International Journal of Engineering & Technology, 7 (2.32) (2018) 136-138

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Attacks and Challenges of Wireless Sensor Network's - a Review

Riaz Shaik[1] ,Shaik Shakeel Ahamad[2]

Department Of CSE, Koneru Lakshmaiah Education Foundation Vaddeswaram, Guntur District, Andhra Pradesh, India[1,2]
CCIS,Majmaah University,Al-Majmaah,Riyadh,Kingdom of Saudi Arabia[2]
**Corresponding author E-mail: sheikriaz@gmail.com*

Abstract

Wireless sensor networks are becoming part of many of the research areas to address different issues related to technological and societal. So, The developments in wireless communication technology have made the deployment of wireless sensor nodes connected through wireless medium, known as wireless sensor networks. Wireless sensor networks have numerous applications in many fields like military , environmental monitoring , health , industry etc.. wireless sensor networks have more benefits over Wired networks .Though there are several advantages of wireless networks, they are prone to security issues. . Security became a major concern for wireless sensor networks because of the wider application. So ,this paper addresses the critical security issues of wireless sensor networks that may encounter in the different layers of the communication protocols like OSI.This paper presents a detailed review on the security issues and its challenges of the wireless sensor networks.

Keywords: *Wireless Sensor Network(WSN),Security, Threat and Attack.*

1. Introduction

Wireless sensor network is a composition of large number of sensors with features like low cost, power ,rapid deployment , self organization capability ,cooperative data processing and also they possess advantages with various applications in real time. Wired local area networks suffers from various limitations such as, deployment of wires in historic buildings is difficult, it will be very expensive and consumes more time to implement such networks in new infrastructure. Further wired networks does not provide flexibility and scalability Wireless networking has overcome the challenges of the wired network and also provides the ease of deployment. In certain applications wireless sensor networks are deployed in important and tactical scenarios that there is need to secure the same because of their limited resources ,unreliable communication .The open and unattended nature of the wireless sensor networks makes the network susceptible and poses threat of an adversary. This allows the users to move around within a local area by remaining users connected to the network.

1.1 Security Requirements:

WSN communication method is a multi-hop system administration where the communication pattern could be one to many, many to one and it can also perform unicast transmission or broadcast data transmission among the other nodes [1] [5]. The prime objective behind the WSN communication is to ensure secure data transmission and to make WSN a tamper proof network. So, to meet up to the criteria they have the general security goals as given under

Confidentiality: Protecting disclosure of communicated data from the unauthorized user.

Integrity: To protect message from unapproved changes of fabrication by an attacker.

Authentication: Authenticating the source of communication and the identity of communicating user/node.

Access Control: To prevent unapproved access.

Availability: to ensure that the desired service is always available to the authorized entity.

Data Freshness: to make sure that the data is recent, correct and not disclosed to the unauthorized user.

Scalability : It should be able to scale it up when required meaning it should be able to manage enormous number of nodes.

1.2 Constraints:

WSN is a remote sensor network which has many variables as compared to other similar networks. These obstacles and restrictions make it complex to implement security techniques in WSN's. Therefore, to develop efficient security mechanisms it is necessary to understand the following constraints to make a wireless sensor networks a constraint-free/efficient network.

Limited Resources: WSN comes with the very limited resources like the battery power, processing speed, memory and ability to propagate the data. Inspire of all these short falls, WSN can be made very effective for secure data transmissions.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Unreliable Communication: The communication between the WSN nodes should be made reliable to overcome the security flaws of unreliable communication.

Unattended Operation: The WSN nodes might be left unattended for longer periods of time basing the application of specific WSN which makes the WSNs prone to various types of attacks.

Due to these obstacles, the nodes and the network in turn may experience many short falls which further effect their overall functioning.

1.3 Security Challenges:

WSNs undergo many restrictions like little computation capability, limited memory, less energy resources, tendency to physical capture, and deficient of infrastructure, which makes them open to many security attacks or challenges and make security techniques inevitable and desirable with some security solutions. All the security mechanisms provide security to WSNs to a certain level only [1] [5]. There are still remaining many issues and challenges which need to be addressed and resolved. It has been deducted and there are still many issues remaining which need to be addressed to make WSNs secure and efficient like:

- Public key cryptographic techniques require excessive computations and capacity in resource constrained WSN.
- Most of the security procedures are particular to certain attack which should be adaptable. Key distribution problem need to be addressed to achieve encrypted and secure communication.
- Key refreshing is an open issue.
- The computational overhead should be lessened in resource constrained condition of WSN.
- The adaptability (scalability) is likewise wanted to make the WSNs adaptable for node expansion and deletion.

2. Threats and Attacks in WSN:

Due to the adhoc operation, Unreliable transmission medium, limited resources and with unattended environment the WSNs become vulnerable to adversaries and attacks. We have categorized these attacks in to three based on the strength of the attacker, information in transit, host and network based.

2.1 Opponents's Capability based attacks:

The adversary, who can eavesdrop the wireless medium easily, is called a "passive attacker". And the adversary who can replay or inject fabricated messages in the original data stream. Called as "Active attacker". there are other security issues also like DoS, physical damage, privacy. Outside attacks are the attacks caused by the other sensors which are part of other WSNs. whereas the insider attacks take place when genuine sensors of a WSN act in an unplanned or the way not permitted.

2.2 Host Based Attacks:

These are classified as:
3.1) Client Compromise: In this attack, the client machine gets compromised by making clients to reveal the significant data like security passwords or keys.

3.2) Hardware Compromise: In this, the attacker tampers the system hardware/hardware components of the nodes so that he can take out or remove the code to compromise the system in total.

2.3 Network Based Attacks:

The attacks discussed here comes under the layer specific attacks, detailed review on the different attacks covering the layers of Open System Interconnection (OSI) protocol have been presented here under.

i. Physical Layer:

(a) **Jamming:** A sort of DoS assaults where the attacker tries to intrude on the administrations of the system by sharing a high energy motion towards the goal is known as Jamming. These attacks can be characterized in four sorts

(1) **Constant jamming** which undermines the package of the message as they sent.

(2) **Deceptive jamming** this type of jamming is a consistent stream of bytes which was sent into the network which is like the certified activity.

(3) **Random jamming:** it exchanges as it likes amongst jamming and inactive state to prevent loss of energy.

(4) **Reactive jamming:** it communicates a jam signal at whatever point in which it will occur transmission.

(b) **Tampering:** An opponent can get to a node physically and pull out stored sensitive information like encrypting/decrypting keys.

(c) **Radio interference:** it will occur where the challenger will either creates a great deal of physical inconsistency.

ii. Data Link Layer:

(a) **Collision:** These circumstances are made when two nodes attempt to convey on similar frequency in the meantime. An adjustment in the information segment will probably happen on packets crash, which may cause an error in checksum at receiver side. This packet with mistakes will be dismissed because of checksum mismatch.

(b) **Continuation Channel Access:** A malicious sensor nodes aggravates the MAC protocol, by continually managing the channel and thus remaining system at starvation of sensors for utilizing channels.

(c) **Unfairness:** These attacks causes duplicate exhaustion, attacks with MAC layer in view of crashes or an unapproved use of need techniques for agreeable MAC layer. It is a kind of unjust DOS assault and results into insignificantly debased execution.

(d) **Sybil Attacks:** the Sybil attack is based on the identification of MAC address. When there is evidence that the node is using forged identity then it is considered to be the node involved in Sybil attack. If not the node is considered to be a legitimate node and the communication is allowed [6]- [10].

iii. Network Layer:

(a) **Hello Flood:** As shown in Figure 1 (b), it is an attack in which a node floods network with message claiming that the path through it is a high quality route. Believing it, every node tries to send their packets thorough this node. In the process, some nodes might send packets with destination are not in the reach of attacker node as the attacker node convinces that all nodes are its neighbours. Moreover the traffic generated by the attacker node is not genuine [6].

(b**) Black Hole Attack:** A black hole attack is characterized by a node dropping all packets that come in its way. Such node acts like a black hole. The attack will have much more impact on the network when the black hole node is the connecting node of two

connecting components of the network [2]. This attack is illustrated in Figure 1 (a).

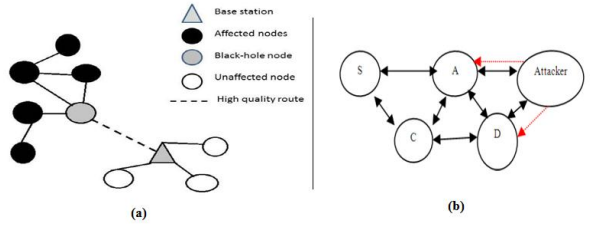


Figure 1 – Shows black hole attack (a) [3] and flooding attack (b) [4]

(c) **Rushing Attack:** Generally, before sending data to destination a node establishes route the destination. A RREQ message is broadcasted by sender node to its neighbourhood. Valid routes come back to the source with RREP with correct route information. However, some protocols follow mechanism known as duplicate suppression which is exploited by adversaries to launch rushing attack. Rushing attack is an attack in which an attacker forwards with RREP with malicious intentions on behalf of a legitimate node without following proper procedure. The attacker node filters packets before sending to correct node. Therefore it appears from outside that everything is done as per protocol. However, the attacker node really caused delay in data transmission [2]. This attack is illustrated in Figure 2 (a).

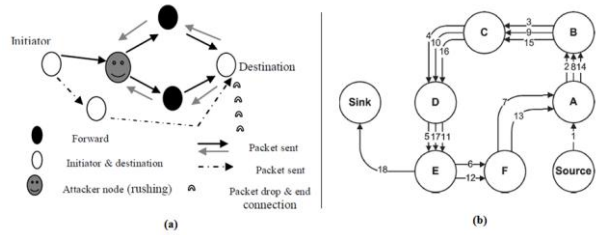


Figure 2 – Rushing attack (a) [5] and carousel attack (b)

(d) **Node Capture:** This will happen when the network nodes are caught from the attacker. Normal perception and thought compresses that the catch of one node is sufficient for a attacker to attack the entire network.

(e) **Wormhole Attack**: It is evident that the attack is detected based on the time flag set in the communication process. If the REQ reaches destination in the given time, it needs to be considered as legitimate else it has to be suspected and communication to such node has to be stopped [2] [3].

(f) **Spoofed Routing Information:** These types of attacks happens when an attacker farces, changes, or replay directing data to scatter the system movement.

IV.**Transport Layer:**

(a) **Flooding:** In this type of attack, the opponent sends the request messages repeatedly till the resources for the actual connection establishments are drained out, wasting the resources in a resource constrained network should be avoided by all means by making the network attack resistant.

V. **Application Layer:**

(a) **Path based DOS attack:** It manages the infusion of the false or replayed packets at leaf nodes of the system. This attack results into the starving.

(b) **Overwhelm Attack:** The opponent tries to generate huge amounts of traffic unnecessarily in to the network so that the network gets congested , resulting into the larger delays to the actual traffic and loss of the sensor nodes energy ,eventually resulting them to be powerless.This attack consumes the band width of the network as well.

3. Conclusion

This paper presents a detailed survey on the security attacks of wireless sensor networks. Wireless networks are increasingly being used in commercial applications, public and private sectors. Security is an significant feature in Wireless Networks for secured transmission of the data but to ensure the same data should be protected from the attacks afore mentioned. The paper discusses different categorization of attacks and it also discusses the vulnerabilities in Wireless devices. We found by the detailed study that how ever strong the security is but always there is a scope for the exploitation , so by knowing at least where the opponents can exactly exploit the network we can prevent the attacks to the extent possible and protect the data and networks.

4. References

[1] Riaz Shaik; Shaik Shakeel Ahamad, Key Management Schemes of Wireless Sensor Networks -A Survey. Fronteiras: Journal of Social, Technological and Environmental Science •v.6, n.2, may-august. 2017.

[2] Riaz Shaik, Shaik Shakeel Ahamad, Enhanced Attack Resistant Agent Based Dynamic Key Management in Dynamic Wireless Sensor Networks. *International Journal of Civil Engineering and Technology*, 8(12), 2017, pp. 69–76.

[3] Riaz Shaik, Shaik Shakeel Ahamad, Attack Resistant Agent Based Dynamic Key Management in Dynamic Wireless Sensor Networks. *International Journal of Engineering and Technology,Accepted.*.

[4] Riaz Shaik,Shaik Shakeel ahamad (2017). An Agent-Based Hybrid Approach for Dynamic Key Management System in Dynamic Wireless Sensor Network.(JARDCS) journal of advanced research in dynamical and control systems-vol-9,issue-2-OCT-2017.

[5] Alla Chandra Sekhar Reddy, Riaz Shaik ,Effective Detection of Denial of Service (Dos) Attacks by Using Snort Rules Architecture , International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 19 (2014) pp. 1635-1646.

[6] Riaz Shaik, Lokesh Kanagala, Hema Gopinath Sukavasi , Sufficient Authentication for Energy Consumption in Wireless Sensor Networks, . International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 2, April 2016, pp. 735~742.

[7] Kuan Zhang,Student Member, IEEE, Xiaohui Liang,Member, IEEE,Rongxing Lu,Member, IEEE, and Xuemin Shen,Fellow IEEE," Sybil Attacks and Their Defenses in the Internet of Things", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 5, OCTOBER 2014

[8] Yan Sun, Lihua Yin, Wenmao Liu," Defending sybil attacks in mobile social networks", Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on, 08 July 2014

[9] Deepti Sharma and Dr. Sanjay Thakur, "SybilDecline: A Survey on Novel Trusted Identity and Threshold Based Path Rank for Sybil Attack Identification in Social Network",International Journal of advanced research in Computer Science and engineering, Vol. 4, Issue 6, No.June 2014.

[10] Wei Chang, Jie Wu, Chiu C. Tan, and Feng Li," Sybil Defenses in Mobile Social Networks", IEEE GLOBECOM, December, 2013