An Optimized Multipath Routing for Secure Communication of Wireless Sensor Network

Mrs. M. Sathiya, M.Sc.,M.Phil.,B.Ed.,
Assistant Professor
Department of Computer Science & Applications
Vivekanandha College of Arts And Sciences for Women
(Autonomous), Namakkal,
TamilNadu, India.

Dr. R. Nandhakumar
Assistant Professor
Department of Computer Science & Applications
Vivekanandha College of Arts And Sciences for Women
(Autonomous), Namakkal,
TamilNadu, India.

***Abstract*— Energy efficiency is the prime concern in Wireless Sensor Network because of the limitations on the power source for the sensor nodes. The proper routing technique can greatly contribute in energy consumption and efficient power dissipation in WSNs. Also the packet loss is major problem in the communication process. This paper emphases on energy conservation and secure data communication in a wireless sensor network using multipath routing technique public and private key cryptography. The optimized multipath routing technique deals the aspect to improve security, reliable transmission of data and power consumption. This paper concentrates on securing the data transmission with energy efficient routing. In this technique communication between nodes is setup in three phase path finding, data transmission and path maintenance with data security. For securing the communication this technique uses public cryptography which is initiated by the source node. This authentication and authorization secures the packets and minimizes the packet loss during the communication. The implementation results shows the improved energy consumption and maximizes the packet delivery ratio with minimizing the packet loss.**

Index Terms*: *Energy efficient; Wireless sensor networks; Multi-path routing;

I.INTRODUCTION

A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology (IT) framework. Network(ed) sensor systems are seen by observers as an important technology that will experience major deployment in the next few years for a plethora of applications, not the least being national security. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. In addition to sensing, one is often also interested in control and activation. There are four basic components in a sensor network: (1) an assembly of distributed or localized sensors; (2) an interconnecting network (usually, but not always, wireless-based); (3) a central point of information clustering; and (4) a set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining.

Wireless sensor network (WSN) now been evolved as a prominent data acquisition tool [1]. At present WSN has been progressively used in industrial fields as well as in a various research field. Wireless sensor network has numerous applications like, short-range communication technique, micro-electrical technique and embedded system technique which are integrated together in wireless sensor network. On the other hand, WSN faces big challenges like its constraints in energy consumption, memory and transmission bandwidth. Despite this, the technique in WSNs which is important, routing algorithms have been given a great concern.

The proper routing protocol should be implemented for the network because of the limitation of the energy source in WSN [2]. Reason for that is we use battery in wireless sensor nodes and for the critical environment we cannot replace batteries that's why, lifetime of sensor nodes should be prolonged by positioning various parameters. So, the energy efficient routing protocol is the vital aspect which should be considered. WSNs have a major concern about security, energy consumption and the routing algorithm. Energy is consumed when a sensor nodes sense the data, transmit it between nodes and process it. Among these operations, transmission of data from one sensor node to another requires maximum energy. Much energy and power is consumed while in the process of authentication of node communication, validation and transmitting the data to the base station.

Wireless technologies differ in a number of dimensions, most notably in just how much bandwidth they provide and how far apart communicating nodes can be. Other important differences include which perhaps the electromagnetic spectrums they choose (including whether or not this has a license) and exactly how much power them consume (very important to mobile nodes). In this section we discuss four prominent wireless technologies: Bluetooth (802.15.1), Wi-Fi (more formally generally known as 802.11), Wi-MAX (802.16), and third-generation or 3G

cellular wireless. In the following sections we present them as a way from shortest range to longest rangeWireless technologies differ in a number of dimensions, most notably in just how much bandwidth they provide and how far apart communicating nodes can be. Other important differences include which perhaps the electromagnetic spectrums they choose (including whether or not this has a license) and exactly how much power them consume (very important to mobile nodes). In this section we discuss four prominent wireless technologies: Bluetooth (802.15.1), Wi-Fi (more formally generally known as 802.11), Wi-MAX (802.16), and third-generation or 3G cellular wireless. In the following sections we present them as a way from shortest range to longest range.

In a wireless sensor network there are various communications like between sensor nodes, communication between sensor nodes and base station all in turns to gather information from nodes to provide the specific result. As in Client-Server architecture, the request for the data and the reply with data is communicated among the base station and the sensor node. Here base station query for data and routing data to sensor node as a server. Where the sensor node reply a request with specific information. The multipath routing with key encryption transfers the data in a secure and reliable environment.

II. RELATED WORK

Wireless sensor networks are scattered networks that can be expand extremely to transmit the data into required destination with the help of tiny bandwidth for infrastructure less environment. All the required components can be integrated into a single small chip. Wireless sensor network is made up of groups of tiny devices which can be in number of hundreds or thousands, these tiny devices are known as Sensor Nodes. They are deployed arbitrarily over the field environment to monitor certain parameters. They are in small size, easy to deploy and low cost. The range of sensor nodes varies with the applications like it can be use in security supervision, disaster management systems, military application and more. Along with the application, energy efficient routing, lifetime improvement of nodes, data acquisition techniques are some of the challenges that sensor network faces during various implementation. Transmitting the data to destined place or node uses routing algorithms in the network. In current scenario mostly research are based on routing algorithms for energy efficiency, improve stability, packet delivery ratio, packet loss ratio and the lifetime of nodes.

Routing Algorithm for wireless sensor network has to be designed in the way that it will efficiently use the battery power of sensor node which is limited. Mainly we can classify routing protocol into two different types namely, hierarchical and flat routing protocol. Every sensor node in flat routing has identical role and same function but in hierarchical routing each node are assigned different functions and roles. During the formation of cluster every senor node can take part and they are clustered to form a cluster or zone. In each cluster the node with highest energy level is selected as the cluster head [3]. This will help to minimalize energy consumption due to long distance transmission. The sensor nodes in cluster are connect with cluster head properly this thing is considered while designing algorithm. Every sensor node is required to communicate information to cluster head and should not be left behind[4]. There could be the case that those far away sensor nodes may contain some relevant data which are required in some specific type of application.

This algorithm outperforms LEACH (Low Energy Adaptive Clustering Hierarchy) protocol and other in case of network connectivity of sensor nodes and the coverage of the whole network environment. [5] In multipath routing high energy node in the cluster is selected as cluster head. Cluster are formed at first and if required the sub-cluster is also form with electing sub-cluster head to cover all sensor nodes. Sensor node will remain in the cluster throughout the life time and remain member of the network.

III. MULTIPATH ROUTING IN WSN

The routing protocol allows us to find the optimal path between the source node and the destination node. Wireless sensor network routing is a major factor for conserving energy. The probability of reliable data transmission increases due to Multipath routing. The multipath routing protocol secures the data from sensor nodes and it ensures the availability of the network. The routing in a wireless sensor network can be categorized into three major categories
namely, flat-based, location-based routing and hierarchical-based. In flat-based routing global addressing is not supported. Whereas in hierarchical routing, nodes are formed into clusters and data are routed through main nodes which are called cluster heads. Sometimes it is also known as cluster based routing. Data aggregation is the advantage of a cluster based routing this saves the energy and increases the efficiency. In case of location based routing, location od sensor node is used for addressing. [6] Multipath routings exploits the diversity and resource in network for assistance like improvement in quality of service QoS, delay metrics, load balancing etc. This helps in improving the network capacity and proper resource utilization. The multipath routing is susceptible to attacks without improvement in security.
Wireless sensor networks are different from mobile ad-hoc networks. Here in wireless sensor network, the nodes are static, if a node fails the topology in this case is changed. Due to this reason the mobile ad-hoc protocols cannot be used in sensor networks directly. For this we need secure protocol known as Secure Protocol for reliable data delivery SPREAD. This protocol delivers the message to destination by dividing it into parts. Sending this message parts through multipath routing. This protocol uses distributed many to one multipath finding protocol which are reliable and secure for data acquisition in a wireless sensor network[7]. From simulation results, we can say that this protocol is efficient multipath technique. There are three main elements in this protocol, namely which are path discovery, traffic distribution and path maintenance and security. The energy

expensed by each node for data transmission will not be same because of the hostile environment. This protocol uses Symmetric key for securing data transmission between base station and sensor nodes.

IV. SECURING MULTIPATH ROUTING

The security of transmitted data in a wireless network is the major concern. It should be prevented from attack or capture by an unauthorized node. The cryptography and end to end security is used for making the routing setup safe. Because of resource limitation, wireless sensor network cannot use normal network security protocol. At present routing protocols does not consider data security they only concentrate on optimizing data transmission. Due to this they are exposed to attacks. Here we need to have both optimal data communication and data security.

The sensor node attack might cause network data transmission failure, the compromise of node, failure to monitoring of received and transmitted data. [8] The protection of confidentiality and authentication of communication channels should be provided by standard cryptographic techniques. For providing information security there are security principle namely authenticity, integrity, confidentiality, availability and data freshness, where the reliability of communication is authorized by authenticity. If there any temper in data or not the integrity provides the detection which also allow only authorized node to access the message. Unauthorized access from malicious node or attacker is blocked by confidentiality.[8] Nodes or system are available or not is insured by availability. Fresh data transmission between nodes is done by data freshness. These security principles are not considered by multipath protocol in the wireless sensor network while protocol is design.

Wireless sensor networks are vulnerable to various type of attacks. In various types of attacks when node is physically captured and information from the node is accessed then these types of attacks is known as the Node capture attack. Similarly, there are various attacks like Sink hole attack, Hello flood attack, Denial of service attack DoS which ultimately harm the network and data communication. The security procedures have different types of metrics in the wireless sensor network. The security protocol should be energy efficient to prolong the lifetime of sensor nodes and network. In case of node failure, security protocol needs to remain flexible for key management and route management. The aim of protocol needs to be reliable and prevent data loss during transmission.

Cryptography prevents illegal access in information while communicating in the network. It protects the communication channel between nodes and also protects from attacks. [9] There are two main types of cryptography; Asymmetric and Symmetric. Public and Private key is required for Asymmetric Cryptography where the same secure key is used for both encryption and decryption in Symmetric cryptography. Attacks blocks the network between source node and destination node. This will make

nodes unable to communicate to base station. The security protocol should create the mechanism that has secure access of multi path to multiple base station and also should protect the information of location of sensor nodes. If node is attacked, the attacker will have access to node's internal state and all security information. So if node is attacked then this node should be considered as malicious node and should be removed from all authorization. The other aspects like key management, data authorization and secure routing are also needs to be included in security protocol. This helps in allocating keys to sensor nodes and protect the routing information from attackers.

V. PROPOSED ALGORITHM

Here we are using Greedy Perimeter Stateless Routing (GPSR), which is an efficient and responsive routing protocol for wireless sensor networks[10]. Unlike other routing protocols, GPSR consider the correspondence between physical position and communication in a wireless sensor network. The packet forwarding decision is made using the positions of nodes. Greedy forwarding is used to forward packets to nodes which are always gradually nearer to the destination node.

Areas in the sensor network where those greedy path are not available there will be one path need to move temporarily away from the destination node. It is recover by forwarding in perimeter mode where a packet is transmitted consecutively closer node of a planar subgraph of full radio network connectivity graph. When it reaches to a node which is closer to the destination node it continues greedy forwarding. Another routing protocol is Dynamic Source Routing DSR, which is a self-maintaining routing technique for wireless sensor networks. Dynamic Source Routing DSR [11] can configure and organize the network itself independently without a human supervision. Each source determines the route to be used for delivering the data packets to required destination in DSR. In DSR there are two main phases, namely Route Discovery and Route Maintenance. Route discovery finds the optimal path between the source node and destination node for data transmission.

Where Route maintenance ensures the communication route remains optimal and loop-free, even if network condition changes and even it requires to change the route during transmission. In our model security protocol provides protection from both inside and outside attacks, both active and passive attack and also from Mote class and Laptop class attacks. [12] Inside an attack can be prevented and the attacker can be stopped inside the network. But for the outside attack should be taken care in the network. In active attack data in a data packet is tempered and also the routing information during data transfer. But in passive attack data packet is unharmed during data transmission. The capability of attacker compare to sensor node can be describe in mote class attack. But Laptop class attack is more computational and powerful. Secure multipath routing with reliable data transmission SMRRD rely on Secure Energy Efficient multipath routing protocol, but SMRRD is much secure because it has more secure technique. It computes average data of senor nodes to find the energy. This needs to be both secure and energy efficient. Unlike sensor node base station

possess the ability to compute power and can compare energy. The Base station decides the route and starts communication.

A. *Network*

In mobile Ad-hoc node can be changed dynamically in the network but in wireless sensor network nodes are statically placed. But in a wireless sensor network we have placed static network. For only static wireless sensor network the secure multipath routing will be applicable. So we are constructing a static network of wireless sensor nodes. Sensor nodes are heterogeneous in nature. The initial energy level for the node is constant. Sensor nodes cannot be reenergized after distribution and if energy is deplete it will be considered dead as dead node.

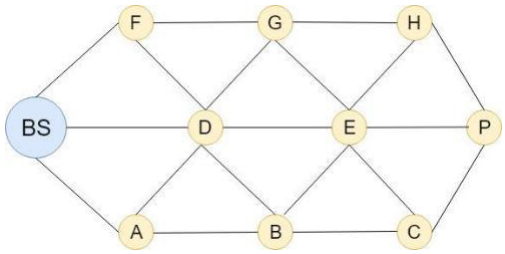

Figure.1 Node Network

Main aim of network is to form the clusters and make selection of the cluster heads. This network is where the sensor nodes are uniformly deposited randomly and after distribution they become static. The sensor nodes collects the data from the field according to its sensing features and they process the data and transmit it to the base station. The sensor nodes are distributed with unique ID, a certificate signed by the base station, a unique shared key which is shared with base station.

B. *Route Construction*

As we know in multipath routing the message is divided into different packet and each packet is transmitted through different path. The order of the packets transmitting will be different in multipath routing. Secure multipath routing is a source initiated for reliable data transmission. For this we need to add some metrics to maintain the packet order which can be called as sequence identifier. Each sensor node will receive Route Request RREQ packet from the base station. To accumulate the RREQ entire network receives packet broadcast. For authenticating a neighbor node current node use public key shared by the base station. When authentication fails node will not add to the neighbor list if key does not match. After getting an address of the Previous nod it will update previous node by current node. When route request is accessible in a received message list along with packet sequence number, it will not resend. Instead of that it will keep the Sequence number of packet in the Received message list and now it will resend. To get the neighbor list for all sensor node, the RREQ packet is sent to all. When neighbor lists are obtained, all the information about the paths between nodes will be gathered in the base station.

When sensor node receives the RCOL packet, they response route reply packet to base station. Which contains data about current node, address, energy consumption in transmission of data among nodes? The base station has the list of all node's neighbor list and energy spent while transmission. Through this information base station can build the weighted directed graph. The Complete weighted directed graph is given by G = (N, E) here N refers to set of nodes, E refers to set of the route which connects all sensor nodes. The positions of nodes is described by i and j. Eij gives the energy between sensor node i and j which are E distance apart. Eij is defined in Euclidean space. Which can be defined as,

$$\sqrt{E_{ij} = (x_i + x_j)^2 + (y_i + y_j)^2} \quad (1)$$

The base station first decides the shortest path and then uses that path and find the next shortest path to transmit the packet of data. The information like energy and distance between nodes are also collected by the base station.

C. *Data Transfer*

Sensor node placed in a different environment has different power consumption. The data transmission uses the optimal shortest route constructed by route construction phase. Network is aware of the energy level for the transmission of every bit of the data All nodes in the network receive data request DREQ from the base station. When the sensor node gets the data request packet it response with the data reply DREP packet. After node gets data request from the base station it follows some procedures. Node authorizes the message with a unique shared key. It accepts the packet if shared key matches. Node uses the unique shared key for entire lifecycle to connect with base station. Here when destination node is a current node then the node will not transmit data because source and destination will be the same.

It rebroadcast the message to neighbor list if the Current Node is not the destination. After collecting data from all the nodes according to a previous phase base station selects the optimal path. Route request is sent after selecting optimal path by base station. Sensor node will acknowledge this message by a route acknowledge the packet. Error Packet ERRP is sent in place of data reply when a security key is not match.

The base station neglects that route because of the malicious node present in the system. To authorize the key public key cryptography is used.

Less energy is spent for authorizing the key. The sensor node sends data packets to the Base station. The sensor node sends the data packets to the Base station. When base station have to wait for certain time to get data reply and does not get on that time it will consider that route to be attacked by the attacker. Data request message is sent through various optimal route to the network to collect the optimal path.

D. *Route security and Maintenance*

If the sensor node fails in the sense to authorize the key or have less energy it will be removed from the network or the path and different routes are used by the network. Error reply packet is also sent as the information update by the sensor

nodes. The route is decided by base station not by source and destination The base station changes the route for data transfer if error message is transferred because of failure in authorizing the public key authentication and also due to the malicious node present in the sensor network. The reason for sensor failure to operation can be physical environment or attack by the attackers.

VI. EXPERIMENTAL RESULTS

In this paper, we use the NS2 simulator for the simulation of the proposed algorithm and created the network environment of wireless nodes and the cluster and base stations. Here we have created the network environment of 53 nodes and the choice of source node 6 and destination node 44 is made. The path nodes selected for the routing are 13, 49, 42, 11, 7. Here data transfer is secured by the shared public key encrypting and decrypting. Table.1 gives the parameters assigned to the network and sensor nodes.

TABLE 1. NETWORK PARAMETERS IN EXPERIMENT

Parameters	Value
Deployed number of sensor nodes	53
optimum number of cluster heads	5
initial energy of node	200J
wireless communication line bandwidth	1Mbps
time of each round	20s
distribution area of nodes	1500m×1100m
network monitor area	1500m×1050m
size of packet header	25Bytes
data size of packet	500Bytes
simulation time	7s

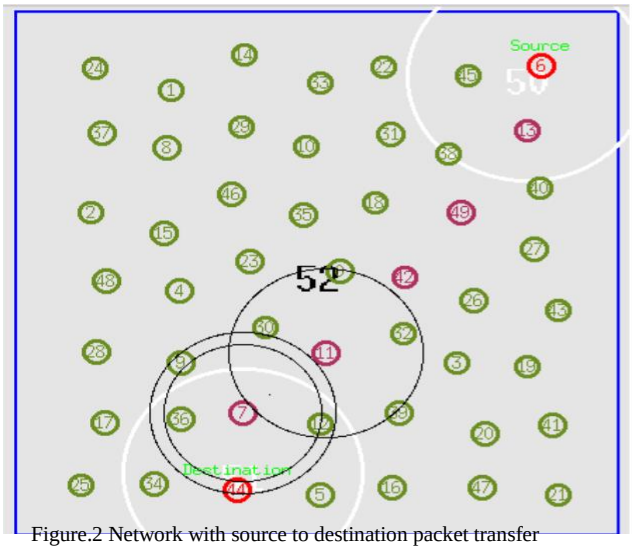

Figure.2 Network with source to destination packet transfer

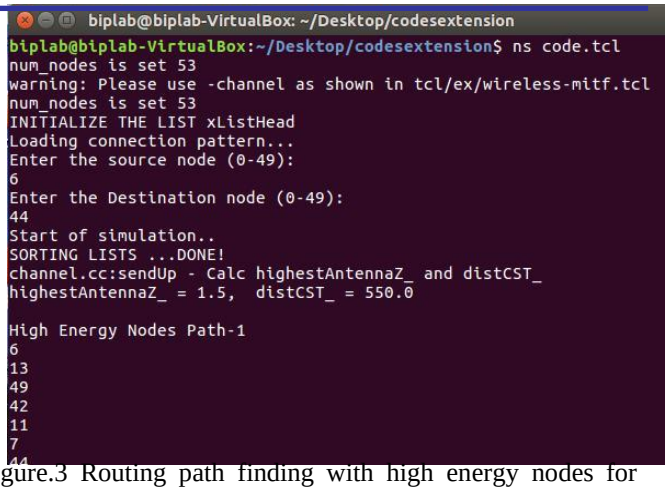

Figure.3 Routing path finding with high energy nodes for efficient routing

The zone partition process is first initiated. In this partitioning process all sensor nodes are divided into different zones. After creating zones the nodes broadcast the message for topology discovery with its public key to their neighbor. After communicating with the entire network we have already assigned the source and destination nodes. Which should be at a minimum distance apart otherwise error message will be shown that source and destination are very close and also shows error if both source node and destination node is same.

So for protocol to work the source node and destination node should be at minimum distance and should be unique. After broadcasting the message the source and destination nodes should be partition in different zones. The source node encrypts the data using public key of a destination node for transmitting. While at the destination node received data is decrypted by using its private key. Fig. 4-7 graphs plotting shows the result of simulation which represent the comparison of this algorithms with existing routing protocols in terms of energy consumption, end to end delay, packet delivery ratio and packet loss ratio.

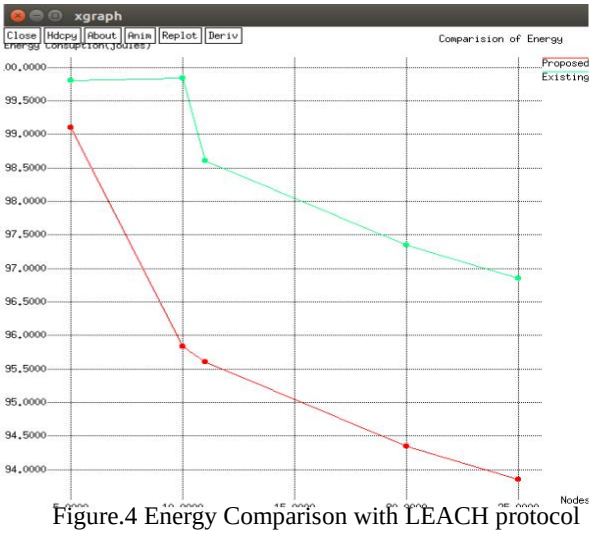

Figure.4 Energy Comparison with LEACH protocol

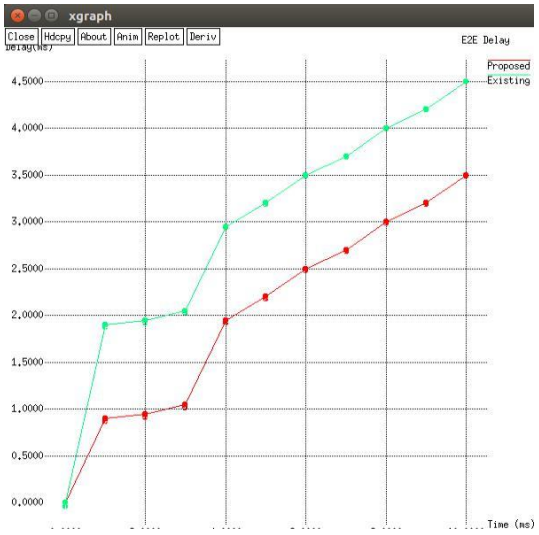

Figure.5 End to End delay Comparison

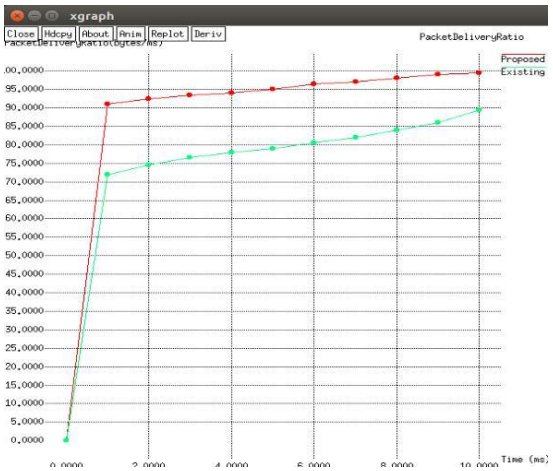

Figure.6 Packet Delivery Ratio

Figure.7 Packet Loss Ratio

VII. CONCLUSION & FUTURE SCOPE

In this paper, we have constructed a wireless sensor network. Communicated the nodes and made the list of every neighbor nodes to choose the optimal path. This proposed algorithm uses the multipath routing protocol along with the security key encryption and decryption which provides energy efficiency and the security to the data being transmitted. The average energy essential for the transmission of each bit of data and securing the data is the average energy consumption.

The data transfer is made more secure by using public key security for authentication and authorization of communication along with private keys provided to sensor nodes. Nodes send the data to base station which selects the optimal path on the basis of energy level, energy consumption, and secure authentication. From the results, we can see that the energy consumption analysis, end to end delay analysis, packet delivery ratio and packet loss ratio, which stand efficient from other, unsecured routing protocols. In future this algorithm can be extended to hardware implementation for various growing IoT applications.

REFERENCES

[1] J. Yick and B. Mukherjee, “Wireless sensor network survey,” Computer Networks, 2008.
[2] Hsiang Liu, Jia-J Su, and Cheng-Fu Chou, “On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks” IEEE System Journal, Vol 11 No. 4, 2017.
[3] J. Zhang, Wenbin LI, Dongxu CUI, X. Zhao, Z. Yin, “The NS2-based Simulation and Research on Wireless Sensor Network Route Protocol”, IEEE, 2009.
[4] G. Sirisha, R. Bulli Babu and K. Raghava Rao, “Establishing Path Quality Management in Wireless Sensor Networks through Cluster Head Determination” Indian Journal of Scinece & Technology, Feb 2016.
[5] Sung-LL Hong and Chi Ho Lin, “A Cluster Routing Algorithm based on RSSI for An Efficient Multi-Hop Data Forwarding”, ISOCC, 2015, IEEE.
[6] M. K. J Kumar, “Evaluation of energy-aware QoS routing protocol for Ad Hoc Wireless Sensor Networks”, International Journal of Electrical, Computer and Systems Engineering, 2010.
[7] Wenjing Lou, “An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks”, IEEE, 2005.
[8] N. Nasser and Y. Chen, “Secure Multipath Routing Protocol for Wireless Sensor Networks”, 27th (ICDCSW'07), 2007, IEEE.
[9] F. Amin, A. H. Jahangir, and H. Rasifard, “Analysis of Public-Key Cryptography for Wireless Sensor Networks Security” ISSRI, 2008.
[10] Available: https://www.icir.org/bkarp/gpsr/gpsr.html.
[11] Routing Dynamic Source Routing , by Margaret Rouse Available: https://searchnetworking.techtarget.com/Dynamic-Source-Routing
[12] Md. Abdul Hamid, Md. Mamun-Or-Rashid and Choong Seon Hong, "Defense against Lap-top Class Attacker in Wireless Sensor Network", ICACT, 2006.