Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review on Security Issues and Attacks in Wireless Sensor Networks

Urvashi Sharma
Assistant Prof., Comp. Sc. Dept.
HMV College, Jalandhar
urvimishra@yahoo.com

Dr. Nischay Bahl
Associate Prof.& Head, Comp. Sc. Dept.
DAV College, Jalandhar
bahl_nischay@rediffmail.com

Abstract –Wireless sensor networks (WSNs) are networks of tiny sensors that are deployed randomly in various geographic conditions to collect information about the environment. The main function of sensor nodes is to gather the data from the environment and send the assembled data to the base station. Since these nodes are deployed in an unattended environment, they are prone to the security attacks. Security is the main threat for wireless sensor networks. In this paper, we have discussed various security attacks like DoS, Sybil attack, sinkhole, wormhole, Hello flood and selective forwarding attack. The attacks are categorized into two categories viz. goal oriented and layer oriented attacks. Goal oriented attacks are furtherclassified as active and passive attacks. Active attacks are more dangerous whereas passive attacks are passive in nature and do not modify any information. Furthermore, the mechanisms to prevent these attacks are also discussed.

Keywords: Wireless sensor networks, security attacks, active attacks, passive attacks.

1. Introduction

In case of WSNs, the communications between the sensor nodes is done using wireless transceivers. Now-a-days, wireless sensor networks are used in many applications which motivate the researchers to work on different issues of such networks but the issues related to security still need to be focussed. The major challenges for implementing any efficient security scheme depends on the various parameters like size of sensors, their processing power, and the types of tasks for which they are deployed. In this paper we have discussed various types of security attacks against WSNs. The security in any network encompasses the characteristics of integrity, privacy, authentication, anti-playback and non-repudiation.

2. Security Goals of WSN

The main security goals of Wireless Sensor networks are discussed as follow:

1. ***Availability of Data***: The availability of data is of utmost importance to maintain the network. The network should be available to move the packets and node should be able to fully utilize the resources.
2. ***Integrity of Data***: Integrity is the ability to ensure that the data has not been altered or tampered when it was on a network. Even the whole packet stream can be changed by adding additional unnecessary packets.
3. ***Authentication of Data***: The receiver needs to ensure that the data has originated from the correct source. The goal of authentication confirms the receiver that the data is sent from the authentic source/sender.
4. ***Confidentiality of Data***: The privacy of data is the most important goal in the network security. It is the ability to hide the message from the passive attacker. It is necessary to build a secured channel in wireless sensor networks because the nodes may carry highly sensitive data like key distribution. Moreover the identity of sensors and public keys should be encrypted to some extent so that they can be protected from traffic analysis attack.
5. ***Secure Localization***: The proper utilization of WSN depends upon the ability to automatically locate each sensor node in the network accurately because the sensors may get displaced while their deployment or after the deployment or after some critical displacement incident.
6. ***Self-Organization***: In WSN, there is no fixed infrastructure. Thus, each sensor node should be independent and shouldhave the capability of self-organizing and self-healing according to the various situations. They should adapt the topology and deployment strategy themselves.
7. ***Freshness of Data***: Freshness of data ensures that the data is novel and recent. This goal is important when the network design has the strategy of shared key that can be changed over time.
8. ***Synchronization of Time***: Some form of time synchronization is required in many applications of WSN like sensor networks performing collaborative tasks may require some form of group synchronization that can trackthe applications.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

3. WSN Attacks

The Wireless Sensor Network attacks can be viewed from different levels like attacks against security mechanisms and against basic mechanisms like routing. We have broadly categorized security attacks of WSN into two categories viz. Goal Oriented Attacks and Layer Oriented Attacks.

3.1 Goal Oriented Attacks

Goal Oriented Attacks are further divided into two categories – active and passive.

3.1.1 Active attacks: In active attacks, the attacker takes active measures to achieve control over the network. In this, the attacker modifies the messages or real data stream or generate the false data in communication. Such types of attacks include DOS attack, Replay attack, Selective forwarding, Worm hole, Sybil, Masquerade attack, node replication, rushing, sinkhole, and modification of messages.

3.1.2 Passive attacks: In passive attacks, the attacker monitors the traffic that is unencrypted and that is looking for sensitive information which can be used in other types of attacks. Such types of attacks include decrypting encrypted traffic, traffic analysis, capturing authentic information and monitoring communications. The passive attacks violate the goal of data confidentiality because it results in the disclosure of data files to an attacker without any knowledge or consent of user. These attacks are basically the pre arrangements before the actual active attacks. They just listen to the communication.

3.2 Layer Oriented Attacks

Wireless sensor networks have a layered architecture which makes these networks vulnerable to various types of attacks.

3.2.1 Physical layer attacks: Physical layer attacks of WSN are difficult to prevent because there is no physical control on each node. The most common physical attacks are jamming and tampering. In case of jamming, the attacker continuously sends high energy radio signals on a wireless medium in order to prevent the communication of nodes by blocking the wireless channel which can further lead to DoS (Denial of Service) attack at this layer.

3.2.2 Link Layer Attacks: The function of link layer is to provide link to the upper layers and to coordinate with neighbouring nodes to access shared wireless channels. Attackers at this layer can violate the predefined behaviour of the protocol intentionally. Link layer attacks include collision, exhaustion and unfairness. Collisions can be induced by disrupting a packet, exhausting energy by repeated retransmissions and causing unfairness by abusing a cooperative MAC layer priority scheme.

3.2.3 Network layer or Routing Attacks: The network layer of WSN is vulnerable to various kinds of attacks like spoofed, altered or replayed routing information, sinkhole, Sybil, selective forwarding, hello flood attacks, wormholes and acknowledgement spoofing. Capturing a single node is sufficient for attacker to get hold of whole network. The malicious nodes refuse to route certain packets and drops them. The routing information is altered or replayed to disrupt traffic in the network.

3.2.4 Transport Layer attacks: In case of transport layer attacks of WSN, the attacker makes new connections repeatedly until the resources reach the maximum limit or are exhausted. Such attacks include session hijacking, DoS, desynchronization, flooding and resource exhaustion.

Thus many types of attacks are possible in wireless sensor networks. Due to its broadcast nature and hostile environment, WSNs are more vulnerable to attacks. Active attacks are dangerous whereas passive attacks are passive in nature and do not modify the information. We have discussed some major attacks of WSN.

4. Common WSN Attacks

4.1 Denial of Service (DoS)

In case of denial of service attack, either there is unavailability of network or the data is altered by sending unnecessary extra packets before it is actually read by the legitimate user. This attack is produced by malicious action or unintentional failure of nodes.DoStry to exhaust the resources of the victim node and prevent legitimate users to access the resources to which they are entitled. Different kinds of DoS attacks can be done in different layers of wireless sensor networks like at physical layer there could be jamming or tampering; at data link layer, there could be collision, exhaustion and unfairness; and in network layer black holes, misdirection, homing and neglect and greed.

Mechanisms to prevent: The various mechanisms to prevent denial of service attacks include pushback, identification of traffic, network resources and strong authentication.

4.2 Sybil Attack

In Sybil attack of WSN, the node forges the identities of more than one node. It pretends to be more than one node by taking the identities of other nodes. The attacker is present in multiple locations by having multiple identities. The security, integrity of data and resource utilisation is degraded with this attack. Sybil attack is mainly performed for attacking fault tolerant systems like data aggregation, routing mechanism, fair resource allocation and distributed storage.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

Mechanisms to prevent:Almost all peer to peer networks are vulnerable to Sybil attack. In WSNs, this attack can be prevented using efficient protocols for gateways or base stations. Though detection of Sybil attack is not easy in wireless networks, but the radio resource testing can be used to detect its presence in the network.

4.3 Wormhole Attack

Wormhole attack establishes a link between malicious nodes. Thus this attack requires the presence of malicious nodes. In this, the attacker node records the data at one location and retransmits it to another location through wormhole link. Wormhole attack is the serious threat to WSNs because this attack can be done even at the initial phase when the sensor node is looking for neighbouring nodes to collect information. The routing race condition (a node taking action based on the first instance of the message and ignoring the subsequent instances) can be exploited by wormhole attacks even if the routing information is encrypted and is authenticated. These attacks replay packets between two distant nodes and convince them that they are neighbouring nodes. The detection of wormhole attack is quite difficult when combined with Sybil attack.

***Mechanism to prevent*:** The wormhole attack can be detected and prevented through packet leashes method by using geographic and temporal information.

4.4 Sinkhole Attack

This is also known as blackhole attack in which the attacker acts as a blackholethat attracts the traffic in the network. This malicious node listens to the route requests especially in case of flooding based protocol and tries to give wrong route by informing the requesting nodes about the shortest path. It makes the compromised node look attractive to lure all nearby traffic like replaying for extremely high quality route to base station. And once the node enters the sink, it can do anything with the packets passing through that node and can even affect the nodes far from base station.

Mechanism to Prevent:The sinkhole attacks can be prevented by using geographic routing protocols that construct a topology on demand using only localised information and interactions. Since the traffic will be naturally routed towards the base station, it will be difficult for the attacker to attract the nodes creating sinkhole.

4.5 Hello Flood Attacks

In Wireless sensor networks, hello flood attacks uses HELLO packets to convince the sensor nodes. The attacker transmits the HELLO packet to the node located in an isolated area using high radio transmission and processing power convincing it that it is a neighbour node and the node starts transmitting the information. In this way the victim node is spoofed by the attacker. The attacker does not require constructing legitimate traffic to use Hello flood attack; it just rebroadcasts messages with sufficient power for each and every node to receive the message in the network.

Mechanism to prevent: The HELLO flood attack can be detected by checking the average signal strength of all nodes in the network. If any node is having more signal strength than the average strength then it is considered as the attacker. This attack can be prevented if each node in the network authenticates its neighbouring nodes with the help of an identity verification protocol using trusted base stations.

4.6 Jamming Attack

The jamming attack is done by the transmission of radio signals. It is caused when the radio frequency of attacker node interferes with the radio frequency of other nodes. This attack also causes denial of service (DoS) attack when nodes in the network are not able to communicate because of jammers.

Mechanism to prevent: Jamming attack can be prevented by various techniques like spreading spectrum, priority messages, region mapping, and lowering duty cycles and by changing mode.

4.7 Selective Forwarding

In selective forwarding attack of WSN, the malicious nodes refuse to forward certain packets and they not only drop these packets but also ensure that they are not propagated further. In this the attacker node acts like a black hole preventing each packet it sees to forward further and the neighbouring nodes conclude that this particular node has failed and they find another route to send messages. The main risk of this attack is when the malicious node forwards packets selectively.

Mechanism to prevent: Such types of selective forwarding attacks can be prevented by using multipath routing in which the messages are routed over *n* routes having disjoint nodes that are protected from selective forwarding. Since it is difficult to create complete disjoint paths, multiple braided paths can also be used.

Table1: Summary of Security Attacks in WSN

Attack	Features	Effect	Security Scheme
Denial of Service (DoS)	Unavailability of network; Data is altered by sending unnecessary extra packets	Collision, Exhaustion, Unfairness; Misdirection, Homing	Pushback, Identification of traffic, Network resources, Strong authentication.
Sybil Attack	Forges the identities of more than one node	Generate false messages; Resource exhaustion	Radio resource testing; Authentication; Monitoring
Wormhole Attack	Attacker records the bits at one location and retransmits it to another location through wormhole link	Exploit routing race condition; Replay packets;	Packet leashes
Sinkhole /Blackhole	The attacker node look attractive to lure all nearby traffic	Attract almost all traffic; Gives false routing information	Geographic routing protocols
Hello Flood Attack	Transmits HELLO packets to convince the sensor nodes	The victim node is spoofed by the attacker; Resource exhaustion	Checking the average signal strength; Authentication
Jamming	The radio frequency of attacker node interferes with the radio frequency of other nodes	Causes DoS attacks; Collision of nodes; Nodes & resource exhaustion	Spreading spectrum; Priority messages; Region mapping; Lowering duty cycles; Changing mode

5. Summary of Countermeasures Strong authentication, pushback, identification of traffic, radio resource testing, monitoring, packet leashes, geographic routing protocols, spread spectrum, region mapping, lower duty cycles are the various mechanisms that can protect the wireless sensor networks against outsiders, false/fake information, spoofing, resource/node exhaustion and collisions.

6. Conclusion

The demand of wireless sensor networks is increasing at a fast pace with advancement in the technology. They are being used in diverse applications due to which the security and reliability of such networks is of utmost importance and has become the issue of main concern. In this paper, we have presented the review of security issues and attacks in wireless sensor networks. We have discussed various security attacks along with the mechanisms to prevent them. Since wireless networks are more vulnerable to attacks, thus, there is a strong need to design efficient and more robust security mechanisms to make wireless networks more secure so that the data in such networks should be handled with full confidentiality and high security.

7. References

[1] C. Karlof, D. Wagner, "Secure Routing in wireless sensor networks: attacks and countermeasures", Elsevier, Vol. 1, Issues 2-3, pp. 293-315

[2] A.S.K. Pathan, Hyung-Woo Lee; C.S. Hong, "Security in Wireless sensor networks: issues and challenges", Advanced Communication technology, IEEE Xplore

[3] S. Shanthi, E.G. Rajan, "Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks", Next Generation Computing Technologies (NGCT) 2016, 2nd International Conference, IEEE Xplore

[4]NischayBahl, Ajay K Sharma and Harsh K Verma."Impact of Physical Layer Jamming on Wireless Sensor Networks with Shadowing and Multicasting", In International Journal of Computer Network and Information Security (IJCNIS), Hong Kong, Vol. 7, pp. 51-56, June 2012. {ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online)}

[5] KehinaChelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering 2015, Vol 1, London, UK.

[6] K. Shabana, N. Fida, F. Khan, S.R. Jan, M.U.Rehman, "Security Issues and Attacks in Wireless Sensor networks", IJARCSEE, Vol. 5, Issue 7, July 2016.

[7] I.F. Akyildiz, "A Survey on Sensor Networks", IEEE Comm. Mag., Vol. 40, No. 8, pp. 102-114.

[8] NischayBahl, Ajay K Sharma and Harsh K Verma. "On Denial of Service Attacks for Wireless Sensor Networks", In International Journal of Computer Applications, Vol 43, No. 6, pp. 43-47, Published by Foundation of Computer Science, New York, USA, April 2012

[9] Culler, D.E, Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, nO. 6, pp. 30-33

[10] Liang, Zhengqiang, John Paul Walters, Vipin Chaudhary, and Weisong Shi. "Wireless Sensor Network Security : A Survey", Security in Distributed Grid Mobile and Pervasive Computing, 2007.

[11] Boudriga, . "Security of Mobile Sensor Networks", Security of Mobile Communications, 2009.

[12] Sadeghi, Mohammad; Khosravi, Farshad; Atefi, Kayvan and Barati, Mehdi. "Security Analysis of Routing Protocols in Wireless Sensor Networks", International Journal of Computer Science Issues (IJCSI), 2012.

[13] Karlof, C.. "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, 200309

[14] Singh, Virendra Pal. "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", International Journal of Computer Science Issues (IJCSI)/16940784, 20100501

[15] U.Sabeel, S. Maqbool, N. Chandra, "Categorized Security Threats in the Wireless Sensor networks: Countermeasures and Security management Schemes", IJCA, Vol. 64 – No. 16, February 2013

[16] E.Shi, A.Perrig, "Designing Secure Sensor Networks", Wireless Comm. Mag., Vol. 11, No. 6, pp. 38-43, Dec 2004.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)