

A Survey of Detection and Mitigation Approaches for Network Layer Security Attacks in Wireless Sensor Networks

Rajwinder Kaur^{*1}, Gurjinder Singh² and Jasmininder Kaur Sandhu³

^{1,2}Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

³IILM university, Greater Noida

*rajwinder.k@chitkara.edu.in

Received: 24th April, 2026; Revised: 20th May 2026; Accepted: 30th June, 2026; Available Online: 10th July, 2026

ABSTRACT

Wireless sensor networks (WSNs) are vulnerable to various security attacks on the network layer due to their wireless nature, resource constraints, and deployment in hostile environments. These attacks include sinkhole, Sybil, wormhole, and blackhole assaults which can adversely damage the performance and reliability of WSNs. In this study, we take a look at the several recently proposed mitigation approaches for identifying and avoiding such network layer assaults. We begin with a high-level introduction to WSNs and the most popular forms of network-layer attacks. We next provide a brief overview of the many processes that may be used to ensure the safety of wireless sensor networks, including intrusion detection systems, trust management, cryptography, and authentication. Each strategy's advantages and disadvantages are discussed. Finally, we provide perspectives on unresolved research questions and potential future approaches for advancing the state-of-the-art, WSN-specific security solutions.

Keywords: *Wireless sensor networks, network layer attacks, intrusion detection, trust management, cryptography, authentication*

How to cite this article: Kaur R, Singh G and Sandhu JK, A Survey of Detection and Mitigation Approaches for Network Layer Security Attacks in Wireless Sensor Networks. *Int J Drug Deliv Technol.* 2026;16(8): 91-101; DOI: 10.25258/ijddt.16.8.7

Source of support: Nil.

Conflict of interest: None

1. INTRODUCTION

1.1 Overview of wireless sensor networks (WSNs)

WLANs (WSNs) are a new and hopeful technology that could be used for a lot of different tracking and control tasks. These tasks include health care, smart cities and homes, controlling industrial processes, and keeping an eye on the environment (Akyildiz et al., 2002), (Khan et.al. 2026). A WSN is made up of many low-cost, low-power, multifunctional sensor nodes that are grouped together in an area that is not being watched (Yick et al., 2008). These sensor points are spread out in different areas and keep an eye on things like temperature, shaking, pressure, motion, pollution, and sound (Jiang et al., 2016). They work together to make a network, and their data is sent to a central place, called a sink node (Alcaraz et al., 2010).

Because they are small and expensive, the sensor nodes don't have a lot of memory, power, or processing power (Sharma et al., 2010). One or more sensors, a processor, memory, a radio receiver, and a power source are built right into them (Singh et al., 2010). The nodes generally run on batteries and only have a small amount of energy stored. They use technologies like WiFi, Bluetooth, ZigBee, or 6LoWPAN (Gubbi et al., 2013) to talk to each other wirelessly. The sink node links the WSN to a public network, like the Internet, so sensor data can be sent to a user far away. WSNs are better than standard wired sensor systems because they can be set up quickly, can organise themselves, can handle errors, are cost-effective, and can adapt to different settings (Yick et al., 2008).

*Author for Correspondence: rajwinder.k@chitkara.edu.in

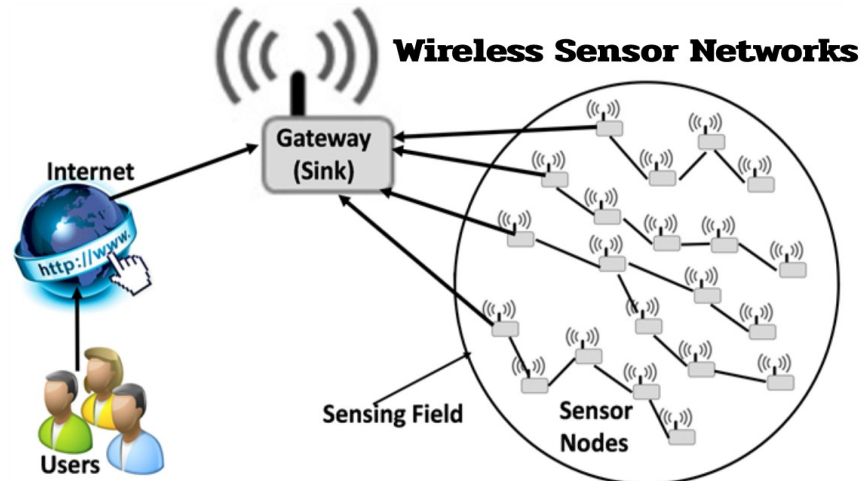


Figure 1: Representation of WSN environment

1.2 Security threats and attacks in WSNs

Even though WSNs have many benefits, they are very open to many types of security risks and attacks because wireless communication is spread, there isn't much infrastructure, sensor nodes don't have a lot of resources, and they are often used in dangerous places (Sharma et al., 2010; Jiang et al., 2016). Attackers can use these flaws to start different kinds of attacks against WSNs and stop them from working normally. Different parts of the wireless sensor networking protocol stack are attacked in this way (Abouelkheir et al 2022). In the layer architecture includes the 5 layer of network namely: physical, data link, network, transport, and application (Sharma et al., 2010). Some of the most important security goals for WSNs are availability, denial-of-service threats resistance, confidentiality, integrity, and identification (Da Silva et al., 2005). But because sensor nodes don't have a lot of resources, it's hard to provide full security in WSNs. To get around these problems, we need protection methods that are small and use little energy.

1.2.1. Attacks on the network layer

The network layer of the protocol stack is responsible for routing sensor data from the source node to the sink node (Sharma et al., 2010). It provides vital connectivity and

data forwarding services. Hence, various types of attacks are directed at the network layer which aim to disrupt, subvert or exploit the multi-hop routing functionality of WSNs (Singh et al., 2010; Sharma et al., 2010). These include sinkhole, Sybil, wormhole, and blackhole attacks which can severely degrade network performance and prevent the sink node from receiving critical sensor data.

A. Sinkhole attack

The goal of an adversary in a sinkhole attack is to get almost all traffic from a certain area to go through a hacked node, putting the adversary in the middle of a sinkhole (Sharma et al., 2010). The offender might be able to do this by making the compromised node look especially appealing to nodes nearby in terms of routing measures like bandwidth, latency, or node stability (Krontiris et al., 2007). After that, network data is collected at the sinkhole, where it is changed, thrown away, or sent to the sink only in some cases (Sharma et al., 2010). More complicated attacks, such as selective sending, tunnel attacks, and so on, can be built on top of this type of attack. Sinkhole attacks are hard to spot because the offender changes route information in a roundabout way, which stops data from flowing as it should (Krontiris et al., 2007).

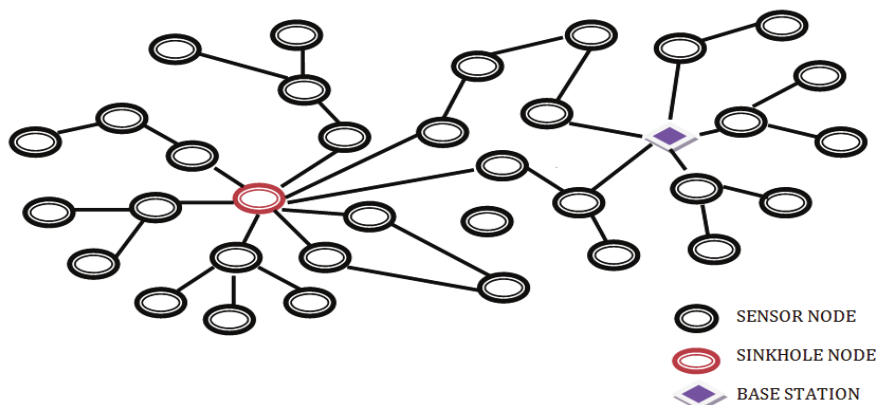


Figure 2 Sinkhole attack

B. Sybil Attack

In a Sybil attack, a single node presents multiple identities to other nodes in the WSN by masquerading as several different nodes (Sharma et al., 2010). This is achieved by impersonating other trusted nodes or simply claiming false identities. This allows the malicious node to exert disproportionate influence over the network and

significantly control the routing topology. For example, a Sybil attack can manipulate a distributed storage system to store multiple copies of malicious data by presenting multiple forged identities (Douceur, 2002). Sybil attacks are especially damaging in geographical routing protocols which rely on location information.

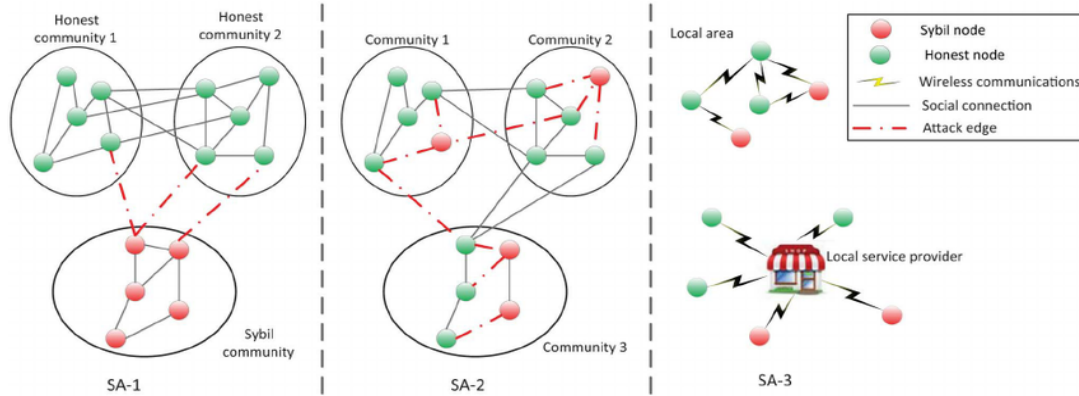


Figure 3 Sybil attack

C. Wormhole Attack

An offender launches a wormhole attack by taking packets from one place in the network and sending them through a path to another place in the network, where they are sent back into the network (Sharma et al., 2010). A wormhole is the name for this tunnel between two strikes that are working together. It makes it possible for a packet to move faster than routes with multiple hops, which changes the structure of a wireless multi-hop network. Wormhole

attacks can weaken routing systems by taking over and short-circuiting routing paths (Hu et al., 2006). For instance, an attacker close to the sink node could send messages from nodes far away straight to the sink, making it look like they are only one hop away. This lets the bad node change the flow of data, attack with a DoS attack, or attack the data in other ways. Wormhole attacks are hard to spot because the network can't see the indirect link between attackers who are working together.

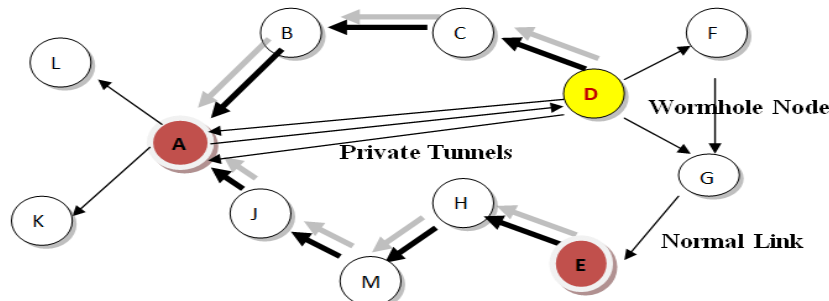


Figure 4 Wormhole attack in WSN

D. Blackhole Attack

In a this, the attacker node falsely shows attractive routing data to neighboring nodes to lure them to route packets destined to the sink through it (Sharma et al., 2010). However, the attacker drops or discards the intercepted packets without forwarding them to the sink. Instead, the packets are lost or consumed at the malicious node – analogous to a blackhole. This effectively denies a range of network services to the packets originating from nodes that route through the blackhole node. This attack can allow an adversary to selectively target and block transmission of critical sensor data while dropping other

routine data (Singh et al., 2010). Blackhole attacks can severely degrade network throughput and performance. The counterfeit routing information makes such attacks hard to detect.

These common network layer attacks highlight the vulnerabilities in multi-hop wireless routing and the need for robust security mechanisms tailored for resource-constrained WSNs. In the next section, we survey the intrusion detection, trust management, cryptography and authentication techniques proposed specifically to mitigate such routing attacks in WSNs.

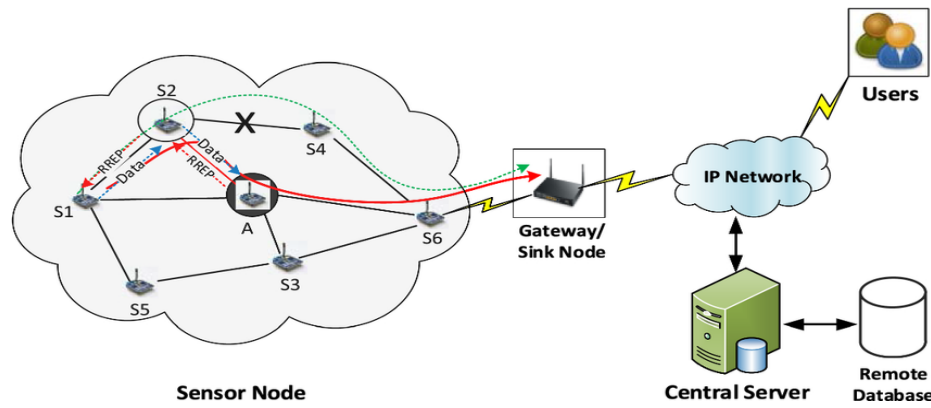


Figure 5 Blackhole attack in WSN

2. MITIGATION TECHNIQUES

2.1 Intrusion Detection Systems (IDS)

An important security method for finding intrusions or attacks is to keep an eye on events and look for signs of them (Butun et al., 2014). It looks like intrusion detection

systems (IDS) could be a good way to protect WSN from threats. IDS systems try to find bad nodes that start attacks by looking at network traffic or node actions and finding any patterns that don't make sense (da Silva et al., 2005). IDS can be broken down into two groups as defined below:

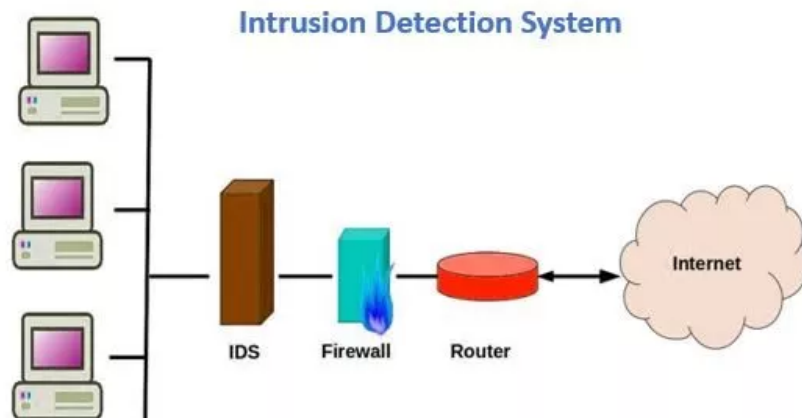


Figure 6: Basic flow of IDS

a. Signature-based IDS (SBIDS)

It is also called misuse-based IDS, which rely on a database of attack signatures or patterns of known threats and vulnerabilities (Sharma et al., 2010). The IDS analyzes the monitored events such as packets or log files to match any pre-defined attack signatures (Rassam et al., 2013). The signature database needs to be updated whenever new attack patterns are discovered. Signature-based techniques are very effective at detecting known attacks with low false positive rates. However, they fail to identify new and unknown (zero-day) intrusions. Some examples of SBIDS proposed for WSNs include the following:

- Sensed-Trust (Bao et al., 2012) builds a threat model that characterizes common routing attacks such as selective forwarding, sinkhole, Sybil, wormhole etc. Attack patterns are translated into unique attack signatures which are distributed to nodes for local pattern matching.
- Ye et al. (2005) design a distributed IDS where nearby cluster heads exchange signatures to detect attacks

across clusters. The sink can also broadcast updated attack signatures network-wide.

- Security-SPINS (Adnan et al., 2013) incorporates lightweight cryptographic primitives into SNEP protocol for authentication and integrity verification. Signatures of known malicious nodes are distributed by the sink to detect compromised nodes.

The main advantages of SBIDS approaches are high detection accuracy, low false positives, and resource efficiency for known attack patterns (Rassam et al., 2013). However, these systems have limited generalization capabilities against new attacks and threats. Frequent signature updates lead to additional communication overheads. Storing signature databases on memory-constrained sensor nodes also poses challenges.

b. Anomaly-Based IDS

Anomaly-based IDS solutions build statistical models of normal network behavior such as traffic load, packet flow, node activities etc. (Sharma et al., 2010). They detect attacks by identifying significant deviations from the established baseline (Rassam et al., 2013). Such systems

can uncover previously unknown threats. However, they suffer from high false positives due to inaccuracies in normal behavior modeling. Anomaly detection is commonly implemented using machine learning, statistical and data mining techniques. Some examples of anomaly-based WSN IDS include:

- Lu et al. (2010) apply data mining algorithms to audit data collected from cluster heads to detect anomalous packets and identify Sybil nodes.
- Rajasegarar et al. (2008) use one-class support vector machines (SVM) to model normal sensor data and detect outliers as possible attacks.
- Da Silva et al. (2005) propose an IDS agent for each node that builds threat models using time-series forecasting of metrics like bandwidth, frequency of soft errors etc.
- Lee et al. (2007) use a reputation-based system where nodes monitor neighbors and assign reputation scores based on behavior. Nodes with scores below a threshold are designated malicious.

The main advantage of anomaly detection is the ability to detect novel zero-day attacks (Sharma et al., 2010). However, high computational complexity of data analysis techniques poses challenges for resource-constrained WSNs. Anomaly IDS also suffer from high false positive rates. Maintaining normal behavior profiles that adapt to changing network conditions is difficult.

c. *Strengths and Weaknesses*

The detection capabilities, resource requirements and accuracy of signature-based and anomaly-based approaches are complementary in nature (Jan et al., 2017). Combining these two techniques can help overcome some of the individual limitations. Hybrid IDS solutions aim to integrate both signature matching and anomaly detection components. For example, da Silva et al. (2005) propose using a lightweight signature-based IDS as the first line of defense on all nodes along with more complex anomaly detection on selected monitor nodes.

Overall, IDS can provide early warning against different types of network layer attacks in WSNs (Sharma et al., 2010). However, IDS technologies must overcome challenges like resource constraints, dynamic topologies, high packet losses and node failures (Rassam et al., 2013). IDS systems designed for traditional networks do not directly apply to WSNs which require energy-efficient and distributed security solutions. Lightweight IDS optimized for accuracy, low communication overhead, and modest resource usage represent a promising direction for mitigating attacks in WSNs.

2.2 Trust management: Trust management is an important approach for securing wireless sensor networks, especially against insider attacks launched by compromised nodes (Bao et al., 2012). Trust management solutions aim to develop robust mechanisms for establishing trust relationships between nodes and identifying malicious or

untrustworthy nodes (Sharma et al., 2010). This allows isolating adversary nodes and taking actions such as blocking or blacklisting them. Various computational trust models have been proposed for WSNs based on monitoring node behavior and maintaining reputation scores.

a. Reputation Systems: Reputation represents the perception of a node's behavior over time based on either direct observations or recommendations from other nodes (Bao et al., 2012). In reputation systems, nodes continuously rate and collect feedback about the trustworthiness of other nodes to distinguish between well-behaved and malicious nodes (Ganeriwal & Srivastava, 2004). Metrics such as remaining energy, frequency of abnormal actions, adherence to protocols etc. are used to calculate reputation scores (Bao et al., 2012). Nodes with scores below a threshold are tagged as malicious. Reputation data can be shared in a distributed manner to isolate adversaries. Some examples of reputation-based trust systems for WSNs include:

- Ganeriwal & Srivastava (2004) propose a decentralized reputation-based framework for sensor networks where nodes monitor neighbors, rate their behavior based on direct observations and recommendations, and calculate reputation scores using a weighted voting algorithm.
- Shaikh et al. (2009) design a group-based trust management scheme where cluster heads monitor member nodes and assign reputation levels which are shared with other clusters.
- Momani et al. (2010) develop a trust-based model using fuzzy logic and weighted voting to compute node reputation scores using parameters like remaining battery power, longevity and packet dropping frequency.
- Bao et al. (2012) introduce a dynamic trust management protocol where sensor nodes continuously monitor their neighbors and update reputation values to identify malicious nodes launching attacks.

The main advantage of reputation systems is detection of insider attacks by compromised legitimate nodes using localized monitoring of nodes (Bao et al., 2012). Malicious nodes can be isolated based on global reputation scores calculated in a distributed manner. However, increased network overhead for reputation sharing and false positives due to subjectivity of trust evaluation pose key challenges (Mohanraj, K., et al. 2024).

b. Behavior monitoring: Behavior monitoring techniques aim to develop trust relationships between nodes by passively monitoring the actions and communications of neighboring nodes (Bao et al., 2012). Behavior profiles are created based on activity patterns such as communications, transactions, resource usage, mobility etc. (Shaikh et al., 2009). Deviations from normal

established behavior trigger suspicion about possible malicious actions. Some examples of behavior monitoring based trust management schemes include:

- Shaikh et al. (2009) propose a group-based scheme where a centralized cluster head observes member node behavior during communications and sharing of sensor data to detect anomalies.
- Ganeriwal et al. (2008) design a distributed framework where a continuous beta reputation system is maintained using direct and indirect observations of neighbors' behavior.
- Du et al. (2005) introduce a trust model based on direct monitoring and indirect recommendations. Nodes monitor one-hop neighbors for abnormal packet drop and delay behavior to evaluate trustworthiness.
- Sun et al. (2007) establish multi-dimensional trust vectors for each node based on monitoring behavior parameters like data consistency, intrusion detection outcomes, anomaly detection results etc.

Behavior monitoring enables passive evaluation of trust levels without additional overhead (Du et al., 2005). However, such techniques are vulnerable to sophisticated attacks that mimic normal behavior patterns. Differentiating between actual anomalies and natural environmental variations also poses challenges.

Strengths and weaknesses

The main advantage of trust management is the ability to handle insider attacks and maintain dynamic trust relationships despite changing network conditions and adversary behavior (Bao et al., 2012). However, increased communication and computation overhead, complex trust aggregation algorithms, ambiguities in trust evaluation, and resilience to sophisticated attacks remain open research issues. Hybrid mechanisms that combine reputation systems and behavior monitoring along with other techniques like machine learning can help build robust trust models for mitigating network layer attacks in WSNs (Sun et al., 2007).

2.3 Cryptography: To protect wireless sensor networks from security risks, cryptographic methods are very important. They do this by offering basic security functions like privacy, authentication, data integrity, and access control (Sharma et al., 2010). Different kinds of network layer threats can be stopped by using lightweight cryptographic methods that are designed to work with WSNs' limited resources. Two main types of cryptography that have been suggested for protecting WSNs are symmetric key cryptography and public key cryptography.

Cryptography with symmetric keys.

- When two nodes talk to each other, symmetric key cryptography uses a shared secret key for both encryption and decryption (Sharma et al., 2010). Both sides of the conversation use the same key, which makes it easy to share keys. But this also means that the key has to be shared ahead of time and kept secret

between the people who are talking. For WSNs, different key pre-distribution methods and symmetric cyphers have been created, such as

- Random key pre-distribution: This method creates a big pool of keys and gives each sensor node a random set of keys from this pool (Eschenauer & Gligor, 2002). Shared key finding methods let nodes agree on a key.
- In pairwise key pre-distribution, a different key is given to each possible pair of nodes. But this needs a lot of memory to store $N-1$ keys on each node of a network with N nodes (Chan et al., 2003).
- An energy-efficient block cypher called Hummingbird (Großschädl et al., 2005) is based on modular math processes.
- Law et al. (2006) describe RC5, AES, and Skipjack block cypher methods that work best on motes with few resources.

Symmetric cryptography provides confidentiality, integrity and authentication for securing routing and data forwarding against attacks like sinkholes, selective forwarding etc. (Sharma et al., 2010). However, key distribution, revocation and storage poses challenges. Public sensors are susceptible to physical capture of nodes and theft of stored keys.

a. Public Key Cryptography

Asymmetric key pairs, with a secret key and a public key for each server, are used in public key cryptography (Sharma et al., 2010). The private key makes signatures and decrypts data, while the public key encrypts data and checks signatures. Public keys can be shared freely without putting security at risk. Public key methods, on the other hand, require a lot more computing power than symmetric cyphers. Some public key cryptography methods that have been suggested for WSNs are:

- TinyPK which provides a public key infrastructure using identity-based encryption and ECC-based digital signatures for distributed sensor networks (Shi & Perrig, 2004).
- TinyECC implementing ECC for key generation (Liu & Ning, 2008).
- NanoPK providing a naming and identity layer integrated with public key security (Aman et al., 2019).
- Key regeneration protocol using public keys of base stations and sensors to generate distributed private keys (Deng et al., 2005)

Public key cryptography provides robust solutions for authentication, non-repudiation and key distribution for WSNs (Shi & Perrig, 2004). However, the intensive computations require hardware acceleration and optimized implementations to be feasible on sensor nodes (Großschädl et al., 2006).

Strengths and Weaknesses

Symmetric key cryptography is efficient but vulnerable to node capture attacks that reveal secret keys (Sharma et al., 2010). Public key schemes offer stronger security guarantees but at the cost of higher overheads. Hybrid mechanisms that optimize symmetric ciphers for bulk data encryption and public key cryptography for key distribution and management provide a balanced approach (Huang et al., 2005). Lightweight cryptographic protocols designed for the unique scale, dynamics, and constraints of WSNs are essential to enable security at the network layer. Standard cryptographic protocols require adaptation to efficiently mitigate resource depletion, DoS, spoofing, alteration and eavesdropping attacks on sensor network communications with modest overheads.

2.4 Authentication

Authentication enables verifying the identities of communicating nodes in a network and ensuring message integrity (Sharma et al., 2010). Attackers often masquerade as legitimate nodes or tamper with packets to disrupt routing. Lightweight authentication protocols designed for resource-constrained WSNs can mitigate impersonation attacks, Sybil attacks and message manipulation. Cryptographic authentication techniques proposed for WSNs include encryption, digital signatures, and hash chains.

a. Encryption and digital signatures

Symmetric encryption with message authentication codes (MAC) can provide authentication along with confidentiality by verifying knowledge of shared keys (Ren et al., 2008). The message payload and a MAC are encrypted using a secret key. The receiver decrypts the message and recomputes the MAC to authenticate the source. However, symmetric techniques are vulnerable if keys are compromised.

Public key digital signatures based on asymmetric cryptography allow strong source authentication using private signing keys (Ren et al., 2008). The signature is generated by the sender using its private key over the

hashed message. The destination node verify the source node key. This prevents spoofing and impersonation attacks. Signature schemes designed for WSNs include TinySec, TinyPK, and ECDSA (Shi & Perrig, 2004; Liu & Ning, 2008).

The advantage of cryptographic authentication is strong protection against identity spoofing, man-in-the-middle attacks, and message forgery with low communication overhead (Sharma et al., 2010). However, the processing and energy costs of encryption and signature verification pose challenges.

b. One-way hash chains

Hash chains generate a chain of keys by iteratively use a hash function (Ren et al., 2008). Each element of the chain authenticates the next element. Hash chains allow efficient source authentication without symmetric ciphers or public key cryptography.

For example, Zhu et al. (2003) propose using hash chains for authentication in the LEAP protocol. The sender discloses the i th key which the receiver hashes i times to verify it matches a previously authenticated value. One-way hash chains prevent identity spoofing and repudiation attacks with low overheads. However, they require temporal synchronization and suffer from replay attacks after chain exhaustion (Ren et al., 2008).

Strengths and Weaknesses

Cryptographic authentication techniques enable strong security guarantees by securely verifying node identities and preventing impersonation attacks, and message forgery (Sharma et al., 2010). However, cryptography often incurs high overheads due to restriction on nodes. Efficient cryptographic protocols optimized for WSN scale and dynamics can provide secure authentication with low communication and computation costs (Huang et al., 2005). Lightweight asymmetric schemes are promising but require hardware acceleration (Shi & Perrig, 2004). Hybrid authentication combining hash chains, MACs and signatures provides a robust and balanced approach for mitigating network layer attacks in WSNs.

Table 1 Comparison table between IDS

IDS Type	Description	Advantages	Disadvantages
Signature-based	Matches monitored events against database of attack signatures	High accuracy, low false positives, efficient for known attacks	Unable to detect new attacks, requires signature database maintenance
Anomaly-based	Builds model of normal behavior, flags deviations as attacks	Detect novel attacks, no need for signature database	Higher false positives, high computational complexity

Table 2 Taxonomy of trust management techniques for WSN security

Approach	Techniques	Metrics Used	Advantages	Disadvantages
Reputation-based	Distributed reputation systems, weighted voting, fuzzy logic	Remaining energy, packet drops, longevity	Handles insider attacks, isolating adversaries	Communication overhead of reputation sharing, subjectivity in trust evaluation
Behavior monitoring	Activity pattern monitoring, consistency checks	Data transactions, resource usage, mobility	Passive evaluation, no overhead	Unable to detect mimicry attacks

Table 3 Comparison of symmetric and public key cryptography for WSN security

Metric	Symmetric Key	Public Key
Example Schemes	LEAP, RC5, Hummingbird	TinyPK, TinyECC, NanoPK
Key Management	Single shared key, key pre-distribution	Public-private key pairs
Security Services	Confidentiality, authentication using shared keys	Digital signatures, authentication using public keys
Performance	Very efficient, low resource usage	Provide stronger security guarantees but high processing overhead
Weaknesses	Vulnerable to stolen keys, no perfect forward secrecy	Feasible on sensors only with hardware acceleration

3. OPEN RESEARCH ISSUES AND FUTURE DIRECTIONS

While intrusion detection, trust management, cryptography, and authentication techniques provide promising capabilities for securing wireless sensor networks against network layer attacks, several open issues and challenges remain to be addressed through future research.

Improving detection accuracy: Existing IDS solutions for WSNs suffer from issues like high false positives, negatives and limited detection coverage (Rassam et al., 2013). More research is required to develop intelligent detection techniques with high accuracy and low overheads. Hybrid anomaly and signature-based approaches using machine learning can potentially improve detection rates (Jan et al., 2017). Deep learning methods are also being explored for more accurate WSN intrusion detection (Meidan et al., 2018).

Resilience against sophisticated attacks: Most proposed IDS techniques cannot detect intelligent attackers who vary attack strategies to avoid detection (Rassam et al., 2013). Adaptive and context-aware solutions using game theory and adversarial learning are required to predict and mitigate evolving attacks (Singh et al., 2017). Robust trust management protocols are also needed to prevent malicious nodes from deliberately building high reputation over time before launching attacks.

Lightweight security solutions: The constrained resources and embedded nature of WSNs necessitate extremely

lightweight security mechanisms (Sharma et al., 2010). Novel lightweight ciphers, authentication protocols, key distribution schemes, and secure routing protocols optimized for energy, memory, computation, and bandwidth continue to warrant further research. Hardware-enabled security techniques also show promise for accelerating cryptographic operations (More, V., et al. 2024).

Integration of security technologies: While numerous security schemes have been proposed independently, integrating different security capabilities efficiently into a holistic framework remains an open challenge (Sharma et al., 2010). Orchestrating intrusion detection, reputation systems, access control, authentication, key management, and secure routing in a modular architecture is required. Standard interfaces can facilitate interoperability of heterogeneous security solutions.

Secure mobile and IoT integration: Emerging trends like mobility, fog computing and integration with the Internet of Things (IoT) introduce new security requirements and challenges for WSNs (Han et al., 2014). Mobility and fog architectures enable new attacks like location and man-in-the-middle attacks (Han et al., 2014). Heterogeneous IoT ecosystems require unified security frameworks. Cross-layer security solutions warrant investigation for integrated WSN-IoT systems.

AI and machine learning for security: Advances in AI and ML hold great promise for improving threat detection, resilience and automated response in WSNs (Rassam et

al., 2013). Training ML models for WSN security poses challenges due to peculiarities of wireless sensor data and lack of structured large-scale security datasets. Novel adversarial machine learning approaches are also required to handle intelligent attackers.

Security testbeds and tools: There is a lack of standard benchmarks, testbeds and tools for analyzing and validating the effectiveness of WSN security solutions (Sharma et al., 2010). Real-world implementation experiences are also limited. Developing security assessment frameworks, test platforms, simulation environments, and emulation tools can significantly strengthen WSN security research (Iyer & Gandham, 2018).

Cross-layer security: The interdependencies between different protocol layers necessitate cross-layer security solutions rather than layer-specific mechanisms for combating network layer attacks in WSNs (Sharma et al., 2010). Attack-resilient protocols integrated across layers can enhance robustness. For example, a trust manager at the network layer can leverage physical layer information to improve detection accuracy.

Theoretical foundations: Rigorous mathematical models and formal analysis techniques can help provide provable security guarantees for WSN protocols and mechanisms (Sharma et al., 2010). The interactions between fundamental constraints like connectivity, lifetime, and resilience need stronger theoretical understanding. Models from cryptography, game theory, control theory, and optimization can provide useful foundations.

Realizing the potential of WSNs in critical applications requires continuous innovation to address their unique security challenges. Advances in intelligent detection, lightweight security protocols, cross-layer techniques, secure mobility support, integration with emerging paradigms like IoT and fog computing, and adoption of technologies like AI, blockchain, and hardware security hold significant promise for building robust and holistic security solutions against network layer attacks in resource-constrained WSN environments.

4. VISION OF THE RESEARCH

Many researchers focus for maintaining the network security and addressing the attacks. Security is important parameter of every network and when intruder attack on layer they harm the confidential information travel within the network from node to node. Due to the network layer challenges Machine learning hold the command to handle the network and train the model on the basis of data. The application of ML techniques has significantly improved it. However, some unexplored terrain is discussed in this section along with a suggested study agenda. While studying the research paper, it has been analysed that the generic proposed technique for addressing network attacks with common behaviours is very limited. The vision this research for maintaining security and handling attack also provide a generic solution for the same. The network

attacks having common behaviour is elaborated are as follows:

4.1. Sinkhole Attack

A WSN node that has been infected can initiate sinkhole attacks. Since the attacker node presents itself as the fastest way for reaching destination, genuine nodes are forced to pass through it due to routing traffic. Therefore, data packet might be lost and it can be changed or in some cases that can be sent to destination.

4.2. Sybil attack

A hostile router that builds numerous bogus identities to tamper with network protocols including routing, data aggregation, and equitable resource allocation causes a Sybil attack, that destabilizes the wireless sensor network (WSN).

4.3 Wormhole attack

A wormhole attack is a type of DoS attack that malicious nodes conduct by building a pathway that allows data to be looped to other unwanted nodes, thereby interrupting connectivity and tampering with the routing of network traffic.

4.4 Blackhole attack

It happens when a hacker obtains all of the network's data and fails to send it to the intended location. When a malicious node disrupts the whole system and collects every data packet from network and every message that is sent towards the black hole location is seized. There are numerous techniques for mitigating the attack and maintaining the network security. In past decade the focus of study shifted to intrusion detection system (IDS) techniques. IDS is divided into two ways one is signature based and other one is anomaly based. Using a signature-based intrusion detection system observed confidence an attack concept describing typical routing threats including wormhole, sinkhole, sybil, and selective forwarding is created. Trust management developing a trust relationship during communication between the nodes. Cryptography and Authentication and many more techniques are used to handle the attacks. But the mentioned techniques are not able to handle some situation, it handles the single and small-scale network. There is limited generic proposed system that handle the common attacks. However, many researchers are building a ML model to handle specific attack but when we talked about generic way there are limited model proposed for maintaining network performance. Our research focus is to proposed and ensemble model to enhance the network performance and handle the malicious node. This ensemble model also improve the network performance parameters such as throughput, delay, latency, packet loss etc.

5. CONCLUSIONS

WSNs are increasingly adopted for applications but remain highly vulnerable to security attacks on the network layer due to their wireless nature, resource constraints, and deployment in untrusted environments. These attacks like sinkhole, Sybil, wormhole and blackhole attacks can severely impact the performance,

reliability and security of WSNs. This paper reviewed the recent mitigation techniques for handling the security attacks of WSNs.

Intrusion detection systems enable early attack warning by analyzing traffic and node behavior for anomalies and known attack signatures. However, providing accurate detection with low overheads remains a key research challenge. Trust management mechanisms allow isolating malicious nodes by dynamically evaluating node reputation and trust levels based on observed behavior. But they need to be resilient against sophisticated attacks. Cryptographic techniques like symmetric and public key cryptography provide fundamental security services and defenses against impersonation, eavesdropping and message manipulation attacks. Still, the constraints of sensor nodes necessitate efficient lightweight cryptographic protocols. Authentication schemes such as encryption, digital signatures and hash chains prevent spoofing and falsification of identities and information. Though promising, they incur significant processing and communication overheads.

While each of these security techniques contributes towards protecting the network layer in WSNs, none provide a comprehensive solution. Open research issues include improving detection accuracy, securing mobile and IoT-integrated WSNs, developing resilient trust models, designing holistic cross-layer security architectures, and leveraging technologies like machine learning to enhance threat mitigation capabilities. Addressing the unique challenges and constraints of WSNs requires continuous innovation in lightweight, decentralized and robust security solutions tailored to resource-limited network environments. Going forward, the adoption of emerging approaches like blockchain, edge computing and hardware security modules in coordination with traditional security mechanisms offers promising directions for enabling secure and trustworthy wireless sensor networks against network layer attacks.

REFERENCES

- Adnan, R., Haider, S. I., Khalid, A., Shafi, S., & Abbas, H. Intrusion detection and security mechanisms for wireless sensor networks. *International Journal of Advanced Networking Applications*, 2013; 4(4): 16-23.
- Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. Wireless sensor networks: a survey. *Computer networks*. 2002; 38(4): 393-422.
- Khan, Amir, Muqem Ahmed, Afrah Fathima, and Mohd Faizaanuddin. "Edge computing-based intrusion detection model wireless sensor networks: leveraging machine learning on WSN-DS dataset." *International Journal of System Assurance Engineering and Management* (2026): 1-15.
- Aman, M. N., Sikdar, B., Mottaghi, K., Mahdin, H. A new public key infrastructure design (NanoPK) for wireless sensor network. *Wireless Networks*, 2019;25(5): 2697-2717.
- Abouelkheir, Eman. "A Provenance-Driven Trust Framework with Physics-Consistent Validation for Secure Wireless Sensor Networks." *Sensors* 26, no. 18 (2026): 56-95.
- Butun, I., Morgera, S. D., & Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 2014;16(1): 266-282.
- Chan, H., Perrig, A., & Song, D. Random key predistribution schemes for sensor networks. *IEEE Symposium on Security and Privacy*, 2003; 197-213.
- da Silva, A. P. R., Martins, M. H. T., Rocha, B. P. S., Loureiro, A. A. F., Ruiz, L. B., & Wong, H. C. Decentralized intrusion detection in wireless sensor networks. *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005;16-23.
- Deng, J., Han, R., & Mishra, S. Security support for in-network processing in wireless sensor networks. *ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005; 83-93.
- Du, W., Deng, J., Han, Y. S., Varshney, P. K. A pairwise key predistribution scheme for wireless sensor networks. *ACM CCS Conference on Computer and Communications Security*, 2005; 42-51.
- Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. *ACM CCS Conference on Computer and Communications Security*, 41-47.
- Ganerwal, S., & Srivastava, M. B. Reputation-based framework for high integrity sensor networks. *ACM Security of Ad Hoc and Sensor Networks*, 2004; 66-77.
- Ganerwal, S., Balzano, L. K., & Srivastava, M. B. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, 2008;4(3): 1-37.
- Großschädl, J., Szekely, A., & Tillich, S. The energy cost of cryptographic key establishment in wireless sensor networks. *ACM Symposium on Applied Computing*, 2005; 380-386.
- Großschädl, J., Howells, W. G., Tillich, S., Henry, C., & McCullagh, W. Energy-efficient software implementation of long integer modular arithmetic. *J Cryptogr Eng*, 2006; 1(3): 197-208.
- Han, G., Jiang, J., Zhang, C., Duong, T. Q., Guizani, M., & Karagiannis, G. K. A survey on mobile anchor node assisted localization in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 2014;18(3): 2220-2243.

17. Hu, L., & Evans, D. Secure aggregation for wireless networks. *Workshop on Security and Assurance in Ad hoc Networks*, 2005; 384-391.
18. Hu, Y. C., Perrig, A., & Johnson, D. B. Wormhole attacks in wireless networks. *IEEE journal on selected areas in communications*, 2006; 24(2): 370-380.
19. Iyer, A. V., & Gandham, S. R. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks*, 2018; 11: 2661-2674.
20. Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. Toward a lightweight intrusion detection framework for smart home ecosystem. *IEEE Access*, 2017; 5: 2509-2522.
21. Krontiris, I., Dimitriou, T., Giannetsos, T., & Mpasoukos, M. Intrusion detection of sinkhole attacks in wireless sensor networks. *International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*, 2007; 150-161.
22. Law, Y. W., Doumen, J., & Hartel, P. Survey and benchmark of block ciphers for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2006; 2(1): 65-93.
23. Lee, H., Choi, Y., & Jung, B. Energy-efficient intrusion detection system based on reputation system in wireless sensor networks. *International Conference on Computational Science and Its Applications*, 2007; 1140-1149.
24. Liu, A., & Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. *International Conference on Information Processing in Sensor Networks*, 2008; 245-256.
25. Lu, R., Lin, X., Luan, T. H., Liang, X., & Shen, X. S. Pseudonym changing at social spots: An effective strategy for location privacy in VANETs. *IEEE Transactions on Vehicular technology*, 2010; 61(1): 86-96.
26. Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv: 2017; 1709.04647*.
27. Mohanraj, K., & Arivazhagan, B. "Detection and Mitigation of Black Hole Attack Using Fuzzy Heuristics in Mobile AdHoc Network (MANET)." *Library Progress International*, 2024, 44(3).
28. Momani, M., Challa, S., & Alhmouz, R. (2010). Can we trust trusted nodes in wireless sensor networks?. *International Symposium on High Capacity Optical Networks and Enabling Technologies*, 2010; 1-5.
29. More, V., & Suryakant, B. "Security Based Improved LEACH Protocol for Wireless Sensor Network." *Library Progress International*, 2024, 44(3), 5167–5180.
30. Rajasegarar, S., Leckie, C., Palaniswami, M., & Bezdek, J. C. Distributed anomaly detection in wireless sensor networks. In *Communication systems*, 2008. ICCS 2008. 10th IEEE Singapore International Conference on (pp. 1-5). IEEE.
31. Rassam, M. A., Maarof, M. A., & Zainal, A. Advancements of data anomaly detection research in wireless sensor networks: A survey and open issues. *IEEE Access*, 2013; 1: 855-885.
32. Ren, K., Lou, W., Kim, K., & Deng, R. H. A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular Technology*, 2008; 55(4): 1373-1384.
33. Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on parallel and distributed systems*, 2009; 20(11): 1698-1712.
34. Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *IEEE Wireless Communications*, 2004; 11(6): 38-43.
35. Sharma, K., Ghose, M. K., & Joshi, K. R. Wireless sensor networks: An overview on its security threats. *International journal of advanced research in computer science and software engineering*, 2010; 2(4): 42-45.
36. Singh, S., Sharma, P. K., Yadav, N., & Upadhyay, R. A secure energy-efficient routing protocol for wireless ad hoc networks. *Security and Communication Networks*, 2017.
37. Sun, B., Yu, F., Wu, K., & Xiao, Y. Trust evaluation-based security solution in ad hoc networks. *IEEE Journal on Selected areas in Communications*, 2007; 25(2): 356-368.
38. Ye, F., Luo, H., Lu, S., & Zhang, L. Statistical en-route filtering of injected false data in sensor networks. *IEEE Journal on Selected Areas in Communications*, 2005; 23(4): 839-850.
39. Zhu, S., Setia, S., & Jajodia, S. LEAP: efficient security mechanisms for large-scale distributed sensor networks. *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, 2003; 62-72.