International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2311-2321
Journal homepage: http://iieta.org/journals/ijsse

Evaluating Blackhole Attack Detection Strategies for Secure Heterogeneous Wireless Sensor Networks

Sonali Prashant Bhoite[1,2*], Ganapati A. Patil[1]

[1] Department of Computer Science and Engineering, JSPM University, Pune 412207, India
[2] Department of Information Technology, Vishwakarma Institute of Technology, Pune 411037, India

Corresponding Author Email: sonalibhoite7@gmail.com

https://doi.org/10.18280/ijsse.151111

Received: 20 October 2025
Revised: 21 November 2025
Accepted: 26 November 2025
Available online: 30 November 2025

Keywords:
heterogeneous wireless sensor networks, security protocol, blackhole attack detection, intrusion detection system, energy efficiency, data aggregation

ABSTRACT

Heterogeneous wireless sensor networks (HWSNs) are increasingly deployed in critical applications such as smart cities, environmental monitoring, and military operations. These networks, consisting of sensor nodes with varied computational capabilities, offer improved efficiency and flexibility but also introduce significant security challenges, particularly vulnerabilities to blackhole attacks that can disrupt communication and compromise network integrity. Existing security mechanisms often struggle to effectively address such attacks while maintaining a balance between real-time detection and resource constraints. This review evaluates existing blackhole attack detection strategies for HWSNs, with particular attention to collaborative architectures where low-power and high-power sensor nodes operate under a centralized sink node. The analysis highlights detection modules that monitor network behavior, perform threat classification, and trigger appropriate countermeasures to ensure secure and reliable communication. Overall, the reviewed strategies demonstrate improvements in detection accuracy while preserving energy efficiency, making them suitable for resource-constrained heterogeneous environments.

1. INTRODUCTION

1.1 Background on wireless sensor networks and transition to heterogeneous wireless sensor networks

Wireless sensor networks (WSNs) are collections of spatially distributed sensor nodes designed to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, or motion. WSNs were traditionally made up of homogeneous sensor nodes, each of which had comparable processing power, energy resources, communication capabilities, and network functions [1]. These networks have been used extensively in industrial automation, healthcare, environmental monitoring, and military surveillance. However, the shortcomings of homogeneous WSNs, particularly with regard to energy economy, processing load, and communication range, became evident as the need for increasingly sophisticated and scalable applications increased [2].

To address these challenges, researchers have introduced heterogeneous wireless sensor networks (HWSNs). The capacities of nodes in HWSNs vary; some have more energy reserves, more computational capacity, or a longer communication range. Increased network longevity, dependability, and scalability are provided by this heterogeneity [3]. Strong nodes, for example, can act as cluster leaders, combining information from lower-tier nodes and sending it to the base station. Although HWSNs increase overall flexibility and efficiency, they also create new security flaws since attackers can target high-capability nodes to cause the most disruption.

1.2 Blackhole attacks: Definition, impact, and the need for detection mechanisms

In WSNs and HWSNs, a blackhole attack is a serious security risk in which a malevolent node deceptively positions itself as possessing the quickest or best route to the target (such as the base station). It creates a "black hole" in the network by silently dropping packets rather than forwarding them once it has begun accepting them. Even one blackhole node can cause significant network disruptions in multi-hop communication networks, such as WSNs, because nodes mostly depend on their neighbors to convey data [4, 5]. This can result in packet loss, reduced throughput, and energy waste from needless retransmissions.

The effects of blackhole assaults are even more severe in HWSNs. When compromised, high-capability nodes like cluster heads or fusion nodes can deceive a sizable section of the network, impairing scalability and dependability. Conventional routing systems are weak because they frequently lack the tools to dynamically assess a node's reliability [6]. Therefore, protecting the availability, confidentiality, and integrity of the data being sensed and sent depends on identifying blackhole assaults. To guarantee the safe and reliable operation of contemporary sensor networks, specific detection methods designed for diverse configurations must be developed.

1.3 Scope and objectives of the survey

The objective of this survey is to provide a thorough analysis of the state of security protocols and detection systems intended to thwart blackhole attacks in HWSNs. Although there is a wealth of research on intrusion detection in homogeneous WSNs, a more concentrated study is necessary due to the special features of HWSNs, including node variety, fluctuating energy profiles, and hierarchical topologies. In the context of HWSNs, the goal is to identify, categorize, and assess current blackhole detection methods, emphasizing their designs, detection tactics, performance indicators, and suitability for practical applications.

A taxonomy of current methods will also be provided by the survey, which will group them into routing-based, AI/ML-based, trust-based, and hybrid models. It will identify research gaps through comparison analysis, such as computational overheads in detection models, energy inefficiencies, or a lack of standardized datasets. The ultimate goal of this work is to give researchers and developers a starting point for creating scalable, lightweight security mechanisms that adapt to changing threats in diverse WSN contexts. The survey advances the development of safe and robust WSN infrastructures by highlighting important issues and suggesting future paths.

2. OVERVIEW OF HETEROGENEOUS WIRELESS SENSOR NETWORKS

2.1 Definition and architecture

Sensor networks that comprise nodes with varying energy, computing power, communication range, and sensing features are known as HWSNs. HWSNs add a combination of resource-constrained sensor nodes and more potent nodes like cluster heads, fusion centers, or gateways, in contrast to conventional homogeneous WSNs, where every node has the same hardware and purpose. Better network performance and resource optimization are made possible by this hierarchical architecture. Typically, an HWSN is organized into tiers, with low-tier sensor nodes collecting data and high-tier nodes handling data processing, aggregation, and base station connection. These layers frequently have a grid-based or clustered architecture to promote effective communication and energy efficiency [7, 8]. HWSNs' architectural adaptability makes them appropriate for use in healthcare, military systems, and smart environments, but it also makes network management more difficult, particularly when it comes to putting in place consistent and effective security measures.

2.2 Types of heterogeneity (energy, computation, sensing, communication)

Heterogeneity in HWSNs arises from variations in node capabilities, which can be broadly classified into four types: energy, computation, sensing, and communication heterogeneity.

Energy heterogeneity refers to differences in battery capacity or energy harvesting capabilities among nodes. High-energy nodes are often assigned roles such as cluster heads or aggregators.

Computation heterogeneity occurs when some nodes have more powerful CPUs or memory, enabling them to perform complex processing tasks like encryption or anomaly detection.

Sensing heterogeneity is present when nodes are equipped with different types of sensors (e.g., temperature, gas, pressure), allowing for multi-modal environmental monitoring.

Communication heterogeneity refers to differences in transmission range or bandwidth; nodes may use varying communication protocols (e.g., Zigbee, Wi-Fi) depending on their role.

These heterogeneous traits enable flexible and robust network design but pose significant challenges for standardizing security mechanisms that can adapt to all node types effectively.

2.3 Benefits and challenges of heterogeneous wireless sensor networks in security protocol design

Numerous advantages provided by HWSNs improve the overall effectiveness and flexibility of networks. High-capability nodes are assigned specific roles, which improves scalability, network lifetime, and data processing efficiency. For example, cluster heads can aggregate data and identify anomalies before forwarding information to the base station, which reduces communication overhead and enhances security by enabling early threat detection. However, this heterogeneity also introduces significant challenges for security protocol design. If a cluster head is compromised, an entire subnetwork may be exposed, making high-tier nodes attractive targets for attackers. Security protocols must also consider the unequal distribution of resource availability among nodes. While high-tier nodes can employ more complex detection and response mechanisms, lightweight security techniques must be sufficiently robust to protect low-tier nodes without excessive resource consumption [9]. Therefore, adaptive, scalable, and context-aware protocols are required to ensure secure communication and maintain trust across diverse node types, which remains challenging given the limited processing and energy capabilities of many network segments.

3. BLACKHOLE ATTACKS IN WIRELESS SENSOR NETWORKS AND HETEROGENEOUS WIRELESS SENSOR NETWORKS

3.1 Mechanism of a blackhole attack

In a WSN, a blackhole attack is a kind of network-layer security risk when a malevolent node deceptively positions itself as having the quickest or most effective route to the target, usually the base station. Because they think the rogue node is a trustworthy middleman, nearby nodes use it to transit their data after learning about it. When the blackhole node begins receiving data packets, it secretly drops them rather than forwarding them, causing significant data loss and interfering with network connections [10].

This attack takes advantage of the fact that several WSN routing protocols, like AODV or DSR, are trust-based and do not automatically confirm the legitimacy of routing packets. These protocols are appropriate for contexts with few resources because of their simplicity and low overhead, but they are also susceptible to manipulation. Detection becomes considerably more difficult when attackers use numerous compromised nodes to perform coordinated blackhole attacks [11]. By decreasing the packet delivery ratio (PDR), raising latency, and using more energy as a result of route rediscovery or retransmissions, these attacks impair network performance.

3.2 Attack scenarios and adversarial models

Depending on the capabilities and objectives of the opponent, blackhole attacks might appear in a variety of ways. One malevolent node interferes with communication in its immediate vicinity in a single-node assault. A cooperative blackhole attack involves several malevolent nodes working together to deceive and intercept data over a larger area, causing a more extensive disruption to the network. In clustered topologies, where a hacked cluster head might impact a whole collection of sensor nodes, these attacks are very dangerous. Adversaries might be internal, where malware or physical access compromises legitimate nodes, or external, when the attacker introduces rogue nodes onto the network [12]. The mobility, processing power, and energy availability of adversarial models can also differ. By sporadically forwarding some packets or altering behavior in response to feedback from network monitoring, a skilled attacker who is familiar with the routing protocol and network layout can vary its approach to avoid detection.

Designing efficient detection techniques requires an understanding of these models. Both static and dynamic attackers must be taken into consideration by protocols, which must also be able to differentiate between malicious activity and normal problems like packet loss brought on by congestion or node failure.

3.3 Specific risks in heterogeneous wireless sensor networks compared to homogeneous wireless sensor networks

Compared to homogeneous networks, HWSNs are particularly vulnerable to blackhole attacks. Certain nodes in HWSNs, including cluster heads or gateway nodes, have more energy stores, processing power, and communication ranges than others. These nodes frequently have key roles in routing and data aggregation. Therefore, communication can be disrupted for a large chunk of the network, not just a small neighborhood, if a high-tier node is compromised or behaves maliciously.

Because HWSNs are hierarchical, lower-tier sensor nodes rely significantly on upper-tier nodes to relay information to the base station. At a higher level, a blackhole node can efficiently function as a sink or a bottleneck, collecting and discarding significant amounts of important data. Furthermore, because of node variability, HWSNs frequently lack consistent trust models, which makes it more challenging to apply uniform security measures throughout the network. The mobility or re-tasking of high-tier nodes in dynamic contexts presents an additional risk. Attackers can escape static detection techniques by launching adaptive blackhole attacks by taking advantage of this mobility or role change [13]. Therefore, in order to effectively combat these increased risks, security procedures in HWSNs need to be more resilient and context-aware.

3.4 Real-world implications and case examples

Blackhole attacks in WSNs and HWSNs have significant practical ramifications, especially in mission-sensitive fields like healthcare, environmental monitoring, and military surveillance. A whole mission may fail, and human lives may be lost, for example, if a blackhole node ignores detection signals regarding enemy activity or landmines in a combat situation. Similar to this, blackhole attacks in smart agriculture may result in the loss of sensor data needed for crop protection or irrigation, which could lower yields or cause financial harm. One prominent example comes from smart grid systems, which use sensor networks to keep an eye on infrastructure and electrical lines. A blackhole attack might delay emergency responses by making it impossible to notice power outages or tampering events. Disaster management systems that use WSNs to identify fires, gas leaks, or structural damage are another example. The impact of the disaster may grow, and rescue efforts may be delayed if blackhole assaults stop alert messages from getting to the command center [14]. These situations highlight the need for real-time blackhole mitigation and detection systems. Furthermore, the ramifications of such assaults can spread to larger digital ecosystems as WSNs interface with the Internet of Things (IoT), which emphasizes the need for robust and intelligent security procedures.

4. TAXONOMY OF DETECTION AND PREVENTION TECHNIQUES

4.1 Classification based on routing-based protocols

Routing-based protocols concentrate on improving or modifying existing routing techniques in order to identify and stop blackhole attacks. These methods include additional verification procedures such as route confirmation, sequence number validation, and acknowledgment schemes while utilizing the framework of conventional routing protocols (AODV, DSR, LEACH, etc.). These protocols detect nodes that maliciously drop data packets or advertise bogus routes by monitoring route request (RREQ) and route reply (RREP) messages. To find irregularities, common methods include cross-verifying route information with nearby nodes or employing extra control packets, such as two-hop acknowledgments. Routing-based solutions are generally lightweight in terms of computation, making them suitable for resource-constrained nodes in both homogeneous and heterogeneous WSNs. However, many of these approaches assume uniform node capabilities and do not explicitly differentiate between low-energy and high-capability nodes during routing and monitoring operations. Their reliance on network topology and routing behavior can limit effectiveness in dynamic or large-scale environments where routing paths frequently change [15]. Additionally, repeated route validation and control message exchanges may introduce increased communication overhead, which can disproportionately affect low-tier nodes with limited energy and processing resources.

4.2 Classification based on trust-based systems

Trust-based systems use node behavior to determine a node's credibility in the network, which serves as the foundation for spotting malicious nodes like blackhole attackers. These systems provide each node a trust score based on parameters including packet forwarding rates, node dependability, and past contacts. To stop more disruptions, nodes with low trust levels are marked as suspicious and excluded from routing decisions. Trust models can be distributed, enabling nodes to compute trust locally based on their observations, or centralized, where a base station maintains trust ratings [16]. Because trust-based systems take into account different node roles and capabilities, they are especially useful in HWSNs. By regularly assessing how high-tier nodes (such as cluster heads) behave in hierarchical organizations, they aid in their security. Although trust-based procedures increase adaptability and resilience, they must be carefully calibrated to prevent false positives or needless energy consumption brought on by ongoing trust updates and monitoring [6]. Additionally, they can have trouble fending off coordinated attackers who can tamper with trust measurements.

4.3 Classification based on machine learning/artificial intelligence-based approaches

Methods based on artificial intelligence (AI) and machine learning (ML) use data-driven strategies to identify unusual activity suggestive of blackhole assaults. These methods entail using labeled datasets that distinguish between benign and malevolent network behavior to train models (such as decision trees, support vector machines, and deep neural networks). These algorithms may identify nodes as malicious or legitimate in real time by examining characteristics including routing patterns, sequence numbers, and packet delivery rates [17]. By identifying intricate patterns in expansive or dynamic WSN environments, sophisticated techniques like deep learning (DL) or ensemble learning can increase detection accuracy.

Because HWSNs have high-capability nodes that can manage computationally demanding activities like model training and inference, ML/AI-based approaches are especially advantageous for these networks [18]. These methods could, however, provide new difficulties, such as the requirement for extensive datasets, processing overhead, and energy usage. Moreover, ML-based models must be updated and retrained on a regular basis because their efficacy rests on their capacity to adjust to changing attack tactics.

4.4 Classification based on cryptographic-based protocols

By guaranteeing data integrity, confidentiality, and authenticity, cryptographic-based protocols seek to secure communication channels and authenticate nodes in order to stop blackhole assaults. These methods use hash functions, digital signatures, encryption algorithms, and key management systems to prevent tampering with routing data. For example, nodes may employ lightweight cryptographic techniques (like AES and ECC) to confirm the authenticity of secure control messages or route ads. By requiring authentication credentials that are only known by genuine nodes, cryptographic techniques also stop adversaries from introducing fictitious routing information.

To lessen the strain on low-energy nodes, cryptographic solutions in HWSNs frequently use high-capability nodes for secure data aggregation and key distribution. Cryptographic-based protocols can be resource-intensive; it's important to strike a balance between security strength and energy efficiency, even if they provide strong protection against both internal and external threats. Effective implementation of these protocols still faces major obstacles in the areas of key management, scalability, and the possibility of compromised nodes disclosing cryptographic material.

4.5 Classification based on hybrid models

To offer a more thorough defense against blackhole attacks, hybrid models include several detection techniques, including ML, cryptography, trust assessment, and routing-based approaches. Hybrid models mitigate individual limits while improving detection accuracy, adaptability, and resilience by utilizing the advantages of each technique. For instance, a hybrid protocol may combine cryptographic authentication and trust-based monitoring to better identify and isolate hostile nodes and protect routing data from manipulation. Additionally, to enhance anomaly detection in dynamic contexts, ML models can be combined with conventional routing checks.

Because of the network's hierarchical structure and diverse node capabilities, hybrid techniques are especially beneficial in HWSNs. Low-tier nodes manage simple activities like basic trust evaluation, while high-tier nodes can carry out sophisticated computations (such as encryption or ML analysis). Hybrid systems must be carefully designed to preserve efficiency because they can increase complexity, communication overhead, and energy usage [18]. Hybrid models offer a potential approach to protecting HWSNs from advanced blackhole assaults in spite of these difficulties.

4.6 Detection criteria and evaluation parameters

A number of performance indicators and detection criteria are taken into consideration in order to assess how well blackhole detection and prevention strategies work. Packet forwarding behavior, routing control message analysis, node trustworthiness, and traffic anomaly detection are examples of common detection criteria. The capacity of protocols to correctly detect malicious nodes while reducing false positives and false negatives is the basis for their evaluation. Key evaluation parameters include:

- PDR: Measures successful data packet delivery despite attacks.
- Detection Accuracy: The rate at which malicious nodes are correctly identified.
- Energy Consumption: Evaluates the energy overhead introduced by security mechanisms.
- End-to-End Delay: Measures the impact on communication latency.
- Throughput: Assesses the network’s data transmission efficiency.
- False Positive/Negative Rates: Indicates the reliability of detection mechanisms.
- Routing Overhead: Additional control messages required for detection and prevention.

Researchers can determine trade-offs between security strength and network performance by examining these factors using a variety of methodologies. This information will help them build protocols that are optimal for heterogeneous WSN environments.

A comparative review of different blackhole attack detection strategies in HWSNs, arranged according to their underlying techniques, is given in Table 1. It provides insight into their applicability for various network settings and resource restrictions by highlighting important detection criteria, evaluation metrics, strengths, and limits.

Table 1. A comparative overview of various blackhole attack detection approaches in heterogeneous wireless sensor networks (HWSNs)

Approach	Detection Criteria	Evaluation Metrics	Strengths	Limitations
Routing-Based Protocols	Route reply verification, sequence number analysis, forwarding check	Packet delivery ratio (PDR), routing overhead, detection latency	Lightweight, suitable for low-power nodes	Vulnerable to dynamic topology changes
Trust-Based Systems	Node behavior, packet forwarding ratio, historical interactions	Trust score accuracy, false positive rate (FPR), packet loss, energy consumption	Adaptive, suitable for hierarchical HWSNs	May fail under collusion or limited observations
ML/AI-Based Approaches	Anomaly detection via statistical learning and pattern recognition	Detection accuracy, false positive/negative rates, model training time, computation overhead	High detection accuracy, adapts to evolving threats	Requires datasets, retraining, and more energy on some nodes
Cryptographic Protocols	Authentication, data integrity, and message encryption	Encryption overhead, key distribution time, packet integrity rate, end-to-end delay	Strong protection against tampering	High energy/computation demands, especially on low-tier nodes
Hybrid Models	Combined trust, routing checks, ML or encryption-based techniques	Comprehensive accuracy, energy-efficiency trade-off, PDR, detection coverage	Balances detection accuracy and robustness	Complexity in design, potential for higher overhead

5. SURVEY OF SECURITY PROTOCOLS FOR BLACKHOLE DETECTION

Blackhole attacks pose a significant threat to the reliability of WSNs. This section reviews recent security protocols for blackhole attack detection, emphasizing detection mechanisms, performance trade-offs, and suitability for heterogeneous deployments.

Khan et al. [16] presented a trust-based optimized reporting scheme designed to detect and prevent blackhole attacks in constrained routing environments such as RPL-based Low-Power and Lossy Networks (LLNs). The proposed protocol computes direct and indirect trust values for neighboring nodes using metrics including honesty, energy, unselfishness, and similarity, and employs a delta-threshold mechanism with a forgetting curve to dynamically weight recent behavior. This approach enables the root or sink node to make more reliable decisions about malicious behavior while reducing false positives and reporting overhead. The scheme also balances detection accuracy with minimal communication and processing costs, addressing a crucial challenge in resource-limited HWSN deployments where energy efficiency and timeliness are essential. Through simulation and evaluation, the authors demonstrate improved detection performance compared to conventional static threshold methods, making this security protocol a valuable strategy for blackhole detection in HWSNs.

Ramesh et al. [18] proposed an energy-aware and adaptive intrusion detection system (IDS) tailored for WSNs that targets both blackhole and wormhole attacks. The security framework leverages DL techniques combined with advanced feature generation and adaptive learning to improve detection accuracy while minimizing energy consumption, which is critical in resource-constrained environments. Specifically, the method uses generative adversarial networks (GANs) for generating distinguishing attack features, meta-heuristic optimization such as the whale optimization algorithm (WOA) for parameter tuning, and deep Q-learning for adaptive learning of attack patterns, ensuring the model can respond to evolving threats in real time. Simulation results demonstrate that this hybrid approach achieves high detection accuracy, recall, and specificity compared with traditional ML and DL models, highlighting its suitability for real-time deployment in heterogeneous sensor environments.

Ramesh et al. [18] introduced an energy aware adaptive intrusion detection and prevention framework to detect blackhole and grayhole attacks with improved accuracy and reduced false alarms. The protocol integrates the Generative adversarial networks (GAN) and whale optimization algorithm to learn the attack behavior. Simulation results indicate that the hybrid IDS achieves higher detection rates and lower energy consumption than traditional standalone IDS methods, making it suitable for resource-constrained heterogeneous environments. Importantly, the study analyzes the trade-offs between detection accuracy, energy overhead, and scalability, providing insight into how multi-layer security protocols can be effectively deployed in diverse wireless sensor deployments.

Ghugar et al. [19] presented DLTIDS, a dual-layer trust-based IDS designed to detect blackhole attacks in WSNs. Two complementary trust mechanisms are employed by the system. By identifying nodes as either suspect or trusted, the first layer assesses direct trust based on node behavior, particularly packet forwarding and hop count. To further examine node activity and confirm malicious intent, the second layer uses a watchdog mechanism. Cluster leaders are essential to the coordination of trust evaluations and data aggregation. To trace and verify network paths, DLTIDS keeps track of three tables: route, source, and destination. It looks for irregularities by comparing sequence numbers and hop counts. The system is evaluated using both watchdog-based and conventional AODV methods after being simulated in MATLAB. The findings demonstrate reduced false alarm rates, enhanced detection accuracy, and trust stability, particularly at higher network densities. DLTIDS is robust against blackhole and jamming attacks and demonstrates adaptability to dynamic WSN environments. Its dual-layer structure makes it a reliable and scalable solution for real-time WSN security.

Khan et al. [20] proposed an artificial neural network (ANN)-based mechanism to detect routing attacks in WSNs, targeting blackhole, grayhole, and wormhole threats. The method makes use of a feed-forward ANN that was trained using characteristics such as the number of packets, energy consumption, and node trust level. The NS2 simulator is used to implement the model, which was trained using the CICIDS2017 dataset. To increase classification and decrease false positives, it makes use of a three-layer ANN (input, hidden, and output) with optimum parameters. Training on labeled data and testing on unlabeled real-time traffic are the two stages of detection. The ANN demonstrated resilience against a range of routing hazards with an accuracy of 99.49% and a detection rate of 99.21%. According to simulation results, performance was consistent across attack scenarios with low energy usage and packet loss. The technology outperforms traditional techniques by maintaining reliable packet delivery even during attacks. This work highlights the viability of ANN models for real-time intrusion detection in resource-constrained, energy-sensitive WSN environments.

Table 2. A comparative analysis of various blackhole attack detection techniques in wireless sensor networks (WSNs)

Paper	Protocol Name / Approach	Architecture	Detection Mechanism	Performance Metrics	Applicability to HWSNs	Strengths	Limitations
[21]	AES-Based Signature Detection	Distributed	Symmetric key cryptography	End-to-end delay, packet delivery ratio (PDR)	Moderate	Low communication delay	Requires key management
[22]	Fuzzy-GA-TLBO Model	Centralized	Fuzzy logic with Genetic algorithm (GA) and teaching-learning-based optimization (TLBO)	Computational cost	Limited	Low computational cost	Centralized nature may hinder scalability
[23]	Deep learning (DL)-Based Detection	Distributed	DL classifiers	True detection rate (TDR)	High	High detection probability	Requires substantial training data
[24]	Encryption with Deep Neural Networks	Cluster-based	Encryption and DL	Packet loss ratio (PLR), throughput, delay	High	High data delivery with minimal delay	Computational overhead
[25]	JDICA Technique	Distributed	Joint detection and isolation	PDR, TDR, energy consumption	Moderate	High accuracy, reduced delay	Potential energy consumption
[26]	Blockchain-Based Detection	Distributed	Blockchain ledger verification	PDR, throughput, delay	High	Effective malicious node identification	Blockchain overhead
[27]	Warning message counter (WMC)	Distributed	Behavior-based monitoring	PDR, FPR, false negative rate (FNR)	Moderate	Improved PDR, low false rates	May require additional communication
[28]	GA with XGBoost Classifier	Distributed	GA and XGBoost	TDR	High	High detection rate	Computational complexity
[29]	Cluster-Based Voting Decision	Cluster-based	Voting among cluster nodes	False detection rate (FDR), energy consumption	High	Low FDR, negligible energy use	Requires reliable cluster formation

Table 3. A Comparative analysis of various blackhole attack detection techniques in wireless sensor networks (WSNs)

Paper	Technique / Model Used	Simulation Tool / Dataset	Performance Metrics and Results	Limitations
[30]	Online ensemble learning (adaptive random forest and hoeffding adaptive tree)	WSN-DS dataset	Detection rates: 96.84% (heterogeneous ensemble), 97.2% (homogeneous ensemble)	Focuses on streaming data; may require adaptation for static datasets
[31]	Hybrid meta-heuristic combining WOA and sine cosine algorithm	Custom simulation	Detection rate: > 85%; warning rate: 0.866	Emphasizes optimization; specific energy consumption metrics not detailed
[32]	Fitness rate-based WOA with optimized LSTM	-	Energy consumption improved by 7.14% over WOA and FireFly; better accuracy than conventional LSTM	Combines DL with optimization; computational complexity considerations apply
[33]	ML classifiers (random forest, etc.)	WSN-DS dataset	Random forest achieved 99.72% accuracy	Focused on multiple DoS attacks; specific metrics for blackhole attacks not isolated
[34]	The trust factor decreases exponentially with consecutive packet drops	-	Early detection of malicious nodes through trust degradation	Older study; may need updates to align with current WSN standards and technologies
[35]	IDS and digital signature integration with the AODV protocol	-	Enhanced PDR and reduced delay compared to standard AODV	Specific simulation parameters and environments not detailed
[36]	Dynamic threshold-based detection with forged RREQ packets	NS-2 simulator	Detection rate: 94.66%; PDR increased by 3%; throughput improved by 6.15%; end-to-end delay reduced by 6.13%	Focused on VANETs; applicability to WSNs may require adaptation
[37]	Forensic analysis approach	-	Detailed analysis of blackhole attack patterns and behaviors	Primarily analytical; lacks implementation of detection/prevention mechanisms
[38]	Cognitive intelligence framework with AI and big data analytics	-	Capable of detecting and preventing various attacks, including DoS; resilient to packet drop occurrences	Broad approach; specific performance metrics for blackhole attacks are not detailed
[39]	Survey of ML techniques for anomaly detection	-	Comprehensive overview of ML-based approaches for anomaly detection in WSNs	Survey paper; does not propose a specific detection/prevention method

Kim et al. [21] introduced a detection mechanism utilizing symmetric key cryptography, specifically AES, combined with signature-based methods. The goal of this distributed architecture method is to identify blackhole attacks without causing appreciable communication lag. Although the technique is successful in preserving a high PDR and minimal end-to-end delay, it necessitates strong key management techniques to manage cryptographic keys throughout the network.

Almseidin et al. [22] proposed a centralized detection model integrating fuzzy logic with genetic algorithm (GA) and teaching-learning-based optimization (TLBO). The goal of this hybrid strategy is to maximize computational efficiency without sacrificing detection precision. However, in large-scale HWSNs, where distributed solutions are frequently more practical, their centralized nature may provide scaling issues.

Saxe and Berlin [23] developed a DL-based detection system employing classifiers trained to identify blackhole attacks. With its high true detection rate (TDR) and distributed operation, this method is appropriate for dynamic and diverse situations. The main drawback is the requirement for large amounts of training data and processing power, which not all sensor nodes may have easily accessible.

Saravanakumar et al. [24] combined encryption methods with deep neural networks in a cluster-based architecture to detect blackhole attacks. This hybrid strategy makes use of cluster heads' processing power to increase data delivery rates and reduce latency. However, the combination of DL and encryption adds computational overhead, which calls for cautious resource management.

Table 2 provides a comparative analysis of various blackhole attack detection techniques in WSNs, focusing on architecture, detection mechanisms, performance metrics, and applicability to HWSNs. Each method is evaluated for its strengths and limitations, highlighting trade-offs such as detection accuracy versus computational or communication overhead.

Clement Sunder and Shanmugam [25] introduced the JDICA technique, a distributed method focusing on joint detection and isolation of malicious nodes. By lowering latency and increasing PDR, this strategy raises network efficiency overall. However, the longevity of sensor nodes may be impacted by the energy consumption related to ongoing monitoring and isolation procedures.

Abdelrahman et al. [26] implemented a blockchain-based detection mechanism, utilizing the immutable ledger to verify node behavior and detect anomalies. This distributed method improves throughput and guarantees efficient detection of rogue nodes. The increased overhead brought about by blockchain operations, which could have an impact on processing time and energy usage, is one of the trade-offs.

Terence and Purushothaman [27] proposed the warning message counter (WMC) method, a behavior-based monitoring system operating in a distributed architecture. This method maintains low false positive and negative rates while increasing the PDR by examining node behavior and delivering warnings. Network traffic may increase if more communication is required to spread warnings.

Ashfaq et al. [28] developed a detection system combining GA with the XGBoost classifier in a distributed setup. Because of its high detection rate, this technique is useful for spotting blackhole attacks. However, such models may not be as applicable in contexts with limited resources due to the computational complexity involved in training and deploying them.

Liu and Wu [29] presented a cluster-based voting decision method, where cluster nodes collaboratively decide on the legitimacy of data packets. This method meets the requirements of HWSNs by achieving low FDRs and low energy usage. The stability and dependability of cluster formations are necessary for this strategy to be effective.

Table 3 offers a comparative analysis of various blackhole attack detection techniques in WSNs, focusing on the simulation tools or datasets used, achieved performance metrics, and limitations of each approach. It includes both ML and meta-heuristic models such as Random Forest, LSTM, and hybrid optimization algorithms. The table highlights detection accuracy, energy efficiency, and improvements in packet delivery or delay metrics. While some techniques show high accuracy, others emphasize adaptive learning or trust-based mechanisms. However, limitations like computational complexity, lack of simulation detail, or applicability to only specific network types are also noted.

5.1 Discussion of trends, performance gaps, and innovative approaches

5.1.1 Several trends emerge from the literature

- Adoption of AI/ML: There is a clear trend toward using ML and DL approaches (e.g., Random Forest, XGBoost, LSTM) for detecting complex or evolving attacks in WSNs, particularly HWSNs.
- Hybrid Approaches: Solutions increasingly combine techniques such as cryptography, trust models, and ML to improve robustness and adaptability (e.g., GA-XGBoost [28], Fuzzy-GA-TLBO [22]).
- Distributed Detection Models: Many techniques favor distributed architectures for scalability and resilience, especially in large and dynamic networks.
- Focus on Energy Efficiency: With the rise of energy-constrained deployments, several models emphasize reduced computation and communication overhead (e.g., cluster-based and low-FDR solutions).
- Behavior-Based Monitoring: Trust-based and behavior-driven models (like WMC) are being used to detect malicious patterns without needing heavy computation.

5.2 Limitations and open challenges in blackhole attack detection

- Lack of Real-Time Validation: Many models perform well in simulation but may not adapt easily to real-time or field conditions.
- Limited Benchmarking: Datasets like WSN-DS are used repeatedly; however, these do not always reflect heterogeneous or real-world traffic conditions.
- Insufficient Focus on HWSNs: While some models claim applicability to HWSNs, many do not account for the diversity in node capability, energy availability, and communication range.
- Overhead from Advanced Techniques: Cryptographic and DL models, while accurate, can impose significant processing and energy burdens, especially on lower-tier nodes.
- Scalability Issues: Centralized models or those requiring heavy coordination (e.g., Fuzzy-GA-TLBO) face challenges in scaling to large networks.

5.3 Few novel methodologies for blackhole detection in heterogeneous wireless sensor networks, including deep learning and blockchain-based systems

- Ensemble Learning [40]: Adaptive ensemble models (e.g., Random Forest, XGBoost, Hoeffding Tree) offer high accuracy and resilience to concept drift in streaming data environments.
- LSTM-Based Detection [41]: DL with LSTM enables modeling of sequential behavior in routing, improving detection of stealthy attacks like blackholes.
- Blockchain-Based Detection [42]: Using distributed ledgers to verify node behavior adds tamper-resistance and traceability to network monitoring.
- Trust Degradation Metrics: Exponential trust reduction strategies help identify persistent malicious nodes by analyzing patterns of packet drops.
- Voting Mechanisms in Clusters: Consensus-based validation among cluster nodes enhances robustness and reduces FDRs.

5.4 Adaptability of existing protocols from homogeneous wireless sensor networks to heterogeneous models

Although many intrusion detection protocols were initially created for homogeneous WSNs, they are still not very adaptable to HWSNs unless they are changed. Networks with heterogeneous node capabilities are incompatible with protocols that assume uniform energy or bandwidth. Nonetheless, certain models can be easily adapted to HWSNs, particularly trust-based, cluster-based, and mobile agent-based architectures. For example:

- Cluster-based IDS can leverage high-power nodes as aggregators or monitors.
- ML models like ensemble learners can handle data from heterogeneous sources if designed with dynamic feature weighting.
- Distributed trust-based systems can be adapted for local anomaly detection across tiered nodes.

Overall, successful adaptation requires that protocols recognize node role and resource diversity, offload complex computation to capable nodes (high-power), and enable lightweight participation for energy-constrained nodes.

The framework overview for HWSNs integrates intelligent, time-sensitive attack detection mechanisms to support secure network communication against blackhole attacks. The network is structured into three major layers: The Sensor Network, Processing and Management, and Security and Attack Detection. In the Sensor Network layer, low-power sensor nodes with limited resources perform basic sensing tasks and transmit raw data to nearby high-power sensor nodes, which possess enhanced aggregation, processing, and communication capabilities. The high-power nodes aggregate the sensed data and forward it to the central sink node within the Processing and Management layer. The sink node collects behavior and communication patterns from multiple nodes and forwards the structured behavior data to a time-aware attack detection module in the Security and Attack Detection layer.

The detection module utilizes sequential behavior analysis to identify anomalous activities such as packet drops and suspicious routing patterns associated with blackhole attacks. Once an anomaly is identified, the information is passed to a response engine responsible for generating alerts, isolating compromised nodes, and updating routing paths to ensure secure network operation. The response engine then communicates routing decisions back to the sink node and the high-power nodes, maintaining the continuity and integrity of data transmission. This modular, learning-based detection architecture supports adaptability to evolving attack behaviors while preserving energy efficiency and meeting the real-time requirements of heterogeneous wireless sensor deployments. Figure 1 shows an overview of HWSN-based attack detection. Table 4 shows the design considerations for security protocols in HWSNs.

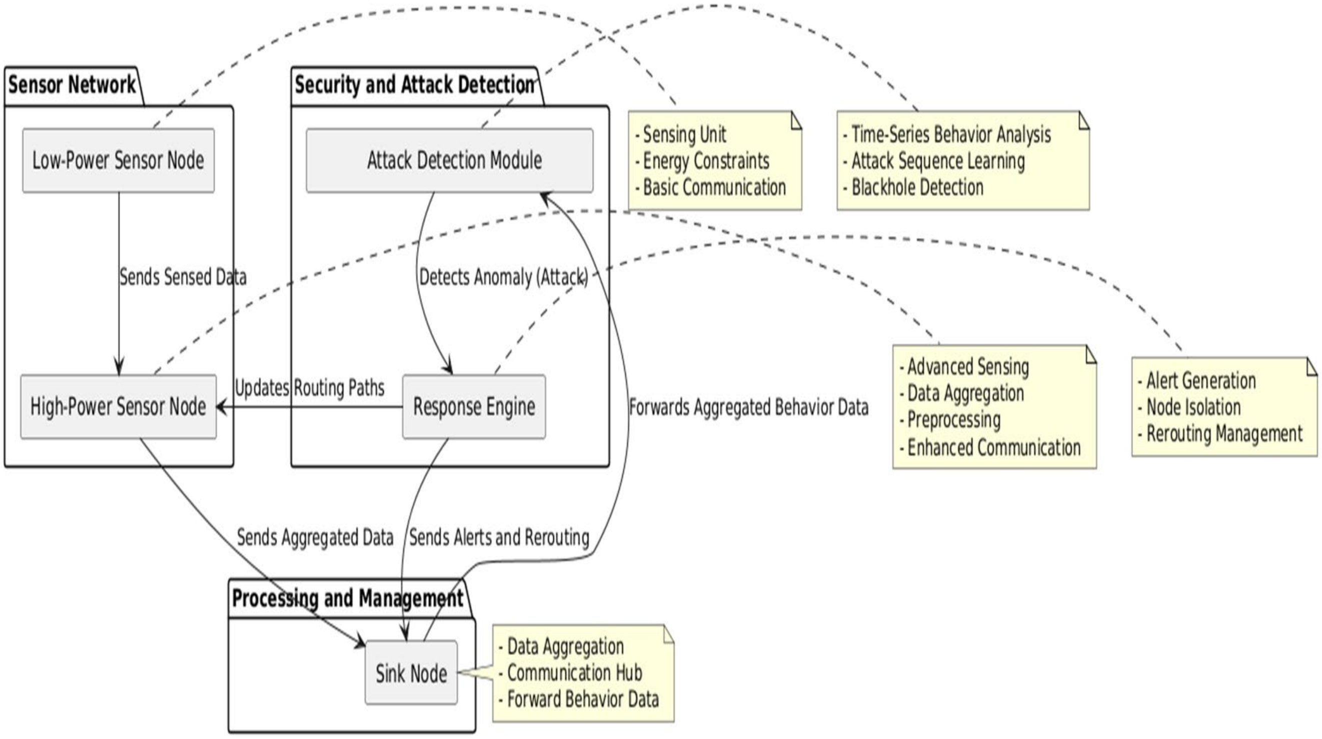

Figure 1. An overview for heterogeneous wireless sensor network (HWSN) based attack detection

Table 4. Design considerations

Design Consideration	Description
Energy Efficiency	Minimize computational and communication overhead to preserve energy, especially on low-power nodes.
Scalability	Ensure effectiveness in large-scale, dense, and expanding networks without performance degradation.
Heterogeneity Awareness	Account for varied node capabilities and distribute detection tasks appropriately.
Accuracy and Low FDRs	Achieve high detection accuracy with minimal false positives/negatives to avoid disruptions.
Lightweight Implementation	Design simple algorithms that require minimal memory, processing, and bandwidth.
Real-Time Detection and Responsiveness	Detect and respond to attacks quickly to minimize data loss and communication disruption.
Robustness Against Collusion and Mobility	Handle both single/cooperative attacks and adapt to dynamic, mobile topologies.
Trust Management	Use dynamic, context-aware trust evaluation to distinguish malicious nodes from faulty ones.
Interoperability with Routing Protocols	Integrate seamlessly with existing energy-efficient and hierarchical routing protocols.
Distributed vs. Centralized Detection Balance	Balance distributed detection to reduce overhead while avoiding single points of failure.
Resilience and Fault Tolerance	Maintain functionality and security even when nodes fail or are compromised.
Adaptability to Evolving Attacks	Adapt to new blackhole strategies through learning or flexible detection rules.
Secure Data Aggregation and Communication	Ensure secure data handling and prevent tampering despite routing disruptions.

6. CONCLUSIONS

This paper presented a comprehensive survey and analysis of security protocols for blackhole attack detection in HWSNs. Through a structured taxonomy and detailed review, the study highlights that trust-based, routing-aware, hybrid models and lightweight learning-assisted approaches are among the most promising strategies for HWSNs, particularly when aligned with node heterogeneity in terms of energy, computation, and communication capability. The analysis reveals critical trade-offs between detection accuracy, communication overhead, scalability, and energy consumption, which significantly influence the practical applicability of existing solutions in real-world deployments. The survey also shows that many existing protocols achieve strong performance in controlled or simulation environments but often lack explicit consideration of heterogeneous node roles, real-time constraints, and scalability to large networks. Approaches that leverage higher-capability nodes or centralized sinks for monitoring and decision-making tend to offer better resilience, while overly complex cryptographic or computation-heavy techniques can impose excessive burdens on low-tier nodes. These findings emphasize the need for adaptive, energy-aware, and role-aware security designs in HWSNs. Based on the insights gained from the surveyed literature, a generalized coordinated detection and response framework—where low-power and high-power nodes collaborate under a centralized sink—emerges as a practical design direction for improving blackhole attack resilience. Future research should focus on extending such frameworks to handle more complex attacks, including wormhole, Sybil, and greyhole attacks, while maintaining low overhead. Additional directions include incorporating lightweight cryptographic mechanisms, adaptive and context-aware detection models, real-world testbed validation, mobility support, and decentralized trust management approaches, such as blockchain, to further enhance robustness and adaptability in heterogeneous wireless sensor environments.

REFERENCES

[1] Arshad, A., Hanapi, Z.M., Subramaniam, S., Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. PeerJ Computer Science, 7: e673. https://doi.org/10.7717/peerj-cs.673

[2] Jadidoleslamy, H. (2011). Designing an agent-based intrusion detection system for heterogeneous wireless sensor networks: Robust, fault tolerant and dynamic reconfigurable. International Journal of Communications, Network and System Sciences, 4(8): 523-543. https://doi.org/10.4236/ijcns.2011.48064

[3] Sreenivasu, M., Kumar, U.V., Dhulipudi, R. (2022). Design and development of intrusion detection system for wireless sensor network. Journal of VLSI Circuits and Systems, 4(2): 1-4. https://doi.org/10.31838/jvcs/04.02.01

[4] John, A., Isnin, I.F.B., Hamid Hussain Madni, S., Faheem, M. (2024). Intrusion detection in cluster-based wireless sensor networks: Current issues, opportunities and future research directions. IET Wireless Sensor Systems, 14(6): 293-332. https://doi.org/10.1049/wss2.12100

[5] Chandre, P.R., Mahalle, P., Shinde, G. (2022). Intrusion prevention system using convolutional neural network for wireless sensor network. IAES International Journal of Artificial Intelligence, 11(2): 504-515. https://doi.org/10.11591/ijai.v11.i2.pp504-515

[6] Gutiérrez-Portela, F., Almenares-Mendoza, F., Calderón-Benavides, L., Romero-Riaño, E. (2021). Security perspective of wireless sensor networks. Revista UIS Ingenierías, 20(3): 189-202. https://doi.org/10.18273/revuin.v20n3-2021014

[7] Ismail, S., Dawoud, D.W., Reza, H. (2023). Cyberattacks in wireless sensor networks. Encyclopedia. https://encyclopedia.pub/entry/49346

[8] Chandre, P.R., Mahalle, P.N., Shinde, G.R. (2018). Machine learning based novel approach for intrusion detection and prevention system: A tool based verification. In 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, pp. 135-140. https://doi.org/10.1109/GCWCN.2018.8668618

[9] Oztoprak, A., Hassanpour, R., Ozkan, A., Oztoprak, K. (2024). Security challenges, mitigation strategies, and

future trends in wireless sensor networks: A review. ACM Computing Surveys, 57(4): 1-29. https://doi.org/10.1145/3706583

[10] Almomani, I., Alromi, A. (2020). Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks. Sensors, 20(5): 1375. https://doi.org/10.3390/s20051375

[11] John, A., Isnin, I.F.B., Madni, S.H.H., Faheem, M. (2024). Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms. Intelligent Systems with Applications, 22: 200381. https://doi.org/10.1016/j.iswa.2024.200381

[12] Jadidoleslamy, H. (2011). A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: Hierarchical, scalable and dynamic reconfigurable. Wireless Sensor Network, 3(7): 241-261. https://doi.org/10.4236/wsn.2011.37026

[13] Sreekumaridevi, R.M. (2011). Cognitive security framework for heterogeneous sensor network using swarm intelligence. Syracuse University.

[14] Bukhari, S.M.S., Zafar, M.H., Abou Houran, M., Moosavi, S.K.R., Mansoor, M., Muaaz, M., Sanfilippo, F. (2024). Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 155: 103407. https://doi.org/10.1016/j.adhoc.2024.103407

[15] Wang, Y., Qin, M. (2010). Security for wireless sensor networks. In ICCAS 2010, Gyeonggi-do, Korea (South), pp. 844-848. https://doi.org/10.1109/ICCAS.2010.5669748

[16] Khan, M.A., Rais, R.N.B., Khalid, O., Ahmad, S. (2024). Trust-based optimized reporting for detection and prevention of black hole attacks in low-power and lossy green IoT networks. Sensors, 24(6): 1775. https://doi.org/10.3390/s24061775

[17] Boubiche, S., Boubiche, D.E., Bilami, A., Toral-Cruz, H. (2016). An outline of data aggregation security in heterogeneous wireless sensor networks. Sensors, 16(4): 525. https://doi.org/10.3390/s16040525

[18] Ramesh, R.B., Thangaraj, S.J.J., Sagayee, G.M.A., Saravanan, K. (2025). Detection and prevention in WSN security framework using deep learning against black hole and wormhole attacks. Ain Shams Engineering Journal, 16(10): 103624. https://doi.org/10.1016/j.asej.2025.103624

[19] Ghugar, U., Dash, S., Jena, S., Swain, N.K., Brahma, B., Sahoo, S.K. (2024). DLTIDS: A dual-layer trust-based intrusion detection system for blackhole attacks in wireless sensor networks. Nanotechnology Perceptions, 20(S6): 171-187. https://doi.org/10.62441/nano-ntp.v20iS6.13

[20] Khan, S., Khan, M.A., Alnazzawi, N. (2024). Artificial neural network-based mechanism to detect security threats in wireless sensor networks. Sensors, 24(5): 1641. https://doi.org/10.3390/s24051641

[21] Kim, I., Oh, D., Yoon, M.K., Yi, K., Ro, W.W. (2013). A distributed signature detection method for detecting intrusions in sensor systems. Sensors, 13(4): 3998-4016. https://doi.org/10.3390/s130403998

[22] Almseidin, M., Al-Sawwa, J., Alkasassbeh, M. (2021). Anomaly-based intrusion detection system using fuzzy logic. In 2021 International Conference on Information Technology (ICIT), Amman, Jordan, pp. 290-295. https://doi.org/10.1109/ICIT52682.2021.9491742

[23] Saxe, J., Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. In 2015 10th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, PR, USA, pp. 11-20. https://doi.org/10.1109/MALWARE.2015.7413680

[24] Saravanakumar, P., Sundararajan, T.V.P., Dhanaraj, R.K., Nisar, K., Memon, F.H., Ibrahim, A.A.B. (2022). Lamport certificateless signcryption deep neural networks for data aggregation security in WSN. Intelligent Automation & Soft Computing, 33(3): 1835-1847. https://doi.org/10.32604/iasc.2022.018953

[25] Clement Sunder, A.J., Shanmugam, A. (2020). Black hole attack detection in healthcare wireless sensor networks using independent component analysis machine learning technique. Current Signal Transduction Therapy, 15(1): 56-64. https://doi.org/10.2174/1574362413666180705123733

[26] Abdelrahman, D., Rasslan, M., Abdelbaki, N. (2025). A blockchain-based malware detection model for IoT devices. International Journal of Safety & Security Engineering, 15(1): 13-20. https://doi.org/10.18280/ijsse.150102

[27] Terence, J.S., Purushothaman, G. (2019). A novel technique to detect malicious packet dropping attacks in wireless sensor networks. Journal of Information Processing Systems, 15(1): 203-216. https://doi.org/10.3745/JIPS.03.0110

[28] Ashfaq, T., Khalid, R., Yahaya, A.S., Aslam, S., Azar, A.T., Alsafari, S., Hameed, I.A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19): 7162. https://doi.org/10.3390/s22197162

[29] Liu, Y., Wu, Y. (2021). Employ DBSCAN and neighbor voting to screen selective forwarding attack under variable environment in event-driven wireless sensor networks. IEEE Access, 9: 77090-77105. https://doi.org/10.1109/ACCESS.2021.3083105

[30] Tabbaa, H., Ifzarne, S., Hafidi, I. (2023). An online ensemble learning model for detecting attacks in wireless sensor networks. Computing and Informatics, 42(4): 1013-1036. https://doi.org/10.31577/cai_2023_4_1013

[31] Rashid, D.A., Mohammed, M.B. (2024). Black hole attack detection in wireless sensor networks using hybrid optimization algorithm. UHD Journal of Science and Technology, 8(1): 142-150. https://doi.org/10.21928/uhdjst.v8n1y2024.pp142-150

[32] Dash, N., Chakravarty, S., Rath, A.K., Giri, N.C., AboRas, K.M., Gowtham, N. (2025). An optimized LSTM-based deep learning model for anomaly network intrusion detection. Scientific Reports, 15(1): 1554. https://doi.org/10.1038/s41598-025-85248-z

[33] Alsulaiman, L., Al-Ahmadi, S. (2021). Performance evaluation of machine learning techniques for DOS detection in wireless sensor network. International Journal of Network Security & Its Applications (IJNSA), 13(2): 21-29. https://doi.org/10.5121/ijnsa.2021.13202

[34] Virmani, D.D., Hemrajani, M., Chandel, S. (2014). Exponential trust based mechanism to detect black hole attack in wireless sensor network. arXiv Preprint arXiv: 1401.2541. https://doi.org/10.48550/arXiv.1401.2541

[35] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K.,

Qamar, F., Ahmed, A.S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021(1): 6693316. https://doi.org/10.1155/2021/6693316

[36] Malik, A., Khan, M.Z., Faisal, M., Khan, F., Seo, J.T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors, 22(5): 1897. https://doi.org/10.3390/s22051897

[37] Hasan, A., Khan, M.A., Shabir, B., Munir, A., Malik, A.W., Anwar, Z., Ahmad, J. (2022). Forensic analysis of blackhole attack in wireless sensor networks/internet of things. Applied Sciences, 12(22): 11442. https://doi.org/10.3390/app122211442

[38] Shreyanth, S. (2023). Prevention of cyberattacks in wsn and packet drop by CI framework and information processing protocol using ai and big data. arXiv Preprint arXiv:2306.09448. https://doi.org/10.48550/arXiv.2306.09448

[39] Haque, A., Chowdhury, N.U.R., Soliman, H., Hossen, M.S., Fatima, T., Ahmed, I. (2023). Wireless sensor networks anomaly detection using machine learning: A survey. In Intelligent Systems Conference, pp. 491-506. https://doi.org/10.1007/978-3-031-47715-7_34

[40] Belkacem, S. (2024). Simultaneous botnet attack detection using long short term memory-based autoencoder and XGBoost classifier. International Journal of Safety & Security Engineering, 14(1): 155-163. https://doi.org/10.18280/ijsse.140115

[41] Nikam, Y., Patil, V., Kamble, P., Shendkar, B., Vanarote, V., Chandre, P. (2025). AI-driven data leakage prevention: A deep learning-based framework for securing sensitive information. In International Conference on ICT for Sustainable Development, pp. 302-314. https://doi.org/10.1007/978-3-032-06665-7_28

[42] El-Kosairy, A., Aslan, H., Abdelbaki, N. (2024). Transforming cybersecurity: Leveraging blockchain for enhanced threat intelligence sharing. International Journal of Safety & Security Engineering, 14(4): 1139-1155. https://doi.org/10.18280/ijsse.140412