International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206242

Enhancing and Securing the Routing Techniques in Wireless Sensor Networks

Dr. Rupinder Singh
Assistant Professor, Chandigarh Group of Colleges, Landran, Ajitgarh, Punjab, India

ABSTRACT

A wireless network node network (WSN) is defined as being composed of a large number of small light weighted nodes called network node nodes with routing, processing and communication facilities, which are densely deployed in physical or environmental condition. Each of these nodes collects data and its purpose is to route this information back to a sink. WSN is highly constrained type of network, having network node nodes with more capabilities. All network node nodes in the wireless network node network are interact with each other by intermediated network node nodes. Physical parameters computations are power, energy, memory, communication range and bandwidth. Wireless ad-hoc networks mainly use broadcast communication. Upon deployment, network node nodes automatically collaborate and form a network, start collecting data without any input from the user. The proposed model has been improved for the route metric calculation along with node and link load availability information module to avoid the connectivity loopholes and link congestions. The proposed model results have been obtained in the form of various network performance parameters such as network load, transmission delay, throughput, energy consumption, etc. In wireless sensor networks, there are many types of attacks that can hinder or obstruct the data to be deliver to the authenticated node so in order to check which node is authenticated various algorithms have been proposed. There are various attacks like Denial of Service, Distributed Denial of Service and various types of Jamming attacks that can disrupt or deny the communication between sender and receiver. It is important to develop some powerful tools for network analysis, design and managing the performance optimization of the network. In this paper some of the most common attacks and threats are explained and the prevention that can be taken by using various tools is implemented. Also the different routes are configured if the particular route is not available. All the nodes and the attacks are been shown by using a simulator NS2.

Keywords : Scheduling Algorithm, Routing, Wireless, Sensor Network

I. INTRODUCTION

In the latest research on Wireless Networks, researchers are trying to find and overcome the limitations of wireless networks such as limited energy resources, ranging energy consumption by location, the high cost of transmission, and limited processing capabilities. All these features of wireless are not present at all in cable networks, where energy consumption is not at all a problem, the cost of transmission of the data is very cheap and nodes have lot of processing power. We need to find the new ways for this new generation to work on the networks. So in order to succeed we have to enhance the routing criteria. Routing is the process used by the data communication networks to deliver packets from a source device to a destination device.

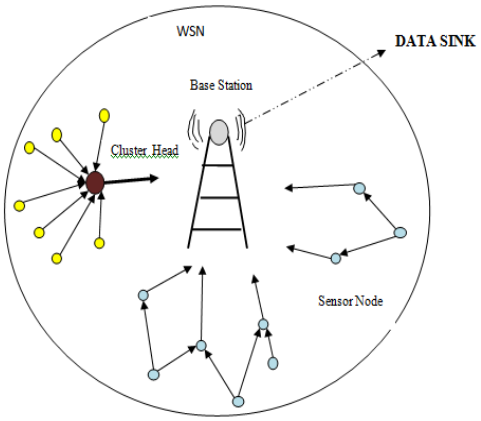

Figure 1 : Wireless Network node Network

A network node node is a tiny device having low power signal processing, power computation and short-range communications capability. These nodes are used to sense data and forward processed data to sink node. Network node nodes having four basic components: network node, a processor, a radio transceiver and a power supply battery. Additional components may include Analog-to-Digital Convertor (ADC), location finding systems etc. After routing analog signal, signal is converted to digital form using convertor. That signal acts as input to the processor, where sensed information is processed and stored in memory.

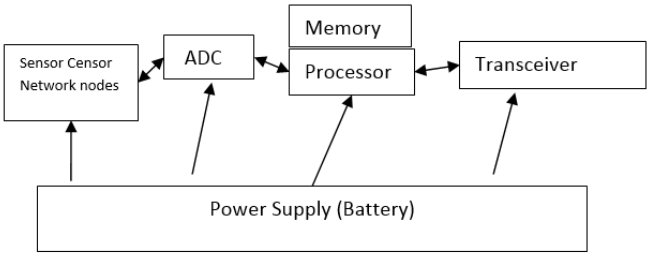

Figure 2 : Components of Network node Nodes

II. PROBLEM FORMULATION

In the existing scheme, authors have used ALBA (Adaptive Load Balancing) and Rainbow mechanism, collectively called ALBA-R, together to solve the problem of geographic routing around connectivity holes. The ALBA with rainbow mechanism is capable of solving the problem of connectivity holes. It bypasses the connectivity holes with geographical awareness based routing. The ALBA is based on proactive routing scheme for its resource based scheduling. Rainbow mechanism is used in this solution to send the data by route other than direct route with connectivity holes to avoid the data loss. ALBA-R in the existing scheme is capable of selecting an alternative path on the basis of their geographical location, once the connectivity hole is detected in the direct path. The ALBA is not very intelligent algorithm and can choose longer path than usual even while using geographical location because ALBA uses route cost/route metric to evaluate the best alternative path. The route cost calculation depends upon the usual routing protocol algorithm. However if the route cost computations process can be made independent of usual routing protocol algorithm on lower layer, it will become more efficient.

III. PROPOSED MODEL

The routing security model has been comprised of the security model to protect against the information disclosure vulnerabilities and man in the middle attack. The existing system is two-column based key management authentication model with the elliptic curve cryptography. The existing model has been made to share four messages for one round of authentication. It utilizes the Simple Password Exponential Key Exchange (SPEKE) model of the base model implementation and has been developed with certain defined improvements.

The proposed model is Multifactor Complex Key based Authorization and Key Authentication (MCK-AKA). This model has been designed as the robust security architecture for the wireless networks. The proposed model is the authentication scheme for the wireless networks using the complex key models. The proposed model has been developed as the complex key architecture where the five columns based key model

has been used for the secure authentication over the wireless networks. The equation driven mathematical programming has been incorporated for the purpose of key data generation over the node with the data origination. The receiver node propagates another set of the mathematical programming written to satisfy the procedure of key verification. The key sharing method is supervised by the transmission module which circulates the key data between both of the nodes in the authentication pair.

Algorithm 1 : Balance Cluster Routing Algorithm for Expanding Wireless Networks (BaCRA-EWN)

1. Obtain the path information among the wireless network for each and every available path in the given wireless cluster.
2. Process each node's individual resource availability by obtaining the on-link factors to compute the load for each node and
3. Compute the given network segment resource availability by using the information from step 2
4. Compute the cluster utility index, which gives the overall status of the wireless cluster in case of inter-cluster link establishment
5. Utility index is added to each micro-cluster in the wireless network to compute the priority among the neighbouring units
6. Apply the decision making algorithm to select the best path among the given network to choose the final path for path forwarding

IV. EXPERIMENTAL RESULTS

There are 28/56/100/500 nodes deployed in random fashion and all are assigned green color with destination fixed as node number 26. The Energy Efficient Wireless Path Optimization (EEWPO) is simulated using network simulator version 2.35. The results are analyzed using .nam and .tr files. The .nam stands for network animator, which shows the node deployment scenario, flow of data between them. The .tr trace files records the value of parameters used for checking performance of network.

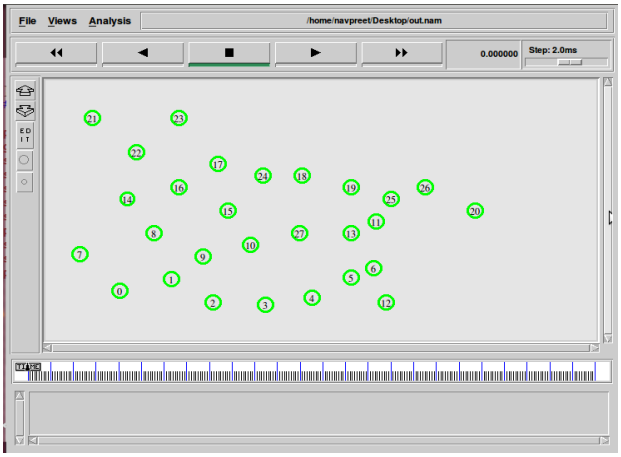

Figure 3 : Node deployment

The proposed solution has been implemented using NS-2 simulator version 2.35. The implementation has been done using 28 numbers of nodes. The node number 26 is programmed as the sink node and any source node can be specified. Every node has been assumed to have a transmission radius of 250 meters. It means that these nodes can't transmit with the nodes which are at the distance more than 250 meters. The paths has been assigned the colors for the effective application of routing protocol based on Rainbow mechanism to mitigate the problem of node failures, path failure or communication holes.

Packet Delivery Ratio:

Packet delivery ratio of network is evaluated after performing path formation and path forwarding. It is represented on Y-axis and number of packets is represented on Y-axis. For comparison, number of packets (no. of packets/1000) value is computed for 100, 500, 1000, 2000, 3000,4000,5000,6000 packets to map the scale precision of existing scheme.

Packet Delivery Ratio		
Time (Sec)	EEWPO	ALBA-R
0	0	0
1	0	0
2	13	10
3	25	20
4	61	50
5	76	62
6	98	81
7	108	88
8	123	101
9	140	118
10	341	252
20	341	276
25	341	300

Values of Packet delivery ratio of ALBA-R and EEWPO

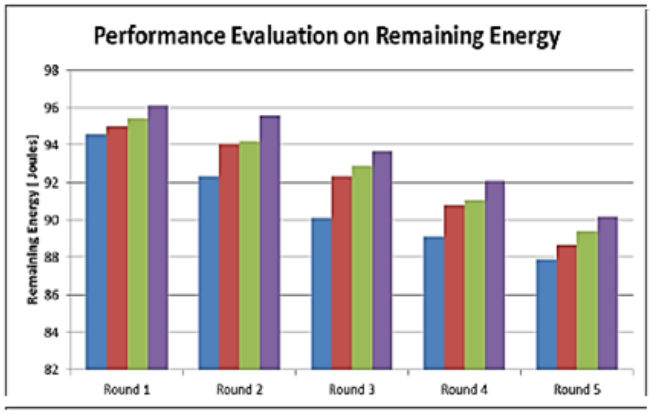

Figure 4 : Performance evaluation based upon the energy consumption

Energy consumption in wireless network is evaluated for the overall performance of the proposed model in order to estimate the overall remaining energy on the nodes. All the nodes transmit the data packets in order to send these packets they lose some of the energy which has been tested. The energy less nodes and the more energetic nodes are the most susceptible nodes in the routing process. Those nodes have to be skipped from the routing for secured and efficient routing process.

V. CONCLUSION

The proposed model has been improved for the route metric calculation along with node and link load availability information module to avoid the connectivity loopholes and link congestions. The game theory adds the robustness and flexibility by adding up the load balancing capability to the proposed model. The proposed model results have been obtained in the form of various network performance parameters such as network load, transmission delay, throughput, energy consumption, etc. The proposed model has been found efficient when compared to the existing model. The proposed model has been proved to be effective by almost 15% than its base models. Also the proposed model is capable of mitigating various types of attacks that can obstruct data from being transferred from sender to receiver.

VI. REFERENCES

[1]. J. Zhu, X. Hu, X. Chen, "Minimum data aggregation time problem in wireless ad-hoc networks" in: Proc. of MSN'05, pp.133-142, IEEE, 2005.

[2]. Yee Wei law & Paul J. M Havinga, "How to Secure a Wireless Network node Network" University of Twente, IEEE Proceedings of the International Conference on intelligent Network nodes, Network node Networks and

Information Processing Conference, page no.89-95, 2005.

[3]. Rajagopalan, Ramesh and Varshney, Parmod K., " Data Aggreagtion Techniques in Network node networks: A survey"(2006). Electrical Engineering and computer Science.Paper 22. http://surface.syr.edu/eecs/22, 2006.

[4]. O.D. Incel, Amitabha Ghosh, B. Krishnamachari, K. Chintalapudi,"Fast data collection in tree-based wireless ad-hoc networks," 2008.

[5]. O. Goussevskaia, T. Moscibroda, R. Wattenhofer,"Local broadcasting in the physical interference model," in Proc. Of DIALM-POMC'08, 2008.

[6]. J. Yick, B. Mukherjee, D. Ghosal, "Wireless Network node Network Survey", Computer Networks, Volume 52, Issue 12, pp 2292-2330, 2008.

[7]. P.J. Wan, S.C.H. Huang, L. Wang, Z. wan, X.Jia, " Minimum-latency aggregation scheduling in multihop wireless networks", in: proc. of MOBIHOC'09, ACM, 2009.

[8]. O. Goussevskaia, R. Wattenhofer, M.M. Halldorsson, E. Welzl," Capacity of arbitrary wireless network," in: Proc. of INFOCOM'09, IEEE, 2009.

[9]. X.Y. Li, X. Xu, S. Wang, S. Tang, G. Dai, J. Zhao,Y. Qi,"Efficient data aggregation in multi-hop wireless ad-hoc networks under physical interference model", in: Proc. of MASS'09, pp. 353-362, IEEE, 2009.

[10]. T. Issariyakul, E. Hossain, Introduction to Network Simulator NS2, DOI: 10.1007/978-0-387-71760-9 1, c_ Springer Science+Business Media, LLC 2009.

[11]. Gaurav Sharma, "Routing in Wireless ad-hoc networks", chapter 2, pp 5, May 2009.

[12]. Hongxing Li, Q.S. Hua, Chaun Wu,"Minimum-latency aggregation scheduling in wireless ad-hoc networks under physical interference model," in: proc. Of MSWiM'10, 2010.

Cite this article as :

Dr. Rupinder Singh, "Enhancing and Securing the Routing Techniques in Wireless Sensor Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 141-145, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206242

Journal URL : http://ijsrcseit.com/CSEIT206242