ASEAN Journal of Science and Engineering Education

Journal homepage: http://ejournal.upi.edu/index.php/AJSEE/

Securing Wireless Sensor Networks, Types of Attacks, and Detection/Prevention Techniques, An Educational Perspective

Tuka Kareem Jebur

Department of Accounting College of Management and Economics, Al-Mustansiriyah University, Iraq
Correspondence: E-mail: tukakareem@uomustansiriyah.edu.iq

ABSTRACT

Wireless sensor networks (WSNs) are gaining popularity in a variety of applications, including smart homes, industrial facilities, and environmental monitoring systems. However, using WSNs exposes them to a variety of attacks that might have major effects, such as data loss, privacy breaches, and safety issues. As a result, understanding the sorts of threats and detection/prevention strategies in WSNs is critical to ensuring their security, especially from an educational perspective. We present an overview of the sorts of attacks that can occur in WSNs, including denial of service attacks, spoofing attacks, jamming attacks, physical assaults, and node compromise attacks. We also examine encryption, authentication and authorization procedures, intrusion detection systems, and physical security measures as methods for detecting and blocking attacks in WSNs. We examine the benefits and drawbacks of each strategy and give case studies to show their efficacy. Finally, we propose future research directions, such as the development of more effective intrusion detection systems and the enhancement of physical security measures. We can assure the security and reliability of WSNs in diverse applications by knowing the types of attacks and detection/prevention mechanisms.

ARTICLE INFO

Article History:
Submitted/Received 18 Feb 2023
First Revised 16 Mar 2023
Accepted 14 May 2023
First Available online 15 May 2023
Publication Date 01 Mar 2024

Keyword:
Authentication,
Authorization,
Detection techniques,
Cryptography,
Intrusion detection systems,
Physical security,
Prevention measures,
Security,
Wireless sensor networks (WANs).

1. INTRODUCTION

Wireless sensor networks (WSNs) are becoming more used in a variety of areas, such as environmental monitoring, healthcare, and security. However, the implementation of WSNs raises security difficulties since these networks are vulnerable to a variety of assaults. Understanding the different types of attacks and detection/prevention mechanisms is critical for guaranteeing WSN security and dependability.

This article review paper will go through several forms of attacks in WSNs, detection and mitigation approaches, case studies, and prospective future research topics. Wireless Sensor Networks (WSNs) have grown in popularity and application in recent years as a result of their capacity to monitor and gather data from physical surroundings with high precision and dependability. WSNs are made up of a large number of tiny, low-cost, and energy-efficient sensors that interact wirelessly with one another to accomplish a specified activity such as environmental monitoring, home automation, and industrial automation. WSN sensors may be utilized in a range of conditions, including harsh and distant areas where wired networks are difficult to construct and operate (Subramani *et al*., 2022). WSNs are important because they may enable real-time data monitoring, efficient resource management, and greater situational awareness.

However, the deployment of WSNs brings many security difficulties, making it critical to understand the types of attacks as well as their detection and mitigation measures to assure the dependability and security of WSNs. Understanding the many sorts of attacks that might occur in wireless sensor networks is critical to maintaining their security and dependability. WSNs are vulnerable to a variety of assaults, including DoS attacks, spoofing attacks, jamming attacks, physical attacks, and node compromise attempts. These attacks have the potential to jeopardize the security, integrity, and availability of data gathered and sent by network sensors, resulting in catastrophic repercussions such as data tampering, theft, or loss, and unauthorized access (Evangelakos *et al*., 2022).

Furthermore, because WSNs are frequently installed in distant and hostile areas, the cost of repairing or replacing damaged sensors can be substantial. Understanding the many sorts of assaults that can occur in WSNs, as well as their prevention and detection procedures, is crucial to assuring the security and stability of these networks and averting possible security breaches or cyber-attacks. The topic of forms of assaults in wireless sensor networks will be the focus of this article review paper. It will begin by discussing the significance of wireless sensor networks and the need of recognizing different forms of assaults in these networks.

The article will then explore and present instances of several sorts of attacks in wireless sensor networks, such as Denial of Service (DoS) attacks, spoofing attacks, Jamming attacks, Physical assaults, and Node compromise attacks. The paper will then explain the advantages and limitations of various techniques for detecting and preventing attacks in wireless sensor networks, such as cryptography, authentication and authorization mechanisms, intrusion detection systems, and physical security measures (Nengroo *et al*., 2022).

Finally, the paper will summarize the key points of the article review, highlight the necessity of understanding different types of assaults and detection/prevention approaches in wireless sensor networks, and recommend prospective future study fields.

2. METHODS

This study is a literature survey, in which data was obtained from Internet sources, especially articles in international journals. Data were collected, reviewed, and summarized to build this argument in this paper.

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

3. RESULTS AND DISCUSSION

3.1 Types of Attacks in Wireless Sensor Networks

There are several attacks on WSNs:

(i) A Denial of Service (DoS): this is a form of attack that aims to disrupt the availability of a wireless sensor network by flooding it with a significant volume of data, leaving it unable to offer the services intended. DoS attacks can be carried out by flooding the network with packets, exploiting network weaknesses, or delivering faked packets that use network resources (Ahmad *et al*., 2022). For example, in the DoS attack, flooding the network with a high number of packets or continually pinging a device to use its resources. A successful DoS attack can cause the network to become unavailable or sluggish, resulting in data transmission delays or the inability to receive data. This has the potential to create major interruptions in network functioning, impacting its performance and dependability. Spoofing attack: An attacker impersonates a genuine node or device to obtain network access.

(ii) Spoofing attacks: this is a sort of attack that attempts to determine the validity of data in a wireless sensor network. In this attack, an attacker attempts to mimic a genuine node or device to obtain network access, modify data, or inflict network damage. Spoofing attacks may be carried out using a variety of ways, including MAC address spoofing and IP address spoofing. Authentication and authorization systems such as Public Key Infrastructure (PKI) or digital certificates can be used to prevent and detect spoofing attacks and ensure that only authenticated nodes can access the network. A successful Spoofing attack can result in unauthorized network access, data tampering, or data theft, possibly jeopardizing the confidentiality and integrity of sensor data gathered and delivered. Jamming attack: An attacker sends a high-powered signal across the same frequency range as the sensors, generating interference and rendering communication between the sensors impossible.

(iii) Jamming attacks: they are a sort of attack that aims to disrupt the availability of a wireless sensor network by jamming or obstructing wireless signals between network nodes. In this assault, the attacker broadcasts a high-powered signal across the same frequency range as the sensors, generating interference and rendering communication between the sensors impossible. Various approaches, like frequency hopping, spread spectrum, and directional antennas, can be employed to avoid and detect jamming attempts (Lăzăroiu *et al*., 2022). A successful Jamming attack can cause the network to become unavailable, resulting in data transmission delays or the inability to receive data. This has the potential to create severe interruptions in network functioning, impacting its performance and dependability. Physical attack: For example, tampering with or stealing network sensors.

(iv) Physical attacks: they are a form of attack that targets the wireless sensor network's physical security. In this assault, the attacker physically damages or destroys the sensors, either by tampering with them or stealing them. Physical assaults can be difficult to prevent and detect because attackers might employ a variety of ways to circumvent physical security measures. Physical security measures such as tamper-evident seals, intrusion detection systems, and video monitoring can thus be used to reduce the danger of physical attacks. A successful physical attack can compromise or destroy the network, resulting in data loss, network outage, and higher costs for repairs or replacement of damaged sensors. Tampering with or stealing network sensors are examples of these attacks. The impact of a successful physical assault is that it can

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

corrupt or destroy the network, resulting in data loss, network outages, and greater maintenance or replacement costs for damaged sensors (Akram *et al*., 2022).

(v) Node compromise attacks: they are a form of attack that compromises the nodes of a wireless sensor network to jeopardize its integrity. The attacker gets unauthorized access to a sensor or device and manipulates the data gathered or communicated by the sensor in this attack. Node compromise attacks may be carried out using a variety of approaches, including malware injection, remote code execution, and buffer overflow attacks. Various measures, including encryption, access control mechanisms, and intrusion detection systems, can be used to prevent and detect node compromise attacks (Temene *et al*., 2022).

3.2 Detection and Prevention of Attacks

Cryptography, Authentication and authorization procedures, Intrusion detection systems, and other approaches are used to identify and prevent assaults in wireless sensor networks, Physical security measures (Hrovatin *et al*., 2022):

(i) Cryptography: is the activity of encrypting data delivered over a network to secure communication. To protect the data gathered and communicated by the sensors, cryptographic techniques such as symmetric key cryptography, public key cryptography, and hash functions can be utilized. Cryptography may also be used to secure key exchange and to construct secure communication channels between network nodes.

(ii) Authentication and authorization techniques: To guarantee that only authenticated nodes may access the network, authentication, and authorization mechanisms such as Public Key Infrastructure (PKI) or digital certificates can be installed. Access control techniques can also be used to restrict network access to critical places. These measures aid in preventing unwanted network access, lowering the danger of Spoofing and Node Compromise attacks (Khalaf *et al*., 2022).

(iii) Intrusion detection systems (IDS): can be used to identify abnormal network behavior such as Denial of Service (DoS) assaults, Node Compromise attacks, and Jamming attacks. IDSs can identify these assaults by analyzing network traffic and monitoring network node activity. When an attack is identified, IDSs can warn the network administrator, allowing them to take prompt action to prevent the assault from spreading (Ouni and Saleem, 2022).

(iv) Physical security measures: such as tamper-evident seals, intrusion detection systems, and video monitoring, can be used to reduce the danger of physical attacks. These techniques can aid in the detection and deterrence of physical attacks, lowering the likelihood of the network being penetrated or destroyed (Gulati *et al*., 2022).

In general, a combination of these strategies can provide multilayer security against assaults in wireless sensor networks. The probability of a successful attack may be considerably decreased by installing several security mechanisms, therefore ensuring the confidentiality, integrity, and availability of the data received and delivered by the network's sensors.

3.3 The advantages and limitations of each technique

There are several points in advantages and limitations (Majid *et al*., 2022):

(i) Cryptography: Advantages: By encrypting data transported across the network, it provides a high level of data security. Aids in the establishment of secure communication channels between network nodes. Protects against data manipulation and illegal data access. Limitations: It is possible that the sensors' computational

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

overhead may rise, lowering their processing power and battery life. The implementation may need extra hardware and software resources. Can be prone to assaults such as side-channel attacks, in which attackers exploit flaws in the cryptographic algorithm's implementation.

(ii) Mechanisms for authentication and authorization: Advantages: Ensures that only authenticated nodes may access the network, resulting in a high level of network security (Hrovatin *et al*., 2022). Aids in the prevention of illegal network access, lowering the danger of Spoofing and Node Compromise attacks. Allows the network administrator to restrict network access to critical regions. Limitations: The network's complexity may rise, making it more difficult to administer and maintain. The implementation may need extra hardware and software resources. Can be subject to assaults such as brute-force attacks, in which attackers attempt to guess a network node's authentication credentials.

(iii) Intrusion detection system: Advantages: By identifying aberrant network activity, it provides a high level of network security (Lakshmanna *et al*., 2022). It can aid in the detection of attacks such as Denial of Service (DoS), Node Compromise, and Jamming. When an attack is discovered, the network administrator is notified, allowing them to take prompt action to prevent the assault from spreading. Limitations: False positives may occur, resulting in unwarranted alarms and network interruptions. The implementation may need large processing power and storage capacity. It may necessitate ongoing monitoring and maintenance to be successful.

(iv) Physical security measures: Advantages: By detecting and repelling physical attacks, it provides a high level of physical security (Lilhore *et al*., 2022). Aids in the prevention of assaults such as theft and manipulation with network sensors. It can be beneficial in situations where other security measures are ineffective. Limitations: It may be costly to implement and maintain. It may not be effective against non-physical assaults. To develop and implement properly, extensive skills may be required (Ganesh, 2022).

While each approach has advantages and disadvantages, a combination of these strategies can provide layered security against assaults in wireless sensor networks. The probability of a successful attack may be considerably decreased by installing several security mechanisms, therefore ensuring the confidentiality, integrity, and availability of the data received and delivered by the network's sensors.

3.4 Case Studies

A few example studies demonstrating the sorts of attacks and detection/prevention strategies previously discussed:

(i) case 1: Jamming attack on a wireless sensor network case study. A jamming assault was conducted against a wireless sensor network placed in an industrial plant in this case study. The attack led the sensors to lose contact with the base station, causing the data-collecting process to be disrupted. To avoid such attacks, the network included a frequency hopping system that enabled sensors to move between multiple frequency channels in the event of interference. The frequency hopping method proved effective in keeping the network from being disrupted by the jamming attempt, allowing the sensors to continue transmitting data. The frequency hopping mechanism has proven to be an efficient method for mitigating jamming assaults on the wireless sensor network. The network was able to evade the attacker's interference by moving between multiple frequency channels, allowing the sensors to continue transmitting data.

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

(ii) Case 2: A wireless sensor network node breach attack. An attacker penetrated a node in a wireless sensor network established in a smart home in this case study. The hacked node was exploited to execute a DDoS assault against a web server housed on the same network. To avoid such assaults, the network was outfitted with an intrusion detection system that monitored network traffic for unusual activities. The intrusion detection system noticed the suspicious traffic generated by the compromised node and notified the network administrator, who took measures to isolate the node and stop the attack from spreading. strategy effectiveness: The intrusion detection system was demonstrated to be an effective strategy for identifying and blocking wireless sensor network node compromise assaults. The system detected the unusual traffic created by the infected node and alerted the network administrator, allowing them to take fast action to prevent the attack from spreading.

(iii) Case 3: Physical Assault on a wireless sensor network case study. An attacker got physical access to a wireless sensor network established in a warehouse in this case study. The attacker interfered with the network's sensors, leading them to send incorrect data to the base station. The network was outfitted with physical security features such as locks, alarms, and surveillance cameras to prevent such assaults. The physical protection measures spotted the intruder and informed security professionals, who apprehended the perpetrator before substantial network damage occurred. Physical security measures were shown to be an effective strategy for preventing physical assaults on the wireless sensor network. The techniques helped to maintain the integrity of the data captured and relayed by the network's sensors by identifying and preventing physical assaults.

4. CONCLUSION

Finally, this article review paper covered the many sorts of assaults that may occur in wireless sensor networks, such as denial of service attacks, spoofing attacks, jamming attacks, physical attacks, and node compromise attacks. The potential network impact of these assaults has also been discussed. The research also looked at encryption, authentication and authorization processes, intrusion detection systems, and physical security measures for detecting and blocking assaults in wireless sensor networks. Each technique's benefits and drawbacks have been examined. Case studies were provided to show the sorts of assaults and detection/prevention measures outlined previously, and their success was evaluated. Because wireless sensor networks are rapidly being utilized in applications such as smart homes, industrial facilities, and environmental monitoring systems, it is critical to understand the types of attacks and detection/prevention approaches.

A successful assault on a wireless sensor network can have major ramifications, such as data loss, privacy violations, and safety risks. Future research might involve the creation of more complex intrusion detection systems capable of detecting sophisticated assaults, the enhancement of physical security measures, and the investigation of novel cryptographic methods for safeguarding data in wireless sensor networks.

5. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

6. REFERENCES

Ahmad, R., Wazirali, R., and Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors, 22*(13), 1-5.

Akram, J., Munawar, H. S., Kouzani, A. Z., and Mahmud, M. P. (2022). Using adaptive sensors for optimised target coverage in wireless sensor networks. *Sensors, 22*(3), 1-23.

Evangelakos, E. A., Kandris, D., Rountos, D., Tselikis, G., and Anastasiadis, E. (2022). Energy sustainability in wireless sensor networks: An analytical survey. *Journal of Low Power Electronics and Applications, 12*(4), 1- 65.

Ganesh, D. E. (2022). Analysis of wireless sensor networks through secure routing protocols using directed diffusion methods. *International Journal of Wireless Network Security, 7*(1), 28-35.

Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., and Saravanan, G. (2022). A review paper on wireless sensor network techniques in internet of things (IoT). *Materials Today: Proceedings, 51*, 161-165.

Hrovatin, N., Tošić, A., Mrissa, M., and Kavšek, B. (2022). Privacy-preserving data mining on blockchain-based WSNs. *Applied Sciences, 12*(11), 1-18.

Khalaf, O. I., Romero, C. A. T., Hassan, S., and Iqbal, M. T. (2022). Mitigating hotspot issues in heterogeneous wireless sensor networks. *Journal of Sensors, 2022*, 1-14.

Lakshmanna, K., Subramani, N., Alotaibi, Y., Alghamdi, S., Khalafand, O. I., and Nanda, A. K. (2022). Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks. *Sustainability, 14*(13), 1-19.

Lăzăroiu, G., Andronie, M., Iatagan, M., Geamănu, M., Ștefănescu, R., and Dijmărescu, I. (2022). Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things. *ISPRS International Journal of Geo-Information, 11*(5), 1-26.

Lilhore, U. K., Khalaf, O. I., Simaiya, S., Tavera Romero, C. A., Abdulsahib, G. M., and Kumar, D. (2022). A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks*. International Journal of Distributed Sensor Networks, 18*(9), 1-16.

Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., and Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors, 22*(6), 1-36.

Nengroo, S. H., Jin, H., and Lee, S. (2022). Management of distributed renewable energy resources with the help of a wireless sensor network. *Applied Sciences, 12*(14), 1-25.

Ouni, R., and Saleem, K. (2022). Framework for sustainable wireless sensor network based environmental monitoring. *Sustainability, 14*(14), 1-26.

Subramani, N., Mohan, P., Alotaibi, Y., Alghamdi, S., and Khalaf, O. I. (2022). An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks. *Sensors, 22*(2), 1-16.

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815

Temene, N., Sergiou, C., Georgiou, C., and Vassiliou, V. (2022). A survey on mobility in wireless sensor networks. *Ad Hoc Networks, 125*, 1-5.

DOI: https://doi.org/10.17509/ajsee.v4i1.57431
p- ISSN 2775-6793 e- ISSN 2775-6815