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 12, April 2025
Impact Factor: 7.67

Learning and Optimization: A Trust-Aware Routing Framework

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 (MANETs), trust-aware routing, federated learning, LSTM networks, multiobjective optimization, security in wireless 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 Nodes in a MANET must cooperate for the network to function correctly, but this reliance on cooperation also exposes the network to various security threats, such as black hole attacks, in which malicious nodes advertise false routes to intercept and discard packets, and gray hole attacks, in which nodes selectively drop packets Therefore, trust

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 12, April 2025
Impact Factor: 7.67

management becomes a critical aspect of securing MANETs, necessitating robust mechanisms for trust prediction and evaluation to enhance network reliability and performance

Traditional methods of trust prediction in MANETs have typically relied on direct and indirect observations of node behavior to establish trust metrics Direct trust is derived from firsthand interactions between nodes, whereas indirect trust is based on recommendations or reports from other nodes These methods often use statistical or rule-based approaches to evaluate trust, employing metrics such as packet forwarding ratios, acknowledgment counts, and historical interaction data While these approaches provide a basic level of trust estimation, they have several limitations. First, they tend to be static and unable to adapt quickly to the dynamic changes in node behavior typical of MANET environments Second, traditional trust models often suffer from high computational overhead and latency which can degrade network performance. Furthermore, centralized trust management systems are not feasible in MANETs because of their decentralized nature, leading to potential scalability and reliability issues. Consequently, enhancing routing decisions based on trust predictions becomes challenging. Effective trust-based routing protocols need to dynamically adapt to changing network conditions and node behavior to maintain high levels of security and efficiency This condition has led to an increased interest in leveraging advanced machine learning (ML) techniques for trust prediction and management in MANETs ML-based methods for trust prediction offer significant advantages over traditional approaches by enabling more accurate and dynamic trust assessments ML algorithms, particularly those based on deep learning, can analyze complex patterns and temporal dependencies in network traffic data that are difficult to capture with conventional methods. For instance, long short-term memory (LSTM) networks, a type of recurrent neural network, are particularly well suited for this task because they can retain information over long sequences, making them ideal for modeling the sequential nature of network interactions However, ML-based trust prediction methods require diverse and up-to-date training data to ensure model accuracy and generalizability. In a decentralized network like MANET, this requirement poses a challenge because collecting and aggregating data centrally without violating privacy concerns is impractical. Federated learning (FL) emerges as a promising solution to this problem It allows individual nodes to train local models on their own data and then share model updates, rather than raw data, with neighboring nodes. This approach preserves data privacy while enabling the collaborative improvement of trust prediction models. The problem of trust-based routing in MANETs is inherently multiobjective because it involves balancing various conflicting metrics, such as trustworthiness, energy consumption, and latency Multiobjective optimization (MOO) techniques, such as nondominated sorting genetic algorithm (NSGA)-II are effective in addressing these complexities by finding Pareto-optimal solutions that provide the best trade-offs between competing objectives.

The rest of this article is structured as follows: Section details our key contributions, highlighting the novel aspects of our approach in enhancing MANET security and performance. Section provides a comprehensive literature survey on trust-based routing in MANETs, emphasizing the evolution from traditional methods to advanced ML approaches and identifying current research gaps. Section presents our methodology, elaborating on the problem formulation, feature space design, LSTM application for trust estimation, FL integration, and MOO technique incorporation. This section also includes detailed explanations of our proposed framework, main algorithm, and complexity analysis. Section showcases our experimental results and analysis, offering a

thorough evaluation of the proposed framework's performance across various network scenarios and comparing it with existing protocols. Section concludes this paper, by summarizing our key findings and suggesting directions for future research.

This study addresses a critical gap in the current literature by proposing a novel framework that integrates MOO with FL-based trust prediction to enhance routing decisions in MANETs. Although previous studies have explored various optimization techniques and FL applications in MANETs, they have not incorporated MOO for tuning trust parameters within the dynamic and complex nonlinear environment of MANETs. Our contributions are as follows:

CONTRIBUTIONS

This study addresses a critical gap in the current literature by proposing a novel framework that integrates MOO with FL-based trust prediction to enhance routing decisions in MANETs. Although previous studies have explored various

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 12, April 2025
Impact Factor: 7.67

optimization techniques and FL applications in MANETs, they have not incorporated MOO for tuning trust parameters within the dynamic and complex nonlinear environment of MANETs. Our contributions are as follows: Integration of MOO with Trust Prediction: We introduce a method that combines MOO techniques with LSTM-based trust prediction models. This integration allows for the simultaneous optimization of multiple performance metrics, such as trustworthiness, energy efficiency, and latency, ensuring a balanced and robust routing decision process.

FL for Decentralized Trust Model Updates: By employing FL, our framework ensures that trust models are updated collaboratively and dynamically across the network without the need for centralized data aggregation. This approach enhances data privacy and scalability while maintaining the accuracy and reliability of trust predictions.

Dynamic Trust Assessment: Utilizing LSTM networks, our framework captures temporal and behavioral data patterns, enabling accurate and dynamic trust assessments. This capability is crucial for adapting to the constantly changing topology and node behavior in MANETs.

Improved Routing Decisions: The proposed framework improves routing decisions by incorporating trust predictions directly into the routing algorithm. This trust-aware routing approach helps identify reliable nodes and mitigate the effect of malicious nodes, thereby enhancing the overall security and performance of the network.

By addressing the lack of algorithms that incorporate MOO for tuning trust parameters within the dynamic and nonlinear MANET environment, this study provides a comprehensive solution that enhances the security and efficiency of MANETs.

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

FL has emerged as a pioneering approach in MANETs, especially for applications involving unmanned aerial vehicles (UAVs) and vehicular ad hoc networks (VANETs). This decentralized learning paradigm enables devices within these networks to collaboratively learn a shared prediction model while keeping the training data localized, thus addressing privacy concerns and communication efficiency.

This literature survey summarizes significant contributions in the domain of FL applications within MANETs, highlighting their methodologies, challenges, and outcomes. Reference introduced an adaptive federated reinforcement learning-based strategy for defending against jamming attacks in FANETs. Utilizing a model-free Q-learning mechanism with an epsilon-greedy policy, their approach demonstrated substantial improvements in detecting jammer locations while maintaining higher average accuracy compared with distributed mechanisms. This innovation underscores the potential of FL in enhancing security measures in MANETs without the need for centralized control, which is often impractical in such networks because of communication and power constraints. In another study by an FL-based security architecture was enhanced with a client group prioritization technique leveraging Dempster–Shafer theory. This approach significantly improved jamming attack detection accuracy in FANETs by enabling the aggregator node to identify and prioritize client groups efficiently for global model updates. The use of FL here addresses the unbalanced data issue characteristic of decentralized networks like FANETs, showcasing its applicability in environments with high mobility and spatial heterogeneity. Reference tackled the challenge of communication efficiency in FL through model quantization in VANETs. Their work, FL with double optimization, introduced a

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 12, April 2025
Impact Factor: 7.67

double optimization technique to minimize squared quantization errors, thereby enhancing model performance. This study

highlights the importance of considering client heterogeneity in FL applications, specifically within the context of VANETs where devices support different quantization precision levels. Reference explored the modification of traditional mesh networking protocols with ML models, implemented via FL for UAV networks. Their approach aimed to predict future network topologies to minimize congestion, emphasizing the potential of FL in improving routing decisions in highly dynamic MANET environments. Reference presented a distributed FL approach for enhancing IDS in VANETs. By constructing an ensemble of federated heterogeneous neural networks, their method significantly reduced communication overhead and improved attack detection rates.

This approach exemplifies the synergy between FL and deep learning in securing VANETs against cyberattacks, crucial for smart city development. Reference proposed wireless ad hoc FL (WAFL), a fully distributed cooperative ML framework for opportunistic networks. WAFL achieved high accuracy in training models from highly partitioned non-IID datasets without centralized mechanisms, highlighting the effectiveness of FL in enhancing privacy and accuracy in decentralized networks. Reference introduced a framework for private data sharing in VANETs using FL with local differential privacy. Their framework demonstrated security against inference and gradient leakage attacks while maintaining superior efficiency, indicating the robustness of FL in safeguarding data privacy in interconnected vehicle networks. TABLE provides an overview of different routing protocols incorporating AI models and FL algorithms.

Despite these advancements, none of the existing methods have employed FL to improve trust prediction specifically for serving MANET routing. Trust prediction is vital for

TABLE 1. Overview of different routing protocols incorporating AI models and FL algorithms.

routing decisions because it helps in identifying reliable nodes and mitigating the effect of malicious nodes on network performance. The integration of FL in trust prediction for routing can significantly enhance the security and reliability of MANETs by enabling a decentralized, privacy-preserving approach to model training. This study aims to fill this gap by proposing a novel framework that leverages LSTM-based trust prediction, FL, and MOO to improve routing decisions in MANETs. By dynamically assessing trust based on temporal and behavioral data patterns and collaboratively updating models through FL, the proposed framework aims to achieve a balance between trustworthiness, energy efficiency, and other critical network performance metrics.

METAHEURISTIC SEARCHING OPTIMIZATION FOR MANETS

In the domain of MANETs, heuristicand metaheuristic-based optimization methods have garnered significant interest for their effectiveness and flexibility; although heuristic approaches are known for their speed in tackling optimization challenges specific to MANETs, they typically focus on satisfying constraints rather than optimizing solution quality and This specificity is often regarded as a limitation in their application.

By contrast, metaheuristic techniques excel in exploring complex, high-dimensional search spaces to identify solutions of satisfactory quality for MANETs These methods have proved their effectiveness, particularly in

addressing nonlinear and intricate optimization problems without the need for explicit mathematical models of the MANET system, thus reducing computational requirements Swarm intelligence (SI) algorithms and evolutionary algorithms are notable for their simplicity and effectiveness in optimizing MANET protocols SI algorithms, inspired by the social behavior of animals like birds, fish, ants, and bees, have been successful in mimicking such behavior for tasks like efficient resource location. PSO, ant colony optimization (ACO), gray wolf optimizer, GA, and bumblebee optimization algorithm are among the prominent SI strategies applied to enhance MANET operations

Reference aimed to enrich the existing theoretical perspective by presenting an innovative method for optimizing the routing performance of the ad hoc on-demand distance vector (AODV) protocol using multiobjective metaheuristics. The focus was on improving AODV's routing recovery performance concerning routing delay, energy consumption, packet loss ratio, and route load metrics. The proposed solution demonstrated superior performance to the original AODV, with average improvements of 56.0%, 59.3%, 48.1%, and 0.7% in route load, routing delay, packet loss ratio, and energy consumption, respectively. Additionally, it presented competitive results compared with other routing protocols.

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 12, April 2025
Impact Factor: 7.67

Reference presented a fitness function integrated with GA to optimize routing in MANETs. Their approach combined the ad hoc on-demand multipath distance vector (AOMDV) routing protocol with GA (AOMDV-GA), selecting routes based on criteria such as shortest path, maximum residual energy, and minimal data traffic. This strategy of AOMDV-GA and the inclusion of TCP congestion control enhancement for random loss in the fitness function showed improvements in managing energy constraints and reducing packet loss due to network dynamics. Reference further investigated GA's application by proposing an adaptive routing protocol optimized by GA for mitigating packet collision and enhancing throughput and packet delivery ratio (PDR) in MANETs. Their model optimized multiple paths provided by AOMDV, selecting the route with the highest fitness value. The study indicated GA's ability to adapt to topological changes and manage node mobility, reducing routing overhead and improving end-to-end (E2E) delay. Reference worked on enhancing the energy-aware location-aided routing (EALAR) protocol by integrating optimized PSO with a uniform mutation operation. This integration aimed to address the limitations of the nonuniform mutation in traditional EALAR, affecting exploration, exploitation, and solution diversity. The optimized routing protocol showed improvements in energy conservation, overhead minimization, and E2E delay reduction. Reference compared PSO and GA in optimizing the OLSR routing protocol. Their analysis indicated GA's effectiveness in managing the dynamic nature of MANETs, enhancing path selection, and optimizing network performance metrics compared with PSO. Reference xamined ACO and PSO for routing in MANETs. Their study showed ACO's performance in terms of PDR, throughput, and power consumption with reduced packet delay. ACO's performance was compared with that of traditional routing protocols like AODV, AOMDV, and DSDV.

Reference addressed the black hole attack using the ACO technique with repetitive route configuration and reactive routing protocol. This approach showed improvements in throughput and reduction in packet loss. Reference addressed the smart gray hole attack by combining the beta reputation system with the ACO metaheuristic in a trust management model. This approach modified the traditional DSR protocol by isolating malicious nodes, affecting PDR, throughput, and energy consumption.

Another study addressed the optimization of routing protocols for VANETs, which are essential for the operation of intelligent transportation systems and various other applications. VANET routing entails awareness about the nature of the road and numerous other parameters that affect protocol performance. Optimizing VANET routing ensures optimal metrics, such as low E2E delay, high PDR, and low overhead. Given the multiobjective nature of VANET performance, MOO is necessary. Most researchers have focused on singleobjective or weighted average approaches for MOO, with only a few studies tackling the actual MOO of VANET routing. In one notable work, a novel reactive routing protocol named tail-based routing, based on the concept of location-aided routing (LAR), was proposed. The study redefined the request zone to reduce lateral width with respect to the lateral distance between the source and destination,
naming it the ‘‘tail.’’ The protocol incorporated angle searching with crowding distance inside the MOO PSO (MO-PSO) algorithm, termed MO-PSO-angle

Despite the numerous approaches based on metaheuristics for MANET optimization, the literature still lacks an algorithm that incorporates MOO for tuning the parameters of trust within the dynamics and the complex nonlinearity of MANETs. This study aims to address this gap by integrating MOO with FL-based trust prediction. TABLE provides a comparative analysis of various MANET routing protocols, indicating proposed techniques, purposes, addressed problems, and key findings.

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.

We present the methodology in Fig . The process begins with system initialization, where the LSTM model and various timers are set up. The system then enters into parallel processing of four key components: Feature Extraction, LSTM Training, FL, and Route Update. These parallel processes feed into Trust Prediction, where the data is consolidated to assess node trustworthiness. The trust predictions then undergo optimization using NSGA-II Multi-Objective Optimization, which balances multiple performance metrics such as energy efficiency, security, and network

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 12, April 2025
Impact Factor: 7.67

performance. Within the Route Management phase, the optimized results are used for Route Selection. The system then checks if the network is still active if yes, the process loops back to the parallel processes for continuous updating and adaptation; if no, the process terminates. This cyclic flow ensures continuous adaptation to network conditions while maintaining security and efficiency through trustaware routing decisions. The mathematical symbols used in the methodology are presented in Table .

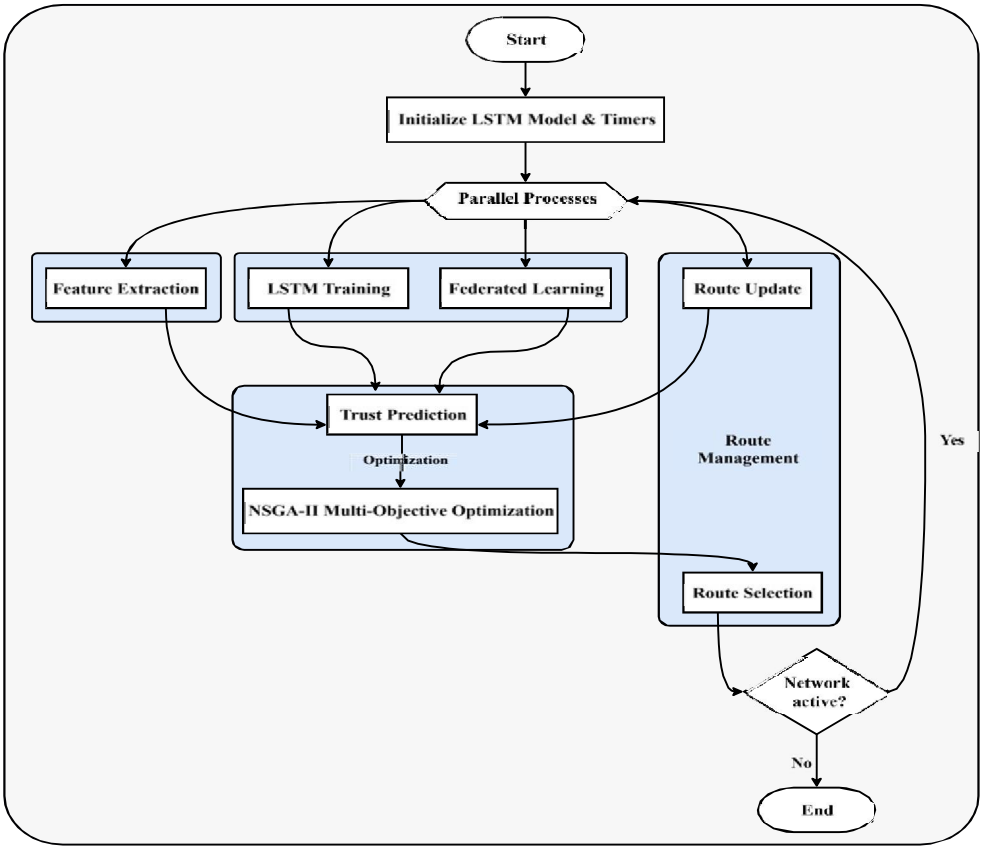

FIGURE 1. Flowchart of trust-aware MANET routing framework integrating LSTM, federated learning, and NSGA-II multi-objective optimization for dynamic route selection.

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.

[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.

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 12, April 2025
Impact Factor: 7.67

[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.
[1] 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.