A Review Paper on Various Wireless Network Attacks

DR.KULDEEP PANWAR[1], DR. GANESH KUMAR[2], DR. SHAMBHOO PRASAD[3]

1Department of Mechanical Engineering, Shivalik College of Engineering, Dehradun
2College of Pharmacy, Shivalik, Dehradun
3Shivalik Institute of Professional Studies, Dehradun

Drkuldeep.panwar@sce.org.in

ABSTRACT:Security for wireless sensor networks (WSNs) is becoming increasingly crucial due to the growth of several security-sensitive applications using WSNs in a range of industries. WSNs have a number of extra weaknesses as compared to conventional wireless and wired networks, such as shifting network topology, the broadcast nature of the medium, resource-constrained nodes, huge network size, and a lack of physical infrastructure. WSNs are more vulnerable to a range of attacks than cable communications because of their open communication environment, including passive eavesdropping operations that result in intercepted transmissions and active jamming attacks that interrupt transmissions. The opponent may now carry out more severe and sophisticated attacks thanks to these additional vulnerabilities. Therefore, a thorough analysis of potential WSN attacks is required. Therefore, 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. Finally, future work in WSN security is discussed, as well as many remaining technical issues that remain unsolved.

KEYWORDS:Jamming, Network, OSI, Security, Wireless.

1. INTRODUCTION

The numerous wireless network threats that different OSI protocol stack levels have to deal with. Figure 1 shows the Wireless Network attacks.

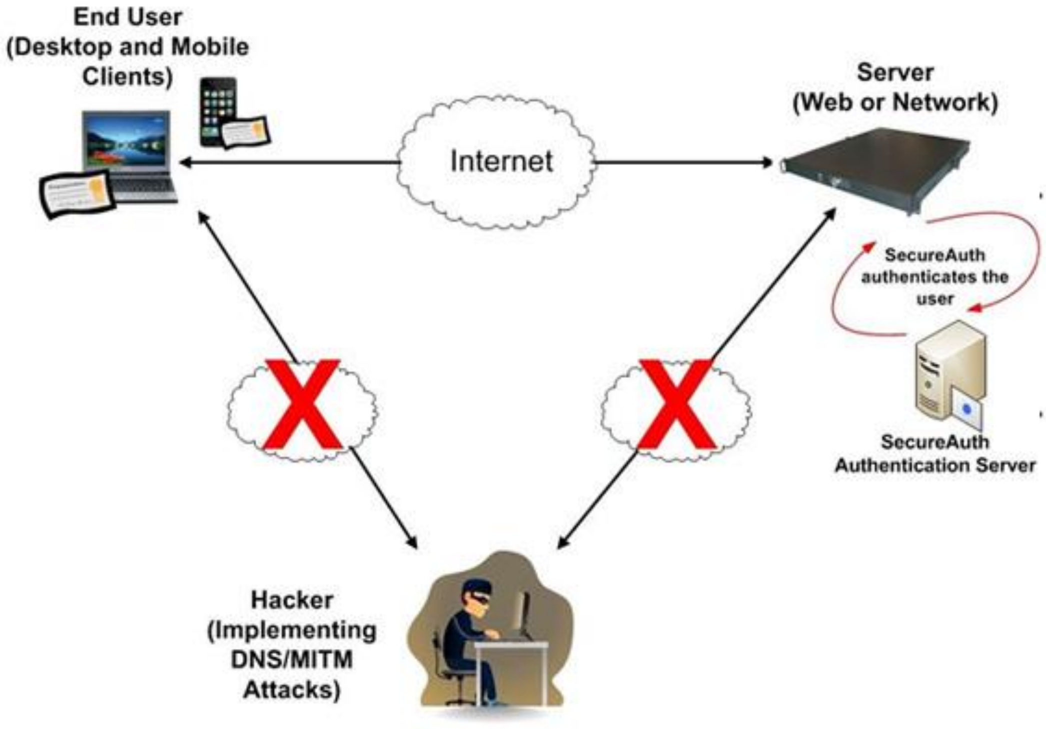

Figure 1: The above figure shows the Wireless Network attacks [snabaynetworking].

1.1 Physical Layer Attack:

The physical characteristics of signal transmission are defined. Since the channel is broadcast, it is susceptible to attacks by jammers and eavesdroppers. An attacker intercepts data in transit between authorised and legitimate users during an eavesdropping attack. The eavesdropper listens to the talk until it is within the transmission range of the source node. To avoid eavesdropping, several cryptographic approaches are utilised. The sensor nodes encrypt the plaintext and transmit the cypher text to the target SNs using a shared secret key. The eavesdropper won't be able to get any useful information even if it hears the encrypted text since it doesn't have the secret key. The use of cryptography normalises eavesdropping assaults as a consequence. A rogue node may prevent data transfer by purposefully interfering with authorised users. A jammer assault is this particular kind of DoS assault [1]–[3].

Attacks on wireless sensor networks' physical layers often include jamming. A common method of protecting WSNs from physical layer jamming assaults is spread spectrum communication. The best defensive strategy is to keep SNs in sleep mode and sometimes wake them to check the communication channel for continuous jamming if a jamming attack is identified in WSNs. By utilising less energy, this increases the SN's lifespan, but also leaves it vulnerable to DoS assaults. An attacker could need to block the channel for a lot longer. Because the jammer prevents authorised users from accessing particular network resources, users are unable to utilise them. Spread spectrum defence techniques are used to counter jamming attacks. This causes the transmitted signal to be spread over a greater frequency range than the original frequency band. FHSS, DSSS, and THSS are a few spread spectrum techniques for thwarting jamming attacks in WSNs [4], [5].

1.2 Attackson the MAC layer:

It allows many nodes to access a shared media utilizing a variety of access control methods like as CDMA, OFDMA, CSMA/CA, and others. For user authentication, each node has its own MAC address and network interface card. By altering the given MAC address, the adversary may conduct a MAC spoofing attack. Although the MAC address is programmed into the NIC card, the rogue node may still use spoofing to carry out illegal actions. The MAC address of legal nodes may be stolen if an adversary listens in on the transmission. Identity theft is the term for this kind of assault. Man-in-the-middle (MITM) attacks and network injection are two additional types of MAC layer attacks. The attacker sniffs network traffic to capture the MAC addresses of lawful nodes in an MITM attack. As a relay between two victims, the MITM enemy cats. Certain networking equipment, such as switches, routers, and so on, are disabled by network injection. If additional components are hacked, the whole network may be rendered inoperable, necessitating the reboot or reprogramming of all affected networking devices. Interrogation, collisions, and packet replay are further dangers linked to the link layer. The collision assault is comparable to the reactive jamming attack. Error correcting codes may reduce collisions in certain cases, but they cost energy and increase transmission overhead. The denial of sleep attack is another link layer attack in WSN. It keeps the radio from going into standby mode[6], [7].

1.3 Network Layer Attack:

The network layer's IP protocol is responsible for sending data or packets from a source to a destination via intermediate routers and their IP addresses. The Smurf attack, IP spoofing, and hijacking are a few examples of network layer attacks that exploit IP vulnerabilities. IP spoofing generates a phoney IP address, concealing the attacker's true identity and enabling them to commit crimes. Nodes send data back to the forged IP address after receiving communications from false IP addresses. This wastes network bandwidth and causes the network to be paralyzed. Hijackers take control of genuine users' IP addresses in IP hijacking[8].

As a result, legitimate users are disconnected from the network, and a new connection is established. As a result, the enemy is able to access the confidential information. A large number of ICMP packets are transmitted to the target node during a Smurf assault. Victims provide ICMP responses in response to ICMP queries. The Smurf attack overwhelms the target network with ICMP queries, which paralyses it. In order to defend against Smurf attacks, routers and individual users are set up such that they don't always answer to ICMP queries. In addition, harmful communications from faked IP addresses are blocked by firewalls. Hello flooding is a kind of attack where the attacker does not have to decrypt the data. To create a hello flood, an attacker gathers hello packets and delivers them with a high transmit power. Geographic and energy-aware routing protocols may be able to stop this attack since each node in a geographic protocol must be aware of its own position and be able to communicate it to other nodes. Homing is a kind of network layer attack that locates and targets nodes performing certain activities, such as cluster leaders and cryptographic key management, using traffic pattern analysis [9].

1.4 Transport Layer Attacks:

Transmission Control Protocol, often known as TCP, is a connection-oriented protocol that enables secure data transfer while transferring files and emails across networks. The connectionless nature of UDP results in decreased latency and overhead. The dependability of packet delivery is not ensured by UDP. TCP flooding, often referred to as ping flooding, is a kind of transport layer denial-of-service attack in which the attacker floods the target nodes with ICMP ping requests. Input and output buffers on the victim are flooded as a result, slowing down connection to the target network. The transmitting node's packets are made and the sequence index is calculated using the TCP prediction technique. As a result, victims get faked packets, resulting in problems with data integrity.

An excessive quantity of UDP packets are sent to the target nodes during a UDP flooding attack, prompting them to send an equal amount of reply packets. The victim nodes become unreachable for numerous legitimate nodes.

It is possible to lessen the impact of a UDP flooding assault by reducing the UDP packet response rate. Additionally, malicious UDP packets may be blocked by firewalls, thwarting UDP flooding assaults. Desynchronization attacks aim to break the connection between two nodes by sending phoney packets with fictitious sequence numbers. By utilising header or complete packet authentication, such an attack may be prevented.

1.5 Application Layer Attacks:

Numerous protocols are supported by the application layer, such as HTTP for online services, SMTP for email, and FTP for file transfers. Each of these protocols may put network security at risk. Malware, sometimes referred to as HTTP attacks, comprises backdoors, worms, Trojan horses, keyloggers, and viruses. Software called malware is intended to obstruct or intercept truly sensitive data.

A method for getting unauthorised access to websites is SQL injection, which takes advantage of data-driven systems. FTP is used to send big data, however there are security dangers involved. One kind of FTP-related attack that takes use of an intermediary are FTP bounce attacks. Password sniffers, email spoofing viruses, and SMTP worms are a few examples of SMTP assaults. To stop such assaults, firewalls and antivirus software are necessary. If an attacker utilises sensor stimuli to overload sensor nodes, the sensor network at this layer may communicate massive amounts of data to the base station. This kind of assault drains the energy of the nodes and uses up network bandwidth. This assault may be stopped by altering the sensors such that only certain stimuli, like moving automobiles, may activate them. The adoption of an efficient rate limiter and data aggregation system may aid in reducing the severity of these attacks. Another kind of application layer attack in a path-based Dos attack involves injecting bogus or replayed packets into the sensor network at leaf nodes. The following table shows several assaults and defences at different OSI reference model levels[10].

1.6 Objectives and Future Works:

Many problems and challenges in WSNs remain unsolved. The following are a few examples of such difficulties.

- The majority of physical layer security research focuses on eavesdropping attacks and ignores other kinds of wireless assaults. In WSNs, these mixed wireless assaults must be addressed.
- When it comes to wireless sensor networks, security, throughput, and dependability are the most important considerations. These variables must be optimized while maintaining high-speed and secure wireless connections.
- For cross-layered networks, WSN security must be enhanced at a lower latency and security overhead than traditional methods where OSI reference levels are protected individually.
- Techniques for secure key management must be developed. As a main security method for user authentication and data encryption, cryptographic keys must be created between the SNs.
- For efficient data, transfers in WSNs, safe user authentication and secure data routing methods must be established.

2. DISCUSSION

The author has discussed about the various wireless Networks attacks,WSNs have a number of extra vulnerabilities as compared to conventional wireless and wired networks, including fluctuating network topology, the broadcasted nature of the medium, resource limited nodes, huge network size, and a lack of physical architecture. Because of their direct communication environment, WSNs are more susceptible to a variety of assaults than cable connections, including passive listening activities that result in recorded messages and active jamming cyberattacks that disrupt transmissions. Because of these new weaknesses, the adversary may now engage out more severe and complex assaults. As a result, a comprehensive examination of possible WSN attacks is needed. As a result, the purpose of this article is to examine wireless security threats and weaknesses in order to develop a dependable and effective defensive approach for improving WSN security. We will start by discussing wireless network security concerns and needs. The discussion of wireless network security flaws and how to classify probable WSN attacks using OSI protocol levels follow. SQL injection is a method for getting unauthorised access to websites by focusing on data-driven systems. Large volumes of data are sent over FTP, however this method is also susceptible to security issues. Attacks connected to FTP that use an intermediary are known as "FTP bounce attacks." Password sniffers and email spoofing worms are examples of SMTP assaults. Antivirus software and firewalls are necessary to defend against such assaults. At this layer, an attacker could use sensor stimuli to overwhelm sensor nodes, leading the sensor network to send a lot of data to the base station.

3. CONCLUSION

According to the author's analysis of the different wireless network assaults, an eavesdropper cannot listen in on a communication session until they are inside the source node's broadcast range. To stop eavesdropping, several cryptographic methods are utilised. The sensor nodes encrypt the plaintext (original data) using a shared secret key and transmit the cypher text to the target SNs. Even if the eavesdropper hears the encrypted text, without the secret key, it won't be able to decipher any relevant information. As a result, adopting encryption increases the frequency of eavesdropping attacks. By purposefully interfering with authorised users, a rogue node may interfere with data delivery. A jammer assault is an example of a denial-of-service attack. To stop such assaults, firewalls and antivirus software are necessary. If an attacker utilises sensor stimuli to overload sensor nodes, the sensor network at this layer may communicate massive amounts of data to the base station. This kind of assault drains the energy of the nodes and uses up network bandwidth. This assault may be stopped by altering the sensors such that only certain stimuli, like moving automobiles, may activate them. The adoption of an efficient rate limiter and data aggregation system may aid in reducing the severity of these attacks. Another kind of application layer attack in a path-based Dos attack involves injecting bogus or replayed packets into the sensor network at leaf nodes.

The most common physical layer assault in wireless sensor networks is jamming. Spread spectrum communication is often used in WSNs as a defence against efforts to jam the physical layer. The best defensive tactic when WSNs are under jamming assault is to maintain the SNs in sleep mode and rouse them occasionally to check the communication channel for ongoing jamming. This lessens the SN's need for power and so increases its lifespan, but it does not shield it from Dos assaults. It could be necessary for an enemy to block the channel for a lot longer. Authorized users cannot access certain network resources because the jammer stops them from doing so. Spread spectrum technologies are used to counter jamming attempts. A wider frequency range than the initial frequency band is covered by the transmitted signal as a consequence. 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. Numerous real-world, real-time WSNs applications need security. The author has also drawn conclusions on the goals and forthcoming work.

REFERENCES

[1] D. Kaur and P. Singh, “Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack,” *ACEEE Int. J. Netw. Secur.*, 2014.

[2] N. Briscoe, “Understanding The OSI 7-Layer Model,” *PC Netw. Advis.*, 2000.

[3] Microsoft, “The OSI Model’s Seven Layers Defined and Functions Explained,” *2017*, 2017. .

[4] B. Mitchell, “The OSI Model Layers from Physical to Application,” *Lifewire*, 2018. .

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

[6] 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.

[7] 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.

[8] 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.

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

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

[11] Panwar, K, Murthy, D, S, “Analysis of thermal characteristics of the ball packed thermal regenerator”, Procedia Engineering, 127, 1118-1125.

[12] Panwar, K, Murthy, D, S, “Design and evaluation of pebble bed regenerator with small particles” Materials Today, Proceeding, 3(10), 3784-3791.

[13] Bisht, N, Gope, P, C, Panwar, K, “ Influence of crack offset distance on the interaction of multiple cracks on the same side in a rectangular plate”, Frattura ed IntegritàStrutturale” 9 (32), 1-12.

[14] Panwar, K, Kesarwani, A, “Unsteady CFD Analysis of Regenerator”, International Journal of Scientific & Engineering Research, 7(12), 277-280.

[15] Singh, I., Bajpai, P. K., & Panwar, K. “Advances in Materials Engineering and Manufacturing Processes