Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.966 – 973

RESEARCH ARTICLE

Secure Routing in Wireless Sensor Network

Renu Bala[1]

[1]Research Scholar, Department of Computer Science and Engineering, Ganga Institute Of Technology & Management, Kablana

Email ID: yadavrenu847@gmail.com

Dr. Yashpal Singh

Email ID: yashpalsingh009@gmail.com

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. As 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.

However, most existing routing algorithms developed for WSNs are vulnerable to attacks in hostile environments.

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.

1. INTRODUCTION

Due to the recent advancement in micro-electro-mechanical systems (MEMS), wireless communication like Bluetooth [1], IEEE 802.11 [2], or MANETs [3], a new concept of networking has emerged known as Wireless Sensor Networks (WSNs). Wireless Sensor Network, consists of large number of sensor nodes having the capability of wireless communication, limited computation and sensing. 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 emerging in public applications. The salient features in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and radio transceiver, so it has the ability of sensing, data processing and communicating with each other.

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 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.

2. STATE OF ART

Many security mechanisms have been proposed for the security of the WSN. Most of the mechanisms for the detection of the malicious nodes are based on the cryptography. The technique requires security keys in the algorithm that consume the memory storage space inside the device. There are different challenges in providing security to a WSN deployment. These are: There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between the two of them. During the design of any security solution we need to take care of following 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.

The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and limitations or constraints of sensor node hardware.

Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message,

The communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire-based security schemes impractical for WSNs.

The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of it is unpredictable.

The problem of detecting 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 [4]. 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. In order to know the performance of the system, the throughput at destination was analyzed. Source and malicious node are sending the packets to the same destination. First examine the throughput without using frequency hopping, and then compare it with throughput by using frequency hopping. After that, throughput from source and from malicious node is compared. 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.

3. CHARCTRISTICS

Scalability*:*-Scalability means that large scale of deployment. A sensor networks are combination of thousands, or more, micro-sensor nodes. So Scalability in sensor network protocols is an important requirement. Because every sensor nodes not containing global information about the network.

Low Complexity:-Sensor nodes are usually highly limited due to limitations from energy resource and cost. For this we need fully distributed, light weight localization one tracking algorithm is needed.

Ad-hoc Network:-Ad-hoc deployment implies no maintenance or battery replacement. To increase network lifetime no raw data is transmitted. Large numbers of self-organizing static as mobile nodes are possibly randomly deployed. Interference is high for Omni-directional antennas.

Lifetime: - Increase lifetime of network nodes is battery-powered. Nobody is going to change the batteries so save energy.

Simple*:* -WSN is a simple mobility of nodes. Distributed sensing as large no, of nodes are used to collect and storing data. Distributed sensing was provided robustness to the system. No need to install extra infra-structure for communication.

4. SECRITY 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.

5. Routing Techniques in Wireless Sensor Networks

Due to WSNs differing from one network to another, many new algorithms have been proposed for the routing problem in WSNs. These routing mechanisms have considered the characteristics of sensor nodes depending on the type of application and underlying architecture requirements. Almost all of the routing protocols can be classified according to the network structure as flat, hierarchical or location-based.

6. Threat Models

As discussed in Security threat in a WSN can be divided into various categories. These are:

External threats versus internal threats: An external threat occurs from outside the sensor network and may amount to mere passive eavesdropping on data transmissions, but can extend to injecting bogus data into the network to consume network resources and rage Denial of Service (DoS) attacks. An internal threat occurs from compromised nodes running malicious data or from attackers who have stolen the cryptographic contents from legitimate nodes.

Mote-class attacker versus laptop-class attacker: A mote-class attacker has access to a few motes with the same capabilities as other motes in the network. However a laptop-class attacker has access to more powerful devices, such as laptops.

Insider attack versus outsider attack: An outside attacker has no special access to the sensor network, such as passive eavesdropping. On the other hand an inside attacker has access to the encryption keys or other codes used by the network.

***Passive attacker versus active attacker*:**
Passive attackers are only interested in collecting sensitive data from the sensor network, which compromises the privacy and confidentiality requirements. These are attempts to reach the owner data and make use of it without the owner realizes it. It is hard to detect this kind of attack because it does not modify the data. So, the prevention of the attack is more useful rather than struggle for detection. The types of passive attacks are:

***Release of message contents*:** Any information transferred through telephone conversation or electronic mail can be release to opponent which data may contains confidential information.

***Traffic Analysis*:** Opponent can observe the frequency and length of data being transmitted and this information can be analyzed to get the nature of communication taking place. The attacker also may know the location of base stations, and the type of protocol being used in the transmission.
Here are four types of active attacks:

- *Masquerade*: Impersonation of an identity that pretends to be an authorized identity.
- *Replay:* A passive capture of information to produce an unauthorized effect.
- *Modification of Message*: The sequence of message has been jumble-up or the message has been delayed or even worst the meaning of message has been modified.
- *Denial of Service (DoS)*: DoS may disrupt the network and degrade its performance. This type of attack can be grouped into three categories: disabling of service (e.g., sinkhole, HELLO flood attack), exhaustion, and service degradation (e.g., selective forwarding attack)

An example of passive attack is - Eavesdropping. An attacker that monitors traffic can read the data transmitted and gather information by examining the source of a packet, its destination, size, number, and time of transmission. The active attackers' goal is to disrupt the function of the network and degrade its performance. These are involving alteration of information that may be disastrous to the organization. Oppose to passive attack, active attack is more likely to be detected rather than to prevent. Furthermore, the detection has a preventive effect that may contribute to prevention as well.
An example of active attack can be - Man-in-the-middle attack, in which a rogue establishes an intermediary, pretending to be a valid sensor.

7. 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.

8. TECHNOLOGY USED

Fedora Core 4

Fedora Core is a free operating system based on Linux. The development of Fedora is sponsored by Red Hat; and being developed by the open source community and the Red Hat engineers. Some primary features of FC4 are extensive performance improvements, support for Intel-based Macs and a new Graphical User Interface (GUI) virtualization manager.

The Network Simulator (NS2)

Simulation can be defined as "Imitating or estimating how events might occur in a real situation". It can involve complex mathematical modelling, role playing without the aid of technology, or combinations. The value lies in the pacing you under realistic conditions that change as a result of behaviour of others involved, so you cannot anticipate the sequence of events or the final outcome.

Tool Command Language (Tcl)

Short for Tool Command Language, Tcl is a powerful interpreted programming language developed by John Ousterhout at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language.

It has a wide range of usage including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

The Network Animation (NAM)

The network animator (NAM) began in 1990 as a simple tool for animating packet trace data. This trace data is typically derived as output from a network simulator like ns or from real network measurements, e.g., using tcpdump. Steven McCanne wrote the original version as a member of the Network Research Group at the Lawrence Berkeley National Laboratory, and has occasionally improved the design as he's needed it in his research. Marylou Orayani improved it further and used it for her Master's research over summer 1995 and into spring 1996. The nam development effort was an ongoing collaboration with the VINT project. Currently, it is being developed at ISI by the SAMAN and Conser projects.

The Tracegraph

It is a data presentation system for Network Simulator ns-2. The simulator doesn't have any options implemented to analyse simulations results so it's hard to use it. Trace graph system provides many options for analysis, including 250 graphs and statistical reports. It is implemented in MATLAB 6.0 and can be compiled to run without MATLAB. Compiled versions for Linux and Windows systems are available for download at http://www.geocities.com/tracegraph/.

Trace graph supports the following ns-2 trace file formats; wired, satellite, wireless (old and new trace), wired-cum-wireless. Trace file loading stage is divided into 4 stages; automatic trace file format recognition, trace file parsing to extract necessary simulation data which is saved to a temporary file, trace files can contain much more data than is needed by the system, so unnecessary information is omitted to speed up trace file loading, temporary file loading, constants calculations (packets types, packets sizes, flows IDs, trace levels, number of nodes, simulation time) – in order to speed up data processing. Wireless and wired-cum-wireless trace files are parsed and saved in Trace graph format.

9. 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. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping.

In this thesis work, AODV over WSN is simulated with different operation modes. An important contribution of this thesis 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.

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.

REFERENCES

[1] ChatschikBisdikian, "*An overview of the Bluetooth Wireless technology*", IEEE Communication Magazine, vol. 39, Dec 2001.

[2] Brain P. Crow, IndraWidjaja, JeonGeun Kim and Prescott T. Sakai, "*IEEE802.11 Wireless Local Area Networks*", IEEE Communication Magazine, Vol.35, Sep 1997

[3] J. Macker and S. C. (chairmen). MANET (Mobile Ad Hoc Networking) working group of the IETF.

[4] K. Jones, A.Waada, S. Olaniu, L.Wison, M. Eltoweissy, "*Towards a newparadigm for Securing Wireless Sensor Networks*", New Security Paradigmsworkshop 2003, Ascona, Switzerland.

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

[6] J. Zheng and Myung J. Lee (2006). *A comprehensive performance study ofIEEE 802.15.4 – Sensor Network Operations*: Wiley Interscience. IEEE PressChapter 4. 218-237.

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

[8] Jose A' Gutirez et al. "*IEEE 802.15.4: A Developing for Low Rate WirelessPersonal Area Network".*

[9] AnisKoubaa, Mario ALVES, Bilel NEFZI, Ye-Qiong SONG, "*Improving theIEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network".*

[11] AnisKoubaa, Mario ALVES, Eduardo TOVAR, "*A ComprehensiveSimulation Study of Slotted CSMA-CA for IEEE 802.15.4 Wireless Sensor Network".* Karp and H. T. Kung, "*GPSR: greedy perimeter stateless routing for wirelessnetworks*", in *Mobile Computing and Networking*, 2000, pp. 243–254.

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

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

[14] Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "*SPINS: security protocolsfor sensor networks*", in: Proceedings of Mobile Networking and Computing2001, 2001.

[15] 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.

[16] Intanagonwiwat, R. Govindan, and D. Estrin, "*Directed diffusion: A scalableand robust communication paradigm for sensor networks*", in *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00)*, August 2000.

[17] Elizabeth M. Royer, Charles E.Perkins, "*An Implementation of the AODVRouting Protocols"*.

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

[19] TeemuVanninen, HannuTuomivaara, JuhaHuovinen "*A Demonstration ofFrequency Hopping Ad Hoc and Sensor Network Synchronization Method on WARP Boards*", WinTech'08, September 19, 2008, San Francisco, California,USA. ACM 978-1-60558-187-3/08/09.

[20] Ye, A. Chen, S. Liu, L. Zhang, "*A scalable solution to minimum costforwarding in large sensor networks*", Proceedings of the tenth InternationalConference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001. Ye, S. Lu, L. Zhang, "*GRAdient broadcast: a robust, long-live large sensornetwork*", Tech. Rep., Computer Science Department, University of Californiaat Los Angeles, 2001.Braginsky, D. Estrin, "*Rumour routing algorithm forsensor networks*", in: First ACM International Workshop on Wireless SensorNetworks and Applications, 2002.

[21] Ganesan, R. Govindan, S. Shenker, and D. Estrin, "*Highly-resilient, energy-efficient multipath routing in wireless sensor networks*", Mobile Computingand Communications Review, vol. 4, no. 5, October 2001.

[22] J. R. Douceur, "*The Sybil Attack*", in *1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, March 2002.

[23] Roosta, T., Shieh, S. and Sastry, S. "*Taxonomy of Security Attacks in SensorNetworks and Countermeasures*". Berkeley, California, University Press,2006.

[24] D. W. Carman, P. S. Krus, and B. J. Matt. "*Constraints and approaches fordistributed sensor network security*". Technical Report 00-010, NAI Labs,Network Associates, Inc., Glenwood, MD, 2000.

[25] L. Li, J. Halpern, Z. Haas, "*Gossip-based ad hoc routing*", in: IEEE Infocom 2002, 2002.

[26] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "*Energy-EfficientCommunication Protocol for Wireless Microsensor Networks*", Proceedings ofthe 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000, pp. 3005–3014.

[27] Y. C. Hu, A. Perrig, D.B. Johnson, "*Packet leashes: a defense againstwormhole attacks in wireless networks*", in: IEEE Infocom, 2003.

[28] D. J. Torrieri, "*Fundamental limitations on repeater jamming of frequency-hopping communications*," IEEE Journal on Selected Areas inCommunications, vol. 7, no. 4, pp. 569–575, May 1989.

[29] K. Tovmark, Chipcon Application Note AN014, "*Frequency Hopping Systems(Rev. 1.0)*", Chipcon AS, Mar. 2002.

