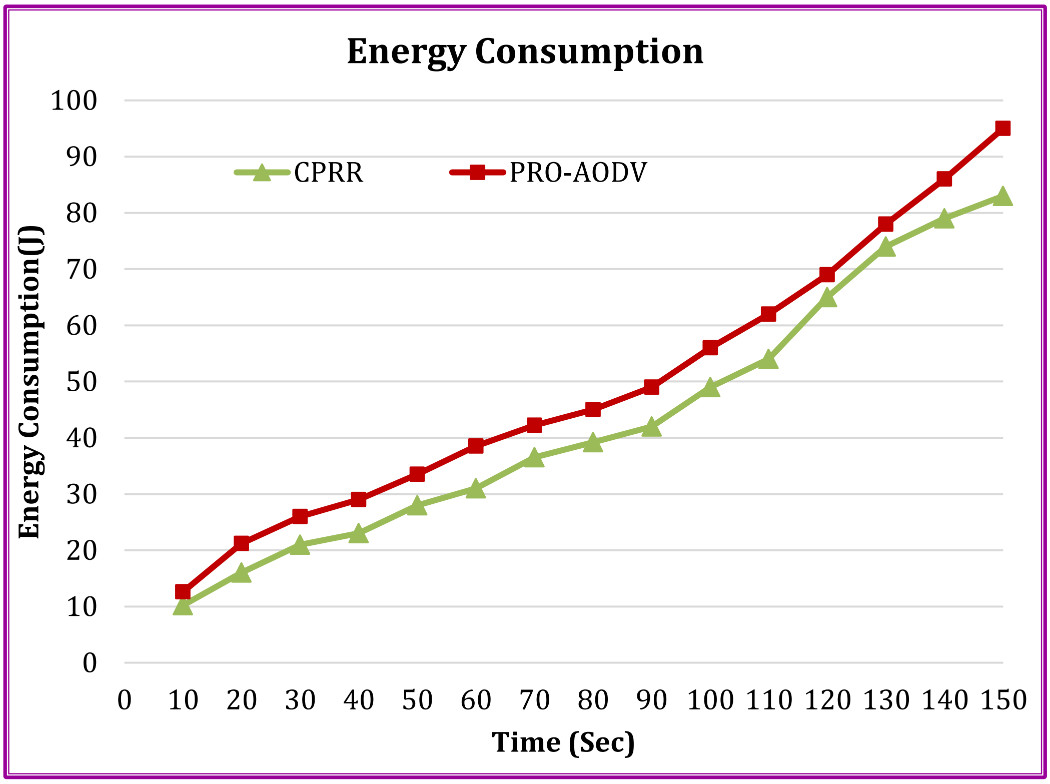


Figure 4.9: Energy Consumption with respect to Time

In the above figure, the energy consumption values of CPRR and PRO-AODV varies from 10.2 to 83 and 12.6 to 95 joules respectively. It is proved that the CPRR consumes the less energy when compared to PRO-AODV method. It is obvious that when energy consumption is less, the lifetime of network may be maximized.

The proposed approach of CPRR chooses the best route with maximum number of mobile sensor nodes. As the energy consumption is very less, the node can survive for a long time. When all nodes can survive for a long time, obviously the lifetime of a mobile sensor network is enhanced.

F. Route Detection Time with respect to Number of nodes

Route detection time is the time it takes to find an optimal route with respect to number of nodes. The formula is given the time at which the route is found is subtracted from the start time of route discovery.

$$\text{Route Detection Time} = \text{Route Discovery Time} - \text{iniatial Time} \quad \text{-------------} \; 4.11$$

Number of Nodes	Route Detection Time (sec)	
	PRO-AODV	CPRR
20	13.1	11.2
40	14.3	12.6
60	15.2	13.6
80	16.4	14.8
100	18.1	16.3
120	19.3	18.2
140	20.5	19.4
160	22.5	21.8
180	23.4	22.4
200	25.6	24.2

Table 4.4. Route Detection Time Analysis

From the table 4.4, as number of nodes is varied from 20 to 200 the route detection time is measured in seconds for CPRR and PRO-AODV. The results are tabulated.

In the following figure-4.10, the number of nodes are represented on x-axis and the route detection time measured in seconds is represented on y-axis.

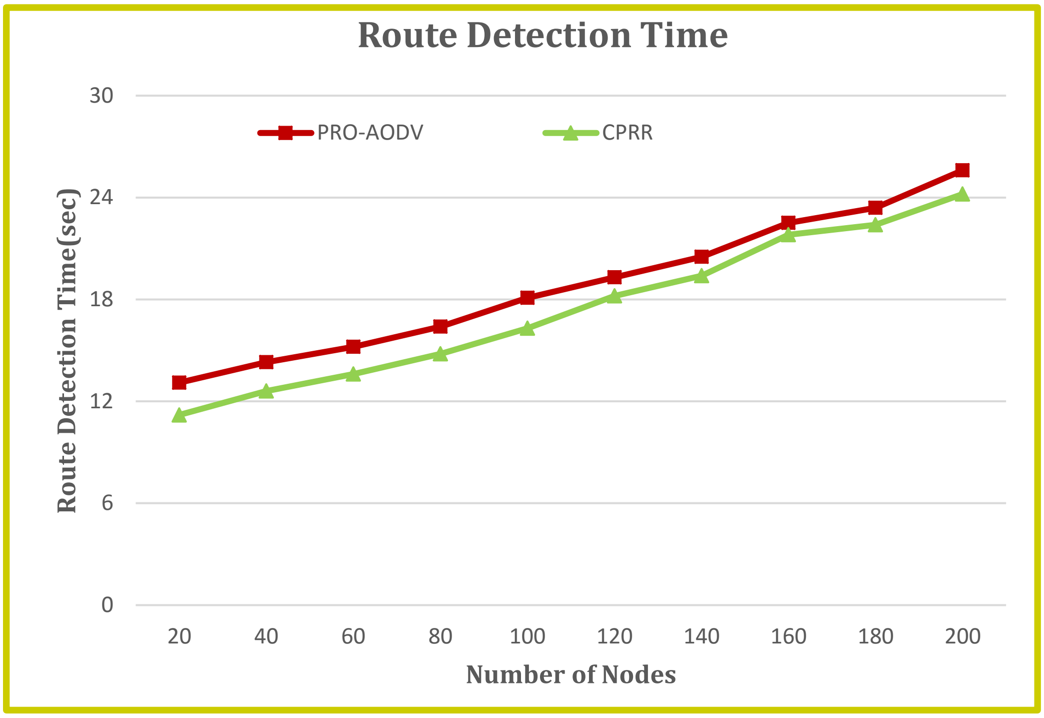


Figure 4.10: Route Detection Time with respect to Nodes

In the above figure, the CPRR frames the route in the least time (24.2) sec, whereas PRO-AODV frames the route is (25.6) sec. It is obvious that if the routes are detected in a streak, then the energy requirement is minimized.

G. Energy Drain Rate

The draining rate of energy for different sensor nodes like actor, static and dynamic nodes are calculated. The draining rate of energy in particular node is calculated by using

$$E_{DR} = \frac{E_{initial} - E_{ramain}}{(\mathrm{Tc} - \mathrm{Tp})} \qquad \text{---------------}4.12$$

Whereas, E_{DR} is Energy Draining Rate

$E_{initial}$ is Initial energy of Particular node

E_{remain} is Remaining energy of Particular node

Tc – current time

Tp - previous time

Simulation Time (sec)	Energy Drain Rate (J)		
	Actor node	Static Node	Dynamic Node
10	98.91	99.95	99.19
20	94.65	96.61	97.23
30	91.23	84.52	86.49
40	86.53	83.52	81.24
50	80.2	78.93	75.68
60	73.25	70.19	72.54
70	67.52	62.32	63.12
80	60.4	58.92	56.82
90	54.68	55.96	52.14
100	48.59	49.56	46.23
110	40.32	41.86	38.25
120	33.25	38.21	29.86
130	28.19	32.89	20.54
140	22.21	20.26	16.52
150	16.14	18.12	12.14

Table 4.5: Energy Draining Rate of all sensor nodes

In the above table 4.5, it is noticed that all the three sensor nodes have 100 joules of energy to begin with. The draining rate of energy is counted in joules. Energy draining rate of all sensor nodes decreases as the time increases and the drain rate of actor and static nodes decreases slowly when compared to the dynamic node decreasing the energy at faster rate.

In the following figure-4.11, the simulation time is represented on x-axis varies from 10 to 150 sec. The energy draining rate of all sensor nodes is measured in joules is represented on y-axis.

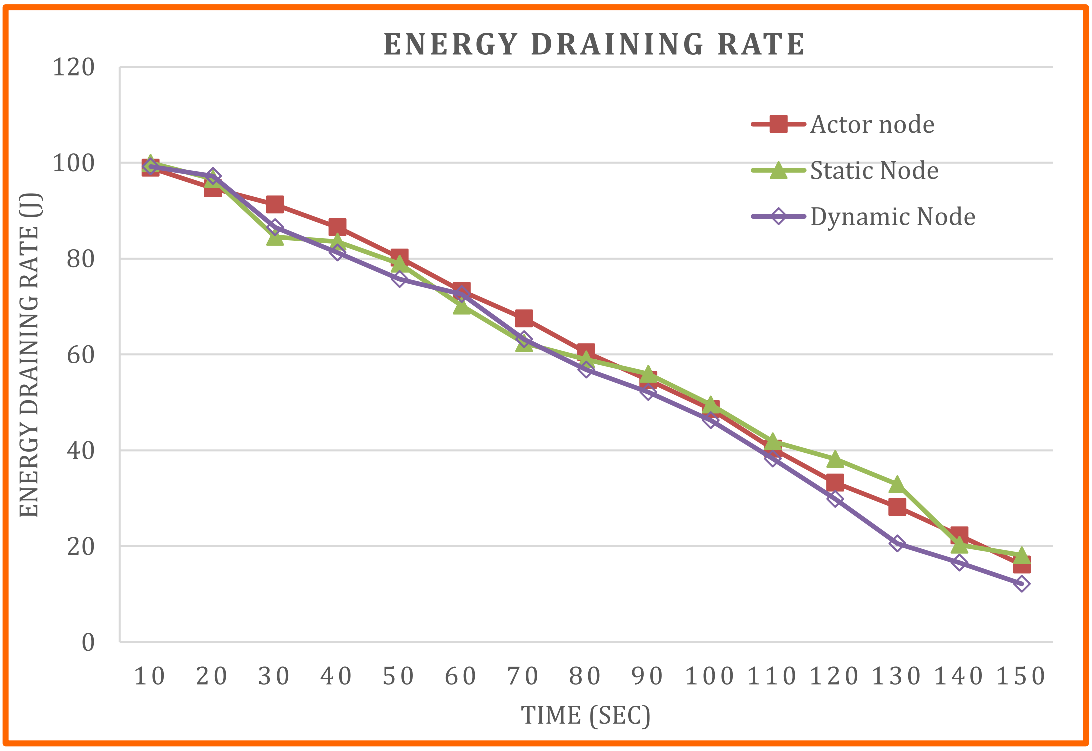


Figure 4.11: Energy Draining Rate of all sensor nodes

In the above figure, it is observed that the draining rate of energy in all the sensor nodes increases as time increases. Among the three sensor nodes, the dynamic sensor node drains energy at faster rate.

The proposed work reduces the energy consumption by detecting effective routes between the source and destination. When effective routes are framed, the data or packets can be forwarded without any overhead. The communication overhead is directly proportional to the energy requirement. Thus, the transmission is made fast and the energy is effectively utilized. The proposed approach CPRR chooses the best route with maximum number of mobile sensor nodes.

The simulated results show that the CPRR algorithm can reduce the energy consumption effectively, and also decreases route detection time for overall performance, when compare to PRO-AODV mechanism.

4.6. SUMMARY

The main emphasis of this chapter is the design of Check Point Route Recovery (CPRR) algorithm to detect failure node and replaces the nearest actor node. The CPRR algorithm proposes the steps which involve route discovery, failure node detection, and selection of node replacement for sensor node and communication links in a mobile sensor network. Network Topology Management (NTM) technique helps to maintain the links between the nodes. The proposed CPRR is to improve the route establishment process, also reduce link failure problem and design for prevention of a node failure in Mobile Sensor Networks.

The performance of CPRR approach is measured by performance metrics such as packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption, route detection time and energy drain rate. The experimental results are compared with the PRO-AODV mechanism and comparative study is represented with graphical analysis.

5.1. Introduction

This chapter presents the comparison and performance evaluation of route recovery process by using DFRR, PRO-AODV, AODV and proposed CPRR mechanisms implemented on Mobile Wireless Sensor Networks (MWSNs) for route re-establishment process.

Link failure problem is a major issue of the current wireless sensor networks due to node mobility, node energy loss or draining of battery power. The energy level of sensor nodes is calculated through check point route recovery (CPRR) mechanism. Initially, the routes are computed based on the energy level of sensor nodes and then the best route is selected by the CPRR algorithm. The CPRR mechanism overcomes the problem of low energy in a node and route rectification process for an active communication. Besides, the energy maintains the sensor activities on actor nodes and the CPRR maintains recovery of route link failure to produce optimal route connection in Mobile WSNs.

The performance comparison among three different methods are analysed by varying different time intervals of time in Network Simulator. The network simulator generates the results by implementing the above mechanism to produce efficient route re-establishment. In this research work, the performance of CPRR is compared with the performances of three other methods known as AODV routing, Proposed AODV (PRO-AODV) routing and Divert Failure Route Recovery (DFRR) routing mechanism. The comparison and performance evaluation with different performance metrics such as packet delivery ratio, end-to-end delay, average delay, throughput, energy consumption and route detection time is analysed in this chapter.

5.2. Description of Comparison Algorithms

The experimental results of the Check Point Route Recovery (CPRR) algorithm results are compared with the other methodologies such as Ad hoc On Demand Vector routing (AODV) [12], Divert Failure Route Recovery(DFRR), and improved or Proposed AODV (PRO-AODV) routing methods.

5.2.1 Ad hoc On Demand Vector (AODV) routing

In the standard AODV[12]protocol, upon a link failure, the node that detects the link failure sends an error message packet back to the source, the source then will initiate a new route discovery. This routing leads to severe control overhead, bandwidth consumptions as these are observed to be unnecessary.

5.2.2 Divert Failure Route Recovery (DFRR) routing

Divert failure route recovery process is made by concentrating on round trip path detection algorithm in mobile sensor networks. It uses Round Trip Path (RTP) algorithm to detect a failure node while going through the number of sensor nodes. The DFRR routing is compared with the proposed (CPRR) work.

5.2.3 Proposed AODV (PRO-AODV) routing

The first part of the proposed work, PRO-AODV routing maintains routing table in only one route from the source node to the destination node and re-initiates the route discovery process and route maintains the route whenever there is a link failure. The PRO-AODV routing is compared with the proposed (CPRR) work.

5.3. Performance Evaluation

In this section, the performance of the proposed work is evaluated in NS2 [76] that carries out the simulation. This work is done with different number of nodes, which are distributed randomly over 500m x 500m region. The time taken for each simulation is 150 seconds. The experimental results of the proposed Check Point Route Recovery (CPRR) work is compared with other mechanisms such as Ad hoc On Demand Vector routing (AODV) [12], Divert Failure Route Recovery (DFRR), and Proposed Ad hoc On Demand Vector (PRO-AODV) mechanisms. The following paragraph discusses network simulator validation support of TCL (Tool Command Language), OTcl (Object Tcl) and C++ languages.

5.3.1. Simulator Validation

The simulator must enable a user to represent a network topology, specifying the nodes on the network, the links between those nodes and the traffic between the nodes. The public domain event-driven network simulator (NS-2) developed at UC Berkeley is available on UNIX, Free BSD and Windows OS platforms. NS-2 [76] is currently a part of the VINT (Virtual Inter-Network Test bed) project [VINT] and is designed to simulate small-scale networks. NS-2 is based on three languages: TCL writes simulation script, OTCL defines simulation parameter and C++ implements the schedulers. The output of trace files produced by NS-2. They are general format trace files, Network Animation format files, and personalized trace files. NS-2 is an open source software, complex scenarios can be easily tested, and results can be quickly obtained and is supported by platform and popular protocols.

5.3.2. Simulation Setup

The performance of the proposed work is evaluated in NS2 [76] and is used for carrying out the simulation. This experimental simulation area is in 500m*500m with the space of 200 random configuration sensor nodes. The time taken for total simulation is 150 seconds. To define option for simulation environment, various distribution of energy parameter values in wireless transmission network area are used. The simulation model of energy parameter values such as initial energy, radio transmission power (Tx), receive power (Rx) and idle power of sensors. The energy consumption for switching between awake and sleeping modes is negligible and thus not considered.

5.4. Comparison on Performance Metrics

In this section, the performance of the parameter metric work is evaluated. NS2 is employed for carrying out the simulation. This work is simulated by using NS2 with 200 sensor nodes, which are distributed randomly configure over 500 x 500m network area. The time taken for each simulation is 150 seconds. The performance metrics employed in this work such as packet delivery ratio, end-to-end delay, average delay, throughput, energy consumption, and route detection time analysis.

5.4.1. Packet Delivery Ratio

Packet delivery ratio is the rate of packets sent to the destination with respect to the total simulation time completed. Packet delivery ratio is calculated by using $\text{Packet delivery ratio} = \frac{\text{Number of Packets received}}{\text{Number of Packets Sent}} \times 100.$

The table 5.1, shows the experimental results of the packet delivery ratio of AODV, DFRR, PRO-AODV and CPRR against simulation time (10-150 Seconds). On an average, CPRR provides the packet delivery ratio value and it reaches 96.54% at the end of the simulation. The comparison of other methods, PRO-AODV, AODV, and DFRR provide 94.56%, 92.54% and 88.96% respectively.

TIME (Sec)	Packet Delivery Ratio (%)			
	AODV	DFRR	PRO-AODV	CPRR
10	9.85	7.69	10.15	8.33
20	35.21	54.92	23.22	60.14
30	46.56	66.17	55.96	66.16
40	69.12	74.05	66.12	75.43
50	75.28	72.64	74.25	83.27
60	80.29	78.51	81.17	87.53
70	83.45	76.17	82.36	83.33
80	84.75	77.06	81.69	88.87
90	85.42	78.09	84.43	90.37
100	85.21	79.05	84.56	91.53
110	84.95	81.64	83.26	94.34
120	86.75	81.25	86.15	93.72
130	88.24	85.76	87.85	92.09
140	89.85	87.33	89.58	92.56
150	92.54	88.96	94.56	96.54

Table 5.1: Analysis of Packet Delivery Ratio

The comparative performance of the CPRR method provides more packet delivery ratio than the other methods such as AODV, DFRR and PRO-AODV methods.

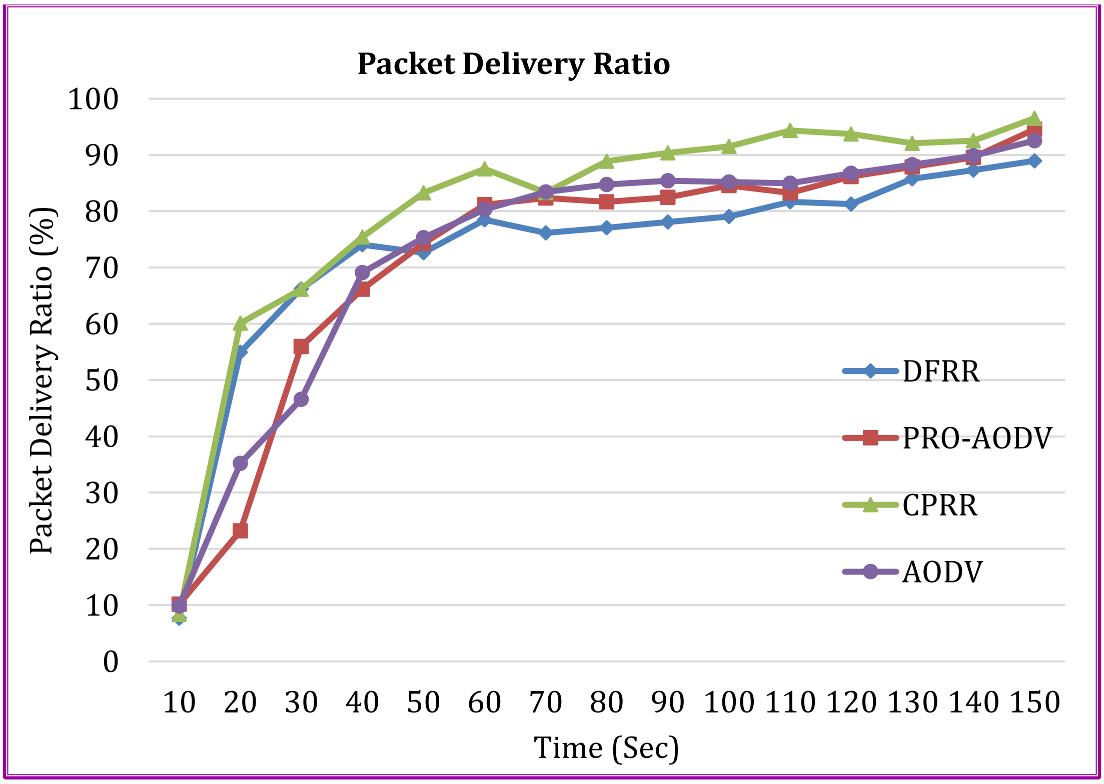


Figure 5.1: Packet Delivery Ratio

From the figure 5.1, it is observed that the packet delivery ratio increases in CPRR method with respect to simulation time whereas in other three methods such as AODV, DFRR and PRO-AODV packet delivery ratio decreases.

5.4.2. End-to-End Delay

End-to-End delay is the time taken by the packet to reach its destination from the source node. End-to-End delay is calculated by using

$$\text{End} - \text{to} - \text{End Delay} = \frac{\text{Arrival time} - \text{sent time}}{\text{Total number of connections}}$$

Time (Sec)	End to End Delay (sec)			
	AODV	DFRR	PRO-AODV	CPRR
10	0.18	0.30	0.21	0.12
20	0.14	0.35	0.23	0.14
30	0.32	0.63	0.45	0.16
40	1.02	1.25	1.12	0.90
50	0.58	0.79	0.65	0.33
60	0.15	0.17	0.23	0.12
70	0.24	0.67	0.36	0.15
80	0.45	0.98	0.65	0.71
90	0.85	1.08	0.98	0.96
100	0.95	1.43	1.29	1.08
110	0.25	0.61	0.35	0.15
120	1.15	1.25	1.25	1.03
130	0.34	1.16	0.76	0.24
140	0.56	1.02	0.68	0.32
150	0.65	0.89	0.52	0.41

Table 5.2: Analysis of End-to-End Delay

The table 5.2, shows the experimental results of the End-to-End delay of AODV, DFRR, PRO-AODV and CPRR against simulation time (10-150 Seconds). It is observed that the CPRR shows the better results when compared with other methods. Specific point of simulation time, all the methods including CPRR consumes peak time more than normal for End-to-End delay transmission due to loss of energy in the nodes.

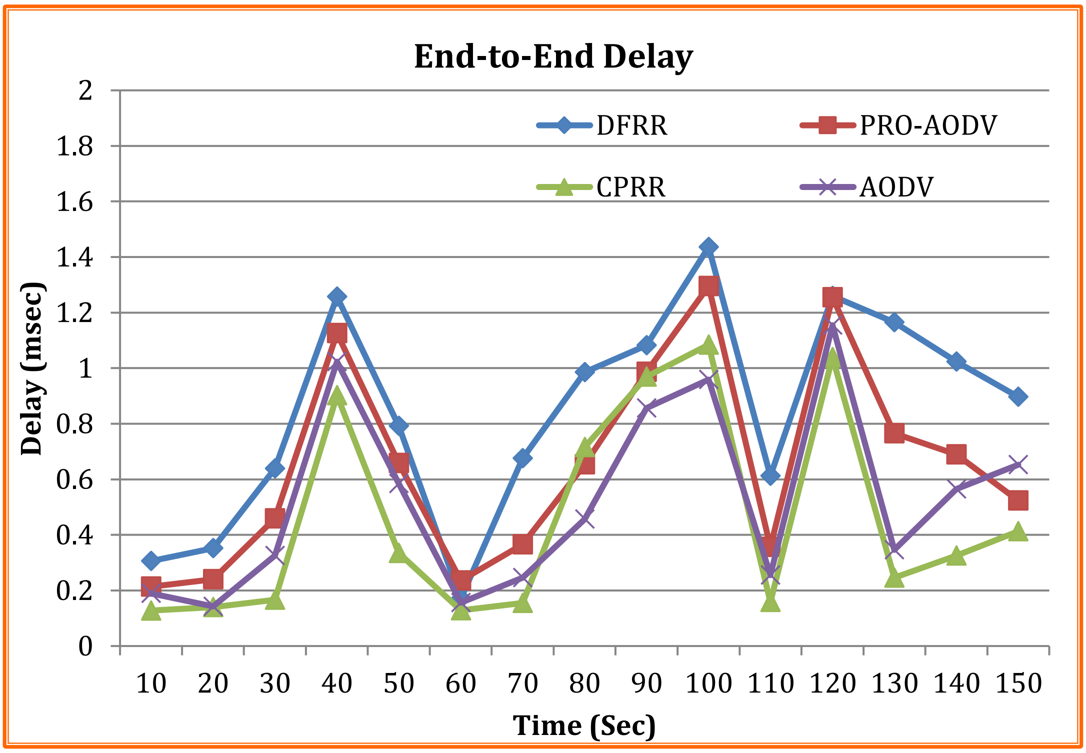


Figure 5.2: End-to-End Delay

The figure 5.2, shows that CPRR proves a minimum end to end delay rather than the other methods. On an average, CPRR takes the least time to deliver a packet from one end to the other i.e., 0.12 to 1.08 seconds. PRO-AODV takes 0.21 to 1.92 seconds to deliver packets from one end to the other. The AODV with the delay of 0.24 to 1.15 seconds. Finally, DFRR takes more time to deliver a packet and it consumes 0.17 to 1.73 seconds.

The comparison of end-to-end delay analysis of data packets reaches minimum time in CPRR method when compared with AODV, DFRR, and PRO-AODV routing methods.

5.4.3. Throughput

Throughput is the amount of data transferred per unit of time. Throughput is calculated by using $\text{Throughput} = \frac{\text{Total number of transferred packets}}{\text{Time taken (secs)}}$

The table 5.3, shows the experimental results of the throughput of AODV, DFRR, PRO-AODV and CPRR against simulation time from 10-150 seconds. It observed that, the throughput is found that the proposed CPRR forwards 2.5 to 15.28 Kbits per second. The PRO-AODV forwards 1.21 to 14.22 Kbits per second. DFRR forwards 1.44 to 13.21 Kbits per second. Finally, AODV forwards 2.35 to 12.16 Kbits per second. The throughput of CPRR is high among all other mechanisms.

Time (Sec)	Throughput(Kbits/sec)			
	AODV	DFRR	PRO-AODV	CPRR
10	2.35	1.44	1.21	2.5
20	2.15	2.55	2.61	2.95
30	5.12	4.64	5.26	5.50
40	4.82	3.92	5.92	6.92
50	5.29	4.93	6.85	8.92
60	8.04	7.69	8.54	9.87
70	8.61	7.80	8.75	10.26
80	9.85	8.50	10.65	10.73
90	9.43	9.34	9.63	11.42
100	10.95	9.93	11.58	12.14
110	11.68	11.16	12.15	12.76
120	11.53	12.89	13.14	14.57
130	12.14	12.78	14.09	13.62
140	13.23	11.42	12.25	14.87
150	12.16	13.21	14.22	15.28

Table 5.3: Analysis of Throughput with Respect to Time

In the following figure 5.3, the simulation time is represented on x-axis. The throughput measured in Kbits per second is represented on y-axis.

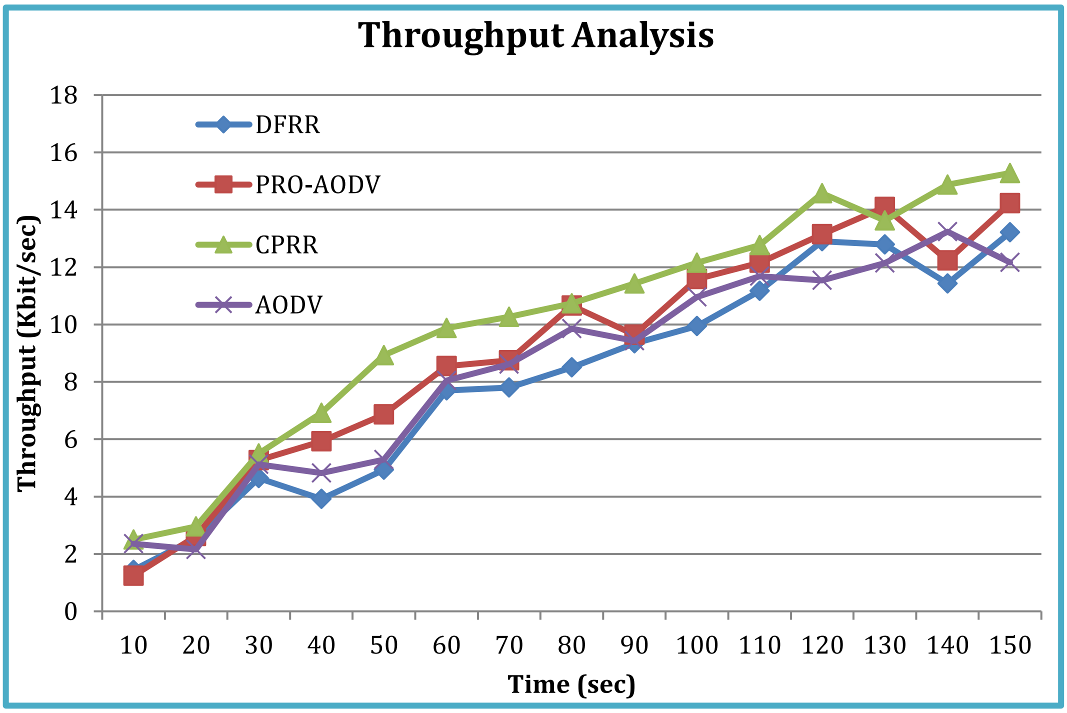


Figure 5.3: Throughput with Respect to Time

The figure.5.3 shows that as simulation time increases, the throughput also increases. The CPRR experimental results shows the highest throughput compared with the results of AODV, DFRR and PRO-AODV methods.

5.4.4. Average Delay

The time difference between the packets received time, sent time and total time taken for the packets received by all nodes. Average delay is calculated by using

$$\text{Average Delay} = \frac{\text{Total End to End Delay}}{\text{Total number of Packets received}}$$

The table 5.4, shows the experimental results of the average delay of AODV, DFRR, PRO-AODV and CPRR against simulation time varies from 10-150 seconds. On an average, CPRR takes the least time to deliver a packet from one end to the other with 0.09 to 0.61 seconds. PRO-AODV takes 0.15 to 0.84 seconds to deliver packets from one end to the other. This is followed by AODV with a delay of 0.12 to 0.76 seconds. Finally, DFRR takes the maximum time to deliver a packet and takes 0.2 to 0.95 seconds.

TIME (Sec)	Average Delay x 10^{-3}			
	AODV	DFRR	PRO-AODV	CPRR
10	121.54	205.85	152.63	99.898
20	135.24	206.36	154.36	168.67
30	196.25	362.71	205.24	296.71
40	375.36	516.86	368.15	477.12
50	465.28	500.85	456.25	578.93
60	503.21	546.34	589.75	604.16
70	625.41	609.50	612.85	611.72
80	654.20	713.98	635.12	605.86
90	671.28	767.22	685.47	629.63
100	663.10	767.22	692.80	629.63
110	692.80	802.52	712.56	622.49
120	668.20	982.19	796.58	611.47
130	706.84	999.12	815.46	631.36
140	742.56	972.91	826.96	632.26
150	768.24	950.04	846.24	619.33

Table 5.4: Analysis of Average Delay with respect to Time

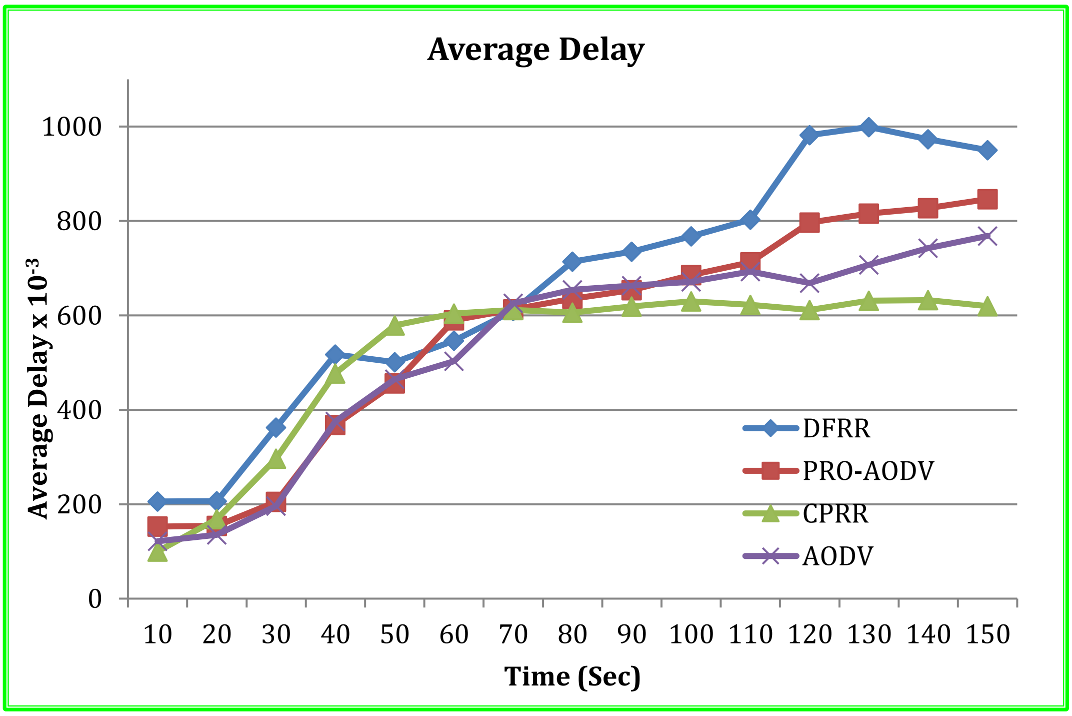


Figure 5.4: Average Delay with respect to Time

From the figure 5.4, it is noticed that CPRR takes the minimum average delay when compared with other methods. The figure also represents that the average delay incurred in CPRR method is shorter time when compared to AODV, DFRR and PRO-AODV methods in a sensor network with fast moving nodes. The

CPRR routing process average delay values is slightly more effective than PRO-AODV routing process.

5.4.5. Energy Consumption with Respect to Time

Energy consumption calculates the present energy of all nodes are subtracted from initial energy of all nodes. This calculates the total energy consumed by the node with respect to time. Energy consumption is calculated by using $\text{Energy consumption} = \text{Initial Energy} - \text{Present Energy}$

The table 5.5 shows that the energy consumption results of AODV, DFRR, PRO-AODV and CPRR against simulation time varies from 10-150 seconds. On an average, it is found that CPRR consumes minimum energy and it ranges from 10.2 to 83 joules. PRO-AODV consumes 12.6 to 95 joules. DFRR consumes 15.2 to 85.5 joules. Finally, AODV consumes the maximum energy from 15.2 to 98 joules.

Time (Sec)	Energy Consumption(J)			
	AODV	DFRR	PRO-AODV	CPRR
10	15.2	11.5	12.6	10.2
20	25.1	16.6	21.2	16.0
30	32.0	22.0	26.0	21.0
40	36.0	27.5	29.0	23.0
50	40.2	29.7	33.5	28.0
60	49.0	32.2	38.5	31.0
70	51.0	38.6	42.2	36.5
80	53.0	41.7	45.0	39.2
90	58.0	43.5	49.0	42.0
100	65.0	52.3	56.0	49.0
110	70.0	60.2	62.0	54.0
120	74.0	69.5	69.0	65.0
130	83.0	75.8	78.0	74.0
140	91.0	82.6	86.0	79.0
150	98.0	85.5	95.0	83.0

Table 5.5: Analysis of Energy Consumption with Respect to Time

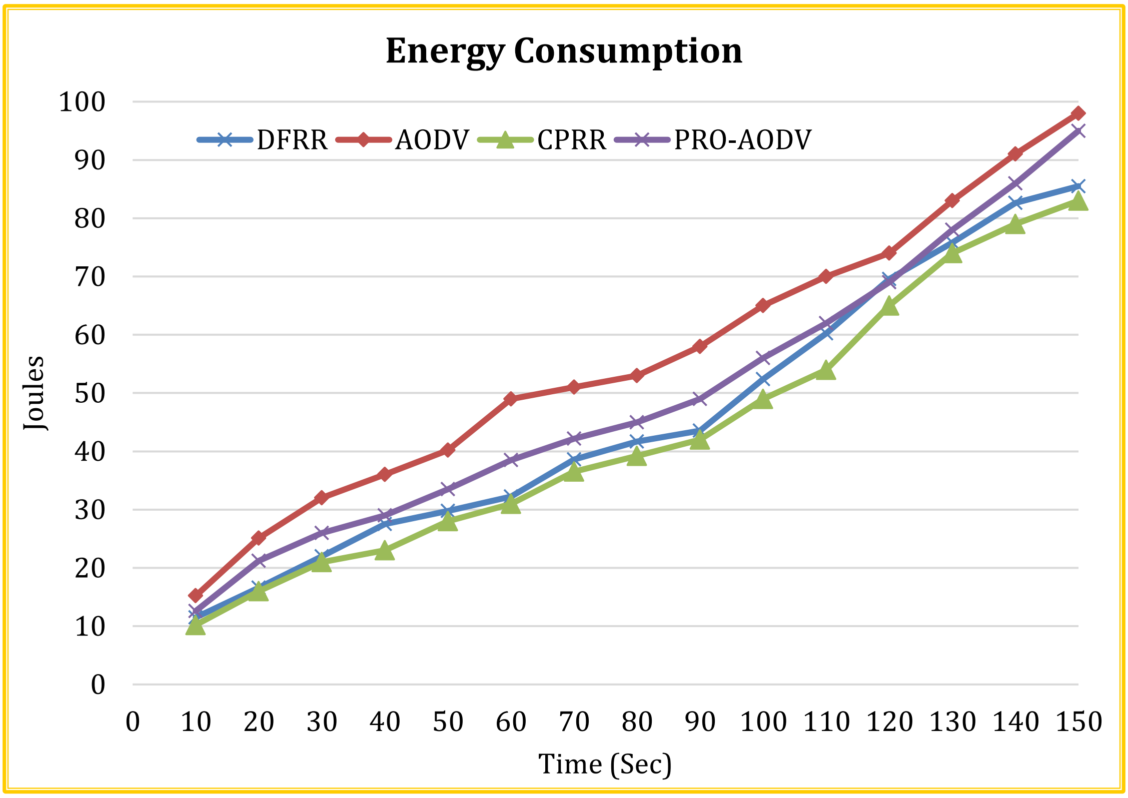


Figure 5.5: Energy Consumption with respect to Time

The figure 5.5 shows that the simulation time represented in graph on x-axis varies from 10 to 150 sec. The energy consumption is measured in joules is represented on y-axis.

From the above it is clear that the CPRR method consumes the least energy when compared to PRO-AODV, DFRR, and AODV. It is obvious that if the energy consumption is less, then the network lifetime is maximized.

The energy consumption analysis includes every neighbour node i.e., as the time increases, energy consumption each node is also increases. The energy consumption of CPRR mechanism is better than PRO-AODV mechanism and the recovery of route process is also faster, as a result, the mobile sensor network becomes stronger in functioning as energy consumption is reduced.

5.4.6. Route Detection Time with Respect to nodes

Route detection time is the time it takes to find an optimal route with respect to number of nodes. The formula is given the time at which the route is found is subtracted from the start time of route discovery. Route detection time is calculated by using

$$\text{Route Detection Time} = \text{Route Discovery Time} - \text{Initial Time}$$

From the table 5.6, as the number of nodes varies from 20 to 200. The time taken by CPRR to find route detection is minimum when compared with other methods. The CPRR takes 11.2 to 24.2 seconds, where PRO-AODV takes 13.1 to 25.6 seconds, DFRR takes 16.3 to 28.8 seconds, and finally, AODV takes the maximum time to find route detection time i.e., 18.1 to 30.4 seconds.

Number of Nodes	Route Detection Time (sec)			
	AODV	DFRR	PRO-AODV	CPRR
20	18.1	16.3	13.1	11.2
40	19.2	17.4	14.3	12.6
60	20.5	18.6	15.2	13.6
80	21.3	17.5	16.4	14.8
100	22.8	19.7	18.1	16.3
120	23.4	20.5	19.3	18.2
140	25.4	21.6	20.5	19.4
160	26.8	23.1	22.5	21.8
180	28.9	24.8	23.4	22.4
200	30.4	28.8	25.6	24.2

Table 5.6: Analysis of Route Detection Time with respect to nodes

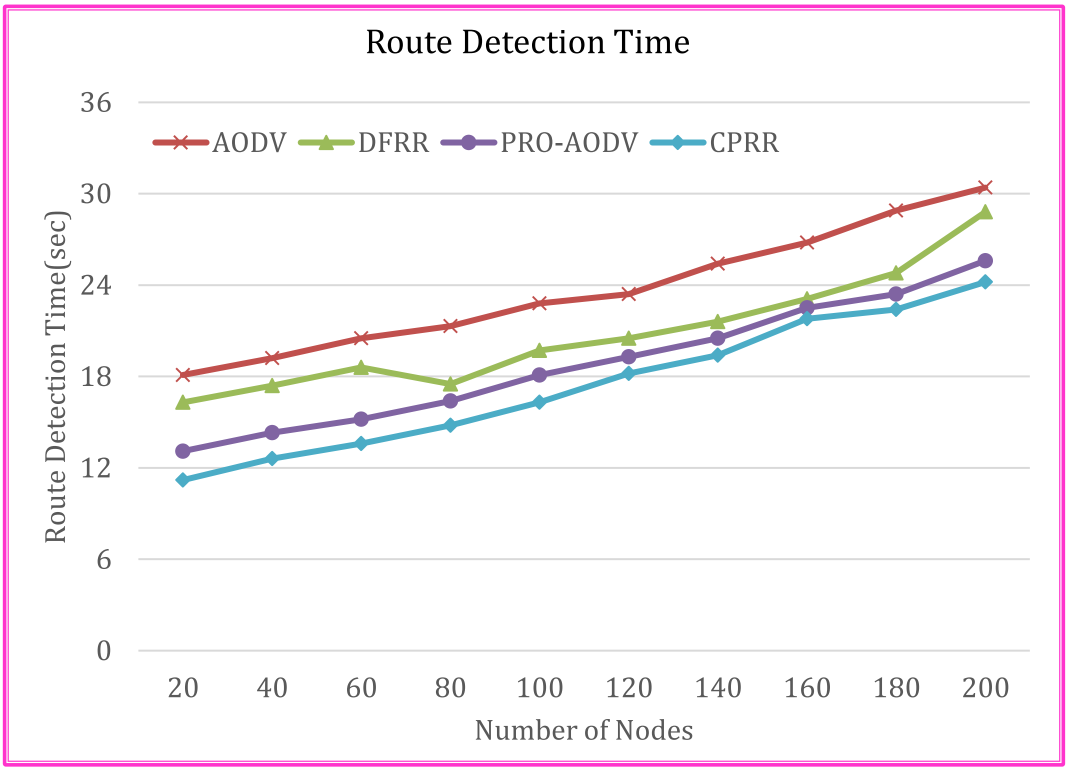


Figure 5.6: Route Detection Time with respect to Nodes

From the figure 5.6 shows that the simulation time is represented on x-axis. The route detection time measured in seconds is represented on y-axis.

The above figure is evident that the CPRR method finds out the route in the minimum time, when compared with AODV, DFRR and PRO-AODV methods. The CPRR takes minimum time to the routes that are detected in a streak, where the energy requirement is minimized.

The route time detection analysis includes processing and queuing delay in each neighbouring node i.e. the time elapsed until a demanded route is available. The CPRR takes the lowest time to establish the route and the recovery of route process is done at a faster pace when compared to DFRR, AODV, and PRO-AODV.

The simulated results show that the CPRR method can reduce the energy consumption of the sensor nodes effectively, and also decrease the route detection time analysis for overall performance is compared with PRO-AODV, DFRR, and AODV methods.

5.5. Summary

The entire theme of this chapter is on performance evaluation of CPRR, for improvement of route establishment process and to reduce the link failure problem. The effectiveness of CPRR is measured by comparing other methods. The experimental results obtained through CPRR, AODV, DFRR and PRO-AODV on route recovery process are tabulated. The performance of the metrics such as packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption and route detection time are effectively studied. Each performance metrics of CPRR is effectively compared with the existing methods known as AODV, DFRR, and PRO-AODV routing methods. The clear analysis is presented in graphical representation.

6.1. Introduction

The major issue of failure node, link failure routing problem and route recovery process are based on energy efficiency of sensor nodes in a Mobile Sensor Network (MSN). An MSN can be easily deployed irrespective of the environment where the human intervention is not possible. Since replacement or recharge of batteries is not practically possible all the times, this problem needs, prevention of node failure is being done by using Check Point Route Recovery (CPRR) algorithm and network topology management.

The three mechanisms (i.e., DFRR, PRO-AODV, and CPRR) are combined together to find the best route for packet transmission without the loss of energy and to detect the node whose energy level is about to drain by using a static node which intimate dynamic node about the energy drop in a particular node. The dynamic node searches for the nearest node whose energy level is high and also has less number of links. This is done with the help of CPRR. Network Topology Management technique maintains the path between all the nodes without breaking for better communication. The link is re-established even after the replacement of the node without affecting loss of data packet transmission. CPRR mechanism can reduce the average end-to-end delay effectively, and also increases throughput, packet delivery ratio in the overall performance.

6.2. Conclusion

The entire theme of the thesis is presented in **six chapters**. The **first chapter** is particularly concerned with the key concepts of sensor node operations. In addition to that, it deals with the **introduction** of WSN, MWSN, architecture, applications, challenges, energy management, and the quality of service matters in detail.

In the **second chapter**, the **Review of Routing Schemes** in WSNs to the recovery process of related work and an overview of literature survey in routing, routing schemes with the fields namely ‘Energy Efficient Techniques’ and highlights their subareas like Data Reduction, Routing schemes, and Topology Control are explained elaborately.

The **third chapter** presents “**Route Recovery Process of DFRR and PRO-AODV mechanisms** “ the description of Divert Failure Route Recovery (DFRR) mechanism which is used round trip path algorithm to improve the route rectification in Mobile Sensor Network. It also gives details about Proposed AODV (PRO-AODV) mechanism which is used to improve the link failure route rectification in Mobile Wireless Sensor Networks (MWSNs).

The **fourth chapter** illustrates **Route Recovery Process of CPRR Algorithm** is used to reduce the energy consumption, link failure problem and improve the route re-establishment process. The CPRR is compared with other mechanisms namely DFRR, AODV and PRO-AODV measured by the performance metrics such as packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption, route detection time, and energy draining rate.

From the experimental results supported by Table 4.1 to 4.5 the following observations are:

i. The percentage of Packet delivery ratio in CPRR varies from 60.14% to 96.54% noticed within the stipulated time.

ii. End-to-end delay of CPRR consumes a minimum of 0.41 seconds to reach the destination whereas PRO-AODV consumes 0.52 seconds.
iii. CPRR takes minimum time to deliver packets by total end to end delay when compared with PRO-AODV. Efficiency is observed in CPRR to reduce average delay.
iv. CPRR and PRO-AODV have 15.28 and 14.22 Kbits per second respectively. Throughput efficiency is clearly observed in CPRR.
v. When compared with PRO-AODV, CPRR consumes less energy that is 10 to 83 joules whereas PRO-AODV consumes 12 to 95 joules.
vi. It is a noticed evident that CPRR takes minimum time to detect the route whereas PRO-AODV stands in seconds.
vii. It is clear that the energy drain rate of all nodes are effectively reduced with implementation of the CPRR mechanism.

The **fifth chapter** elucidates the description of the **performance evaluation** of proposed Check Point Route Recovery (CPRR) mechanism which is measured by experimental results. The CPRR mechanism is compared with the other mechanisms of DFRR, AODV and PRO-AODV which are measured by performance metrics such as packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption, and route detection time.

From the experimental results supported by Table 5.1 to 5.6 the following observations are noticeable.

i. The percentage of packet delivery ratio in CPRR reaches to highest value 96.54% when compared with PRO-AODV, AODV, and DFRR. Where the packet delivery ratio of PRO-AODV, AODV and DFRR is

94.56%, 92.54% and 88.96% respectively. Overall CPRR is showing better delivery rate.

ii. CPRR takes 0.12 sec minimum time to reach the destination of end-to-end delay when compared to other mechanisms known as DFRR, AODV, and PRO-AODV takes 0.65, 0.89 and 0.52 respectively.

iii. Average delay of CPRR is minimum to reach packets to the destination nodes, whereas DFRR, AODV and PRO-AODV stands next to CPRR.

iv. In connection with throughput, CPRR forwards 2.5 to 15.28 Kbits per second whereas PRO-AODV forwards 1.21 to 14.22, DFRR forwards 1.44 to 13.21 and AODV forwards 2.35 to 12.16 Kbits per second. Where the better throughput is observed with CPRR.

v. Energy consumption of CPRR is less noted as 10 to 83 joules whereas AODV, DFRR and PRO-AODV consumes 15-98, 11-85 and 12-95 joules respectively.

vi. The route detection time with respect to number of nodes, the CPRR takes minimum time to detect the best route when compared with DFRR, PRO-AODV and AODV mechanisms.

From the above performance metrics, it is clear that the CPRR mechanism is proved to be quite efficient in terms of packet delivery ratio, end-to-end delay, throughput, average delay, energy consumption, and route detection time.

6.3. Future scope of work

In future, this approach may get be extended by the following perspectives known as future scope of the work is as follows.

1. With the present work, there is a possibility of producing results while combining CPRR Algorithm with other existing routing protocol such as AOMDV and Ant colony algorithm.
2. There is a scope for improvement in finding the best route and energy efficiency of the nodes.
3. The sensing and communication ranges are fixed as heterogeneous sensors are considered.

REFERENCES

[1] G. Miao, J. Zander, K-W Sung, and B. Slimane, **Fundamentals of Mobile Data Networks**, Cambridge University Press, ISBN 1107143217, 2014.

[2] C. Siva Ram Murthy and B. S. Manoj, **Ad hoc Wireless Networks: Architectures and Protocols**, Prentice Hall PTR, May 2004.

[3] Chai-Keong Toh "**Ad Hoc Mobile Wireless Networks: Protocols and Systems** 1st Edition", Prentice Hall PTR, 2002.

[4] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward, "**A Distance Routing Effect Algorithm for Mobility (DREAM)**," Proc. ACM/IEEE International Conference on Mobile Computing and Networking, pp. 76-84, 1998.

[5] C.E. Perkins, and P. Bhagwat, "**Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers**," Proc. ACM 1994, pp. 234-244.

[6] S. Murthy and J.J. Garcia-Luna-Aceves, "**An Efficient Routing Protocol for Wireless Networks**", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996.

[7] Chiang, "**Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel**," Proceedings of IEEE SICON '97, April 1997, pp. 197-211.

[8] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz,"**A Overview of Routing Protocols For Mobile Ad Hoc Networks**",4 June 2003.

[9] Tsu-Wei Chen and Mario Gerla, "**Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks**" Proc. IEEE ICC'98.

[10] David B. Johnson, Davis A. Maltz, "**The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks**" October 1999 IETF Draft, 49 pages.

[11] R. Dube et al., "**Signal Stability based adaptive routing for Ad Hoc Mobile networks**", IEEE Pers. Comm., Feb. 1997, pp. 36-45.

[12] C. B. PerKins. "**Ad hoc on-demand distance vector (AODV) routing**," Mobile Computing, vol. 353, pp. 28, 1996.

[13] McDonald, A. B.; and Znabi, T.; "**A Path Availability Model for Wireless Ad Hoc Networks**". Proceedings of IEEE Wireless Communications and Networking Conference 1999 (WCNC.99), New Orleans, LA, USA, September 1999, pp. 35-40.

[14] M. Jiang, J. Li, Y. C. Tay: Cluster Based Routing Protocol (CBRP) Functional Specification, Internet Draft, work in progress, June 1999.

[15] George Aggelou, Rahim Tafazolli " **Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) Protocol**", Mobile Ad Hoc Networking Working Group University of Surrey, UK, 13 September 1999.

[16] Zygmunt J. Haas, Marc R. Pearlman, IEEE/ACM Transactions on Networking (TON), Volume 9 Issue 4, pages: 427-438, August 2001.

[17] J. Yick, B. Mukherjee, and D. Ghosal. **Wireless sensor network survey**. Computer Networks, 52:2292-2330, 2008.

[18] X. Bai, C. Zhang, D. Xuan, J. Teng, and W. Jia. "**Low-connectivity and full-coverage three dimensional wireless sensor networks**". International symposium on Mobile ad hoc networking and computing, MobiHoc '09, pages 145{154. ACM, 2009.

[19] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "**A survey on Sensor networks**". IEEE Communications Magazine, 40(8):102-114, November 2002.

[20] Javad Rezazadeh, Marjan Moradi, Abdul Samad Ismail," **Mobile Wireless Sensor Networks Overview**", International Journal of Computer Communications and Networks(IJCCN), Volume 2, Issue 1, February 2012

[21] W. Alsalih, H. Hassanein, and S. G. Akl, "**Placement of multiple mobile data collectors in wireless sensor networks**". Ad Hoc Networks, 8(4):378 -390, 2010.

[22] S. A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, and J. Ma, "**Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing**". International Conference on Advanced Information Networking and Applications Workshops, volume 2 of AINAW '07, pages 113-120, 2007.

[23] I. Amundson and X. D. Koutsoukos. "**A survey on localization for mobile wireless sensor networks**". In Proceedings of the 2nd international conference on Mobile entity localization and tracking in GPS-less environments, MELT'09, pages 235-254, Berlin, Heidelberg, 2009.

[24] R. N. Duche and N. P. Sarwade, "**Sensor node failure or malfunctioning detection in wireless sensor network**," ACEEE Int. J. Commun., vol. 3, pp. 57–61, Mar. 2012.

[25] A.Savvidas, M.B. Srinivasan and C.Han, "**Dynamic Fine-Grained Localization in AD Hoc Networks of Sensors**", proceedings of ACM MOBICOM 2001, pp. 166-179, July 2001.

[26] Nabil Ali Alrajeh, Maryam Bashir, and Bilal Shams, “International Journal of Distributed Sensor Networks “ Volume 2013.

[27] X. Chen, K. Makki, K. Yen, and N. Pissinou, "**Sensor network security: A survey**", IEEE Commun. Surveys Tuts., vol. 11, no. 2, pp. 52–73, 2009.

[28] B.Prabhakar, E.U. Biyikoglu, and A.E. Gamal, "**Energy Efficient Transmission over a Wireless Link Lazy Packet Scheduling**", Proceddings of IEEE INFOCOM 2001,vol 1, pp.386-394,April 2001.

[29] M. Adamon and S.Sarkar, "**A Framework for Optimal Battery Management for Wireless Nodes**", Proceddings of IEEE INFOCOM 2002, pp.1783-1792, June 2002.

[30] K.Lahiri, A.Raghunathan, and S.Dey, "**Battery-Driven System Design: A New Frontier in Low-Power Design**", Proceddings of ASP-DAC/VLSI Design 2002, pp. 261-267, January 2002.

[31] J.H Saltzer, D.P. Reed and D.D. Clark, "**End-End Arguments in system design**", ACM Transcations on Computer Systems, pp. 277-288,2004.

[32] Kazem Sohraby, Daniel Minoli, Taieb Znati, “**Wireless Sensor Networks: Technology, Protocols, and Applications**”, a John Wiley & sons Inc. publication book, 2007.

[33] Edward Tetz, “**Pros and Cons of Static Routing**”, from Cisco Networking ebook.

[34] Terrence Mak; Peter Y. K. Cheung; Kai-Pui Lam; and Wayne Luk. "**Adaptive Routing in Network-on-Chips Using a Dynamic-Programming Network**". 2011.

[35] Y. Yao, J. Gehrke, ‘‘**The Cougar Approach to In-Network Query Processing in Sensor Networks**,’’ SIGMOD Record, Sept. 2002.

[36] M. Chu, H. Haussecker, 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, Aug. 2002.

[37] J. N. Al-Karaki, R. Ul-Mustafa, A. E. Kamal, "**Data Aggregation in Wireless Sensor Networks: Exact and Approximate Algorithms**," IEEE Workshop on High Performance Switching and Routing (HPSR'04), Phoenix, AZ, Apr. 2004.

[38] K. Akkaya, M. Younis, "**A survey on routing protocols for wireless sensor networks**", Ad Hoc Networks Volume: 3, Issue: 3, Pages: 325-349, 2005.

[39] J. N. Al-Karaki, A. E. Kamal, "**Routing Techniques in Wireless Sensor Networks: A Survey**," IEEE Wireless Communications, Vol. 11, No. 6, Dec. 2004, pp. 6–28.

[40] W. R. Heinzelman, A. Ch , H. Balakrishnan, "**Energy-efficient communication protocol for wireless micro sensor networks**", In Proc. the 33rd Hawaii International Conference on System Sciences (HICSS'00), 2000.

[41] M. Handy, M. Haase, D. Timmermann, "**LEACH: Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster Head Selection**," IEEE MWCN, Stockholm, Sweden,Sep. 2002.

[42] S. Lindsey, C. Raghavendra, "**PEGASIS: Power-Efficient Gathering in Sensor Information Systems**," IEEE Aerospace Conference Proceedings, 2002, Vol. 3, No. 9–16 pp. 1125–1130.

[43] J. Kulik, W. R. Heinzelman, H. Balakrishnan, "**Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks**," Wireless Networks, Vol. 8, 2002, pp. 169–185.

[44] C. Intanagonwiwat, R. Govindan, D. Estrin, "**Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks**," the 6th ACM International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, Aug. 2000, pp. 56–67.

[45] Karthick Raghunath K.M, Rengarajan N, "**Investigation of Faults, Errors and Failures in Wireless Sensor Network: A Systematical Survey**", International Journal of Advanced Computer Research, Volume-3 Number-3 Issue-12 September-2013.

[46] Ridha Soua, Pascale Minet, "**A survey on energy efficient techniques in wireless sensor networks**", WNNC 2011 - 4th Joint IFIP Wireless and Mobile Networking Conference, Toulouse, France. IEEE, pp.1 - 9, 2011.

[47] N. Kimura, S. Latifi, "**A Survey on Data Compression in Wireless Sensor Networks**", International Conference on Information Technology: Coding and Computing (ITCC'05), pp.8-13, 2005.

[48] Yujie Zhu, Sundaresan, K., Sivakumar, R, "**Practical limits on achievable energy improvements and useable delay tolerance in correlation aware data gathering in wireless sensor networks**", In Proc. IEEE Secon 2005.

[49] G. Pei, M. Gerla, T.-W. Chen, "**Fisheye state routing: a routing scheme for ad hoc wireless networks**", In Proc. IEEE Icc00, New Oreleans, LA, June 2000.

[50] Van Der Schaar, M. Sai Shankar N, "**Cross-layer wireless multimedia transmission: challenges, principles, and new paradigms**", IEEE Wireless Communications, vol. 12, pp. 50-58, 2005.

[51] E.O. Blass, J. Horneber, M. Zitterbart, "**Analyzing Data Prediction in Wireless Sensor Networks**", In Proc. IEEE Vehicular Technology Conference, VTC Spring, 2008.

[52] W. B. Heinzelman, "**An application-specific protocol architecture for wireless networks**", IEEE Transactions on Wireless Communications, Vol. 1, No. 4, October 2002.

[53] M. Bhardwaj and A.P. Chandrakasan, "**Bounding the Lifetime of Sensor Networks via Optimal Role Assignments**", the 21st IEEE Infocom, 2002.

[54] M. Cagalj, J.P. Hubaux, and C. Enz, "**Minimum-energy Broadcast in All-wireless Networks: NP-completeness and Distribution Issues**", In Proc. the 8th ACM MobiCom, 2002.

[55] L. Pelusi, A. Passarella, M. Conti, "**Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks**", IEEE Communications Magazine, Vol.44, No. 11, pp.134-141, Nov.2006.

[56] Dulman.S and Niberg.T "**Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks**", WCNC workshop, Louisiana,2003.

[57] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "**TinyDB: An acquisitional query processing system for sensor networks**", ACM Trans. Database Syst., vol. 30, no. 1, pp. 122–173, 2005.

[58] W. Ye, J. Heidemann, D. Estrin, "**Medium access control with coordinated adaptive sleeping for wireless sensor networks**", IEEE/ACM Transactions on Networking, vol. 12, No.3, pp. 493-506, June 2004.

[59] I. Rhee, A. Warrier, M Aia, J. Min, "**Z-MAC: a hybrid MAC for wireless sensor networks**", In Proc. ACM SenSys 2005, S Diego, USA, November 2005.

[60] F. Ingelrest, D. Simplot-Ryl, I. Stojmenovic, "**Optimal Transmission Radius for Energy Efficient Broadcasting Protocols in Ad Hoc Networks**", IEEE Transactions on Parallel and Distributed Systems, June 2006.

[61] R. Zhang, M.A, Labrador, "**Energy-aware topology control in heterogeneous wireless multihop networks**", In Proc. 2nd IEEE International Symposium on Wireless Pervasive Computing, Puerto Rico, 2007.

[62] Li Ya ,Wang Pengjun , Luo Rong, Yang Huazhong , Liu Wei "**Reliable Energy-Aware Routing Protocol for Heterogeneous WSN Based on Beaconing**", Page(s): 109 – 112, Publication Year: 2014.

[63] Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre,"**Know Thy Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing**", vol. 10, no. 3, pp. 1319-1342, 2013.

[64] Qinghua Li and Guohong Cao,"**Mitigating Routing Misbehavior in Disruption Tolerant Networks**", vol. 4, no. 1, pp. 423-427, 2013.

[65] Arjan Durresi, Vamsi Paruchuri,"**Delay-Energy Aware Routing Protocol for Sensor and Actor Networks**", vol. 2, no. 4, pp. 1342-1346, 2013.

[66] Reuven Cohen and Boris Kapchits,"**Energy-Delay Optimization in an Asynchronous Sensor Network with Multiple Gateways**", vol. 10, pp. 34-39, 2012.

[67] Sayid Mohamed Abdule, Suhaidi Hassan, "**Divert Failure Route Protocol Based on AODV**", vol.8, pp. 67-71, 2010 IEEE.

[68] K.A.Shah, M.R.Gandhi, "**Performance Evaluation of AODV Routing Protocol with Link Failures**" vol.4, 2010 IEEE.

[69] P.Priya Naidu, Meenu Chawla, "**Enhanced Ad Hoc on Demand Distance Vector Local Repair Trial for MANET**", vol.8, pp. 212-216, 2011 IEEE.

[70] LIU Jian, LI Fang-min, "**An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks**", vol.09, pp.507-510, 2009.

[71] Qing Li, Cong Liu, Han-hong Jiang, "**The Routing Protocol of AODV Based on Link Failure Prediction**", vol.04, pp.1993-96, 2008.

[72] Li Qiong and Yang Jun, "**An Improved AODV Routing Protocol of Wireless Sensor Network** ", vol. 9-11 Nov. 2012 IEEE.

[73] Reinaldo Gomes, Eduardo Souto, Judith Kelner, Djamel Sadok, "**Advantages of Node Energy Control for Routes Selection in Wireless Sensor Networks**",vol.06, pp. 336-342, 2006 IEEE.

[74] Michael Pan, Sheng-Yan Chuang and Sheng-De Wang," **Local Repair Mechanisms for On-Demand Routing in Mobile Ad hoc Networks** ", the 11th Pacific Rim International Symposium on Dependable Computing 2005, pages, 317-324.

[75] Jing Feng, Huaibei Zhou, "**A Self-Repair Algorithm for Ad Hoc On-Demand Distance Vector Routing**", International Conference on Wireless Communications, Networking and Mobile Computing, IEEE2006.

[76] "**The Network Simulator Ns-2**, the VINT project," link: http://www.isi.edu/nsnam/ns/ns-build.html, Retrieved in December 2007.

[77] Hua Qu, Peng Zhang, Ji-hong Zhao, "**A New Local Repair Scheme Based on Link Breaks for Mobile Ad Hoc Networks**", Annual Communications Networks and Services Research Conference, IEEE 2009.

[78] LIU Jian, LI Fang-min, "**An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks**", International Conference on Information Assurance and Security, IEEE 2009.

[79] Suhazlan Suhaimi, Kamaruddin Mamat, S.R Azzuhri, "**Comparative Study of AODV Route Repair Mechanism with Impact on Node Mobility and Traffic Load in Wireless Mesh Networks**", IEEE 2010.

[80] Zilu Liang, Yuzo Taenaka, Takefumi Ogawa, Yasushi Wakahara, "**Pro-Reactive Route Recovery with Automatic Route Shortening in Wireless Ad Hoc Networks**", International Symposium on Autonomous Decentralized Systems, 2011 IEEE.

[81] Jyoti Jain, Roopam Gupta, T.K. Bandhopadhyay," **Performance analysis of proposed local link repair schemes for ad hoc on demand distance vector**", IET Networks, 2014, Vol. 3, Iss. 2, pp. 129–136.

[82] P. Priya Naidu and Meenu Chawla, "**Enhanced Ad Hoc on Demand Distance Vector Local Repair Trial for MANET**" IEEE 2011.

[83] Banoj Kumar panda, Bibhudatta Dash, Rupanita Das, Ajit Sarangi," **Mobility and its impact on Performance of AODV and DSR in Mobile Ad hoc Network**", IEEE 2012.

[84] Shijie Li, Xu Li, Qijing Feng," **An Improved AODV Local Repair Algorithm Based on Delay Constraint**", ICSP2012 Proceedings, IEEE 2012.

[85] Muhammad Khalil Afzal, Hyun-Ho Shin, Byung-Seo Kim, and Sung Won Kim,” **link quality aware local repair in AODV-based ad-hoc networks**”, ICSSC 2013.

[86] Xingyun PENG, Yi WU, Zhexin XU, and Xiao LIN,” **AODV-MR: AODV with multi-RREP for VANET**”, Advanced Infocomm Technology (ICAIT), Nov. 2014 IEEE.

[87] Krishna Mahajan Devesh Malik M.A Rizvi D. Singh Karaulia,” **Event Driven Dynamic Path Optimization for AODV in MANET**”, International Conference on Computational Intelligence and Communication Networks, IEEE 2014.