Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Comprehensive Review Of Security Challenges And Attack Vectors In Wireless Sensor Networks

Chaya P[1], Nandini Prasad K S[2]

[1]Assistant Professor, Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysore
[2]Professor, Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Affiliated to VTU, Belagavi, Karnataka, India.
e-mail: chayaneetha@gmail.com , e-mail: drnandini.prasad1@gmail.com

Wireless sensor networks are an area of study where energy efficiency is a major issue. Its practical problem-solving capabilities and affordable solutions make it highly recommended.Because WSN has limited resources, its nodes make it highly vulnerable to attacks.Wireless networks are vulnerable due to their orientation transmission and unfavorable architecture.Security is a broad subject with numerous facets and is particularly important for various assaults.As expertise expands, security, which is advancing daily, increases.Despite the network's excellent security during design, hackers and intruders always receive past security measures and launch assaults.This research comprehensively examines the security risks associated with wireless sensor networks.Active and passive assaults are two types of threats.While active assaults alter the data in communication lines, passive assaults only listen to the communication lines.Various risks that occur within active and passive hazards are thoroughly examined.In addition, a detection system that functions as a firewall and has real-time intrusion detection capabilities is required.This study aims to provide a comprehensive analysis that surpasses the typical risks and the protective strategies suggested by related studies.

1.Introduction

The research community is becoming more interested in Wireless Sensor Networks (WSNs) due to their exceptional qualities and promise of low-cost solutions to practical issues.Wireless nodes with ad hoc sensing capabilities comprise WSNs [1], which collaborate to conduct shared activities. Due to their wireless operation and sensing capabilities, WSNs are a significant and profitable choice for corporate organizations and scientific studies. Additionally, they lead to improvements that create new security problems.The main problem is that WSN battery-operated devices have limited energy capacity and computing capability. Therefore, techniques are required to assure security against intrusions and minimize power consumption for more extended operations without changing or recharging the battery.

Table 1: Security Challenges in WSN

Security Challenges	**Description**
Limited Resources	Sensor nodes are constrained by hardware, energy, computational power, memory capacity, and hardware.
Network Topology	The network's vulnerability to assaults due to its topology is crucial.
Energy Optimization	In WSNs, balancing low power consumption and robust security is a significant issue.
Shared Cryptographic Keys	Effective shared key management is essential to safeguard the integrity and safety of data.

WSN research is aided by developing long-term unattended systems for various security- and homeland-focused applications, including critical infrastructure protection, military sensing, and environmental monitoring. Due to their vulnerability to attacks and node breaches that take advantage of known and unknown hardware, software, and protocol defects, wireless sensor networks (WSNs) risk compromising data availability, security, integrity, and validity. Adequate security measures must be developed to protect WSN functioning from inadvertent attacks and operational or accidental failures, which can cause sudden and unexpected changes to traffic load, link capacity, and network topology. To address the security issues in WSN, it is necessary to understand the challenges in Table 1 fully.Some examples of security techniques include using cryptographic primitives, key management, network layer routing protocols with security features, MAC-level authentication, and safe data aggregation.
Energy limits in WSNs also require data aggregation, and secure data aggregation requires encryption to ensure data integrity and confidentiality. Secure data aggregation can be accomplished with cryptography, but its limits in WSN and the particularities of its methods and routing architectures must be considered [2]. A flawless WSN security strategy should handle assaults and compromised nodes to protect data and maintain connection. Nodes that can identify compromised nodes can act without reconfiguring the network to eliminate possible risks. In summary, WSNs have several advantages: enhanced performance, scalability, delay tolerance, and adequate load balancing [3]. However, because they are broadcast, they are open to several types of harmful assaults.

As per the study literature, fig. 1 depicts the distribution of energy consumptionacross the various tasks a sensor node completes during its active period. Communication activities account for almost 50% of energy, highlighting the importance of addressing this component.

The installed wireless sensor network must ensure maximum coverage area and sustain network connectivity for effective communication. Since wireless sensor nodes have limited energy resources, this research investigates energy-efficient alternatives [4]. Radio modules, microcontrollers, and sensors are the components that use the most energy out of all of them. This paper discusses these issues to enhance energy utilization in wireless sensor networks and suggests several solutions.

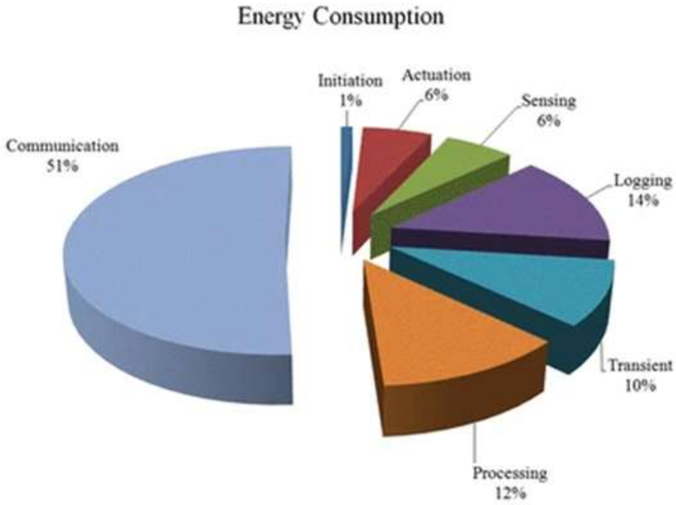


Figure 1: Energy Consumption in WSN over Time

The energy consumption trends seen in WSNs over a given time are depicted in this graph. As shown in Figure 1, energy usage varies because of different network activity and communication requirements. Ensuring the lifetime and efficiency of WSNs requires overcoming the fundamental obstacle of optimizing energy usage while preserving security.
This paper thoroughly examines WSN security, based on earlier research on threats and assaults, to address these issues. To configure WSNs, it highlights several vulnerabilities and operational paradigms, highlighting the significance of putting robust security protocols in place. The study also examines the benefits and drawbacks of the security solutions currently used for data gathering and routing methods. Emphasis is paid to energy optimization measures within security implementations to achieve effective resource use. In addition, the paper highlights unresolved research issues. It makes recommendations for possible further investigation directions to support the continuous endeavors to improve the security of wireless sensor networks.

2.Security Threats

Numerous risks, vulnerabilities, and attacks present severe obstacles to the performance and integrity of wireless sensor networks (WSNs). These dangers can cause energy loss and device malfunctions, compromising the system's dependability. A common threat is posed by malicious nodes, which frequently aim to damage the network infrastructure. As seen in Figure 2, these security lapses usually fall under type-wise [5] and layer-wise attacks.

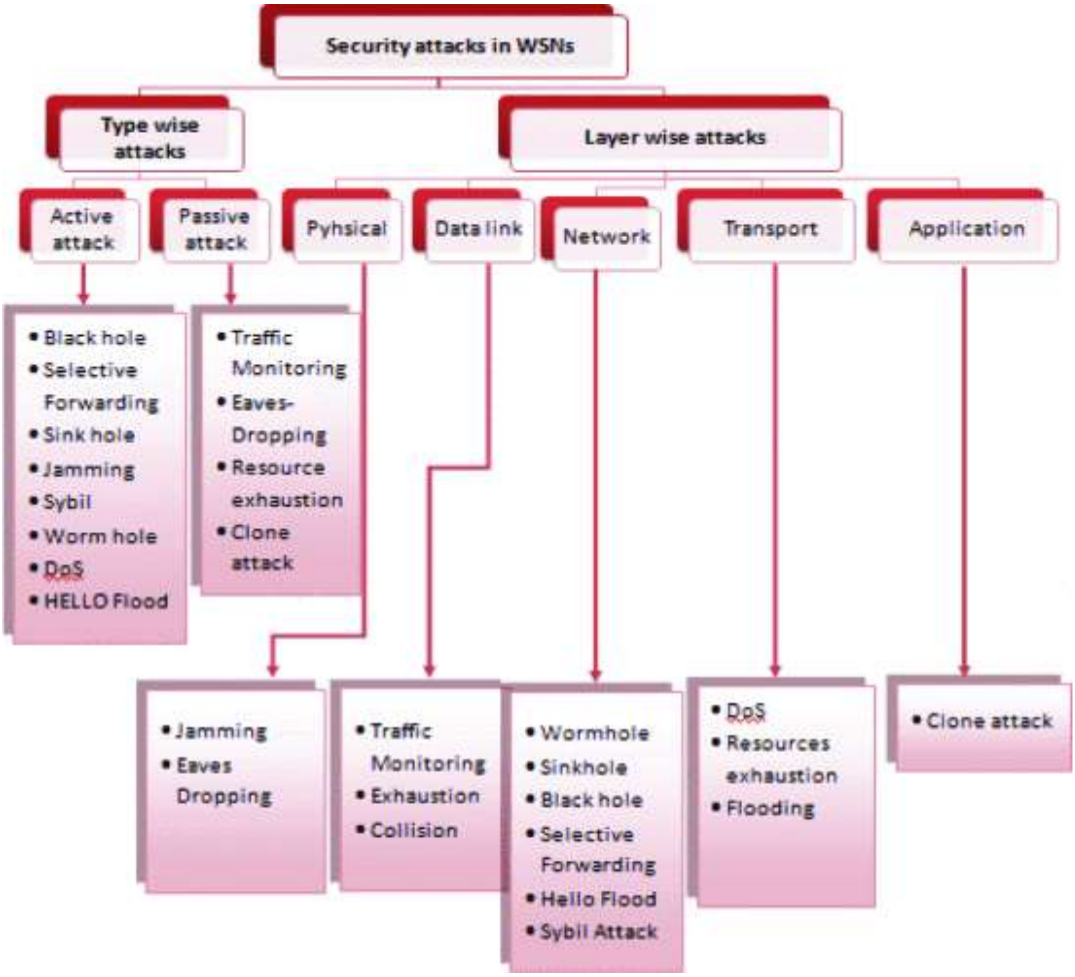


Figure 2: Security attacks in WSN

A.Passive attacks

Passive attacks [6] occur when unauthorized intruders watch and listen on the communication channel. The nature of the attacks on privacy is passive.

Privacy-related Attacks It is not the primary privacy issue that sensor networks make data collecting possible. Indeed, direct site monitoring may gather much information via sensor networks. Instead, sensor networks exacerbate the privacy issue because they provide easy remote access to vast amounts of information. Therefore, enemies don't need to be there in person to continue spying. They can obtain information anonymously and with minimal risk. Among the more prevalent assaults on sensor privacy are the following:

- **Monitoring and eavesdropping**: Privacy breaches are most frequently caused by monitoring and eavesdropping. The enemy could quickly determine the content of the transmission by examining the data. If the communication contains control information about the design of the sensor network, eavesdropping [7] can seriously compromise confidentiality protection since it could reveal more information than the location server does.

- **Detecting traffic:** Even when messages are transmitted encrypted, there is still an increased chance of analysis of the transmission patterns. The sensor network may be subject to intentional damage from an adversary if sufficient information is revealed by sensor operations [8].
- **Resource exhaustion**: DoS attacks come in various forms, including flooding and resource depletion assaults. Attacks known as resource exhaustion force the targeted infrastructure to use up all its memory and storage capacity, drastically reducing or stopping the service altogether.
- **Clone attacks**: There are many approaches to identify clone assaults [9], which are common in WSNS. A few of these methods include random walk-based strategy, distributed detection of node capture assaults, hierarchical node replication attacks, compressed sensing-based clone identification, random walk-based method, mobility-assisted replication detection in mobile WSNS, random key pre-distribution, and protocol detection of node replication assaults in mobile WSN. These techniques make wireless sensor networks less susceptible to clone assaults.

B.Active attacks

Active assaults [10] are defined as creating bogus data during transmission or modifying genuine data streams and messages. A hacker could replicate previous data streams, alter the messages, or omit a portion of crucial communication messages. Numerous assaults, such as denial of service attacks, physical attacks, message corruption, fake nodes, node replication attacks, routing attacks, node subversion, node malfunction, and node outage, can affect sensor networks. Passive information collecting is also susceptible to these kinds of attacks. Routing attacks include replayed, manipulated, and spoofing routing information and physical assaults, wormholes, sinkholes, Sybil attacks, and HELLO floods.

Sinkhole attacks direct traffic toward a particular node by making it appear desirable to other nodes. Sybil attacks make several copies of a single node and display them to other network nodes as different identities. Techniques like encryption and authentication can stop outsiders from using the sensor network to conduct a Sybil assault. Attacks using wormholes capture packets at one point, tunnel them via another point, and then retransmit them into the network. Attacks known as denial of service (DoS) can occur at several levels, including the physical, link, network, neglect, greed, homing, misdirection, black hole, and transport layers. Malicious activities or unintentional node failures are the sources of DoS attacks. Among the protections against denial-of-service attacks include pushback, strong authentication, traffic identification, and payment for network services.

By capturing a node that could divulge information, including cryptographic keys, node subversion jeopardizes the security of the entire sensor network. Erroneous data from malfunctioning nodes might compromise the integrity of the sensor network, especially if such nodes are cluster leaders or other data-aggregating nodes. A node outage results from a node failure. To mitigate the effects of node failures, robust protocols that provide a fallback path should be implemented. Sensor networks in hazardous outdoor locations are vulnerable to physical assaults due to their tiny form size and unprotected environments. Physical attacks irreversibly degrade sensors, resulting in irreversible losses. Message corruption affects a message's content, whereas malicious data inserted by an attacker when they add a node result in bogus nodes. Clone an existing sensor node's nodeID [11] to add a node to an already-existing sensor network is one form of node replication attack. Incoherent or misdirected packets might result in inaccurate sensor readings or a disconnected network. An attacker with substantial resources can obtain data from sensor networks using a technique known as passive information gathering, which does not need encryption.Table 2 provides a summary of recent attacks and their attributes in WSNs.

Table 2: Overview of Active Attacks and Their Characteristics in WSNs

Attack Type	**Description**	**Impact**	**Countermeasures**
Injection/Alteration	Modifies or alters packets to disrupt data	Data corruption, unauthorized access	MACs, digital signatures, encryption
Replication	Clones' nodes to increase presence	Compromised resources, integrity, reliability	Node authentication, intrusion detection systems
Looping	Creates routing loops to disrupt communication	Network congestion, packet collisions	Loop prevention mechanisms, sequence number checks
Jamming [12]	Flood channels with interference signals	Packet loss, latency, performance degradation	Spread spectrum, frequency hopping, power control
Sinkhole [13]	Attracts traffic to a compromised node	Data compromise, routing inefficiency	Secure routing protocols, node authentication
Wormhole [14]	Creates covert tunnels to bypass nodes	Routing compromise, confidentiality breach	Distance bounding, secure localization
Black Hole [15]	Selectively drops all received packets	Communication disruption, data loss	Secure routing protocols, packet acknowledgment
Grey Hole	Selectively drops or delays packets	Data delivery compromise, performance impact	Intrusion detection, anomaly detection
Rushing [16]	Flood network with excessive traffic	Denial of service, congestion	Rate limiting, traffic shaping, access control
Route Table Poisoning	Injects false routing information	Routing errors, traffic redirection	Authentication mechanisms, route verification

Sybil	Creates multiple fake identities	Network resource compromise, influence gain	Node authentication, reputation-based systems
Flooding [17]	Floods network with excessive packets	Denial of service, congestion	Rate limiting, traffic filtering, access control
Hello flooding,	Floods network with excessive "hello" messages	Topology disruption, performance degradation	Rate limiting, message authentication, encryption

Active and passive assaults are the two main categories of security risks in WSNs, each withtraits and techniques. Comprehending various kinds of assaults facilitates the creation of efficient security plans and the successful resolution of problems.

Table 3: Characteristics and modalities of attack execution

Aspect	**Active Attacks**	**Passive Attacks**
Nature of Attack	Involve direct manipulation or disruption of data or network components	Do not involve immediate alteration of data or network configurations
Detection	Often easier to detect due to visible alterations or disruptions	More challenging to detect as they do not visibly alter data or network configurations
Objective	Aim to interfere with the integrity, confidentiality, or availability of data.	Aim to secretly gather sensitive information without raising suspicion.
Impact	Can have immediate and noticeable impacts on network performance, reliability, and security	The impact may be less immediately apparent but can lead to significant privacy breaches or data leakage over time.
Interaction	Require interaction with the target system or network components to execute malicious actions.	Do not require interaction and typically involve monitoring or observing network traffic.
Examples	Injection, alteration, jamming, replication	Eavesdropping, traffic analysis, monitoring
Complexity	Often more complex as they involve actively manipulating data or network behavior.	Generally, they are more straightforward as they involve passive observation without modifying the data.
Mitigation	Requires active countermeasures such as	Mitigation strategies often focus on encryption, traffic

	intrusion detection systems, firewalls, and encryption	analysis detection, and access control measures.

3 Cryptographic Techniques to Strengthen Network Security

Security and attack prevention in Wireless Sensor Networks depend on using cryptographic techniques to secure data. Encryption techniques transform data packets from direct original data packets to protected coded data packets transferred over the network. Usually, encrypted data consists of a set of extra bits in addition to the original data.A form of cryptography known as symmetric cryptography [18] encrypts and decrypts data packets using a single secret key in a converse network, as shown in Figure 3. Large networks, where there is a greater chance that an attacker knows the key, make this strategy less effective. For instance, small sensor networks with pre-loaded secret keys are suitable for small networks but not big ones.

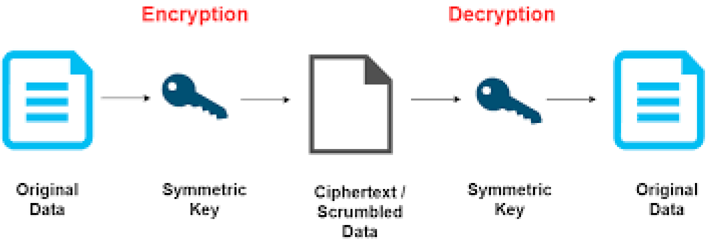


Figure 3: Symmetric cryptography

Asymmetric cryptography [19] encrypts and decrypts data using public and private keys, as Figure 4 illustrates. The private key is made available to authorized users so they may access information, while the sender utilizes the public key to decode conversations. Key management is made easier using public key cryptography, providing extra features not seen with symmetric key techniques. We refer to this safe technique as asymmetric cryptography.

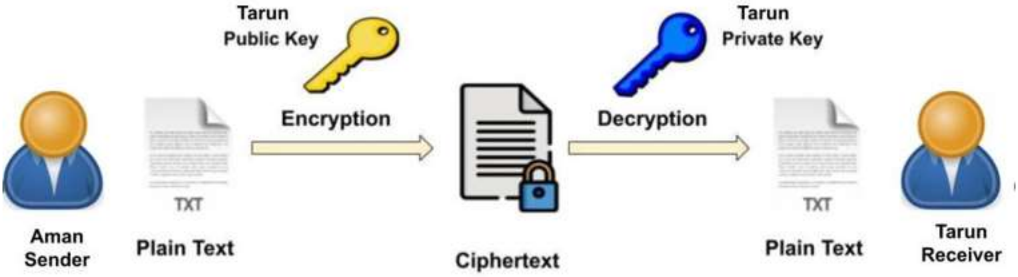
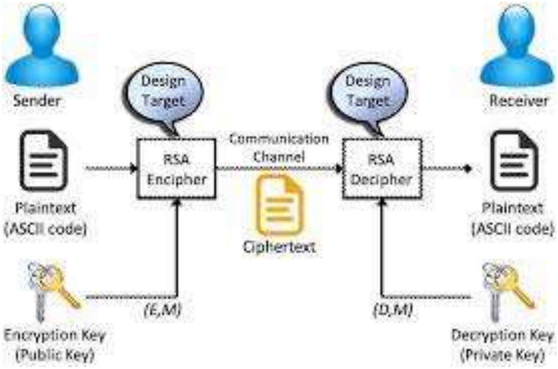


Figure 4: Asymmetric cryptography

The challenge of factoring big prime integers is at the heart of the public key encryption technique known as RSA [20], as seen in Figure 5. A well-liked public key cryptography technique for encrypting data and generating digital signatures is RSA.



.
Figure 5:RSA

Another cryptographic method that uses the algebraic construction of elliptic curves is called Elliptic Curve Cryptography (ECC) [21]. Because of its small key size, ECC requires less transmission power and storage space. Although it is more complicated than RSA, it offers a similar level of security.With ECC as its core component, TinyECC [22] is software that makes growing WSN-based organizations simpler, more adaptable, and ready-made. TinyECC maintains all ECC operations, including point addition, duplication, and multiplications, making it a suitable safety solution for wireless sensor networks.
Collective research efforts continue to improve network security and reduce new threats at all phases of WSN architecture.

Table 4: Comparison of Public Key Cryptography Solutions in WSN

Reference No.	**PKCSolutions**	**Security Requirements**	**Drawbacks**	**Attack Alleviation**	**Mitigation Strategies**
[23,24,25]	Unsigned keys and credentials	Certification, privacy preservation	High computational overhead due to unsigned keys. Unsigned keys may be susceptible to interception.	Eavesdropping: Attackers intercept communication to obtain sensitive information. Replay attacks: Attackers replay intercepted messages to deceive the system.	Key rotation: Regularly updating keys can mitigate the impact of interception.
[26,27]	Identity-based proxy signatures	Authentication, non-repudiation,	Vulnerability to private key leaks	Denial of Service (DoS):	Multi-factor authentication: Adding

		privacy preservation	due to centralized management.	Attackers flood the system, disrupting services. Impersonation attacks: Attackers masquerade as legitimate users to gain unauthorized access.	additional authentication factors can enhance security.
[28,29]	ECC (Elliptic curve cryptography)	Certification, privacy preservation	Vulnerability to replay attacks. ECC key sizes may be smaller, making them susceptible to brute-force attacks.	DoS: Attackers flood the system with requests overwhelming resources. Replay attacks: Attackers replay intercepted messages to manipulate system behavior.	Secure key generation: Using robust random number generators can strengthen ECC keys against brute-force attacks.
[30]	RSUs-based signature schemes	Certification, privacy preservation	Compromised RSUs may lead to information disclosure—complex key management and distribution.	Impersonation: Attackers pose as legitimate nodes to inject false data or disrupt communication. Data routing attacks: Attackers manipulate routing paths	Reputation-based trust: Utilizing reputation systems can help detect compromised RSUs and limit their influence.

				to intercept or alter data.	
[31,32]	Smart cards for identification	Certification, privacy preservation	Storage complexity and vulnerability to physical theft or loss of smart cards.	Sybil attacks: Attackers create multiple fake identities to gain undue influence. Impersonation attacks: Attackers use stolen or forged smart cards to impersonate legitimate users.	Biometric authentication: Adding biometric verification to smart card authentication can enhance security.

To sum up, cryptographic techniques are essential for safeguarding data in wireless sensor networks. They offer excellent protection while stabilizing prices, performance, and safety standards. Still, WSNs, like conventional preconfigured networks, must embrace more adaptable key distribution strategies.

4. WSN Security requirements

Wireless sensor networks frequently must deal with issues including DOS assaults, intrusive code insertion, and eavesdropping. Minimum security qualities and standards are anticipated to be met to guarantee the security of WSNs. Availability, authentication, secrecy, data freshness, adaptability, integrity, scalability, self-organizing quality, and scalability are all essential security goals.

- **Availability:**Availability is a crucial factor in ensuring the WSN's durability [33]. Denial-of-service attacks are typically the result of a WSN's inability to guarantee the availability of its sensor nodes, and these assaults can ultimately cause a significant loss in terms of potential data detection and financial crises.
- **Authenticity:**The authentication of data communicated via wireless channels is crucial because these networks employ them to transfer vital information that has either been processed or must be processed. Even if source authentication or data origin verification can stop external assaults, some security issues must be resolved [34].
- **Confidentiality:** The detected data must remain confidential to avoid malicious code insertion and spoof packet detection [35]. It guarantees the security of the sent data. And for that, deploying a shared encryption key amongst the communicating nodes may be adequate. An attacker might examine network traffic or employ any decryption

technique to access the network. Therefore, limiting access control rights at base stations is usually recommended.

- **Data freshness:**Additionally, all information obtained must be current and fresh, meaning no outdated records may be repeated, and the most recent data must be gathered. Each shared secret key is examined and ensured not to be utilized again by any other user on the same network to achieve that [36].
- **Flexibility:**Wireless sensor networks' sensor nodes operate in demanding situations where threats, duties, node positions, and conditions can all change rapidly. Any sensor node can blow a fuse or be disconnected from the network. Depending on the circumstances, additional nodes may be added to the network, or a larger network may be divided into smaller sensor networks.Therefore, the established security plan should be adaptable [37].
- **Integrity**: One of the most crucial tasks of a wireless sensor network is data aggregation.When data aggregation occurs, the sensor node collects readings from nearby nodes, aggregates them, and sends the data to the base station for processing. Data integration ensures that the recorded measurements are genuine and have not been compromised during this procedure.
- **Scalability:** The number of sensor nodes in a WSN, their sizes, and even the sensor network design are all subject to frequent modifications to facilitate the addition of new, unfused nodes and removing fused nodes from a network**.**Replacing malfunctioning physical components or expanding or contracting the sensor network shouldn't affect the WSN's performance. Thus, scalability is crucial for the security system.
- **Self-organizing:**A wireless sensor network is considered self-organized instead of deterministic. The designed solutions must accommodate this feature because, in a typical scenario, a neighbor sensor in a WSN won't know in advance which node it corresponds to, nor will the number of sensors, sink nodes, distance between nodes, needed power consumption, or even the data transmission rate be known in advance. This guarantees the sensor network's security and calls for flexibility.

5. Data and Routing security in WSN

WSNs are vulnerable to various assaults because of resource constraints, self-organization, and dynamic topology. Data compiled from network resources may exhibit network fluctuation because of these assaults. Researchers have created several security techniques to solve these issues, including key management, certification and authentication, re-keying, cluster head selection schemes, and more.

To reduce network overhead and stop sinkhole attacks, hello flooding, and selective forwarding, the SLEACH [38] protocol has been developed. However, storage capacity is limited, and network failure issues arise with conventional cryptographic techniques like encryption and SLEACH. ECC was introduced to give more robust security with a smaller key size to overcome these issues.

According to [39] work, cluster heads may quickly aggregate encrypted data and gather it without decryption, thanks to the homomorphic encryption technique. ECC and homomorphic encryption schemes were presented by [40] to enable safe data transfer over the WSN. The study aims to extend the network's lifespan by producing private and public keys for sensor nodes using the ECC technique.

Nevertheless, safe data collecting and data analytics for identifying malicious attacks in WSNs have not been the emphasis of any approaches now in use to identify different types of assaults. In literature studies, ad-hoc networks, mobile phones, data analytics, and secure data collecting have received scant attention. While classifying anomaly detection techniques, [41]the attack detection model did not assess performance or concentrate on data security.

Routing protocols are critical to WSN security and are regarded as basic network restrictions. Numerous routing protocols, including multipath routing schemes, location-based routing protocols, hierarchical routing protocols, linear routing protocols, and quality of services (quality of service), have been shown and categorized according to their characteristics and routing topology. SLEACH is widely used for secure WSN routing, where cluster heads are chosen in a dispersed order.

In order to ensure quality of service and support a wide range of IoT applications, [42] suggested a computational model for the ensuing routing protocol for quality of service. In order to fulfill the needs for validity and reliability of WSNs as well as defend against denial-of-service attacks, [43] developed a selective authentication architecture. [44] described a multipath safe routing architecture for MANET that is energy-efficient, QoS-aware, and secure. It makes use of the Cuckoo search algorithm to determine safe pathways.

The increasing number of WSN applications presents several issues for QoS-based communication. A unique technique to link quality-based routing was given by [45], which improves the lifespan of the whole network by selecting relay nodes. A QoS-based multipath routing system was introduced by [46]. It permits several pathways between source and sink nodes, increasing network overhead and improving the data delivery ratio with optimal latency.

Table 7: Classification of Security Attacks in WSNs

Type of Attack	**Need for Security**	**Layer**	**Threat Type**	**Attacks**
Flooding attack	Interruption	Network	Availability	Active
Replay attack	Interruption, Interception	Network	Availability, Confidentiality	Active
Flooding attack	Interruption	Network	Availability	Active
Replay attack	Interruption, Interception	Network	Availability, Confidentiality	
Sinkhole attack	Modification, Fabrication	Network	Integrity, confidentiality, Availability	Active
Spoofing attack	Interruption, Interception	Network	Authenticity, Availability	Active
Sybil attack	Interruption, Interception	Network	Authenticity, Availability	Active

Selective forwarding attacks	Interruption, Interception	Network	Confidentiality, Availability	Active
Session hijacking	Interruption	Transport	Availability	Active
Malicious node attack	Interruption	Application	Availability	Active
Traffic analysis	Interception	Network	Confidentiality	Passive
Packet Tracing	Interception	MAC Layer	Confidentiality	Passive
Jamming attack	Modification	MAC Layer	Integrity, Availability	Active
Blackhole attack	Interruption, Interception	Network	Integrity, confidentiality, availability	Active
Redundant data sorting attack	Interruption, Modification	Application	Integrity, availability	Active
Time synchronization attack	Interruption	Application	Availability	Active
Packet dropping attack	Interruption	Network	Availability	Active
Transmission Failure	Modification	Network	Integrity, confidentiality, availability	Active/Passive
Node duplication	Modification,	Physical Layer	Integrity, Availability	Active
Passive data collection	Modification	Physical Layer	Integrity, availability, confidentiality	Active

Specific performance parameters, including energy conservation, network longevity, packet delivery ratio, delay, throughput, computation, and communication cost, are the subject of most WSN security research investigations. While network topology and other performance metrics are dynamic, some survey papers focus mainly on attack types and do not provide a thorough performance analysis [47,48].

Numerous measurements about attack detection techniques and security metrics in WSNs are identified in the literature review. By considering a variety of performance indicators, approaches, and simulation tools, this thorough survey offers a concise summary and essential contributions to WSN security systems. Figure 4's statistical analysis, which focuses on crucial performance metrics, shows how current research is being done on WSN security. Most recent research focuses on energy saving, with comparatively little done to lower the costs associated with computing and communication. In the current state of WSN security, minimizing communication overhead is essential due to the constrained resources of WSNs and the extra communication overhead that security systems entail. Ensuring WSN security requires bolstering the network lifetime during communication.

Table 5 summarizes the statistical analysis of previous studies for different wireless sensor network security performance criteria.

Performance Parameter	**Focus of Research**	**Key Findings**
Energy Conservation	Most studies centered on optimizing energy usage.	Emphasizes the importance of prolonging network lifetime.
Network Lifetime	Extensive research aimed at extending the operational life.	Strategies include efficient energy management and routing.
Packet Delivery Ratio	Many studies aimed to enhance the efficiency of data delivery.	Highlighted the importance of reliable data transmission.
Delay	Considerable focus on minimizing delays in data transmission.	Critical for real-time applications and response mechanisms.
Throughput	Various approaches are used to improve the overall network throughput.	Key for maximizing data transfer rates within the network.
Computation Cost	Limited research addressing reduction in computational costs.	Potential area for further exploration and optimization.
Communication Cost	Few studies focus on reducing communication overhead.	It presents an opportunity for enhancing network efficiency.

6 Research Issues and Solutions

A Research Issues

Numerous research studies have been conducted on this topic. Additionally, there are still hot and developing areas for scholars to explore. Additionally, advanced domains of this WSN, such as IoT and IoE, are essential, as are subdomains like WBAN and WPAN. IoT is pervasive in this fifth generation. Therefore, researchers can conduct a study and publish a paper on this subject. While there has been a noticeable trend in this domain's growth, core WSN has several drawbacks. It contains seven layers, for example. Every layer faces various problems, such as outdated simulator software and ancient configurations for the simulator tools. Hardware problems exist, such as the need for computers to support devices. Energy use, sensor battery life, and other concerns are also crucial. Instead of those problems, security is the most important one because there are no privacy restrictions. The following are a few significant challenges:

- Node deployment: The primary difficulty with WSN is the deployment of sensor nodes. Deployment must always be done correctly. Suppose there is an entirely pointless deployment, for example, in a critical region where more sensors are required to gather data instead of that necessary deployment. In that case, additional empty sensors are sent to a faraway place.

- Relay node selection: Sensor data is occasionally transmitted from source to destination (sink/base station) for data collection. Information from source nodes is sometimes transferred to the destination via a node (a relay node) to get the quickest path. Numerous steps must be taken to select the shortest route and relay node. Choosing the right strategy for this aim is a highly time-consuming task. Additionally, this takes a lot of time.
- Choosing a cluster head: Cluster head selection is quite tricky, just as relay node selection due to the deployment of grouping nodes in some areas. In that scenario, the cluster head, size, and nodes should be chosen to transmit data to the coordinator (base station). The routing protocol has been created based on this choice.
- Energy consumption: Sensor nodes form the foundation of WSN. So, communication will be interrupted if the battery in the sensor node runs out. As a result, longer-term energy savings require battery power rather than increased energy use.
- Security concerns: These are a significant problem in this sector. An attacker can lose, compromise, or deceive data at any time. Corrupted communications and malicious nodes are also considered security risks.
- Heterogeneity: The situation in which node structures are required can occasionally be ambiguous. It is better to use diverse nodes for health monitoring.
- Pathloss: Numerous issues have arisen in obtaining multipath for the most direct data transmission. For many people, path loss is a significant issue. This occurs not just on multipath paths but also on single-path or direct paths.
- Delay: Time is a fundamental unit of measurement during the transfer of data and messages. For WSN, a nanosecond delay is significant. This delay may impede the delivery of the message and acknowledgment.
- Failure of the system: The leading causes of this include sensor node physical damage, hardware-software malfunctions, etc. This scenario might arise in WSN for both client-server architectures.

B. Effective,secure solutions

Even though there are a lot of challenges in this subject, experts are continually working to find solutions. Researchers may conduct several updates on their work by using an advanced simulator with suitable hardware. Computer experts are constantly upgrading gadgets, which will benefit their studies. In general, studies are attempting to provide insight into the network lifespan of sensor batteries. Cryptography algorithms are also being developed to increase field security. Below are several solutions as listed:

- Maintaining a non-ad-hoc network topology, or one that is well-planned and structured, is essential for node deployment.
- The choice of relay node should be made using the Euclidean distance method, which calls for maintaining an equal distance between the relay and the source node.
- The KNN method and k-means clustering should be the basis for choosing the cluster head node. You can fit a better algorithm somewhere.

- Reducing energy usage can occur when the multi-hop routing protocol is followed. Less energy can be used when the shortest path is selected. It directly relates to the longevity of the network. Therefore, more significant energy savings translate into extended sensor battery nodes and network lifetimes.
- Data confidentiality, integrity, and authentication are there to provide security. Data should be encrypted using cryptography techniques to prevent data theft. Specific procedures like verification should be implemented to ensure the data is legitimate. Data integrity always verifies whether received data matches previously sent data.
- Fault tolerance is a mechanism used in WSNs to quantify system failure and can withstand many forms of failure.

Conclusion

This paper studies WSN security concerns and defensive strategies to safeguard transmission availability, confidentiality, integrity, and authenticity against hostile wireless assaults. Due to their many additional vulnerabilities, including changeable network topology, resource-constrained nodes, broadcast nature of the medium, and absence of physical infrastructure, WSN security is a rapidly developing field of study. The research covered several dangers and security issues, as well as the benefits and drawbacks of using the public critical cryptography technique to meet security requirements. Wireless assaults and security risks are examined at various OSI protocol tiers and current defenses. Security is crucial in many real-time WSN applications that are used in practice.

References

[1] BenSaleh MS, Saida R, Kacem YH, Abid M. Wireless sensor network design methodologies: A survey. Journal of Sensors. 2020 Jan 25;2020:1-3.

[2] Prodanović R, Rančić D, Vulić I, Zorić N, Bogićević D, Ostojić G, Sarang S, Stankovski S. Wireless sensor network in agriculture: Model of cyber security. Sensors. 2020 Nov 25;20(23):6747.

[3] Jia XC. Resource-efficient and secure distributed state estimation over wireless sensor networks: A survey. International Journal of Systems Science. 2021 Dec 10;52(16):3368-89.

[4] Nakas C, Kandris D, Visvardis G. Energy efficient routing in wireless sensor networks: A comprehensive survey. Algorithms. 2020 Mar 24;13(3):72.

[5] Keerthika M, Shanmugapriya D. Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Transitions Proceedings. 2021 Nov 1;2(2):362-7.

[6] Shahzad F, Pasha M, Ahmad A. A survey of active attacks on wireless sensor networks and their countermeasures. arXiv preprint arXiv:1702.07136. 2017 Feb 23.

[7] Padmavathi DG, Shanmugapriya M. A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576. 2009 Sep 3.

[8] Luo X, Ji X, Park MS. Location privacy against traffic analysis attacks in wireless sensor networks. In2010 International Conference on Information Science and Applications 2010 Apr 21 (pp. 1-6). IEEE.

[9] Numan M, Subhan F, Khan WZ, Hakak S, Haider S, Reddy GT, Jolfaei A, Alazab M. A systematic review on clone node detection in static wireless sensor networks. IEEE Access. 2020 Mar 24;8:65450-61.

[10] Gaware A, Dhonde SB. A survey on security attacks in wireless sensor networks. In2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) 2016 Mar 16 (pp. 536-539). IEEE.

[11] Ryu J, Yu J, Noel E, Tang KW. Node ID assignment in group theoretic graphs for WSNs. In2011 Wireless Telecommunications Symposium (WTS) 2011 Apr 13 (pp. 1-8). IEEE.

[12] Verma R, Darak SJ, Tikkiwal V, Joshi H, Kumar R. Countermeasures against jamming attack in sensor networks with timing and power constraints. In2019 11th International Conference on Communication Systems & Networks (COMSNETS) 2019 Jan 7 (pp. 485-488). IEEE.

[13] Rehman AU, Rehman SU, Raheem H. Sinkhole attacks in wireless sensor networks: A survey. Wireless Personal Communications. 2019 Jun 30;106:2291-313.

[14] Giri D, Borah S, Pradhan R. Approaches and measures to detect wormhole attack in wireless sensor networks: a survey. InAdvances in Communication, Devices and Networking: Proceedings of ICCDN 2017 2018 (pp. 855-864). Springer Singapore.

[15] Jilani SA, Koner C, Nandi S. Security in wireless sensor networks: attacks and evasion. In2020 National conference on emerging trends on sustainable technology and engineering applications (NCETSTEA) 2020 Feb 7 (pp. 1-5). IEEE.

[16] Bharti D, Nainta N, Monga H. Performance Analysis of Wireless Sensor Networks under adverse scenario of attack. In2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) 2019 Mar 7 (pp. 826-828). IEEE.

[17] Gill RK, Sachdeva M. Detection of hello flood attack on LEACH in wireless sensor networks. InNext-Generation Networks: Proceedings of CSI-2015 2018 (pp. 377-387). Springer Singapore.

[18] Sasi SB, Dixon D, Wilson J, No P. A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security. IOSR Journal of Engineering. 2014 Mar;4(3):1.

[19] Amin F, Jahangir AH, Rasifard H. Analysis of public-key cryptography for wireless sensor networks security. International Journal of Computer and Information Engineering. 2008 May 21;2(5):1448-53.

[20] Gulen U, Alkhodary A, Baktir S. Implementing RSA for wireless sensor nodes. Sensors. 2019 Jun 27;19(13):2864.

[21] Chatterjee U, Ray S, Adhikari S, Khan MK, Dasgupta M. An improved authentication and key management scheme in context of IoT-based wireless sensor network using ECC. Computer Communications. 2023 Sep 1;209:47-62.

[22] Saqib N, Iqbal U. Security in wireless sensor networks using ECC. In2016 IEEE International Conference on Advances in Computer Applications (ICACA) 2016 Oct 24 (pp. 270-274). IEEE.

[23] Studer A, Bai F, Bellur B, Perrig A. Flexible, extensible, and efficient VANET authentication. Journal of Communications and Networks. 2009 Dec;11(6):574-88.

[24] Ying B, Makrakis D, Mouftah HT. Privacy preserving broadcast message authentication protocol for VANETs. Journal of Network and Computer Applications. 2013 Sep 1;36(5):1352-64.

[25] Lin X, Sun X, Wang X, Zhang C, Ho PH, Shen X. TSVC: Timed efficient and secure vehicular communications with privacy preserving. IEEE transactions on wireless communications. 2008 Dec 22;7(12):4987-98.

[26] Zhang C, Lu R, Lin X, Ho PH, Shen X. An efficient identity-based batch verification scheme for vehicular sensor networks. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications 2008 Apr 13 (pp. 246-250). IEEE.

[27] Biswas S, Mišić J. A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs. IEEE Transactions on Vehicular Technology. 2013 Jan 9;62(5):2182-92.

[28] Lo NW, Tsai JL. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Transactions on Intelligent Transportation Systems. 2015 Dec 31;17(5):1319-28.

[29] Chatterjee U, Ray S, Adhikari S, Khan MK, Dasgupta M. An improved authentication and key management scheme in context of IoT-based wireless sensor network using ECC. Computer Communications. 2023 Sep 1;209:47-62.

[30] Jiang Y, Shi M, Shen X, Lin C. BAT: A robust signature scheme for vehicular networks using binary authentication tree. IEEE Transactions on Wireless Communications. 2008 Nov 17;8(4):1974-83.

[31] Zia T, Zomaya A. Security issues in wireless sensor networks. In2006 International Conference on Systems and Networks Communications (ICSNC'06) 2006 Oct 29 (pp. 40-40). IEEE.
[32] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019 Nov 13;22(1):616-44.
[33] Singh R, Singh DK, Kumar L. A review on security issues in wireless sensor network. journal of Information Systems and Communication. 2010 Jan 1;1(1):1.
[34] Ahmed M, Huang X, Sharma D, Shutao L. Wireless sensor network internal attacker identification with multiple evidence by dempster-shafer theory. InAlgorithms and Architectures for Parallel Processing: 12th International Conference, ICA3PP 2012, Fukuoka, Japan, September 4-7, 2012, Proceedings, Part II 12 2012 (pp. 255-263). Springer Berlin Heidelberg.
[35] Tseng CH, Wang SH, Tsaur WJ. Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection. IEEE Transactions on Reliability. 2015 May 13;64(3):1078-85.
[36] Yang G, Dai L, Si G, Wang S, Wang S. Challenges and security issues in underwater wireless sensor networks. Procedia Computer Science. 2019 Jan 1;147:210-6.
[37] Ferrari P, Giorgi G, Narduzzi C, Rinaldi S, Rizzi M. Timestamp validation strategy for wireless sensor networks based on IEEE 802.15. 4 CSS. IEEE Transactions on Instrumentation and Measurement. 2014 Jun 12;63(11):2512-21.
[38] Daanoune I, Abdennaceur B, Ballouk A. A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. Ad Hoc Networks. 2021 Apr 1;114:102409.
[39] Zhou Q, Yang G, He L. A secure-enhanced data aggregation based on ECC in wireless sensor networks. Sensors. 2014 Apr 11;14(4):6701-21.
[40] Elhoseny M, Elminir H, Riad A, Yuan X. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences. 2016 Jul 1;28(3):262-75.
[41] Xie H, Yan Z, Yao Z, Atiquzzaman M. Data collection for security measurement in wireless sensor networks: A survey. IEEE Internet of Things Journal. 2018 Nov 25;6(2):2205-24.
[42] Ali S, Humaria A, Ramzan MS, Khan I, Saqlain SM, Ghani A, Zakia J, Alzahrani BA. An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International journal of distributed sensor networks. 2020 Jun;16(6):1550147720925772.
[43] Li G, Yan Z, Fu Y, Chen H. Data fusion for network intrusion detection: a review. Security and Communication Networks. 2018 May 15;2018.
[44] Kasthuribai PT, Sundararajan M. Secured and QoS based energy-aware multipath routing in MANET. Wireless Personal Communications. 2018 Aug;101:2349-64.
[45] Bapu BT, Gowd LS. Link quality based opportunistic routing algorithm for QOS: aware wireless sensor networks security. Wireless Personal Communications. 2017 Nov;97:1563-78.
[46] Deepa O, Suguna J. An optimized QoS-based clustering with multipath routing protocol for wireless sensor networks. Journal of King Saud University-Computer and Information Sciences. 2020 Sep 1;32(7):763-74.
[47] Jing X, Yan Z, Pedrycz W. Security Data Collection and Data Analytics in the Internet. Institute of Electrical and Electronics Engineers.
[48] Lin H, Yan Z, Chen Y, Zhang L. A survey on network security-related data collection technologies. IEEE Access. 2018 Mar 21;6:18345-65.