International Journal of Engineering, Applied and Management Sciences Paradigms
Volume 51, Issue 01, Quarter 04 (2017)
An Indexed and Referred Journal
ISSN (Online): 2320-6608
www.ijeam.com

Review on Study of Active Routing Attacks in Wireless Sensor Network

Poonam[1] and Puneet Garg[2]

**[1]Research scholar, Department of Computer Science and Engineering,
UIET, M.D. University, Rohtak, Haryana (India)
[2]Assistant Professor, GITAM, Kablana, Jhajjar, Haryana (India)**

Publishing Date: December 26, 2017

Abstract

In the course of recent decades Wireless Sensor Networks (WSNs) and their applications have been the theme of many investigations. WSN is a network in charge of gathering, preparing and circulating wireless data to the planned database stockpiling focus. Since these sensors are typically introduced at remote destinations, notwithstanding the current advances in the WSN innovation, its applications still face noteworthy difficulties. Wireless Sensor Networks (WSNs) are utilized as a part of an assortment of fields including military, agriculture, health and manufacturing. Out of these, network security dangers, network engineering, data accumulation, arrangement and network scope ascend as the significant concerns. Sensor networks are connecting with extremely delicate data and conveyed in threatening unattended conditions, where the security issues ought to be concentrated to accomplish their potential. This review paper lights a light on security of WSN and diverse attacks in it.

Keywords: *Wireless sensor networks, Network security, routing protocols, security attacks.*

1. Introduction

WSN is a substantive piece of the network, flew out with a sprinkle application, for example, medical applications, environmental pollution detection, agribusiness and so on., Even there is a nearness of repressions over qualities like battery power, low energy consumption which requires a considerable measure of care to keep off network's life time diminishment benefitting from security issues in remote sensor networks. To show signs of improvement of execution in WSN[1], it is an order thing to give a decent way. Here this paper heels on flooding attack which would have done by developing a way , since the remote sensor networks has contributed on different sorts of attack[2].

2. WSN Security Goals

Security goals guarantee the Confidentiality, Integrity and Authenticity of data.

i) Confidentiality: Confidentiality means bounding the data access and revealing only to authorize users and preventing from unauthorized folks. The message should be known only to sender and receiver it will be garbage to any other. This can be achieved by using the concept of cryptography[3].

ii) Integrity: Message that is sent by sender receiver by receiver in exact form that is sent by sender. Message should not be changer in between sender and receiver. Integrity actually means the concept of validity. This can be achieved by the concept of message digest[3].

iii) Authentication: There should be some mechanism that after receiving the message by receiver he should be able to identify the correct sender. This sis achieved by the concept of message authentication code.

iv) Non-repudiation: If sender has transmitted the message that after some time sender cannot deny that message is not sent by him. This is achieved by the concept of digital signature.

v) Availability: Availability refers to the availability of data resources. Data should be available always to the legal users throughout the network even if there occurs internal or external failures, faults, errors or attacks.

3. Attacks in Wireless Sensor Network

Attacks on WSN is can be classified into active attacks and passive attacks [4].

The passive attack is imperfect to listening and analyzes exchanged traffic. This type of attacks is easier to realize (it is enough to have the adequate receiver), and it is difficult to detect. Since, the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network (cluster head node), by analyzing routing information, to prepare an active attack.

In the active attacks, an attacker tries to remove or modify the messages transmitted on the network. He can also inject his own traffic or replay of old messages to disturb the operation of the network or to cause a denial of service.

Types of active routing attacks

i) **Selective Forwarding Attack:** The Selective Forwarding attack, an uncommon occurrence of foreswearing of administration attack, where the bargained node decreases to forward particular messages and just drops them ensuring they are not caused any further. Acquainting excess with the network as multi-path routing will decrease the exertion of selective forwarding attack in the WSN[5].

ii) **Sink Hole Attack:** Sinkhole attack is a kind of attack was traded off node tries to draw in network activity by publicize its phony directing refresh. One of the effects of sinkhole attack is that, it can be utilized to dispatch different attacks like selective forwarding attack, acknowledge spoofing attack and drops or changed directing data[6].

iii) **Wormhole Attack:** In the wormhole attack, a foe tunnels messages over a low dormancy connect which have been gotten in one a player in the network and has back them in an alternate impact. Wormhole attack is extremely hard to recognize on the grounds that it utilizes out-of-bound channel to course bundles. A foe records bundles or bits from whatever area in the work that can puncture them to another area and passes on them into the network[5].

iv) **Hello flood attack:** A flood attack is the route toward sending countless to "flood" the mempool, filling new pieces to the most extraordinary size of 1MB, and as needs be putting off various trades. Despite whether an attacker needs to waste money, trades are furthermore organized when since the coins were last spent, so attacks spending comparative coins again and again are less convincing. This attack will builds the deferral since the messages are should be routed mulit-bounce to their parent nodes. The evasion of this attack can undoubtedly be dodged by confirming the bi-directionality of a link through personality check protocol before making a move in view of the data got over the link[6].

v) **Sybil attack:** Node imitates itself and includes their reality in the distinctive areas. At the end of the day it is characterized as a "vindictive gadget misguidedly going up against various identifiers". The presence of this attack is at physical layer, data link layer and network layer. The answer for Sybil attack is to confirm the personalities of partaking nodes by having every node share an extraordinary key with the base station. Two neighboring nodes at that point speak with each other utilizing a mutual key to encrypt and check the link between them.

vi) **Spoofing attack:** A parodying attack is the point at which a malevolent gathering mimics another gadget or client on a network with a specific end goal to dispatch attacks against network has, take data, spread malware or sidestep get to controls. There are a few unique sorts of ridiculing attacks that pernicious gatherings can use to achieve this.

Types of Spoofing Attacks

ARP Spoofing Attack: This type of spoofing attack occurs when a malicious attacker links the hacker's MAC address with the IP address of a company's network. This allows the attacker to intercept data intended for the company computer. ARP spoofing attacks can lead to data theft and deletion, compromised accounts and other malicious

consequences. ARP can also be used for DoS, hijacking and other types of attacks.

DNS Spoofing Attack: For a DNS spoofing attack to be successful, a malicious attacker reroutes the DNS translation so that it points to a different server which is typically infected with malware and can be used to help spread viruses and worms. The DNS server spoofing attack is also sometimes referred to as DNS cache poisoning, due to the lasting effect when a server caches the malicious DNS responses and serving them up each time the same request is sent to that server.

IP Spoofing Attack: The most commonly-used spoofing attack is the IP spoofing attack. This type of spoofing attack is successful when a malicious attacker copies a legitimate IP address in order to send out IP packets using a trusted IP address. Replicating the IP address forces systems to believe the source is trustworthy, opening any victims up to different types of attacks using the 'trusted' IP packets.

4. Related Work

According to Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong[7] in their paper "Security in Wireless Sensor Networks: Issues and Challenges" discussed the security related issues and challenges in wireless sensor networks. They identify the security threats, review proposed security mechanisms for wireless sensor networks. They also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

C.Dhivya Devi , B.Santhi [5] in their paper" Study on Security Protocols in Wireless Sensor Networks" discussed This paper lights a torch on security of WSN and different attacks in it and mainly focuses on the effect of Denial of Service (DoS) attacks, which is caused by a flood attack where there is a composition of many illegitimate nodes sits inside the network can produce traffic and dampen the security of WSN. On behalf of the security aspects, this paper also has concentrating on the anatomy of security protocols.

Mohd Fauzi Othman, Khairunnisa Shazali[8] discussed about wireless sensor network in the paper "Wireless Sensor Network Applications: A Study in Environment Monitoring System". They discussed and review wireless sensor network applications for environmental monitoring. In order to implement a good monitoring system, there are several requirements to be followed. From the studies, it has been proved to be an alternative way to replace the conventional method that uses men force to monitor the environment. It is also proven that these approaches can improve the system performance, provide a convenient and efficient method and can also fulfill functional requirements.

Yasaroglu Pinar, Abduljabbar Zuhair, Alotaibi Hamad, Akcam Resit, Kadavarthi Shiva, Abuzaghleh Omar[9] discussed about wsn in their work in paper "Wireless Sensor Networks (WSNs)". This study aimed at introducing and analyzing various shortcomings and challenges of WSNs such as, WSN security threats, WSN data collection processes, WSN deployment techniques, the WSN coverage problem and the WSN network architecture. Regardless of the challenge, power consumption is found as a common problem in WSN applications. Therefore, the objective of this research was to obtain a solution that would conserve the battery power of the network while preserving the overall efficiency.

Muhammad Umar Aftab, Omair Ashraf, Muhammad Irfan , Muhammad Majid, Amna Nisar, Muhammad Asif Habib[10] in their paper" A Review Study of Wireless Sensor Networks and Its Security" discussed about wsn and the possible solutions for tackling the listed problems and solution of many other problems. This paper will deliver the knowledge about the WSN and types with literature review so that a person can get more knowledge about this emerging field.

5. Conclusion

Security in WSN is imperative to keep up the great execution of the whole wireless network. Numerous authors study work has been considered. This examination went for presenting and different inadequacies and difficulties of WSNs, for example, WSN security threats, WSN security attacks. The survey work is done to consider the different

dynamic directing attacks in wireless sensor networks. The vast majority of the attacks against security in wireless sensor networks are caused by the addition of false data by the compromised nodes inside the network.

References

[1] Dimple Juneja, Atul Sharma, and A.K. Sharma," Wireless Sensor Network Security Research and Challenges: A Backdrop", HPAGC, CCIS 169, pp. 406–416, 2011.
[2] Saurabh Singh, Dr. Harsh Kumar Verma,"Security for Wireless Sensor Network ", International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 6 pp. 2303-2399 June 2011.
[3] Hemanta Kumar, Kalita and Avijit Kar," Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, pp. 1-10, December 2009.
[4] C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures". Proceedings of The First IEEE International Workshop on Sensor Networks, Protocols and Applications, pp. 113-127, May 2003.
[5] C. Dhivya Devi, B.Santhi" Study on Security Protocols in Wireless Sensor Networks", International Journal of Engineering and Technology (IJET) ISSN: 0975-4024 Vol 5 No 1 Feb-Mar 2013.
[6] Zdravko Karakehayov "Security - Lifetime Tradeoffs for Wireless Sensor Networks" , 1-4244-0826-1/07/$20.00 © 2007 IEEE.
[7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges" ISBN 89-5519-129-4 - Feb. 20-22, 2006 ICACT2006.
[8] Mohd Fauzi Othman, Khairunnisa Shazali, "Wireless Sensor Network Applications: A Study in Environment Monitoring System", International Symposium on Robotics and Intelligent S ensors 2012 (IR IS 2012) Procedia Engineering 41 (2012) 1204 – 1210.
[9] Yasaroglu Pinar, Abduljabbar Zuhair, Alotaibi Hamad, Akcam Resit, Kadavarthi Shiva, Abuzaghleh Omar, "Wireless Sensor Networks (WSNs).
[10] Amna Nisar, Muhammad Asif Habib," A Review Study of Wireless Sensor Networks and Its Security", Communications and Network, 2015, 7, 172-179 Published Online November 2015 in SciRes. http://www.scirp.org/journal/cn and http://dx.doi.org/10.4236/cn.2015.74016.