A Review on Study & Analysis of WSN, Attacks & its Applications

Yogesh Hassani[1], Prof. Rakesh Shivhare[2]

1. M.Tech. Scholar, Radharaman Engineering College, Bhopal (MP)
2. Assistant Professor, Radharaman Engineering College, Bhopal (MP)

ABSTRACT

A collection of various sensor nodes is called as Wireless sensor network (WSN). These sensor nodes sense data from the surrounding and send it to its destination following a proper route. A sensor network has various applications to monitor physical phenomenon in military, agriculture and medical applications where it can be used to make human life better in many ways. There are many issues in WSN like security, energy efficiency and QoS etc. which needs attention of today's research. There are several security attacks which affect the process of data dissemination. These security attacks spawn at various layers of Internet model which hampers the security of the network. In this paper, a comparative study of some detection and prevention methods of wormhole attack is presented. The various wormhole attack models and different modes of wormhole attack are also discussed in the paper. A wireless sensor network consists of sensors having autonomous wireless communication with the ability to sense their surrounding conditions and an ability to connect to the Internet through a base station. In most cases, sensors are spatially distributed and, hence, must have a low cost; for this reason, they have limited batteries, computational ability, and memory size. Sensors' restrained ability to implement common security measures makes them vulnerable to various types of attacks. Moreover, their applications are sensitive to delay or packets corruption, e.g., forest fire detection, disaster relief operations, and lots of other applications. Therefore, improving security is compulsory. There are various types of attacks targeting different network layers. One type is a wormhole attack that is a harmful and easily deployed attack that targets the routing layer.

Key words: Wireless Network, Sensor Network, Wormhole Attack, Network Venerability, Security, AODV

1. INTRODUCTION

A Network is use to connect the devices for sending and receiving the data. To install any network there are three basic needs. These are 1) Computers 2) Connecting Media and 3) Protocol. As the network is a way to provide communication between two or more than two devices [1]. Whether, wireless network uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network. Using this approach, the wireless LAN can create to establish it in a required area [2].

Above figure shows the simple scenario in which there are many nodes which are connected with the wireless medium. This wireless medium may created by the centralized device like router, switch or a computer.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance, a group of industry-set, promoting inter operability between 802.11 devices. 802.11 provide two ways to configure an ad hoc and wireless network infrastructure. Previously, there was a discussion of the wireless network may refer to a network, wherein all devices communicate without using a wired connection. Wireless networks are usually applied with some information about the remote transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network [1, 3].

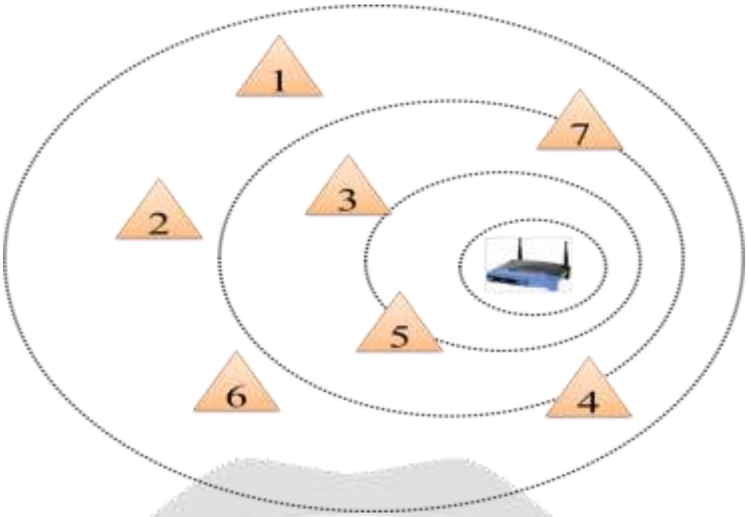

Figure 1: Wireless Network

The wireless network has a very limited band width and is relatively less reliable due to the effects of the environment compared to the wired network providing abundant bandwidth and reliable wired network connections. Therefore, in the wireless network, It is not enough that the use of conventional networking techniques that are used in wired networks.

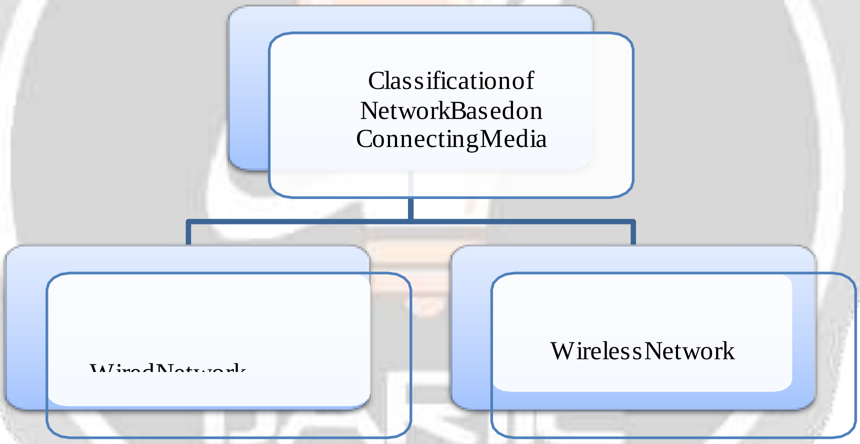

Figure 2: Media Based Classification of Network

1.1 Cellular Network

Cell communication is supported by a structure called a cellular network, which includes cell phones on the public switched telephone network. The mobile network has experienced three generations. To accommodate more users of mobile phones, digital TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access) technologies are used in the second generation (2G) to increase network capacity. With digital technologies, digitized voice can be encoded and encrypted. Accordingly, the cellular network is also safer 2G. The third generation (3G) mobile phones integrate the world of the Internet, providing the packet data transmission of high speed, and the transmission of circuit switched voice. 3G cellular networks have been deployed in parts of Asia, Europe and the United States since 2002 and will be widely deployed in the coming years [7, 8].

1.2 Mobile Ad Hoc Network

An ad hoc network does not have a network infrastructure. This is a network which is spontaneously formed in order to meet the immediate need for communication between mobile nodes. Mobile ad-hoc network is operating in ad hoc manner. A mobile ad hoc network is a set of nodes that are able to change their position randomly, but can communicate. Coordinate with other nodes there no centralized device available. These nodes are able to send and receive data on their own. They can also perform routing. And the Ad-hoc network is very popular due to unstructured network. Due to this asset, there are so many practical applications used in this time[9,10].

1.3 Sensor Network

Sensor networks are dense wireless without small low-cost sensors, which collect and disseminate environmental data networks. Wireless sensor networks facilitate monitoring of physical environments from remote locations with greater accuracy. They have applications in a variety of areas such as environmental monitoring, military purposes and the gathering of sensitive information in hospitable places. Sensor nodes have various energy and computational constraints because of their ad hoc nature and low-cost method of implementation [11, 12].

1.4 Applications of Sensor Network

The three main categories of applications commonly referred to sensor network. Collection of environmental data, the security monitoring and tracking sensor node are those categories. It seems that most implementations of wireless sensor networks are one of those class models

1.5 Challenges and Constraints of WSN

In the WSN, there are many challenges faced by the sensor network to develop reliable communication in the transmission of data, Quality of Service, and also in energy consumption, hardware, and software complexity. The constraints of WSN rely on Power consumption, storage, and computation

1.6 Wireless Sensor Network Challenges

The challenges in the WSN according to the requirement of the applications in which some are listed below:

- **Energy efficiency: -** Energy efficiency is the main issue as WSN is a resource-constrained network. The consumption of energy is utilized during the data packet routing activity. It mainly depends on the lifespan of the sensor nodes' battery.
- **Prolonged network lifetime: -** Another challenge is to prolong the lifetime of the nodes by decreasing the energy consumption and extend the WSN's life cycle.
- **Quality of service: -** Each application has its terms of QoS, and it may request different QoS Processing. Due to the limitations of hardware devices, providing QoS is still a challenging task.
- **Fault tolerance: -** The nodes can sustain the functions carried out in the network even when there is limited power in the battery, failure rate of nodes, and interference from the external environment.
- **Dynamic environment: -** The ability of the WSN to withstand harsh environmental conditions where they are primarily deployed in hazardous areas and some of the locations may be unattended.

2. ATTACKS IN SENSOR NETWORK

With the rapid development of wireless technology, sensor network has become a new type of wireless network. The world today is experiencing a fight, and the battlefield is on the road, the estimated number of deaths is approximately 1.2 million people per year worldwide [4, 8]. Network sensors are new type of networks is expected to support a wide range of distributed mobile applications. A sensor array is a set of nodes or mob ile routers connected to an automatic transmission.

2.1 External vs. Internal Attack

Attacks can also be classified as external attacks and internal attacks, according to the area of attacks [6, 7]. Nodes that do not belong to the network domain conduct external attacks. Internal attacks are compromised nodes, which are actually part of the network. Internal attacks are more harmful compared to external attacks since the insider knows secret and valuable information, and has confidential access rights.

2.2 Active Vs Passive Attack

The attacks in MANET can be classified into two main categories: passive attacks and active attacks. A passive attack obtains data exchanged over the network without disrupting communications, while an active attack involves information disruption, modification or manufacturing, which disrupts the normal operation of a sensor.

An active attack attempts to alter or destroy the data exchanged on the network, disrupting the normal operation of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network.

3. WORM HOLE ATTACK

In a worm hole attack, two attacker nodes join. An attacker node receives packets at one point and "tunnels" Forward to another node via a private network connection, and then played on the network.

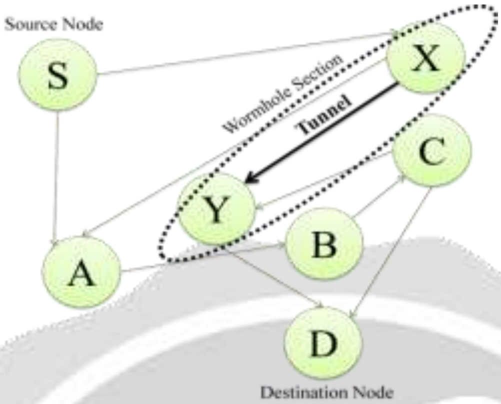

Figure 3: Worm hole Attack

Worm hole attack is a relay-based to attack the routing protocol is interrupted and thus interrupts or failure of a network and, for this reason, this attack is serious. We can use 4 steps to explain a general attack worm hole [5, 6].

- An attacker has two trusted nodes in two different networks with a direct link between the two nodes places.
- Attacker logs packets to a location on a network.
- Tunnels Striker after packages stored in a different location.
- Attacker sends packets to the network location from step 1.

4. RELATED WORK

The Wireless Sensor Network is vulnerable to numerous security attacks, and there is loss of information variable to the physical environment and invasion of the attacks. The author in [3] proposed a survey of protocols and design constraints of specific tools. The main challenge is to design robust security protocols with low maintenance. The author proposed in [4] has improved and discussed the security mechanism at the different layers of the network. The author also stated that improving the efficiency and defense mechanisms to overcome the attacks in all the layers. The work is given in [5] a security scheme for the system with robust security protocols for managing sensor nodes in networks and energy efficiency.

5. CONCLUSION

The paper summarized the security challenges and constraints of wireless sensor networks and various security attacks in the WSN. The active and passive attacks are analyzed, which gives the researchers an insight into various attacks in WSN. The users should also know about the privacy issues and permissions given for the data and how they misuse the information and propose future research exploring the effective security mechanisms and counter measures.

REFERENCES

[1] Surinder Singh, Hardeep Singh Saini, “Intelligent Ad-Hoc-On Demand Multipath Distance Vector for Wormhole Attack in Clustered WSN”, Springer Science Business Media, LLC, part of Springer Nature 2021.
[2] Ghasem Farjamnia · Yusif Asimov · Cavanshir Kazimov, “Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Network”, © Springer Science Business Media, LLC, part of Springer Nature 2019.
[3] WATEEN A. ALIADY AND SAAD A. AL-AHMAD, “Energy Preserving Secure Measure Against

Wormhole Attack in Wireless Sensor Networks”, VOLUME 7, IEE ACCESS2019.

[4]Rajendra Kumar Dwivedi , Prachi Sharma , Rakesh Kumar, “Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network”, 2018 IEEE.

[4] Bharat Bhushan1 · Gadadhar Sahoo, “Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks”,©Springer Science+Business Media, LLC 2017

[5] Farkhana Muchtar, Abdul Hanan Abdullah , Mosleh AlAdhaileh ,Kamal Zuhairi Zamli, “Energy conservation strategies in Named Data Networking based MANET using congestion control: A review”, Journal of Network and Computer Applications Elsevier 2020

[6] Y. Harold Robinson, E. Golden Julie, Krishnan Saravanan, Raghvendra Kumar, Le Hoang Son, “FD-AOMDV: faulttolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks”, Journal of Ambient Intelligence and Humanized Computing, Pp. 4455– 4472, 2018.

[7] Neelam Sharma, Shyam Singh Rajput, Amit Kumar Dwivedi, Manish Shrimali, “P-RED: Probability Based Random Early Detection Algorithm for Queue Management in MANET, Advances in Computer and Computational Sciences, Vol 554. Springer, Pp. 637-643, 2018.

[8] K. Y. Ajay, T. Sachin, "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs," Peer-to-Peer Networking and Applications, vol. 10, Pp. 897–909, 2017

[9] Louazani Ahme, Sekhri Larbi, Kechar Bouabdellah, “A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Network” Published Online November 2014 in MECS.

[10] Jegan Govindasamy ∗, Samundiswary Punniakody, “ A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack, ScienceDirect 2018.

[11] Sunil Kumar and Pankaj Negi , “A Link Failure Solution in Mobile Adhoc Network through Backward AODV (B-AODV)”, IJCEM International Journal of Computational Engineering & Management, Vo11,January 2011 ISSN (Online): 2230-7893, 2011

[12] Nabila Labraoui *, Mourad Gueroui and Makhlouf Aliouat, “Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks,” TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES John Wiley & Sons, Ltd2011, 1(8): 64-67 ISSN: 2231 – 2587, 2011.

[13] Srinath Perur, Abhilash P. and Sridhar Iyer , “Router Handoff: A Preemptive Route Repair Strategy for AODV” IEEE, 2003.

[14] Amandeep Singh Bhatia and Rupinder Kaur Cheema ,“Analysing and Implementing the Mobility over MANETS using Random Way Point Model” ,International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013

[15] Priyanka Goyal, Vintra Parmar and Rahul Rishi , “ MANET: Vulnerabilities, Challenges, Attacks, Application” , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011.