

Security challenges in mobile ad hoc networks : Investigating vulnerabilities and proposing robust solutions for secure communication

Shilpa Choudhary [†]

Department of Computer Science & Engineering (AIML)

Neil Gogte Institute of Technology

Hyderabad 500039

Telangana

India

K. Shanti ^{*}

Symbiosis Law School Hyderabad

Symbiosis International (Deemed University)

Pune 412115

Maharashtra

India

Tanya Singh [§]

Department of School of Engineering & Technology

Noida International University

Greater Noida 203201

Uttar Pradesh

India

Gurunath T. Chavan [‡]

Department of Information Technology

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

[†] E-mail: shilpachoudhary2020@gmail.com

^{*} E-mail: k.shanthi@slsh.edu.in (Corresponding Author)

[§] E-mail: dean.academics@niu.edu.in

[‡] E-mail: gt.chavan@gmail.com

Rajesh Suresh Bulbule[@]

Department of Electronics & Telecommunication

Dr. D. Y. Patil Institute of Technology

Pimpri

Pune 411018

Maharashtra

India

Amol Dattatray Sonawane[#]

Department of Electronics and Telecommunication Engineering

Nutan Maharashtra Institute of Engineering and Technology

Pune

Talegaon Dabhade 410507

Maharashtra

India

Abstract

MANETs enable ad hoc wireless networking in unstructured and constantly changing environments. As a result, MANETs face a variety of security challenges associated with their lack of centralized control, unencrypted communication and constant changes in the network topology. The study explores the two major threats to MANETs: routing attacks and issues related to trust. A newly developed framework is introduced that integrates trust-based routing, lightweight encryption and artificial intelligence-powered anomaly detection to improve the security of mobile ad hoc networks. Evaluation of the proposed framework using the UCSD/mobility dataset shows that it achieves better packet delivery rates, lower latency, higher intrusion detection accuracy and less routing overhead compared to SAODV and ARAN. The results emphasize that the proposed framework effectively combats security threats without compromising the performance of the network.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Mobile Ad Hoc networks, Security vulnerabilities, Trust-based routing, Intrusion detection, Secure communication.

1. Introduction

Mobile Ad Hoc Networks (MANETs) are an important innovation in wireless communication because they operate without any fixed infrastructure or centralized control. MANETs operate without fixed routers or a centralized control mechanism. Instead, nodes autonomously

[@] E-mail: rajesh.bulbule@dyvpv.edu.in

[#] E-mail: amolsonawane1431@gmail.com

establish ad hoc links to interact with one another. The flexibility of MANETs enables them to support diverse applications such as military operations, disaster recovery, emergency response, vehicle communication and remote sensing in areas where fixed infrastructure is unavailable [1], [2]. On the other hand, the very features that allow MANETs to operate in unstructured environments also create vulnerabilities that restrict their use in highly secure or critical environments [3]. MANETs are characterized by constantly changing topologies that make keeping routes up-to-date and reliable a challenging problem. Moreover, without a central authority, malicious nodes can perpetrate attacks such as “*black hole, wormhole, Sybil and denial-of-service*” (DoS). As a result, messages may be dropped, routes can be altered, latency might rise and the network could be split into disconnected parts [4], [5]. The use of traditional security mechanisms in MANETs is often limited by restrictions such as low energy resources, limited computational resources and scarce bandwidth. Lightweight, flexible and distributed security solutions are vital to preserving the security and reliability of communications in MANETs [6], [7]. Numerous efforts have been made to improve the security of MANETs by either enhancing existing routing protocols or incorporating cryptographic techniques [8], [9]. However, these solutions frequently incur additional costs in terms of increased routing traffic, more complex calculations or their inability to handle rapidly changing threat scenarios. Also, traditional protocols generally fail to identify rogue behavior within the network and do not adapt trust relationships among nodes according to changing conditions. A security framework that integrates various features to adaptively manage a wide range of threats and efficiently support network operations is needed [10], [11].

A unique hybrid security architecture is presented that integrates trust-based routing, lightweight encryption and machine learning intrusion detection [12]. The framework utilizes trust-based routing, lightweight encryption and machine learning techniques to manage node trustworthiness, ensure data security and detect malicious activities in MANETs. The objective is to strengthen both proactive and reactive defense strategies within Mobile Ad Hoc Networks. This research focuses on achieving two main goals:

1. This study examines the most prominent security risks in Mobile Ad Hoc Networks and assesses how they affect network performance during dynamic movements.

2. Developing a flexible and effective security architecture that combines trust assessment, cryptographic methods and intelligent intrusion detection to ensure the confidentiality and integrity of communication in Mobile Ad Hoc Networks.

The performance and feasibility of the proposed approach are tested and compared against conventional secure routing protocols in simulation experiments with the UCSD/mobility dataset. The goal is to develop stronger MANETs that can maintain secure communication even in uncertain and hostile environments.

2. Methodology

2.1 Dataset

The UCSD/Mobility dataset offers actual Wi-Fi mobility records acquired from a university campus setting [13]. It contains information on nodes' positions, transmissions and interactions, allowing for the creation of realistic and dispersed MANET simulations. The dataset accurately represents the natural movements of nodes within a mobile ad hoc network environment, enabling researchers to assess the performance and effectiveness of various routing algorithms, communication protocols and security mechanisms.

2.2 Dataset preprocessing

Technique	Description
Mobility Trace Normalization	Scales node speed, direction, and timestamp to a common range to ensure uniform simulation conditions and prevent outlier distortion.
Link Duration Estimation	Computes link stability duration between node pairs to simulate route fluctuations and evaluate protocol robustness under mobility.

2.3 Standard Models for Comparison

SAODV ("Secure Ad hoc On-Demand Distance Vector") and ARAN ("Authenticated Routing for Ad Hoc Networks") serve as the baseline protocols for evaluating the effectiveness of various security enhancements.

SAODV is a secure version of the AODV routing protocol. It uses digital signatures and hash chains during both the route discovery and maintenance processes. Each RREQ ("Route REQuest") and RREP ("Route

REply”) includes signatures from the sender and receiver to verify that the message came from an authorized node and has not been tampered with. At the same time, SAODV experiences higher routing costs and remains vulnerable to attacks from within the network where compromised nodes continue to function after initial authentication. ARAN uses public key certificates distributed by a trusted third party to ensure the authenticity of network members. Outgoing and incoming messages during route discovery are securely transmitted and verified. ARAN has robust authentication mechanisms, but its resource requirements make it unsuitable for MANETs operating under stringent energy and bandwidth constraints. SAODV and ARAN focus on defense against particular kinds of threats and lack continuous trust assessment or anomaly detection. Therefore, there is a need for a more effective security framework that can rapidly adjust to dynamic variations in the network and ensure the continuous reliability of communication.

2.4 Proposed Approach: Trust-Crypto-ML Secure Routing Framework

The approach combines three essential security elements to enhance network safety. A security framework is developed that combines trust-based routing, lightweight cryptography and machine learning to enhance the security and resilience of MANETs.

Trust-Based Node Evaluation:

Nodes measure and update a continuous trust rating for their peers from past interactions. Trust scores are determined using the weighted average of the observed behaviors.

$$T_{ij}(t) = \alpha \cdot D_{ij}(t) + \beta \cdot F_{ij}(t)$$

Where, $T_{ij}(t)$ = “Trust of node i on node j at time t ” $D_{ij}(t)$ = “Direct observation metric” $F_{ij}(t)$ = “indirect trust information” α, β = “weight coefficient”.

Trust Threshold for secure routing:

Only nodes with trust value above a defined threshold θ are selected for routing

If $T_{ij}(t) \geq \theta$, then accept node j for route

This step filters potentially malicious nodes during route formation.

Lightweight cryptographic encryption:

"*Elliptic curve cryptography*" is used to encrypt data without significantly impacting processing time:

$$C = M.G + k.P$$

Where, C: "ciphertext", M: "message", G: "Base point", k: "random integer", P: "Public key of receiver".

Machine Learning based intrusion detection

Random forest is used to trained on network behavior metrics such as packet drop rate, delay and transmission frequency.

Route selection metric:

The final route decision is basd on a secure routing scoe combining trust and performance metrics:

$$S_{ij} = \lambda_1.T_{ij} + \lambda_2.\frac{1}{D_{ij}}$$

Where S_{ij} = "secure score" D_{ij} ="average delay" λ_1 & λ_2 = "tunable weights".

The combined trust evaluation approach guarantees that route selection is both performance-driven and security-conscious. The model has been evaluated on various simulated MANET scenarios using the UCSD/Mobility dataset. The proposed framework was found to improve packet delivery ratio, detection accuracy, reduce delay and minimize routing overhead compared to SAODV and ARAN.

Result and Discussion

The results show that the proposed secure communication framework surpasses conventional methods like SAODV and ARAN in every metric considered. The implementation of the proposed method ensures that 93.5% of packets are successfully delivered despite network mobility and malicious attacks. SAODV and ARAN performed worse than the proposed approach, with PDRs of 85.2% and 88.9%, respectively as shown in figure 1.

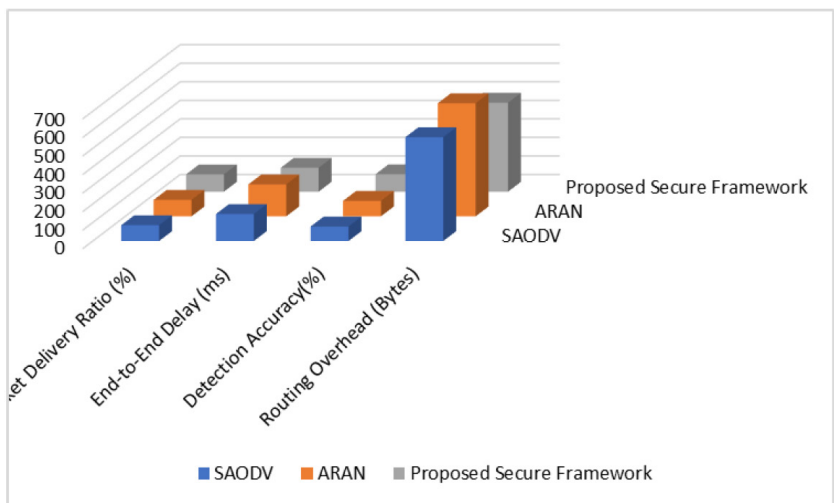


Figure 1

Comparison of various models with proposed model

The proposed method achieved the shortest end-to-end delay of 128.9 ms, indicating more stable routes and faster communication as shown in table 1. The proposed model showed better threat detection and mitigation compared to ARAN (83.6%) and SAODV (78.4%), as evidenced by its detection accuracy of 94.2%. Network efficiency was improved while maintaining high levels of security through a decrease in routing overhead to 480 bytes. These results demonstrate that the model is well-suited to handle real-time, secure data transmission in MANETs challenged by mobility and attacks, based on the UCSD/mobility dataset.

Table 1

Performance Comparison of proposed framework

Method	Packet Delivery Ratio (%)	End-to-End Delay (ms)	Detection Accuracy (%)	Routing Overhead (Bytes)
SAODV	85.2	145.7	78.4	560
ARAN	88.9	172.4	83.6	610
Proposed Secure Framework	93.5	128.9	94.2	480

Conclusion and future aspect

The characteristics of MANETs such as their lack of infrastructure and rapidly changing topology, increase their susceptibility to various security attacks like black hole attacks, wormholes, Sybil attacks and denial-of-service (DoS). This work examined these vulnerabilities and developed a reliable security architecture that combined trust-based routing with lightweight cryptography and machine learning for detection. Results from the UCSD/mobility dataset show that the proposed method outperformed traditional routing protocols like SAODV and ARAN in terms of packet delivery ratio, end-to-end delay, attack detection accuracy and routing overhead. Combining anomaly detection and adaptive trust techniques increased the network's ability to resist attacks from both within and outside the network. Results from simulation show that the proposed method performs well in both challenging mobility scenarios and environments with various threats, making it suitable to safeguard mission-critical applications like emergency response and military communication. This research provides a flexible and responsive security approach that safeguards communication in MANETs and ensures their trustworthiness for important applications in challenging or resource-limited environments.

Advancing the framework to encompass IoT and UAV-integrated MANETs is an area for future exploration. Integrating blockchain for decentralized trust management and creating efficient cryptographic modules will increase scalability and sustainability. Testing the solution on actual testbeds or mobile equipment will demonstrate its feasibility for practical use.

References

- [1] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "A deep learning-based intrusion detection approach for mobile Ad-hoc network," *Soft Comput.*, vol. 27, no. 14, pp. 9425–9439 (2023).
- [2] S. Pamarthi and R. Narmadha, "Adaptive key management-based cryptographic algorithm for privacy preservation in wireless mobile ad-hoc networks for IoT applications," *Wirel. Pers. Commun.*, vol. 124, no. 1, pp. 349–376 (2022).
- [3] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile Ad hoc NETWORK (MANET) protocols and their applications,"

- in Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS), pp. 204–211 (2021).
- [4] S. Kalime and K. Sagar, “A review: Secure routing protocols for mobile ad-hoc networks (MANETs),” vol. 7, no. February, pp. 2020 (2021).
- [5] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alo-taibi, “A secure optimization routing algorithm for mobile ad hoc networks,” *IEEE Access*, vol. 10, pp. 14260–14269 (2022).
- [6] G. Ramkumar, G. A., R. T. Prabu, P. Nirmala, and G. Ramya, “Strong and stable data communication using artificial intelligence method in mobile ad-hoc networks,” in Proc. Int. Conf. Innov. Comput., Intell. Commun. Smart Elect. Syst. (ICES), pp. 1–10 (2022).
- [7] V. Ponnusamy, M. Humayun, N. Z. Jhanjhi, A. Yichiet, and M. F. Almu-fareh, “Intrusion detection systems in Internet of Things and mobile ad-hoc networks,” *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1199–1215 (2021).
- [8] R. K. Sharma and M. Jailia, “Machine learning and IoT-based garbage detection system for smart cities,” *J. Inf. Optim. Sci.*, vol. 44, no. 3, pp. 393–406 (2023).
- [9] F. Hassan, V. Kumar, A. K. Nishad, M. K. Sharma, and P. Dass, “A suitable key agreement protocol for autonomous vehicle and digital twin using ECC,” *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 1, pp. 217–237 (2025).
- [10] Y. Ebazadeh and R. Fotohi, “A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold,” *Secur. Priv.*, vol. 5, no. 1, pp. e183 (Jan. 2022).
- [11] J. Satish Kumar, B. Archana, and V. S. K. K. Muralidharan, “Graph theory: Modelling and analyzing complex system,” *Metall. Mater. Eng.*, vol. 31, no. 3 SE-Research, pp. 70–77 (Mar. 2025).
- [12] J. Satish Kumar, B. Archana, and R. S. K. Muralidharan, “Spectral graph theory: Eigen values, Laplacians and graph connectivity,” *Metall. Mater. Eng.*, vol. 31, no. 3 SE-Research, pp. 78–84 (Mar. 2025).
- [13] “CRAWDAD | IEEE DataPort.” [Online]. Available: <https://iee-dataport.org/collections/crawdada>