ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Route Planning Algorithm for Localization in Wireless Sensor Network

Prof. Shubhangini Ugale[1], Ms. Poonam B. Kshirsagar[2], Mr.Ashwin W. Motikar[3]

Professor, Dept. of Electronics & Comm. Engg, G.H.Raisoni Academy Of Engg.& Technology, Nagpur, India[1]

M.Tech.Student, Dept.of Electronics & Comm. Engg. G.H.Raisoni Academy Of Engg. & Technology, Nagpur ,India[2]

Assistant Professor, Dept. of E&TC Engg., J.D.I.E.T, Yavatmal, India[3]

Abstract: Node deployment is an important issue in wireless sensor networks (WSNs). Sensor nodes should be efficiently deployed in a predetermined region in a low-cost and high coverage-quality manner. Localization methods based on mobile anchor nodes have been proposed for assisting the mobile nodes to determine their locations; none of these methods attempt to optimize the trajectory of the mobile anchor node. Route planning scheme, ensures that all of the mobile node can determine their locations. One of the main active attacks is Black hole attack, it is a denial of service attack and it drops entire incoming packets between one source to destination. The attempt is to focus on analysing and strengthening the security of routing protocol Ad-hoc On Demand Distance Vector (AODV) for MANET.

Keywords: Path planning Algorithm , Black hole, AODV.

I. INTRODUCTION

In Mobile Networks, schemes broadly classified into two types, proposed to deal with the localization. First, range based, needs either node-to-node distances or angles to estimate locations. The range based schemes typically have higher location accuracy but require additional hardware to measure distances or angles. Second, range free scheme do not need the distance or angle information for localization? These schemes cannot accomplish as high accuracy as the range-based ones, they provide an economic approach. The accuracy of current algorithms is environmentally sensitive which leads to low reliability and low success rate about the location results. MANET is a collection of wireless mobile nodes that can communicate with each other by point to point transmission type. Due to the limited transmission range, multiple hops are essential for one node to communicate with faraway node in the network. In such a network each mobile node act as a host as well as a router, receiving and forwarding packets for other mobile node that may not be within transmission range of each other. The applications of ad hoc networks are growing significantly, and there are different domains where it is preferable to use ad hoc networks for communication, in order to reduce the time and cost of setting up an infrastructure network. The following are the main applications of ad hoc networks: military communication, mobile conferencing, and emergency and rescue mission. Ad hoc networks have the following features: power limitations, node mobility, topology changes, broadcast transmission medium, self organization and configuration of the nodes. These features have a direct impact on the following: link reliability, routing information, and network security.

II. NECESSITY OF ROUTING ALGORITHM

Consider the route planning problem of localization. We ask the question of what should be considered as a better path to be taken by the nodes with sensor localization as our primary objective. For this problem, we assume that, although we do not know the exact sensor locations, the sensors are uniformly distributed over a predefined deployment area. The objective of our route planning is to design a path to guide the mobile nodes such that i) a higher percentage of the sensors can be localized (i.e., better coverage),ii) the localization error is minimized (i.e., better accuracy), and iii) the path length the mobile beacon travels is shortened.

III. STEPS FOR SHORTEST ROUTE PLANNING ALGORITHM

1 Find the position of each node x & y coordinates
2 Enter the path to find
For ex 1
3 Enter the source & Destination
4 calculate the distance between each node
Repeat the above step til finding the distance between each node
5 After getting the distance find the path which has less cost
6 calculate the hop count between the path & total cost for sending data
7 send the data towards the destination.

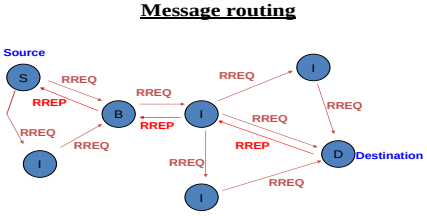


Figure 1: Black hole problem

DOI 10.17148/IJARCCE.2015.46113

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Figure 1 shows a network consisting of seven nodes: the source (S), the destination (D), the black hole (BH), and four intermediate nodes (Ij). Firstly, S sends a RREQ asking for a route to D. The RREQ is received by all of its neighboring nodes (I1, BH, and I2). As shown in Figure 1, both I1 and I2 re-broadcast the RREQ. On the other hand BH does not rebroadcast the RREQ, where BH is a black hole. Instead it replies immediately claiming that it has a direct link to D. As usual, S responds to the RREP by sending the data to D through BH. Once the data is received by BH, it will be dropped directly. Moreover, BH will also send the same RREP to both I1 and I2 as soon as it receives the rebroadcasted RREQ from them. This implies that BH will be added to the route table of both I1 and I2 as the first hop to D.

IV. RELATED WORK

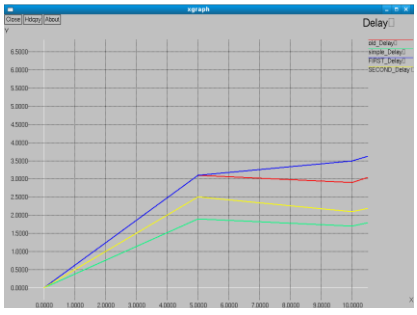
Different ideas and studies discuss the black hole problem and its effects on the routing process. One of them proposes to solve the problem by preventing the intermediate nodes from replying to the received route requests. Such idea forces the intermediate nodes to broadcast the route request. In this solution, only the destination node holds the responsibility of sending the route reply. Such idea limits the cooperative behavior of the nodes, where it prevents the exchange of route information between the nodes, and hence increases the overhead of route discovery.

V.RESULTS

The Route planning scheme proposed is specifically designed to

1. Minimize the localization error of the individual mobile nodes.
2. Maximize the number of sensor nodes which can determine their locations. The performance of the proposed scheme is evaluated by conducting a series of simulations using the ns-2 network simulator.

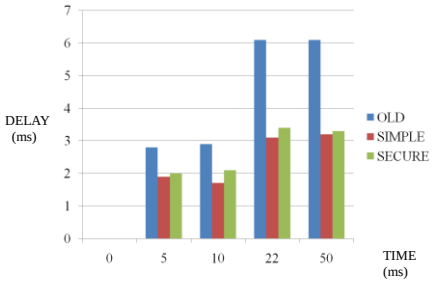
DELAY RESULTS:



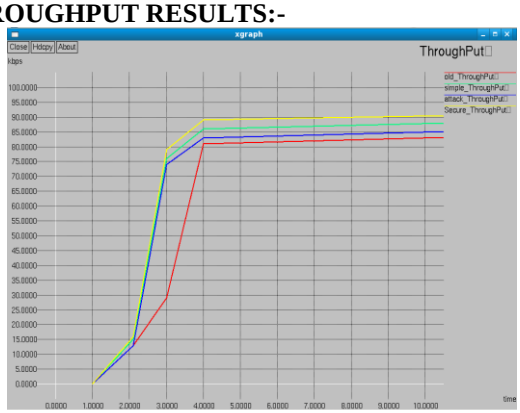
DELAY RESULT

TIME	OLD	SIMPLE	ATTACK	SECURE
0 ms	0	0	0	0
5 ms	2.8	1.9	3.1	2.0
10 ms	2.9	1.7	3.5	2.1
22 ms	6.1	3.1	6.5	3.4
50 ms	6.1	3.2	6.5	3.3
ADDITION	17.9	9.9	19.6	10.8
PERCENTGE	3.20	0.98	3.84	1.16

GRAPH FOR DELAY



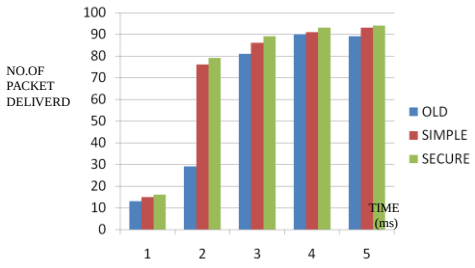
THROUGHPUT RESULTS:-



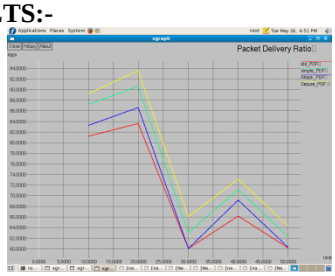
THROUGHPUT RESULTS

TIME(ms)	OLD	SIMPLE	ATTACK	SECURE
1	13	15	13	16
2	29	76	74	79
3	81	86	83	89
4	90	91	89	93
5	89	93	91	94
ADDITION	302	361	350	371
AVERAGE	60.4	72.2	70	74.2

GRAPH FOR THROUGHPUT



PDR RESULTS:-



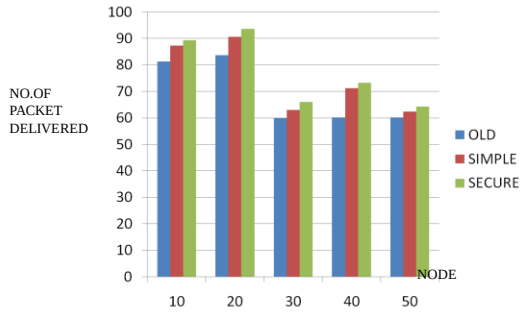
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

PDR RESULTS

NODE	OLD	SIMPLE	ATTACK	SECURE
10	81.24	87.24	83.24	89.24
20	83.61	90.61	86.61	93.61
30	60.04	63.04	60.04	66.04
40	60.18	71.18	69.18	73.18
50	60.19	62.29	60.29	64.29
ADDITION	351.26	374.36	359.36	386.36
AVERAGE	70.25	74.87	71.87	77.27

GRAPH FOR PDR



VI. CONCLUSION

In this paper each node has a table prepared to hold the addresses of the reliable nodes. During the process of route discovery, for each node receives a RREQ, it checks the behaviour of the broadcasting node. Once the behaviour of the broadcasting node is normal, it is added to the trust table of the receiving nodes.

The results shows that we can get better results for End to end delay, Packet delivery ratio, Throughput.

REFERENCES

[1] Johnson, B. Maltz, A. and Josh, B. (2001). "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," in Perkins, Charles E. (ed.) Ad Hoc Networking, Chapter 5, Addison-Wesely, pp. 139-172.

[2] Perkins, Charles E. and Royer, Elizabeth M. (1999)."Ad-hoc On-Demand DistanceVector Routing". Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (IEEE WMCSA '99), New Orleans, Louisiana, February 1999: 90-100.

[3] Li, Wenjia. and Joshi, Anupam. "Security in mobile ad hoc network (survey)". Department of Computer Science and Electrical Engineering, University of Maryland, Baltimor County.

[4] Ghaffari, Ali. (2006). "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24.

[5] Kargl, F. ,Schlott, S., Klenk, A., Geiss, A. and Weber, M. (2002). "Securing Ad hoc Routing Protocols", Proceedings of the 1st ACM Workshop on Wireless Security. Atlanta, GA, USA. Pages 1-10.

[6] Tamilselvan, Latha and Sankaranarayanan, V. (2007). "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (Aus Wireless 2007) India, 2007 IEEE.

[7] Hu, Y., Perrig, A. and Johnson, D. (2002). "A secure On-demand Routing Protocol for Ad Hoc Networks", in Proceedings of ACM MOBIC' 02. Atlanta, USA September 23–26.

[8] Marti, S., Giuli, T. J., Lai, K. and Bake, M. (2000). Mitigating Routing Misbehavior. In Mobile Ad hoc networks. 6th MobiCom, BA Massachuestts.

[9] Tamilselvan, Latha and Sankaranarayanan, V. (2008). "Prevention of cooperative black hole attack in MANET", in Journal of Networks, Vol. 3, NO. 5, MAY 2008.