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

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 4, April 2013*

# Throughput Analysis of the Frequency Hopping Technique Against Malicious Node Attacks in Wireless Sensor Networks

Eliza Gail Maxwell[1], Mintu Philip[2]

M.Tech Student, Department of Computer Science, Rajagiri School of Engineering and Technology, Kochi, India [1]

Asst. Professor, Department of Computer Science, Rajagiri School of Engineering and Technology, Kochi, India [2]

**Abstract**: Wireless Sensor Networks (WSN) is the recent concept in the networking field that consists of a large number of tiny nodes capable of sensing, processing and transmitting data. Most routing protocols are designed with the aim to decrease power consumption at the cost of security. The insecure nature of the wireless channels and the fact that packets can easily be tampered with, makes wireless sensor networks easily prone to internal and external attacks. Thus security is a major requirement to ensure the transmission and reception of reliable data in a WSN. Many of the standing routing algorithms developed for WSN's are susceptible to attacks in hostile environments. An important security concern is the threat of a malicious node. The routing protocols at present presume the networks to be altruistic and incapable of dealing with the misbehavior of nodes. A malicious node can get unauthorized access to data if it comes within the frequency range at which the data is being transmitted in the network. This paper discusses how the concept of frequency/channel hopping is an efficient method to tackle the attacks from a malicious node by analyzing the throughput of the proposed AODV routing protocol using NS2.

**Keywords**: Wireless Sensor Network, Security, Malicious node, Frequency hopping

## I. INTRODUCTION

Latest innovations in wireless communications and integrated circuit technology have enabled the technological advancement of low-priced, low-power, infrastructure-less, multifunctional sensor nodes that require low bandwidth for communication [1]. A sensor network is composed of a large number of these sensor nodes that are densely deployed to monitor the conditions like temperature, pressure, sound etc. Hence reliable sensor network protocols and algorithms must have the capability to self-organize and work in a co-operative fashion.

A remote user can give commands to the sink node to assigned tasks to the nodes such as data collection, data processing and data transfer. Wireless Sensor Network is categorized in IEEE 802.15.4 task group that is in Low Rate Wireless Personal Area Network. The insecure nature of the wireless channels and the fact that packets can easily be tampered with, makes wireless sensor networks easily prone to internal and external attacks. Many of the standing routing algorithms developed for WSN's are susceptible to attacks in hostile environments.

An important security concern is the threat of a malicious node. The routing protocols at present presume the networks to be altruistic and incapable of dealing with the misbehavior of nodes. When a malicious node is inserted into a network it interferes with the data transmission by creating, altering and transmitting unwanted packets in the sensor network. This is mainly due to the fact that when any new device enters the network within a particular frequency range it can easily tamper with the packet transfer taking place at that frequency. This either disturbs the normal operation of packet forwarding or it will convince the other nodes that the malicious packets are indeed legitimate. Thus the network has to be secured against these malicious node attacks.

The remainder of this paper is organized as follows. Section II discusses the related work regarding various security mechanisms in wireless sensor networks. Section III explains the problem statement. In Section IV the working of the frequency hopping algorithm is explained. Section V explains the performance analysis of the frequency

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

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 4, April 2013*

hopping/channel approach. Finally, the paper is concluded in Section VI.

## II. RELATED WORK

Many security mechanisms have been formulated for the security of the WSN [2]. Cryptography is one of the most commonly used security mechanism for the detection of the malicious nodes. The technique requires security keys in the algorithm that consume the memory storage space inside the device. Public key algorithms such as RSA [3] are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single security operation. Private key operations are still too expensive in terms of computation and energy cost to accomplish in a sensor node. Key management is another core mechanism to ensure the security of network services and applications in WSNs. Secure establishment of required keys between sensor nodes for exchange data is the goal of key management. A pair-wise private key sharing scheme [4] requires pre-distribution and storage of n – 1 keys in each node, where n is the number of nodes in a sensor network. This requires large amount of memory so pair-wise schemes are not recommended when the network size is large. Furthermore, many key pairs would be unusable since direct communication is possible only among neighboring nodes. There are different challenges in providing security to a WSN deployment [5]. The problem of detecting the malicious nodes has been addressed separately in different protocols [6], which are either extensions or based on secure routing protocols. There are various ways for providing security to networks. These are encryption, steganography, and securing access to the physical layer; frequency hopping can provide this service to sensor networks. So, in WSN that aims to use as minimal space as they can in order to save energy, frequency-hopping techniques was chosen.

## III. PROBLEM STATEMENT

Security attacks consist of passive attacks and active attacks [7]. When there is an observer who trying to obtain any information being transmitted, it is considered passive attack. Eavesdropping or monitoring of transmission is an example of passive attacks. When there is an attack to modify the data stream, it is considered an active attack such as denial of services. Many of the standing routing algorithms developed for WSN's are susceptible to attacks in hostile environments. An important security concern is the threat of a malicious node. The routing protocols at present presume the networks to be altruistic and incapable of dealing with the misbehavior of nodes. A malicious node can get unauthorized access to data if it comes within the frequency range at which the data is being transmitted in the network. Most of these protocols deal well with the dynamically changing topology. However, the problem of the misbehavior of nodes in the network is often not addressed. Packet dropping is one of the commonly observed misbehavior. In a WSN, the devices have limited processing and battery power while packet transmission consumes a lot of such resources. Thus, some devices would not choose to forward packets for the advantage of other nodes.

They simply drop the packets not destined to them while they use the other nodes to forward packets that are originated by them. It is very difficult to examine whether the packet dropping is done intentionally by a misbehaving node or whether the drop is due to a communication link failure in the network. In order to achieve secure routing in WSN, the frequencies used need to be varied within a short time interval. So if there is any malicious node that is trying to transmit information or retrieve information from inside the network, the attack can be avoided if the node cannot detect the randomly changing frequencies at which the packet transmission is taking place in the network. Therefore, by using frequency hopping, any intruder can be prevented from attaining that frequency.

## IV. FREQUENCY/CHANNEL HOPPING APPROACH

Frequency/channel hopping is one of many ways to secure data transmission in wireless networks [8, 9]. This solution provides integrity, confidentiality and availability for the sensor networks that consist of anonymous nodes. The frequency/channel hopping approach does not allow an intruder or malicious node to access the channel easily [10]. The frequency at which the network is functioning will be hopped to different frequencies/channels frequently. Thus, the malicious node will find it difficult to tamper with the data being transmitted. Suppose a set of frequencies are hopping in a limited time period fixed earlier and an intruder gets access to the channel and jams the channel, only that particular channel will be affected. The other channels will be still available for data transmission.

When the number of frequencies is increased or when the time slot of each frequency is randomly set, the probability of the intruder accessing the channels and jamming the frequency will be significantly small. In a frequency hopping ad hoc network, the phase of hopping sequence is usually estimated from each node's local clock reading. This is required to synchronize all the nodes in the network to simultaneously hop to the same frequency channel. A random function determines the time slot for each frequency. The Ad hoc On Demand distance Vector (AODV) routing protocol is used since the main focus is on ad-hoc networks [11].

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

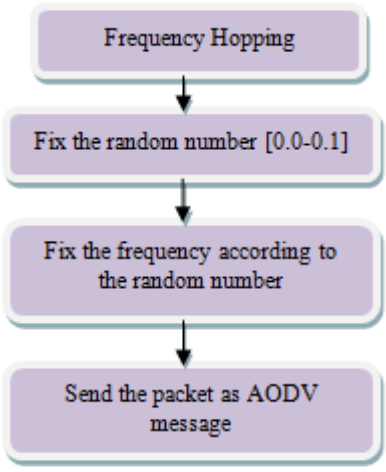


Fig. 1. Frequency hopping at transmitting side

Fig. 1 shows a flow chart of additional code added inside the AODV function modules that will forward the AODV message. The frequency held by a packet was set according to the random number generated.

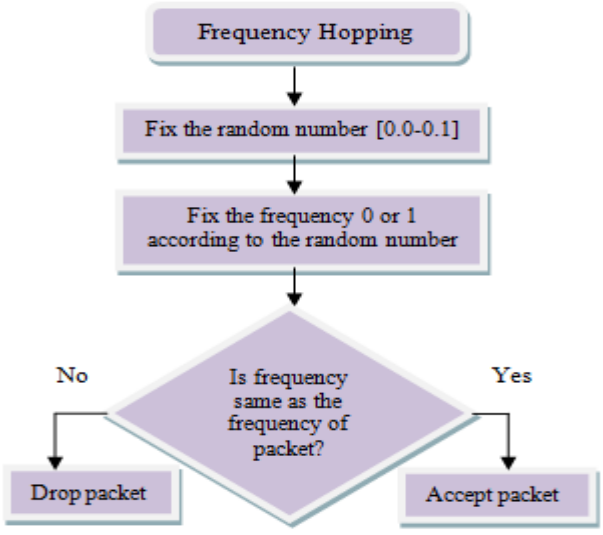


Fig. 2. Frequency hopping at receiving side

The additional coding that is added inside the AODV function modules that will receive the AODV message is shown in Fig. 2. A basic random generator function is used to generate a random float uniformly in the range [0.0, 1.0]. If the packet is transmitted at a frequency same as that of the fixed frequency the packet will be accepted. If the frequencies don't match then the packet is dropped.

## V. PERFORMANCE ANALYSIS

The simulation of the proposed AODV routing protocol was done in NS2 [12]. The sensor network consisted of 25 nodes randomly deployed in a field of 50m x 50m square area. Source node and malicious node send the packets to the same destination. In order to know the performance of the system, the throughput at the destination node was analyzed. Three scenarios are analyzed below.

In Scenario 1, the throughput in the absence of a malicious node before using frequency hopping was analyzed.

In Scenario 2, the throughput in the absence of a malicious node after using frequency hopping was analyzed.

In Scenario 3, the throughput in the presence of a malicious node after using frequency hopping was analyzed.

Finally, the throughput from source and from malicious node is compared.

In Scenario 1, the throughput is 100% as shown in Fig. 3. The high throughput is expected because all nodes are using the same frequency. Thus, each node is reachable between one and another.

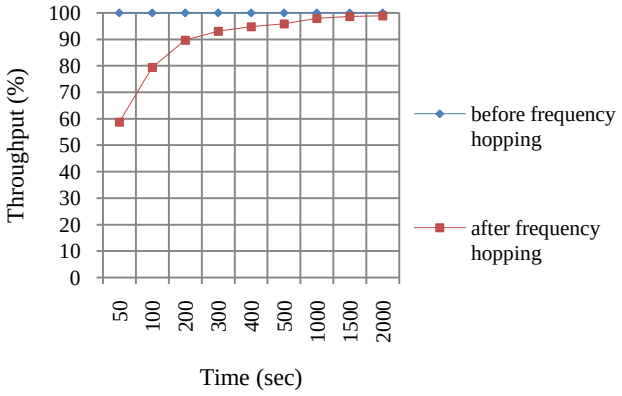


Fig. 3. Throughput over time in absence of malicious node

In Scenario 2, the throughput decreases because of the hopping taking place between two frequencies. So all packets do not reach the destination node and are therefore dropped. However, the throughput increases as simulation time increases. As seen in Fig. 3, after a simulation time of 2000 seconds approximately 98% of the packets reach the destination unharmed.

In Scenario 3, when the malicious node is inserted into the network it interferes with the data transmission between the source node and destination node. The network performance is affected badly. But after applying frequency hopping, the throughput at the destination nodes increases as the simulation time period is increased. Hence the network becomes secure enough to overpower the malicious node.

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

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 4, April 2013*

The throughput is observed to be 98.7% after 1500 seconds of simulation time and it becomes exactly 99 percent after 2000 seconds.

Fig. 4 shows the comparison of throughput from the source node and the malicious node using two frequency hops and four frequency hops. When using two frequencies, throughput from source is 91% while from malicious node is 80%. But when four frequencies are used, throughput from malicious node decreased rapidly to 27%. This is seen in Fig. 4. Even though throughput from source also decreased to 82% the amount is too small to be significant when compared to throughput from malicious node. Therefore, WSN's security is improved.

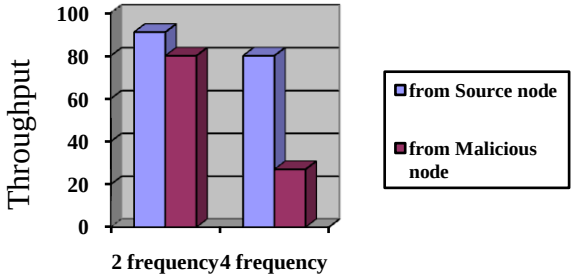


Fig. 4. Comparison of throughput at the detination node between 2 frequency hops and 4 frequency hops

## VI. CONCLUSION

The frequency hopping security approach against malicious nodes was discussed in this paper. The throughput at the destination node was analyzed before and after the implementation of frequency hopping to compare the network performance. Without frequency hopping the WSN network is open to malicious attack, thus allowing high throughput from the malicious node. Then, the network was tested with the frequency hopping security technique was applied. The throughput from source and from malicious node is compared. Results show that the throughput from malicious node decreases in the presence of frequency hopping thus providing security in the network.

## REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, no. 38, pp. 393–422, 2001.

[2] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures Ad Hoc Networks, 1 (2003), pp. 293‑315

[3] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and **public-key** cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978

[4] Du, W., Deng, J., Han, Y. S., and Varshney, P. 2003. A pairwise key pre-distribution scheme for wireless sensor networks, Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03). 42–51.

[5] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks: Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[6] W. J¶unior, T. Figueiredo and H. Wong. Malicious node detection in wireless sensor networks. In Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS 2004).

[7] Chris Karlof, David Wagner, "Secure routing in WSNs: attacks and countermeasures", Ad hoc networks Journal, vol. 1, Issue 2-3, Sept. 2003, pp.293-315.

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

[9] Vanninen, T., Tuomivaara, and H., Huovinen, J., 2008. A Demonstration of Frequency Hopping Ad Hoc and Sensor Network Synchronization Method on WARP Boards.

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

equencyHopping.pdf

[11] C.E Perkins and E.M. Royer, "Ad hoc On-Demand Distance Vector Routing," in *The Proceedings of the 2nd IEEE Workshop on mobile Computing Systems and Applications*, New Orleans, 1999,pp. 90-100.

[12] Marc Greis. Ns Tutorial. http://www.isi.edu/nsnam/

ns/tutorial/index.html

## BIOGRAPHY

**Eliza Gail Maxwell** is currently pursuing M.Tech in Computer Science and Engineering with Specialization in Information Systems at Rajagiri School of Engineering and Technology, Kochi, Kerala. She received B.Tech degree in Computer Science and Engineering from College of Engineering, Perumon affiliated to CUSAT, Kerala in 2011.

**Mintu Philip** is currently working as Assistant Professor in Department of Computer Science at Rajagiri School of Engineering and Technology. She received B.Tech degree in Computer Science and Engineering from Rajagiri School of Engineering and Technology, Kerala in April 2008. She completed M.tech in Computer Science with Specialization in Data Security under CUSAT, Kerala in 2011.