Study the attacks in OSI layer of WSN Using MATLA

Varun Slathia
Chandigarh University

***Abstract*—With this study we investigate security vulnerabilities within the Open Systems Interconnection (OSI) layers of wireless sensor networks (WSN) using MATLAB simulations. WSNs have played an important role in a variety of modern applications like environmental supervision or smart city construction. However, they are vulnerable to different levels across their OSI layers. This research is focused on detecting and categorizing attacks such as jamming, spoofing, sinkhole, wormhole and Sybil attacks, at various levels of the OSI layers. The study simulates these attacks using MATLAB and examines their effects on network performance metrics such as throughput, latency and packet delivery ratios. The goal of this research is to provide guidance in creating powerful protective measures for WSN. The fact that this work makes. is the foundation for further research into overall network security. And it provides effective tools for these kinds of attacks.**

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are essential for modern technology--used for things like environmental monitoring, the smart city, industrial automation and health care. They are made up of sensor nodes scattered throughout various places to collect, process and transmit information wirelessly. But despite their benefits, WSNs are susceptible to attacks in different layers of the OSI needs a thorough evaluation of these systems to find potential security vulnerabilities and keep them secure. More devastating is that these attacks can disrupt network operations and threaten data confidentiality. Following is a brief introduction to jamming, spooking, sinkhole, wormhole and Sybil attacks. By means of MATLAB simulations, these attacks and their impacts on network performance can be studied. It enables researchers to have a clearer picture of Vulnerability detection has serious correlation with the physical layer technology as well as network protocol. The purpose of this research is to implement effective security control means in wireless sensor networks where those attacks can be easily detected and defended against and thus that it is to say assured both the dependability of WSNs in general and their efficiency across different Application platforms By studying the paper trying to gain an understanding of practical methods for enhancing security on WSNs.

2. OSI LAYERS

The OSI Model is a conceptual model used to define and standardize the functions of a telecommunication or computing system. Generally; there are seven layers each of which has distinct functions which it performs. The following are the seven layers of the OSI Model:

Physical Layer
This layer transmits raw bit streams over the physical medium-whether cable, radio waves or optical fiber. It consists of the hardware that will intervene with physical medium such transmission speed, modulation techniques. The primary function of this layer is to ensure that the data is transmitted and received accurately and efficiently. This can only be done by converting the data into signals after which it is fed into network cables as raw data is of digital form.

Data link layer:
Collision: An attacker intentionally transmits signals with legitimate nodes simultaneously, resulting in data collisions and packet loss. This can lead to increased effort due to retransmissions and reduced network performance. loss. This can cause network instability and node fatigue. This can make the network more efficient and trustworthy of other nodes.

Network layer:
Sinkhole attack: An attacker disrupts nodes to attract data traffic, thus creating a "cesspool" effect. This allows attackers to intercept, manipulate or destroy data, potentially disrupting the network and causing data loss. Use metrics to control data flow. This will cause delays and interruptions in data transfer. Interception or forwarding of packets based on certain criteria (such as packet content or destination) affects

data transmission and integrity. (DoS) and exploits. This can block legitimate connections and degrade network performance. This can cause communication to fail and require frequent reconnections. This allows them to capture, modify or inject information, leading to information leakage and integrity issues. This can lead to incorrect conclusions, incorrect behavior, and disruption of services that rely on accurate information. Wrong assessments or wrong answers. This could also allow an attacker to gain unauthorized control over the network. Regular maintenance and maintenance can also help identify and mitigate attacks to maintain the integrity and performance of wireless sensor networks. threats.

3. ATTACKS ON THE OSI LAYER

In Wireless Sensor Networks (WSNs), attacks can occur at multiple layers of the Open Systems Interconnect (OSI) model. These attacks can have significant impacts on network performance, data integrity, and security. Below is a detailed description of the types of attacks that can occur at each OSI layer in a WSN:

1. Application Layer
The application layer is the layer closest to the user in the OSI model and supports direct interaction between the user and the applications he uses. One of the threats at this layer is the exploitation of software vulnerabilities. Errors in code implementation allow an attacker to gain unauthorized access or perform malicious actions. Attackers can also exploit this vulnerability to conduct DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks that can cripple a website or server. Some vulnerabilities allow an attacker to gain superuser-level access to the victim.

2. Presentation layer
The presentation layer defines the coding, encryption and compression method for the correct communication of devices. It receives data from the application layer and prepares it to be transmitted by the application layer. Phishing attacks are included in this layer. This is often done through fake websites or emails that appear to be from legitimate sources. The goal is to steal information such as access credentials or credit card information or to install malware on the victim's body.

3.Session Layer
The layer controls the creation, maintenance, and termination of communication sessions (called sessions) between devices. Hijacking is an attack on this process. They exploit vulnerabilities in the communication process or manipulate network connections. Hackers may gain access to unauthorized or sensitive information. Session hijacking includes:

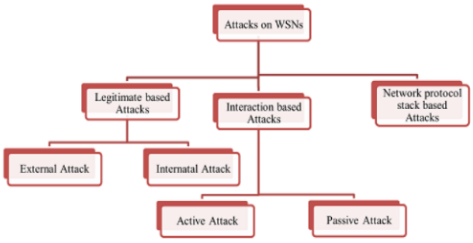
4.Active session hijacking
An attacker can control the active session, interrupt it and change data instantly.

5.Transport Layer
The transport layer provides data flow and error control so that the transmission rate is equal to the receiver's link speed. One of the challenges of this level is exploration. Information on the Internet. This includes port scanning to identify open and inactive ports and packet sniffing to capture and monitor network traffic.

6. Network Layer
The network layer is responsible for packet routing and reassembly. It also finds the best path for packet transmission. Man in the Middle (MITM) attacks feature many of these techniques. communication. The attacker controls the route or uses techniques such as ARP spoofing to trick the target into sending packets to the attacker's device.

7. Data Link Layer
The data link layer establishes and terminates communication between network nodes. Divides data into frames for transmission. Attackers can perform spoofing attacks at this layer. Another network device. This allows attackers to access network resources or intercept and modify traffic. MAC spoofing methods include ARP spoofing, DHCP spoofing, and MAC flooding.

8. Physical layer
The physical layer connects network nodes via wired or wireless means. Sniffing is the antidote to this process. This is done using a packet sniffing tool that captures and decodes data sent over the network. Sniffing can lead to the theft of sensitive information such as login credentials, credit card numbers and personal information.



4. COMPONENTS OF OSI MODEL

There are seven abstraction layers in the OSI model; top layer:

1. Data link layer
3. Network Layer
4. Box Set
5. Session Layer
6. Presentation layer
7. Application Layer

Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the physical connection of the equipment. The physical process involves information in the form of objects. It is responsible for delivering goods from one place to another. When receiving data, this layer takes the received signal and converts it into 0s and 1s and then transmits them to the data link layer, which reassembles the frames.

Function of physical layer

Bit synchronization: The physical layer provides bit synchronization by providing a clock. This pulse controls the transmitter and receiver, ensuring bit phase synchronization. Specify how different devices/nodes are organized in the network (e.g. bus, star or network topology). There are different types of transmission: simplex, half duplex and full duplex. The main function of this layer is to ensure that no data is erroneously sent from one to another by the physical system. When packets reach the network, the DLL is responsible for forwarding them to the host using its MAC address.

The data link layer is divided into two layers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

Packets received from the network layer are further divided into frames based on the frame size of the NIC (Network Interface Card). The DLL also encapsulates the sender and receiver MAC addresses in the headers. Recipient's MAC address, "Who owns this IP address?" It is obtained by sending an ARP (Address Resolution Protocol) request asking: and the target host responds with its MAC address.

Functions of the Data Link Layer

™ Framing: Framing is a function of the Data Link Layer. It provides a way for the sender to send a group of items that will be beneficial to the recipient. This is done by adding a special bit pattern to the beginning and end of the frame. Title of the article. It may be corrupted, so run a check on the amount of information that can be sent before confirmation is received. The amount of time the device has channel management.

Network Layer

The network layer is used to transfer data from one host to another host on a different network. It is also responsible for packet routing, that is, choosing the shortest path to send the packet over the number of available channels. The IP address of the sender and receiver is placed in the header by the network layer.

Working of the Network Layer

Routing: The network layer determines the appropriate route from destination to destination. This network layer process is called routing. The IP address of the sender and receiver is placed in the header by the network layer. It contains a unique and global address that identifies each device. The data transport layer is called segment. It is responsible for the end-to-end delivery of the finished message. The upload process also provides assurance of successful data transfer and resends data if errors are detected. Change the correct information. It also adds the location and port number to its header and sends the segmented data to the network layer.

Presentation Layer

The presentation layer is also known as the interpretation layer. Here, information from the application layer is extracted and processed in the desired format for transmission on the network. Encrypted data is called ciphertext, and decrypted data is called plaintext. The key value is used to encrypt and decrypt data. The application layer is used by web applications. These applications create data to be sent over the network. This process also serves as a window for services to access the network and display the received information to the user.

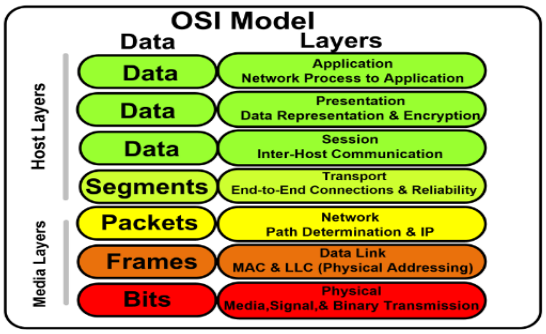
Application layer

The main functions of the application layer are as follows. The program allows users to access data via

remote control, store data on a remote host, and view or control data on a remote computer. : This application provides information distribution and access to international information on various products and services.

Segmentation and Reassembly: This process accepts messages from the session and divides the messages into smaller pieces. Each section created has a title associated with it. The destination station transport layer repeats the message. Therefore, the transport layer ensures that the message is sent to the correct process by specifying this address. Function

Creating, maintaining, and disconnecting: This layer allows two functions to create, maintain, and disconnect connections. point. These synchronization points help identify errors so that data can be copied correctly without prematurely terminating the last message, preventing data loss. Or communicate with each other in full duplex mode.



5. APPLICATIONS OF OSI MODEL

The Open Systems Interconnect (OSI) standard is a seven-layer system for organizing business communications. Although the OSI model is mostly conceptual, its structure has important applications in many communication and communications fields. The use of the OSI model in various situations is as follows:

1. Interoperability and Standardization

Inter-Vendor Compatibility-The OSI model forms the basis for establishing communication technologies and standards between vendors and different systems. This increases interoperability and ensures that hardware and software from different companies can communicate effectively. This promotes international cooperation and relationships.

Layered Approach The OSI model divides network communications into separate processes, allowing experts to discuss individual problems and resolve them in specific procedures. **Debugging and Diagnostic Analysis**: Tools such as Packet Analyzer and Protocol Analyzer analyze traffic across different protocols to identify problems such as collisions, network issues, and incorrect request forms.

Network Design and Planning-The OSI model guides network designers in selecting appropriate technologies and equipment such as switches and data link layer networks, Routing layer router at each layer. Scalability and Flexibility. The OSI model organizes network operations hierarchically, allowing the model to adapt to changes and needs.

Security Layers- The OSI model helps identify vulnerabilities at each layer by providing security such as network layer firewalls and acceleration layer encryption.

Structured Framework-The OSI model provides a framework for designing and developing new network protocols and standards that can be used as frameworks for any system.

Teaching Tools-The OSI model provides a clear and concise framework for teaching communication and networking vocabulary to students and professionals. Better understanding. This model helps students understand communication more easily when learning online.

Application Development-Application developers use the OSI model to enable their software to interact with various network services and layers, such as data processing and management. A framework for managing and troubleshooting network errors. Although most today's networks use the TCP/IP standard as the actual implementation, the content of the OSI model continues to influence the connection model and implementation.

6. CHALLENGES AND LIMITATIONS

Network systems are the basis of modern communications and enable information to flow across large networks. However, these layers do not provide security and protection against threats. In this article, we will examine security problems that may occur at different layers, from the physical layer to the application layer, and discuss strategies to reduce these problems. Physical media delivers raw content and is virtually immune to cyber threats. However, it faces security issues such as:

Headset Interception: Attackers can intercept data by eavesdropping on communication cables or wireless signals. Encryption and physical security measures are crucial to combat this threat. Access control and monitoring are critical to protecting physical assets. Common security issues include:

MAC address spoofing: An attacker can impersonate a legitimate user by spoofing their MAC address, causing permission to be granted. Port security and MAC address filtering help reduce this risk. Using VLANs and configuring port security can improve data link layer security. Security issues of this layer include:

IP spoofing: An attacker can create an IP address to bypass security or perform an attack. Using input and output filtering can help prevent IP spoofing. Complying with security policies and monitoring network connections can reduce these threats. Authors can interact and exchange information between two communicating parties. Accessing and using secure transfer protocols such as TLS/SSL can help prevent these attacks. Implementing speed restrictions and access restrictions can help prevent DoS attacks.
Session, Presentation, and Application Layer Security Issues
The layers of the OSI model manage application communications and are vulnerable to a variety of security issues:
>Session Hijacking: An attacker can impersonate a user by stealing a session ID or cookie to do. Implementing a strong authentication and contact management system is crucial. Regular patching, antivirus solutions and code reviews are crucial for security. Security awareness training and email filtering can help prevent these threats. A comprehensive security strategy includes a combination of physical security measures, encryption, access control, access control, and user education. By addressing security at every level of the network, organizations can increase their ability to prevent harm from cyber threats and ensure the security, integrity, and availability of their information and services.

7. FUTURE DIRECTION OF SAFETY IN OSI LAYER

Many ideas and new technologies can be leveraged to improve security across the OSI model layer and protect the network from cyber-attacks. Here are some future applications for securing each layer of the OSI model:
Protect physical network elements. Rules and secure communication methods, such as WPA3, to protect wireless networks
Advanced Filtering Implement advanced MAC address filtering and access control to prevent spoofing. Define your network (SDN) to isolate traffic and reduce your downtime
IPsec-Implement Internet Protocol Security (IPsec) to encrypt and secure communications at the IP layer. Deep packet inspection and application-level network filtering.

TLS-Use the latest version of Transport Layer Security (TLS 1.3) to improve encryption and security during data transfer. **: Use DDoS mitigation programs and technologies to prevent large-scale attacks on network services.
Strong Authentication- Implement Strong Multi-Factor Authentication (MFA) for security initiation and management. It is used to encrypt communications and chats.

Data Encryption- Ensure that data is encrypted when the presentation layer is created (for example, during compression or formatting for transfer). Hashing is an algorithm used to verify data integrity and detect fraud. Secure Coding-Use secure coding techniques such as access validation and code inspection to prevent vulnerabilities. A programmatic firewall (WAF) to filter malicious traffic and prevent SQL injection and cross-site scripting (XSS). > In addition to the above, holistic measures across all layers of the OSI model include:

Zero Trust Architecture- Adopting a Zero Trust Policy that authenticates all requests regardless of their history, improving security.
Continuous monitoring-Use real-time monitoring tools, security intelligence, and event management (SIEM) to quickly respond to threats. (AI) makes searching, responding, and predicting more efficient. Thanks to the policies and technologies in the OSI system, organizations can create strong defenses against cyber-attacks and effectively protect their networks.

8. CONCLUSION

In summary, using MATLAB to analyze attacks at the Wireless Sensor Network (WSN) OSI layer provides a better understanding of vulnerabilities and risks at each layer. This approach allows researchers to simulate, measure, and analyze different attacks and their effects on WSNs. MATLAB's powerful simulation and analysis tools can identify vulnerabilities in the network and develop strategies to counter these threats. Since WSNs are still an essential part of many applications, protecting them across all OSI layers is crucial to ensuring their reliability, integrity, and robustness. This research not only improves the security of wireless sensor networks, but also provides important insights into the protection of other network architectures in different contexts.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener.Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[3] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005, June, pp. 719–724.

[4] A. Bagula, M. Zennaro, G. Inggs, S. Scott, and D. Gascon, "Ubiquitous Sensor Networking for Development (USN4D): An Application to Pollution Monitoring," Sensors, vol. 12, no. 1, pp. 391–414, Jan. 2012.

[5] J. Jeong and Z. J. Haas, "An integrated security framework for open wireless networking architecture," IEEE Wireless Communications, vol. 14, no. 2, pp. 10–18, 2007.

[6] X. Guo and J. Zhu, "Research on security issues in Wireless Sensor Networks," in 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011, vol. 2, pp. 636–639.

[7] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, p. 53, Jun. 2004.

[8] Ma, Y., Richards, M., Ghanem, M., Guo, Y., Hassard, J.: Air Pollution Monitoring and Mining Based on Sensor Grid in London. Sensors 8, 3601–3623 (2008).

[9] Zhao, Y., Shouzhi, X., Shuibao, Z., Xiaomei, Y.: Distributed detection in landslide prediction based on Wireless Sensor Networks. In: Proceedings of World Automation Congress, Puerto Vallarta, Mexico, June 24-28, pp. 235–238 (2012).

[10] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cabiric, E.: Wireless Sensor Networks: A Survey. Computer Networks 38, 393–422 (2002).

[11] Istepanian, R., Jovanov, E., Zhang, Y.: Guest editorial introduction to the special section on M-Health: Beyond seamless mobility and global wireless Health-Care connectivity. IEEE Trans. Inf. Technol. Biomed. 8, 405–414 (2004)

[12] Milenkovic, A., Otto, C., Jovanov, E.: Wireless sensor network for personal health monitoring: Issues and an implementation. Comput. Commun. 29, 2521–2533 (2006).

[13] Junnila, S., Kailanto, H., Merilahti, J., Vainio, A.-M., Vehkaoja, A., Zakrzewski, M., Hyttinen, J.: Wireless, Multipurpose In-Home Health Monitoring Platform: Two Case Trials. IEEE Trans. Inf. Technol. Biomed. 14, 447–455 (2010).

[14] Bachmann, C., Ashouei, M., Pop, V., Vidojkovic, M., Groot, H.D., Gyselinckx, B.: Low-power wireless sensor nodes for ubiquitous long-term biomedical signal monitoring. IEEE Commun. Mag. 50, 20–27 (2012).

[15] Han, K., Shon, T., Kim, K.: Efficient mobile sensor authentication in smart home and WPAN. IEEE Trans. Consum. Electr. 56, 591–596 (2010).[9] Byun, J., Jeon, B., Noh, J., Kim, Y., Park, S.: An intelligent self-adjusting sensor for smart home services based on ZigBee communications. IEEE Trans. Consum. Electr. 58, 591–596 (2012).

[16] Nakamura, M., Igaki, H., Yoshimura, Y., Ikegami, K.: Considering Online Feature Interaction Detection and Resolution for Integrated Services in Home Network System. In: Proceedings of the 10th International Conference on Feature

Interactions in Telecommunications and Software Systems, Lisbon, Portugal, June 11-12, pp. 191–206 (2009).

[17] Shakhov, Vladimir V. "Protecting wireless sensor networks from energy exhausting attacks." In International Conference on Computational Science and Its Applications, pp. 184-193. Springer, Berlin, Heidelberg, 2013.