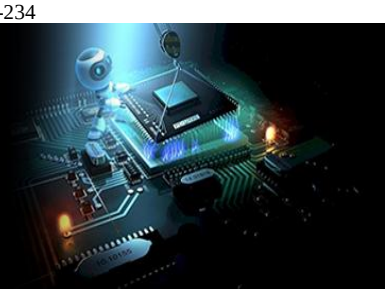
International Journal of Engineering in Computer Science



**E-ISSN:** 2663-3590
**P-ISSN:** 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2025; 7(1): 227-234
Received: 05-04-2025
Accepted: 08-05-2025

**Priya MR**
Research Scholar, Department of MCA, RV College of Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India

**Usha J**
Professor, Department of MCA, RV College of Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India

**Corresponding Author:**
**Priya MR**
Research Scholar, Department of MCA, RV College of Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India

# A comprehensive survey on security attacks in wireless sensor network

**Priya MR and Usha J**

**DOI:** https://www.doi.org/10.33545/26633582.2025.v7.i1c.185

**Abstract**
In Wireless Sensor Network (WSN), the sensors offer fascinating real-time data about the physical environment. WSN is rapidly expanding its application areas such as environmental monitoring, industrial security, battlefield awareness, context-aware computing, and so on. One of the most difficult tasks is safeguarding real-time data due to sensor node resource limitations. This article covers a comprehensive survey of WSN security, which includes characteristics, applications, architecture, vulnerabilities, security needs, different forms of attacks on sensors, and security techniques that researchers have examined in recent years on WSN. This might provide guidance for future WSN security research.

**Keywords:** Wireless sensor network, active attacks, passive attacks, security, machine learning

## 1. Introduction
A wireless sensor network is a grouping of sensor nodes that work together to achieve a common goal. Wireless sensors are battery-powered devices that can detect physical characteristics. Sensors have the ability to perceive, communicate, store data, and a limited amount of computation and signal processing [1]. With advancements in IC design, weight, cost, and size of sensor devices are constantly dropping while their precision and resolution are improving. Simultaneously, new wireless network technology that enables coordination and networking of a massive number of devices.

Sensor nodes might be distributed at random over the region of interest (battlefield monitoring, wildfire detection) or deterministically at the designated places (temperature, light monitoring in buildings, seismic monitoring in bridges and buildings).

Every sensor node includes sensors, radio transceiver, and microprocessor. Various types of sensors are available for tight integration, capturing data from a physical phenomenon. The sensor node's microprocessor is configured to do a difficult task than just transmitting what they detect. The transceiver provides a wireless connection for observable communication.

The function of the sensor is to segment the WSN in the network based on the topologies such as Bus, Tree, Ring, Star, Mesh, Circular, Grid [2]. The information regarding the position of nodes, as well as the nodes themselves, is grouped in a topology in the network. Network types are selected and deployed based on applications. The different types of WSNs are underground WSN, terrestrial WSN, underwater WSN, mobile WSN, and multimedia WSN.

The rest of the paper is structured as follows: In Section II Characteristics of WSN, Section III Applications of WSN, Section IV WSN Architecture, Section V Security requirement, Section VI Types of attacks, Section VII Security mechanisms in WSN and followed by Conclusion.

## 2. Characteristics of WSN
WSNs are currently used to measure many different types of metrics in an unsupervised physical environment. Therefore, the characteristics of the WSN must be taken into account in order to organize the network effectively. The primary properties of sensor networks are as follows [3]

1. **Low-cost:** To assess each physical environment, WSN generally deploys huge numbers of sensor nodes. The cost of sensor nodes is maintained as low as feasible to

lower the total cost of the network.

2. **Energy efficiency:** WSN energy is used for many purposes like computation, storage, and communication. Sensor nodes need more power than other types of communication. When the power is depleted, it is usually turned off because there is no way to recharge it. WSNs have limited energy, they are powered by batteries, which must be replaced or recharged (using solar energy) when they run out. Therefore, power consumption should be considered at the design stage when developing protocols and algorithms.
3. **Self-Organization:** Sensor nodes need to self-organize to form a network. Self-organizing WSNs is difficult due to bandwidth and power constraints available on these networks. Sensors can also be mobile and cannot engage in a long time. As a result, the topology of the WSN is dynamic and requires frequent reconfiguration, which results in significant processing and communication overhead.
4. **Computational power:** Each sensor node can collect, store, aggregate, process and send data to the receiver node. The computing power of a node is limited by cost and capacity considerations.
5. **Communication capabilities:** WSNs communicate using radio waves transmitted over wireless channels. It is distinguished by short-range communication with a limited and dynamic bandwidth. Communication channels are two-way or one-way. In an unsupervised and hostile production environment, it is very difficult to get the WSN to function properly. WSNs employ a variety of communication paradigms, including flat, distributed, and hierarchical WSNs, as well as heterogeneous and homogeneous WSNs. Therefore, communication hardware and software must be robust, secure, and recoverable.
6. **Security and privacy:** All sensor nodes require sufficient security procedures to prevent unauthorized access, attack, and accidental corruption of information contained by the sensor node. Must include additional data protection mechanism.
7. **Distributed sensing and processing:** Many sensor nodes are deployed either randomly or equally. Every sensor node is capable of sensing and processing data. As a result, system resilience should be provided via distributed detection.
8. **Dynamic network topology:** WSN stands for "dynamic networking" in general. In a few applications, nodes are allowed to traverse at arbitrary rates and may occasionally fail to function to add or modify node details. The topology of the network may change due to joining a new node or environmental changes. Therefore, WSN nodes should incorporate reconfiguration and self-adaptation capabilities.
9. **Application Oriented:** WSN is application-specific, which means that its architecture is built on applications. The nodes are randomly distributed and configured based on their intended purpose.
10. **Robust operations:** Sensor networks are large and sometimes installed in hostile environments. Therefore, the sensor node must be fault-tolerant, self-testing, auto-calibration, and auto-correction capabilities.
11. **Small Physical size:** Sensors are typically tiny with a restricted range. It has less energy and weak communication abilities due to its small stature.
12. **Multi-functional:** Sensor nodes conduct data collecting from various sensors, buffering and caching of sensor data, data processing; self-inspection and supervision; receive, transmit and forward data packets; and coordinate network tasks.
13. **Multi-hop communication:** One or more intermediate nodes are used in WSNs to receive and forward packets via wireless networks. The advantages of multi-hop wireless networks include increased network coverage and connection. This technology is to reduce energy consumption and extending network lifetime.
14. **Scalability:** WSNs must have the ability to scale or adapt the network for future growth. So, designing an efficient routing protocol for WSNs is important. Routing protocols need to be scalable and adaptable to changes in network topology. If a result, as the network becomes larger or the workload rises, the scalable protocol should function efficiently. WSNs must be able to scale or adapt their networks to allow future expansion. As a result, creating an efficient routing mechanism for WSNs is essential. A routing protocol must be scalable and adaptable to network topology changes. If a consequence, as the network becomes larger or the workload increases, the scalable protocol should function effectively. A WSN with these features can prove to be very beneficial and widely used in many applications.

## 3. Applications of WSN

Temperature, Pressure, Humidity, Optical, Mechanical, Motion, Vibration, Acoustic, Flow, Position, Electromagnetic, Chemical, and Radiation are some of the physical properties that should be monitored by sensors. Applications are categorized into military, environment, health, commercial areas, space exploration, chemical processing, home, and disaster relief. Major applications of WSN are [4, 6].

1. **Military Applications:** Sensor networks are used in the military to monitor friendly forces, discharged material, and equipment, as well as to investigate enemy forces and fields, assess combat damage, target, and detect and investigate nuclear, biological, and chemical.
2. **Environmental Applications:** Tracking the movement of birds, tiny animals, and insects in the environment. Environ- mental factors affecting crops and livestock are monitored. A macroscopic instrument for large-scale, Earth observation and planetary study. Biological, terrestrial, and environmental monitoring of marine, land, and atmospheric conditions; chemical and biological detection; Precision farming; and biological, terrestrial, and environmental monitoring in marine, land, and atmospheric situations. Environmental bio-synthetic mapping, wildfire detection, meteorological studies, pollution studies, and flood detection.
3. **Health Applications:** Providing an interface for people with disabilities. Monitoring the movement and internal processes of insects and other tiny animals; diagnostics; hospital medicine administration. Human physiological data may be monitored remotely. Keep track of hospital physicians and patients.
4. **Home Applications:** smart environments, and home automation.
5. **Commercial Applications:** Material fatigue is

monitoring; creating virtual keyboards; warehouse management; Items quality monitoring; Smart office building. Controlling and guiding robots in automated production environments. Interactive-toys and museum; Control and automate factory processes. Monitoring disaster area. Mechanical diagnostics; Carriage; Factory instrumentation; Local control of the actuator. Vehicle theft detection and monitoring service. Vehicle tracking and detection; Instrumentation of semiconductor processing chambers, wind tunnels, spinning machine, reflector chambers.

## 4. WSN Architecture

The Wireless Sensor Network is a network of sensor nodes, as shown in Fig. 1. Sensor nodes gather information about a physical object. Data collected from the sensor is transmitted to the sink/base station through a multi-hop infra-structureless design. The sink connects with the user through the Internet or satellite [4].

The sensor network layered architecture consists of five layers there are [5]: Application, Transport, Network, Data Link, and Physical. The layered architecture and related planes utilized by the sensor nodes, cluster head, and sink are depicted in Fig. 2. Functions of each layer are:

1. **Application:** Processing of applications, external querying, data aggregation, external database, and query processing.
2. **Transport:** Data propagation, caching, and storage.

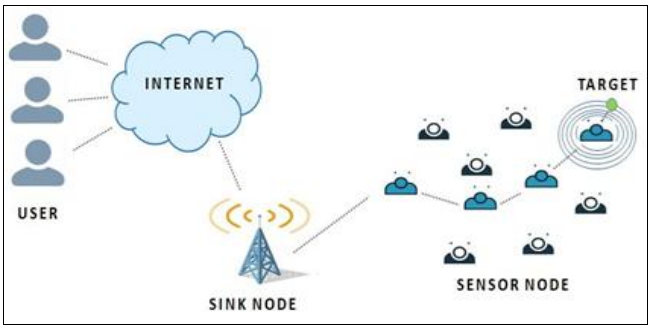



**Fig 1:** WSN Architecture

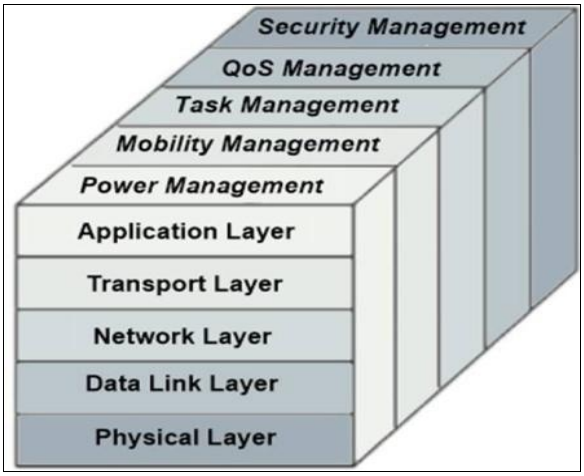



**Fig 2:** WSN Layered Architecture

3. **Network:** Take care of data supplied by the transport layers, Power efficiency, data-centric communication, adaptive topology management and routing.
4. **Data Link:** Data frame detection, channel sharing (MAC), media access, and error control, the timing and location.
5. **Physical:** Signal processing, communication channel sensing, actuation, modulation and data encryption.

WSN also need to be aware of multiple management planes. There are five management planes that are mostly utilized to regulate the network and to make the sensors operate as one in order to improve overall network efficiency. Responsibilities of Management planes are as follows:

6. **Power Management:** In order to save energy, it is responsible for limiting power usage and may switch off functionality.
7. **Mobility Management:** The movement of nodes is detected and recorded in order to keep a data path to the sink open at all times.
8. **Task Management:** Schedule and balance and detection tasks assigned to the detection field and the ability to focus on data aggregation and routing.
9. **QoS Management:** In WSN, real-time data services are very important. It also addresses fault tolerance, performance improvement, and error management using specific QoS matrices.
10. **Security Management:** The process of controlling, monitoring, and regulating a network's security-related behavior.

## 5. Security Requirements

Wireless sensor networks have constrained on power, processing power and storage. Securing the data has become a challenging task. The major security requirements are as shown as follows [7-11]

1. **Confidentiality:** To guarantee that sensitive information is adequately safeguarded and not divulged to unauthorized third parties, confidentiality is essential. Confidentiality extends not just to the preservation of information, but also to the transit of information.
2. **Authentication:** Each sensor node and base station must be able to ensure that the data it receives comes from a trusted sender, not from a malicious sender.
3. **Integrity:** Information/packet can be altered when exchanged over an insecure network. Integrity is essential to guarantee that only authorized entities may make modifications.
4. **Availability:** The information that an organization creates and stores must be accessible to authorized parties. Information unavailable is also detrimental to the organization as the loss of data confidentiality or integrity.
5. **Quality of service:** Quality and performance of sensor networks involve rapid data delivery.
6. **Freshness:** The data freshness goal assures that messages are new and fresh, which means they follow message ordering and have not been repeated. According to the literature, there are two forms of freshness. Weak freshness, which provides only partial message ordering without delay, and memory freshness, which provides delay but overall ordering.
7. **Self-organization:** In a sensor network, there is no fixed infrastructure for network administration; each sensor node is flexible and independent enough to self-heal and self-organize in response to changing circumstances. This inherent characteristic presents a major challenge for wireless networks.
8. **Source localization:** In order to determine the site of a

defect, a wireless sensor network designed to find faults will require precise location information. Unfortunately, replaying signals, by reporting bogus signal strengths, and so on, an attacker may readily manipulate insecure location information.

9. **Time synchronization:** To schedule their uptime and standby time intervals, most sensor networks require time synchronization. Some sensor network applications may require determining a packet's end-to-end transmission latency.
10. **Secure management:** At the base station level, we require secure management. Since communication from the sensor node terminates at the base station, issues such as key distribution to sensor nodes to establish routing information and encryption require secure management.

## 6. Types of Attacks

Major vulnerabilities in WSN are sensor nodes and data during transmission. Since sensor nodes are scattered in an insecure place, an adversary can physically access the node and can read the secret information which is stored in the node. WSN data are transmitted through the air, so easily adversary can listen, modify or disturb the data. Security attacks can be classified into two different categories as shown in fig. 3 [12-15]

1. **Passive Attack:** An attacker's purpose is to get information merely, not to alter it or harm the system. It's tough to spot this kind of attack. The focus of passive assault is on prevention. Passive attacks are usually used as a warm-up before aggressive attacks. The following are the most prevalent passive attacks:

a) **Monitoring and Eavesdropping:** Data privacy is the most common type of attack. The attacker passively listens to network connections to get access to private information and does not compromise data integrity in this sort of attack.

b) **Traffic Analysis:** An attacker can gain important information by monitoring the frequency and timing of network packets. This attack could include information about the amount of data transmitted, identify of communication nodes, or their locations. To counter this assault, the network will be checked on a regular basis.

c) **Camouflage Adversaries:** An attacker implants or compromises a sensor node in a wireless sensor network. This node draws packets from other nodes and may route those packets incorrectly to various routes.

d) **Homing Attack:** Nodes with unique duties, such as gateway, cluster head, or sink node, are targeted by attackers. Techniques to protect these nodes are encrypted header to hide sensor nodes placement and sensor nodes are using dummy packets to mislead intruders.

2. **Active Attack:** Attacker attempts to modify the data, harm the system or disrupt network services. In this attack, attention is paid on detection. The most common active attacks are

a) **DOS Attack:** The most prevalent current assault against WSN is a denial-of-service (DoS) attack. Any DOS attack that reduces a network's ability to execute its intended purpose. Different types of DOS assaults at different layers are jamming, tampering, unfairness, collision, fatigue, misdirection, flooding, and so on.

b) **Physical Attack:** Senor Networks are primarily used in harsh outdoor conditions. The sensors' compact form size, along with the unsupervised and distributed nature of their implementation, makes them very vulnerable to physical attacks.

c) **Routing protocol attacks**

1. **Spoofed Routing Information:** In this attack, an attacker could forge routing information as it is being transmitted between nodes, causing network traffic disruption as well as bogus error messages and routing loops. This causes increasing in end-to-end latency.
2. **Selective Forwarding:** A node in a WSN serves as a router. In this attack, malicious nodes forward only a few messages, and other messages were simply dropped.
3. **Sinkhole/Blackhole Attack:** In a sinkhole attack, an attacker pretends to be a sink node and inhales all traffic from the node or group of nodes. In a black hole attack, an attacker controls some of the compromised nodes and announces incorrect routing information to neighboring nodes.
4. **Sybil Attack:** Sybil attacks are just a single node that generates multiple IDs to other nodes. Communication with an unauthorized node causes data loss and makes the network unsafe.
5. **Wormhole Attack:** Wormhole attacks are severe attack in which two attackers strategically position themselves within the network. The attackers then continue to listen to the network, collect wireless information, and establish a tunnel to traffic at one network point and route it to another.
6. **HELLO Flood Attack:** This attack utilizes HELLO packets. An attacker can send this sort of packet to every single node in the WSN. As a result, they assume the hacked node is their neighbor's. As a result, massive numbers of nodes send packets to this fictional neighbor, causing oblivion.
7. **Acknowledgment Spoofing:** The attacker spoofs the acknowledgments of a packet sent by a node or a collection of nodes. The attacker has the ability to send replica information to its neighbor's node.

d) **Node Capture Attack:** In this attack, to take control over the entire network it is sufficient for an adversary to capture a single node.

e) **Node Replication Attack:** The adversary tries to add a node to the existing sensor network, by duplicating the node ID of an existing sensor node. Packages can be tampered with or even redirected.

f) **Node Outage Attack:** This type of attack disables all Network capabilities, either physically or logically.

g) **Passive Information Gathering:** In this attack, the attacker can acquire unencrypted information, including physical location, using a sophisticated algorithm. This information could be useful in destroying the node.

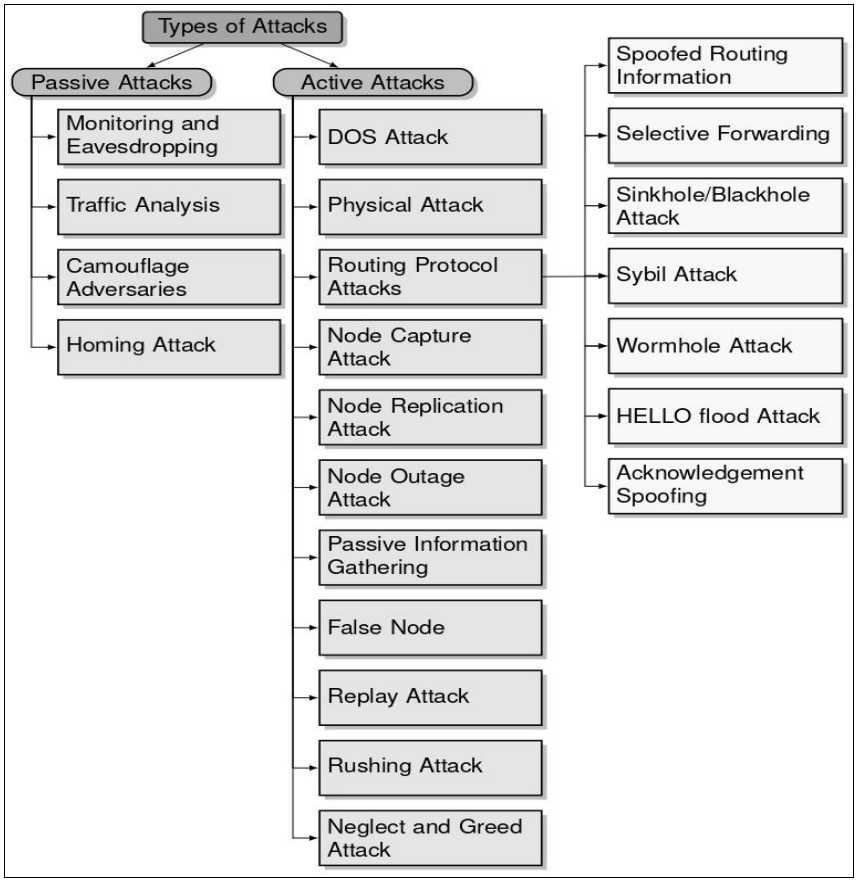



**Fig 3:** Taxonomy of Types of Attacks

**h) False Node:** In the network, an attacker introduces a fake node. This erroneous node delivers wrong data to the rest of the network's nodes.

**i) Replay Attack:** This attack is accomplished by continuously monitoring the message exchanged between entities and replaying it afterward to bring down the target entity or affect the performance of the target network.

**j) Rushing Attack:** The attacking node receives the request routing packet; it instantly forwards it to its neighbors without analyzing it.

**k) Neglect and Greed Attack:** The malicious node chooses the longest path to forward the packet by routing the packet to the wrong node. This can result in information loss.

**l) Clock Skewing:** Time synchronization plays an important role in WSN. The attacker targets the node that wants to perform the synchronization operation. Therefore, the attacker broadcasts the wrong time on the network. This is intended to bring the node out of sync.

**m) Vampire Attack:** An attacker entirely disables the network by consuming the power of the sensor node.

**Security Mechanisms in WSN**

The fundamental purpose of the security mechanism is to provide fictitious ideas on how to detect, recover, prevent and protect against different types of security attacks. To combat different types of attacks, different security techniques can be devised. Table 2 [9, 15, 16, 17] shows counter measures for different types of attack. We can divide security systems into two categories as shown in fig. 4 [17]. WSN security concerns are divided into two categories: protocol security and trust and privacy. Protocol security entails safeguarding the entire layer rather than securing each layer individually. Master setup and trust configuration, privacy and authentication, privacy, secure routing, node capture resilience, and secure routing are all part of the layered security. These security measures are referred to as low-level procedures. Secure group administration, intrusion detection, and data aggregation are examples of high-level techniques.

**Low Level Security**

1. **Key establishment and trust setup:** For the creation of secure routing schemes for WSNs, key management is a prerequisite. Several cryptographic keys are distributed to sensor nodes across the network in key management techniques. Trusted server, key pre-distribution, and self-enforcing key management protocols are the three key management systems.
2. **Secrecy and authentication:** In a sensor network, since nodes are connected to one or more base stations, packets are more vulnerable to active attacks. Cryptography is the standard mechanism for secure communication in the presence of adversarial behavior. Different types of cryptography are symmetric and asymmetric (public) keys. Choosing cryptography for WSN has become a challenging task due to the limitation of energy, computational capability, and storage resources of sensor nodes. The most widely used scheme is symmetric, due to its ease of implementation of limited hardware and small energy demands. Since symmetric-based cryptography scales poorly well as the number of sensor nodes grows, public key-based schemes are widely used. In public key-based schemes like RSA, Diffie-Hellman, Elliptic curve cryptography

(ECC), etc. ECC has a substantial benefit in that it decreases calculation time as well as the amount of data sent and stored [18].

3. **Privacy:** In WSN, privacy is one of the major issues like other traditional networks. Data privacy is needed in most applications like military, health, home, and office-based applications. Privacy prevention schemes are multipath routing, secret sharing, and hashing.
4. **Robustness to communicate DOS:** In a DOS attack, network communication is distributed by transmitting a multitude of high-energy signals to overload the communication channel, which may be available to other nodes in the network.
5. **Secure routing:** Secure data transmission is one of the most essential challenges in a wireless network. Data transmission via a wireless media is subject to a variety of security threats, including denial of service attacks and malicious routing attacks. Various secure routing systems for WSNs have been devised; however, none of them meet the severe requirements of WSNs. Furthermore, because the majority of these routing protocols were developed for static WSNs, the mobility issue remains unresolved.

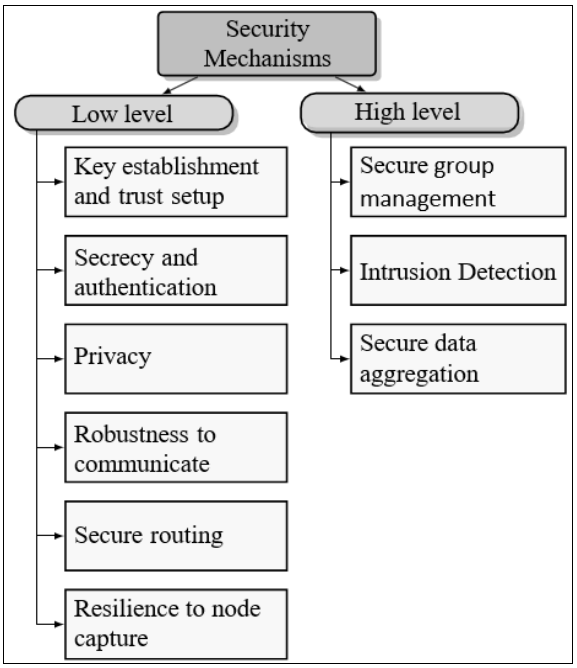



**Fig 4:** Taxonomy of Security Mechanisms

1) **Resilience to node capture:** The nodes in the WSN are vulnerable to a variety of security threats. An attacker may capture its data or accesses its data or reprogram it to behave maliciously. A compromised node's irregular behavior could lead to abnormalities. To overcome these problems, need a strong algorithm to detect/monitor the malicious node.

2) **High Level Security**

a) **Secure group management:** Each node in the wireless sensor network has limited processing and communication capabilities. A group of nodes can perform all network tasks such as data collection and data analysis. In WSN, mobile WSN node groups can vary. This group is also responsible for providing important services. Therefore, a secure protocol is required for a group of nodes to securely authorize new group members and provide secure communication to newly authorized group members. The group key's result is forwarded to the base station. It is confirmed that the output is validated and originates from a group to which permission has been granted. The members of the group must have control over the group key.

b) **Intrusion Detection:** The intrusion detection system detects malicious activity on a node or network and issues an alert to notify the user of the malicious activity.

c) **Secure data aggregation:** An advantage of wireless sensor network is, detail detection large and dense groupings of nodes can provide. To decrease the massive amounts of traffic returning to base station, the discovered data must be aggregated. Data aggregation is handled by the aggregation nodes and may be used for real-world event detection to average a geographic region's temperature, integrate sensor outputs to compute the position and velocity of a moving item, or aggregate data to prevent false alarms. Depending on the design, aggregation can happen in a variety of places within the WSN. Every aggregation site needs to be protected.

Machine learning techniques are now being applied in WSN to detect and prevent threats. Machine Learning (ML) is a process that improves or learns without being explicitly programmed as a result of a study or experience. ML creates models by automatically, quickly, and accurately interpreting even more complicated data. Recent improvements in machine learning have been used to overcome a variety of problems in WSNs. ML not only increases the performance of WSNs, but it also reduces the need for human intervention or reprogramming. Different types of machine learning are as shown in fig 5:

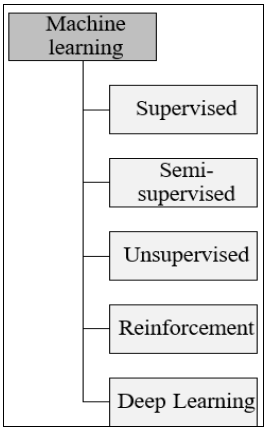



**Fig 5:** Taxonomy of Types of Machine Learning

1. **Supervised Learning:** In supervised learning, the machine is trained on a "labelled" dataset and based and the machine predicts the output based on the training. Linear Regression, SVM, Nearest Neighbor, Gaussian Naïve Bayes, Decision trees, and Random Forest are the most extensively used supervised algorithms.
2. **Unsupervised Learning:** Machines are trained with unlabeled dataset and predict outputs without any supervision, during unsupervised learning. K-Means Clustering method, Meanshift algorithm, DBSCAN algorithm, Apriori algorithm, principal component analysis, independent component analysis and FP-growth algorithm are the most commonly used unsupervised algorithms.
3. **Semi-Supervised:** The advantages of both supervised and unsupervised machine learning are combined in semi-supervised machine learning. During the training stage, it employs a combination of labelled and unlabeled datasets, representing a middle ground between unsupervised and supervised learning and techniques.
4. **Reinforcement Learning:** Reinforcement learning is based on a feedback-based process, where AI agents automatically explore the environment by hitting and tracking, performing actions, learning from experience, and improving performance. The most popular reinforcement algorithms are Q-learning, TD-learning, and R-learning.
5. **Deep Learning:** Artificial neural networks are used in deep learning to execute difficult computations on enormous volumes of data. A type of machine learning based on the structure and task of the human brain. CNNs, LSTMs, RNNs, GANs, RBFNs, MLPs, SOMs, and Auto encoders are examples of deep learning algorithms.

**Table 1:** Counter Measures for various types of attacks.

| Attacks | Counter Measures | Attacks | Counter Measures |
|---|---|---|---|
| Monitoring and Eavesdropping | Directional Antenna | Selective Forwarding | Routing Multipath |
| | | | Identifying a New Routing Path |
| | | | Monitoring of Sensor Node |
| Traffic Analysis | Network Monitoring | Sinkhole Attack | Identification with unique information |
| Camoutflage Adversaries | Privacy Analysis | Blackhole Attack | Network Monitoring |
| | | | Authentication Mechanism |
| | | | Changing the Routingof Packets |
| Homing Attack | Encryption | Sybil Attack | ID-Based and Authentication |
| | | | Symmetric-Key Encryption Techniques |
| DOS Attack | Encryption Algorithms | Wormhole Attack | Packet leashes |
| | Regular Monitoring | | Geographic and temporal leashes |
| | Prioritizing Messages | | |
| Physical Attack | Tamper Proofing | HELLO Flood At -tack | Packet Leash Mechanism |
| Spoofed Routing Information | MAC Authentication | Node Capture Attack | LEAP Protocol |

**Table 2:** Counter Measures (continued)

| Attacks | Counter Measures | Attacks | Counter Measures |
|---|---|---|---|
| Acknowledgment Spoofing | Bi-directional link verification Mechanism | Replay Attack | Timestamp with message |
| | | | Session Tokens |
| Node Replication Attack | Unique pair-wise Key | Rushing Attack | Embedding a node list |
| False Node | En-Routing Scheme | Neglect and Greed Attack | Redundancy |
| | | | Authentication Mechanisms |
| Passive Information Gathering | Well-designed Antenna | Clock Skewing | Synchronization Period |
| | | | Changing Time and FTSP |
| Node Outage Attack | Time Protocols | Vampire Attack | Validation Techniques |
| | Powerful Algorithms | | |

## Conclusion

WSNs are vulnerable to a range of attacks that target all network components, including nodes, packets, routing protocols, and so on, because they are frequently utilized in unsupervised scenarios and have limited resources. This survey outlines WSN attacks and their classification, as well as security mechanisms used so far to over form attacks. This research aims to encourage future researchers to develop smarter and more robust security technologies to make networks more secure.

## References

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Commun Mag. 2002;40(8):102-114.
2. Sharma D, Verma S, Sharma K. Network Topologies in Wireless Sensor Networks: A Review. Int J Electron Commun Technol. 2013;4(Spl-3):93-97.

3. Ahmed MR, Huang X, Sharma D, Cui H. Wireless sensor network: characteristics and architectures. Int J Inf Commun Eng. 2012;6(12):1398-1401.
4. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. Comput Netw. 2002;38(4):393-422.
5. Alkhatib AAA, Baicher GS. Wireless Sensor Network Architecture. Int Proc Comput Sci Inf Technol. 2012;35:11-15.
6. Kumar A, Kumar A. An Overview of Wireless Sensor Networks (WSN) Applications and Security. Int J Comput Sci Eng. 2019;7(7):98-100.
7. Burhanuddin MA, Mohammed AAJ, Ismail R, Hameed ME, Kareem AN, Basiron H. A review on security challenges and features in wireless sensor networks: IoT perspective. J Telecommun Electron Comput Eng. 2018;10(1-7):17-21.
8. Grover J, Sharma S. Security issues in Wireless Sensor Network—A review. In: 5th Int Conf Reliability, Infocom Technologies and Optimization (ICRITO); 2016. p. 397-404.
9. V K B, Brahmanand SH. Wireless sensor networks security issues and challenges: A survey. Int J Eng Technol. 2018;7(33):89.
10. Pandey A, Tripathi R. A Survey on Wireless Sensor Networks Security. Int J Comput Appl. 2010;3(2):43-49.
11. Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: a survey. IEEE Commun Surv Tutor. 2008;10(3):6-28.
12. Ghildiya S, Mishra AK, Gupta A, Garg N. Analysis of Denial Of Service (Dos) Attacks In Wireless Sensor Networks. Int J Res Eng Technol. 2014;3(22):140-143.
13. Biswas S, Adhikari S. A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network. Int J Comput Appl. 2015;131(17):28-35.
14. Gavrić Ž, Simić D. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ing Investig. 2018;38(1):130-138.
15. Keerthika M, Shanmugapriya D. Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Glob Transit Proc. 2021;2(2):362-367.
16. Niksaz P, Kargar M. A Full Review of Attacks and Countermeasures in Wireless Sensor Networks. Int J Inf Secur Priv. 2012;6(4):1-39.
17. Wahid A, Kumar P. A survey on attacks, challenges and security mechanisms in wireless sensor network. Int J Innov Res Sci Technol. 2015;1(8):189-196.
18. Kardi A, Zagrouba R. Attacks classification and security mechanisms in Wireless Sensor Networks. Adv Sci Technol Eng Syst J. 2019;4(6):229-243.