

Hybrid Optimization based on Genetic Routing and Scheduling Scheme with Secure Transmission in Wireless Sensor Networks

Submitted in partial fulfilment of the requirements for the award of

Bachelor of Engineering Degree in Electronics and Communication Engineering

By

**KAKOLLU SAI KRISHNA NARASIMHA (37130177) GOKAVARAPU
DEEKSHITHA SRIHARI (37130144)**



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

**INSTITUTE OF SCIENCE AND
TECHNOLOGY (DEEMED TO BE
UNIVERSITY)**

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL 2021



**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **KAKOLLU SAI KRISHNA NARASIMHA (37130177)** and **GOKAVARAPU DEEKSHITHA SRIHARI (37130144)** who carried out the project entitled **“Hybrid Optimization based on Genetic Routing and Scheduling Scheme with Secure Transmission in Wireless Sensor Networks”** under our supervision from.

Internal Guide

Dr. P. KAVIPRIYA

**Head of the Department
(Dr. T. RAVI)**

Submitted for Viva voce Examination held on _____

INTERNAL EXAMINER

EXTERNAL EXAMINER

DECLARATION

We **KAKOLLU SAI KRISHNA NARASIMHA (37130177)** and **GOKAVARAPU DEEKSHITHA SRIHARI (37130144)** here by declare that the Project Report entitled **“Hybrid Optimization based on Genetic Routing and Scheduling Scheme with Secure Transmission in Wireless Sensor Networks”** done by us under the guidance of **“Dr. P. KaviPriya”, Associative Professor** Department of Electronics and Communication Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING**.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

1.

2.

ACKNOWLEDGEMENT

We are pleased to acknowledge my sincere thanks to Board of Management of SATHYABAMA for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

We convey our thanks to **Dr. N. M. NANDHITHA M.E.P.hD., Prof. & Dean, School of Electrical and Electronics Engineering** and **Dr. T. Ravi M.E.P.hD., Head of the Department, Dept. of ELECTRONICS AND COMMUNICATION ENGINEERING** for providing me necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. P. KAVIPRIYA, Associate Professor** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

We wish to express my thanks to all Teaching and Non-teaching staff members of the Department of **Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The main objective of this project is nodes in networks are constrained with limited power for their vital operations since the connectivity of the network will go down as soon as node energy gets exhausted. Node failures due to power constraints cause system failures and hence minimize end-to-end connectivity in the network. And also mobility and congestion of the nodes lead to frequent link failures and packet losses affecting the QoS performance of the protocol.

In this work, we used an effective proposed scheme, named as Hybrid Optimization System (HOS), for efficient and routing and transmission for wireless networks. As to enhance the network lifetime as well as for reliable and efficient communication in wireless sensor network the protocol employed should be energy efficient, which can be further achieved by using a good quality routing technique.

Nodes in wireless sensor networks (WSN) are resource and energy-constrained because they are generally batteries powered and therefore have limited computational capability. Due to the less secure environment in WSN, some malicious nodes at one point can tunnel packets to another location to damage the network in terms of packets dropping and eavesdropping and this is a so-called wormhole attack.

Many of the current protocols solve the wormhole attack problem in isolation from the node energy consumption. However, some other proposed solutions consider reducing the energy consumption to detect such attacks but still it is needed to probe better performance. In this paper, we present a lightweight multi-hop routing protocol for 802.15.4 WSN that aims to minimize the energy consumption and also to detect the wormhole attacks.

Simulation results prove that our MAC Centralized Routing Protocol (MCRP) outperforms other existing similar protocols.

TABLE OF CONTENT

CHAPTER NO	TITLE	PAGE NO
	Bonafide Certificate	i
	Declaration	ii
	Acknowledgement	iii
	Abstract	iv
	Table of content	v-vii
	List of Figures	vii
1	Introduction	1-21
	1.1. Wireless Sensor Networks	1
	1.2. Applications of Wireless Sensor Network	2
	1.2.1 Agriculture Sensor and irrigation	2
	1.2.2 Industrial Alarm Systems	2
	1.2.3 Arena Lighting	2
	1.2.4 Asset Training in Wormhouses & Transportation	3
	1.2.5 Automated control of Blinds and shutters	3
	1.2.6 Building Energy Management Systems	3
	1.2.7 Occupancy Sensing in Car parking systems	4
	1.2.8 Indoor climate sensors	4
	1.2.9 Remote Industrial Controls	4
	1.2.10 Energy Efficient Street lighting	5
	1.2.11 Vehicle Traffic Monitoring	5
	1.3 Network Routing Scheme	6
	1.3.1 Types of routing	7
	1.3.2 Routing Algorithms for Network	8
	1.3.3 Routing Algorithms	11
	1.4 Genetic Optimization Algorithm	14
	1.4.1 Foundation of Genetic Algorithms	14
	1.4.2 Fitness Score	15

	1.4.3 Operators of Genetic Algorithm	15
	1.5 Routing Security	20
	1.5.1 Key Consideration	20
	1.5.2 Challenges	21
2	Literature Review	22-42
	2.1. Energy Aware Probabilistic broadcasting for Ad hoc network	22
	2.2. Energy Efficient Probabilistic broadcasting for Ad hoc Network	24
	2.3. Distance based cluster head selection Algorithm for Wireless Sensor Network	26
	2.4. Detection and prevention Mechanism for Black Hole attack in WSN	28
	2.5. Security issue of WSN based on cloud Computing	30
	2.6. Cluster Head Selection Protocol using Fuzzy Logic for WSN	32
	2.7. Chef-Cluster head election mechanism Using Fuzzy Logic in WSN	34
	2.8 ACE- an emergent algorithm for highly Uniform Cluster Formation	36
	2.9 Intelligent Probabilistic Broadcasting in mobile Ad-hoc network column a PSO approach	38
	2.10 Two-Dimensional Particle swarm optimization Algorithm for load flow Analysis	40
	2.11 Hybrid Optimization	40-41

3	RESEARCH METHODOLOGIES	42-59
	3.1. Existing Methodology	42-44
	3.2. Proposed Methodology	45-47
	3.2.1 Stable Broadcast Routing	45
	3.2.2 Multi-point Relays	46
	3.3 Methodologies	47
	3.3.1 Initialization	47
	3.3.2 Balanced Multipath routing and Scheduling	49-53
	3.3.3 Robust Route Selection-Genetic Optimization	53-56
	3.3.4 Route Maintenance	57-59
4	RESULTS AND DISCUSSION	50-71
5	CONCLUSION	72
6	FUTURE WORK	82
7	BIBLIOGRAPHY	83-84

LIST OF FIGURES

FIG NO	TITLE	PAGE NO
1.4.3.1	population, chromosomes and genes	16
1.4.3.2	Cross over point	17
1.4.3.3	Exchanging Genes among Parents	17
1.4.3.4	New offspring	17
1.4.3.5	Mutation	18
3.1.1	Wormhole tunnel Constructed between nodes X and Y.	42
3.1.2	Route Discovery Process of WRHT	43
3.1.3	Worm Detection Process of WRHT	44
3.3.2.1	Multiple Multicast Routes	50
3.3.2.2	Multipath Discovery Algorithm	51
3.3.3.1	Flow Chart for fitness-based Routing Protocol	56
4.1	End to End Delay Graph	61
4.2	Packet Delivery Ratio Graph	62
4.3	Average Throughput Graph	62
4.4	Energy Consumption Graph	63
4.5	Node Initialization	64
4.6	Neighbor Communication	65
4.7	Source, Destination and Route Selection	65
4.8	Attacker Detection	66
4.9	Data Sharing Between Source and Destination	66
4.10	Neighbor Table and Data reports	67-71
4.11	Geotagged photo	80

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Networks

Wireless Sensor Networks (WSN) are used in many industrial applications and they are a key ingredient in the growing Internet of Thing (IoT). Wireless sensors can collect useful data on the status of equipment or their operating environment. The data is collected wirelessly, as cables are costly to install, especially when there is a long distance to the sensor, or when the network is retrofitted into an existing operation. The data is then moved from the network via a gateway to a software application. The software's intelligence then makes decisions based on the data, either from single data points, or from trends and statistics derived from large data sets.

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery.

WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic, and many other consumer and industrial areas. A WSN consists of anywhere from a few hundreds to thousands of sensor nodes. The sensor node equipment includes a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit, and an energy source, usually a battery. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. As such, their prices also vary from a few pennies to hundreds of dollars depending on the functionality parameters of a sensor like energy consumption, computational speed rate,

bandwidth, and memory.

1.2 Applications of WSN

1.2.1 Agricultural sensors and irrigation

Agricultural sensors are typically used to monitor the humidity in the soil. They decide how and when irrigation systems are used, but also other environmental measures such as temperature, sunlight and various gases are monitored. The monitored area can range from large outdoor fields, where long-range communications transmission is key, to small indoor greenhouses. The sensors need to be battery operated, as cabling is typically not an option. Battery operation is best achieved with a star network such as Wireless M-Bus or RC232. Mesh networking is typically more power hungry as the nodes need to be active and always in listening mode.

1.2.2 Industrial alarm systems

Industrial alarm systems continuously monitor an environment to alert employees or authorities about hazardous conditions, including high temperatures, smoke, fire, high pressure, high water, etc. Often these alarm sensors are located far from the “mains” supply lines. An additional challenge is that they are used infrequently, yet they must reliably send off an alarm on short notice when triggered. A robust radio with highest industry standard security is recommended for such applications. Robustness is achieved with Ultra-Narrowband radios which is available in the Radio crafts RC12xx and RC17xx platforms. Ultra-Narrowband means that the radio is only open for a very narrow frequency spectrum, which means that receiver noise is minimized. Security in the Radio crafts modules is achieved with AES-128 encryption, the most used industry standard encryption protocol for secure communication.

1.2.3 ARENA lighting

Arenas use numerous lights that need to be repositioned for every event. The lights are often located in places where cabling is a challenge, especially in arenas where the lighting was not installed as part of the original construction. The distance between each node is typically short, but the distance from the control unit to some remote units can be large. What is needed is a mesh network where long distances are possible via individual nodes such as a TinyMesh network on a sub-gig frequency such as 169 MHz, 433 MHz, 868 MHz and 915 MHz. Keep in mind that the lower the frequency, the longer the reach. Radiocrafts modules at 169 MHz offer a few kilometers reach in real urban environments.

1.2.4 Asset tracking in warehouses & transportation

Asset tracking in warehouses or during transportation ensures that the location of each asset is known at all times. Additional data can also be wirelessly communicated via RF — such as temperature or humidity — so the asset’s environment can be controlled; for example, to help preserve food or medicine. Battery operated sensors communicating wirelessly are ideal for this. The specific requirement of the wireless link is determined by the geographical location, required range, the radio environment and data-rate needed. Wireless M-Bus on the right frequency is ideal for many applications as it is robust, secure with low power, and can handle many nodes. Radiocrafts has a large portfolio of modules where an ideal solution is readily available.

1.2.5 Automated control of blinds & shutters

Blinds and shutters (aka “louvres”) in buildings are used to control sunlight and airflow from windows. Sensors gather the input data needed for the system and control signals are sent to the motors that drive the blinds and shutters to open and close. An intelligent master is in charge to determine when to open or shut the blind and shutters to provide for a cost efficient and comfortable climate in the building. Wireless communication is often used as the blind and shutters are located in the periphery of the building which makes cabling expensive. Key parameters for selecting the radio technology are range and power, but also predictable latency. This is best supported by a low frequency radio in a star network operation. Products from Radiocrafts include the transparent RC232 family or the Wireless M-Bus, but also the TinyMesh if the Mesh structure remains at low complexity to avoid network congestion.

1.2.6 Building Energy Management Systems

Energy Management is becoming paramount to the future of organizations worldwide. Much of the importance in saving energy stems from a global need to save energy which affects global energy prices, emission targets, and legislations, all of which are compelling reasons why an organization should take energy saving strategies seriously. A Building Energy Management System provides real-time control and monitoring of a wide range of connected systems, environmental conditions, energy use, and more. You can then collect and analyse all this data to create a more comfortable and energy-friendly environment in the building. Sensors monitor operational conditions of buildings and building equipment.

Examples include monitoring airflow in the building, sunlight exposure, temperature, and much more. Then, device controllers process all this collected data and actuators perform.

the appropriate actions to optimize the environmental settings. The requirements on the Wireless Sensor network is that it can support long range and coverage, can be deployed quickly and easily, and must support most cloud applications.

1.2.7 Occupancy sensing in car parking systems

Car parking occupancy systems use magnetic or IR sensors to determine if a specific space is in use or if it is available. Providing cable connections to each parking spot is prohibitively expensive, so battery powered Radiocrafts Wireless RF networks are used instead. This drives a need for low power, reliable, long-range wireless connection. The networking can be quite complex, so a robust star network is ideal. The Radiocrafts Wireless M-Bus are developed for gas and water metering sharing many of the same requirements. Wireless M-Bus has been field tested in large volumes, ensuring that the protocol is very robust and reliable, while supporting low power applications.

1.2.8 Indoor climate sensors

Indoor climate sensors are used in a variety of applications to control temperature, humidity, light, carbon dioxide, etc. The applications range from museums — where ancient artifacts need precisely controlled atmospheres — all the way to saunas and ice-bars, where we enjoy extreme temperatures that need to be, nevertheless, kept comfortable and safe. Many of the sensors are put in remote locations driving a need for low power dissipation for battery operation and radio technology with long range. Radiocrafts modules support both those criteria with modules based on TinyMesh, Wireless M-Bus and RC232 RF protocols.

1.2.9 Remote industrial controls

RF technologies can be ideal for Industrial Control applications when:

- a) The controlled equipment is remote.
- b) Cabling is not an option.
- c) Predictable latency is acceptable.

Typical applications include turning on or off equipment or controlling slow-moving devices such as an overhead crane or pump-operated valve.

These applications demand exceptionally reliable communications — over long distances and penetrating through common objects — which makes Radiocraft's Ultra Narrowband devices an excellent choice as they are very robust in noisy environments. Data security is supported with AES-128 encryption, the industry standard for secure communication. Predictable latency is best supported from star networks such as RC232 or Wireless M-Bus, but also a low complexity mesh implemented with TinyMesh can be used.

1.2.10 Energy-efficient street lighting

Networked street lighting is gaining significant traction in Smart Cities and is a great way for cities and utilities to improve safety and cut costs for their customers. A networked street lighting system incorporates a cluster of streetlamps that can communicate with each other and provide lighting data to a local concentrator. The concentrator manages and transmits the relevant data, via a wireless RF module, to a secure server that captures the data and presents it in a dashboard interface.

A smart street lighting system also allows facility managers to remotely control streetlights while keeping track of electrical power consumption in the lamps. The lamp status is constantly monitored meaning scheduling maintenance becomes more efficient and cost-effective. Additionally, in case a lamp fails, the problematic lamp can be pinpointed remotely and fixed. Another example of what can be done with smart street lighting includes brightening and dimming lights depending on the weather conditions.

The requirements on the Wireless Sensor network are that it can support long range and cover long “pearl of strings” networks and can be deployed quickly while requiring low maintenance.

1.2.11 Vehicle traffic monitoring

Understanding the flow of traffic is key to optimizing transportation in crowded cities. Additional traffic management factors include the occupancy of parking lots and the traffic in bottleneck areas (e.g., bridges, construction zones, detours, etc.). Some of these information needs are temporary (construction zones, detours), so both traffic and occupancy sensors need to be moveable, precluding the use of fixed cables. A mesh network on sub-gig frequencies, such as a TinyMesh network, allows for long range between nodes and at the same time the network flexibility provided by the mesh structure. If an incredibly low power solution is needed, then Wireless M-Bus is an alternative that provides for a robust low power solution.

1.3 Network Routing Scheme

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are

typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

Routing schemes differ in how they deliver messages:

- unicast delivers a message to a single specific node.
- broadcast delivers a message to all nodes in the network.
- multicast delivers a message to a group of nodes that have expressed interest in receiving the message.
- Anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source.
- Geocast delivers a message to a group of nodes based on geographic location. Unicast is the dominant form of message delivery on the Internet.

1.3.1 Types of Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

1. Static routing –

Static routing is a process in which we have to manually add routes in routing table.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.

- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have particularly good knowledge of the routes of the topology.

2. Dynamic Routing –

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol has following features:

1. The routers should have the same dynamic protocol running in order to exchange routes.
2. When a router finds a change in the topology then router advertises it to all other routers.

Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

1.3.2 Routing Algorithms for Networks

Following are the **routing algorithms for networks**:

- Distance Vector Algorithm
- Link State Algorithm
- Path Vector Algorithm
- Hybrid Algorithm

Distance Vector Routing: Distance vector algorithms use the Bellman- Ford algorithm. Distance vector algorithms are examples of dynamic routing protocols. Algorithms allow each device in the network to automatically build and maintain a local routing table or matrix.

Routing table contains list of destinations, the total cost to each, and the next hop to send data to get there. This approach assigns a number, the cost, to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest total cost i.e., the sum of the costs of the links between the nodes used.

The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbours, and the direct cost involved in reaching them. The routing table from each node, on a regular basis, sends its own information to each neighbouring node with current idea of the total cost to get to all the destinations it knows of.

The neighbouring node(s) examine this information and compare it to what they already 'know'; anything which represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost. The main advantage of distance vector algorithms is that they are typically easy to implement and debug.

They are extremely useful in small networks with limited redundancy. When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries and create new routing-table information.

They then pass this information to all adjacent nodes, which then repeat the process. Eventually all the nodes in the network receive the updated information and will then discover new paths to all the destinations which they can still "reach".

Link State Routing: A link state is the description of an interface on a router and its relationship to neighbouring routers. When applying link-state algorithms, each node uses as its fundamental data a map of the network in the form of a graph.

To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm.

The result is a tree rooted at the current node such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

Shortest-Path First (SPF) Algorithm: The **SPF algorithm is used to process the information in the topology database.** It provides a **tree representation of the network.** The device running the SPF algorithm is the root of the tree.

The output of the algorithm is the **list of shortest paths to each destination network.** Because each router is processing the same set of LSAs, each router creates an identical link state database. However, because each device occupies a different place in the network topology, the application of the **SPF algorithm produces a different tree for each router.**

Path Vector Routing: Distance vector and link state routing are both intra-domain routing protocols. They are used inside an autonomous system, but not between autonomous systems. Both of these routing protocols become intractable in large networks and cannot be used in Inter-domain routing. Distance vector routing is subject to instability if there are more than few hops in the domain. Link state routing needs huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. Path vector routing is used for inter-domain routing. It is similar to Distance vector routing.

In path vector routing we assume there is one node (there can be many) in each autonomous system which acts on behalf of the entire autonomous system. This node is called the speaker node. The speaker node creates a routing table and sends information to its neighboring speaker nodes in neighboring autonomous systems. The idea is the same as Distance vector routing except that only speaker nodes in each autonomous system can communicate with each other.

The speaker node sends information of the path, not the metric of the nodes, in its autonomous system or other autonomous systems. The path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router

advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks send information as destination addresses and path descriptions to reach those destinations.

A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector that contains paths to a set of destinations. The path, expressed in terms of the domains traversed so far, is carried in a special path attribute that records the sequence of routing domains through which the reachability information has passed. The path represented by the smallest number of domains becomes the preferred path to reach the destination. The main advantage of a path vector protocol is its flexibility.

Hybrid Routing: This algorithm attempts to combine the positive attributes of both distance vector and link state protocols. Like distance vector, hybrid algorithm uses metrics to assign a preference to a route. However, the metrics are more accurate than conventional distance vector algorithm.

Like link state algorithms, routing updates in hybrid algorithm are event driven rather than periodic. Networks using hybrid algorithm tend to converge more quickly than networks using distance vector protocols. Finally, algorithm potentially reduces the costs of link state updates and distance vector advertisements.

A system that performs this function is called an IP router. This type of device attaches to two or more physical networks and forwards packets between the networks. When sending data to a remote destination, a host passes packet to a local router. The router forwards the packet toward the final destination. They travel from one router to another until they reach a router connected to the destination's LAN segment.

1.3.3 Routing Algorithms

Let the network be represented by graph $G(V, E)$ and let the number of nodes be 'N'. For all the algorithms discussed below, the costs associated with the links are assumed to be positive. A node has zero cost w.r.t itself. Further, all the links are assumed to be symmetric, i.e. if $d_{i,j}$ = cost of link from node i to node j , then $d_{i,j} = d_{j,i}$. The graph is assumed to be complete. If there exists no edge between two nodes, then a link of infinite cost is assumed. The algorithms given below find costs of the paths from all nodes to a

particular node: the problem is equivalent to finding the cost of paths from a source to all destinations.

A. Bellman-Ford Algorithm

This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

Notation:

$d_{i,j}$ = Length of path between nodes i and j , indicating the cost of the link.
 h = Number of hops.
 $D[i, h]$ = Shortest path length from node i to node 1, with up to ' h ' hops.
 $D[1, h] = 0$ for all h .

Algorithm:

Initial condition: $D[i, 0] = \text{infinity}$, for all i ($i \neq 1$)

Iteration : $D[i, h+1] = \min \{d_{i,j} + D[j, h]\}$ over all values of j .

Termination : The algorithm terminates when

$$D[i, h] = D[i, h+1] \quad \text{for all } i.$$

Principle:

For zero hops, the minimum length path has length of infinity, for every node. For one hop the shortest-path length associated with a node is equal to the length of the edge between that node and node 1. Hereafter, we increment the number of hops allowed, (from h to $h+1$) and find out whether a shorter path exists through each of the other nodes. If it exists, say through node ' j ', then its length must be the sum of the lengths between these two nodes (i.e. $d_{i,j}$) and the shortest path between j and 1 obtainable in up to h paths.

B. Dijkstra's Algorithm

Notation:

D_i = Length of shortest path from node ' i ' to node 1.
 $d_{i,j}$ = Length of path between nodes i and j .

Algorithm

Each node j is labeled with D_j , which is an estimate of cost of path from node j to node 1.

Initially, let the estimates be infinity, indicating that nothing is known about the paths. We now iterate on the length of paths, each time revising our estimate to lower values, as we obtain them. Actually, we divide the nodes into two groups; the first one, called set P contains the nodes whose shortest distances have been found, and the other Q containing all the remaining nodes. Initially P contains only the node 1. At each step, we select the node that has minimum cost path to node 1. This node is transferred to set P. At the first step, this corresponds to shifting the node closest to 1 in P. Its minimum cost to node 1 is now known. At the next step, select the next closest node from set Q and update the labels corresponding to each node using:

$$D_j = \min [D_j, D_i + d_{i,j}]$$

Finally, after N-1 iterations, the shortest paths for all nodes are known, and the algorithm terminates.

Principle

Let the closest node to 1 at some steps be i. Then i is shifted to P. Now, for each node j, the closest path to 1 either passes through i or it does not. In the first case D_j remains the same. In the second case, the revised estimate of D_j is the sum $D_i + d_{i,j}$. So, we take the minimum of these two cases and update D_j accordingly. As each of the nodes get transferred to set P, the estimates get closer to the lowest possible value. When a node is transferred, its shortest path length is known. So finally, all the nodes are in P and the D_j 's represent the minimum costs. The algorithm is guaranteed to terminate in N-1 iterations and its complexity is $O(N^2)$.

C. The Floyd War shall Algorithm

This algorithm iterates on the set of nodes that can be used as intermediate nodes on paths. This set grows from a single node (say node 1) at start to finally all the nodes of the graph. At each iteration, we find the shortest path using given set of nodes as intermediate nodes, so that finally all the shortest paths are obtained.

Notation

$D_{i,j} [n]$ = Length of shortest path between the nodes i and j using only the nodes 1,2, n as intermediate nodes.

Initial Condition

$D_{i,j}[0] = d_{i,j}$ for all nodes i,j .

Algorithm

Initially, $n = 0$. At each iteration, add next node to n .i.e. For $n = 1, 2, \dots, N-1$

$$D_{i,j}[n+1] = \min \{D_{i,j}[n], D_{i,n+1}[n] + D_{n+1,j}[n]\}$$

Principle

Suppose the shortest path between i and j using nodes $1, 2, \dots, n$ is known. Now, if node $n+1$ is allowed to be an intermediate node, then the shortest path under new conditions either passes through node $n+1$ or it does not. If it does not pass through the node $n+1$, then $D_{i,j}[n+1]$ is same as $D_{i,j}[n]$. Else, we find the cost of the new route, which is obtained from the sum, $D_{i,n+1}[n] + D_{n+1,j}[n]$. So, we take the minimum of these two cases at each step. After adding all the nodes to the set of intermediate nodes, we obtain the shortest paths between all pairs of nodes together. The complexity of Floyd-Warshall algorithm is $O(N^3)$.

It is observed that all the three algorithms mentioned above give comparable performance, depending upon the exact topology of the network. The network layer is concerned with getting packets from the source all the way to the destination. The packets may require making many hops at the intermediate routers while reaching the destination. This is the lowest layer that deals with end-to-end transmission. In order to achieve its goals, the network layer must know about the topology of the communication network.

1.4 Genetic Optimization Algorithm

Genetic Algorithms (GAs) are adaptive heuristic search algorithms that belong to the larger part of evolutionary algorithms. Genetic algorithms are based on the ideas of natural selection and genetics. These are intelligent exploitation of random search provided with historical data to direct the search into the region of better performance in solution space.

They are commonly used to generate high-quality solutions for optimization problems and search problems. Genetic algorithms simulate the process of natural selection which means those species who can adapt to changes in their environment are able to survive and

reproduce and go to next generation.

In simple words, they simulate “survival of the fittest” among individual of consecutive generation for solving a problem. Each generation consist of a population of individuals and each individual represents a point in search space and possible solution. Each individual is represented as a string of character/integer/float/bits. This string is analogous to the Chromosome.

1.4.1 Foundation of Genetic Algorithms

Genetic algorithms are based on an analogy with genetic structure and behavior of chromosome of the population. Following is the foundation of GAs based on this analogy –

1. Individual in population compete for resources and mate.
2. Those individuals who are successful (fittest) then mate to create more offspring than others.
3. Genes from “fittest” parent propagate throughout the generation, that is sometimes parents create offspring which is better than either parent.
4. Thus, each successive generation is more suited for their environment.

Search space

The population of individuals are maintained within search space. Each individual represents a solution in search space for given problem. Each individual is coded as a finite length vector (analogous to chromosome) of components. These variable components are analogous to Genes. Thus, a chromosome (individual) is composed of several genes (variable components).

1.4.2 Fitness Score

A Fitness Score is given to each individual which shows the ability of an individual to “compete”. The individual having optimal fitness score (or near optimal) are sought. The GAs maintains the population of n individuals (chromosome/solutions) along with their fitness scores. The individuals having better fitness scores are given more chance to reproduce than others.

The individuals with better fitness scores are selected who mate and produce better offspring by combining chromosomes of parents. The population size is static so the room

has to be created for new arrivals. So, some individuals die and get replaced by new arrivals eventually creating new generation when all the mating opportunity of the old population is exhausted. It is hoped that over successive generations better solutions will arrive while least fit die.

Each new generation has on average more “better genes” than the individual (solution) of previous generations. Thus each new generations have better “partial solutions” than previous generations. Once the offspring’s produced having no significant difference than offspring produced by previous populations, the population is converged. The algorithm is said to be converted to a set of solutions for the problem.

1.4.3 Operators of Genetic Algorithms

Five phases are considered in a genetic algorithm.

1. Initial population
2. Fitness function
3. Selection
4. Crossover
5. Mutation

Initial Population

The process begins with a set of individuals which is called a **Population**. Each individual is a solution to the problem you want to solve.

An individual is characterized by a set of parameters (variables) known as **Genes**. Genes are joined into a string to form a **Chromosome** (solution).

In a genetic algorithm, the set of genes of an individual is represented using a string, in terms of an alphabet. Usually, binary values are used (string of 1s and 0s). We say that we encode the genes in a chromosome.

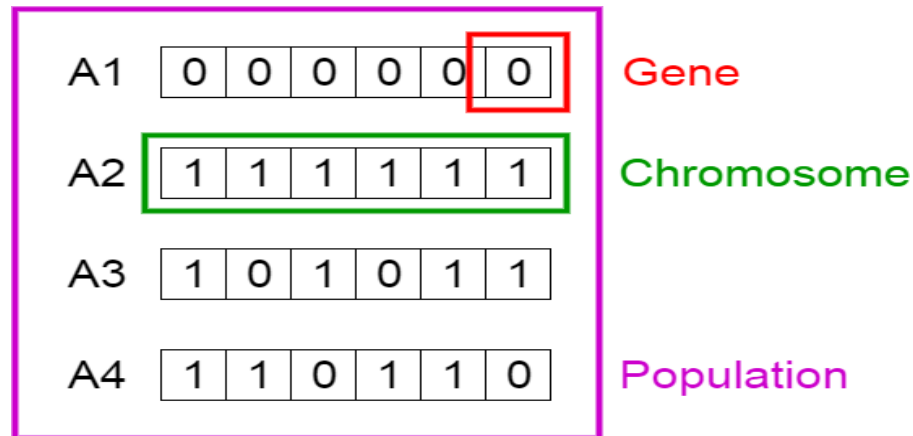


FIG 1.4.3.1 Population, Chromosomes and Genes

Fitness Function

The **fitness function** determines how fit an individual is (the ability of an individual to compete with other individuals). It gives a **fitness score** to each individual. The probability that an individual will be selected for reproduction is based on its fitness score.

Selection

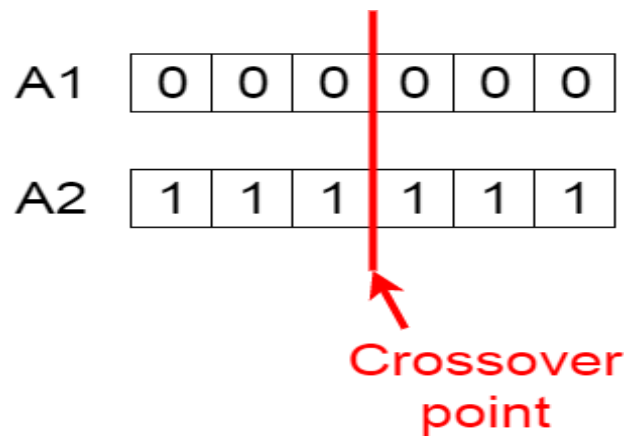
The idea of **selection** phase is to select the fittest individuals and let them pass their genes to the next generation.

Two pairs of individuals (**parents**) are selected based on their fitness scores. Individuals with high fitness have more chance to be selected for reproduction.

Crossover

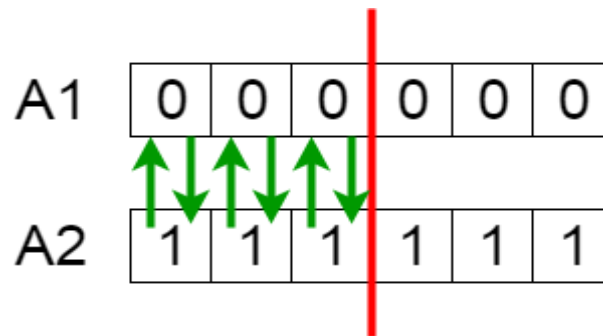
Crossover is the most significant phase in a genetic algorithm. For each pair of parents to be mated, a **crossover point** is chosen at random from within the genes.

For example, consider the crossover point to be 3 as shown below.



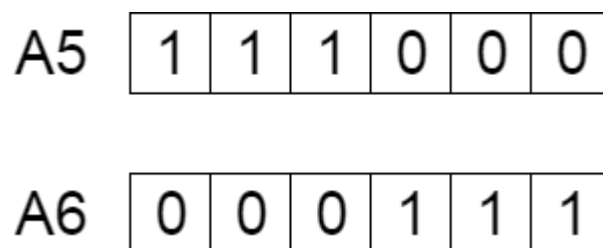
1.4.3.2 Crossover point

Offspring are created by exchanging the genes of parents among themselves until the crossover point is reached.



1.4.3.3 Exchanging genes among parents

The new offspring are added to the population.



1.4.3.4 New offspring

Mutation

In certain new offspring formed, some of their genes can be subjected to a **mutation** with a low random probability. This implies that some of the bits in the bit string can be flipped.

Before Mutation

A5

1	1	1	0	0	0
---	---	---	---	---	---

After Mutation

A5

1	1	0	1	1	0
---	---	---	---	---	---

1.4.3.5 Mutation: Before and After

Mutation occurs to maintain diversity within the population and prevent premature convergence.

Termination

The algorithm terminates if the population has converged (does not produce offspring which are significantly different from the previous generation). Then it is said that the genetic algorithm has provided a set of solutions to our problem.

Comments

The population has a fixed size. As new generations are formed, individuals with least fitness die, providing space for new offspring.

The sequence of phases is repeated to produce individuals in each new generation which are better than the previous generation.

Pseudocode

START

Generate the initial population

Compute fitness
REPEAT
 Selection
 Crossover
 Mutation
 Compute fitness
UNTIL population has converged
STOP

Why use Genetic Algorithms

- They are Robust.
- Provide optimization over large space state.
- Unlike traditional AI, they do not break on slight change in input or presence of noise

Application of Genetic Algorithms

Genetic algorithms have many applications, some of them are –

- Recurrent Neural Network
- Mutation testing
- Code breaking
- Filtering and signal processing
- Learning fuzzy rule base etc.

1.5 Routing Security

Every year, thousands of routing incidents occur, each with the potential to harm user trust and handicap the Internet's potential. These routing incidents can also create real economic harms. Key services may become unreachable, disrupting the ability of companies and users to participate in e-commerce. Or packets may get diverted through malicious networks, providing an opportunity to spy on them. While known security measures can address many of these routing incidents, misaligned incentives limit their use.

All stakeholders including policymakers, must take steps to strengthen the security of the global routing system. This can only be done while also preserving the vital aspects of the

routing system that has enabled the Internet to be so ubiquitous and improving their security. Through leading by example in their own networks, strengthening communication, and helping realign incentives to favour stronger security, policymakers can help improve the routing security ecosystem.

1.5.1 Key Considerations

At its core, the routing system is built on trust among networks. The global routing system is a complex, decentralized system made up of tens of thousands of individual networks. Independent business decisions and trusted relationships between individual network operators implementing the Border Gateway Protocol (referred to as BGP in short) determine how the network operates. The meshed system's architecture contributes to its resilience, scalability, and ease of adoption.

With no single point of failure or single controller, the routing system is difficult to break on a global level, easy to connect to and scales well. When a path becomes congested or fails, networks can choose to route traffic around the problem areas. The structure of the routing system also allows a great amount of flexibility for network operators to run their own networks. This allows network operators to develop novel network architectures and solutions to best fit the needs of their users. These qualities have made the Internet so successful and enabled its growth.

1.5.2 Challenges

While the routing system's qualities have enabled its overall success, these same attributes also contribute to some of its challenges. The system is based on chains of trust; each network relies on its neighbouring networks (which in turn rely on their own neighbors, etc.) to act appropriately. There is no built-in verification and misrepresentation can be easy. This leads to ongoing routing incidents. The complexities and decentralization of the global routing system also bring ecosystem challenges, including misaligned incentives and externalized risks posed by routing insecurity. Solutions to address many routing incidents are known, but ecosystem challenges hamper their implementation. Any efforts to address these challenges must recognize the routing system's core technical functions and maintain the benefits provided by the routing system's architecture.

There are three major types of routing incidents:

- Route/prefix hijacking, where a network operator or attacker impersonates another network operator, pretending that it is the correct path to the server or network being sought on the Internet.
- Route leaks are the propagation of routing announcements beyond their intended scope (in violation of their policies).
- IP spoofing, where someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system.

The global routing system is incredibly resilient. Its decentralized structure provides flexibility, scalability, and overall durability. While its structure has played a crucial role in the growth of the Internet, it has also enabled routing incidents to occur.

Best practices, like the Mutually Agreed Norms for Routing Security, provide a clear path for network operators to take towards addressing these routing threats. However, all stakeholders, need to take actions to address the ecosystem challenges preventing the widespread application of best practices.

Only through collective action, can we address the challenges of routing security while maintaining the benefits of a decentralized routing system.

CHAPTER 2

LITERATURE REVIEW

2.1 Energy Aware Probabilistic Broadcasting for Mobile Ad hoc Network

Broadcasting is the primary procedure employed in Mobile ad hoc network for different kinds of functions like sending data and route discovery. Simple flooding is the direct method for broadcasting which can degrade the network performance. To resolve the broadcast storm issue which potentially leads to contention, collision and replicated messages, recently a new probabilistic approach has been proposed. In this paper we put forward this new probabilistic approach, namely Energy aware probabilistic broadcasting which ameliorates the network performance by decreasing the RREQ overhead in route discovery phase. In comparing the simulation results of AODV which employs blind flooding and fixed probability against the combination of AODV and the presented probabilistic broadcasting, the later has been found to reduce both overhead as well as the end-to-end delay.

In broadcast communication which is an extremely useful collective communication operation, the sender node forwards the same packet to the rest of the nodes in the network. For overall performance of a network, broadcasting efficiency is important as it is used widely. Some of the important applications of broadcasting are data movement, resource discovery and advertisements, etc. Broadcasting is elementary for the implementation of major higher-level communication programs as it offers the needed control and route establishment functionality for these. The examples of such operations that use broadcasting as their fundamental block are barrier synchronization, gossip, gather, etc. Efficient implementation of broadcast communication is a necessity for ensuring an adaptive implementation of a variety of distributed applications.

Broadcasting technique is not only a fundamental part of protocols like AODV and Dynamic Source Router (DSR) but also an approach that allows to send out control and data packets between mobile devices in MANET. However, the overall efficiency and the performance in MANETs is impacted due to issues like collisions and contention, duplicate transmission; these issues are referred to as the broadcast storm problem. In the standard on-demand routing protocols like AODV.

A mobile host floods the Route request control packet (RREQ) to its neighbors in order to find out a route to an unambiguous destination, followed by each neighbor

resending the RREQ control packets to setup the path between source and required destination. Broadcasting has been the default approach in many distributed and networked systems.

The node choice is a vital part in designing the proposed scheme. Thus, in this analysis, we classify the mobile nodes as Dependable (DNs) and Non-dependable (NDNs) with respect to the remaining energy of a node. Note that, DNs are those nodes which have a sufficient remaining energy and are more likely to broadcast. On the other hand, NDNs are those nodes with less amount of remaining energy. Therefore, any retransmission by NDN should be buried in order to avoid early link failure due to dead nodes having limited battery and decrease overhead of routing packets. So, the method to decide which node is DN and which is NDN is taken on the basis of threshold energy. The nodes, for which the remaining energy is less than the threshold, will be categorized as NDNs; else DNs.

To calculate the average energy of any network, we need to exchange packets and for this we modify the existing control packets in AODV to broadcast the required energy information instead of adding new control packets. HELLO packet: All nodes in EAPB make use of the HELLO packet in AODV to exchange the information of their remaining energy among each other. In order to accumulate such information, a new field called Remaining Energy is added to the HELLO packet. With the help of the HELLO packet, every node creates a Local Remaining Energy Table (LRET), which store the remaining energy of all one-step neighbors.

The proposed protocol is based on the remaining energy of the node and the average energy of the whole network, which adjusts the rebroadcast probability adaptively and differentiates nodes according to energy and uses high energy nodes more for rebroadcasting. As the number of rebroadcasts are saved which further decreases the overhead? The main advantage of this scheme is to utilize high energy nodes, which further increase the link stability and avoid route discovery each time after link failure in AODV. Thus, EAPB overcomes the existing shortcomings of AODV.

i.e., Link stability and overhead. Other parameters like velocity with remaining energy for categorization of the nodes can be incorporated to further enhance the performance of the algorithm.

2.2 Energy Efficient Probabilistic Broadcasting for Mobile Ad-Hoc Network

In mobile ad-hoc network (MANETs) flooding method is used for broadcasting route request (RREQ) packet from one node to another node for route discovery. This is the

simplest method of broadcasting of RREQ packets but it often results in broadcast storm problem, originating collisions and congestion of packets in the network. A probabilistic broadcasting is one of the widely used broadcasting scheme for route discovery in MANETs and provides solution for broadcasting storm problem. But it does not consider limited energy of the battery of the nodes. In this paper, a new energy efficient probabilistic broadcasting (EPPB) is proposed in which probability of broadcasting RREQs is calculated with respect to remaining energy of nodes.

The analysis of simulation results clearly indicates that an EPPB route discovery scheme in ad-hoc on demand distance vector (AODV) can increase the network lifetime with a decrease in the average power consumption and RREQ packet overhead. It also decreases the number of dropped packets in the network, in comparison to other EPPB schemes like energy constraint gossip (ECG), energy aware gossip (EAG), energy-based gossip (EBG) and network lifetime through energy efficient broadcast gossip (NEBG).

A new scheme EPPB is proposed which overcomes the shortcomings of previously proposed scheme AODV_EAPB as mentioned earlier while using the same concept of categorizing the nodes as DNs and NDNs and changing the fixed timer used in a previous scheme to variable timer depending on the DNs and NDNs. In this segment, the proposed EPPB technique will be explained in detail. The definition of various EPPB parameters is specified in Table1. The method for determining the energy threshold is calculated by using local average energy of all the nodes.

The objective of our algorithm is to broadcast a control packet depending upon their remaining energy and also balancing energy utilization among all nodes in the network. For calculating the average energy of the network, one needs to have information of all nodes of network for this exchange of packets. Therefore, in place of adding new control packets for this purpose, the existing control packets in AODV for sending the essential energy knowledge of other nodes are changed. The remaining energy of all nodes in EPPB is exchanged between all nodes by using HELLO packets in AODV.

For accumulating this knowledge, a fresh field named remaining energy (Pr) is inserted in HELLO packet. EPPB uses the modified RREQ of AODV for broadcasting in the route discovery process and as well as to get the local average remaining energy knowledge downside the node path traced by the packets.

So, in our proposed scheme (EPPB) following are the advantages as compared to other existing protocols:

- The proposed algorithm decreases the rebroadcast figure without considerable negotiation on its reachability.
- In EEPB scheme the RREQ packets are broadcasted with a smaller number of nodes than the original probability schemes where fixed probability or blind flooding is used.
- By using the EEPB scheme, the nodes having more energy are used which further increases the network lifetime.

Mainly the battery usage of EEPB gets better in contrast to that of traditional AODV with fixed flooding. The EEPB performs best at each and every point of the node density range as compared with other four protocols. The reason for this improvement is mainly due to categorization of nodes as DNs and NDNs on the basis of remaining energy of nodes whereas the other four protocols do not use categorization concept. The EAG protocol uses additional battery in contrast to NEBG and EBG because they employ multipoint relay scheme. Other than this it performs exceptionally well in contrast to ECG as the node number within the network is near about 100 nodes because of stochastic traffic (Pareto traffic) use instead of CBR in ECG. In contrast, the energy usage within any network implemented with ECG as well as EAG increases rapidly starting from quite elevated levels.

EEPB technique for transmitting RREQ packets is proposed and implemented in the AODV routing protocol for MANETs which outperforms the other EEPB techniques. As compared with other probability-based broadcasting techniques where every node broadcast with fixed probability without considering the remaining energy of the nodes. The proposed scheme in this paper decides probability of RREQ broadcast depending on the remaining energy of the nodes. Further, one may intend to implement a new parameter such as velocity and node density along with remaining energy of nodes in the route discovery phase, which involves another extensive research for analyzing, whether it can remove the broadcasting storm problem or not with increasing link stability.

2.3 Distance based Cluster Head Selection Algorithm for Wireless Sensor Network

A distance-based Cluster head selection algorithm is proposed for improving the sensor network lifetime. This protocol achieves a good performance in terms of lifetime by balancing the energy load among all the nodes. This clustering technique help to prolong the life of wireless sensor network, especially in hostile environment where battery replacement of individual sensor nodes is not possible after their deployment in the given target area.

Therefore, the proposed technique to distribute the role of the cluster head (CH) among the wireless sensor nodes in the same cluster is vital to increase the lifetime of the network. This algorithm uses a distance-based method for providing the cluster head

selection. Clustering techniques also provide good load balancing, and in-network data aggregation.

Obviously, WSNs need to be stable in design and structure to transfer data among the wireless sensors safely and without any problems, because of their use in critical areas and real time systems. Moreover, consuming less energy and increasing the lifetime of the wireless sensor nodes are the main objectives in designing the WSN, because of the limitation of the power resources and the difficulties of replacing the batteries of the wireless sensors.

Dividing the sensor networks into small manageable units is called as clustering & process known as clustering process. Though the main reason behind the implementation of the clustering approach is to improve the scalability of the network (prolong), it is an important factor in achieving energy efficient routing of data within the network.

Study on energy efficient routing in WSN brings this two-broad classification of approaches. They are,

- Clustering approach
- Tree based approach

In a wireless sensor network, cluster is a group of sensor nodes in which one node will act as a cluster head (CH), and remaining nodes will act as member nodes. Clustering helps in reducing the number of exchanged communications in wireless sensor network resulting in low consumption of battery power of individual sensor nodes.

This increases the life span of the wireless sensor network. A cluster head is selected for each cluster based on the energy level of that node or distance based also. The main objective is to make only the cluster head communicate with the base station so that the remaining node can be put to a sleep state. Sensors measure real-world conditions, such as heat or light, and then convert this condition into an analogue or digital representation.

Many greedy algorithms have been proposed to choose cluster heads in ad hoc networks, and wireless sensor networks. They are based on the criteria of highest degree, lowest- ID, highest-ID, and node-weight, residual energy, probability, and any combination of these. The clustering techniques can also be classified based on cluster size, namely Single hop, and Multi-hop.

HEED (Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach) periodically selects cluster heads according to a combination of their residual energy, and communication cost. Distributed Weight-Based Energy-Efficient

Hierarchical Clustering (DWEHC) is modified version of the HEED. It claims to provide more balanced cluster size and intra cluster topology. HEED uses two clustering parameters to select CH: one is residual energy, and the other is communication cost. The communication cost is defined as an average minimum reach ability power, which means the minimum power levels required by all nodes within the cluster range to reach the CH. The communication cost held by CHs is used to let a node which belong to several CHs choose the best one.

In HEED, each node must be mapped to exactly one cluster, and each node belongs to its only CH within one hop. After a clustering process, each node can either elect to become a CH due to a probability or join a cluster according to CH messages.

In clustering hierarchy, the cluster head decision is a major challenge. If network is taken as a whole, then the power consumption can be optimized by the rotation of this cluster head inside the individual clusters. Energy conservation is a significant concern in the WSNs, especially as the energy conservation of the cluster head in the cluster- tree network has to be higher because of the different operations, which they control in the network. In this paper, a new technique is proposed to select cluster head among some of the wireless sensor nodes based on net distance with base station. The proposed technique aims to increase the lifetime of the whole network, and to increase the number of nodes, which will remain alive for the maximum period of time.

2.4 Detection and Prevention Mechanism for Black hole Attack in Wireless Sensor Network

Wireless Sensor Networks (WSNs) are prone to various attacks in which Blackhole a kind of Denial of Service (DoS) attack is very difficult to detect and defend. In blackhole attack, an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result, any information that enters the blackhole region is captured and not able to reach destination causing high end- to- end delay and low throughput. Previously little amount of work is done for detection and prevention of the Blackhole attack in the WSN making its detection and prevention very crucial as per network performance is concerned. In this paper initially the effect of Blackhole attack is measured on the network parameters followed by the proposal of a novel technique for the detection and prevention of Blackhole attack in WSN.

Sometimes the sensitive data is communicated to the destination node through an insecure medium. Thus, WSN can be easily attacked by Denial-of Service (DoS) attacks,

which cause information loss along with large energy expenditure. Therefore, securing the links is important in designing a sensor network. Blackhole attack is also DoS in nature. Blackhole attacks occur when an intruder captures and re-programs a set of nodes in the network to block the packets, they receive instead of forwarding them towards the base station. As a result, any information that enters in the blackhole region is captured and does not reach destination. This produces long delay in packet delivery and decreases the throughput of the network.

So, detection prevention of this attack is necessary. We have proposed a mechanism for detection and prevention of Blackhole attack in WSN which is Cluster based. In this technique a coordinator is elected by all sensor nodes depending upon the selection criteria (fairness and efficiency). Coordinator is responsible for authentication, checking of the failure of intermediate node and detection of Blackhole attacker if present in the network.

Blackhole attack is a kind of denial of service (DoS) in nature. When Blackhole attack occurs in WSN it affects the performance of network especially the end-to- end delay and throughput. In this paper we have initially measured the impact of Blackhole attack on the performance of WSN which degrades rapidly. So it becomes very important to detect and prevent Blackhole attack as the detection and prevention techniques for the Blackhole attack occurring in WSN are missing in the previous research. In this paper we are proposing the same.

Black hole attacks occur when an intruder captures and reprograms a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result, any information that enters in the black hole region is captured. Black hole attacks are easy to constitute, and they are capable of undermining network effectiveness by partitioning the network, such that important event information do not reach the base stations. The network performance parameters i.e., throughput and end- to-end delay are affected in the presence of blackhole nodes; throughput becomes very less and end- to-end delay increases. Due to Blackhole attack packets does not reach the destination within time.

producing long delay in the network and decrement in throughput.

Here we have proposed a blackhole attack detection and prevention mechanism which detects the blackhole attacker node and also prevents this attack from occurrence. In the proposed mechanism we build clusters from sensor nodes. Cluster contains nodes which are in the communication range of each other. A cluster coordinator (Co) is elected by the sensor nodes. Election of a cluster coordinator requires two things to be considered.

Fairness: Any node can become cluster coordinator meaning that the probability of

every node to be a cluster coordinator should be equal.

Efficiency: There should be some method that can select a node from the cluster periodically which has high efficiency (i.e., battery backup). When cluster is formed, cluster coordinator is elected, and it becomes the responsibility of the cluster coordinator to detect the intruder node in that cluster. All the sensor nodes are in the supervision of coordinator node.

In the presence of blackhole attack both parameters of network i.e., End-to-end delay and Throughput are affected. We have observed that in the presence of blackhole attack the performance of network degraded very rapidly. The End-to-end delay increases to 4.03 msec and throughput decreases to 5027.85 bps. So, it has become important to provide a detection and prevention mechanism for blackhole attack. The proposed algorithm is capable to detect and prevent the Blackhole attack occurring in the WSN.

In future this work can be extended with varying number of attackers. This analysis is done only for tree topology so can also add some more topologies.

We can implement this algorithm in Blackhole prone WSN where it will efficiently detect and prevent the Blackhole attack especially in defence sector.

2.5 The Security Issue of WSNs Based on Cloud Computing

The combination of WSNs and cloud computing actually does overcome the problems such as storage issues, real-time processing aporia, and ubiquitous accessibility challenge due to the low-power, small-size characteristics of WSNs. But there still exist some other issues, particularly security issues. In this paper, we present a pub/sub based framework of the combination paradigm, and we discuss about the advantages and disadvantages including the security challenges of the new paradigm. Finally, the solutions to security problem will be presented at last.

As Cloud computing may become ubiquitous in future, researchers consider the probability of combining WSN with cloud computing to solve the problems which are owing to the unique property of WSN. In fact, the combination does overcome some challenges such as storage problems and accessibility, the on-demand services characteristic that cloud services provide is an attracting property for most small-size enterprises who have limited resource. But vulnerabilities still exist, especially in security issues. According to an International Data Corporation (IDC) survey in 2008, security is a main consideration issue. In this paper, we focus on the framework for the new combination of WSNs and cloud and its security framework description. After presenting the new framework model, the security challenges of the new paradigm analysis are given.

In our proposed framework, the publish/subscribe model is utilized as one of the

major basic architecture. A pub/sub system enables subscribers to get their desired data from the system after they register to it and express the interested events, as long as the publishing data arrives at the interface of the system after filtering and classifying, the system sends the subscriptions to subscribers via some sorts of channel. In fact, a pub/sub system has already been the first choice for integrating WSN to cloud recently because of its very nature that subscribers can get the desired data in real-time or near real-time, due to which researchers in some special areas, e. g., health care, climate changing, the smart grid and disaster monitoring could get vital information in time.

Another basic architecture of the proposed framework is pipes and filters, which can always be noticed in digital signal processing, but it also works well in domain of WSN. In our model, pipes do not store or process sensing data, their main purpose is buffering data and providing filters with a uniform format data instead.

And the data is transmitted through an output port at the end of pipes. The output port is connected to a filter, whose main job is slightly modified the data from pipes via some algorithms designed to eliminate noise mixing in raw data. We make a filter chain which can be constructed by certain number of pipes and filters, a filter chain can be regarded as the gateway used to transmit sensing data to cloud.

On the WSN side, it works just like normal WSN systems except that all the sensing data are transported to the bridge, which is the filter chains and three layers in our circumstance. On the cloud side, consumers of cloud services mostly urge real-time data, that's the most valuable property of pub/subbased sensor-cloud, in order to implement the idea, the brokering layer is connected to specific applications of SaaS. Consumers can get their subscriptions by registering to the applications and browsing via the Internet.

The cloud-side workflow is as follows:

- 1) Consumers of cloud services register their information and subscription to specific SaaS application.
- 2) The subscriptions are transmitted to the brokering layer, which will classify and organize the subscriptions by the subscription attributes.
- 3) Brokering layer sends the classified subscriptions to the interaction layer.
- 4) The subscriptions are compared with the publications coming from a publishing layer, if certain data suits the subscription, then the data will be sent to the SaaS application registered by the consumer, and applications send the data to its consumer, otherwise, the publishing data will be sent to IaaS or DaaS of cloud.

The security challenges we discuss mainly focus on data security through the whole workflow, especially on the architecture integrating WSNs to cloud instead of data security in WSNs or cloud services, otherwise, it may perform beyond the topic of the paper.

The new framework of combination of WSNs and cloud and its security challenges are presented. We pointed out pros and cons of this combined system. The analysis of security issues for the combination paradigm is given and some solutions are offered to solve corresponding problems. But there still exist many challenges unsolved, we are hoping researchers can provide appropriate solutions on this area, and sensor-cloud can develop prosperously.

2.6 Cluster Head Selection Protocol using Fuzzy Logic for Wireless Sensor Networks

Recent trends in field of wireless networks are setting up Wireless Sensor Networks that, senses specified parameter(s) related to environment; processes sensed data and wirelessly communicates it to a base station. Such networks open up a whole new range of applications, including precision agriculture, monitoring and tracking vehicles, animals and humans, battle-field surveillance, civil structural monitoring etc.

All these applications require extended network lifetime, scalability, and traffic balancing among nodes in the network. Clustering is one of the effectual techniques for achieving these requirements. In clustering, geographically adjacent nodes are organized into virtual groups called clusters. One of the cluster node acts as a cluster head and rest as cluster members. This paper presents Cluster Head selection protocol using Fuzzy Logic (CHUFL). It uses node's parameters like residual energy, reachability from its neighborhoods, quality of communication link with its neighborhood and distance from base station as fuzzy input variables for cluster head selection.

The proliferation in Micro Electromechanical Systems (MEMS) technology for the development of smart sensors and advances in wireless communication technologies have geared growth in the field of Wireless Sensor Networks (WSN). Nodes in WSN are densely deployed in hostile environments where they may technically fail, die due to lack of power, be physically damaged or may face environmental interference. Further, nodes have severely limited computational, storage and power capabilities. This demands energy efficient techniques to be used at all the stages of WSN protocol design.

Clustering is one of techniques to prolong the network lifetime. In a clustering protocol the geographically adjacent nodes are organized into virtual groups called "clusters". One of the nodes is selected as a cluster head and rest in its neighborhood as cluster

members. Clustering offers following advantages:

- (i) reduces collision during intra-cluster communication by coordinating media access mechanism of its cluster members
- (ii) offers load balancing by rotating cluster head
- (iii) reduces amount of information updates required (node deaths and joins in a cluster, need to be updated only by their cluster members)
- (iv) offers scalability and spatial reuse (non-neighbor clusters may use same frequency or code for transmission).

In clustering protocol, cluster head works as a local coordinator for its cluster and does following: (i) arranges intra-cluster transmission schedule (ii) collects data from its cluster members (iii) combines several correlated data signals into a smaller set of information (data aggregation) (iv) forwards data to Base Station (BS). Several computational intelligence techniques like fuzzy logic, neural networks, reinforcement learning, swarm intelligence, evolutionary algorithms, artificial immune systems and reinforcement learning have been proposed for cluster head selection in WSN.

For WSN protocol design fuzzy logic offers following advantages: (i) the terms used in WSN protocol's performance ("lower latency", "longer lifetime") and the transmission media characteristics ("less noisy", "more busy") make their fuzzy representation easy and realistic. (ii) it can easily and efficiently deal with various uncertainties of WSNs, such as unreliable media, unpredictable changes in network topology and still arrive at a definite conclusion. (iii) fuzzy logic is flexible, scalable, fault tolerant, requires less system development cost, resources (computation and memory requirements) and design time.

Nodes make independent decisions for becoming cluster heads using fuzzy logic without any central control as discussed below. Fuzzy Inference System (FIS) design for cluster head selection: Mamdani Model is used for developing FIS for cluster head selection since it is simple, has widespread acceptance and is well suited to imprecise inputs. FIS design steps are discussed next. Fuzzification of inputs and outputs: Input variables: Residual Energy (indicated as RESIDUAL_ENERGY): For node to become a cluster head it should have more RESIDUAL_ENERGY compared to its neighbouring nodes. Node's reachability (indicated as REACHABILITY): It is measure of how much the node is reachable to its neighbor nodes within its transmission range.

Protocols for WSN require to be energy efficient and reliable. These features led to design of CHUFL, a clustering protocol which minimizes energy consumption of cluster head by choosing cluster heads nearer to BS, having more residual energy and neighbors.

Reliability of the protocol is increased by choosing cluster heads with a high value of LQI. Simulation results show that CHUFL provides best performance under tight energy, memory and computational constraints of the nodes and constraints of wireless transmission media compared to protocol by Indranil et.al., CHEF and protocol by Anno.

2.7 CHEF: Cluster Head Election mechanism using Fuzzy logic in Wireless Sensor Networks

In designing the Wireless Sensor Networks, the energy is the most important consideration because the lifetime of the sensor node is limited by the battery of it. To overcome this demerit many research have been done. The clustering is the one of the representative approaches. In the clustering, the cluster heads gather data from nodes, aggregate it and send the information to the base station.

In this way, the sensor nodes can reduce communication overheads that may be generated if each sensor node reports sensed data to the base station independently. LEACH is one of the most famous clustering mechanisms. It elects a cluster head based on probability model. This approach may reduce the network lifetime because LEACH does not consider the distribution of sensor nodes and the energy remains of each node. However, using the location and the energy information in the clustering can generate big overheads.

In this paper we introduce CHEF-Cluster Head Election mechanism using Fuzzy logic. By using fuzzy logic, collecting and calculating overheads can be reduced and finally the lifetime of the Sensor Networks can be prolonged. To prove efficiency of CHEF, we simulated CHEF compared with LEACH using the Matlab. Our simulation results show that CHEF is about 22.7% more efficient than LEACH.

Designing the WSNs is very difficult because the sensor nodes have limited computation capability, limited power and small memory size. Among these three factors, the energy consumption is the most important one because the battery is not changeable if once the sensor nodes are deployed. The energy is also the major consideration in designing the routing of the WSNs. One kind of the famous routing algorithms to achieve the energy efficiency is cluster routing.

In the cluster routing, sensor nodes divide into some number of groups and form clusters. In each cluster, one sensor node is the head of the cluster and is called the cluster head. The Cluster head collects data from nodes within the cluster and aggregates the data and report the aggregated information to the base station. By making only the cluster head communicate with the base station, the overheads that can be occurred if all nodes in that

cluster communicate with the base station would be reduced.

To maximize the lifetime, we introduce CHEF that is a localized cluster head election mechanism using fuzzy logic. This paper defines some factors that can affect the lifetime. Based on these factors, we apply the fuzzy if-then rule to the cluster head election mechanism. By using fuzzy logic, the computational overhead is reduced, and the network lifetime is extended. In addition, the operation of this mechanism is localized. The base station does not collect and elect cluster heads. The sensor nodes only elect cluster heads among themselves using the fuzzy logic.

The basic system model of this paper is depicted in Figure

Each sensor node sends the sensed data to its cluster head. The cluster head aggregates the collected data and transmits the aggregated information to the base station. This operation is general in the WSNs. Here are some assumptions for our mechanism. The WSNs consist of the homogeneous sensor nodes. The distance can be measured based on the wireless radio signal power. Once deployed, the nodes dose not move. All sensor nodes have the same initial energy. The base station is located in the outside of the WSNs.

Energy and distance is considered in electing cluster heads. This makes the more efficient cluster heads are elected and finally the network lifetime is extended. By using fuzzy logic, the calculation overhead is minimized. The cluster head election is localized. The overhead that comes from centralized process can be reduced. Any two cluster heads cannot exist within r distance.

The energy is the major factor in designing the WSNs. To achieve the energy efficiency, many clustering algorithm is proposed and LEACH is the representative one. LEACH uses the probability model to distribute the concentrated energy consumption of the cluster heads. However, it only depends on the probability model and the energy efficiency is not maximized.

In this paper, we proposed a cluster head election mechanism-CHEF. We evaluated CHEF compare with LEACH using the matlab. The simulation results show that CHEF is 22.7% more efficient than LEACH. This is because the energy and local distance is considered in electing cluster heads.

Although we compared CHEF with LEACH, there are many clustering algorithms that have to be compared and there are many factors that can affect the network lifetime. A further direction of this study will be to find the optimal fuzzy set and to compare the enhanced version of CHEF with other clustering algorithms.

2.8 ACE: An Emergent Algorithm for Highly Uniform Cluster Formation

The efficient subdivision of a sensor network into uniform, mostly non-overlapping clusters of physically close nodes is an important building block in the design of efficient upper layer network functions such as routing, broadcast, data aggregation, and query processing.

We present ACE, an algorithm that results in highly uniform cluster formation that can achieve a packing efficiency close to hexagonal close packing. By using the self-organizing properties of three rounds of feedback between nodes, the algorithm induces the emergent formation of clusters that are an efficient cover of the network, with significantly less overlap than the clusters formed by existing algorithms. The algorithm is scale-independent — it completes in time proportional to the deployment density of the nodes regardless of the overall number of nodes in the network. ACE requires no knowledge of geographic location and requires only a small constant amount of communications overhead.

Clustering is a fundamental mechanism to design scalable sensor network protocols. A clustering algorithm splits the network into disjoint sets of nodes each cantering around a chosen cluster-head. A good clustering imposes a regular, high-level structure on the network. It is easier to design efficient protocols on this high-level structure than at the level of the individual nodes. Many efficient protocols rely on having a network partitioned into clusters of uniform size.

Conventional algorithms that use centralized control and global properties of the sensor network have inherent difficulties in the properties of scalability and robustness, which are two important design goals for protocols in large-scale sensor networks. Centralized, top-down algorithms often need to operate with knowledge of the conditions and variables at every point of the network.

In a very large network, the network traffic and time delay induced by the collection of this large amount of data may be undesirable. Finally, since some specific nodes, commands or data are usually of higher importance in a centralized protocol, an error in transmission or a failure of a critical node could potentially cause a serious protocol failure.

As an alternative to centralized algorithms, localized algorithms reduce the amount of central coordination necessary and only require each node to interact with its local neighbors. While sometimes harder to design, these algorithms do not have the limitations of centralized algorithms and are often highly scalable, fast and efficient.

Here provides an introduction to the definitions and motivations of localized and emergent algorithms. To demonstrate the potential of emergent algorithms in sensor

networks, we present a new emergent protocol for node clustering called ACE (for Algorithm for Cluster Establishment). ACE has high cluster packing efficiency approaching that of hexagonal close-packing, and only incurs a small constant amount of communications overhead. ACE is scale independent and operates without needing geographic knowledge of node positions or any kind of distance or direction estimation between nodes.

Efficiently organizing sensor nodes into clusters is an important application in sensor networks. Many proposed protocols for both sensor networks and ad-hoc networks rely on the creation of clusters of nodes to establish a regular logical structure on top of which efficient functions can be performed. For example, clustering can be used to perform data aggregation to reduce communications energy overhead; or to facilitate queries on the sensor network; clusters can be used to form an infrastructure for scalable routing; clustering also can be used for efficient network-wide broadcast. Single-level clustering is sufficient for many applications; for others, multi-level hierarchical clustering can be performed.

ACE (the Algorithm for Cluster Establishment), an emergent cluster formation algorithm. The algorithm consists of two logical parts — the first controls how clusters can spawn (by having a node elect itself to be leader) and the second controls how clusters migrate dynamically to reduce overlap. In general, clusters are only created when the overlap of the new cluster with existing clusters is small. After creation, clusters will move apart from each other to minimize the amount of mutual overlap, thus yielding a near-optimal packing in very few iterations.

ACE, the Algorithm for Cluster Establishment. ACE is an emergent algorithm that uses just three rounds of feedback to induce the formation of a highly efficient cover of uniform clusters over the network. This efficiency of coverage approaches that of hexagonal close-packing. ACE is fast, robust against packet loss and node failure, and efficient in terms of communications. It completes in constant time regardless of the size of the network and uses only local communications between nodes.

The algorithm does not require geographic location information or any kind of distance or directional estimation between nodes. Besides its practical usefulness, ACE is a good demonstration of the power and flexibility of emergent algorithms in large-scale distributed systems.

2.9 Intelligent probabilistic broadcasting in mobile ad hoc network: a PSO approach

MANETs are collection of independent nodes, which communicate with each other to perform a task. Broadcasting methods are widely used in this infrastructure less networks. Although broadcasting is easy to implement and a method to perform routing and safety

functions, in a wide and high mobility MANET it is a difficult and expensive task to achieve. It is required that the underlying algorithm used for communication must consider parameters such as neighborhoods density, the size and shape of the network, and the efficient use of channel. Probabilistic strategies are frequently used, as they do not introduce additional latency.

Several researchers have proposed using various parameter instances which are managed dynamically, for instance, the change in the number of neighbor nodes and corresponding change in retransmission probability. But the authors did not optimize the parameters for specific environments. The proposed work in this research article suggests and determines the most efficient strategy for each node to decide the retransmission probability according to its neighborhood density, available bandwidth and remaining energy of a node.

It describes a tool combining a network simulator (ns 2) and a particle swarm optimization algorithm. Then, it is applied to the MANET broadcasting problem. The simulation results show that the proposed particle swarm optimization probabilistic broadcasting (PSOPB) scheme is reliable and efficient in comparison with the other artificial intelligence broadcasting schemes such as elitist simulated binary evolutionary algorithm (ESBEA), multi-objective problems with Pareto front solution (MOP_PF) and efficient fuzzy logic-based probabilistic broadcasting (EFPB).

This system is said to be philanthropic for the reason that all nodes within the network does not consider only about their own benefit. In addition, it considers the relation and the possible recipient's advantages to allocate precedence to the messages. So, in all of these techniques, deciding the values of the factors (like lowered and higher bounds of probability as well as threshold values) is the most important difficulty.

In best cases, a small number of authors have presented procedures to adjust these factors or to calculate them, but they have not optimized them for a variety of situations. In this article, we put forward a scheme that uses three parameters: the node density, remaining energy and available bandwidth to adjust the probability of broadcasting through fuzzy logic and particle swarm optimization.

Employing these three factors, we have designed a self-reliable scheme that considers the network topology framework in relation. Our goal is to reduce the broadcasting storm problem which is due to the contention and collision of broadcast packets and has opened a new window of research issues.

In two-dimensional PSO, each particle is thought to be a probable key to the numerical optimization issue in a two-dimensional space. The PSO process based on the

above conception can be explained as follows. The bird flocking process optimizes a certain object function. Every agent identifies its preeminent value so far (p best) as well as its XY location. Moreover, every agent has the knowledge of the preeminent value within the group (g best) between bests. For changing its location, every agent employs the present velocity as well as the distance from pbest and gbest. The changes can be characterized in requisites of velocity. The velocity of every agent can be modified using the subsequent equation.

The proposed PSOPB algorithm forecasts the node density, remaining energy and available bandwidth based on factors such as relative mobility of the nodes, energy drain rate as well as link capacity, respectively. It is illustrated below. A. Fuzzy logic-based probability determination in PSOPB This technique involves the prediction of broadcasting probability by the fuzzy logic technique. We have employed Mamdani's method in the inference process as it is more frequently used in applications the steps to determine the fuzzy rule-based interference are as follows: there are five steps as shown in Fig.1 to get the crisp value from our FIS system.

The purpose of this work is to apply the idea of PSO for deciding the probability in probabilistic broadcasting in MANETs. The speculative structure selected is based on the seek for food by swarms. Folks, add evolutionary benefit of membership information along with a crowd when a mission is given to them. The proposed scheme in this paper decides the probability of the RREQ broadcast depending on the output of fuzzy controllers, which depend on the node density, remaining energy and available bandwidth of the nodes.

Moreover, PSOPB achieves better results as compared to elitist simulated binary evolutionary algorithm (ESBEA), multi-objective problem with Pareto front solution (MOP_PF) and efficient fuzzy logic-based probabilistic broadcasting (EFPB). Further, the same technique can be implemented also with the other parameters such as node velocity. It can be used in the route discovery phase and analyzed whether it can remove the broadcasting storm problem with increasing link stability.

2.10 Two-dimensional particle swarm optimization algorithm for load flow analysis

Methods generally used for load flow analysis have been found to be time consuming and complex. This paper presents an optimization algorithm for load flow analysis inspired from swarm optimization techniques. Particle swarm optimization (PSO) is a type of swarm intelligence that is based on social-psychological principles and provides insights into social behavior, as well as contributes to engineering applications. This algorithm optimizes the power flows on different branches of network using the particles memory-based algorithm. The feasibility of the concept has been proved by performing simulations in ETAP

environment.

A PSO system follows social behavior of the birds and based on social behavior the swarms improve their knowledge and in each iteration they get adapted to that new value. Based on the updated results PSO works as a simulator for different applications. The features of the method are described as follows: This method is based on research on swarms such as fish schooling and bird flocking. The computation time is short and it requires small amount of memory. It was originally developed for nonlinear optimization problems with continuous variables. However, it can be also used to solve problems with discrete variables.

Thereby, it can be applied to mixed integer nonlinear optimization problems with both continuous as well as discrete variables. The above features are suitable for load flow problems as well as for Voltage Control problem because practically efficient methods have not been developed for nonlinear problems with both continuous and discrete variables. The above features allow PSO to handle the load flow problem and also require less computation time.

According to the research performed, bird flocking phenomenon, birds find food by flocking (not by each individual). It leads to the assumption that information is shared in flocking. It has been seen from the observations made about behavior of human groups and behavior of each individual i.e. agent, that each individual's behavior is also based on behavior patterns governed by the groups such as customs and other behavior patterns according to the experiences by each individual. This basic assumption is the underlying concept of PSO.

PSO procedures based on the above concept can be described as follows. The bird flocking procedure optimizes a given objective function. Each agent knows its best value so far (pbest) and its XY position. Also, each agent has the information of the best value in the group (g best) among pbests. For modifying its position, each agent uses the current velocity and the distance from pbest and gbest. The modification can be represented in terms of velocity.

PSO makes use of several searching points like Genetic Algorithm (GA) and the searching points gradually get close to the global optimal point using its pbest and gbest. The features of the searching procedure can be summarized as follows:

- (i) Initial positions of pbest and best are different. By using the different direction of pbest and gbest all agents gradually move towards the global optimum.
- (ii) The modified value of the agent position is continuous, and the method can be applied to the continuous problem. However, the method can be applied to the discrete problem using grids for XY position and its velocity.
- (iii) There is no inconsistency in searching procedures even if continuous and discrete state.

variables are utilized with continuous axis and grids for XY positions and velocities. The method can be used for solving mixed integer nonlinear optimization problems with continuous and discrete state variables naturally and easily.

The particle movement is influenced by the three major components: memory, inertia and co-operation. The movement results in new positions of particle with updated data. The movement of particle start from the current position and it is influenced by the best position of his life as well as the best position found by the other particle in their life. Load flow analysis is the solution of the network under steady state condition subject to certain inequality constraints under which the system operates. Load flow calculation provides the power flows and voltages for a specified power system subject to the regulating capabilities of the generator, condensers and specified net interchange between individual operating system.

The objective of this work was to use the concept of particle swarm optimization for the nonlinear load flow optimization. PSO has been used for power system management. The theoretical framework chosen was based on the search of swarms for food. Individuals gain evolutionary advantage by sharing information among group when a task is given to them. This idea leads to the search of solution into an optimization problem. The initial aim of the particle swarm concept was to graphically simulate the graceful and unpredictable choreography of a bird flock, the motive of discovering patterns that govern the ability of birds to fly synchronously, and to suddenly modify direction with a regrouping in an optimal fashion. From the initial objective, the concept evolved into a simple and efficient optimization algorithm as the voltages and angles obtained by Load Flow using PSO are much closer than the ideal values.

2.11 Hybrid Optimization:

Optimization Wireless Sensor Network (WSN) is necessary to reduce redundancy and energy consumption. To optimizing wireless sensor networks for secured data transmission both at cluster head and base station data aggregation is needed. Data aggregation is performed in every router while forwarding data. The lifetime of sensor network reduces because of employing energy inefficient nodes for data aggregation. Hence aggregation process in WSN should be optimized in energy efficient manner. When sensors are deployed at different locations in wider area, it is possible to compromising attacks by adversaries. false data injected in compromised sensors during data aggregation process which results in false decision making at the Base Station (BS). Simple average data aggregation process is suitable only in attacker free environment. So, to filter the false data during data aggregation, induced

by the attacker. For every round of data aggregation need to observe the behaviour of nodes. So that it easy to minimize an impact of attacker contribution at the final result. For secure data aggregation process along with trustworthiness estimation using Trust weighted Secure Data Aggregation algorithm (TESDA). Data aggregation process is optimized by performing aggregation in energy efficient manner through clustering If the aggregator is compromised, then it affects entire aggregation accuracy. Hence it is necessary to propose a aggregation protocol that is resilient against compromised sensor and compromised aggregator in energy efficient and secure manner.

Hybrid optimizations choose dynamically at compile time which optimization algorithm to apply from a set of different algorithms that implement the same optimization. They use a heuristic to predict the most appropriate algorithm for each piece of code being optimized.

Specifically, we construct a hybrid register allocator that chooses between linear scan and graph colouring register allocation. Linear scan is more efficient, but sometimes less effective; graph colouring is generally more expensive, but sometimes more effective. Our setting is Java JIT compilation, which makes optimization algorithm efficiency particularly important.

Our hybrid allocator decides, based on features of a method, which algorithm to apply to that method. We used supervised learning to induce the decision heuristic. We evaluate our technique within Jukes RVM [1] and show on average it outperforms graph colouring by 9% and linear scan by 3% for a typical compilation scenario. To our knowledge, this is the first time anyone has used heuristics induced by machine learning to select between different optimization algorithms.

CHAPTER 3

RESEARCH METHODOLOGIES

3.1 Existing Methodology

Wireless sensor networks (WSNs) are infrastructure-less and self-configured wireless networks to monitor the environment or physical conditions, such as temperature, sound, and humidity, and to cooperatively pass their data gathered through the network to a central location or sink (base station) so that the data can be analyzed for further processing. WSN is deployed in the environments that are usually unfriendly and unsafe. WSN has a large number of constraints which result in new challenges. The sensor nodes have unreliable communication medium and extreme resource limitations which make it difficult to deploy security mechanism. Most of the protocols for WSNs in the past assumed that all nodes are trustworthy and cooperative. But this is not the case for many sensor network applications today and a variety of attacks are possible in WSN including wormhole.

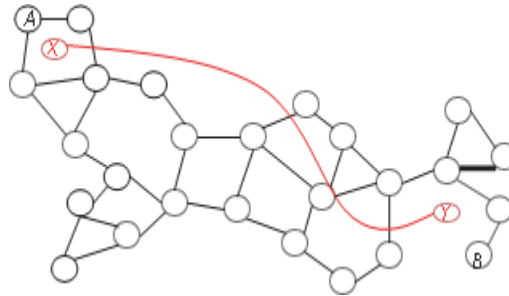


Fig 3.1.1 Wormhole tunnel constructed between nodes $\square$ and $\square$

Wormhole Resistant Hybrid Technique (WRHT)

The proposed technique, WRHT, is a hybrid technique based on the concept of watchdog and Delphi. Watchdog (packet drop) and RTT based technique Delphi are based on the assumption that the packet drops and RTT of a route in the network are very closely related to the value of its HC (hop count) and distance. In practical WSN environments, there exist probability that a normal route without wormhole with a small distance and short value of HC may produce a high value of RTT and packet drop value due to traffic congestion and other reasons. Conversely, a route in the sensor network that is infected with wormhole with a lengthy distance may result in providing a low value of RTT. This may be due to the small packet processing delays by all in-between nodes. Furthermore, there may be less packet drop by an attacker to force AODV to follow the wormhole affected path. For these reasons, sometimes wormhole exposure performance is compromised when separately watchdog and Delphi are used in realistic WSN environments.

WRHT makes use of the information about the packet drop and the delay per each hop and for the complete route in the sensor network. The foundation behind WRHT is to build up a wormhole detection methodology that is able to manage every category of wormholes and is possible for every type of WSN device and scenarios of the network, without the earning of significant computational costs. WRHT is considered as an extension to AODV protocol. The proposed WRHT allows the source node in the sensor network to calculate the wormhole presence probability (WPP $\square$) for a path in addition to

HC information.

During the AODV route discovery phase, per hop time delay probability (TDP_p) is calculated in order to discover the presence of wormhole in the path. This information can be further used for the calculation of time delay probability for the complete path, that is, TDP_p . In the next phase of the WRHT, per hop packet loss probability (PLP_p) is calculated. This is further used for the calculation of packet loss probability for the complete path, that is, PLP_p . The values of TDP_p and PLP_p are used for making the decision whether a path P contains a wormhole or not. This will help the AODV to take a secure path for the transmission. The complete working of the proposed WRHT.

The sender at time t initiates process of detection broadcast of the RREQ (route request) packet and at time $t + RTT$ it receives RREP (route reply) packet from its neighboring node. Assume that round trip time (RTT) of a path in the sensor network through node i is specified by $RTT = t_2 - t_1$; then delay/hop value (DPH) of the path to the receiver via node i is given by $DPH = (RTT)/2l = (t_2 - t_1)/2l$. Here, l is the hop count field in the RREP of node i . Per hop time delay probability (TDP_p) is the probability of time delay caused at each hop in the established path from the source to the destination. The difference between the times when the packet was forwarded by hop to the time when the packet was received is used for the calculation of TDP_p .

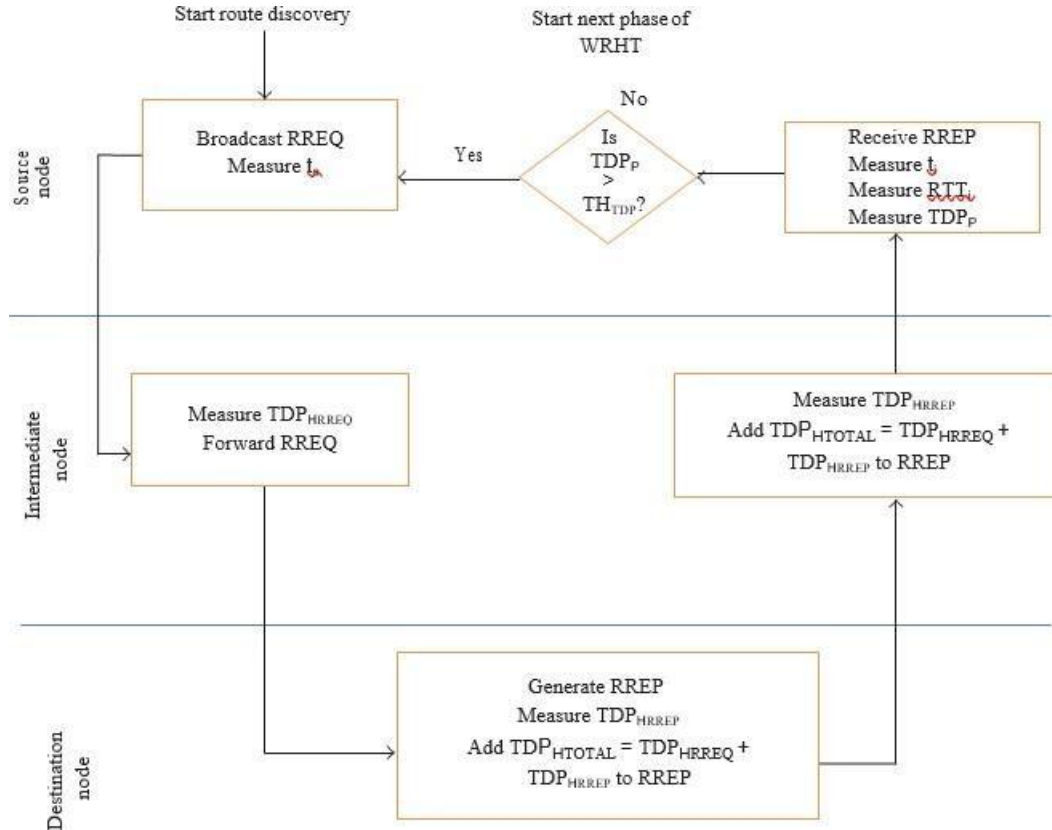


Fig 3.1.2 Route Discovery Process of WRHT

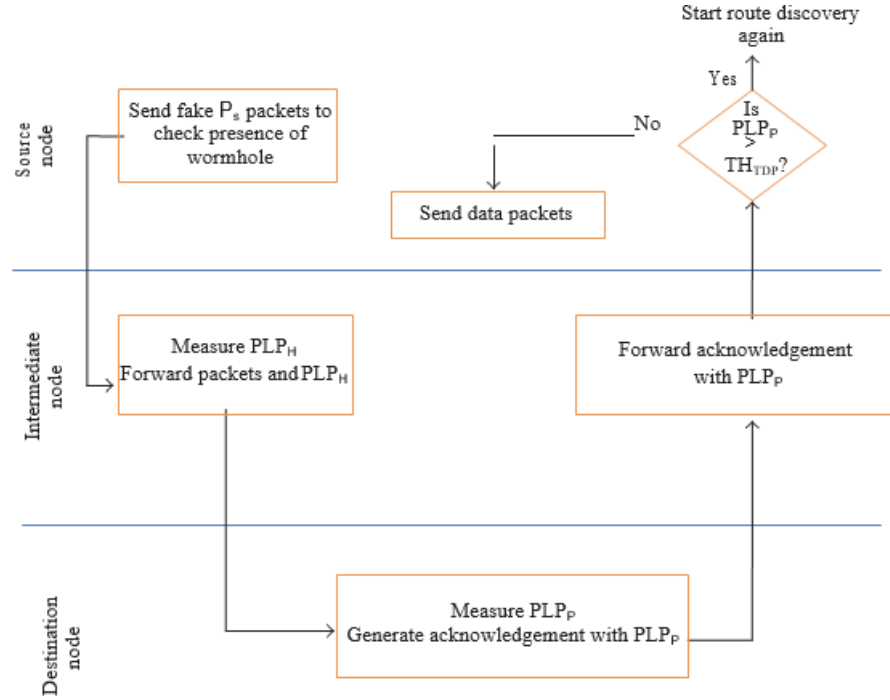


FIG 3.1.3 Worm hole Detection Process of WRHT

Many of the current protocols solve the wormhole attack problem in isolation from the node energy consumption.

- However, some other proposed solutions consider reducing the energy consumption to detect such attacks but still it is needed to probe better performance.
- In this paper, we present a lightweight multi-hop routing protocol for 802.15.4 WSN that aims to minimize the energy consumption and also to detect the wormhole attacks.
- Simulation results prove that our MAC Centralized Routing Protocol (MCRP) outperforms other existing similar protocols.

Disadvantages:

- Lesser ratio in network lifetime.
- Malicious Node Detection confirms to be the superior option where the less energy utilization as well as the improvement of the network lifetime is required.
- The employment of a huge quantity of sensor nodes in unrestrained environments, it is common that some malicious nodes may enter into the network and can hamper mainstream functioning, decrease the energy efficiency.

3.2 Proposed Methodology

- In this work, we used an effective proposed scheme, named as **Hybrid Optimization System (HOS)**, for efficient and routing and transmission for wireless networks.
- Our Hybrid scheme consist of many techniques such as,
- **Dynamic Opportunistic Routing,**
- **Multipath Scheduling Scheme** and
- **Robust Transmission** in networks to overcome above limitations in networks.
- Our proposed scheme which maximizes end-to-end connectivity in the network and minimizes faults at link or/and node level. A set of multiple paths are established from source to multicast destinations using energy efficient neighbor node selection mechanism.
- It provides load balancing at the node and finds a stable path between the source and destination meeting the delay requirement.
- Results, that the proposed protocol outperforms in terms of packet delivery ratio, throughput, routing overhead and average end to end delay.

Advantages:

- The outperforms proposed in terms of packet delivery ratio, normalized routing overhead, throughput and average end to end delay.
- Here obtained motion parameters i.e., velocity, direction of the nodes. Based on these parameters the network selects the path to transmit the data packets between the nodes.
- This approach is that best path can be chosen during the routing based on all these factors. Also, the battery level of the nodes can be taken care in the network. This results in network's good throughput and high efficiency.

3.2.1 Stable broadcast Routing

An on-demand routing protocol contains route discovery phase and route maintenance

phase for data transmission. In the route discovery phase, the source broadcasts route of request message to the MHs in the covered area of the source. When an MH first receives the route of request, it re-broadcasts or replied the message if it is the destination. When a routing path is broken, the route of error message is generated and replied to the source. The source re-invokes the route discovery phase to find another routing path to the destination when it receives the route of error message.

In such a broadcasting scheme (usually called “flooding”), all MHs will re-broadcast once they want to communicate with other MHs. This leads to the serious redundancy, contention, and collision of messages when the node density is high. The energy of MHs and the bandwidth of wireless network will be used up quickly. This condition called the “broadcasting storm problem”. In the last decade, researchers have developed different broadcasting scheme [2-to reduce the negative impacts of “broadcasting storm problem”.

The MPR is a popular broadcasting scheme for solving the broadcasting storm problem. A greedy algorithm is used to find a connected dominating set (CDS) by the exchange of 2-hop neighbor information. The CDS is selected from 1-hop neighbors and can cover entire 2-hop neighbors. In order to reduce the size of CDS, the greedy algorithm usually selects the farthest nodes from the source called the border nodes as the forwarding nodes.

Since the border nodes have a higher probability of moving out the transmission range, the routing paths in MPR from the source to some destinations may be unstable. Therefore, in this paper, we propose an improved MPR scheme called Dynamic Power-aware and Stability-aware Multipoint Relays (DPS-MPR) which avoids selecting the border nodes as the forwarding nodes.

The MPR does not sufficiently take into consideration the effect of the routing maintenance needed for data communication. Routing maintenance is invoked when the routing path is broken due to the movement of MHs. The nodes which are selected by the greedy algorithm easily move out the transmission range because the forwarding nodes are usually border nodes. If a node moves out the transmission range of the routing path, the source must re-broadcast for finding a new routing path to the destination, which results in the “broadcast storm problem”.

3.2.2 Multipoint Relays (MPR)

In MPR, each MH uses the localized 2-hop neighbor information to select the set of forwarding nodes, called MPR set. The MPR uses a greedy algorithm to select MPR set from the 1-hop neighbors. A MH which receives a broadcasting packet will not re-broadcast if it is

not in the MPR set. Thus, the MPR scheme can reduce the number of re-broadcast significantly.

MPR sets form a connected dominating set (CDS) to cover the entire MHs in the networks. The routing path is consisted of the nodes which are in the CDS between the source and the destination.

The proposed greedy algorithm uses maximum transmission range to exchange neighbor information and then selects a minimal set of 1-hop neighbors to cover the entire 2-hop neighbors. Therefore, the border nodes of 1-hop neighbors are usually selected to be included in the MPR set because the border node usually has higher probability to cover most 2-hop neighbors. This greedy algorithm is finished until the entire 2-hop neighbors are covered.

The greedy algorithm is operated as follows: Each MH-x maintains 2-hop neighbor information. $N(x)$ is the set of 1-hop neighbors and $N2(x)$ is the set of its 2-hop neighbors of MH-x. The heuristic can be stated as:

1. Start with an empty multipoint relay set, $MPR(x)$,
2. First select those 1-hop neighbor nodes in $N(x)$ as multipoint relays which are the only neighbor of some node in $N2(x)$, and add these one-hop neighbor nodes to the multipoint relay set $MPR(x)$
3. While there still exist some node in $N2(x)$ which is not covered by $MPR(x)$:
 - (a) For each node in $N(x)$ which is not in $MPR(x)$, compute the number of nodes that it covers among the uncovered nodes in the set $N2(x)$.
 - (b) Add that node of $N(x)$ in $MPR(x)$ for which this number is maximum. When MH-x selects v as a forwarding node, MH-x put v in $MPR(x)$.

Until $N2(x)$ can all be covered by nodes in $MPR(x)$. Two papers proposed several extensions of source-independent MPR to generate a smaller CDS using complete the 2-hop neighbor information to cover each node's 2-hop neighbor set.

3.3 Methodologies:

3.3.1 Initialization

- **Protocol Initialization:**

Dynamic source routing (DSR) is an on-demand reactive routing protocol designed to restrict the bandwidth consumed by control packets, by eliminating the periodic table update messages required in the table-driven proactive approach. It uses source routing instead of

relying on the routing table at each intermediate node. DSR is beaconless and hence does not require periodic hello packet transmissions.

- **Node Stability:**

The stable nodes are necessary in forwarding group to provide better packet delivery services. Node stability in terms of movement around its current position gives us an idea of stationary property of node. Node stability metrics are used to identify stable nodes in a path for forwarding packets from a source to Anycast node. Two metrics are identified to represent node movement stability as the quality of connectivity -self stability, and neighbor nodes stability.

A. Residual energy-based neighbour node selection

Energy efficient neighbour node selection mechanism is used to establish stable multicast routes in WSN using computed power level of a node. Any two nodes that are within each other's transmission range are called neighbour nodes. In this section, we discuss neighbor node selection which comprises of two components: defining node energy model to compute node degree and pruning the nodes that consume more energy.

B. Energy model of a node

WSN nodes operate in four different modes. (1) Transmission mode, (2) Receiving mode, (3) Idle or standby mode, and Sleep mode. Energy consumption by a node in sleep state is negligible as compared to node in transmission mode. Recent studies have shown that the relation of energy consumption of a node in idle mode to the receiving mode and transmission modes are 1:1.2:1.8, respectively. On the basis of assumptions and existing literature survey on energy transaction of a node, we adopt the following energy model to calculate residual energy of a node.

C. Computation of node degree

Degree of a node is a positive integer which represents the maximum number of neighbors that a node can support in a multicast routing. Let $d_i(t)$ denote the degree of node i in a multicast session t and $N_n(T)$ represents total number of nodes in a network then $d_i(t)$ implies that node i can simultaneously transmit packets to maximum of $d_i(t) - 1$ nodes, because one link is busy in receiving incoming packets. Node degree depends on the transmission range and bandwidth of a node.

D. Node pruning using differential dominant set theory.

Node which wishes to send a data to the destination in a network, it identifies the neighbors.

by flooding HELLO packets (containing its own table) periodically and gathers information about all neighbors including their computed power level and node density. Source node or node in question will prune its neighbor nodes whose energy level is less than the threshold residual energy value. We desire to establish stable multicast routes using no pruned nodes that have less node density.

3.3.2 Balanced Multipath Routing & Scheduling

Stable multicast routes are constructed with the help of neighbor node selection mechanism in which next node is selected based on residual energy and density. In the following section, we discuss the RQ and RP packet format, process of request and reply phase, route establishment process and route maintenance in detail.

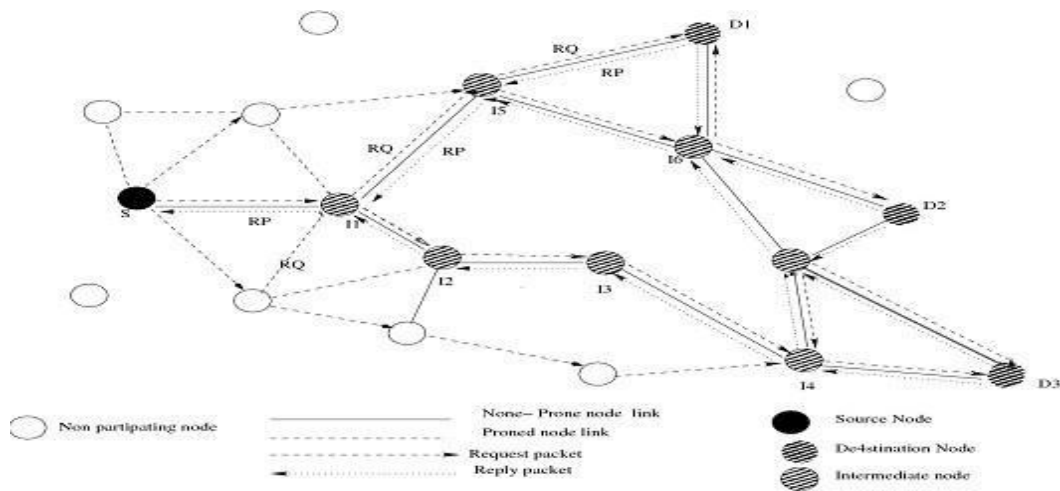
Request Phase: A source node finds the route to its group of destinations by using RQ packets. The sequence operations that occur in route request phase are as follows. In phase (1) Source node prepares a RQ packet with residual energy and node density. In phase (2) Selective transmission of RQ packet to neighbours who satisfy selection criteria (power level threshold), and node density requirement. In phase (3) intermediate receiving node discards RQ packet, if it is already received (using sequence number in RQ packet). In phase (4) if RQ packet is not a duplicate, checks Routing Information table for availability of route if available, RP packet will be generated, and start reply propagation to source.

In phase (5) if RQ packet is a duplicate, then discard it and stop transmission of RQ packet. In phase (6) if not duplicate and no route available in Routing Information table, transmit the RQ packet by updating its fields (route record, computed power level, node density, time stamp, and next hop address) to its neighbors as in step 2. (7) Perform steps 3 to 6 until destination is reached, and in phase (8) if receiver is not reached within certain hops, sends RQ packet back to the source node.

Reply Phase: Multicast destinations initiates the reply phase. When RQ packet reaches the destination node, following sequence of operations are taking place in the reply phase. In phase (1) RP packet is generated from RQ packet by performing following changes in RQ packet; destination and source node addresses are interchanged, route record is reversed, updates visited history records residual energy record as power level, node density record as node density. In phase (2) update route information at destination node with destination IP, path information, Power level, node density and time. In phase (3) RP packet is forwarded to next hop node as per the route record route information table if power level and node density are satisfied. (4) Source that receives RP packet checks whether available power level is greater than threshold value, and node density is less than the threshold, if so,

updates routing table by using contents of RP packet.

Updates will happen only if current time is greater than the time recorded in routing table. If remaining energy is less than threshold value, and node density is greater than the threshold, sends RQ packet to destination and visited intermediate nodes to stop RP packet propagation. In phase (5) perform steps 3 and 4 until source is reached. In phase (6) if source is not found due to link breaks, send RQ packet to the destination, and in phase (7) the source node chooses one of the received paths with higher residual energy and less node density and keep remaining paths as backup paths.



node will use RQ and RP packets to discover paths to destination from itself and informs the source about the path.

Multiple Path Discovery (MPD) Algorithm

If no route is found between the source and destination, then the source node seeks a route to the destination by flooding the Route request packet (RREQ) to the entire network. After receiving the RREQ the destination node sends the Route reply packets (RREP) to the source node. To discover multiple paths, the destination node returns the RREP packet to the sender for the first RREQ packet immediately. This becomes the shortest delayed path meant for the sender. The remaining RREQ packets which comes from the sender in different paths, the destination node computes the maximally node disjoint path or maximally link disjoint path by using the proposed MPD algorithm.

Computation of Multiple Path Discovery

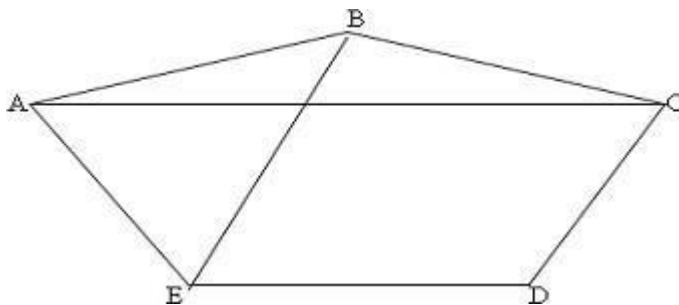


FIG 3.3.2.2 MULTIPATH DISCOVERY ALGORITHM

In this figure each node maintains different addresses. Assume Node A as source and Node D as Sink (Destination). The possible paths from source A to destination D is ABCD, AED, ACD, AEBCD, ABED, ACBED and these paths are stored by the destination (D).

All possible paths are computed by using the Depth First Search Algorithm. In this algorithm to find the possible paths either we can use adjacency list or adjacency matrix. In this thesis we have chosen the adjacency list approach.

Head Nodes					
A	→	B	→	C	→ E → Null
B	→	A	→	C	→ E → Null
C	→	B	→	A	→ D → Null
D	→	C	→	E	→ Null
E	→	A	→	B	→ D → Null

As mentioned above, six possible paths are possible from the source A to destination D. Let these paths be termed as P1, P2, P3, P4, P5 and P6 (P1-ABCD, P2-AED, P3-ACD, P4-AEBCD, P5-ABED and P6-ACBED).

Algorithm to find all Possible Paths from the Source to Destination

Algorithm Depth FirstSearch(n)

1. Read n number of nodes in the given network.
2. Read the source and destination node.
3. Read an array containing the adjacency lists.
4. Initially mark all the nodes as not visited and visited [] is set to zero
5. Create a queue for DFS.
6. Mark the current node as visited and enqueue it.
7. By using the adjacency list, we find all the adjacent nodes of a node.
8. While queue is not empty dequeue a node from the queue
9. Get all the adjacent nodes of the dequeued node i.e., source node.
10. If adjacent node has not been visited, then mark it visited and enqueue it.
11. If the adjacent node is the last node and it is not a destination node in the adjacency list then remove the last node from the visited []
12. If this adjacent node is the destination node, then return true or else continue to do Depth FirstSearch.
13. If step 7 is not satisfied, then return false.
14. If step 10 returns true, then there is a path from source to destination and print the path (current path indicated as 'I').
 - a. While queue is not empty then delete all the nodes from queue and assign all these nodes to the path [].

b. Increment the I value for the next path.

Algorithm to find Multiple Paths

Design an adjacency matrix of size $N \times N$, where N is the number of nodes in the network. The existence of direct path between any two nodes is denoted with '1' and if there is no direct path, it is denoted with '0'.

1. Read the number of nodes (N)
2. Read the edges information (0 corresponds to no edge, 1 corresponds to existence of edge)
3. Select the source and destination nodes.
4. Find all possible paths from the source to destination node by using Depth First Search algorithm
5. Calculate path matrix either by using the node disjoint or link disjoint method (Rows corresponds to path and Columns corresponds to nodes).
6. Find the weight of each path (row sum)
7. Choose the path with minimum weight as primary path.
8. Calculate the hamming distance matrix (the hamming distance between two paths = sum (bit-wise Ex-OR of two paths in path matrix)).
9. Initialize 'sum' array whose size is equals to number of distinct paths with zeros.
10. Repeat the steps (a) – (d) below until all the paths are ranked (current ranked path indicated with 'I').
 - a. Add the Path ranked I to sum array
 - b. Find the column index corresponding to maximum value from the sum array.
 - c. Path corresponding to the column found in the previous step.
(b) Is ranked as $I + 1$.
 - d. I value point to the next value ($I = I + 1$)

3.3.3 Robust Route Selection– Genetic Optimization

Genetic Algorithm is an evolutionary algorithm based on the evolutionary ideas of natural selection and genetics. Optimization is the process in which GA selects the best, fit or optimal node for data transmission. The Genetic Algorithm is an optimization technique which includes the process like initial population creation, fitness evaluation, selection, crossover and mutation. The algorithm ends when it meets the termination criteria.

Every node in the network is referred as sequence of bits. The Genetic algorithm

starts with the initial points called as Initial Population. The sensor nodes within the transmission radius are selected for the initial population. The Fitness function determines the quality of the node in extending the network lifetime. The fitness function is calculated for the nodes based on the distance and the residual energy. The node with higher fitness value has the better chance of survival in the network.

Then the Selection process starts which selects two nodes as parent nodes to produce the next generation. There are different types of selection methods exist. The Tournament Selection is used in this paper which selects two nodes randomly from the current population. For a predefined probability p , the fit node is selected and with the probability $(1-p)$ the node with less fitness is selected.

Crossover or recombination is the process in which the two nodes exchange the genetic information. The outcome of the crossover depends on the selection of nodes from the population. The Single point crossover is used in this paper in which the two parent nodes exchange information after the crossover point chosen at random.

The Table.1 shows the example for single point crossover. In Table.1, the bit sequences of the parent nodes are copied to new offspring until the crossover point and after that the first parent node bits are replicated in the second offspring node and vice versa. The next process is the Mutation in which a node is randomly selected from the best nodes obtained in the past generation and a randomly selected bit is changed to produce new offspring. An example for Mutation process is shown in Table.2

Table.1. Single point crossover

	Parent 1	Parent 2
Node	10011 10011001101	11001 01100110101
Offspring	10011 01100110101	11001 10011001101

The Table.2 shows the nodes before and after mutation process in which the eighth bit of the offspring 1 is changed from 1 to 0. Thus, the new offspring is produced after the mutation process

Table.2. Mutation

	Offspring 1	Offspring 2
Before Mutation	1001101100110101	1100110011001101
After Mutation	1001101000110101	1100110011001101

Then the fitness value is calculated for the newly produced nodes. Then it is compared with the parent nodes and will be replaced if the new generated nodes have higher

fitness value. Then the termination criteria should be checked. The algorithm terminates when the maximum number of generations has elapsed, or the energy of the network has fallen below predefined level. The GA process continues and finds the fit node when it meets the termination criteria. Genetic Algorithm is simple to implement. Genetic Algorithm finds its application in different fields like electronics, computer science including wireless sensor networks.

3.3.3.1 FITNESS BASED ROUTING PROTOCOL

A new energy efficient Fitness based routing protocol is designed to extend the network lifetime through the conservation of energy of the sensor nodes. The routing of packet is based on the fitness value of the node which is calculated using the genetic algorithm.

The fitness function uses the distance of the node to calculate fitness value. The new protocol consists of four phases: Network Initialization phase, Data Congregation phase, Fitness Calculation phase and Packet routing phase.

The flow chart for the Fitness based routing protocol. The protocol starts with the node deployment and after that hop count is initialized to all the nodes in the network. After detecting the event the node gathers information from the neighbouring nodes within the transmission radius.

Using Genetic Algorithm the fit node is selected among those nodes based on the distance and packet is routed to it. The process continues until the data packet reaches the base station.

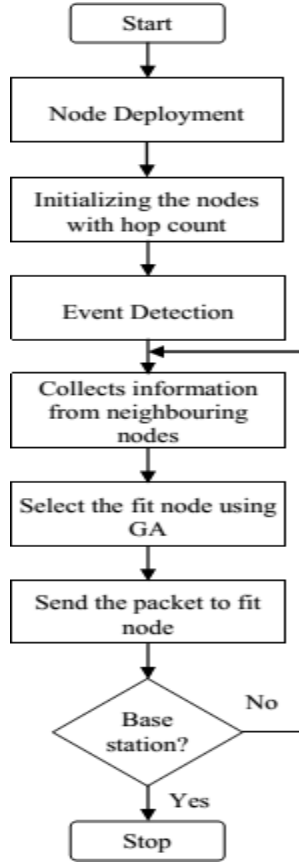


Fig 3.3.3.1 Flow chart for Fitness based Routing Protocol.

3.3.3.2 FITNESS CALCULATION

After receiving the requested message, the source node should select the next node to transmit the packet. Selection of the node is based on the fitness value which extends the network lifetime. Genetic Algorithm is used in this paper to calculate the fitness of the nodes and select the fit node. The fitness value of a node is calculated based on the distance of the node to the base station.

$$\text{Fitness} = \text{dist}(i, j) + \text{dist}(j, \text{bs})$$

The distance between two nodes or node to the base station is calculated using the formula.

$$\text{dist}(i, j) = \sqrt{(x1 - x)^2 + (y1 - y)^2}$$

Where, i, j are parent nodes, bs is the base station.

Genetic Algorithm

In the genetic algorithm process is as follows:

Step 1. Determine the number of chromosomes, generation, and mutation rate and crossover rate value

Step 2. Generate chromosome-chromosome number of the population, and the initialization value of the genes chromosome-chromosome with a random value

- Step 3. Process steps 4-7 until the number of generations is met
- Step 4. Evaluation of fitness value of chromosomes by calculating objective function
- Step 5. Chromosome's selection
- Step 6. Crossover
- Step 7. Mutation
- Step 8. Solution (Best Chromosomes)

Pseudocode

START

Generate the initial population

Compute fitness.

REPEAT

 Selection

 Crossover

 Mutation

 Compute fitness

UNTIL population has converged

STOP

3.3.4 Route Maintenance

Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works.

Neighbour Optimization

Neighbor discovery (ND) is one of the most important protocols of IPv6. It is a message-based protocol that combines the functionality of the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Router Discovery. ND allows nodes to advertise their link layer addresses and obtain the MAC addresses or link layer addresses of the neighboring nodes. This process is performed by the Neighbor Discovery protocol (ND6).

Delay and Link aware

Delay aware Routing in which route discovery mechanism of AODV is modified to include multiple metrics of signal strength, queue length, drain rate and the delay. The protocol finds a stable path between source and destination based on received signal strength and provides load balancing at every node by adding some constraints (queue length and drain rate) before finding the path between source and destination.

3.3.4.2 Data Transfer

Server initiates the reply phase. When RR packet reaches the server, following operations are performed in the reply phase. (1) Server computes RET for all the received RR packets. (2) Among the multiple paths, server selects a path with higher RET. (3) RP packet is generated for RR packet which has higher RET. Server forwards RP packet to neighbor address as present in route record by updating RIC at server. Updates RIC with server id/anycast address, path information, RET, hops, and recorded time stamp. (4) Node receiving RP packet updates RIC by using contents of RP packet, and forwards to next neighbor. Updates will happen only if current time is greater than the time recorded in RIC. If next neighbor or link is failed, sends RE packet to server and visited intermediate nodes and stops RP packet propagation. (5) Perform step 3 until client is reached without link/node failures. (6) If client is not found due to link breaks, send RE packet to the server. (7) Once all RP packets reach the client, the client node chooses a server based on path with higher RET. (8) For the chosen server, select a path with lesser hops, and keep other paths to the server as backup paths. Chosen path to the server will be used by the client as a source route for data transmission.

Route maintenance is required in case of link failures. There are three cases of link failures: link failure between stable intermediate nodes, link failure between source and stable intermediate node, and link failure between destination and stable intermediate node. We can tackle the problem in following ways. (1) In case of link failure between two stable intermediate nodes, the node detecting failure condition will use RR and RP packets to find stable and less congested path between itself and the destination. The new path from intermediate node to destination will be informed to client. If a new path is not found, the node sends RE packet to client to rediscover the paths. (2) In case of link failure between client and stable intermediate node, client node will probe backup path, if it is working, it will

use backup path. Routes will be rediscovered if backup path does not exist. (3) In case of link failure between destination and stable intermediate node, the intermediate node will use RR and RP packets to discover paths to destination from itself and informs the client about the path. If route is not discovered, the node sends RE packet to client to initiate route rediscovery. The client constructs a new path in all the cases for further routing of packets.

3.3.4.3 PACKET ROUTING

The packet routing phase is done after the information is collected by the source node. Initially, the source node sends the message to the selected fit node. Then the process repeats from the data congregation phase until the packet reaches the destination node. During transmission, if any network failure occurs, the network chooses an alternate path. This is done by selecting the other node among the two nodes that were selected in the previous phase. Hence, transmission errors are minimized.

The packet being transmitted holds the message and the packet header. The packet header consists of fields like Source, Destination, Address of the current node, Address of the next node, TTL, Hop count, distance. When the message finally reaches the base station, the base station broadcasts a successful reception message to its neighbouring nodes. This helps in preventing other nodes to stop sending the same message again. The packet routing phase is shown in the Fig.4. The packet is transmitted from the source node to the base station through the intermediate nodes. The intermediate nodes are selected based on its fitness and it routes the data packet to the other nodes until it reaches the base station.

Generally, when a sensor node detects the events, it requires time for sensing the information. This sensing cycle increases the data traffic of the sensor nodes in a routing path. So overflow occurs in the data queue and urgent important events could be lost. Packet Loss also occurs when one or more packets travelling across a network fail to reach their destination. The source will send the packet to the destination node. The number of packets to be sent is set to 200, each packet is of 50 bytes and hence a total of 10000 bytes is sent.

The analysis is carried out based on the QoS parameters like Packet loss,

Throughput, End to end delay, Energy consumption, Residual energy, Energy efficiency and routing overhead ratio.

CHAPTER 4

RESULTS AND DISCUSSION

This work use NS-2 to simulate our proposed Dominant Optimization System (DOS) technique. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile node is 40 moves in a 1000 meter x 1000-meter rectangular region for 100 seconds simulation time. The speed varied as 2,4,6,8 and 10m/s. The simulated traffic is Constant Bit Rate (CBR).

The sensor network consisting of N nodes is planned and implemented using network simulator with other parameters based on which the network is framed. Each simulation is run for 200s, and during this time, the mobile nodes are moved in accordance with the random way point model. When the node reaches its destination, it is immediately moved to another destination.

The average velocities of the nodes are 5, 10, 15, 20 and 25 m/s, as specified in accordance with a normal distribution. The power drained on received packets is set in the range of 200-400mW. The detailed energy consumption model for nodes with ranges less than R_{max} can be found in NS2 documentations. Experiment has been performed for different set of mobile nodes to calculate packet delivery ratio and end to-end delay.

The simulation is done using network simulator. The assessment of performance parameters is discussed in this section. Effect of group size on PDR for different value of energy levels and node density. The fall in PDR is due to fall of non-pruned nodes energy level, thus creating different set of end-to-end multipath with energy efficient intermediate nodes.

During packet transmission sometimes node failure and link failure occur due to node low remaining battery power which causes drops in the PDR value. However we have reasonable PDR achieved for this case by considering nodes with higher remaining battery

(i.e higher energy level) for route establishment. If energy spent by node on transmission and receiving of a packet and/or control information is low then as per our precise mathematical energy model, the computed residual energy remains high.

THE FOUR MAIN PARAMETERS REQUIRED FOR SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS ARE

- END TO END DELAY.
- PACKET DELIVERY RATIO.
- AVERAGE THROUGHPUT.
- ENERGY CONSUMPTION.
- **End-to-End Delay compares the proposed low delay ratio comparing to existing frameworks.**

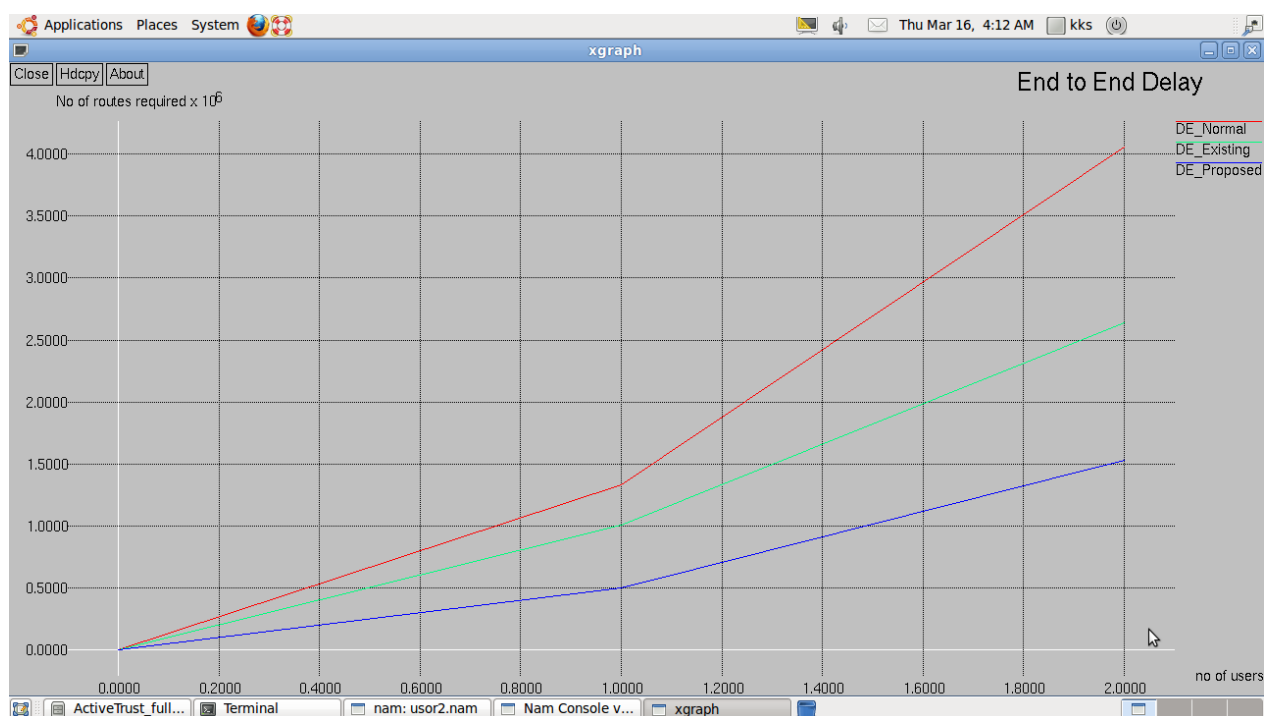


FIG 4.1 END TO END DELAY GRAPH

End-to-End Delay compares the proposed low delay ratio comparing to existing frameworks. Data is transferred faster with the less period of time and high speed. Delay time is extremely low.

Packet Delivery Ratio compares the proposed high delivery ratio comparing to existing frameworks.

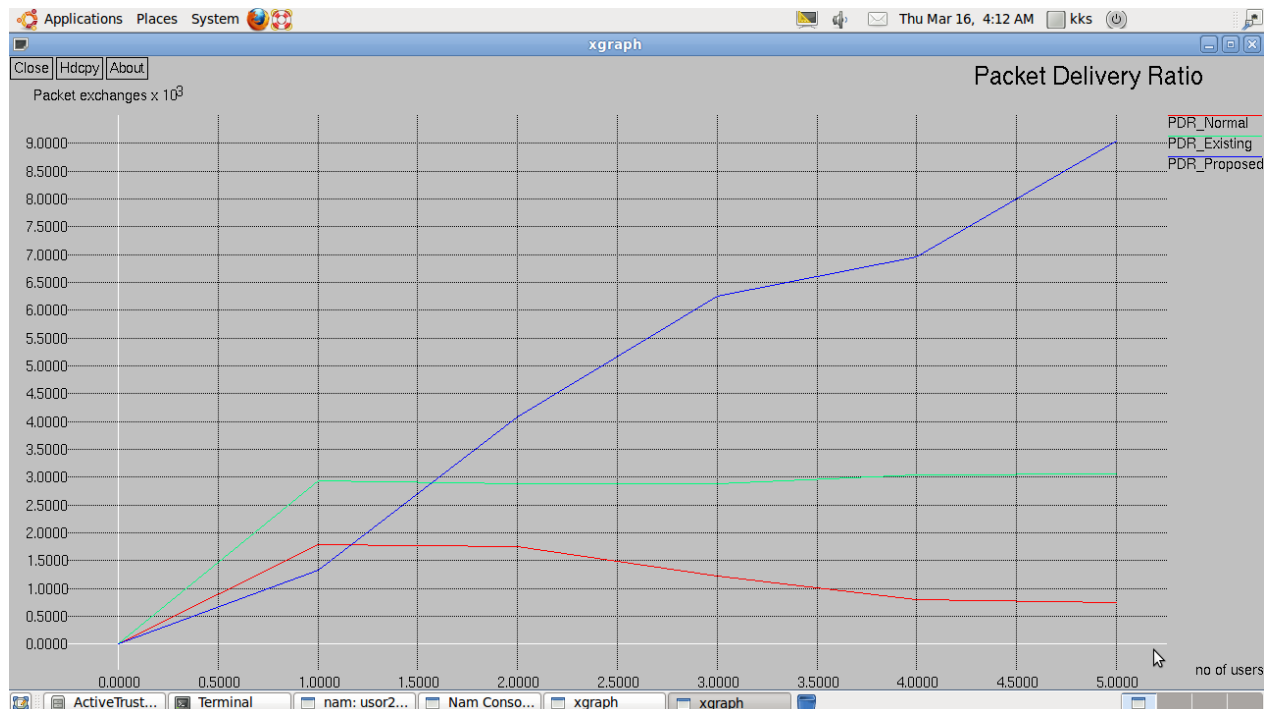


FIG 4.2 PACKET DELIVERY RATIO

Packet Delivery Ratio compares the proposed high delivery ratio comparing to existing frameworks. An extremely high amount of data packets is transferred. Here, the Packet delivery ratio is huge.

Here we are comparing Throughput ratio for Existing, proposed and Modification. In our modification lifetime ratio increased comparing to existing and proposed methods.

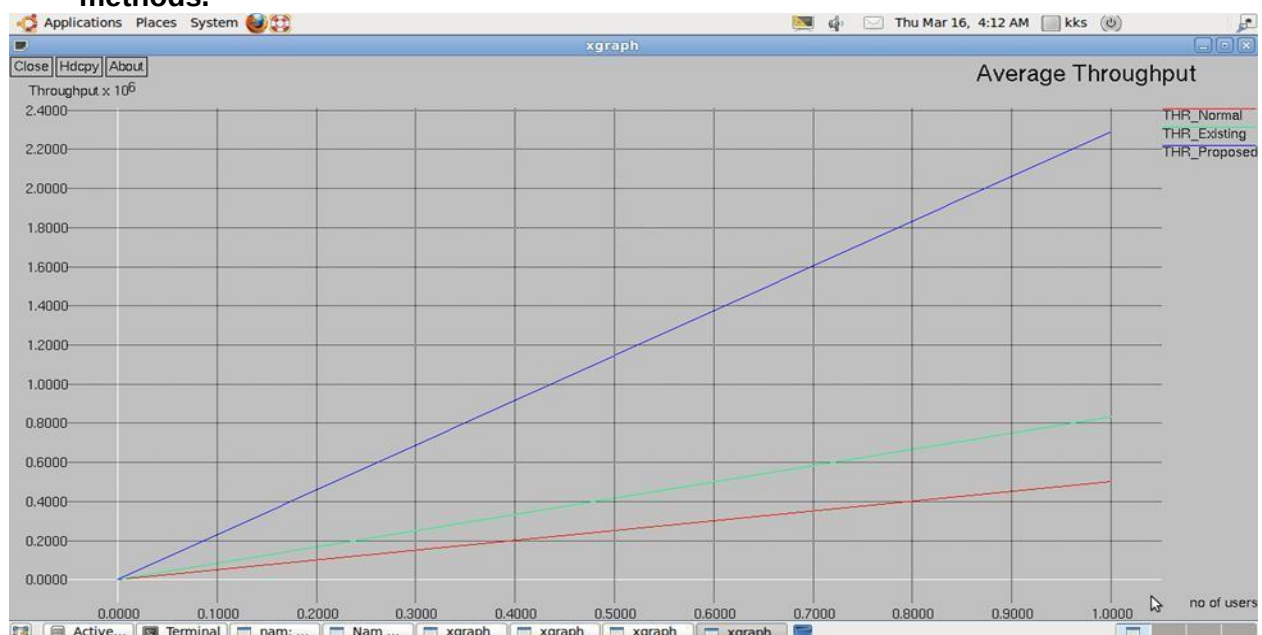
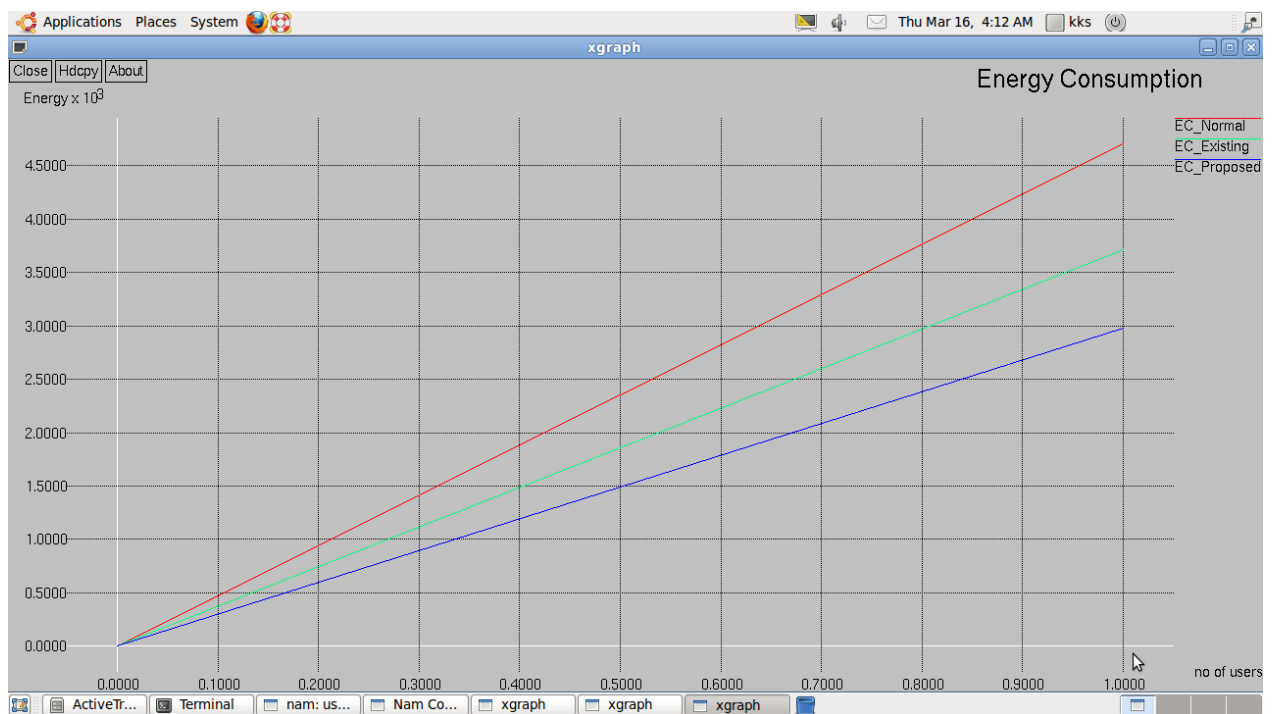


FIG 4.3 AVERAGE THROUGHPUT

Here we are comparing Throughput ratio for Existing, proposed and Modification. In our modification lifetime ratio increased comparing to existing and proposed methods. Universally through put ratio is wide.

Here we comparing Energy consumption for Existing and proposed methods.

FIG 4.4 ENERGY CONSUMPTION



Here we comparing Energy consumption for Existing and proposed methods. Battery lifetime is very high in this method. Energy consumption is extremely low.

APPENDIX

SNAPSHOTS

```
ns main.tcl
num_nodes is set 42
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Enter Source Node(0 to 41)
20
Enter Destination Node(0 to 41)
30
```

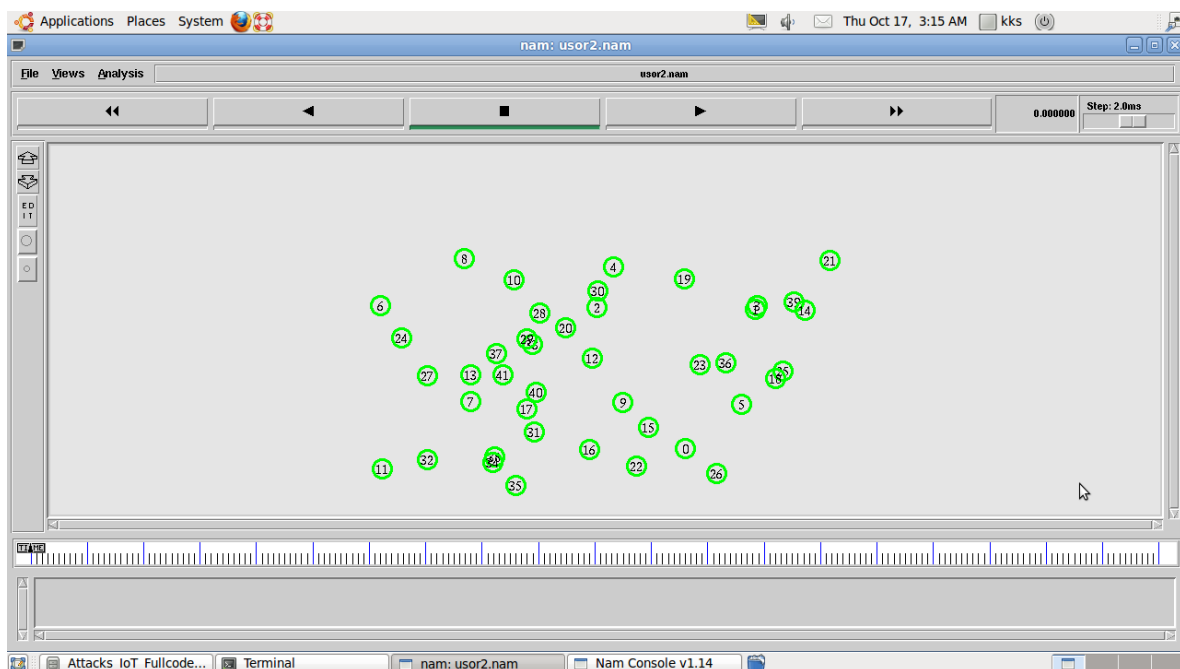


FIG 4.5 NODE INITILIZATION

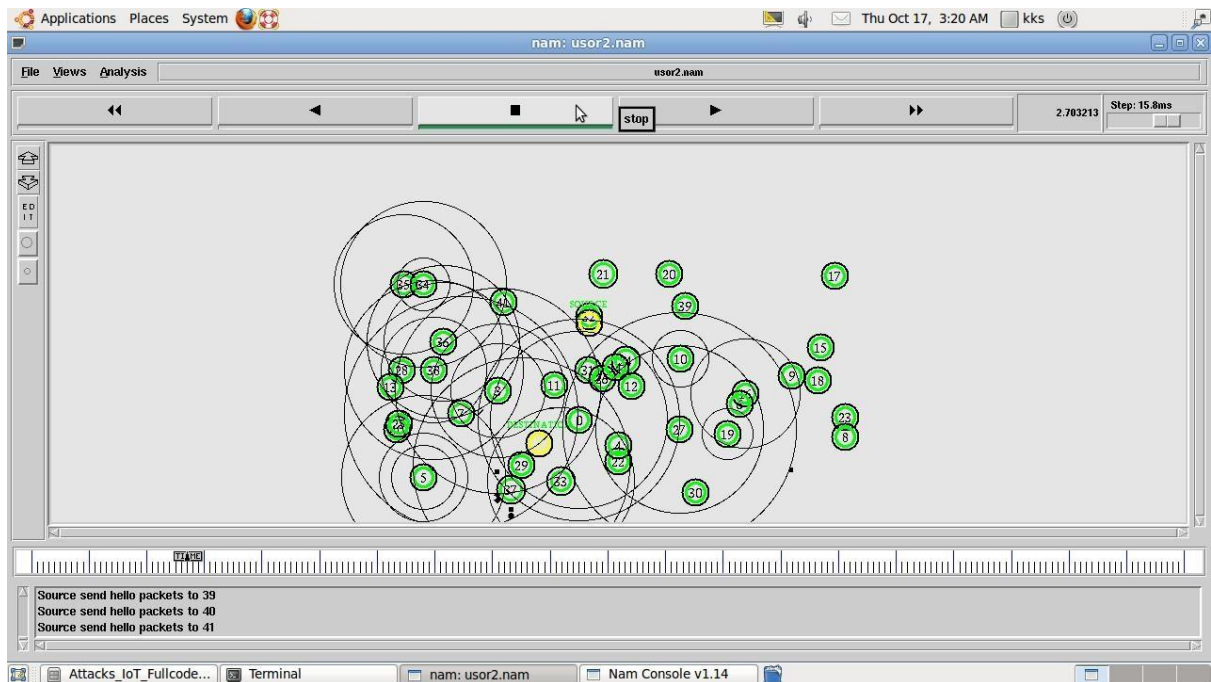


FIG 4.6 NEIGHBOUR COMMUNICATION

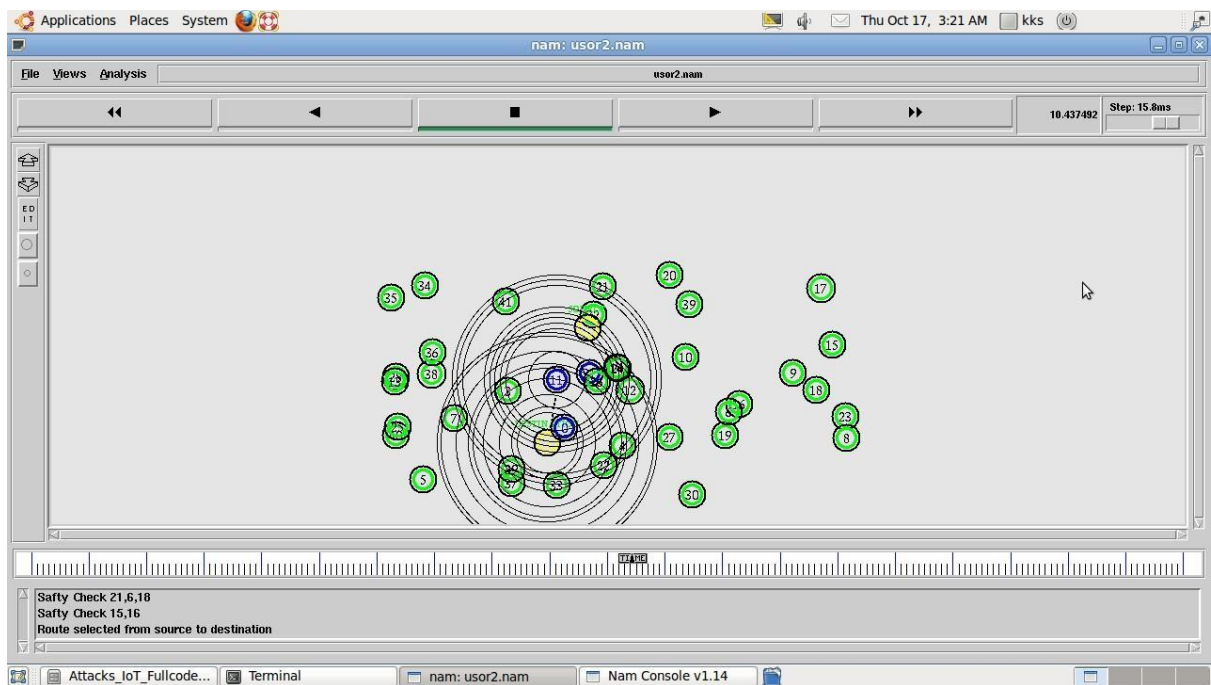


FIG 4.7 SOURCE, DESTINATION AND ROUTE SELECTION

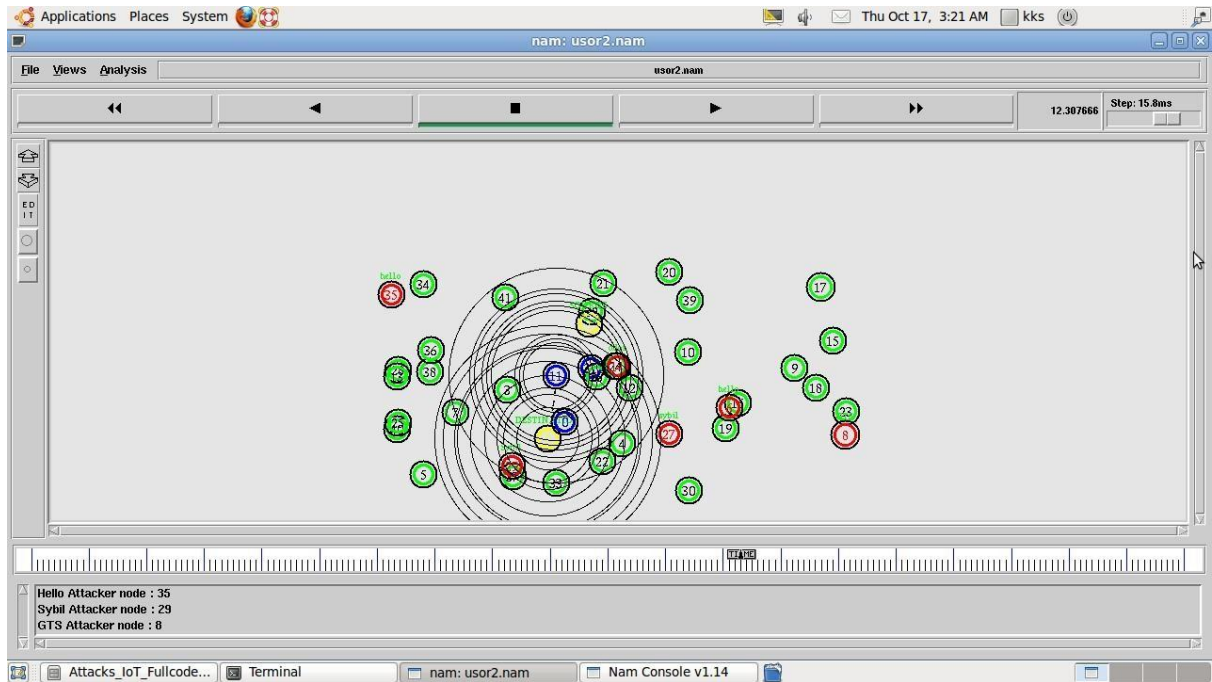


FIG 4.8 ATTACKER DETECTION

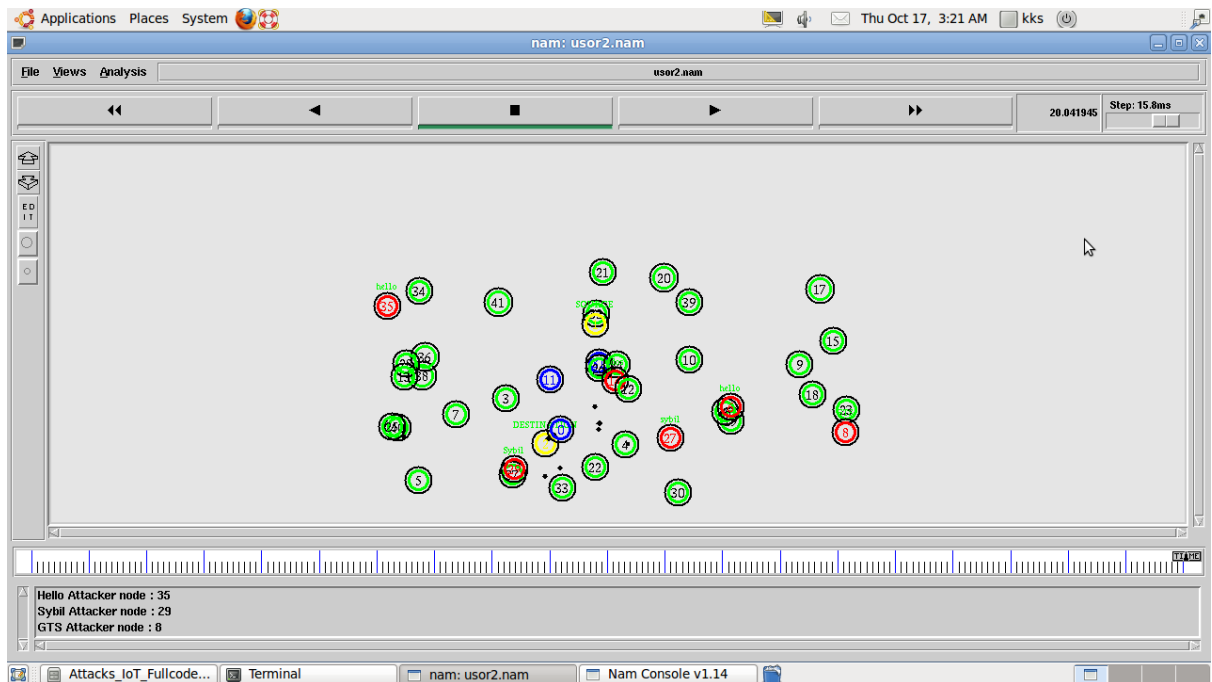
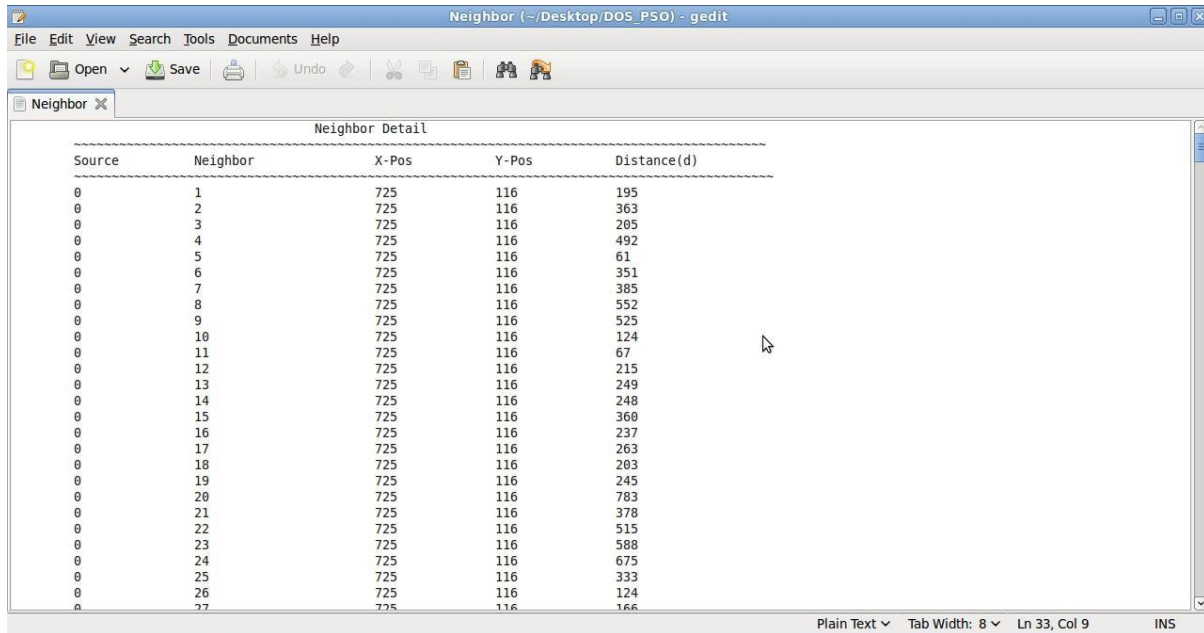


FIG 4.9 DATA SHARING BETWEEN SOURCE AND DESTINATION

Neighbor Table and Data reports



Source	Neighbor	X-Pos	Y-Pos	Distance(d)
0	1	725	116	195
0	2	725	116	363
0	3	725	116	205
0	4	725	116	492
0	5	725	116	61
0	6	725	116	351
0	7	725	116	385
0	8	725	116	552
0	9	725	116	525
0	10	725	116	124
0	11	725	116	67
0	12	725	116	215
0	13	725	116	249
0	14	725	116	248
0	15	725	116	360
0	16	725	116	237
0	17	725	116	263
0	18	725	116	203
0	19	725	116	245
0	20	725	116	783
0	21	725	116	378
0	22	725	116	515
0	23	725	116	588
0	24	725	116	675
0	25	725	116	333
0	26	725	116	124
0	27	725	116	166

file Edit Miew Search }bo\s o< uments delp				
Open Save				
neighbor ,				
Pe zghbo r De ta< L				
Source	Nc J § h bo r	X-Pos	Y - Pos	Distance(d)
7	0	943	609	2L3
7	1	943	609	B19
7	2	943	609	192
7	3	943	609	727
7	4	943	609	9S
7	5	943	609	540
7	6	943	609	525
7	7	943	609	387
7	9	943	609	449
7	10	943	609	821
7	11	943	609	640
7	12	943	609	2E16
7	14	943	609	62
7	15	943	609	st
7	17	943	609	128
7	18	943	609	716
7	20	943	609	570
7	21	943	609	183
7	22	943	609	IB
7	24	943	609	426
7	25	943	609	549

yiIe Edit yiew Search Tools Documents Help	
Open Save :	
☐ Report_Data	
Gene ratedDa7 as	8043
Recel vedDa7as	79S6
Data De11very Radio	9Z.56Z
Ave rage Delay	0.842Z3
Throughput Rail a	8L3419
Packet: Loss Radio	19.1212

File Edit View March Tools documents Help



Neighbor OC Ea II

S0ti r£ e	heiqhbor	X - 005	Y - POs	Distance(d)
16	0	456	214	L12
16	1	456	214	469
16	2	456	214	96
16	3	456	214	540
16	4	456	214	53
16	5	456	214	361
16	6	456	214	4B2
16	7	456	214	216
16	8	456	214	67
16	9	456	214	2B4
16	1D	456	214	S27
16	11	456	214	470
16	12	456	214	101
16	13	456	214	94
16	14	456	214	173
16	15	456	214	761
16	16	456	214	486
16	[7	456	214	147
16	18	456	214	576
16	19	456	214	495
16	20	456	214	321
16	21	456	214	147
16	22	456	214	56
16	24	456	214	299

File Edit View Search Tools Documents Help

Open

Save

I Report_Data

Gene ratedDa£as 4261
 Recei vedDa£as 39gs
 Data Del 1very Real a 83.7924
 Average Del ay 0.064293
 Throughput Ratio 6B.4682
Packet Loss Ratio 9.2648



neighbor

Neighbor Detail

Source	Neighbor	x - Pos	Y - Pos	Distance(d)
32	0	691	328	291
32	1	691	328	346
32	2	691	328	129
32	3	691	328	340
32	4	691	328	252
32	5	691	328	96
32	6	691	328	282
32	7	691	328	316
32	8	691	328	119
32	9	691	328	507
32	10	691	328	78
32	12	691	328	341
32	13	691	328	607
32	14	691	328	431
32	17	691	328	147
32	19	691	328	495
32	20	691	328	92
32	21	691	328	479
32	22	691	328	174
32	24	691	328	285

Report_Data /.

Gene eat edDa7as	6S12
Recel vedDalas	6124
Data De11very Radio	88.6946
Average Delay	0.29325
Throughput Raila	24.6852
Packed Loss Radio	13.6860

Neighbor X

he•qnl:»r D.°t 9i”.

Source	Neighbor	K-Pos	Y-Pos	D:s-ar re ?;
25	1	846	234	346
25	2	046	zaa	195
"S	3	846	:5	50?
ZS	5	B46	zao	327
:S	6	846	234	376
25	7	84S	234	921
E5	8	846	230•	491
25	9	84G	234	ioZ
25	10	846		
25	11	846	234	z00
25	12	046	234.	237
"S	:13	846	234	238
ZS	15	B46	zao	228
:S	16	846	234	241
25	17	84S	234	IG 2
25	18	846	23e	z1ñ
	19	846	234	747
25	z*	846	234	487
25	22	046	234	497
	23	84G	234	605
25	25	R0d	224	107
25	26	B46	234.	142

File Edit View Search Tools Documents Help

Open

save

en

= 101.842

1.243681

az aozi

ta

arwit

ivkec

De

age

ug

vor

et

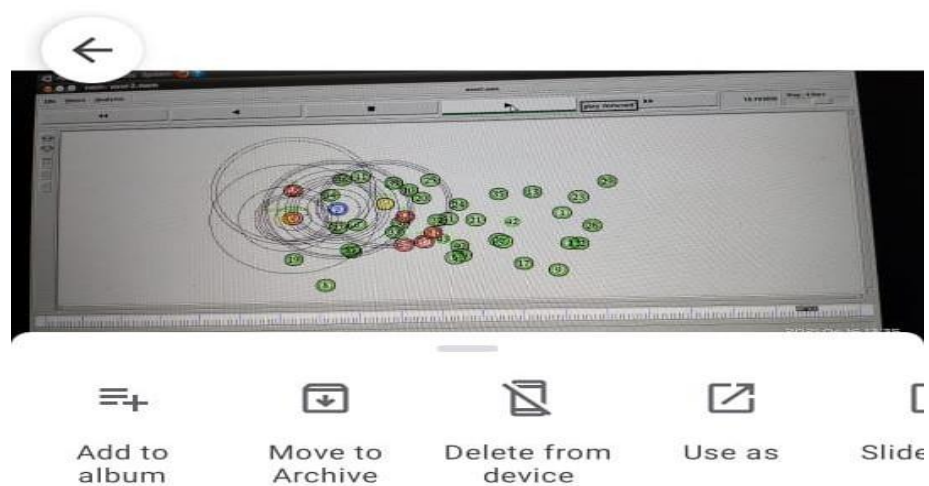
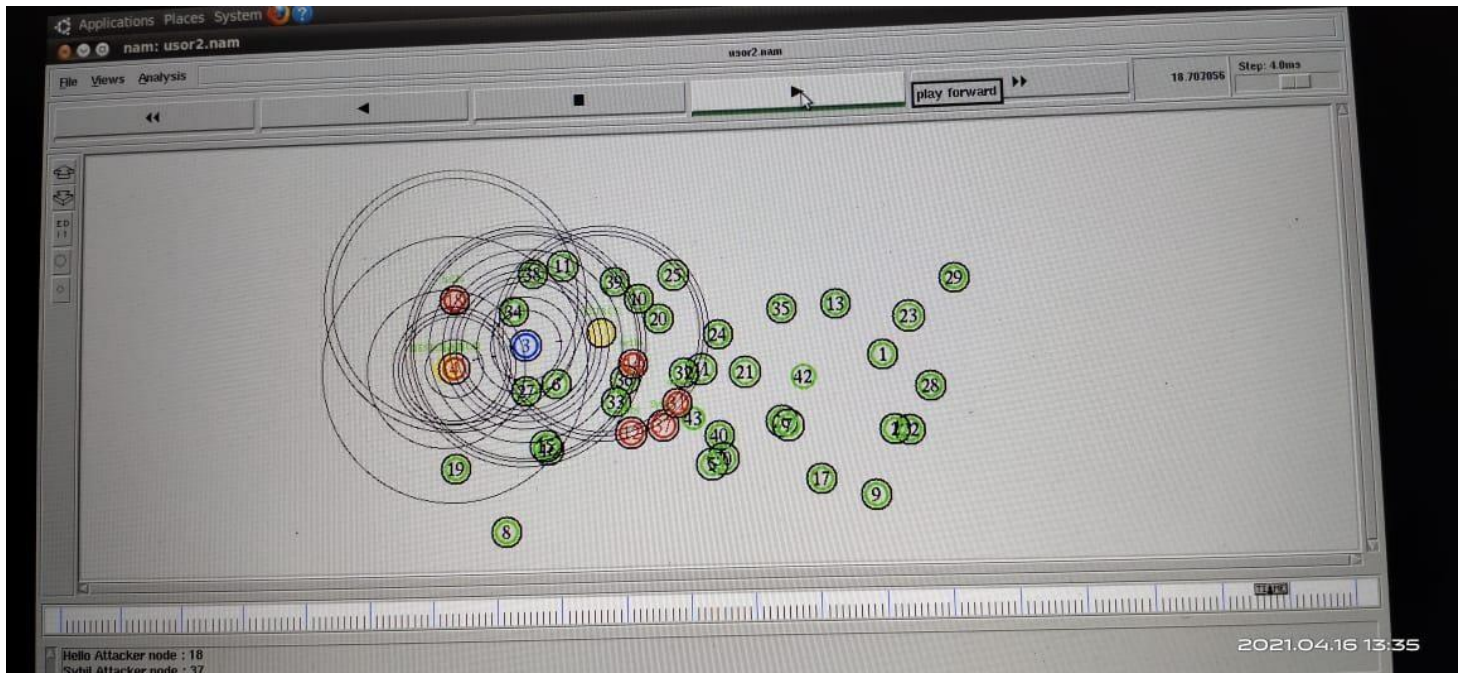
s

ati

io

io

Geotagged output

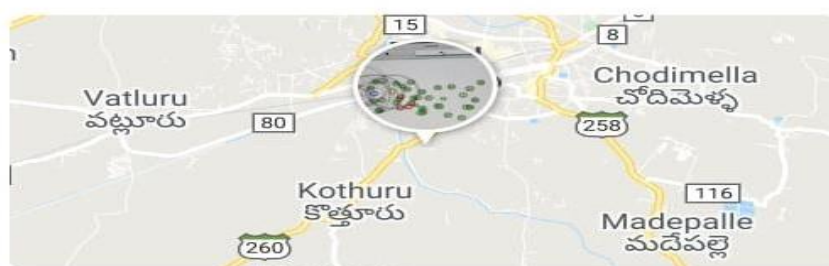


Fri, Apr 16, 2021 • 1:35 PM

Add description...

LOCATION

[Open in Maps](#)



Duggirala, Andhra Pradesh

16.695, 81.094

DETAILS

CHAPTER 5

CONCLUSION

In this work, we used an effective proposed scheme, named as Hybrid Optimization System (HOS), for efficient routing and transmission for wireless networks. Our dominant scheme consists of many techniques such as, Accomplished Capable Routing, Manifold Coordinate Scheme and Secure Transmission in networks to overcome above limitations in networks. Our proposed scheme which maximizes end-to-end connectivity in the network and minimizes faults at link or/and node level.

A set of multiple paths are established from source to multicast destinations using energy efficient neighbor node selection mechanism. It provides load balancing at the node and finds a stable path between the source and destination meeting the delay requirement. Results, that the proposed protocol outperforms in terms of packet delivery ratio, throughput, routing overhead and average end to end delay.

The proposed a novel security and trust routing scheme based on active detection, and it has the following excellent properties: (1) High successful routing probability, security and scalability. The Trust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The Trust scheme fully uses residue energy to construct multiple detection routes.

The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, our scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

CHAPTER 6

FUTURE WORK

We plan to extend our work to concurrent scheduling where multiple networks are considered simultaneously to further improve the scheduling performance.

We will also design different scheduling strategies for networks with different priorities.

As the network scale, complexity, and heterogeneity rapidly increase, nodes and links may fail at a certain rate, especially for long-lasting data transfers.

Therefore, fault tolerance has become another important aspect of the network performance.

It is of our future interest to investigate the reliability issue in the bandwidth scheduling problem in high-performance networks with faulty nodes and links.

CHAPTER 7

BIBLIOGRAPHY

REFERENCE

- [1] Shabana Mehfuz, Sumit Kumar “Energy Aware Probabilistic Broadcasting for Mobile Ad Hoc Network” in 2nd IEEE International Conference on Computing for Sustainable Global Development, 2015, pp 1028 – 1033
- [2] Sumit Kumar, Shabana Mehfuz “Energy Efficient Probabilistic broadcasting for mobile ad hoc network” Journal of the Institution of engineers (India): Series B, Volume 98, Issue 3, pp 289–294, June 2017.
- [3] Raghavendra V. Kulkarni, Anna Forster, and Ganesh Kumar Venayagamoorthy, “Computational Intelligence in Wireless Sensor Networks: A Survey,” IEEE Communications Surveys and Tutorials, vol. 13, no. 1, pp.68- 96, 2011.
- [4] Bhawmesh Kumar, Vinit Kumar Sharma, Distance based Cluster Head Selection Algorithm for Wireless Sensor Network. International Journal of Computer Applications (0975 – 8887) Volume 57– No.9, November 2012.
- [5] Mohammad Wazid, Avita Katal, Roshan Singh, Sachan, R H Goudar, D P Singh, Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network. International conference on Communication and Signal Processing, April 3-5, 2013.
- [6] Yuanpeng Xie, Jinsong Zhang, Ge Fu, Hong Wen, Qiyi Han, Xiping Zhu, Yixin Jiang, Xiaobin Guo, The Security Issue of WSNs Based on Cloud Computing. IEEE Conference on Communications and Network Security 2013 – Poster Session.
- [7] Sachin Gajjar, Mohanchur Sarkar, Kankar Dasgupta, Cluster Head Selection Protocol using Fuzzy Logic for Wireless Sensor Networks. International Journal of Computer Applications (0975 – 8887) Volume 97– No.7, July 2014.
- [8] J. M. Kim, S. H. Park, Y. J. Han, and T. M. Chung, “CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks”, Proc. Of International Conference on Advanced Communication Technology, pp.654–659, 2008.
- [9] Chan H. and Perrig A. “ACE: An Emergent Algorithm for Highly Uniform Cluster Formation”, Proc. Of 1st European Workshop on Sensor Networks, pp. 154–171, 2004.
- [10] Sumit Kumar, Shabana Mehfuz, “Intelligent probabilistic broadcasting in mobile ad hoc network: A PSO approach”, Journal of Reliable Intelligent Environments, Vol. 2, Issue 2, pp.

107-115, July 2016.

- [11] Shabana Mehfuz, Sumit Kumar “Two-dimensional particle swarm optimization algorithm for load flow analysis” International Journal of Computational Intelligence Systems, Vol. 7, Iss. 6, pp. 1074-1082, Sept 2014.
- [12] Bagheri, T.: ‘DFMC: decentralized fault management mechanism for cluster based wireless sensor networks’. Second Int. Conf. on IEEE Digital Information and Communication Technology and it’s Applications (DICTAP), 2012, 2012, pp. 67-- -71.
- [13] Sumit Kumar, Shabana Mehfuz, “Efficient Fuzzy Logic Based Probabilistic broadcasting for mobile ad hoc network”, International Journal of Computational Intelligence Systems, Vol. 9, No. 4, pp. 666-675, June 2016.
- [14] A. Pratapa Reddy, Dr. N. Satyanarayana “Energy Efficient Stable Multi path Routing in MANET”, International conference on Signal Processing, Communication, Power and Embedded System (SCOPEs)-2016, 1115-11121, 2016.
- [15] Yeim-Kuan Chang, Yi-Wei Ting, and Shang-Chun Wu, “Power-Efficient and Path-Stable Broadcasting Scheme for Wireless Ad Hoc Networks”, International Conference on Advanced Information Networking and Applications Workshops (AINAW’07) 2007.
- [16] Gyanappa A. Walikar, Rajashekar C. Biradar, “Energy aware multicast routing in mobile ad-hoc networks using NS-2” 2012.
- [17] Mandeep Kaur Gulati, Krishan Kumar “Stable Energy efficient QoS based Congestion and Delay aware Routing (SEQCDR) Protocol forMANETs”, IEEE ICCSP conference, 2015.
- [18] Sumit Kumar, Shabana Mehfuz “A PSO based malicious node detection and energy efficient clustering in wireless sensor network”, International Conference on Signal Processing and Integrated Networks (SPIN), 2019.
- [19] A Balamurugan, “An Energy Efficient Fitness Based Routing Protocol in Wireless Sensor Networks”, ICTACT Journal on Communication Technology, March 2014, DOI: 10.21917/ijct.2014.0127
- [20] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, “An Implementation of Intrusion Detection System Using Genetic Algorithm”, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.
- [21] Shaveta, Er. Abhinav Bhandari and Dr. Krishan Kumar Saluja “Applying Genetic Algorithm in Intrusion Detection System: A Comprehensive Review” Recent Trends in Information, Telecommunication and Computing, ITC 2014.

Serials, O... WhatsApp Y2Mate YouTube to... Video Conferencing...

Project

9%

9%

0%

0%

1

9%

Exclude bibliography On