Future Technology
Open Access Journal
ISSN 2832-0379

May 2026| Volume 05 | Issue 02 | Pages 59-70

Journal homepage: https://fupubco.com/futech

https://doi.org/10.55670/fpll.futech.5.2.7

Future Publishing LLC

Review

A descriptive systematic review of contemporary MANET security research: themes, design structures, and reporting rigor

Augustina Dede Agor[1], Prince Silas Kwesi Oberko[1], Stephen Kofi Dotse[1], Benjamin Tei Partey[2], David Aboagye-Darko[1], Emmanuel Junior Tapany[3]

[1]Department of Information Technology Studies, University of Professional Studies, P. O. Box LG 149, Accra, Ghana
[2]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Private Mail Bag, University Post Office, Kumasi, Ghana
[3]Department of Information Technology, Wisconsin International University College, P. O. Box LG 751, Legon, Accra, Ghana

ARTICLE INFO

Article history:
Received 29 July 2025
Received in revised form
10 November 2025
Accepted 15 January 2026

Keywords:
Mobile ad hoc networks (MANETs), Systematic literature review, MANET security, Trust-based security, Threat modeling, Detection logic

*Corresponding author
Email address:
augustinadede.agor@upsamail.edu.gh

DOI: 10.55670/fpll.futech.5.2.7

ABSTRACT

Mobile Ad hoc Networks remain vulnerable to a wide range of security threats, yet existing MANET security reviews provide fragmented insight into how recent studies frame security problems, model threats, and report design choices. This descriptive systematic review follows PRISMA guidelines and examines MANET security studies published between January and August 2025. A total of 51 studies were analyzed using a structured coding process covering security themes, attack types, defense techniques, threat modeling assumptions, detection logic, and reporting completeness. The results show convergence around a limited set of recurring attack models and reusable defense patterns. Both machine learning and deep learning, along with detection-oriented, trust-based, and optimization techniques, appear across multiple security themes rather than being confined to a single problem framing. However, threat specification, detection target definition, and trust design reporting are often incomplete or inconsistent, which limits reproducibility and cross-study comparison. Evaluation orientation, including performance metrics and experimental validation practices, is identified as an important direction for future work.

1. Introduction

Artificial Mobile Ad hoc Networks (MANETs) enable peer-to-peer, multi-hop communication without fixed infrastructure or centralized administration. This flexibility supports networking in mobility-heavy and infrastructure-disrupted settings, but it weakens conventional security boundaries. The open wireless medium, rapid topology change, and reliance on cooperative operation create conditions where compromised or malicious nodes can interfere with communication while blending into normal network behavior [1]. MANET security concerns extend beyond any single protocol layer or one class of defenses. Studies address threats that target routing control, packet forwarding, identity and reputation, and service availability. Attacks such as blackhole and wormhole remain prominent because they exploit protocol assumptions and can degrade connectivity with limited external visibility [2,3]. Still, attack labels are not self-explanatory. The same-named attack can be modeled with different behaviors, attacker capabilities, and observables. That variation changes what a proposed defense is actually intended to detect or prevent [4,5]. The defense landscape is equally diverse. MANET security research spans cryptographic protection and authentication, intrusion and anomaly detection, trust management, and integrated approaches that combine multiple mechanisms within one architecture [6]. Trust-centered security is often motivated by decentralization because trust converts observed or reported behavior into decision logic that can influence cooperation, control, isolation, or routing preference [7]. Detection-centered designs also remain necessary because purely preventive controls can be bypassed when insiders participate in routing and forwarding processes [8]. As hybrid designs become more common, synthesis becomes harder when studies do not state threat assumptions, malicious behaviors, and detection targets with consistent technical clarity. This review is therefore framed around what recent MANET security studies explicitly report at the security-design level. The synthesis emphasizes how studies describe attacks and adversary assumptions, how they define detection logic and evidence, and how trust is specified when it is used as a security decision construct. More broadly, MANET research continues to develop adaptive, multi-factor decision logic for protocol design, including energy-aware routing variants that are often later extended to security-aware or trust-aware [9–11]. By consolidating how security is articulated across studies and defense families, this review clarifies where the literature is precise versus underspecified and supports more consistent, verifiable, and technically comparable MANET security research.

1.1 MANET security

Figure 1 presents the major attacks that occur at the different layers of a MANET. These attacks arise because MANETs operate in open, decentralized environments in which nodes cannot rely on fixed protection boundaries [12]. At the application layer, adversaries may corrupt data or insert malicious code, including viruses and worms [13]. Some nodes may also deny their actions, making accountability difficult [14]. These threats reduce data integrity and weaken application-level trust.

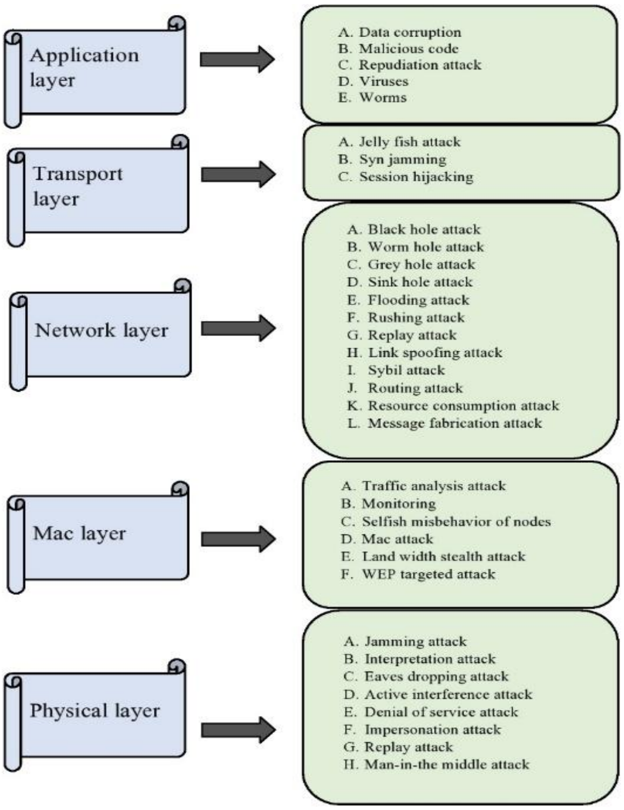

Figure 1. Attacks at the various layers of a MANET [21]

At the transport layer, attackers target end-to-end communication. Jellyfish attacks delay, reorder, or drop packets. SYN-based disruption affects the setup of connections [14]. Session hijacking occurs when an attacker intercepts a session and spoofs the identity of a communicating node. Attackers may also disrupt reception by monitoring the wireless medium to identify the frequency used by the destination and then transmitting on that frequency to block legitimate signals. These threats disturb transport reliability. The network layer remains the most targeted layer. Attacks such as black hole, grey hole, sinkhole, and wormhole mislead routing protocols by advertising false paths. Flooding attacks generate excessive control packets [15]. Rushing attacks suppress legitimate route replies [16]. Replay attacks reuse captured routing information. Sybil attacks use multiple fake identities. Message fabrication and routing table poisoning can alter or create false routing entries [17]. Resource-consumption attacks drain node energy by forcing unnecessary transmissions [18]. These activities compromise routing accuracy and packet delivery.

At the MAC layer, attackers disrupt medium access and forwarding coordination. Traffic-analysis attacks expose communication patterns [19]. Selfish behaviour reduces cooperation among nodes. MAC-focused interference affects fair access to the channel. Bandwidth-stealth behaviour covertly occupies channel resources. Weaknesses in WEP can be exploited to bypass confidentiality [14]. Nodes may also be monitored by verifying and auditing packet transactions and other activities to infer behavior and expose operational details. These threats weaken shared-medium efficiency. The physical layer is exposed to direct manipulation of wireless signals. Jamming and active interference prevent legitimate transmissions [12,14]. Eavesdropping captures radio signals without detection [20]. Impersonation misleads nearby nodes by altering identity information [15]. Replay attacks at this layer reuse previously captured signals. Man-in-the-middle attackers may also intercept and monitor communication between two nodes, impersonating either endpoint to manipulate the exchange. These threats weaken availability and confidentiality at the lowest communication layer.

1.2 Objectives

- To classify MANET security studies into dominant security themes and attack types based on their stated focus.
- To analyze patterns of technique-use and integration across the identified security themes.
- To examine how threats are modeled and how detection logic is specified within the reviewed studies.
- To assess the rigor and completeness of reported security and trust design elements.

1.3 Methodology

This study adopts a descriptive systematic literature review design to examine how MANET security research conceptualizes threats, specifies detection logic, and documents defense mechanisms. The review analyzes thematic organization, technique-use patterns, threat modeling practices, and reporting rigor, without engaging in performance comparison.

The literature search was conducted in 2025 using Google Scholar as a discovery tool to ensure broad and unbiased coverage across publishers. Google Scholar was used strictly for record identification. All included articles were subsequently retrieved in full from their original publisher platforms, and the publisher of each study was recorded explicitly in the dataset. The final corpus spans multiple publishers, including Elsevier, IEEE, Springer Nature, John Wiley & Sons, and several smaller academic presses. Figure 2 presents the distribution of studies by publisher platform.

Studies were included if they focused explicitly on MANET security, proposed or analyzed a security mechanism, and were published as peer-reviewed full-text articles. Only studies providing sufficient technical detail to support structured extraction were retained. Records were excluded if they were duplicates, outside the MANET context, non-security focused, or unavailable in full text. Implementation was defined as a security mechanism validated through simulation, experimentation, or measurable analytical verification. Conceptual proposals without implementation or validation were excluded.

After duplicate removal, 270 records were screened at the title and abstract level. Screening was performed independently by two reviewers using the predefined eligibility criteria. Disagreements were resolved through discussion before full-text assessment. Inter-rater reliability was assessed using Cohen's kappa on the screened set. Out of 270 records, 265 decisions were concordant, and 5 were discordant, yielding an observed agreement of 98.15% and a Cohen's κ of 0.9425, indicating near-perfect agreement. Following screening, 51 full-text articles were assessed for eligibility and included in the final review. The selection process is summarized using a PRISMA flow diagram shown in Figure 3.

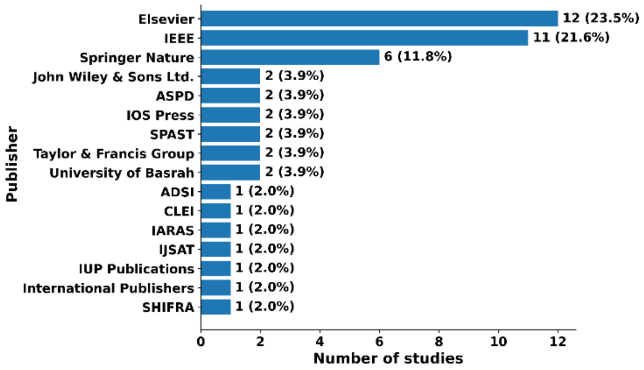

Figure 2. Publisher platform distribution of included MANET security studies (N = 51)

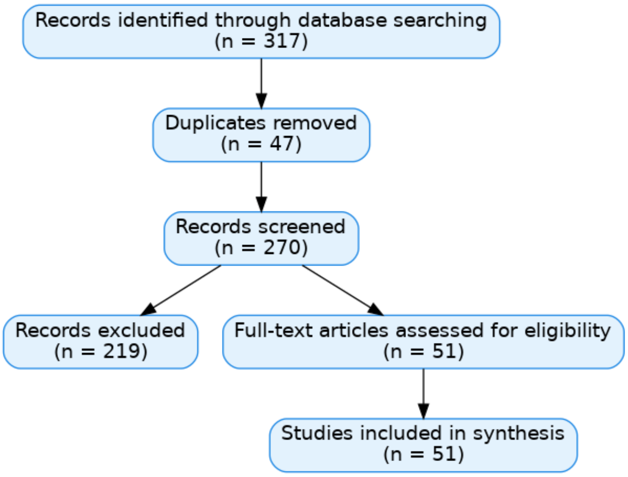
Records identified through database searching
(n = 317)
Duplicates removed
(n = 47)
Records screened
(n = 270)
Records excluded
(n = 219)
Full-text articles assessed for eligibility
(n = 51)
Studies included in synthesis
(n = 51)

Figure 3. PRISMA flow diagram of study identification and selection

A structured extraction template was applied uniformly to all included studies. The template captured publication metadata, security themes, defense techniques, modeled attack types, detection targets, adversary assumptions, and reporting characteristics. Because individual studies frequently address multiple security aspects, multi-label coding was permitted where appropriate.

Data synthesis was conducted using descriptive quantitative techniques. Frequency distributions, co-occurrence matrices, and reporting-depth indices were computed to reveal dominant patterns and gaps in the literature. For threat modeling and trust-based studies, composite depth indices were derived by assigning one point for each explicitly reported design component. This approach provides a transparent measure of reporting completeness while remaining consistent with the review's descriptive scope.

2. Results

2.1 Objective 1: Taxonomy and classification

Across the reviewed MANET security studies (N = 51), the literature was first classified according to the primary security theme that each study explicitly emphasized. Table 1 reports the resulting taxonomy, grouping articles into eight dominant security themes and showing the number of studies associated with each theme. The distribution indicates substantial variation in thematic focus across the dataset, with some themes represented by many studies and others appearing only once or twice. In parallel, attack-type coverage was extracted from the same studies and summarized separately, with the frequency of addressed attacks reported in Figure 4 to complement the thematic classification.

Table 1. Articles grouped by primary theme

Primary theme	Study	Frequency
Artificial Intelligence and Machine Learning for MANET Security	[22-32]	11
Authentication, Key Management, and Access Control Schemes	[33,34]	2
Blackhole, Wormhole, and Other Specific Attack Mitigations	[35-39]	5
Blockchain and Cryptographic Frameworks for MANET Security	[40-42]	3
Energy-Aware and Resource-Constrained Security Models	[43]	1
Integrated and Infrastructure-Oriented Security Architectures	[44-46]	3
Intrusion Detection and Anomaly Detection Systems (IDS/ADS)	[47-61]	15
Trust-Based and Hybrid Metaheuristic Security Models	[62-72]	11

2.2 Objective 2: Structural synthesis of security approaches

Across the 51 studies, technique–attack associations concentrate on a small set of frequently modeled attacks. Blackhole attacks show the strongest alignment with multiple technique families, including trust-based approaches in 12 studies, Intrusion Detection Systems (IDS) and ADS (Anomaly Dection Systems) in 11 studies, and metaheuristic optimization in 10 studies. Wormhole and DoS or DDoS attacks also exhibit repeated co-occurrence with learning-based and detection-oriented techniques, particularly IDS and ADS in 9 studies and deep learning in 8 studies. Less frequent attacks, including Sybil, flooding, eavesdropping, and man-in-the-middle, appear with fewer and more narrowly applied technique categories. This distribution is illustrated in Figure 5.

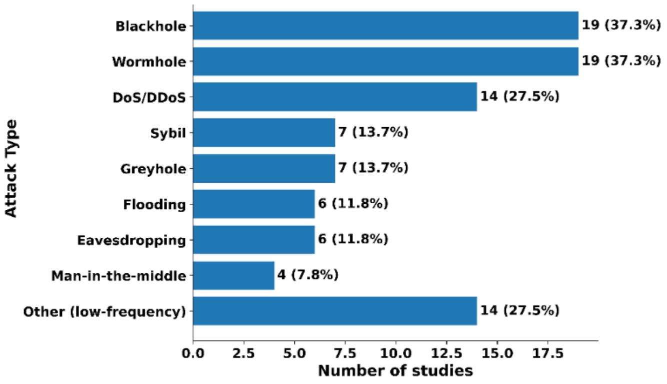

Figure 4. Attack types addressed in MANET security studies (N = 51). Bars show study counts and percentages; studies may include multiple attack types

Figure 6 summarizes technique–theme co-occurrence by counting how often each defense technique family appears in studies addressing each dominant security theme. The highest concentrations occur in the most populated themes, particularly Artificial Intelligence and Machine Learning for MANET Security and Intrusion Detection and Anomaly Detection Systems. Deep learning appears 18 times in Artificial Intelligence and Machine Learning studies, IDS/ADS appears 19 times in detection-centered studies, and metaheuristic optimization appears 16 times in AI-driven security work. Trust-based methods and metaheuristic optimization also recur across several themes, reflecting their use in routing-centric, detection-centric, and hybrid security models. Cell values represent co-occurrence counts, since studies may address multiple themes and apply more than one technique family.

Across the coded corpus, security solutions are rarely built as single-mechanism designs. Instead, studies repeatedly combine technique families into integrated pipelines. The co-occurrence structure suggests that detection systems, learning-oriented methods (i.e., machine learning and deep learning), trust mechanisms, and metaheuristic optimization function as interoperable building blocks rather than standalone answers.

The learning-oriented methods frequently co-occur with IDS/ADS components, reflecting a design logic that emphasizes observable behavior and classification-based decision support. Metaheuristic optimization connects broadly across the network, which supports its role as a coordination or tuning layer that can be embedded within different defense configurations. Figure 7, therefore, points to a literature organized around reusable technique combinations, not one-to-one mappings between a threat label and a single defense.

2.3 Objective 3: Threat modeling and detection logic

As shown in Figure 8, adversary capability is most often modeled as a simplified or non-adaptive attacker. The highest behavior counts under this capability are forwarding abuse through packet dropping or selective dropping (14 studies), flooding or resource exhaustion (7), routing misinformation or spoofing (7), and tunneling or relaying, such as wormhole attacks (6). Adaptive attackers are explicitly considered less often and are mainly paired with forwarding abuse (5 studies), flooding or resource exhaustion (3), and identity manipulation, including Sybil or impersonation (3). Insider and passive attackers are rare, appearing mostly with forwarding abuse, routing misinformation, tunneling or relaying, and passive eavesdropping, each reported in two studies.

As shown in Figure 9, detection targets most often focus on node-level behavior such as forwarding or trust (14/51, 27.5%). Routing-level behavior or control messages appear in 10/51 studies (19.6%), and traffic or IDS-level anomaly targets also appear in 10/51 (19.6%). A large share of studies do not state a codable detection target (17/51, 33.3%). This shows that many papers discuss attacks without clearly defining what the detector monitors.

As illustrated in Figure 10, among trust-based studies (n = 25), the most common evidence is packet forwarding or delivery behavior (15/25, 60.0%). Energy reliability is next (10/25, 40.0%), followed by trust score formulation choices and behavior or anomaly evidence (7/25 each, 28.0%). Reporting or consistency evidence appears in 6/25 studies (24.0%). Four studies (4/25, 16.0%) are classified as trust-based but do not specify the trust metric.

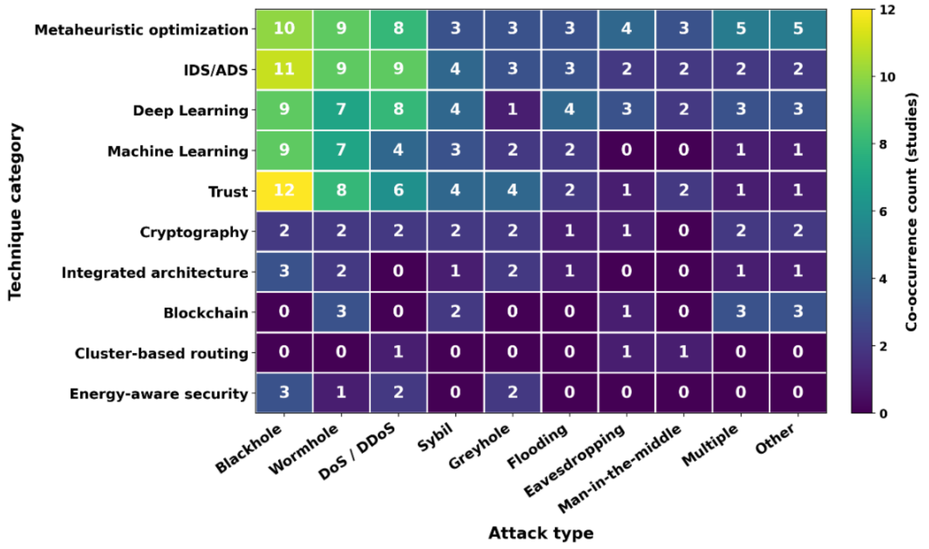

Figure 5. Technique × attack co-occurrence heatmap (Top 10 × Top 10; N = 51). Cell values are study counts for each technique–attack pairing.

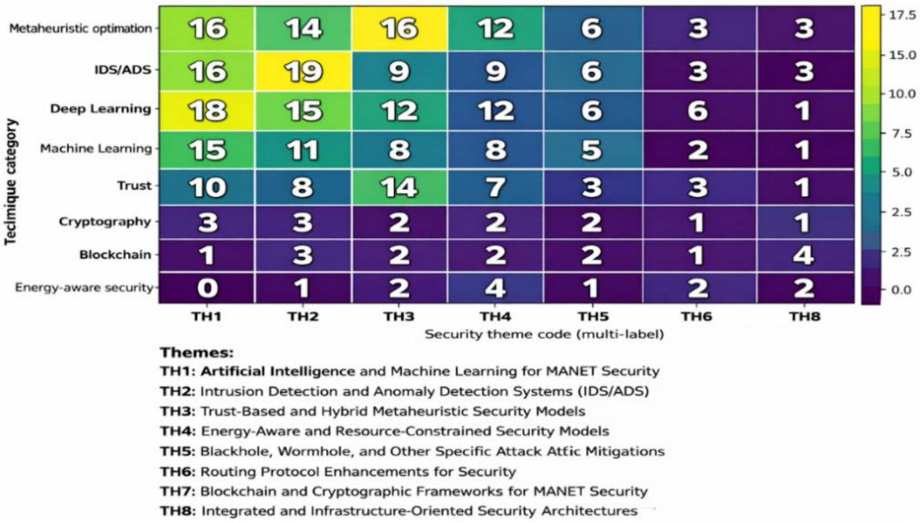

Figure 6. Technique × theme co-occurrence heatmap (Top techniques × Top themes; N = 51). Cell values are study counts; themes and techniques are multi-label.

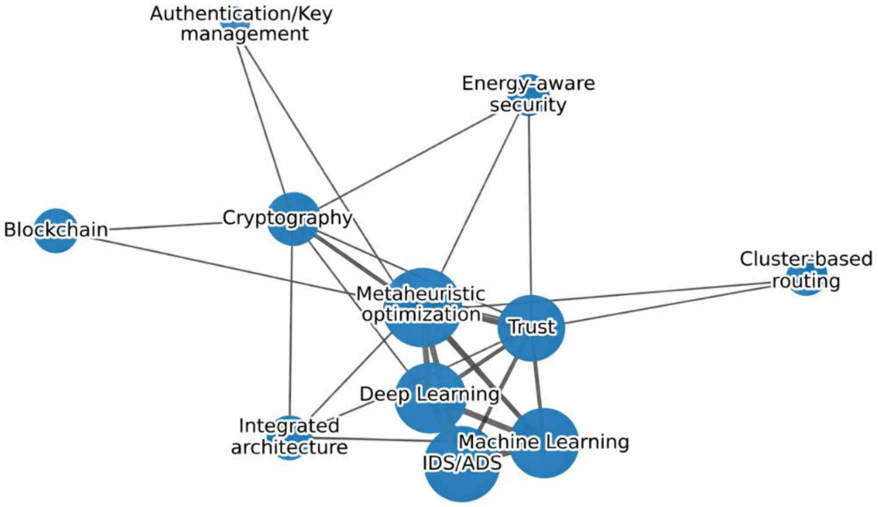

Figure 7. Technique-pair co-occurrence network (N = 51). Edges indicate technique pairs observed in the same study; node size reflects frequency.

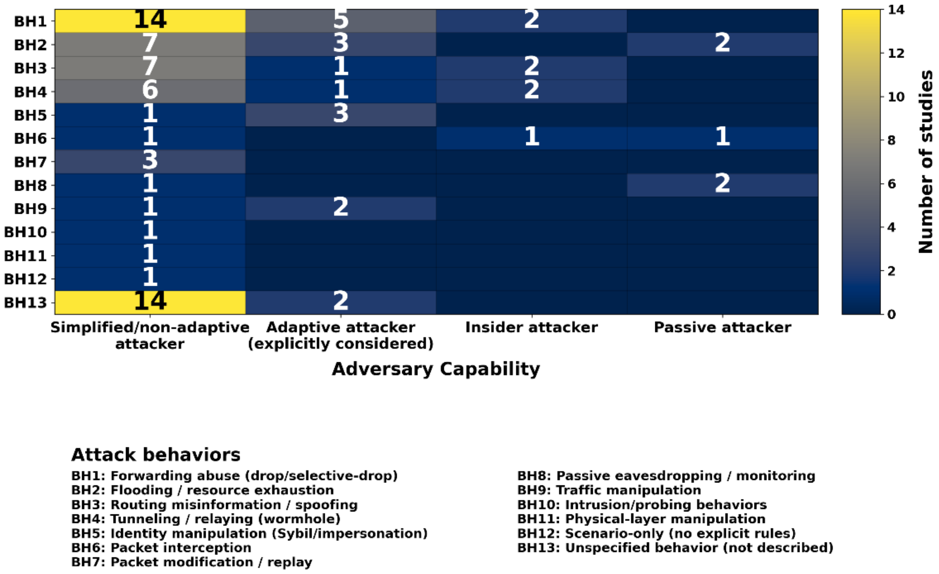

Figure 8. Attack behavior × adversary capability heatmap (N = 51). Cell values are study counts; "Unspecified behavior" indicates capability was stated but behavior rules were not codable.

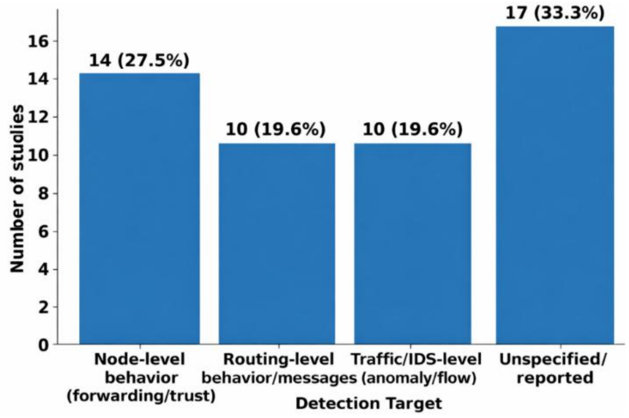

Figure 9. Detection target distribution (N = 51). Bars show study counts and percentages; "Unspecified/Not reported" indicates the detection target was not codable.

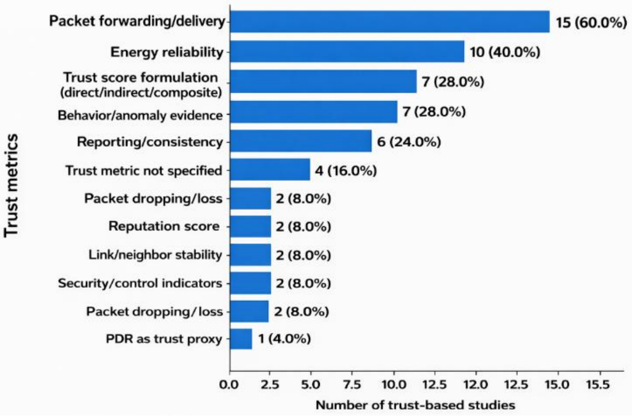

Figure 10. Trust metrics used for detection in trust-based studies (n = 25). Bars show counts and percentages; studies may report multiple metrics.

2.4 Objective 4: Rigor and Completeness of Security Reporting

Figure 11 summarizes threat-model completeness using a five-component depth index across the reviewed studies (N = 51). The mean score is 3.24, and the median is 3, showing that partial threat models are common. Nearly half of the studies report four or more components (25/51, 49.0%), while only 9/51 (17.6%) report all five. Fifteen studies report two or fewer components (15/51, 29.4%), which signals ongoing gaps in basic threat-model specification.

Figure 12 shows that threat-model reporting clusters into repeated component bundles rather than a single standard. The most common bundle includes attack type, attack behavior, adversary capability, and detection target, but omits % malicious nodes, appearing in 12/51 studies (23.5%). Full five-component reporting occurs in 9/51 studies (17.6%). The least included element is % malicious nodes, which helps explain why many studies score below the maximum depth in Figure 11.

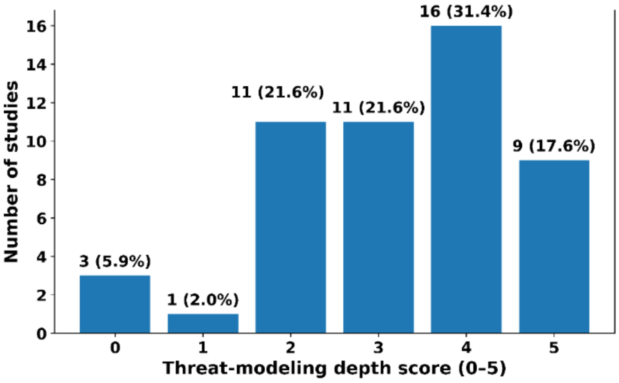

Figure 11. Threat-modeling depth index (N = 51). One point is assigned for each reported component: attack type, attack behavior, adversary capability, detection target, and % malicious nodes. Bars show counts and percentages.

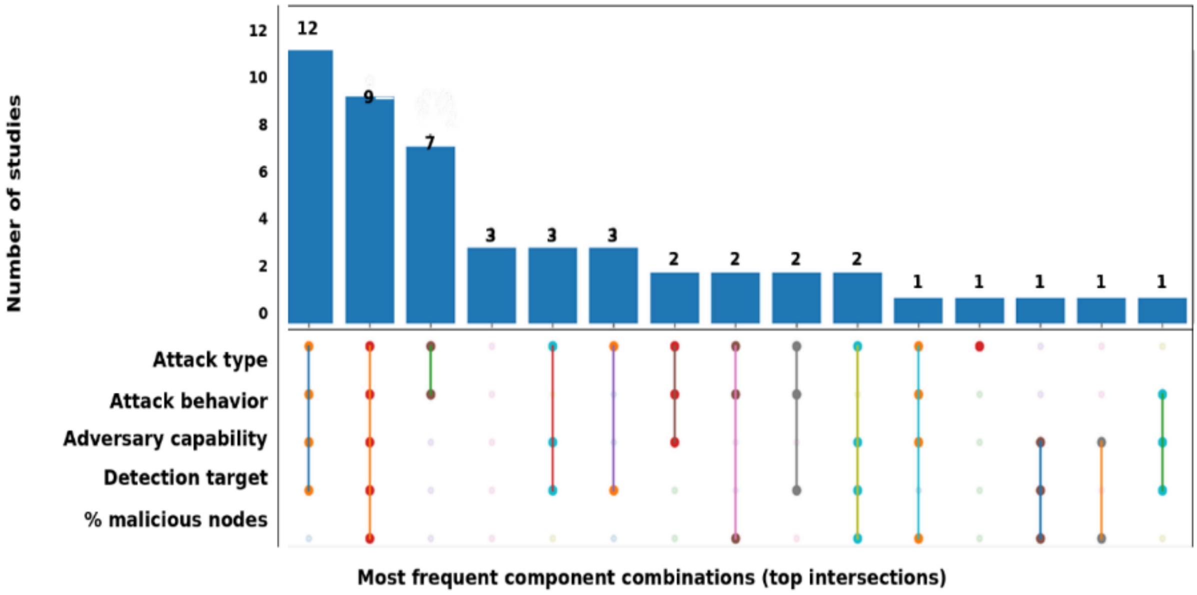

Figure 12. UpSet-style co-occurrence of reported threat-model components (N = 51). Bars show the most frequent component combinations; dots indicate included components.

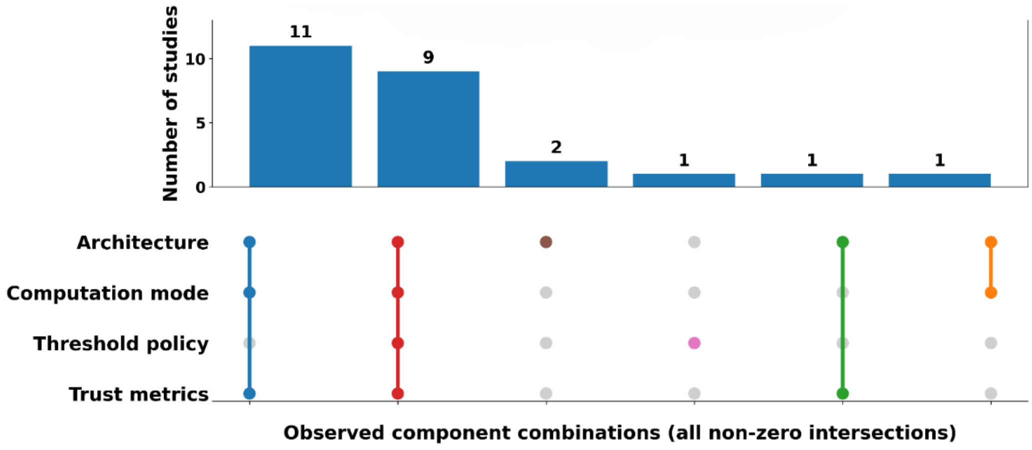

Figure 13. UpSet-style co-occurrence of reported trust-design components (n = 25). Bars show observed combinations; dots indicate included components.

Figure 13 shows how trust-based studies bundle trust-design elements instead of reporting them one by one (n = 25). The most common combination reports architecture, computation mode, and trust metrics but omits a threshold policy (11/25, 44.0%). Complete reporting of all four elements occurs in 9/25 studies (36.0%). This pattern highlights threshold policy as the main missing piece, even when trust is otherwise well specified.

Figure 14 summarizes trust-design completeness using a four-component depth index among trust-based studies (n = 25). Scores cluster at 3 and 4, with a mean of 3.00 and a median of 3. Full reporting of all four elements occurs in 9/25 studies (36.0%). Five studies score 2 or below (5/25, 20.0%), showing that some trust proposals still omit key operational details.

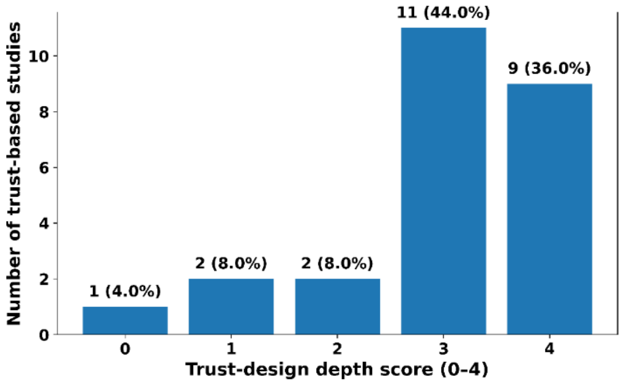

Figure 14. Trust-design depth index (n = 25). One point is assigned for each reported element: architecture, computation mode, threshold policy, and trust metrics. Bars show counts and percentages.

3. Discussion

Objective 1 shows that the reviewed literature clusters into a small set of dominant security themes and repeatedly modeled attack types. The dominance of routing and forwarding attacks suggests that many studies still frame MANET security around disruptions to cooperation rather than broader system compromise. The attack distribution indicates that a few canonical threats anchor much of the problem framing in recent work. Together, Table 1 and Figure 4 establish the classification foundation that Objective 2 then uses to examine how defense techniques are selected and combined across those themes. Objective 2 shows that integration, rather than replacement, is the dominant design logic in contemporary MANET security solutions. The technique–attack heatmap and the technique–theme alignment indicate that technique families are not confined to single problem framings. Instead, they are reused across multiple themes and repeatedly applied to the most common attack settings. This helps explain why several security themes share the same technique families rather than developing as fully separate lines of work. The technique-pair network reinforces this point by showing recurring combinations that function as reusable design templates. This is reflected in the repeated co-occurrence of learning with IDS/ADS and the frequent coupling of optimization with trust, which together suggest a common pipeline structure rather than isolated mechanisms. These combinations often divide roles across detection, decision making, and optimization. The learning-oriented methods frequently appear alongside IDS/ADS components, which fit a workflow where inference supports detection and classification. Metaheuristic optimization and trust mechanisms connect broadly, which is consistent with their use as coordination or control layers that can be embedded in different configurations.

This recurring structure suggests that novelty is often introduced through recombination and operational choices, not only through selecting a new technique family. While this supports reuse and comparability, it also increases the risk of design convergence when integrations are not clearly justified. As a result, the value of a study increasingly depends on how techniques are composed, parameterized, and linked to the stated threat and theme, rather than on the technique labels alone. Many hybrid learning and optimization solutions are presented as superior, but practical MANET operation requires models that can be understood, monitored, and overridden when needed. In particular, IDS or learning components should not be treated as black boxes, since misclassification can trigger unnecessary isolation, route suppression, or cascading partition risk. The reviewed designs also vary in whether they specify safe fallback behavior, such as conservative routing defaults, confidence thresholds, or bounded response actions when uncertainty is high. This matters because accurate detection alone does not guarantee operational reliability in dynamic MANET conditions, especially when false positives carry networkwide cost. A stronger discussion of interpretability and fail-safe behavior would improve the credibility of integration-heavy designs.

Objective 3 reveals a disconnect between how attacks are labeled and how they are operationally defined for detection. Many studies rely on simplified adversary assumptions and do not fully specify behavioral rules, even when detection mechanisms are proposed. This creates ambiguity about what evidence is actually used to infer malicious activity. The uneven specification of detection targets further limits interpretability, since it is often unclear whether detection operates at the node, route, or traffic level. Within trust-based studies, detection logic is most often grounded in observable forwarding behavior, with less emphasis on richer or adaptive evidence sources. These patterns suggest that threat modeling remains driven by evaluation convenience rather than by systematic adversary characterization, which constrains reproducibility and cross-study comparison.

The reviewed corpus contains limited explicit modeling of adaptive attackers relative to simplified attacker assumptions, which means many detection claims are implicitly bounded to stationary behavior. This is especially relevant for learning-based defenses, where evasion and poisoning threats can invalidate assumptions about feature stability, label reliability, or model generalization. When adaptive capability is not modeled, reported robustness may reflect the convenience of the threat setup rather than resilience to intelligent opposition. As a result, effective detection should be interpreted as conditional on the stated adversary capability and on whether behavioral rules are explicitly defined and testable.

Many IDS and learning-based approaches depend on labeled traffic or labeled node-behavior traces, yet the reviewed studies often vary in how labels are obtained, validated, or maintained over time. In MANET settings, ground truth labeling is difficult because malicious behavior can be intermittent, context-dependent, or indistinguishable from congestion and mobility effects. This creates a practical constraint that affects deployability and comparability across studies, particularly when labels are assumed rather than operationalized. It also reinforces why clear reporting of detection targets and evidence sources is essential, since labels ultimately depend on what a system claims to observe and measure.

The results imply that technique choice should be guided by operational context, not by popularity alone, because MANET deployments differ sharply in resource budgets, urgency, and privacy constraints. Detection and learning pipelines can impose data collection burdens, including monitoring overhead, feature extraction cost, and storage or sharing of sensitive traces. Privacy risk also increases when security logic relies on collecting detailed behavior logs, especially in domains such as health, emergency response, or civilian IoT where monitoring itself can be sensitive. Label scarcity is not an edge case in MANET security; it is a baseline condition, so approaches that assume abundant labeled traces should be treated as less deployment-ready unless they include label-minimizing strategies such as transfer learning, weak supervision, or carefully bounded synthetic augmentation.

Objective 4 highlights that many limitations in the literature stem from incomplete reporting rather than from missing security mechanisms. Although multiple security components are often mentioned, their interactions and enforcement conditions are not consistently documented. Depth indices show that partial specification is common, which implies that assumptions about adversary behavior, trust computation, or decision thresholds are frequently left implicit. In trust-based studies, architectural and computational aspects are more often described than policy-level details, such as thresholding and enforcement logic. This imbalance suggests that authors prioritize demonstrating conceptual feasibility over formalizing operational completeness. Improving reporting rigor would therefore have a greater impact on cumulative progress than introducing additional mechanisms without clear specification.

Based on the combined findings across Objectives 1–4, the following checklist summarizes practical considerations for selecting and deploying MANET security mechanisms in real-world settings.

3.1 Practitioner checklist

- Extreme resource constraints: Prefer lightweight detection targets and low-overhead evidence. Favor trust and rule-based checks only if computation and messaging cost are bounded. Avoid heavy feature pipelines unless explicitly optimized for energy and bandwidth.
- Emergency or disaster operations: Prioritize fast-deployable mechanisms with clear fail-safe defaults. Prefer conservative actions under uncertainty. Avoid solutions that require long training windows or centralized labeling steps.
- IoT or 6G-integrated MANETs: Favor methods that can adapt across heterogeneous devices and traffic. Prefer modular designs where IDS, optimization, and trust components can be updated independently. Require clear reporting of assumptions about device capability and link stability.
- Privacy-sensitive domains: Minimize raw trace collection and long-term storage. Prefer on-device inference and aggregated evidence where feasible. Require explicit statements about what is observed, what is stored, and how identity or location leakage is mitigated.

Taken together, the four objectives show a field that has matured around a stable set of threats, themes, and technique families, but remains uneven in how security designs are operationalized and documented. The same canonical attacks and reusable technique combinations appear across many themes, yet the underlying threat assumptions, detection targets, labeling foundations, and enforcement policies are often left underspecified. This combination of design convergence and reporting variability helps explain why results can look comparable at the level of labels while remaining difficult to reproduce or deploy. Future progress is therefore likely to depend as much on stronger specification and operational transparency as on proposing new mechanisms.

4. Conclusion

This descriptive systematic review examined contemporary MANET security research from January to August 2025, using structured coding to classify studies by security theme, modeled attacks, defense techniques, and reporting practices. The findings indicate convergence toward a small set of recurring attack models and reusable technique combinations, with integration-heavy pipelines occurring more frequently than single-mechanism defenses. At the same time, incomplete specification of adversary capability, detection targets, labeling foundations, and enforcement policies limits interpretability, reproducibility, and operational confidence. Future work will analyze evaluation orientation, including simulation settings, performance metrics, baselines, and validation practices, to clarify how security claims are empirically supported and how deployment realism is handled across MANET studies.

Ethical issue

The authors are aware of and comply with best practices in publication ethics, specifically with regard to authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with policies on research ethics. The authors adhere to publication requirements that the submitted work is original and has not been published elsewhere. All survey participants provided informed consent prior to participation, and the anonymity and confidentiality of all respondents were strictly maintained throughout the research process.

Data availability statement

The manuscript contains all the data. However, additional data will be provided by the corresponding author upon reasonable request.

Conflict of interest

The authors declare no potential conflict of interest.

References

[1] Swain J, Pattanayak BK, Pati B. A Systematic Study and Analysis of Security Issues in Mobile Ad-hoc Networks. International Journal of Information Security and Privacy (IJISP) 2018;12:38–45. https://doi.org/10.4018/IJISP.2018040103.

[2] Gurung S, Chauhan S. A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. Wireless Networks 2019 26:3 2019;26:1981–2011. https://doi.org/10.1007/S11276-019-01966-Z.

[3] Hassan SM, Mohamad MM, Muchtar FB. Advanced Intrusion Detection in MANETs: A Survey of Machine Learning and Optimization Techniques for Mitigating Black/Gray Hole Attacks. IEEE Access 2024. https://doi.org/10.1109/ACCESS.2024.3457682.

[4] Zhang C, Zhou MC, Yu M. Ad hoc network routing and security: A review. International Journal of Communication Systems 2007;20:909–25. https://doi.org/10.1002/DAC.840.

[5] Rodriguez-Baeza JA, Magan-Carrion R, Ruiz-Villalobos P. Advances on Security in Ad Hoc Networks: A preliminary analysis. Iberian Conference on Information Systems and Technologies, CISTI, Chaves, Portugal: IEEE Computer Society; 2021, p. 1–5. https://doi.org/10.23919/CISTI52073.2021.9476278.

[6] Mohandas R, Sivapriya N, Vaigandla KK, Kirubasankar K. Detection and Mitigation of Attacks in MANETs: A Comprehensive Survey of Security Techniques. Proceedings of the 4th International Conference on Ubiquitous Computing and Intelligent Information Systems, ICUIS 2024, Gobichettipalayam, India: IEEE; 2024, p. 1478–85. https://doi.org/10.1109/ICUIS64676.2024.10866793.

[7] Cho JH, Swami A, Chen IR. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys and Tutorials 2011;13:562–83. https://doi.org/10.1109/SURV.2011.092110.00088.

[8] Sathiya R, Yuvaraj N. Analyzing intrusion detection systems in mobile ad-hoc network architectures: A systematic review. In: Dagur A, Singh K, Mehra PS, Shukla DK, editors. Intelligent Computing and Communication Techniques, vol. 3. 1st ed., CRC Press; 2025, p. 238–42. https://doi.org/10.1201/9781003635680-37.

[9] Agor AD, Ami-Narh JT, Banning LA, Brown SA, Elliot MAA, Tanye HA. Hybridizing Intelligent Water Drops and River Formation Dynamics for Optimal Routing Path Selection with Minimum Energy in MANETs. Journal of Artificial Intelligence and Technology 2025:1–9. https://doi.org/10.37965/JAIT.2025.0575.

[10] Agor AD, Asante M, Hayfron-Acquah JB, Ami-Narh JT, Aziale LK, Peasah KO. A power-aware river formation dynamics routing algorithm for enhanced longevity in MANETs. International Journal of Computer Networks and Applications 2024;11:274–89. https://doi.org/10.22247/ijcna/2024/17.

[11] Agor AD, Asante M, Hayfron-Acquah JB, Peasah KO, Agangiba M, Elliot MAA, et al. Power-aware intelligent water drops routing algorithm for best path selection in MANETs. International Journal of Communication Networks and Information Security 2024;16:1–13.

[12] Nazir MK, Rehman RU, Nazir A. A novel review on security and routing protocols in MANET. Communications and Network 2016;8:205–18. https://doi.org/10.4236/cn.2016.84020.

[13] Prasath S. A study on manet and its security issues. National Conference on Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020), vol. 22, Avadi, Chennai-62: Department of Commerce, VEL TECH Ranga Sanku Arts College; 2020, p. 66–74.

[14] Paliwal G, Mudgal AP, Taterh S. A study on various attacks of TCP/IP and security challenges in MANET layer architecture. Fourth International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing 336, 2018, p. 195–209. https://doi.org/10.1007/978-81-322-2220-0_16.

[15] Panda N, Patra B, Hota S. MANET routing attacks and their countermeasures: A survey. Journal of Critical Reviews 2020;7:2777–92. https://doi.org/10.31838/jcr.07.13.428.

[16] Karthigha M, Latha L, Sripriyan K. A comprehensive survey of routing attacks in wireless mobile ad hoc networks. 5th International Conference on Inventive Computation Technologies, ICICT 2020, Institute of Electrical and Electronics Engineers Inc.; 2020, p. 396–402. https://doi.org/10.1109/ICICT48043.2020.9112588.

[17] Saha HN, Bhattacharyya D, Banerjee B, Mukherjee S, Singh R, Ghosh D. A review on attacks and secure routing protocols in MANET. International Journal of Innovative Research and Review 2013;1:12–36.

[18] Ali MA, Sarwar Y. Security issues regarding MANET (Mobile Ad Hoc Networks): challenges and solutions. Blekinge Institute of Technology, 2011.

[19] Tayal S, Gupta V. A survey of attacks on manet routing protocols. International Journal of Innovative Research in Science, Engineering and Technology 2013;2:1180–2285.

[20] Joshi K, Kumar K. Security breaches of mobile ad-hoc networks (MANET) - A review. Educational Administration Theory and Practice 2024;30:2656–65. https://doi.org/10.53555/kuey.v30i4.1912.

[21] Agor AD, Kwami Aziale L, Kataka Banaseka F, Owusu-Agyemang K, Brown SA, Partey BT. Trust and adaptiveness enhancements to PRFDRA for secure metaheuristic path selection in MANETs 2025;5:168–79. https://doi.org/10.55670/fpll.futech.5.1.15.

[22] Arulselvan G, Rajaram A. Routing attacks detection in MANET using trust management enabled hybrid machine learning. Wireless Networks 2025;31:1481–95. https://doi.org/10.1007/S11276-024-03846-7/METRICS.

[23] Akanksha, Mahapatra RP, Chaudhary H. Analysis and Design of Reliable Node Routing Mechanism for MANET using Fuzzy Logic. 2025 3rd International Conference on Communication, Security, and Artificial Intelligence, ICCSAI 2025, Greater Noida, India: Institute of Electrical and Electronics Engineers Inc.; 2025, p. 1346–51. https://doi.org/10.1109/ICCSAI64074.2025.11064038.

[24] Sarangi SK, Lenka R, Nanda A, Panda BS. Development of MD-LSTM for malicious detection and hybrid coati and dolphin swarm optimization for QoS-aware multicast routing in MANET environment. Computers and Electrical Engineering 2025;123:110086. https://doi.org/10.1016/J.COMPELECENG.2025.110086.

[25] Adilakshmi Y, Raziya S, Avinash S, Chaitanya VS, Siddi NG. A Secure Defensive Mechanism Against DDoS Attack in MANETs Using ML: Classification Algorithms. 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal: IEEE; 2025, p. 1021–9. https://doi.org/10.1109/ICSADL65848.2025.

[26] Bhutia R, Mothukuri R. Design of a one-dimensional network model for evaluating security threats in MANET. Information Security Journal: : A Global Perspective 2025:1. https://doi.org/10.1080/19393555.2025.2522436.

[27] Mohammed FJ, Andalib A, Azgomi H, Sharifi SA. Enhancing the Security of Mobile Ad-hoc Networks: A Black Hole Attack Mitigation Approach Using Response Time and Machine Learning Models. Journal of Industrial and Systems Engineering 2025;17:204–16. https://doi.org/10.1002/ETT.3676.

[28] Jangade V, Nirkhi S. A Novel Approach For Optimising Communication And Secure Connectivity In Mobile Ad-Hoc Networks (Manets). International Journal of Environmental Sciences 2025;11:1229–39. https://doi.org/10.64252/T0ANXP71.

[29] Priya SS, Vijayabhasker R, Rajaram A. Advanced Security and Efficiency Framework for Mobile Ad-Hoc Networks Using Adaptive Clustering and Optimization Techniques. Journal of Electrical Engineering and Technology 2025;20:1815–26. https://doi.org/10.1007/S42835-024-02119-9/METRICS.

[30] Mohsen Hassan S, Mohamad MM, Binti Muchtar F. Enhancing MANET Security Through Long Short-Term Memory-Based Trust Prediction in Location-Aided Routing Protocols. IEEE Access 2025;13:120142–68. https://doi.org/10.1109/ACCESS.2025.3572619.

[31] Pramodh Krishna D, Sandhya E, Khaja Shareef S, Mantena SV, Desanamukula VS, Koteswararao C, et al. Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection. Scientific Reports 2025;15:1–16. https://doi.org/10.1038/S41598-024-84421-0.

[32] Addula SR, Mamodiya U, Jiang W, Almaiah MA. Generative AI-Enhanced Intrusion Detection Framework for Secure Healthcare Networks in MANETs. SHIFRA 2025;2025:62–8. https://doi.org/10.70470/SHIFRA/2025/003.

[33] Swathi R, Perumalla S, Arun M, Bharathi DVN, Srinivas E, Krishnan VG. Security Enhancement in MANET using Modified Crow Search Optimization Algorithm for IoT Applications. 2025 International Conference on Emerging Smart Computing and Informatics, ESCI 2025 2025. https://doi.org/10.1109/ESCI63694.2025.10988271.

[34] Mathiazhagan P, Dhayashankar JM. Enhanced Authenticated Routing for MANET: A Comprehensive Solution for Reliable routing path selection. Networks 2025;1.

[35] Alyoubi AA. High-speed adaptive and efficient ad hoc on-demand distance vector for secure routing in mobile ad hoc networks using reinforcement learning and artificial bee colony optimization. Journal of High Speed Networks 2025;31:123–44. https://doi.org/10.1177/09266801241299920.

[36] Huang S, Raad R, Tubbal F, Odeh N. An ARP-integrated enhancement of AODV for wormhole attack detection in mobile ad hoc networks. Journal of Network and Computer Applications 2025;243:104283. https://doi.org/10.1016/J.JNCA.2025.104283.

[37] Aravind A, Poongodi A. Quantum-Driven Resilient Pathway Discovery for Optimized Security and Performance in MANETs under Adversarial Conditions. 2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Institute of Electrical and Electronics Engineers (IEEE); 2025, p. 1440–6. https://doi.org/10.1109/ICICV64824.2025.11085529.

[38] Gopalasamy K, Muthaiya KG. Optimizing packet routing and security in MANETs with the H-MAntnetSVM algorithm for energy efficiency and blackhole detection. Sustainable Computing:

Informatics and Systems 2025;46:101123. https://doi.org/10.1016/J.SUSCOM.2025.101123.

[39] Schweitzer N, Cohen L, Hirst T, Dvir A, Stulman A. Achieving manet protection without the use of superfluous fictitious nodes. Computer Communications 2025;229:107978. https://doi.org/10.1016/J.COMCOM.2024.107978.

[40] Majumder S, Bhattacharyya D, Chowdhuri S. ABCD: advanced blockchain DSR algorithm for MANET to mitigate the different security threats. Eurasip Journal on Wireless Communications and Networking 2025;2025:1–39. https://doi.org/10.1186/S13638-025-02430-7.

[41] Sugumaran VR, Dinesh E, Ramya R, Muniyandy E. Distributed blockchain assisted secure data aggregation scheme for risk-aware zone-based MANET. Scientific Reports 2025;15:1–21. https://doi.org/10.1038/S41598-025-92656-8.

[42] Gopinath S, Chairman M, Natraj NA, Sarankumar R. BDSCRP: Blockchain based Dynamic Secure Cluster Routing Protocol for MobileAd hoc Networks (MANETs). Proceedings of 8th International Conference on Inventive Computation Technologies, ICICT 2025, Institute of Electrical and Electronics Engineers Inc.; 2025, p. 1717–24. https://doi.org/10.1109/ICICT64420.2025.11005260.

[43] Dudala DSS, Patamsetti R, Nuli PB, Nagendranath M. WOA-DE Hybrid for Energy-Efficient and Secure Routing in MANETs. IJSAT - International Journal on Science and Technology 2025;16:1–8. https://doi.org/10.71097/IJSAT.V16.I1.3034.

[44] Saravanan T, Preetham DS, Venkatasubramanian A. Optimized Adaptive Routing and Link Health Management in Mobile Ad Hoc Networks using Enhanced Meta Ant Advanced Beaconing with Integrated Auto-Repair and Security Protocols. Proceedings of 2025 AI-Driven Smart Healthcare for Society 50, AdSoc50 2025, Institute of Electrical and Electronics Engineers Inc.; 2025, p. 278–82. https://doi.org/10.1109/IEEECONF64992.2025.10962821.

[45] Naveen N, Nirmaladevi J. Secure bio-inspired optimization with intrusion aware on-demand routing in MANETs. Scientific Reports 2025;15:1–31. https://doi.org/10.1038/S41598-025-99269-1.

[46] Begum MB, Suganthi B, Sivagamasundhari P, Arunmozhi SA, Suhail SJM. An Enhanced Heterogeneous Local Directed Acyclic Graph Blockchain With Recalling Enhanced Recurrent Neural Networks for Routing in Secure MANET-IOT Environments in 6G. International Journal of Communication Systems 2025;38:e6110. https://doi.org/10.1002/DAC.6110.

[47] Vikas, Teotia S. Optimization of Graph Neural Networks for Real-TimeIntrusion Detection in Dynamic Mobile Ad-Hoc Networks. International Journal of Environmental Sciences 2025;11:740–8. https://doi.org/10.64252/79452G17.

[48] Rajkumar M, Karthika J, Abinayaa SS. Multi-view consistent generative adversarial network for enhancing intrusion detection with prevention systems in mobile ad hoc networks against security attacks. Computers & Security 2025;150:104242. https://doi.org/10.1016/J.COSE.2024.104242.

[49] Hemalatha S, Shalini S, Kumar PS, Srinivas R, Thilagam T, Kumbhar DV, et al. A hybrid approach for intrusion detection and prevention in mobile ad hoc networks. Journal of Theoretical and Applied Information Technology 2025;15:1128–44.

[50] Sardar TH, Dar SA, Jaiswal J, Guru Prasad MS, Mittal M, Kumar V. Enhancing Security in MANETs with Deep Learning-Based Intrusion Detection. Procedia Computer Science 2025;259:120–9. https://doi.org/10.1016/J.PROCS.2025.03.313.

[51] Aakunuri M, Manjula A, Vaishali K, Gachikanti S. A Novel Intrusion Detection System for Mitigating Black Hole Attacks in Wireless Networks. Communications on Applied Nonlinear Analysis 2025;32:640–50.

[52] Gayathri Devi S, Chandia S, Savithri V, Saraswathi K. Optimized high-dimensional memristive hopfield neural network for DoS attack detection in Mobile Adhoc Network. Knowledge-Based Systems 2025;310.

[53] Muhammad MM, AL-Asadi HAA. A Deep Learning-Based Enhancement to OLSR for Robust Attack Detection and Secure Multimedia Transmission in MANETs. Basrah Researches Sciences 2025;51:15.

[54] Martin JJ, George JP, Alapatt BP. A Novel Approach to Packet Dropping and Malicious Attack Detection using Ensemble Techniques 2025:1458–63. https://doi.org/10.1109/ICICV64824.2025.11085510.

[55] Saminathan K, Perumal L, Shajin FH, Shakya RK. Multicast On-Route cluster propagation to detect network intrusion detection systems on MANET using Deep Operator Neural networks. Expert Systems with Applications 2025;271:125864. https://doi.org/10.1016/J.ESWA.2024.125864.

[56] Sunitha D, Latha P. A secure routing and black hole attack detection system using coot Chimp Optimization Algorithm-based Deep Q Network in MANET. Computers & Security 2025;148:104166. https://doi.org/10.1016/J.COSE.2024.104166.

[57] Pushpalatha S, Narasimhulu N. A hybrid approach for detecting network layer attacks in MANET. International Journal of System Assurance Engineering and Management 2025:1–14. https://doi.org/10.1007/S13198-025-02854-W/METRICS.

[58] Pavani V, Vyshnavi A, Divya C, Jayalakshmi M, Jyothi P. QOS-aware Secure and Energy Efficient MAC framework for MANETs 2025:1–6. https://doi.org/10.1109/RFCON62306.2025.11085407.

[59] Anugraha DM, Ebenezer DSS, Maheswari DS. Hybrid elk herd green anaconda-based multipath routing and deep learning-based intrusion detection in MANET. Pervasive and Mobile Computing 2025;112:102079. https://doi.org/10.1016/J.PMCJ.2025.102079.

[60] Khandekar VA, Gupta P. Machine learning-based hybrid SSO-MA with optimized secure link state

routing protocol in Manet. China Communications, vol. 22, Institute of Electrical and Electronics Engineers (IEEE); 2025, p. 164–80. https://doi.org/10.23919/JCC.JA.2023-0401.

[61] Sudhaakar K, Meena Abarna KT, Mohan E. Detection of Selfish Node in Mobile Ad Hoc Network by Adaptive Multi-Serial Cascaded Network. International Journal of Communication Systems 2025;38:e70059. https://doi.org/10.1002/DAC.70059.

[62] Messabih H, Cheriguene Y, Ahmad F, Hadjkouider AM, Kerrache CA. Digital Twins with Stackelberg Game for Mobile Ad-hoc Networks' Security. In 7th International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE; 2025.

[63] Dhand G, Rao M, Chaudhary P, Sheoran K. A secure routing and malicious node detection in mobile Ad hoc network using trust value evaluation with improved XGBoost mechanism. Journal of Network and Computer Applications 2025;235:104093. https://doi.org/10.1016/J.JNCA.2024.104093.

[64] Dalal K. Hybrid optimization-based secured routing in mobile ad-hoc network. Intelligent Decision Technologies 2025;19:312–36. https://doi.org/10.3233/IDT-240739.

[65] Prasanna KS, Ramesh B. Multiobjective Secure Trust Aware Redundant Array Shifting Encryption and Clustering Based Routing in Mobile Ad Hoc Networks. International Journal of Communication Systems 2025;38:e6074. https://doi.org/10.1002/DAC.6074.

[66] Anand MV, Krishnamurthy A, Kannan A, Govindarajan N. Secure Routing in Mobile Ad Hoc Networks with Hybrid Tasmanian Gazelle Optimization. IETE Journal of Research 2025:1. https://doi.org/10.1080/03772063.2025.2466683.

[67] Nivedita V, Shieh CS, Horng MF. An integrated trust-based secure routing with intrusion detection for mobile Ad Hoc network using adaptive snow geese optimization algorithm. Ain Shams Engineering Journal 2025;16:103385. https://doi.org/10.1016/J.ASEJ.2025.103385.

[68] Zubairu B, Gide AI. Machine Learning-Based Framework for Detecting and Mitigating DoS Attacks in Mobile Ad-Hoc Networks (MANETs). International Journal of Computers 2025;10:151–60.

[69] Vincent SSM. Mitigating Sinkhole Attacks in MANET Routing Protocols using Federated Learning HDBNCNN Algorithm. CLEI Electronic Journal 2025;28:1–9. https://doi.org/10.19153/CLEIEJ.28.1.7.

[70] Sudha B, Midhunchakkaravarthy, Khekare G, Aishwarya M. High-Security Voice Data Encryption in MANETs Using AES, Wavelets, and AI Optimization Optimization. SGS - Engineering & Sciences 2025;1:1–7.

[71] Sudha B, Midhunchakkaravarthy, Khekare G. Biometrically Enhanced Dual-Layer Voice Encryption for MANETs using DWT-AES and Deep Reinforcement Learning Optimization. SGS - Engineering & Sciences 2025;1:1–2.

[72] Mabina A. Enhancing Security Protocols for MANETs in 5G-Enabled Smart Healthcare Systems. International Journal of Artificial Intelligence and Science 2025;2:18–39. https://doi.org/10.63158/IJAIS.V2.I1.15.