A Survey Wireless Network Security

Lalitha Gayatri[1] Preeti Raj[2] Sonalika Kumari[3]
[1,2,3]Department of Computer Science and Engineering
[1,2,3]Centurion University, Bhubaneswar

Abstract— Wireless Sensor networks (WSN) termed as the dominant technology trends in the coming decades and also plays a very important role in our daily life applications such as remote environmental monitoring and target tracking. It is an emerging technology and one of the most exciting and challenging research domains of our time. The sensing technology merged with a processing power and wireless communication creates beneficial for being exploited in affluence in future. They have a great potential to be utilized in wide mission critical applications such as, military monitoring and health care's which are very highly sensitive information which makes security in these special networks a crucial concern. In addition, of wireless communication technology runs into a variety of security threats. Here, In this paper, we present a survey of concerned security issues in WSNs and also its various threats and attacks in WSNs. And it's basic Security Schemas in WSNs. And finally, we conclude the paper delineating the research challenges and future objectives towards the research in wireless sensor network devices.

Key words: Basic Security Schemas in WSNs, Threats and attacks in WSNs, WSN security goals

I. INTRODUCTION

WSNs are being used widely in application areas. The fundamental goals for collect information from the physical world. A wireless sensor network (WSN) is designed to monitor and control physical environment from remote areas with better precision and accuracy. Wireless Sensor Networks can work in any environment especially, for those areas where wired connections are not possible. Basically, WSNs are consisting of battery-controlled or operated sensor devices with data processing, computing, and communicating components. The sensor node is smart, self-organizing multi-functional, equipped with a battery, microcontroller, and sensors. WSNs are used to make better and easier system design and operation to monitor the environment without the need of wired connection networks with better accuracy. Many other important factors of WSNs which are used for self-organizing, self-healing, having dynamic network topology to deal effectively with node errors and failures with the rough environment, a mobility of installed nodes, the capability to withstand bad environmental conditions, scalability, at the time of installed nodes and after installation, as well easy use.

The rest of the paper is outlined as follow: Section I provides the introduction of WSN. Section II provides the various security threats of WSNs. Section III. Describes the goals of network security. Section IV concludes the highlighted issues as well as point outs our future observation.

II. VARIOUS SECURITY THREATS OF WSN

Wireless Sensor Devices are unsafe to security attack (In computer networks an attack is an attempt to destroy, alter, expose or gain unauthorized access to or make unauthorized use of assets.) due to the broadcast nature of the transmission media. An attacker in WSNs can be categorized as active attacks and passive attacks. Figure1 shows the attacks classification on WSN and Figure 2 shows the classification of attacks under general categories

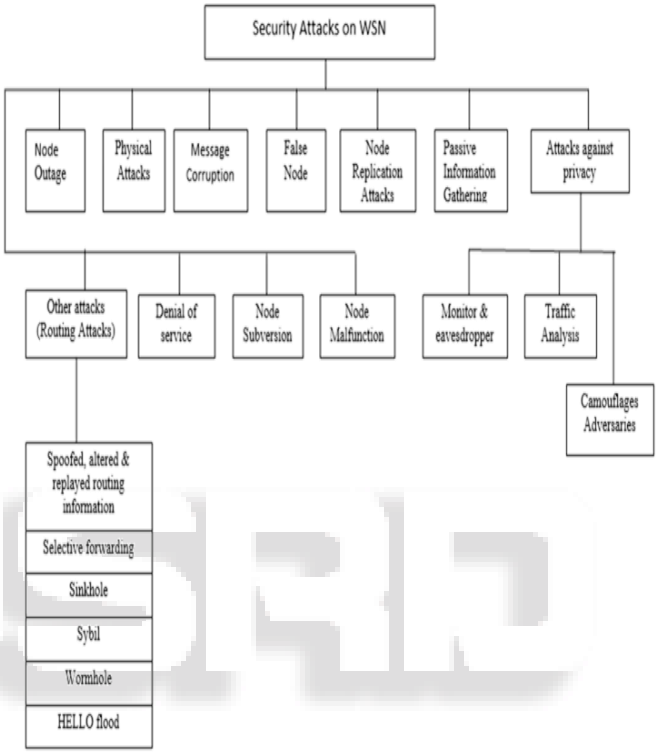

Fig. 1: The attacks classification on WSN.

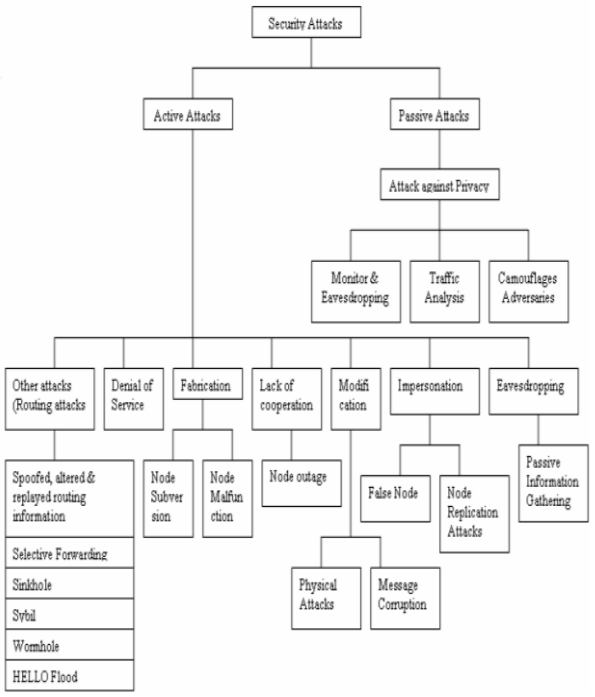

Fig. 2: General Classification of security attacks

A. Passive Attacks:

A passive attack is a network attack in which a system is observed and sometimes scanned for open ports and vulnerabilities. The purpose is mere to gain information about the target and no data is changed on the target.

- Traffic Analysis
- Non-evasive eavesdropping and monitoring of transmissions
- Because of data unaffected, tricky to detect

Types of Passive Attacks:

1) Traffic Analysis: Here, in this attack, the eavesdropper analyzes the traffic, determines the location, identifies the communicating hosts and observes the frequency and length of the message being exchanged. Using all these information they can anticipate the nature of communication. All incoming and outgoing traffic of network is analysed but not altered.
2) Release of message contents: A telephonic conversation, an E-mail message or a transferred file may consist of confidential data. A passive attack may monitor the contents of these transmission data.

These Passive attacks are very difficult to diagnose because they do not involve any alteration of the data. When a third party accessed the information neither the sender nor the receiver is aware someone other party has read the message. This can be prevented by encryption of data.

B. Active Attacks:

An active attack, in computing security, is an attack characterized by the attacker who tries to break into the system. During an active attack, the intruder will introduce the new data into the system as well as change data within the system.

- Denial-of-service attack
- DNS spoofing
- Man in the middle
- VLAN hopping
- ARP poisoning
- Buffer Overflow
- Smurf attack
- Heap Overflow
- Format String attack

1) Denial-of-service attack: A denial-of-service attack is an effort to make a machine or network resource unavailable to its conscious users, such as to temporarily or permanently interrupts the services of a host connected to the Internet.
2) DNS Spoofing: DNS spoofing, can also be as the Domain Name System cache poisoning, is a form of computer hacking in which corrupt DNS data is introduced into a DNS resolver's cache, causes the name server to return an incorrect IP address, which results in diverting traffic to the attacker's computer.
3) Man in the middle: Man in the middle is an attack where the attacker secretly relays and possibly changer or alters the inter communication between two parties who believe they are directly communicating with one other.
4) ARP Poisoning: ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker transfer Address Resolution Protocol (ARP) messages onto a LAN. Basically, the aim is to accomplice the attacker's MAC address with the IP address of different network host, such as the default gateway, causing any data meant for that IP address to be dispatch to the attacker instead of the network host.
5) Buffer Overflow: A buffer overflow, or buffer overrun, is a program bug where a program, while writing data to a buffer, exceeds the buffer's boundary and overwrites to its adjacent memory locations. This is a special case of the violation of safety. Buffer overflows can be generated by inputs that are designed to execute code, or can change the way the program operates. This may result in eccentric program behavior, including memory access errors or a breach of system security. Therefore, they are the basis of many software vulnerabilities and can be poisonously exploited.
6) Smurf attack: The Smurf Attack is a distributed denial-of-service attack in which huge numbers of Internet Control Message Protocol (ICMP) packets with the victim's spoofed source IP are transmit to a computer network using an IP Broadcast address. Most devices on a network, by default, will respond to this by sending a reply to the source IP address. If the number of machines on the network that receives and responds to these packets is very large, then the victim's computer will be flooded with traffic. This results the slowdown of victim's computer to the point where it becomes impossible to work on.
7) Heap Overflow: A heap overflow is a type of buffer overflow which occurs in the heap data area. These are exploitable in a different manner to that of stack-based overflows. Heap memory is dynamically assigned by the application at run-time and typically contains the data. Exploitation can be done by corrupting this data in a specific way to cause the application to overwrite internal structures such as linked list pointers.

III. Goals of Network Security

There exists large number of exposed in the network. Thus, during transmission, data is highly exposed to attacks. An attacker can mark the communication channel, obtain the data, and read the same or re-insert a false message to achieve his immoral aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to guarantee that the entire network is secure.

Network security entails protecting the usability, sureness, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or propagates on a network.

The primary goal of network security is Confidentiality, Integrity, and Availability. These three columns of Network Security are often represented as CIA triangle.

- Confidentiality −The function of confidentiality is to protect precious business data from unwarranted persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.
- Integrity − This goal means maintaining and assuring the accuracy and fixture of data. The function of integrity is

to make sure that the data is reliable and is not changed by unwarranted persons.

– Availability − The function of availability in Network Security is to make sure that the data, network resources/services are continually available to the legitimate users, whenever they require it.

IV. CONCLUSION

The wireless sensor networks had become widely used in many mission-critical applications. Wireless sensor networks are increasingly being used in defense force, environmental issues, health, and commercial applications. Security is a very important feature for the deployment of WSN. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. This paper summarizes the attacks and its classifications in wireless sensor networks and also what are the network security goals available in Wireless Sensor networks.

REFERENCES

[1] (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009 A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks.
[2] Wikipedia: Security threats in wireless sensor devices
[3] Tutorialspoint.com: Goals of network security
[4] A SURVEY OF WIRELESS SENSOR NETWORK ARCHITECTURES Almir Davis, Hwa Chang Department of Electrical and Computer Engineering, Tufts University, Medford, MAUSAalmir.davis@tufts.edu,hchang@ece.tufts.edu
[5] Wireless Sensor Networks: Security Issues, Challenges and Solutions Vikash Kumar1, Anshu Jain2 and P N Barwal3 1, 2, 3e-Governance, C-DAC,C-56/1, GB NAGAR, NOIDA, INDIA
[6] Security in Wireless Sensor Networks: Issues and Challenges Mahsa Teymourzadeh1, Roshanak Vahed2, Soulmaz Alibeygi3, Narges Dastanpor4 1, 2 Faculty of Engineering, Department of Computer Engineering, Islamic Azad University Khorasgan, Iran 3 Faculty of Engineering, Department of Electronic Engraining, Islamic Azad University Shahrekord, Iran4 Faculty of Engineering, Department of Electronic Engraining, Islamic Azad University Naein, Iran
[7] Security threats in wireless sensor networks sona malhotra, assistant prof. Cse dept. Uiet (Kurukshetra University, Kurukshetra) Rahul Research Scholar, CSE Dept. UIET (Kurukshetra University, Kurukshetra)
[8] Security Issues in Wireless Sensor Networks: Attacks and Countermeasures Kahina CHELLI

