Security in Wireless Sensor Networks using Frequency Hopping

Gaurav Sharma
ABES Engineering College
Ghaziabad, India

Suman Bala
Thapar University,
Patiala, India

A. K. Verma
Thapar University,
Patiala, India

Tej Singh
Dept. of Mathematics
AIT, Ghaziabad, India

ABSTRACT
A Wireless Sensor Network (WSN) is a collection of thousands of tiny sensor nodes having the capability of wireless communication, limited computation and sensing. These networks are vulnerable to internal and external attacks due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels. Since most of the existing routing protocols are application specific and hence do not satisfy the security constraints of wireless sensor networks. Whenever any device comes within the frequency range can get the access to the transmitting data and may affect the transmission. In this paper, we simulated the concept of frequency hopping and proved it a better approach to provide security in WSN..

General Terms
Wireless Sensor Networks, Security, Frequency Hopping.

1. INTRODUCTION
Sensors are small nodes which are capable of data processing and communication. The sensor node measures ambient conditions from environment, transform it into electrical signals and sends via radio transceiver to a sink and then this aggregated information is sent back to a base station through a gateway [2]. Sensor networks are distributed sensors to monitor conditions like temperature, sound, vibration, pressure and pollutants etc. WSN links physical world and digital data network and provide a distributed network having the constraint of scalability, lifetime and energy efficiency. WSN was initially developed for military and disaster rescue purposes but because of the availability of ISM band (2.4 GHz), the technology is now developing in public applications. The significant features in Wireless Sensor Network makes it different from other network; as they are self-organizing, consumes low power, requires low memory for storage and low bandwidth for communication, consists of large number of nodes, self-configurable, wireless, and infrastructure-less. Therefore, in order to provide a reliable network, WSN design must encounter the above mentioned features. However each sensor node in the network is equipped with its own sensor, processor and radio transceiver, so that a node has the ability of sensing, data processing and communicating to other node in the network.

Nodes are deployed densely throughout the area where they monitor specific phenomena and communicate with each other and with one or more sink nodes; that interact with a remote user. The user can insert commands into the sensor network via the sink to assign data collection; data processing and data transfer tasks to the sensors in order to receive the data sensed by the network. However, these networks are vulnerable to internal and external attacks due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels.

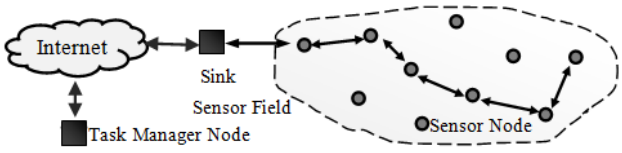

Figure 1. A Wireless Sensor Network

WSN are susceptible to failure and malicious user attack since the network is not physically strong. A normal sensor node is very easy to be captured to convert it into a malicious node. The insertion of a malicious node in the network is a quite easy task if security is not upto the mark. The malicious nodes or adversaries try to disrupt the network operation by modifying, fabricating, or injecting extra packets; they may mislead the operation of packet forwarding or will try to consume the resources of the nodes by making them believe that the packets are legitimate. The malicious node will not unite in the network operation resulting in the malfunction of the network operation. As we are aware that wireless communication only affects the physical, data link and network layers of the OSI layer, then getting access is not a difficult job for an adversary by attaining the same frequency band.

2. SECURITY IN WIRELESS SENSOR NETWORKS
Due to inherent limitations in wireless sensor networks, security is a crucial issue and a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. This section looks at the security problems that sensor networks face due to node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed [4, 8, 9, 14].

2.1 Security Goals for Wireless Sensor Networks
The security goals [4, 8, 9, 14] comprise both traditional networks and goals suited to the unique constraints of sensor networks. The security goals for sensor networks are:

2.1.1 Confidentiality
It confirms the ability to the concealment of messages from a passive attacker so that any message communicated via the sensor network remains confidential.

2.1.2 Integrity
It confirms the reliability of the data and refers to the ability to confirm a message has not been tampered with, altered or changed while on the network.

2.1.3 Authentication
It confirms the reliability of the message by identifying its origin. Data authentication verifies the identity of senders.

2.1.4 Availability
It confirms the ability to use the resources and whether the network is available for the messages to communicate.

2.2 Secure Routing in Wireless Sensor Networks
The major concern in WSN is not only the routing of information from source to destination through the network but also to take care of security measures which are necessary for transmission [8, 9]. Indeed; limited resources like energy, is one of the primary design requirements for these routing protocols. Moreover, the transmission range of a sensor is severely limited to save energy so that information that should be transmitted across the network have to be forwarded via multiple hops. Additionally, the energy of each single node has to be taken into account for the routing algorithm, so that overburdened nodes will run out of energy. While, the routing of information in sensor networks is an essential service, which makes communication possible in the first place, security issues in the area of routing were mostly ignored. Instead, most of the current routing protocols aiming at metrics such as reliability, robustness, responsiveness and preserving energy. However, security issues are not considered in the area of routing. As the sensor nodes are deployed in a hostile or in an unattended environment, this provides the opportunity for adversaries to launch certain attacks against sensor nodes, mainly, the capturing and compromising of the nodes. Reason is the physical access of the sensor nodes. This results in the transmission of wrong data in the network.

3. PROBLEM STATEMENT
Most current WSN routing protocols assume that the wireless network in benign and every node in the network strictly follow the routing behavior and is willing to forward packets for other nodes. Dynamic behavior of nodes in the network is also an addressable issue because most of the protocols do not send any information regarding misbehavior of any adversary node.

A commonly observed misbehavior is packet dropping. Basically, in a WSN, most devices have limited computing and battery power though packet forwarding consumes a lot of such resources. Consequently some devices would not like to forward the packet for the benefit of others and they drop packets not destined to them. In contrast, they still make use of other nodes to forward packets that they originate. These misbehaved or malicious nodes are very difficult to examine; whether the packet dropping is intentionally by malicious node or dropped due to link error. WSNs have many characteristics that make them vulnerable to malicious attacks. These are:

Due to open wireless channel (radio) to everyone, an interface is configured on same frequency band anyone can monitor or partake in communications. This provides a convenient way for attackers to break into the network.

Due to standard activity many routing protocols for WSNs are well-known in public; furthermore these do not include potential security considerations at the design stage. Thus, attackers can easily launch attacks by exploiting security holes in the protocols.

Due to the complexity of the algorithms, the constrained resources make it difficult to implement strong security algorithms on a sensor platform. It is difficult to design such security protocol. A stronger security protocol needs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a balance must be made between security and performance.

Due to deployment of nodes in the hostile areas, it is difficult to perform continuous monitoring. Thus, a WSN may face various attacks.

The problem of detection of the malicious nodes has been addressed separately in different protocols, which are either extensions or based on secure routing protocols. There are various approaches for providing security to networks. These are encryption, steganography, securing access to the physical layer; frequency hopping, etc. can provide security service to sensor networks.

Table 1. Network Parameter Definition

Parameter Name	Parameter Value
Channel Type	Channel/Wireless Channel
Radio Model	TwoRayGround
Netif	Phy/WirelessPhy/802_15_4
Mac Protocol	Mac/802_15_4
Number of Nodes	25
Number of malicious nodes	1
Routing Protocol	AODV
Grid Size	50 x 50 sq.m
Packet Size	70
Simulation Time	Varies
Traffic Type	CBR

4. SIMULATION
We use simulation to evaluate the performance of the proposed AODV routing protocol [1, 13] with and without the malicious node. We simulate a sensor network consisting of 25 nodes randomly deployed in a field of 50m × 50m square area. The base station is located in the middle of one edge. Nodes have same transmission range in our experiment. The simplest and usually the first thing to setup a network is creating a node. A network is

build up from its layer components such as Link layer, MAC layer and PHY layer. The components have to be defined before a node can be configured. Table 1 show the parameters used in the simulation.

5. RESULTS, PERFORMANCE EVALUATION & ANALYSIS

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) [11] and tracegraph [18] by plotting the 2D and 3D graphs. We also evaluate the performance of the protocol by using AWK Programming [3]. With the help of AWK programming we obtain the results in percentage. Simulation has been divided in four parts (i) AODV, (ii) AODV with frequency hopping, (iii) AODV with malicious node, and (iv) AODV with malicious node and frequency hopping.

5.1 Simulation of AODV

In the simulation of simple AODV [1], 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 (Tool Command Language) [15] file is written, NAM is invoked inside that file. Figure 2 and figure 3 are animation capture of WSN with 25 nodes.

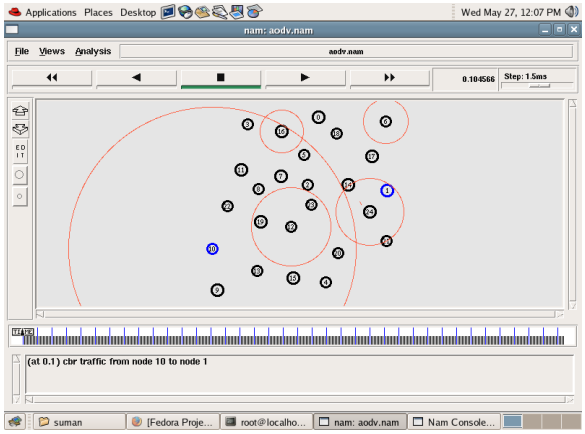

Figure 2. Source node broadcasts RREQ

The source (node 10) is broadcasting RREQ message to all its neighbors and Node 1 which 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 neighbor, while the nodes with different frequency will drop the packet. In figure 3, 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 4 tracegraph proves that dropped packets are zero. This high throughput is expected because all the nodes are using the same frequency.

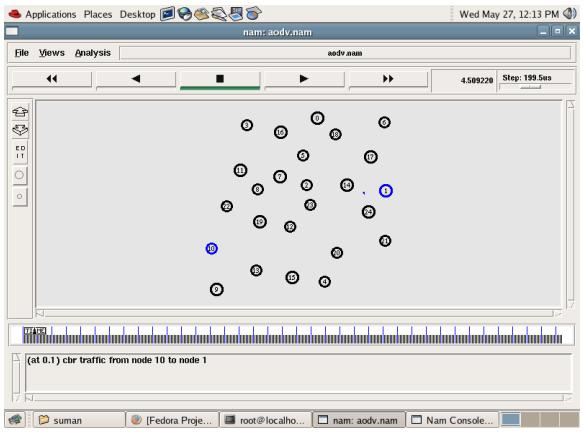

Figure 3. Transmission of data packets from source node to destination node

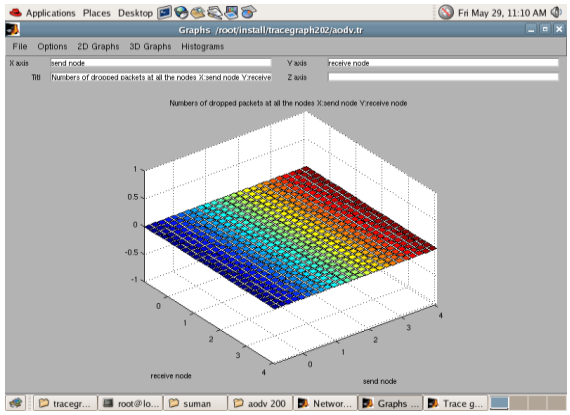

Figure 4. No packet dropping

5.2 Simulation of 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 [16, 19, 21] 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. In table 2, tracegraph shows the received packets on the destination node. The table shows how the throughput changes with different simulation time.

5.3 Simulation of 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.

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 7 shows the throughput of dropping packets with malicious node.

Table 2. Percentage Of Received Packets At The Destination Node

Simulation Time (sec)	*Throughput* (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

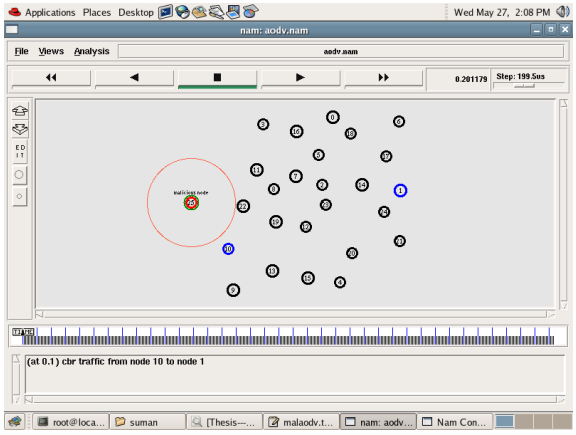

Figure 5. Malicious node broadcasts a RREQ

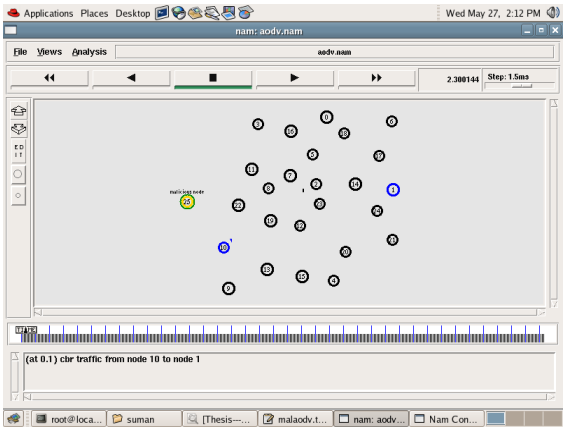

Figure 6. Malicious node attacks the network

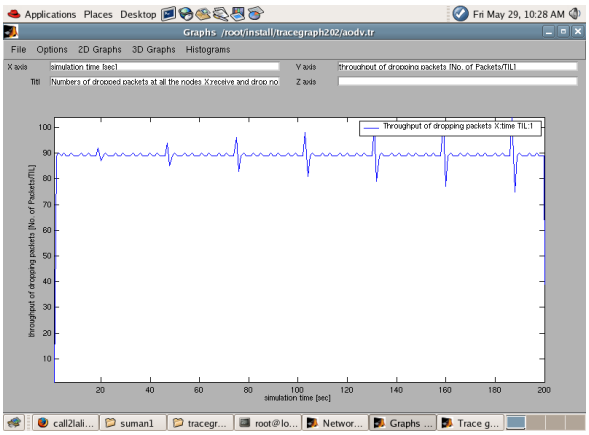

Figure 7. Throughput of dropping packet with malicious node

5.4 Simulation of 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 3, explains how the throughput increases as the simulation time increases. Figure 8 shows the throughput of dropping packets with malicious node and frequency hopping.

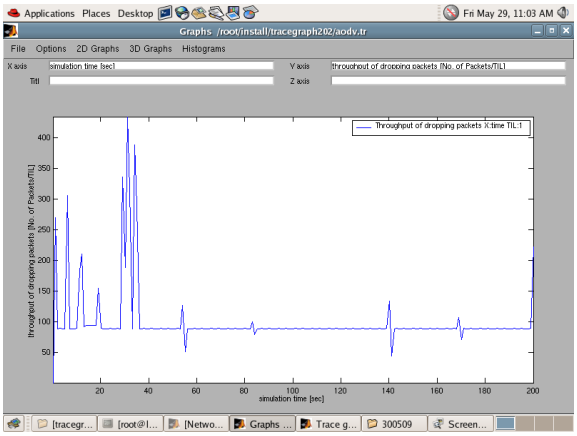

Figure 8. Throughput of dropping packet with malicious node and frequency hopping

5.5 Evaluation and Analysis

In the presented work, we have discussed all the modes of AODV (simple mode, frequency hopping and malicious node) along with their working. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping. In this paper, AODV over WSN is 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, we can conclude 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.

Table 3. Table captions should be placed above the table

Simulation Time (sec)	***Throughput*** **(percentage) (10-1)**	***Throughput*** **(percentage) (25-1)**
50	60	0.4272
100	80	0.2132
200	90	0.1065
300	93.3	0.0709
400	95	0.0532
500	96	0.0425
1000	98	0.0212
1500	98.6	0.0141
2000	99	0.0106

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. After 1500 seconds throughput is 98.66 percent and after 2000 seconds it is exactly 99 percent. Even malicious node 25 is about not able to affect the network performance for long period of time. So, frequency hopping works well and can be used as a reliable method for IEEE 802.15.4 [7, 10, 20]. Practical WSN security is a balancing act that is constantly in search of the highest level of protection that can be squeezed out of the judicious use of limited resources. A large number of security problems are still open in WSN. One of the open problems is authentication of sensor nodes. To secure the sensor network when a new node enters into the network, it should be authenticated. Another, aspect of future research direction can be a non-beacon enabled WSN. Further, path hopping is another optional concept that can be used to secure the sensor network.

6. REFERENCES

[1] Ad hoc on-demand distance vector (AODV) routing. Online Available: http://www.ietf.org/rfc/rfc3561.txt

[2] Bisdikian, C. 2001. An overview of the Bluetooth Wireless technology. IEEE Communication Magazine, vol. 39.

[3] Bruce Barnett. AWK – A Tutorial and Introduction. http://www.grymoire.com/Unix/Awk.html

[4] Carman, D., Krus, P., and Matt, B., 2000. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs.

[5] Crow, B., Widjaja, I., Kim, J., and Sakai, P. 1997. IEEE 802.11 Wireless Local Area Networks. IEEE Communication Magazine, Vol. 35.

[6] Ganesan, R., Govindan, S., Shenker, and Estrin, D., 2001. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. Mobile Computing and Communications Review, vol. 4.

[7] IEEE 802.15.4 WPAN-LR Task Group Website: http://www.ieee802.org/15/pub/TG4.html

[8] Jones, K., Waada, A., Olaniu, S., Wison, L., and Eltoweissy, M. 2003. Towards a new paradigm for Securing Wireless Sensor Networks. New Security Paradigms workshop 2003.

[9] Karlof, C., and Wagner, D., 2003. Secure routing in wireless sensor networks: attacks and countermeasures. University of California at Berkeley, USA, Ad Hoc Networks 1 (2003).

[10] Koubaa,A., Mario, A., Bilel, N., SONG, Y. Improving the IEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network.

[11] Marc Greis. Ns Tutorial. http://www.isi.edu/nsnam/ns/tutorial/index.html

[12] Roosta, T., Shieh, S. and Sastry, S., 2006. Taxonomy of Security Attacks in Sensor Networks and Countermeasures. Berkeley, California, University Press.

[13] Royer, E., and Perkins, C. An Implementation of the AODV Routing Protocols. http://reference.kfupm.edu.sa/content/i/m/an_implementation_study_of_the_aodv_rout_2328699.pdf

[14] Sastry, N., and Wagner, D., 2004. Security considerations for ieee 802.15.4 networks. In Proceedings of ACM workshop on Wireless security.

[15] TCL Tutorial. http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[16] Torrieri, D., 1989. Fundamental limitations on repeater jamming of frequency-hopping communications. IEEE Journal on Selected Areas in Communications, vol. 7, no. 4.

[17] Tovmark, K., 2002. Frequency Hopping Systems (Rev. 1.0). Chipcon Application Note AN014. http://electronix.ru/forum/index.php?act=Attach&type=post&id=3712

[18] Tracegraph http://www.tracegraph.com/download.html

[19] Vanninen, T., Tuomivaara, and H., Huovinen, J., 2008. A Demonstration of Frequency Hopping Ad Hoc and Sensor Network Synchronization Method on WARP Boards. WinTech'08, ACM 978-1-60558-187-3/08/09.

[20] Zheng, J., and Lee, M. 2006. A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations. Wiley Interscience. IEEE Press Chapter 4. 218-237.

[21] Zyren, J., Godfrey T., and Eaton, D. Does frequency hopping enhance security? http://www.packetnexus.com/docs/20010419_frequencyHopping.pdf