Secure Routing in Wireless Sensor Networks

Haridas Kataria[1], Ravinder Singh Sheoran[2]

[1] *Lecturer CSE, Govt. Polytechnic for Women, Sirsa*
[2] *Lecturer CSE, Govt. Polytechnic for Women, Sirsa*

Abstract – The **Wireless Sensor Networks consists of small huge number of sensing nodes which have the sensing, computational and transmission power. Due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks. The security plays an important role in the ability to deploy and retrieve trustworthy data from a wireless sensor network. The proper operations of many WSNs rely on the knowledge of routing algorithms.**

This paper represents that the current routing protocols assume the networks to be benevolent and cannot cope with misbehaviour of nodes. The misbehaviour may be due to node being malicious to save the battery power. Whenever any device comes within the frequency range can get the access to the transmitting data and may affect the transmission. Thus, this work has significant importance, to build a highly secure system through frequency hopping.

Keywords: Security, Wireless Sensor Networks, Frequency hopping.

I. INTRODUCTION

Wireless Sensor Network is a heterogeneous network composed of a large number of small low-cost devices called nodes and few general-purpose computing devices referred to as base stations. The definition from SmartDust program of DARPA is:

"A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" [5].

The characteristics of WSN are wireless medium, low power consumption, low cost and low data rate. Other characteristics of WSN are large numbers of sensors, collaborative signal processing, easily deployed, self-configurable and self-organize, and infrastructure-less. Whereas, the characteristics of IEEE 802.15.4 (Low Rate Wireless Personal Area Network – LR WPAN) are data rates of 250 kb/s, 40 kb/s, and 20 kb/s, star or peer-to-peer operation, allocated 16 bit short or 64 bit extended.

WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don't have a global identification tags [11]. The major components of a typical sensor network are:

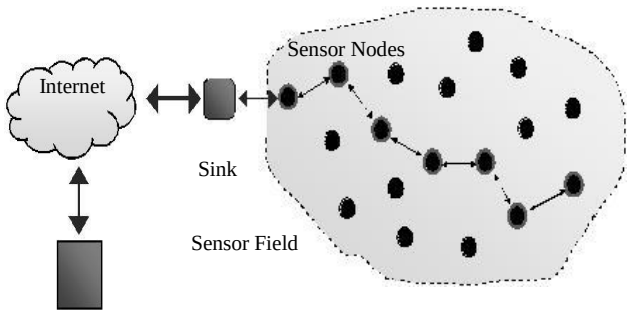

Figure 1. Components of Wireless Sensor Networks

Sensor Field: A sensor field can be considered as the area in which the nodes are placed.

Sensor Nodes: Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.

Sink: A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network.

Task Manager: The task manager also known as base station is a centralised point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation. Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So, the objective is to develop security in Wireless Sensor Network using frequency-hopping method, and to analyze the throughput before and after the implementation of frequency hopping.

The paper is divided into sections. Section I gives the introduction. Section II gives the routing concepts, Section III gives the proposed adaptive routing algorithm, Section IV gives the simulation results and fi nally Section V concludes the work.

II. ROUTING CONCEPTS

A router in the network needs to be able to look at a packet's destination address and then determines which of the output ports are the best choice to get the packet to that address. The router makes this decision by consulting a forwarding table. The fundamental problem of routing is: How do routers acquire the information in their forwarding tables?

Routing algorithms are required to build the routing tables and hence forwarding tables. The basic problem of routing is to find the lowest-cost path between any two nodes, where the cost of a path equals the sum of the costs of all the edges that make up the path. Routing is achieved in most practical networks by running routing protocols among the nodes. The protocols provide a distributed, dynamic way to solve the problem of finding the lowest-cost path in the presence of link and node failures and changing edge costs. Routing algorithms[3,4] are classified as adaptive and non-adaptive types. Non-adaptive routing algorithms are also known as forwarding tables or static routing algorithms, while the adaptive routing algorithms are dynamic in nature and automatically adjust to changes in the network topology or traffic. Dynamic routing algorithms are used in all modern routers, but some amount of programming is required to customize the routes according to the priority. Adaptive routing algorithms base their routing decisions upon current state of the system. In packet-switched mesh topology network the routing tables are created dynamically by obtaining neighbour and route information from other routers. Routers are constantly updated because routes are added or removed or may fail due to break in link. Convergence is the part of routing table update process. Convergence is complete when all routers in the network have updated their routing tables based on the information from other routers due to change in topology of network.
The routing algorithms are classified as Single Shortest path , Single Widest Path and Equal cost multi-path. In case of single shortest path and Single widest path routing algorithms all packets are forwarded to a single next hop where as in case of equal cost multi-path routing algorithm the packets are forwarded to each of several next hops in proportions specified by the routing parameters. Here we assume two types of traffic i.e. one tolerates out of order packet delivery(e.g. UDP) and the other does not tolerate(e.g. TCP).

The shortest path routing algorithm (SSP) is the simplest and default routing algorithm chosen by packet when routed from source node to destination node. But for large amount of data packets transmission, it has bandwidth limitation and drops the packets and performance degrades. So if there is a widest path available between the source and destination router then by adding some software routine, the data may be routed from source to destination router on the widest path available and packet drops may be reduced and performance may be improved. Further if the incoming data is large as compared to the capacity of outgoing link of routers then the packet drops will be observed so if there is a provision of equal cost multi-paths between the source router & destination router then by making the use of available resources the performance of the network may be improved by using the equal cost multi-path adaptive link state routing algorithm[8]. The Packet forwarding techniques are packet-level and flow-level. The packet-level technique is easy to implement in multi-path adaptive routing algorithm. The simulation results are evaluated for multi-paths routing algorithm (having two outgoing paths towards destination) along with SSP & SWP. Considering two outgoing paths being less costly & less complicated system, of course throughput increases as the no. of outgoing paths increases but at the same time the complexity and cost also increases but it depends upon the requirement of applications/ situations how many outgoing paths towards destination are there in a particular internet topology.

III. PROPOSED ALGORITHM

The Paessler traffic grapher [6] is easy to use software that monitors the bandwidth usuage of leased lines, routers and firewalls via SNMP, packet sniffing or netflow. So packet sniffing helps in deciding to select a particular routing algorithm in a network for better performance. The proposed adaptive routing algorithm operates in following three phases.

1. Light Load
2. Medium Load
3. Heavy Load

1. Start
2. Let P1=MLS, P2=SWP, P3=SSP
3. Monitor and measure current incoming traffic using PRTG software.
4. Based on current Incoming traffic router decides
   If Incoming Traffic<=L1 or L2 Mbps
   Run P3
   Else if Incoming Traffic (>L1 AND <L2 Mbps) or (>L2 AND <L1)
   Run P2
   Else
   Run P1
5. Continue the above steps till routing completes
6. Stop.

Here P1,P2,P3 are routing algorithms and L1 & L2 are the bottleneck links of path1 & path2 of the network or Path costs of Path1 & Path2 of the network under consideration.

IV. RESULTS AND PERFORMANCE ANALYSIS

Here, the results of the simulation are shown and the performance evaluation and their analysis is done. The analysis is being done on the basis of the results of *.nam file and the *.tr file with the help of Network Animator (NAM) and tracegraph by plotting the 2D and 3D graphs. We also evaluate the performance of the protocol by using AWK programming. With the help of AWK programming we obtain the results in percentage. Simulation has been divided in four parts that are given below:
In the simulation of simple AODV, experiment is carried over 25 nodes. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of route request (RREQ) and route reply (RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. Figure 1 and figure 2 are animation capture of WSN with25 nodes. The source (node 10) is broadcasting RREQ message to all its neighbours and Node 1which is the destination node, is sending RREP (route reply) back to the source. The nodes with the same frequency will receive the message and

forward it to its neighbours, while the nodes with different frequency will drop the packet. In figure 2, a packet of blue color is on transmission from the source (node 10) to the destination (node 1).

Since there is peer-to-peer communication between source node (10) and destination node (1), so no packet will be dropped. In figure 3 tracegraph proves that dropped packets are zero. This high throughput is expected because all the nodes are using the same frequency.

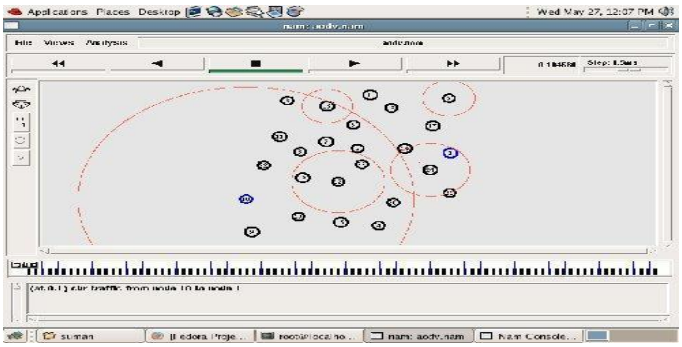

Figure 2. Source node broadcasts RREQ

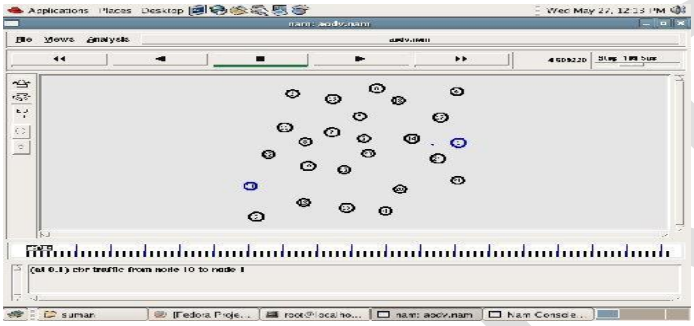

Figure 3. Transmission of data packets from source node to destination node

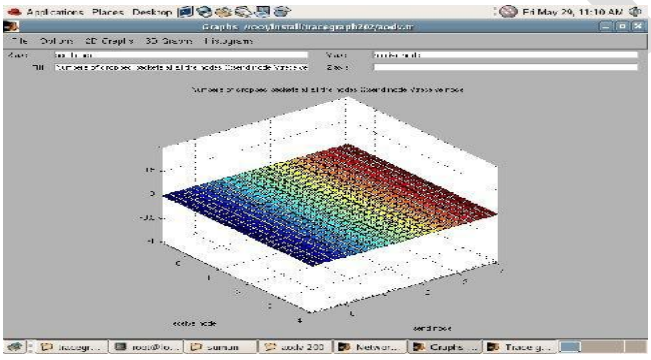

Figure 4. No packet dropping

AODV with Frequency Hopping

A data packet is received by the destination only when source and destination are using the same frequency. When frequency hopping is applied in the AODV without malicious node, throughput decreases because due to two frequencies in the network all the packets do not reach to the destination and drops in between. The throughput varies as two frequencies are hopped with different period of simulation time. The throughput is increased when period of simulation becomes longer. The throughput has been analyzed with awk script and tracegraph.

Simulation Time(sec)	Throughput in Percentage
50	58.8
100	79.4
200	89.7
300	93.1
400	94.8
500	95.8
1000	97.9
1500	98.6
2000	98.9

Table1. Percentage of received packets at the destination node

In table 1. tracegraph shows the received packets on the destination node. The table shows how the throughput changes with different simulation time.

AODV with Malicious Node

When malicious node (25) is inserted into the network as shown in the figure 5, it receives the broadcast packets and tries to behave like regular node of the network. In figure 5, malicious node 25 is broadcasting to all network nodes.

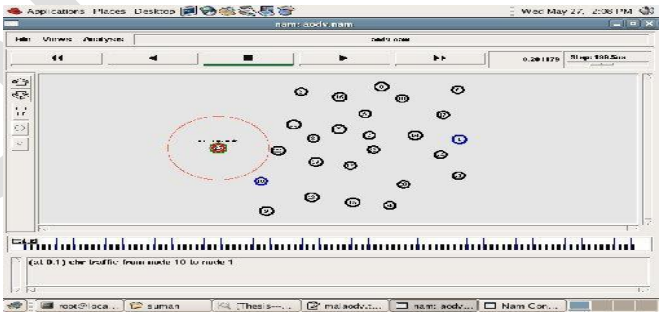

Figure 5. Malicious node broadcasts a RREQ.

Now malicious node (25) receives RREP packet from the destination node and sends its own data to the destination node 1. In figure 6, malicious node and source node both are sending their own data to the destination node. The packet from malicious node is of black color and it sends more packets than source node. The malicious node tries to jam the channel by sending more and more packets so that the throughput decreases.

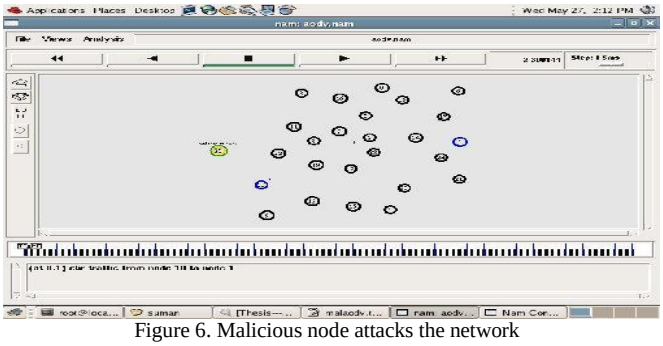

Figure 6. Malicious node attacks the network

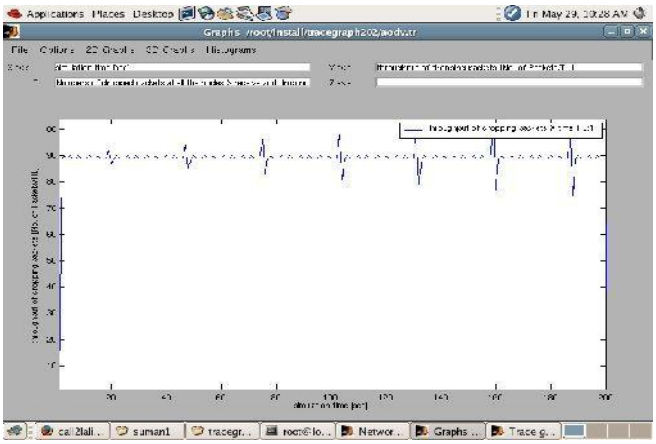

Figure 7. Throughput of dropping packet with malicious node

AODV with Malicious Node and Frequency Hopping

When frequency hopping is applied to the network (with malicious node), the network performance increases as the simulation time increases. Table 2 explains how the throughput increase as the simulation time increases.

Simulation Time(secs)	Throughput in % (10-1)	Throughput in % (25-1)
50	60	.4272
100	80	.2132
200	90	.1065
300	93.3	.0709
400	95	.0532
500	96	.0425
1000	98	.0212
1500	98.6	.0141
2000	99	.0106

Table2. Percentage of received packets at the destination node

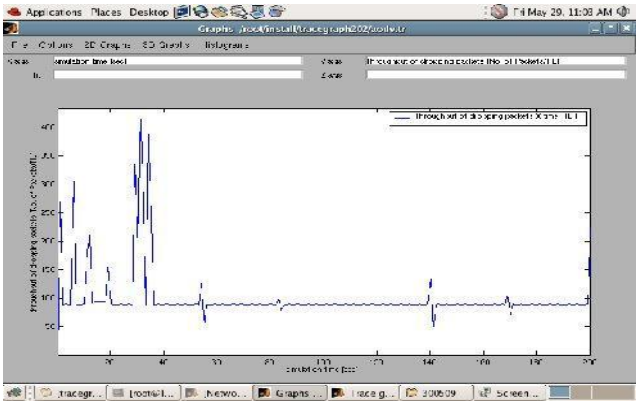

Figure 8. Throughput of dropping packet with malicious node and frequency hopping

V. CONCLUSION

Security is a significant issue in Wireless Sensor Networks. Intrusion of malicious nodes may cause serious impairment to the security. The objectives listed have been carried out. Here, all the modes of AODV (simple mode, frequency hopping and malicious node) along with their working have been discussed.

Here, AODV over WSN have been simulated with different operation modes. An important contribution of this paper is the comparison of the WSN with and without malicious node using the frequency hopping technique.

With the results of AWK programming and tracegraph, it can be concluded that in the case of simple AODV there is no packet drop and throughput is 100%. But when two frequencies are hopped in the network with different simulation times, throughput is less than 100% but increases continuously with respect to simulation time. After a simulation time of 2000 seconds (~33 minutes) almost 98 percent packets reach the destination safely.

As the malicious node enters into the network, it tries to capture the network. The performance of the network is affected badly. But, after applying frequency hopping, as the simulation time increases the throughput at the destination node also increases, which means that the network is secure enough to overpower the malicious node.

It is believed that the work will contribute in providing further research directions in the area of security based on frequency hopping.

REFERENCES

[1]. Brian Hill, "The Complete Reference, CISCO", TATA MCGRAW-Hill Publishing Ltd., N.Delhi, 3rd reprint, 2004.

[2]. James Irvine, David Harle," Data Communication and networks", John Wiley & Sons Ltd.,NewYork, USA,2002.

[3]. William Stallings, "Data and Computer Communications", PHI Pvt. Ltd. N.Delhi, 7th Edition , 2003.

[4]. Routing Basics http://www.cisco.com/ univercd/cc/ td/ doc/ cisintwk/ito-doc/ routing.htm.

[5]. Srinivas Vutukury, J.J. Garcia-Luna-Aceves, "A Traffic Engineering

[6]. Approach based on Minimum Delay Routing", Proceedings, Ninth International Conference on Computer Communications and Networks, 2000.

[7]. "PRTG Traffic Grapher V6 user manual",available at www.paessler.com/prtg/ download.

[8]. Srinidhi Varadarjan, Naren Ramakrishnan, Muthukumar Thirunavukkarasu, "Reinforcing reachable routes", Vol 43, PP. 389-416, Computer Networks, 2003.

[9]. Johnny chen, Peter Drushel,Devika Subramania " An efficient multi-path forwarding method", Proceedings of IEEE INFOCOM, SAN Francisco, CA, March,1998.

[10]. The Network Simulator NS-2, http://www.isi.edu/ nsnam/ns/ ns-documentation.

[11]. T. Wan, E. Kranakis and P.C. van Oorschot", S-RIP: A secure distance vector routing protocol," *Proceedings of Applied Cryptography and Network Security* (academic track), Yellow Mountain, China. LNCS vol.3089, pp.103-119. Springer-Verlag, June 8-11 2004

[12]. Z. Xu , S. Dai and J J. G.L. Aceves," A more efficient distance vector routing algorithms," 0-7803-4249-6/97 IEEE,1997

[13]. Niaz Morshed Chowdhury, Syed Murtoza Baker and Ershadhul H. Choudhury "Ant Navigation-based Adaptive Routing Technique for Mobile Ad hoc Networks", 2006.

[14]. H. Kumar, "Effectiveness of Distance Vector Routing Using Genetic Algorithm", Dissertation, Computer Dept., Chaudhary Devi Lal University, Sirsa, 2011.

[15]. K. Sunita, "Performance Analysis of Distance Vector Routing Using Genetic", Dissertation, Department of Computer Science & Engineering Guru Jambheshwar University of Science & Technology, Hisar, 2007.