International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 09 – Issue 04 || Jul - Aug 2024 || PP. 99-107

An Overview on Wireless Sensor Network Security and Challenge

Mohsin Raad Kareem
Computer science
Collage of Basic Education, University of Mustansiriyah
Baghdad, Iraq

Abstract: A wireless sensor network (WSN) consists of small, low-powered communication devices often deployed in hostile environments. Due to their limited resources, security becomes crucial and challenging, especially with the emergence of various attacks targeting these networks. These randomly deployed nodes are susceptible to attacks like selective forwarding and flooding, which directly impact network performance and compromise network security. in this paper, an over view about the essential, component, application's, security requirements, and attacks of WSN.

Keywords: wireless sensor network (WSN), WSNs attacks, Denial-of-Service (Dos).

1. Introduction

Wireless sensor networks (WSN) have been identified as among the most significant emerging technologies of the past century and serve as the foundation for the Internet of Things paradigm (Ávila et al., 2022a). Their importance is rapidly expanding, with their increasing ubiquity making them indispensable in modern life. The demand for wireless communication services and infrastructure has surged in recent times (Kumar & Kumar, 2023). reflecting the growing necessity for such technologies. WSNs encompass a collection of self-guiding sensors monitoring various parameters such as pressure, vibration, temperature, and sound, demonstrating their versatility and applicability across different domains (Verma & Jha, 2021a).

These networks comprise numerous low-power, multi-functional sensor nodes deployed to monitor diverse physical or environmental phenomena, often operating in challenging and remote environments without access to a renewable energy source. Despite their wide range of applications, including disaster management, military reconnaissance, and security surveillance (Ahutu & El-Ocla, 2020). WSNs face significant challenges, particularly in terms of security. The limited resources available to WSNs, such as processing power, memory, and battery backup, pose obstacles to implementing robust security measures (Ahmad et al., 2021a).

One of the primary security concerns in WSNs is the susceptibility to various threats, including denial-of-service attacks facilitated by the nature of sensor nodes. One significant threat is the wormhole attack, where malicious sensor nodes use low-latency links to disrupt the network's routing paths. This attack is particularly dangerous because it can bypass many cryptographic defenses and is difficult to detect within the network (Kumar & Kumar, 2023).

In essence, while WSNs offer immense potential for various applications, their inherent limitations and vulnerabilities necessitate robust security measures to safeguard against potential threats and ensure the reliability and integrity of data transmission (Hanif et al., 2022).

2. Wireless Sensor Networks

A Wireless Sensor Network (WSN) consists of a collection of sensor nodes distributed across various locations and interconnected through wireless communication. As illustrated in Figure 1, a sensor node, or mote, is an electronic device comprising a processor, a storage unit, a transceiver module, one or more sensors, an analog-to-digital converter (ADC), and a power source, typically a battery. Additionally, it may include a positioning unit and/or a mobilization unit (Kandris et al., 2020).

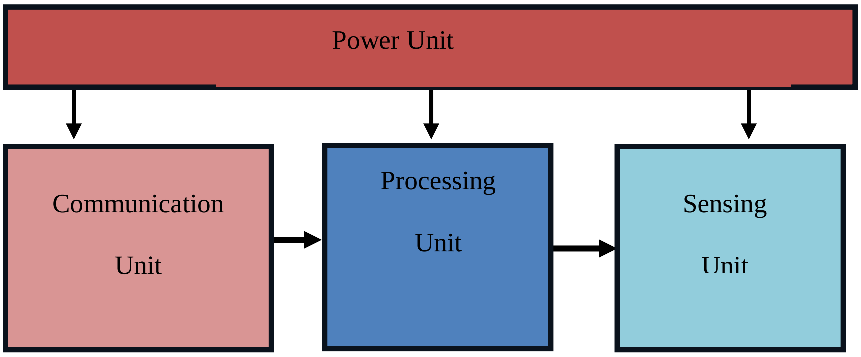

Figure1 The typical architecture of a sensor node used in (WSNs).

A sensor node utilizes its sensors to detect changes in surrounding environment. These measurements are transferred into electrical signals by the ADC unit and processed by the node's processor. The node's transceiver then wirelessly transmits the processed data to another nodes or a designated sink point, known as the BS (Base Station). As shown in Fig 2, the BS uses the transmitted information to supervise and control the wireless sensor network (WSN) and relay the data to other networks or human users (Kandris et al., 2020).

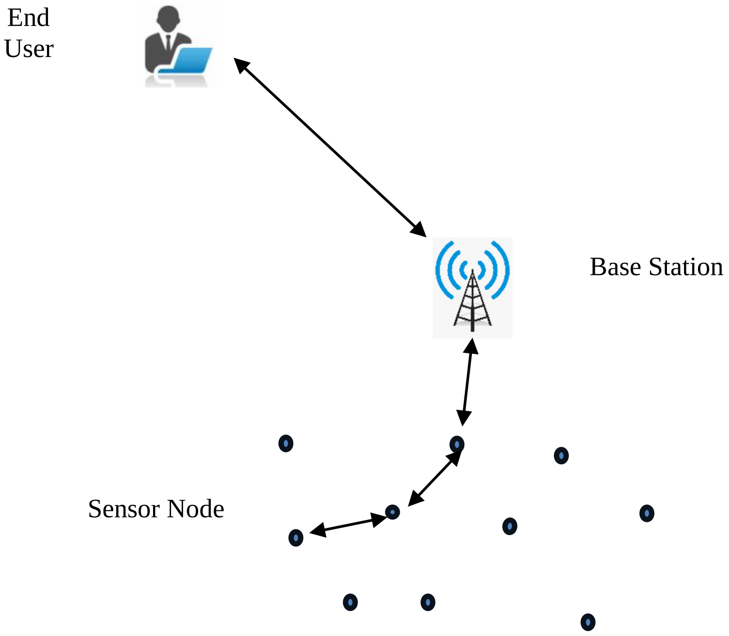

Figure 2 architecture of a Wireless Sensor Network.

The combined use of a appropriate number of such sensor nodes allows a Wireless Sensor Network to simultaneously acquire ambient information from multiple points of interest across wide areas. Continuous technological advancements have made it possible to produce these relatively small yet highly advanced sensor nodes at a low cost. As a result, although WSNs were at first developed primarily towards military applications, its now supporting an increasingly diverse domain of uses (Kandris et al., 2020).

3. Applications of wireless sensor networks

A variety of uses of WSNs are either already widely used or still in the early stages of development. In this paper, WSN applications are categorized into six main groups based on their usage: military, health, environmental, flora and fauna, industrial, and urban, as shown in Figure 3. Each category encompasses several subcategories (Garg et al., 2023b). This section explains the nature of each category and subcategory, and provides illustrative examples to highlight their specific features, benefits, and challenges.

Furthermore, the various methodologies and technical approaches employed in these applications for processing and sensing purposes are discussed, highlighting their differences and similarities

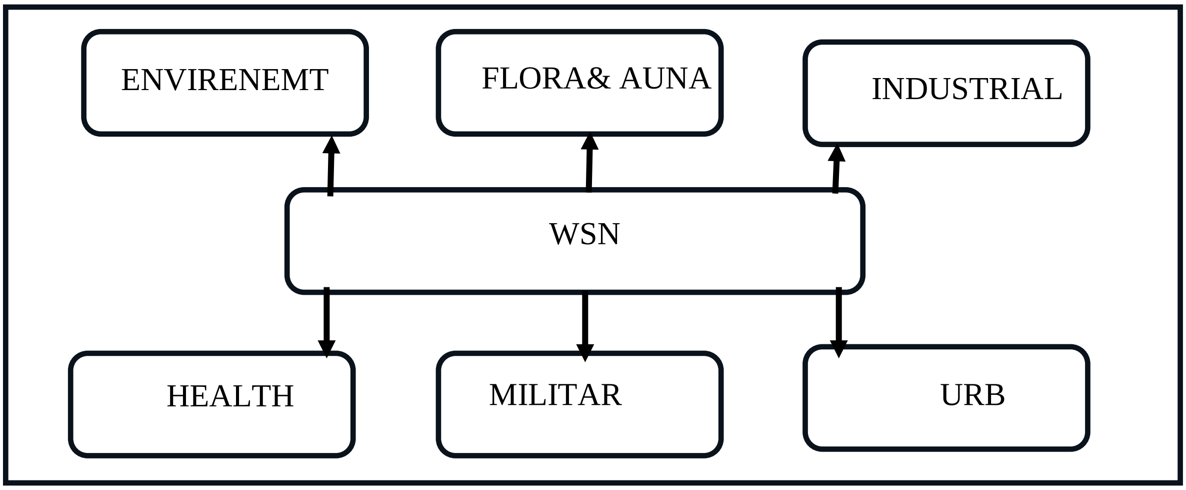

Figure 3. popular types of applications in WSNs.

3.1 Environmental applications

The utilization of WSNs can significantly enhance the continuous monitoring of ambient conditions in hostile and remote areas. The primary subtypes of environmental applications for WSNair monitoring, emergency alerting, and water monitoring are illustrated, including the types of sensors commonly used in each. These environmental applications of WSNs are explored in detail in the following subsection(Garg et al., 2023a).

3.2 Flora and Fauna Applications

The domains are vital for every country. The primary sub types of WSN application in these areas green house monitoring, crop monitoring, and livestock farming are depicted, including the types of sensors commonly used in each.

3.3 Industrial Applications

Wireless Sensor Networks can be utilized in various industrial applications to address numerous related challenges. The main subcategories of industrial WSN applications logistics, robotics, and machinery health monitoring is illustrated. These specific application categories are examined in detail in the remainder of this subsection.

3.4 Military Applications

The military domain was not only the first field to utilize WSNs but also played a pivotal role in initiating sensor network research. A notable example of these early research efforts is Smart Dust, developed in the late 1990s. This project aimed to create sensor nodes that, despite their size, could effectively perform surveillance activities (Kumar & Kumar, 2023).

3.5 Health Applications

WSN utilize sophisticated medical sensors to monitor patients in healthcare facilities, for instance hospitals, as well as in home settings. They offer real-time monitoring of patients' vital signs through wearable devices. The primary subcategories of health applications for WSNs patient monitoring, hospital patient monitoring, and home assisting systems are outlined, along with the types of sensors typically employed in each. (Premkumar et al., 2023).

3.6 Urban Applications

The diverse sensing capabilities of WSNs offer an unparalleled opportunity to gather detailed information about any target area, whether it's a room, a building, or an outdoor space. WSNs enable the measurement of spatial and temporal characteristics of various phenomena within an urban environment, leading to a vast array of applications. The most popular urban applications of WSNs include smart cities, smart homes, and structural health monitoring, transportation systems (Ávila et al., 2022a).

4. Security Requirements for Wireless Sensor Networks

Wireless sensor networks (WSNs) face special security challenges because they lack wires, have limited resources, and operate in difficult environments with critical tasks. Securing WSNs is more complex than securing other networks for these reasons. WSNs need to meet the same basic security requirements as other networks: confidentiality, integrity, authentication, and availability (known as the CIAA triad). On top of that, WSNs have unique security requirements to protect them from attacks and malfunctions.

4.1 Confidentiality

Is the cornerstone of network security, shielding data from prying eyes. It guarantees that only authorized recipients can access messages, keeping them secret from anyone else. This protection extends to preventing attackers from passively analyzing network traffic or modifying data in transit. Encryption is a key tool for achieving confidentiality, scrambling information into an unreadable format until it reaches its intended destination (Garg et al., 2023b).

4.2 Integrity

Maintaining data integrity is paramount for ensuring the trustworthiness of data packets in WSNs. It guarantees that data remains unaltered during transmission, protecting it from unauthorized modifications (additions, deletions, or corruptions) introduced by malicious nodes or channel noise (Verma & Jha, 2021a).

4.3 Authentication

In WSNs, verifying the authenticity of data is essential for ensuring message reliability. This process allows each communicating node to confirm the origin of data and mutually authenticate each other's identities. Authentication is crucial to prevent security threats such as packet injection, spoofing, and dissemination of misleading routing information. However, the inherent resource limitations of sensor nodes and the absence of wired communication channels pose significant challenges to implementing robust authentication mechanisms in WSNs (Aliady & Al-Ahmadi, 2019a).

4.4 Availability

Availability is a critical aspect of sensor networks, influencing various aspects of their operation. It determines if a node can utilize resources when required, if services and data are accessible on-demand, and if network is consistently available for communication even in the face of malicious attacks. The unavailability can have severe consequences, potentially opening backdoors for malicious invasions and rendering sensed information useless or less valuable. However, ensuring availability can also impact network lifetime, particularly when dealing with limited energy resources (Ahmad et al., 2021).

5. Attacks in Wireless Sensor Networks

Wireless sensor networks (WSNs) are vulnerable to two main categories of attacks: passive and active. Passive Attacks attacks aim to eavesdrop on communication flowing through the network without interrupting it. The attacker remains hidden and undetected while listening and collecting data. This stolen information can be used later to launch more aggressive attacks. On the other hand, Active Attacks, In contrast to passive attacks, active attacks directly disrupt the normal operation of the WSN. Attackers may modify or fabricate data, inject false information streams, or intercept communication altogether. Their goal is to cause harm to the network, such as damaging its functionality or preventing it from collecting accurate data. Active attacks are generally more aggressive than passive attacks (Hanif et al., 2022; Heydarishahreza et al., 2020). Some of the most known attacks in WSNs include:

5.1 Jamming attack

Tacking advantage of the wireless medium's vulnerability to interference, jamming attacks cause a DoS in the network. Attackers locate the radio frequencies used by the targeted wireless sensor network (WSN) and try to disrupt or block communications by emitting signals (unnecessary information) on those same frequencies. This interference hinders communication (message transmission and/or reception) between nodes (Amish & Vaghela, 2016). interference can be intermittent, permanent, or temporary, impacting part or all of the network depend on the jamming source's radio range, which can be as powerful as the network nodes themselves. Jamming can take various forms: it could be targeting, constant and corrupting data packets in transit; deceptive, sending a continuous data stream into a network; random, dispersing injected data streams over time; or reactive, sending a jamming signal in response to detected traffic (Kardi & Zagrouba, 2019a).

5.2 Tampering or destruction

Wireless sensor networks (WSNs) are vulnerable to physical attacks since they are often deployed in Harsh and unprotected environment. Tampering attack involves physically capturing a node to extract cryptographic material, such as stored program code and encryption keys. This information can be used to launch other attacks, like altering routing information, will create duplicate data packets, or tampere with routing services. The attacker might also manipulate the captured node by installing new code to induce unusually behavior, thereby disrupting the network (Ávila et al., 2022b).

5.3 Continuous Channel Access (Exhaustion)

This type of attack falls under Denial of Service (DoS) attacks, aiming to deplete the batteries of nodes and reduce the network's lifespan. This attack targets the Media Access Control (MAC) protocol, the network's traffic coordinator. The attacker floods the network with useless data packets and makes excessive requests for data transmission. This disrupts the normal flow of communication and forces legitimate nodes to waste energy on retransmitting packets that get lost in the chaos.

A potential defense against this attack is to implement rate limiting at the MAC layer's admission control. This mechanism can identify and ignore corrupted packets and excessive requests originating from malicious sources, helping to maintain order in the network(Heydarishahreza et al., 2020).

5.4 Collision attack

Similar to continuous channel attacks, collision attacks aim to disrupt communication within the network. Malicious nodes intentionally transmit packets at specific times to create collisions. These collisions scramble data packets, rendering them unusable and forcing legitimate nodes to resend them. This repeated retransmission process wastes valuable energy and delays communication significantly. This not only affects throughput but also wastes energy and causes data loss. Collision attacks are challenging to detect in WSNs because they are short-duration attacks using malicious packets that resemble legitimate ones.

Researchers have proposed several collision detection techniques to address this issue, such as error-correcting codes (Kandris et al., 2020).

5.5 Unfairness attack

A form of Denial-of-Service (Dos) attack can cause marginal performance degradation by significantly reducing the utility and efficiency of services. This attack, derived from other attacks like collision and exhaustion, involves attackers continuously requesting access to the channel, thereby undermining communication and limiting channel capacity.

One countermeasure to such attacks is time-division multiplexing, which allocates specific time slots for each node to transmit, preventing continuous access requests from a single node.

5.6 Interrogation

Interrogation attacks target a vulnerability in the handshake process used by the Media Access Control (MAC) protocol. This handshake, known as RTS/CTS, helps prevent collisions caused by hidden nodes (nodes that are out of each other's direct radio range). Attackers exploit this mechanism by repeatedly sending RTS (Request to Send) packets. Nearby nodes, tricked by the attacker, respond with CTS (Clear to Send) messages. This excessive back-and-forth exchange wastes valuable battery power in the responding nodes.

To defend against interrogation attacks, nodes can implement security measures like anti-replay protection and link layer authentication. These techniques help to identify and ignore illegitimate RTS packets, stopping the attacker from draining energy reserves (Kandris et al., 2020).

5.7 Sybil Attack

This attack allows malicious nodes to assume multiple identities, using the identities of legitimate nodes targeted by the attack. This enables the malicious nodes to participate in distributed algorithms, such as elections, exploiting legitimate nodes and endorsing the creation of multiple routes passing through the malicious node. Occurring between the link and network layers, this attack aims to compromise data integrity, security, and resource utilization.

Data aggregation attacks aim to falsify aggregated messages, while voting attacks affect routing paths and node selection. Various research efforts have sought to counter the Sybil attack using mechanisms such as public key cryptography and digital signatures (Aliady & Al-Ahmadi, 2019b).

5.8 Sinkhole attack

Sinkhole attacks are a type of Denial-of-Service (DoS) attack specifically designed to wreak havoc on Wireless Sensor Networks (WSNs). In this attack, a malicious node poses as a highly desirable route for data transmission. By appearing to be the "fastest way" to the destination, the attacker lures a large volume of data packets towards itself.

Once a significant amount of data is flowing through the attacker, it acts like a black hole. It absorbs the data packets but prevents them from reaching their intended destination. This manipulation disrupts the network's routing service and creates a bottleneck, hindering the overall functionality of the WSN.

To make the attack even more damaging, the attacker often targets strategically located nodes within the network. This allows them to control a larger portion of the data flow and inflict more significant disruption(Kumar & Kumar, 2023).

5.9 Hello Flood

A form of Denial-of-Service (DoS), disrupts Wireless Sensor Networks (WSNs) by exploiting routing protocols. In this attack, a malicious node acts like a siren song, broadcasting fake routing information that makes it appear as the most desirable path for data transmission. This "Hello" message flood attracts a large volume of data packets towards the attacker.

Once a significant amount of data is flowing, the attacker transforms into a black hole. It intercepts the data packets but prevents them from reaching their intended destination, effectively creating a well of lost information. This manipulation disrupts the network's routing service and creates a bottleneck, hindering the overall functionality of the WSN.

To maximize damage, attackers often target strategically located nodes within the network. This allows them to control a larger portion of the data flow and inflict more significant disruption.

fortunately, geo-routing protocols offer a layer of defense against Hello Flood attacks. These protocols rely on localized information, such as the physical location of nodes, to determine the best route for data transmission. By taking location into account, geo-routing protocols make it more difficult for attackers to disguise themselves as optimal routes. This helps maintain the integrity of the network's routing service and prevents attackers from manipulating data flow (Verma & Jha, 2021b).

5.10 Selective Forwarding

Is a form of attack where nodes in a network fail to relay packets as expected by the routing protocol. In this attack, a malicious node may selectively forward packets, either by dropping some incoming packets randomly (neglectful node) or by prioritizing its own messages over others (greedy node).

To defend against Selective Forwarding attacks, strategies such as routing braided paths, multipath, and the random selection of paths to the destination can be used. These techniques help ensure that even if some nodes are malicious, the overall reliability and efficiency of the network are maintained (Ávila et al., 2022b).

5.11 Black Hole Attack

A dangerous threat to Wireless Sensor Networks (WSNs). They fall under the category of selective forwarding attacks, where a malicious node acts like a data vacuum cleaner. The attack unfolds in two stages Infiltration and Deception, in Infiltration, The attacker either inserts a new malicious node into the network or compromises an existing one. in Deception, The compromised node broadcasts false routing information, portraying itself as the shortest and most desirable path to the destination (often a sink or base station). This entices neighboring nodes to update their routing tables and send data through the attacker.

However, the malicious node doesn't forward the data packets. Instead, it discards them, creating a "black hole" where information disappears. This disrupts the network's routing service and can lead to Packet Loss, Resource Exhaustion, and Network Partitioning. These attacks are particularly damaging when targeted at strategically located nodes, such as aggregator nodes in hierarchical networks.

There are ways to defend against Black Hole attacks. One effective strategy is to implement multi-path routing. This approach allows nodes to choose from several alternative routes when sending data. If one path leads to a black hole, the network can reroute traffic through another path, bypassing the compromised node. This redundancy helps maintain network functionality and data flow (Kardi & Zagrouba, 2019).

5.12 Wormhole Attacks

Wormhole attacks, also known as tunneling attacks, are a serious threat to Wireless Sensor Networks (WSNs). They require a coordinated effort by at least two malicious nodes. These attackers establish a high-speed, private connection – like a tunnel – between themselves, often using a powerful wired or radio link (Amish & Vaghela, 2016).

Wormhole attacks exploit hidden tunnels to manipulate data flow in a network. These tunnels rely on two malicious nodes working together. One way they achieve this is through encapsulation:

Multi-hop Encapsulation, This technique conceals the intermediate nodes between the attackers. Data packets are wrapped in new packages as they travel through multiple hops within the tunnel, making it appear like the malicious node is a legitimate neighbor. This deception can trick routing protocols that rely on hop count (number of hops) to choose the shortest path. Attackers can exploit this to create sinkholes, attracting and dropping data packets (Tamilarasi & Santhi, 2020a).

Direct Communication, Alternatively, attackers can use a high-bandwidth link to create a "shortcut" tunnel between themselves. This direct connection allows for incredibly fast data transfer (often a single hop). This technique can bypass protocols that rely on the first discovered path or prioritize the fastest path (based on latency).Both encapsulation methods disrupt routing protocols and enable attackers to manipulate data flow within the network. (Verma & Jha, 2021b).

5.13 Flooding

Attacks aim to disrupt a network by overwhelming it with data. Attackers bombard the network with a massive number of connection requests or continuous data streams. This overload consumes resources like memory and bandwidth, making it impossible for legitimate users to connect. Flooding attacks essentially shut down the network by denying service (DoS) to everyone.

The attackers can come from one or more locations, and they typically keep bombarding the network until resources are depleted or a pre-set limit is reached (Kardi & Zagrouba, 2019b).

To show the effect of these attacks on WSNs in OSI model. In Physical Layer (PL), Data Link Layer (DLL), Network Layer (NL), Transport Layer (TL), Application Layer (AL) As indicated in Table1(Kardi & Zagrouba, 2019).

Table 1 show the effects of attack on OSI layer.

	PL	DLL	NL	TL	AL
Jamming attack	*	*	*		
Tampering or destruction	*				
Continuous Channel Access (Exhaustion)		*			
Collision attack		*			
Unfairness attack		*			
Interrogation		*			
Sybil Attack		*	*		
Sinkhole attack			*		
Hello Flood			*		
Selective Forwarding			*		
Black Hole Attack			*		
Wormhole Attacks			*		
Flooding				*	

6. Summary

This research provides an overview of the characteristics and limitations and attacks of WSNs. It employs a Systematic Literature Review to identify previous studies that have helped uncover the main issues in WSNs. while WSNs offer immense potential for various applications, their inherent limitations and vulnerabilities necessitate robust security measures to safeguard against potential threats. Ensuring the reliability and integrity of data transmission is crucial for the continued expansion and success of WSNs in modern life.

References

[1]. Ahmad, B., Jian, W., Enam, R. N., & Abbas, A. (2021a). Classification of DoS Attacks in Smart Underwater Wireless Sensor Network. *Wireless Personal Communications*, *116*(2), 1055–1069. https://doi.org/10.1007/s11277-019-06765-5

[2]. Ahutu, O. R., & El-Ocla, H. (2020). Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks. *IEEE Access*, *8*, 63270–63282. https://doi.org/10.1109/ACCESS.2020.2983438

[3]. Aliady, W. A., & Al-Ahmadi, S. A. (2019a). Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE Access*, *7*, 84132–84141. https://doi.org/10.1109/ACCESS.2019.2924283

[4]. Amish, P., & Vaghela, V. B. (2016). Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol. *Procedia Computer Science*, *79*, 700–707. https://doi.org/10.1016/j.procs.2016.03.092

[5]. Anand, C., & Vasuki, N. (2021). Trust Based DoS Attack Detection in Wireless Sensor Networks for Reliable Data Transmission. *Wireless Personal Communications*, *121*(4), 2911–2926. https://doi.org/10.1007/s11277-021-08855-9

[6]. Ávila, K., Sanmartin, P., Jabba, D., & Gómez, J. (2022b). An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN. *Wireless Personal Communications*, *122*(4), 3687–3718. https://doi.org/10.1007/s11277-021-09107-6

[7]. Bai, S., Liu, Y., Li, Z., & Bai, X. (2019). Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures. *Computer Networks*, *150*, 190–200. https://doi.org/10.1016/j.comnet.2019.01.008

[8]. Bhosale, S. A., & Sonavane, S. S. (2022). Wormhole Attack Detection System for IoT Network: A Hybrid Approach. In *Wireless Personal Communications* (Vol. 124, Issue 2, pp. 1081–1108). Springer. https://doi.org/10.1007/s11277-021-09395-y

[9]. Garg, R., Gulati, T., & Kumar, S. (2023a). Range free localization in WSN against wormhole attack using Farkas' Lemma. *Wireless Networks*, *29*(5), 2029–2043. https://doi.org/10.1007/s11276-023-03279-8

[10]. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models. *Alexandria Engineering Journal*, *82*, 82–100. https://doi.org/10.1016/j.aej.2023.09.064

[11]. Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks. In *Electronics (Switzerland)* (Vol. 11, Issue 15). MDPI. https://doi.org/10.3390/electronics11152324

[12]. Heydarishahreza, N., Ebadollahi, S., Vahidnia, R., & Dian, F. J. (2020). Wireless Sensor Networks Fundamentals: A Review. *11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, IEMCON 2020*, 791–796. https://doi.org/10.1109/IEMCON51383.2020.9284873

[13]. Hua, J., Zhou, Z., & Zhong, S. (2021). Flow Misleading: Worm-Hole Attack in Software-Defined Networking via Building In-Band Covert Channel. *IEEE Transactions on Information Forensics and Security*, *16*, 1029–1043. https://doi.org/10.1109/TIFS.2020.3013093

[14]. Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. In *Applied System Innovation* (Vol. 3, Issue 1, pp. 1–24). MDPI AG. https://doi.org/10.3390/asi3010014

[15]. Kardi, A., & Zagrouba, R. (2019a). Attacks classification and security mechanisms in Wireless Sensor Networks. *Advances in Science, Technology and Engineering Systems*, *4*(6), 229–243. https://doi.org/10.25046/aj040630

[16]. Kardi, A., & Zagrouba, R. (2019b). Attacks classification and security mechanisms in Wireless Sensor Networks. *Advances in Science, Technology and Engineering Systems*, *4*(6), 229–243. https://doi.org/10.25046/aj040630

[17]. Kumar, Y., & Kumar, V. (2023). A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. In *Wireless Personal Communications* (Vol. 133, Issue 1, pp. 395–452). Springer. https://doi.org/10.1007/s11277-023-10773-x

[18]. Luo, X., Chen, Y., Li, M., Luo, Q., Xue, K., Liu, S., & Chen, L. (2019). CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack. *IEEE Access*, *7*, 18194–18205. https://doi.org/10.1109/ACCESS.2019.2894637

[19]. Premkumar, M., Ashokkumar, S. R., Jeevanantham, V., Mohanbabu, G., & AnuPallavi, S. (2023). Scalable and Energy Efficient Cluster Based Anomaly Detection against Denial of Service Attacks in Wireless Sensor Networks. *Wireless Personal Communications*, *129*(4), 2669–2691. https://doi.org/10.1007/s11277-023-10252-3

[20]. Raghu, R., Roshan Zameer, S., Suhailkhan, F., & Kumar, V. (n.d.). *Detection of Wormhole Attack in WSN Using Hybrid Approach*. http://jscglobal.org/

[21]. Saini, P. K., Singh, A., & Sohal, J. S. (2023). Proactive Prevention Key Solution for Wormhole Attack in IEEE 802.11 Networks Using AODV. *Wireless Personal Communications*, *128*(1), 89–108. https://doi.org/10.1007/s11277-022-09942-1

[22]. Tamilarasi, N., & Santhi, S. G. (2020b). Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network. *Wireless Personal Communications*, *114*(1), 329–345. https://doi.org/10.1007/s11277-020-07365-4

[23]. Teng, Z., Du, C., Li, M., Zhang, H., & Zhu, W. (2022). A Wormhole Attack Detection Algorithm Integrated With the Node Trust Optimization Model in WSNs. *IEEE Sensors Journal*, *22*(7), 7361–7370. https://doi.org/10.1109/JSEN.2022.3152841

[24]. Thangaiyan, J., Mani, G., Nivedhitha, V., Pradeep, N. S., Jayasankar, T., & Vinoth Kumar, K. (2020). Reliable Wormhole Detection System Based Secure Routing and Authentication for Environmental Monitoring. In *Journal of Green Engineering* (Vol. 10, Issue 3). https://www.researchgate.net/publication/353752336