Security Vulnerabilities and Attack Classification in Wireless Sensor Networks

Jyoti Bhati[1], Vikram Singh Chouhan[2], Dr. Manoj Kuri[3]

[1,2,3] Engineering College Bikaner

bhatijs.12@gmail.com

vikksecb@gmail.com

kuri.manoj@gmail.com

Submitted: 05/12/2025 **Revised:** 18/12/2025 **Published:** 28/12/2025

Abstract

Wireless Sensor Networks (WSNs) have emerged as a transformative technology with applications spanning military, healthcare, environmental monitoring, and smart infrastructure. However, their resource-constrained nature—limited energy, computation, and memory—makes them particularly vulnerable to security threats. This paper provides a systematic classification of attacks targeting WSNs, detailing their mechanisms, impacts, and relevance to network security requirements. We also discuss the inherent restrictions of WSNs and outline essential security countermeasures. This survey aims to serve as a reference for researchers and practitioners in designing robust, attack-resilient WSN architectures.

Keywords*:* Wireless Sensor Networks, Network Security, Attack Taxonomy, Resource Constraints, Security Protocols, Intrusion Detection

1. Introduction

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous sensors that monitor environmental or physical conditions and cooperatively transmit data to central locations [1]. Their low cost, scalability, and flexibility have enabled deployment in diverse domains, from battlefield surveillance to climate monitoring [3]. Despite their advantages, WSNs face significant security challenges due to limited node resources, unattended operations, and dynamic topologies [2]. This paper surveys the security landscape of WSNs, classifying attacks and analyzing their implications on network integrity, availability, and confidentiality.

2. Constraints and Design Challenges in WSNs

WSNs differ fundamentally from traditional networks in several aspects:

- **Resource Limitations:** Sensor nodes have restricted energy, memory, and processing capabilities.
- **Dynamic Topology:** Networks are self-organizing with no predefined structure.
- **Unreliable Communication:** Wireless channels are prone to interference and loss.
- **Large-Scale Deployment:** Networks may comprise thousands of nodes.
- **Centralized Data Flow:** All data converges toward base stations or sinks. These constraints necessitate lightweight, energy-efficient security solutions tailored for WSNs [4][5].

3. WSN Security Requirements

Due to hostile nature of WSNs, various security mechanisms are required that ensure secure data transmission between the nodes and protect against various attacks and intrusions. Hence, the requirements of a WSN are circumscribing both the typical network requirements and the unique requirements appropriate intended for wireless sensor networks.

3.1 Data Confidentiality

Confidentiality is a security mechanisms to prevent unauthorized disclosure of data. A sensor network should not leak sensor readings to its surrounding networks, when nodes communicated highly sensitive data [19]. The standard approach to keeping data secret is by encrypting the sensor data.

3.2Data Integrity

However, after achieving a certain level of confidentiality, an adversary may be unable to steal the information, but it does not symbolize that the data is safe. An adversary is still capable to change the data. Data integrity ensures that the received data has not tempered or manipulated in transit.

3.3Data Freshness

It suggests that the data is recent and it verifies that no old messages have been replayed. In this case, it is easy to obstruct the normal working of the sensor by the adversary to use a replay attack [11].

3.4Availability

Availability in WSN guarantees that services, resources and information are accessible to authorized users when requested. This means a reliable service will be provided by the networks, by ensuring that data is delivered to the intended destination, even during the instance of attack threat [24].

3.5Self-Organization

Self-organization is the property in which the sensor nodes must have to organize themselves to form the network. A self-organized sensor network can be clustered or grouped into an easily manageable network. Self-organization is critical for a WSN, due to the large number of nodes, and to the fact that these nodes may be spread over a remote area [41].

3.6Time-Synchronization

Time-synchronization in wireless sensor networks is extremely important for basic communication, but it also provides the ability to detect movement, location and proximity. Time-synchronization does not necessarily mean that all clocks are perfectly matched across the network, hence, precise clock synchronization is not always essential.

3.7Secure Localization

This is the property of sensor network to be able to accurately and automatically locate each sensor node in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. An attacker can easily manipulate location information of a non secured network by reporting false signal strengths, replaying signal, etc [12].

3.8 Authentication

A dynamic user authentication allows the genuine user to query the sensor data any one of the sensor data from any one of the sensor. An intruder is not only modify the data packet, but also change the whole packet stream by infusing additional packets. So receiver have to ensure the data originates from the correct source. In two entity communication, both entities have to share a common secret key to calculate Message Authentication Code (MAC) of all communicated data [29].

4.Attacks

Wireless Sensor Networks are vulnerable and sensitive to various types of security attacks that trigger the communication. Another serious reason is the deployment of sensor nodes in dangerous environments like the battlefield. These reasons lead to a variety of security threat and attacks in wireless sensor networks.

4.1HELLO Flood Attack

The HELLO flooding attack is related to the network layer attack, which targets the routing protocols. The protocol requires the nodes used for communicating the HELLO packets for reporting to the neighbours that they are existing. It can be caused by a node which broadcasts a HELLO packet with very high power, so that a large number of nodes even far away in the network choose it as the parent node. all messages now need to be routed multi-hop to this parent, which increases delay. By this, sensor nodes are convinced that the attacker node is neighbor and respond to the HELLO message, that eventually waste their energy. The identity verification protocol can be used to authenticate and raise the alarm if an attacker attempts to become a neighbor node, preventing this attack. The packet leash mechanism is also used when this attack is detected in the network layer [8].

4.2Denial of Service (DoS) Attack

A Denial of Service is an attempt to make a node or complete network unavailable to legitimate users. This attack is considered as a threat to a computer network. The aim of a DoS attack is completely depend on the adversary, but, in general, it targets to block some services from functioning efficiently either for sometime or permanently. Generally, a DoS attack saturates the sensor node by excessive communication requests and due to this, the targeted nodes cannot respond to the legitimate users or responds with delay that degraded the effectiveness. It may occupy all the resources by obstructing its communication path to the targeted node. The DoS attack can be identified or detected easily by decay in network performance, few nodes become unavailable and loss or delay of packets and their acknowledgement.

4.3Replay Attack

It is a type of Denial of Service (DoS) attack. In replay attack, the adversary captures the packets communicated within the network and re-transmits them at a later time to the node to be attacked resulting in huge wastage of energy of node under attack. This may lead to network partitioning due to exhaustion of energy of the node under replay attack. This attack aims to fool the MAC receiver by forwarding the replayed packet to the following sensor network node and then persuade the destination node to take in the replayed packet as original or authorized packet. Replay attacks can be accomplished by manipulating packet contents like hide header information and impersonate the original source or without change any packet information, re-transmit it in a different time frame.

4.4Jamming

Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. In WSN, jamming can be defined as an attack which interfere in radio frequencies used by network nodes. Jamming attack can be categorized as a special case of Denial of Service attack. It also includes interfering with the sensing abilities of the motes. It may be done by an external source or by a compromised node. This attack may take place at all the layers of protocol stack. The constant jammer emits continually a radio signal. A deceptive jammer sends a constant stream of regular packets in the channel, without leaving any gap between them. The random jammer alternates between jamming and go to sleep. And reactive jammer maximizes its lifespan [14].

4.5Node Replication Attack

It is also known as clone attack. It is an application independent security threat, where sensor nodes will be directly operated by the adversary in the network. The captured node is supposed to be original or legitimate sensor node. In the node replication attack, an adversary first captures the node, then, reproduce it by using its secret information like codes, identity and cryptographic details, and place the node back to the network. The adversary is then able to monitor the whole network and induce various types of attacks in the network. Detection of such types of captured nodes are even harder because there nodes are served as a legitimate sensor node before and there is no difference between these nodes. Mobility of a sensor node introduces additional complexity to detect node replication or clone attack in WSN [28].

4.6Black-Hole Attack

In this type of attack, the attacker drops packet selectively, or all control and data packets that are routed through it. Therefore, any packet routed through this intermediate malicious node will suffer from partial or total data loss. A malicious node uses its routing technique to be able to promote itself for having the quickest direction to the place node or to the bundle it wants to identify. It then denies to forward all the data to its desired destination. It is a passive attack. There are two types of black hole attack. First, single black hole node, in which an adversary captures only one sensor node to introduce the black hole attack. Secondly, collaborative black hole attack, in which more than two node collectively perform black hole attack [27].

4.7Sybil Attack

In this type of attacks, a malicious node masquerades as more than on node, by asserting more that one identity to the network, hence, enlarges the size of a network. An attacker may generate any number of additional node identities, by using only one physical node. Sybil attack can be imposed by various methods. When a legitimate node sends a message to a node, one of the adversary node listen to the message. In this method, a malicious node directly communicates with sybil node. But in another, there may be no direct communication between both of them. An adversary may place fabricated node with random identity or stole the identity from pre-existing node, after their battery drainage or identity theft [15,16].

4.8Sink Hole Attack

It id considered as an insider attack, in which an adversary compromises a node from the network. Then, the compromised node advertises itself to attract all the traffic from neighboring nodes, on the basis of various routing parameters that are commonly used by routing protocols. The communication pattern of a WSN is many to one communication, where each sensor node collect the information and transmit it to the base station, framed the WSN vulnerable to the sink hole attack. Remaining battery power is the key characteristic by which an adversary advertises itself to attract all the communication traffic through it. The main challenge to detect sink hole attack is the unpredictable nature of the node's authenticity [8].

4.9Grey-Hole Attack

It is an advanced transformation of black hole attack. Both of them are a common type of attack in wireless sensor networks. Malicious nodes may constantly or randomly drop packets and therefore, reduce the efficiency of the networking system. A Grey-Hole may exhibit its malicious behavior in multiple ways. Another type of Grey-Hole attack is a node behaves malicious for some particular time duration by dropping packets but may switch to normal behavior later or it may receive packets of certain packet ID and forward the other packets. This random behavior of the node to drop some packets while forwarding other packets, makes its detection even more difficult [33].

4.10Worm Hole Attack

In WSN, a node determines its neighbor by the process called neighbor discovery process. Once communication is established between nodes, a link is then formed to transmit the packet in a single hop distance. As in WSN, a single node transmission range is limited, hence, cannot transmit packets to a long distance. Thus, single hop transmission process is repeated until packets arrived at its destination. An adversary can attack by acting like a real neighbor to the source and destination, and create a low latency link between the malicious nodes, for a falsely packet transmission. A series of such attacks cause huge impact on the sensor network is called worm hole attack. One of the reason for this attack is to disrupt the neighbor discovery mechanism [31].

34.11Exhaustion Attack

The mobile and remote nature of the sensor and the possibility of their functioning in an autonomous mode as well as the constraints on available battery resources has led the devices to be vulnerable to energy resources exhaustion attack. The complexity of an ERE attack detection is determined, first, by the fact that often the effect on the node is implicit and second, to keep track of ERE attacks, it is not necessary to only analyze the discharging speed change also. The detection of ERE attacks may be determined by independent aspects of energy resource discharge due to legal software and clients.

4.12 Acknowledgement Spoofing

Routing algorithm of WSN mainly rely on implicit or explicit link layer acknowledgement. An adversary can spoof link layer acknowledgements for overhead packets addressed to neighboring nodes due to the inherent broadcast medium. Protocols that choose the next hop based on reliability issues is susceptible packets being lost when travel along such links. The goal includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. Acknowledgement spoofing attacks can be prevented by proper authentication for communication and using good encryption techniques.

4.13 Homing Attack

Homing attack determines the special node with some responsibilities like cluster head, getaway or sink and focusing completely on them. Once a cluster head or sink is captured, an intruder easily imposes jamming attacks or destroy the network nodes or even complete network. Intruders investigate the network traffic to understand the geographical area of cluster heads or base station. There are two common approaches to protect against Homing Attack. The first method is based on header encryption to hide sensor node placement from adversary. In the second method, sensor nodes use dummy packets to mislead intruders.

4.14 Sniffing Attack

In this type of attack, a malicious node is placed in the vicinity of the sensor grid to take over the data. The adversary transfers all the collected sensor readings by means of subsidiary apportion. An outside adversary launches this attack to collect certain pieces of data from legitimate sensor node. This vulnerability derives WSN unsafe as shared medium. Sniffing attack can be prevented by means of proper encryption techniques for communication. It is also quite hard to detect such type of attacks. The sniffer node does not affect the network performance nor its lifetime. It eavesdrops the sent packet by looking for any valuable information. This attack is vulnerable in the case of sensitive data applications like military based services [18].

4.15 Energy Drain Attack

It can be defined as transmission and composition of messages that lead to more energy consumption by the network than honest node transmitted a message of same size to the same destination by using different packet header. It is also known as vampire attack. These types of attacks do not depend upon any protocol, design property of implementation failures of particular routing protocols, but rather they exploit simple properties of property classes like distance vector, link state, geographic and beacon routing and source routing. These attacks try to drain largest part of energy by transmitting as little data as possible, preventing rate limiting solution. These attacks are difficult to detect or prevent because adversary use protocol compliant messages [30].

4.16 White Washing Attack

This is a type of attack in which a malicious node tries to re-enter the network with a new identifier and a new reputation. The attack takes place when the system successfully detects a malicious node and isolates it from the network, then this malicious node tries to re-join the network with a new identifier to delude the system and have a new trust value.

4.17 Node Outage Attack

In this attack, the functionality of the wireless sensor components like sensor nodes or communication link or parent node, such as reading or sensing, gathering information and launching the functions, are completely stopped. Hence, the communication to other clustered nodes in different areas is interrupted by applying physical or logical attacks in networks. The time protocols are designed in such a way that they provide packets with an alternate routing path. The attack is belong to modification model the availability and authenticity are main threats for this attack in networks.

4.18 Intelligent Attack

In this attack, the adversary plays smart enough to get the threshold of malicious behavior value. If the adversary get its trust value is near the threshold of the malicious behavior, then it behave normally so that it can gain its trust value again. Once it improves in its trust value, it is ready to re-attack the network again. This type of attack is harder to detect and may require a lot of time and efforts, because adversary plays intelligent as both legitimate and malicious according to the requirements.

4.19 Stealthy Attack

In stealthy packet dropping, the attacker achieves the objective of disrupting the packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious node gives impression to its neighbors participating in local monitoring that it has performed the required action. This class of attacks is applicable to packets that are neither acknowledged end-to-end nor hop-to-hop. Due to the resource constraints of bandwidth and energy, much traffic in multi-hop ad hoc wireless networks is unacknowledged or selectively acknowledged.

4.20 Neglect and Greed Attack

This is an active type of attack in which it affects the route of the transmission. The affected node selects the longest route to transmit the packets to the wrong node. The key objective of this attack is to target the information loss and availability of the node in the network. The malicious node receives the packet and refuses to forward them to other node in their proximity from the same network. Detection of malicious node and better authentication can help to avoid this attack.

4.21 Garnished Attack

In this type of attack, the malicious node plays smart enough to behave both good and bad to intentionally target for remaining undetected. The behavior of the malicious node varies based on time or features. In this type of attack, in the group of malicious nodes, one node drops the received packets for a specific time period, while before and after that time stamp, it completely behaves normal with respect to send and receive. Whereas, another node with multi-model senses more than one feature such as temperature, humidity, pressure and brightness. It forwards all data packets for all features except any particular above mentioned features, or forward corrupted information. This behavior of the node purposefully leads to remain undetected as much as possible.

4.22 Bad Mouthing Attack

It has been demonstrated that rating trust and reputation of individual nodes is an effective approach in distributed environments in order to improve security, support decision-making and promote node collaboration. Nevertheless, these systems are vulnerable to deliberate false or unfair testimonies. In this scenario, the attackers collude to give negative feedback on the victim in order to lower or destroy its reputation. This attack is known as bad mouthing attack, and it can significantly get worse the performance of the network [41].

4.23 Good Mouthing Attack

In this attack, intruders try to mislead the base station or the cluster head by sending positive reputation value of bad nodes. This attack is the contradictory of bad mouthing attack. In this type of attack, any malicious node (A) announces positive reputation of another malicious node (B). The purpose of this attack is to dominate the network traffic, to break down the entire network [41].

5 Conclusion

As sensor network have their tremendous uses in many crucial application in real world, improve their importance and give a promising reason to investigate about their security. As the sensor network and their node has various constraints about resources, battery, calculations and transmission range; it encounters with various attacks that cannot be avoided. The purpose of this paper is to listed down various attacks to sensor networks and illustrate all the current attacks on network. In addition, the paper also describe about the features which are affected by particular attack. Many of these attacks target node performance, remaining battery power, power consumption rate, lost packets, freshness of the route and message, and network traffic, which leads to the degrade of the overall network performance. In future, we plan to explore various trust models, detection and prevention techniques for sensor network to avoid the numerous attacks discussed in this paper.

References

[1] Wireless Sensor Network. (n.d.). In *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/WirelessSensorNetworks.

[2] Estrin, D., Govindan, R., Heidemann, J., & Kumar, S. (1999). Next century challenges: Scalable coordination in sensor networks. *USC/Information Sciences Institute*.

[3] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422.

[4] Chandel, A., Chouhan, V. S., & Vyas, D. (2019). A survey on architecture and protocols for wireless sensor networks. *Advances in Information Communication Technology and Computing*, 127–141.

[5] Chandel, A., Chouhan, V. S., & Sharma, S. (2019). A survey on routing protocols for wireless sensor networks. *Advances in Information Communication Technology and Computing*, 143–164.

[6] Hu, F., & Sharma, N. K. (2005). Security considerations in ad hoc sensor networks. *Ad Hoc Networks*, 69–89.

[7] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, 47(6), 53–57.

[8] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *IEEE International Workshop on Sensor Network Protocols and Applications*.

[9] Culler, D. E., & Hong, W. (2004). Wireless sensor networks. *Communications of the ACM*, 47(6), 30–33.

[10] Turakulovich, K. Z., & Tokhirovich, S. L. (2019). Analysis of security protocols in wireless sensor networks. *International Conference on Information Science and Communications Technologies (ICISCT)*, 1–4.

[11] Zhu, S., Setia, S., Jajodia, S., & Ning, P. (2004). An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. *IEEE Symposium on Security and Privacy*, 259–271.

[12] Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *IEEE Wireless Communications*, 11(6), 38–43.

[13] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534.

[14] Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer*, 35(10), 54–62.

[15] Douceur, J. R. (2002). The Sybil attack. *1st International Workshop on Peer-to-Peer Systems.

[16] Newsome, J. (2002). The Sybil attack in sensor networks: Analysis and defenses. *IEEE International Conference on Information Processing in Sensor Networks*.

[17] Przydatek, B., Song, D., & Perrig, A. (2003). SIA: Secure information aggregation in sensor networks. *ACM International Conference on Embedded Networked Sensor Systems*, 255–265.

[18] Ukil, A. (2010). Security and privacy in wireless sensor networks. *Smart Wireless Sensor Networks*.

[19] Ghormare, S., & Sahare, V. (2015). Implementation of data confidentiality for providing high security in wireless sensor network. *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*.

[20] Li, Z., & Gong, G. (2008). A survey on security in wireless sensor networks. *University of Waterloo, Canada*.

[21] Du, X., & Chen, H. H. (2008). Security in wireless sensor networks. *IEEE Wireless Communications*, 15(4), 60–66.

[22] Hu, L., & Evans, D. (2003). Secure aggregation for wireless networks. *International Symposium on Applications and the Internet Workshops*.

[23] Hartung, C., Balasalle, J., & Han, R. (2004). Node compromise in sensor networks: The need for secure systems. University of Colorado at Boulder, Technical Report CU-CS-988-04.

[24] Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer*, 35(10), 54–62.

[25] Perrig, A., et al. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534.

[26] Wang, X., et al. (2004). Sensor network configuration under physical attacks. Ohio State University, Technical Report OSU-CISRC-7/04-TR45.

[27] Sen, J. (2010). Routing security issues in wireless sensor networks: Attacks and defense. *Sustainable Wireless Sensor Networks*, 279–309.

[28] Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. *IEEE Symposium on Security and Privacy*, 49–63.

[29] Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer Magazine*, 36(10), 103–105.

[30] Wander, A. S., et al. (2005). Energy analysis of public-key cryptography for wireless sensor networks. *IEEE International Conference on Pervasive Computing and Communication*, 324–328.

[31] Hu, Y., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against worm-hole attacks. *IEEE INFOCOM*, 3, 1976–1986.

[32] Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. *ACM Workshop on Wireless Security*, 51–60.

[33] Sen, J., et al. (2007). A mechanism for detection of gray hole attack in mobile ad hoc networks. *International Conference on Information, Communications and Signal Processing*.

[34] Aura, T., Nikander, P., & Leiwo, J. (2000). DOS-resistant authentication with client puzzles. *International Workshop on Security Protocols*, 170–177.

[35] Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. *ACM International Conference on Mobile Computing and Networking*, 56–67.

[36] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11(6), 6–28.

[37] Sen, J., & Ukil, A. (2010). A secure routing protocol for wireless sensor networks. *International Conference on Computational Science and its Applications*, 277–290.

[38] Huang, Y., & Lee, W. (2004). Attack analysis and detection for ad hoc routing protocols. *International Symposium on Recent Advances in Intrusion Detection*, 125–145.

[39] Cam, H., Muthuavinashiappan, D., & Nair, P. (2003). Energy-efficient security protocol for wireless sensor networks. *IEEE VTC Conference*, 2981–2984.

[40] Cam, H., et al. (2004). Secure differential data aggregation for wireless sensor networks. In *Sensor Network Operations*. Wiley-IEEE Press.

[41] Sen, J. (2010). Reputation- and trust-based systems for wireless self-organizing networks. In *Security of Self-Organizing Networks* (pp. 91–124). CRC Press.

[42] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys and Tutorials*, 8(2), 2–23.

[43] Khemapech, I., Duncan, I., & Miller, A. (2005). A survey of wireless sensor networks technology. *PGNET, Proceedings of the 6th Annual PostGraduate Symposium*.

[44] Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, 52(12), 2292–2330.