

Security Threat Assessment and Defence Strategies for Mobile Ad Hoc Networks

Priyanka Jangra

Department of Electronics & Communication Engineering, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, INDIA

Abstract: Mobile Ad Hoc Networks (MANETs) are networks of multi-hop wireless nodes that self-organize and connect without any infrastructure, suitable for use in applications ranging from disaster response, tactical communication, vehicular networks, wireless sensor networks, and emerging IoT edge environments. MANETs are prone to a variety of security threats, however, due to their dynamic topology, open wireless medium, decentralized control, limited resources and cooperative forwarding. This paper gives an in-depth survey of security issues and security Defence solutions in MANETs. A layer wise taxonomy of representative attacks at the physical, MAC, network, transport and application layer is provided and special focus is given to attacks such as blackhole, wormhole, Sybil, rushing, sinkhole and sleep-deprivation attacks. Key security methods are reviewed, such as cryptographic mechanisms, secure routing protocols, trust-management approaches, intrusion detection systems (IDS), and machine-learning (ML) and deep-learning (DL)-based detection methods. We compare representative protocols like SAODV, ARAN, SEAD, Ariadne and SAR with trust-based protocols such as Watchdog/Pathrater, CONFIDANT, fuzzy and bio-inspired trust models, and hybrid ML-trust routing. The review also emphasizes the growing prevalence of the use of ML/DL for detecting previously unknown and complex attack patterns, and the inherent challenges of computations, data, and explanations. The comparative study shows that no single Defence mechanism is enough to address all the security needs of MANET only integrated schemes with a mix of cryptographic mechanisms, behavioural trust and intelligent intrusion detection provide a security-adaptable and resource-efficient balance. Finally, major research challenges are identified such as energy-security trade-offs, few datasets for MANETs, scalability in high mobility, collusion, adversarial machine learning, post quantum readiness, privacy preserving detection and real world validation to be investigated in future.

Keywords: Mobile Ad hoc Network (MANET); routing security; blackhole attack; wormhole attack; secure routing protocols; trust management; intrusion detection system; machine learning.

1. Introduction

A Mobile Ad hoc Network (MANET) is a network consisting of a collection of mobile wireless nodes that randomly form multiple hops communication links between each other without relying on a fixed infrastructure like a base station, an access point or a fixed backbone. Each node in a MANET is also a host, and forwards packets on behalf of other nodes, thus enabling communication to be maintained even if two nodes are outside each other's radio range [1]. This flexibility has led to MANETs being used in various scenarios such as battlefield and tactical communication, disaster relief and emergency response, vehicular ad hoc networks (VANETs), wireless sensor networks (WSNs), and quickly deployable Internet-of-Things (IoT) edge networks [2].

This same set of features that make MANETs flexible and adaptable to a variety of applications, the lack of centralized control, the availability of an open and shared wireless medium, the high dynamic and unpredictable topology, and the reliance on the voluntary cooperation of the resource-constrained nodes for the routing service, are also the reasons for their severe vulnerability to security attacks [3]. In contrast to wired networks or infrastructure based wireless networks, there is no fixed point at which traffic can be monitored, filtered, or authenticated; each node in a MANET is also a potential communication relay, and a potential point of compromise [4]. Thus MANETs are vulnerable to various attacks including passive attacks such as eavesdropping and traffic analysis, active attacks at the routing layer like blackhole, wormhole, Sybil attacks, and high layer attacks like session hijacking and denial of service (DoS) flooding [5].

In the last 20 years, the research community proposed numerous countermeasures ranging from cryptographic key-management schemes, secure extension of routing protocols, trust and reputation management frameworks and in recent years, machine-learning (ML) and deep-learning (DL) based intrusion detection systems [6]. Most of these solutions, however, come with non-trivial security, computation and communication trade-offs, as well as with the extreme energy and bandwidth limitations imposed on MANET nodes. As a result, a systematic knowledge of the attack landscape and relative strengths and limitations of the available defences is essential to those researchers and practitioners designing security solutions for MANETs and their derivative technologies

There are several surveys on MANET security in the literature, but many of them are limited to a particular attack category (such as routing attacks) and a single defence category (such as trust management) or are dated as they come before the last 5 years of machine learning based intrusion detection in MANETs. This paper seeks to offer an up-to-date, comprehensive overview that (i) classifies attacks in a layer-wise manner, (ii) compares cryptographic, trust-based and learning-based defences in a single framework and (iii) consolidates the comparison aspects in tabular and graphical form.

The remainder of this paper is organized as follows. Section 2 presents a layer-wise taxonomy of security attacks in MANETs. Section 3 discusses defence mechanisms, with emphasis on cryptographic approaches, secure routing protocols, and their associated limitations. Section 4 reviews trust-management approaches and intrusion detection systems, including machine-learning- and deep-learning-based techniques. Section 5 provides a comparative analysis of representative studies and discusses major open research challenges. Section 6 presents the conclusion and future research directions.

Contributions

A layer-wise taxonomy of MANET security attacks (physical, MAC, network, transport, and application), consolidated in a single comparison table and an accompanying schematic diagram.

Detailed mechanistic illustrations of two of the most extensively studied network-layer attacks — the blackhole attack and the wormhole attack — supported by schematic figures.

A structured comparison of secure routing protocols (SAODV, ARAN, SEAD, Ariadne, SAR) and trust-management frameworks (Watchdog/Pathrater, CONFIDANT, fuzzy and bio-inspired trust models, and hybrid ML-trust routing).

A consolidated view of intrusion detection system (IDS) categories and of the detection-accuracy ranges reported for machine-learning and deep-learning-based IDS techniques across the surveyed literature.

2. Taxonomy of Security Attacks in MANETs

Security attacks on MANETs are typically classified based on the protocol layer at which they are targeted because the technique, visibility and impact of an attacker substantially vary between protocol layers. This taxonomy is presented in Figure 1 and Table 1 describes each of these representative attacks with its main impact on network operation.

Figure 1 illustrates the layer-wise taxonomy of security attacks targeting MANETs across the physical, MAC, network, transport, and application layers.

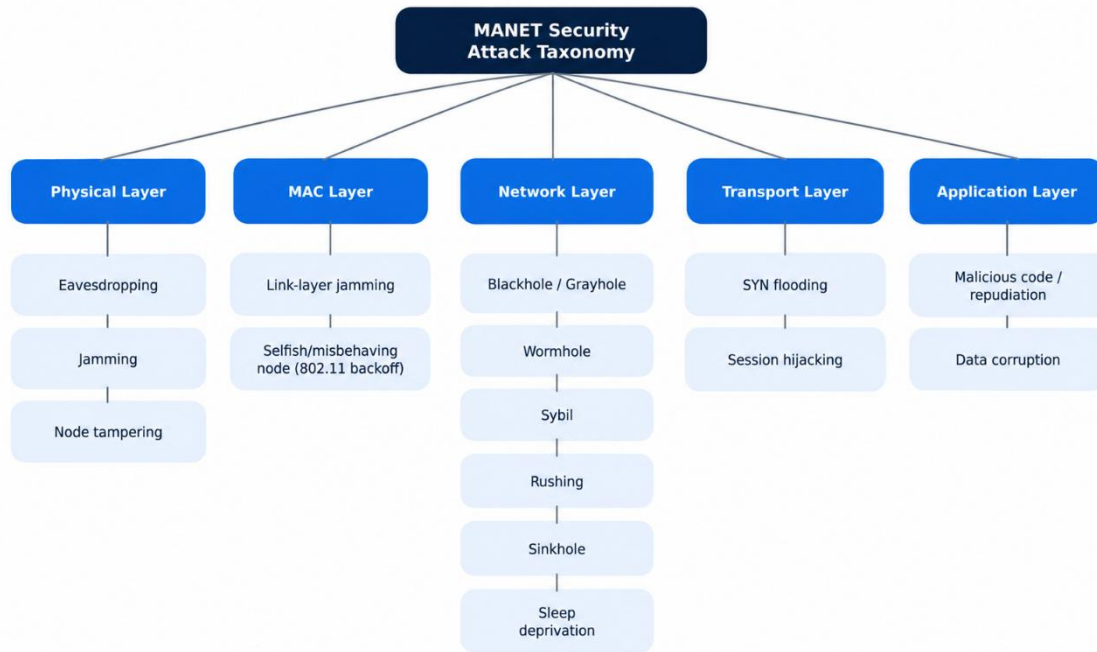


Figure 1. Layer-wise taxonomy of security attacks targeting MANETs.

Table 1 summarizes the representative security attacks across different MANET protocol layers, along with their brief descriptions and primary impacts on network operation.

Table 1. Layer-wise classification of representative MANET security attacks.

Layer	Attack	Brief description	Primary impact
Physical	Eavesdropping	Passive interception of transmissions over the shared wireless medium	Loss of confidentiality
Physical	Jamming	Deliberate radio interference to disrupt legitimate transmissions	Denial of service, reduced availability
MAC	Selfish node / backoff manipulation	A node manipulates 802.11-style contention parameters to gain unfair channel access	Unfairness, reduced throughput for cooperative nodes
Network	Blackhole / Grayhole	Malicious node falsely advertises the best route and drops all (blackhole) or selected (grayhole) data packets	Severe packet loss, route disruption
Network	Wormhole	Two colluding nodes tunnel packets	Traffic hijacking, route

Layer	Attack	Brief description	Primary impact
		between distant network regions to fabricate a fictitious short path	disruption, enables further attacks
Network	Sybil	A single malicious node presents multiple fabricated identities	Undermines trust, voting and reputation-based schemes
Network	Rushing attack	Attacker forwards route-discovery packets before legitimate nodes, forcing routes through itself	Route hijacking, especially against on-demand protocols
Network	Sinkhole	Malicious node advertises highly attractive routing metrics to draw traffic towards itself	Traffic funneling and subsequent dropping/tampering
Network	Sleep deprivation	Repeated, unnecessary route requests exhaust a victim node's battery	Premature node failure, reduced network lifetime
Transport	SYN flooding	Flood of connection-initiation requests exhausts transport-layer resources	Denial of service
Transport	Session hijacking	Attacker takes over an authenticated transport session after initial handshake	Loss of confidentiality/integrity of the session
Application	Malicious code / repudiation	Injection of malicious payloads or denial of a previously sent message	Data corruption, loss of accountability

3. Defence Mechanisms: Secure Routing and Cryptographic Approaches

3.1 Cryptographic Foundations and Key Management

The majority of the secure routing proposals for MANETs rely on the familiar symmetric and asymmetric cryptographic primitives such as MACs, digital signatures, and hash chains and use them to provide authentication of routing control messages and integrity protection. One of the first solutions to this problem was proposed by Zhou and Haas, who used threshold cryptography to distribute the tasks of a certificate authority among a threshold of nodes; that is, no single node compromising the system is able to forge certificates and the system is robust to the failure of any small set of nodes. Later research has focused on identity-based cryptographic approach and cluster-head based approach for key distribution to minimize the communication and computation cost for key management in resource constrained MANET environment.

3.2 Secure Routing Protocols

Many secure routing protocols are adaptations of the traditional MANET routing protocols like AODV and DSR with some cryptographic authentication of control messages. Secure Ad hoc On-Demand Distance Vector (SAODV): Propose to extend AODV with digital signatures to secure the non-mutable parts of a RREQ and RREP message, and hash chains to secure the mutable hop-count field, thus preventing routing packets from being tampered with. The Authenticated Routing for Ad hoc Networks (ARAN) protocol adopts a certificate-based approach, where each node signs and authenticates each routing message with certificates from a trusted authority with the associated overhead of public-key operations at each node. In a proactive routing context, the Secure Efficient

Distance vector routing protocol (SEAD) uses one-way hash chains to provide authentication for distance-vector routing updates, which is a less expensive alternative to public-key signatures. Ariadne uses a similar hash-chain per-hop message-authentication-code approach in the context of on-demand source routing (building on DSR), and the Security-Aware ad hoc Routing (SAR) protocol takes a complementary approach, adding explicit trust or security levels to the route-discovery process with the idea that routes should be chosen not only because they are the shortest, but because they provide a route with at least a minimum required level of trust.

Table 2 shows a comparative analysis of some representative secure routing protocols (SAODV, ARAN, SEAD, Ariadne, SAR, GTAODV and ML-AODV) with respect to their security mechanism, the attacks targeted and key limitations.

Table 2. Comparison of representative secure routing protocols for MANETs.

Protocol	Base protocol	Security mechanism	Attacks addressed	Key limitation
SAODV	AODV	Digital signatures + hash chains	Route message forgery, hop-count tampering	Public-key operations add computational overhead at each node
ARAN	AODV-style on-demand routing	Certificate-based authentication of every routing message	Impersonation, message tampering, replay	Requires a trusted certificate authority; per-hop signing overhead
SEAD	DSDV (proactive/distance-vector)	One-way hash chains for update authentication	Routing-table poisoning, unauthorized updates	Limited protection against colluding insiders; proactive overhead
Ariadne	DSR (source routing)	Hash chains and per-hop MACs; optional TESLA	Route forgery, unauthorized route modification	Requires loose time synchronization for TESLA-based variants
SAR	On-demand routing (generic)	Trust/security-level tagging of route requests	Routing through untrusted/low-trust nodes	Requires a priori trust-level assignment and management
GTAODV (trust-augmented AODV)	AODV	Direct, indirect and global trust metrics	Blackhole attack	Trust convergence time; overhead of trust propagation
ML-AODV	AODV	Trust estimation via hop count, residual energy and link-expiration time, combined with machine learning	Flooding and blackhole attacks	Depends on quality/representativeness of training data

Table 2 compares representative secure routing protocols, including SAODV, ARAN, SEAD, Ariadne, SAR, GTAODV, and ML-AODV, in terms of their underlying security mechanisms, targeted attacks, and key limitations.

Cryptographic and secure-routing techniques provide dense mathematical securities against forgery, tampering and impersonation, and are the basis for most other higher-level protection techniques. But the subsequent two constraints appear repeatedly in this family of solutions. First, the computation and communication costs involved in per-hop signature verification or certificate exchange may be high compared to the limited processing capacity and energy supply of most MANET nodes, especially when MANET nodes are highly mobile and the routes and associated cryptographic state need to be re-established often. Second, relying on pure cryptographic authentication does not, alone, prevent an authenticated misbehaving insider node (one with valid keys but forwarding packets unfaithfully, such as blackhole or grayhole attacks from disrupting the network. This restriction is the motivation for the complementary trust-management and intrusion detection approaches mentioned in Section 4.

4. Trust Management and Intrusion Detection Systems

Since cryptographic authentication is not enough to prevent an authenticated node from acting selfishly or maliciously, there has been a significant amount of research on MANET security focusing on two complementary approaches: trust management, which makes an estimate of the reliability of nodes observed from their behavior; and intrusion detection, which monitors traffic or routing behavior to detect an attack in progress. The overall taxonomy of Defence mechanisms is summarized in Figure 2. Figure 2 presents a taxonomy of MANET Defence mechanisms, covering preventive, trust-based, detection, and response-oriented approaches.

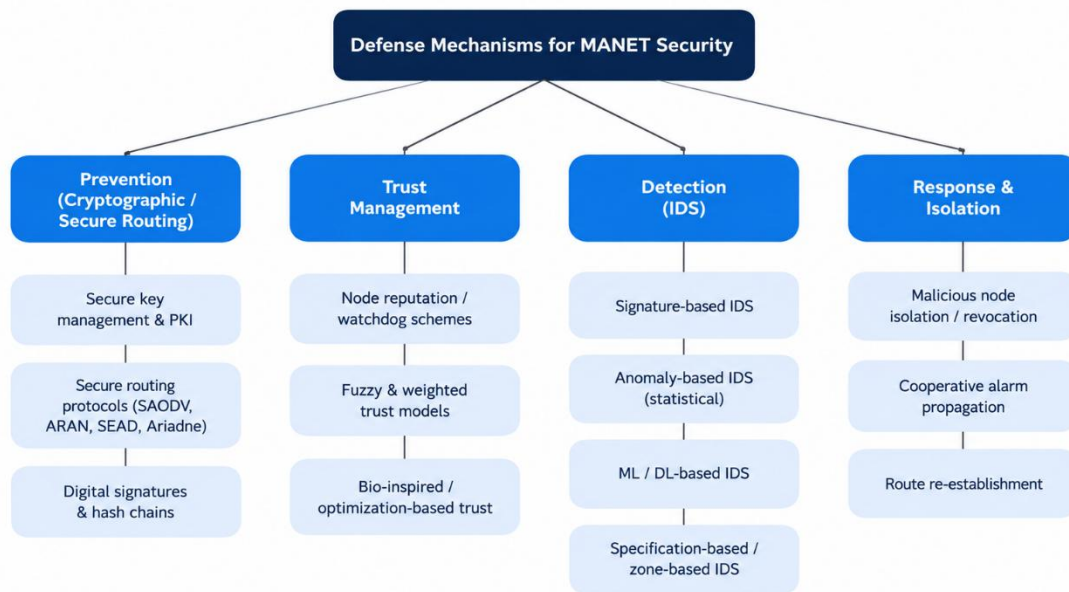


Figure 2. Taxonomy of Defence mechanisms proposed for securing MANETs, spanning preventive, trust-based, detective and responsive measures.

4.1 Trust Management Frameworks

In one of the earlier and more influential MANET trust schemes, the Watchdog and Pathrater scheme, Marti, Giuli, Lai and Baker introduced the idea of promiscuous mode for each node to listen to each other and identify nodes that fail to relay packets they had the responsibility to relay, blocking them and/or routing around them. Buchegger and Le Boudec took this one step further with the CONFIDANT protocol, which has nodes cooperatively propagate reputation information, thus

making misbehavior detected by one node available to the routing decision of others, but adds vulnerabilities to propagation of false accusations. More recent trust frameworks add fuzzy-logic-based trust estimation, such as combining wormhole, blackhole and DDoS indicators within a fuzzy inference system, and bio-inspired optimization, e.g., elephant-herding-optimization-based trust routing, to ensure that security and energy efficiency are taken into account. Some hybrid schemes that integrate trust estimation with machine learning like ML-AODV protocol, take parameters like hop count, residual energy, link expiration time as the criteria for trust to recognize the cooperative intermediate nodes and prevent flooding attack and blackhole attack.

Representative trust-management schemes are compared in Table 3 based on their trust measures, attack targets, evaluation methods, and reported results, which shows the progresses from behavioral monitoring to intelligent and optimization-based trust assessment

Table 3. Comparison of representative trust-management schemes for MANETs.

Scheme	Trust metric	Attacks mitigated	Evaluation approach	Reported outcome
Watchdog / Pathrater	Promiscuous overhearing of forwarding behavior	Selfish nodes, simple packet dropping	Simulation (ns-2 style)	Improved throughput by routing around misbehaving nodes; vulnerable to collusion
CONFIDANT	Cooperatively propagated reputation	Selfish and misbehaving nodes	Simulation	Faster reaction to misbehavior via reputation sharing; sensitive to false accusations
Fuzzy trust estimation	Fuzzy-logic combination of behavioral indicators	Wormhole, blackhole, DDoS	Simulation	Improved detection accuracy over single-metric trust models
Sec-BIO (bio-inspired trust)	Elephant-herding-optimization-based trust score	Blackhole, wormhole, flooding, unauthorized access	Simulation	Improved energy efficiency alongside security
GTAODV	Direct, indirect and global trust	Blackhole attack	NS-3 simulation	Demonstrated effectiveness against blackhole attacks relative to baseline AODV
ML-AODV	Hop count, residual energy, link expiration time	Flooding, blackhole	Simulation	Reduced unnecessary routing overhead and improved delivery ratio

4.2 Intrusion Detection System (IDS) Categories

MANET intrusion detection systems can be broadly classified into signature-based, where the observed traffic or routing behavior is matched to a database of known attack patterns and typically achieve high detection accuracy for known attacks, but are unable to detect new attacks; anomaly-based, where the system builds a statistical model of what should be considered normal behavior and marks deviations from that as suspicious, and thus potentially malicious, but often result in high false-positive rates; specification-based and zone-based, where the observed behavior is checked

against a formal specification of the protocol's correct behavior, and where the protocol behavior is monitored in a bounded zone of the network, respectively, to reduce the overhead of monitoring; and, more recently, machine-learning and deep-learning, which are trained directly from labelled or unlabelled traffic or routing features to distinguish between good and bad behavior.

Table 4 provides a summary on the most significant IDS classes employed in MANET security, which provides the reader with a comparison of the operating principles, advantages, limitations, and representative implementations.

Table 4. Comparison of intrusion detection system categories for MANETs.

IDS type	Operating principle	Advantage	Limitation	Representative example
Signature-based	Match against a database of known attack signatures	High accuracy and low false-positive rate for known attacks	Cannot detect novel/zero-day attacks	Rule-based misuse detection systems
Anomaly-based (statistical)	Flag significant deviation from a learned model of normal behavior	Can detect previously unseen attacks	Higher false-positive rate; requires reliable normal-behavior baseline	Statistical traffic-profile monitors
Specification / zone-based	Compare behavior against a formal specification of correct protocol operation, often within a bounded zone	Low false-positive rate; reduced monitoring overhead via zoning	Requires accurate, complete protocol specification	Modified zone-based IDS for AODV-style networks
Trust-based hybrid IDS	Combine behavioral trust scores with detection rules	Adapts to gradual/partial misbehavior (e.g., grayhole)	Convergence delay; vulnerable to badmouthing/collusion	Trust-augmented AODV variants
ML / DL-based	Learn discriminative or generative models from traffic/routing features	Can capture complex, non-linear attack patterns; adaptable via retraining	Requires representative training data; computational cost for training/inference	ANN, DNN, CNN-LSTM hybrid intrusion detectors

4.3 Machine-Learning and Deep-Learning-Based IDS

Since machine learning and deep learning are able to model complex, non-linear relationships between traffic and routing features that are hard to represent as fixed signatures or thresholds, an increasing number of recent works in MANET security research have focused on using these approaches to detect intrusions. Some classical machine learning classifiers like Naive Bayes, Decision Trees, Support Vector Machines (SVM), K Nearest Neighbours and Random Forests have been used to differentiate between benign and malicious nodes using features like packet-delivery ratio, route-request frequency, hop count and energy consumption. Recent studies have focused on artificial neural networks, deep neural networks, and hybrid models that integrate both CNN and RNN layers (such as CNN-LSTM) to model both spatial and temporal traffic dynamics. Although caution needs to be exercised when comparing performance of different techniques numerically across the various studies due to differences in the datasets, simulation environments, and attack

scenarios, it is clear that ensemble and deep-learning-based methods tend to achieve higher and more consistent detection accuracy at the expense of greater computation requirements for training and in some cases for performing the detection.

5. Comparative Analysis and Open Research Challenges

5.1 Key Reviewed Studies

Table 5 summarizes a representative sample of the literature surveyed in this paper from fundamental secure-routing protocols, attack specific surveys, and recent Defence protocols based on trust and machine learning.

Table 5. Summary of key studies reviewed in this paper.

Author(s) / Ref.	Focus area	Methodology	Key contribution
Zapata [7]	Secure routing	Digital signatures + hash chains over AODV	Proposed SAODV, one of the earliest secure extensions of AODV
Sanzgiri et al. [8]	Secure routing	Certificate-based per-hop authentication	Proposed ARAN, a certificate-based secure routing protocol
Hu, Johnson & Perrig [9]	Secure routing	One-way hash chains over distance-vector routing	Proposed SEAD for proactive secure routing
Hu, Perrig & Johnson [10]	Secure routing	Hash chains + per-hop MACs over DSR	Proposed Ariadne, a secure on-demand source routing protocol
Hu, Perrig & Johnson [11]	Wormhole Defence	Geographic/temporal packet leases	Introduced packet leases as a wormhole-attack countermeasure
Marti et al. [12]	Trust / misbehavior detection	Promiscuous-mode monitoring	Proposed the Watchdog and Pathrater mechanisms
Zhou & Haas [13]	Key management	Threshold cryptography	Proposed distributed certificate authority for ad hoc networks
Buchegger & Le Boudec [14]	Trust / reputation	Cooperative reputation propagation	Proposed the CONFIDANT protocol
Islabudeen & Devi [15]	Intrusion detection/prevention	Rule- and behavior-based hybrid IDPS	Proposed a smart IDPS for MANET routing attacks
Tahboush & Agoyi [16]	Wormhole detection	Hybrid detection technique	Proposed a hybrid wormhole-attack detection scheme
Shafi, Mounika & Velliangiri [17]	Trust-based / ML routing	Trust estimation + machine learning over AODV	Proposed ML-AODV to mitigate flooding and blackhole attacks
Momand, Jan & Ramzan [18]	IDS survey	Systematic literature review	Comprehensive survey of ML/DL-based IDS, datasets and attack taxonomy
Karthigha, Latha & Sripriyan [19]	Routing-attack survey	Literature review	Comprehensive survey of routing attacks in wireless

Author(s) / Ref.	Focus area	Methodology	Key contribution
			MANETs
Jari & Thomas [20]	Trust-based routing	NS-3 simulation of global trust AODV	Proposed GTAODV, incorporating direct, indirect and global trust

Overall, the literature reviewed revealed a positive rather than a negative relationship between the three major Defence families. Cryptographic and secure-routing mechanisms provide the highest level of guarantees against forgery, tampering, and impersonation but cannot prevent an authenticated node from acting maliciously, and require more computation on the most constrained nodes that may be hard to justify. Despite their ability to be fine-tuned to the energy and mobility patterns of a deployment, trust-management mechanisms are also subject to collusion, false-accusation (badmouthing), and slow convergence, especially in high-mobility scenarios where the history of interactions that the trust is based upon is ephemeral. For the set of attacks reported in the literature, IDSs based on machine learning or deep learning are the most accurate, and in principle can extend to variants of the known attacks, but are dependent on training data, have a high training cost and sometimes inference cost, and — like most learning-based systems — are opaque, making formal security assurances difficult. Most recent proposals (such as ML-AODV and GTAODV) mix elements of more than one family, that is, trust measures are either paired with cryptographic authentication or learned classifiers to obtain the right compromise between security, overhead, and adaptability.

5.2 Open Research Challenges

Despite two decades of active research, several challenges remain open in MANET security research and are summarized in Table 6. Table 6 summarizes the major open research challenges in MANET security and highlights potential directions for addressing these challenges.

Table 6. Open research challenges and potential future directions in MANET security.

Challenge	Description	Potential direction
Energy–security trade-off	Stronger cryptographic and monitoring mechanisms increase energy consumption on already resource-constrained nodes	Lightweight cryptography; adaptive/selective monitoring based on risk level
Scarcity of MANET-specific datasets	Most ML/DL IDS work relies on simulation traces or datasets built for wired/IoT networks rather than real ad hoc deployments	Community-shared, standardized MANET/VANET intrusion-detection benchmark datasets
Scalability under high mobility	Trust convergence and route re-establishment overhead grow with node count and mobility rate	Hierarchical/clustered trust and routing architectures
Collusion and coordinated attacks	Multiple colluding malicious nodes can defeat many single-node-focused trust and detection schemes	Group-behavior and graph-based anomaly detection
Integration with IoT / VANET / 5G-6G ecosystems	MANET principles increasingly underpin vehicular and IoT edge networks with additional constraints (e.g., high speed,	Cross-layer, context-aware security frameworks tailored to VANET/IoT mobility patterns

Challenge	Description	Potential direction
	heterogeneous devices)	
Adversarial machine learning	ML/DL-based IDS can themselves be evaded or poisoned by adversarially crafted traffic	Adversarially robust training and continuous model validation
Post-quantum readiness	Widely used public-key primitives in secure routing protocols are vulnerable to future quantum attacks	Lightweight post-quantum cryptographic primitives suited to constrained nodes
Privacy-preserving collaborative detection	Sharing trust/reputation or training data across nodes raises privacy concerns	Federated-learning-based collaborative IDS with local data retention
Real-world validation	Most proposed schemes are validated only in simulation (NS-2/NS-3), with limited testbed or field deployment evidence	Larger-scale physical testbeds and standardized evaluation protocols

Conclusion

This paper provides an extensive survey of security issues and solutions in MANETs. The analysis showed that the intrinsic features of MANETs such as decentralized operation, dynamic topology, open wireless communication, constraints on node resources and reliance on cooperative forwarding, contribute to a wide and constantly changing attack surface. A layer-wise taxonomy was presented which encompassed physical, MAC, network, transport, and application-layer threats and offered a structured perspective of representative attacks and their implications on the aspects of confidentiality, integrity, availability, routing reliability, and network lifetime. Three major categories of security mechanisms were then investigated in the review: cryptographic and secure-routing approaches, trust-management mechanisms and intrusion detection techniques. Secure routing protocols offer good protection against routing-message forgery, tampering, impersonation and unauthorized updates, but they are often computationally and communication intensive and thus may be unsuitable for resource-limited, highly mobile nodes. IDS approaches using ML and DL have a higher ability to learn complex and nonlinear attack pattern and can potentially detect variations of known attacks. However, they are highly reliant on representative training data and their computational needs and interpretability are still concerns.

The overall results show that there is no single security mechanism which is the best solution for MANETs. Rather, literature has been moving towards hybrid architectures, where complementary approaches can be merged, such as cryptographic authentication for message integrity and identity verification, trust management for behavior assessment and ML / DL based IDS for adaptive attack detection. This kind of integration can offer a better trade-off between security, detection capabilities, adaptability, power usage, and communication overhead. There are a number of research gaps. It encompasses the energy-security trade-off, the lack of realistic MANET-specific datasets, the scalability with high mobility, coordinated/colluding attacks, integration with VANET/IoT/5G-6G environments, adversarial machine learning, post-quantum cryptography, privacy-preserving collaborative detection, and limited real-world validation of proposed solutions. The paper thus calls for lightweight, adaptive, context-aware and experimented validated security frameworks using standard datasets and physical large scale testbeds.

References

- [1] A. A. Korba, M. Nafaa, and G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks," presented at the International Conference on Computer and Information Technology (CIT), Chengdu, China, Apr. 2013.
- [2] R. Meddeb, B. Triki, F. Jemili, and O. Korbaa, "A Survey of Attacks in Mobile Ad Hoc Networks," in Proc. International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, 2017, pp. 1–7.
- [3] S. Agrawal, S. Jain, and S. Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," arXiv:1105.5623, 2011.
- [4] M. S. Sheikh, J. Liang, and W. Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, vol. 19, no. 16, Art. no. 3589, 2019.
- [5] T. K. Saini and S. C. Sharma, "Recent Advancements, Review Analysis, and Extensions of the AODV With the Illustration of the Applied Concept," *Ad Hoc Networks*, vol. 103, Art. no. 102148, 2020.
- [6] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," *Sensors*, vol. 23, no. 5, Art. no. 2415, 2023.
- [7] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106–107, 2002.
- [8] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in Proc. 10th IEEE International Conference on Network Protocols (ICNP), Paris, France, 2002, pp. 78–87.
- [9] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," in Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 2002, pp. 3–13.
- [10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in Proc. 8th Annual International Conference on Mobile Computing and Networking (MobiCom), Atlanta, GA, USA, 2002, pp. 12–23.
- [11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks," in Proc. IEEE INFOCOM, San Francisco, CA, USA, 2003, pp. 1976–1986.
- [12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proc. 6th Annual International Conference on Mobile Computing and Networking (MobiCom), Boston, MA, USA, 2000, pp. 255–265.
- [13] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.
- [14] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," in Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, Switzerland, 2002, pp. 226–236.
- [15] M. Islabudeen and M. K. Devi, "A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad hoc Networks Against Security Attacks," *Wireless Personal Communications*, vol. 112, no. 1, pp. 193–224, 2020.
- [16] M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-hoc Network (MANET)," *IEEE Access*, vol. 9, pp. 11872–11883, 2021.
- [17] S. Shafi, S. Mounika, and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," *Procedia Computer Science*, vol. 218, pp. 2309–2318, 2023.
- [18] A. Momand, S. Jan, and N. Ramzan, "A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy," *Journal of Sensors*, vol. 2023, Art. no. 6048087, 2023.

- [19] M. Karthigha, L. Latha, and K. Sripriyan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," in Proc. 5th International Conference on Intelligent Computing and Control Systems (ICICT), 2020, pp. 396–402.
- [20] H. Jari and N. Thomas, "Performance Evaluation of Global Trust Management in MANETs Routing Protocols," in Computer Performance Engineering and Stochastic Modelling: Proc. 19th European Performance Engineering Workshop (EPEW 2023), 2023, pp. 383–397.