

Wireless Data Routing with Security Keys

Vishal Gupta¹, Pankaj Sharma², Harjas Gill³

¹ PG Student, ² Assistant Professor, ³ Assistant Professor

Department of Electronics & Communication Engineering, AIET Faridkot, Punjab, India

Received: 12-07-2014, Revised: 02-08-2014, Accepted: 03-10-2014, Published online: 28-11-2014

Abstract: Routing in wireless sensor network is basically done through distance approaches where protocols which are generally used: - AODV, DSR. But these techniques are bit old and are not that much efficient because of use only single quality parameter consideration. Along with this security is main concern for the data transmission in network which will provide major advancement in field of wireless communication. But previously work is either done only on routing or individually in security fields. In this paper we introduce the working of distance with the collaboration of throughput in order to enhance the data transfer rate and delay reduction. This also includes the security issues though it can also be overcome by combining our new protocols for routing process with the key based data transfer method which helps in providing fast data transfer than the previous method and also overcomes the major security issue. Here proposed work combines two of the major objectives for QOS of wireless sensor networking to avoid previous consequences.

Keywords – Routing protocol, mat lab, AODV, Security and wireless sensor network.

1. INTRODUCTION

Now days, WSNs has a wide range of application areas such as industrial process monitoring & control, robot control, environmental monitoring, habitat monitoring, health care applications, home automation, object tracking, traffic control and etc. However, WSN has its own design and resource constraints issues in practices. Resource constraints include a limited energy, low range communication, low bandwidth, and limited processing power & storage capacity. The recent research in WSNs intend to convene these constraints by introducing new design concepts, creating or improving existing protocols, building new applications, and developing new algorithms. Many researchers are currently engaged in developing schemes that accomplish these requirements.

In WSNs route selection is one of major issues which needs to be carefully done by sensor node to “maximize the network lifetime as well as to reduce the delay”. Many sensor network applications rely on the ability to relay information across multiple nodes along a multi-hop path. In particular, most sensor applications include

one or more sink nodes that disseminate queries or other tasking information to sensor nodes and sensor nodes deliver results back to the sink. Here, it is important that a path exists from a sink to each sensor node, and from each sensor node to a sink. Note that information may be changed as it is traversing such a path, for example due to data aggregation. Two common problems in such applications are hence bad path to sink and bad path to node. In, for example, selfish nodes have been observed that did not forward receive traffic, but succeeded in sending locally generated messages. Since a path consists of a sequence of links, the former inherits many of the possible problems from the latter such as asymmetric paths, high latency, path oscillations, and high message loss. For example, a total message loss of about 58% was observed across a multi-hop network.

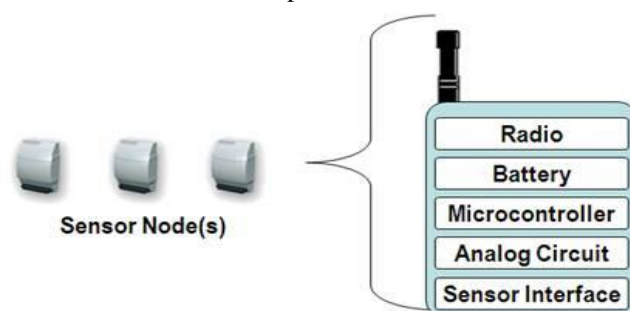


Figure 1: Basic Architecture of WSN

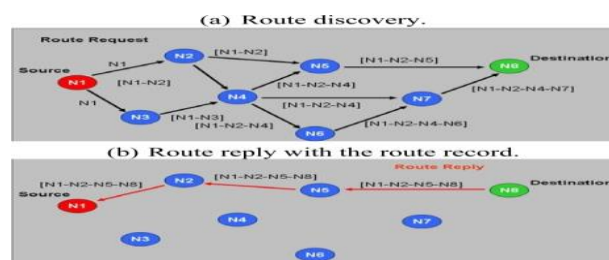


Figure 2: Route selection to Transfer Data from source to destination

2. PROBLEM FORMULATION

A wireless sensor network may comprise thousands of sensor nodes. Each sensor node has a sensing capability as well as limited energy supply, compute power, memory and communication ability. Data is transmitted

through node to node where distance determination was necessary in previous methods.

In distance based systems, energy is more utilized due to large distances. In earlier systems only distance is considered and even few enhancements have been made by experts had also gone through distances and energy but throughput of nodes for correct data transmission is given no importance.

1. Bandwidth allocation and determination of nodes on its bases was a topic of considerations.
2. Attack of malicious nodes causing loss of data and interferences in data were various factors which incurrup the transmission in Wireless sensor networks.

3. PROPOSED WORK

In this paper an approach is proposed which is solving the coming issues of routing and finding best optimal path on the basis of throughput and distance. Keeping in mind all the arising issues

In proposed system firstly source will send the data to the node by detecting the highest throughput of the node and distance among all.

Here task is to determine the distance and throughput of the nodes. Now which path has to be followed for accurate /healthy communication is detected. Shortest way to select is determining the throughput of various nodes. After transmitting data to it again note the various factors as distance and throughput of nodes and repeat the process till data reach the destination. An acknowledgment is provided back to the transmitting node as the information regarding whether data is received properly or is lost.

As communication starts total area to be covered by the deployment of the nodes is to be defined. A coverage area is defined with the total numbers of nodes in the area. Then the nodes distance is checked among each and every node and with respect to the source node also. , For example if there lays three nodes which are very close to the source.

Then proposed algorithm will pick the value on the basis of bandwidth/ throughput of all three nodes. Node with the highest throughput is selected to carry out the communication. The node which has receive the data, now for further communication will act as source and will transmit the data onwards. Now again the throughput is calculated. Data from node to node is transmitted by keeping a check on the distance and throughput until the data is received by the sink (destination).

Later on an approach of secure data transmission which work on basis of keys matching is given in which each node in selected route is generating individual keys up to 8 bit keys methodology. After assigning keys to each node these node match keys generated by them and do the repetition of generation up to 70% of keys get matched when the desired objective is achieved later on the transmitter node provide a dedicated key for receiver to whom it has to transfer data. This same scenario is repeated up to the data reached to destination.

4. FLOW CHART

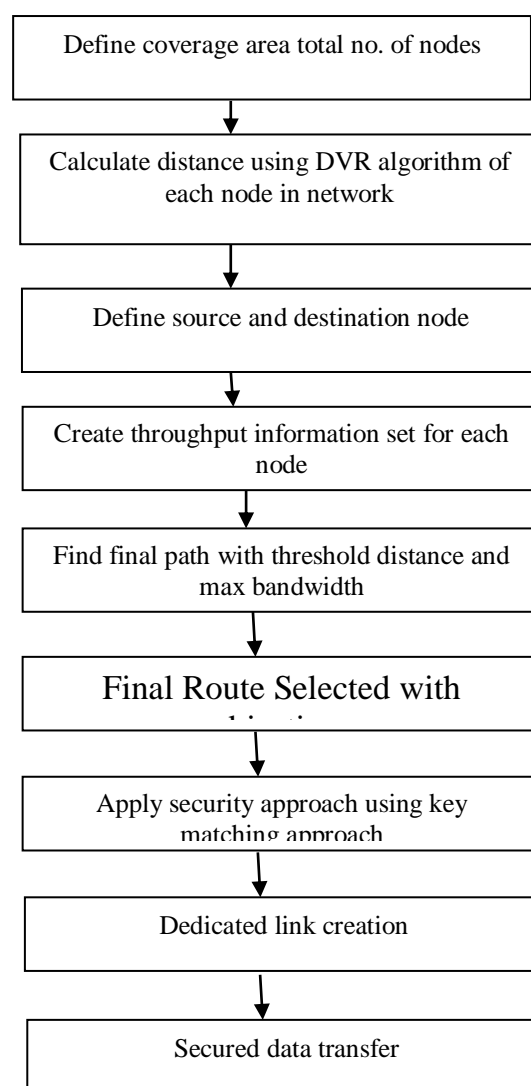


Fig.3: Proposed Algorithm design

5. METHODOLOGY

1. First step is to initialize all the parameters of the network such as antenna, coverage area, etc
2. Now determine total numbers of nodes and define them.
3. To find the efficient path of transmission follow as explained:
4. Next step is to determine the distances between the nodes which is performed using Distance Vector Routing algorithm in full network.
5. Here we need to get a check on the throughput of the each and every node and prepare a set of database only containing the throughput.
6. Among the total numbers of nodes select source and destination node.
7. Finally find the exact path of transmission with following of threshold distance and the proposed methodology of high bandwidth.
8. Later on an key management or matching based approach is applied in which nodes selected in route match keys for link creation
9. Dedicated link creation for data transmission up to defined time interval
10. Secured data is transmitted from source to destination with fulfilling all objectives

6. RESULTS

After implementing the proposed methodology the following results are obtained by applying the minimizing the QOS factors as distance, throughput delay. Along with this the security is main concern.

Simulation results show that the route discovered after working the algorithm developed which will be used for data transfer from source to destination.

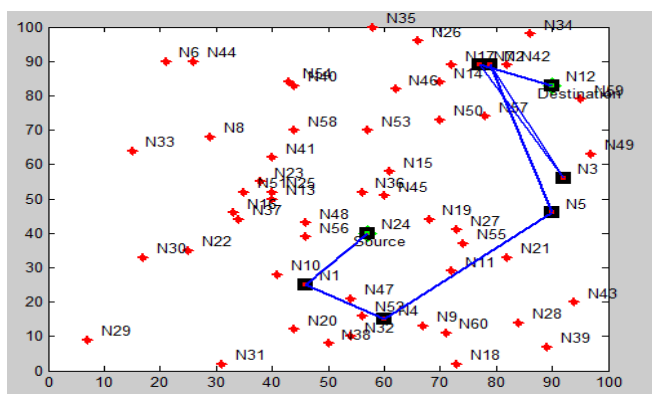


Figure 4: Simulation results based less distance and high throughput based path



Figure 5: Total distance achieved from source to destination

Later on when the final route is found in previous mode next concern is to provide security to data from node to node travelling from source to destination. These simulation results determine that the work proposed in this paper is more efficient in finding the optimized result and capable of providing the security to the data from malicious nodes

7. CONCLUSION

To increase efficiency and performance of the network and find the best optimal short path a new approach is developed. We had implemented a new approach in keeping the distance concept constant with an introduction of throughput of nodes. Reduction in the delay for the transmission of data with a hand increment in the efficiency of the network this proposed methodology is implemented. This provides a network which is faster than earlier proposed energy and distance approaches. Including this as security is main concern in today networking so this paper provide security for data transmission which make it an hybrid approach of fast secured data transmission.

REFERENCES

1. Seema, Reema Goyal "A Survey on Deployment Methods in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 7,PP.540-543, (2013).
2. Amith Khandakar "Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol", Mobile Ad hoc network is network where nodes communicate without any central administration

or network infrastructure, Academic Journal Vol. 40, p36 (2012)

3. Vibha Yadav “Localization Scheme For Three Dimensional Wireless Sensor Networks Using GPS enabled Mobile Sensor Nodes” International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1 (2009)

4. Rajesh Sharma “Dynamic Source Routing Protocol (DSR)”, The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Volume 3, Issue 7 ,(2013)

5. Amit N. Thakare”Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks”, IJCA Journal, vol 3, pp- 125-128, (2010)

6. Parul Kansal “Compression of Various Routing Protocol in Wireless Sensor Networks” have emerged as an important new area in wireless technology. International Journal of Computer Applications (0975 – 8887) PP 14-19 ,Volume 5–No.11 (2010)

7. Matthias Ringwald, Kay Romer, Deployment of Sensor Networks: Problems and Passive Inspection, PP 1-23, 2007

8. Rajeshwar Singh Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks, Int. J. Advanced Networking and Applications 732 Volume: 02, Issue: 04, PP. 732-737, (2011)

9. Bikash Rath “Implementing And Comparing DSR And DSDV Routing Protocols For Mobile Ad Hoc Networking”, (2009)

10. Guoyou He, “Destination-Sequenced Distance Vector (DSDV) Protocol, An ad hoc network is a collection of mobile nodes forming an instant network without fixed topology.

11. Hemanth Narra, Yufei Cheng, “Destination-Sequenced Distance Vector (DSDV) Routing Protocol”, PP. 2-5, (2011)