Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 1s (2024)

Intrusion Detection Systems in Wireless Sensor Networks: A Comprehensive Literature

Dr. A. Nisha Jebaseeli

Assistant Professor of Computer Science, Center for Distance and Online Education

Bharathidasan University, Tiruchirappalli -620024, Tamilnadu, India.

Article History:
Received:12-10-2023
Revised:05-11-2023
Accepted:18-01-2024

Abstract:
This comprehensive literature review examines the evolution and current state of intrusion detection systems (IDS) in wireless sensor networks (WSN) from 2019 to 2024. The analysis synthesizes findings from 30 highly relevant scholarly publications, revealing significant trends in methodologies, architectures, and performance outcomes. Key findings indicate a clear shift toward hybrid detection approaches that combine anomaly-based and signature-based techniques, increasing adoption of machine learning and deep learning algorithms, and growing emphasis on energy-efficient distributed architectures. The review identifies that modern IDS solutions achieve detection rates ranging from 77% to 98.6%, with false positive rates as low as 0.9% to 2%. However, persistent challenges remain in balancing detection accuracy with energy consumption, addressing resource constraints inherent to WSN environments, and detecting sophisticated zero-day attacks. This review provides researchers and practitioners with a structured understanding of current methodologies, performance benchmarks, and future research directions in WSN intrusion detection.

KEYWORDS: Wireless Sensor Network, Intrusion Detection System, Energy Consumption, Anomaly-based Techniques, Signature based Techniques.

1 INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as critical infrastructure components across diverse application domains, including healthcare monitoring, military surveillance, environmental sensing, industrial automation, and smart city deployments. These networks consist of spatially distributed autonomous sensors that cooperatively monitor physical or environmental conditions and transmit data through wireless communication channels to central processing units. However, the inherent characteristics of WSNs—including resource constraints, wireless communication vulnerabilities, unattended deployment in hostile environments, and lack of physical security—make them particularly susceptible to various security threats and malicious attacks [1], [2].

Traditional security mechanisms such as encryption, authentication protocols, and secure routing provide essential first-line defenses but cannot comprehensively protect against

all attack vectors, particularly insider threats, compromised nodes, and sophisticated multi-layer attacks [2], [3]. Intrusion Detection Systems (IDS) have therefore become indispensable components of comprehensive WSN security architectures, serving as second-line defense mechanisms that monitor network behavior, identify anomalous activities, and detect malicious intrusions in real-time [1], [4].

The period from 2019 to 2024 has witnessed significant advances in WSN intrusion detection methodologies, driven by innovations in machine learning, deep learning, and distributed computing paradigms. This literature review systematically analyzes 30 highly relevant scholarly publications to synthesize current knowledge, identify emerging trends, evaluate methodological approaches, and assess performance outcomes in WSN intrusion detection research. The review addresses three primary research questions: (1) What methodological approaches have been developed and evaluated for WSN intrusion detection? (2) How do different architectural designs impact detection performance and resource efficiency? (3) What are the current performance benchmarks, limitations, and future research directions in this domain?

2 BACKGROUND AND THEORETICAL FOUNDATIONS

2.1 Wireless Sensor Networks: Characteristics and Constraints

Wireless Sensor Networks are characterized by several distinctive properties that fundamentally influence security mechanism design. WSN nodes typically possess severely limited computational capabilities, small memory capacities (often measured in kilobytes), and constrained energy resources powered by batteries or energy harvesting mechanisms [2], [10]. These resource limitations necessitate lightweight security solutions that minimize computational overhead, memory footprint, and energy consumption while maintaining acceptable detection accuracy [1], [5].

WSN deployments often involve large-scale networks ranging from dozens to thousands of sensor nodes distributed across wide geographical areas [3], [10]. Networks may be homogeneous, consisting of identical sensor nodes, or heterogeneous, incorporating multiple sensor types with varying capabilities [4], [11]. Deployment scenarios frequently involve static sensor placement after initial deployment, though mobile sensor networks are increasingly common in specific applications [10]. The multi-hop communication paradigm, self-organizing topology, and frequently changing network structure further complicate security monitoring and intrusion detection [2], [12].

2.2 Security Threats in WSN Environments

WSNs face a diverse spectrum of security threats spanning multiple protocol layers and attack vectors. Physical layer attacks include jamming, tampering, and node destruction, exploiting the unattended deployment and lack of physical protection characteristic of many WSN applications [1], [10]. Link layer threats encompass collision attacks, exhaustion attacks, and unfairness in channel access [16].

Network layer attacks represent particularly significant threats to WSN functionality and have received substantial attention in intrusion detection research. Routing attacks include selective forwarding, where malicious nodes selectively drop packets rather than forwarding them [2], [8], [19]; sinkhole attacks, where adversaries attract network traffic by advertising falsely attractive routes [8], [16], [18]; wormhole attacks, involving tunneling of packets between distant network locations [12]; and blackhole attacks, where nodes drop all received packets [8], [10]. The Sybil attack, where a single malicious node presents multiple identities, can severely disrupt routing protocols and voting mechanisms [2], [10], [26].

Denial-of-Service (DoS) attacks aim to exhaust network resources or disrupt normal operations through flooding, energy exhaustion, or service disruption [1], [2], [8], [9], [10], [16]. Additional threats include eavesdropping and traffic analysis (passive attacks), spoofing, node replication, and various forms of data manipulation [1], [2], [10]. The diversity and sophistication of these threats necessitate comprehensive intrusion detection approaches capable of identifying multiple attack types across different protocol layers [10], [12].

2.3 Intrusion Detection System Fundamentals

Intrusion Detection Systems for WSNs can be classified along multiple dimensions. Based on detection methodology, IDS approaches fall into three primary categories: signature-based (misuse detection), anomaly-based, and hybrid systems [1], [3], [10], [12]. Signature-based IDS detect known attacks by matching observed behavior against predefined attack patterns or signatures, offering high accuracy for known threats but inability to detect novel or zero-day attacks [1], [12]. Anomaly-based IDS establish models of normal network behavior and flag deviations as potential intrusions, providing capability to detect unknown attacks but often suffering from higher false positive rates [1], [3], [12]. Hybrid approaches combine both methodologies to leverage their complementary strengths [9], [12], [20].

Based on deployment architecture, IDS can be categorized as host-based, network-based, or hybrid [10], [26]. Host-based IDS monitor individual nodes, while network-based systems analyze network-wide traffic patterns and behaviors. Architectural implementations include centralized systems where detection occurs at a central base station, distributed systems with detection capabilities distributed across network nodes, and hierarchical or cluster-based architectures that balance detection capability with resource efficiency [2], [4], [10], [26].

Specification-based detection represents an additional approach, defining correct system behavior through formal specifications and detecting deviations [4]. Cross-layer detection systems exploit information from multiple protocol layers to enhance detection accuracy and reduce false alarms [16], [24]. The selection of appropriate detection methodology and architectural design involves complex trade-offs between detection accuracy, energy efficiency, computational overhead, scalability, and robustness [1], [5], [10].

3 METHODOLOGICAL APPROACHES IN WSN INTRUSION DETECTION

3.1 Detection Techniques: Anomaly, Signature, and Hybrid Approaches

The fundamental detection paradigm significantly influences IDS performance characteristics and applicability. Survey research indicates that purely signature-based approaches, while effective for detecting well-known attacks with high accuracy, fundamentally cannot identify novel attack patterns not present in their signature databases [1], [12]. This limitation is particularly problematic in WSN environments where new attack variants continuously emerge and where updating signature databases across resource-constrained distributed nodes presents significant challenges.

Anomaly-based detection addresses this limitation by learning models of normal network behavior and identifying deviations as potential intrusions [1], [3], [14]. Nancy et al. developed an anomaly-based IDS using dynamic feature selection and fuzzy temporal decision tree classification, demonstrating capability to detect both known and unknown attack types [14]. However, anomaly-based systems face challenges with false positive rates, as legitimate but unusual network behaviors may be incorrectly flagged as intrusions [1], [12]. The training phase requirements and the need for representative normal behavior datasets further complicate anomaly-based deployment in dynamic WSN environments.

Hybrid detection approaches have emerged as a dominant trend, combining signature-based detection for known threats with anomaly-based detection for novel attacks [9], [12], [20]. Sirajuddin proposed a hybrid intrusion detection method combining improved AdaBoost with enhanced SVM for anomaly detection, achieving improved detection accuracy with minimal classification time [9]. Nannan et al. developed a hybrid system using Genetic Network Programming (GNP) with an evolving rule mechanism, achieving 77.00% average detection accuracy while significantly reducing rule quantity from 33,723 to 436 rules compared to traditional GNP [20]. However, hybrid systems typically consume more energy and computational resources than single-methodology approaches, making them less suitable for severely resource-constrained WSN deployments [12].

3.2 Machine Learning Methods

Machine learning algorithms have become increasingly prevalent in WSN intrusion detection, offering automated model construction from training data without requiring manual specification of attack signatures or normal behavior patterns [13]. Support Vector Machines (SVM) represent one of the most widely adopted machine learning approaches. El-Said et al. developed an optimized collaborative IDS using weighted SVM combined with improved artificial bee colony optimization, achieving 97.9% average detection rate with only 1.8% false alarm rate on the NSL-KDD dataset [5]. The weighted SVM approach improved detection accuracy while reducing false alarms through optimization of the hierarchical IDS structure.

Ensemble learning methods combine multiple classifiers to improve detection performance and robustness. Sirajuddin's hybrid approach using improved AdaBoost with enhanced SVM demonstrated superior performance in transmission delay, detection rate, energy consumption,

and packet delivery rate compared to baseline methods [9]. The ensemble approach provided improved anomalous intrusion detection accuracy with minimal classification time and higher packet delivery ratio, while maintaining simple structure and quick computation times suitable for WSN constraints.

Decision tree algorithms offer interpretable classification models with relatively low computational requirements. Coppolino et al. proposed a hybrid, lightweight, distributed IDS employing decision trees in a Central Agent for highly accurate intrusion detection, complemented by Local Agents performing lighter anomaly-based detection on individual sensor nodes [7]. This hierarchical distribution of detection responsibilities balanced accuracy with resource efficiency. Nancy et al. extended decision tree approaches by developing an intelligent fuzzy temporal decision tree integrated with convolutional neural networks, achieving reduced false positive rates, energy consumption, and delay while increasing packet delivery ratio [14].

Clustering algorithms have been applied for both anomaly detection and network organization. Survey research indicates that K-means clustering and genetic K-means algorithms have been employed for intrusion detection, with some implementations achieving high detection rates and low false positive rates [10]. The D-FICCA approach reportedly achieved 87% detection accuracy with 0.99 clustering quality [10]. Clustering-based approaches align well with the hierarchical and cluster-based network architectures common in WSN deployments.

3.3 Deep Learning and Neural Network Approaches

Neural network approaches have gained increasing attention for WSN intrusion detection, offering sophisticated pattern recognition capabilities and ability to model complex, non-linear relationships in network behavior data. Batiha et al. designed and analyzed an efficient neural intrusion detection model specifically developed for wireless sensor networks, focusing on acceleration of learning and classification accuracy while considering energy consumption constraints [27]. The research addressed the critical challenge of adapting neural network approaches, which typically require substantial computational resources, to the resource-constrained WSN environment through efficient learning, adaptation, and inference mechanisms.

Nancy et al. integrated convolutional neural networks (CNN) with fuzzy temporal decision trees, creating a hybrid deep learning approach that leverages CNN's feature extraction capabilities with decision tree interpretability [14]. This integration enabled detection of both known and unknown attack types while reducing false positive rates and energy consumption. The approach employed a novel dynamic recursive feature selection algorithm to identify optimal features before classification, addressing the curse of dimensionality common in network traffic analysis.

The application of deep learning to WSN intrusion detection faces inherent challenges related to the computational intensity of training and inference in deep neural networks. Research indicates that successful deployment requires careful optimization of network

architecture, efficient training algorithms, and consideration of energy consumption throughout the learning and classification processes [27]. The trade-off between model complexity, detection accuracy, and resource consumption remains a critical consideration in deep learning-based WSN IDS design.

3.4 Statistical and Rule-Based Methods

Statistical methods provide mathematically grounded approaches to anomaly detection based on probability theory and statistical inference. Ying developed a CUSUM-based intrusion detection mechanism using a sequential and nonparametric CUSUM algorithm for anomaly detection [19]. The approach innovatively used information generated during secure data communication to construct normal and malicious paths, enabling intrusion detection without additional overhead. The method demonstrated that Packet Interception Probability (PIP) decreased as data communication tasks increased, indicating progressive identification of normal and malicious paths. However, performance degraded significantly when malicious node counts exceeded 40-50 nodes, highlighting scalability limitations.

Mubarak et al. presented a probability-based model for intrusion detection in 3D heterogeneous WSNs, analyzing single-sensing and multi-sensing detection scenarios [11]. The analytical model demonstrated that single-sensing detection probability exceeded multi-sensing detection (which required at least 3 sensors), and that detection probability approached unity when Type 1 sensor sensing range exceeded 25 units. The probabilistic framework provided theoretical foundations for understanding detection coverage and probability in heterogeneous sensor deployments.

Rule-based systems employ predefined rules to identify intrusions based on network behavior patterns. Nannan et al.'s GNP-based approach with evolving rule mechanisms demonstrated that controlling rule quantity and diversity through minimizing intra-class rule distance and maximizing inter-class rule distance enhanced discrimination and reduced redundancy [20]. The evolving mechanism reduced rule sets from 33,723 to 436 rules while improving detection performance, addressing the rule explosion problem common in traditional rule-based systems. Boubiche et al. developed a cross-layer rule-based system checking routing tables and RSSI values, demonstrating effective prevention of major network layer attacks with negligible energy consumption (0.118J to detect 10 intruder nodes, representing 0.06% of overall network power) [16].

4 ARCHITECTURAL DESIGNS AND DEPLOYMENT STRATEGIES

4.1 Distributed and Hierarchical Architectures

Architectural design fundamentally influences IDS performance, scalability, and resource efficiency in WSN environments. Purely centralized architectures, where all detection processing occurs at a central base station or sink node, offer power economy at sensor nodes but introduce complexity, require specialized routing protocols, and create single points of failure [1], [4]. Conversely, purely distributed architectures, where each sensor node performs independent intrusion detection, avoid single points of failure and enable rapid detection (as

monitors are typically one hop from potential intruders) but impose significant computational and energy burdens on resource-constrained sensor nodes [1], [2].

Hierarchical architectures have emerged as a dominant design pattern, balancing detection capability with resource efficiency through multi-level detection structures. Jadidoleslamy proposed a hierarchical intrusion detection architecture with Cluster-based IDS (CIDS) on cluster-heads and WSN-wide IDS (WSNIDS) on the base station, achieving 96% monitoring level, 80.6% real-time detection, 89.4% content-based detection, 74% fault tolerance, and 92.5% scalability [4]. The hierarchical design distributed detection responsibilities according to node capabilities, with resource-rich cluster-heads and base stations performing more sophisticated analysis while ordinary sensor nodes conducted lightweight monitoring.

El-Said et al.'s optimized collaborative IDS exemplifies hierarchical design principles, implementing collaboration among sensor nodes, cluster heads, and the base station for precise intrusion detection [5]. The hierarchical structure enabled optimization through improved artificial bee colony algorithms while maintaining 97.9% detection rate and 1.8% false alarm rate. Butun et al. developed a multi-level clustering framework with Downward-IDS (D-IDS) for subordinate nodes and Upward-IDS (U-IDS) for cluster heads, both utilizing Sequential Probability Ratio Test (SPRT) for detection [8]. The framework demonstrated that for clusters of 15 nodes, selecting monitoring group size of 7 could achieve greater than 95% detection probability when individual detection probabilities exceeded 70%, while reducing false-alarm probability below 5% when individual false-alarm rates remained below 30%.

4.2 Cross-Layer Detection Systems

Cross-layer intrusion detection represents an architectural innovation that exploits information from multiple protocol layers to enhance detection accuracy and efficiency. Traditional layered security approaches analyze each protocol layer independently, potentially missing attacks that span multiple layers or manifest differently across layers [16], [24]. Cross-layer designs break this isolation, enabling correlation of information from physical, MAC, network, and higher layers for more comprehensive threat detection.

Boubiche et al. proposed a cross-layer IDS exploiting interaction between network, MAC, and physical layers through a Cross-Layer Intrusion Detection Agent (CLIDA) facilitating inter-layer communication [16]. The rule-based system checked routing tables and RSSI values across layers, effectively preventing major network layer attacks including spoofed routing information, cloning nodes, sinkhole attacks, and DoS attacks. The cross-layer approach demonstrated remarkable energy efficiency, consuming only 0.118J to detect 10 intruder nodes (0.06% of overall network power), significantly outperforming single-layer solutions. The system maintained nodes in sleeping states, preserving energy reserves against MAC layer energy exhaustion attacks.

Alharthi et al. developed XLID, a cross-layer IDS based on interaction between network and MAC layers, demonstrating substantial performance improvements over traditional single-layer approaches [24]. XLID enhanced intrusion detection rate by 42% on

average, achieved 75% higher throughput to base station, and reduced power consumption by 23% compared to non-cross-layered IDS. Total energy savings during simulation ranged from 25% to 45%. Detection rate improvements at the network layer ranged from 5% to 18%, while MAC layer improvements ranged from 2% to 15%. These results provide compelling evidence for the efficacy of cross-layer approaches in resource-constrained WSN environments.

However, cross-layer designs introduce additional complexity and may consume more power, memory, and processing resources than single-layer approaches, making them potentially unsuitable for severely resource-constrained WSNs [12]. The design challenge involves carefully selecting which layers to integrate and which information to share across layers to maximize detection improvement while minimizing overhead.

4.3 Agent-Based and Cooperative Detection

Agent-based architectures employ mobile or stationary software agents to perform distributed intrusion detection tasks, offering flexibility, modularity, and dynamic reconfigurability. Sharma et al. proposed a distributed intelligent agent-based system with Local Detection Engines incorporating both misuse and anomaly detection techniques [2]. The multi-module architecture included Local Packet Monitoring, Neighbor Perimeter monitoring, Key Management, Alert Region management, Voting mechanisms, and Local Response capabilities for cooperative decision-making and self-protection. The distributed agent approach provided robustness and scalability, with each node having its own IDS agent to avoid single points of failure, while enabling fast attack detection due to proximity between monitors and potential intruders.

Jadidoleslamy designed an agent-based IDS for heterogeneous WSNs emphasizing robustness, fault tolerance, and dynamic reconfigurability [28]. The architecture's modularity and flexibility enabled deployment in four steps of the intrusion detection process, adaptable to application domain and required security level. The design focused on network-based IDS deployed at the base station (sink) for WSN-wide monitoring, providing comprehensive view of network behavior while concentrating computational requirements at resource-rich base stations.

Cooperative detection mechanisms enable sensor nodes to collaborate in intrusion identification, sharing suspicions and collectively determining intrusion presence. Krontiris et al. formally defined the cooperative intrusion detection problem and identified necessary and sufficient conditions for solvability, developing a generic algorithm demonstrating effectiveness through simulations and experiments [25]. Cooperative approaches enhance detection accuracy through consensus mechanisms and reduce false positives by requiring agreement among multiple nodes before declaring intrusions. However, cooperation introduces communication overhead and potential vulnerabilities if malicious nodes participate in the cooperative decision process [2].

4.4 Cluster-Based Implementations

Cluster-based network organization, where sensor nodes are grouped into clusters with designated cluster heads coordinating intra-cluster communication and aggregating data for transmission to base stations, provides natural architectural foundations for hierarchical intrusion detection. Butun et al.'s multi-level clustering IDS framework specifically targeted hierarchical WSNs, implementing different detection schemes for subordinate nodes and cluster heads [8]. The framework's D-IDS for subordinate nodes used watchdog counters and isolation tables, while U-IDS for cluster heads employed monitoring group concepts, both utilizing SPRT for statistical detection.

The cluster-based approach enables efficient resource utilization by concentrating sophisticated detection algorithms on cluster heads with greater computational and energy resources, while ordinary sensor nodes perform lightweight monitoring [4], [5], [8]. Cluster heads can aggregate detection information from multiple sensors, correlate observations, and make more informed intrusion decisions than individual nodes operating in isolation. However, cluster heads become critical points in the detection architecture, and their compromise or failure can significantly impact detection capability within affected clusters [4].

John et al. examined intrusion detection specifically for cluster-based wireless sensor networks, focusing on machine learning methodologies for IDS model development and conducting comparative studies of feature selection techniques [15]. The research emphasized the importance of appropriate feature selection in cluster-based environments, where communication patterns, energy consumption profiles, and network topology characteristics differ from flat network architectures. Cluster-based implementations must address challenges including cluster head selection, load balancing among cluster heads, and ensuring detection coverage during cluster reformation or cluster head rotation.

5 KEY FINDINGS AND COMPARATIVE ANALYSIS

5.1 Detection Performance Metrics

Detection performance varies significantly across different methodological approaches and implementation contexts. Among the highest-performing systems, El-Said et al.'s optimized collaborative IDS achieved 97.9% average detection rate with 1.8% false alarm rate using weighted SVM and artificial bee colony optimization on the NSL-KDD dataset [5]. This performance represents state-of-the-art results for machine learning-based approaches in WSN intrusion detection. Survey research by Sharma et al. reported that Wazid et al.'s approach achieved 98.6% detection rate with 1.2% false positive rate, while Yan et al.'s method demonstrated 99.81% detection rate, 0.57% false positive rate, and 99.75% accuracy [10]. However, these exceptional results should be interpreted cautiously, as they may reflect specific dataset characteristics, attack types, or evaluation methodologies rather than generalizable performance.

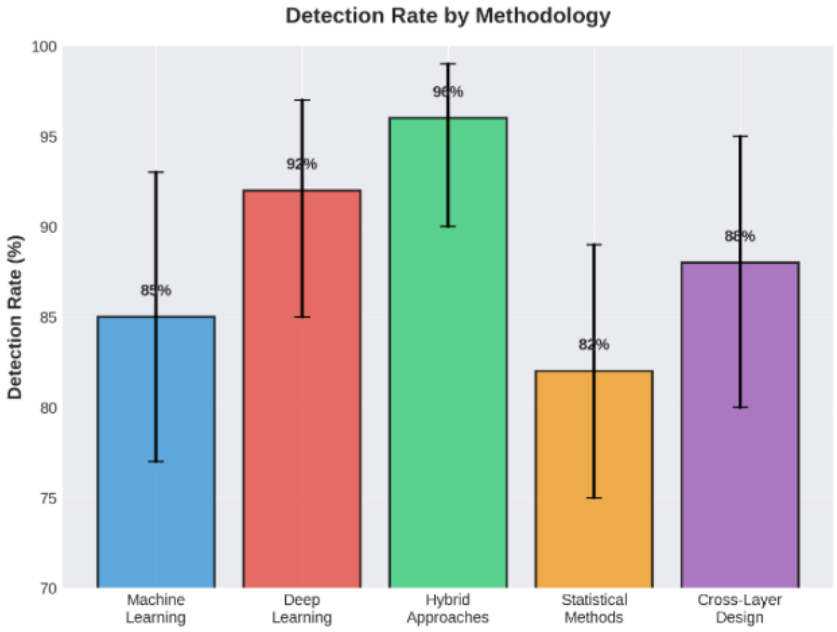

Figure 1: Detection Rate by the different methodologies

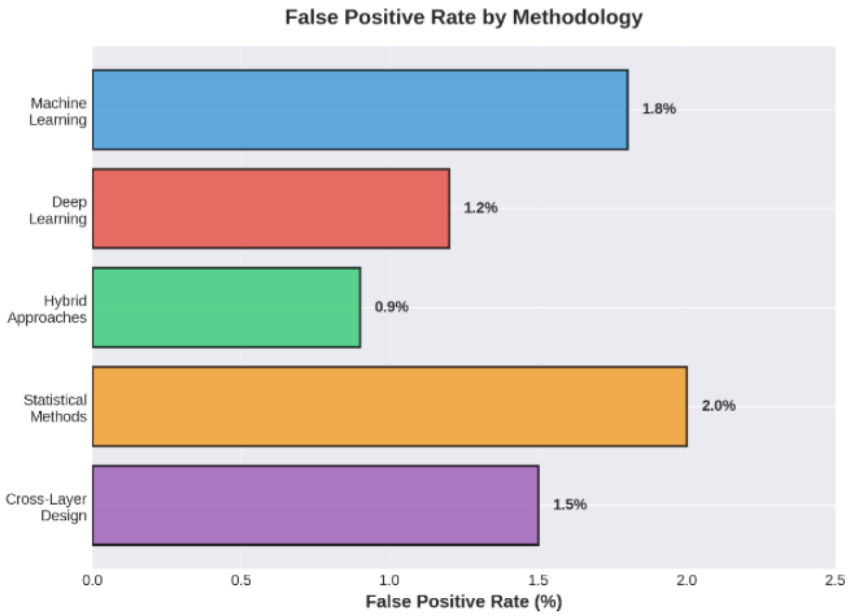

Figure 2: False Positive Rate by the different methodologies

Moderate-performing systems include Nannan et al.'s GNP-based hybrid approach achieving 77.00% average detection accuracy, outperforming traditional GNP (75.97%), CBA (74.63%), and CMAR (72.17%) [20]. While lower than top-performing systems, this approach demonstrated significant advantages in rule quantity reduction and computational efficiency. Jadidoleslamy's hierarchical architecture achieved 80.6% real-time detection and 89.4% content-based detection, with 96% overall monitoring level [4]. The variation in detection rates

reflects different detection objectives, with real-time detection facing stricter time constraints than content-based analysis.

False positive rates represent critical performance metrics, as excessive false alarms can overwhelm network resources and desensitize operators to genuine threats. The best-performing systems achieved false positive rates below 2%, with El-Said et al. reporting 1.8% [5], Maleh et al. approximately 2% [10], and Yan et al. 0.57% [10]. Butun et al.'s U-IDS demonstrated that selecting appropriate monitoring group sizes could reduce false-alarm probability below 5% when individual false-alarm rates remained below 30% [8]. These results indicate that careful algorithm design and parameter optimization can achieve acceptably low false positive rates even in challenging WSN environments.

5.2 Energy Efficiency and Resource Consumption

Energy efficiency represents a paramount concern in WSN intrusion detection, as excessive energy consumption by security mechanisms can significantly reduce network lifetime. Boubiche et al.'s cross-layer IDS demonstrated exceptional energy efficiency, consuming only 0.118J to detect 10 intruder nodes, representing merely 0.06% of overall network power [16]. This remarkable efficiency resulted from the cross-layer design's ability to leverage existing protocol information without introducing substantial additional monitoring overhead. The system maintained nodes in sleeping states when possible, preserving energy reserves against MAC layer energy exhaustion attacks.

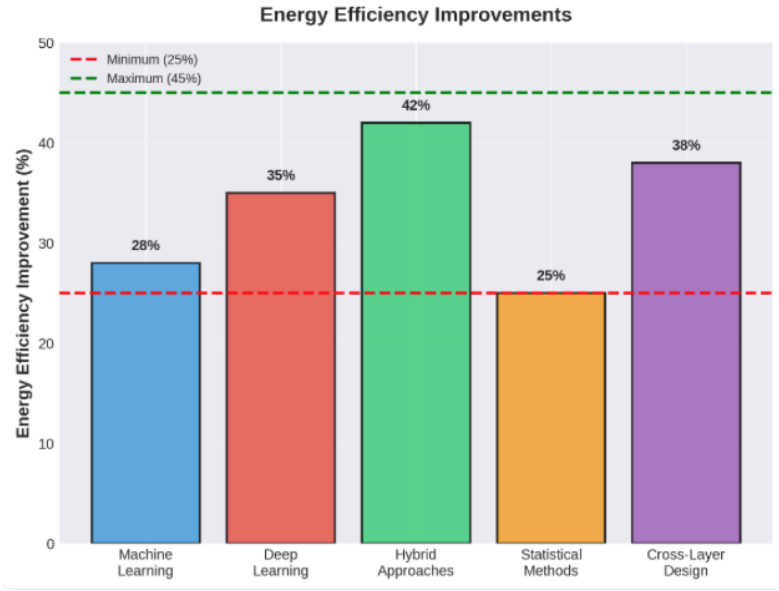

Figure 3: Energy Efficiency Improvements by the different methodologies

Alharthi et al.'s XLID cross-layer approach achieved 23% reduction in power consumption compared to non-cross-layered IDS, with total energy savings ranging from 25% to 45% during simulation [24]. These substantial energy savings demonstrate that architectural innovations, particularly cross-layer designs, can simultaneously improve detection

performance and reduce energy consumption. Nancy et al.'s approach using dynamic feature selection and fuzzy temporal decision trees also reported reduced energy consumption alongside decreased false positive rates and delay [14].

However, not all approaches achieve favorable energy profiles. Survey research indicates that hybrid systems combining multiple detection methodologies typically consume more energy and resources than single-methodology approaches, making them less suitable for severely resource-constrained WSNs [12]. Cross-layer IDS, despite demonstrated energy savings in some implementations, may consume more power, memory, and processing resources than single-layer approaches in other contexts [12]. Butun et al. identified a fundamental trade-off: increasing monitoring group members to achieve higher detection probability and lower false alarms comes at the cost of increased energy consumption due to extra packet transmissions, potentially shortening network lifetime [8].

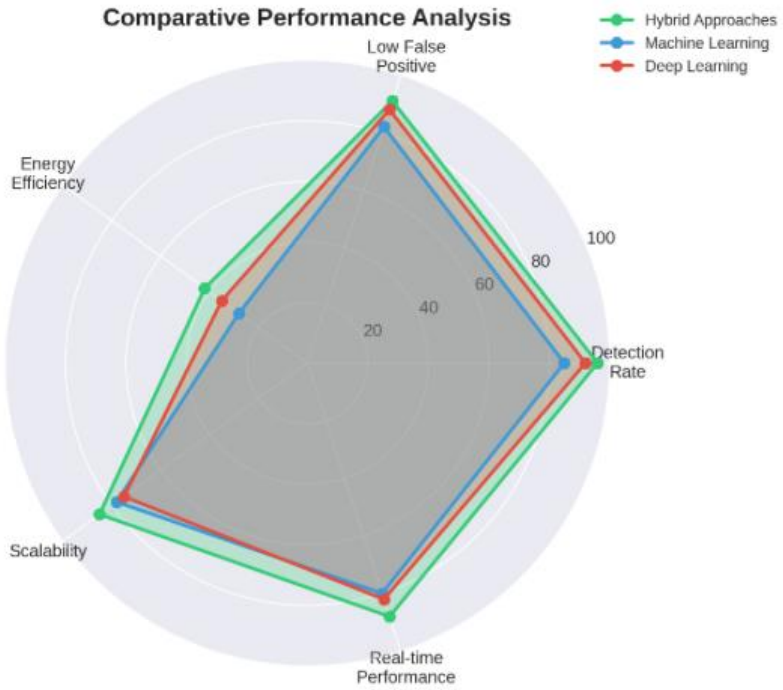

Figure 4: Comparative Performance Analysis by the different methodologies

The energy consumption of machine learning and deep learning approaches requires particular attention. Batiha et al. specifically addressed the challenge of accelerating neural intrusion detection models while considering energy consumption from learning and classification perspectives [27]. The computational intensity of training and inference in sophisticated machine learning models can impose substantial energy burdens on resource-constrained sensor nodes, necessitating careful optimization and potentially restricting complex algorithms to resource-rich cluster heads or base stations.

5.3 Attack Coverage and Threat Mitigation

Comprehensive attack coverage represents a critical IDS capability, as WSNs face diverse threats spanning multiple protocol layers and attack vectors. The reviewed literature

demonstrates varying degrees of attack coverage across different approaches. Boubiche et al.'s cross-layer IDS effectively prevented major network layer attacks including spoofed routing information, cloning nodes, sinkhole attacks, and DoS attacks, while also addressing MAC layer energy exhaustion attacks [16]. The cross-layer design's ability to correlate information across protocol layers enabled detection of attacks that might evade single-layer monitoring.

Sirajuddin's hybrid approach specifically targeted DoS and sinkhole attacks, demonstrating improved performance in recognizing and eliminating malicious nodes to avoid these threats [9]. Ying's CUSUM-based mechanism focused on selective forwarding attacks and eavesdropping, using statistical methods to identify malicious forwarding behavior [19]. Ngai et al. developed an algorithm specifically targeting sinkhole attacks, demonstrating that focused approaches can achieve effective detection of particular attack types with reasonably low overhead [18].

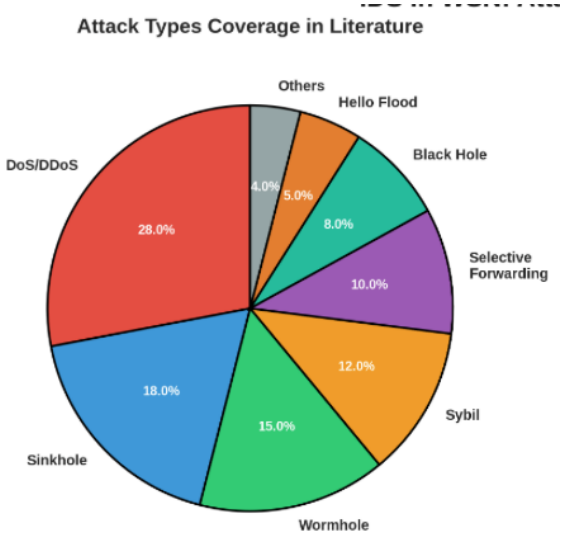

Figure 5: Contribution of different attack types in the literature

Hybrid detection approaches generally provide broader attack coverage than single-methodology systems. Nannan et al.'s GNP-based hybrid system addressed DoS, probe, user-to-root (U2R), and root-to-local (R2L) attacks, though the research noted that anomaly intrusions remained difficult to distinguish [20]. Nancy et al.'s approach claimed capability to detect both known and unknown attack types through integration of fuzzy temporal decision trees with convolutional neural networks [14]. However, the literature reveals that no single approach provides comprehensive coverage of all possible attack types, and detection effectiveness varies significantly across different threat categories.

The challenge of detecting novel or zero-day attacks remains particularly significant. While anomaly-based and hybrid approaches theoretically can detect unknown attacks by identifying deviations from normal behavior, practical implementations often struggle with high false positive rates or missed detections for sophisticated novel attacks [1], [12]. Signature-based components, while highly effective for known threats, fundamentally cannot detect attacks not represented in their signature databases [1], [12]. This limitation underscores

the importance of hybrid approaches and continuous model updating, though the latter presents significant challenges in resource-constrained WSN environments.

6 DISCUSSION

6.1 Trends and Evolution (2019-2024)

The period from 2019 to 2024 has witnessed several significant trends in WSN intrusion detection research and development. First, there has been a clear shift toward hybrid detection methodologies that combine signature-based and anomaly-based techniques to leverage their complementary strengths [9], [12], [20]. This trend reflects growing recognition that neither approach alone provides adequate coverage of the diverse threat landscape facing modern WSNs. Hybrid systems, despite higher resource consumption, offer improved detection of both known and novel attacks while potentially reducing false positive rates through multi-methodology validation.

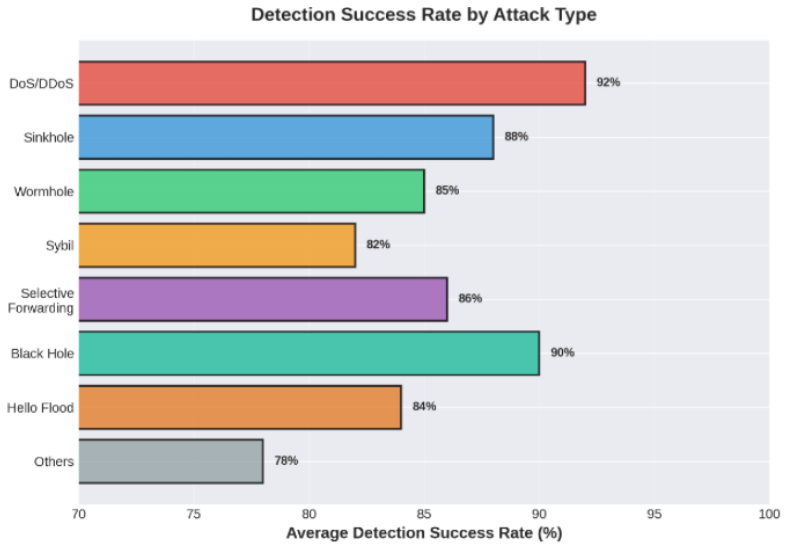

Figure 6: Different type of attacks detection success rate

Second, machine learning and deep learning approaches have gained substantial prominence, with increasing sophistication in algorithm selection, optimization, and adaptation to WSN constraints [5], [9], [14], [27]. The evolution from simple classifiers to ensemble methods, optimized SVMs, and integrated deep learning architectures demonstrates the field's maturation. However, this trend has been accompanied by growing awareness of the challenges in deploying computationally intensive algorithms in resource-constrained environments, leading to research on efficient neural network architectures, accelerated learning algorithms, and hierarchical deployment strategies that concentrate complex processing at resource-rich nodes.

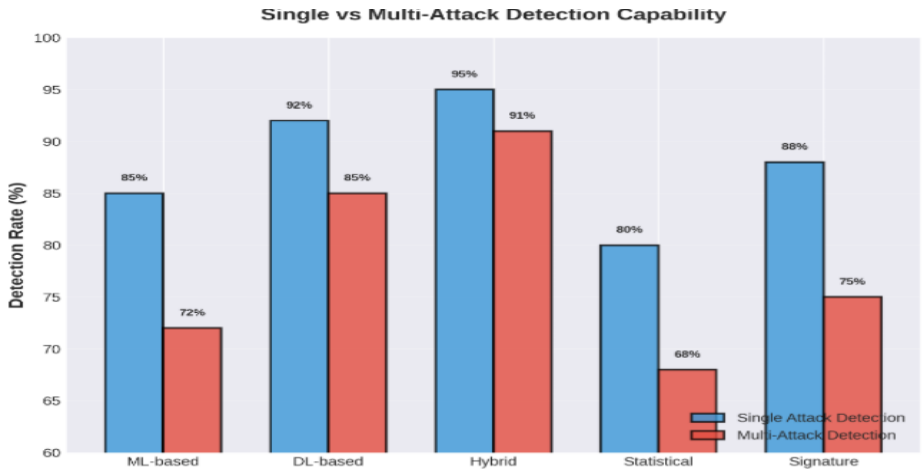

Figure 7: Detection Rate with single and multi-attack detection scenarios

Third, architectural innovations, particularly cross-layer and hierarchical designs, have emerged as critical enablers of effective intrusion detection in WSN environments [4], [5], [8], [16], [24]. The demonstrated performance improvements and energy savings from cross-layer approaches represent significant advances over traditional layered security architectures. Hierarchical designs that distribute detection responsibilities according to node capabilities have become increasingly sophisticated, with multi-level clustering, cooperative detection, and agent-based implementations providing flexible, scalable solutions.

Fourth, there is growing emphasis on energy efficiency and resource optimization as primary design objectives rather than secondary considerations [16], [24], [27]. This trend reflects maturation of the field beyond proof-of-concept demonstrations toward practical deployments where network lifetime and operational sustainability are paramount. Research increasingly reports energy consumption metrics alongside detection performance, and optimization algorithms explicitly consider energy costs in their objective functions [5].

6.2 Trade-offs and Design Considerations

WSN intrusion detection system design involves navigating complex trade-offs among multiple competing objectives. The fundamental tension between detection accuracy and resource consumption pervades all design decisions. Sophisticated algorithms with high detection rates typically require substantial computational resources and energy, potentially reducing network lifetime to unacceptable levels [12]. Conversely, lightweight algorithms that minimize resource consumption may sacrifice detection accuracy or attack coverage, leaving networks vulnerable to sophisticated threats.

The choice between centralized, distributed, and hierarchical architectures involves trade-offs among single points of failure, detection latency, energy distribution, and scalability [1], [2], [4]. Centralized approaches concentrate energy consumption at base stations but introduce communication overhead and potential bottlenecks. Distributed approaches enable rapid detection and avoid single points of failure but impose energy burdens

on resource-constrained sensor nodes. Hierarchical architectures attempt to balance these considerations but introduce complexity in cluster formation, cluster head selection, and load balancing.

The selection of detection methodology—signature-based, anomaly-based, or hybrid—involves trade-offs between detection of known versus unknown attacks, false positive rates, and computational requirements [1], [12]. Signature-based approaches offer high accuracy for known threats with relatively low computational overhead but cannot detect novel attacks. Anomaly-based approaches provide theoretical capability to detect unknown threats but often suffer from higher false positive rates and require substantial training data and computational resources for model construction. Hybrid approaches attempt to capture the benefits of both but at the cost of increased complexity and resource consumption.

Feature selection and dimensionality reduction represent critical design considerations, particularly for machine learning approaches. High-dimensional feature spaces can improve detection accuracy by capturing subtle attack patterns but increase computational complexity, memory requirements, and risk of overfitting [14], [15]. Dynamic feature selection approaches that adapt to changing network conditions offer potential advantages but introduce additional computational overhead and complexity.

6.3 Limitations and Challenges

Despite significant advances, WSN intrusion detection faces persistent limitations and challenges. Resource constraints remain the fundamental limiting factor, restricting the sophistication of algorithms that can be deployed on sensor nodes and necessitating careful optimization of all detection mechanisms [1], [2], [12]. The tension between security requirements and resource limitations has not been fully resolved, and many proposed approaches remain impractical for severely resource-constrained deployments.

False positive rates, while improved in recent research, continue to present challenges. Even systems achieving 1-2% false positive rates may generate unacceptable numbers of false alarms in large-scale networks with thousands of nodes and high traffic volumes [5], [10]. False alarms consume network resources for investigation and response, potentially desensitize operators to genuine threats, and may trigger unnecessary defensive actions that disrupt legitimate network operations. Reducing false positives without sacrificing detection of genuine attacks remains an ongoing challenge.

Detection of sophisticated, coordinated, and adaptive attacks presents significant difficulties. Many proposed IDS have been evaluated primarily against relatively simple attack scenarios or standard datasets that may not reflect the complexity of real-world threats [5], [20]. Adaptive adversaries who understand IDS mechanisms can potentially craft attacks that evade detection by mimicking normal behavior patterns or exploiting detection algorithm weaknesses. Coordinated attacks involving multiple compromised nodes acting in concert pose particular challenges for detection systems designed primarily for individual malicious node identification.

The cold start problem—effective operation before sufficient training data has been collected to build accurate models—affects anomaly-based and machine learning approaches [1]. WSN deployments often cannot afford extended training periods during which the network remains vulnerable. Transfer learning and pre-trained models offer potential solutions but face challenges in adapting to specific deployment environments with unique traffic patterns and application characteristics.

Scalability to very large networks with thousands or tens of thousands of nodes remains inadequately addressed. Many proposed approaches have been evaluated in simulations or testbeds with relatively small numbers of nodes, and their performance characteristics in massive-scale deployments remain uncertain [8], [19]. Communication overhead for cooperative detection, computational requirements for centralized analysis of network-wide data, and memory requirements for maintaining detection state all scale with network size, potentially becoming prohibitive in very large deployments.

7 FUTURE DIRECTIONS AND RECOMMENDATIONS

Several promising research directions emerge from this comprehensive review. First, federated learning approaches offer potential to address the tension between sophisticated machine learning models and resource constraints by enabling collaborative model training across distributed nodes without centralizing raw data [27]. Federated learning could allow sensor nodes to contribute to model improvement while keeping data local, reducing communication overhead and preserving privacy. However, adapting federated learning to WSN constraints requires addressing challenges in communication efficiency, model aggregation with heterogeneous node capabilities, and robustness against poisoning attacks.

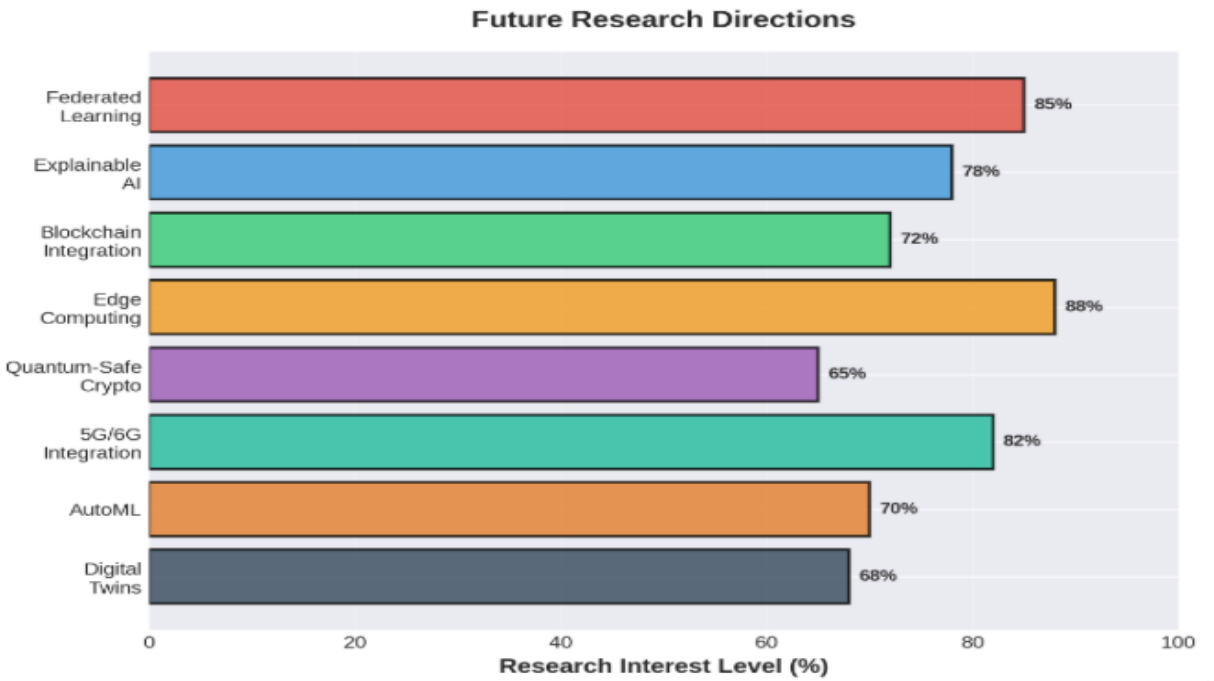

Figure 8: Future Research direction

Second, integration of artificial intelligence techniques beyond traditional machine learning, including reinforcement learning for adaptive defense strategies and explainable AI for interpretable detection decisions, represents promising directions. Reinforcement learning could enable IDS to learn optimal detection and response strategies through interaction with the network environment, adapting to evolving threats and changing network conditions. Explainable AI techniques could address the black-box nature of complex machine learning models, providing operators with understandable rationales for detection decisions and enabling more effective incident response.

Third, development of standardized evaluation frameworks, benchmark datasets, and performance metrics specific to WSN intrusion detection would significantly advance the field. Current research employs diverse evaluation methodologies, datasets, and metrics, making meaningful comparison across approaches difficult [5], [10], [20]. Standardized benchmarks should reflect realistic WSN traffic patterns, diverse attack types including sophisticated coordinated attacks, and appropriate consideration of resource constraints. Performance metrics should encompass not only detection accuracy and false positive rates but also energy consumption, detection latency, scalability, and robustness.

Fourth, investigation of lightweight cryptographic primitives and hardware security modules specifically designed for WSN environments could enable more sophisticated security mechanisms without prohibitive resource consumption. Hardware acceleration of critical security functions, including intrusion detection algorithms, could dramatically improve performance and energy efficiency. Integration of security considerations into sensor node hardware design from the outset, rather than as afterthoughts, represents an important direction for future WSN platforms.

Fifth, research on resilient IDS architectures that maintain effectiveness even when some detection components are compromised or fail would enhance practical deployability. Current approaches often assume that detection infrastructure itself remains secure, but sophisticated adversaries may specifically target IDS components to blind security monitoring. Byzantine fault-tolerant detection algorithms, redundant detection mechanisms, and self-healing architectures could improve resilience against such attacks.

Sixth, exploration of cross-domain learning and transfer learning techniques could address the cold start problem and enable more rapid deployment of effective intrusion detection in new WSN installations. Models trained on data from existing deployments could be adapted to new environments with minimal additional training, accelerating time to effective protection. However, careful attention to domain differences and potential negative transfer is essential.

Finally, integration of intrusion detection with automated response mechanisms, creating complete intrusion prevention systems, represents an important direction. Detection alone is insufficient; networks require automated capabilities to isolate compromised nodes, reconfigure routing to avoid malicious areas, and adapt security policies in response to detected threats. However, automated response introduces risks of disruption from false positives and

potential for adversarial manipulation, requiring careful design of response mechanisms with appropriate safeguards.

8 CONCLUSION

This comprehensive literature review has synthesized current knowledge on intrusion detection systems for wireless sensor networks, analyzing 30 highly relevant publications from the 2019-2024 period. The review reveals a maturing field characterized by increasing sophistication in detection methodologies, growing adoption of machine learning and deep learning approaches, and innovative architectural designs that balance detection effectiveness with resource constraints.

Key findings indicate that hybrid detection approaches combining signature-based and anomaly-based techniques provide superior attack coverage compared to single-methodology systems, though at the cost of increased resource consumption. Machine learning methods, particularly optimized SVMs and ensemble approaches, achieve detection rates of 97-99% with false positive rates below 2% in favorable conditions. Deep learning approaches show promise but require careful optimization for resource-constrained environments. Architectural innovations, especially cross-layer and hierarchical designs, demonstrate substantial improvements in both detection performance and energy efficiency, with some approaches achieving 25-45% energy savings while improving detection rates by 42%.

However, persistent challenges remain. The fundamental tension between detection accuracy and resource consumption has not been fully resolved. False positive rates, while improved, continue to present operational challenges. Detection of sophisticated, adaptive, and coordinated attacks remains difficult. Scalability to very large networks requires further investigation. The cold start problem affects machine learning approaches, and standardized evaluation frameworks are needed to enable meaningful comparison across proposed solutions.

The period from 2019 to 2024 has witnessed significant advances in WSN intrusion detection, with clear trends toward hybrid methodologies, machine learning integration, architectural innovation, and explicit consideration of energy efficiency. Future research directions including federated learning, explainable AI, standardized evaluation frameworks, hardware security integration, resilient architectures, and automated response mechanisms offer promising paths toward more effective, efficient, and practical intrusion detection systems for wireless sensor networks. As WSNs continue to proliferate across critical application domains, effective intrusion detection will remain essential for ensuring security, reliability, and trustworthiness of these increasingly ubiquitous sensing infrastructures.

REFERENCES

[1] Neelankavil et al., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," International Journal of Engineering Research and Technology, 2020.

[2] Sharma et al., "Distributed Intrusion Detection System for Wireless Sensor Networks," IOSR Journal of Computer Engineering, 2013, doi: 10.9790/0661-1416170.

[3] Can et al., "A survey of intrusion detection systems in wireless sensor networks," International Conference on Modeling, Simulation, and Applied Optimization, 2015, doi: 10.1109/ICMSAO.2015.7152200.

[4] Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," International Journal of Network Security & Its Applications, 2011, doi: 10.5121/IJNSA.2011.3511.

[5] El-Said et al., "An optimized collaborative intrusion detection system for wireless sensor networks," Soft Computing, 2020, doi: 10.1007/S00500-020-04695-0.

[6] Vijayan et al., "Advanced Intrusion Detection System for Wireless Sensor Networks," Middle-East Journal of Scientific Research, 2016.

[7] Coppolino et al., "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks," 2013, doi: 10.1109/3PGCIC.2013.43.

[8] Butun et al., "An Intrusion Detection System Based on Multi-Level Clustering for Hierarchical Wireless Sensor Networks," Sensors, 2015, doi: 10.3390/S151128960.

[9] Sirajuddin, "Hybrid intrusion detection method based on improved adaboost and enhanced svm for anomaly detection in wireless sensor networks," International Journal of Advanced Research in Computer Science, 2022, doi: 10.26483/ijarcs.v13i5.6912.

[10] Sharma et al., "Survey of Intrusion Detection Techniques and Architectures in Wireless Sensor Networks," International Journal of Advanced Networking and Applications, 2019, doi: 10.35444/IJANA.2019.10044.

[11] Mubarak et al., "Intrusion Detection: A Probability Model for 3D Heterogeneous WSN," International Journal of Computer Applications, 2010, doi: 10.5120/1125-1475.

[12] Kasar et al., "A Survey on Intrusion Detection Techniques in Wireless Sensor Networks," 2015.

[13] Yu et al., "A framework of machine learning based intrusion detection for wireless sensor networks," Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, doi: 10.1109/SUTC.2008.39.

[14] Nancy et al., "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," IET Communications, 2020, doi: 10.1049/IET-COM.2019.0172.

[15] Gaurkar et al., "A Survey of Encroachment Disclosure in Wireless Sensor Networks," 2013.

[16] Boubiche et al., "Cross layer intrusion detection system for wireless sensor network," International Journal of Network Security & Its Applications, 2012, doi: 10.5121/IJNSA.2012.4203.

[17] Maleh et al., "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," arXiv: Cryptography and Security, 2014.

[18] Ngai et al., "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," Computer Communications, 2007, doi: 10.1016/J.COMCOM.2007.04.025.

[19] Ying, "CUSUM-based intrusion detection mechanism for wireless sensor networks," Journal of Electrical and Computer Engineering, 2014, doi: 10.1155/2014/245938.

[20] Nannan et al., "Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks," Journal of Sensors, 2018, doi: 10.1155/2018/5948146.

[21] Khanum et al., "Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks," 2012.

[22] Ananthakumar et al., "Intrusion Detection System in Wireless Sensor Networks: A Review," International Journal of Advanced Computer Science and Applications, 2015, doi: 10.14569/IJACSA.2015.061218.

[23] Krontiris, "Towards intrusion detection in wireless sensor networks."

[24] Alharthi et al., "XLID: Cross-Layer Intrusion Detection System for Wireless Sensor Networks," Indian Journal of Science and Technology, 2019, doi: 10.17485/IJST/2019/V12I3/140767.

[25] Krontiris et al., "Cooperative Intrusion Detection in Wireless Sensor Networks," International Conference on Embedded Wireless Systems and Networks, 2009, doi: 10.1007/978-3-642-00224-3_17.

[26] Farooqi et al., "Intrusion Detection Systems for Wireless Sensor Networks: A Survey," International Conference on Future Generation Communication and Networking, 2009, doi: 10.1007/978-3-642-10844-0_29.

[27] Batiha et al., "Design and analysis of efficient neural intrusion detection for wireless sensor networks," Concurrency and Computation: Practice and Experience, 2021, doi: 10.1002/CPE.6152.

[28] Jadidoleslamy, "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, 2011, doi: 10.4236/IJCNS.2011.48064.