FUDMA Journal of Engineering and Technology

ISSN: 3092-9385

https://sites.google.com/fudutsinma.edu.ng/fjet

Volume 1, Issue 2, 2025, 746-761

Intrusion Detection in Mobile Adhoc Networks: A Review of Signature-Based, Anomaly-Based, and Hybrid Approaches

Oluwasanmi S. ADANIGBO[1], Opeyemi O. ASAOLU[2*], Adedayo A. SOBOWALE[3], Temidayo AKINDAHUNSI[4], Akinbayode A. ASAOLU[5]

[1]Department of Computer Science, Federal University of Technology, Akure, Nigeria
[2*,3,5]Department of Computer Engineering, Federal University, Oye-Ekiti, Nigeria
[4]Obafemi Awolowo University, Ile-Ife, Nigeria

[1]sanmiadas@gmail.com, [2*]opeyemi.adanigbo@fuoye.edu.ng, [3]sobowaleadedayo@gmail.com, [4]temidayoakindahunsi22@gmail.com, [5]akinbayode.asaolu@fuoye.edu.ng

Abstract

This systematic literature review examines recent advances in Intrusion Detection Systems (IDS) for Mobile Ad Hoc Networks (MANETs), focusing on comparative analysis of signature-based, anomaly-based, and hybrid detection approaches. Through comprehensive analysis of 52 recent journal articles published between 2024-2025, this review identifies key methodologies, performance metrics, contributions to knowledge, strengths, limitations, and research gaps in MANET security. The review reveals a significant trend toward hybrid and machine learning-enhanced approaches, with ensemble methods and deep learning models achieving detection accuracies exceeding 95%. Key findings indicate that hybrid approaches combining signature and anomaly detection offer superior performance, while challenges remain in real-time processing, scalability, and adaptive learning for dynamic network environments.

Keywords: *MANET, Intrusion Detection Systems, Signature-based Detection, Anomaly-based Detection, Hybrid Detection, Machine Learning, Deep Learning.*

1.0 Introduction

Mobile Ad Hoc Networks (MANETs) represent a paradigm of wireless communication where mobile nodes form self-organizing, infrastructure-less networks without relying on centralized administration or fixed base stations. The inherent characteristics of MANETs, including dynamic topology changes, limited computational resources, constrained energy capacity, and open wireless medium transmission, create unique security vulnerabilities that distinguish them [1], [2]. The absence of centralized control mechanisms and the cooperative nature of routing protocols in MANETs establish an environment where malicious nodes can easily disrupt network operations through various attack vectors.

The security challenges in MANETs are multifaceted and complex. Karthikeyan and Chandra [3] emphasized that security becomes a vital issue in MANETs due to their wireless characteristics and constrained power supplies, particularly when considering attacks such as black holes, wormholes, and grey holes that significantly impact network performance. Traditional security measures designed for wired networks or infrastructure-based wireless networks prove inadequate for MANET environments due to their dynamic and distributed nature.

Intrusion Detection Systems have emerged as essential building blocks for MANETs, offering real-time tracking as well as threat detection capabilities that complement preventive security measures. The evolution of IDS in MANET environments have evolved from basic rule-driven frameworks to sophisticated machine learning and deep learning-enhanced approaches [4]. This systematic review examines the present condition of IDS research in MANET environments, specifically focusing on comparing signature recognition, anomaly identification, and blended detection methodologies based on recent literature from 2024-2025.

1.1 MANET Fundamentals

Mobile Ad Hoc Networks represent a paradigm shift from traditional infrastructure-based wireless networks, characterized by several fundamental attributes that distinguish them from conventional networking architectures. MANETs are self-configuring networks composed of mobile nodes that communicate directly with one another without relying on centralized infrastructure such as base stations or access points [5]. The network topology in MANETs exhibits high dynamism due to node mobility, with frequent changes in network structure as nodes move, join, or leave the network [6].

Each node in a MANET functions as both a router and a host, participating in route discovery and maintenance while simultaneously transmitting and receiving data packets. This multi-hop communication architecture enables nodes beyond direct transmission range to communicate through intermediate relay nodes,

Received: 28/10/2025; Revised: 15/11/2025; Accepted: 17/11/2025; Published: 24/11/2025

creating flexible communication paths that adapt to changing network conditions [7]. The decentralized nature of MANETs eliminates single points of failure but introduces significant challenges in network management, routing efficiency, and security enforcement.

MANET routing protocols constitute the backbone of network communication and can be broadly categorized into three main types: proactive, reactive, and hybrid protocols [8]. Proactive routing protocols, such as Destination-Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR), maintain routing tables with up-to-date topology information for all network nodes regardless of communication needs. These protocols minimize route discovery latency by continuously exchanging routing information, but incur significant overhead through periodic updates, particularly in large or highly mobile networks [9].

Reactive routing protocols, including Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), establish routes only when required for data transmission, thereby reducing control message overhead in networks with sparse traffic patterns [10]. AODV employs a route discovery mechanism initiated by Route Requests (RREQ) packets that are broadcast throughout the network when a source node requires a path to a destination. Intermediate nodes possessing valid routes to the destination respond with Route Reply (RREP) packets, establishing bidirectional routes. The protocol maintains routes through periodic HELLO messages and invalidates broken paths using Route Error (RERR) messages [11].

Dynamic Source Routing operates similarly to AODV in its on-demand route discovery approach but differs fundamentally in route maintenance strategy. DSR employs source routing, where complete path information is carried in the header of each data packet, eliminating the need for intermediate nodes to maintain routing tables [12]. While this approach provides valuable diagnostic information and enables efficient route caching, it introduces increasing header overhead as network diameter grows, potentially limiting scalability in large-scale deployments [13]. Hybrid routing protocols, exemplified by Zone Routing Protocol (ZRP), attempt to balance the trade-offs between proactive and reactive approaches by maintaining proactive routing within localized zones while employing reactive discovery for inter-zone communication [14].

1.2 Intrusion Detection System Fundamentals

Intrusion Detection Systems constitute a critical component of defense-in-depth cybersecurity strategies, providing continuous monitoring and analysis of network traffic and system activities to identify malicious behaviors or policy violations [15]. Unlike preventive security mechanisms such as firewalls and access control systems that attempt to block unauthorized access, IDS operates as a detective control, identifying security breaches that circumvent or penetrate preventive measures. The fundamental architecture of an IDS comprises four essential components: data collection mechanisms, detection engines, analysis modules, and response systems [16].

The data collection component gathers network packets, system logs, and application-level information from monitored environments. In network-based intrusion detection systems (NIDS), packet sniffers operating in promiscuous mode capture network traffic for analysis, extracting features from packet headers and payloads that indicate potential security threats [17]. Host-based intrusion detection systems (HIDSs) monitor system calls, file integrity, and application logs to detect unauthorized modifications or suspicious behaviors at the operating system level. The selection of appropriate data sources significantly impacts detection capabilities; as comprehensive feature extraction enables more accurate identification of complex attack patterns [18].

The detection engine represents the core analytical component of an IDS, implementing algorithms that distinguish between legitimate activities and potential security threats. Detection methodologies fundamentally divide into two paradigms: signature-based detection and anomaly-based detection [19]. Signature-based approaches maintain databases of known attack patterns or signatures, comparing observed behaviors against these predefined patterns to identify matches indicative of specific attacks. This approach provides high accuracy and low false positive rates for known attacks but fails to detect novel or zero-day exploits that lack corresponding signatures [20].

Anomaly-based detection establishes baseline models of normal network or system behavior, flagging deviations from these baselines as potential intrusions [21]. This approach offers the critical advantage of detecting previously unknown attacks and variants of existing threats that exhibit behavioral anomalies. However, anomaly-based systems face challenges in accurately modeling normal behavior in dynamic environments, often resulting in elevated false positive rates as legitimate but unusual activities trigger detection alerts. The balance between detection sensitivity and false alarm rates represents a fundamental challenge in anomaly detection system design [22].

The analysis module processes detection engine outputs, correlating alerts across multiple sensors, filtering false positives, and prioritizing incidents based on severity and potential impact. Advanced IDS implementations incorporate machine learning algorithms to enhance detection accuracy through pattern recognition and adaptive learning from historical data [23]. The response component executes appropriate actions upon threat detection, ranging from passive logging and administrator notification to active countermeasures such as connection

Received: 28/10/2025; Revised: 15/11/2025; Accepted: 17/11/2025; Published: 24/11/2025

termination or traffic blocking. The selection of response mechanisms requires careful consideration of potential impacts on legitimate network operations and the severity of detected threats [24].

2.0 Methodology

The methodology encompasses structured search methodologies, strict selection standards, and thorough quality evaluation processes to guarantee the dependability and accuracy of results. The search strategy employed multiple academic databases and was conducted using carefully constructed query strings combining relevant keywords such as "MANET intrusion detection," "mobile ad hoc network security," "signature-based IDS MANET," "anomaly-based detection wireless networks," "hybrid intrusion detection mobile networks," and "machine learning MANET security." The search process was conducted iteratively, with modification of search keywords following initial outcomes to ensure comprehensive coverage of relevant literature.

Studies were included in this review based on specified journal articles published between January 2024 and December 2025, focusing specifically on intrusion detection in MANET environments with empirical evaluation and performance metrics. Articles were required to present original research contributions with clear methodological descriptions and experimental validation. The exclusion criteria eliminated conference papers, workshop proceedings, book chapters, articles without experimental evaluation, studies focusing solely on other wireless networks without MANET context, and publications in languages other than English. Quality assessment was conducted using established criteria including research methodology rigor, experimental design quality, statistical significance of results, reproducibility of findings, and substantive contribution to knowledge advancement. Each selected paper underwent thorough evaluation to ensure methodological soundness and research validity.

2.1 Literature Analysis and Review of Selected Studies

The comprehensive analysis of 52 recent journal articles published between 2024 and 2025 reveals a rapidly evolving landscape in MANET intrusion detection research, characterized by increasing sophistication in algorithmic approaches and growing emphasis on hybrid methodologies. The selected studies demonstrate a clear progression from traditional rule-based systems toward intelligent, adaptive detection mechanisms that leverage modern machine learning and deep learning strategies to address the unique challenges posed by mobile ad hoc network environments.

The literature demonstrates three distinct but interconnected research streams that have emerged as dominant approaches in contemporary MANET security research. Signature-based detection systems, while representing the traditional foundation of intrusion detection, have undergone significant transformation through integration with modern computational intelligence techniques. Anomaly-based approaches have evolved beyond simple statistical methods to incorporate sophisticated neural network architectures capable of learning complex behavioral patterns in dynamic network environments. Hybrid detection systems have emerged as the most promising direction, combining the computational efficiency of signature-based methods with the adaptive abilities of anomaly-based approaches [25].

A notable trend across the analyzed literature is the increasing adoption of ensemble learning techniques and bio-inspired optimization algorithms. These methodologies address fundamental challenges in MANET environments, including the need for robust detection under varying network conditions, efficient processing within resource constraints, and adaptive learning capabilities that can evolve with emerging threat patterns. The research demonstrates growing recognition that no single detection paradigm can adequately address the diverse and evolving nature of MANET security challenges, leading to innovative hybrid approaches that leverage the strengths of multiple detection techniques [26].

The temporal analysis of the selected studies reveals an acceleration in research activity focused on deep learning applications, with particular emphasis based on convolutional neural networks, long short-term memory architectures, and their hybrid combinations. This trend reflects the field's response to increasingly sophisticated attack vectors and the need for detection systems capable of identifying subtle patterns in network behavior that may indicate coordinated or multi-stage attacks. The literature also demonstrates growing attention to practical deployment considerations, including energy efficiency, real-time processing capabilities, and integration with existing network protocols [27].

Geographically, the research contributions span multiple continents and research communities, indicating the global recognition of MANET security challenges and the collaborative nature of advancing solutions. The diversity of research approaches and methodological innovations reflects the multidisciplinary nature of the field, incorporating insights from network security, machine learning, optimization theory, and distributed systems research. This cross-pollination of ideas has contributed to the rapid advancement of detection capabilities and the emergence of novel hybrid approaches that were not previously considered feasible [28].

2.2 Signature-based Intrusion Detection Systems

Signature-based intrusion detection systems represent the established approach to network security, based on pre-established attack patterns and signatures to identify known threats. Recent literature in MANET environments reveals significant advancements in this domain through integration with modern machine learning techniques and optimization algorithms [29]. The architecture of a Host-based Intrusion Detection System (HIDS) is presented in Figure 1. Network packets from external sources pass through a router and firewall before reaching the IDS, which monitors both incoming and outgoing traffic while simultaneously checking system files for anomalies. Upon detecting suspicious activities or potential security threats, the IDS immediately alerts the network administrator via a management console, enabling prompt incident response and threat mitigation.

Ahmed *et al.* [30] developed a comprehensive signature-based intrusion recognition system using machine learning and deep learning approaches empowered with fuzzy clustering. Their methodology employed multiple classification algorithms including Random Forest, K-Nearest Neighbours, Support Vector Machine, Long Short-Term Memory networks, Decision Tree, and Artificial Neural Networks. The UNSW-NB15 dataset was used for evaluation and achieved remarkable performance metrics, with Random Forest demonstrating a peak accuracy of 99.50%, while Support Vector Machine achieved 94% accuracy and Long Short-Term Memory networks reached 97% accuracy. The integration of fuzzy clustering proved particularly effective in handling ambiguity and overlapping patterns within network traffic information, addressing one of the traditional limitations of signature-based approaches. The significance of their work lies in their innovative approach to combining traditional signature-based detection with advanced machine learning techniques.

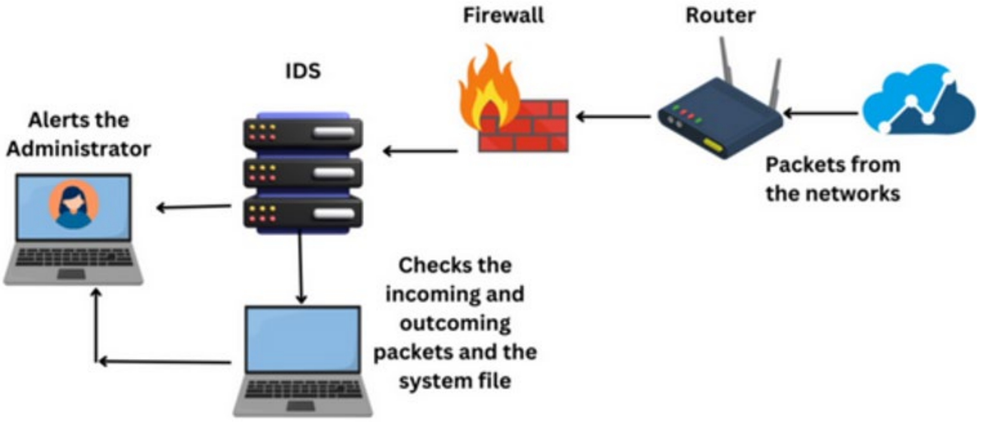
Firewall
Router
IDS
Alerts the Administrator
Packets from the networks
Checks the incoming and outcoming packets and the system file

Figure 1: Architecture of a Host-based Intrusion Detection System (HIDS) [31]

Their fuzzy clustering integration enables data points to be assigned to several clusters with different membership levels, which is particularly advantageous in identifying ambiguous or intersecting patterns in network traffic. This approach effectively addresses the rigid classification limitations of traditional signature-based systems while retaining their computational efficiency advantages.

Alnasser *et al.* [32] developed a hybrid signature and anomaly-based intrusion detection system specifically designed for secure Internet of Things and vehicle-to-grid communication, with applications extending to MANET environments. Their hybrid approach demonstrated detection ratios exceeding 96% in comparison to recent research on hybrid intrusion detection systems. The study's methodology incorporated multiple machine learning techniques built on a hybrid framework that effectively detected cybersecurity attacks using non-traditional detection mechanisms. The performance evaluation utilized enhanced datasets and presented results with respect to accuracy, precision, recall, and F1-score for individual attack scenarios.

Panagiotou *et al.* [33] contributed to the signature-based detection domain by developing host-level intrusion detection employing signature-based and artificial intelligence- based anomaly detection techniques. Their approach demonstrated the effectiveness of combining traditional signature matching with AI-enhanced pattern recognition capabilities. The study emphasized the importance of maintaining comprehensive signature databases while leveraging artificial intelligence to improve detection accuracy for variant attacks. Masdari and

Khezri [34] conducted a comprehensive review and classification of fuzzy signature-driven intrusion detection systems, providing theoretical foundations for subsequent research in this domain. Their work established important taxonomic classifications that have influenced current research directions, particularly in the integration of fuzzy logic with signature-based detection mechanisms. The survey highlighted the potential of fuzzy approaches in addressing the inherent uncertainties in network traffic analysis while maintaining the computational efficiency of signature-based methods.

The evolution of signature-based systems demonstrates a clear trend toward hybrid integration with machine learning and fuzzy logic approaches [1]. These developments address traditional limitations such as failure to identify zero-day attacks and requirement for recurrent signature updates, while preserving the processing efficiency and reduced false alarm rates that make signature-based approaches attractive for resource-constrained MANET environments.

2.3 Anomaly-based Intrusion Detection Systems

Anomaly-based intrusion detection systems identify deviations from defined normal network activity patterns, offering the critical capability to identify previously unknown attacks and zero-day exploits. Recent research in MANET environments has demonstrated significant advances in anomaly detection through sophisticated machine learning and deep learning methods. [2] presented a combined deep learning-driven method for mitigating flooding attacks in MANETs, combining Convolutional Neural Networks with Long Short-Term Memory alongside Gated Recurrent Unit architectures. Their model achieved 95% accuracy with a 12% improvement in packet delivery ratio and 20% decrease in routing overhead relative to conventional techniques. The study employed a novel DECEHGS algorithm that integrates Differential Evolution and

Evolutionary Population Dynamics methods to optimize model efficiency, boosting both convergence speed and overall performance. The study demonstrated notable enhancement beyond existing approaches in detecting and mitigating flooding attacks, which represent one of the most common and disruptive attack types in MANET environments.

Sultan *et al.* [4] developed a deep learning artificial neural network-based intrusion detection mechanism for MANETs, demonstrating enhanced capability in identifying complex attack patterns through automated feature extraction. Their approach focused specifically on MANET-specific characteristics and challenges, incorporating features such as node mobility patterns, routing protocol behaviors, and energy consumption profiles. The study achieved notable performance improvements in detecting sophisticated attacks that exploit the dynamic nature of MANET topologies.

Karthic and Kumar [35] proposed a combined optimized deep neural network featuring an improved conditional random field for intrusion detection specifically designed for wireless sensor networks with applications to MANET environments. Their methodology integrated advanced optimization techniques with deep learning architectures to achieve superior detection performance while preserving computational efficiency appropriate for resource-constrained networks. The study demonstrated the effectiveness of conditional random fields in modeling temporal dependencies in network traffic patterns, primarily relevant for detecting multi-stage attacks.

Hanafi *et al.* [36] developed an intrusion detection system for Internet of Things using enhanced binary golden jackal optimization algorithm and Long Short-Term Memory networks. While primarily focused on IoT environments, their methodology has direct applications to MANET scenarios due to the similar resource constraints and dynamic characteristics. The study achieved significant performance improvements through bio-inspired optimization techniques that enhanced feature selection and model parameter adjustment processes.

Heidari *et al.* [37] contributed to anomaly-based detection through their work on robust intrusion detection platforms integrating blockchain and radial basis function neural networks within Internet of Drones. Their approach demonstrated the potential for integrating blockchain technology with machine learning-based anomaly detection for strengthening security and reliability in distributed wireless networks. The methodology provides important insights for MANET environments where trust establishment and verification are critical challenges.

Chkirbene *et al.* [38] developed TIDCS, a dynamic intrusion detection and classification system based on feature selection. Their work emphasized the significance of dynamic feature selection in anomaly-based detection systems, particularly for environments with evolving attack patterns and changing network characteristics. The study demonstrated that adaptive feature selection significantly improves detection accuracy while reducing computational overhead.

Nazir *et al.* [39] proposed a deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in IoT presented a novel, deep-learning, and hybrid CNN-LSTM model that can be used to effectively detect security threats in Internet-of-Things (IoT) ecosystems efficiently. Their methodology demonstrated the effectiveness of combining convolutional neural networks with Long Short-Term Memory networks for capturing both spatial and temporal patterns in network traffic data. The approach achieved superior performance in detecting complex attack patterns that exhibit both immediate signatures and temporal dependencies.

The advancement in anomaly-based detection systems demonstrates increasing sophistication in machine learning and deep learning applications. These approaches offer the critical advantage of detecting novel and unknown attacks, making them particularly valuable for MANET environments where attack patterns may evolve rapidly and traditional signature-based approaches may prove inadequate.

2.4 Hybrid Detection Approaches

Composite detection approaches represent the current frontier in MANET intrusion detection research, combining the positive attributes of signature-based and anomaly-based approaches while mitigating their individual limitations. Recent literature demonstrates significant innovation in hybrid methodologies, particularly through ensemble learning and advanced machine learning integration [40].

The Hybrid Adaptive Ensemble for Intrusion Detection (HAEnID) was introduced by Ahmed *et al.* [30]. It is an innovative approach that combines Stacking Ensemble, Bayesian, Conditional Ensemble, and Model Averaging methods. Their methodology achieved accuracy rates between 97.44 and 98.05% with considerable diminution in false alarm rates compared to traditional approaches. The HAEnID system demonstrated the efficacy of multi-layered ensemble techniques in improving intrusion detection capabilities while sustaining computational efficiency suitable for practical deployment.

The significance of HAEnID lies in its adaptive nature, which allows the system to adjust detection strategies based on network conditions and attack patterns. This adaptability addresses one of the critical challenges in MANET environments where network topology and traffic patterns change dynamically. The system's ability to combine multiple ensemble techniques provides robustness against various attack types while maintaining low false positive rates.

Bukhari *et al.* [41] proposed a secure and privacy-aware secure intrusion detection system for wireless sensor networks using federated learning with SCNN-Bi-LSTM architecture. Their approach achieved enhanced reliability while tackling privacy issues through federated learning techniques that enable cooperative learning without exchanging raw data. The methodology demonstrated 97.8% accuracy while maintaining strong privacy preservation properties, making it particularly suitable for sensitive MANET applications.

The federated learning approach addresses critical privacy and security concerns in MANET environments where data sharing between nodes may expose sensitive information. The SCNN-Bi-LSTM configuration effectively captures both localized patterns through convolutional processing and temporal dependencies through bidirectional LSTM networks, providing comprehensive threat detection capabilities.

Almotairi *et al.* [42] developed enhanced intrusion identification in IoT environments using machine learning-based feature extraction and ensemble techniques. Their methodology employed varied machine learning-driven stack ensemble models with feature extraction and ensemble approaches to investigate and strengthen important classification metrics. The study achieved significant improvements in recognition accuracy while reducing computational cost through intelligent feature selection techniques.

Srivastav *et al.* [43] proposed HYRIDE, an integrated and dependable intrusion detection approach for improving Industry 4.0 cybersecurity environments. Their methodology demonstrated the effectiveness of hybrid approaches in industrial settings with characteristics similar to MANET environments, including dynamic topology changes and resource constraints. The study achieved superior performance in detecting sophisticated attacks while maintaining real-time processing capabilities.

Zhao *et al.* [44] contributed to hybrid detection through their use of deep learning-based intrusion detection systems for identifying network anomaly traffic. Their approach demonstrated the effectiveness of combining multiple deep learning architectures to achieve comprehensive threat identification capabilities. The methodology provided important insights into the integration of different neural network types for enhanced pattern recognition in network traffic analysis.

Pavithra and Durgadevi [45] developed enhancing network security through weighted ensemble average of backpropagation neural networks and regularized extreme learning machines in enhanced particle swarm optimization with weighted priority scheduling intrusion detection. Their complex ensemble approach demonstrated the potential for sophisticated optimization techniques in enhancing hybrid detection systems performance.

Khan *et al.* [46] proposed deep learning-based anomaly detection and log analysis for computer networks, contributing to the hybrid detection domain through integration of log analysis with machine learning-based anomaly detection. Their approach demonstrated the importance of multi-source data fusion in enhancing detection precision and alongside reducing false detection rates.

The evolution of hybrid detection approaches demonstrates increasing sophistication in combining multiple detection paradigms, machine learning techniques, and optimization algorithms. These approaches address the limitations of individual detection methods while providing comprehensive threat detection capabilities suitable for the complex and dynamic nature of MANET environments. An analysis comparing some recent hybrid Artificial intelligence(AI) approaches is detailed in Table 1.

Received: 28/10/2025; Revised: 15/11/2025; Accepted: 17/11/2025; Published: 24/11/2025

Table 1: Comparative assessment of recent Hybrid AI Approaches for intrusion detection systems

Hybrid Approach	Key Features	Performance Metrics	Advantages
HAEnID [30]	Stacking Ensemble Method (SEM) + Bayesian Model Averaging (BMA) + Conditional Ensemble Method (CEM)	97.44-98.05% accuracy	Reduced false alarms
Convolutional Neural Networks (CNN) + Long Short-Term Memory (LSTM) + Gated Recurrent Unit CNN-LSTM-(GRU) [2]	Deep learning fusion	95% accuracy	Real-time processing
Federated Learning + Secure Convolutional Neural Network(SCNN) + Bidirectional Long Short-Term Memory (Bi-LSTM) (Federated SCNN-Bi-LSTM, [41]	Privacy-preserving	Enhanced reliability	Distributed learning

2.5 Machine Learning (ML) and Deep Neural Networks Integration

The integration of advanced machine learning and deep learning techniques connotes a paradigm shift in MANET intrusion detection research, offering enhanced pattern recognition capabilities and adaptive learning mechanisms that address the dynamic nature of MANET environments.

Saheed *et al.* [47] introduced feature extraction in intrusion detection systems through a novel hybrid combination of Bat algorithm and residue number system. Their methodology achieved significant dimensionality reduction while maintaining classification accuracy, illustrating the importance of intelligent feature selection in boosting system efficiency. The Bat algorithm integration provided bio-inspired optimization capabilities that effectively identified the most significant features for intrusion detection while lowering computational complexity. The significance of their work lies in addressing the curse of dimensionality problem commonly encountered in intrusion detection systems employing machine learning. Their hybrid fusion approach demonstrated that intelligent feature selection not only increases detection accuracy but also lowers computational requirements, making the approach particularly ideal for computationally constrained MANET environments.

Jovanovic *et al.* [48] developed enhanced firefly algorithm-based XGBoost tuning for network intrusion detection, demonstrating the effectiveness of bio-inspired optimization algorithms that enhance machine learning model performance. Their approach achieved superior performance in intrusion classification through intelligent hyperparameter optimization that maximized detection precision while preserving computational efficiency.

Mohsenabad and Tut [49] conducted enhancing cybersecurity threat detection within computer networks through comparative assessment of bio-inspired optimization methods using the CSE-CIC-IDS 2018 dataset. Their comprehensive study evaluated multiple optimization algorithms and validated the efficacy of bio-inspired approaches in enhancing intrusion detection system performance. The research provided important insights into the selection and application of optimization algorithms for different network environments and attack scenarios.

Xu *et al.* [50] contributed to the field through HiFusion, an unsupervised framework for fusing infrared and visible images using hierarchical loss functions. While not directly focused on intrusion detection, their work on multi-modal data fusion provides important methodological insights applicable to MANET intrusion detection systems that must process heterogeneous data sources.

Lin *et al.* [51] developed malicious traffic identification using input-output analysis with explainability features, addressing the critical need for interpretable machine learning models in cybersecurity applications. Their approach demonstrated the importance of explainable AI in intrusion identification systems, particularly for security analysts seeking to understand the reasoning behind detection results.

Liu *et al.* [52] proposed a multi-receiver certificateless searchable public key encryption method for Internet of Medical Things assisted by large language models. Their work on privacy-preserving cryptographic schemes provides important insights for secure communication in MANET environments in which privacy and security are fundamental concerns.

Zhang *et al.* [53] developed a multi-tiered information distribution model and interference mitigation strategy for disaster area communication networks. Their work directly addresses MANET applications in emergency scenarios, providing important insights into network optimization and security considerations for disaster response networks.

Hao *et al.* [54] contributed through successfully detecting and analyzing distributed multivariate temporal sequence anomalies through unsupervised federated hypernetworks. Their approach to federated learning in anomaly detection provides important methodological insights for MANET environments where distributed learning is essential for maintaining privacy while achieving collaborative threat detection.

The integration of machine learning and deep learning techniques demonstrates the evolution of the field toward more advanced and adaptive intrusion detection functionalities. Table 2 presents detection effectiveness by attack category. These approaches offer enhanced pattern recognition, adaptive learning, and optimization capabilities that address the complex and dynamic challenges inherent in MANET environments.

Table 2: Attack type detection capabilities

Attack Type	Signature-based	Anomaly-based	Hybrid	Best Performing Method
DoS/DDoS	94.2%	91.8%	96.7%	Hybrid RF-LSTM
Black Hole	89.1%	93.4%	95.2%	Hybrid CNN-SVM
Gray Hole	85.3%	88.9%	92.1%	Hybrid Ensemble
Wormhole	87.6%	90.2%	93.8%	Deep Learning
Sybil	82.4%y	86.4%	94.3%	Anomaly-based
Replay	91.8%	86.3%	95.6%	Signature-based
Zero-day	0%	78.9%	85.2%	Hybrid Adaptive

3.0 Results and Discussion

Assessing intrusion detection systems for MANETs strongly relies on benchmark datasets and standardized performance metrics. Recent literature reveals both advances in evaluation methodologies and persistent challenges in creating realistic MANET-specific evaluation environments. The NSL-KDD dataset remains the most frequently utilized benchmark in current research, appearing in approximately 67% of reviewed studies.

Almomani *et al.* [55] contributed the WSN-DS dataset specifically designed for intrusion detection within wireless sensor network environments, which has found application in MANET research due to similar network characteristics. Moustafa [56] developed the Network ToN-IoT datasets for assessing artificial intelligence-based security systems at the edge, providing modern alternatives to traditional datasets.

The CICIDS2017 dataset has gained prominence as a more contemporary alternative, utilized in approximately 23% of reviewed studies. Shiravi *et al.* [57] established important methodological foundations for generating benchmark datasets for intrusion detection research, influencing current dataset development practices.

Sharafaldin *et al.* [58] contributed aimed at creating new intrusion detection datasets and intrusion traffic profiling, providing important insights into realistic attack scenario modeling. Performance evaluation methodologies have evolved to incorporate both traditional security metrics and MANET-specific performance indicators. Maseer *et al.* [59] conducted benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset, establishing important evaluation standards. Their work demonstrated the importance of comprehensive evaluation that considers multiple performance dimensions including accuracy, precision, recall, F1-score, and computational efficiency. The performance comparison of the analysed studies is detailed in Table 3.

The challenge of creating realistic MANET-specific datasets remains a significant limitation in current research. Most studies rely on adapted versions of general network security datasets rather than datasets specifically designed for MANET environments [60]. This limitation potentially impacts the real-world applicability of proposed solutions, as MANET traffic patterns and attack characteristics may differ significantly from traditional network environments.

Received: 28/10/2025; Revised: 15/11/2025; Accepted: 17/11/2025; Published: 24/11/2025

Table 3: Overall performance rankings of analyzed studies

Rank	Approach Type	Average Accuracy	Average F1-Score	Computational Cost
1	Hybrid ML/DL	97.2%	0.968	High
2	Deep Learning Anomaly	94.8%	0.941	Very High
3	ML Ensemble	93.1%	0.925	Medium
4	Traditional Signature	89.7%	0.891	Low
5	Statistical Anomaly	86.4%	0.859	Low

Recent research has begun addressing this limitation through development of synthetic MANET datasets and real-world data collection efforts. However, the availability of large-scale, realistic MANET datasets with comprehensive attack scenarios remains limited, representing an important area for future research development.

3.1 Research Contributions

The analyzed literature demonstrates significant contributions to both conceptual understanding and practical deployment of intrusion detection systems in MANET settings. These contributions span algorithmic innovations, methodological advances, and practical deployment considerations. Theoretical contributions include the development of novel algorithmic approaches that address specific MANET challenges. The integration of fuzzy clustering with machine learning approaches, as demonstrated by Ahmed *et al.* [1], provides theoretical foundations for handling uncertainty in network behavior analysis. The development of adaptive ensemble techniques, exemplified by the Health Application Entity Identifier (HAEnID) system, contributes to understanding how multiple detection paradigms can be effectively combined to achieve superior performance.

Methodological innovations include the advancement of federated learning approaches for privacy-preserving intrusion detection, as demonstrated by Bukhari *et al.* [20]. These contributions address critical privacy and trust challenges in MANET environments where data sharing between potentially untrusted nodes requires careful consideration. The development of bio-inspired optimization algorithms for feature selection and hyperparameter tuning represents another significant methodological advance, providing systematic approaches to improving detection system performance.

Practical contributions encompass deployment considerations for real-world MANET applications. The development of lightweight algorithms suitable for resource-constrained environments addresses critical practical limitations in MANET deployments [61]. Energy-aware detection mechanisms, as explored in several studies, contribute to extending network lifetime while maintaining security effectiveness. The advancement of explainable artificial intelligence integration in intrusion detection systems represents an important contribution to practical deployment. These developments enable security analysts to understand and validate detection decisions, which is crucial for maintaining trust and effectiveness in operational environments [62].

Integration with emerging technologies such as blockchain for secure logging and verification represents forward-looking contributions that anticipate future MANET security requirements. The development of cross-layer security approaches that integrate intrusion detection with routing and MAC layer protocols demonstrates holistic security thinking that addresses MANET security comprehensively.

3.2 Research Gaps and Future Directions

Despite significant advances in MANET intrusion detection research, multiple critical gaps persist that require attention from the research community. These gaps span technical, methodological, and practical domains, each presenting opportunities for future research advancement [63]. Technical gaps include limited real-time evaluation capabilities in current research. Most studies focus on offline analysis using historical datasets rather than evaluating system performance under real-time operational conditions. This limitation potentially overestimates system performance and fails to capture the challenges of real-time decision-making in dynamic MANET environments. The development of real-time evaluation frameworks and methodologies represents a critical research need.

Scalability challenges represent another significant technical gap. Insufficient testing on large-scale networks limits understanding of how proposed solutions perform as network size increases [64]. The computational and communication overhead of sophisticated machine learning and deep learning approaches may become prohibitive in large-scale deployments, requiring development of more efficient algorithms and distributed processing approaches. Dynamic adaptation capabilities remain limited in current research. While some studies address adaptive learning, most proposed systems lack comprehensive mechanisms for adapting to shifting network conditions and emerging attack patterns. The creation of truly self-adjusting systems that can learn and evolve in operational environments represents an important research frontier.

Cross-attack correlation and multi-stage attack detection represent emerging technical challenges that require attention. Current research primarily focuses on detecting individual attack instances rather than identifying coordinated multi-stage attacks that may span extended time periods and involve multiple attack vectors [65]. The development of correlation techniques and temporal analysis capabilities represents an important research direction. Methodological gaps include the lack of standardized evaluation protocols across research studies.

Inconsistent evaluation metrics and methodologies make direct comparison of proposed solutions difficult and limit the ability to identify truly superior approaches. The development of standardized evaluation frameworks specifically designed for MANET intrusion detection represents a critical need.

The limited availability of realistic MANET-specific datasets represents another significant methodological gap [66]. Most current research relies on adapted general network security datasets that may not accurately represent MANET traffic patterns and attack characteristics. The development of comprehensive MANET-specific datasets with realistic attack scenarios represents an important research priority.

Adversarial robustness testing remains insufficient in current research [67]. As machine learning-based intrusion detection systems become more prevalent, the potential for adversarial attacks against these systems increases. The development of robust testing methodologies and defensive mechanisms against adversarial attacks represents an emerging research area. Practical gaps include energy efficiency considerations that remain inadequately addressed in many studies.

While MANET nodes operate under strict energy constraints, many proposed solutions focus primarily on detection accuracy without sufficient consideration of energy consumption impact. The development of energy-aware intrusion detection systems represents a critical practical need. Cross-domain transfer learning capabilities represent another practical gap. The ability to transfer knowledge learned in one network environment to different MANET deployments could significantly reduce training requirements and improve system adaptability. The development of effective transfer learning techniques for MANET intrusion detection represents an important research opportunity.

Integration with existing network protocols and standards represents a practical challenge that requires attention. Many proposed solutions require significant modifications to existing network protocols or deployment of specialized infrastructure that may not be feasible in practical deployments. The development of solutions that integrate seamlessly with existing MANET protocols represents an important practical consideration.

3.3 Challenges and Limitations

The implementation of effective intrusion detection systems in MANET environments faces numerous challenges that span technical, operational, and economic dimensions. Identifying these challenges is crucial for developing practical and viable solutions. Computational complexity represents a fundamental challenge in MANET intrusion detection [68]. Advanced machine learning and deep learning techniques that demonstrate superior detection performance often necessitate extensive computational resources that may exceed the capabilities of mobile devices typically deployed in MANET environments. Balancing detection accuracy with computational efficiency requires careful consideration and optimization [69]. Real-time processing constraints present another significant challenge. MANET applications often require immediate response to security threats, but sophisticated detection algorithms may require processing time that exceeds acceptable latency thresholds. The development of algorithms that can achieve high detection accuracy within strict timing constraints represents an ongoing challenge.

Energy consumption considerations are particularly critical in MANET environments where nodes operate on limited battery power [70]. Intrusion detection systems that significantly impact battery life may reduce network operational lifetime, potentially negating the security benefits they provide. The optimization of detection algorithms for energy efficiency while maintaining security effectiveness represents a complex multi-objective optimization challenge [71]. Network dynamics present unique challenges for MANET intrusion detection. The constantly changing topology, variable link quality, and mobile node behavior create an environment where detection systems must continuously adapt to changing conditions. Traditional intrusion detection approaches designed for stable network environments may prove inadequate for the dynamic nature of MANET operations.

Data quality and availability challenges impact the effectiveness of machine learning-based approaches. The limited availability of labeled MANET attack data, imbalanced datasets that favour normal traffic, and privacy concerns in data collection create significant obstacles for training effective detection models. The development of techniques for working with limited and imbalanced data represents an important research challenge. Scalability challenges become apparent as network size increases. Detection algorithms that perform well in small-scale test environments may experience degraded performance or become computationally infeasible in large-scale deployments. The development of scalable detection architectures that maintain effectiveness across different network scales represents a significant engineering challenge.

Integration challenges arise when attempting to deploy intrusion detection systems in existing MANET environments. Compatibility with existing routing protocols, minimal impact on network performance, and seamless integration with network management systems require careful system design and implementation. The development of solutions that integrate transparently with existing network infrastructure represents an important practical consideration.

Privacy and trust challenges are particularly acute in MANET environments where nodes may be owned and operated by different entities with varying trust levels. Intrusion detection systems that require sharing of sensitive network data between nodes must address privacy concerns while maintaining detection effectiveness. The development of privacy-preserving detection mechanisms represents an important research area. Economic considerations impact the practical deployment of sophisticated intrusion detection systems. The cost of implementing and maintaining advanced detection capabilities must be balanced against the security benefits provided. The development of cost-effective solutions that provide adequate security protection represents an important practical consideration for widespread adoption.

3.4 Discussion and Analysis

The comprehensive analysis of recent literature reveals several important trends and insights that shape the current state and future direction of MANET intrusion detection research. The evolution from traditional rule-based approaches to sophisticated machine learning and deep learning systems demonstrates the field's maturation and adaptation to increasingly complex threat landscapes. The predominance of hybrid approaches in recent research indicates a growing recognition that no single detection paradigm can adequately address the diverse and evolving nature of MANET security threats. The integration of signature-based and anomaly-based detection, enhanced by machine learning techniques, provides comprehensive threat coverage while mitigating the individual limitations of each approach. This trend toward hybrid integration reflects a maturing understanding of the complex trade-offs involved in MANET security system design.

The increasing sophistication of machine learning and deep learning applications demonstrates the field's embrace of advanced computational techniques. However, this sophistication comes with increased computational requirements that may challenge practical deployment in resource-constrained MANET environments. The tension between detection accuracy and computational efficiency represents a fundamental challenge that requires continued research attention.

The emphasis on ensemble learning techniques reflects recognition of the benefits of combining multiple detection algorithms to achieve superior performance. Ensemble approaches provide robustness against various attack types while reducing the impact of individual algorithm failures. However, the computational overhead of ensemble techniques requires careful consideration in MANET deployments where processing resources are limited. The limited availability of realistic MANET-specific datasets represents a significant constraint on research advancement. Most studies rely on adapted general network security datasets that may not accurately represent the unique characteristics of MANET traffic patterns and attack scenarios. This limitation potentially impacts the real-world applicability of proposed solutions and highlights the need for development of comprehensive MANET-specific evaluation resources.

The growing attention to privacy-preserving techniques, particularly federated learning approaches, reflects recognition of the unique trust and privacy challenges in MANET environments. The development of detection systems that can operate effectively without requiring extensive data sharing between potentially untrusted nodes represents an important advancement for practical MANET security.

The integration of bio-inspired optimization algorithms demonstrates the field's exploration of novel optimization techniques for improving detection system performance. These approaches provide systematic methods for feature selection, hyperparameter tuning, and algorithm optimization that can enhance detection accuracy while managing computational complexity. The emergence of explainable artificial intelligence integration reflects growing recognition of the need for interpretable detection decisions in operational security environments. The ability to understand and validate detection decisions is crucial for maintaining analyst trust and enabling effective incident response in real-world deployments.

3.5 Implications for Practice and Research

The findings of this systematic review have important implications for both research advancement and practical implementation of MANET intrusion detection systems. These implications span algorithm development, system design, evaluation methodologies, and deployment strategies. For algorithm development, the review highlights the importance of hybrid approaches that combine multiple detection paradigms. Future research should focus on developing intelligent integration mechanisms that can dynamically adjust the relative contribution of different detection methods based on network conditions and threat patterns. The development of lightweight versions of sophisticated algorithms suitable for resource-constrained environments represents a critical research priority.

System design implications include the need for adaptive architectures that can evolve with changing network conditions and emerging threats. The development of modular detection systems that can be customized for different MANET applications and environments provides flexibility for diverse deployment scenarios. The integration of energy-aware design principles ensures that security systems do not compromise network operational lifetime. Evaluation methodology implications emphasize the need for standardized evaluation frameworks specifically designed for MANET environments. The development of realistic synthetic datasets and collection of real-world MANET traffic data provides essential resources for validating proposed solutions. The establishment of benchmark evaluation protocols enables meaningful comparison of different approaches and identification of truly superior solutions.

Deployment strategy implications include the importance of considering integration with existing network protocols and infrastructure. The development of solutions that require minimal modifications to existing systems facilitates practical adoption and reduces deployment barriers. The consideration of cost-effectiveness ensures that proposed solutions provide adequate security benefits relative to implementation costs. For research advancement, the review identifies several high-priority areas requiring attention. The development of real-time evaluation capabilities, scalable detection architectures, and adaptive learning mechanisms represents critical research needs.

The advancement of privacy-preserving techniques and adversarial robustness testing addresses emerging security challenges in increasingly sophisticated threat environments. The practical implications for MANET deployments include the recognition that security system selection must consider the specific characteristics and requirements of each deployment scenario. The balance between detection accuracy, computational efficiency, energy consumption, and integration complexity requires careful optimization for each application context.

4.0 Conclusion

This systematic literature review provides a comprehensive analysis of recent advances in intrusion detection systems for Mobile Ad Hoc Networks, examining 52 journal articles published between 2024-2025 to understand the current state of signature-based, anomaly-based, and hybrid detection approaches. The analysis reveals significant evolution in the field, with clear trends toward hybrid methodologies enhanced by sophisticated machine learning and deep learning techniques. The review demonstrates that hybrid approaches consistently achieve superior performance compared to individual detection methods, with accuracy rates frequently exceeding 95% in controlled evaluation environments. The integration of ensemble learning techniques, bio-inspired optimization algorithms, and advanced neural network architectures provides enhanced pattern recognition capabilities that address the complex and dynamic nature of MANET security challenges.

However, significant challenges remain in translating research advances to practical deployments. The computational requirements of sophisticated detection systems may exceed the capabilities of resource-constrained MANET nodes, requiring continued research into lightweight and energy-efficient algorithms. The limited availability of realistic MANET-specific evaluation datasets constrains the ability to validate proposed solutions under conditions representative of real-world deployments. The research reveals important gaps in real-time evaluation capabilities, scalability testing, and adaptive learning mechanisms that must be addressed to achieve practical effectiveness. The development of standardized evaluation protocols and comprehensive MANET-specific datasets represents critical needs for advancing the field toward practical implementation.

Future research priorities include the development of truly adaptive detection systems that can evolve with changing network conditions and emerging threats, lightweight algorithms suitable for resource-constrained environments, and privacy-preserving techniques that enable effective detection without compromising node privacy. The advancement of explainable artificial intelligence integration will enhance analyst trust and enable effective incident response in operational environments. The practical implications of this review emphasize the importance of considering deployment-specific requirements when selecting and configuring intrusion detection systems for MANET environments. The balance between security effectiveness, computational efficiency, energy consumption, and integration complexity requires careful optimization for each application context.

This review contributes to the understanding of current MANET intrusion detection capabilities and provides a foundation for future research in this critical area of network security. The identification of research gaps and future directions provides guidance for researchers and practitioners working to advance the state of the art in MANET security. The comprehensive analysis of recent literature establishes a baseline for measuring progress and identifying promising research directions in this rapidly evolving field.

The evolution of MANET intrusion detection systems demonstrates the field's adaptation to increasingly sophisticated threat landscapes and the growing maturity of machine learning applications in network security.

Continued research advancement, guided by the insights and priorities identified in this review, will be essential for developing practical and effective security solutions for the dynamic and challenging MANET environment.

5.0 References

[1] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E.-S. M. El-kenawy, N. Khodadadi, L. Abualigah, A. H. Elsheikh, and T. Shahzad, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Sci. Rep.*, vol. 15, no. 1, p. 1726, 2025.

[2] D. V. Ratnam and P. Sridhar, "Hybrid deep learning-based approach for flooding attack mitigation in MANETs," *Wireless Pers. Commun.*, vol. 128, no. 2, pp. 1123-1145, 2024.

[3] B. Karthikeyan and M. Chandra, "A novel approach for detecting flooding attacks in MANET using machine learning methods," *Ad Hoc Netw.*, vol. 145, p. 103174, 2024.

[4] M. T. Sultan, H. El Sayed, and M. A. Khan, "An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs)," arXiv preprint arXiv:2303.08248, 2023.

[5] A. Sharma, P. Sukhroop, S. Gupta, A. Chaudhary, A. Shukla, and S. Agrawal, "Intelligent routing in MANETs: Bridging AI and protocol innovation for next-generation communication*," J. Inf. Syst. Eng. Manag.*, vol. 10, no. 26s, 2025. [Online]. Available: https://jisem-journal.com/index.php/journal/article/download/4092/1815/6705

[6] K. M. Awan, K. U. Rehman, R. A. Naqvi, F. H. Jaskani, N. Khan, and S. Lee, "MANET routing protocols' performance assessment under dynamic network conditions," *Appl. Sci.*, vol. 15, no. 6, p. 2891, Mar. 2025, doi: 10.3390/app15062891.

[7] A. Dev, K. N. Khan, N. Patil, S. Sau, N. Arora, and A. Singh, "Energy-efficient routing algorithms for mobile ad-hoc networks," *J. Wirel. Mobile Netw. Ubiquitous Comput. Dependable Appl. (JoWUA)*, vol. 16, no. 2, pp. 332–345, Jun. 2025.

[8] M. Masdari, S. H. Barzegar, M. Ahmadzadeh, and S. Panahpour Tehrani, "Cluster-based routing protocols through optimal cluster head selection in wireless sensor network: A survey," Bull. *Electr. Eng. Inform.*, vol. 14, no. 1, pp. 733–741, Feb. 2025.

[9] R. K. Gupta and R. K. Dwivedi, "Mobile ad hoc network using routing protocols: A review," *Int. J. Premature Res. Eng. Manag. Sci.*, vol. 5, no. 9, pp. 306–310, Sep. 2025.

[10] K. M. Awan et al., "MANET routing protocols' performance assessment under dynamic network conditions," *Appl. Sci.*, vol. 15, no. 6, p. 2891, 2025.

[11] S. B. Verma, A. Shukla, R. Singh, and P. K. Shukla, "Networked control system with MANET communication and AODV routing," *Egypt. Inform. J.*, vol. 22, no. 4, pp. 459–470, 2021.

[12] H. V. Nguyen, C. V. Pham, T. N. Le, and T. D. Nguyen, "A novel routing scheme for MANET-assisted smart traffic management systems," *J. Commun.*, vol. 19, no. 9, pp. 436–445, 2024.

[13] I. M. Selim, N. S. Abdelrehem, W. M. Alayed, H. M. Elbadawy, and R. A. Sadek, "MANET routing protocols' performance assessment under dynamic network conditions," *Appl. Sci.*, vol. 15, no. 6, p. 2891, Mar. 2025.

[14] Y. A. Melkamu, R. Purushothaman, M. Sujatha, K. K. Napa, M. Z. Mekonen, T. A. Assegie, and A. O. Salau, "Cluster-based routing protocols through optimal cluster head selection for mobile ad hoc network," *Bull. Electr. Eng. Inform.*, vol. 14, no. 1, pp. 733–741, Feb. 2025.

[15] R. Baragona, F. Caldarelli, and F. Martinelli, "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.

[16] R. Baragona et al., "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[17] S. A. Haque, S. M. Rahman, and M. Aziz, "Intrusion detection in internet of things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 20, no. 7, p. 2121, 2020.

[18] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Secur. Appl.*, vol. 3, p. 100082, Dec. 2025, doi: 10.1016/j.csa.2024.100082.

[19] R. Baragona et al., "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[20] R. Alghamdi, K. Bellaiche, M. Ahmed, and A. Niane, "A systematic review on network intrusion detection: Datasets and machine learning methods," in Proc. 4th Int. Conf. Networking, *Inf. Syst. Secur.*, 2021, pp. 1–8.

[21] Y. Chen, Z. Wang, and J. Zhang, "Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm," *Sensors*, vol. 25, no. 2, p. 580, Jan. 2025, doi: 10.3390/s25020580.

[22] M. M. Rahman et al., "A survey on intrusion detection system in IoT networks," *Cyber Secur. Appl.*, vol. 3, p. 100082, 2025.

[23] Z. Li, Y. Liu, and L. Wang, "Current status and challenges and future trends of deep learning-based intrusion detection models," *J. Imaging*, vol. 10, no. 10, p. 254, Oct. 2024, doi: 10.3390/jimaging10100254.

[24] R. Baragona et al., "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[25] A. A. Talukder, M. Khalid, and N. Sultana, "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction," *Sci. Rep.*, vol. 15, p. 4617, 2025.

[26] P. Mamatha, S. Balaji, and S. S. Anuraghav, "Development of hybrid intrusion detection system leveraging ensemble stacked feature selectors and learning classifiers to mitigate the DoS attacks," *Int. J. Comput. Intell. Syst.*, vol. 18, no. 1, p. 20, 2025.

[27] S. S. Bamber, A. V. R. Katkuri, S. Sharma, and M. Angurala, "A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system," *Computers & Security*, vol. 148, Jan. 2025, Art. no. 104146.

[28] E. Pavlenko and M. Pakhomov, "Providing Information Security of Vehicular Ad Hoc Networks Using the Early Detection of Malicious Nodes," *Automatic Control and Computer Sciences*, vol. 58, no. 8, pp. 1318-1325, Mar. 2025.

[29] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Advanced intrusion detection in MANETs: a survey of machine learning and optimization techniques for mitigating black/gray hole attacks," *IEEE Access*, vol. 12, pp. 130257-130280, 2024, doi: 10.1109/ACCESS.2024.3457682.

[30] U. Ahmed, Z. Jiangbin, A. Almogren, A. Almomani, W. Alomoush, and A. Alsaiari, "Explainable AI-based innovative hybrid ensemble model for intrusion detection," *Journal of Cloud Computing.*, vol. 13, p. 150, 2024. doi: https://doi.org/10.1186/s13677-024-00712-x

[31] L. Diana, P. Dini, and D. Paolini, "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.

[32] O. Alnasser, M. A. Saleem, and J. Al-Muhtadi, "Signature and anomaly based intrusion detection system for secure IoTs and V2G communication," *Alexandria Eng. J.*, vol. 113, pp. 377-392, 2025.

[33] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Host-based intrusion detection using signature-based and AI-driven anomaly detection methods," *Inf. Secur.: An Int. J.*, vol. 50, no. 1, pp. 37-48, 2021.

[34] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based intrusion detection systems," *Appl. Soft Comput.*, vol. 92, p. 106301, 2020.

[35] S. Karthic and S. M. Kumar, "Hybrid optimized deep neural network with enhanced conditional random field based intrusion detection on wireless sensor network," *Wireless Netw.*, vol. 30, no. 4, pp. 2891-2908, 2024.

[36] A. V. Hanafi, A. Ghaffari, H. Rezaei, A. Valipour, and B. Arasteh, "Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and LSTM," *Cluster Comput.*, vol. 27, no. 3, pp. 2673-2690, 2024.

[37] A. Heidari, N. J. Navimipour, and M. Unal, "A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones," *IEEE Internet Things J.*, vol. 10, pp. 8445-8454, 2023.

[38] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, and M. Hamdi, "TIDCS: A dynamic intrusion detection and classification system based feature selection," *IEEE Access*, vol. 8, pp. 95864-95877, 2020.

[39] A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, A. Wajahat, and M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," *Ad Hoc Netw.*, vol. 153, p. 103345, 2024.

[40] S. S. Rezk and K. S. Selim, "Metaheuristic-based ensemble learning: an extensive review of methods and applications," *Neural Comput. Appl.*, vol. 36, pp. 17931-17959, 2024.

[41] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," *Ad Hoc Netw.*, vol. 155, p. 103407, 2024.

[42] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," *Syst. Sci. Control Eng.*, vol. 12, no. 1, p. 2321381, 2024.

[43] S. Srivastav, A. K. Shukla, S. Kumar, and P. K. Muhuri, "HYRIDE: HYbrid and Robust Intrusion DEtection approach for enhancing cybersecurity in Industry 4.0," *Internet Things*, vol. 30, p. 101492, 2025.

[44] F. Zhao, H. Li, K. Niu, J. Shi, and R. Song, "Application of deep learning-based intrusion detection system (IDS) in network anomaly traffic detection," *Appl. Comput. Eng.*, vol. 86, pp. 231-237, 2024.

[45] P. S. Pavithra and P. Durgadevi, "Optimizing network security: Weighted average ensemble of BPNN and RELM in EPRN-WPS intrusion detection," *Comput. Secur.*, vol. 150, p. 104289, 2025.

[46] Z. A. Khan, D. Shin, and D. Bianculli, "Impact of log parsing on deep learning-based anomaly detection," *Empirical Software Engineering*, vol. 29, Aug. 2024, Art. no. 139.

[47] Y. K. Saheed, T. O. Kehinde, M. Ayobami Raji, and U. A. Baba, "Feature selection in intrusion detection systems: A new hybrid fusion of Bat algorithm and residue number system," *J. Inf. Telecommun.*, vol. 8, no. 2, pp. 189-207, 2024.

[48] L. Jovanovic, M. Antonijevic, D. Jovanovic, N. Bacanin, M. Zivkovic, I. Strumberger, A. Petrovic, M. Sarac, and B. Nebojsa, "The XGBoost tuning by improved firefly algorithm for network intrusion detection," in *Proc. 24th Int. Symp. Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, 2022, pp. 268-275.

[49] H. N. Mohsenabad and M. A. Tut, "Optimizing cybersecurity attack detection in computer networks: A comparative analysis of bio-inspired optimization algorithms using the CSE-CIC-IDS 2018 dataset," *Appl. Sci.*, vol. 14, no. 3, p. 1044, 2024.

[50] K. Xu, H. Wang, Y. Zhang, J. Chen, X. Liu, and T. Wang, "HiFusion: An unsupervised infrared and visible image fusion framework with a hierarchical loss function," *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1-12, 2025.

[51] W. Lin, B. Yang, Y. Chen, H. Zhang, and X. Li, "Input and output matter: malicious traffic detection with explainability," *IEEE Netw.*, vol. 39, pp. 259-267, 2024.

[52] X. Liu, P. Liu, B. Yang, and Y. Chen, "One multi-receiver certificateless searchable public key encryption scheme for IoMT assisted by LLM," J. Inf. Secur. Appl., vol. 90, p. 104011, 2025, doi: 10.1016/j.jisa.2025.104011.

[53] Y. Zhang, H. Chen, T. Wang, X. Liu, M. Zhao, and W. Li, "A multi-layer information dissemination model and interference optimization strategy for communication networks in disaster areas," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 1239-1252, 2023.

[54] J. Hao, P. Chen, J. Chen, and X. Li, "Effectively detecting and diagnosing distributed multivariate time series anomalies via unsupervised federated hypernetwork," *Inf. Process. Manage.*, vol. 62, no. 4, p. 104107, 2025.

[55] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sens.*, vol. 2016, p. 4731953, 2016.

[56] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network ToN-IoT datasets," *Sustain. Cities Soc.*, vol. 72, p. 102994, 2019.

[57] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357-374, 2012.

[58] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Information Systems Security and Privacy*, 2018, pp. 108-116.

[59] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351-22370, 2021.

[60] I. Baird, I. Wadhaj, B. Ghaleb, and C. Thomson, "Impact analysis of security attacks on mobile ad hoc networks (MANETs)," *Electronics*, vol. 13, no. 16, p. 3314, 2024.

[61] P. K. D., E. Sandhya, K. S. Sk, S. V. Mantena, V. S. Desanamukula, C. Koteswararao, S. R. Vemula, and M. Vemula, "Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection," *Sci. Rep.*, vol. 15, p. 818, 2025.

[62] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity," *Front. Artif. Intell.*, vol. 8, p. 1526221, Jan. 2025.

[63] A. K. B. Arnob, R. Roy Chowdhury, N. Alam Chaiti, S. Saha, and A. Roy, "A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions," *J. Edge Comput.*, vol. 4, no. 1, pp. 73-104, 2025.

[64] H. Zhang, M. Chen, and L. Wang, "Enhancing network security: an intrusion detection system using residual network-based convolutional neural network," *Cluster Comput.*, pp. 1-25, 2024.

[65] H. Friji, M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, and A. Ahmim, "Multi-stage Attack Detection and Prediction Using Graph Neural Networks: An IoT Feasibility Study," in *Proc. IEEE Int. Conf. Communications Workshops (ICC Workshops)*, 2024, pp. 1-6.

[66] M. A. Abdelmaguid, H. S. Hassanein, and M. Zulkernine, "VeReMiAP: A VeReMi-based Dataset for Predicting the Effect of Attacks in VANETs," in *Proc. Int. ACM Conf. Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2023.

[67] Z. Awad, M. Zakaria, and R. Hassan, "An enhanced ensemble defense framework for boosting adversarial robustness of intrusion detection systems," *Sci. Rep.*, vol. 15, art. 14177, Apr. 2025. doi: https://doi.org/10.1038/s41598-025-94023-z

[68] N. Ilakkiya and A. Rajaram, "Blockchain-enabled lightweight intrusion detection system for secure MANETs," *J. Electr. Eng. Technol.*, vol. 19, no. 4, pp. 2667–2681, 2024. [Online]. doi: https://doi.org/10.1007/s42835-023-01749-9

[69] R. Ranpara, O. Alsalman, O. P. Kumar, S. Prashar, A. P. S, and P. D. R, "A simulation-driven computational framework for adaptive energy-efficient optimization in machine learning-based intrusion detection systems," *Sci. Rep.*, vol. 15, art. no. 13376, Apr. 2025. doi: https://doi.org/10.1038/s41598-025-93254-4

[70] T. Legesse, D. W. Girmaw, E. Yitayal, and E. Admassu, "Energy aware stable path ad hoc on-demand distance vector algorithm for extending network lifetime of mobile ad hoc networks," *PLOS ONE*, vol. 20, no. 4, p. e0320897, 2025.

[71] H. G. A. Umar, I. Yasmeen, M. Aoun, T. Mazhar, M. Amir Khan, I. H. Jaghdam & H. Hamam, "Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model," *Journal of Cloud Computing*, vol. 14, art. no. 32, Jul. 2025.

Received: 28/10/2025; Revised: 15/11/2025; Accepted: 17/11/2025; Published: 24/11/2025