A Protected Routing Approach in WSN's

Shankar Singh
M.Tech Student, JEC Kukas, Jaipur

Balram Singh
M.Tech Student, JEC Kukas, Jaipur

Narendra Kumar Agrawal
Reader & HOD, JEC Kukas, Jaipur

Abstract - Wireless Sensor Networks is the new concept in the field of networks consists of small, large number of sensing nodes which is having 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. Moreover, routing protocols are designed, taking the consideration of power consumption not security as a goal. Current routing protocols assume the networks to be benevolent and cannot cope with misbehavior of nodes. The misbehavior 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 Networks (WSN) relies on collaborative work of large number of sensors. For this reason, they 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 inject 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, 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. WSN are prone to failure and malicious user attack because it is physically weak, a normal node is very easy to be captured to become a malicious node or by inserting a malicious node in the network. The malicious nodes 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 cooperate in the network operation resulting in the malfunction of the network operation. This happens because any device within the frequency range can get access to the data. So, we need a secure way to protect the network. Wireless communication only affects the physical, data link and network layers of the OSI layer.

1.1 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 examines 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.

1.1.1 Security Goals for Sensor Networks

The security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The four security goals for sensor networks are:

- *Confidentiality*: The ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.
- *Integrity*: It ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. Even if the network has confidentiality measures in place, there is still a possibility that the data's integrity has been compromised by alterations.
- *Authentication*: It ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional bogus packets. Therefore, the receiving node needs to be able to confirm that a packet received does in fact stem from the node claiming to have sent it. Data authentication verifies the identity of senders. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys to compute the Message Authentication Code (MAC).
- *Availability*: The ability to use the resources and whether the network is available for the messages to communicate.

1.1.2 Secure Routing in Wireless Sensor Networks

A wireless sensor network is only as good as the information it produces. In this respect, the most important concern is information security. Indeed; in most application domains sensor networks will constitute a mission critical component requiring commensurate security protection. Sensor network communications must prevent disclosure and undetected modification of exchanged messages. Due to the fact that individual sensor nodes are anonymous and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks. If an adversary can thwart the work of the network by perturbing the information produced, stopping production, or pilfering information, then the perceived usefulness of sensor networks will be drastically curtailed. Thus, security is a major issue that must be resolved in order for the potential of wireless sensor networks to be fully exploited.

II. 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. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

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

- A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
- Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
- Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.
- A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, a WSN may face various attacks.

The problem, 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 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.

III. RESULTS

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:

Simple AODV Simulation:

- AODV with frequency hopping
- AODV with malicious node

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.

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.

Table: Percentage of received packets at the destination nod

Simulation Time(secs)	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

With the results, 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. 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.

IV. 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. In the presented work, we have discussed all the modes of AODV (simple mode, frequency hopping and malicious node) along with their working. In this work, AODV over WSN is simulated with different operation modes. An important contribution of this work is the comparison of the WSN with and without malicious node using the frequency hopping technique. 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.

REFERENCES

[1] Stephan Olariu, "*Information assurance in wireless sensor networks*", Sensor network research group, Old Dominion University.

[2] J. Zheng and Myung J. Lee (2006). *A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations*: Wiley Interscience. IEEE Press 218-237.

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

[4] Anis Koubaa, Mario ALVES, Bilel NEFZI, Ye-Qiong SONG, "*Improving the IEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network*".

[5] Anis Koubaa, Mario ALVES, Eduardo TOVAR, "*A Comprehensive Simulation Study of Slotted CSMA-CA for IEEE 802.15.4 Wireless Sensor Network*".

[6] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "*A survey on sensor networks*", IEEE Communication Magazine, Aug. 2002.

[7] Dr. A.K. Verma, Mayank Dave, R C Joshi, "*DNA-Cryptography a novel paradigm for securing MANETs*", vol-11-2008, no-4PP-393-404" J. Discrete Mathematics Science & Cryptography.

[8] Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "*SPINS: security protocols for sensor networks*", in: Proceedings of Mobile Networking and Computing 2001, 2001.

[9] Chris Karlof, David Wagner, "*Secure routing in wireless sensor networks: attacks and countermeasures*", University of California at Berkeley, Berkeley, CA 94720, USA, Ad Hoc Networks 1 (2003) 293–315.