Impact of Mobility Models on Long Short-Term Memory -Enhanced Routing Protocols in Mobile Ad Hoc Networks

Saad Mohsen Hassan[1, 2]* Mohd Murtadha Bin Mohamad[1] Nawar T. Thannon[3] Farkhana Binti Muchtar[1]

[1]*Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Skudai, Malaysia*
[2]*Computer Science Department, Faculty of Basic Education, AL-Mustansiriya University, Baghdad 10011, Iraq*
[3]*Computer Nwtorks and Internet Department, College of Information Technology, Nineveh University, Mosul, Iraq.*
* Corresponding author's Email: murtadha@utm.my
(Received: August 8, 2025. Accepted: August 28, 2025. Published: September 7, 2025.)

Abstract

Mobile Ad Hoc Networks (MANETs) face routing challenges due to dynamic topology and lack of infrastructure. This study enhances Location-Aided Routing (LAR) protocols by integrating Long Short-Term Memory (LSTM) models to predict node trustworthiness, improving routing decisions. LSTM models leverage historical traffic and trust data for adaptive routing. The research evaluates mobility model impacts on energy consumption, end-to-end delay, and packet delivery ratio. The LSTM-enhanced LAR protocol was tested under standing and random walk scenarios. Results show 15% improvement in packet delivery ratio compared to traditional methods, particularly in dynamic environments. However, energy consumption and end-to-end delay increased. Findings highlight machine learning's potential for enhancing MANET routing protocols while identifying optimization needs. This research emphasizes adaptive, trust-based routing importance for improving MANET performance.

Keywords: MANETs, LAR, LSTM, Mobility Models, Trust prediction.

1. Introduction

One of the goals of smart environments is to improve the quality of human life in terms of comfort and efficiency. The Internet of Things (IoT) has become crucial for building smart environments, but security and privacy issues are significant concerns due to various threats [1, 2]. Therefore, Intrusion Detection Systems (IDSs) are essential for mitigating IoT-related security attacks [3, 4]. Comprehensive taxonomies have systematically categorized various schemes for detecting and mitigating blackhole attacks in MANETs [5]. Advanced machine learning and optimization techniques have emerged as powerful tools for developing intrusion detection systems to counter black and gray hole attacks [6]. However, the limited computing and storage capabilities of IoT devices make conventional IDSs impractical [7]. Surveys emphasize the need for robust and efficient IDSs tailored for IoT environments [8]. The spread of information through digital platforms has increased the prevalence of fake news, necessitating sophisticated detection mechanisms [9]. Deep learning models, such as Bidirectional Long Short-Term Memory (Bi-LSTM) and attention-based Bi-LSTM, have shown promise in detecting fake news [10-12]. Integrating attention mechanisms enhances these models' accuracy and effectiveness. However, challenges like data dependency, overfitting, and context specificity must be addressed to improve model robustness across different contexts [12].

Wireless sensor networks (WSNs) are used for data monitoring and collection in various applications but are vulnerable to security threats due to limited resources. Effective IDSs are necessary to protect WSNs from attacks like Denial of Service (DoS). Studies have developed deep learning-based IDSs to detect DoS attacks, highlighting the need for advanced security mechanisms to enhance WSN resilience [13]. The Border Gateway Protocol (BGP) facilitates routing information exchange between autonomous systems, but anomalies can cause significant disruptions [1, 9, 14]. LSTM-based autoencoder networks have been proposed for detecting BGP anomalies, leveraging their ability to model time series data for accurate anomaly detection, these models effectively identify various types of routing anomalies, highlighting the potential of LSTM-based approaches in enhancing network security [9].

Mobile ad-hoc networks (MANETs) face security and privacy challenges due to their lack of infrastructure, unpredictable topology, and restricted resources. Novel detection approaches, like the dipper-throated optimization (DTO) algorithm, classify passive and active black-hole attacks, improving attack detection accuracy and network performance [15]. Recent advances have demonstrated the effectiveness of integrating LSTM-based trust prediction mechanisms into location-aided routing protocols [16]. Underwater Acoustic Sensor Networks (UASNs) are used in marine applications but face security challenges due to limited node capabilities. Trust management-based secure routing protocols, such as T-SAPR, use attention-based LSTM models to evaluate node trust and optimize routing policies, enhancing packet delivery and energy efficiency [1]. MANETs require routing protocols that adapt to frequent changes in dynamic topologies [17, 18]. Simulative studies comparing reactive and proactive routing protocols across different mobility models provide insights into their performance under varying conditions, emphasizing the importance of selecting suitable models to optimize network performance. Research shows that node mobility significantly impacts routing protocols' performance, influencing metrics like packet delivery ratio, throughput, and delay [17, 19]. The random waypoint model is used to simulate mobility patterns and assess their impact on network performance [20].

Vehicular ad-hoc networks (VANETs) require reliable and secure communication for time-critical data exchange. Enhanced routing protocols, such as the Enhanced Location-Aided Ant Colony Routing (ELAACR), combine location-aided key management with ant colony optimization to ensure secure and efficient data transmission in VANETs [21]. These protocols improve metrics like throughput, packet delivery ratio, and end-to-end delay [21]. Despite significant advancements in security mechanisms and routing protocols for various network environments, challenges remain. There is a critical need for adaptive, efficient, and scalable solutions that respond dynamically to changing network conditions and diverse security threats [2]. Further investigation is required to understand how different mobility models impact MANET performance, particularly in terms of energy consumption and delay [22]. Emerging research has explored federated learning with multiobjective optimization to develop trust-aware routing frameworks [23]. This gap underscores the need for enhancing MANET routing efficiency using LSTM models trained on network traffic features and trust labels to predict neighboring nodes' trustworthiness, improving overall network performance and adapting to various mobility scenarios.

2. Methodology

This section presents the developed methodology. It starts with the problem formulation. Next, the proposed solution is presented.

2.1 Problem formulation

In MANET utilizing a Location-Aided Routing (LAR) protocol, we seek to enhance routing efficiency by integrating an LSTM model trained on network traffic features and corresponding trust labels. Each node in the network is equipped with an LSTM model, trained based on its historical experiences, to predict the trustworthiness of neighboring nodes. This predicted trust level is then utilized as an additional criterion alongside the conventional location and mobility criteria inherent in LAR. Consider a MANET represented as a graph $G = (V, E)$, where V denotes the set of nodes and E denotes the set of edges, which represent the links between nodes. Each node $v \in V$ possesses an LSTM model M_v, trained to predict the trust level of its neighbors. The trust prediction at time t for a neighboring node j as predicted by node i is denoted as $\hat{T}_{ij}(t)$. The input to the LSTM model comprises traffic features at node i at time t, represented as $\mathbf{x}_i(t)$, leading to the trust prediction given by $\hat{T}_{ij}(t) = M_i(\mathbf{x}_i(t))$. The routing decision at node i at time t is formulated based on the location, mobility, and predicted trust levels of its neighbors. This decision is encapsulated in a routing metric $R_{ij}(t)$, defined as a function f incorporating the location and mobility of node j, and the trust prediction $\hat{T}_{ij}(t)$. Mathematically, this can be expressed in Eq. (1):

$$R_{ij}(t) = f\left(\text{location}_j\,(t), \text{mobility}_j\,(t), \hat{T}_{ij}(t)\right) \tag{1}$$

A critical aspect of this study is the influence of various mobility models on the performance of the proposed LSTM-augmented LAR protocol. Let $\mathcal{M}$ denote the set of potential mobility models, such as random waypoint, and random walk. The mobility model $m \in \mathcal{M}$ governing each node's movement plays a significant role in shaping the network dynamics. The probability $P(\text{ encounter }_{ij})$ of node

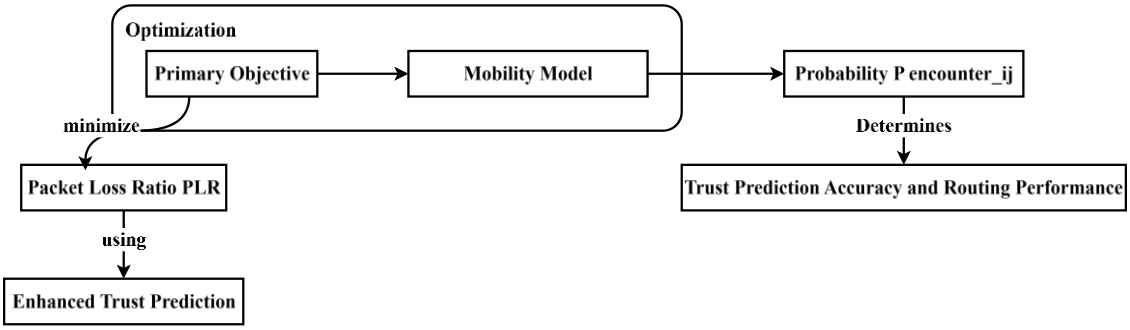

Figure. 1 Diagram illustrating the optimization process for minimizing PLR in MANETs using LSTM-augmented LAR protocols influenced by various mobility models

i encountering node j is determined by the underlying mobility model and significantly impacts the trust prediction accuracy and routing performance. The primary objective of this research is to minimize the packet loss ratio (PLR) attributable to black/gray hole attacks by leveraging the enhanced trust prediction capabilities of the LSTM models under different mobility scenarios. The problem can be formally stated as the minimization of PLR subject to the dynamics induced by various mobility models and the efficacy of the LSTM-based trust predictions and can be described in Equation 2:

$$\text{minPLR subject to } m \in \mathcal{M} \text{ and } \hat{T}_{ij}(t) = M_i(\mathbf{x}_i(t)) \quad (1)$$

Developing an optimization solution to such a complex problem is challenging due to the inherent variability and unpredictability of node mobility. Therefore, we propose to explore the effect of different decision models on the performance of the LSTM-augmented LAR protocol. By analyzing how various mobility models impact trust prediction accuracy and routing efficiency, we aim to provide insights that will help researchers narrow down the problem space. This, in turn, will guide the formulation of more specific optimization problems that are tailored to particular mobility models, thereby simplifying the decision-making process and enhancing overall network performance.

Figure 1 depicts a diagram to illustrate the optimization process for enhancing routing efficiency in MANET using an LSTM-augmented LAR protocol.

The primary objective is to minimize the Packet Loss Ratio (PLR) by leveraging enhanced trust predictions. This is achieved through an optimization framework where each node is equipped with an LSTM model trained on network traffic features and corresponding trust labels to predict the trustworthiness of neighboring nodes. The mobility model, which dictates node movement patterns, significantly influences the probability of node encounters (P($encounter_{ij}$)). This probability affects trust prediction accuracy and overall routing performance. By accurately predicting trust levels, the routing decisions are improved, thereby reducing the PLR. The enhanced trust predictions, influenced by various mobility models, form the crux of the optimization strategy aimed at improving MANET performance, particularly under dynamic conditions. This integrated approach underscores the importance of mobility models in shaping network dynamics and routing efficiency.

The primary objective is to minimize the Packet Loss Ratio (PLR) by leveraging enhanced trust predictions. This is achieved through an optimization framework where each node is equipped with an LSTM model trained on network traffic features and corresponding trust labels to predict the trustworthiness of neighboring nodes. The mobility model, which dictates node movement patterns, significantly influences the probability of node encounters (P(encounter_ij)). This probability affects trust prediction accuracy and overall routing performance. By accurately predicting trust levels, the routing decisions are improved, thereby reducing the PLR. The enhanced trust predictions, influenced by various mobility models, form the crux of the optimization strategy aimed at improving MANET performance, particularly under dynamic conditions. This integrated approach underscores the importance of mobility models in shaping network dynamics and routing efficiency.

2.2 Proposed solution

The methodology for enhancing routing efficiency in MANETs through LSTM-augmented LAR protocol is illustrated in Figure 2. The process begins by defining the network model, represented as a graph $G = (V, E)$, where V denotes the set of nodes and E the set of edges, indicating links between nodes. Next, various mobility models ($\mathcal{M}$),

such as Random Waypoint, Gauss-Markov, and Manhattan Grid, are defined to govern node movements. Following this, each node is equipped with an LSTM model M_v, trained on historical traffic features and trust labels to predict the trustworthiness of neighboring nodes. The experiments conducted are designed to assess the impact of these mobility models on the performance of the LSTM-augmented LAR protocol.

The first experiment, "Standard Test with 0% Malicious Nodes-Standing," serves as a baseline, evaluating network performance metrics under stationary conditions with no malicious nodes. The second experiment, "Node 55 - Random Walk," investigates the effect of a single node following a random walk mobility model. The third experiment, "Standard Test-Standing," replicates the baseline under different network conditions or configurations. The fourth experiment, "Partition Test-Random Walk," evaluates network performance in a partitioned scenario with nodes following a random walk mobility model. The fifth experiment, "Stress Test-Random Walk," stresses the network by increasing traffic load while nodes follow a random walk. The sixth experiment, "Different Number of Black Hole Test," examines the impact of varying numbers of black hole nodes on network performance.

Performance metrics, including Packet Delivery Ratio (PDR), End-to-End (E2E) Delay, Energy Consumption, Overhead, and Throughput, are collected from each experiment and analyzed to understand how different mobility models affect trust prediction accuracy and routing efficiency. The results guide researchers to narrow down the problem space to a more specific decision model based on mobility models. This approach simplifies the decision-making process, leading to the development of targeted optimization strategies, enhancing overall network performance. The methodology concludes by integrating these strategies into the network model, aiming to minimize packet loss and maximize routing efficiency.

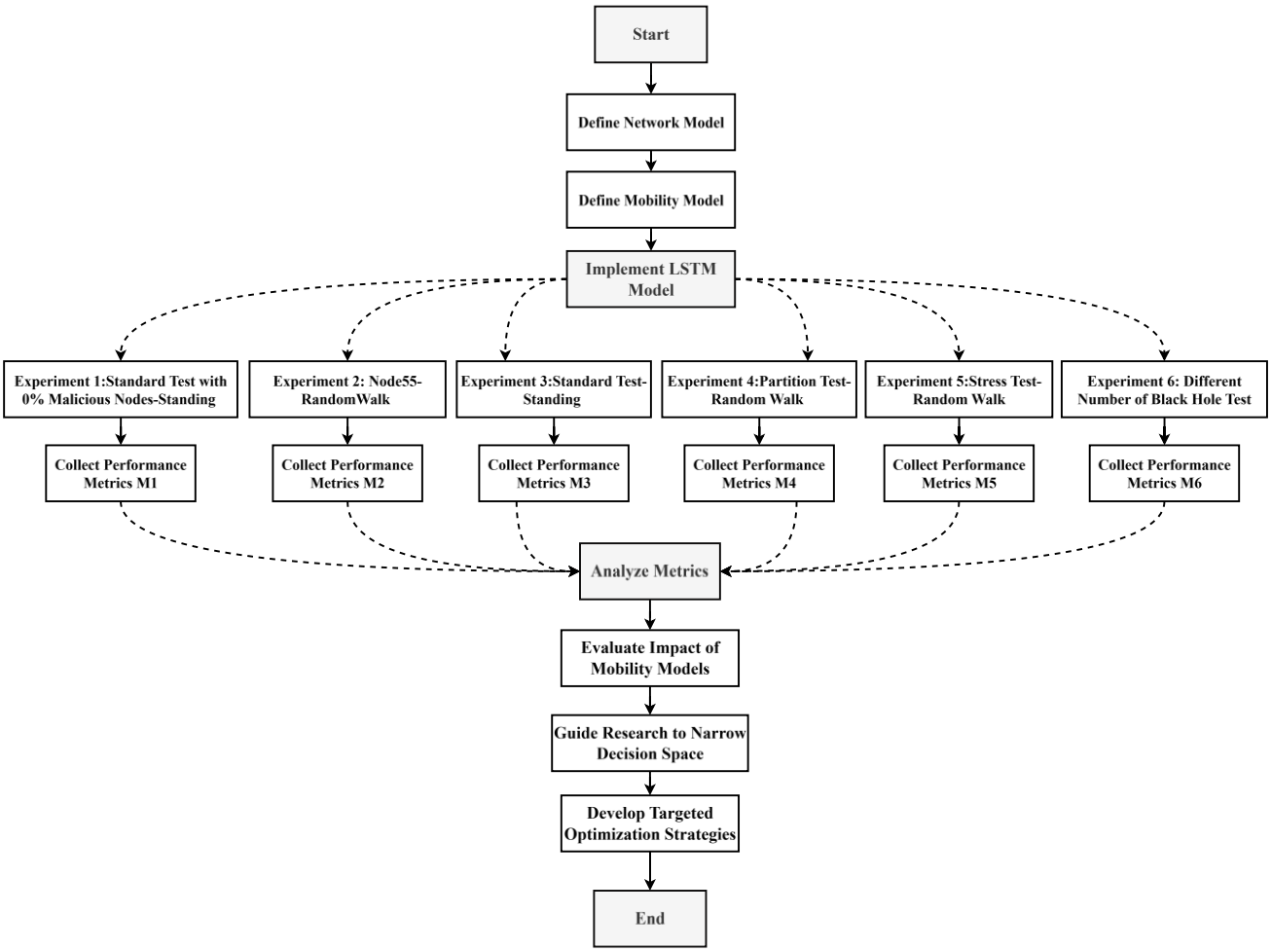

Figure. 2 Flowchart illustrates the step-by-step process of defining relation between network and mobility models from trust perspective

Table 1. Summarizes the experimental design parameters for evaluating the performance of different protocols under various mobility models and network conditions in a MANET

Experiment	Run Until (time step)	Data Packet Life Time (time step)	Mobility Model	Malicious Nodes (%)	Number of Nodes	Node Speed (m/s)	Packet Generation Parameters
1	550	100	Standing	0	30	0	-
2	550	100	Random Walk	30	55	1	$Poisson\ distribution, \lambda$ $0.3, N(t) = N(t) * (t/30) N(t) = N(t) * (t/30)$
3	550	100	Random Walk	30	55	1	-
4	550	100	Standing	30	30	0	-
5	550	100	Random Walk	25	20	1	$Poisson\ distribution, \lambda$ $0.3,\ N(t) = N(t) * (t/30) N(t) = N(t) * (t/30)$
6	550	100	Random Walk	30	30	1	-
7	1000	100	Standing	10, 20, 30, 40, 50, 60, 70, 80, 90	30	0	Poisson distribution, λ = 0.3
8	550	100	Random Walk	33	100	1	Poisson distribution, λ = 0.3

3. Experimental results and analysis

The experimental design aims to evaluate the performance of various routing protocols in a MANET under different mobility models and conditions. Table 1 summarizes the key parameters for each experiment, including simulation duration, data packet lifetime, mobility model, percentage of malicious nodes, number of nodes, node speed, and packet generation parameters. Experiments were conducted in environments with dimensions of 1000×1000 meters, running until 550- or 1000-time steps. The data packet lifetime was set to 100-time steps. Mobility models varied between Standing and Random Walk, with malicious node percentages ranging from 0% to 90% . We deliberately selected Standing and Random Walk mobility models as they represent the fundamental extremes of the mobility spectrum. The Standing model serves as a baseline for static or low-mobility scenarios, while Random Walk provides insights into highly dynamic, unpredictable movement patterns. These two models allow us to establish the foundational performance boundaries of our LSTM-enhanced protocol under minimal and maximal mobility conditions, providing essential baseline data for understanding the protocol's behavior across the mobility spectrum.

The number of nodes in the network varied from 20 to 100, with node speeds of $0\ \mathrm{m/s}$ for Standing models and $1\ \mathrm{m/s}$ for Random Walk models. Packet generation followed a Poisson distribution with a lambda of 0.3, and in some experiments, the number of nodes varied over time according to $N(t) = N(t) * (t/30)$. This design facilitates a comprehensive analysis of how mobility models and malicious activities affect key performance metrics such as PDR, E2E delay, Energy consumption, Overhead, and Throughput, thereby providing insights into the robustness and efficiency of the routing protocols under study.

The combined results Table 2 provides an overview of various routing protocols' performance across different mobility models and node configurations. The focus is on identifying the most suitable mobility model for improving performance metrics under different packet generation models.

In stationary scenarios (Standing model), the LSTM Trust-Based protocol achieved the highest PDR and Throughput. For example, with 0% malicious nodes, it recorded a PDR of 0.95 and a Throughput of 8.54, but with higher E2E delay (3.10) and Energy consumption (6177.18). In another test, it achieved a PDR of 0.72 and a Throughput of 6.48, with an E2E delay of 1.16 and Energy consumption of 144.71. These results

Table 2. Performance Evaluation of Various Routing Protocols under Different Testing Conditions

Experiment	Protocol	PDR	E2E Delay	Energy Consumption	Overhead	Throughput
Standard Test with 0% Malicious Nodes	Random	0.86	2.26	359.01	0.47	7.84
	Distance Based LAR [24]	0.93	1.26	82.74	0.35	8.45
	Rectangle Based LAR [25]	0.87	1.03	843.62	0.41	7.79
	Con Based LAR [26]	0.70	1.12	204.21	0.52	6.26
	LSTM Trust Based	0.95	3.10	6177.18	0.30	8.54
Node 55 - Random Walk	Random	0.86	2.26	359.01	0.47	7.84
	Distance Based LAR [24]	0.93	1.26	82.74	0.35	8.45
	Rectangle Based LAR [25]	0.87	1.03	843.62	0.41	7.79
	Con Based LAR [26]	0.70	1.12	204.21	0.52	6.26
	LSTM Trust Based	0.95	3.10	6177.18	0.30	8.54
Standard Test – Standing	Flood	0.40	0.85	11075.21	0.29	3.59
	Random	0.36	1.43	584.93	0.26	3.17
	Distance Based LAR [24]	0.55	1.05	127.53	0.36	5.01
	Rectangle Based LAR [25]	0.48	0.79	1510.22	0.32	4.41
	Con Based LAR [26]	0.54	1.00	362.26	0.35	4.87
	LSTM Trust Based	0.72	1.16	144.71	0.42	6.48
Partition Test - Random Walk	Flood	0.57	0.68	576.02	0.36	3.47
	Random	0.35	0.72	53.88	0.26	2.11
	Distance Based LAR [24]	0.51	0.78	40.95	0.34	3.03
	Rectangle Based LAR [25]	0.42	0.67	59.47	0.29	2.54
	Con Based LAR [26]	0.43	0.75	31.24	0.30	2.53
	LSTM Trust Based	0.59	0.71	44.24	0.37	3.52
Stress Test - Random Walk	Flood	0.29	0.78	5251.64	0.22	11.45
	Random	0.17	1.14	432.16	0.15	7.06
	Distance Based LAR [24]	0.25	0.82	211.04	0.20	9.40
	Rectangle Based LAR [25]	0.28	0.54	879.58	0.22	10.53
	Con Based LAR [26]	0.23	0.65	226.91	0.18	8.12
	LSTM Trust Based	0.35	0.96	229.42	0.26	13.19
Different Number of Black Hole Test (10%)	10%	0.87	1.22	152.53	0.41	7.95
	20%	0.86	1.17	152.59	0.36	7.74
	30%	0.72	1.16	145.26	0.36	6.47
	40%	0.78	1.18	169.04	0.45	6.93
	50%	0.79	1.20	170.55	0.45	7.05
	60%	0.40	1.14	118.71	0.35	3.63
	70%	0.58	1.32	188.06	0.53	5.28
	80%	0.35	1.10	113.97	0.35	3.25
	90%	0.19	0.67	152.56	0.52	1.64
Node 100 Test	Distance Based LAR [24]s	0.49	0.87	299.47	0.38	14.41
	Rectangle Based LAR [25]	0.39	0.89	51067.25	0.55	11.63
	Con Based LAR [26]	0.43	0.75	11459.75	0.58	12.64
	LSTM Trust Based	0.67	1.02	308.08	0.34	19.97

indicate that while the LSTM Trust-Based protocol excels in reliability and efficiency, optimization is needed to balance resource usage. In dynamic environments (Random Walk model), the LSTM Trust-Based protocol maintained the highest PDR and Throughput in most scenarios. For instance, in the partition test, it achieved a PDR of 0.59 and a Throughput of 3.52, with an E2E delay of 0.71 and Energy consumption of 44.24. In the stress test, it recorded a PDR of 0.35 and a Throughput of 13.19, with an E2E delay of 0.96 and energy consumption of 229.42. The protocol's adaptability to changing network conditions highlights its effectiveness in managing node mobility and trust prediction. However, increased energy consumption and delay suggest areas for improvement, particularly in energy-constrained applications.

The Standing model showed better performance in stable and low-mobility scenarios, suitable for static sensor networks or low-mobility urban environments. Under this model, the LSTM Trust-Based protocol achieved the highest PDR (0.95) and Throughput (8.54) with 0% malicious nodes, indicating its effectiveness in low mobility scenarios. The packet generation model did not significantly impact performance metrics, suggesting that LSTM Trust-Based can maintain high performance in steady traffic patterns. Conversely, the Random

Walk model is suitable for dynamic and high-mobility environments, such as VANETs or mobile sensor networks. The LSTM Trust-Based protocol excelled in maintaining high PDR and Throughput even in this model. For example, in the stress test, it achieved a PDR of 0.35 and Throughput of 13.19. The packet generation model, based on a Poisson distribution, showed the protocol's effectiveness in handling varying traffic intensities.

The impact of malicious nodes on network performance was evident in different black hole tests. As the percentage of malicious nodes increased, PDR significantly decreased. For instance, the PDR dropped from 0.874 at 10% malicious nodes to 0.186 at 90% malicious nodes. Energy consumption peaked at 188.061 with 70% malicious nodes. Overhead generally increased with higher malicious node percentages, affecting network efficiency. The LSTM Trust-Based protocol's performance, though superior, diminished with increasing malicious nodes, emphasizing the need for enhanced security mechanisms in adversarial environments. In larger network configurations, such as the Node 100 test, the LSTM Trust-Based protocol demonstrated scalability, achieving the highest PDR (0.67) and Throughput (19.97), with relatively low Overhead (0.34). This indicates the protocol's potential for application in extensive MANETs, aligning with the goal of incorporating dynamic and mobility-aware scheduling to improve network performance.

A critical limitation observed in our results is the significantly higher energy consumption of the LSTM Trust-Based protocol, particularly evident in the baseline test where it consumed 6177.18 units compared to 82.74 units for Distance-Based LAR. This represents a 74-fold increase in energy consumption, which severely limits the protocol's applicability in energy-constrained environments such as IoT and wireless sensor networks. While the protocol demonstrates superior performance in terms of PDR and throughput, this energy overhead makes it impractical for many real-world MANET deployments where battery life is the primary constraint.

In general, the analysis suggests that the Standing model is more suitable for low mobility and static node environments, providing high reliability and efficiency under steady traffic patterns. In contrast, the Random Walk model is more appropriate for high-mobility environments, demonstrating robustness in dynamic conditions and varying traffic loads. The LSTM Trust-Based protocol consistently performed well across both mobility models, indicating its versatility and effectiveness in diverse MANET environments. However, further optimization for energy efficiency and delay reduction is needed to leverage its potential in different application scenarios fully.

4. Conclusion

The study aimed to enhance routing efficiency in MANETs by incorporating an LSTM model trained on network traffic features and corresponding trust labels into LAR protocol. This integration was evaluated under different mobility models Standing and Random Walk to understand their impact on performance metrics such as PDR, E2E delay, Energy consumption, Overhead, and Throughput. The LSTM Trust-Based protocol consistently demonstrated superior PDR and Throughput across both mobility models. In the Standing model, it achieved a PDR of 0.95 and Throughput of 8.54, while in the Random Walk model, it maintained a high PDR and Throughput, achieving 0.35 and 13.19 respectively during stress tests. However, the protocol also showed higher E2E delay and Energy consumption, indicating areas for optimization. Despite its promising performance, the LSTM Trust-Based protocol exhibited significant limitations.

One major limitation is its high Energy consumption, particularly evident in the standard test with 0% malicious nodes, where it recorded an energy usage of 6177.18. This high energy requirement limits its applicability in energy-constrained environments, such as sensor networks. Additionally, the protocol's higher E2E delay, observed across various scenarios, may affect real-time applications requiring low latency. The most pressing concern is addressing the excessive energy consumption of our LSTM-based approach. Future work will focus on implementing lightweight alternatives such as Gated Recurrent Units (GRUs), model pruning techniques, and quantization methods to achieve a target 80-90% reduction in energy consumption while maintaining acceptable performance levels.

We plan to develop dynamic model selection algorithms that can switch between full LSTM inference, lightweight models, and rule-based trust assessment based on remaining energy levels and network conditions.

While our current study establishes baseline performance using Standing and Random Walk models, future work will comprehensively evaluate more realistic mobility models including:

- **Gauss-Markov Model:** For scenarios with temporal correlation in

 doi: 10.22266/inassexpress.2025.009

movement patterns, applicable to pedestrian networks and wildlife monitoring

- **Manhattan Grid Model:** For urban vehicular environments with structured road networks
- **Reference Point Group Mobility (RPGM):** For disaster recovery and military applications where nodes move in coordinated groups
- **Smooth Random Mobility:** For aerial networks and UAV swarms with bounded acceleration constraints

The study also primarily focused on the impact of mobility models without extensively exploring other environmental factors, such as varying traffic loads and different types of malicious attacks beyond black hole nodes.

Conflicts of interest

The authors declare no conflict of interest. The research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Author contributions

Conceptualization, Saad Mohsen Hassan and Mohd Murtadha Bin Mohamad; methodology, Saad Mohsen Hassan; software, Saad Mohsen Hassan; validation, Mohd Murtadha Bin Mohamad, Nawar T. Thannon, and Farkhana Binti Muchtar; formal analysis, Saad Mohsen Hassan; investigation, Saad Mohsen Hassan; resources, Mohd Murtadha Bin Mohamad; data curation, Saad Mohsen Hassan; writing-original draft preparation, Saad Mohsen Hassan; writing-review and editing, Mohd Murtadha Bin Mohamad and Farkhana Binti Muchtar; visualization, Nawar T. Thannon; supervision, Mohd Murtadha Bin Mohamad; project administration, Mohd Murtadha Bin Mohamad; funding acquisition, Mohd Murtadha Bin Mohamad.

Acknowledgement

Appreciation to Universiti Teknologi Malaysia, researchers and whom involved in preparing this paper under Faculty of Computing Publication Incentive and vot no. Q.J 130000.5028.10G12: IMPACT OF MOBILITY MODELS ON LONG SHORT-TERM MEMORY -ENHANCED ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS.

References

[1] R. Zhu, A. Boukerche, L. Feng, and Q. Yang, "A trust management-based secure routing protocol with AUV-aided path repairing for Underwater Acoustic Sensor Networks," *Ad Hoc Networks,* vol. 149, p. 103212, 2023.

[2] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IOT devices against emerging security threats: Challenges and mitigation techniques," *Journal of Cyber Security Technology,* vol. 7, no. 4, pp. 199-223, 2023.

[3] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors,* vol. 24, no. 2, p. 713, 2024.

[4] A. Basharat and M. M. B. Mohamad, "Security challenges and solutions for internet of things based smart agriculture: A review," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, 2022, pp. 102-107: IEEE.

[5] S. M. Hassan, M. M. B. Mohamad, and F. B. Muchtar, "Comprehensive Taxonomy of Schemes for Detecting and Mitigating Blackhole Attacks in Mobile Ad-Hoc Networks: A Study on Tactics, Classifications, and Future Directions," *Ingénierie des Systèmes d'Information,* vol. 29, no. 6, 2024.

[6] 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,* 2024.

[7] J. Chen, D. Wu, and R. Xie, "Artificial intelligence algorithms for cyberspace security applications: a technological and status review," *Frontiers of Information Technology Electronic Engineering,* vol. 24, no. 8, pp. 1117-1142, 2023.

[8] M. R. Ayyagari, N. Kesswani, M. Kumar, and K. Kumar, "Intrusion detection techniques in network environment: a systematic review," *Wireless Networks,* vol. 27, no. 2, pp. 1269-1285, 2021.

[9] A. H. Muosa and A. Ali, "Internet routing anomaly detection using LSTM based autoencoder," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*, 2022, pp. 319-324.

[10] M. F. Mridha, A. J. Keya, M. A. Hamid, M. M. Monowar, and M. S. Rahman, "A comprehensive review on fake news detection

with deep learning," *IEEE access,* vol. 9, pp. 156151-156170, 2021.
[11] M. Chen, "Deep Learning for Fake News Detection," Stevens Institute of Technology, 2022.
[12] H. Padalko, V. Chomko, and D. Chumachenko, "A novel approach to fake news classification using LSTM-based deep learning models," *Frontiers in big Data,* vol. 6, p. 1320800, 2024.
[13] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems,* vol. 189, p. 105124, 2020.
[14] J. Li, V. Giotsas, Y. Wang, and S. Zhou, "Bgp-multipath routing in the internet," *IEEE Transactions on Network Service Management,* vol. 19, no. 3, pp. 2812-2826, 2022.
[15] R. Alkanhel, E.-S. M. El-kenawy, A. A. Abdelhamid, A. Ibrahim, M. Abotaleb, and D. S. Khafaga, "Dipper Throated Optimization for Detecting Black-Hole Attacks in MANETs," *Computers, Materials Continua,* vol. 74, no. 1, 2023.
[16] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Enhancing MANET Security Through Long Short-Term Memory-Based Trust Prediction in Location-Aided Routing Protocols," *IEEE Access,* 2025.
[17] A. H. Wheeb, R. Nordin, A. A. Samah, M. H. Alsharif, and M. A. Khan, "Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions," *Drones,* vol. 6, no. 1, p. 9, 2021.
[18] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile ad hoc NETwork (MANET) Protocols and their Applications," in *2021 5th international conference on intelligent computing and control systems (ICICCS)*, 2021, pp. 204-211.
[19] M. U. Rahman, "Investigating the effects of mobility metrics in mobile ad hoc networks," *arXiv preprint*, arXiv:.16441, 2020.
[20] S. Kaur, S. Kour, M. Singh, B. Singh, and H. Sarangal, "Performance Analysis of Diverse Mobility Speeds on MANET Routing Protocols," in *International Conference on Microelectronics, Electromagnetics and Telecommunication*, 2023, pp. 91-101: Springer.
[21] R. Ramamoorthy, "An Enhanced Location-Aided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks," *Human-Centric Intelligent Systems,* vol. 4, no. 1, pp. 25-52, 2024.
[22] V. K. Krishnamoorthy *et al.*, "Energy saving optimization technique-based routing protocol in Mobile ad-hoc network with IOT Environment," *Energies,* vol. 16, no. 3, p. 1385, 2023.
[23] S. M. Hassan, M. M. Mohamad, F. B. Muchtar, and F. B. Y. P. Dawoodi, "Enhancing MANET Security through Federated Learning and Multiobjective optimization: A Trust-aware Routing Framework," *IEEE Access,* 2024.
[24] T.-A. N. Abdali, R. Hassan, R. C. Muniyandi, A. H. Mohd Aman, Q. N. Nguyen, and A. S. Al-Khaleefa, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in manet," *Information,* vol. 11, no. 11, p. 529, 2020.
[25] F. T. Al-Dhief *et al.*, "Forest fire detection using new routing protocol," *Sensors,* vol. 22, no. 20, p. 7745, 2022.
[26] S. Kumar, R. S. Raw, and A. Bansal, "Minimize the routing overhead through 3D cone shaped location-aided routing protocol for FANETs," *International Journal of Information Technology,* vol. 13, no. 1, pp. 89-95, 2021.