National Conference on Information Technology & Digital Application (NCITSA-2025)
International Journal of Advanced Engineering Research and Science (IJAERS) Special Issue
https://dx.doi.org/10.22161/ijaers.ncitsa.2025.4 ISSN: 2349-6495(P) | 2456-1908(O)

Data Security in Wireless Network

Mr. Brijesh Kumar Singh[1] , Rishabh Jain[2], Rohan Kumar Tailor[3] ,

[1]AssistantProfessor
Department of Information Technology, Jaipur Engineering College & Research Centre, Jaipur
[2]Student
Department of Information Technology, Jaipur Engineering College and Research Centre, Jaipur
Email: rishabhjain.it25@gmail.com
[3] Student
Department of Information Technology, Jaipur Engineering College and Research Centre, India
Email: rohankumartailor.it25@gmail.com

Abstract**—***Wireless networks are an integral part of day-to-day life for many people, with businesses and home users relying on them for connectivity and communication. This scholarly research will examine the security vulnerabilities and threats in wireless communications. The security requirements of wireless networks including their authenticity, confidentiality, integrity, and availability will be identified and summarized. Different research and surveys have been undertaken by academic researchers on the current trend of wireless security from inception to date. These research findings will be analysed, and efficient defense mechanisms and countermeasures will be investigated and provided for improving the security of wireless networks.*

Keywords**—WirelessNetwork,Wireless Security, CIAtriad, WLANs, WEP, WPA, WiMAX, WiGIG.**

I. INTRODUCTION

Wireless networks allow endpoints or devices to connect to the internet without the use of a wire or a cable. They are computer networks that use wireless connections between network devices. Wired technology uses wires or cables to transmit data, communicate with devices and connect to the internet but wireless technology uses radio waves for data transmission. These transmissions could be done in four (4) ways: Radio Frequency Transmission, Infrared Transmission, Microwave Transmission, Light wave Transmission. Wireless networks follow the protocols from the Open Systems Interconnection (OSI) protocol architecture. Ranging from the application layer, presentation layer, session layer, transport layer, network layer, data link layer and physical layer. Each layer of the OSI model has threats and vulnerabilities found in them and the security requirements implemented are independent of each protocol in the layers. Every security measure implemented satisfies the confidentiality, integrity, and availability of the wireless network. The paper aims to ensure that end-users and customers understand the security threats associated with wireless security and identify the countermeasures that are suitable for each threat found in the network.

II. Security Requirements in Wireless Networks

Wireless communication presents unique security challenges due to its open and easily accessible nature. This section elaborates on the primary security requirements essential for protecting wireless data.

2.1 Confidentiality

Confidentiality ensures that sensitive information transmitted over a wireless network is only accessible to authorized users. Encryption is the primary method used to preserve confidentiality. Symmetric encryption algorithms like AES rely on a single key shared between sender and receiver, whereas asymmetric encryption utilizes public and private keys to secure communication. Without proper encryption, wireless data is vulnerable to eavesdropping and data breaches.

2.2 Integrity

Data integrity guarantees that the transmitted information remains unaltered during transit. Any unauthorized modifications to data can lead to misinformation or corrupted files. Integrity is enforced through cryptographic hash functions and digital signatures, which detect changes in data and verify the authenticity of the sender.

2.3 Availability

Availability ensures uninterrupted access to wireless services for authorized users. Denial-of-Service (DoS) and jamming attacks threaten availability by overwhelming the network or blocking access. Ensuring redundancy, implementing load balancing, and utilizing interference detection technologies are essential strategies to maintain network availability.

2.4 Authenticity

Authenticity validates the identity of users and devices within a wireless network. This prevents impersonation attacks such as spoofing. Authentication mechanisms include passwords, biometrics, and digital certificates, often reinforced through multi-factor authentication protocols and TLS encryption at the transport layer.

III. OSI Layers and Security Vulnerabilities

The OSI model provides a structured framework for networking protocols and communication. Each layer has its unique set of protocols and associated vulnerabilities. Understanding these threats allows the development of targeted security measures.

Table 1: OSI Layers and Main Protocols

Layer	***Main Protocols***
Application	*HTTP, FTP, SMTP*
Transport	*TCP, UDP*
Data Link (MAC)	*Ethernet, PPP, IEEE 802.11*
Physical	*Copper, Optical Fiber*

3.1 Physical Layer

This layer is concerned with the transmission of raw data over physical mediums. Threats include eavesdropping, jamming, and hardware tampering. Countermeasures involve physical security controls, spread spectrum communication, and signal encryption.

3.2 Data Link Layer

Responsible for framing, addressing, and error detection, this layer is vulnerable to MAC spoofing and replay attacks. Implementing MAC address filtering, using robust encryption standards like WPA3, and dynamic MAC address randomization help defend against these threats.

3.3 Network Layer

This layer manages data routing and addressing. It is vulnerable to IP spoofing, route hijacking, and packet sniffing. Securing routing protocols with cryptographic authentication and deploying IPsec can mitigate these threats.

3.4 Transport Layer

The transport layer ensures end-to-end communication. Attacks include TCP SYN flooding and session hijacking. TLS/SSL encryption, proper session management, and firewalls are essential countermeasures to secure this layer.

3.5 Application Layer

The highest layer in the OSI model interacts with user applications. Malware, phishing, and data leakage are common risks. Firewalls, antivirus software, and secure coding practices play a key role in securing this layer.

IV. CONCLUSION

To counter vulnerabilities, several wireless security protocols have been developed and deployed over the years.

4.1 Wired Equivalent Privacy (WEP)

WEP was the first wireless security protocol. It uses RC4 encryption but suffers from severe cryptographic weaknesses. Due to its vulnerabilities, WEP is considered obsolete.

4.2 Wi-Fi Protected Access (WPA/WPA2)

WPA was introduced as a quick fix to WEP's flaws and uses TKIP for encryption. WPA2, a more secure successor, employs AES-based encryption and is widely adopted today.

4.3 WPA3

The latest security protocol, WPA3, offers stronger encryption, resistance to brute-force attacks, and individualized encryption for open networks. It also supports forward secrecy.

4.4 Bluetooth Security

Bluetooth networks implement unique device identifiers (BD_ADDR) and use pairing mechanisms to prevent unauthorized access. Protocols like SSP (Secure Simple Pairing) enhance Bluetooth security.

CONCLUSION

This research analysed wireless networks through the lens of the OSI model and identified security vulnerabilities at each layer. Emphasis was placed on the critical security requirements—confidentiality, integrity, availability, and authenticity—that form the foundation for secure wireless communication. The paper also explored widely adopted wireless security protocols and their effectiveness in addressing emerging threats. To ensure robust wireless security, it is crucial to implement layered defense mechanisms, stay updated with the latest cryptographic standards, and adopt proactive network monitoring.

ACKNOWLEDGEMENTS

We extend our sincere thanks to Jaipur Engineering College and Research Centre for providing the infrastructure and environment to pursue this research.

REFERENCES

[1] Abel, V.S. (2011). Survey of Current and Future Trends in Security in Wireless Networks. International Journal of Scientific & Engineering Research, 2(2), 2-7.
[2] Zhou, Y.L., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends. Proceedings of the IEEE, 104(9), 1727-1765. https://doi.org/10.1109/JPROC.2016.2558521
[3] Millar, G., et al. (2020). 5G Security: Current Status and Future Trends. Intelligent Security and Pervasive Trust for 5G and Beyond, 1-101.
[4] Hakeem, A.S.A., Hussein, H.H., &HyungWon, K. (2022). Security Requirements and Challenges of 6G Technologies and Applications. Sensors, 22(5), 1969. https://www.mdpi.com/1424-8220/22/5/1969
[5] Nagarajan, V., Arasan, V., & Huang, D. (2010). Using Power Hopping to Counter MAC Spoof Attacks in WLAN. 2010 7th IEEE Consumer Communications and Networking Conference, 1-5. https://doi.org/10.1109/CCNC.2010.5421588
[6] Ioannou, C., & Vasos, V. (2016). The Impact of Network Layer Attacks in Wireless Sensor Networks. International Workshop on Secure Internet of Things (SIoT), 20-28. https://doi.org/10.1109/SIoT.2016.009
[7] Edvald, S. (2018). A Review of Network Layer and Transport Layer Attacks on Wireless Networks. International Journal of Modern Engineering Research (IJMER), 8(12), 23-27.
[8] Alok, P., &Jatinderkumar, S. (2014). Attacks & Defense Mechanisms for TCP/IP Based Protocols. International Journal of Engineering Innovation & Research, 3(1), 17-23.