International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 05 | May -2019 ISSN: 2395-0126

Energy Efficient Secure Multipath Routing Scheme with Packet Delivery Ratio for Wireless Sensor Network

Mrs. Vidya Kamath[1], Aishwarya[2], Deeksha Bangera[3], Moksha Salian B[4], Vaishali[5]

Department of Computer Science and Engineering, Srinivas School of Engineering, Mukka

[1]*vidya.kuldeep@yahoo.com*
[2]*aishwaryaudp@gmail.com*
[3]*deekshabangera365@gmail.com*
[4]*moksahakatapadi@gmail.com*
[5]*vaishalikotian1997@gmail.com*

Abstract - *Wireless Sensor Network refers to the dedicated sensors for monitoring and recording the physical conditions. Since wireless sensor network has muti-hop wireless network it has some issues related to unreliable data transfer, energy consumption, Lack of security. Compromised-node and denial-of-service are two key attacks that create the black hole in the network. The proposed approach provides confidentiality, optimised multi-path routing; prolong lifetime energy based routing with minimised energy consumption. Optimal energy path is used to restrict the obstacle made to the data transfer between the sensor networks. To attain peak network connectivity and throughput, new scheduling based energy efficient scheme is established. Successful communication ratio based routing will help us to improve the quality of service.*

Key Words: **Wireless Sensor Networks, Multipath Routing, Optimum Energy Path, Network Life Time, Energy Consumption.**

1.INTRODUCTION

A wireless sensor network is be defined as network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes and with the gateway. The sensor is the device that respond and detects some type of input from both the physical and environment conditions. The position of the sensor node is not predefined. End-to-End security is possible in more conventional network.

The many applications of wireless sensor network give many demands. So this small no of wireless sensor nodes are controlled by sensor battery and are initialized by the sensor randomly or passivity in crucial area. There are some crucial issues like less energy, less computation capacity, open place. Wireless communication makes the wireless sensor network fail most of the time. Once the sensor nodes are initialized that nodes have full battery power to sustain that place without any interruption. A most serious designs issue in wireless sensor network to decrease the energy consumption by using hardware conserving, operating system and communication protocols. To propose the importance of data collection, of the application, full life extension sensor is most important. Even through more different types of technique are proposed to increase the network life of sensor's, the more famed application is to stable the sensor connection in the network in order to decrease the energy at an almost identical time or bitrate.

In such proposal, routing protocol decisions to execute most important category in selecting the nodes paths in order to stable energy in the sensor node. Nowadays most advances in battery-powering sensors nodes are increased their applications and functionality, include full life monitoring like pollution monitoring environment monitoring, failure detection's, surveillance's, and internet-of-things applications. Less cost and less size sensors nodes have gain the particular point in effective monitoring that involves millions of sensors nodes are measured and reported within a deployed area. sensors nodes are typically scatter in a wide region without a sophisticate coordination. Since recharging the battery is not possible, wireless sensor networks (WSNs) are subject to energy management for maximizing their lifetime. The design goal of wireless sensor notes includes energy considerations, Energy deployment, Energy consumption without losing accuracy, and quality of service. The security goals and threats of wireless sensor network are eavesdropping, Data tampering and packet injection, ciphertext attack etc.

1.1 Problem Statement

The different attack to the wireless sensor network may be eavesdropping, data tampering, ciphertext attack, denial attack, false packet injection. The intruder who interested in gathering the data may eavesdrop or add a false information to the existing data when the data is transferred from the source to the destination because of this data may be misused. Because of this data is retransmitted from the source to the destination and due this more energy consumption takes place in the node. To reduce these types

of attack during the data transfer stability of the path is taken into consideration. If any loss of packet or error message occur residual energy of the sensor node is calculated which determines the efficiency of our proposed system. To reduce energy consumption for the data transfer there is need for the scheduling data transfer for this purpose we use multipath routing based scheduling mechanism.

2. RELATED WORK

S Saira Banu, Kalvikarasi S, Aruna R[1] analysed that the node which transfer the data Wireless Sensor Networks are generally composed of large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Some of the major issues in wireless sensor networks are energy consumption, lack of authentication data integrity and instability of path link between sensor nodes, which reduces the popularity of the sensor network. The research work consists of optimized multipath routing; residual energy based routing, authentication and scheduling based approach to make the wireless sensor networks more secure with minimum energy consumption. The optimal energy path is established to maintain the data packet flow in the wireless sensor network unobstructed and the energy consumption model is developed to produce the minimum energy. A New Scheduling based Energy Efficient Scheme is established which attains both throughput and peak network connectivity while keeping the nodes moving in dynamic manner.

A. SenthilKumar, /chandrashekar[2] analyzed that base station will be capable of both wired connectivity to the internet as well as wireless connectivity to the sensor network. Basestation serving as a gateway for collecting data for multi-hop network of resource- constrained sensor nodes. The policy for multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks and are compromised
Sabarinathan K and Ramesh S [3] analyzed that multipath routing approaches are vulnerable to attacks like denial-of service and compromised-node. Once the advisory receives the routing algorithm, it can compute the same routes known to the source, hence making all the information vulnerable to attack. This approach makes use of the randomized multipath routes even if the routing algorithm is made know to the advisory. Beside randomness the generated routs is highly dispersive and energy efficient. The proposed approach provides confidentiality, minimized packet interception probability, end –end energy consumption and solution to cut around sink attack.

2.Implementation

Network initialization:

In this module, 'N' number of sensor nodes are created and are randomly deployed in network area. Each sensor have their own latitude and longitude address based in this each sensor nodes equipped with initial energy to perform its functionalities such as data transaction and routing.

Neighbor Discovery:

Neighbor discovery is based on each sensor node location like latitude, longitude based on this two attribute we are going to discover the neighbors. It collects the all sensors node latitude and longitude apply Euclidean distance formula discover the neighbors of each node.

Step 1: Set neighbor threshold.

Step 2: Calculate the distance using the formula.

$$\text{Distance}[n_1,n_2] = (x_2 - x_1)^2 + (y_2 - y_1)^2$$

Step 3: if (distance$[n_1,n_2]$ ≤ neighbor threshold)

Neighbors

Else

Non neighbors

Energy Efficient Secure Multipath Routing

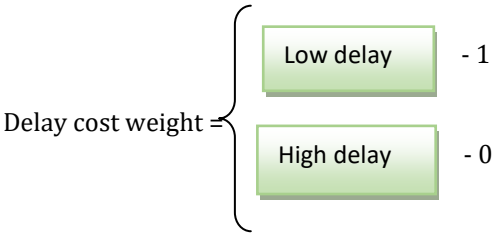
In path discovery, phase source node broadcast the hello packet request to all other nodes. When all node receives that request and respond to the source with energy details. Source node will decide the neighbour node as next hop, which is having higher remaining energy. In this way route will be identified until reaching the destination. Once over all route identified source node will initiate the data transaction in secure mode. To maintain energy efficiency multiple path will be identified using energy efficiency logic, data will be divided into many packets and it will be transmitted via multiple path. Number of path will be identified based on the count of packets. To achieve secure mode elliptic curve cryptography is used to encode and decode the data.

Link cost:

Link cost = energy cost weight + delay cost weight + delivery ratio weight.
Energy cost = Distance[src,dst]*packet size*power consumption.

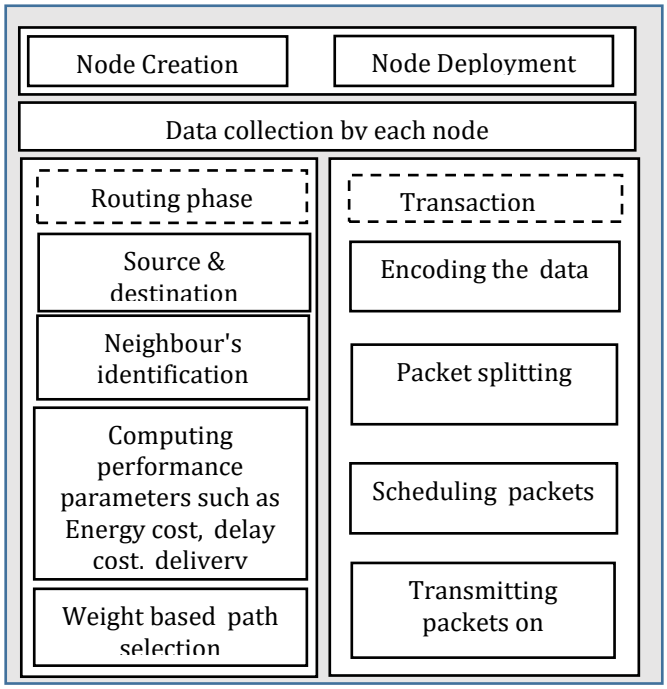
Energy cost weight =
- Lesser energy cost & good future - 1
- Higher energy cost - 0

Delaycost=Distance[Sender, Receiver]*noise in channel

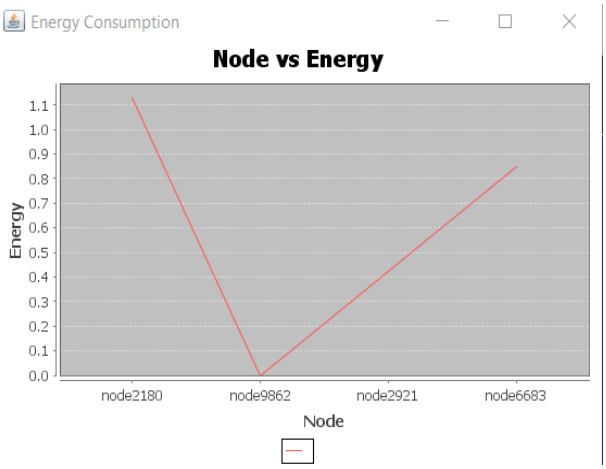


Packet delivery ratio=Packets delivered/packets sent

3. SYSTEM DESIGN



4. CONCLUSIONS



The proposed scheme provides the multipath routing by selecting the optimized path from source to destination. It identifies the rout between one ends to another end by energy efficient multipath routing. To reduce the issues in the network security is provided by encrypting and decrypting the data. Packet delivery ratio is used to increase the accuracy of the data transfer.

REFERENCES

[1] S Saira Banu, Kalvikarasi S, Aruna R, "An enhanced energy efficient secure multipath routing scheme for wireless sensor network."

[2]A.Senthilkumar, Chandrasekar, "Secure Routing in Wireless Sensor Networks: Routing Protocols", International Journal on Computer Science and Engineering. Vol. 02, No.,Pp.1266-1270, 2010

[3] Sabarinathan K and Ramesh S, "Secure Data Delivery in Wireless Sensor Network Using Collaborative Randomized Dispersive Routes", Journal of Computer Applications, Volume-5, Issue2, pp.174-178, 2012.

[4] Shuang Li, Raghu Kisore Neelisetti, Cong Liu and Alvin Lim, "Efficient Multi-path protocol for Wireless Sensor Networks", International Journal of Wireless & MobileNetworks, Vol.2, No.1, pp.110-130, 2010.