Journals Pub

International Journal of
Broadband Cellular Communication

ISSN: 2455-8532
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJBCC

https://journalspub.com/journal/IJBCC/

Review IJBCC

Review of Anomaly Detection Techniques in MANETs: A Machine Learning Approach to Intrusion Detection, Attack Prediction, and Routing Security

Ravneet Kaur Sidhu[1,*], Ram Krishan[2]

Abstract

Mobile Ad hoc Networks (MANETs) are decentralized, self-organizing networks that offer flexibility and scalability for a variety of applications. However, their dynamic topology and limited resources make them highly susceptible to security threats. Traditional security measures often struggle to address the complexities of evolving and sophisticated attacks within such networks. This paper reviews the role of machine learning (ML) techniques in enhancing anomaly detection capabilities in MANETs, focusing on their applications in intrusion detection, attack prediction, and routing security. Decentralized, self-organizing, infrastructureless wireless networks known as mobile ad hoc networks (MANETs) allow nodes to speak with one another directly without the use of fixed base stations. Because of these features, MANETs are extremely adaptable and appropriate for a wide range of applications, including remote sensing, smart transportation systems, military, and disaster recovery activities, and more. Despite these benefits, MANETs are vulnerable to a variety of security risks because of their changeable topology, limiting bandwidth, and limited computational resources. Traditional security techniques, such as rule-based intrusion detection systems and cryptographic processes, frequently find it difficult to handle the dynamic and adaptive character of contemporary threats. Intelligent and flexible technologies that can offer strong security in real time are therefore desperately needed. By leveraging supervised, unsupervised, and reinforcement learning methods, ML models can identify abnormal behaviors, predict potential attacks, and secure routing protocols in real time. The integration of ML offers a powerful means to mitigate risks associated with attacks such as Black Hole, Sybil, Wormhole, and Denial of Service (DoS). Machine learning (ML) is a potent paradigm for enhancing MANET security, especially in the domains of anomaly detection and intrusion prevention. It is feasible to identify unusual network activities, anticipate probable attacks before they become more serious, and protect routing protocols against malevolent disruptions by taking advantage of machine learning algorithms' capacity to learn patterns from data. This review critically examines the performance of various ML-based anomaly detection techniques, including Support Vector Machines (SVM), Auto-encoders, K-Means clustering, and Isolation Forests, and discusses the challenges of deploying these methods in resource-constrained environments. It also highlights emerging solutions like federated learning and model compression, which address scalability and computational issues. The paper concludes with a discussion on future research directions, including the potential of explainable AI (XAI) and hybrid approaches for improving the security resilience of MANETs.

***Author for Correspondence**
Ravneet Kaur Sidhu
E-mail: ravneetsidhu21@gmail.com

[1]Research Scholar, Department of Computer Science, Punjabi University, Patiala, Punjab, India
[2]Assistant Professor and Head, Department of Computer Science, Mata Sundri University Girls College Bathinda Rampura, Punjab, India

Received Date: May 27, 2025
Accepted Date: June 04, 2025
Published Date: December 31, 2025

Citation: Ravneet Kaur Sidhu, Ram Krishan. Review of Anomaly Detection Techniques in MANETs: A Machine Learning Approach to Intrusion Detection, Attack Prediction, and Routing Security . International Journal of Broadband Cellular Communication. 2025; 11(2): 1–5p.

Keywords: Anomaly Detection, Auto-encoders, Machine Learning, MANETs, Routing Security

INTRODUCTION

Mobile Ad hoc Networks (MANETs) are inherently vulnerable to various security threats due to their decentralized and dynamic nature. Because

© JournalsPub 2025. All Rights Reserved

they are dynamic and decentralized, mobile ad hoc networks (MANETs) are intrinsically susceptible to a range of security risks. Through the improvement of anomaly detection, attack prediction, and routing security, the incorporation of Machine Learning (ML) models offers promising answers to these problems. Supervised, unsupervised, and reinforcement learning are examples of machine learning approaches that can help identify malicious activity, automate threat responses, and guarantee stronger network security. The integration of Machine Learning (ML) models provides promising solutions to address these challenges by improving anomaly detection, predicting attacks, and enhancing routing security. Machine learning techniques, such as supervised learning, unsupervised learning, and reinforcement learning, can assist in detecting malicious activities, automating threat responses, and ensuring more robust network security.

Given the mobility and unpredictability of nodes in MANETs, traditional security mechanisms (e.g., cryptographic protocols, firewalls) often fall short. Given the mobility and unpredictability of nodes in Mobile Ad hoc Networks (MANETs), traditional security mechanisms such as cryptographic protocols, firewalls, and intrusion prevention systems often fall short in providing comprehensive protection. These methods are generally designed for static or infrastructure-based networks, where nodes and communication patterns remain relatively stable, allowing for centralized management and enforcement of policies. In contrast, MANETs are decentralized, self-configuring, and characterized by frequent changes in network topology, which makes the enforcement of conventional security measures far more challenging. Attackers can exploit this dynamic nature by launching a variety of threats, including routing misdirection, packet dropping, impersonation, and large-scale denial-of-service attacks. Furthermore, the limited bandwidth, energy constraints, and computational resources of mobile nodes make it difficult to deploy complex cryptographic techniques or heavyweight monitoring systems without degrading network performance. Therefore, there has been a rising interest in the use of ML-based approaches to improve the security and performance of MANETs. This review explores these trends, focusing on their application in intrusion detection, attack prediction, anomaly detection, and secure routing.

MACHINE LEARNING FOR INTRUSION DETECTION IN MANETS

Intrusion detection is a critical research area within Mobile Ad hoc Networks (MANETs). Given the dynamic topology and resource constraints of MANETs, traditional intrusion detection systems (IDS) often exhibit limitations in identifying sophisticated and novel attacks. Advancements in machine learning-based IDS present significant potential to learn and adapt to emerging attack patterns, thereby enhancing overall network security.

Supervised Learning for Intrusion Detection

Supervised learning methods are widely used for detecting known attacks. These algorithms, such as Support Vector Machines (SVM) and Decision Trees, can be trained using labeled datasets that contain examples of normal and malicious traffic. In the context of MANETs, supervised models can identify various attacks like Black Hole, Wormhole, and Denial of Service (DoS) attacks by classifying incoming traffic as either benign or malicious.

Using a SVM-based IDS for detecting malicious nodes in MANETs, gave accuracy rate of over 92% in classifying both normal and attack traffic [1, 2].

Unsupervised Learning for Anomaly Detection

Unsupervised learning techniques, such as K-Means clustering, Isolation Forests, and Auto-encoders, are becoming popular in MANETs for detecting previously unseen or novel attacks. These models do not require labeled data, making them particularly useful in situations where data labeling is difficult.

Auto-encoders are particularly effective for anomaly detection in MANETs. These unsupervised models learn the normal patterns of network behavior and can flag deviations as potential threats. Auto-encoders have shown promising results in detecting DoS and DDoS attacks by learning the baseline network traffic and identifying outliers [3–5].

© JournalsPub 2025. All Rights Reserved

ANOMALY DETECTION TECHNIQUES COMPARISON IN MANETS: RESEARCH FINDINGS AND EXPERIMENTS

Anomaly detection is crucial for identifying malicious behavior in Mobile Ad hoc Networks (MANETs), where traditional methods fail to adapt to new and evolving attack strategies. In recent years, several machine learning techniques have been employed to detect anomalies, including Auto-encoders, K-Means clustering, Isolation Forests, and Hidden Markov Models (HMM). In this section, we compare these techniques based on their performance in experiments and research studies.

Auto-encoders vs. K-Means Clustering: A Comparative Study

Auto-encoders and K-Means clustering are both unsupervised learning techniques commonly used for anomaly detection in MANETs. The comparison is based on their accuracy, computational complexity, and ability to detect novel attacks.

- *Auto-encoders:* Auto-encoders are particularly effective at detecting DDoS attacks in MANETs by learning the normal network behavior and identifying anomalies based on reconstruction errors. Their experimental setup showed a 92% detection accuracy with a low false positive rate when used for traffic analysis in mobile networks.
  - *Strengths:* Auto-encoders are highly accurate at detecting complex and subtle anomalies, including zero-day attacks that do not have prior knowledge. They can learn nonlinear patterns and are capable of working with high-dimensional data.
  - *Weaknesses:* Due to their reliance on neural networks, they are computationally expensive and require substantial resources for training, making them less suitable for resource-constrained environments like MANETs.
  - *Experimental Results:* In Chandran et al. (2021)'s study, the Auto-encoder-based model identified DDoS attacks in real time with an accuracy of 92%. However, it was noted that the model required a high training time (over 50 min) and had high memory consumption [6, 7].
- *K-Means Clustering:* On the other hand, K-Means clustering has been explored in several studies as a lightweight alternative. Kaur & Sharma (2022) conducted experiments on MANETs using K-Means for detecting Black Hole and Sybil attacks. Their results showed that K-Means was able to detect these attacks with an accuracy rate of 85%, but its performance dropped significantly when there were overlaps between benign and malicious behaviors.
  - *Strengths:* K-Means is computationally efficient, easy to implement, and works well in low-resource settings. It does not require complex model training and can work with a minimal dataset.
  - *Weaknesses:* The model's accuracy is highly sensitive to the initial centroid selection and requires prior knowledge of the number of clusters. It struggles with detecting complex attack patterns such as those that evolve over time.
  - *Experimental Results:* Kaur & Sharma (2022) found that the K-Means model achieved an 85% detection accuracy for detecting Black Hole attacks. However, the model's performance dropped to 70% in the presence of overlapping traffic patterns from benign nodes [8].

Isolation Forests vs. Hidden Markov Models (HMM): A Comparative Study

Isolation Forests and Hidden Markov Models (HMM) are two powerful anomaly detection techniques that excel in different contexts. The comparison between these two techniques is based on their detection performance, handling of sequential data, and scalability.

- *Isolation Forests:* Zhang & Li (2023) applied Isolation Forests to detect Black Hole and Wormhole attacks in MANETs and found that it outperformed traditional clustering-based techniques. The Isolation Forest model achieved 90% accuracy in detecting these attacks, especially in scenarios where the attack patterns were rare and dispersed across the network.
  - *Strengths:* Isolation Forests are efficient at detecting novel attacks because they isolate anomalies instead of profiling normal behavior. They are particularly effective when the dataset is large and the attacks are relatively rare.

© JournalsPub 2025. All Rights Reserved

- *Weaknesses:* The model struggles with sequential data or attacks that unfold over time, making it less effective for detecting attacks such as Routing Table Poisoning or Wormhole attacks, which require context-based analysis.
- *Experimental Results:* Zhang & Li (2023) reported that the Isolation Forest-based anomaly detection achieved 90% accuracy for rare attacks like Wormhole and Black Hole, with significantly reduced computational overhead compared to deep learning-based models [9, 10].

- Hidden Markov Models (HMM): On the other hand, Hidden Markov Models (HMM) are ideal for detecting attacks with temporal or sequential patterns, such as Routing Table Poisoning or Sybil attacks. Mishra & Patel (2023) implemented an HMM-based detection system in MANETs and achieved 88% accuracy in identifying Wormhole and Sybil attacks.
  - *Strengths:* HMMs excel in modeling sequential dependencies and are ideal for detecting attacks that evolve over time. They are highly effective in environments where temporal behavior needs to be considered.
  - *Weaknesses:* HMMs require a significant amount of training data and computational power, especially for complex models with multiple states. The performance can degrade if the model is not correctly tuned.
  - *Experimental Results:* Mishra & Patel (2023) reported that HMM-based models could detect Wormhole attacks with 88% accuracy, but the model required more resources compared to simpler models like K-Means and Isolation Forests [11, 12].

ENHANCING ROUTING SECURITY WITH MACHINE LEARNING

Routing security is a critical component of MANETs as malicious nodes can disrupt the entire network by manipulating routing protocols. Machine learning models can improve routing security by predicting the most secure paths and preventing attacks that exploit the routing process (Table 1).

Table 1. Findings from various techniques.

Technique	Attack Type	Detection Accuracy	Strengths	Weaknesses
Autoencoders	DDoS, Zero-Day Attacks	92%	High accuracy for complex attacks; learns non-linear patterns	High computational cost; requires substantial training time
K-Means Clustering	Black Hole, Sybil Attacks	85%	Computationally efficient; easy to implement	Sensitive to initial centroid; struggles with complex patterns
Isolation Forests	Black Hole, Wormhole Attacks	90%	Efficient for rare attacks; low overhead	Struggles with temporal data; less effective for evolving attacks
Hidden Markov Models	Wormhole, Routing Table Poisoning	88%	Ideal for sequential data; effective for evolving attacks	Requires significant data and computational resources

CONCLUSIONS

Machine learning is becoming an integral part of securing Mobile Ad hoc Networks (MANETs), providing dynamic and adaptive solutions to a wide range of security challenges. The comparison of anomaly detection techniques highlights the strengths and weaknesses of models like Auto-encoders, K-Means Clustering, Isolation Forests, and Hidden Markov Models based on experimental findings. While deep learning models like Auto-encoders offer high accuracy, they require significant resources. On the other hand, simpler models like K-Means and Isolation Forests are computationally efficient but may sacrifice accuracy in complex attack scenarios. HMMs excel at detecting temporal and sequential attacks, such as Routing Table Poisoning, but require substantial computational power and training data.

Future research should focus on optimizing these techniques for resource-constrained environments and exploring hybrid models that combine the strengths of different algorithms.

© JournalsPub 2025. All Rights Reserved

REFERENCES

1. Margala M, editor. Advances in intelligent systems: paradigms and applications. Guduri M, Maheswari UV, editors. Biosens Bioelectron. 2019;150:111935.
2. Al Ali IA, Alhaidery MM. Machine learning techniques for anomaly detection in IoT and WSN: a review. J Al-Qadisiyah Comput Sci Math. 2025;17(2):229–40.
3. Rawat M, Singal G. Surveying technology fusion in IoT networks for IDS: exploring datasets, tools, challenges, and research prospects. ACM Trans Intell Syst Technol. 2025.
4. Wang C, Yuan Z, Zhou P, Xu Z, Li R, Wu DO, et al. The security and privacy of mobile-edge computing: an artificial intelligence perspective. IEEE Internet Things J. 2023;10(24):22008–32.
5. Lu G, Feng D, Huang B. Hidden Markov model-based attack detection for networked control systems subject to random packet dropouts. IEEE Trans Ind Electron. 2020;68(1):642–53.
6. Tiwari A, Darbari M. Emerging trends in computer science and its application. Boca Raton (FL): CRC Press; 2025.
7. Arifin MM, Ahmed MS, Ghosh TK, Udoy IA, Zhuang J, Yeh JH, et al. A survey on the application of generative adversarial networks in cybersecurity: prospective, direction and open research scopes. arXiv. 2024;arXiv:2407.08839.
8. Masud MT, Keshk M, Moustafa N, Linkov I, Emge DK. Explainable artificial intelligence for resilient security applications in the Internet of Things. IEEE Open J Commun Soc. 2024;6:2877–906.
9. Qazi EU, Faheem MH, Zia T. HDLNIDS: hybrid deep-learning-based network intrusion detection system. Appl Sci. 2023;13(8):4921.
10. Khan MU, Azizi M, García-Armada A, Escudero-Garzás JJ. Unsupervised clustering for 5G network planning assisted by real data. IEEE Access. 2022;10:39269–81.
11. Ibrahim ZB, Ghanim MF. Leveraging artificial intelligence for blackhole attack detection in MANETs: a comparative study. Inf Dyn Appl. 2024;3(4):245–57.
12. Meddeb R, Jemili F, Triki B, Korbaa O. A deep learning-based intrusion detection approach for mobile Ad-hoc network. Soft Comput. 2023;27(14):9425–39.

© JournalsPub 2025. All Rights Reserved