Security Assaults, Flaws, and Defences in Wireless Sensor Networks at Different OSI Reference Model Levels

Mithilesh Pandey[1],Dr. Abhilash Singh[2], Mr. Rahul Pandey[3]

1Assistant Professor, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun

2Associate Professor Shivalik Institute of Professional Studies, Dehradun

3Assistant Professor, College of Pharmacy, Shivalik, Dehradun

Mithilesh.Pandey@sce.org.in

ABSTRACT:Because of the development of numerous security-sensitive applications in many areas using WSNs, wireless sensor networks (WSNs) security is a subject of significant significance. Compared to traditional wireless and wired networks, WSNs have a variety of additional vulnerabilities, such as a dynamic network topology, the broadcast nature of the medium, resource-constrained nodes, a significant network size, and a lack of physical infrastructure. WSNs are more vulnerable to various attacks than wired communications because of the open communication environment, including passive eavesdropping operations that lead to intercepted transmissions and active jamming attacks that lead to transmission interruption. These new flaws allow the opponent to carry out more severe and complex assaults. As a result, a comprehensive examination of possible attacks against WSNs is needed. As a result, the purpose of this article is to examine wireless security weaknesses and threats in order to develop a reliable and efficient defense method for improving WSN security. First, we will go through the security problems and needs of wireless networks. The next section of the paper examines security flaws in wireless networks and groups probable WSN attacks into OSI protocol levels. Finally, a number of unsolved technical issues are mentioned, along with future work in WSN security.

KEYWORDS:Layer, Network, OSI, Sensor, Wireless.

1. INTRODUCTION

Wireless sensor networks have evolved because of advancements in communications, electronics, internet, and information technologies (WSNs). WSN is a new study field that is gaining traction in academia, research institutions, and industry. These are used in many different applications, including as tracking objects, monitoring smart homes, and healthcare. WSNs are networks made up of a lot of inexpensive sensors with limited resources, memory, such low bandwidth, computing power, and battery life. The sensors have a sensing unit and wireless sensing capabilities. These sensors are tiny in size and are used to effectively do the duties they were designed to do[1].

Heterogeneous sensor networks are more practical since they perform better. These provide all scalability, delay tolerance, and efficient load balancing. With the growing usage of WSNs in real-time applications such as military, hospitals, and wildlife monitoring, data must be accessible at all times, from any location. These WSNs' data is very important and sensitive. As a result, an attacker may expose sensor data by adding rogue nodes into the sensor network. An adversary may potentially disrupt the network's functioning[2].

WSNs use a multi-level OSI layers protocol structure. At each tier, the security holes in these protocol layers are guarded separately. Security requirements like confidentiality, authentication, integrity, and availability are met by this. Data confidentiality may be protected using cryptographic techniques that stop information from being revealed to unauthorised users. Data confidentiality is increased via cryptography, but it adds latency and requires more computational power. This is because data encryption and decryption take a lot of time. WSNs use a range of authentication techniques to guarantee the accuracy of the data. Examples of these techniques include MAC layer authentication, transport layer authentication, and network layer authentication. At the network layer, WPA and WPA2 are used to secure authentication. Data authentication in WSNs is done at the transport layer using the SSL and TSL protocols. The primary wireless security methods are authentication, encryption, authorisation, delay, and complexity. The OSI layer Model is shown in Figure 1 [3].

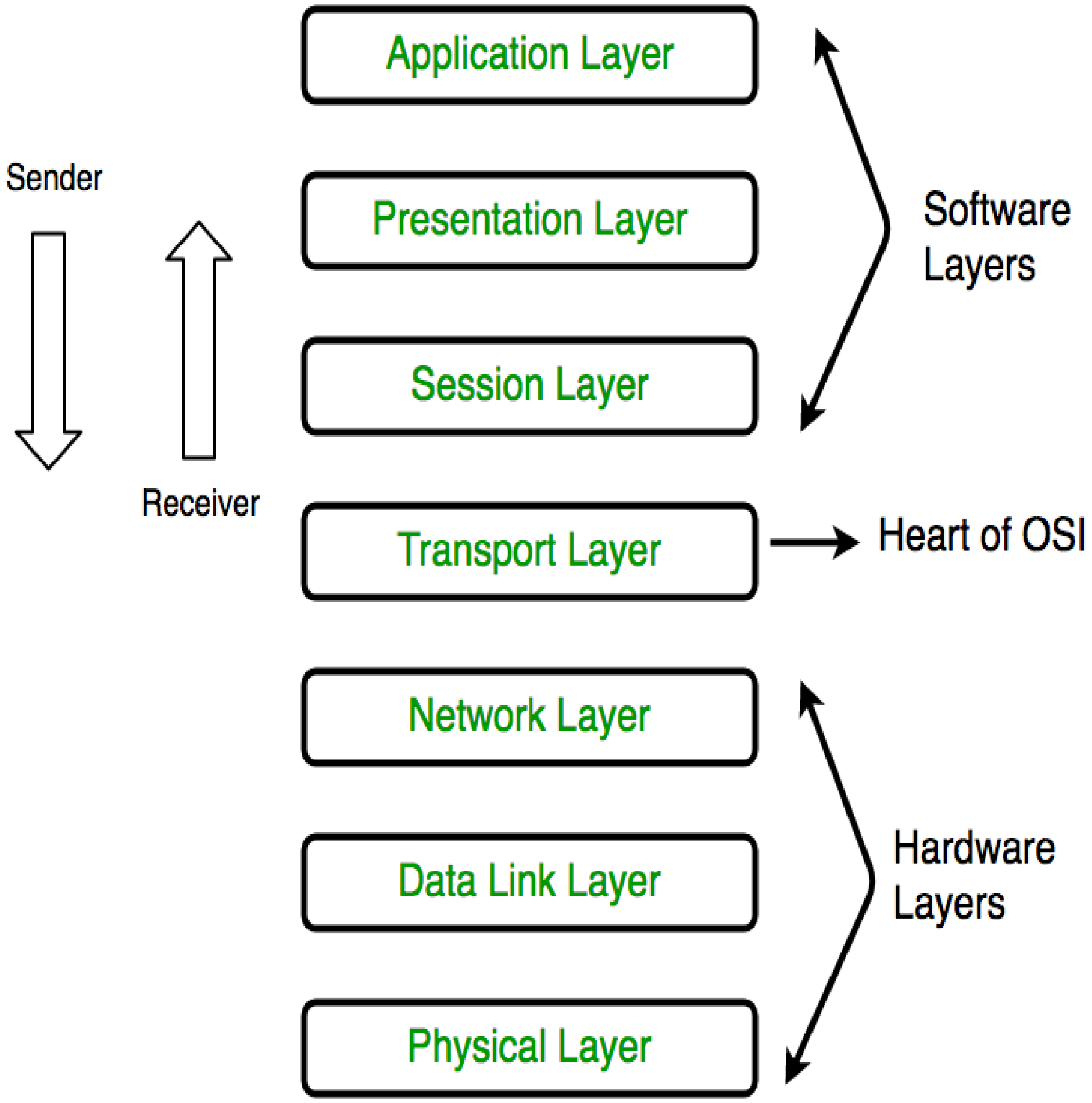

Figure 1: The above figure shows the OSI layer model [geeksforgeeks].

The communication nodes in wired networks are physically linked via wires. Due to the broadcast nature of wireless networks, they are prone to a wide range of malicious attacks, such as DoS attacks, eavesdropping attacks, MITM attacks, spoofing attacks, message falsification attacks, etc. In a wireless network, unauthorised nodes might cause interference and obstruct legitimate users from sending data to one another. Eavesdroppers may be able to hear the wireless communication sessions if they are within the sender node's broadcast range. Data between authorised users may be kept secret by using cryptographic techniques to prevent eavesdroppers from reading it.

As a consequence, encryption techniques assume that the processing power of the listeners is constrained.

The remainder of this essay is organised as follows. The medium's broadcast nature, a lack of physical infrastructure, a dynamic network topology, resource-constrained nodes, and the scale of WSNs are all contributing factors. Section 3 of the security requirements and goals of WSNs addresses the secrecy, integrity, authenticity, and network availability. The security holes in wireless networks are covered in Section 4. Below is a description of each of the numerous protocols used at each level of the OSI protocol stack. Additionally, the section examines the many wireless network vulnerabilities that must be managed by the various OSI protocol stack layers, including the transport layer, physical layer, network layer, MAC layer, and application layer [4]–[6].

1.1 Security Problems:

WSNs have various security flaws because of the wireless medium's broadcast and open nature. Wormhole attacks, denial of service attacks, sinkhole attacks, black hole attacks, flooding assaults, and other types of attacks are carried out by malicious adversaries using known network vulnerabilities.

1.1.1 The medium's broadcast nature:

Because wireless medium access is accessible to everyone, a hostile attacker may obtain network access by aligning itself with the sensor network nodes' radio range. As a result, an attacker may intercept, replay, modify, or eavesdrop on network communications[7].

1.1.2 Sensornodes with limited resources:

Sensor nodes (SNs) have limited processing, energy, and computing capacity, as well as memory, storage, and bandwidth. As a result, the SN's resources are limited, limiting the use of some preventative measures like data aggregation and encrypting. These methods may be used as a first line of defense against assaults on the whole network as well as individual nodes.

1.1.3 Inadequatephysical protection:

In hostile situations, SNs are used. In such hazardous settings, attackers may physically damage, capture, or destroy SNs. Device capture in wartime battlefields may have serious implications.

1.1.4 Topology of a dynamic network:

WSNs have a dynamic network topology, which means there are no fixed boundaries or structures since SNs may leave or join the network at any moment. As a result, security methods that can deal with such high network dynamics are necessary.

1.1.5 Massivescale:

In comparison to small-scale networks, intrusion detection is more challenging in networks with thousands of SNs.

1.2 Security Objectives:

WSN's security assessment is based on a set of criteria known as security objectives. If networks fall short of any of these objectives, security methods must be devised. Various security objectives are discussed in this part, which should be present for all network types. The following are some of these objectives[8].

1.2.1 Information security:

In order to avoid intrusion, the message's content is concealed from all nodes save the destination. This limits access to data to just those who are permitted. To guarantee data privacy, a variety of cryptographic techniques may be used. In symmetric key encryption techniques, the transmitting node encrypts the plaintext (original data) using a secret key and an encryption algorithm. The destination receives cypher text (encrypted data), which is then decoded using proprietary keys that are only known to the destination. Because it is ignorant of the secret key, Eavesdropper is unable to decrypt the CT. There are several key management techniques required for key exchange between the source and the destination.

1.2.2 Data consistency

The term "data integrity" refers to the message content not being changed or altered in any way. Adversary may also change the message's substance on purpose. This may happen because of the attacker injecting false data. Unintentional changes to message content may result in data loss or harm. Throughout the life cycle of a wireless network, information must be trustworthy and accurate without being tampered with or falsified by unauthorized users. Insider attacks that undermine the data integrity are known as node compromise attacks. If an attacker compromises or alters a legal node, it is referred to as a compromised node. The compromised nodes may launch malicious attacks such as false reporting, message injection and data manipulation[9], [10].

1.2.3 Message sincerity:

The destination nodes must identify the source of the message to determine its reliability after message reception. This stops malicious nodes or attackers from sending data that will be approved. Authenticity is the ability to determine the true identity of SNs and distinguish between legitimate and unauthorised users. Each sensor node has its own MAC address and network interface card to simplify the authentication process. In addition to these techniques, there are several more message authentication systems for safeguarding communicated data in the sensor network.

1.2.4 Network connectivity:

This stops genuine nodes from accepting data from attacker. This enables authorized users to connect to the network at any time and from anywhere. A breach of network availability causes a denial of service. This prevents authorized users from accessing the network, resulting in poor user experiences. A kind of DoS attack known as jamming prevents the flow of legal data.

2. DISCUSSION

At several levels of the OSI reference model, the author has examined security flaws, threats, and defences in wireless sensor networks. Wireless sensor networks have emerged as a result of developments in communications, electronics, internet, and information technologies (WSNs). WSN is a relatively young field of research that is picking up steam in education, research, and industry. These have a broad variety of uses, including as tracking objects, monitoring smart homes, and healthcare.

In wired networks, the communication nodes are physically connected via wires. Since wireless networks are broadcast, they are susceptible to a variety of malicious attacks, including DoS attacks, espionage attacks, MITM attacks, spoofing attacks, message falsification attacks, and so forth. Unauthorized nodes have the potential to interfere with authorised users' data transmission in a wireless network. Snoopers may be able to hear wireless communication sessions if they are close enough to the broadcasting node to benefit from its possibilities and assistance. By preventing eavesdroppers from intercepting data between authorised users, cryptographic methods may be utilised to keep such information private. As a result, encryption methods presumptively consider the eavesdroppers' limited computing power. The rest of this essay is structured as follows. Considerable reasons include the broadcast nature of the media, a lack of physical infrastructure, a dynamic network architecture, wealth nodes, and the enormous size of WSNs. Secrecy, integrity, authenticity, and network availability are all addressed in Section 3 of the security criteria and purposes of WSNs. The security flaws in wireless networks are examined in the fourth part. Here we describe the many levels of the many protocols in the OSI protocol stack. The section also looks at the many wireless network hazards that must be addressed by the physical layer, MAC layer, core network, tcp/ip model, and application layer of the OSI protocol stack. WSNs consist of a large number of inexpensive sensors with constrained bandwidth, computational power, memory, and battery life. The sensors feature a sensing unit and wireless sensing capabilities. These little sensors are used to carry out the tasks for which they were designed.

Heterogeneous sensor networks are more useful since they perform better. They provide complete scalability, tolerance for delays, and effective load balancing. Since WSNs are utilised in real-time applications including the military, hospitals, and wildlife monitoring, data must always be accessible from everywhere. These WSNs gather sensitive and important data. As a result, an attacker may be able to access sensor data by inserting rogue nodes into the sensor network. It's possible that an attacker will make the network unreliable.

3. CONCLUSION

At several levels of the OSI reference model, the author has examined security flaws, threats, and defences in wireless sensor networks. This article provides an overview of WSN security concerns and defensive strategies for defending the authenticity, integrity, secrecy, and availability of transmission against malicious wireless attacks. Since WSNs have a variety of additional problems, including variable network topology, resource-constrained nodes, the broadcast nature of the medium, and a lack of physical infrastructure, WSN security is a new research topic. These weaknesses in WSNs are exploited by adversaries to carry out several significant attacks. At different OSI protocol levels, a broad range of wireless attacks, security problems, and existing remedies are discussed.

WSNs have a number of extra weaknesses as compared to conventional wireless and wired networks, including shifting network topology, the broadcast nature of the medium, resource-constrained nodes, huge network size, and a lack of physical infrastructure. Due to their open communication environment, WSNs are more susceptible to a variety of assaults than cable connections, including passive espionage operations that lead to message interceptions and active jamming attempts that stop transmissions. The opponent may now carry out more severe and sophisticated attacks thanks to these additional vulnerabilities. Consequently, a thorough analysis of potential WSN attacks is required. Consequently, the goal of this article is to look at wireless security flaws and threats in order to come up with a reliable and efficient defensive strategy for enhancing WSN security. First, we will go through wireless network security issues and requirements. The paper then goes on to talk about wireless network security flaws and how to classify possible attacks in WSNs based on OSI protocol levels.Security is critical in a number of practical real-time WSNs applications.

REFERENCES

[1] V. Beal, “The 7 Layers of the OSI Model,” *webopedia*, 2015. .

[2] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, “Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey,” in *Proceedings of IEEE International Conference on Signal Processing and Communication, ICSPC 2017*, 2018, doi: 10.1109/CSPC.2017.8305855.

[3] M. G. Moreira Santos and P. A. Alcívar Marcillo, “Security in the data link layer of the OSI model on LANs wired Cisco,” *J. Sci. Res. Rev. Cienc. e Investig.*, 2018, doi: 10.26910/issn.2528-8083vol3isscitt2017.2018pp106-112.

[4] G. Sondakh, M. E. I. Najoan, and A. S. Lumenta, “Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat,” *J. Tek. Elektro dan Komput.*, 2018.

[5] T. Banerjee and A. Sheth, “IoT Quality Control for Data and Application Needs,” *IEEE Intell. Syst.*, 2017, doi: 10.1109/MIS.2017.35.

[6] H. H. Khalil and T. Eltaeib, “Importance of Application Layer in OSI Model,” *J. Multidiscip. Eng. Sci. Technol.*, 2015.

[7] A. Pertiwi, “Identifikasi Masalah Pada Jaringan Komputer Berbasis Model Osi,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, 2017.

[8] Y. Mardiana and J. Sahputra, “Analisa Performansi Protokol TCP, UDP dan SCTP Pada Lalu Lintas Multimedia,” *J. MEDIA INFOTAMA*, 2017, doi: 10.37676/jmi.v13i2.455.

[9] K. Nagesh, R. Sumathy, P. Devakumar, and K. Sathiyamurthy, “A survey on denial of service attacks and preclusions,” *Int. J. Inf. Secur. Priv.*, 2017, doi: 10.4018/IJISP.2017100101.

[10] U. I. Ikechukwu, “A Survey on Bandwidth Management Techniques Via the OSI Model Network and Application Layers,” *Glob. J. Comput. Sci. Technol. E Network, Web Secur.*, 2017.