IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Dynamic Trust and Attack-Resilient Routing in MANET Using Multiobjective Optimization and Reinforcement Learning

Mr. Thangadurai K[1], Sarathi S[2], Sanjai S[3], Sasikumar V[4], Sarathi M[5]
Assistant Professor, Computer Science and Engineering[1]
Students, Computer Science and Engineering[2-5]
Mahendra Institute of Engineering and Technology, Namakkal, India

Abstract: *Mobile ad hoc networks (MANETs) face significant challenges in maintaining secure and efficient communication owing to their dynamic nature and vulnerability to security threats. Traditional routing protocols often struggle to adapt to rapidly changing topologies and potential malicious nodes, compromising network performance and security. This study addresses these challenges by proposing FLSTMT-LAR (Federated Learning Long Short-Term Memory Trust-aware Location-aided Routing), a novel framework that integrates multiobjective optimization with LSTM-based trust prediction for robust routing decisions, implements a decentralized federated learning mechanism for collaborative trust model updates while preserving node privacy, incorporates dynamic trust assessment using LSTM networks for accurate temporal behavior pattern analysis, and provides an adaptive routing decision mechanism that effectively balances multiple performance objectives including trustworthiness, energy efficiency, and network latency. We evaluate this framework against existing protocols across various scenarios, including different network densities, mobility patterns, and malicious node percentages. Results demonstrate FLSTMT-LAR's superior performance in high-threat environments, achieving up to 80% packet delivery ratio compared with 45% for traditional approaches. In mobile scenarios, it shows improved adaptability, maintaining consistent performance as network density increases. MOO, particularly nondominated sorting genetic algorithm III, effectively balances conflicting network objectives, offering a 15% improvement in overall network performance compared with single-objective approaches. These findings highlight the potential of integrating advanced machine learning and optimization techniques in MANET routing protocols, paving the way for secure, efficient, and adaptive network communications in challenging environments*

Keywords: Mobile ad hoc networks

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have garnered significant attention given their self-configuring, infrastructure-less nature, making them indispensable in various applications, such as military communications, disaster recovery, and mobile sensing Unlike traditional networks,

The associate editor coordinating the review of this manuscript and approving it for publication was Nurul I. Sarkar .

MANETs do not rely on fixed infrastructure instead, they consist of mobile nodes that communicate with one another over a wireless link This flexibility enables rapid deployment and reconfiguration, which is particularly beneficial in scenarios in which conventional network infrastructure is either impractical or unavailable However, the very characteristics that make MANETs attractive also introduce significant challenges, specifically in terms of ensuring secure and reliable communication; one of the primary concerns in MANETs is the variability in the trustworthiness of network nodes because the dynamic topology and lack of centralized control make malicious behavior difficult to detect and mitigate.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

II. LITERATURE SURVEY

This literature survey provides a focused examination of two key areas that are crucial to our research on enhancing MANET security and performance. The survey is structured into two main subsections. First, we explore FL-based approaches in ad-hoc networks. This section highlights the recent advancements in applying FL techniques to MANETs and similar decentralized networks, emphasizing their potential for enhancing distributed learning while preserving data privacy and reducing communication overhead. We review various implementations, their challenges, and the benefits they offer in the context of MANET operations. The second subsection delves into meta-heuristic searching optimization techniques for MANETs. Here, we examine a range of optimization algorithms that have been applied to improve routing efficiency, energy consumption, and overall network performance in MANETs. This includes genetic algorithms (GAs), particle swarm optimization (PSO), and other nature-inspired optimization methods

FL-BASED AD HOC NETWORKS

Federated Learning (FL) has gained prominence in MANETs, especially for UAV and VANET applications, by enabling decentralized model training while preserving data privacy. Studies like [32] and [33] demonstrate FL's effectiveness in detecting jamming attacks through reinforcement learning and client prioritization. Research such as [34] and [35] addressed communication efficiency and dynamic routing via FL-enhanced optimization and topology prediction. FL has also improved IDS in VANETs ([36]) and enabled private, distributed learning on non-IID data ([37], [38]). These works highlight FL's potential to secure MANETs without centralized control.

METAHEURISTIC SEARCHING OPTIMIZATION FOR MANETS

Heuristic and metaheuristic optimization methods are widely used in MANETs, with heuristics offering speed but limited solution quality. Metaheuristics, like swarm intelligence and evolutionary algorithms, effectively tackle complex, nonlinear problems without needing detailed models

Algorithms such as PSO, ACO, and GA have enhanced MANET protocol performance. Reference [29] used multiobjective metaheuristics to optimize AODV routing, achieving significant improvements in delay, energy, and packet loss. These techniques demonstrate strong potential in optimizing MANET operations efficiently.

III. METHODOLOGY

In this section, we detail the systematic approach employed to enhance trust estimation and routing decisions in MANETs using LSTM networks, FL, and MOO. The methodology integrates these advanced techniques to address the dynamic and decentralized nature of such networks, ensuring optimal performance and security.

PROBLEM FORMULATION

In a MANET using the LAR protocol, each node nin_ini is assigned a trust value T(ni)∈[0,1]T(n_i) \in [0, 1]T(ni)∈[0,1] representing its reliability in routing. Nodes with T(ni)<θT(n_i) < \thetaT(ni)<θ are considered malicious (black or gray holes). The goal is for node nin_ini to estimate another node's trust T^ni,nj\hat{T}_{n_i,n_j}T^ni,nj as closely as possible to the actual trust value.

FEATURE SPACE AND LSTM

For the task of predicting the trustworthiness of nodes in a MANET employing the LAR protocol, various features can be extracted to serve as meaningful inputs for the LSTM model. These features capture the static and dynamic characteristics of the network and the behavior of nodes over time. The feature space was developed in our recent work and provides a comprehensive representation of the interactions between nodes. The feature vector X_{ij} represents the set of features concerning the relationship between n_i and n_j at time t, i.e., $X_{ij}(t) = [x1(t)x2(t) \ldots x_i(t) \ldots x_n(t)]$

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

FRAME WORK

The framework of our proposed routing for enhancing trust estimation and routing decisions in MANETs operating under the LAR protocol is presented in Fig 2. This framework leverages LSTM networks, FL, and MOO to optimize network performance. The process begins with four distinct timers: the feature, LSTM, FL, and routing update timers.

PROPOSED SYSTEM

The proposed system secures MANETs using Federated Learning (FL) to train intrusion detection models locally, preserving data privacy.Multi-objective Optimization (MOO) improves accuracy, energy efficiency, and communication performance.Trust values help identify and limit the impact of malicious nodes during model aggregation.This approach ensures adaptive, decentralized, and robust security in dynamic MANET environments

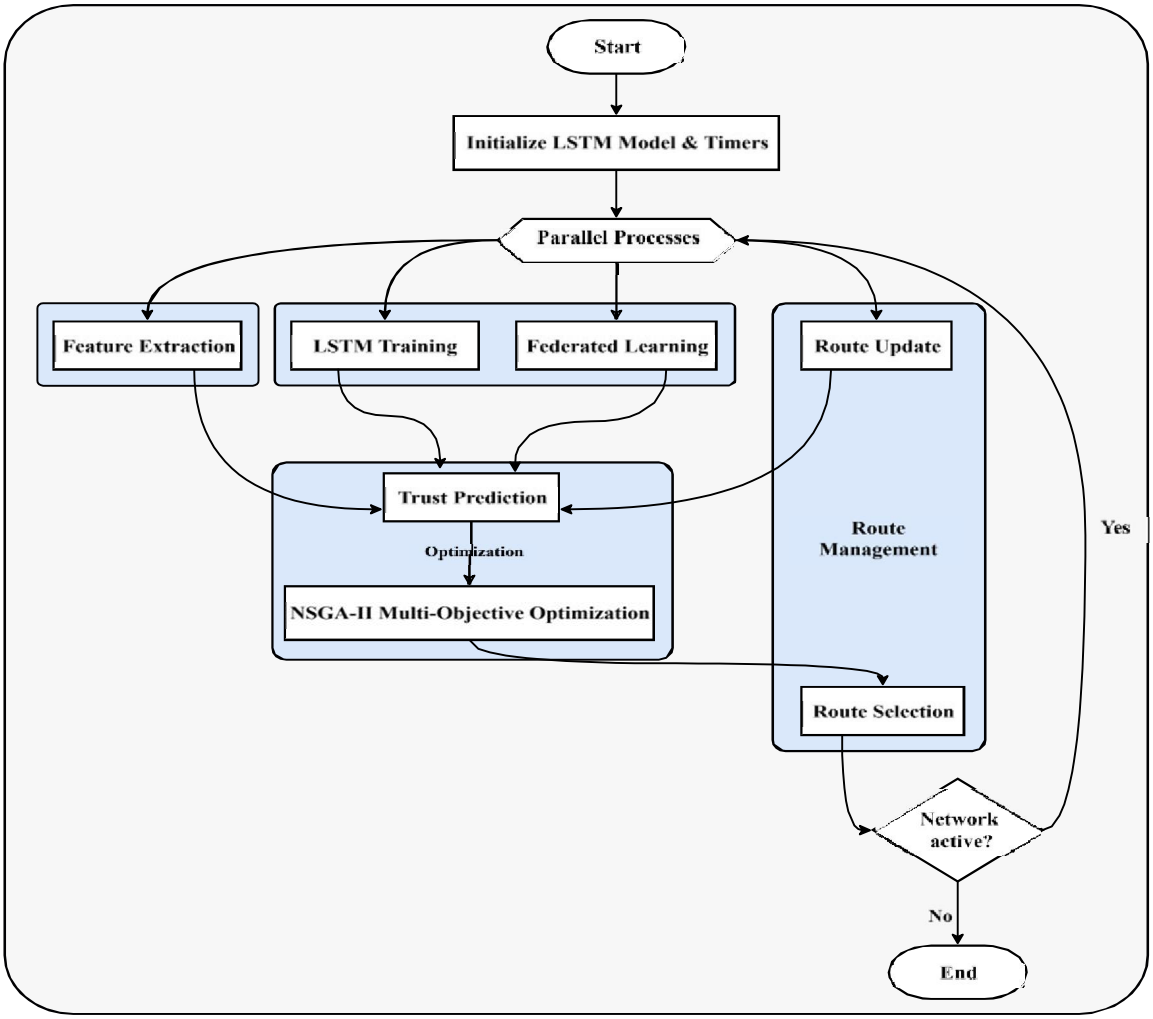

Fig 1. Example

The proposed system aims to strengthen MANET security by integrating Federated Learning (FL) with Multi-objective Optimization (MOO) techniques. In this framework, each mobile node collaboratively trains a local intrusion detection model using its own data without sharing it, thereby preserving privacy and reducing communication overhead. A central aggregator (or selected leader node) periodically collects the local model updates to build a global model that can detect various network attacks such as black hole, gray hole, and Sybil attacks.To ensure efficiency and adaptability in the dynamic MANET environment, MOO algorithms—such as NSGA-II or Particle Swarm Optimization—are

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

applied to optimize key performance objectives, including detection accuracy, energy consumption, communication cost, and model convergence time. Trust values are also integrated into the FL process, where nodes with low trust are weighted less during global aggregation to mitigate model poisoning.

V. RESULT AND DISCUSSION

A. EXPERIMENTAL DESIGN

While our evaluation uses simulated environments, the framework's design inherently supports realtime data processing through its event-driven architecture and timers. The LSTM model's sequential processing capability allows it to handle streaming network metrics as they arrive, while the FL mechanism enables continuous model updates based on live node interactions. Our implementation of Poisson packet generation and random walk mobility patterns closely approximates real-world MANET behavior, suggesting the framework would maintain comparable performance with real-time data streams. All scenarios were conducted in a simulated area of 1000 m × 1000 m with a packet lifetime of 100-time steps.

B. EXPERIMENTAL RESULTS AND ANALYSIS

The results from scenario 1, which simulate a standing MANET environment with 30% malicious nodes, provide valuable insights into the performance of various routing protocols, as detailed in TABLE 7. In this static setting, LSTMTLAR and FLSTMT-LAR emerge as the standout performers across multiple metrics. Both protocols achieve the highest PDR of 0.77, significantly outpacing other approaches. This high PDR is coupled with the best energy efficiency, with LSTMT-LAR and FLSTMT-LAR consuming only 90.86 and 91.38 units, respectively, considerably less than those of other protocols.

VI. CONCLUSION

The proposed FLSTMT-LAR protocol significantly improved MANET security and performance, maintaining high PDR and energy efficiency even under high threat levels. Federated Learning enhanced adaptability in dynamic conditions, while NSGA-III optimization effectively balanced network objectives. Despite strong results, future work should address end-to-end delay and computational overhead in constrained environments.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the following individuals and organization for the invaluable contribution to the project:

• My mentor, Mr. Thangadurai k (AP-CSE) for his guidance, support and expert insights throughout the development and execution for the research.

• Sarathi S, Sanjai S, Sasikumar V, Sarathi M as my team members, for their help in collecting data, analyzing result and providing valuable feedback during the course of the study.

• Mahnedra Institution, and the Department of the Computer Science and Engineering, for providing access to the necessary resources and research facilities.

• I also wish to acknowledgement the participants for the study, whose cooperation and time were essential for the success of the project.

REFERENCES

[1] I. Seth, K. Guleria, and S. N. Panda, ''A comprehensive review on vehicular ad-hoc networks routing protocols for urban and highway scenarios, research gaps and future enhancements,'' Peer-Peer Netw. Appl., vol. 17, no. 4, pp. 2090–2122, Jul. 2024, doi: 10.1007/s12083-024-
01683-1.

[2] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, ''Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks,'' IEEE Access, vol. 12, pp. 150046–150090, 2024, doi: 10.1109/ACCESS.2024. 3457682.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

[3] P. Bondada, D. Samanta, M. Kaur, and H.-N. Lee, ‘‘Data security-based routing in MANETs using key management mechanism,’’ Appl. Sci., vol. 12, no. 3, p. 1041, Jan. 2022, doi: 10.3390/app12031041.
[4] M. U. Rahman and A. Alam, ‘‘Investigating the effects of mobility metrics in mobile ad hoc networks,’’ 2020, arXiv:2006.16441.
[5] N. Khanna and M. Sachdeva, ‘‘A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs,’’ Comput. Sci. Rev., vol. 32, pp. 24–44, May 2019, doi: 10.1016/j.cosrev.2019. 03.001.
[6] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, ‘‘An improved hybrid secure multipath routing protocol for MANET,’’ IEEE Access, vol. 9, pp. 163043–163053, 2021, doi: 10.1109/ACCESS.2021.3133882.
[7] 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), May 2021, pp. 204–211, doi: 10.1109/ICICCS51141.2021. 9432258.
[8] K. A. P. Yamini, J. Stephy, K. Suthendran, and V. Ravi, ‘‘Improving routing disruption attack detection in MANETs using efficient trust establishment,’’ Trans. Emerg. Telecommun. Technol., vol. 33, no. 5, p. e4446, May 2022, doi: 10.1002/ett.4446.
[9] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, ‘‘Security challenges and attacks in dynamic mobile ad hoc networks MANETs,’’ in Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT), Apr. 2019, pp. 28–33, doi: 10.1109/JEEIT.2019. 8717449.
[10] J. A. A. Aldana, S. Maag, and F. Zaïdi, ‘‘MANETs interoperability: Current trends and open research,’’ in 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), May 2018, pp. 481–487, doi: 10.1109/WAINA.2018.00132.