Research Article

Open Access CrossMark

Intrusion threats and security solutions in wireless sensor networks

Abstract

Wireless Sensor networks (WSN) is the most emerging technology and it has great potential to be employed in some of the critical situations which includes battlefields and most emerging commercial applications. Some of them are surveillance of traffic, healthcare and smart homes and habitat monitoring and many other scenarios. WSNs are extremely vulnerable to different types of attacks internally and also mainly external attacks, because of various factors such as nodes with resource that are constrained and packages that are resistant to tamper. As a result, security is an important factor while the infrastructure and protocols of sensor networks are designed. Various types of security threats become possible using wireless communication technology. Sensor networks become vulnerable to a variety of potential attacks, while some of the environment remains unattended. In our comparative study, we discuss a wide variety of attacks that affects the performance of nodes in sensor network and also few mechanisms necessary for intrusion detection that gives right directions for further research work.

Keywords: wireless sensor network, security goals and issues, intruder attacks, intrusion detection mechanisms, challenges

Volume 4 Issue 1 - 2018

Gauri Kalnoor, Jayashree Agarkhed

Department of Computer Science, Engineering, PDA College of Engineering, India

Correspondence: Gauri Kalnoor, Department of Computer Science, Engineering, PDA College of Engineering, India, Email kalnoor.gauri@gmail.com

Received: December 27, 2017 | **Published:** February 09, 2018

Introduction

Intrusions are basically considered as unauthorized access to system resources where a network compromises integrity and availability. It also may compromise confidentiality maintained by the nodes in the network. The process of intrusion detection involves first analyze and then identify the intrusions that needs to safeguard and secure the system from malicious activities and harm from adversaries. Intrusion detection is a technology to provide security that helps to identify the adversary who is trying to break into the network or misuse a system without any authentication as a user. This helps the IDS to identify those who have legitimate access to the system and its resources but are misusing their privileges. The systems in WSN can be a host computer, a firewall, or network equipment. They may also be a router, a corporate network, or any of the system holding information that is being monitored by an intrusion detection system. In WSN, performance of individual nodes and collaboratively sharing information between the nodes to achieve the required task is a major challenge. Basically, Sensor nodes are application dependent. Examples of applications of wireless sensor networks that includes automation of a home, tracking of a vehicle,[1,2] monitoring of an environment, and detection of a target.[3,4]

Disasters

In most of the scenarios that includes disasters, and are induced by wide variety of terrorist activities. In such cases, it is required to protect the casualties' location from an unauthorized and confidential disclosure.

Safety of public

Most applications which involve chemical, other environmental threats or biological threats are monitored, it is most vital that the availability of the network is never threatened by any attacker. Attacks that cause false alarms may lead to responses that may panic the situation and make the environment worse by disregarding signals.

Home healthcare

In some of the applications where healthcare is most vital, privacy protection is very essential. Only users that are authorized should be allowed to monitor the network and able to query. WSNs,[5] which consists of hundreds or thousands of sensing devices of low-powered or less expensive with limited resources for computation and communication between nodes. Sensor network with its wireless capability provides an interface to the real world with their acquisition of data and processing capabilities. Thus, it is most essential to provide security, or at least to decide if security is required to be applied or not. Sensor nodes are usually deployed densely inside the object that is under observation, and all the measurements must be routed to the base station where only authorized and authenticated users can access them. Attacks of wide range[6,7] exists which manipulates the subsystem of routing and can take control over the routes that are manipulated, resulting in eavesdropped, spoofed, altered, or packets to discard.

Related work

Extensive literature survey has been done for handling attacks in security. Some of them are discussed as follows: Sourour et al.[8] examined and reduced False Positives (FPs) and False Negative (FNs) in Intrusion detection and prevention system with their environmental awareness. Wu and Banzhaf[9] proposed fuzzy inference system and collaborative intelligent IDS for reducing FPs. This reduction is through fuzzy alert correlation as in respectively.[10,11] They provided algorithms for different IDS for ex, artificial neural network, fuzzy sets, artificial immune system, swarm intelligence, soft computing and evolutionary computation. Zhang & Lee[12] proposed system where an IDS agent is installed on each host and implemented IDS architecture to run such an agent. Sterne et al.[13] proposed architecture with dynamic hierarchy in which the nodes are represented in clustering at different levels of hierarchy in hierarchical based IDS. The architecture was termed as co-operative IDS. Jayashree Agarkhed et al.[14] in explain different mechanisms for preventing attacks and providing security in WSN. Intrusion detection and prevention algorithms are discussed by the authors to improve the performance of the sensor network. Jayashree Agarkhed et al.[15] in have proposed pattern matching technique where the intruder is detected based on the data stored in the database of sensor nodes in the network. An algorithm is used to find the attacks and detect an intruder. The authors Jayashree Agarkhed & Gauri Kalnoor[16] discussed the Artificial Intelligence (AI) techniques with different mechanisms based on the type of attacks. The AI mechanisms discussed are DCA, Back Propagation, ANN and so on. These techniques of AI re used to detect an intruder and prevent the nodes from the adversaries. Based on these discussed results, security attacks and IDS are classified and discussed in the following sections.

Security attacks in wireless sensor networks

Wireless Sensor networks are vulnerable to security attacks due to the nature of broadcasting through the transmission medium. Also, wireless sensor networks have an additional vulnerability because of the nodes placement in a hostile or dangerous environment where they are not physically protected. Classifications of security attacks where they are classified as active attacks and passive attacks as shown in Figure 1.

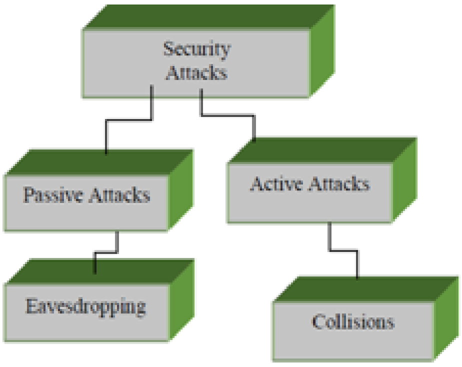

Figure 1 Types of Attacks.

Passive attacks

The listening of the communication channel by unauthorized attackers and the channel are monitored by the attackers are known as passive attacks.

Attacks against privacy: The main privacy problem is not that sensor networks enable the collection of information. Sensor networks may notice one of the privacy problems as they have large volumes of information easily available through remote access. Also adversaries are not required to be physically present to maintain such surveillance. In an anonymous manner, they can collect information at low-risk. The most common attacks[17] against sensor privacy are:

a. **Monitoring and Eavesdropping:** This is the most common attack which compromises with privacy. Here, the adversary may easily find out the contents of communication just by snooping to the data. Eavesdropping can be effective against protection of privacy, whenever, there is traffic of packet flow containing the control information about the configuration of sensor network. This traffic may contain most important detailed information through the location server.

b. **Analysis of traffic:** There is a high possibility of analyzing communication patterns, even whenever the messages transferred are encrypted. This can enable an adversary to cause malicious attack to the sensor network which can reveal some important information.

c. **Camouflage Adversaries:** An adversary can insert their node or they can make the nodes compromise which can be hidden in the sensor network. Later, these nodes can become a copy of a normal node to attract the packets, then misroute the packets for conducting the privacy analysis.

Active attacks

In active attacks, the unauthorized attackers first monitors the network, then listens to the channel and then tries to modify the data stream in the communication channel . The following attacks can be considered as active.

Routing attacks in sensor networks

Routing attacks are one which acts on the network layer. The following attacks are routing attacks which can happen while routing the messages

a. Routing information that is Spoofed, altered and replayed

I. As every node acts as a router, an unprotected ad hoc routing can be vulnerable to such type of attacks and can therefore directly affect routing information.

II. These attacks also create routing loops and extend service routes.

b. Selective forwarding

Whenever an attacker gathers information through nodes, such malicious node can selectively drop only some packets and this attack is effective in such situations. In sensor networks, nodes forward received messages. But if some of the nodes are compromised, they may start refusing to forward packets. In such case, the neighbor nodes start using another route.[18]

c. Sinkhole attack

A specific node can be attracted by traffic of packet flow. This kind of attack is called sinkhole attack. In this attack, the main goal of an adversary is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes.

d. Sybill attack

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

e. Wormholes attacks

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network.

Denial of service (DoS)

DoS attacks are produced by the unintentional failure of nodes or malicious action. An adversary attempts to subvert, disrupt, or destroy a network, and also tries to reduce the network's capability when providing a service. The mechanisms which can prevent DoS attacks are pushback, strong authentication and identification of traffic.[19]

a. Jamming: In WSN, the nodes utilize radio frequencies for data transmission because of usage of wireless channels by sensor networks for communications. In this attack, the frequencies for transmission of radio signals are same as compared to other signals in wireless network. The messages sent to or received from the jammed node is permantely or temporarily suspended.

b. Physical attacks: The nodes in WSN are prone to any other attacks or physical tampering. The adversary tries to extract the source code which can further provide information for the attacker to access the network and make required modifications. The nodes are further modified and replaced with malicious nodes.

Node subversion

Captured node reveals its information which includes disclosure of cryptographic keys and thus compromises the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

Node malfunction

A malfunctioning node creates or generates an inaccurate data. This can expose the data by compromising the integrity of sensor network, especially if the data is a data-aggregating node such as a cluster head.

Node outage

Node outage is the situation which occurs whenever a node functioning stops. If a cluster head stops functioning, the sensor network protocols become robust to mitigate the effects of node outages and then provide an alternate route.[20]

Intrusion detection solutions

IDS are passive in nature and can detect only the intruders and the attacks in the network. This type of system cannot provide any preventive action; instead they can only detect alarms or give alerts to the users of the system. Further, the preventive measures against attacks are taken care by the administrator. Furthermore, some IDS mechanisms are used based on the type of IDS used for detection. Discussed below are the IDS mechanisms provided which can be considered as preventive measures. In Signature based IDS, a decentralized rule based mechanism is used which has three main phases, namely, data acquisition, rule application, and intrusion detection. Signature-based IDSs are well suited for known intrusions; however they cannot detect new security attacks or those attacks having no predefined rules. The proposed mechanism is capable of detecting many routing attacks such as worm-hole, black-hole, selective-forwarding, and delay attacks. Different signature-based IDSs mechanisms are given in Table 1. In Anomaly-based IDS monitors network activities and classify them as either normal or malicious using heuristic approach. Different Anomaly-based IDSs mechanisms are given in Table 2. The solutions or countermeasures for attacks in WSN are discussed (Figure 2).

Jamming

This type of Denial of Service attack depends on the sensor nodes and resources used by the attacker. To avoid such attacks, the code spreading or spread spectrum is being used in mobile communications. The wide band of frequency cannot be jammed by the attacker and if the jamming attack is detected, then malicious node is put to sleep foe some duration of time.

Table 1 Signature Based IDS

IDS mechanisms	Attacks
Collaborative[20]	Black hole
Local and co-operative detection[20]	Sink hole
Genetic Programming[21]	DOS, unauthorized access
Soft computing]	Probing

Table 2 Anomaly Based IDS Mechanisms

IDS mechanisms	Attacks
Artificial neural network[22]	Time related changes
Set of techniques at OSI layer[22]	Masquerade, routing attacks
Cluster based[22]	Periodic route hole attack, sink hole attack
Support Vector[23]	Black hole attacks
Cross features[23]	Packet dropping attacks

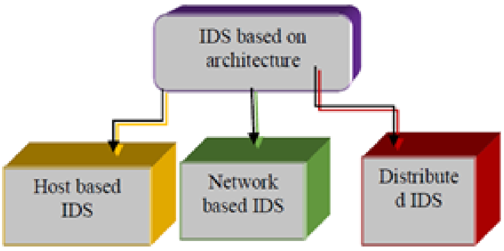

Figure 2 Types of IDS.

Physical attacks

The physical weakness of nodes in WSN can be exploited by the attacker and makes possible to access crucial data damaging or replicating the nodes. The nodes in such environment can be made temper-proof, such that the nodes are not compromised by the attacker. The other solution to avoid physical attacks is to hide the sensor nodes in which the critical data is stored. Statistical Model of Intrusion Detection Technique, Operational Model is one of the statistical models which describe the basic IDS framework as shown in Figure 3 [21].

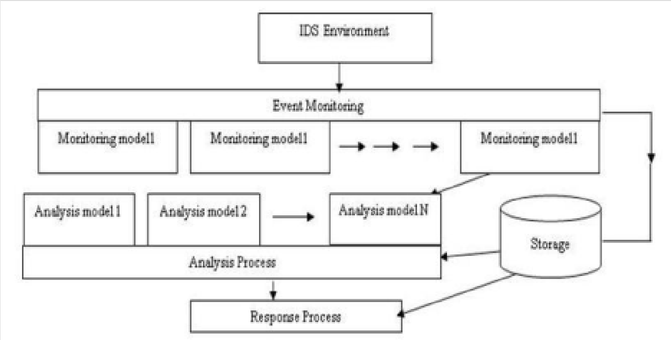

Figure 3 IDS framework.

Analysis

In Table 3, major types of security attacks in wireless sensor networks are listed.

Table 3 Security Attacks in Wsn

S.I	Attacks	Description
1	Jamming[22]	Jamming is a type of attack in which radio frequencies interference takes place to one the network nodes are being used.
2	Tampering[23]	Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node.
3	Collisions[23]	A collision occurs when two nodes attempt to transmit on the same frequency simultaneously.
4	Exhaustion[24]	Repeated collisions can also be used by an attacker to cause resource exhaustion

Detection Rate (DR) of an Intruder attack

DR is the rate of accurately detected records that are observed as malicious attacks.

$$D_R = \frac{TP}{TP+TN} \quad (1)$$

Where,

a. TP is rate of True Positive detection: The no. of malicious records that are detected correctly based on intrusion classification that has been done.

b. FN is rate of False Negative detection: The no. of records that are detected incorrectly that are classified as legitimate activities.

False positive rate (FPR)

It is the rate of False Positive, the no. of records that are incorrectly classified as attacks. No. of false positive rate in IDS is evaluated using equation 2.

$$FP_R = \frac{FP}{TN+FP} \quad (2)$$

Where,

TN is the rate of True Negative, the no. of legitimate records that are incorrectly classified as intrusion. FP is the rate of false positive. It evaluates the no. of records that are detected incorrectly.

The equations used to compute detection rate and false positive rate are shown graphically in the Figure 4. The rate of detection is increased whenever the true positive rate is increased. The false positive rate depends on true positive rate.

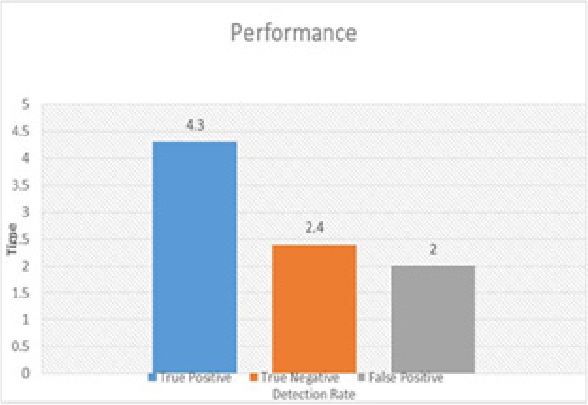

Figure 4 Graphical Representation.

Conclusion

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks. While designing a security mechanism, we must consider the limited resources of WSNs. Anomaly-based IDSs are light weight in nature; however they create more false alarms. Signature based IDS are suitable for relatively large sized IDS. We present an effective intrusion detection mechanisms .WSN are vulnerable to several attacks as they are deployed in an open and unprotected environment. We also describe the major security threats that can take place in WSN with different protective measures and performance metrics.

Acknowledgments

None.

Conflicts of interest

None.

References

1. Akyildiz IF, W Su, Sankarasubramaniam Y, et al. Wireless Sensor Networks: A Survey. *Computer Networks*. 2002;38(4):393–422.

2. da Silva A, Marcelo HT, Bruno PS, et al. Decentralized Intrusion Detection in Wireless Sensor Networks. *Proc 1st ACM Int'l Wksp QoS & Sec in Wireless and Mobile Networks*. 2005. p. 16–23.

3. Djenouri D, Khelladi L, Badache A. A Survey of Security Issues in Mobile Ad Hoc and Sensor Net– works. *IEEE Commun Surveys & Tutorials*. 2005;7(4):2–28.

4. Shi E, Perrig A. Designing Secure Sensor Net–works. *IEEE Wireless Communications*. 2004;11(6):38–43.

5. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. In: *Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Application*. 2003.

6. Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: analysis & defenses. *Proceedings of 3rd IEEE International Workshop on Information Processing in Sensor Networks (IPSN'04)*. 2004.

7. Undercoffer J, Avancha S, Joshi A, et al. Security for sensor networks. In Proceedings of the CADIP Research Symposium. 2002.

8. Chris Karlof, David Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *AdHoc Networks (elsevier)*. 2003. p: 299–302.

9. Pathan ASK, Hyung–Woo Lee, Choong Seon Hong. Security in wireless sensor networks: issues and challenges. *Advanced Communication Technology (ICACT)*. 2006. p. 1–6.

10. Huang Zhilong. Research on computer network security analysis model. *Research on computer network security analysis model*. 2014.

11. Zhang Tao, Hu Mingzeng, Yun Xiaochun, et al. Research on computer network security analysis model. *Journal of communications*. 2005.

12. Zhang Baoshi. Research on computer network security analysis model. *Electronic technology and software engineering*. 2014.

13. Jayashree Agarkhed, Gauri Kalnoor. Preventing Attacks for Intrusion Detection and Prevention in Wireless Sensor Network. *Wireless Communications, Signal Processing and Networking*. 2016. p. 1062–1067.

14. Jayashree Agarkhed, Gauri Kalnoor. Pattern Matching Intrusion Detection Technique in Wireless Sensor Network. *Advances in Electrical, Electronics, Information, Communication and Bioinformatics*. 2016. p. 724–728.

15. Jayashree Agarkhed, Gauri Kalnoor. Artificial Intelligence based Technique for Intrusion Detection in Wireless Sensor Network. *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. 2017. p. 835–845.

16. Hong Yaling. On modeling of computer network security. *Computer CD Software and Applications*. 2013.

17. Xv Liuwei. Modeling of computer network security. *Computer CD Software and Applications*. 2013.

18. Liu Y, Comaniciu C, Man H. Modeling Mis behaviour in Ad Hoc Networks: a Game Theoretic Approach for Intrusion Detection. *International Journal of Security and Networks*. 2006;1(3/4):243–254.

19. Khan S, KK Loo, Din ZU. Cross layer design for routing and security in multi–hop wireless networks. *International Journal of Information Assurance and Security*. 2009;4(2):170–173.

20. Byunggil Lee, Seungjo Bae, Dong Won Han. Design of network management platform and security frame work for WSN. *IEEE International conference on signal image technology and internet based system*. 2008.

21. Qi Wang, Shu Wang. Applying an Intrusion detection algorithm to wireless sensor networks. *Second international workshop on Knowledge Discovery and Data Mining*. 2009.

22. Brutch P, C Ko. Challenges in intrusion detection for wireless ad–hoc networks. *In 2003 Symposium on Applications and the Internet Workshops*. 2003.

23. Jyothsna V, Rama Prasad VV. A Review of Anomaly Based Intrusion Detection Systems. *International Journal of Computer Applications*. 2001;28(7):1–10.